PIX 6.2 : Esempio di configurazione dei comandi di autenticazione e autorizzazione

Sommario

Introduzione

L'autorizzazione dei comandi PIX e l'espansione dell'autenticazione locale sono state introdotte nella versione 6.2. Questo documento fornisce un esempio di come impostare questa opzione su un PIX. Le funzionalità di autenticazione disponibili in precedenza sono ancora disponibili ma non discusse in questo documento (ad esempio, Secure Shell (SSH), connessione client IPsec da un PC e così via). I comandi eseguiti possono essere controllati localmente sul PIX o in remoto tramite TACACS+. L'autorizzazione del comando RADIUS non è supportata. si tratta di una limitazione del protocollo RADIUS.

L'autorizzazione dei comandi locali viene eseguita assegnando comandi e utenti ai livelli di privilegio.

L'autorizzazione remota dei comandi viene eseguita tramite un server di autenticazione, autorizzazione e accounting TACACS+ (AAA). È possibile definire più server AAA nel caso in cui uno non sia raggiungibile.

L'autenticazione può essere effettuata anche con connessioni IPSec e SSH configurate in precedenza. Per l'autenticazione SSH, è necessario usare questo comando:

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

Nota: se si utilizza un gruppo di server TACACS+ o RADIUS per l'autenticazione, è possibile configurare il PIX in modo che utilizzi il database locale come metodo **FALLBACK** se il server AAA non è disponibile.

Ad esempio

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

Se si immette solo LOCAL, è possibile utilizzare il database locale come metodo di autenticazione principale (senza fallback).

Ad esempio, per definire un account utente nel database locale ed eseguire l'autenticazione locale per una connessione SSH, usare questo comando:

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

Per ulteriori informazioni su come creare l'accesso autenticato AAA a un firewall PIX con software PIX versione 5.2-6.2 e per ulteriori informazioni su come abilitare l'autenticazione, il syslog e l'accesso quando il server AAA non è attivo, consultare il documento sulla modalità di esecuzione dell'autenticazione e dell'attivazione sul firewall Cisco Secure PIX (da 5.2 a 6.2).

Per ulteriori informazioni, fare riferimento al documento PIX/ASA: Esempio di proxy cut-through per l'accesso alla rete con TACACS+ e configurazione del server RADIUS per ulteriori informazioni su come creare un accesso con autenticazione AAA (proxy cut-through) a un firewall PIX con software PIX versione 6.3 e successive.

Se la configurazione viene eseguita correttamente, non bloccare il PIX. Se la configurazione non viene salvata, il riavvio del PIX dovrebbe riportarlo allo stato precedente alla configurazione. Se il PIX non è accessibile a causa di una configurazione errata, fare riferimento alla procedura di recupero della password e della configurazione AAA per PIX.

Operazioni preliminari

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Prerequisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Software PIX versione 6.2
- Cisco Secure ACS per Windows versione 3.0 (ACS)
- Cisco Secure ACS for UNIX (CSUnix) versione 2.3.6

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Test prima dell'aggiunta dell'autenticazione/autorizzazione

Prima di implementare le nuove funzioni di autenticazione/autorizzazione della versione 6.2, accertarsi di poter accedere al PIX utilizzando i seguenti comandi:

```
!--- 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>
```

Informazioni sulle impostazioni dei privilegi

La maggior parte dei comandi PIX si trova al livello 15, sebbene alcuni siano al livello 0. Per visualizzare le impostazioni correnti per tutti i comandi, utilizzare questo comando:

```
show privilege all
```

La maggior parte dei comandi è al livello 15 per impostazione predefinita, come mostrato nell'esempio:

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

Alcuni comandi sono al livello 0, come mostrato nell'esempio:

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

Il PIX può funzionare in modalità abilitazione e configurazione. Alcuni comandi, ad esempio **show logging**, sono disponibili in entrambe le modalità. Per impostare i privilegi per questi comandi, è necessario specificare la modalità in cui il comando esiste, come illustrato nell'esempio. L'opzione dell'altra modalità è **attiva**. Viene visualizzato il messaggio di errore `logging is a command available in multiple mode`. Se non si configura la modalità, utilizzare il comando **mode [enable|configure]**:

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

In questi esempi viene utilizzato il comando **clock**. Utilizzare questo comando per determinare le impostazioni correnti del comando **clock**:

```
show privilege command clock
```

L'output del comando **show privilege command clock** visualizza il comando **clock** nei tre formati seguenti:

```
!--- 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
```

Autenticazione/autorizzazione - Nomi utente locali

Prima di modificare il livello di privilegio del comando **clock**, accedere alla porta della console per configurare un utente amministrativo e attivare l'autenticazione di accesso LOCALE, come mostrato nell'esempio:

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

Il PIX conferma l'aggiunta dell'utente, come mostrato nell'esempio:

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

L'utente "poweruser" deve essere in grado di collegarsi in modalità Telnet al PIX e di eseguire l'abilitazione con la password PIX enable locale esistente (quella del comando **enable password <*password*>**).

Èpossibile aumentare la protezione aggiungendo l'autenticazione per l'attivazione, come illustrato nell'esempio seguente:

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

L'utente deve immettere la password sia per l'accesso che per l'abilitazione. Nell'esempio, la

password "poweruser" viene utilizzata sia per il login che per enable. L'utente "poweruser" dovrebbe essere in grado di collegarsi in modalità Telnet al PIX e di abilitare la funzione con la password PIX locale.

Se si desidera che alcuni utenti possano utilizzare solo determinati comandi, è necessario impostare un utente con privilegi inferiori, come illustrato nell'esempio seguente:

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

Poiché praticamente tutti i comandi sono al livello 15 per impostazione predefinita, è necessario spostare alcuni comandi al livello 9 in modo che gli utenti "ordinari" possano emetterli. In questo caso, si desidera che l'utente di livello 9 sia in grado di utilizzare il comando **show clock**, ma non di riconfigurare l'orologio, come mostrato nell'esempio:

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

Èinoltre necessario che l'utente sia in grado di disconnettersi dal PIX (se si desidera eseguire questa operazione, è possibile che si trovi al livello 1 o 9), come mostrato nell'esempio seguente:

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

Ènecessario che l'utente sia in grado di utilizzare il comando **enable** (l'utente si trova al livello 1 quando tenta di eseguire questa operazione), come mostrato nell'esempio seguente:

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

Spostando il comando **disable** al livello 1, qualsiasi utente tra i livelli 2 e 15 può uscire dalla modalità di abilitazione, come mostrato nell'esempio:

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

Se si esegue la connessione in modalità Telnet come utente "ordinario" e si esegue l'abilitazione come stesso utente (la password è anche "ordinaria"), è necessario utilizzare il **comando privilege configure level 1 command disable**, come mostrato nell'esempio:

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

Se la sessione originale è ancora aperta (quella che ha preceduto l'aggiunta di qualsiasi autenticazione), il PIX potrebbe non sapere chi sei perché inizialmente non hai effettuato l'accesso con un nome utente. In questo caso, usare il comando **debug** per visualizzare i messaggi relativi all'utente "enable_15" o "enable_1" se non è presente un nome utente associato. Pertanto, è necessario accertarsi che il PIX possa associare un nome utente ai comandi da tentare prima di configurare l'autorizzazione del comando. È possibile testare l'autorizzazione del comando utilizzando questo comando:

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

L'utente "poweruser" dovrebbe essere in grado di eseguire tutte le operazioni di Telnet, abilitazione ed esecuzione. L'utente "ordinario" deve essere in grado di usare i comandi **show clock**, **enable**, **disable** e **logout**, ma non altri, come mostrato nell'esempio:

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

Autenticazione/autorizzazione con server AAA

Èinoltre possibile autenticare e autorizzare gli utenti utilizzando un server AAA. TACACS+ offre risultati migliori in quanto è possibile autorizzare i comandi, ma è anche possibile utilizzare RADIUS. Verificare se vi sono comandi Telnet/console AAA precedenti sul PIX (nel caso in cui il comando **LOCAL AAA** sia stato utilizzato in precedenza), come mostrato nell'esempio:

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

Se sono presenti comandi AAA Telnet/console, rimuoverli usando questi comandi:

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

Come per la configurazione dell'autenticazione locale, verificare che gli utenti possano connettersi al PIX in modalità Telnet utilizzando questi comandi.

```
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.
```

A seconda del server in uso, configurare il PIX per l'autenticazione/autorizzazione con un server AAA.

ACS - TACACS+

Configurare ACS in modo che comunichi con PIX definendo PIX in Network Configuration con "Authenticate Using" TACACS+ (per software Cisco IOS®). La configurazione dell'utente ACS dipende dalla configurazione del PIX. Come minimo, l'utente ACS deve essere configurato con un nome utente e una password.

Sul PIX, utilizzare i seguenti comandi:

```
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
```

A questo punto, l'utente ACS dovrebbe essere in grado di collegarsi in modalità Telnet al PIX, attivarlo con la password di abilitazione esistente sul PIX ed eseguire tutti i comandi. Attenersi alla seguente procedura:

1. Se è necessario eseguire l'autenticazione PIX enable con ACS, scegliere **Configurazione interfaccia > Impostazioni avanzate TACACS+**.
2. Selezionare la casella **Funzionalità avanzate TACACS+ in Opzioni di configurazione avanzate**.
3. Fare clic su **Invia**. Le impostazioni avanzate TACACS+ sono ora visibili nella configurazione utente.
4. Impostare il privilegio Max per ogni client AAA sul livello 15.
5. Scegliere lo schema di abilitazione della password per l'utente (che potrebbe comportare la configurazione di una password di abilitazione separata).
6. Fare clic su **Invia**.

Per attivare l'autenticazione tramite TACACS+ nel PIX, utilizzare questo comando:

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

A questo punto, l'utente ACS deve essere in grado di connettersi al PIX in modalità Telnet e di eseguire l'abilitazione con la password di abilitazione configurata in ACS.

Prima di aggiungere l'autorizzazione del comando PIX, è necessario applicare le patch ad ACS 3.0. È possibile scaricare la patch dal Software Center (solo utenti registrati). Per visualizzare ulteriori informazioni sulla patch, accedere all'ID bug Cisco CSCdw78255 (solo utenti registrati).

L'autenticazione deve funzionare prima dell'autorizzazione del comando. Se è necessario eseguire l'autorizzazione del comando con ACS, scegliere **Configurazione interfaccia > TACACS+ (Cisco) > Shell (exec) per l'utente e/o il gruppo** e fare clic su **Invia**. Le impostazioni di autorizzazione dei comandi della shell sono ora visibili nella configurazione dell'utente (o del gruppo).

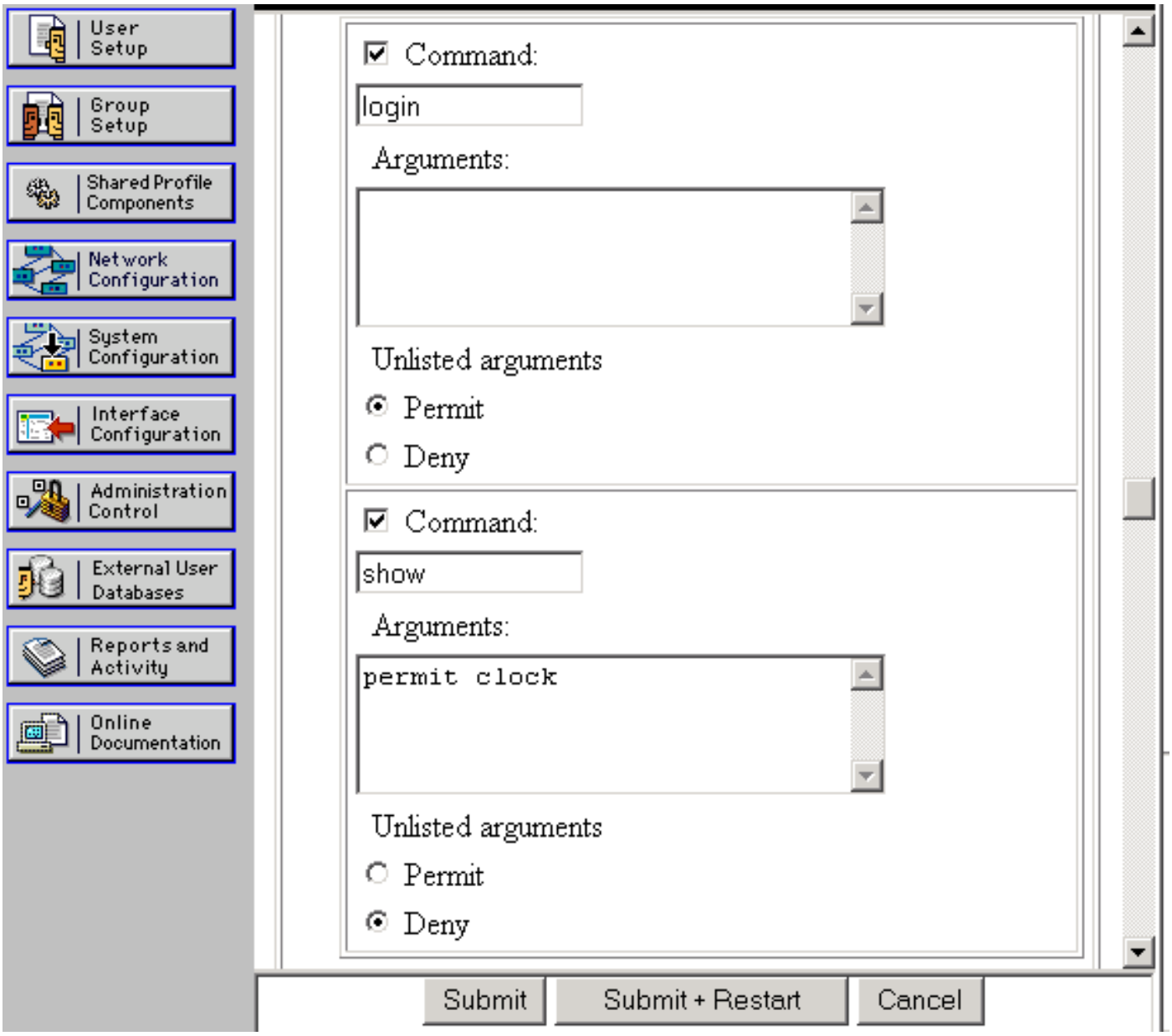
Èbuona norma configurare almeno un utente ACS potente per l'autorizzazione dei comandi e per consentire l'uso di comandi Cisco IOS non corrispondenti.

Altri utenti ACS possono essere configurati con l'autorizzazione di un comando autorizzando un sottoinsieme di comandi. In questo esempio viene utilizzata la procedura seguente:

1. Scegliere Impostazioni gruppo per trovare il gruppo desiderato nella casella a discesa.
2. Fare clic su **Modifica impostazioni**.
3. Scegliere **Set di autorizzazioni comandi shell**.
4. Fare clic sul pulsante **Comando**.
5. Immettere **login**.
6. Scegliere Autorizza in Argomenti non in elenco.
7. Ripetere questa procedura per i comandi **logout**, **enable** e **disable**.
8. Scegliere Shell Command Authorization Set.

9. Fare clic sul pulsante **Comando**.
10. **Entrate in mostra**.
11. In Argomenti immettere **clock di autorizzazione**.
12. Scegliere Nega per argomenti non in elenco.
13. Fare clic su **Invia**.

Di seguito è riportato un esempio di questi passaggi:



Se la sessione originale è ancora aperta (quella precedente all'aggiunta di un'autenticazione), il PIX potrebbe non sapere chi si è, in quanto inizialmente non è stato eseguito l'accesso con un nome utente ACS. In questo caso, usare il comando **debug** per visualizzare i messaggi relativi all'utente "enable_15" o "enable_1" se non è associato alcun nome utente. È necessario assicurarsi che il PIX possa associare un nome utente ai comandi che si stanno tentando di eseguire. A tal fine, è possibile collegarsi in modalità Telnet al PIX come utente ACS di livello 15 prima di configurare l'autorizzazione del comando. È possibile testare l'autorizzazione del comando utilizzando questo comando:

```
aaa authorization command TACSERVER
```

A questo punto, è necessario disporre di un utente che sia in grado di eseguire Telnet, abilitare e utilizzare tutti i comandi e di un secondo utente che possa eseguire solo cinque comandi.

CSUnix - TACACS+

Configurare CSUnix in modo che comunichi con il PIX come con qualsiasi altro dispositivo di rete. La configurazione dell'utente CSUnix dipende dalla configurazione del PIX. Come minimo, l'utente CSUnix deve essere configurato con un nome utente e una password. Nell'esempio sono stati impostati tre utenti:

```
!--- 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 ".*"
}
}
}
```

Sul PIX, utilizzare i seguenti comandi:

```
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
```

A questo punto, qualsiasi utente di CSUnix dovrebbe essere in grado di collegarsi in modalità Telnet al PIX, di eseguire l'abilitazione con la password di abilitazione esistente sul PIX e di utilizzare tutti i comandi.

Abilitare l'autenticazione tramite TACACS+ in PIX:

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

A questo punto, gli utenti di CSUnix che dispongono di password "privilege 15" devono essere in grado di connettersi in modalità Telnet al PIX e di eseguire l'abilitazione con queste password "enable".

Se la sessione originale è ancora aperta (quella che ha preceduto l'aggiunta di qualsiasi autenticazione), il PIX potrebbe non sapere chi sei perché inizialmente non hai effettuato l'accesso con un nome utente. In questo caso, il comando **debug** potrebbe visualizzare messaggi relativi all'utente "enable_15" o "enable_1" se non è associato alcun nome utente. Telnet nel PIX come utente "pixtest" (nostro utente "livello 15") prima di configurare l'autorizzazione del comando, perché dobbiamo essere sicuri che il PIX possa associare un nome utente ai comandi che si stanno tentando. L'abilitazione dell'autenticazione deve essere attivata prima dell'autorizzazione del comando. Se è necessario eseguire l'autorizzazione dei comandi con CSUnix, aggiungere questo comando:

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

Dei tre utenti, "pixtest" può fare tutto, e gli altri due utenti possono fare un sottoinsieme di comandi.

ACS - RADIUS

Autorizzazione del comando RADIUS non supportata. Con ACS è possibile abilitare l'autenticazione Telnet e enable. È possibile configurare ACS per comunicare con PIX definendo PIX in Network Configuration con "Authenticate Using" RADIUS (qualsiasi varietà). La configurazione dell'utente ACS dipende dalla configurazione del PIX. Come minimo, l'utente ACS deve essere configurato con un nome utente e una password.

Sul PIX, utilizzare i seguenti comandi:

```
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
```

A questo punto, l'utente ACS deve essere in grado di connettersi al PIX in modalità Telnet, di eseguire l'abilitazione con la password di abilitazione esistente sul PIX e di utilizzare tutti i comandi (il PIX non invia comandi al server RADIUS; autorizzazione comando RADIUS non supportata).

Se si desidera attivare ACS e RADIUS sul PIX, aggiungere questo comando:

```
aaa authentication enable console RADSERVER
```

A differenza di TACACS+, la stessa password viene utilizzata per RADIUS enable e per RADIUS login.

CSUnix - RADIUS

Configurare CSUnix in modo che parli con il PIX come con qualsiasi altro dispositivo di rete. La configurazione dell'utente CSUnix dipende dalla configurazione del PIX. Questo profilo funziona per l'autenticazione e l'attivazione:

```
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
}
```

Sul PIX, utilizzare i seguenti comandi:

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

Se si desidera attivare la funzione con ACS e RADIUS sul PIX, utilizzare questo comando:

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

A differenza di TACACS+, la stessa password viene utilizzata per RADIUS enable e per RADIUS login.

Restrizioni accesso alla rete

Le restrizioni di accesso alla rete possono essere usate sia in ACS che in CSUnix per limitare gli utenti che possono connettersi al PIX per scopi amministrativi.

- **ACS** - Il PIX viene configurato nell'area Restrizioni accesso alla rete (Network Access Restrictions) di Impostazioni gruppo (Group Settings). La configurazione PIX può essere "Denied Calling/Point of Access Locations" o "Permissions Calling/Point of Access Locations" (a seconda del piano di sicurezza).
- **CSUnix**: questo è un esempio di utente a cui è consentito l'accesso al PIX, ma non ad altri dispositivi:

```
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
}
}
```

Debug

Per attivare il debug, utilizzare questo comando:

```
logging on
logging
```

Ecco alcuni esempi di debug positivi e negativi:

- **Buon debug**: l'utente è in grado di utilizzare il **login**, **abilitare** ed **eseguire** i comandi.
```
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
```
- **Debug errato**: l'autorizzazione per l'utente non riesce, come mostrato nell'esempio seguente:
```
610101: Authorization failed: Cmd: uauth Cmdtype: show
```
- **Il server AAA remoto non è raggiungibile:**
```
AAA server host machine not responding
```

Contabilità

Non è disponibile un'accounting dei comandi effettiva, ma attivando syslog sul PIX è possibile verificare le azioni eseguite, come mostrato nell'esempio:

```
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.
```

Informazioni da raccogliere se si apre una richiesta TAC

Se dopo aver eseguito le procedure di risoluzione dei problemi sopra descritte si desidera continuare a ricevere assistenza e si desidera aprire una richiesta con Cisco TAC, includere le seguenti informazioni per la risoluzione dei problemi di PIX Firewall.
• Descrizione del problema e dettagli sulla topologia • Risoluzione dei problemi eseguita prima dell'apertura della richiesta • Output del comando **show tech-support** • Output del comando **show log** dopo l'esecuzione con il comando **logging buffered debugging** o acquisizioni della console che dimostrano il problema (se disponibili) Allegare i dati raccolti alla richiesta in formato testo normale non compresso (txt). È possibile allegare informazioni alla richiesta caricandola tramite lo strumento Case Query Tool (solo clienti registrati). Se non è possibile accedere allo strumento Case Query, inviare le informazioni in un allegato e-mail a attach@cisco.com con il numero della richiesta in oggetto.

Informazioni correlate

- Informazioni di riferimento sui comandi PIX
- Software Cisco PIX Firewall - Documentazione e supporto tecnico
- Cisco Secure Access Control Server per Windows - Documentazione e supporto tecnico
- Cisco Secure Access Control Server per Unix - Documentazione e supporto tecnico