配置 ASA Virtual

ASA Virtual部署会预配置 ASDM 访问。您可以使用网络浏览器从您在部署过程中指定的客户端 IP 地址连接到ASA Virtual管理IP地址。本章还介绍如何允许其他客户端访问ASDM以及如何允许CLI访问（SSH 或 Telnet）。本章涵盖的其他必要配置任务包括安装许可证和 ASDM 中的向导提供的常见配置任务。

启动 ASDM

过程

步骤 1 在指定为 ASDM 客户端的 PC 上，输入以下 URL：

https://*asa_ip_address*/**admin**

系统将显示 ASDM 启动窗口和以下按钮：

- **安装 ASDM 启动程序并运行 ASDM (Install ASDM Launcher and Run ASDM)**
- **Run ASDM**
- **运行启动向导 (Run Startup Wizard)**

步骤 2 要下载启动程序，请执行以下操作：

a) 点击**安装 ASDM 启动程序并运行 ASDM (Install ASDM Launcher and Run ASDM)**。

b) 将用户名和密码字段留空（适用于新安装），然后点击**确定 (OK)**。如果未配置 HTTPS 身份验证，可以在没有用户名和 **enable** 密码（默认为空）的情况下获得对 ASDM 的访问权限。如果您启用了 HTTPS 身份验证，则输入您的用户名及关联的密码。

c) 将安装程序保存到 PC，然后启动安装程序。安装完成后，将自动打开 ASDM-IDM 启动程序。

d) 输入管理 IP 地址，将用户名和密码留空（适用于新安装），然后点击**确定 (OK)**。如果您启用了 HTTPS 身份验证，则输入您的用户名及关联的密码。

步骤 3 要使用 Java Web Start，请执行以下操作：

a) 点击**运行 ASDM (Run ASDM)** 或**运行启动向导 (Run Startup Wizard)**。
b) 出现提示时，将快捷方式保存到计算机上。或者，也可以选择打开快捷方式，而不是保存快捷方式。
c) 从该快捷方式启动 Java Web Start。
d) 根据显示的对话框接受所有证书。系统将显示思科 ASDM-IDM 启动程序。
e) 将用户名和密码留空（适用于新安装），然后点击**确定 (OK)**。如果您启用了 HTTPS 身份验证，则输入您的用户名及关联的密码。

使用 ASDM 执行初始配置

您可以使用以下 ASDM 向导和程序执行初始配置。

- 运行启动向导
- （可选）允许访问 ASA Virtual后面的公共服务器
- （可选）运行 VPN 向导
- （可选）在 ASDM 中运行其他向导

有关 CLI 配置，请参阅《思科 Cisco Secure Firewall ASA 系列 CLI 配置指南》。

运行启动向导

运行 **Startup Wizard**，自定义适合您的部署的安全策略。

过程

步骤 1 依次选择**向导 (Wizards)** > **启动向导 (Startup Wizard)**。
步骤 2 自定义适合您的部署的安全策略。您可以设置以下各项：

- 主机名
- 域名
- 管理密码
- 接口
- IP 地址
- 静态路由

- DHCP 服务器
- 网络地址转换规则
- 以及更多设置...

（可选）允许访问 ASA Virtual后面的公共服务器

配置 (Configuration) > **防火墙 (Firewall)** > **公共服务器 (Public Servers)** 窗格会自动将安全策略配置为使内部服务器可从互联网访问。作为业务主管，您可能具有需要向外部用户开放的内部网络服务，如 Web 和 FTP 服务器。您可以将这些服务放置在 ASA Virtual 后面称为隔离区 (DMZ) 的单独网络中。通过将公共服务器放置在 DMZ 中，对公共服务器发起的任何攻击都不会影响您的内部网络。

（可选）运行 VPN 向导

您可以使用以下向导配置 VPN (**Wizards** > **VPN Wizards**)：

- 站点间 VPN 向导 - 在 ASA Virtual与另一个支持 VPN 的设备之间创建 IPsec 站点间隧道。
- AnyConnect VPN 向导 - 为思科 AnyConnect VPN 客户端配置 SSL VPN 远程访问。Secure Client 通过企业资源的全 VPN 隧道来为远程用户提供到 ASA 的安全 SSL 连接。您可以将 ASA 策略配置为当远程用户首次通过浏览器连接时下载 Secure Client。使用 Secure Client 3.0 及更高版本，客户端可以运行 SSL 或 IPsec IKEv2 VPN 协议。
- 无客户端 SSL VPN 向导 - 配置浏览器的无客户端 SSL VPN 远程访问。通过基于浏览器的无客户端 SSL VPN，用户可以使用网络浏览器与 ASA 建立安全的远程访问 VPN 隧道。在身份验证之后，用户将访问门户页，并且可以访问特定的受支持内部资源。网络管理员以组为基础按用户提供资源访问。可以应用 ACL 来限制或允许对特定企业资源的访问。
- IPsec（IKEv1 或 IKEv2）远程访问 VPN 向导 - 配置 Cisco IPsec 客户端的 IPsec VPN 远程访问。

有关如何配置与 Azure 的 ASA Virtual IPsec Virtual Tunnel Interface (VTI) 连接的信息，请参阅配置与 Azure 的 ASA IPsec VTI 连接。

（可选）在 ASDM 中运行其他向导

您可以在ASDM中运行其他向导，配置可实现高可用性的故障转移、VPN集群负载均衡和数据包捕获。

- 高可用性和可扩展性向导 - 配置故障转移或 VPN 负载均衡。
- 数据包捕获向导 - 配置和运行数据包捕获。该向导在每个入口接口和出口接口上运行一次数据包捕获。捕获数据包之后，您可以将数据包捕获结果保存到PC，从而在数据包分析仪中进行检查和重放。

高级配置

要继续配置您的 ASA Virtual，请参阅 Cisco Secure Firewall ASA 系列文档导航。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。