PIX 6.2 ：Authentication 和 Authorization命令配置示例

Contents

Introduction

本地身份验证的 PIX 命令授权和扩展是在版本 6.2 中引入的。本文在PIX提供示例如何设置此。以前的身份验证功能仍可使用，但本文档不进行讨论（例如，安全壳 (SSH)、从 PC 进行的 IPsec 客户端连接，等等）。执行的命令可能被控制本地在PIX或远程通过TACACS+。不支持 RADIUS 命令授权；这是 RADIUS 协议的一个限制。

本地命令授权是通过向权限级别分配命令和用户完成的。

远程命令授权是通过 TACACS+ 身份验证、授权和记帐 (AAA) 服务器完成的。可以定义多个 AAA 服务器，以防某个服务器无法访问。

身份验证也可用于以前配置的 IPSec 和 SSH 连接。SSH 身份验证要求您发出此命令：

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

Note: 如果使用 TACACS+ 或 RADIUS 服务器组进行身份验证，则可将 PIX 配置为使用本地数据库

，以作为 AAA 服务器无法使用时的一种**回退**方法。

例如

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

如果仅输入 LOCAL，则可以将本地数据库用作主身份验证方法（没有回退）。

例如，发出此命令以定义本地数据库中的某个用户帐户以及对 SSH 连接执行本地身份验证：

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

有关如何创建对运行 PIX 软件版本 5.2 - 6.2 的 PIX 防火墙进行 AAA 身份验证访问的详细信息，以及有关启用身份验证、系统日志记录和 AAA 服务器关闭时进行访问的详细信息，请参阅如何对 Cisco Secure PIX 防火墙（5.2 - 6.2）执行和启用身份验证。

请参阅 PIX/ASA： 有关如何创建对运行 6.3 及更高版本 PIX 软件的 PIX 防火墙进行 AAA 身份验证（直通代理）访问的详细信息，请参阅使用 TACACS+ 和 RADIUS 服务器进行网络访问的直通代理配置示例。

如果配置正确完成，则不会被锁在 PIX 之外。如果配置没有被保存，重新启动PIX应该返回它到其预配置状态。如果PIX不可访问归结于误配置，请参见密码恢复和AAA配置恢复流程PIX的。

开始使用前

Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

Prerequisites

本文档没有任何特定的前提条件。

Components Used

本文档中的信息基于以下软件和硬件版本：

- PIX 软件版本 6.2
- Cisco Secure ACS for Windows v3.0 (ACS)
- Cisco Secure ACS for UNIX (CSUnix) v2.3.6

本文档中的信息都是基于特定实验室环境中的设备创建的。All of the devices used in this document started with a cleared (default) configuration.如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

测试在添加认证/授权之前

在实现新的 6.2 身份验证/授权功能之前，确保当前能够使用下列命令访问 PIX：

```
!--- 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>
```

了解特权设置

多数in命令PIX在第15级，虽然一些在级别0。若要查看所有命令的当前设置，请使用下面的命令：

```
show privilege all
```

默认情况下，大多数命令都处于级别 15，如下例所示：

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

少数命令处于级别 0，如下例所示：

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

PIX 可在启用模式和配置模式下运行。某些命令（如 **show logging**）具有两种模式。若要对这些命令设置权限，必须指定命令所处的模式，如示例所示。另一个模式选项为 **enable**。您会看到 logging is a command available in multiple modes 错误消息。如果不配置该模式，请使用 **mode [enable|configure]** 命令：

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

这些示例涉及 **clock** 命令。使用下面的命令可确定 **clock** 命令的当前设置：

```
show privilege command clock
```

通过 **show privilege command clock** 命令的输出可以看到，存在以下三种格式的 **clock** 命令：

```
!--- 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
```

认证/授权-本地用户名

在更改 clock 命令的权限级别之前，应转到控制台端口配置管理用户并启用本地登录身份验证，如下例所示：

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

PIX 确认用户的添加，如下例所示：

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

用户“poweruser”应该能远程登录到PIX和enable (event)与现有的本地PIX特权密码(那个从**特权密码<password>**命令)。

通过添加启用身份验证可以提高安全性，如下例所示：

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

这需要用户输入登录和启用的密码。在本示例中，登录和启用都使用密码“poweruser”。用户“poweruser”应该能远程登录到PIX并且enable (event)用本地PIX密码。

如果要让某些用户只能使用特定命令，必须设置具有更低权限的用户，如下例所示：

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

默认情况下因为实际上所有您的命令在第15级，您必须移动一些down命令向第9级，以便“普通的”用户能发出他们。这种情况下，您希望级别 9 用户能够使用 show clock 命令，但不能重新配置时钟，如下例所示：

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

您还需要用户能够注销 PIX（执行此操作时，用户可能处于级别 1 或 9），如下例所示：

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

您需要用户能够使用 enable 命令（尝试此操作时，用户处于级别 1），如下例所示：

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

通过将 **disable** 命令移动到级别 1，任何处于级别 2-15 之间的用户都可从启用模式退出，如下例所示：

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

如果以“ordinary”用户身份远程登录，并以该用户身份执行启用（密码也为“ordinary”），则应使用 **privilege configure level 1 command disable**，如下例所示：

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

如果仍然有开放的原始会话(那个在添加任何认证之前)，PIX可能不知道谁您是，因为您最初没有登陆与用户名。如果是这样，在没有关联用户名的情况下，请使用 **debug** 命令查看有关用户“enable_15”或“enable_1”的消息。所以，Telnet到PIX里作为用户“poweruser” (“第15"级用户)在配置authorization命令之前，因为您需要是肯定的PIX能连结用户名与尝试的命令。现在可以使用下面的命令测试命令授权：

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

用户“poweruser”应该能远程登录，enable (event)，并且执行所有命令。用户“ordinary”应能够使用 **show clock**、**enable**、**disable** 和 **logout** 命令而不能使用其他命令，如下例所示：

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

与AAA服务器的认证/授权

您还可通过使用 AAA 服务器对用户进行身份验证和授权。TACACS+ 最为适用，因为可以进行命令授权；但也可以使用 RADIUS。请检查 PIX 上是否有以前的 AAA Telnet/控制台命令（万一以前使用过 **LOCAL AAA** 命令），如下例所示：

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

如果存在以前的 AAA Telnet/控制台命令，请使用以下命令将它们删除：

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

与配置本地身份验证一样，请进行测试以确保用户可以使用这些命令远程登录到 PIX。

```
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.
```

根据什么服务器您使用，请用AAA服务器配置认证/授权的PIX。

ACS - TACACS+

配置ACS与PIX沟通通过定义在网络配置的PIX用“验证使用” TACACS+ (Cisco IOS软件)。ACS 用户的配置取决于 PIX 的配置。至少应为 ACS 用户设置用户名和密码。

在 PIX 上，请使用以下命令：

```
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
```

这时， ACS用户应该能远程登录到PIX， enable (event)它与在PIX的现有的特权密码，并且执行所有命令。完成这些步骤：

1. 如果需要通过 ACS 执行 PIX 启用身份验证，请选择 **Interface Configuration > Advanced TACACS+ Settings**。
2. 选中 **Advanced Configuration Options > Advanced TACACS+ Features** 框。
3. 单击 **submit**。此时，高级 TACACS+ 设置显示在用户配置下面。
4. 将 Max Privilege for any AAA Client 设置为 Level 15。
5. 为用户选择启用密码方案（可能需要配置单独的启用密码）。
6. 单击 **submit**。

若要通过 PIX 中的 TACACS+ 开启启用身份验证，请使用以下命令：

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

这时， ACS用户应该能远程登录到PIX和enable (event)用在ACS的特权密码配置。

在添加 PIX 命令授权之前，必须对 ACS 3.0 进行修补。您可以从软件中心下载修补程序（仅限注册用户）。您还可通过访问 Cisco Bug ID CSCdw78255 查看有关此修补程序的其他信息（仅限注册用户）。

身份验证必须在执行命令授权之前完成。如果需要使用 ACS 执行命令授权，请为用户和/或组选择 **Interface Configuration > TACACS+ (Cisco) > Shell (exec)**，然后单击 **Submit**。Shell 命令授权设置此时显示在用户（或组）配置下面。

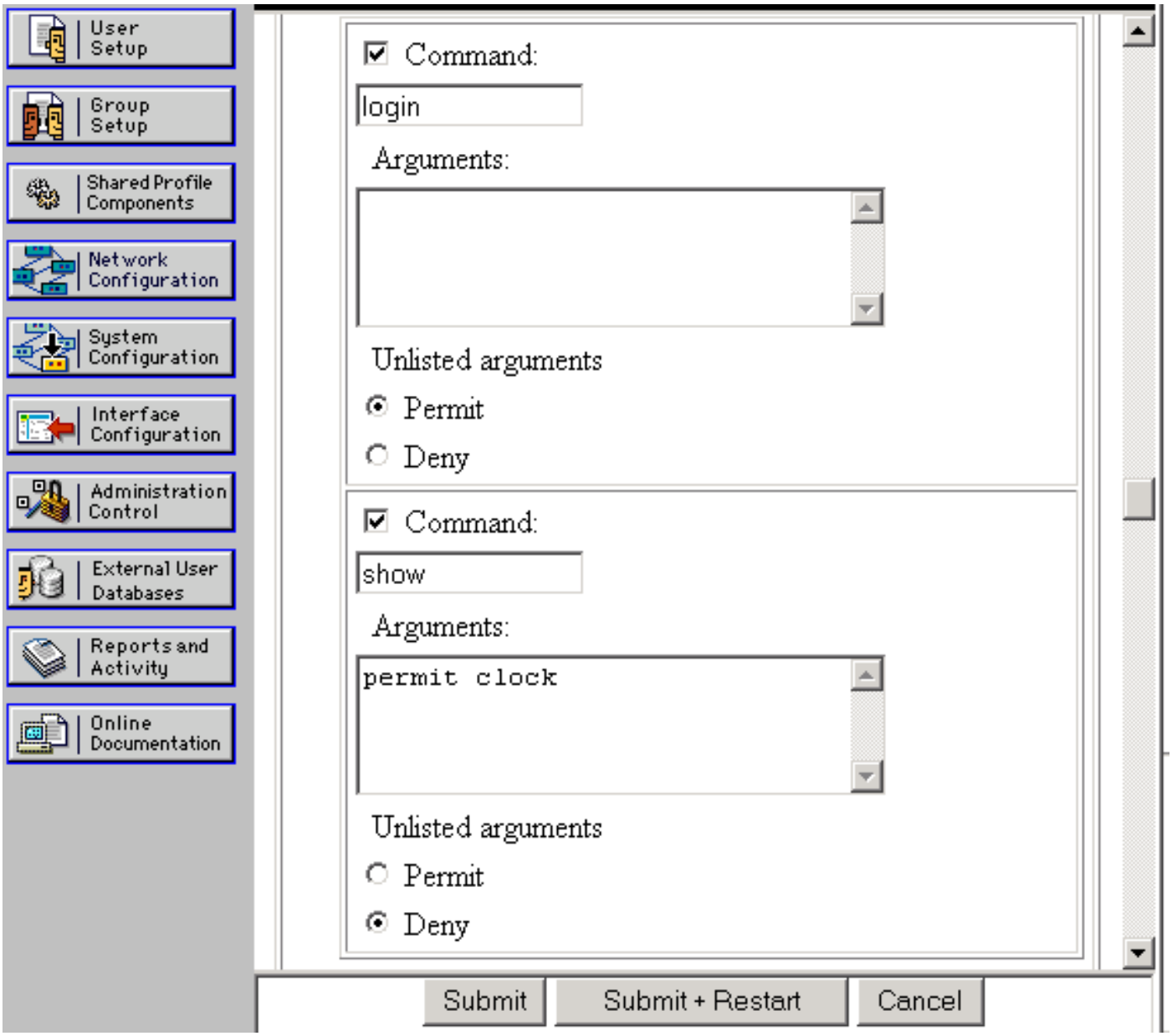
它是一个好想法设置authorization命令的至少一个强大的ACS用户和允许不匹配Cisco IOS命令。

其他ACS用户可以设置authorization命令通过允许命令的一子集。此示例采用以下步骤：

1. 选择 Group Settings，从下拉框中找到所需的组。
2. 单击 **Edit Settings**。
3. 选择 Shell Command Authorization Set。

4. 单击 **Command** 按钮。
5. 输入**登录**。
6. 在 Unlisted Arguments 下，选择 Permit。
7. 针对 **logout**、**enable** 和 **disable** 命令重复此过程。
8. 选择 Shell Command Authorization Set。
9. 单击 **Command** 按钮。
10. 输入 show。
11. 在 Arguments 下，输入 **permit clock**。
12. 针对 Unlisted Arguments，选择 deny。
13. 单击 **submit**。

下面是这些步骤的示例：



如果仍然有开放您的原始会话(那个在添加任何认证之前)，PIX可能不知道谁您是，因为您最初没有登陆与ACS用户名。如果是这样，请在没有关联用户名的情况下，使用 **debug** 命令来查看有关用户“enable_15”或“enable_1”的消息。您需要确保 PIX 可以将用户名与所尝试的命令相关联。为此，您可以在配置命令授权之前，以级别 15 ACS 用户的身份远程登录到 PIX。现在可以使用下面的命令测试命令授权：

```
aaa authorization command TACSERVER
```

此时，您应该有一个能够远程登录、启用和使用所有命令的用户，并有另外一个只能执行 5 个命令的用户。

CSUnix - TACACS+

将 CSUnix 配置为与 PIX 通信，就像您希望与任何其他网络设备通信那样。CSUnix 用户的配置取决于 PIX 的配置。至少应为 CSUnix 用户设置用户名和密码。本示例中设置了三个用户：

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

在 PIX 上，请使用以下命令：

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

此时，任何 CSUnix 用户都应能够远程登录到 PIX，使用 PIX 上的现有启用密码执行启用，并能够使用所有命令。

通过 PIX 中的 TACACS+ 启用身份验证：

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

这时，有“权限15"密码的CSUnix用户应该能远程登录到PIX和enable (event)用那些使能密码。

如果仍然有开放您的原始会话(那个在添加任何认证之前)， PIX可能不知道谁您是，因为您最初没有登陆与用户名。如果那是实际情形，发出**debug命令**可能显示关于用户的消息"enable_15"或"enable_1"，如果没有被关联的用户名。Telnet到PIX里作为用户“pixtest” (我们的“第15"级用户)在配置authorization命令之前，因为我们需要是肯定的PIX能连结用户名与尝试的命令。启用身份验证必须在执行命令授权之前进行。如果需要使用 CSUnix 来执行命令授权，请添加以下命令：

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

三个用户， “pixtest”能执行一切，并且另外两个用户能执行命令的一子集。

ACS - RADIUS

不支持 RADIUS 命令授权。可以使用 ACS 来执行 Telnet 和启用身份验证。ACS可以通过使用”RADIUS (任何种类)，定义在网络配置的PIX配置沟通与PIX与“验证。ACS 用户的配置取决于 PIX 的配置。至少应为 ACS 用户设置用户名和密码。

在 PIX 上，请使用以下命令：

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server RADSERVER protocol radius GOSS(config)
            # aaa-server RADSERVER (inside)
              host <ip> <key> timeout 10
GOSS(config)# aaa authentication telnet console RADSERVER
```

此时，ACS 用户应能够远程登录到 PIX，使用 PIX 上的现有启用密码来执行启用，并能够使用所有命令（PIX 不向 RADIUS 服务器发送命令；不支持 RADIUS 命令授权）。

如果要在 PIX 上使用 ACS 和 RADIUS 来执行启用，请添加以下命令：

```
aaa authentication enable console RADSERVER
```

与 TACACS+ 不同，RADIUS 登录密码与 RADIUS 启用密码相同。

CSUnix - RADIUS

将 CSUnix 配置为与 PIX 通信，就像使用任何其他网络设备那样。CSUnix 用户的配置取决于 PIX 的配置。此配置文件适用于身份验证和启用：

```
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
}
```

在 PIX 上，请使用以下命令：

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server RADSERVER protocol radius
GOSS(config)# aaa-server RADSERVER (inside) host <ip> <key> timeout 10
```

如果要在 PIX 上使用 ACS 和 RADIUS 执行启用，请使用以下命令：

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

与 TACACS+ 不同，RADIUS 登录密码与 RADIUS 启用密码相同。

网络访问限制

ACS 和 CSUnix 中都可以使用网络访问限制，以限制谁可以出于管理目的而连接到 PIX。

- **ACS** —PIX在组设置的Network Access Restrictions区域将被配置。PIX 配置是“Denied Calling/Point of Access Locations”或“Permitted Calling/Point of Access Locations”（取决于安全计划）。
- **CSUnix** — 这是能够访问 PIX 但不能访问其他设备的用户的示例：
  ```
  GOSS(config)# aaa authentication enable console RADSERVER
  ```

调试

若要启用调试，请使用下面的命令：

```
logging on
logging <console|monitor> debug
```

下面是正确调试和错误调试的示例：

- **正确调试** — 用户能够使用 log in、enable 和 perform 命令。

```
logging on
logging <console|monitor> debug
```

- **错误调试** — 用户的授权失败，如下例所示：

```
logging on
logging <console|monitor> debug
```

- **无法访问远程 AAA 服务器：**

```
logging on
logging <console|monitor> debug
```

认为

没有实际命令记帐，但通过在 PIX 上激活 syslog，可以看到所执行的操作，如下例所示：

```
logging on
logging <console|monitor> debug
```

应收集的信息，如果开TAC案例

如果在遵从上面故障排除步骤以后还需要援助并且要开与Cisco TAC的一个Case，请务必包括排除您的PIX防火墙故障以下信息。
• 问题说明和相关拓扑详细信息 • 在开Case前进行的排除故障 • **show tech-support** 命令的输出 • **show log命令的**输出在运行以(若有)展示问题的 **logging buffered debugging命令**或者控制台获取以后请附有收集的数据您的在非压缩的，无格式文本格式(.txt)的情况。您能附上信息到情况通过加载它使用案例查询工具(仅限注册用户)。如果不能访问案例查询工具，您在电子邮件附件在您的消息标题栏能发送信息到attach@cisco.com同您的案例编号。

Related Information

- pix命令参考资料
- Cisco PIX 防火墙软件 — 技术支持和文档
- 用于 Windows 的 Cisco 安全访问控制服务器 — 技术支持和文档
- 用于 Unix 的 Cisco 安全访问控制服务器 — 技术支持和文档