实验十二：利用防火墙实现 VPN

一、实验简介

园区网内部的一些重要资源通常只允许园区网内部用户访问，因为位于互联网的用户主机在访问园区网内部服务器时，数据传输要经过 Internet，而 Internet 中存在多种不安全因素，有可能造成数据泄密、重要数据被破坏等后果。但是，当园区网用户位于互联网上时（称为“远程用户”），例如用户出差在外，此时访问园区网内部资源时，就会因受到限制而无法完成有关工作。为了使位于互联网上的园区网远程用户能够安全的访问园区网内部资源，可以使用 VPN 方式。

本实验在 eNSP 中构建两个网络，分别用来表示内部网和外部网，内部网用户通过 NAT 访问外部网。以 CLI 方式在内部网边界防火墙上配置 SSL VPN，采用本地认证，使得外部网用户可以通过 SSL VPN 访问内部网主机。

二、实验目的

1、以 CLI 方式完成防火墙上 SSL VPN 的配置；
2、实现外部网用户通过 SSL VPN 访问内部网中的主机。

三、实验类型

综合性

四、实验理论

1. VPN

VPN（Virtual Private Network）即虚拟专用网，用于在公用网络上构建私人专用虚拟网络，并在此虚拟网络中传输私网流量。VPN 把现有的物理网络分解成逻辑上隔离的网络，在不改变网络现状的情况下实现安全、可靠的连接。

在 VPN 出现之前，跨越 Internet 的数据传输只能依靠现有物理网络，具有很大的不安全因素。例如，某企业的总部和分支机构位于不同区域（比如位于不同的国家或城市），当分支机构员工需访问总部服务器的时候，数据传输要经过 Internet。由于 Internet 中存在多种不安全因素，则当分支机构的员工向总部服务器发送访问请求时，报文容易被网络中的黑客窃取或篡改，最终造成数据泄密、重要数据被破坏等后果。

为了防止信息泄露，可以在总部和分支机构之间搭建一条物理专网连接，但其费用会非常昂贵。VPN 出现后，通过部署不同类型的 VPN 便可解决上述问题。VPN 对数据进行封装和加密，即使网络黑客窃取到数据，也无法破解，确保了数据的安全性。且搭建 VPN 不需改变现有网络拓扑，没有额外费用。因其具有廉价、专用和虚拟等多种优势，在现网中应用非常广泛。

VPN 具有以下两个基本特征：

- 专用（Private）：VPN 网络是专门供 VPN 用户使用的网络，对于 VPN 用户，使用 VPN 与使用传统专网没有区别。VPN 能够提供足够的安全保证，确保 VPN 内部信息不受外部侵扰。VPN 与底层承载网络（一般为 IP 网络）之间保持资源独立，即 VPN 资源不被网

络中非该 VPN 的用户所使用。

- 虚拟（Virtual）：VPN 用户内部的通信是通过公共网络进行的，而这个公共网络同时也可以被其他非 VPN 用户使用，VPN 用户获得的只是一个逻辑意义上的专网。这个公共网络称为 VPN 骨干网（VPN Backbone）。

1.2 VPN 的封装原理

VPN 的基本原理是利用隧道（Tunnel）技术，对传输报文进行封装，利用 VPN 骨干网建立专用数据传输通道，实现报文的安全传输。

隧道技术使用一种协议封装另外一种协议报文（通常是 IP 报文），而封装后的报文也可以再次被其他封装协议所封装。对用户来说，隧道是其所在网络的逻辑延伸，在使用效果上与实际物理链路相同。

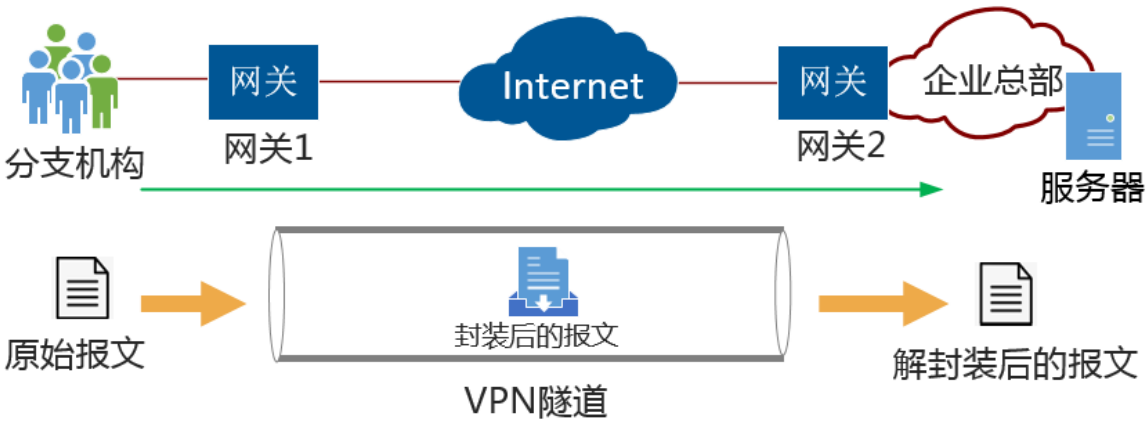

图 12-1 VPN 的封装原理

VPN 的封装原理如图 12-1 所示。当园区网远程用户访问园区网内部服务器时，报文封装过程如下：

- 当远程用户登录 VPN 以后，就在远程用户和 VPN 网关之间建立了隧道连接；
- 远程用户发出的报文（数据）封装在 VPN 隧道中，发送（加密传输）给位于园区网的 VPN 网关；
- VPN 网关收到报文后进行解封装，并将原始数据发送给园区网内部的最终接收者，即服务器；
- 反向的处理也一样。VPN 网关在封装时可以对报文进行加密处理，使 Internet 上的非法用户无法读取报文内容，因而通信是安全可靠的。

2. 各种 VPN 技术简介

2.1 L2TP VPN

L2TP 协议（Layer 2 Tunneling Protocol，第 2 层隧道协议）是典型的被动式隧道协议，L2TP VPN 是一种用于承载 PPP 报文的隧道技术，该技术主要应用在远程办公场景中为出差员工远程访问企业内网资源提供接入服务。

出差员工跨越 Internet 远程访问企业内网资源时需要使用 PPP 协议向企业总部申请内网 IP 地址，并供总部对出差员工进行身份认证。但 PPP 报文受其协议自身的限制无法在 Internet 上直接传输。于是，PPP 报文的传输问题成为了制约出差员工远程办公的技术瓶颈。L2TP VPN 技术出现以后，使用 L2TP VPN 隧道“承载”PPP 报文在 Internet 上传输成为了解决上述问题的一种途径。无论出差员工是通过传统拨号方式接入 Internet，还是通过以太网方式接入 Internet，L2TP VPN 都可以向其提供远程接入服务。

2.2 IPSec

IPSec（Internet Protocol Security）是 IETF（Internet Engineering Task Force）制定的一组开放的网络安全协议。它并不是一个单独的协议，而是一系列为 IP 网络提供安全性的协议和服务的集合。IPSec 定义了一种标准的、健壮的以及包容广泛的机制，它提供了 Internet 第三层 IP 层上的安全措施，它也被用于通过 Internet 传输的 VPN 封装技术中。

在 Internet 的传输中，绝大部分数据的内容都是明文传输的，这样就会存在很多潜在的危险，比如：密码、银行帐户的信息被窃取、篡改，用户的身份被冒充，遭受网络恶意攻击等。网络中部署 IPSec 后，可对传输的数据进行保护处理，降低信息泄露的风险。

2.3 GRE

General Routing Encapsulation，简称 GRE，是一种三层 VPN 封装技术。GRE 可以对某些网络层协议（如 IPX、Apple Talk、IP 等）的报文进行封装，使封装后的报文能够在另一种网络中（如 IPv4）传输，从而解决了跨越异种网络的报文传输问题。异种报文传输的通道称为 Tunnel（隧道）。

GRE 除了可以封装网络层协议报文以外，它还具备封装组播报文的能力。由于动态路由协议中会使用组播报文，因此更多时候 GRE 会在需要传递组播路由数据的场景中被用到，这也是 GRE 被称为通用路由封装协议的原因。以下几个场景就是 GRE 在路由封装方面的应用。

2.4 SSL VPN

SSL VPN 是以 SSL 协议为安全基础的 VPN 远程接入技术，移动办公人员（在 SSL VPN 中被称为远程用户）使用 SSL VPN 可以安全、方便的接入企业内网，访问企业内网资源，提高工作效率。

2.5 MPLS IP VPN

MPLS（Multi-Protocol Label Switching，多标签协议转换）是一种用于快速数据包交换和路由的体系，它为网络数据流提供了目标、路由、转发和交换等能力。此外，它还具有管理各种不同形式通信流的机制。

MPLS VPN 采用 MPLS 技术在骨干的宽带 IP 网络上构建企业 IP 专网，实现跨地域、安全、高速、可靠的数据、语音、图像多业务通信，并结合差别服务、流量工程等相关技术，将公众网可靠的性能、良好的扩展性、丰富的功能与专用网的安全、灵活高效地结合在一起，为用户提供高质量的服务。

3. SSL VPN 的应用

3.1 SSL VPN 简介

SSL VPN 是以 SSL 协议为安全基础的 VPN 远程接入技术，移动办公人员（在 SSL VPN 中被称为远程用户）使用 SSL VPN 可以安全、方便的接入企业内网，访问企业内网资源，提高工作效率。

SSL VPN 凭借自身的技术特点使其在远程接入应用场景中与早期 VPN 相比更具优势，其特点如下：

- SSL VPN 采用 B/S 架构设计，远程用户终端上无需安装额外的客户端软件，直接使用 Web 浏览器就可以安全、快捷的访问企业内网资源；
- 可以根据远程用户访问内网资源类型的不同，对其访问权限进行高细粒度控制；
- 提供了本地认证、服务器认证、证书匿名和证书挑战多种身份认证方式，提高了身份认证的灵活性；
- 主机检查策略可以检查远程用户终端的操作系统、端口、进程以及杀毒软件等是否符合安

全要求，并且还具备防跳转、防截屏的能力，消除了潜藏在远程用户终端上的安全隐患；

- 缓存清理策略用于清理远程用户访问内网过程中在终端上留下的访问痕迹，加固了用户的信息安全。

3.2 SSL VPN 的访问方式

SSL VPN 的主要应用场景是保证远程用户能够在企业外部安全、高效的访问企业内部的网络资源。防火墙向远程用户提供 SSL VPN 接入服务的功能模块称为虚拟网关，虚拟网关有独立的 IP 地址。网络管理员可以在虚拟网关下配置用户、资源以及用户访问资源的权限等。

虚拟网关是远程用户访问企业内网资源的统一入口。远程用户在 Web 浏览器中输入虚拟网关的 IP 地址，并在虚拟网关登录界面输入用户名和密码，虚拟网关将会对用户进行身份认证。身份认证通过后，虚拟网关会向远程用户提供可访问的内网资源列表，远程用户点击资源列表链接即可访问对应资源。远程用户在资源访问列表中只能看到网络管理员为其开通的业务资源，例如为远程用户 A 开通了 Web 代理业务，则远程用户 A 在资源列表中就只能看到有权访问的 Web 资源，而看不到企业内网中的文件资源、TCP 资源等其他资源。

如图 12-2 所示，防火墙作为企业出口网关连接至 Internet，并向远程用户提供 SSL VPN 接入服务。远程用户可以使用移动终端（如便携机、PAD 或智能手机）随时随地访问防火墙并接入到企业内网，访问企业内网资源。

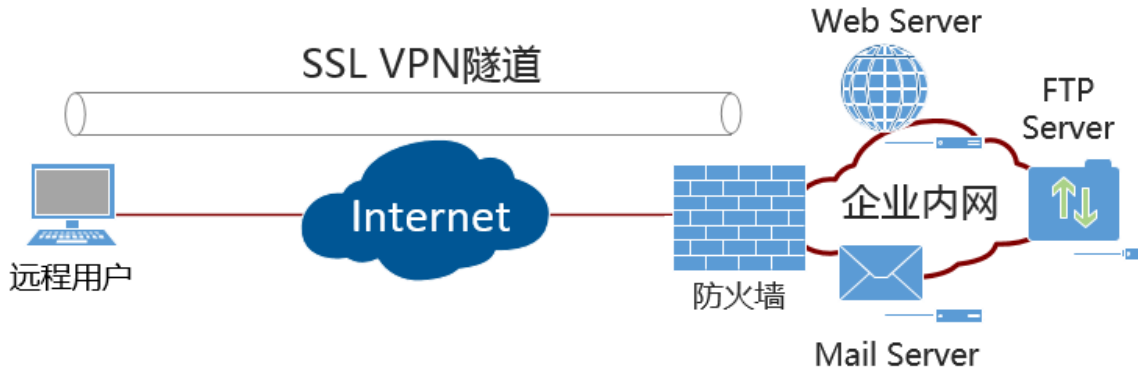

图 12-2 SSL VPN 访问方式

五、实验内容及打分

本实验共包含 3 个任务，由学生独立完成。教师在实验课上检查实验完成情况并提出相应问题，将根据各任务的完成情况及回答问题情况进行打分。

【提示】各任务的具体操作，可参考教材或课程网站

任务一：设计并部署内部网和外部网（30 分）

在 eNSP 中设计两个网络，分别表示内部网和外部网。

【要求 1】

1. 内部网和外部网中，都要包含路由器、路由交换机、二层交换机、用户主机，二层交换机上必须配置不同 VLAN（即用户主机分别属于不同 VLAN）。
2. 内部网的边界是一台防火墙，用来实现相关功能需求；
3. 内部网以 NAT 方式访问外部网，外部网主机在默认情况下，不能访问内部网主机。
4. 内部网用户主机的 IP 地址格式为 192.A.*.*/24，其中 A 表示学生的学号后 3 位。外部网主机的 IP 地址格式为*.A.*.*/24，其中 A 表示学生学号后 3 位。路由接口的 IP 地址由学生自定。
5. 内部网和外部网都采用 OSPF 路由协议。

注意：本实验提交检查时，将检查本要求

任务二：在内部网边界防火墙上配置 SSL VPN（20 分）

在内部网边界防火墙上配置 SSL VPN，使得外部网用户可以以 Web 方式登录 VPN 后，可以以安全的方式访问内部网中用户主机。

【要求 2】

1. SSL VPN 的访问方式：SSL VPN 的访问方式采用网络扩展方式；
2. 设定外部网用户登录 VPN 以后，VPN 服务器分配给外部网用户的 IP 地址范围是 172.A.1.1/24～172.A.1.200/24，A 表示学生的学号后 3 位。
3. SSL VPN 登录用户名为学生姓名全拼+01，例如张三，其用户名为 zhangsan01，密码为 abcd@1234。

注意：本实验提交检查时，将检查本要求

任务三：启用 SSL VPN 并抓包分析通信过程（20 分）

通过抓包，分析以下通信过程。

1. 启用 SSL VPN 之前，外部网用户访问内部网用户主机的过程（为何 Ping 不通？）；
2. 启用 SSL VPN 之后，外部网用户访问内部网用户主机的过程，具体包括：

（1）分析外部网用户发出的报文，其首部地址是什么？

（2）在外部网中的通信，是如何实现安全的？

（3）报文经过内部网边界防火墙后，其首部地址又是什么？

注意：本实验提交检查时，将检查上述分析结果。

4、回答问题（30 分）

教师在实验课上检查实验完成情况并提出相应问题，将根据各任务的完成情况及回答问题情况进行打分。

六、实验拓展及分析

1、思考：外部主机 B-C-2 访问内部网主机 A-C-2 时，假设 B-C-2 已经登录了 VPN，则 B-C-2 发出的报文，是如何被路由到 A-C-2 的？有是如何从 A-C-2 被路由到 B-C-2 的？分析报文在经过每一个路由设备时，依据哪条路由进行转发的？