项目 1　防火墙基础知识

案例场景

小蔡毕业后入职了 CY 公司的信息技术部门，负责公司防火墙产品的网络运维工作。入职第一天，项目经理给他安排了两个任务：第一，要求小蔡在办公计算机上安装 eNSP 仿真环境，并且要能够支持防火墙，通过仿真熟悉防火墙的相关技术。第二，通过搭建网络拓扑，熟悉 Wireshark 软件的常规操作，比如捕获常见 TCP/IP 协议栈报文，以方便后期进行网络拓扑排错。

1.1　知 识 引 入

1.1.1　防火墙基本概念

“防火墙”一词起源于建筑领域，用来隔离火灾，阻止火势从一个区域蔓延到另一个区域。防火墙这一具体设备引入通信领域，通常表示两个网络之间有针对性的、逻辑意义上的隔离。这种隔离是选择性的，隔离“火”的蔓延，而又保证“人”可以穿墙而过。这里的“火”是指网络中的各种攻击，而“人”是指正常的通信报文。

在通信领域，防火墙是一种安全设备，它用于保护一个网络区域免受来自另一个网络区域的攻击和入侵，通常被应用于网络边界，如企业互联网出口、企业内部业务边界、数据中心边界等。

防火墙在企业边界防护、内网管控与安全隔离、数据中心边界防护、数据中心安全联动等场景中起着重要作用。图 1-1 是防火墙在企业边界防护中的应用场景。

1.1.2　防火墙产品分类

产品分类主要可以从形态和技术原理上进行划分。

1. 按形态分类

防火墙产品从形态上可以分为硬件防火墙和软件防火墙两大类。软件防火墙运行于特定的计算机上，它需要客户预先安装好计算机操作系统。软件防火墙就像其他的软件产品一样，需要先在计算机上安装并做好配置才可以使用。常见的软件防火墙有 Windows 系统防火墙、Linux 系统的防火墙 Iptables，以及其他各安全厂家的软件防火墙。软件防火墙以个人用户使用为主。

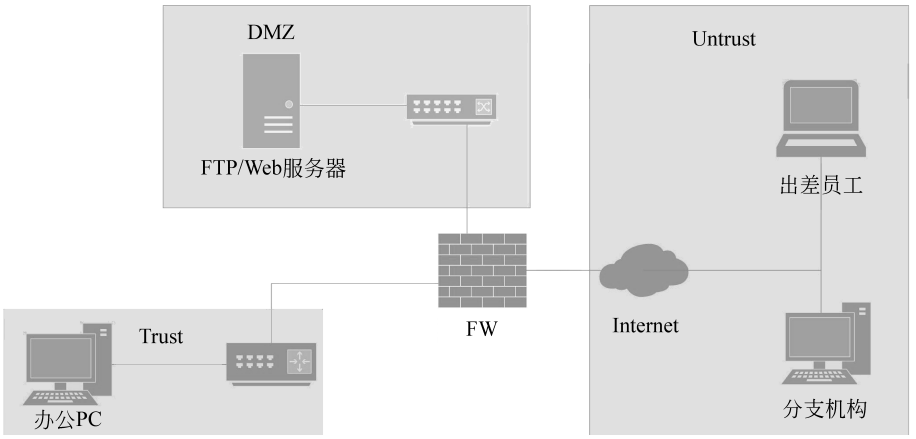

图 1-1　防火墙企业边界防护应用场景

硬件防火墙从形态上可以分为盒式防火墙、桌面型防火墙、框式防火墙，以华为防火墙产品为例，如图 1-2～图 1-4 所示。

图 1-2　盒式防火墙

图 1-3　桌面型防火墙

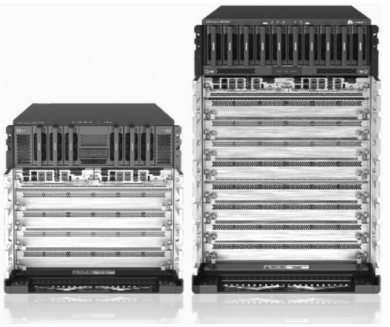

图 1-4　框式防火墙

2. 按技术原理分类

从技术原理角度观察防火墙，防火墙经历了包过滤防火墙、代理防火墙、状态检测防火墙、统一威胁管理（united threat management，UTM）防火墙、下一代防火墙（next generation firewall，NGFW）、AI 防火墙，从其发展的历程来看有以下特点：①访问控制越来越精细；②防护能力越来越强；③性能越来越高。下面简单介绍几种防火墙。

包过滤防火墙通过配置访问控制列表（access control list，ACL）实施数据包的过滤，主要基于数据包中的源 / 目的 IP 地址、源 / 目的端口号、IP 标识和报文传递的方向等信息。

状态检测防火墙就是支持状态检测功能的防火墙。状态检测是包过滤技术的发展，它考虑报文前后的关联性，检测的是连接状态而非单个报文。状态检测防火墙通过对连接的首个数据包（后续简称首包）检测而确定一条连接的状态。后续数据包根据所属连接的状态进行控制（转发或阻塞）。本书主要介绍这种防火墙。

AI 防火墙是结合 AI 技术的新一代防火墙。它通过结合 AI 算法或 AI 芯片等多种方式，进一步提高了防火墙的安全防护能力和性能。

1.1.3　支持防火墙仿真环境的 eNSP 软件

本书实验环境采用 eNSP（enterprise network simulation platform），这是一款由华为提供的、可扩展的、采用图形化操作方式的网络仿真工具平台。该平台可以很方便地进行交换机、路由器、防火墙等网络设备的仿真实验，其图形界面如图 1-5 所示。

图 1-5　eNSP 图形界面

安装支持防火墙仿真环境的 eNSP 软件需要准备 WinPcap、Wireshark、VirtualBox、USG6000V.zip 设备包，各文件主要作用说明如下。

（1）WinPcap：WinPcap（Windows packet capture）是 Windows 平台中一个免费、公共的网络访问系统。

（2）Wireshark：网络封包分析软件的功能是截取网络封包，并尽可能显示出最为详细的网络封包资料。

（3）Virtualbox：这是一款虚拟机产品，eNSP 中所使用路由器、交换机、防火墙等网络设备需要通过该产品虚拟化运行后使用。

（4）USG6000V.zip 设备包：下载解压后得到 vfw_usg.vdi 文件，该文件是防火墙设备包文件。它需要在安装好 eNSP 后，首次使用防火墙虚拟设备时需要进行导入。

注意：以上软件在进行安装时需要根据系统选择合适的版本。本书在 Windows 10 环境下选用相关软件版本如下，供参考。

- WinPcap 采用的版本是 WinPcap_4_1_3；
- Wireshark 采用的版本是 Wireshark_v3.0.0rc2；
- VirtualBox 采用的版本是 VirtualBox-5.2.26-128414-Win；
- eNSP 模拟器采用的版本是 eNSP V100R003C00SPC100。

1.1.4　TCP/IP 协议栈及典型代表协议

TCP/IP（transmission control protocol/Internet protocol，传输控制协议 / 网际协议）是

指能够在多个不同网络间实现信息传输的协议簇。TCP/IP 不仅仅指的是 TCP 和 IP 两个协议，而是指一个由 FTP、SMTP、TCP、UDP、IP 等协议构成的协议簇，只是因为在 TCP/IP 中 TCP 和 IP 最具代表性，所以被称为 TCP/IP。

TCP/IP 是 Internet 最基本的协议，它采用四层结构，如图 1-6 所示。应用层的主要协议还有 Telnet、FTP、SMTP 等，它们是用来接收来自传输层的数据或者按不同应用要求与方式将数据传输至传输层；传输层的主要协议有 UDP、TCP，是使用者使用平台和计算机信息网内部数据结合的通道，可以实现数据传输与数据共享；网络层的主要协议有 ICMP、IP、IGMP，主要负责网络中数据包的传送等；网络访问层也叫网络接口层或数据链路层，主要协议有 ARP、RARP 等，主要功能是提供链路管理错误检测，并对不同通信媒介有关信息细节问题进行有效处理。

应用层	HTTP/Telnet/FTP/TFTP/DNS	提供应用程序接口
传输层	TCP/UDP	建立端到端连接
网络层	IP ICMP/IGMP, ARP/RARP	寻址和路由选择
数据链路层	Ethernet/802.3/PPP/HDLC/FR	物理介质访问

图 1-6　TCP/IP 协议栈各层典型代表协议

1.1.5　Wireshark 工具介绍

Wireshark 是一个网络封包分析软件。Wireshark 使用 WinPcap 作为接口，直接与网卡进行数据报文交换。图 1-7 是 Wireshark 工作主界面。

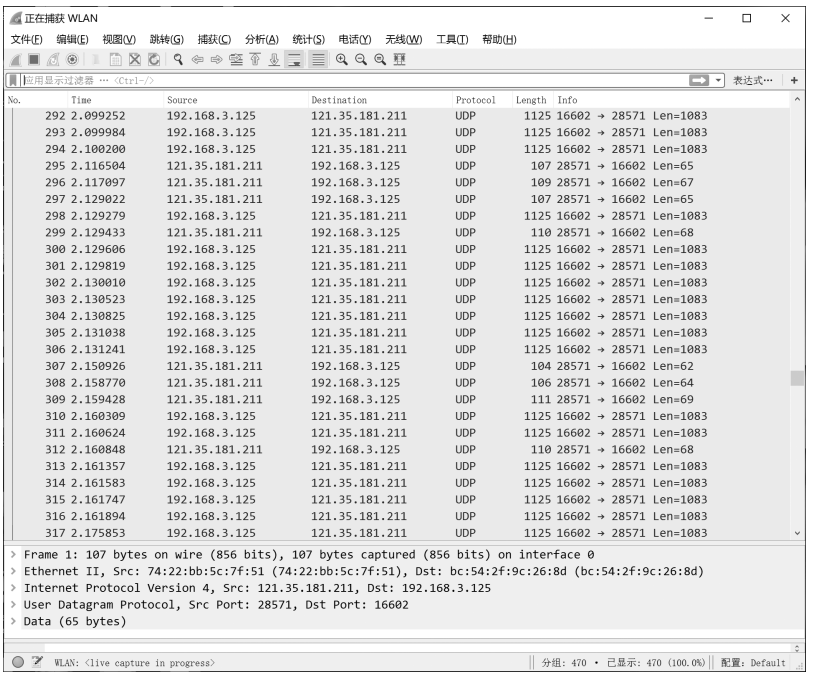

图 1-7　Wireshark 工作主界面

eNSP 中可以调用 Wireshark 进行网络数据包捕获，从而对捕获的数据包进行数据分析和网络排错的任务。图 1-8 是在 eNSP 中调用 Wireshark 的一个例子。

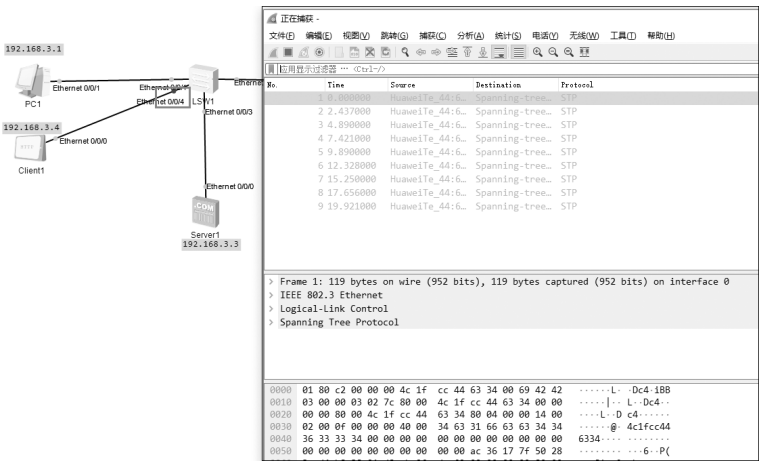

图 1-8　在 eNSP 中调用 Wireshark 界面

1.2　任务 1：安装支持防火墙仿真环境的 eNSP 软件

1.2.1　任务说明

在 Windows10 操作系统上安装支持防火墙仿真环境的 eNSP 软件。

任务 1　安装支持防火墙仿真环境的 eNSP 软件

1.2.2　任务实施过程

1. 明确安装顺序

WinPcap、Wireshark、VirtualBox 这三款软件在安装华为 eNSP 模拟器前需要提前安装好，安装顺序依次是 WinPcap、Wireshark、VirtualBox，注意要以管理员权限运行。按照默认路径选择下一步进行安装即可，操作过程比较简单，在此省略。

2. 安装华为 eNSP 模拟器

（1）以管理员身份双击运行 eNSP_Setup.exe，出现如图 1-9 所示的对话框，选择“中文（简体）”。

图 1-9　选择安装语言界面

（2）在图 1-10 的安装向导对话框中单击“下一步”按钮。

图 1-10　安装向导对话框（1）

（3）在图 1-11 的安装向导对话框中选中“我愿意接受此协议”选项，单击“下一步”按钮。

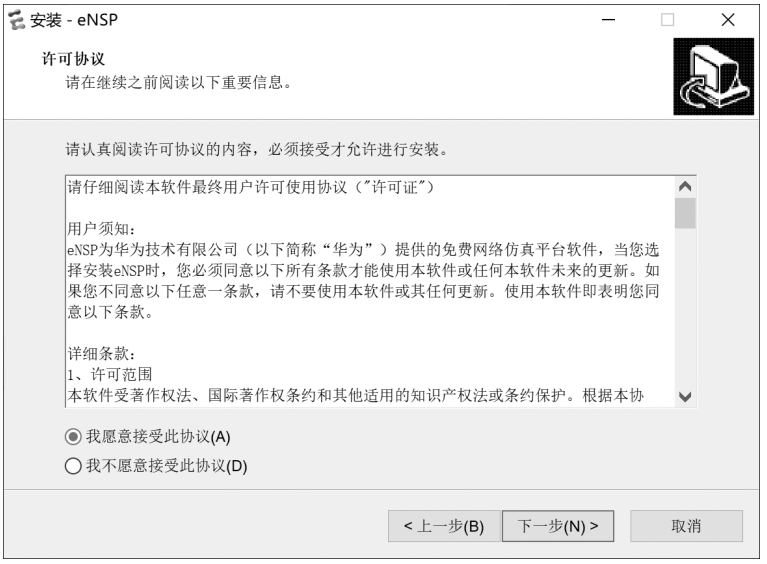

图 1-11　安装向导对话框（2）

（4）在图 1-12 的安装向导对话框中选择安装路径，单击“下一步”按钮。

（5）在图 1-13 的安装向导对话框中选择安装文件夹，单击“下一步”按钮。

（6）在图 1-14 的安装向导对话框中选中“创建桌面快捷图标”选项，单击“下一步”按钮。

图 1-12　安装向导对话框（3）

图 1-13　安装向导对话框（4）

图 1-14　安装向导对话框（5）

（7）在图 1-15 的安装向导对话框中单击“下一步”按钮，因为之前已经安装了 WinPcap、Wireshark、VirtualBox 软件，所以这里能检测到。如果没有安装，需要先完成以上软件的安装。

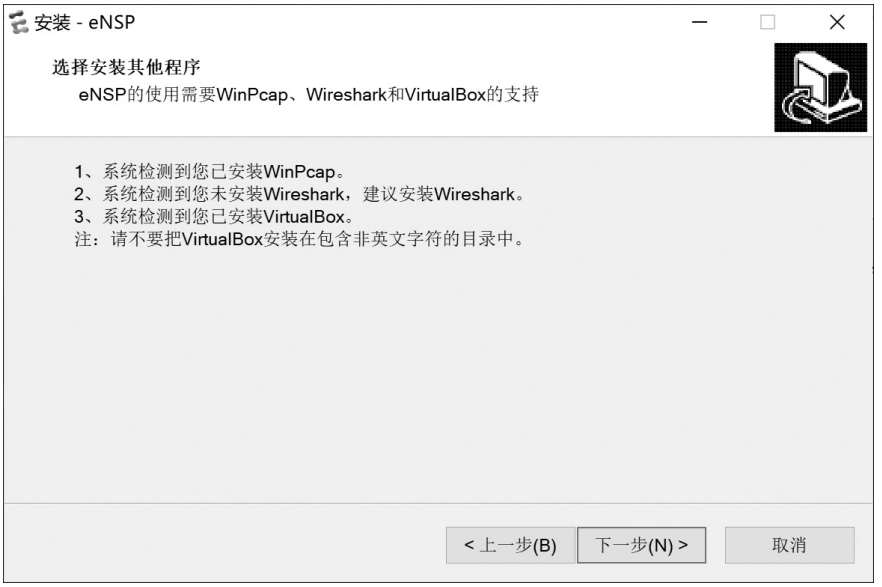

图 1-15　安装向导对话框（6）

（8）在图 1-16 中的安装向导对话框中单击“安装”按钮。

图 1-16　安装向导对话框（7）

（9）进入图 1-17 中的安装向导对话框进行安装。

（10）安装完成后，进入图 1-18 中的安装完成对话框。选中“运行 eNSP”选项，单击

“完成”按钮，即可运行软件。

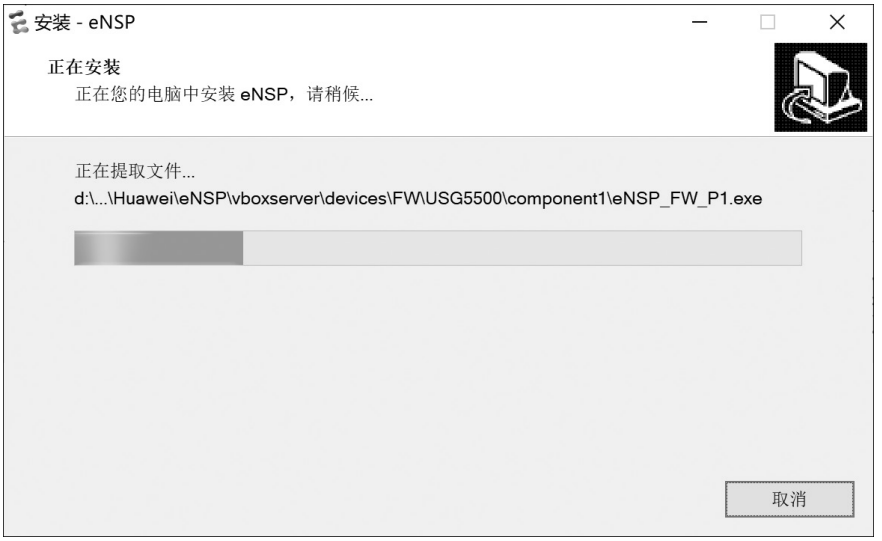

图 1-17　安装向导对话框（8）

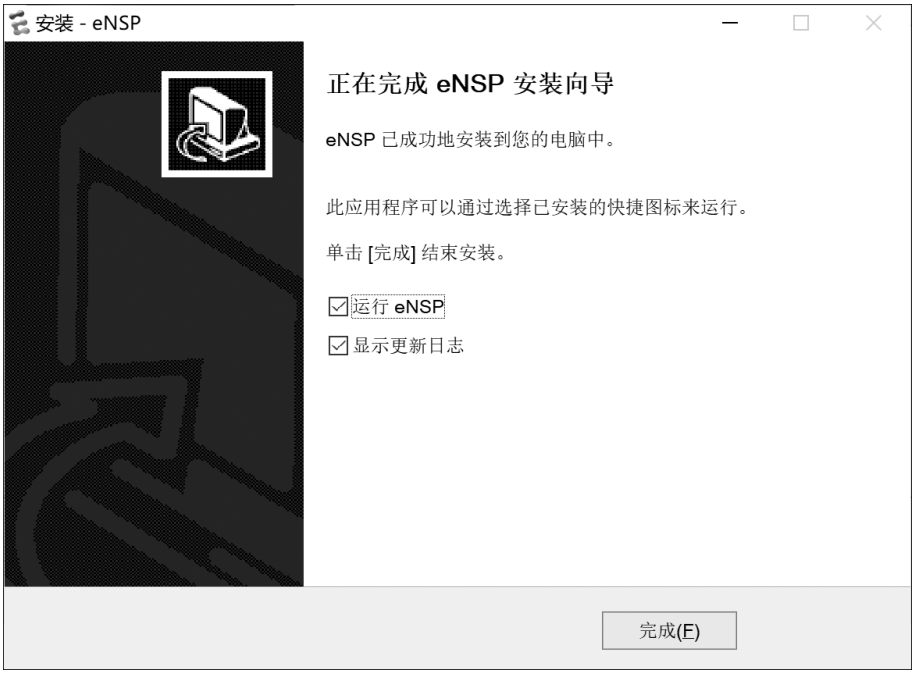

图 1-18　安装向导对话框（9）

3. 导入 USG6000V.zip 设备包

（1）运行 eNSP 模拟器，新建一个网络拓扑，拖入 USG6000V 防火墙中，如图 1-19 所示。

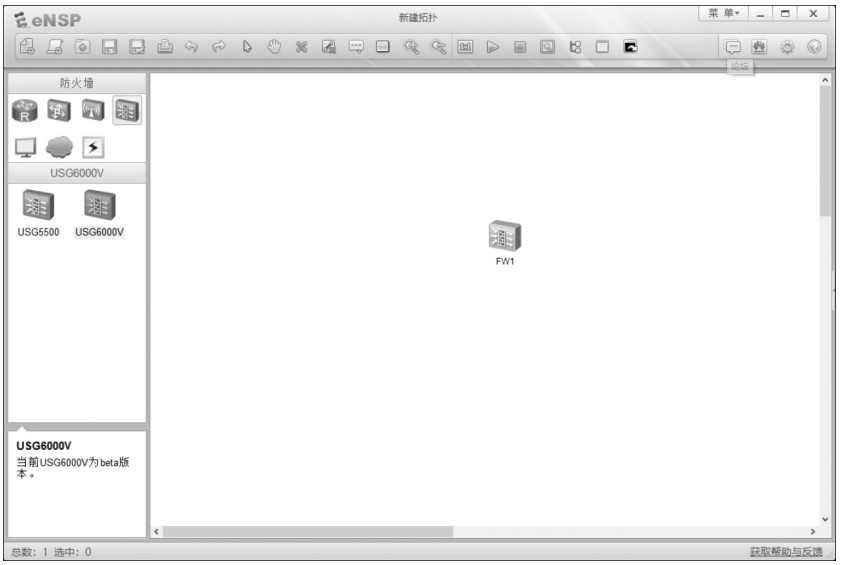

图 1-19　拖入防火墙后的界面

（2）选中防火墙，然后右击并从快捷菜单中选择“启动”命令，启动防火墙，如图 1-20 所示。

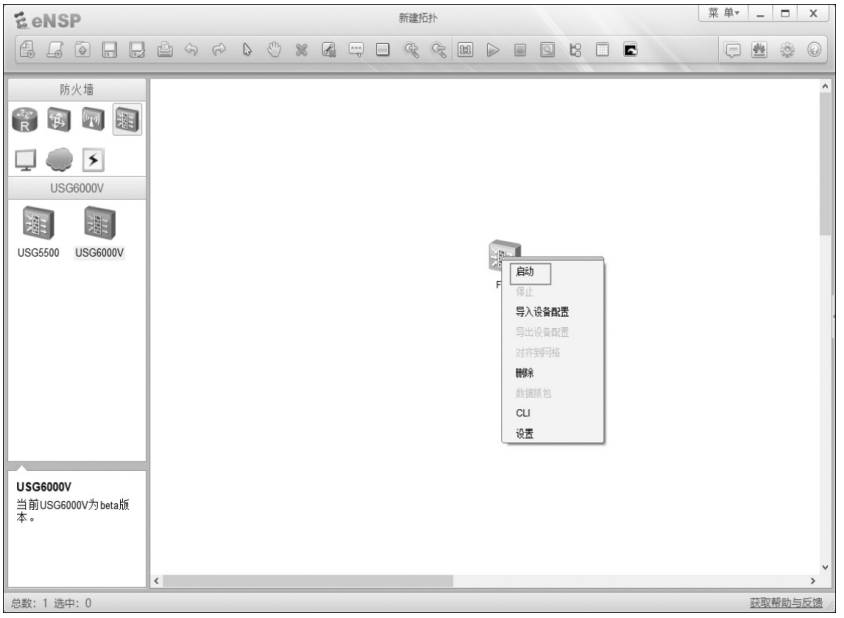

图 1-20　启动防火墙

（3）初次启动防火墙，弹出“导入设备包”对话框，提示需要导入设备包，如图 1-21 所示。

（4）单击步骤（3）中的“浏览”按钮后，出现如图 1-22 所示对话框，在文件系统中选择准备好的 vfw_usg.vdi 文件（注意该文件要从 USG6000V.zip 设备包中解压）。