PIX 6.2: Konfigurationsbeispiel für Authentifizierungs- und Autorisierungsbefehle

Inhalt

Einführung

Die PIX-Befehlsautorisierung und die Erweiterung der lokalen Authentifizierung wurden in Version 6.2 eingeführt. Dieses Dokument enthält ein Beispiel für die Einrichtung auf einem PIX. Zuvor verfügbare Authentifizierungsfunktionen sind noch verfügbar, werden aber in diesem Dokument nicht behandelt (z. B. Secure Shell (SSH), IPsec-Clientverbindung von einem PC usw.). Die ausgeführten Befehle können lokal auf dem PIX oder remote über TACACS+ gesteuert werden. Die RADIUS-Befehlsautorisierung wird nicht unterstützt. Dies ist eine Einschränkung des RADIUS-Protokolls.

Die lokale Befehlsautorisierung erfolgt durch die Zuweisung von Befehlen und Benutzern zu Berechtigungsebenen.

Die Remote-Befehlsautorisierung erfolgt über einen TACACS+-Server (Authentication, Authorization, Accounting - AAA). Wenn ein Server nicht erreichbar ist, können mehrere AAA-Server definiert werden.

Die Authentifizierung funktioniert auch mit zuvor konfigurierten IPSec- und SSH-Verbindungen. Für die SSH-Authentifizierung muss der folgende Befehl ausgeführt werden:

```
aaa authentication ssh console <LOCAL | server_tag>
```

Hinweis: Wenn Sie eine TACACS+- oder RADIUS-Servergruppe für die Authentifizierung verwenden, können Sie das PIX so konfigurieren, dass die lokale Datenbank als **FALLBACK-**Methode verwendet wird, wenn der AAA-Server nicht verfügbar ist.

Zum Beispiel

```
pix(config)#aaa authentication ssh console TACACS+ LOCAL
```

Sie können auch die lokale Datenbank als Hauptauthentifizierungsmethode (ohne Fallback) verwenden, wenn Sie nur LOCAL eingeben.

Führen Sie diesen Befehl beispielsweise aus, um ein Benutzerkonto in der lokalen Datenbank zu definieren und eine lokale Authentifizierung für eine SSH-Verbindung durchzuführen:

```
pix(config)#aaa authentication ssh console LOCAL
```

Unter How To Perform Authentication and Enabling on the Cisco Secure PIX Firewall (5.2 bis 6.2) finden Sie weitere Informationen zum Erstellen eines AAA-authentifizierten Zugriffs auf eine PIX-Firewall, die die PIX-Softwareversion 5.2 bis 6.2 ausführt, sowie weitere Informationen zur Aktivierung der Authentifizierung, Syslogging und Zugriffsberechtigungen, wenn der AAA-Server ausfällt.

Weitere Informationen finden Sie unter PIX/ASA: Cut-Through-Proxy für Netzwerkzugriff mit TACACS+ und RADIUS-Server-Konfigurationsbeispiel für weitere Informationen zum Erstellen eines AAA-authentifizierten (Cut-Through-Proxy) Zugriffs auf eine PIX-Firewall, die PIX-Softwareversionen 6.3 und höher ausführt.

Wenn die Konfiguration ordnungsgemäß durchgeführt wurde, sollten Sie nicht aus dem PIX ausgesperrt werden. Wenn die Konfiguration nicht gespeichert wird, sollte der PIX-Neustart in den Zustand vor der Konfiguration zurückversetzt werden. Wenn der Zugriff auf das PIX aufgrund von Fehlkonfigurationen nicht möglich ist, finden Sie weitere Informationen unter Verfahren zur Kennwortwiederherstellung und AAA-Konfigurationswiederherstellung für PIX.

Bevor Sie beginnen

Konventionen

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

Voraussetzungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- PIX Software Version 6.2
- Cisco Secure ACS für Windows Version 3.0 (ACS)
- Cisco Secure ACS für UNIX (CSUnix) Version 2.3.6

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Tests vor dem Hinzufügen von Authentifizierung/Autorisierung

Stellen Sie vor der Implementierung der neuen 6.2-Authentifizierungs-/Autorisierungsfunktionen sicher, dass Sie derzeit mithilfe der folgenden Befehle Zugriff auf das PIX erhalten:

```
!--- IP range allowed to Telnet to the PIX (values depend on network). telnet 172.18.124.0
255.255.255.0
!--- Telnet password. passwd <password>
!--- Enable password. enable password <password>
```

Privilegieneinstellungen verstehen

Die meisten Befehle in PIX haben Level 15, einige sind jedoch auf Stufe 0 eingestellt. Um die aktuellen Einstellungen für alle Befehle anzuzeigen, verwenden Sie den folgenden Befehl:

```
show privilege all
```

Die meisten Befehle befinden sich standardmäßig auf Ebene 15, wie in diesem Beispiel gezeigt:

```
privilege configure level 15 command route
```

Einige Befehle befinden sich auf Ebene 0, wie in diesem Beispiel gezeigt:

```
privilege show level 0 command curpriv
```

Der PIX kann im Aktivierungs- und Konfigurationsmodus betrieben werden. Einige Befehle, z. B. **die Protokollierung anzeigen**, sind in beiden Modi verfügbar. Um Berechtigungen für diese Befehle festzulegen, müssen Sie den Modus angeben, in dem der Befehl vorhanden ist, wie im Beispiel gezeigt. Die andere Modusoption ist **enable**. Sie erhalten die `Protokollierung ist ein Befehl in mehreren Modi` Fehlermeldung `verfügbar`. Wenn Sie den Modus nicht konfigurieren, verwenden Sie den Befehl **[enable|configure]**:

```
privilege show level 5 mode configure command logging
```

Diese Beispiele beziehen sich auf den Befehl **clock**. Verwenden Sie diesen Befehl, um die aktuellen Einstellungen für den Befehl **clock** zu bestimmen:

```
show privilege command clock
```

Die Ausgabe des Befehls **show privilege clock** zeigt, dass der Befehl **clock** in den folgenden drei Formaten vorhanden ist:

```
!--- Users at level 15 can use the show clock command.

privilege show level 15 command clock
!--- Users at level 15 can use the clear clock command.

Privilege clear level 15 command clock
!--- Users at level 15 can configure the clock !--- (for example, clock set 12:00:00 Jan 01
2001).

privilege configure level 15 command clock
```

Authentifizierung/Autorisierung - Lokale Benutzernamen

Bevor Sie die Berechtigungsebene des Befehls **clock** ändern, müssen Sie zum Konsolenport gehen, um einen administrativen Benutzer zu konfigurieren und die LOKALE Anmeldeauthentifizierung zu aktivieren, wie in diesem Beispiel gezeigt:

```
GOSS(config)# username poweruser password poweruser privilege 15
GOSS(config)# aaa-server LOCAL protocol local
GOSS(config)# aaa authentication telnet console LOCAL
```

Das PIX bestätigt das Hinzufügen des Benutzers, wie im folgenden Beispiel gezeigt:

```
GOSS(config)# 502101: New user added to local dbase:
      Uname: poweruser Priv: 15 Encpass: Nimjl8wRa7VAmpm5
```

Der Benutzer "poweruser" sollte Telnet in das PIX integrieren und mit dem vorhandenen lokalen PIX enable password (dem Passwort aus dem **enable password <*password*>** Befehl) aktivieren können.

Sie können mehr Sicherheit hinzufügen, indem Sie Authentifizierung für die Aktivierung hinzufügen, wie in diesem Beispiel gezeigt:

```
GOSS(config)# aaa authentication enable console LOCAL
```

Dazu muss der Benutzer das Kennwort sowohl für die Anmeldung als auch für die Aktivierung eingeben. In diesem Beispiel wird das Kennwort "poweruser" sowohl für die Anmeldung als auch für die Aktivierung verwendet. Der Benutzer "poweruser" sollte Telnet in den PIX integrieren und auch mit dem lokalen PIX-Kennwort aktivieren können.

Wenn Sie möchten, dass einige Benutzer nur bestimmte Befehle verwenden können, müssen Sie einen Benutzer mit geringeren Berechtigungen einrichten, wie in diesem Beispiel gezeigt:

```
GOSS(config)# username ordinary password ordinary privilege 9
```

Da praktisch alle Ihre Befehle standardmäßig auf Stufe 15 stehen, müssen Sie einige Befehle auf Stufe 9 herabsetzen, damit "normale" Benutzer sie ausgeben können. In diesem Fall soll der Benutzer der Stufe 9 den Befehl **show clock** verwenden, die Uhr jedoch nicht neu konfigurieren können, wie in diesem Beispiel gezeigt:

```
GOSS(config)# privilege show level 9 command clock
```

Sie müssen sich auch vom PIX abmelden können (der Benutzer kann sich auf Ebene 1 oder 9 befinden, wenn er dies tun möchte), wie in diesem Beispiel gezeigt:

```
GOSS(config)# privilege configure level 1 command logout
```

Der Benutzer muss den Befehl **enable** verwenden können (der Benutzer befindet sich auf Ebene 1, wenn er dies versucht), wie in diesem Beispiel gezeigt:

```
GOSS(config)# privilege configure level 1 mode enable command enable
```

Wenn Sie den Befehl **disable** auf die Ebene 1 verschieben, kann jeder Benutzer zwischen den Ebenen 2 und 15 den Aktivierungsmodus verlassen, wie in diesem Beispiel gezeigt:

```
GOSS(config)# privilege configure level 1 command disable
```

Wenn Sie Telnet als Benutzer "normal" eingeben und als gleichen Benutzer aktivieren (das Kennwort ist auch "normal"), sollten Sie den **Befehl "configure level 1" deaktivieren** verwenden, wie in diesem Beispiel gezeigt:

```
GOSS# show curpriv
Username : ordinary
Current privilege level : 9
Current Mode/s : P_PRIV
```

Wenn Sie die ursprüngliche Sitzung immer noch geöffnet haben (die Sitzung vor dem Hinzufügen einer Authentifizierung), weiß PIX möglicherweise nicht, wer Sie sind, da Sie sich ursprünglich nicht mit einem Benutzernamen angemeldet haben. Wenn dies der Fall ist, verwenden Sie den Befehl **debug**, um Meldungen über den Benutzer "enable_15" oder "enable_1" anzuzeigen, wenn kein zugewiesener Benutzername vorhanden ist. Daher muss Telnet vor der Konfiguration der Befehlsautorisierung als Benutzer "poweruser" (Benutzer der Stufe 15) in das PIX-System integriert werden, da Sie sicherstellen müssen, dass das PIX den zu testenden Befehlen einen

Benutzernamen zuordnen kann. Sie können die Befehlsautorisierung mithilfe des folgenden Befehls testen:

```
GOSS(config)# aaa authorization command LOCAL
```

Der Benutzer "poweruser" sollte in der Lage sein, alle Befehle einzuschalten, zu aktivieren und auszuführen. Der Benutzer "normal" sollte die Befehle **show clock**, **enable**, **disable** und **login** verwenden können, jedoch keine weiteren Befehle, wie im folgenden Beispiel gezeigt:

```
GOSS# show xlate
Command authorization failed
```

Authentifizierung/Autorisierung mit einem AAA-Server

Sie können Benutzer auch mithilfe eines AAA-Servers authentifizieren und autorisieren. TACACS+ funktioniert am besten, da eine Befehlsautorisierung möglich ist, aber RADIUS auch verwendet werden kann. Überprüfen Sie, ob auf dem PIX frühere AAA-Telnet-/Konsolenbefehle vorhanden sind (falls der **LOKALE AAA-**Befehl bereits verwendet wurde), wie im folgenden Beispiel gezeigt:

```
GOSS(config)# show aaa
AAA authentication telnet console LOCAL
AAA authentication enable console LOCAL
AAA authorization command LOCAL
```

Wenn es bereits AAA-Telnet-/Konsolenbefehle gibt, entfernen Sie diese mithilfe der folgenden Befehle:

```
GOSS(config)# no aaa authorization command LOCAL
GOSS(config)# no aaa authentication telnet console LOCAL
GOSS(config)# no aaa authentication enable console LOCAL
```

Testen Sie wie beim Konfigurieren der lokalen Authentifizierung mithilfe dieser Befehle, um sicherzustellen, dass die Benutzer Telnet in das PIX-System integrieren können.

```
telnet 172.18.124.0 255.255.255.0
!--- IP range allowed to telnet to the PIX (values would depend on network). passwd <password>
!--- Telnet password. Enable password <password>
!--- Enable password.
```

Konfigurieren Sie das PIX für die Authentifizierung/Autorisierung mit einem AAA-Server, je nachdem, welchen Server Sie verwenden.

ACS - TACACS+

Konfigurieren Sie den ACS für die Kommunikation mit dem PIX, indem Sie das PIX in der Netzwerkkonfiguration mithilfe von TACACS+ (für Cisco IOS®-Software) definieren. Die Konfiguration des ACS-Benutzers hängt von der Konfiguration des PIX ab. Der ACS-Benutzer sollte mindestens einen Benutzernamen und ein Kennwort einrichten.

Verwenden Sie auf dem PIX die folgenden Befehle:

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server TACSERVER protocol tacacs+
GOSS(config)# aaa-server TACSERVER (inside) host   timeout 10
GOSS(config)# aaa authentication telnet console TACSERVER
```

An diesem Punkt sollte der ACS-Benutzer Telnet in das PIX integrieren, es mit dem vorhandenen enable-Kennwort auf dem PIX aktivieren und alle Befehle ausführen können. Gehen Sie wie folgt vor:

1. Wenn die PIX-Authentifizierung mit ACS aktiviert werden muss, wählen Sie **Schnittstellenkonfiguration > Erweiterte TACACS+-Einstellungen aus**.
2. Aktivieren Sie das Kontrollkästchen **Erweiterte TACACS+-Funktionen in erweiterten Konfigurationsoptionen**.
3. Klicken Sie auf **Senden**. Die erweiterten TACACS+-Einstellungen werden jetzt unter der Benutzerkonfiguration angezeigt.
4. Legen Sie die maximale Berechtigung für einen AAA-Client auf Stufe 15 fest.
5. Wählen Sie das Kennwortschema enable für den Benutzer aus (das die Konfiguration eines separaten enable-Kennworts beinhalten kann).
6. Klicken Sie auf **Senden**.

Um die Authentifizierung über TACACS+ in PIX zu aktivieren, verwenden Sie den folgenden Befehl:

```
GOSS(config)# aaa authentication enable console TACSERVER
```

An diesem Punkt sollte der ACS-Benutzer Telnet in das PIX integrieren und mit dem in ACS konfigurierten enable-Kennwort aktivieren können.

Vor dem Hinzufügen der PIX-Befehlsautorisierung muss ACS 3.0 gepatcht werden. Sie können den Patch vom Software Center herunterladen (nur registrierte Kunden). Weitere Informationen zu diesem Patch finden Sie unter Cisco Bug ID CSCdw78255 (nur registrierte Kunden) .

Die Authentifizierung muss vor der Befehlsautorisierung funktionieren. Wenn eine Befehlsautorisierung mit ACS erforderlich ist, wählen Sie **Schnittstellenkonfiguration > TACACS+ (Cisco) > Shell (exec) für Benutzer und/oder Gruppe aus,** und klicken Sie auf **Submit (Senden)**. Die Shell-Befehls-Autorisierungseinstellungen sind jetzt unter der Benutzer- oder Gruppenkonfiguration sichtbar.

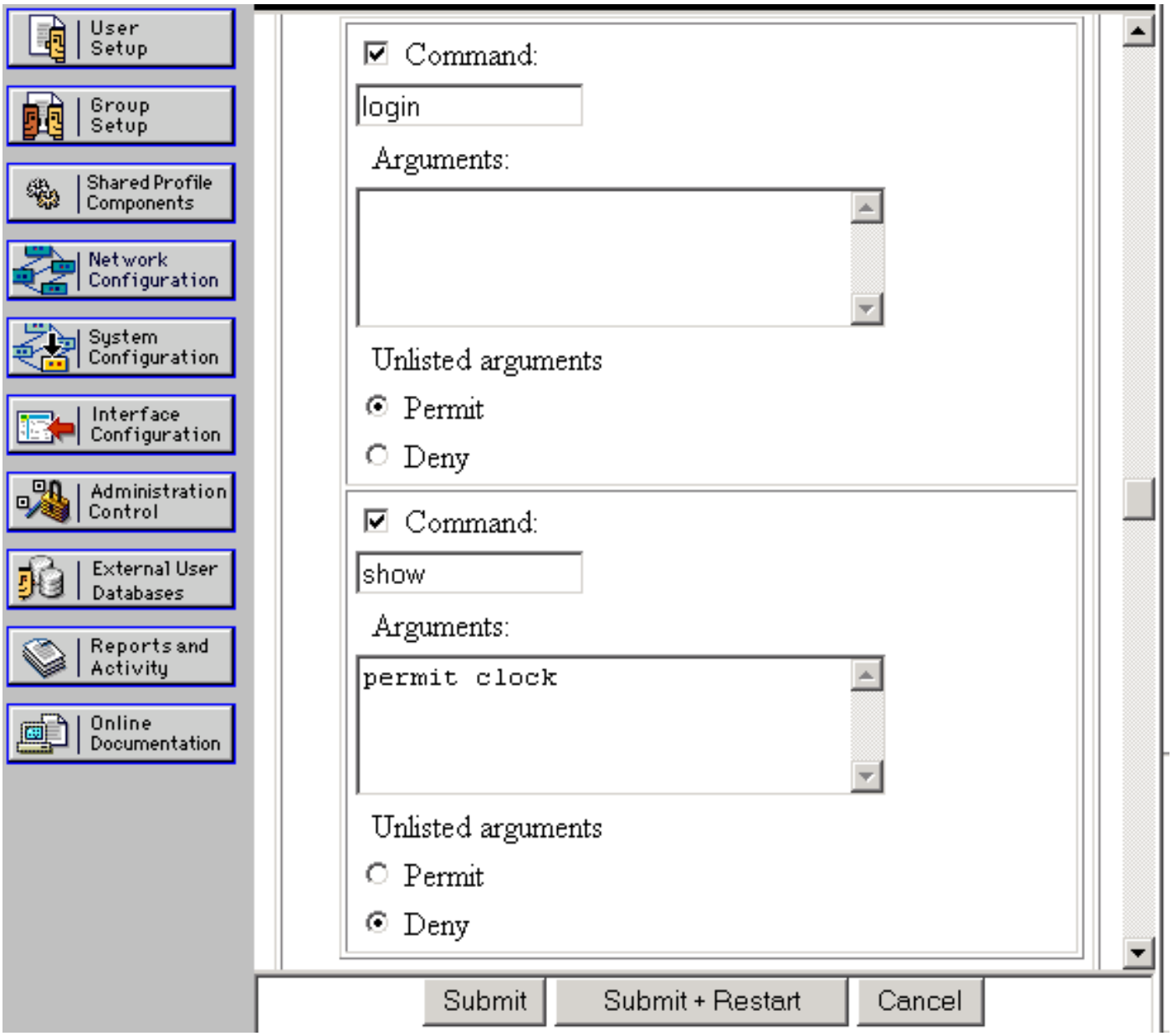
Es empfiehlt sich, mindestens einen leistungsstarken ACS-Benutzer für die Befehlsautorisierung einzurichten und unerreichte Cisco IOS-Befehle zuzulassen.

Andere ACS-Benutzer können mithilfe der Befehlsautorisierung eingerichtet werden, indem eine Teilmenge von Befehlen zugelassen wird. In diesem Beispiel werden folgende Schritte ausgeführt:

1. Wählen Sie Gruppeneinstellungen aus dem Dropdown-Feld, um die gewünschte Gruppe zu suchen.
2. Klicken Sie auf **Einstellungen bearbeiten**.
3. Wählen Sie **Shell Command Authorization Set aus**.

4. Klicken Sie auf die Schaltfläche **Command**.
5. Geben Sie **login ein**.
6. Wählen Sie unter Nicht aufgeführte Argumente die Option Zulassen aus.
7. Wiederholen Sie diesen Vorgang für die Befehle **Abmelden**, **Aktivieren** und **Deaktivieren**.
8. Wählen Sie Shell Command Authorization Set aus.
9. Klicken Sie auf die Schaltfläche **Command**.
10. **Entershow**.
11. Geben Sie unter Argumente die **Genehmigungsuhr ein**.
12. Wählen Sie Ablehnen für nicht aufgeführte Argumente aus.
13. Klicken Sie auf **Senden**.

Hier ein Beispiel für diese Schritte:



Wenn Sie Ihre ursprüngliche Sitzung immer noch geöffnet haben (die Sitzung vor dem Hinzufügen einer Authentifizierung), weiß PIX möglicherweise nicht, wer Sie sind, da Sie sich ursprünglich nicht mit einem ACS-Benutzernamen angemeldet haben. Wenn dies der Fall ist, verwenden Sie den Befehl **debug**, um Meldungen über den Benutzer "enable_15" oder "enable_1" anzuzeigen, wenn kein Benutzername zugeordnet ist. Sie müssen sicherstellen, dass das PIX den zu testenden Befehlen einen Benutzernamen zuordnen kann. Hierzu können Sie Telnet in das PIX als Benutzer der Stufe 15 ACS einbinden, bevor Sie die Befehlsautorisierung konfigurieren. Sie

können die Befehlsautorisierung mithilfe des folgenden Befehls testen:

```
aaa authorization command TACSERVER
```

An diesem Punkt sollten Sie einen Benutzer haben, der alle Befehle einbinden, aktivieren und verwenden kann, und einen zweiten Benutzer, der nur fünf Befehle ausführen kann.

CSUnix - TACACS+

Konfigurieren Sie CSUnix so, dass die Kommunikation mit dem PIX wie mit jedem anderen Netzwerkgerät erfolgt. Die Konfiguration des CSUnix-Benutzers hängt von der Konfiguration des PIX ab. Der CSUnix-Benutzer sollte mindestens mit einem Benutzernamen und einem Kennwort eingerichtet werden. In diesem Beispiel wurden drei Benutzer eingerichtet:

```
!--- This is our "poweruser" who can enable, use all commands, and log in. !--- The login
password is in the 'clear "*********"' statement. !--- The enable password is in the 'clear
"*********" 15' statement. user = pixtest{ password = clear "*********" privilege = clear
"*********" 15 service=shell { default cmd=permit default attribute=permit } } !--- This user can
Telnet in, enable, and use four commands !--- (such as show clock, logout, exit, and enable). !-
-- The login password is in the 'clear "*********"' statement. !--- The enable password is in the
'clear "*********" 15' statement.

user = limitpix{
password = clear "*********"
privilege = clear "*********" 15
service=shell {
cmd=show {
permit "clock"
}
cmd=logout {
permit ".*"
}
cmd=enable {
permit ".*"
}
cmd=exit {
permit ".*"
}
}
}

 !--- This user can Telnet in, but not enable. This user can use any !--- show commands in non-
enable mode as well as logout, exit, and ?.

user = oneuser{
password = clear "*********"
service=shell {
cmd=show {
permit ".*"
}
cmd=logout {
permit ".*"
}
cmd="?" {
permit ".*"
}
```

```
cmd=exit {
permit ".*"
}
}
}
```

Verwenden Sie auf dem PIX die folgenden Befehle:

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server TACSERVER protocol tacacs+
GOSS(config)# aaa-server TACSERVER (inside) host
```

```
GOSS(config)# aaa authentication telnet console TACSERVER
```

Zu diesem Zeitpunkt sollte jeder CSUnix-Benutzer Telnet in das PIX-System einbinden, das vorhandene enable-Kennwort auf dem PIX aktivieren und alle Befehle verwenden können.

Aktivieren Sie die Authentifizierung über TACACS+ in PIX:

```
GOSS(config)# aaa authentication enable console TACSERVER
```

An diesem Punkt sollten CSUnix-Benutzer, die "privilege 15"-Kennwörter haben, Telnet in den PIX integrieren und mit diesen "enable"-Kennwörtern aktivieren können.

Wenn Sie Ihre ursprüngliche Sitzung immer noch geöffnet haben (die Sitzung vor dem Hinzufügen einer Authentifizierung), weiß PIX möglicherweise nicht, wer Sie sind, da Sie sich ursprünglich nicht mit einem Benutzernamen angemeldet haben. In diesem Fall kann der Befehl **debug** Meldungen über den Benutzer "enable_15" oder "enable_1" anzeigen, wenn kein Benutzername zugeordnet ist. Telnet in den PIX als Benutzer "pixtest" (unser Benutzer "Stufe 15") vor der Konfiguration der Befehlsautorisierung ein, da wir sicherstellen müssen, dass der PIX den auszuprobierenden Befehlen einen Benutzernamen zuordnen kann. Die Authentifizierung muss aktiviert sein, bevor die Befehlsautorisierung durchgeführt wird. Wenn eine Befehlsautorisierung mit CSUnix durchgeführt werden muss, fügen Sie den folgenden Befehl hinzu:

```
GOSS(config)# aaa authorization command TACSERVER
```

Von den drei Benutzern kann "pixtest" alles tun, und die anderen beiden Benutzer können eine Teilmenge von Befehlen ausführen.

ACS - RADIUS

Die RADIUS-Befehlsautorisierung wird nicht unterstützt. Mit ACS ist die Telnet- und Aktivierungs-Authentifizierung möglich. ACS kann für die Kommunikation mit dem PIX konfiguriert werden, indem das PIX in der Netzwerkkonfiguration mithilfe von RADIUS (beliebiger Art) für die Authentifizierung konfiguriert wird. Die Konfiguration des ACS-Benutzers hängt von der Konfiguration des PIX ab. Der ACS-Benutzer sollte mindestens einen Benutzernamen und ein Kennwort einrichten.

Verwenden Sie auf dem PIX die folgenden Befehle:

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server RADSERVER protocol radius GOSS(config)
            # aaa-server RADSERVER (inside)
              host
```

```
GOSS(config)# aaa authentication telnet console RADSERVER
```

An diesem Punkt sollte der ACS-Benutzer Telnet in das PIX-System integrieren, das vorhandene enable-Kennwort auf dem PIX aktivieren und alle Befehle verwenden können (das PIX sendet keine Befehle an den RADIUS-Server). RADIUS-Befehlsautorisierung wird nicht unterstützt).

Wenn Sie mit ACS und RADIUS auf dem PIX aktivieren möchten, fügen Sie den folgenden Befehl hinzu:

```
aaa authentication enable console RADSERVER
```

Im Gegensatz zu TACACS+ wird für die RADIUS-Aktivierung dasselbe Kennwort wie für die RADIUS-Anmeldung verwendet.

CSUnix - RADIUS

Konfigurieren Sie CSUnix so, dass mit dem PIX kommuniziert wird, wie dies bei jedem anderen Netzwerkgerät der Fall ist. Die Konfiguration des CSUnix-Benutzers hängt von der Konfiguration des PIX ab. Dieses Profil dient zur Authentifizierung und Aktivierung:

```
user = pixradius{
profile_id = 26
profile_cycle = 1
!--- The login password is in the 'clear "********"' statement; !--- this is used for the login,
enable, and non-enable commands.

password = clear "*********" < pixradius
}
```

Verwenden Sie auf dem PIX die folgenden Befehle:

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server RADSERVER protocol radius
GOSS(config)# aaa-server RADSERVER (inside) host
```

Wenn Sie mit ACS und RADIUS auf dem PIX aktivieren möchten, verwenden Sie den folgenden

Befehl:

```
GOSS(config)# aaa authentication enable console RADSERVER
```

Im Gegensatz zu TACACS+ wird für die RADIUS-Aktivierung dasselbe Kennwort wie für die RADIUS-Anmeldung verwendet.

Netzwerkzugriffsbeschränkungen

Sowohl im ACS als auch im CSUnix können Einschränkungen für den Netzwerkzugriff verwendet werden, um die Anzahl der für Verwaltungszwecke mit dem PIX verbundenen Benutzer zu begrenzen.

- **ACS** - Der PIX wird im Bereich Network Access Restrictions (Netzwerkzugriffsbeschränkungen) der Gruppeneinstellungen konfiguriert. Die PIX-Konfiguration lautet entweder "Denied Calling/Point of Access Locations" (Anrufer-/Zugangspunkt-Standorte verweigern) oder "Permitted Calling/Point of Access Locations" (Zulässige Anrufe-/Zugangspunkte) (Je nach Sicherheitsplan).
- **CSUnix** - Dies ist ein Beispiel für einen Benutzer, dem der Zugriff auf den PIX, jedoch nicht auf andere Geräte gestattet ist:

```
user = naruser{
profile_id = 119
profile_cycle = 1
password = clear "********"
privilege = clear "********" 15
service=shell {
allow "10.98.21.50" ".*" ".*"
refuse ".*" ".*" ".*"
default cmd=permit
default attribute=permit
}
}
```

Debuggen

Um das Debuggen zu aktivieren, verwenden Sie den folgenden Befehl:

```
logging on
logging
```

Dies sind Beispiele für gute und schlechte Debuggen:

- **Good debug** (**gutes Debuggen**) - Der Benutzer kann die **Anmeldung** verwenden, **aktivieren** und Befehle **ausführen**.

```
307002: Permitted Telnet login session from 172.18.124.111
111006: Console Login from pixpartial at console
502103: User priv level changed: Uname: pixpartial From: 1 To: 15
111009: User 'pixpartial' executed cmd: show clock
```

- **Ungültiges Debuggen** - Die Autorisierung schlägt für den Benutzer fehl, wie im folgenden Beispiel gezeigt:
  ```
  610101: Authorization failed: Cmd: uauth Cmdtype: show
  ```
- **Der Remote-AAA-Server ist nicht erreichbar:**
  ```
  AAA server host machine not responding
  ```

Buchhaltung

Es ist keine Befehlsabrechnung verfügbar. Wenn jedoch Syslog auf dem PIX aktiviert ist, können Sie sehen, welche Aktionen ausgeführt wurden, wie im folgenden Beispiel gezeigt:

```
307002: Permitted Telnet login session from 172.18.124.111
111006: Console Login from pixtest at console
611103: User logged out: Uname: pixtest
307002: Permitted Telnet login session from 172.18.124.111
111006: Console Login from pixtest at console
502103: User priv level changed: Uname: pixtest From: 1 To: 15
111008: User 'pixtest' executed the 'enable' command.
111007: Begin configuration: 172.18.124.111 reading from terminal
111008: User 'pixtest' executed the 'configure t' command.
111008: User 'pixtest' executed the 'write t' command.
```

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 die folgenden Informationen ein.
• Problembeschreibung und relevante Topologiedetails • Fehlerbehebung vor dem Öffnen des Gehäuses durchgeführt • Ausgabe des Befehls **show tech-support** • Ausgabe des Befehls **show log** nach der Ausführung mit dem Befehl **logging puffered debugging** oder Konsolenerfassungen, die das Problem veranschaulichen (falls verfügbar) Bitte fügen Sie die gesammelten Daten in einem nicht zippierten Textformat (.txt) an Ihr Ticket an. Sie können Informationen zu Ihrem Ticket hinzufügen, indem Sie es mithilfe des Case Query Tool hochladen (nur registrierte Kunden). Wenn Sie nicht auf das Fallabfrage-Tool zugreifen können, können Sie die Informationen in einem E-Mail-Anhang an attach@cisco.com senden, der Ihre Fallnummer in der Betreffzeile Ihrer Nachricht enthält.

Zugehörige Informationen

- PIX-Befehlsreferenz
- Cisco PIX Firewall-Software - Technischer Support und Dokumentation
- Cisco Secure Access Control Server für Windows - Technische Unterstützung und Dokumentation
- Cisco Secure Access Control Server für Unix - Technische Unterstützung und Dokumentation