PIX 6.2 ：Authentication 和 Authorization命令配置示例

目录

简介

PIX命令授权和本地身份验证的扩展在版本6.2中引入。本文档提供了如何在PIX上设置此设置的示例。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）。 执行的命令可以在PIX上本地控制，或通过TACACS+远程控制。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>
```

注意：如果使用TACACS+或RADIUS服务器组进行身份验证，则可以将PIX配置为在AAA服务器不

可用时将本地数据库用作回退方法。

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应该将它返回到其预配置状态。如果PIX由于配置错误而不能访问，请参见PIX的密码恢复和AAA配置恢复过程。

开始使用前

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

先决条件

本文档没有任何特定的前提条件。

使用的组件

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。本文档中使用的所有设备最初均采用原始（默认）配置。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。

增加验证/授权前的测试

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

PIX中的大多数命令处于15级，但有些命令处于0级。要查看所有命令的当前设置，请使用以下命令：

```
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` 如果未配置模式，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
```

验证/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
```

"poweruser" 能远程登录到PIX，并用现有本地PIX 启用密码（来自enable password < password >命令)进行操作。

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，并且使用本地PIX口令。

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
```

由于在实际情况中您的所有命令都默认设置在L15，您必须将部分命令移到L9，以便"普通" 用户能够执行它们。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
```

如果您仍有原始会话开放(在添加任何鉴权前的那个)，PIX可能不知道您是谁，因为您最初没有用用户名登录。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。因此，在配置命令授权前，以"pixtest"用户（L15用户）远程登录到PIX，因为您需要确保PIX能将用户名与正在尝试的命令联系起来。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，启用和执行所有命令。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
```

使用 AAA 服务器进行验证/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.
```

根据您使用的是服务器，采用AAA服务器配置PIX进行鉴权/授权。

ACS - TACACS+

在网络配置中使用“使用TACACS+进行身份验证”（对于Cisco IOS®软件）定义PIX，将ACS配置为与PIX通信。 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用户能够远程登录PIX，在PIX上启用现有密码，执行所有命令。请完成以下步骤：

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用户应该能够远程登录到PIX，并用ACS中配置的启用密码进行启用。

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。

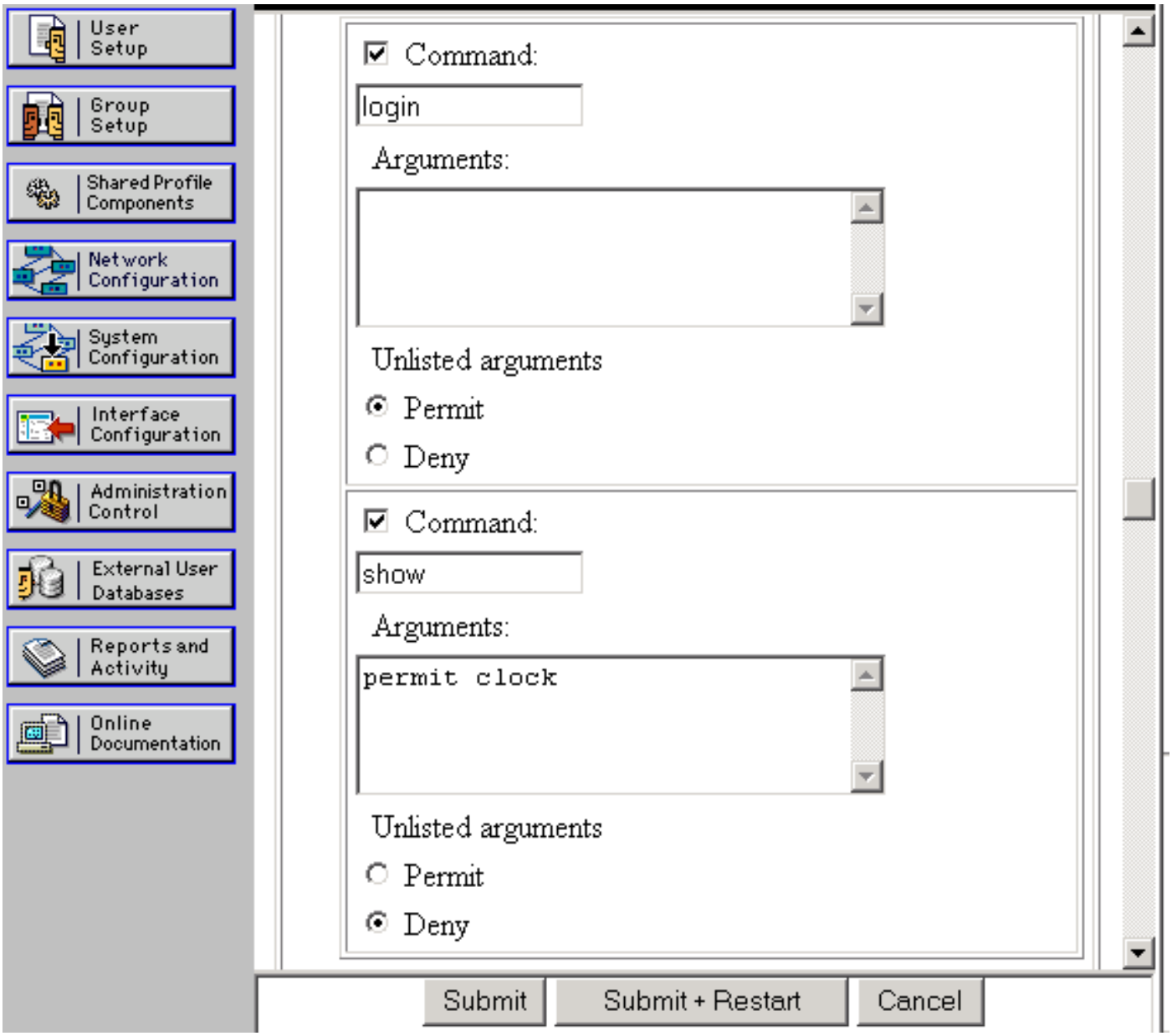
为命令授权设置至少一个强大的ACS用户，并允许不匹配的Cisco IOS命令是一个好想法。

其它ACS用户可以通过允许子集命令进行命令授权的设置。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 login。
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：



如果您仍有原始会话开放(在添加任何鉴权前使用的那个)，PIX可能不知道谁您，因为您最初没有使用ACS用户名登录。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
```

```
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，拥有"权限15"密码的CSUnix用户应该能够远程登录到PIX，并能用那些"启用" 密码进行启用。

如果您仍有原始会话开放(在添加任何鉴权前的那个)，PIX可能不知道谁您，因为您最初没有用用户名登录。如果那是实际情形，在没有相关用户名的情况下，发送debug命令可以显示有关用户"enable_15"或"enable_1"的信息。在配置命令授权前，以"pixtest"用户（L15用户）远程登录到PIX，因为我们需要确保PIX能将用户名与正在尝试的命令联系起来。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
```

在这三个用户中，pixtest"能执行所有命令，而另外二个用户能执行一个子集的命令。

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。在网络中通过配置“鉴权使用” RADIUS (任何种类)来定义PIX，配置ACS与PIX通信。 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
```

```
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
```

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将配置在组设置的Network Access Restrictions区域。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：**

```
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
}
}
```

调试

若要启用调试，请使用下面的命令：

```
logging on
logging
```

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。**
  ```
  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
  ```
- **错误调试 — 用户的授权失败，如下例所示：**
  ```
  610101: Authorization failed: Cmd: uauth Cmdtype: show
  ```
- **无法访问远程 AAA 服务器：**
  ```
  AAA server host machine not responding
  ```

记账

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：

```
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.
```

报告TAC案例应收集的信息

如果在完成上述故障排除步骤后，您还需要帮助，并希望在Cisco TAC打一个案例，请提供下列信息供PIX防火墙故障排除时使用。
• 问题说明和相关拓扑详细信息 • 在建立案例前所执行的故障诊断及处理措施 • **show tech-support 命令的输出** • 运行 logging buffered debugging 命令后 **show log 命令的输出，或演示问题的控制台捕获信息（如果可用）** 请将您所收集到的上述数据附加在一个非压缩的、纯文本格式（.txt）文件中。 通过使用Case Query工具进行上载，您可以将此信息附加到您的案例(仅限于注册用户)。 如果您不能访问案例查询工具，您也可以将相关信息发送到 attach@cisco.com，请将您的案例编号注在邮件的标题栏上。

相关信息

- PIX 命令参考
- 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