PIX 6.2: Exemplo de configuração do comando de autenticação e autorização

Contents

Introduction

A autorização do comando PIX e a expansão da autenticação local foram introduzidas na versão 6.2. Este documento fornece um exemplo de como configurar isso em um PIX. Os recursos de autenticação disponibilizados anteriormente ainda estão disponíveis, porém, não foram abordados neste documento (Secure Shell (SSH), conexão de cliente IPSec em um PC, etc.) Os comandos executados podem ser localmente controlados no PIX ou remotamente por meio do TACACS+. A autorização de comando RADIUS não é suportada; esta é uma limitação do protocolo RADIUS.

A autorização local dos comandos é feita atribuindo-se comandos e usuários a níveis de privilégio.

A autorização de comando remota é feita através de uma autenticação de TACACS+, autorização e servidor de relatório (AAA). Múltiplos servidores AAA podem ser definidos no caso de um estar inalcançável.

A autenticação também funciona com conexões IPSec e SSH anteriormente configuradas. A autenticação SSH exige que você emita este comando:

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

Observação: se você usar um grupo de servidores TACACS+ ou RADIUS para autenticação, poderá configurar o PIX para usar o banco de dados local como um Método **FALLBACK** se o servidor AAA não estiver disponível.

Por exemplo

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

Você pode usar o banco de dados local como seu principal método de autenticação (sem fallback) se você inserir LOCAL sozinho.

Por exemplo, execute este comando para definir uma conta de usuário no banco de dados local e executar a autenticação local para uma conexão de SSH:

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

Consulte Como Executar Autenticação e Habilitação no Cisco Secure PIX Firewall (5.2 a 6.2) para obter mais informações sobre como criar acesso autenticado por AAA a um PIX Firewall que execute o PIX Software versão 5.2 a 6.2 e para obter mais informações sobre habilitar autenticação, syslogging e obter acesso quando o servidor AAA estiver inoperante.

Consulte o PIX/ASA: Exemplo de Configuração de Proxy Cut-through para Acesso à Rede usando TACACS+ e RADIUS Server para obter mais informações sobre como criar acesso autenticado por AAA (Cut-through Proxy) a um PIX Firewall que execute o Software PIX versões 6.3 e posteriores.

Se a configuração for realizada corretamente, você não deverá bloquear o PIX. Se a configuração não for salva, a reinicialização do PIX deve retorná-lo ao seu estado de pré-configuração. Se o PIX estiver inacessível devido a um erro de configuração, consulte Recuperação de Senha e Procedimento de Recuperação de Configuração de AAA para PIX.

Antes de Começar

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Prerequisites

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software PIX versão 6.2
- Cisco Secure ACS para Windows versão 3.0 (ACS)
- Cisco Secure ACS para UNIX (CSUnix) versão 2.3.6

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Testando antes de adicionar a autenticação/autorização

Antes de implementar os novos recursos de autenticação/autorização 6.2, certifique-se de que você possa obter acesso ao PIX usando estes comandos:

```
!--- 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>
```

Entendendo configurações de privilégios

A maioria dos comandos no PIX está no nível 15, embora alguns estejam no nível 0. Para exibir as configurações atuais de todos os comandos, use este comando:

```
show privilege all
```

A maioria dos comandos está no nível 15 por padrão, como mostrado neste exemplo:

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

Alguns comandos estão no nível 0, como mostrado neste exemplo:

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

O PIX pode operar nos modos de ativação e configuração. Alguns comandos, como **show logging**, estão disponíveis em ambos os modos. Para definir privilégios nesses comandos, você deve especificar o modo no qual o comando existe, como mostrado no exemplo. A outra opção de modo é **enable**. Você obtém que o `registro é um comando disponível em vários modos` de mensagem de erro. Se você não configurar o modo, use o comando **mode [enable|configure]**:

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

Esses exemplos abordam o comando **clock**. Use este comando para determinar as configurações atuais do comando **clock**:

```
show privilege command clock
```

A saída do comando **show privilege command clock** mostra que o comando **clock** existe nestes três formatos:

```
!--- 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
```

Autenticação/autorização – Nomes de usuários locais

Antes de alterar o nível de privilégio do comando **clock**, você deve ir até a porta do console para configurar um usuário administrativo e ativar a autenticação de login LOCAL, como mostrado neste exemplo:

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

O PIX confirma a adição do usuário, como mostrado neste exemplo:

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

O usuário "poweruser" deve ser capaz de executar Telnet no PIX e habilitar com a senha de habilitação do PIX local existente (a senha do comando **enable password <*password*>**).

Você pode adicionar mais segurança adicionando autenticação para habilitação, como mostrado neste exemplo:

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

Isso exige que o usuário digite a senha para login e habilitar. Neste exemplo, a senha "poweruser" é usada para login e habilitação. O usuário "avançado" deve conseguir fazer Telnet no PIX e ainda habilitar a senha local de PIX.

Se quiser que alguns usuários possam usar apenas determinados comandos, você deve configurar um usuário com privilégios menores, como mostrado neste exemplo:

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

Como praticamente todos os comandos estão em um nível 15, por padrão, você deve mover alguns comandos abaixo do nível 9, para que usuários "comuns" possam emiti-los. Nesta instância, você deseja que o usuário de nível 9 possa usar o comando **show clock**, mas não reconfigure o relógio, como mostrado neste exemplo:

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

Você também precisa que seu usuário possa fazer logoff do PIX (o usuário pode estar no nível 1 ou 9 quando quiser fazer isso), como mostrado neste exemplo:

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

Você precisa que o usuário possa usar o comando **enable** (o usuário está no nível 1 ao tentar isso), como mostrado neste exemplo:

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

Ao mover o comando **disable** para o nível 1, qualquer usuário entre os níveis 2 e 15 pode sair do modo de ativação, como mostrado neste exemplo:

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

Se você usar o Telnet como o usuário "normal" e ativar como o mesmo usuário (a senha também é "normal"), você deverá usar o **privilégio de configurar o comando de nível 1 desabilitado**, como mostrado neste exemplo:

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

Se a sessão original ainda estiver aberta (a anterior à autenticação), é possível que o PIX não o reconheça por você não ter feito o login inicialmente com um nome de usuário. Se esse for o caso, use o comando **debug** para exibir mensagens sobre o usuário "enable_15" ou "enable_1" se não houver um nome de usuário associado. Portanto, faça um Telnet para o PIX como o usuário "poweruser" (o usuário de "nível 15") antes de configurar a autorização de comando, porque é necessário ter certeza de que o PIX pode associar um nome de usuário aos comandos que estão sendo tentados. Você está pronto para testar a autorização do comando usando este comando:

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

O usuário "poweruser" deve poder realizar o Telnet, ativar e executar todos os comandos. O

usuário "normal" deve ser capaz de usar os comandos **show clock**, **enable**, **disable** e **logout**, mas não outros, como mostrado neste exemplo:

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

Autenticação/autorização com um servidor AAA

Também é possível autenticar e autorizar usuários utilizando um servidor AAA. TACACS+ funciona melhor, já a autorização de comando é possível, mas o RADIUS também pode ser usado. Verifique se há comandos AAA Telnet/console anteriores no PIX (caso o comando **LOCAL AAA** tenha sido usado anteriormente), como mostrado neste exemplo:

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

Se houver comandos AAA Telnet/console anteriores, remova-os usando estes comandos:

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

Como ocorre com a configuração da autenticação local, teste para certificar-se de que os usuários possam executar telnet no PIX usando esses comandos.

```
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.
```

Dependendo do servidor que você estiver usando, configure o PIX para autenticação/autorização com um servidor AAA.

ACS - TACACS+

Configure o ACS para se comunicar com o PIX definindo o PIX na configuração de rede com o TACACS+ "Authenticate Using" (para o software Cisco IOS®). A configuração do usuário do ACS depende da configuração do PIX. No mínimo, o usuário do ACS deve ser configurado com um nome de usuário e uma senha.

No PIX, use estes comandos:

```
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
```

Neste ponto, o usuário do ACS deve ser capaz de executar telnet no PIX, ativá-lo com a senha de ativação existente no PIX e executar todos os comandos. Conclua estes passos:

1. Se houver necessidade de habilitar a autenticação do PIX com ACS, escolha **Interface Configuration > Advanced TACACS+ Settings**.
2. Marque a caixa **Advanced TACACS+ Features in Advanced Configuration Options (Recursos avançados do TACACS+ em Opções de configuração avançada)**.
3. Clique em Submit. As Configurações avançadas do TACACS+ estão visíveis na configuração do usuário.
4. Defina o privilégio máximo para qualquer cliente AAA como Nível 15.
5. Escolha o esquema enable password para o usuário (que pode envolver a configuração de uma senha enable separada).
6. Clique em Submit.

Para ativar a autenticação de ativação por meio do TACACS+ no PIX, use este comando:

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

Neste ponto, o usuário do ACS deve ser capaz de executar telnet no PIX e habilitar com a senha de ativação configurada no ACS.

Antes de adicionar a autorização do comando PIX, o ACS 3.0 deve ser corrigido. Você pode baixar o patch do Centro de Software (somente clientes registrados) . Você também pode visualizar informações adicionais sobre este patch acessando a ID de bug da Cisco CSCdw78255 (somente clientes registrados) .

Énecessário que a autenticação esteja funcionando antes que se faça a autorização de comandos. Se houver necessidade de executar a autorização de comando com ACS, escolha **Interface Configuration > TACACS+ (Cisco) > Shell (exec) para usuário e/ou grupo** e clique em **Submit**. As configurações de autorização do comando shell agora estão visíveis na configuração do usuário (ou grupo).

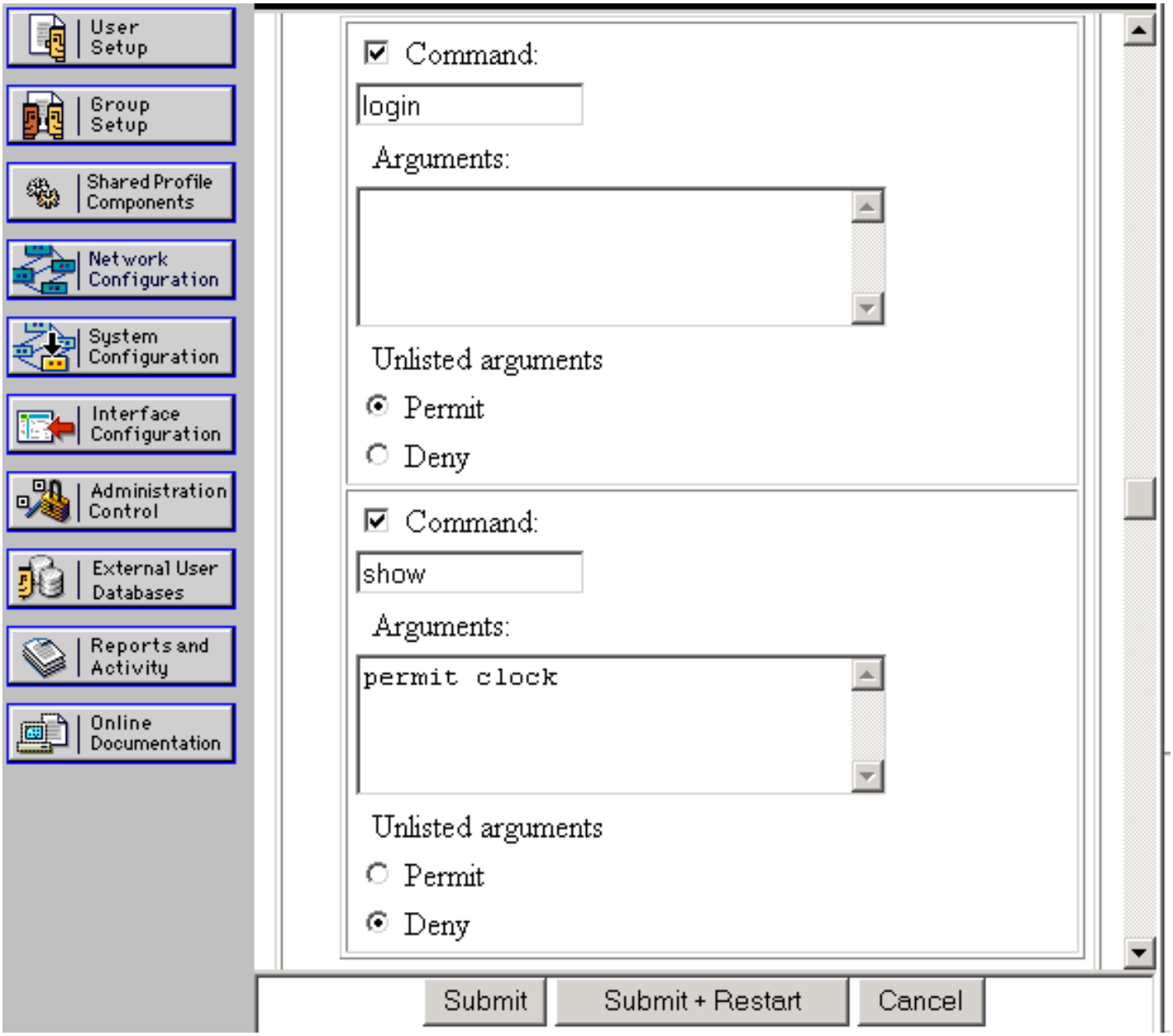
Éuma boa ideia configurar pelo menos um usuário avançado do ACS para autorização de comandos e permitir comandos incomparáveis do Cisco IOS.

Outros usuários do ACS podem ser configurados com autorização de comando permitindo um subconjunto de comandos. Este exemplo usa estas etapas:

1. Escolha Group Settings (Configurações de grupo) para localizar o grupo desejado na caixa suspensa.
2. Clique em **Editar configurações**.
3. Escolha **Shell Command Authorization Set**.
4. Clique no botão **Command**.
5. Digite **login**.
6. Escolha Permitir em Argumentos não listados.
7. Repita esse processo para os comandos **logout**, **enable** e **disable**.
8. Escolha Shell Command Authorization Set.
9. Clique no botão **Command**.
10. **Mostra**.

11. Em Argumentos , digite **permit clock**.
12. Escolha negar para Argumentos não listados.
13. Clique em Submit.

Aqui está um exemplo destas etapas:



Se você ainda tiver sua sessão original aberta (a anterior a adicionar qualquer autenticação), o PIX pode não saber quem você é porque você não fez logon inicialmente com um nome de usuário ACS. Se esse for o caso, use o comando **debug** para exibir mensagens sobre o usuário "enable_15" ou "enable_1" se não houver nenhum nome de usuário associado. Você precisa ter certeza de que o PIX pode associar um nome de usuário aos comandos que estão sendo tentados. Você pode fazer isso fazendo Telnet no PIX como o usuário ACS nível 15 antes de configurar a autorização do comando. Você está pronto para testar a autorização do comando usando este comando:

```
aaa authorization command TACSERVER
```

Nesse ponto, você deve ter um usuário que possa executar telnet, ativar e usar todos os comandos e um segundo usuário que só pode executar cinco comandos.

CSUnix - TACACS+

Configure o CSUnix para se comunicar com o PIX como faria com qualquer outro dispositivo de rede. A configuração do usuário CSUnix depende da configuração do PIX. No mínimo, o usuário do CSUnix deve ser configurado com um nome de usuário e uma senha. Neste exemplo, três usuários foram configurados:

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

No PIX, use estes comandos:

```
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
```

Nesse ponto, qualquer usuário do CSUnix deve ser capaz de executar telnet no PIX, habilitar com a senha de ativação existente no PIX e usar todos os comandos.

Ative a autenticação através do TACACS+ no PIX:

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

Nesse ponto, os usuários do CSUnix que tiverem senhas de "privilégio 15" devem ser capazes de estabelecer uma sessão Telnet no PIX e habilitarem essa sessão com senhas do tipo "enable".

Se a sessão original ainda estiver aberta (a anterior à autenticação), é possível que o PIX não o reconheça por você não ter feito o login inicialmente com um nome de usuário. Se for esse o caso, a emissão do comando debug pode mostrar mensagens sobre user "enable_15" ou "enable_1" caso não haja nome de usuário associado. Efetue Telnet no PIX como usuário "pixtest" (nosso usuário "nível 15") antes de configurar a autorização de comandos, pois precisamos ter certeza de que o PIX pode associar um nome de usuário aos comandos que estão sendo tentados. A habilitação da autenticação deve ser anterior à autorização do comando. Se houver necessidade de executar autorização de comando com CSUnix, adicione este comando:

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

Dos três usuários, "pixtest" pode fazer tudo, e os outros dois usuários podem fazer um subconjunto de comandos.

ACS - RADIUS

A autorização de comando RADIUS não é suportada. A autenticação Telnet e enable é possível com o ACS. O ACS pode ser configurado para se comunicar com o PIX definindo o PIX na configuração de rede com o RADIUS "Authenticate Using" (Autenticar usando) (qualquer variedade). A configuração do usuário do ACS depende da configuração do PIX. No mínimo, o usuário do ACS deve ser configurado com um nome de usuário e uma senha.

No PIX, use estes comandos:

```
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
```

Neste ponto, o usuário do ACS deve ser capaz de executar telnet para o PIX, habilitar com a senha de ativação existente no PIX e usar todos os comandos (o PIX não envia comandos para o servidor RADIUS; A autorização do comando RADIUS não é suportada).

Se quiser ativar com ACS e RADIUS no PIX, adicione este comando:

```
aaa authentication enable console RADSERVER
```

Ao contrário do TACACS+, a mesma senha é usada para habilitação de RADIUS como para login de RADIUS.

CSUnix - RADIUS

Configure o CSUnix para se comunicar com o PIX como faria com qualquer outro dispositivo de rede. A configuração do usuário CSUnix depende da configuração do PIX. Este perfil funciona para autenticação e ativação:

```
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
}
```

No PIX, use estes comandos:

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

Se você quiser ativar com ACS e RADIUS no PIX, use este comando:

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

Ao contrário do TACACS+, a mesma senha é usada para habilitação de RADIUS como para login de RADIUS.

Restrições de acesso à rede

As restrições de acesso à rede podem ser usadas no ACS e no CSUnix para limitar quem pode

se conectar ao PIX para fins administrativos.

- **ACS** — O PIX seria configurado na área Network Access Restrictions (Restrições de acesso à rede) das Group Settings (Configurações do grupo). A configuração do PIX é "Chamada Negada/Locais de Ponto de Acesso" ou "Chamada Permitida/Locais de Ponto de Acesso" (dependendo do plano de segurança).
- **CSUnix** —Este é um exemplo de um usuário com permissão de acesso ao PIX, mas não outros dispositivos:

```
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

Para ativar a depuração, use este comando:

```
logging on
logging
```

Estes são exemplos de depurações boas e ruins:

- **Boa depuração**—O usuário pode usar os **comandos** de **login**, **enable** e **executar**.
  ```
  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
  ```
- **Depuração incorreta** — A autorização falha para o usuário, como mostrado neste exemplo:
  ```
  610101: Authorization failed: Cmd: uauth Cmdtype: show
  ```
- **Não é possível chegar ao servidor remoto AAA:**
  ```
  AAA server host machine not responding
  ```

Relatório

Não há contabilidade de comando real disponível, mas com o syslog ativado no PIX, você pode ver quais ações foram executadas, como mostrado neste exemplo:

```
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.
```

Informações a serem coletadas se você abrir um caso de TAC

Se você ainda precisar de assistência após seguir as etapas de solução de problemas acima e quiser abrir um caso no Cisco TAC, inclua as seguintes informações para a solução de problemas do seu PIX Firewall.
• Descrição do problema e detalhes relevantes de topologia • Troubleshooting executado antes de abrir o caso • Saída do comando **show tech-support** • Saída do comando show log após a execução com o comando de depuração de registro colocado em buffer ou capturas do console que demonstram o problema (se disponível) Anexe os dados coletados para o seu caso em um formato não compactado e texto simples (.txt). Você pode anexar informações para o seu caso, carregando-o com o uso da Case Query Tool (somente clientes registrados). Se não conseguir acessar a Case Query Tool, você poderá enviar as informações em um anexo de e-mail para attach@cisco.com com o número do caso na linha de assunto da sua mensagem.

Informações Relacionadas

- Referências de comando PIX
- Software Cisco PIX Firewall - Suporte técnico e documentação
- Cisco Secure Access Control Server para Windows - Suporte técnico e documentação
- Cisco Secure Access Control Server para Unix - Suporte técnico e documentação