# 网络运维管理

## 第9讲　VPN

# 一、认识VPN

# 认识VPN

- 什么是VPN？
- 为什么需要使用VPN？

# 认识VPN

- 为什么需要使用VPN？
  - 【场景1】，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。
  - VPN之前，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

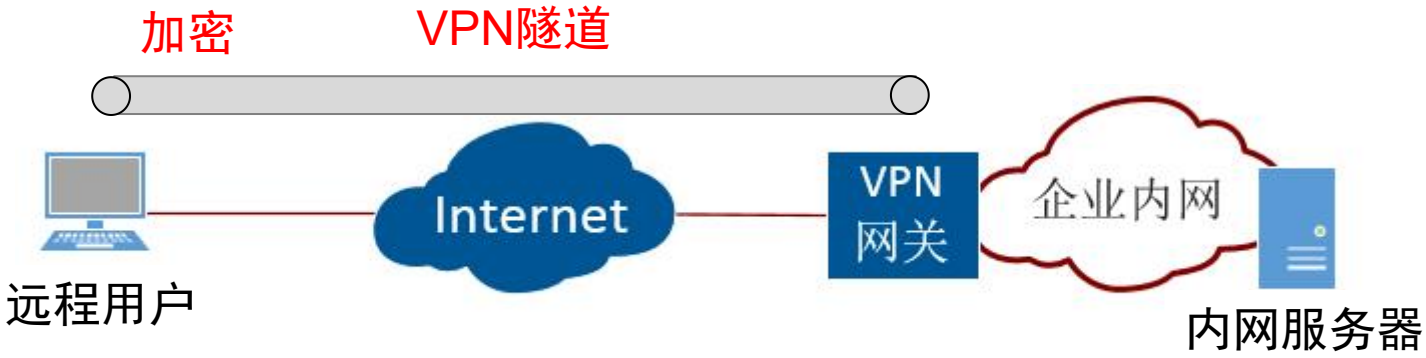
# 认识VPN

- 为什么需要使用VPN？
  - 【场景2】：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，即远程用户可以像内部网用户那样，访问内部服务器。

# 认识VPN

## 场景2的解决方案

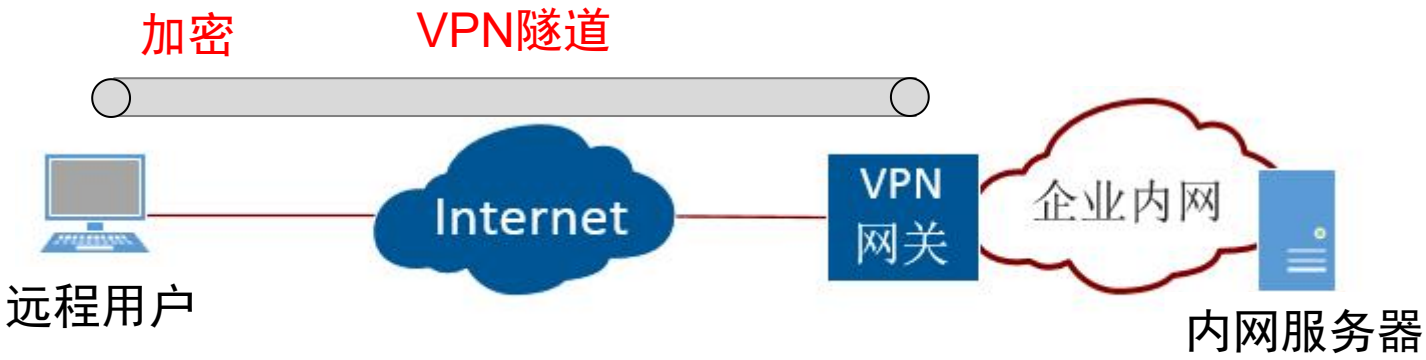
- 在内网中架设一台VPN网关设备（也可理解为VPN服务器）。外地员工在当地连上互联网后，通过互联网连接VPN网关，然后通过VPN网关进入企业内网。
- 为了保证数据安全，VPN网关和远程用户之间的通讯数据都进行了加密处理，可以认为数据是在一条专用的数据链路上进行安全传输，就如同专门架设了一个专用网络一样，但实际上VPN使用的是互联网上的公用链路。



# 认识VPN

## 定义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。



# 认识VPN

- 定义VPN
  - 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）。

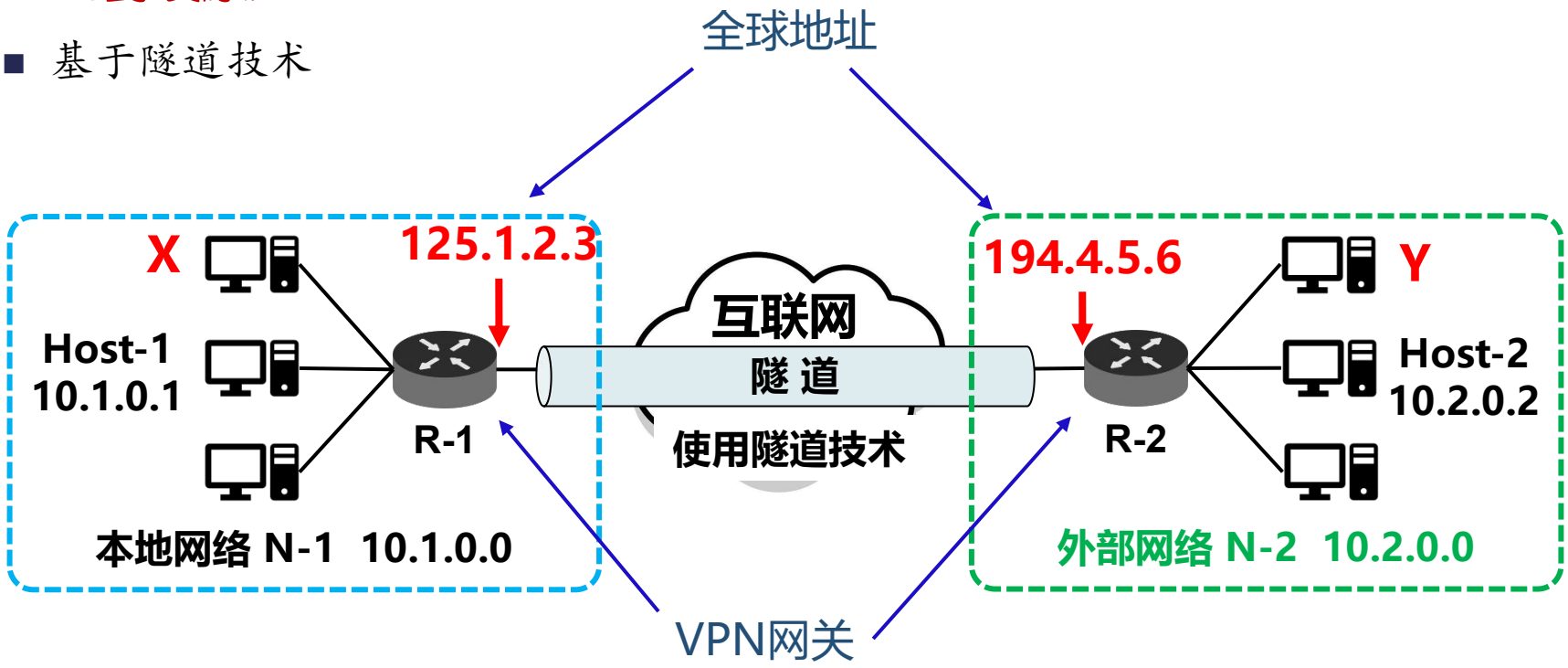
# 认识VPN

## VPN的封装原理

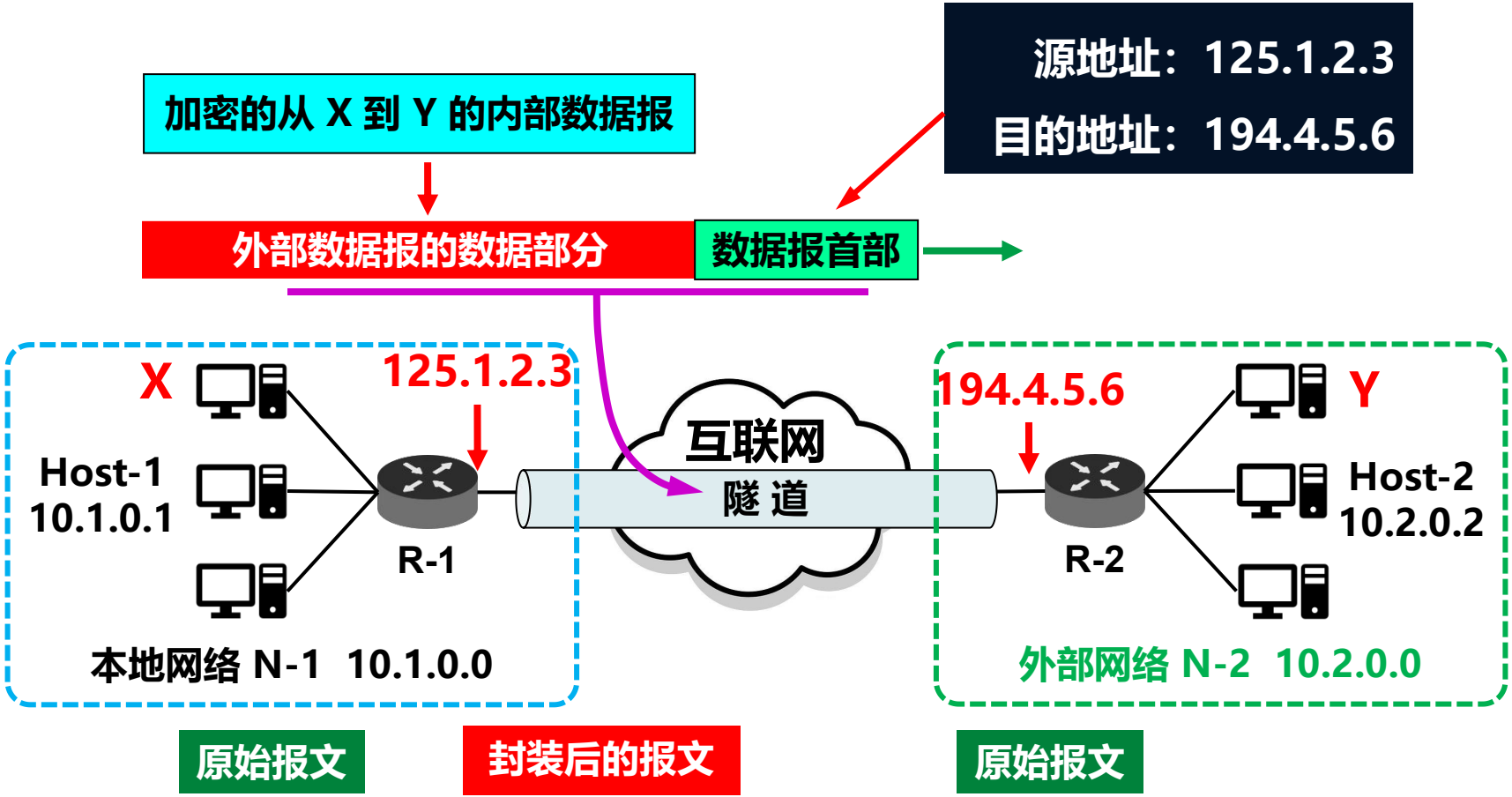
- VPN的基本原理是利用隧道（Tunnel）技术，对传输报文进行封装，利用VPN骨干网建立专用数据传输通道，实现报文的安全传输。
- 隧道技术使用一种协议封装另外一种协议报文（通常是IP报文），而封装后的报文也可以再次被其他封装协议所封装。对用户来说，隧道是其所在网络的逻辑延伸，在使用效果上与实际物理链路相同。
- 图例见下图

# 认识VPN

- VPN的封装原理
  - 基于隧道技术



# VPN的封装原理


源地址：125.1.2.3
目的地址：194.4.5.6
加密的从 X 到 Y 的内部数据报
外部数据报的数据部分
数据报首部
X
125.1.2.3
Host-1
10.1.0.1
R-1
互联网
隧 道
194.4.5.6
Y
Host-2
10.2.0.2
R-2
本地网络 N-1 10.1.0.0
外部网络 N-2 10.2.0.0
原始报文
封装后的报文
原始报文

# 二、SSL VPN的应用

# VPN

- 各种VPN技术简介
  - L2TP VPN
  - IPSec
  - GRE
  - SSL VPN
  - MPLS IP VPN

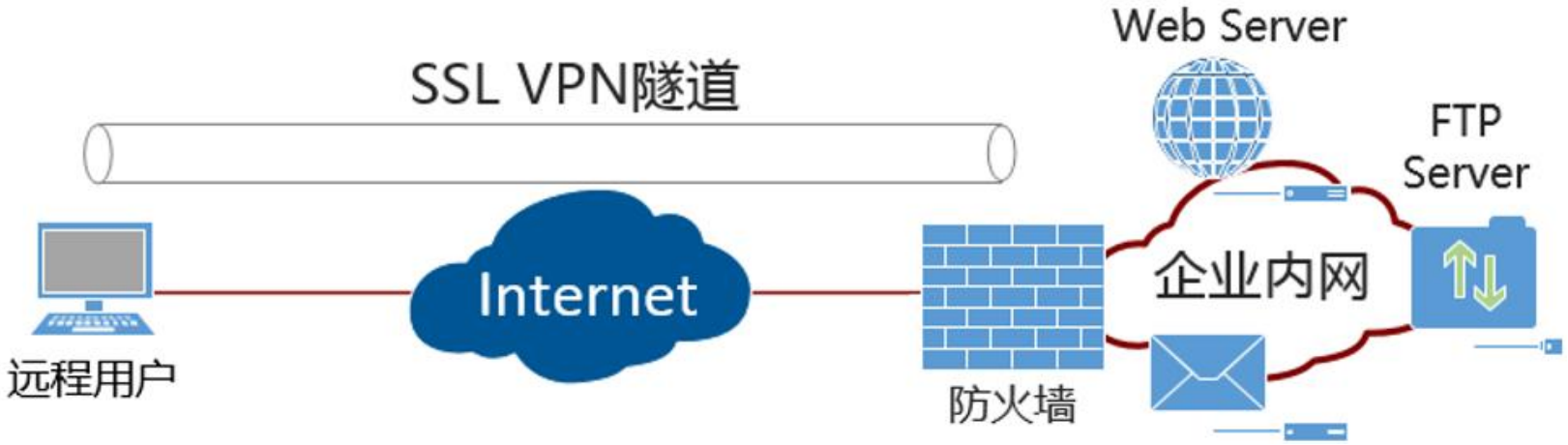
# SSL VPN的应用

## 认识SSL VPN

- SSL VPN是以SSL协议为安全基础的VPN远程接入技术。SSL VPN的主要应用场景是保证企业的远程用户能够在企业外部，安全、高效地访问企业内部的网络资源。
- 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；

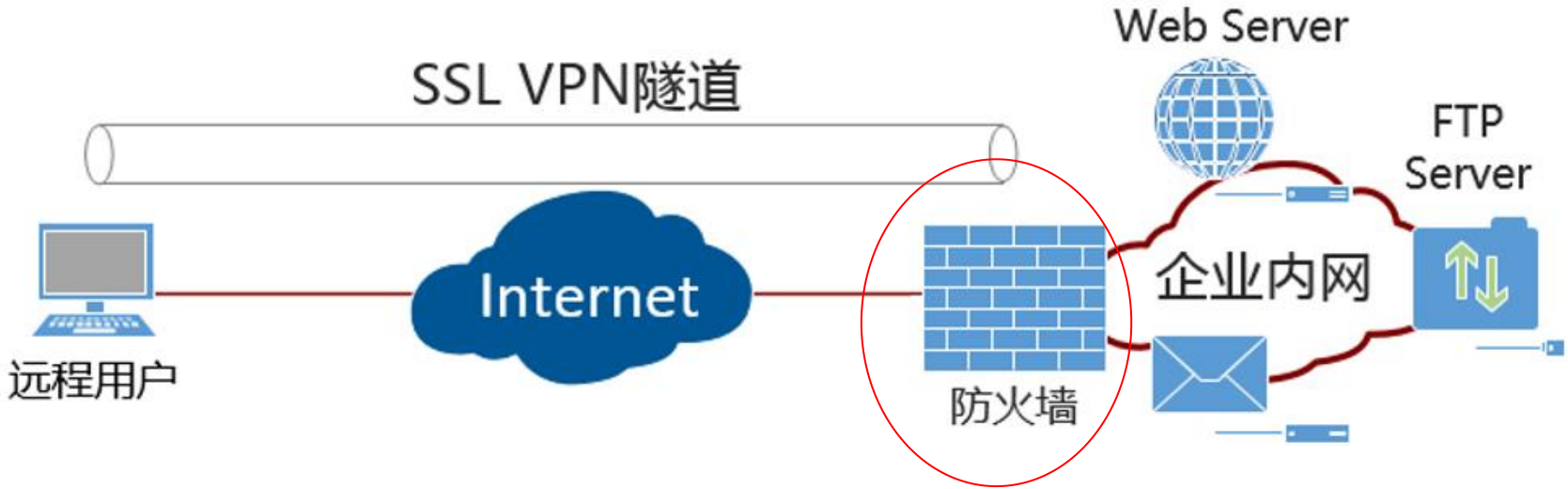
# SSL VPN的应用

- 远程用户通过SSL VPN访问企业内部资源的基本过程（1）
  - **例：**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。
  - 具体分析见下页



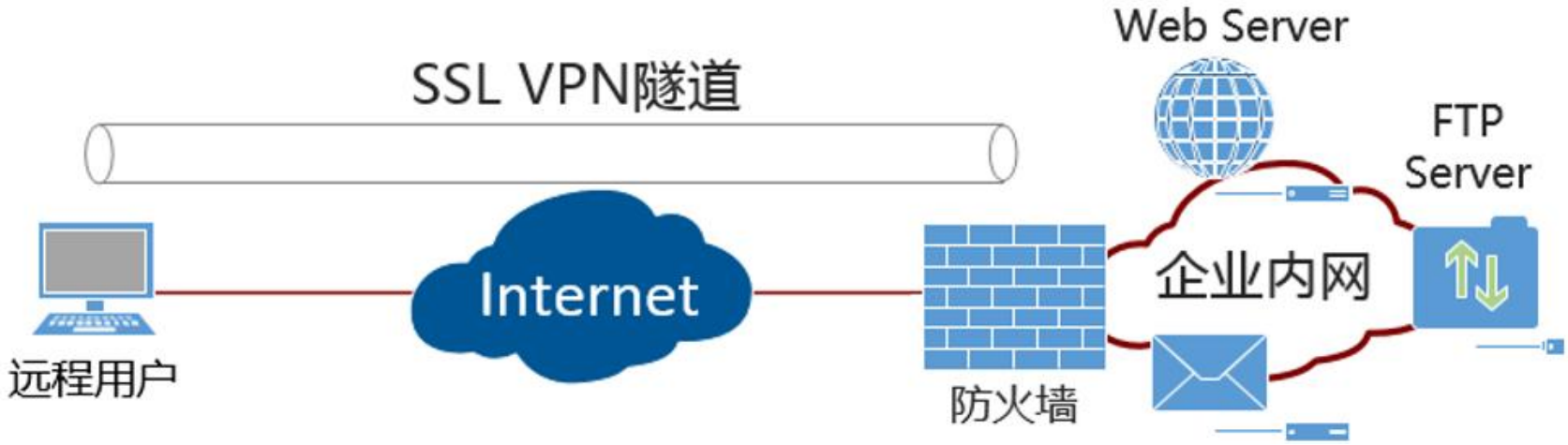
# SSL VPN的应用

- 远程用户通过SSL VPN访问企业内部资源的基本过程（2）
  - 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。



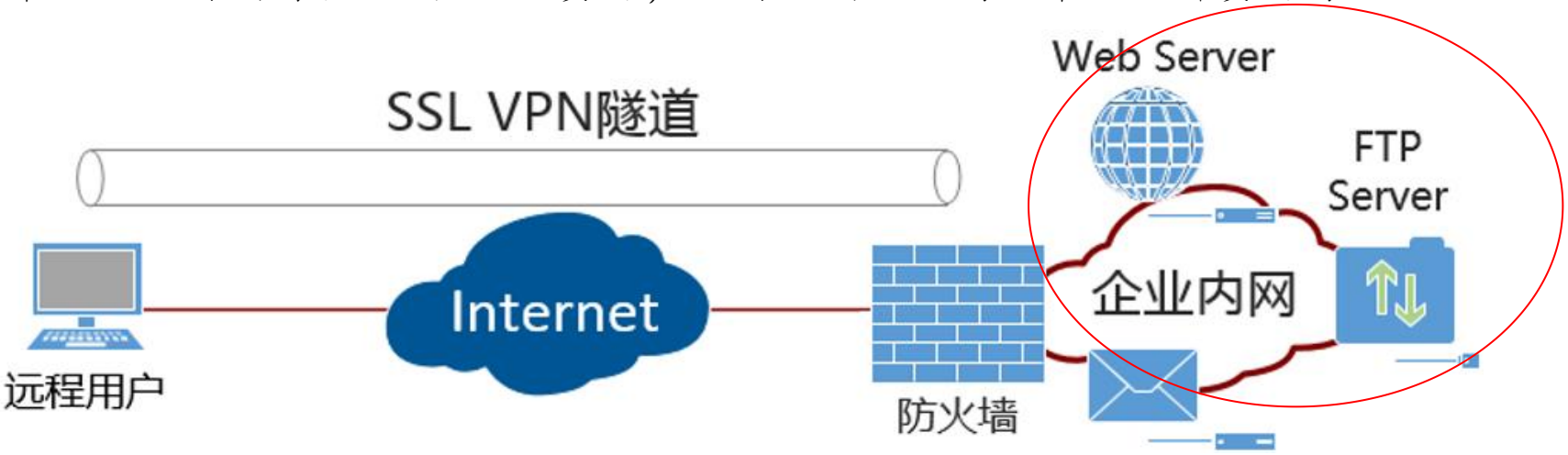
# SSL VPN的应用

- 远程用户通过SSL VPN访问企业内部资源的基本过程（3）
  - 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。



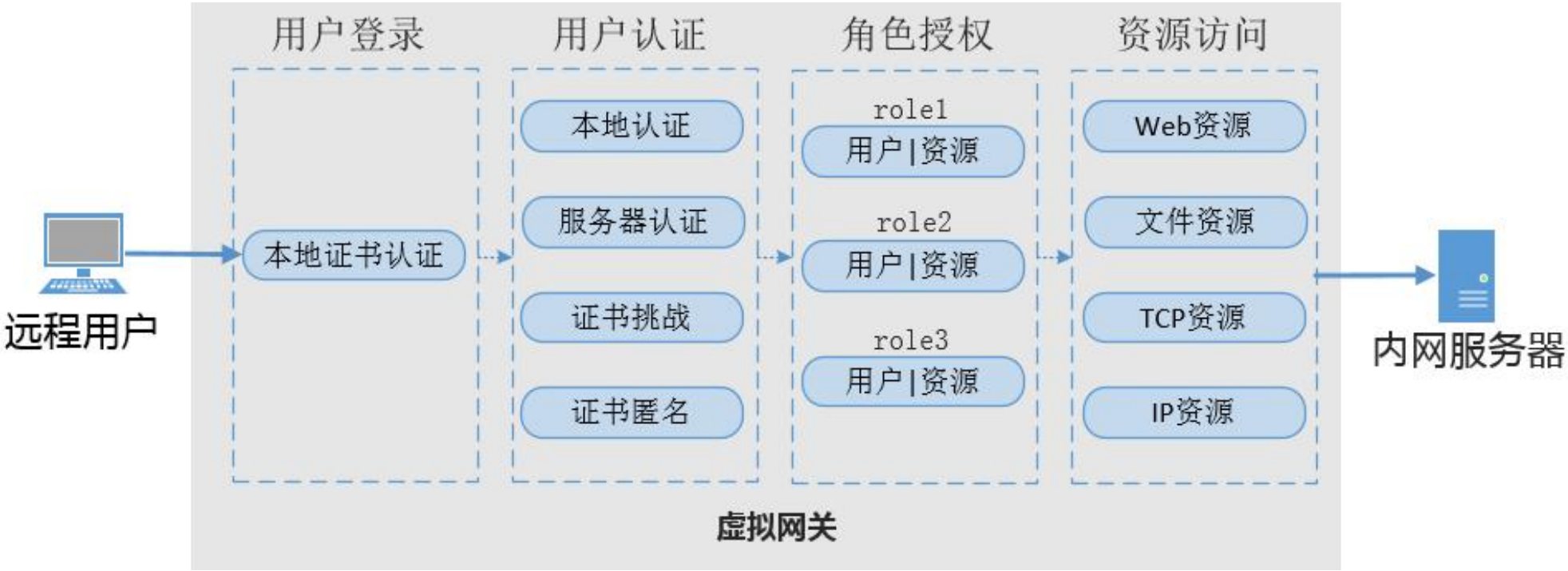
# SSL VPN的应用

- 远程用户通过SSL VPN访问企业内部资源的基本过程（4）
  - 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等。



# SSL VPN工作流程

- 远程用户通过SSL VPN访问企业内部资源的总体流程



# SSL VPN工作流程

- 远程用户通过SSL VPN访问企业内网资源的总体流程
  - 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

# SSL VPN的应用

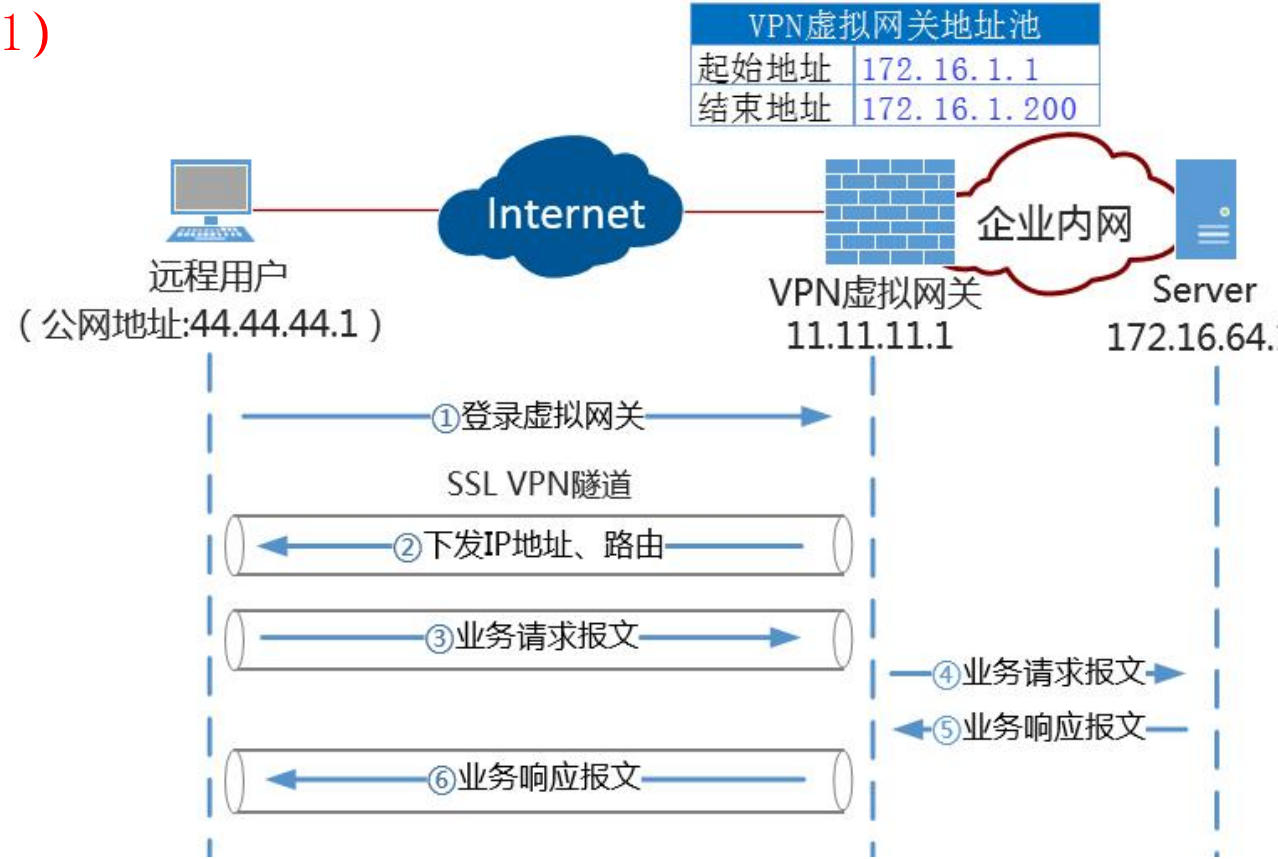
## SSL VPN的四种访问方式

- 根据远程用户访问内网资源类型的不同，SSL VPN提供了四种内网访问方式

| 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时使用文件共享业务。<br>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。<br>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。 |

# SSL VPN的应用

- SSL VPN网络扩展访问过程（1）
  - 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，其内部交互过程如右图



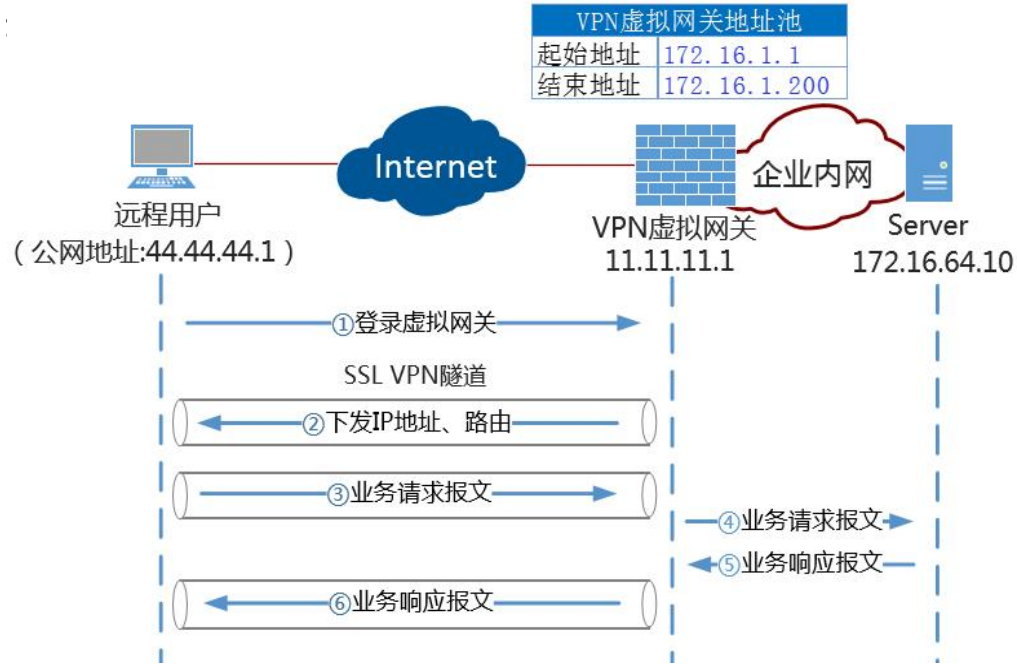
# SSL VPN的应用

- SSL VPN网络扩展访问过程（2）

1. 远程用户通过Web浏览器登录虚拟网关

   - 报文首部的IP地址？
     - 源IP： 44.44.44.1
     - 目的IP：11.11.11.1

- 成功登录虚拟网关后启动网络扩展功能



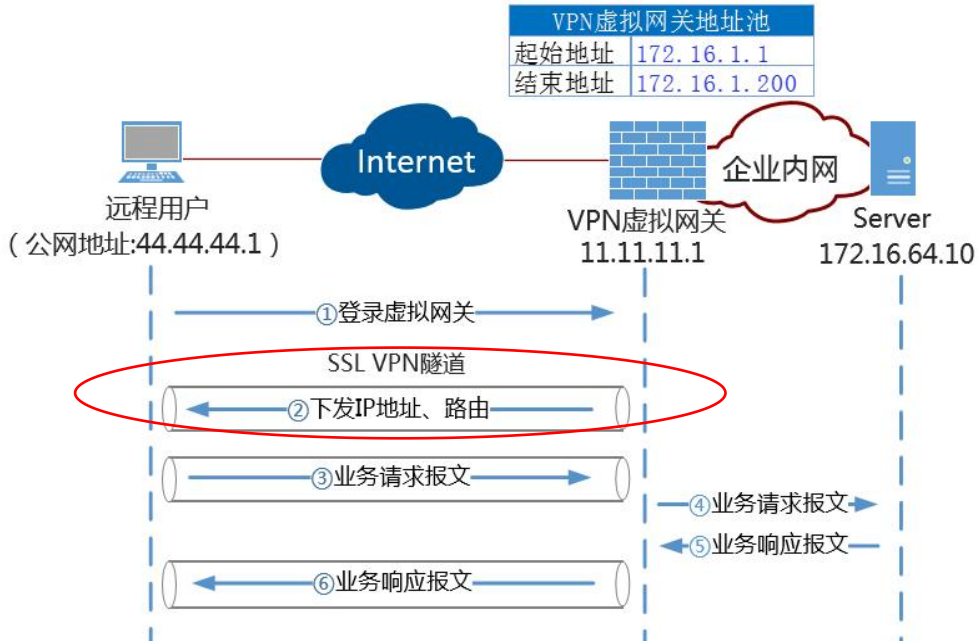
# SSL VPN的应用

- SSL VPN网络扩展访问过程（3）

2. 启动网络扩展功能会触发以下几个动作：

① 远程用户与虚拟网关之间会建立一条SSL VPN隧道；

② 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；

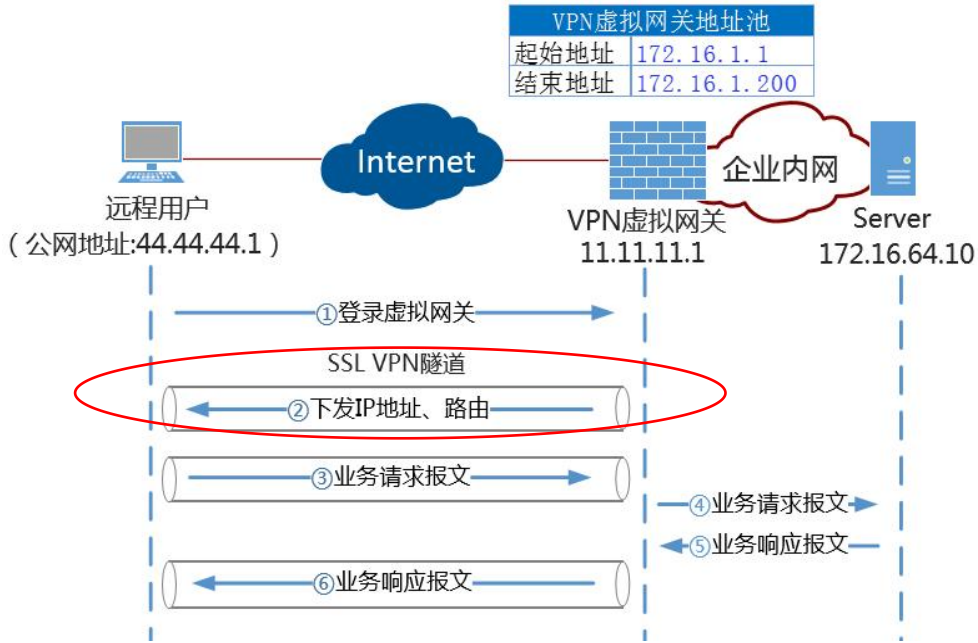


# SSL VPN的应用

- SSL VPN网络扩展访问过程（4）

2. 启动网络扩展功能会触发以下几个动作：

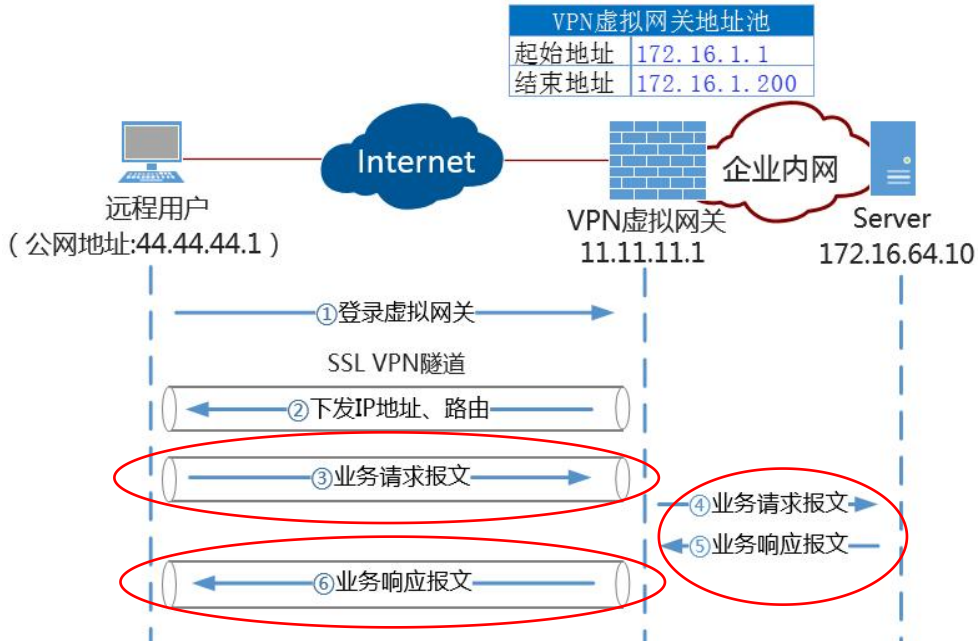
③ 虚拟网关向远程用户下发到达企业内网Server的路由信息。虚拟网关会根据网络扩展业务中的配置，向远程用户下发不同的路由信息。



# SSL VPN的应用

- SSL VPN网络扩展访问过程（5）

3. 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。
4. 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。
5. 内网Server响应远程用户的业务请求。
6. 响应报文到达虚拟网关后进入SSL VPN隧道。
7. 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

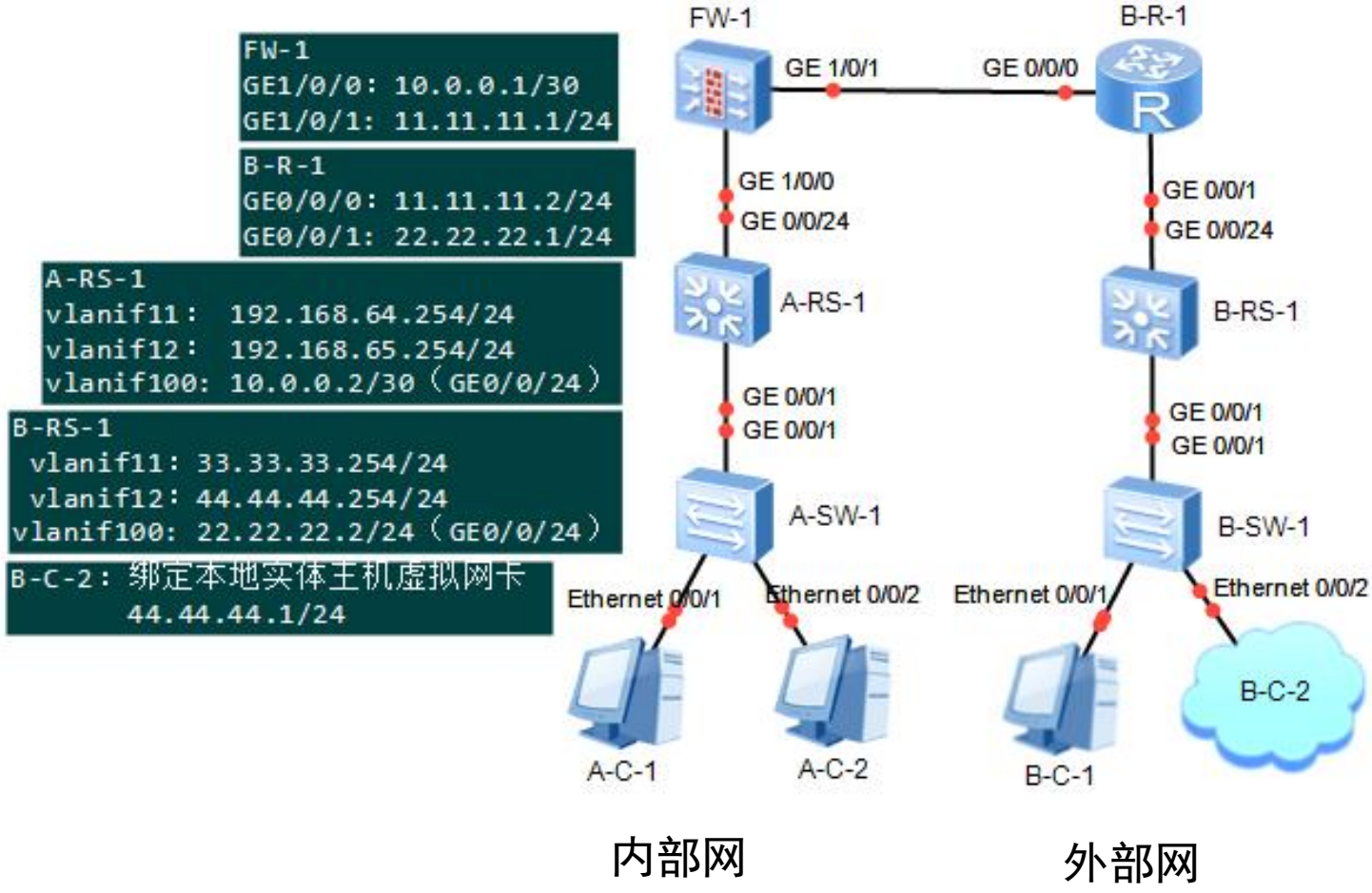


# 三、SSL VPN案例分析

# 案例1：

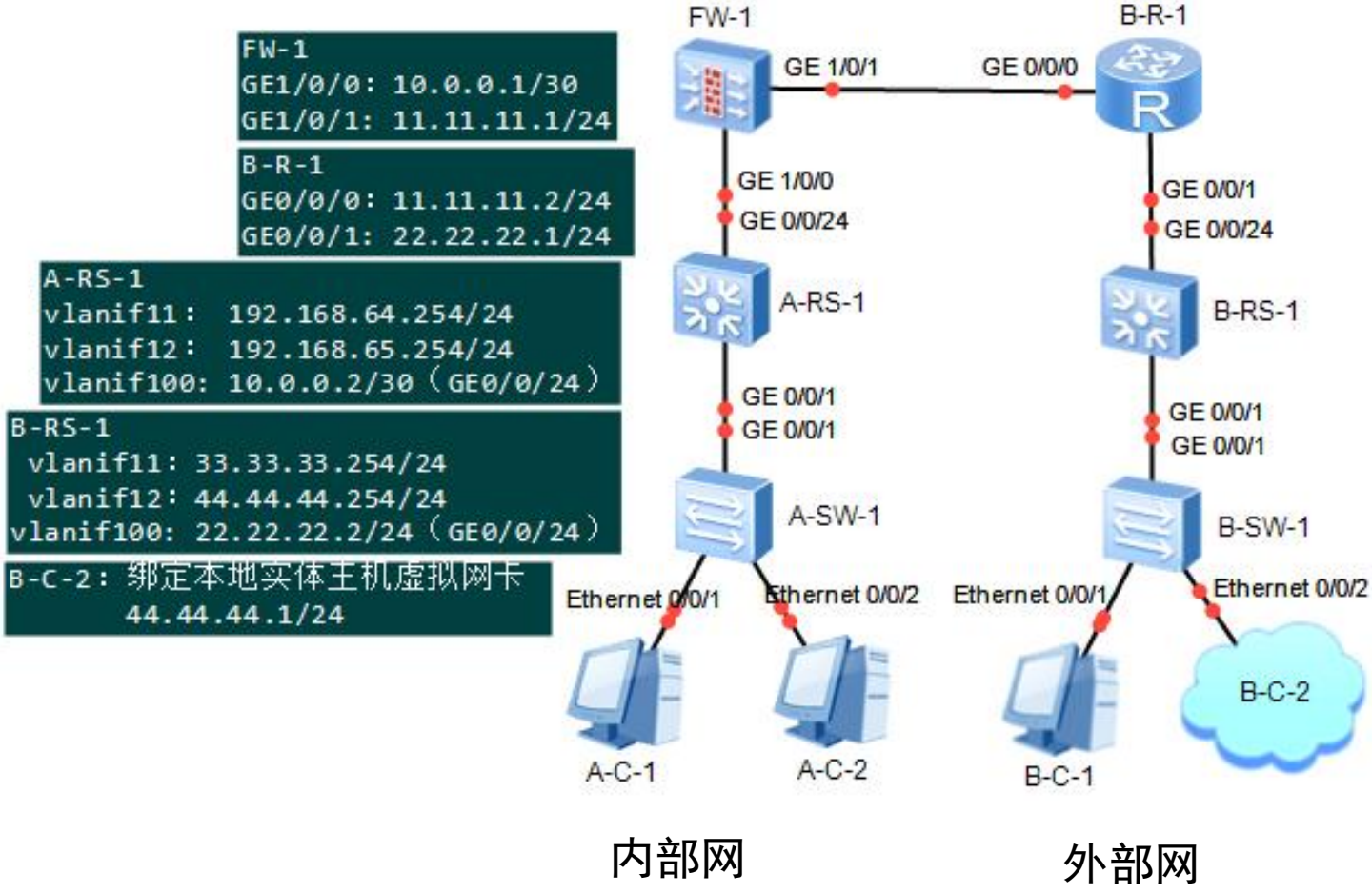
## 拓扑分析

- 内部网用户通过NAT访问外部网。
- 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。



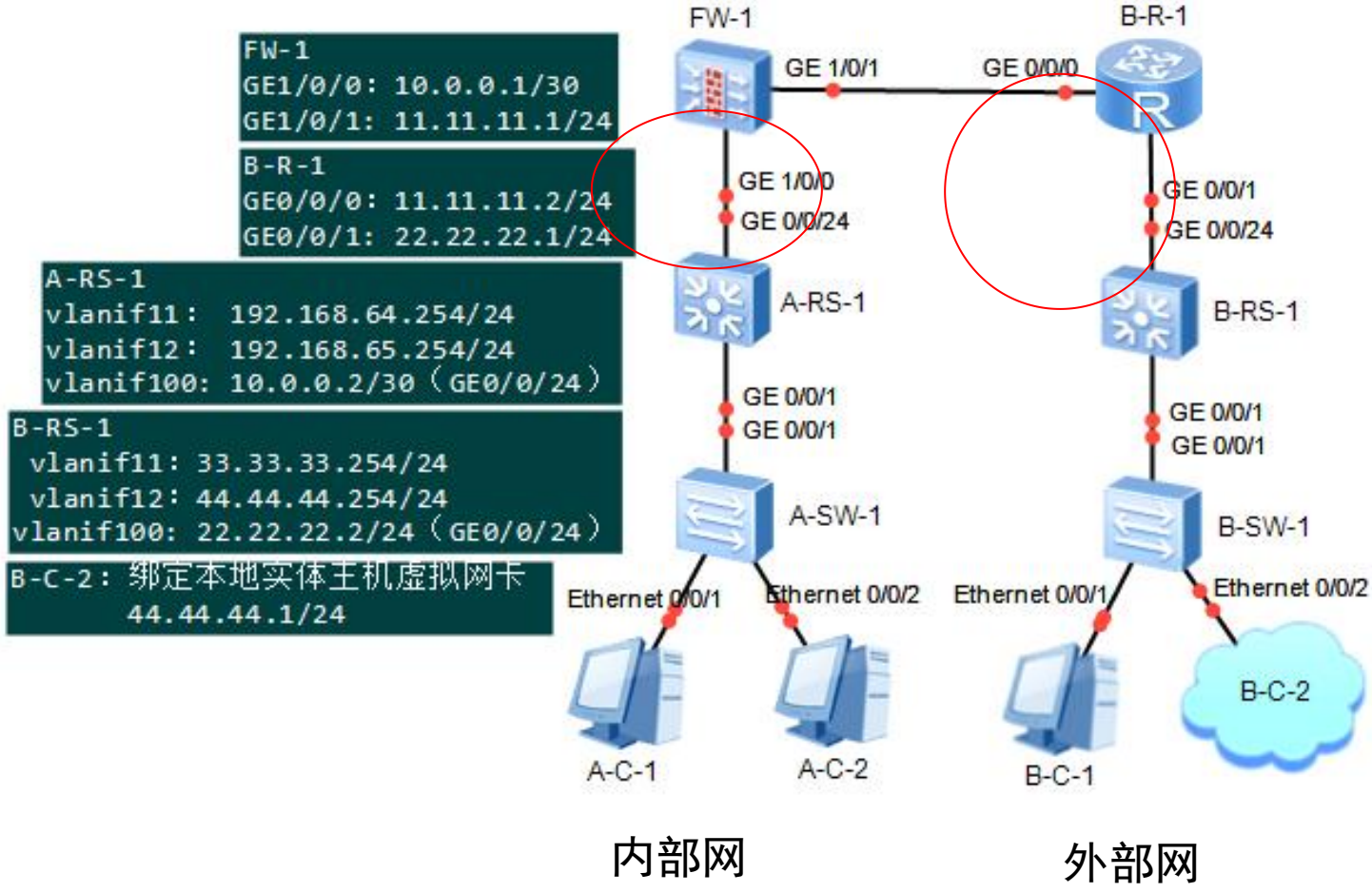
# 案例1：

- IP分析
- 内部网
  - 192.168.64.0/23
- 外部网
  - 11.11.11.0/24
  - 22.22.22.0/24
  - 33.33.33.0/24
  - 44.44.44.0/24



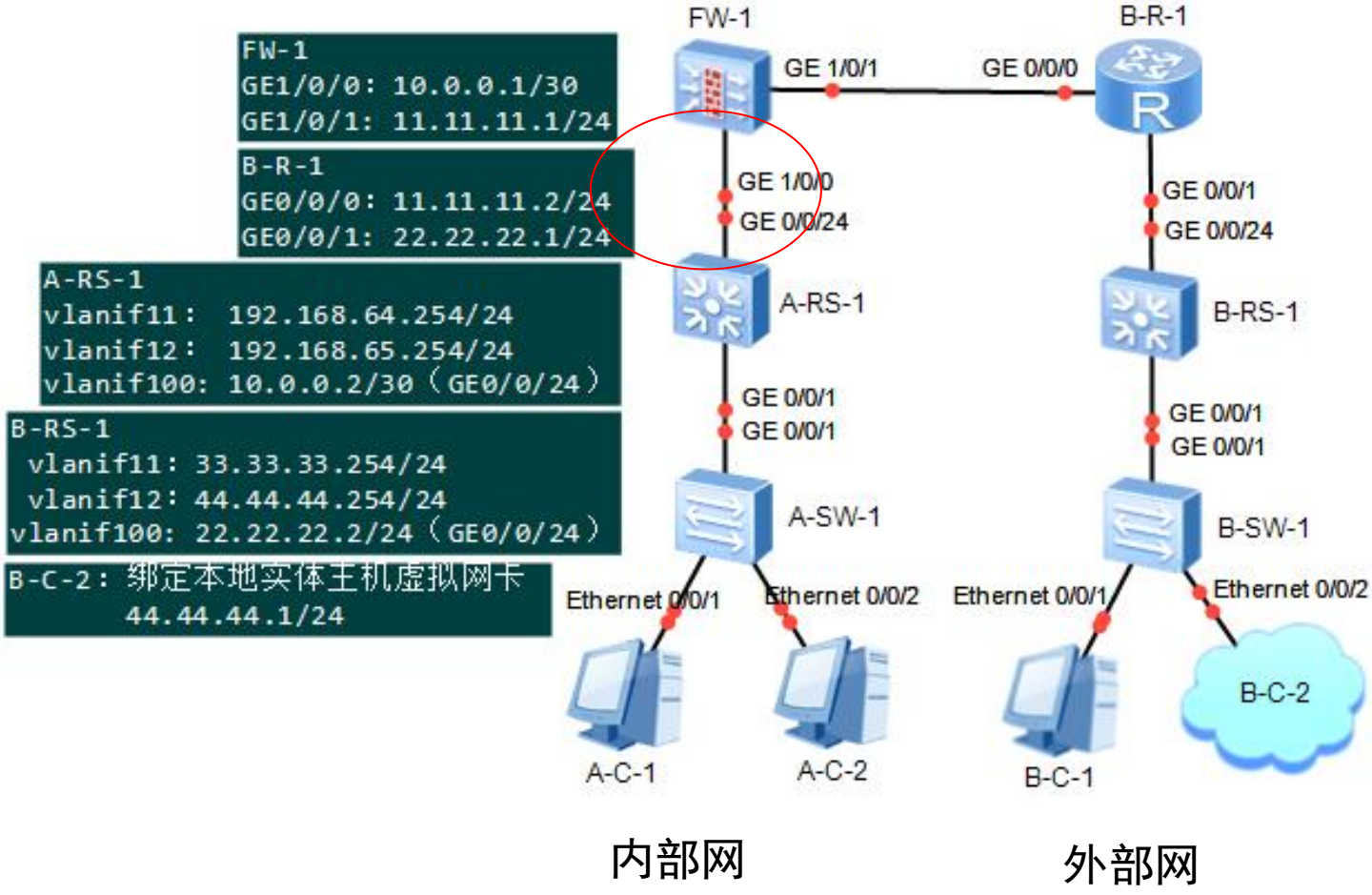
# 案例1：

- 路由分析
- OSPF
  - 区域设置？
- FW-1的静态路由
- A-RS-1能否获取外部网的网络路由信息？反之，B-RS-1能否获取内部网的网络路由信息？



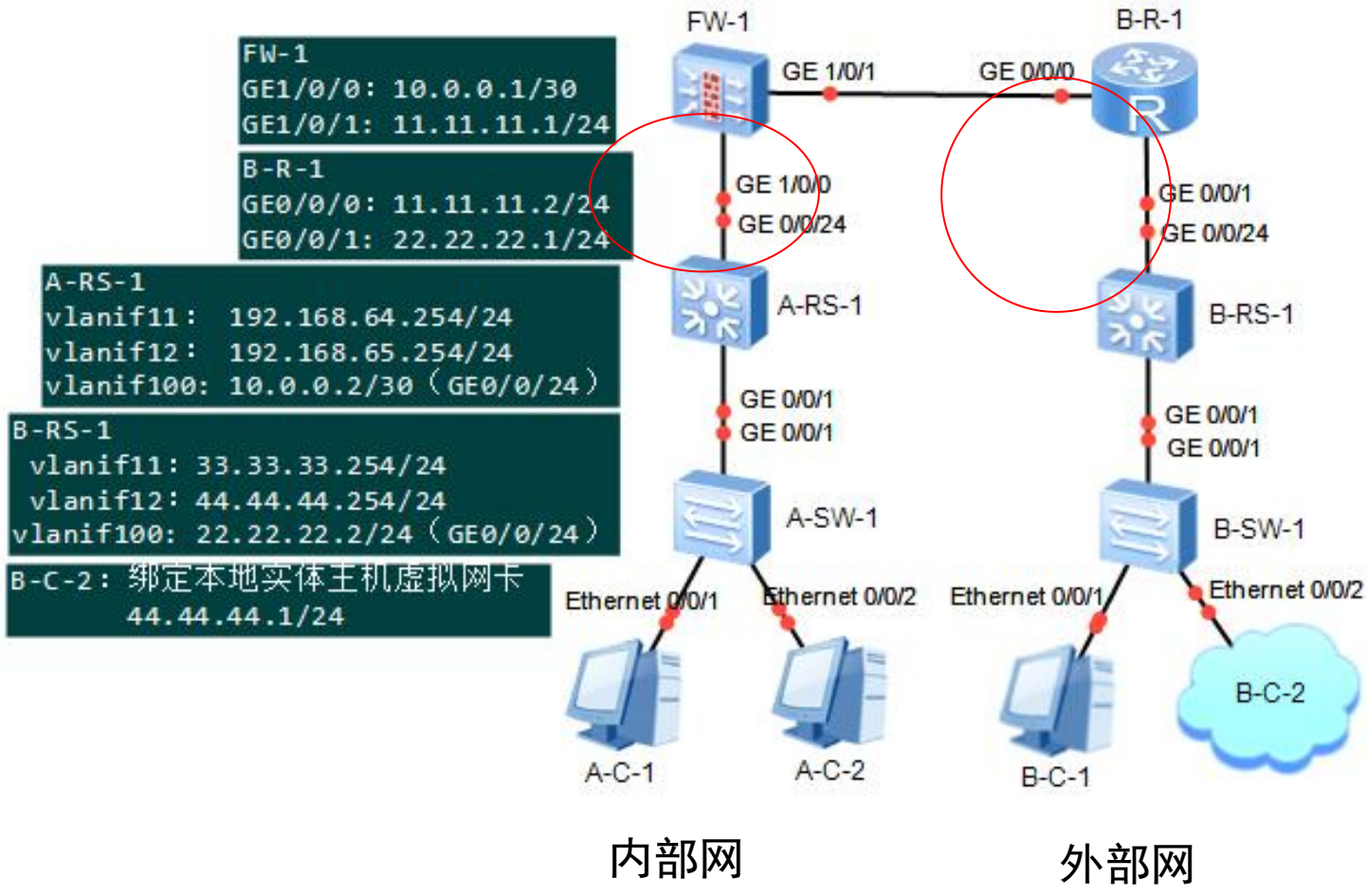
# 案例1：

- 步骤1：实现内部网通信



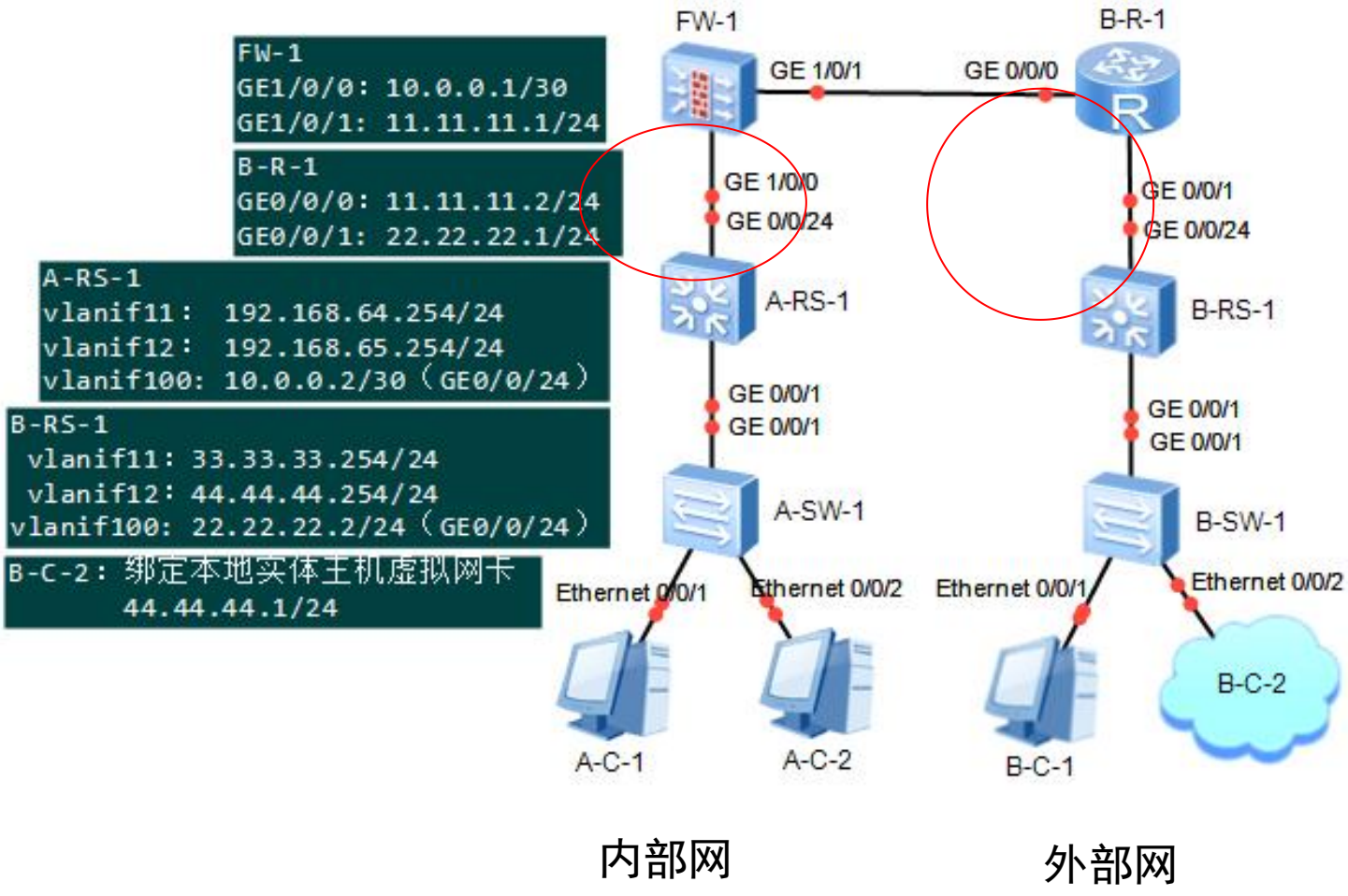
# 案例1：

- 步骤2：实现外部网通信
  - B-C-1能否ping通FW-1的GE1/0/1口？



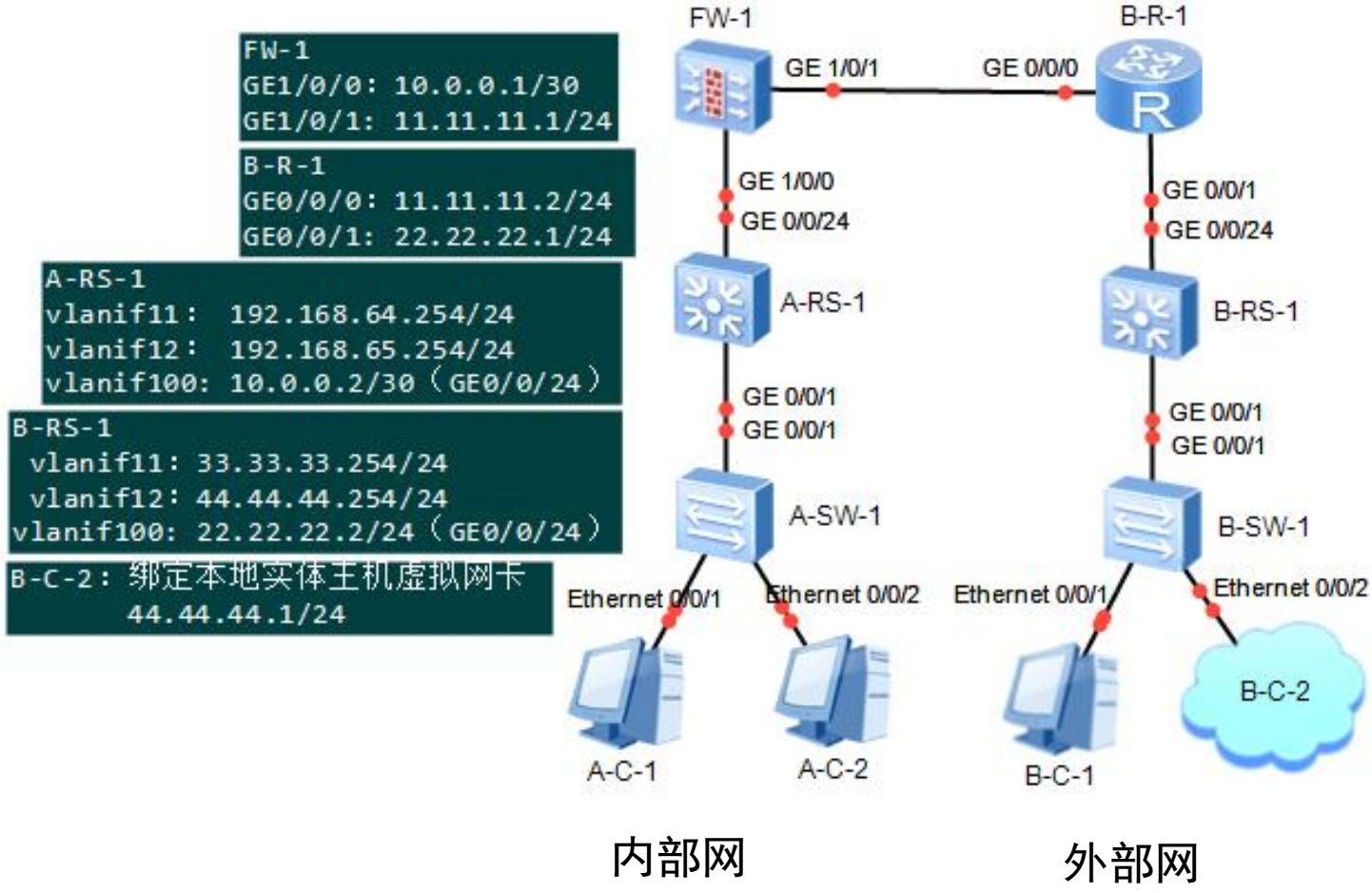
# 案例1：

- 步骤3：内部网用户NAT访问外部网
  - FW-1中的缺省路由
  - Default-route-advertise always//在ospf中引入缺省路由



# 案例1：

- 步骤4：在FW-1上配置SSL VPN
- 本地认证
- 创建SSL VPN用户组和用户
- 启用网络扩展业务
- 配置网络扩展的地址池（不能包含内网已经分配的IP地址）
- 设置VPN客户可以访问的网段



# 案例1：

- 步骤5：外网用户登录认证

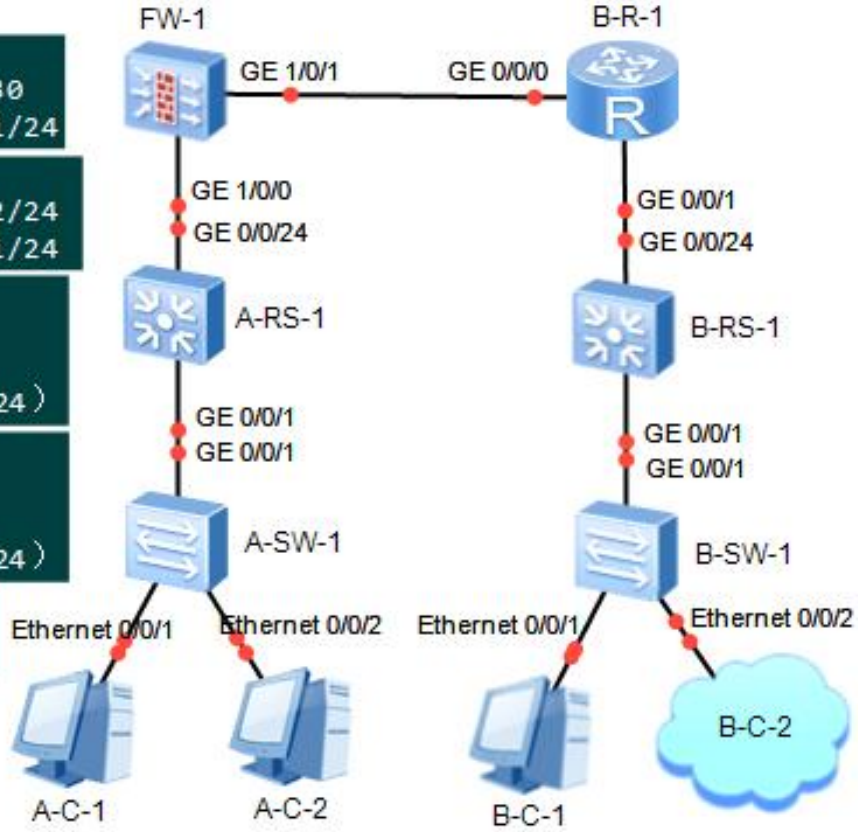
```
FW-1
GE1/0/0: 10.0.0.1/30
GE1/0/1: 11.11.11.1/24
```

```
B-R-1
GE0/0/0: 11.11.11.2/24
GE0/0/1: 22.22.22.1/24
```

```
A-RS-1
vlanif11:  192.168.64.254/24
vlanif12:  192.168.65.254/24
vlanif100: 10.0.0.2/30（GE0/0/24）
```

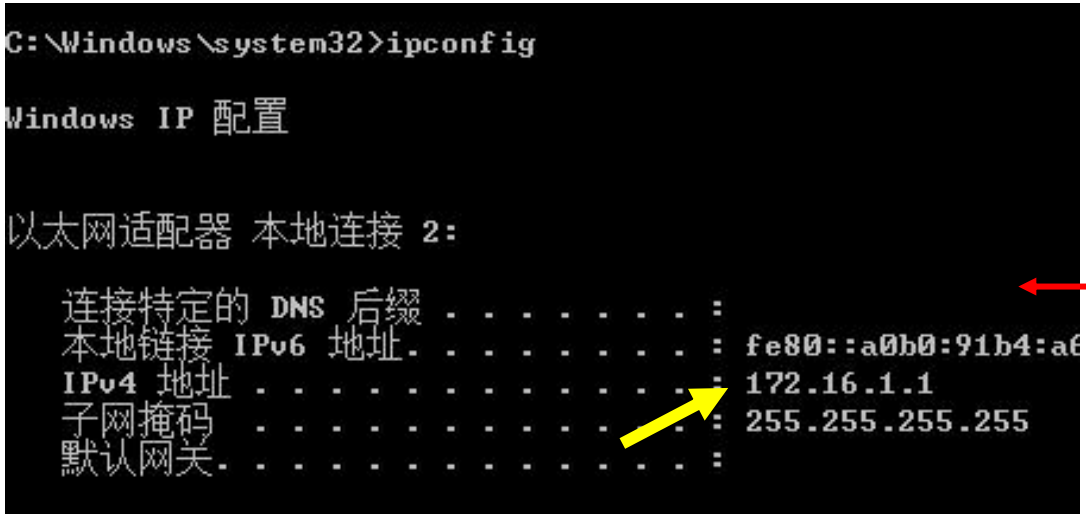
```
B-RS-1
 vlanif11: 33.33.33.254/24
 vlanif12: 44.44.44.254/24
vlanif100: 22.22.22.2/24（GE0/0/24）
```

```
B-C-2：绑定本地实体主机虚拟网卡
       44.44.44.1/24
```



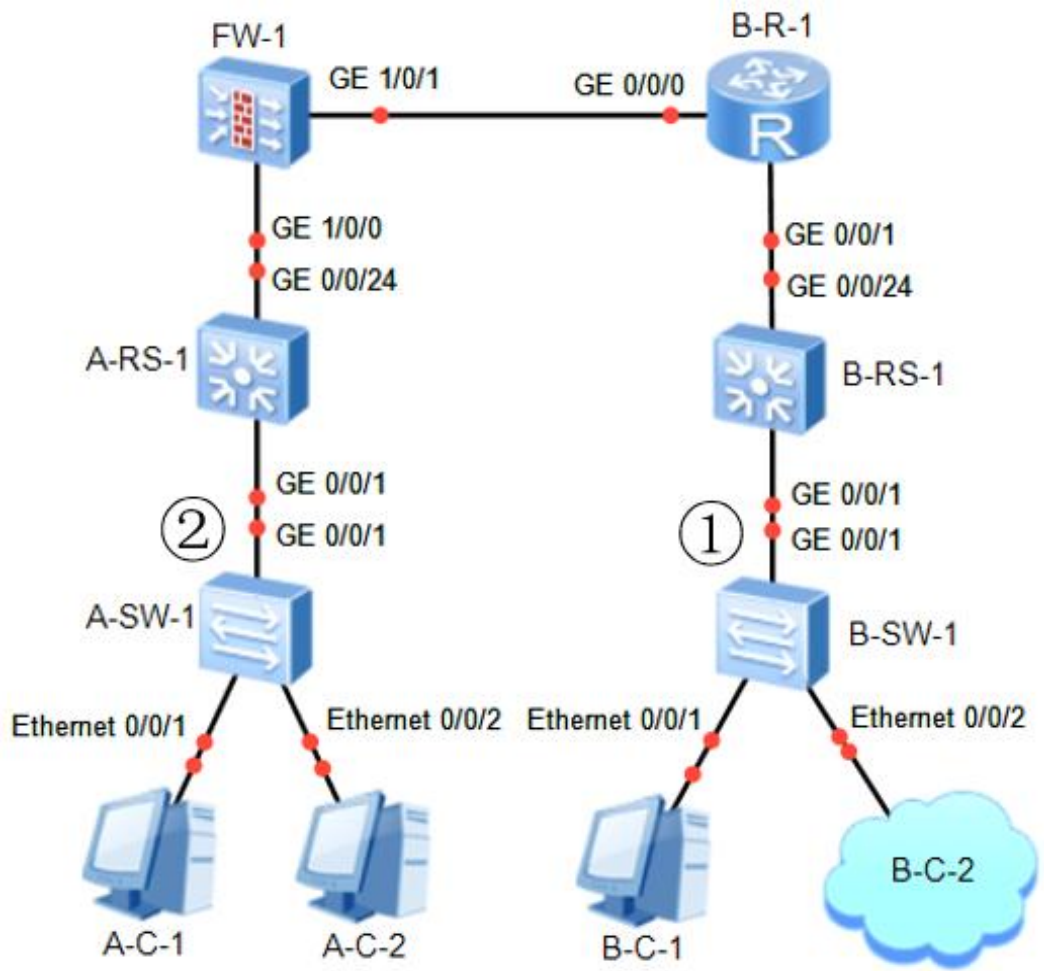
# 案例1：

- 步骤5：外网用户登录认证

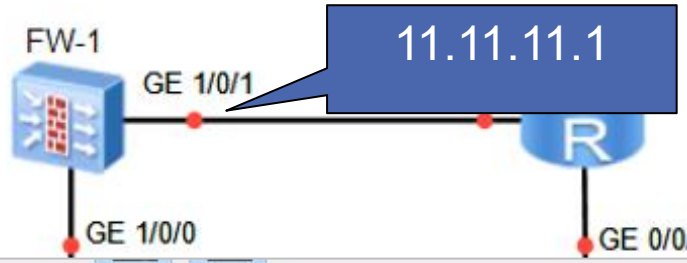

# 案例1：

- 步骤6：外网用户访问内网服务器
  - B-C-2可以访问A-C-1
  - 在①②处设置抓包点
  - 抓包分析见下页



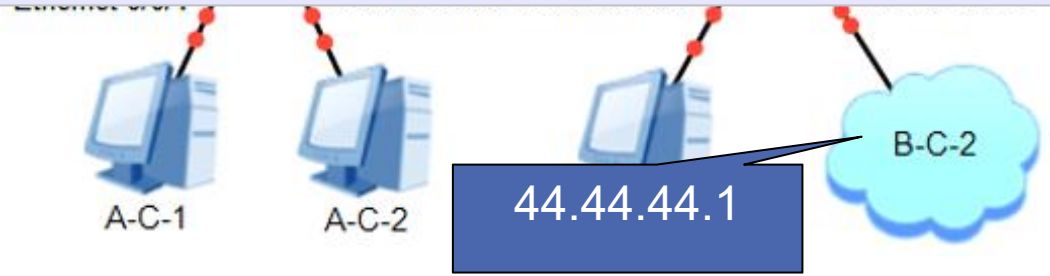
# 案例1：

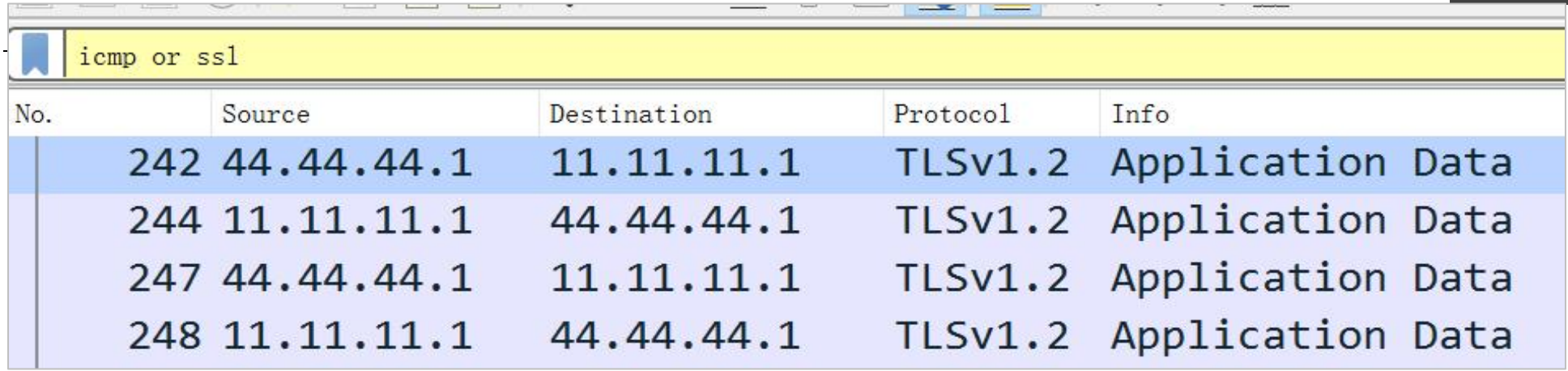
- 分析①处抓取到的报文



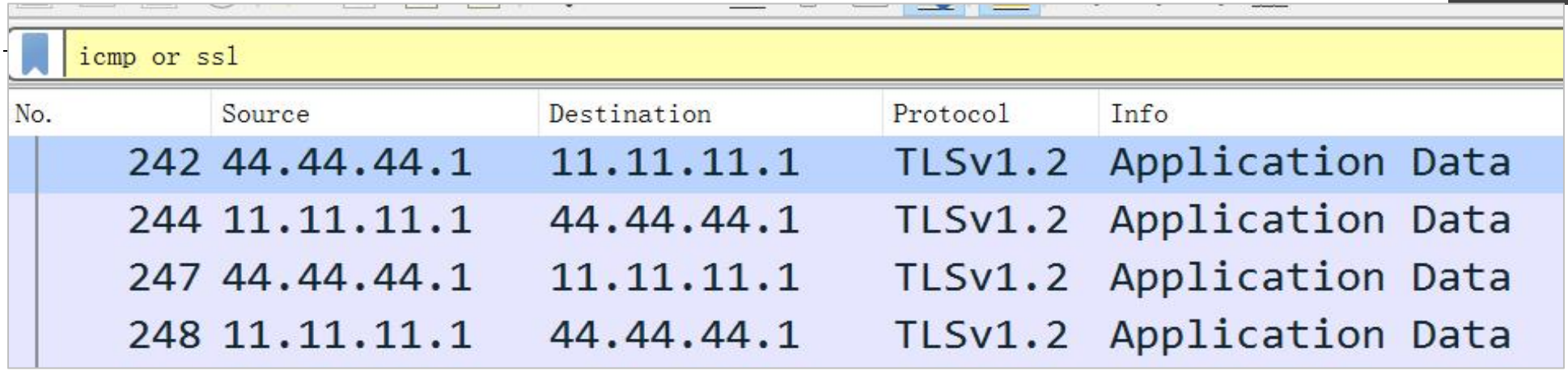

icmp or ssl

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 242 | 44.44.44.1 | 11.11.11.1 | TLSv1.2 | Application Data |
| 244 | 11.11.11.1 | 44.44.44.1 | TLSv1.2 | Application Data |
| 247 | 44.44.44.1 | 11.11.11.1 | TLSv1.2 | Application Data |
| 248 | 11.11.11.1 | 44.44.44.1 | TLSv1.2 | Application Data |






分析1：虽然B-C-2在登录SSL VPN后获取了SSL VPN虚拟网关指派的内网IP（172.16.1.1），并且执行的命令是ping 192.168.64.10，但从①处抓取的报文可以看出，这些报文并不是ICMP报文，而是SSL VPN报文（即TLSv1.2协议报文）。这些报文的源IP和目的IP分别是外网用户主机的IP（即44.44.44.1）和SSL VPN虚拟网关的IP（即11.11.11.1）。



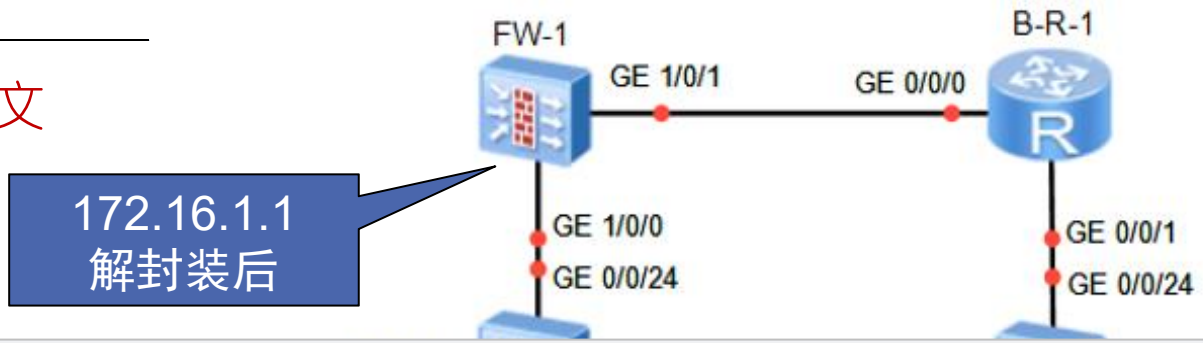

分析2：以242号报文为例，这是从外网用户B-C-2发往内网主机A-C-1的报文。但是根据SSL VPN的工作原理，在主机B-C-2和SSL VPN虚拟网关之间会建立隧道，B-C-2发出的ICMP报文（源IP是VPN分配的172.16.1.1，目的IP是192.168.64.10）会被封装起来（相当于放入隧道里），封装后的报文源IP是外网IP地址44.44.44.1，并且要发送到SSL VPN的虚拟网关，所以目的IP是SSL VPN虚拟网关的IP（11.11.11.1）。

```
Frame 242: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits) on interface 0
Ethernet II, Src: 0a:00:27:00:00:0d (0a:00:27:00:00:0d), Dst: HuaweiTe_7d:45:1b (4c:1f:c
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 12
Internet Protocol Version 4, Src: 44.44.44.1, Dst: 11.11.11.1
Transmission Control Protocol, Src Port: 51242, Dst Port: 443, Seq: 12481, Ack: 3352, Le
Transport Layer Security
▾ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 128
    Encrypted Application Data: 399bb17f66fe69598a3adbad1fe4a6d72e9274aa3b0d343a…
```

分析3：242号报文的内容如图所示，根据SSL VPN工作原理可以看出，报文的数据部分是加密的。

# 案例1：

- 分析②处抓取到的报文




172.16.1.1
解封装后

icmp or ssl

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 25 | 172.16.1.1 | 192.168.64.10 | ICMP | Echo (ping) request id=0x0001, seq=89/22784, |
| 26 | 192.168.64.10 | 172.16.1.1 | ICMP | Echo (ping) reply id=0x0001, seq=89/22784, |
| 28 | 172.16.1.1 | 192.168.64.10 | ICMP | Echo (ping) request id=0x0001, seq=90/23040, |
| 29 | 192.168.64.10 | 172.16.1.1 | ICMP | Echo (ping) reply id=0x0001, seq=90/23040, |


192.168.64.10

icmp or ssl

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 25 | 172.16.1.1 | 192.168.64.10 | ICMP | Echo (ping) request id=0x0001, seq=89/22784, |
| 26 | 192.168.64.10 | 172.16.1.1 | ICMP | Echo (ping) reply id=0x0001, seq=89/22784, |
| 28 | 172.16.1.1 | 192.168.64.10 | ICMP | Echo (ping) request id=0x0001, seq=90/23040, |
| 29 | 192.168.64.10 | 172.16.1.1 | ICMP | Echo (ping) reply id=0x0001, seq=90/23040, |

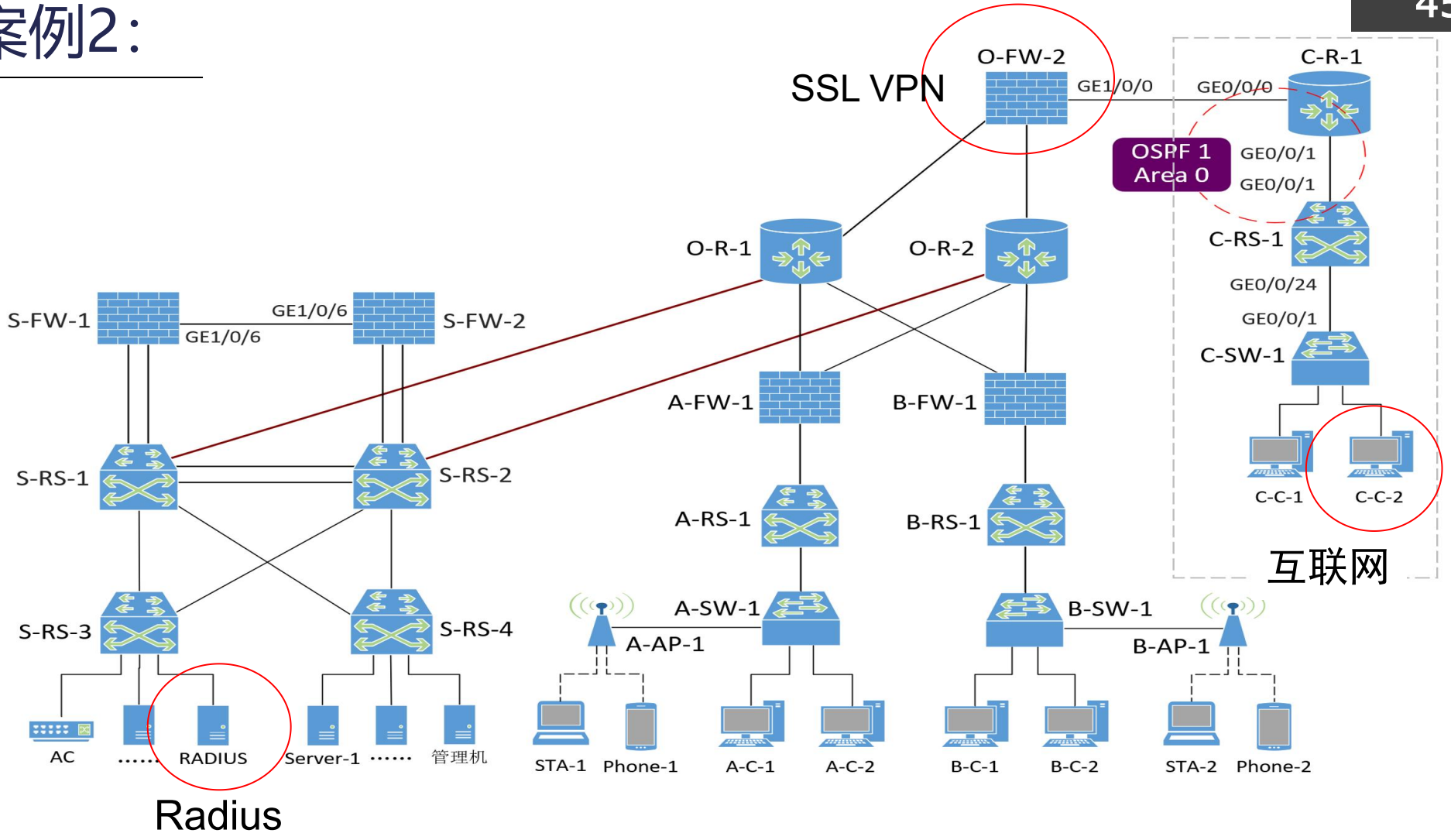
分析1：B-C-2登录SSL VPN后，从B-C-2发出的ICMP报文被重新封装后，以加密的方式先发送到SSL VPN的虚拟网关。在虚拟网关处，报文被解封装，然后发送到内部网主机

```
> Frame 25: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
> Ethernet II, Src: HuaweiTe_60:04:b6 (4c:1f:cc:60:04:b6), Dst: HuaweiTe_ac:0f:36 (54:89:98:ac:0f:36)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 11
> Internet Protocol Version 4, Src: 172.16.1.1, Dst: 192.168.64.10
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d02 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 89 (0x0059)
    Sequence number (LE): 22784 (0x5900)
    [Response frame: 26]
  v Data (32 bytes)
      Data: 61626364656667686 96a6b6c6d6e6f707172737475767761…
      [Length: 32]
```

ICMP报文

分析2：解封装后，报文的协议显示为ICMP，源IP就是SSL VPN虚拟网关指派的内网IP（172.16.1.1），目的IP为内部网主机A-C-1（192.168.64.10）的IP地址，并且该报文不再加密，

# 案例2：


SSL VPN
O-FW-2
GE1/0/0
C-R-1
GE0/0/0
OSPF 1
Area 0
GE0/0/1
GE0/0/1
C-RS-1
GE0/0/24
GE0/0/1
C-SW-1
C-C-1
C-C-2
互联网
O-R-1
O-R-2
S-FW-1
GE1/0/6
GE1/0/6
S-FW-2
A-FW-1
B-FW-1
S-RS-1
S-RS-2
A-RS-1
B-RS-1
S-RS-3
S-RS-4
A-SW-1
B-SW-1
A-AP-1
B-AP-1
AC
RADIUS
Server-1
管理机
STA-1
Phone-1
A-C-1
A-C-2
B-C-1
B-C-2
STA-2
Phone-2
Radius

# Thanks