PIX 6.2:인증 및 권한 부여 명령 컨피그레이션 예

목차

소개

PIX 명령 권한 부여 및 로컬 인증 확장은 버전 6.2에서 도입되었습니다. 이 문서에서는 PIX에서 이 기능을 설정하는 방법에 대한 예를 제공합니다.이전에 사용 가능한 인증 기능은 여전히 사용 가능하지만 이 문서(예: SSH(Secure Shell), PC에서 IPsec 클라이언트 연결 등)에서는 다루지 않습니다. 수행되는 명령은 PIX에서 로컬로 또는 TACACS+를 통해 원격으로 제어할 수 있습니다.RADIUS 명령 권한 부여는 지원되지 않습니다.이는 RADIUS 프로토콜의 제한입니다.

로컬 명령 권한 부여는 명령과 사용자를 권한 레벨에 할당하여 수행됩니다.

원격 명령 권한 부여는 TACACS+ 인증, 권한 부여 및 계정 관리(AAA) 서버를 통해 수행됩니다.연결할 수 없는 경우 여러 AAA 서버를 정의할 수 있습니다.

인증은 이전에 구성된 IPSec 및 SSH 연결에서도 작동합니다.SSH 인증에서는 다음 명령을 실행해야 합니다.

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

참고: 인증에 TACACS+ 또는 RADIUS 서버 그룹을 사용하는 경우 AAA 서버를 사용할 수 없는 경우

로컬 데이터베이스를 FALLBACK 방법으로 사용하도록 PIX를 구성할 수 있습니다.

예:

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

LOCAL만 입력할 경우 로컬 데이터베이스를 기본 인증 방법으로 사용할 수도 있습니다(대체 방법 없음).

예를 들어 로컬 데이터베이스에서 사용자 계정을 정의하고 SSH 연결에 대해 로컬 인증을 수행하려면 다음 명령을 실행합니다.

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

PIX 소프트웨어 버전 5.2 ~ 6.2를 실행하는 PIX 방화벽에 대한 AAA 인증 액세스를 생성하는 방법 및 AAA 서버가 다운되었을 때 인증, syslogging 및 액세스 권한 부여에 대한 자세한 내용은 Cisco Secure PIX Firewall(5.2~6.2)에서 인증 및 활성화 방법을 참조하십시오.

PIX/ASA 참조:TACACS+ 및 RADIUS 서버 컨피그레이션을 사용하는 네트워크 액세스용 컷스루 프록시의 경우 PIX 소프트웨어 버전 6.3 이상을 실행하는 PIX 방화벽에 대한 AAA 인증(컷스루 프록시) 액세스를 생성하는 방법에 대한 자세한 내용은 Cut-through Proxy for Network Access를 참조하십시오.

컨피그레이션이 올바르게 완료되면 PIX에서 잠기지 않아야 합니다.컨피그레이션이 저장되지 않은 경우 PIX를 재부팅하면 사전 컨피그레이션 상태로 돌아갑니다.컨피그레이션 오류로 인해 PIX에 액세스할 수 없는 경우 PIX에 대한 비밀번호 복구 및 AAA 컨피그레이션 복구 절차를 참조하십시오.

시작하기 전에

표기 규칙

문서 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

사전 요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- PIX 소프트웨어 버전 6.2
- Cisco Secure ACS for Windows 버전 3.0(ACS)
- Cisco Secure ACS for UNIX(CSUnix) 버전 2.3.6

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.라이브 네트워크에서 작업하는 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

인증/권한 부여를 추가하기 전에 테스트

새로운 6.2 인증/권한 부여 기능을 구현하기 전에 다음 명령을 사용하여 현재 PIX에 액세스할 수 있는지 확인하십시오.

```
!--- 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>
```

권한 설정 이해

PIX의 대부분의 명령은 레벨 15이지만 일부 명령은 레벨 0에 있습니다. 모든 명령에 대한 현재 설정을 보려면 다음 명령을 사용하십시오.

```
show privilege all
```

대부분의 명령은 다음 예와 같이 기본적으로 레벨 15입니다.

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

다음 예와 같이 레벨 0에는 몇 가지 명령이 있습니다.

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

PIX는 활성화 및 구성 모드에서 작동할 수 있습니다.**show logging**과 같은 일부 명령은 두 모드에서 모두 사용할 수 있습니다.이러한 명령에 대한 권한을 설정하려면 예와 같이 명령이 있는 모드를 지정해야 합니다.다른 모드 옵션은 **enable**입니다. 오류 메시지 `logging` 가져옵니다.모드를 구성하지 않으면 **mode [enable|configure]** 명령을 사용합니다.

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

다음 예에서는 **clock** 명령을 다룹니다.**clock** 명령에 대한 현재 설정을 결정하려면 다음 명령을 사용합니다.

```
show privilege command clock
```

show privilege **명령 clock** 명령의 출력에서는 **clock** 명령이 다음 세 가지 형식으로 존재함을 보여줍니다.

```
!--- 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
```

인증/권한 부여 - 로컬 사용자 이름

clock 명령의 권한 수준을 변경하기 전에 다음 예와 같이 콘솔 포트로 이동하여 관리 사용자를 구성하고 로컬 로그인 인증을 켜야 합니다.

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

PIX는 다음 예와 같이 사용자를 추가했음을 확인합니다.

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

사용자 "poweruser"는 PIX에 텔넷하고 기존 로컬 PIX enable 비밀번호(enable password ***<password>*** 명령의 비밀번호)로 활성화할 수 있어야 합니다.

다음 예와 같이 활성화를 위한 인증을 추가하여 보안을 추가할 수 있습니다.

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

이렇게 하려면 사용자가 로그인 및 enable에 모두 비밀번호를 입력해야 합니다.이 예에서는 비밀번호 "poweruser"가 로그인 및 enable에 모두 사용됩니다.사용자 "poweruser"는 PIX에 텔넷하고 로컬 PIX 비밀번호를 사용하여 활성화할 수 있어야 합니다.

일부 사용자가 특정 명령만 사용할 수 있도록 하려면 다음 예와 같이 낮은 권한을 가진 사용자를 설정해야 합니다.

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

기본적으로 모든 명령이 레벨 15이므로 일부 명령을 레벨 9로 이동하여 "일반" 사용자가 실행할 수 있도록 해야 합니다.이 경우 레벨 9 사용자가 **show clock** 명령을 사용할 수 있지만 다음 예와 같이 시계를 재구성할 수는 없습니다.

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

또한 다음 예와 같이 사용자가 PIX에서 로그아웃할 수 있어야 합니다(사용자가 이 작업을 원할 때 레벨 1 또는 9가 될 수 있음).

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

사용자가 enable 명령을 사용할 수 있어야 합니다(사용자가 이 작업을 시도할 때 레벨 1에 있음). 이 예와 같이

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

이 예와 같이 **disable** 명령을 레벨 1로 이동하면 레벨 2-15 사이의 모든 사용자가 enable 모드에서 벗어날 수 있습니다.

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

텔넷을 "common" 사용자로 설정하고 동일한 사용자로 활성화한 경우(비밀번호도 "일반"임), 다음 예와 같이 **privilege configure level 1 명령 disable**을 사용해야 합니다.

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

원래 세션이 열려 있는 경우(인증을 추가하기 전의 세션), 사용자 이름으로 처음 로그인하지 않았기 때문에 PIX가 사용자가 누구인지 알지 못할 수 있습니다.이 경우 **debug** 명령을 사용하여 연결된 사용자 이름이 없는 경우 "enable_15" 또는 "enable_1" 사용자에 대한 메시지를 봅니다.따라서 명령 권한 부여를 구성하기 전에 PIX가 사용자 이름을 시도 중인 명령과 연결할 수 있는지 확인해야 하므로 명령 권한 부여를 구성하기 전에 사용자 "poweruser"("level 15" 사용자)로 PIX에 텔넷합니다.다음 명령을 사용하여 명령 권한 부여를 테스트할 준비가 되었습니다.

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

사용자 "poweruser"는 모든 명령을 텔넷으로 입력, 활성화 및 수행할 수 있어야 합니다."일반" 사용자는 **show clock**을 사용할 수 있어야 하며, **enable**, disable 및 logout 명령은 다음 예에 나와 있습니다.

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

AAA 서버를 사용한 인증/권한 부여

AAA 서버를 사용하여 사용자를 인증하고 권한을 부여할 수도 있습니다.명령 권한 부여가 가능하지만 RADIUS도 사용할 수 있으므로 TACACS+가 가장 적합합니다.다음 예와 같이 PIX에 이전 AAA 텔넷/콘솔 명령이 있는지 확인합니다(**LOCAL AAA** 명령이 이전에 사용된 경우).

```
GOSS(config)# show aaa
```

```
AAA authentication telnet console LOCAL
AAA authentication enable console LOCAL
AAA authorization command LOCAL
```

이전 AAA Telnet/console 명령이 있는 경우 다음 명령을 사용하여 제거합니다.

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

로컬 인증 구성과 마찬가지로, 사용자가 이러한 명령을 사용하여 PIX에 텔넷할 수 있는지 테스트합니다.

```
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.
```

사용 중인 서버에 따라 AAA 서버를 사용하여 인증/권한 부여를 위해 PIX를 구성합니다.

ACS - TACACS+

"Authenticate Using" TACACS+(Cisco IOS® 소프트웨어용)를 사용하여 네트워크 컨피그레이션에서 PIX를 정의하여 PIX와 통신하도록 ACS를 구성합니다. ACS 사용자의 컨피그레이션은 PIX의 컨피그레이션에 따라 달라집니다.최소한 ACS 사용자는 사용자 이름과 비밀번호로 설정해야 합니다.

PIX에서 다음 명령을 사용합니다.

```
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
```

이때 ACS 사용자는 PIX에 텔넷하고 PIX의 기존 enable 비밀번호로 활성화하고 모든 명령을 수행할 수 있어야 합니다.다음 단계를 완료하십시오.

1. PIX에서 ACS를 사용하여 인증을 활성화해야 하는 경우 Interface Configuration(인터페이스 컨피그레이션) **> Advanced TACACS+ Settings(고급 TACACS+ 설정)를** 선택합니다.
2. Advanced Configuration **Options(고급 컨피그레이션 옵션)에서 Advanced TACACS+ Features(고급 TACACS+ 기능)** 상자를 선택합니다.
3. Submit(제출)**을 클릭합니다**.이제 고급 TACACS+ 설정이 사용자 컨피그레이션 아래에 표시됩니다.
4. 모든 AAA 클라이언트에 대한 최대 권한을 레벨 15로 설정합니다.
5. 사용자에 대한 enable 비밀번호 체계를 선택합니다(별도의 enable 비밀번호 구성과 관련될 수 있음).
6. Submit(제출)**을 클릭합니다**.

PIX에서 TACACS+를 통해 enable 인증을 설정하려면 다음 명령을 사용합니다.

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

이때 ACS 사용자는 PIX에 텔넷하고 ACS에 구성된 enable 비밀번호로 활성화할 수 있어야 합니다.

PIX 명령 권한 부여를 추가하기 전에 ACS 3.0을 패치해야 합니다.소프트웨어 센터에서 패치를 다운로드할 수 있습니다(등록된 고객만 해당). Cisco 버그 ID CSCdw78255에 액세스하여 이 패치에 대한 추가 정보를 볼 수도 있습니다(등록된 고객만 해당).

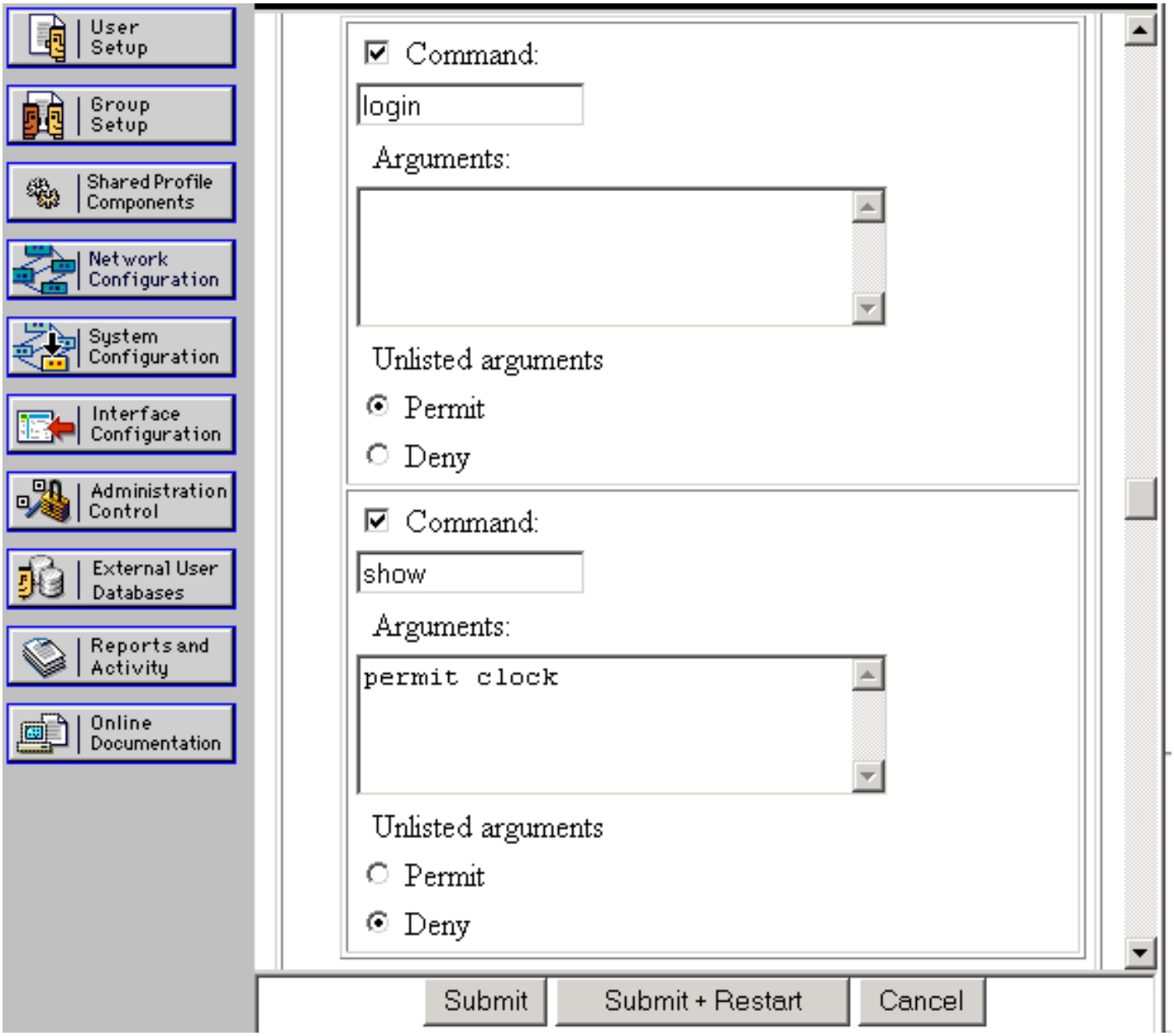
명령 권한 부여를 수행하기 전에 인증이 작동해야 합니다.ACS를 사용하여 명령 권한 부여를 수행해야 하는 경우 **Interface Configuration(인터페이스 컨피그레이션) > TACACS+(Cisco) > Shell(exec) for user and/or group(사용자 및/또는 그룹의 경우)을** 선택하고 **Submit(제출)**을 클릭합니다.이제 셸 명령 권한 부여 설정이 사용자(또는 그룹) 컨피그레이션 아래에 표시됩니다.

명령 권한 부여를 위해 하나 이상의 강력한 ACS 사용자를 설정하고 일치하지 않는 Cisco IOS 명령을 허용하는 것이 좋습니다.

명령 하위 집합을 허용하여 명령 권한 부여를 사용하여 다른 ACS 사용자를 설정할 수 있습니다.이 예에서는 다음 단계를 사용합니다.

1. 드롭다운 상자에서 원하는 그룹을 찾으려면 Group Settings(그룹 설정)를 선택합니다.
2. Edit **Settings를 클릭합니다**.
3. Shell **Command Authorization Set를 선택합니다**.
4. Command(명령) 버튼**을** 클릭합니다.
5. **로그인**을 **입력합니다**.
6. 목록에 없는 인수 아래에서 Permit을 선택합니다.
7. logout, enable 및 disable 명령**에 대해 이** 프로세스를 반복합니다.
8. Shell Command Authorization Set를 선택합니다.
9. Command(명령) 버튼**을** 클릭합니다.
10. **를 입력합니다**.
11. Arguments(인수)에 **permit clock을 입력합니다**.
12. 목록에 없는 인수에 대해 거부를 선택합니다.
13. Submit(제출)**을 클릭합니다**.

다음은 이러한 단계의 예입니다.



원래 세션이 열려 있는 경우(인증을 추가하기 전의 세션), ACS 사용자 이름으로 처음 로그인하지 않았기 때문에 PIX에서 사용자가 누구인지 알지 못할 수 있습니다.이 경우 **debug** 명령을 사용하여 연결된 사용자 이름이 없는 경우 사용자 "enable_15" 또는 "enable_1"에 대한 메시지를 봅니다 .PIX가 사용자 이름을 시도 중인 명령과 연결할 수 있는지 확인해야 합니다.명령 권한 부여를 구성하기 전에 레벨 15 ACS 사용자로 PIX에 텔네팅을 사용하여 이를 수행할 수 있습니다.다음 명령을 사용하여 명령 권한 부여를 테스트할 준비가 되었습니다.

```
aaa authorization command TACSERVER
```

이때 텔넷을 통해 모든 명령을 활성화 및 사용할 수 있어야 하는 사용자와 5개의 명령만 수행할 수 있는 두 번째 사용자가 있어야 합니다.

CSUnix - TACACS+

다른 네트워크 디바이스와 마찬가지로 PIX와 통신하도록 CSUnix를 구성합니다.CSUix 사용자의 컨피그레이션은 PIX의 컨피그레이션에 따라 달라집니다.최소한 CSUnix 사용자는 사용자 이름과 비밀번호를 사용하여 설정해야 합니다.이 예에서는 세 명의 사용자가 설정되었습니다.

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

PIX에서 다음 명령을 사용합니다.

```
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
```

이 시점에서 CSUnix 사용자는 PIX에 텔넷하고, PIX에서 기존 enable 비밀번호로 활성화하며, 모든 명령을 사용할 수 있어야 합니다.

PIX에서 TACACS+를 통한 인증을 활성화합니다.

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

이때 "권한 15" 비밀번호를 가진 CSUnix 사용자는 텔넷으로 PIX에 접속하여 "enable" 비밀번호를 사용할 수 있어야 합니다.

원래 세션이 열려 있는 경우(인증을 추가하기 전의 세션), 사용자 이름으로 처음 로그인하지 않았기 때문에 PIX가 사용자가 누구인지 알지 못할 수 있습니다.이 경우 **debug** 명령을 실행하면 사용자 이름이 연결되어 있지 않은 경우 "enable_15" 또는 "enable_1" 사용자에 대한 메시지가 표시될 수 있습니다.명령 권한 부여를 구성하기 전에 PIX에 사용자 이름을 "pixtest"(사용자 "수준 15")로 텔넷합니다. PIX가 사용자 이름을 시도 중인 명령과 연결할 수 있는지 확인해야 합니다.명령 권한 부여를 수행하기 전에 enable 인증을 설정해야 합니다.CSUnix를 사용하여 명령 권한 부여를 수행해야 하는 경우 다음 명령을 추가합니다.

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

세 사용자 중 "pixtest"는 모든 작업을 수행할 수 있으며 나머지 두 사용자는 명령의 하위 집합을 수행할 수 있습니다.

ACS - RADIUS

RADIUS 명령 권한 부여는 지원되지 않습니다.텔넷 및 활성화 인증은 ACS에서 가능합니다 ."Authenticate Using(인증 사용)" RADIUS(모든 종류)로 네트워크 구성에서 PIX를 정의하여 PIX와 통신하도록 ACS를 구성할 수 있습니다. ACS 사용자의 컨피그레이션은 PIX의 컨피그레이션에 따라 달라집니다.최소한 ACS 사용자는 사용자 이름과 비밀번호로 설정해야 합니다.

PIX에서 다음 명령을 사용합니다.

```
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
```

이 시점에서 ACS 사용자는 PIX에 텔넷하고, PIX에서 기존 enable 비밀번호로 활성화하며, 모든 명령을 사용할 수 있어야 합니다(PIX는 RADIUS 서버에 명령을 전송하지 않습니다.RADIUS 명령 권한 부여는 지원되지 않습니다.

PIX에서 ACS 및 RADIUS를 사용하여 활성화하려면 다음 명령을 추가합니다.

```
aaa authentication enable console RADSERVER
```

TACACS+와 달리 RADIUS 로그인에 사용되는 것과 동일한 비밀번호가 RADIUS enable에 사용됩니다.

CSUnix - RADIUS

CSUnix가 다른 네트워크 디바이스에서와 마찬가지로 PIX와 통신하도록 구성합니다.CSUix 사용자의 컨피그레이션은 PIX의 컨피그레이션에 따라 달라집니다.이 프로파일은 인증 및 활성화용으로 작동합니다.

```
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
}
```

PIX에서 다음 명령을 사용합니다.

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

PIX에서 ACS 및 RADIUS를 사용하여 활성화하려면 다음 명령을 사용합니다.

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

TACACS+와 달리 RADIUS 로그인에 사용되는 것과 동일한 비밀번호가 RADIUS enable에 사용됩니다.

네트워크 액세스 제한

ACS와 CSUnix에서 모두 네트워크 액세스 제한을 사용하여 관리 목적으로 PIX에 연결할 수 있는 사용자를 제한할 수 있습니다.

- **ACS**—PIX가 Group Settings(그룹 설정)의 Network Access Restrictions(네트워크 액세스 제한) 영역에서 구성됩니다.PIX 구성은 "Denied Calling/Point of Access Locations" 또는 "Permitted Calling/Point of Access Locations"(보안 계획에 따라 다름)입니다.
- **CSUnix**—PIX에 대한 액세스가 허용되지만 다른 디바이스에는 액세스가 허용된 사용자의 예입니다.

  ```
  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
}
}
```

디버그

디버깅을 설정하려면 다음 명령을 사용합니다.

```
logging on
logging
```

다음은 좋은 디버깅 및 잘못된 디버그의 예입니다.

- **Good debug**—사용자가 **log in**, enable 및 **명령**을 사용할 수 있습니다.
  ```
  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
  ```
- **잘못된 디버그** - 다음 예와 같이 사용자에 대해 권한 부여가 실패합니다.
  ```
  610101: Authorization failed: Cmd: uauth Cmdtype: show
  ```
- **원격 AAA 서버에 연결할 수 없습니다.**
  ```
  AAA server host machine not responding
  ```

회계

사용 가능한 실제 명령 어카운팅은 없지만 다음 예와 같이 PIX에서 syslog가 활성화되면 어떤 작업이 수행되었는지 확인할 수 있습니다.

```
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.
```

TAC 케이스를 열 경우 수집할 정보

위의 트러블슈팅 단계를 거친 후에도 지원이 필요한 경우 Cisco TAC에서 케이스를 열려면 PIX 방화벽 트러블슈팅을 위해 다음 정보를 포함해야 합니다.
• 문제 설명 및 관련 토폴로지 세부사항 • 케이스를 열기 전에 수행된 트러블슈팅 • **show tech-support** 명령의 출력 • **logging buffered 디버깅** 명령을 사용한 실행 후 **show log** 명령 또는 문제를 보여 주는 콘솔 캡처(사용 가능한 경우)의 출력 수집된 데이터를 압축되지 않은 일반 텍스트 형식(.txt)으로 케이스에 첨부하십시오. Case Query Tool(등록된 고객만)을 사용하여 케이스를 업로드하여 해당 케이스에 정보를 첨부할 수 있습니다. Case Query Tool에 액세스할 수 없는 경우 이메일 첨부 파일의 정보를 attach@cisco.com으로 보낼 수 있으며, 케이스 번호는 메시지의 제목 줄에 있습니다.

관련 정보

- PIX 명령 참조
- Cisco PIX Firewall Software - 기술 지원 및 문서
- Cisco Secure Access Control Server for Windows - 기술 지원 및 문서
- Unix용 Cisco Secure Access Control Server - 기술 지원 및 문서