项目八

安全设备管理器（ASDM）

08

思科公司迄今为止推出了多个防火墙系列产品线，也推出了多种类型、多个版本的命令行界面和图形化界面管理系统。在本项目中，我们会对如何访问最新的思科防火墙产品线的图形化界面管理系统进行介绍。思科最早通过收购 Network Translation 公司，推出了自己的防火墙产品线，这一代产品称为 PIX。PIX 可以通过两种方式对防火墙进行管理，最常用的管理方式是通过 PIX OS 的命令行界面输入命令。从 PIX OS 4.1 版本开始，PIX 也提供了图形用户界面（GUI）。最开始的 PIX GUI 称为 PIX 防火墙管理器，运行在 Windows NT 客户端本地。从 PIX OS 6.0 版本开始，PIX GUI 变为需要使用客户端上的浏览器，通过 HTTPS 来进行访问，称为 PIX 设备管理器（PDM）。到了 PIX OS 7.0 版本，PIX GUI 同时支持在客户端本地或者通过浏览器使用 HTTPS 进行访问，称为自适应安全设备管理器（ASDM）。

到了 2005 年，思科推出了自己的新一代防火墙，名为 ASA。2008 年，思科正式宣布 PIX 停产。ASA 设备和 PIX 一样也提供了两种管理方式，一种是通过 CLI 输入命令来进行管理，另一种也是通过 ASDM 进行管理。ASA 的操作系统延续了 PIX OS 的命名方式，但版本号从 7.0 变成了 8.0。由于 PIX 是收购 Network Translation 公司获得的产品线，因此早先的 PIX OS 和 IOS 很不相同。但是从 PIX OS 8.0 版本开始，PIX OS 变得和 IOS 非常相似了。关于图形化界面管理，在销售 ASA 的十余年中，ASDM 也推出了大量的更新版本。2013 年，思科收购了一家名为 Sourcefire 的企业。这家企业是空间安全领域的领导企业之一。此后，思科在很多自身的产品上使用了 Sourcefire 的技术，其中就包括 ASA 5500-X 系列设备。同时，思科也推出了下一代防火墙，如 Firepower 2100 系列、4100 系列和 9300 系列。

关于下一代防火墙的定义，本书已经在前面进行了介绍，实际上，Firepower 也确实非常符合上面的定义。比如，Firepower 集成了高级威胁智能、思科防御编排器、高级恶意软件防护、下一代入侵防御系统和思科威胁响应等功能。Firepower 既然是思科收购 Sourcefire 的结果，它的管理方式就也有可能不同于 PIX OS 和 IOS 的 8.x 及更新版本。实际上，在设

备管理方面，Firepower 可以通过其可扩展操作系统，进行基本的设置和排错工作，但主要的策略部署工作，则需要通过 Firepower 设备管理器（FDM）来完成，因为 FXOS 几乎不能配置安全策略。显然，ASA 和 Firepower 在管理上（无论是 CLI 还是 GUI）存在很大的差异。为了降低用户的培训成本，提升管理界面的友好度。ASA 5500-X 系列防火墙也可以使用 FDM 进行管理，同时 Firepower 也可以通过安装 ASA 的 PIX OS 来执行命令行管理。

配置与管理思科 ASA 的两种方式是通过 CLI 和通过 ASDM。CLI 运行速度快，但需要更多时间学习；而 ASDM 非常直观，简化了 ASA 配置。具体而言，思科 ASDM 是一种基于 Java 的 GUI 工具，利于思科 ASA 的配置、监控和排除故障操作。ASDM 会降低管理员输入命令的复杂度，使其不需要广泛了解 ASA CLI 即可简化配置。它可与 SSL 配合使用，以确保与 ASA 的通信安全。同时 ASDM 提供快速配置向导，以及使用 CLI 无法实现的日志记录和监控功能。因此，ASDM 是配置、管理和监控 ASA 的首选方法。

要启用 ASDM 访问，ASA 需要一些最低配置。具体而言，ASDM 使用 SSL 将 Web 浏览器连接到 ASA Web 服务器实现访问。SSL 会对客户端和 ASA Web 服务器之间的流量加密。ASA 至少要求配置管理接口，管理接口取决于 ASA 型号。ASA 5505 的管理接口中包含内部逻辑 VLAN 接口（VLAN 1）和除 E0/0 外的物理 Ethernet 端口。为所有其他 ASA 型号提供了专用的第 3 层接口 G0/0。具体而言，要准备 ASDM 访问 ASA 5505，必须配置以下内容。

- 内部逻辑 VLAN 接口：分配第 3 层地址和安全级别。
- 物理 Ethernet 0/1 端口：默认分配给 VLAN 1，但必须启用。
- 启用 ASA Web 服务器：默认已禁用。
- 允许访问 ASA Web 服务器：默认情况下，ASA 在封闭策略中运行，因此，访问 HTTP 服务器的所有连接都将被拒绝。

要启动 ASDM，请在允许的主机 Web 浏览器中输入 ASA 的管理 IP 地址。允许的主机必须使用 HTTPS 通过浏览器建立与 ASA 内部接口 IP 地址的连接。选择 **Continue to this website**（继续访问此网站），启动 ASDM 窗口，此时将显示 ASDM 启动窗口。窗口提供以下两个选项。

- Run Cisco ASDM as a local application（将思科 ASDM 作为本地应用运行），其中包括 Install ASDM Launcher（安装 ASDM 启动程序）选项，可通过 SSL 从主机桌面连接 ASA。此操作的优势在于，可利用一个应用管理多个 ASA 设备，而且启动 ASDM 不需要互联网浏览器。
- Run Cisco ASDM as a Java Web Start application（将思科 ASDM 作为 Java Web Start 应用运行），其中包括 Run ASDM（运行 ASDM）选项。与思科 ASDM 建立连接需要使用互联网浏览器。如果未在本地主机上安装 ASDM，可以选择 **Run Startup Wizard**（运行启动向导）选项。该选项提供与 CLI 设置初始化向导类似的分步初始化配置。

因为浏览器存在不同的设置，可能会出现多个安全警告。如果主机之前并未访问过ASDM，浏览器可能会显示以下两个不同的安全警告。如果显示了一个安全警告，指出与该网站的连接不可信，请单击 **Continue**（继续）。接下来会显示另一个安全警告（出现此安全警告，是因为 ASA 上的证书是自签名证书，只要对话框中显示的地址是 ASA 的地址，则可以接受本地证书），指出 ASDM 可能存在安全风险。需要接受风险，然后单击 **Run**（运行）。如果主机之前访问过 ASDM，可能不会显示这些安全警告。然后，ASDM 会显示思科 ASDM IDM 启动程序，需要输入用户名和密码。由于无初始配置，请将这些字段留空，然后单击 **OK**（确定）。接下来会显示思科 Smart Call Home 窗口，选择所需选项，然后单击 **OK**（确定）。

主页上的状态信息每隔 10s 更新一次。虽然主页上提供的许多详细信息都可从 ASDM 的其他位置获得，但在此页面可以快速查看 ASA 的运行状态。ASDM 提供两个视图选项卡。默认情况下，主页上显示 Device Dashboard（设备控制面板），其中提供有关 ASA 的重要信息，例如接口状态、OS 版本、许可信息和性能相关信息。单击 Firewall Dashboard（防火墙控制面板）选项卡所示的视图，其中提供通过 ASA 的流量的安全相关信息，例如连接统计信息、丢包、扫描和 SYN 攻击检测。主页中可能显示的其他选项卡如下。

- Intrusion prevention（入侵防御）：仅当安装 IPS 模块或卡时显示。此选项卡显示有关 IPS 软件的状态信息。
- Content security（内容安全）：仅当 ASA 中安装内容安全和控制安全服务模块时显示。此选项卡显示有关的内容安全和控制安全服务模块的状态信息。思科 ASDM 用户界面旨在轻松使用 ASA 支持的许多功能。

本项目会使用 ASA 的 GUI ASDM 来完成基本的设备和安全设置。在本项目中，需要配置拓扑和非 ASA 设备及准备用于 ASDM 访问的 ASA，并且使用 ASDM 启动向导配置基本的 ASA，以及内部与外部网络之间的防火墙。接下来，还需要通过 ASDM 配置菜单配置其他内容，以及在 ASA 上配置 DMZ 并提供对 DMZ 服务器的访问。

任务 1：使用 ASDM 对自适应安全设备进行访问的配置

1．任务目的

通过本任务，读者可以掌握：

- 配置 R1、R2 和 R3 之间的静态路由，包括默认路由；
- 启用 R1 上的 HTTP 服务器并设置启用密码和 VTY 密码；
- 配置计算机主机 IP；
- 配置 ASDM 并验证对 ASA 的访问；

- 访问 ASDM 并了解 GUI 的使用。

2．任务拓扑

本任务所用的拓扑如图 7-1 所示。

本任务的 IP 地址分配见表 7-1。

3．任务步骤

步骤 1：基本路由器/交换机/计算机的配置。

第 1 步：为网络布线并清除之前的设备配置。

按照图 7-1 连接设备，并根据需要布线，确保已经清除路由器和交换机的启动配置。

第 2 步：为路由器和交换机配置基本参数。

a．为每台路由器配置主机名。

b．配置路由器接口 IP 地址。

第 3 步：在路由器上配置静态路由。

a．配置从 R1 到 R2 以及从 R3 到 R2 的静态默认路由。

```
R1(config)# ip route 0.0.0.0 0.0.0.0 s1/0
R3(config)# ip route 0.0.0.0 0.0.0.0 s1/1
```

b．配置从 R2 到 R1 接口 E0/0 子网（连接到 ASA 端口 G0/0）的静态路由以及从 R2 到 R3 LAN 的静态路由。

```
R2(config)# ip route 209.165.200.224 255.255.255.248 s1/0
R2(config)# ip route 172.16.3.0 255.255.255.0 s1/1
```

第 4 步：配置计算机主机 IP。

为 PC-A、PC-B 和 PC-C 配置静态 IP 地址、子网掩码和默认网关。

第 5 步：在 R1 上配置并加密密码。

注意：此任务中的最小密码长度被设置为 10 个字符，但为了执行任务，密码相对较为简单。建议在生产网络中使用更复杂的密码。

a．配置最小密码长度。使用 **security passwords** 命令将最小密码长度设置为 10 个字符。

```
R1(config)# security passwords min-length 10
```

b．使用密码 **cisco12345** 配置两台路由器上的启用加密密码。使用 9 类（SCRYPT）散列算法。

```
R1(config)# enable algorithm-type scrypt secret cisco12345
```

c．使用密码 **admin01pass** 创建本地 **admin01** 账户。使用 9 类（SCRYPT）散列算法并将权限级别设置为 15。

```
R1(config)#username admin01 privilege 15 algorithm-type scrypt secret
admin01pass
```

d．将控制台和 VTY 线路配置为使用本地数据库进行登录。为了提高安全度，请将线路配置为 5 分钟内无任何操作即注销。发出 **logging synchronous** 命令以防止控制台消息中断命令的输入。

```
R1(config)# line console 0
R1(config-line)# login local
R1(config-line)# exec-timeout 5 0
R1(config-line)# logging synchronous
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exec-timeout 5 0
```

e．在 R1 上启用 HTTP 服务器访问。使用本地数据库进行 HTTP 认证。

步骤 2：准备用于 ASDM 访问的 ASA。

第 1 步：配置 ASDM 接口。

a．为内部网络配置接口 G0/1，并将安全级别设置为最高 100。

```
CCNAS-ASA(config)# interface g0/1
CCNAS-ASA(config-if)# nameif inside
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)# security-level 100
CCNAS-ASA(config-if)# no shutdown
```

为外部网络配置接口 G0/0，将安全级别设置为最低 0。

```
CCNAS-ASA(config-if)# interface g0/0
CCNAS-ASA(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)# no shutdown
```

b．通过从 PC-B 对 ASA 接口 VLAN 1 IP 地址 **192.168.1.1** 执行 ping 操作来测试连接。ping 操作应当能成功。

第 2 步：配置 ASDM 并验证对 ASA 的访问。

a．使用 **http** 命令将 ASA 配置为接受 HTTPS 连接并允许从内部网络上的任何主机访问 ASDM。

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.0 255.255.255.0 inside
```

b．在 PC-B 上打开浏览器，输入 https://192.168.1.1 以测试对 ASA 的 HTTPS 连接的访问。

注意：请务必在 URL 中指定 HTTPS。

第 3 步：访问 ASDM 并了解 GUI 的使用。

a．输入 https://192.168.1.1 后，您应该会看到有关网站安全证书的安全警告，如图 8-1 所示。单击**高级→添加例外**。在“添加安全例外”对话框，单击**确认安全例外**，如图 8-2 所示。

注意：在 URL 中指定 HTTPS。

图 8-1　浏览器弹出安全警告

图 8-2　确认安全例外

b．在 ASDM 欢迎界面中，可以看到两种运行 ASDM 的方式，**Install ASDM Launcher** 和 **Install Java Web Start**，这里我们使用 **Install ASDM Launcher**，如图 8-3 所示。

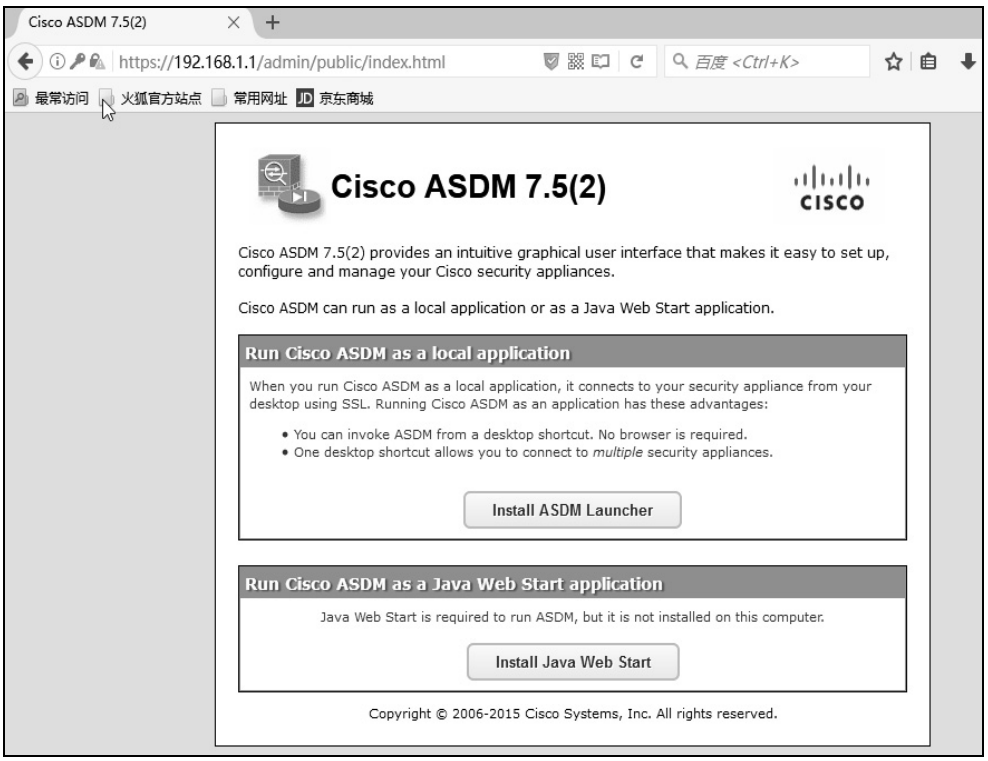

图 8-3　ASDM 欢迎界面

c．单击 **Install ASDM Launcher**，会弹出**正在打开 dm-launcher.msi** 对话框，选择保存路径后单击**保存文件**，如图 8-4 所示。

d．右键单击 **dm-launcher.msi** 文件，选择安装，安装完成后会在桌面出现 ASDM 启动器，如图 8-5 所示。

图 8-4　保存 dm-launcher.msi 文件

图 8-5　桌面上的 ASDM-IDM 启动器

e．双击 ASDM-IDM 启动器，在弹出的对话框的地址一栏输入 192.168.1.1，如图 8-6 所示。

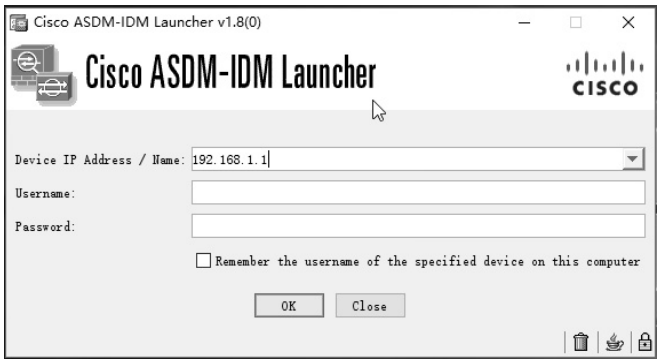

图 8-6　思科 ASDM-IDM 启动器

f. 在弹出的“安全警告”对话框中单击**继续**，如图 8-7 所示。

图 8-7　“安全警告”对话框

g. 单击 **Yes**（**是**）以响应任何其他安全警告。您应该会看到“需要授权”对话框，可以在其中输入用户名和密码。此时，我们将这些字段留空，因为它们尚未被配置，如图 8-8 所示。

图 8-8　“需要授权”对话框

h. 单击**确定**继续。ASDM 会将当前配置加载到 GUI 中。

i. 初始 GUI 界面显示各种区域和选项。ASDM 主界面左上角的菜单包含 3 个主要部分：“Home”（主页）、“Configuration”（配置）和“Monitoring”（监控），如图 8-9 所示。“Home”（主页）部分是默认设置，有“Device Dashboard”（设备控制面板）和“Firewall Dashboard”（防火墙控制面板）。“Device Dashboard”（设备控制面板）是默认界面，显示类型（ASAv）、ASA 和 ASDM 版本、内存量和防火墙模式（已

路由）等设备信息。“Device Dashboard”（设备控制面板）上有 6 个区域：

- Device Information（设备信息）；
- Interface Status（接口状态）；
- VPN Sessions（VPN 会话）；
- Failover Status（故障切换状态）；
- System Resources Status（系统资源状态）；
- Traffic Status（流量状态）。

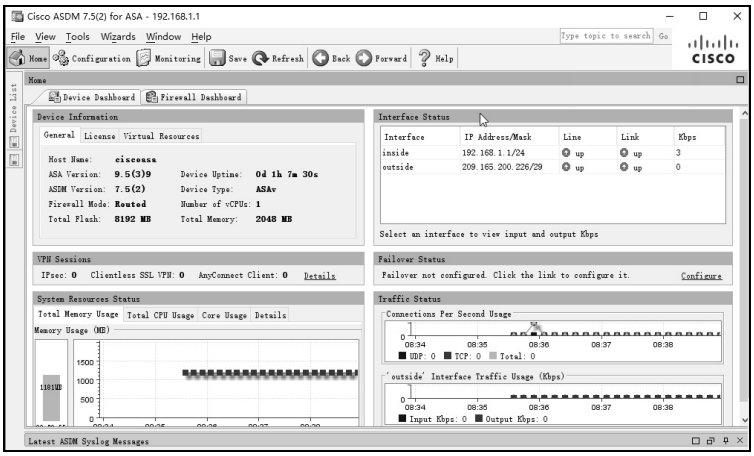

图 8-9　ASDM 主界面

注意：如果显示“Cisco Smart Call Home”（思科 Smart Call Home）窗口，单击 **Do not enable Smart Call Home**（请勿启用 Smart Call Home），然后单击 **OK**（确定）。

j．单击 **Configuration**（配置）和 **Monitoring**（监控），以熟悉其布局并查看可用选项。

任务 2：使用 ASDM 对自适应安全设备进行基础的配置

1．任务目的

通过本任务，读者可以掌握：

- 访问“Configuration”（配置）菜单并启动“Startup Wizard”（启动向导）；
- 配置主机名、域名和启用密码；
- 配置内部和外部接口；
- 配置 DHCP、地址转换和管理访问；
- 查看摘要并将命令传递给 ASA；
- 从 PC-B 测试对外部网站的访问；
- 使用 ASDM Packet Tracer 实用程序测试对外部网站的访问。

2．任务拓扑

本任务所用的拓扑如图 7-1 所示。

本任务的 IP 地址分配见表 7-1。

3．任务步骤

第 1 步：访问“Configuration”（配置）菜单并启动“Startup Wizard”（启动向导）。

a．在菜单栏上单击 **Configuration**（配置）。界面中有 5 个主要配置区域：

- Device Setup（设备设置）；
- Firewall（防火墙）；
- Remote Access VPN（远程访问 VPN）；
- Site-to-Site VPN（站点间 VPN）；
- Device Management（设备管理）。

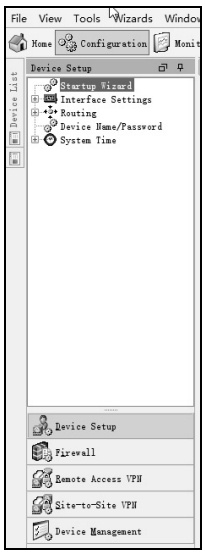

图 8-10　配置菜单

配置菜单如图 8-10 所示。

b．“Device Setup”（设备设置）启动是第一个可用选项，默认情况下系统将显示该向导。仔细阅读界面上描述启动向导的文本，然后单击 **Launch Startup Wizard**（启动启动向导），如图 8-11 所示。

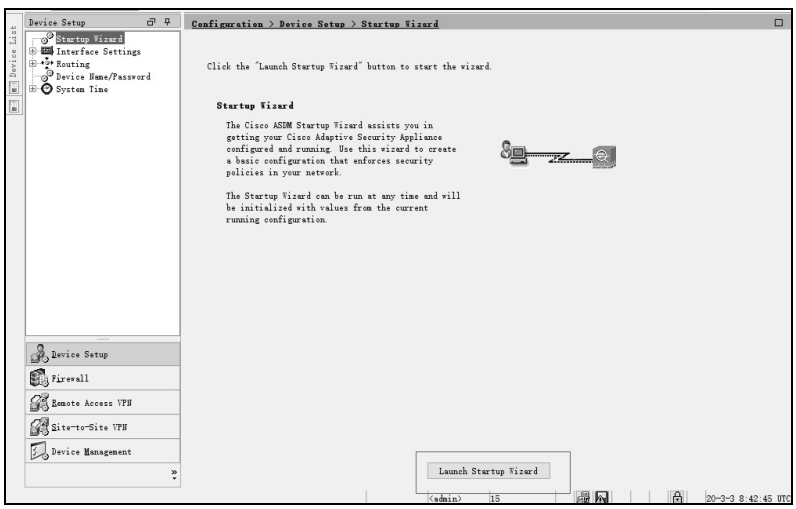

图 8-11　启动启动向导

第 2 步：配置主机名、域名和启用密码。

a．在“Startup Wizard Step1”（启动向导步骤 1）界面→“Starting Point”（开始配置）上，修改现有配置，或将 ASA 重置为出厂默认设置。确保选中 **Modify existing configuration（修改现有配置）**选项，然后单击 **Next**（下一步）继续，如图 8-12 所示。

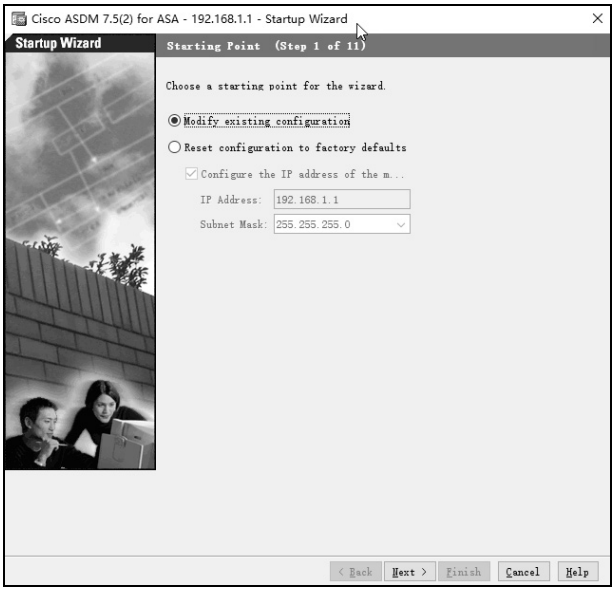

图 8-12　开始配置

b．在基础“Startup Wizard Step 2”（启动向导步骤 2）界面→“Basic Configuration”（基础配置）上，配置 ASA 主机名 **CCNAS-ASA** 和域名 **ccnasecurity.com**。单击复选框以更改启用模式密码，将密码从空白（无密码）更改为 cisco12345，再输入一次以进行确认。完成条目后，单击 **Next**（下一步）继续，如图 8-13 所示。

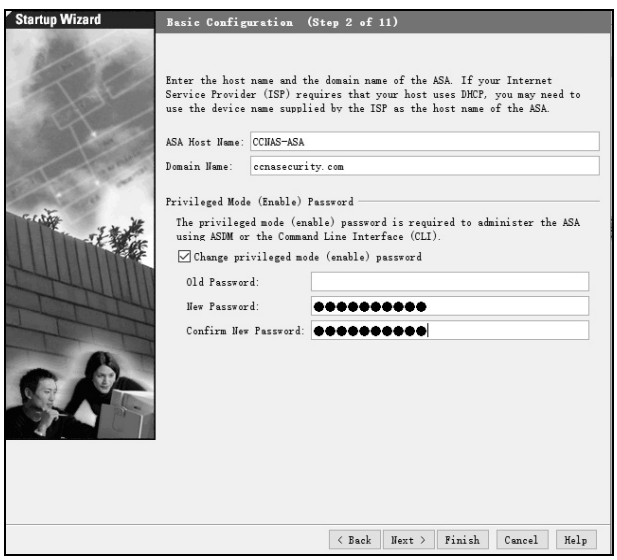

图 8-13　基础配置

第 3 步：配置外部和其他接口。

a．在“Startup Wizard Step 3”（启动向导步骤 3）界面→“Outside Interface Configuration”

（外部接口配置）上，请勿更改当前的设置，因为这些都是先前使用 CLI 定义的设置，如图 8-14 所示，单击 **Next**（下一步）继续。

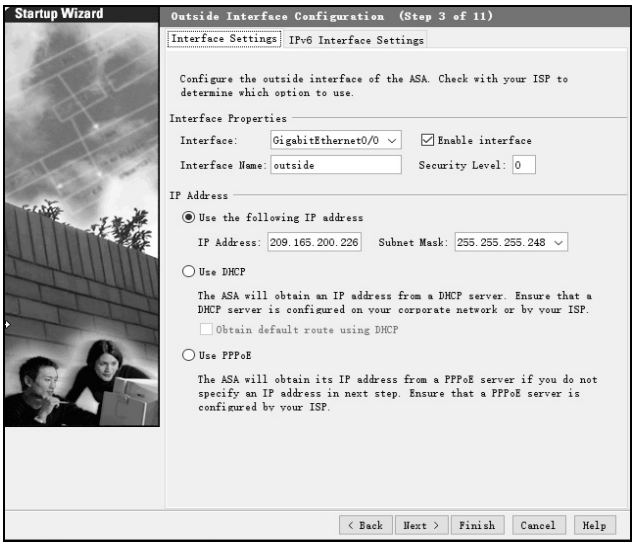

图 8-14　外部接口配置

b．在“Startup Wizard Step 4”（启动向导步骤 4）界面→“Other Interface Configuration”（其他接口配置）上，验证内部接口 G0/1 和外部接口 G0/0 是否设置正确，如图 8-15 所示。单击 **Next**（下一步）继续。

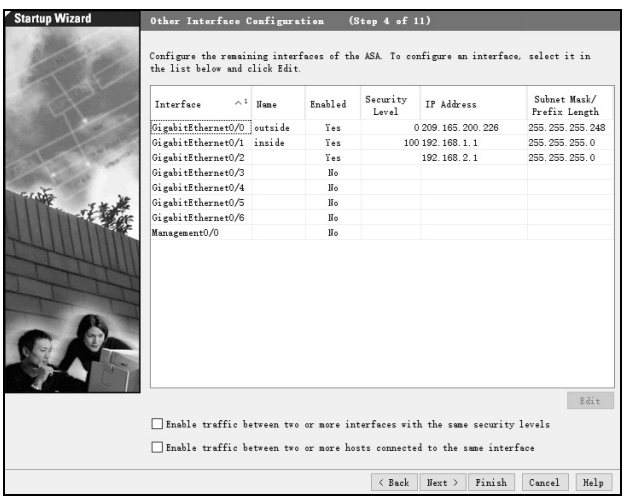

图 8-15　其他接口配置

第 4 步：配置静态路由。

在“Startup Wizard Step 5”（启动向导步骤 5）界面→“Static Routes”（静态路由）上，保持默认配置（**Filter:Both**）不变。单击 **Next**（下一步）继续，如图 8-16 所示。

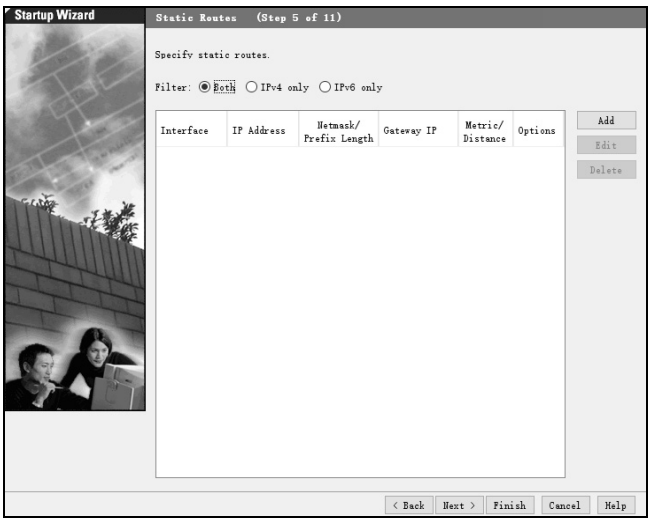

图 8-16　静态路由

第 5 步：配置 DHCP、地址转换和管理访问。

a．在“Startup Wizard Step 6”（启动向导步骤 6）界面→“DHCP Server”（DHCP 服务器）上，选中 **Enable DHCP server on the inside interface**（在内部接口上启用 DHCP 服务器）复选框。输入起始 IP 地址 **192.168.1.31** 和结束 IP 地址 **192.168.1.39**。输入 DNS 服务器 1 地址 **10.20.30.40** 和域名 **ccnasecurity.com**。请勿选中 Enable auto-configuration from interface（启用接口自动配置）复选框。单击 **Next**（下一步）继续，如图 8-17 所示。

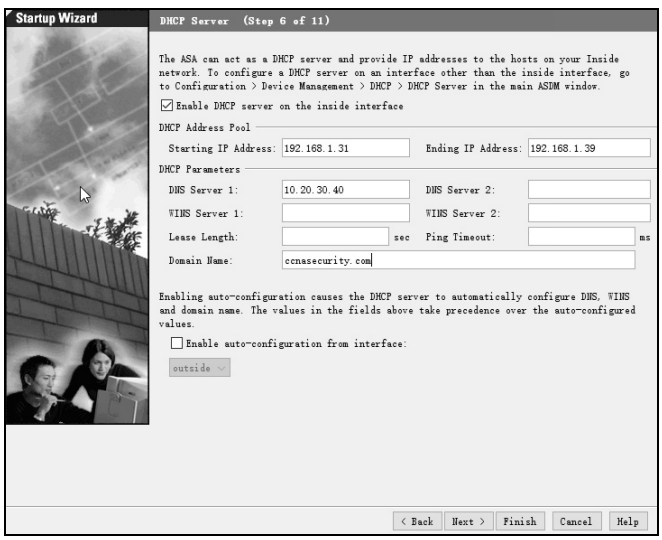

图 8-17　DHCP 服务器

b．在“Startup Wizard Step 7”（启动向导步骤 7）界面→“Address Translation (NAT/PAT)”

[地址转换（NAT/PAT）]上，单击 **Use Port Address Translation (PAT)**[使用端口地址转换（PAT）]，如图 8-18 所示。默认设置是使用外部接口的 IP 地址。单击 **Next**（下一步）继续。

图 8-18　地址转换

注意：您还可以为 PAT 指定特定 IP 地址或使用 NAT 指定一系列地址。

c．在“Startup Wizard Step 8”（启动向导步骤 8）界面→“Administrative Access”（管理访问）上，可以看到当前为第一个内部网络上的主机配置了 **HTTPS/ASDM** 访问。为第二个内部网络上的主机添加了对 ASA 的 **SSH** 访问。从外部网络上的主机 **172.16.3.3** 添加了对 ASA 的 **SSH** 访问。确保选中 **Enable HTTP server for HTTPS/ASDM access**（启用 HTTP 服务器的 HTTPS/ASDM 访问）复选框，如图 8-19 所示。单击 **Next**（下一步）继续。

图 8-19　管理访问

d．在“Startup Wizard Step 9”（启动向导步骤 9）界面→“Auto Update Server”（自动更新服务），“Startup Wizard Step 10”（启动向导步骤 10）界面→“Cisco Smart Call Home Enrollment”（思科 Smart Call Home 注册）上，保持默认配置，单击 **Next**（下一步）继续，分别如图 8-20 和图 8-21 所示。

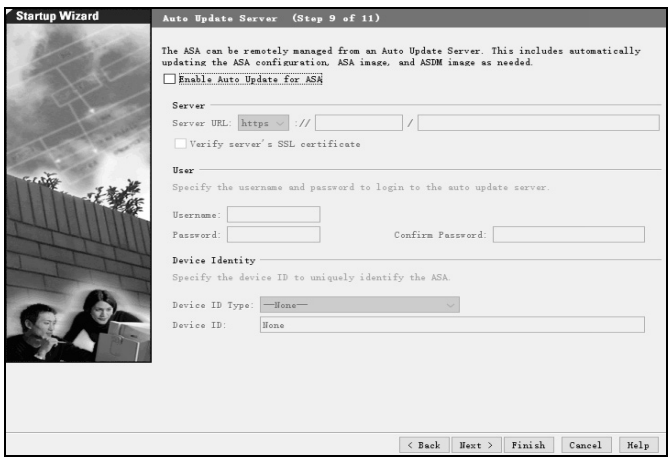

图 8-20　自动更新服务

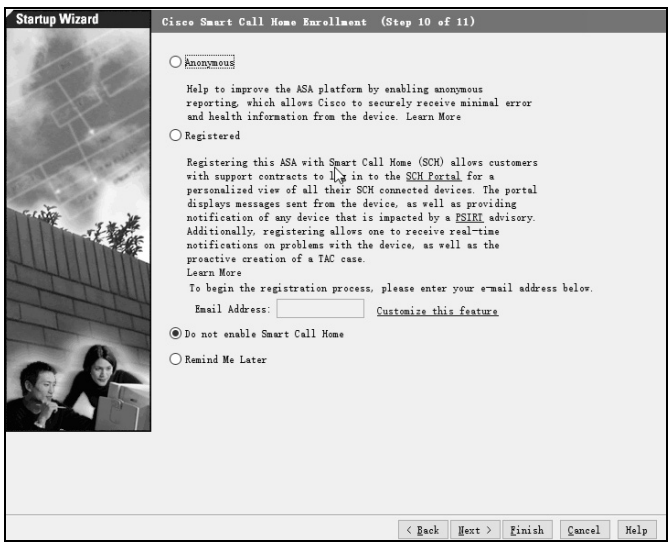

图 8-21　思科 Swart Call Home 注册

第 6 步：查看摘要并将命令传递给 ASA。

a．在“Startup Wizard Step 11”（启动向导步骤 11）界面→“Startup Wizard Summary”（启动向导摘要）上，查看 **Configuration Summary**（配置摘要），并单击 **Finish**（完成），如图 8-22 所示。ASDM 会首先将命令传递给 ASA 设备，然后重新加载修改后的配置。

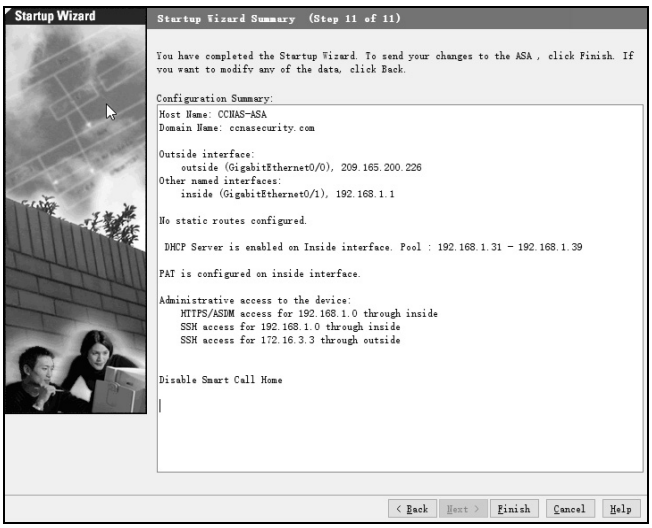

图 8-22　配置摘要

注意：如果 GUI 对话框在重新加载过程中停止响应，请首先将其关闭，退出 ASDM，然后重新启动浏览器和 ASDM。如果系统提示将配置保存到闪存，请回复 Yes（是）。即使 ASDM 似乎没有重新加载配置，也会传递命令。ASDM 如果在传递命令时遇到错误，将通知您成功的命令列表和失败的命令列表。

b．重新启动 ASDM 并提供没有用户名的新启用密码 cisco12345。返回“Device Dashboard”（设备控制面板），然后选中“Interface Status”（接口状态）窗口。您会看到内部接口和外部接口状态，以及 IP 地址和流量状态。内部接口应显示多个 kbit/s。“Traffic Status”（流量状态）窗口可能会将 ASDM 访问显示为 TCP 流量高峰，如图 8-23 所示。

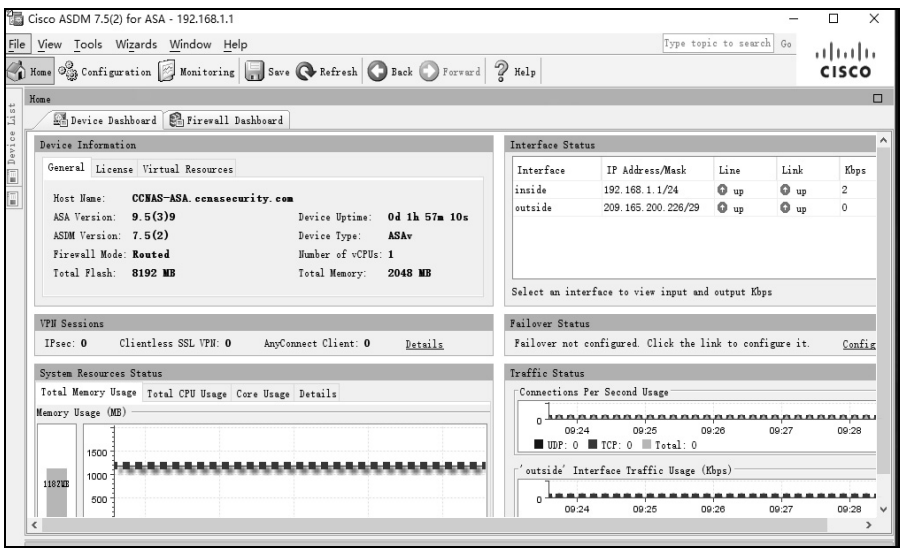

图 8-23　ASDM 主界面

第 7 步：从 PC-B 测试对外部网站的访问。

a．在 PC-B 上打开浏览器并输入 R1 接口 E0/0 的 IP 地址（**209.165.200.225**）以模拟对外部网站的访问。

b．上述部分中启用了 R1 HTTP 服务器。R1 的 GUI 设备管理器会通过“需要授权”对话框来提示您。输入用户名 **admin01** 和密码 **admin01pass**，如图 8-24 所示。退出浏览器，您会在“Home”（主页）上“Device Dashboard”（设备控制面板）的“Traffic Status”（流量状态）窗口中看到 TCP 活动，如图 8-25 所示。

图 8-24　登录 ASDM

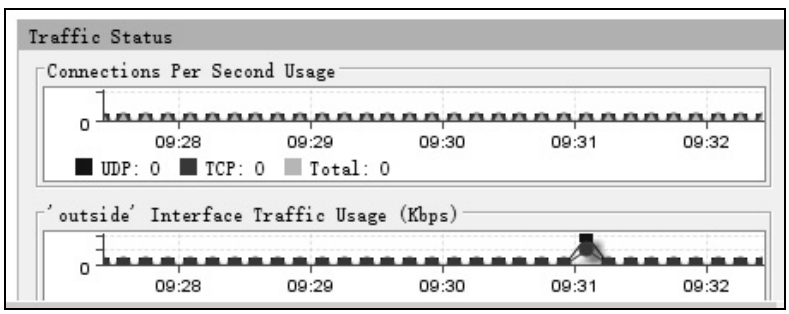

图 8-25　流量状态

第 8 步：使用 ASDM Packet Tracer 实用程序测试对外部网站的访问。

a．单击 **Tools**（工具）→**Packet Tracer**。

b．从“Interface”（接口）下拉列表中选择 **inside**（内部）接口，然后在“Packet Type”（Packet 类型）选项中单击 **TCP**。从“Source”（源）下拉列表中选择 **IP Address**（IP 地址），然后输入地址 **192.168.1.3**（PC-B）和源端口 **1500**。从“Destination”（目的）下拉列表中选择 **IP Address**（IP 地址），然后输入 **209.165.200.225**（R1 接口 E0/0）和目的端口 **http**。单击 **Start**（开始）跟踪数据包，如图 8-26 所示。应允许此数据包通过。

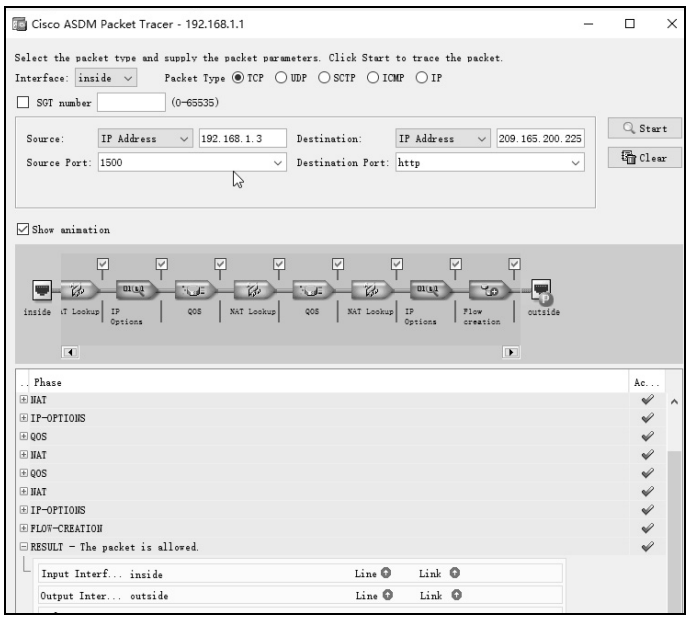

图 8-26　跟踪数据包

c．单击 **Clear**（清除）以重置条目。尝试另一个跟踪，从“Interface”（接口）下拉列表中选择 **outside**（外部）并将 TCP 保留为数据包类型。从“Source”（源）下拉列表中选择 **IP Address**（IP 地址），然后输入 **209.165.200.225**（R1 接口 E0/0）和源端口 **1500**。从“Destination”（目的）下拉列表中选择 **IP Address**（IP 地址），然后输入地址 **209.165.200.226**（ASA 外部接口）和目的端口 **telnet**。单击 **Start**（开始）跟踪数据包，如图 8-27 所示。应丢弃此数据包，单击 **Close**（关闭）继续操作。

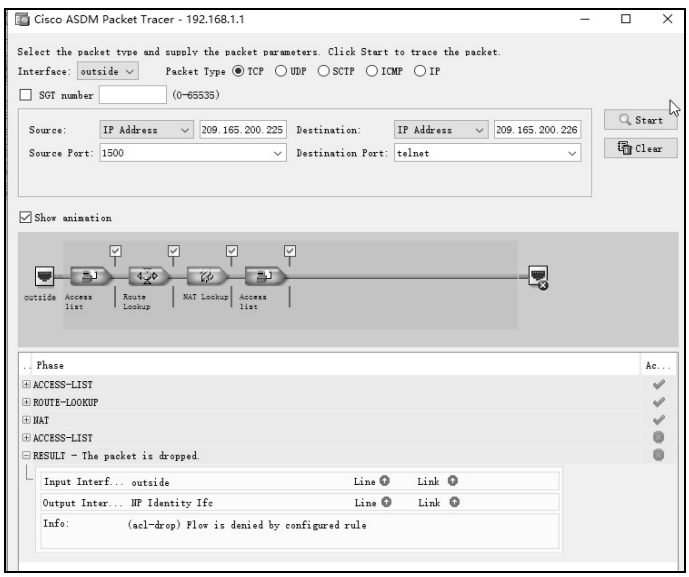

图 8-27　从源（209.165.200.225）到目的（209.165.200.226）的数据包跟踪

任务 3：使用 ASDM 对自适应安全设备进行连通性的配置

1．任务目的

通过本任务，读者可以掌握：

- 设置 ASA 的日期和时间；
- 配置 ASA 的静态默认路由；
- 使用本地 ASA 数据库配置 AAA 用户认证；
- 测试 ASA 的 SSH 访问；
- 使用 ASDM ping 和 Traceroute 测试连接；
- 修改 MPF 应用检查策略。

2．任务拓扑

本任务所用的拓扑如图 7-1 所示。

本任务的 IP 地址分配见表 7-1。

3．任务步骤

第 1 步：设置 ASA 日期和时间。

a．在 **Configuration**（配置）界面→**Device Setup**（设备设置）菜单上，单击 **System Time**（系统时间）→**Clock**（时钟）。

b．从 Clock（时钟）下拉列表中选择 **Time Zone**（时区）并在所提供的字段中输入当前日期和时间（时钟为 24 小时制）。单击 **Apply**（应用），将命令发送至 ASA。

第 2 步：配置 ASA 的静态默认路由。

a．在 **ASDM Tools**（ASDM 工具）菜单中，选择 **Ping**。在“Ping”对话框中输入路由器 R1 接口 S1/0 的 IP 地址（**10.1.1.1**）。ASA 没有通往未知外部网络的默认路由，因此 ping 操作应该会失败。单击 **Close**（关闭）继续操作，如图 8-28 所示。

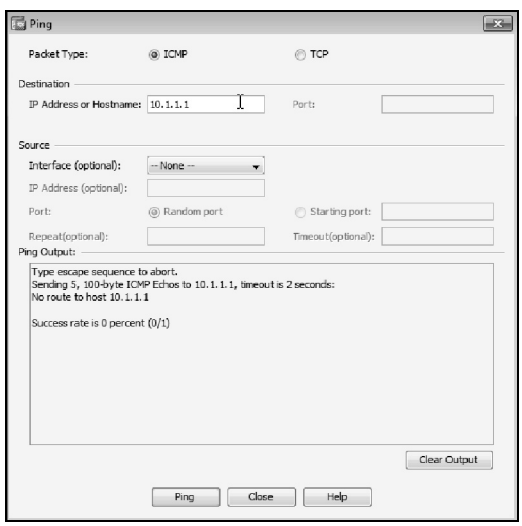

图 8-28　ping 10.1.1.1 操作失败

b．在 **Configuration**（配置）界面→**Device Setup**（设备设置）菜单中，单击 **Routing**（路由）→**Static Routes**（静态路由）。单击 **IPv4 only**（仅 IPv4），然后单击 **Add**（添加）以添加新的静态路由，如图 8-29 所示。

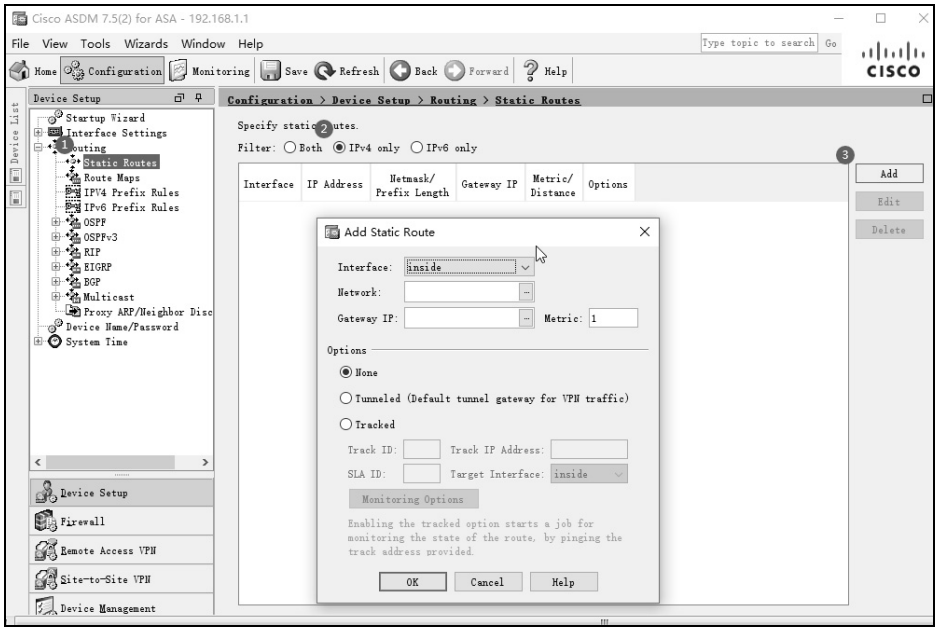

图 8-29　静态路由窗口

c．在“Add Static Route”（添加静态路由）对话框中，从 Interface（接口）下拉列表中选择 **outside**（外部）。单击 **Network**（网络）右侧的省略号按钮，从网络对象列表中选择 **any4**，将转换为“全零”路由，然后单击 **OK**（确定）。对于 **Gateway IP**（网关 IP），请输入 **209.165.200.225**（R1 接口 E0/0），如图 8-30 所示。

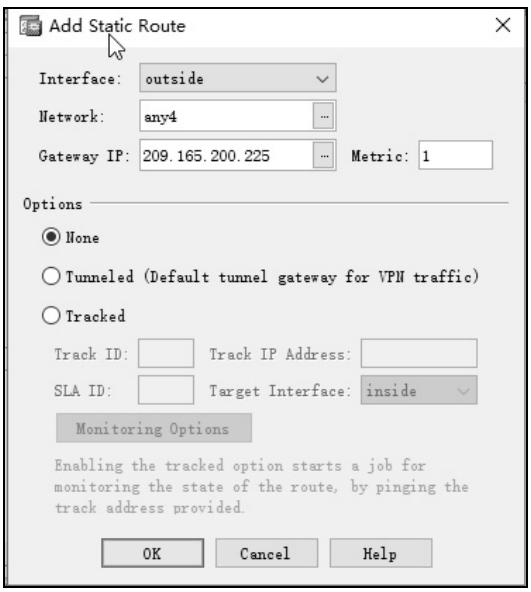

图 8-30　添加静态路由

d．单击 **OK**（确定）→**Apply**（应用），将命令发送至 ASA，如图 8-31 所示。

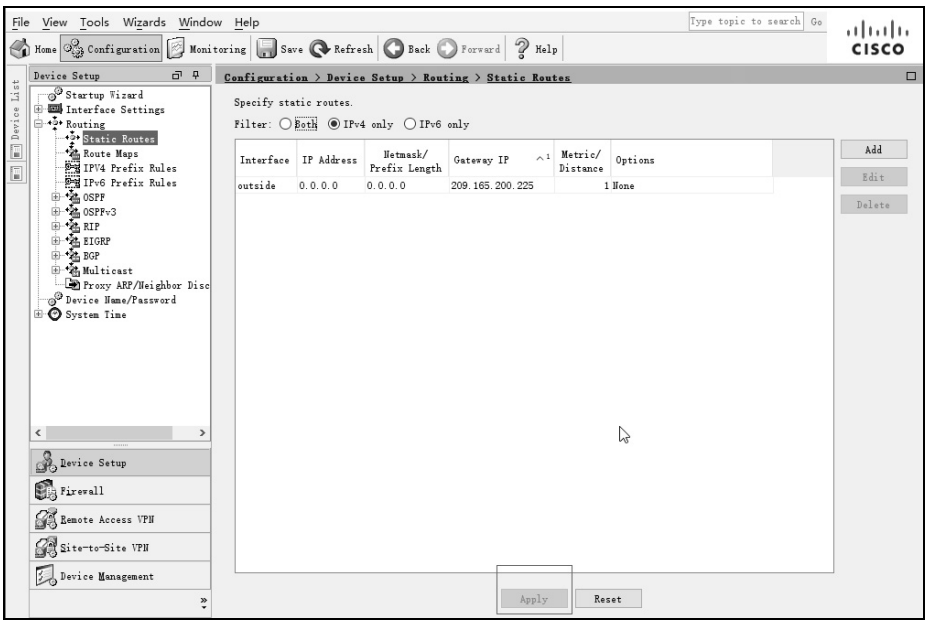

图 8-31　应用设置

e．在 **ASDM Tools**（ASDM 工具）菜单中，选择 **Ping**。在“Ping”对话框中输入路由器 R1 接口 S1/0 的 IP 地址（**10.1.1.1**），如图 8-32 所示。此次 ping 操作应该会成功，单击 **Close**（关闭）继续操作。

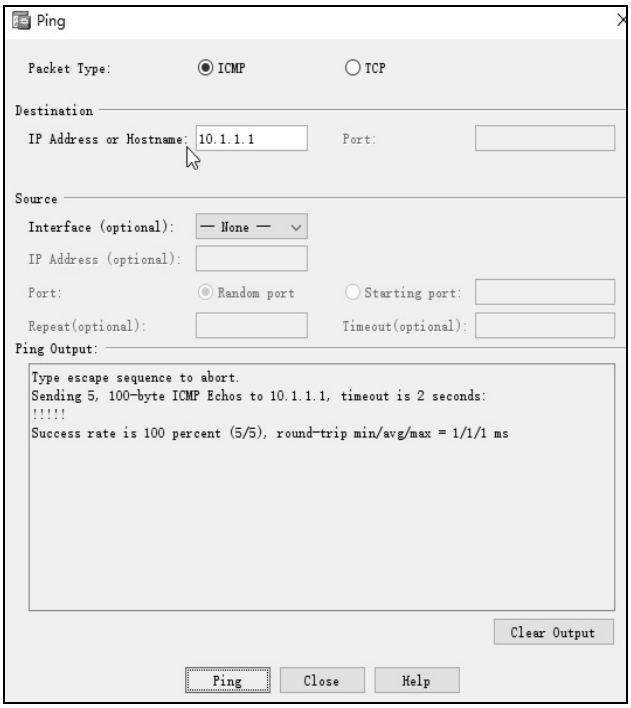

图 8-32　ping 10.1.1.1 操作成功

f. 在 ASDM Tools（工具）菜单中，选择 **Traceroute**。在“Traceroute”对话框中输入外部主机 PC-C 的 IP 地址（**172.16.3.3**），单击 **Trace Route**（跟踪路由）。Traceroute 应该会成功并显示从 ASA（通过 R1、R2 和 R3）到主机 PC-C 的跳数。单击 **Close**（关闭）继续操作。

第 3 步：使用本地数据库配置 AAA 用户认证。

启用 AAA 用户认证以使用 SSH 访问 ASA。运行 **Startup Wizard（启动向导）**时，您已经允许从内部网络和外部主机 PC-C 对 ASA 进行 SSH 访问。要允许管理员具有对 ASA 的 SSH 访问权限，需要在本地数据库中创建用户。

a. 在 **Configuration**（配置）界面→**Device Management**（设备管理）区域中，单击 **Users/AAA**（用户/AAA）。单击 **User Accounts**（用户账户）→**Add**（添加）。创建一个名为 **admin01** 的新用户，密码为 **admin01pass**，再次输入密码进行确认。允许此用户完全访问（ASDM、SSH、Telnet 和控制台）并将权限级别设置为 **15**，如图 8-33 所示。单击 **OK**（确定）添加用户，然后单击 **Apply**（应用），以将命令发送至 ASA。

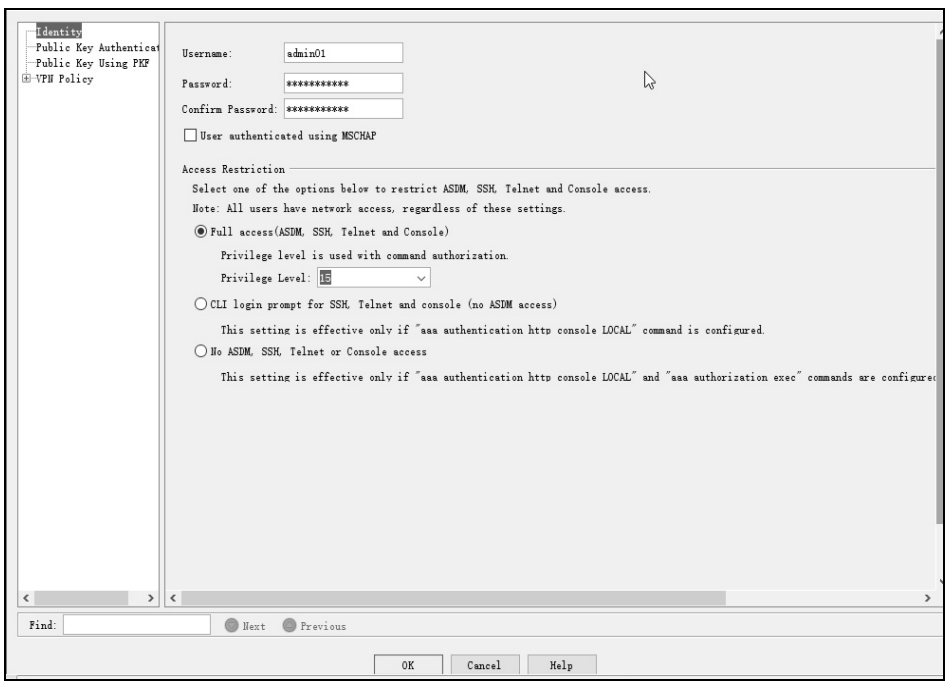

图 8-33　添加用户

b. 在 **Configuration**（配置）界面→**Device Management**（设备管理）区域中，单击 **Users/AAA**（用户/AAA），再单击 **AAA Access**（AAA 访问）。在 **Authentication**（认证）选项卡中，单击 **HTTP/ASDM** 和 **SSH** 复选框以要求对这些连接进行认证，并为每种连接类型指定 **LOCAL** 服务器组，如图 8-34 所示。单击 **Apply**（应用），以将命令发送至 ASA。

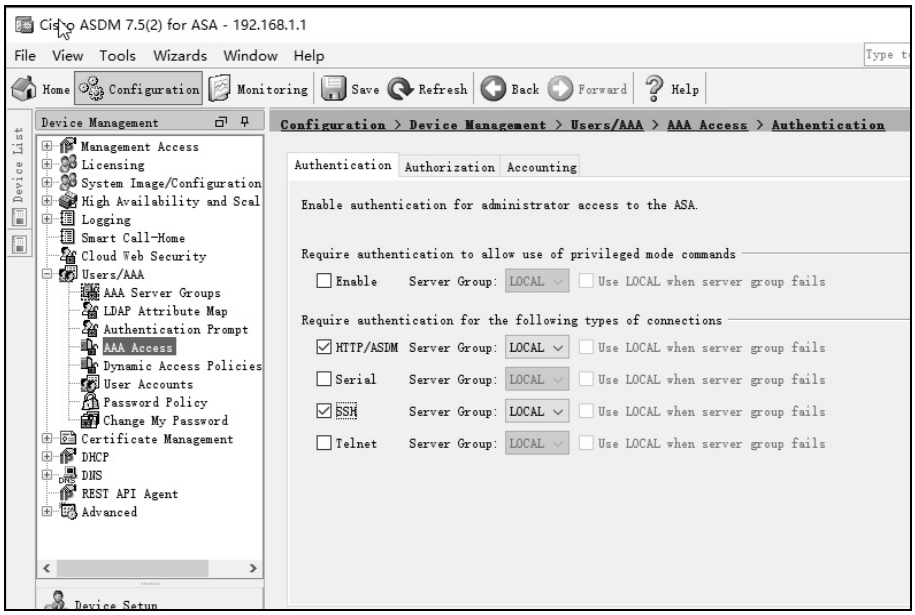

图 8-34　为连接指定 LOCAL 服务器组

注意：您在 ASDM 中尝试的下一项操作将要求您以 admin01 用户名，使用 admin01pass 密码登录。

第 4 步：测试 ASA 的 SSH 访问。

a．在 PC-B 上打开 SSH 客户端(例如 PuTTY)，并连接到 IP 地址为 **192.168.1.1** 的 ASA 内部接口，如图 8-35 所示。系统提示登录时，请输入用户名 **admin01** 和密码 **admin01pass**，如图 8-36 所示。

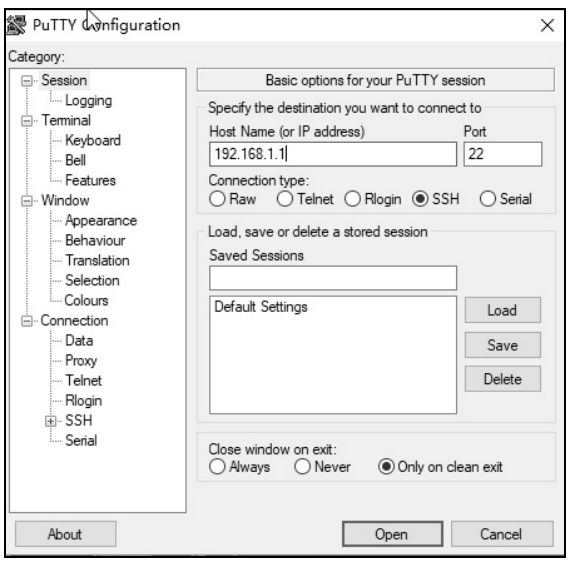

图 8-35　登录 PuTTY

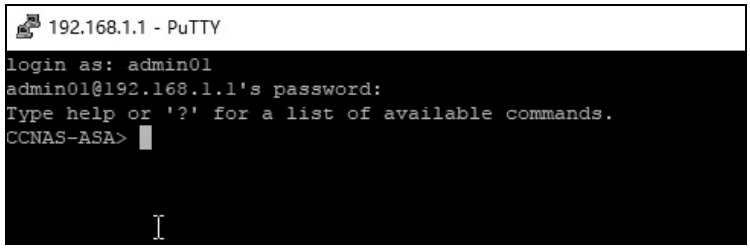

图 8-36　输入用户名和密码

b．从 PC-C 打开 SSH 客户端（例如 PuTTY），并尝试访问位于 **209.165.200.226** 的 ASA 外部接口。系统提示登录时，请输入用户名 **admin01** 和密码 **admin01pass**。

c．使用 SSH 登录 ASA 后，输入 enable 命令并提供密码 cisco12345。发出 show run 命令以显示您使用 ASDM 创建的当前配置，如图 8-37 所示。

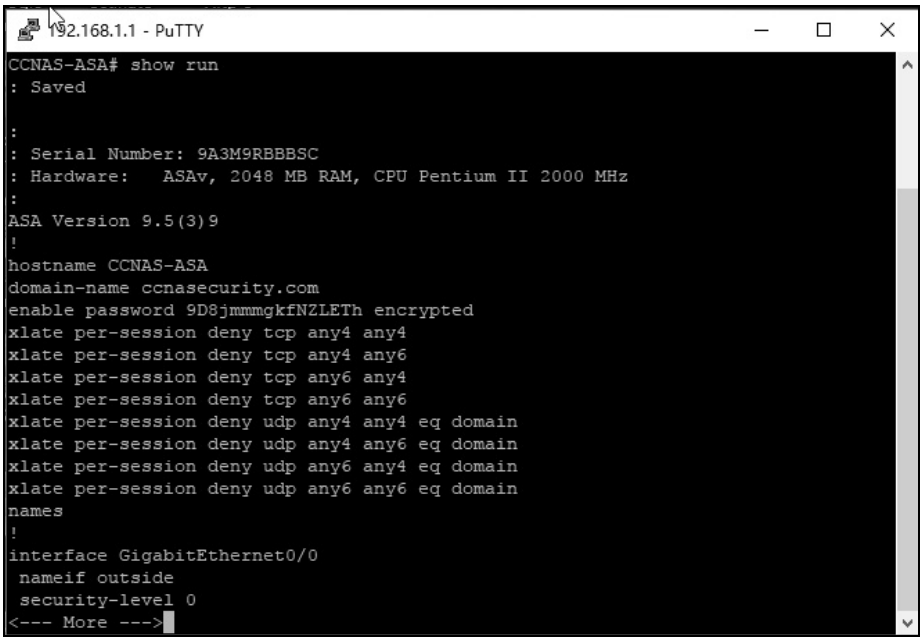

图 8-37　发出 show run 命令

注意：可以修改 SSH 的空闲超时。您可以使用 CLI logging synchronous 命令或转至 **Device Management**（设备管理）→**Management Access**（管理访问）→**ASDM/HTTP/Telnet/SSH** 来更改此设置。

第 5 步：修改 MPF 应用检查策略。

a．对于应用层检查和其他高级选项，可在 ASA 上使用思科 MPF。

默认全局检查策略不检查 ICMP。要使内部网络上的主机能够对外部主机执行 ping 操作并接收回复，必须检查 ICMP 流量。在 **Configuration**（配置）界面→**Firewall**（防火墙）区域中，单击 **Service Policy Rules**（服务策略规则），如图 8-38 所示。

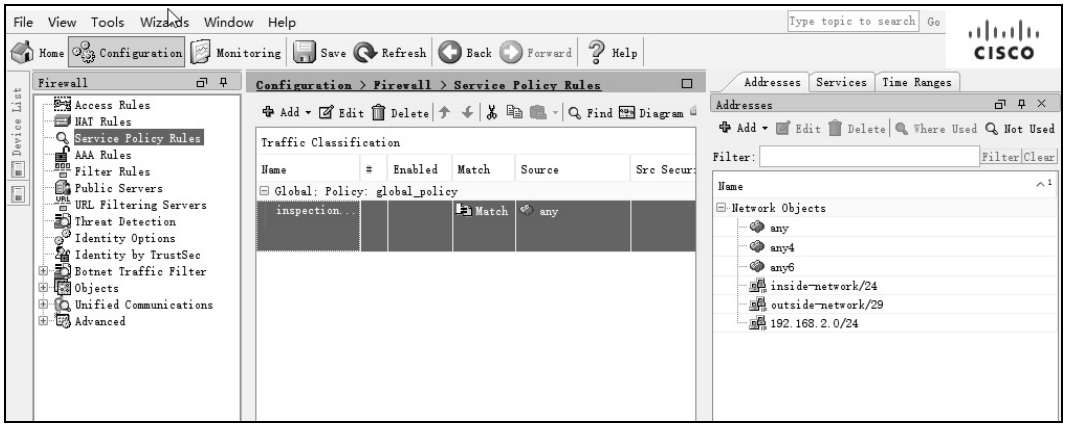

图 8-38　服务策略规则

b. 选择 **inspection_default** 策略，然后单击 **Edit**（编辑）以修改默认检查规则。在“Edit Service Policy Rule”（编辑服务策略规则）窗口中，单击 **Rule Actions**（规则操作）选项卡并选中 **ICMP** 复选框，如图 8-39 所示。请勿更改已检查的其他默认协议。单击 **OK**（确定）→**Apply**（应用），以将命令发送至 ASA。系统提示时，请以 **admin01** 身份使用密码 **admin01pass** 登录，如图 8-40 所示。

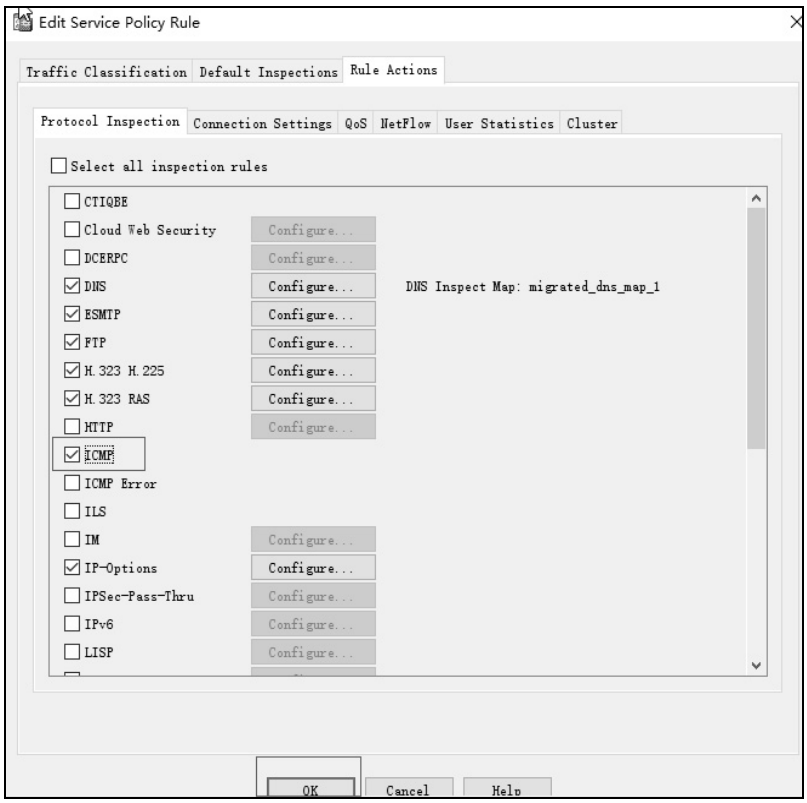

图 8-39　勾选 ICMP 复选框

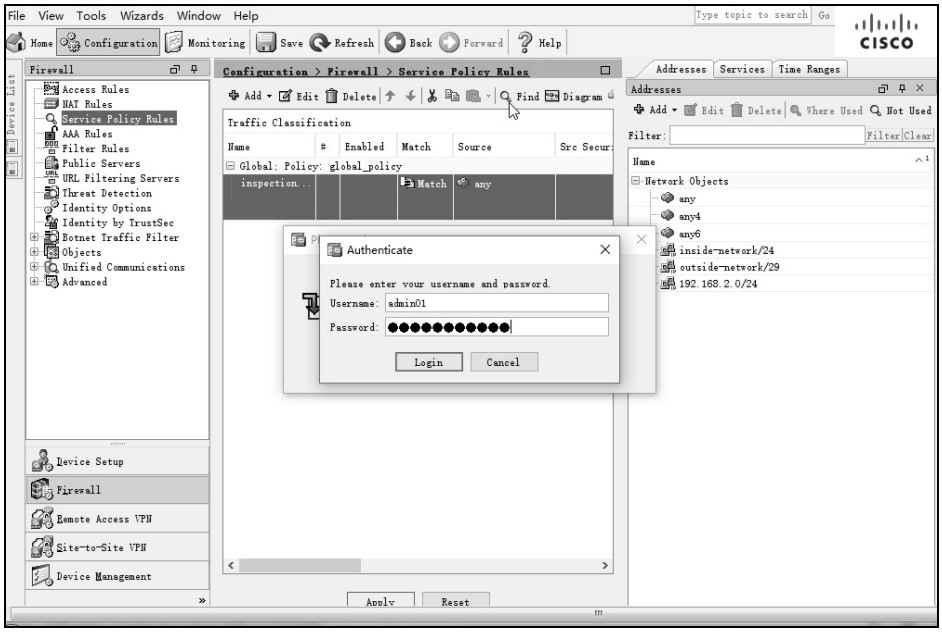

图 8-40　输入用户名和密码

c．从 PC-B 对 R1 的外部接口 S1/0（10.1.1.1）执行 ping 操作，如图 8-41 所示。Ping 操作应当能成功。

图 8-41　从 PC-B ping R1

任务 4：使用 ASDM 配置 DMZ 服务器、静态 NAT 和 ACL

1．任务目的

通过本任务，读者可以掌握：

- 配置 ASA DMZ 接口 G0/2；
- 配置 DMZ 服务器和静态 NAT；
- 查看 ASDM 生成的 DMZ 访问规则；
- 从外部网络对 DMZ 服务器的访问进行测试。

2．任务拓扑

本任务所用的拓扑如图 7-1 所示。

本任务的 IP 地址分配见表 7-1。

3．任务步骤

第 1 步：配置 ASA DMZ 接口 G0/2。

a．在 **Configuration**（配置）界面→**Device Setup**（设备设置）菜单上，单击 **Interfaces**（接口）。默认情况下将显示 **Interface**（接口）选项卡，并列出当前定义的内部接口（G0/1）和外部接口（G0/0）。单击 **Add**（添加），以创建新接口。在接口显示界面中，选择接口 **G0/2**，然后单击 **edit**（编辑）。在 **General**（常规）框下的 **Interface Name**（接口名称）中，将接口命名为 **dmz**，为其分配安全级别 **70**，并确保选中 **Enable Interface**（启用接口）复选框，如图 8-42 所示。

b．除内部接口和外部接口外，您应该还会看到名为 dmz 的新接口，如图 8-43 所示。选中 **Enable traffic between two or more interfaces which are configured with the same security levels**（启用使用相同安全级别配置的两个或多个接口之间的流量）单选框。单击 **Apply**（应用），以将命令发送至 ASA。

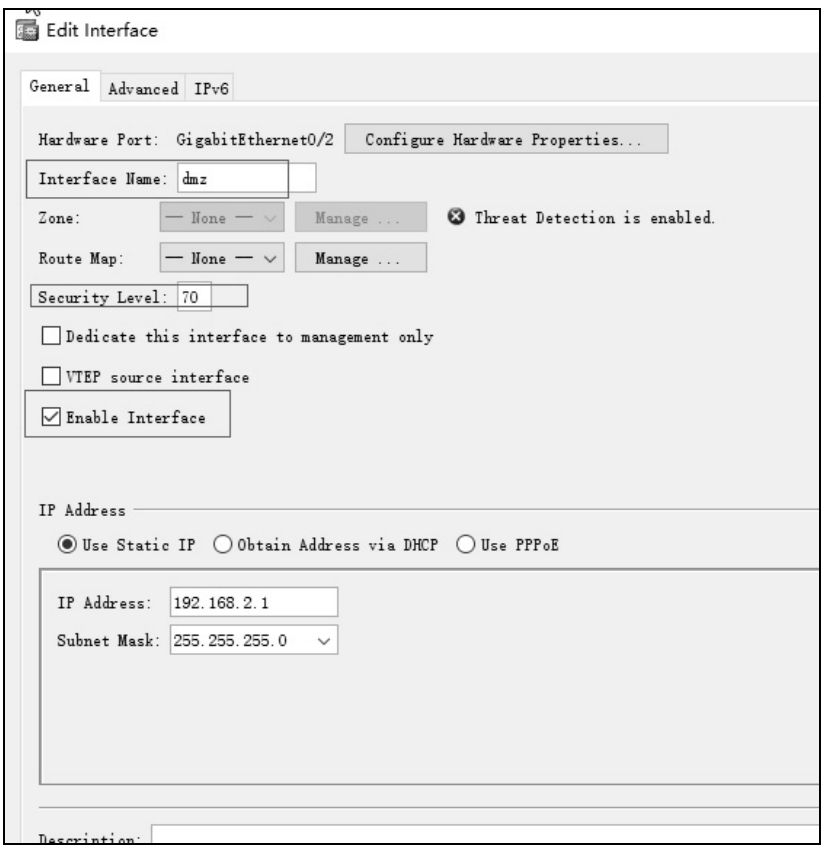

图 8-42　添加 DMZ 接口

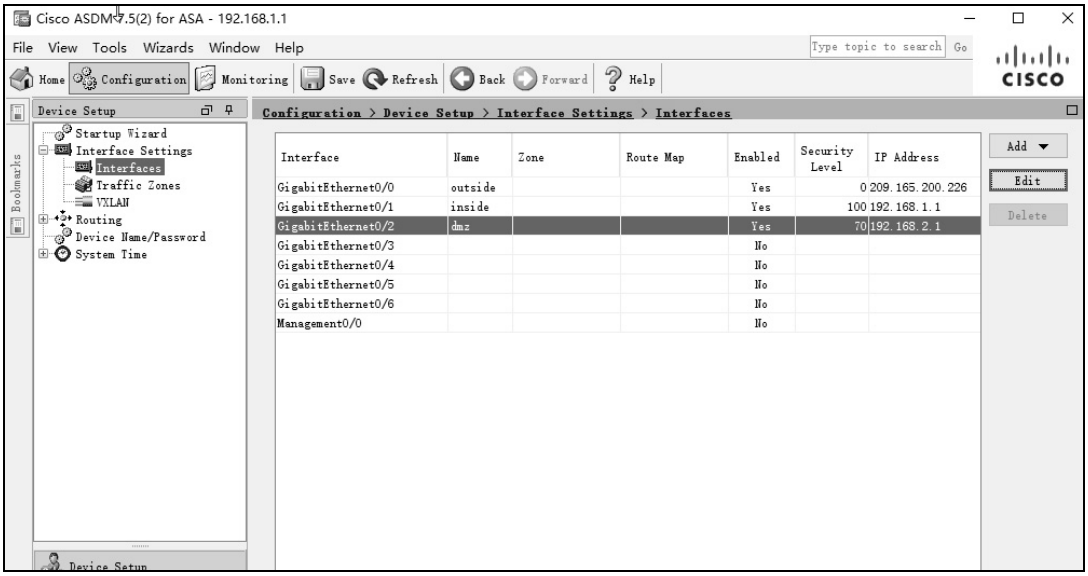

图 8-43　应用设置

第 2 步：配置 DMZ 服务器和静态 NAT。

a．在 **Firewall**（防火墙）菜单中，单击 **Public Servers**（公共服务器）选项，然后单击 **Add**（添加），以定义 DMZ 服务器和所提供的服务。在“Add Public Server”（添加公共服务器）对话框中，将专用接口指定为 **dmz**，将公共接口指定为 **outside**（外部），将公共 IP 地址指定为 **209.165.200.227**，如图 8-44 所示。

图 8-44　添加公共服务

b．单击 **Private IP Address**（专用 IP 地址）右侧的省略号按钮。在“Browse Private IP Address”（浏览器专用 IP 地址）窗口中，单击 **Add**（添加）以将该服务器定义为网络对象。在“Add Network Object”（添加网络对象）对话框中，输入名称

DMZ-Server，从 Type（类型）下拉菜单中选择 **Host**（主机），输入 IP 地址 **192.168.2.3** 以及 **PC-A** 的说明，如图 8-45 所示。

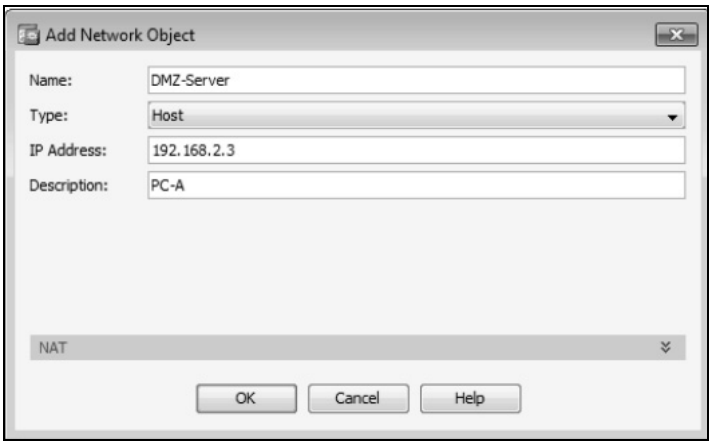

图 8-45　添加网络对象

c．在“Browse Private IP Address”（浏览器专用 IP 地址）窗口中，验证 **DMZ-Server** 是否出现在“Selected Private IP Address”（选定的专用 IP 地址）字段中，然后单击 **OK**（确定），如图 8-46 所示。您将返回到“Add Public Server”（添加公共服务器）对话框。

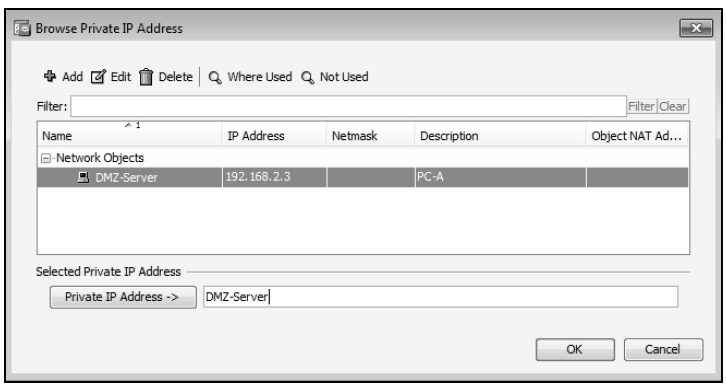

图 8-46　验证专用 IP 地址

d．在“Add Public Server”（添加公共服务器）对话框中，单击 **Private Service**（专用服务）右侧的省略号按钮。在“Browse Private Service”（浏览专用服务）窗口中，双击以选择 **tcp/ftp**、**tcp/http**、**icmp/echo** 和 **icmp/echo-reply**（向下滚动可查看所有服务）服务。单击 **OK**（确定）继续并返回到“Add Public Server”（添加公共服务器）对话框。

注意：如果公共服务与私有服务不同，则可以使用此界面上的选项指定公共服务。

e．填写好“Add Public Server”（添加公共服务器）对话框中的所有信息，如图 8-47 所示。单击 **OK**（确定），添加该服务器。在“Public Servers”（公共服务器）界面中，单击 **Apply**（应用）以将命令发送至 ASA。

图 8-47　填写“添加公共服务”对话框

第 3 步：查看 ASDM 生成的 DMZ 访问规则。

a．创建 DMZ 服务器对象和选择服务后，ASDM 会自动生成访问规则（ACL）以允许对服务器的适当访问，并将该规则应用于传入方向的外部接口。

b．要在 ASDM 中查看此 ACL，请依次单击 **Configuration**（配置）→**Firewall**（防火墙）→**Access Rules**（访问规则）。它显示为外部传入规则。您可以选择此规则并使用水平滚动条查看所有组件，如图 8-48 所示。

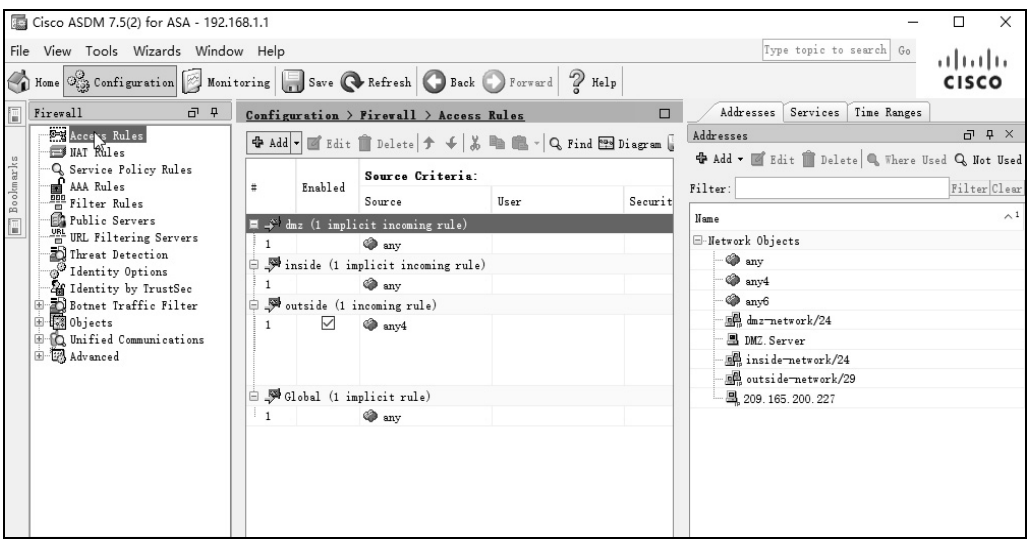

图 8-48　访问规则

注意：您还可以使用 **Tools**（工具）→**Command Line Interface**（命令行界面）并输入 show run 命令来查看这些内容。

第 4 步：从外部网络对 DMZ 服务器的访问进行测试。

a. 从 PC-C 对静态 NAT 公共服务器地址（209.165.200.227）的 IP 地址执行 ping 操作。Ping 操作应当能成功，如图 8-49 所示。

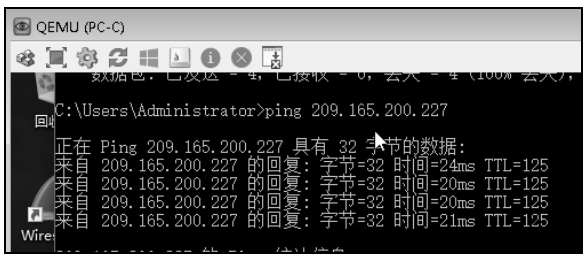

图 8-49　从 PC-C ping 209.165.200.227

b. ASA 内部接口（G0/1）的安全级别被设置为 100（最高），DMZ 接口（G0/2）的安全级别被设置为 70，您还可以从内部网络上的主机访问 DMZ 服务器。ASA 的作用类似两个网络之间的路由器，从内部网络主机 PC-B（192.168.1.3）对 DMZ 服务器（PC-A）内部地址（**192.168.2.3**）执行 ping 操作。接口安全级别被设置并且已按照全局检查策略检查了内部接口上的 ICMP，因此 ping 操作应当会成功，如图 8-50 所示。

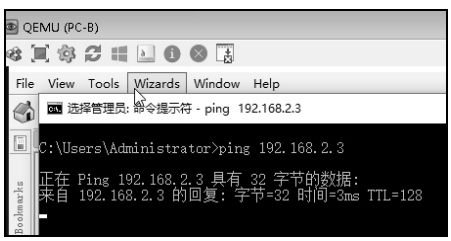

图 8-50　从 PC-B ping PC-A

c. DMZ 服务器无法对内部网上的 PC-B 执行 ping 操作，因为 DMZ 接口 G0/2 的安全级别较低并且在创建接口 G0/2 时有必要指定 no forward 命令。可以尝试从 DMZ 服务器 PC-A 对位于 IP 地址 **192.168.1.3** 处的 PC-B 执行 ping 操作。ping 操作应当不会成功，如图 8-51 所示。

图 8-51　从 PC-A ping PC-B

第 5 步：使用 ASDM 监控功能来绘制数据包活动图。

我们可以使用 Monitoring（监控）界面监控 ASA 的方方面面。此界面上的主要类别包括接口、VPN、路由、属性和日志记录。在此步骤中，您将创建一个图形来监控外部接口的数据包活动。

a．在 **Monitoring**（监控）界面→**Interfaces**（接口）菜单中，单击 **Interface Graphs**（接口图）→**outside**（外部）。选择 **Packet Counts**（数据包计数），然后单击 **Add**（添加）以添加图形。图 8-52 显示了已添加数据包计数的情形。

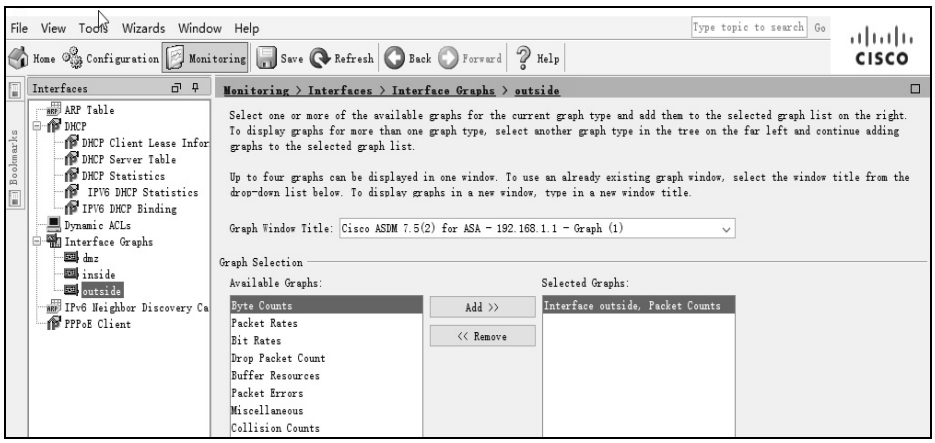

图 8-52　已添加数据包计数的情形

b．单击 **Show Graphs**（显示图形），来显示图形。最初，没有显示流量，如图 8-53 所示。

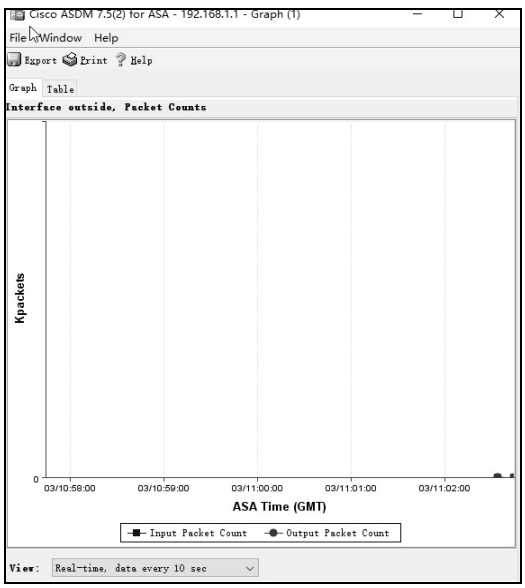

图 8-53　显示图形

c. 根据 R2 上的特权模式命令提示符，通过对重复计数为 1000 的 DMZ 服务器公共地址执行 ping 操作，来模拟 ASA 的互联网流量。如有需要，可以增加 ping 操作的次数。

```
R2# ping 209.165.200.227 repeat 1000
      Type escape sequence to abort.
      Sending 1000, 100-byte ICMP Echos to 209.165.200.227, timeout is
      2 seconds:
      !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
      !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
      <output omitted>
      !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
      !!!!!!!!!!!!!!!!!!!
      Success rate is 100 percent (1000/1000), round-trip min/avg/max =
      1/2/12 ms
```

d. 您可以在图 8-54 上看到来自 R2 的 ping 操作结果，显示为输入数据包计数。图形的比例将自动调整，具体取决于流量。您还可以单击 **Table**（表）选项卡以表格形式查看数据。请注意，“Graph”（图形）界面左下角选择的 **View**（视图）是每 10s 及时更新一次的数据。单击下拉列表以查看其他可用选项。

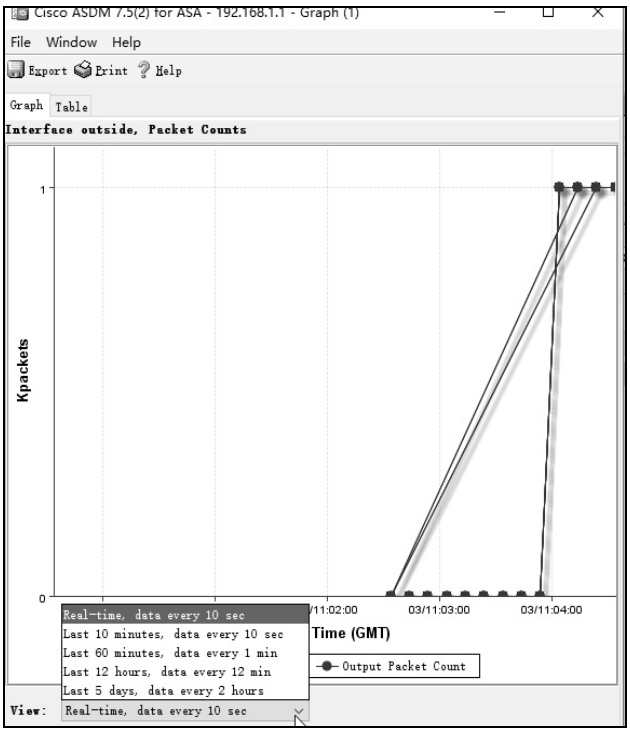

图 8-54　来自 R2 的 ping 操作结果

e. 使用–n 选项（数据包的数量）从 PC-B 对 **10.1.1.1** 处的 R1 接口 S1/0 执行 ping 操作，以指定 100 个数据包，如图 8-55 所示。结果如图 8-56 所示。

图 8-55　从 PC-B ping R1

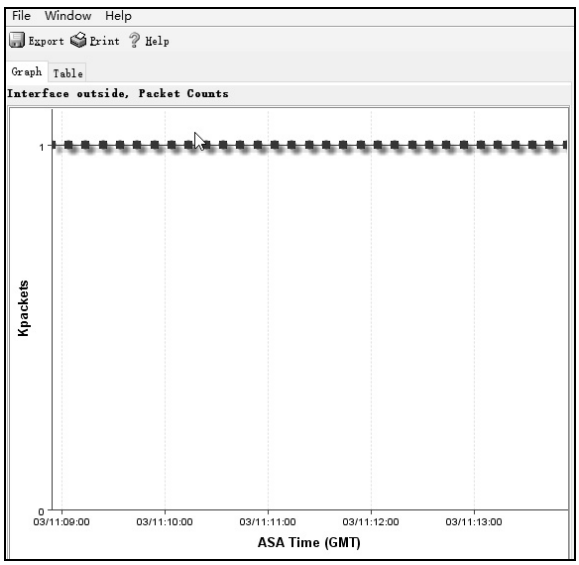

图 8-56　从 PC-B 对 **10.1.1.1** 执行 ping 操作的结果