Konfigurieren von PIX 5.1.x: TACACS+ und RADIUS

Inhalt

Einführung

Die RADIUS- und TACACS+-Authentifizierung kann für FTP-, Telnet- und HTTP-Verbindungen erfolgen. Die Authentifizierung für andere, weniger häufig verwendete Protokolle kann in der Regel durchgeführt werden. Die TACACS+-Autorisierung wird unterstützt. Die RADIUS-Autorisierung ist nicht aktiviert. Änderungen bei PIX 5.1 Authentication, Authorization, Accounting (AAA) gegenüber der vorherigen Version beinhalten erweiterte Authentifizierung (xauth) - Authentifizierung von IPSec-Tunneln vom Cisco Secure VPN Client 1.1.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

Konventionen

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

Hintergrundinformationen

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.
- Die Abrechnung ist das, was der Benutzer getan hat.

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

Angenommen, *einer* dieser sechs Benutzer, "Festus", ist nicht vertrauenswürdig. Sie möchten Festus erlauben, FTP zu machen, aber nicht HTTP oder Telnet nach außen. Dies bedeutet, dass *Autorisierung* hinzugefügt werden muss, d. h. die Autorisierung, *was* Benutzer zusätzlich zur Authentifizierung des Benutzers tun können. Dies gilt nur für TACACS+. Wenn wir *Autorisierung* zum PIX hinzufügen, sendet der PIX zunächst den Benutzernamen und das Kennwort von Festus an den Sicherheitsserver und sendet dann eine Autorisierungsanfrage, die dem Sicherheitsserver mitteilt, was "*Befehl*" Festus zu tun versucht. Wenn der Server korrekt eingerichtet ist, könnte Festus "ftp 1.2.3.4" erlauben, aber die Möglichkeit, HTTP oder Telnet überall.

Was der Benutzer mit Authentifizierung/Autorisierung auf

Wenn Sie versuchen, 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 den Benutzernamen. Der Benutzer muss **local_username@remote_username** als Benutzername und **local_password@remote_password** als Kennwort eingeben. Der PIX sendet den local_username und das 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 Ziel-FTP-Server 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, wird wahrscheinlich eine erneute Authentifizierung mit dem Browser durchgeführt, der den zwischengespeicherten Benutzernamen und das Kennwort an den PIX ausrichtet, der diesen dann an den Authentifizierungsserver weiterleitet. Dieses Phänomen zeigt PIX Syslog und/oder Server-Debugging. Wenn Telnet und FTP normal arbeiten, HTTP-Verbindungen jedoch nicht, dann ist dies der Grund dafür.
- **Tunnel** - Wenn versucht wird, IPSec-Datenverkehr mit dem VPN-Client in das Netzwerk zu tunneln, wird ein graues Feld für "User Authentication for New Connection" (Benutzerauthentifizierung für neue Verbindung) für Benutzername/Kennwort angezeigt.**Hinweis:** Diese Authentifizierung wird ab Cisco Secure VPN Client 1.1 unterstützt. Wenn das Menü **Hilfe > Info** die Version 2.1.x oder höher nicht anzeigt, funktioniert dies nicht.

Für alle Szenarien verwendete Sicherheitsserver-Konfigurationen

Cisco Secure UNIX TACACS-Serverkonfiguration

In diesem Abschnitt werden die Informationen zum Konfigurieren des Sicherheitsservers angezeigt.

Stellen Sie sicher, dass Sie die PIX-IP-Adresse oder den vollqualifizierten Domänennamen und -schlüssel in der CSU.cfg-Datei haben.

```
user = ddunlap {
password = clear "rtp"
default service = permit
}

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

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

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

Cisco Secure UNIX RADIUS-Serverkonfiguration

Fügen Sie über die Benutzeroberfläche die PIX-IP-Adresse und den PIX-Schlüssel der Liste Network Access Server (NAS) hinzu.

```
user=adminuser {
radius=Cisco {
check_items= {
2="all"
}
reply_attributes= {
6=6
}
}
}
```

Cisco Secure ACS für Windows 2.x RADIUS

Führen Sie diese Schritte aus, um den Cisco Secure ACS für Windows 2.x RADIUS zu konfigurieren.

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

EasyACS TACACS+

Die EasyACS-Dokumentation beschreibt die Einrichtung.

1. Klicken Sie im Gruppenbereich auf **Shell Exec**, um Exec-Berechtigungen zu gewähren.
2. Um dem PIX die Autorisierung hinzuzufügen, klicken Sie unten im Gruppensetup auf **Nicht übereinstimmende IOS-Befehle verweigern**.
3. Wählen Sie für jeden Befehl, den Sie zulassen möchten, z. B. **Telnet**, **neuen Befehl hinzufügen/bearbeiten aus**.
4. Wenn Telnetting zu bestimmten Standorten erlaubt ist, geben Sie die IP-Adresse(n) im Argumentabschnitt im Formular "permit #.#.#.#" ein. Andernfalls klicken Sie auf **Alle nicht aufgeführten Argumente zulassen**, um Telnetting zuzulassen.
5. Klicken Sie auf **Bearbeitungsbefehl beenden**.
6. Führen Sie die Schritte 1 bis 5 für jeden der zulässigen Befehle aus (z. B. Telnet, HTTP oder FTP).
7. Fügen Sie die PIX-IP im Abschnitt "GUI der NAS-Konfiguration" hinzu.

Cisco Secure 2.x TACACS+

Der Benutzer erhält ein Kennwort im Abschnitt "GUI" der Benutzereinrichtung.

1. Klicken Sie im Gruppenbereich auf **Shell Exec**, um Exec-Berechtigungen zu gewähren.
2. Um dem PIX die Autorisierung hinzuzufügen, klicken Sie unten im Gruppen-Setup auf **Nicht übereinstimmende IOS-Befehle verweigern**.
3. Wählen Sie für jeden Befehl, den Sie zulassen möchten (z. B. **Telnet**) **den Befehl Neu hinzufügen/bearbeiten aus**.
4. Um Telnet für bestimmte Standorte zuzulassen, geben Sie die IP-Adresse im Argumentabschnitt im Formular "permit #.#.#.#" ein. Um Telnetting für alle Standorte zuzulassen, 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 oder FTP).
7. Stellen Sie sicher, dass die PIX-IP-Adresse im Abschnitt "GUI der NAS-Konfiguration" hinzugefügt wird.

Konfiguration des Livingston RADIUS-Servers

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

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

RADIUS-Serverkonfiguration vermerken

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

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

TACACS+ Freeware Server-Konfiguration

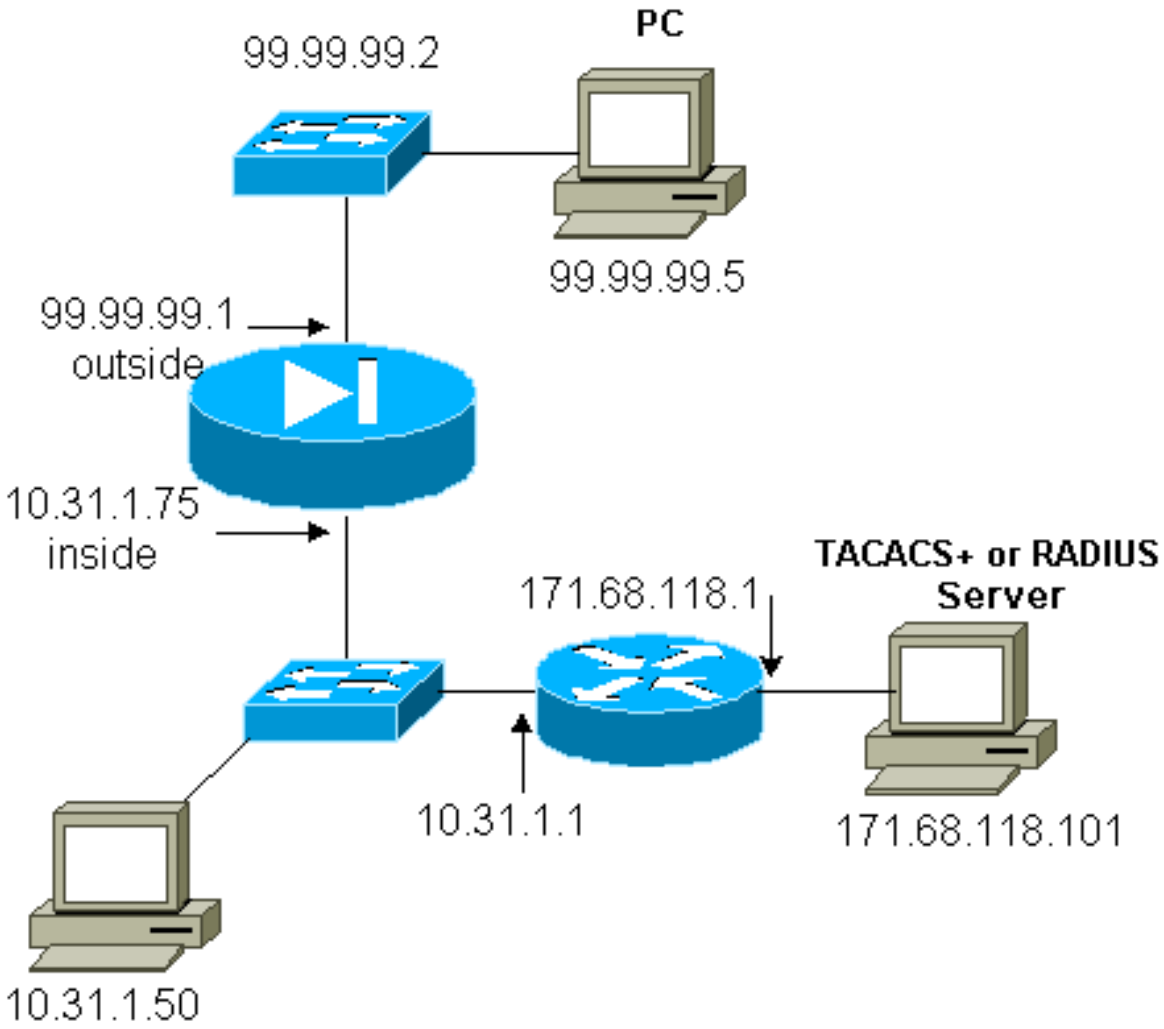
```
key = "cisco"
user = adminuser {
login = cleartext "all"
default service = permit
}

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

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

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

Debugschritte

Hinweis: Bestimmte **show**-Befehle werden vom Output Interpreter Tool (nur registrierte Kunden) unterstützt, mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- Stellen Sie sicher, dass die PIX-Konfiguration funktioniert, bevor Sie AAA hinzufügen. Wenn Sie keinen Datenverkehr weiterleiten können, bevor Sie eine Authentifizierung und Autorisierung einrichten, können Sie dies später nicht mehr tun.
- Aktivieren Sie die Protokollierung im PIX.Das Debuggen von Protokollkonsolen sollte auf einem stark ausgelasteten System nicht verwendet werden.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 (alle Server haben diese Option).

Netzwerkdiagramm



PIX-Konfiguration
PIX Version 5.1(1) nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 pix/intf2 security10 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname pix3 fixup protocol ftp 21 fixup protocol http 80 fixup protocol smtp 25 fixup protocol h323 1720 fixup protocol rsh 514 fixup protocol sqlnet 1521 names pager lines 24 no logging timestamp no logging standby **logging console debugging** no logging monitor no logging buffered no logging trap no logging history logging facility 20 logging queue 512 interface ethernet0 auto interface ethernet1 auto interface ethernet2 auto shutdown

```
mtu outside 1500
mtu inside 1500
mtu pix/intf2 1500
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
ip address pix/intf2 127.0.0.1 255.255.255.255
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address pix/intf2 0.0.0.0
arp timeout 14400
global (outside) 1 99.99.99.7-99.99.99.10 netmask
255.255.255.0
nat (inside) 1 10.31.1.0 255.255.255.0 0 0
static (inside,outside) 99.99.99.99 10.31.1.50 netmask
255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp any any
conduit permit udp any any
route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
route inside 171.68.118.0 255.255.255.0 10.31.1.1 1
route inside 171.68.120.0 255.255.255.0 10.31.1.1 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 171.68.118.101
cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101
cisco timeout 5
aaa authentication include telnet outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include telnet inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include http inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include ftp outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include ftp inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
terminal width 80
Cryptochecksum:b26b560b20e625c9e23743082484caca
: end
[OK]
```

Authentifizierungs-Debug-Beispiele aus PIX

In diesem Abschnitt werden Beispiele für Authentifizierungsdebugs für verschiedene Szenarien

veranschaulicht.

Eingehend

Der externe Benutzer unter 99.99.99.2 initiiert Datenverkehr nach 10.31.1.50 (99.99.99.99) und wird über TACACS authentifiziert (d. h. der eingehende Datenverkehr verwendet die Serverliste "AuthInbound", die den TACACS-Server 171.68.18.18 enthält. 001).

PIX Debug - Gute Authentifizierung - TACACS+

Das nachfolgende Beispiel zeigt ein PIX-Debugging mit guter Authentifizierung:

```
109001: Auth start for user '???' from
    99.99.99.2/11008 to 10.31.1.50/23
109011: Authen Session Start: user 'cse', sid 4
109005: Authentication succeeded for user 'cse'
    from 10.31.1.50/23 to 99.99.99.e
302001: Built inbound TCP connection 10 for
    faddr 99.99.99.2/11008 gaddr 99.99.)
```

PIX Debug - Schlechte Authentifizierung (Benutzername oder Kennwort) - TACACS+

Das nachfolgende Beispiel zeigt ein PIX-Debugging mit schlechter Authentifizierung (Benutzername oder Kennwort). Der Benutzer sieht drei Benutzername/Kennwort-Sets, gefolgt von der folgenden Meldung: `Fehler: Die maximale Anzahl von Versuchen wurde überschritten.`

```
109001: Auth start for user '???' from
     99.99.99.2/11010 to 10.31.1.50/23
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11010 on
     interface outside
```

PIX Debug - Can Ping Server, No Response - TACACS+

Das nachfolgende Beispiel zeigt ein PIX-Debuggen, bei dem der Server pingfähig ist, jedoch nicht mit dem PIX-Protokoll spricht. Der Benutzer sieht den Benutzernamen einmal, aber der PIX fragt nie nach einem Passwort (dies ist auf Telnet). Der Benutzer sieht `Fehler: Die maximale Anzahl von Versuchen wurde überschritten.`

```
109001: Auth start for user '???' from 99.99.99.2/11011
     to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109006: Authentication failed for user '' from 10.31.1.50/23
     to 99.99.99.2/11011 on interface outside
```

PIX Debug - Ping-Server nicht möglich - TACACS+

Das nachfolgende Beispiel zeigt ein PIX-Debuggen, bei dem der Server nicht pingbar ist. Der Benutzer sieht den Benutzernamen einmal, aber der PIX fragt nie nach einem Passwort (dies ist auf Telnet). Folgende Meldungen werden angezeigt: `Timeout für TACACS+-Server` und `Fehler: Die maximale Anzahl der Versuche wurde überschritten` (ein fehlerhafter Server wurde in der Konfiguration ausgetauscht).

```
111005: console end configuration: OK
  109001: Auth start for user '???' from
     99.99.99.2/11012 to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11012 on interface
     outside
```

PIX Debug - Gute Authentifizierung - RADIUS

Das nachfolgende Beispiel zeigt ein PIX-Debugging mit guter Authentifizierung:

```
109001: Auth start for user '???' from
     10.31.1.50/11008 to 99.99.99.2/23
  109011: Authen Session Start: user 'pixuser', sid 8
  109005: Authentication succeeded for user
     'pixuser' from 10.31.1.50/11008 to
     99.99.99.2/23 on interface inside
  302001: Built outbound TCP connection 16 for faddr
     99.99.99.2/23 gaddr 99.99.99.99/11008
     laddr 10.31.1.50/11008 (pixuser)
```

PIX Debug - Schlechte Authentifizierung (Benutzername oder Kennwort) - RADIUS

Das nachfolgende Beispiel zeigt ein PIX-Debugging mit schlechter Authentifizierung (Benutzername oder Kennwort). Der Benutzer sieht die Anfrage nach einem Benutzernamen und einem Kennwort und hat drei Möglichkeiten, diese einzugeben. Wenn der Eintrag nicht erfolgreich ist, wird die folgende Meldung angezeigt: `Fehler: Die maximale Anzahl von Versuchen wurde überschritten`.

```
109001: Auth start for user '???' from 10.31.1.50/11010
     to 99.99.99.2/23
  109006: Authentication failed for user ''
     from 10.31.1.50/11010 to 99.99.99.2/23
     on interface inside
```

PIX Debug - Can Ping Server, Daemon Down - RADIUS

Das nachfolgende Beispiel zeigt ein PIX-Debuggen, bei dem der Server pingfähig ist, der Daemon jedoch nicht verfügbar ist und nicht mit dem PIX kommuniziert. Der Benutzer sieht Benutzername, Kennwort, die Meldung `RADIUS-Server fehlgeschlagen` und den `Fehler: Die maximale Anzahl von Versuchen wurde überschritten`. Fehlermeldung.

```
109001: Auth start for user '???' from 10.31.1.50/11011
     to 99.99.99.2/23
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  1ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  09002: Auth from 10.31.1.50/11011 to 99.99.99.2/23
     failed (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11011
     to 99.99.99.2/23 on interface inside
```

PIX Debug - Nicht in der Lage, Server oder Schlüssel-/Client-Nichtübereinstimmung zu pingen - RADIUS

Das nachfolgende Beispiel zeigt ein PIX-Debuggen, bei dem der Server nicht pingbar ist oder eine Client/Schlüssel-Diskrepanz vorliegt. Der Benutzer sieht einen Benutzernamen, ein Kennwort, die Meldung `Timeout für RADIUS-Server` und den `Fehler: Max. Anzahl von Versuchen überschritten` die Meldung, dass ein fehlerhafter Server in der Konfiguration ausgetauscht wurde).

```
109001: Auth start for user '???' from 10.31.1.50/11012
     to 99.99.99.2/23
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11012
     to 99.99.99.2/23 on interface inside
```

Autorisierung hinzufügen

Wenn Sie die Autorisierung hinzufügen möchten, da die Autorisierung ohne Authentifizierung nicht gültig ist, müssen Sie die Autorisierung für denselben Quell- und Zielbereich verlangen.

```
aaa authorization telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Beachten Sie, dass Sie keine Autorisierung für ausgehende Datenverkehr hinzufügen, da ausgehender Datenverkehr mit RADIUS authentifiziert wird und die RADIUS-Autorisierung ungültig ist.

Debug-Beispiele für Authentifizierung und Autorisierung aus PIX

PIX Debug - Gute Authentifizierung und erfolgreiche Autorisierung - TACACS+

Das nachfolgende Beispiel zeigt ein PIX-Debugging mit guter Authentifizierung und erfolgreicher Autorisierung:

```
109001: Auth start for user '???' from 99.99.99.2/11016
   to 10.31.1.50/23
109011: Authen Session Start: user 'cse', Sid 11
109005: Authentication succeeded for user 'cse'
   from 10.31.1.50/23 to 99.99.99.2/11016 on interface outside
109011: Authen Session Start: user 'cse', Sid 11
109007: Authorization permitted for user 'cse' from
   99.99.99.2/11016 to 10.31.1.50/23 on interface outside
302001: Built inbound TCP connection 19 for faddr 99.99.99.2/11016
   gaddr 99.99.99.99/23 laddr 10.31.1.50/23 (cse)
```

PIX Debug - Gute Authentifizierung, fehlgeschlagene Autorisierung - TACACS+

Das nachfolgende Beispiel zeigt das PIX-Debuggen mit guter Authentifizierung, aber fehlgeschlagener Autorisierung. Hier sieht der Benutzer auch die Meldung `Error: Autorisierung verweigert.`

```
109001: Auth start for user '???' from
    99.99.99.2/11017 to 10.31.1.50/23
109011: Authen Session Start: user 'httponly',
   Sid 12
109005: Authentication succeeded for user 'httponly'
   from 10.31.1.50/23 to 99.99.99.2/11017 on
   interface outside
109008: Authorization denied for user 'httponly' from
   10.31.1.50/23 to 99.99.99.2/11017 on interface outside
```

Hinzufügen von Buchhaltung

TACACS+

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

Ausgabe von TACACS+-Freeware:

```
Tue Feb 22 08:52:20 2000  10.31.1.75 cse PIX
   99.99.99.2 start task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet
Tue Feb 22 08:52:25 2000  10.31.1.75 cse PIX
   99.99.99.2 stop task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet elapsed_time=5
   bytes_in=39 bytes_out=126
```

RADIUS

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

RADIUS-Ausgabe vermerken:

```
Tue Feb 22 08:56:17 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        User-Name = pixuser

        Tue Feb 22 08:56:24 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        Username = pixuser
        Acct-Session-Time = 6
        Acct-Input-Octets = 139
        Acct-Output-Octets = 36
```

Verwendung des Befehls Exclude

Wenn wir unserem Netzwerk einen weiteren Host hinzufügen (unter 99.99.99.100) und dieser Host vertrauenswürdig ist, können Sie diese mit den folgenden Befehlen von der Authentifizierung und Autorisierung ausschließen:

```
aaa authentication exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100
 255.255.255.255 AuthInbound

aaa authorization exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100 255.255.255.255
AuthInbound
```

Max. Sitzungen und Anzeigen angemeldeter 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 aufgrund der Art der Verbindung nicht gut. Im folgenden Beispiel wird eine andere Netzwerkkonfiguration verwendet, die Konzepte sind jedoch identisch.

Benutzer-Telnet über den PIX authentifizieren sich auf dem Weg:

```
   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 Startdatensatz, aber keinen Stoppdatensatz 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 für diesen Benutzer auf **1** festgelegt ist (vorausgesetzt, der Server unterstützt max. Sitzungen), wird die Verbindung vom Server verweigert.

Der Benutzer führt seine Telnet- oder FTP-Geschäfte auf dem Ziel-Host durch und verlässt dann die Leitung (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:

Der Benutzer wählt zwischen 171.68.118.100 und 9.9.9.25 mithilfe des 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
```

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). Ist der Benutzer immer noch bei der Website angemeldet und die Verbindung bleibt geöffnet, wenn der Benutzer die Webseite liest? Nein. Funktionieren hier die max. Sitzungen oder die Ansicht der angemeldeten Benutzer? Nein, weil die Verbindungszeit (die Zeit zwischen "Built" und "Teardown") in HTTP zu kurz ist. Der Start- und Stopp-Datensatz ist eine Sekunde. Es gibt keinen Startdatensatz ohne Stopp-Record, 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. Aufgrund der Art der HTTP-Verbindungen funktionieren jedoch keine Max-Sessions und keine Ansicht der angemeldeten Benutzer.

Authentifizierung und Aktivierung auf dem PIX selbst

Die vorige Diskussion betrifft die Authentifizierung von Telnet- (und HTTP-, FTP-) Datenverkehr über das PIX. Stellen Sie sicher, dass Telnet zu PIX ohne Authentifizierung funktioniert in:

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

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

```
aaa authentication telnet console AuthInbound
```

Wenn Benutzer Telnet an den PIX anschließen, werden sie zur Eingabe des Telnet-Kennworts (**WW**) aufgefordert. Der PIX fordert außerdem den TACACS+- oder RADIUS-Benutzernamen und das -Kennwort an. Da in diesem Fall die AuthInbound-Serverliste verwendet wird, fordert PIX den TACACS+-Benutzernamen und das TACACS+-Kennwort an.

Wenn der Server ausgefallen ist, können Sie auf das PIX zugreifen, indem Sie **pix** für den Benutzernamen und dann das enable-Kennwort (**Kennwort *unabhängig vom* Status aktivieren**) eingeben. Mit dem Befehl:

```
aaa authentication enable console AuthInbound
```

Der Benutzer wird aufgefordert, einen Benutzernamen und ein Kennwort einzugeben, die an den TACACS- oder RADIUS-Server gesendet werden. Da in diesem Fall die AuthInbound-Serverliste verwendet wird, fordert PIX den TACACS+-Benutzernamen und das TACACS+-Kennwort an.

Da das Authentifizierungspaket für "enable" mit dem Authentifizierungspaket für die Anmeldung übereinstimmt, kann der Benutzer, wenn er sich mit TACACS oder RADIUS beim PIX anmelden kann, über TACACS oder RADIUS mit demselben Benutzernamen/Kennwort aktivieren. Diesem Problem wurde die Cisco Bug-ID CSCdm47044 zugewiesen (nur registrierte Kunden).

Wenn der Server ausgefallen ist, können Sie auf den PIX-Aktivierungsmodus zugreifen, indem Sie **pix** für den Benutzernamen und das normale enable-Kennwort aus dem PIX eingeben (**Kennwort *unabhängig***). Wenn Sie **das Kennwort aktivieren*, was auch immer* nicht in der PIX-Konfiguration enthalten ist**, geben Sie **pix** als Benutzernamen ein, und drücken Sie die **Eingabetaste**. Wenn das enable-Kennwort festgelegt, aber nicht bekannt ist, muss eine

Kennwortwiederherstellungsdiskette erstellt werden, um das Kennwort zurückzusetzen.

Benutzer auffordern anzeigen

Wenn Sie den Befehl besitzen:

```
auth-prompt PIX_PIX_PIX
```

Benutzer, die den PIX durchlaufen, sehen die folgende Sequenz:

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

Bei der Ankunft am endgültigen Ziel sehen die Benutzer den Benutzernamen: und Kennwort: wird im Zielfeld 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.

Anpassen der Meldung "Erfolgreich/Fehler" für Benutzer

Wenn Sie über die Befehle verfügen:

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

sehen die Benutzer bei einer fehlgeschlagenen/erfolgreichen Anmeldung über PIX die folgende Sequenz:

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

Timeouts pro Benutzer bei Inaktivität und absoluten Zeitüberschreitungen

Diese Funktion funktioniert derzeit nicht und das Problem wurde der Cisco Bug ID CSCdp93492 zugewiesen (nur registrierte Kunden) .

Virtuelles HTTP

Wenn an Standorten außerhalb des PIX sowie auf dem PIX selbst eine Authentifizierung erforderlich ist, kann gelegentlich ein ungewöhnliches Browserverhalten beobachtet werden, da

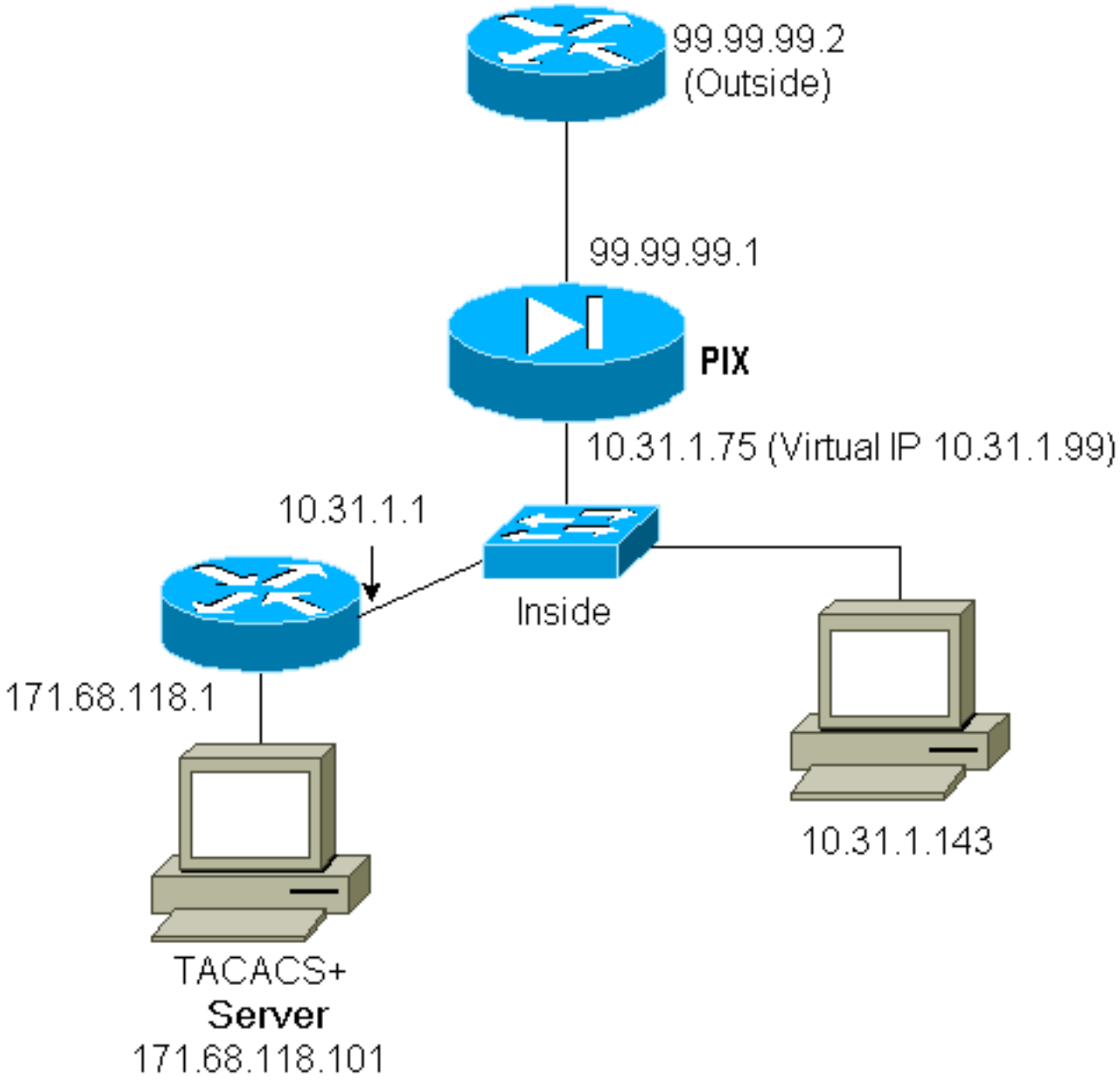
Browser den Benutzernamen und das Kennwort zwischenspeichern.

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

```
virtual http #.#.#.# [warn]
```

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.

Beispiel für ausgehenden virtuellen HTTP-Verkehr



PIX-Konfiguration Virtual HTTP Outbound:

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
global (outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0
timeout uauth 01:00:00
aaa authentication include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa-server RADIUS protocol radius
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 5
virtual http 10.31.1.99
```

Virtuelles Telnet

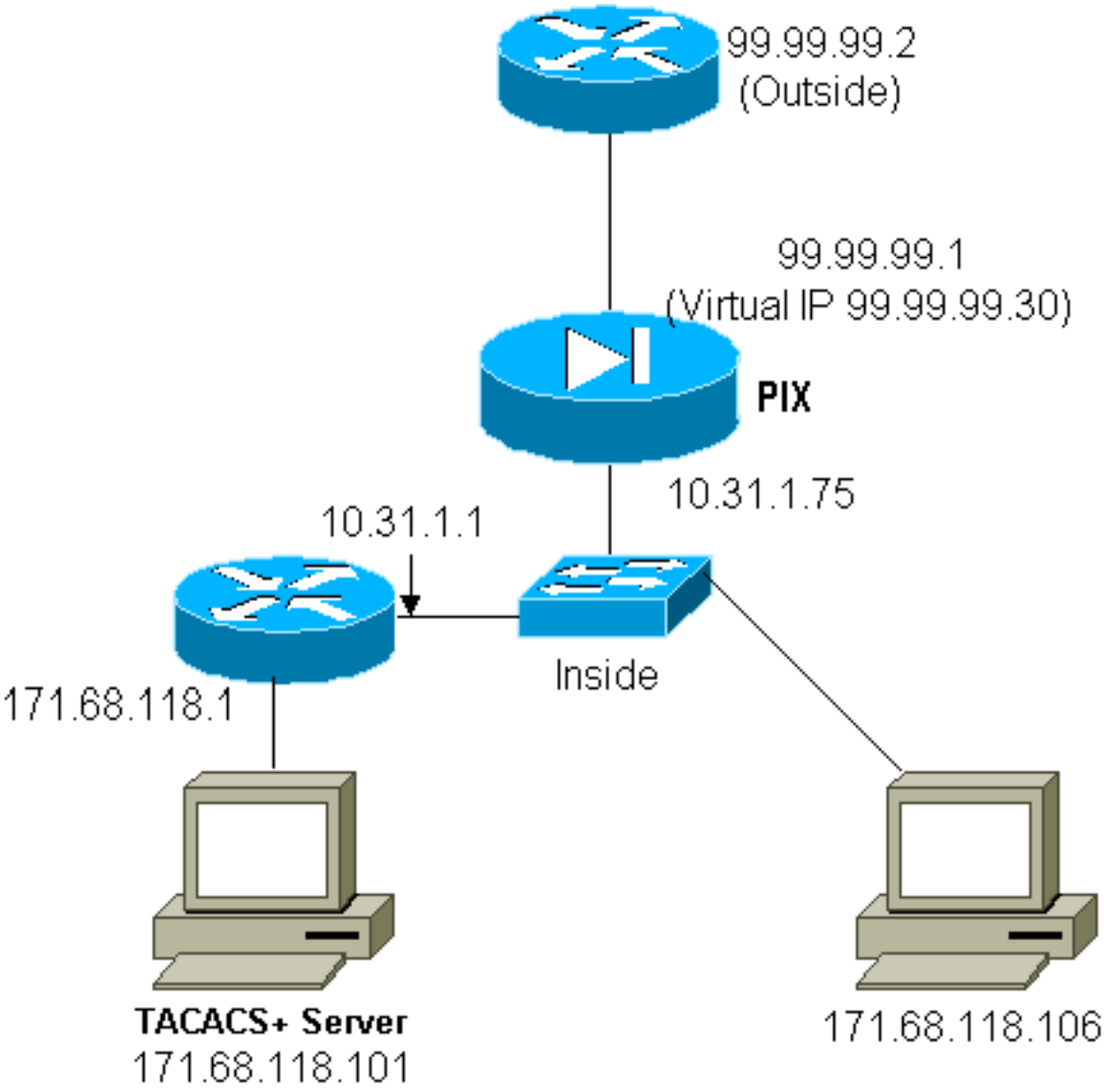
Es ist möglich, den PIX so zu konfigurieren, dass alle ein- und ausgehenden Nachrichten authentifiziert werden. Es ist jedoch nicht empfehlenswert, da einige Protokolle wie E-Mail nicht einfach authentifiziert werden können. Wenn ein Mail-Server und Client versuchen, über das PIX zu kommunizieren, wenn der gesamte Datenverkehr über das PIX authentifiziert wird, zeigt das PIX-Syslog für nicht authentifizierbare Protokolle folgende Meldungen an:

```
109013: User must authenticate before using
    this service
109009: Authorization denied from 171.68.118.106/49
    to 9.9.9.10/11094    (not authenticated)
```

Wenn jedoch wirklich eine Authentifizierung eines ungewöhnlichen Dienstes erforderlich ist, kann dies mithilfe des **virtuellen telnet-**Befehls erfolgen. Dieser Befehl ermöglicht die Authentifizierung der virtuellen Telnet-IP-Adresse. Nach dieser Authentifizierung kann der Datenverkehr für den ungewöhnlichen Dienst an den echten Server weitergeleitet werden.

In diesem Beispiel soll der TCP-Port 49-Datenverkehr von dem externen Host 99.99.99.2 an den internen Host 171.68.118.106 fließen. Da dieser Datenverkehr nicht wirklich authentifizierbar ist, richten Sie ein virtuelles Telnet ein. Für virtuelles Telnet muss ein statisches Protokoll zugeordnet sein. Hier sind sowohl 99.99.99.20 als auch 171.68.118.20 virtuelle Adressen.

Virtual Telnet Inbound



PIX-Konfiguration Virtual Telnet Inbound

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
static (inside,outside) 99.99.99.20 171.68.118.20 netmask 255.255.255.255 0 0
static (inside,outside) 99.99.99.30 171.68.118.106 netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.20 eq telnet any
conduit permit tcp host 99.99.99.30 eq tacacs any
aaa-server TACACS+ protocol tacacs+
aaa-server Incoming protocol tacacs+
aaa-server Incoming (inside) host 171.68.118.101 cisco timeout 5
aaa authentication include telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Incoming
aaa authentication include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Incoming
virtual telnet 99.99.99.20
```

PIX Debug Virtual Telnet Inbound

Der Benutzer unter 99.99.99.2 muss sich zunächst mithilfe von Telnetting an die Adresse 99.99.99.20 auf dem PIX authentifizieren:

```
109001: Auth start for user '???' from
    99.99.99.2/22530 to 171.68.118.20/23
 109011: Authen Session Start: user 'cse', Sid 13
 109005: Authentication succeeded for user
    'cse' from 171.68.118.20/23 to
    99.99.99.2/22530 on interface outside
```

Nach erfolgreicher Authentifizierung zeigt der Befehl **show uauth** an, dass der Benutzer die Zeit auf dem Messgerät hat:

```
pixfirewall# show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 99.99.99.2, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

Wenn das Gerät unter 99.99.99.2 TCP/49-Datenverkehr an das Gerät unter 171.68.118.106 senden möchte:

```
302001: Built inbound TCP connection 16
    for faddr 99.99.99.2/11054 gaddr
    99.99.99.30/49 laddr 171.68.118.106/49 (cse)
```

Autorisierung kann hinzugefügt werden:

```
aaa authorization include tcp/49 inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Wenn TCP/49-Datenverkehr über das PIX versucht wird, sendet das PIX außerdem die Autorisierungsabfrage an den Server:

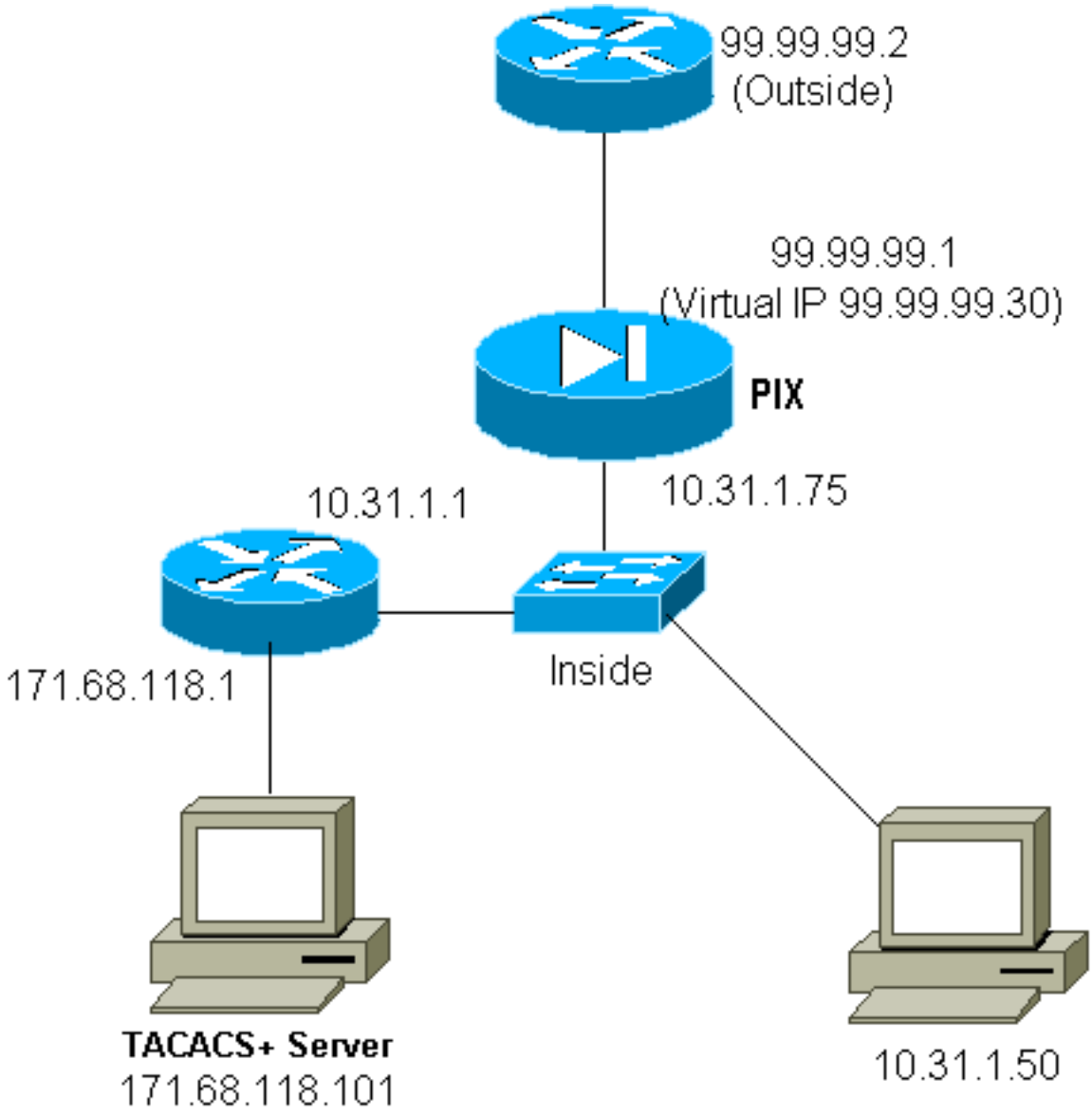
```
109007: Authorization permitted for user 'cse'
    from 99.99.99.2/11057 to 171.68.118.106/49
    on interface outside
```

Auf dem TACACS+-Server wird Folgendes angezeigt:

```
service=shell,
  cmd=tcp/49,
  cmd-arg=171.68.118.106
```

Virtuelles Telnet - Ausgehend

Da ausgehender Datenverkehr standardmäßig zulässig ist, ist für die Verwendung von ausgehenden virtuellen Telnet-Verbindungen kein statisches Gerät erforderlich. Im folgenden Beispiel authentifiziert der interne Benutzer 10.31.1.50 Telnets zu virtual 99.99.99.30 und erhält eine Authentifizierung. Die Telnet-Verbindung wird sofort getrennt. Nach der Authentifizierung ist TCP-Datenverkehr vom 10.31.1.50 zum Server unter 99.99.99.2 zulässig:



PIX Configuration Virtual Telnet Outbound:

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
global (outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0
timeout uauth 0:05:00 absolute
aaa-server RADIUS protocol radius
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 5
aaa authentication include telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include tcp/49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
virtual telnet 99.99.99.30
```

Hinweis: Es gibt keine Autorisierung, da es sich um RADIUS handelt.

PIX Debug Virtual Telnet Outbound:

```
109001: Auth start for user '???' from 10.31.1.50/11034
    to 99.99.99.30/23
```

```
109011: Authen Session Start: user 'pixuser', Sid 16
109005: Authentication succeeded for user 'pixuser'
   from 10.31.1.50/11034 to 99.99.99.30/23 on interface
   inside
302001: Built outbound TCP connection 18 for faddr
   99.99.99.2/49 gaddr 99.99.99.8/11036 laddr
   10.31.1.50/11036 (pixuser)
302002: Teardown TCP connection 18 faddr 99.99.99.2/49
   gaddr 99.99.99.8/11036 laddr 10.31.1.50/11036
   duration 0:00:02 bytes 0 (pixuser)
```

Logout für virtuelles Telnet

Wenn Benutzer Telnet zur virtuellen Telnet-IP-Adresse wechseln, wird der Befehl **show uauth** angezeigt. Wenn die Benutzer verhindern möchten, dass Datenverkehr nach Beendigung der Sitzungen weitergeleitet wird, wenn noch Zeit in der Warteschlange verbleibt, müssen sie erneut Telnet zur virtuellen Telnet-IP-Adresse verbinden. Dadurch wird die Sitzung deaktiviert.

Nach der ersten Authentifizierung:

```
pix3# show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'pixuser' at 10.31.1.50, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
pix3# 109001: Auth start for user 'pixuser' from
   10.31.1.50/11038 to 99.99.99.30/23
109005: Authentication succeeded for user 'pixuser'
   from 10.31.1.50/11038 to 99.99.99.30/23 on
   interface inside
```

Nach der zweiten Authentifizierung (d. h., das Loch wird geschlossen):

```
pix3# show uauth
                        Current    Most Seen
Authenticated Users       0          2
Authen In Progress        0          1
```

Port-Autorisierung

Die Autorisierung ist für Port-Bereiche (wie TCP/30-100) zulässig. Wenn auf dem PIX virtuelles Telnet konfiguriert und für einen Port-Bereich autorisiert wird, gibt das PIX nach dem Öffnen des Lochs mit virtuellem Telnet einen **tcp/30-100-**Befehl für die Autorisierung an den TACACS+-Server aus:

```
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.75 host 99.99.99.2
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0
virtual telnet 99.99.99.75
aaa authentication include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization include tcp/30-100 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
virtual telnet 99.99.99.30
```

TACACS+ Freeware Server-Konfiguration:

```
user = anyone {
         login = cleartext "anyone"
         cmd = tcp/30-100 {
         permit 10.31.1.50
         }
         }
```

AAA-Abrechnung für Datenverkehr außer HTTP, FTP und Telnet

Nachdem sichergestellt wurde, dass virtuelles Telnet TCP/49-Datenverkehr zum Host im Netzwerk zulässt, entschieden wir uns für eine Berücksichtigung dieser Tatsache. Daher haben wir Folgendes hinzugefügt:

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

Dies führt dazu, dass bei der Übertragung des TCP/49-Datenverkehrs der Datensatz für die Accounting-Daten gekürzt wird (dieses Beispiel stammt von der Freeware TACACS+):

```
Sun Feb 27 05:24:44 2000 10.31.1.75 cse PIX
    99.99.99.2 start task_id=0x14 foreign_ip=99.99.99.2 local_ip=171.68.118.106
    cmd=tcp/49
```

Erweiterte Authentifizierung (Xauth)

Beispielkonfigurationen

- Terminierende IPSec-Tunnel auf mehreren Cisco Secure PIX Firewall-Schnittstellen mit Xauth
- IPSec zwischen der Cisco Secure PIX Firewall und einem VPN-Client mit erweiterter Authentifizierung

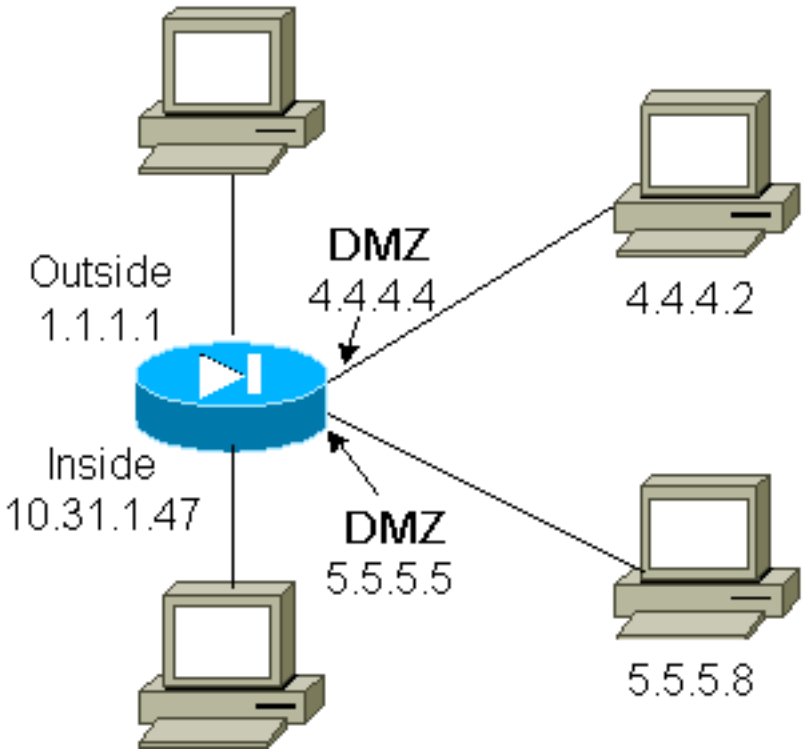
Authentifizierung auf der DMZ

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 unserem PIX ist Folgendes möglich:

```
least secure

PIX outside (security0) = 1.1.1.1

pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2

pix/intf5 (DMZ - security25) = 5.5.5.5 & device 5.5.5.8

(static to 4.4.4.15)
```

```
PIX inside (security100) = 10.31.1.47

 most secure
```

Netzwerkdiagramm



PIX-Konfiguration

Wir möchten den Telnet-Datenverkehr zwischen pix/intf4 und pix/intf5 authentifizieren:

```
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
ip address outside 1.1.1.1 255.255.255.0
ip address inside 10.31.1.47 255.255.255.0
(ip address pix/intf2 127.0.0.1 255.255.255.255
ip address pix/intf3 127.0.0.1 255.255.255.255)
ip address pix/intf4 4.4.4.4 255.255.255.0
ip address pix/intf5 5.5.5.5 255.255.255.0
static (pix/intf5,pix/intf4) 4.4.4.15 5.5.5.8 netmask 255.255.255.255 0 0
aaa authentication telnet pix/intf4 5.5.5.0 255.255.255.0
4.4.4.0 255.255.255.0 AuthInbound
aaa authentication telnet pix/intf5 5.5.5.0 255.255.255.0
4.4.4.0 255.255.255.0 AuthInbound
aaa-server TACACS+ protocol tacacs+
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
```

Xauth Accounting

Wenn der Befehl **sysopt connection permit-ipsec**, nicht der **sysopt ipsec pl-kompatible** Befehl, im PIX mit xauth konfiguriert ist, gilt das Accounting für TCP-Verbindungen, jedoch nicht für ICMP oder UDP.

Zugehörige Informationen

- PIX-Produktsupport-Seite
- PIX-Befehlsreferenz
- RADIUS-Support-Seite
- Anforderungen für Kommentare (RFCs)
- Support-Seite für Cisco Secure UNIX
- Support-Seite für Cisco Secure ACS für Windows
- Technischer Support - Cisco Systems