实验九：通过VPN访问园区网内部主机

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

设计性

四、实验理论

1. VPN

2. SSL VPN

如图-1 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。

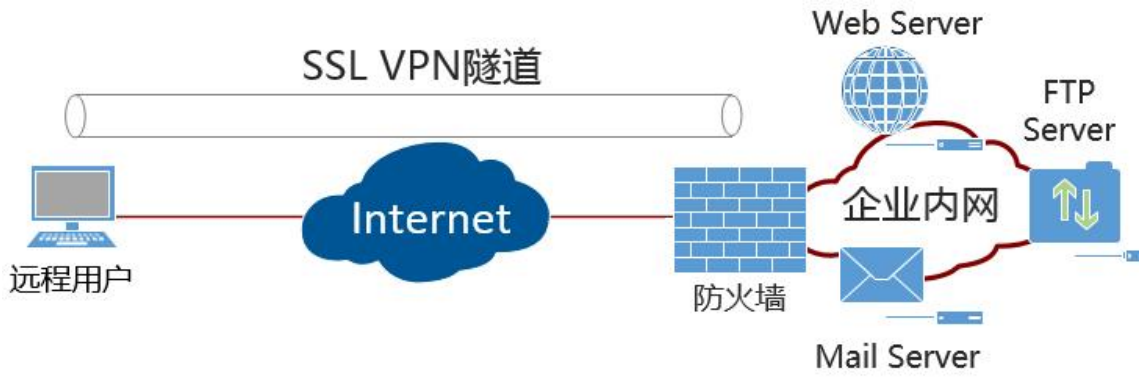

图-1 SSL VPN 访问方式

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？