实验十八：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”），例如企业分支结构与企业总部位于不同区域，或者园区网用户出差在外，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。

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. 认识 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。

1.1 VPN 的出现背景

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。

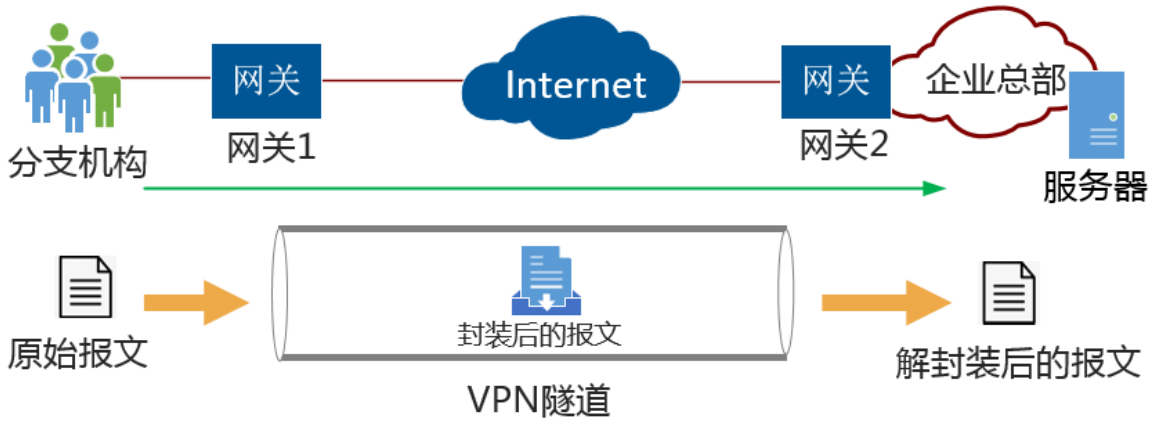

图 18-0-1 VPN 的封装原理

VPN 的封装原理如图 10-0-1 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。

1.3 VPN 的应用场景

（1）site-to-site VPN

site-to-site VPN 即两个局域网之间通过 VPN 隧道建立连接。

如图 18-0-2 所示，企业的分支和总部分别通过网关 1 和网关 2 连接到 Internet。出于业务需要，企业分支和总部间经常相互发送内部机密数据。为了保护这些数据在 Interner 中安全传输，在网关 1 和网关 2 之间建立 VPN 隧道。

图 18-0-2 site-to-site VPN 拓扑图

这种场景的特点为：两端网络均通过固定的网关连接到 Internet，组网相对固定并且访问是双向的，即分支和总部都有可能向对端发起访问。

此场景可以使用以下几种 VPN 实现：IPSec、L2TP、GRE over IPSec、IPSec over GRE。

（2）client-to-site VPN

client-to-site VPN 即客户端与企业内网之间通过 VPN 隧道建立连接。

如图 18-0-3 所示，外出差员工（客户端）跨越 Internet 访问企业总部内网，完成向总部传送数据、访问内部服务器等需求。为确保数据安全传输，可在客户端和企业网关之间建立 VPN 隧道。

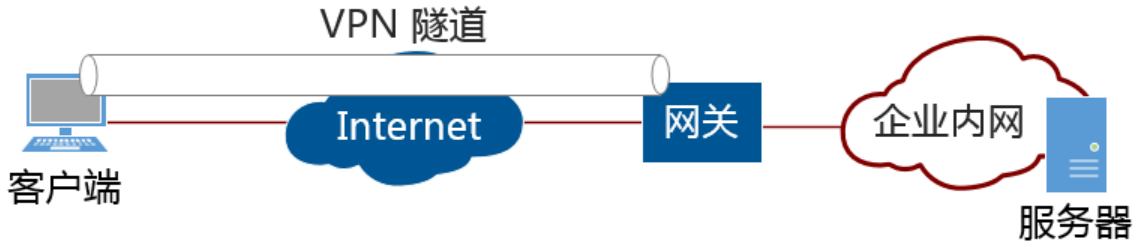

图 18-0-3 client-to-site VPN 拓扑图

这种场景的特点为：客户端的地址不固定。且访问是单向的，即只有客户端向内网服务器发起访问。适用于企业出差员工或临时办事处员工通过手机、电脑等接入总部远程办公。

此场景可以使用以下几种 VPN 实现：SSL、IPSec（IKEv2）、L2TP。

（3）BGP/MPLS IP VPN

BGP/MPLS IP VPN 主要用于解决跨域企业互连等问题。当前企业越来越区域化和国际化，同一企业的不同区域员工之间需要通过服务提供商网络来进行互访。服务提供商网络往往比较庞大和复杂，为严格控制用户的访问，确保数据安全传输，需在骨干网上配置 BGP/MPLS IP VPN 功能，实现不同区域用户之间的访问需求。

如图 18-0-4 所示，BGP/MPLS IP VPN 为全网状 VPN，即每个 PE 和其他 PE 之间均建立

BGP/MPLS IP VPN 连接。服务提供商骨干网的所有 PE 设备都必须支持 BGP/MPLS IP VPN 功能。

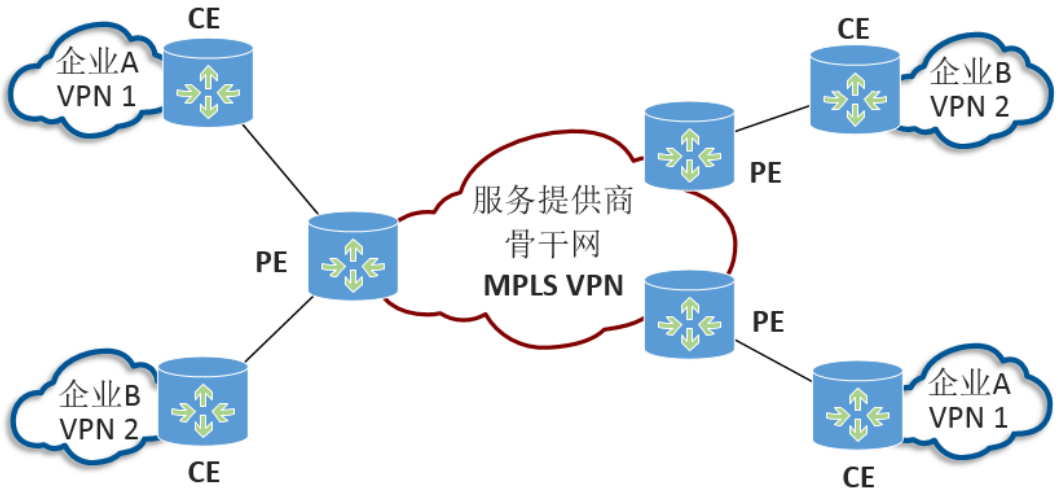

图 18-0-4 BGP/MPLS IP VPN 拓扑图

CE 指用户边缘路由器，PE 指运营商边缘路由器。其中，PE 充当 IP VPN 接入路由器。

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 18-0-5 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。

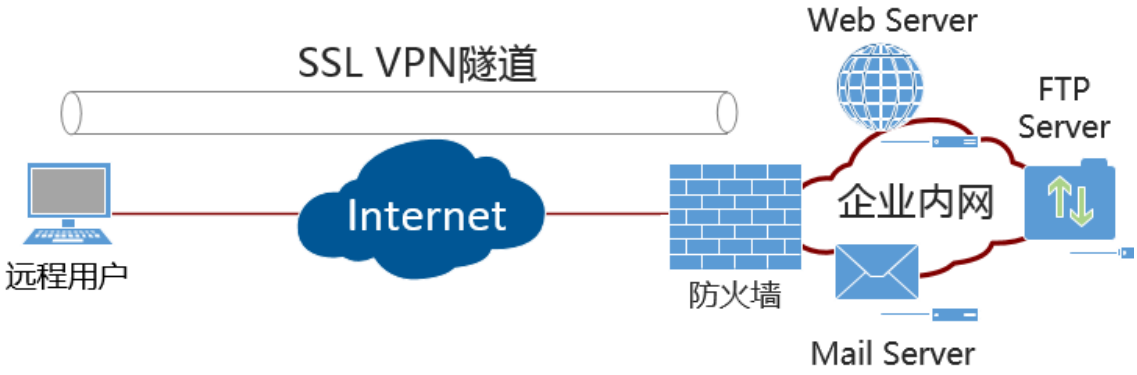

图 18-0-5 SSL VPN 访问方式

根据远程用户访问内网资源类型的不同，SSL VPN 提供了 Web 代理、文件共享、端口转发、网络扩展这四种内网访问方式，即 SSL VPN 业务。表 18-0-1 说明了 SSL VPN 的四种业务。

表 18-0-1 SSL VPN 的业务列表

业务	定义
Web 代理	远程用户访问内网 Web 资源时使用 Web 代理业务。
文件共享	远程用户访问内网文件服务器（如支持 SMB 协议的 Windows 系统、支持 NFS 协议的 Linux 系统）时使用文件共享业务。 远程用户直接通过 Web 浏览器就能在内网文件系统上创建和浏览目录，进行下载、上传、改名、删除等文件操作，就像对本机文件系统进行操作一样方便。
端口转发	远程用户访问内网 TCP 资源时使用端口转发业务。适用于 TCP 的应用服务包括 Telnet、远程桌面、FTP、Email 等。端口转发提供了一种端口级的安全访问内网资源的方式。
网络扩展	远程用户访问内网 IP 资源时使用网络扩展业务。 Web 资源、文件资源以及 TCP 资源都属于 IP 资源，通常在不区分用户访问的资源类型时为对应用户开通此业务。

3.3 SSL VPN 总体流程

图 18-0-6 描述了远程用户通过 SSL VPN 访问企业内网资源的总体流程。

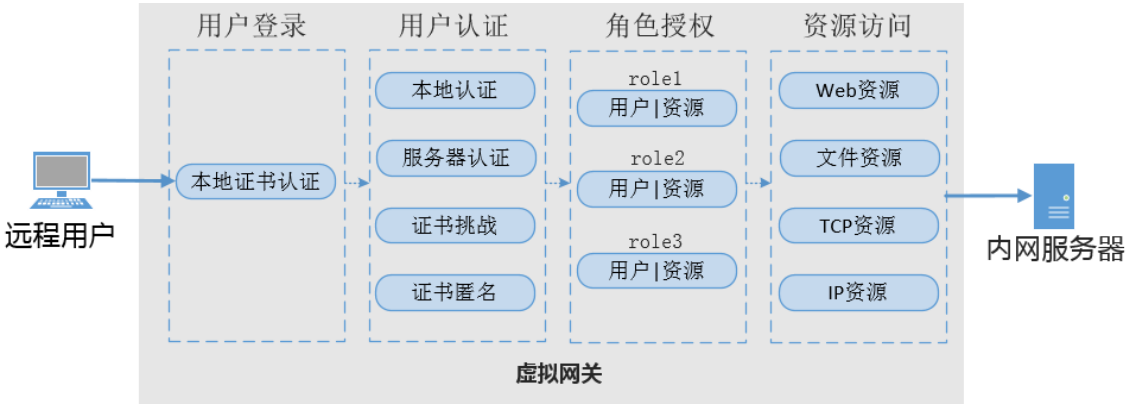

图 18-0-6 SSL VPN 的总体流程

- 用户登录：远程用户通过 Web 浏览器（客户端）登录虚拟网关，请求建立 SSL 连接。虚拟网关向远程用户发送自己的本地证书，远程用户对虚拟网关的本地证书进行身份认证。认证通过后，远程用户与虚拟网关成功建立 SSL 连接；
- 用户认证：虚拟网关对远程用户进行用户认证，验证用户身份。用户认证可以选择本地认证、服务器认证、证书匿名认证、证书挑战认证中的一种；
- 角色授权：用户认证完成后，虚拟网关查询该用户的资源访问权限。用户的权限分配通过角色实现，先将具有相同权限的用户/组加入某个角色，然后角色关联可访问的业务资源，角色是联系用户和资源的纽带；
- 资源访问：虚拟网关根据远程用户的角色信息，向用户推送可访问的资源链接，远程用户点击对应的资源链接进行资源访问。

3.4 SSL VPN 网络扩展交互过程

防火墙通过网络扩展业务，在虚拟网关与远程用户之间建立安全的 SSL VPN 隧道，将用户连接到企业内网，实现对企业 IP 业务的全面访问。远程用户使用网络扩展功能访问内网资源时，其内部交互过程如图 18-0-7 所示。

- 远程用户通过 Web 浏览器登录虚拟网关；
- 成功登录虚拟网关后启动网络扩展功能；
- 启动网络扩展功能，会触发以下几个动作：
  - 远程用户与虚拟网关之间会建立一条 SSL VPN 隧道；
  - 远程用户的 PC 会自动生成一个虚拟网卡。防火墙的虚拟网关从地址池中随机选择一个 IP 地址，分配给远程用户的虚拟网卡，该地址作为远程用户与企业内网 Server 之间通信之用。有了该私网 IP 地址，远程用户就如同企业内网用户一样可以方便访问内网 IP 资源；
  - 虚拟网关向远程用户下发到达企业内网 Server 的路由信息。虚拟网关会根据网络扩展业务中的配置，向远程用户下发不同的路由信息。
- 远程用户向企业内网的 Server 发送业务请求报文，该报文通过 SSL VPN 隧道到达虚拟网关。
- 虚拟网关收到报文后进行解封装，并将解封装后的业务请求报文发送给内网 Server。

- 内网 Server 响应远程用户的业务请求。
- 响应报文到达虚拟网关后进入 SSL VPN 隧道。
- 远程用户收到业务响应报文后进行解封装，取出其中的业务响应报文。

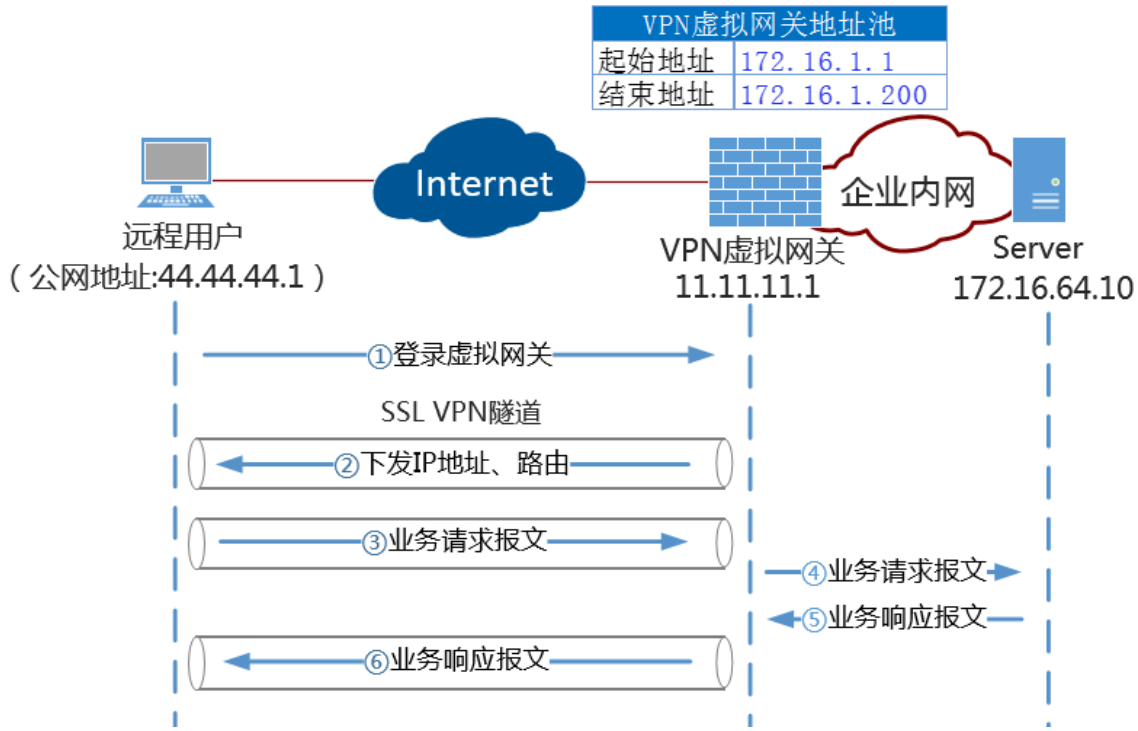

图 18-0-7 SSL VPN 网络扩展业务交互流程

五、实验过程

步骤 1：网络设计

（1）网络拓扑设计

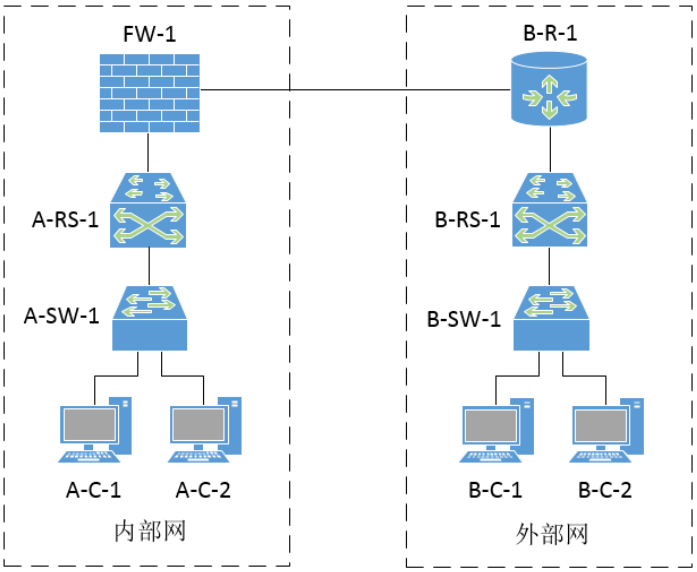

图 18-1-1 任务一的网络拓扑

（2）交换机接口与 VLAN

自行设计

（3）主机 IP 地址

表 18-1-1 主机 IP 地址规划表

序号	设备名称	IP 地址 /子网掩码	默认网关	备注
1	A-C-1	192.168.64.10 /24	192.168.64.254	内部网用户，使用私有 IP 地址
2	A-C-2	192.168.65.10 /24	192.168.65.254	内部网用户，使用私有 IP 地址
3	B-C-1	33.33.33.10 /24	33.33.33.254	外部网用户，使用公有 IP 地址
4	B-C-2	44.44.44.1 /24	44.44.44.254	外部网用户，使用公有 IP 地址

（4）路由接口 IP 地址

表 18-1-2 路由接口 IP 地址规划表

序号	设备名称	接口名称	接口地址	备注
1	A-RS-1	vlanif100	10.0.0.2 /30	连接防火墙 FW-1 的内部网接口
2	A-RS-1	vlanif11	192.168.64.254 /24	作为内部网用户 VLAN11 的默认网关
3	A-RS-1	vlanif12	192.168.65.254 /24	作为内部网用户 VLAN12 的默认网关
4	B-RS-1	vlanif100	22.22.22.2 /30	连接防火墙 FW-1 的外部网接口
5	B-RS-1	vlanif11	33.33.33.254 /24	作为外部网用户 VLAN11 的默认网关
6	B-RS-1	vlanif12	44.44.44.254 /24	作为外部网用户 VLAN12 的默认网关
7	FW-1	GE1/0/1	11.11.11.1 /24	公有 IP 地址，用于与外部网的连接
8	FW-1	GE1/0/0	10.0.0.1 /30	私有 IP 地址，用于与内部网的连接
9	B-R-1	GE0/0/0	11.11.11.2 /24	公有 IP 地址，作为内部网路由器的下一跳
10	B-R-1	GE0/0/1	22.22.22.1 /24	公有 IP 地址，用于与外部网的连接

本任务中，内部网中各主机通过防火墙 NAT 访问外部网，NAT 服务会将报文的源 IP 地址（私有 IP 地址）转换成 FW-1 的 GE1/0/1 接口的公有 IP 地址（即 11.11.11.1/24）发送出去，从而使得该报文能够被外部网上的路由器转发。

（5）路由表规划

表 18-1-5 路由规划表

序号	路由设备	目的网络	下一跳地址	备注
1	A-RS-1	内部网	配置 OSPF	实现内部网内部的通信
2	FW-1	内部网	配置 OSPF	实现内部网内部的通信
3	FW-1	0.0.0.0 /0	11.11.11.2	所有对外部网的访问，下一跳是外部网路由器 B-R-1
4	B-RS-1	外部网	配置 OSPF	实现外部网中各设备的通信
5	B-R-1	外部网	配置 OSPF	实现外部网中各设备的通信

注意，外部网路由器中必须具有到达内部网边界防火墙的 GE1/0/1 接口（连接外部网）所在网络的路由信息（即外部网路由器必须知道前往 11.11.11.0/24 网络该怎么走），一是用于内部网主机访问外部网的返回报文，二是因为外部网用户访问内部网主机时登录 SSL VPN。

（6） OSPF 的区域规划

本任务中内部网和外部网的 OSPF 区域规划如图 18-1-2 所示。

由于内部网主机通过 NAT 访问外部网，所以边界 FW-1 不能将内部网信息发送到外部网上，因此 FW-1 不需要宣告其外部网接口网段。为了让外部网上的路由器知道前往 11.11.11.0/24 网络（即 FW-1 的外部网接口所在网络）该怎么走，B-R-1 在宣告自身网络时，要宣告①处接口所在网络信息。此处内部网和外部网中的 OSPF 区域可以都可以是 Area 0，

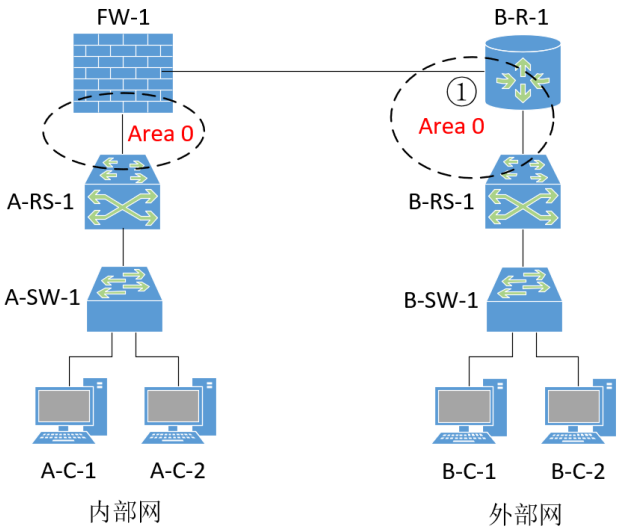

图 18-1-2 OSPF 的区域规划

相互没有影响。

（7）防火墙 SSL VPN 设计

- SSL VPN 的访问方式：SSL VPN 的访问方式采用网络扩展方式，设定用来分配给外部网用户的 IP 地址范围是 172.16.1.1/24～172.16.1.200/24。
- SSL VPN 的登录认证：认证方式采用本地认证，SSL VPN 登录用户名为 user_sslvpn，密码为 abcd@1234，并且要在 SSL VPN 虚拟网关上配置 MAC 认证功能对用户终端的 MAC 地址进行认证。

步骤 2：在 eNSP 中部署网络

启动 eNSP，根据本任务的【拓扑规划】添加网络设备并连线，启动全部设备。

本任务在 eNSP 中的拓扑图如图 18-1-3 所示。

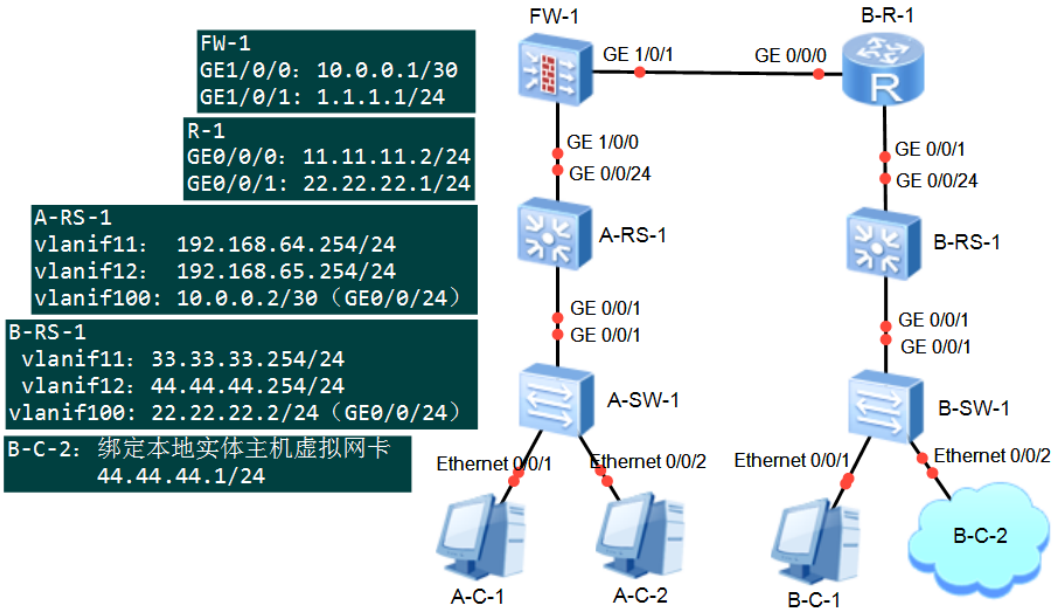

图 18-1-3　任务一在 eNSP 中的网络拓扑

步骤 2：实现内部网通信

对内部网中的主机、交换机进行配置，实现内部网内部各主机之间的通信。

具体配置略，自行完成。

步骤 3：配置内部网用户 NAT 访问外部网

在内部网边界防火墙 FW-1 上进行路由配置、NAT 配置，使得内部网用户可以通过 NAT 方式访问外部网。

具体配置略，自行完成。

步骤 4：配置外部网

对外部网中的主机、交换机和路由器进行配置，实现外部网中各设备的通信。

（1）配置用户主机地址参数

给外部网用户主机 B-C-1、B-C-2 配置 IP 地址等信息。B-C-2 使用本地实体主机代替，Cloud 设备绑定的虚拟网卡地址是 44.44.44.1/24。

（2）配置 B-SW-1

略

（3）配置 B-RS-1

略

（4）配置路由器 B-R-1

略

步骤 5：启用 SSL VPN 之前的通信测试

在当前状态下（尚未配置 SSL VPN），使用 Ping 命令测试内部网和外部网的通信情况，测试结果见表 18-1-6。

表 18-1-6 配置 SSL VPN 之前内部网和外部网的通信情况

序号	源设备	目的设备	通信结果
1	A-C-1	A-C-2	通
2	A-C-1	B-C-1	通
3	A-C-1	B-C-2	通
4	B-C-1	A-C-1	不通
5	B-C-2	A-C-1	不通

从测试结果可以看出，内部网内部各主机间可以相互通信，内部网各主机可以访问外部网，外部网各主机无法访问内部网主机。

注意：

1. 由于此处的外部网主机 B-C-2 是用本地实体主机代替的，所以需要以管理员身份在本地实体主机上添加静态路由：route add 192.168.64.0 mask 255.255.254.0 44.44.44.254；
2. 由于本地实体主机操作系统自带防火墙的问题，内部网主机有可能 ping 不通 B-C-2，此时关闭本地实体主机防火墙即可。

步骤 6：在 FW-1 上配置 SSL VPN

（1）配置 SSL VPN 用户和认证方案

```
//以下操作配置认证域
[FW-1] aaa
//创建并进入 default 认证域。domain 命令用来创建域，并进入域视图。缺省情况下，设备上存在名为“default”的域，可以修改这个域下的配置，但是不能删除这个域。“default”域默认绑定认证方案“default”
[FW-aaa] domain default
//在 AAA 视图下执行 authentication-scheme 命令，用来创建认证方案，并进入认证方案视图。缺省存在的认证方案“default”，不能被删除，只能被修改。“default”认证方案的策略为：认证模式采用本地认证，若认证失败则强制用户下线。
[FW-aaa-domain-default] authentication-scheme default
//在认证域视图下，表示认证域的接入控制为允许 SSL VPN 用户接入。仅 USG6000V 支持该参数。
[FW-aaa-domain-default] service-type ssl-vpn
[FW-aaa-domain-default] quit
[FW-aaa] quit

//以下操作用来创建 SSL VPN 用户组和用户
//在 default 认证域的根组（/default）中创建用户组 group_sslvpn。使用 user-manage group 命令用来指定（或创建）用户组，并进入用户组视图（仅 USG6000V 支持该命令）。创建或删除用户组时，必须指定用户组所在的组路径及用户组名称。default 是设备缺省存在的认证域，它的根组为/default，
```

可以在其下级继续创建用户组。如果需要创建其他认证域下的用户组，需要首先创建认证域。

[FW-1]user-manage group /default/group_sslvpn

[FW-1-usergroup-/default/group_sslvpn]quit

// 在 default 认证域下创建用户 user_sslvpn，用户密码为 abcd@1234，并设置该用户属于 group_sslvpn 用户组。

[FW-1]user-manage user user_sslvpn domain default

[FW-1-localuser-user_sslvpn]password abcd@1234

[FW-1-localuser-user_sslvpn]parent-group /default/group_sslvpn

[FW-1-localuser-user_sslvpn]quit

（2）配置 SSL VPN 虚拟网关

//以下操作用来创建 SSL VPN 虚拟网关并配置接口

//创建名为 gateway_ssl 的 SSL VPN 虚拟网关。

[FW-1]v-gateway gateway_ssl interface GigabitEthernet 1/0/1 private

[FW-1-gateway_ssl]quit

//配置虚拟网关的 UDP 端口号为 443。客户端的网络扩展隧道模式配置为“快速传输模式”时，客户端向虚拟网关的 UDP 端口发送业务报文。

[FW-1]v-gateway gateway_ssl udp-port 443

//配置虚拟网关（gateway_ssl）和认证域（default）绑定

[FW-1]v-gateway gateway_ssl authentication-domain default

//以下操作用来配置 SSL VPN 的网络扩展业务。

[FW-1]v-gateway gateway_ssl

[FW-1-gateway_ssl]service

//network-extension enable 命令用来启用网络扩展功能。

[FW-1-gateway_ssl-service]network-extension enable

//network-extension keep-alive enable 命令用来启用网络扩展的保持连接功能。客户端启动网络扩展功能后，如果一段时间内没任何操作，没有向防火墙发送任何流量，客户端和防火墙的网络扩展连接会因为 SSL 会话超时或客户端到防火墙的 HTTPS 会话表项老化而断开，客户端需要重新登录或重新连接才能再次使用网络扩展功能。网络扩展的保持连接功能可以保持客户端和防火墙的连接不中断，从而规避上述问题。启用网络扩展的保持连接功能后，客户端会定期向防火墙发送保活报文，防火墙收到保活报文时，会刷新 SSL 会话超时时间和 HTTPS 会话表项老化时间，重新开始计时。

[FW-1-gateway_ssl-service]network-extension keep-alive enable

//配置网络扩展保活报文的发送时间间隔为 120 秒。

[FW-1-gateway_ssl-service]network-extension keep-alive interval 120

//在网络扩展时采用地址池方式为 VPN 客户端分配 IP 地址，范围是 172.16.1.1～200。

[FW-1-gateway_ssl-service]network-extension netpool 172.16.1.1 172.16.1.200 255.255.255.0

//配置网络扩展默认地址池开始的 IP 地址，该 IP 地址作为地址池的名字。

[FW-1-gateway_ssl-service]netpool 172.16.1.1 default

//设置网络扩展的路由模式为 manual（手动模式）。手动模式下，在防火墙端，管理员必须手动配置内网网段静态路由（使用 network-extension manual-route 命令进行配置），然后在客户端识别前往该

网段的数据，交由虚拟网卡转发。

[FW-1-gateway_ssl-service]network-extension mode manual

//配置网络扩展手动模式下的 IP 网段为 192.168.64.0/23，使得 VPN 客户可以访问该网段地址。

[FW-1-gateway_ssl-service]network-extension manual-route 192.168.64.0 255.255.254.0

[FW-1-gateway_ssl-service]quit

注意：

1. 在配置 SSL VPN 虚拟 IP 地址池时，该地址池范围内的 IP 地址不能为虚拟网关或接口的 IP 地址，以免 VPN 客户端无法获取虚拟 IP 地址，无法使用网络扩展业务；
2. 选择 IP 地址池方式时，至少指定一个 IP 地址池。SSL VPN 虚拟 IP 地址池不能包含内网已经分配的 IP 地址；
3. 配置虚拟 IP 地址池时，若用户使用的是 Windows XP 及之前版本 Windows 操作系统，不要使用包含 192.168.x.255 的地址，以免启用网络扩展失败；
4. 在多虚拟网关的组网中，配置网络扩展地址池时，注意地址池中的地址不要和 DHCP 服务器的 IP 地址池中的地址冲突。

//以下操作用来配置 SSL VPN 角色绑定。

//进入虚拟网关 VPN 数据库视图。

[FW-1-gateway_ssl]vpndb

//添加用户组/default/group_sslvpn 到虚拟网关

[FW-1-gateway_ssl-vpndb]group /default/group_sslvpn

[FW-1-gateway_ssl-vpndb-group-/default/group_sslvpn]quit

[FW-1-gateway_ssl-vpndb]quit

[FW-1-gateway_ssl]role

//配置用户登录虚拟网关时，需要通过角色中关联的所有主机检查策略才能访问角色中的资源。

[FW-1-gateway_ssl-role]role default condition all

[FW-1-gateway_ssl-role]quit

//以下操作用来配置 MAC 认证功能。

[FW-1-gateway_ssl]security

[FW-1-gateway_ssl-security]authentication-mode cert-none

[FW-1-gateway_ssl-security]mac-authentication enable

//在 MAC 认证场景中，管理员需要在虚拟网关上先创建一个 MAC 地址组，并在 MAC 地址组中加入用户的 MAC 地址。当用户携带 MAC 地址的认证请求到达虚拟网关时，虚拟网关会通过用户名查找到该用户所属的用户组，然后再根据用户组与 MAC 地址组的绑定关系来确定 MAC 地址组。如果 MAC 地址组中可以找到该用户的 MAC 地址，则表示用户身份认证通过，用户正常上线；找不到，则表示用户身份认证失败，虚拟网关拒绝用户上线。此处创建名为 mac-group-ssl 的 MAC 地址组。

[FW-1-gateway_ssl-security]mac-group mac-group-ssl

//设置 VPN 客户端 MAC 地址，0a00-2700-000d 是 B-C-2 绑定的虚拟网卡的 MAC 地址。

[FW-1-gateway_ssl-security-macgroup-mac-group-ssl]mac-address 0a00-2700-000d

```
[FW-1-gateway_ssl-security-macgroup-mac-group-ssl]quit
[FW-1-gateway_ssl-security]bind user-group /default/group_sslvpn mac-group mac-g
roup-ssl
[FW-1-gateway_ssl-security]quit
[FW-1-gateway_ssl]quit

//以下操作用来配置安全策略，允许外部网用户访问内部网主机
//创建安全策略，允许外部网用户以 https 方式访问 VPN 的虚拟网关地址 11.11.11.1。
[FW-1]security-policy
[FW-1-policy-security]rule name allow-visit-sslvpn
[FW-1-policy-security-rule-allow-visit-sslvpn]source-zone untrust
[FW-1-policy-security-rule-allow-visit-sslvpn]destination-zone local
[FW-1-policy-security-rule-allow-visit-sslvpn]destination-address 11.11.11.1 24
[FW-1-policy-security-rule-allow-visit-sslvpn]service https
[FW-1-policy-security-rule-allow-visit-sslvpn]action permit
[FW-1-policy-security-rule-allow-visit-sslvpn]quit
[FW-1-policy-security]
//创建安全策略，允许外部用户（指 VPN 客户端）访问内部网中指定的网段（192.168.64.0/23）。
[FW-1-policy-security]rule name allow-visit-lanhost
[FW-1-policy-security-rule-allow-visit-lanhost]source-zone untrust
[FW-1-policy-security-rule-allow-visit-lanhost]destination-zone trust
[FW-1-policy-security-rule-allow-visit-lanhost]destination-address 192.168.64.0 23
[FW-1-policy-security-rule-allow-visit-lanhost]action permit
[FW-1-policy-security-rule-allow-visit-lanhost]quit
[FW-1-policy-security]quit
```

步骤 7：在防火墙上配置 Web 登录

本任务中，外部网用户 B-C-2（用本地实体主机代替）需要以 Web 方式通过防火墙 FW-1 的外网接口 GE1/0/1 登录 SSL VPN，所以需要在该接口上启用 https 服务。

```
[FW-1]interface GigabitEthernet 1/0/1
[FW-1-GigabitEthernet1/0/1]service-manage https permit
[FW-1-GigabitEthernet1/0/1]quit
[FW-1]quit
<FW-1>save
```

步骤 8：外部网用户登录 SSL VPN

外部网用户登录内部网边界防火墙的 SSL VPN 虚拟网关（11.11.11.1）。以主机 B-C-2 为例，在其浏览器地址栏中输入 https://11.11.11.1:443， 打开防火墙的 SSL VPN 登录界面，输入用户名 user_sslvpn，密码 abcd@1234，如图 18-1-4 所示，然后点击【登录】按钮。

图 18-1-4 登录 SSL VPN

注意：

1. 为了使 B-C-2（即本地实体主机）能够访问 11.11.11.1，需要以管理员身份在本地主机上添加路由：route add 11.11.11.1 mask 255.255.255.0 44.44.44.254；
2. 使用 IE 浏览器进行登录，其他浏览器可能无法登录，使用 IE 登录时根据提示可能会需要安装插件。

在接下来的“welcome”界面中，点击【启动】按钮，待显示“已成功启动网络扩展业务”，如图 18-1-5 所示，说明此时已成功登录 SSL VPN，外部网用户可以访问内部网资源了。

图 18-1-5 登录 SSL VPN 成功

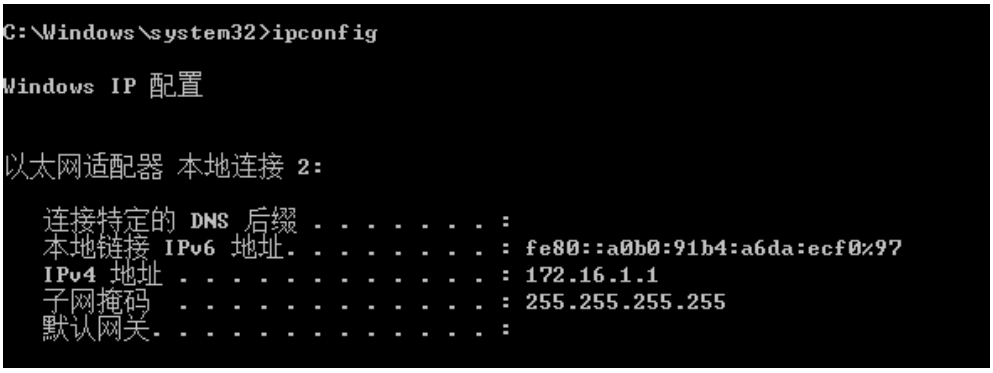

图 18-1-6 外部网主机 B-C-2 被分配了一个 VPN 指定的 IP 地址

成功登录 SSL VPN 后，在本地实体主机（即 B-C-2）的命令提示符窗口中，输入 ipconfig，

可以看到新增了一个“本地连接 2”，其 IP 地址是 172.16.1.1，子网掩码是 255.255.255.0，没有配置默认网关地址，如图 18-1-6 所示。这说明外部网用户 B-C-2 登录 SSL VPN 后，VPN 分配给登录用户一个指定的内网地址（此处是 172.16.1.1/24），外部网用户主机可以使用该地址与内部网主机进行通信。

步骤 9：配置 SSL VPN 之后的通信测试

此时，外部网主机 B-C-2 已经登录并通过了 SSL VPN 的认证（使用用户名 user_sslvpn，密码 abcd@1234），B-C-1 没有登录 SSL VPN。使用 Ping 命令测试内部网和外部网的通信情况，测试结果见表 18-1-7。可以看出，B-C-2 登录 SSL VPN 之后，就可以访问内部网主机了。

表 18-1-7 配置 SSL VPN 之后内部网和外部网的通信情况

序号	源设备	目的设备	通信结果
1	A-C-1	B-C-1	通
2	A-C-1	B-C-2	通
3	B-C-1	A-C-1	不通
4	B-C-2	A-C-1	通

步骤 10：抓包分析 SSL VPN 通信报文

此时，外部网用户主机 B-C-2 可以通过 SSL VPN 访问内部网主机 A-C-1。

（1）设计抓包位置

分别在①处和②处启动抓包程序，如图 18-1-7 所示。

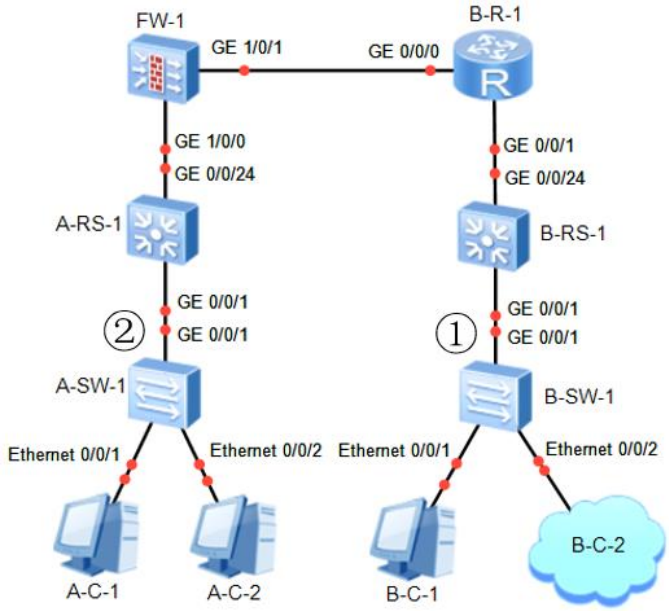

图 18-1-7 设计抓包位置，分析 SSL VPN 报文

在外部网主机 B-C-2（用本地实体主机代替，绑定的虚拟网卡地址 44.44.44.1）的命令提示符窗口中执行命令：ping 192.168.64.10，即访问内部网主机 A-C-1。

自行查看并分析报文，理解通过 VPN 访问内部资源时，报文的变化。