

# 网络技术与信息安全



## 第12讲 VPN实现安全通信

# 本讲教学目标

---

- 理解为什么需要使用VPN
- 理解VPN的安全通信原理
- 掌握SSL VPN的部署配置

## 一、认识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。
- 应用VPN之前，为了防止信息泄露，需要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，还是通过Internet进行通信，但通过在总部和分支机构部署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

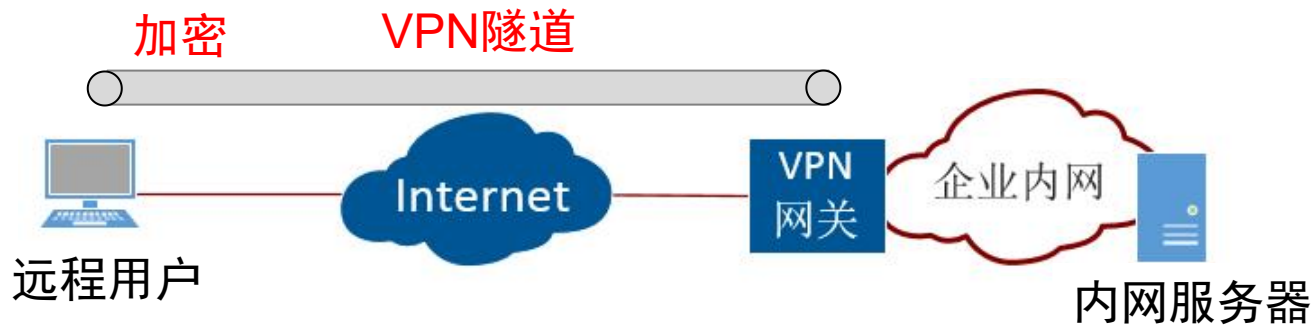
## □ 为什么需要使用VPN？

- 【场景2】：园区网内部的一些重要资源（服务器）通常只允许园区网内部用户访问，因为位于互联网上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“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，安全地访问内部服务器。

# 认识VPN

## □ 场景2的解决方案

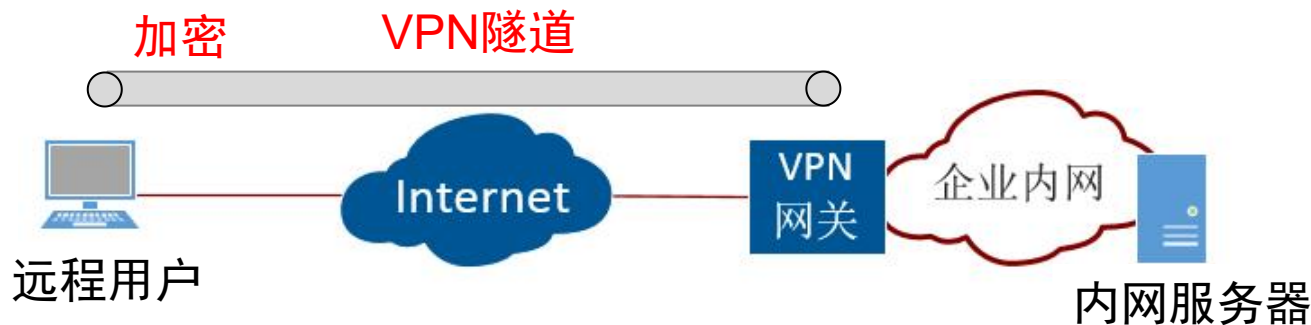
- 在内网中架设一台VPN网关（或VPN服务器）。外地员工在当地连上互联网后，首先登录VPN网关。登录成功后，远程用户和VPN网关之间的通信都被进行了特殊的封装加密处理，仿佛在两者之间建立了一条安全的“隧道”。
- 这样，虽然VPN网关和远程用户之间仍然使用的是互联网的公共链路，但就好像是在一个专用网络上通信，提升了安全性。



# 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

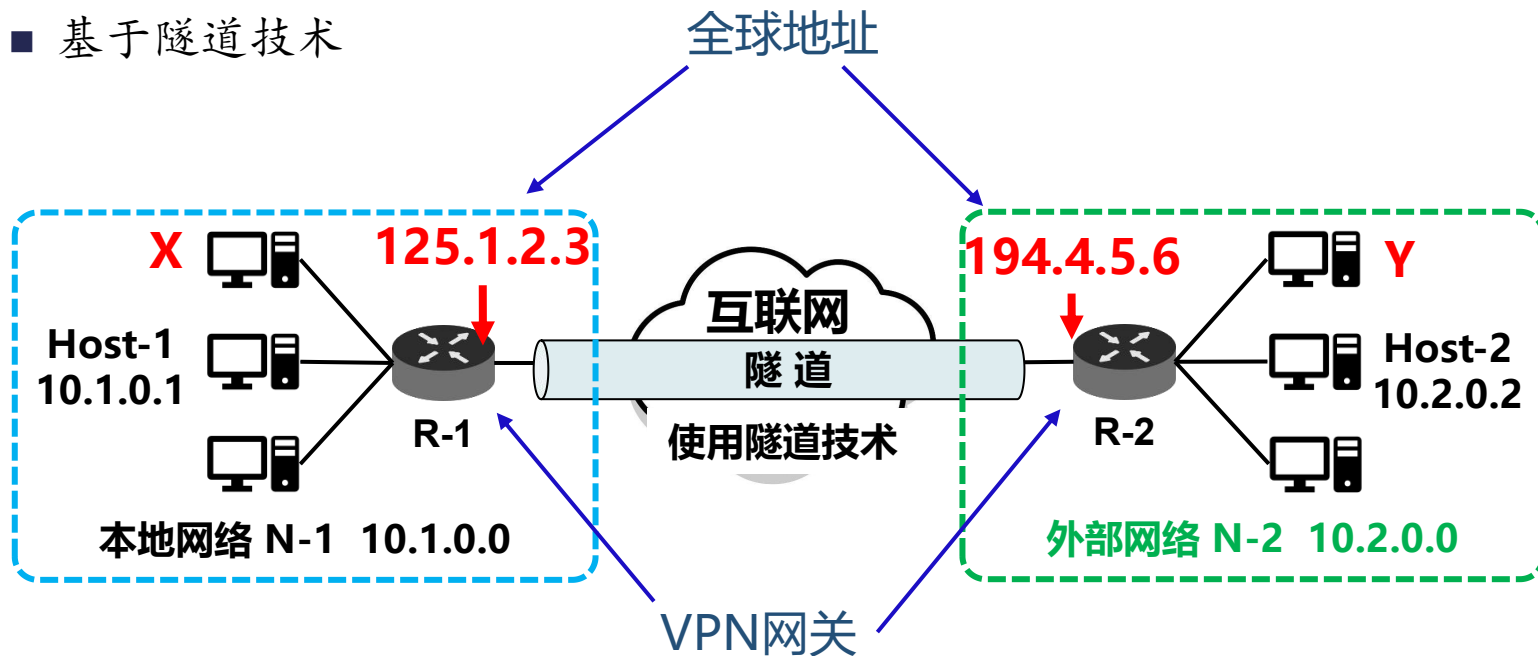
## □ VPN的封装原理

- 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

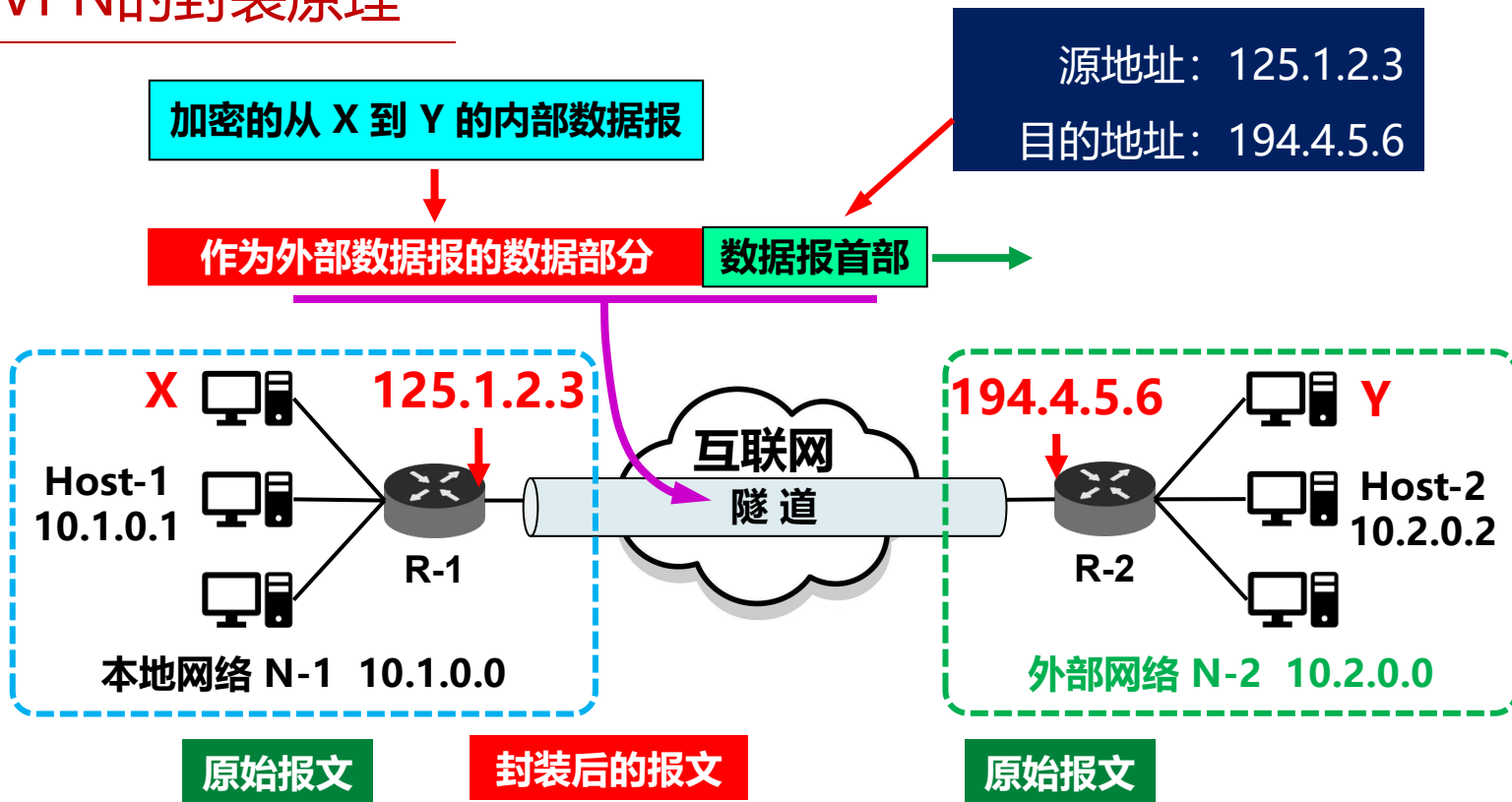
# 认识VPN

## □ VPN的封装原理

### ■ 基于隧道技术



## ➤ VPN的封装原理



## 二、SSL VPN的应用

# VPN

---

- 各种VPN技术简介
  - L2TP VPN
  - IPSec
  - GRE
  - SSL VPN（本课程讲授）
  - MPLS IP VPN

# SSL VPN的应用

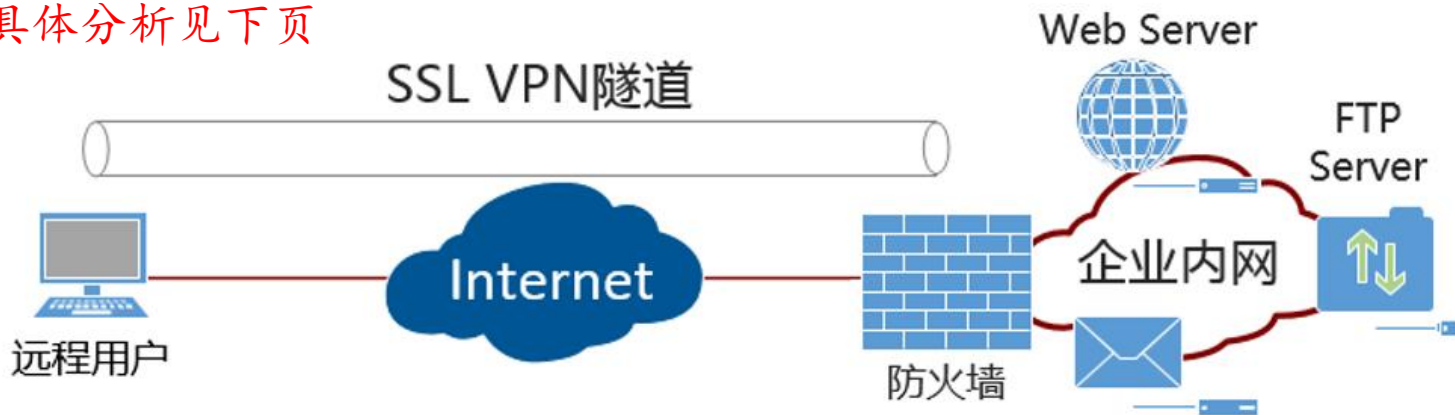
## □ 认识SSL VPN

- SSL VPN是以SSL（Secure Sockets Layer，一种为网络通信提供安全及数据完整性的安全协议）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；
- SSL VPN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）

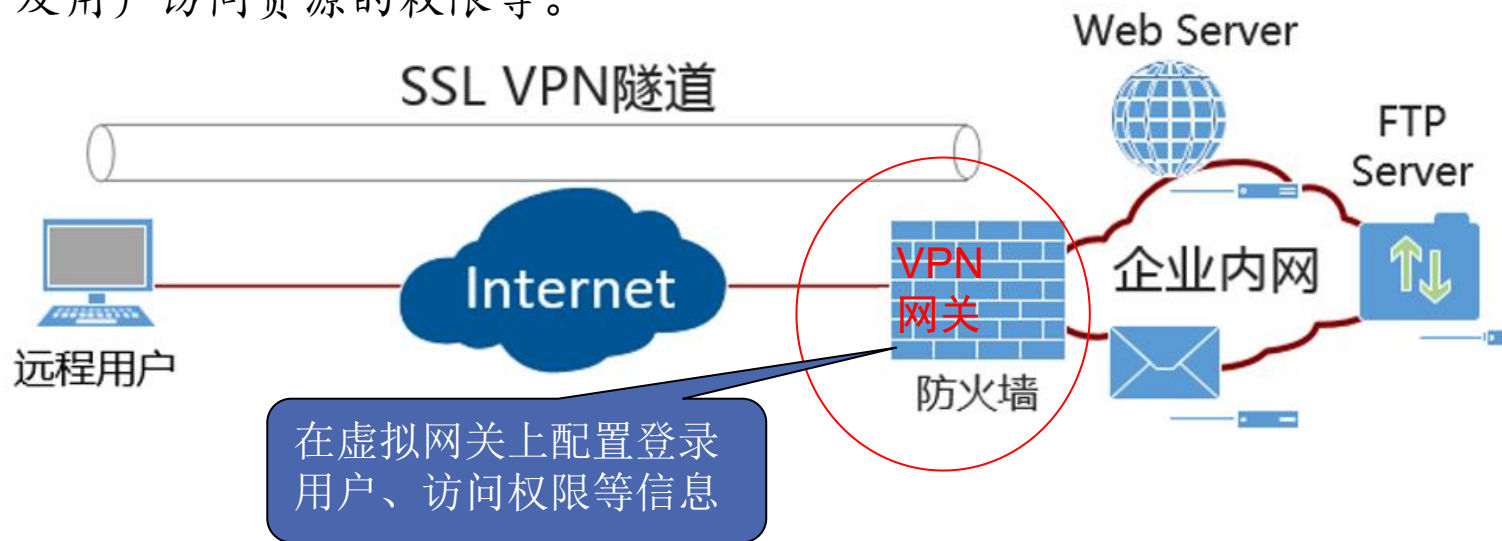
- **例：**防火墙作为企业出口网关连接至Internet，并向远程用户提供SSL VPN接入服务。远程用户可以使用移动终端（如便携机、PAD或智能手机）随时随地登录防火墙上的SSL VPN网关，进而接入到企业内网，访问企业内网资源。
- 具体分析见下页



# 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）

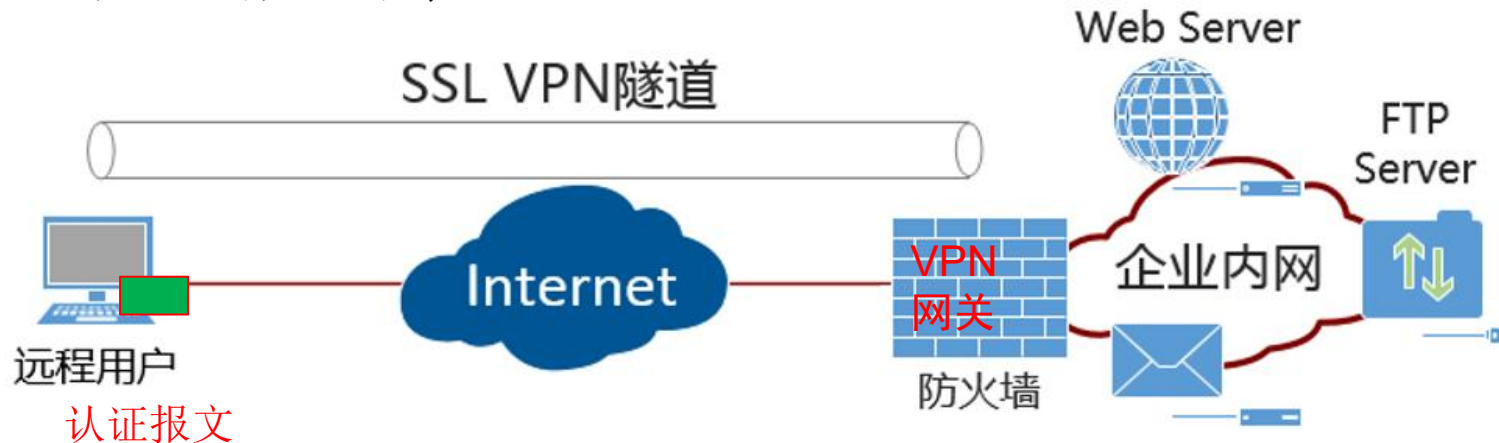
- 防火墙向远程用户提供SSL VPN接入服务的功能模块称为**VPN虚拟网关**，虚拟网关有独立的IP地址。网络管理员可以在虚拟网关上配置登录用户、资源以及用户访问资源的权限等。



# 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）

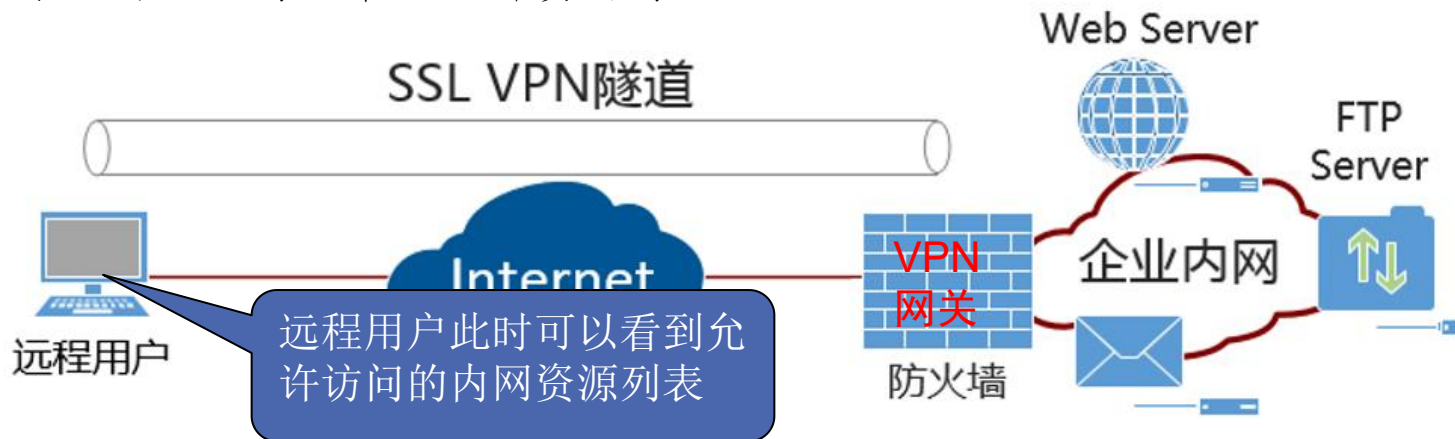
- 虚拟网关是远程用户访问企业内网资源的统一入口。远程用户在Web浏览器中输入虚拟网关的IP地址，并在虚拟网关登录界面输入用户名和密码，虚拟网关将会对用户进行身份认证。



# 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（管理员允许）访问的内网资源列表，且列表中只能看到管理员为其开通的业务资源，例如为远程用户A开通了Web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。

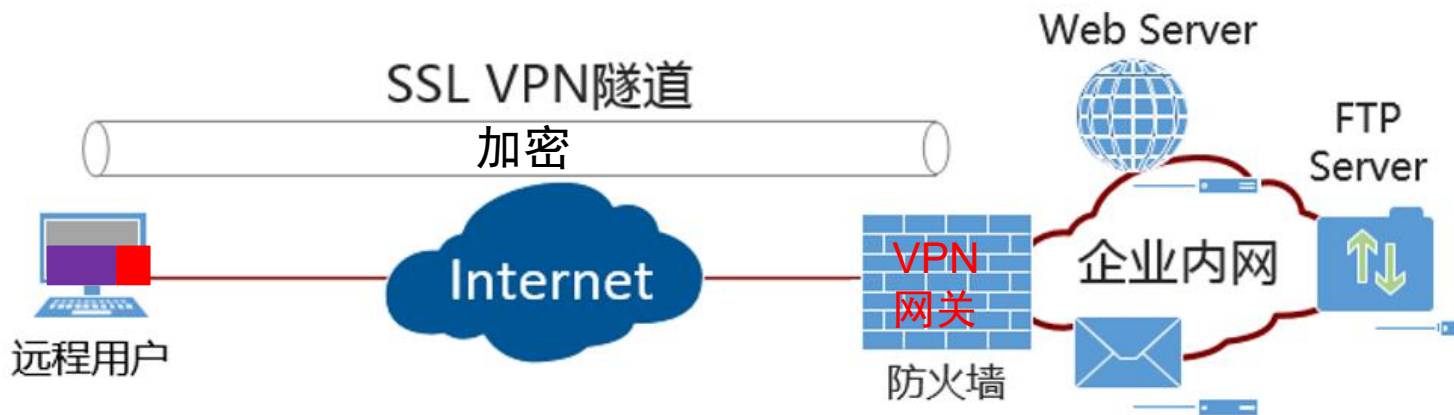


# SSL VPN的应用

## □ 远程用户通过SSL VPN访问企业内部资源的基本过程（5）

■ **接下来**，远程用户即可通过安全方式访问内网资源。注意，此时：

- 远程用户——VPN网关之间，重新封装、加密、隧道安全通信；
- VPN网关—— Web Server之间，解封装、普通内网通信，不加密。

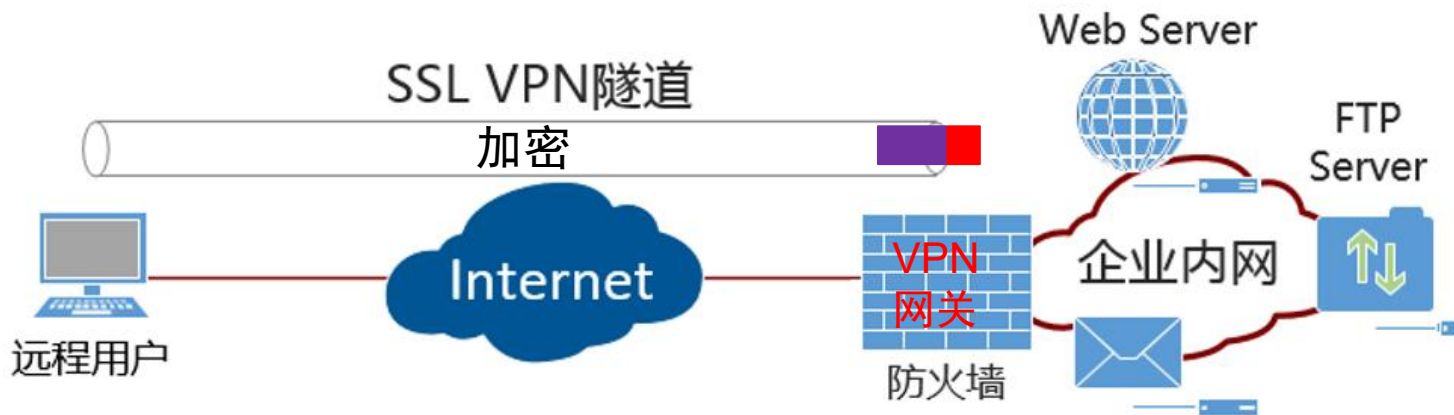


# SSL VPN的应用

## □ 远程用户通过SSL VPN访问企业内部资源的基本过程（5）

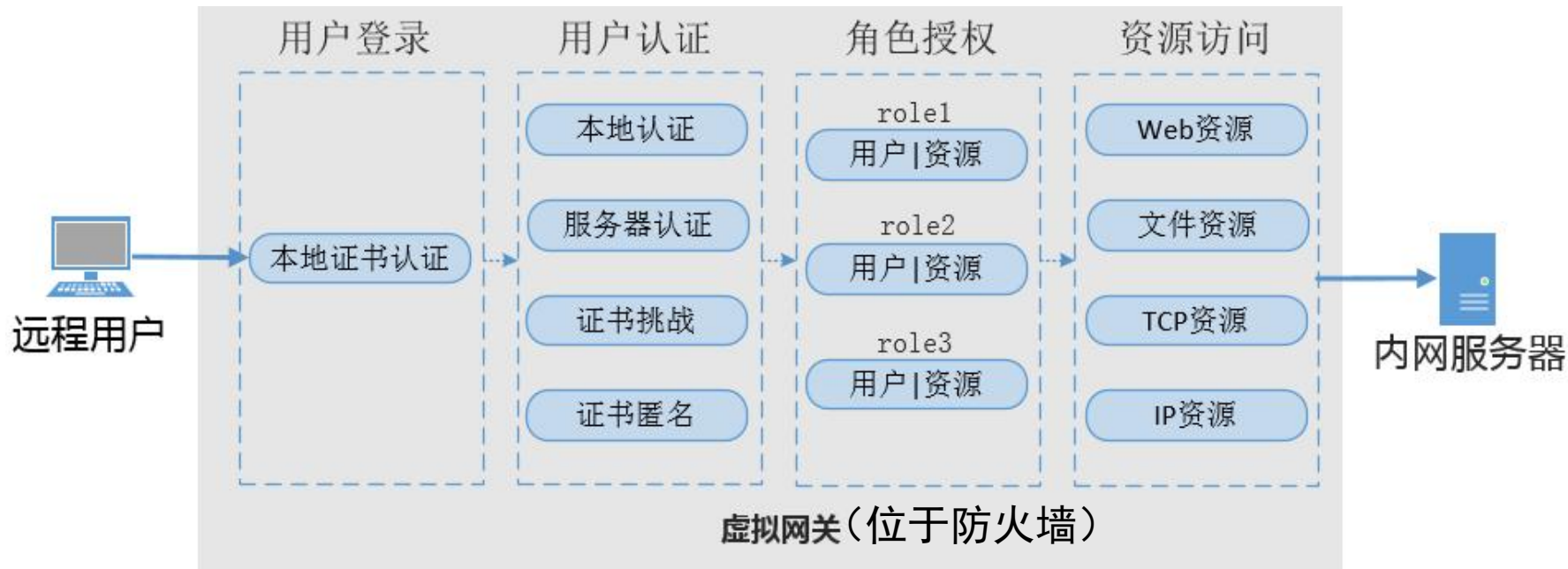
■ **接下来**，远程用户即可通过安全方式访问内网资源。注意，此时：

- 远程用户——VPN网关之间，重新封装、加密、隧道安全通信；
- VPN网关—— Web Server之间，解封装、普通内网通信，不加密。



# 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（总结）**



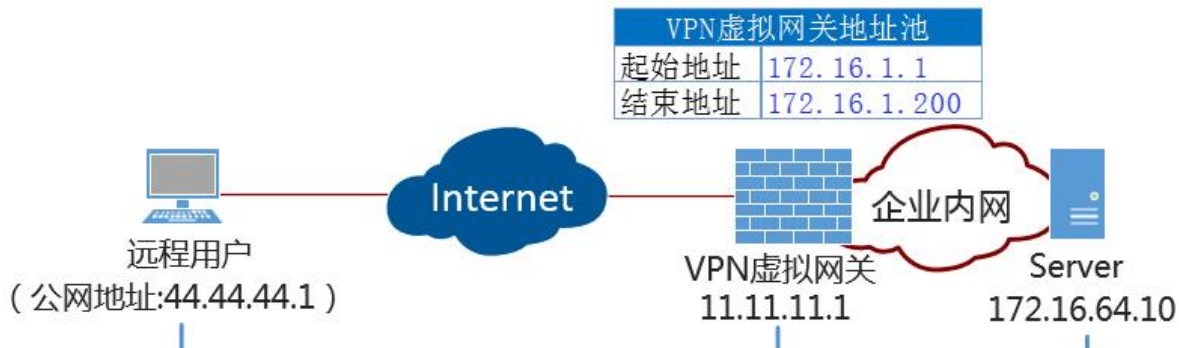
# SSL VPN工作流程

## □ 远程用户通过SSL VPN访问企业内网资源的**总体流程**（总结）

- **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

### 三、SSL VPN案例分析

## 案例1：SSL VPN应用

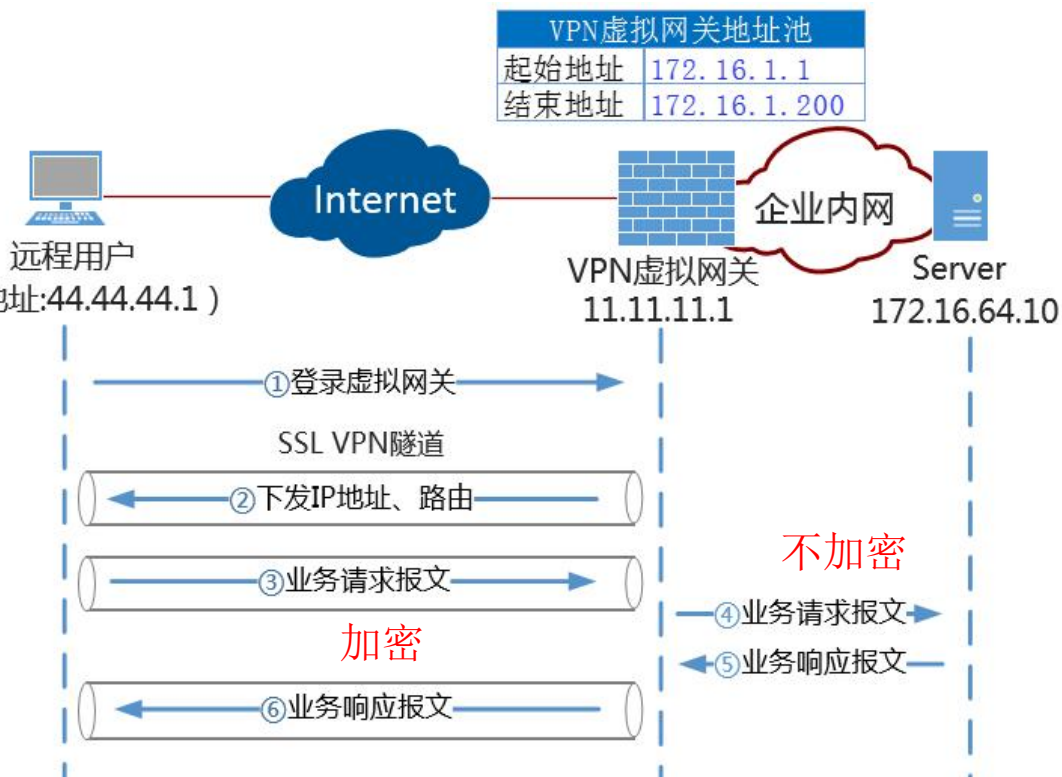


## ➤ 案例1：SSL VPN应用

- 企业内网在边界防火墙上配置SSL VPN虚拟网关，使得互联网上的远程用户可以通过SSL VPN方式，安全访问内网资源。

- 具体过程如右图

- 具体过程分析如下页

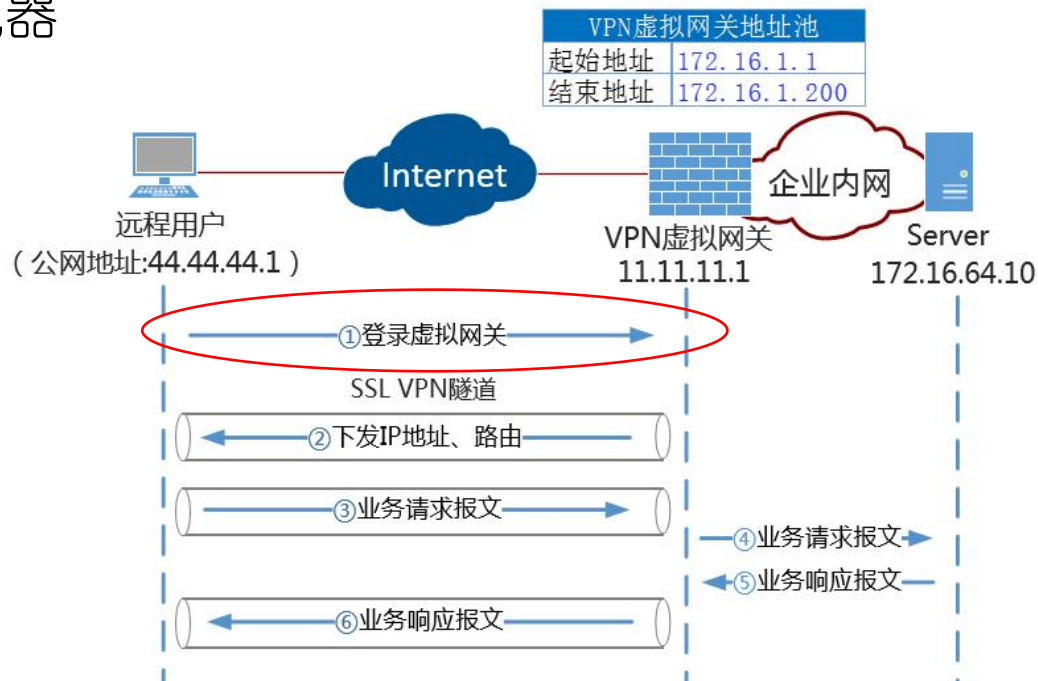


## ➤ 案例1：SSL VPN应用

### □ 步骤1：远程用户通过Web浏览器登录VPN虚拟网关

#### ■ 报文首部的IP地址？

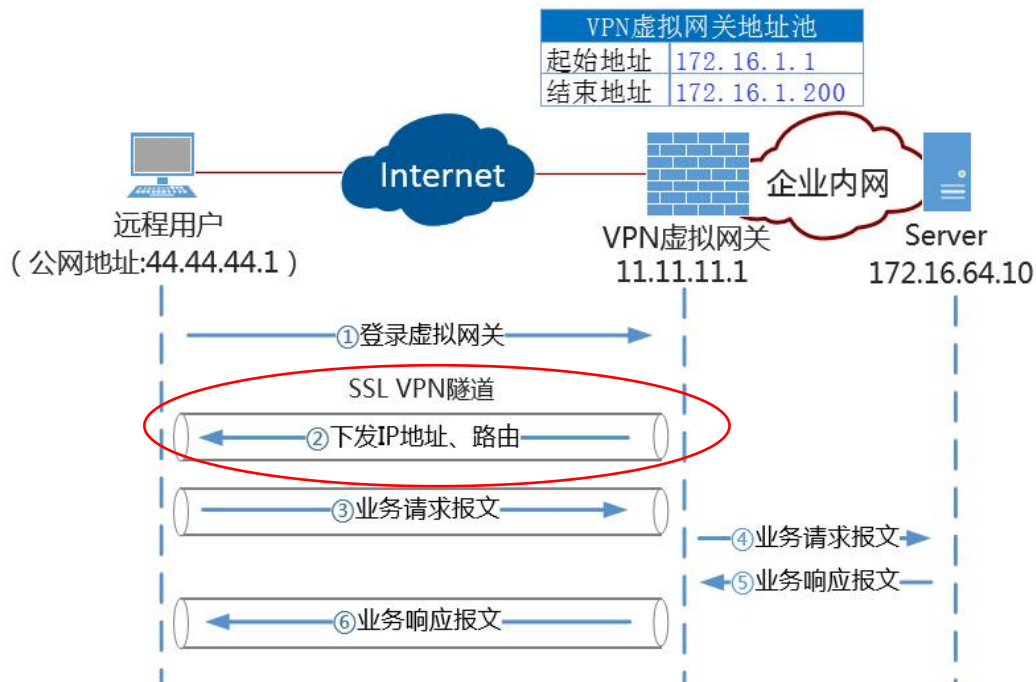
- 源IP： 44.44.44.1
- 目的IP： 11.11.11.1



## ➤ 案例1：SSL VPN应用

### □ 步骤2：认证成功，会触发以下动作

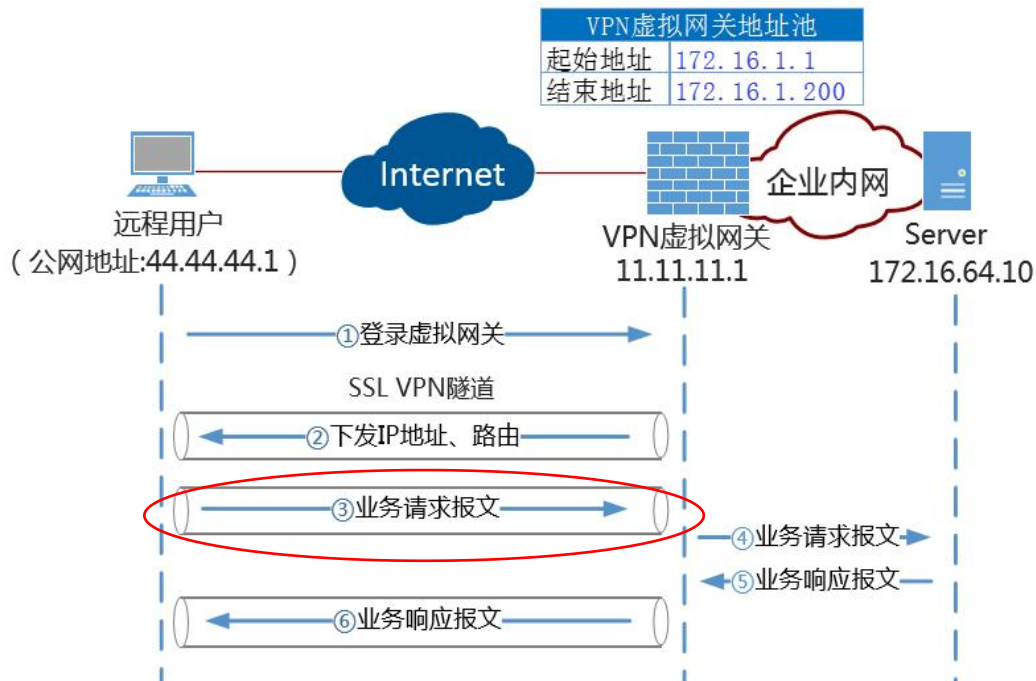
- ① 远程用户自动生成一个虚拟网卡。防火墙的虚拟网关从地址池选择一个IP地址（例172.16.1.1），分配给远程用户的虚拟网卡。该地址作为远程用户与企业内网Server之间通信之用。有了该私网IP地址，远程用户就如同企业内网用户一样可以方便访问内网IP资源；
- ② VPN虚拟网关向远程用户下发到达企业内网Server的路由信息。



## ➤ 案例1：SSL VPN应用

### □ 步骤3：远程用户发出业务请求报文

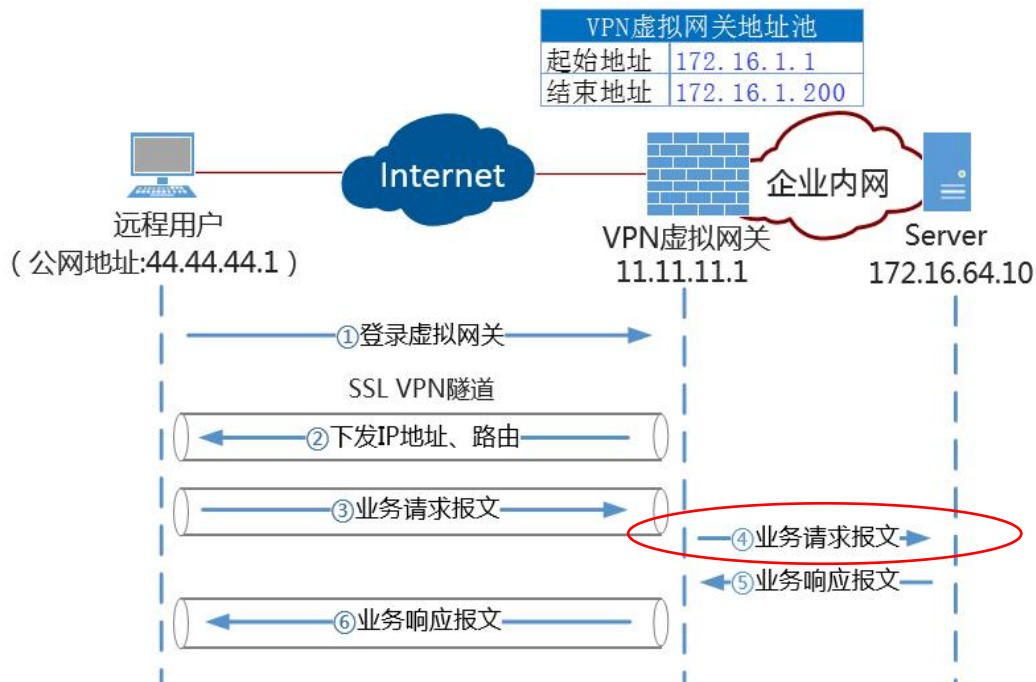
- 远程用户使用获得的内网地址向企业内网的Server发送业务请求报文，即源IP是172.16.1.1，目的IP是172.16.64.10
- 上述报文会被加密并重新封装，封装后的报文首部源IP是44.44.44.1，目的IP是11.11.11.1
- 该报文被加密并重新封装，如同在一条专用隧道中传输，最后到达VPN虚拟网关。



## ➤ 案例1：SSL VPN应用

### □ 步骤4：虚拟网关转发业务请求报文至内网服务器

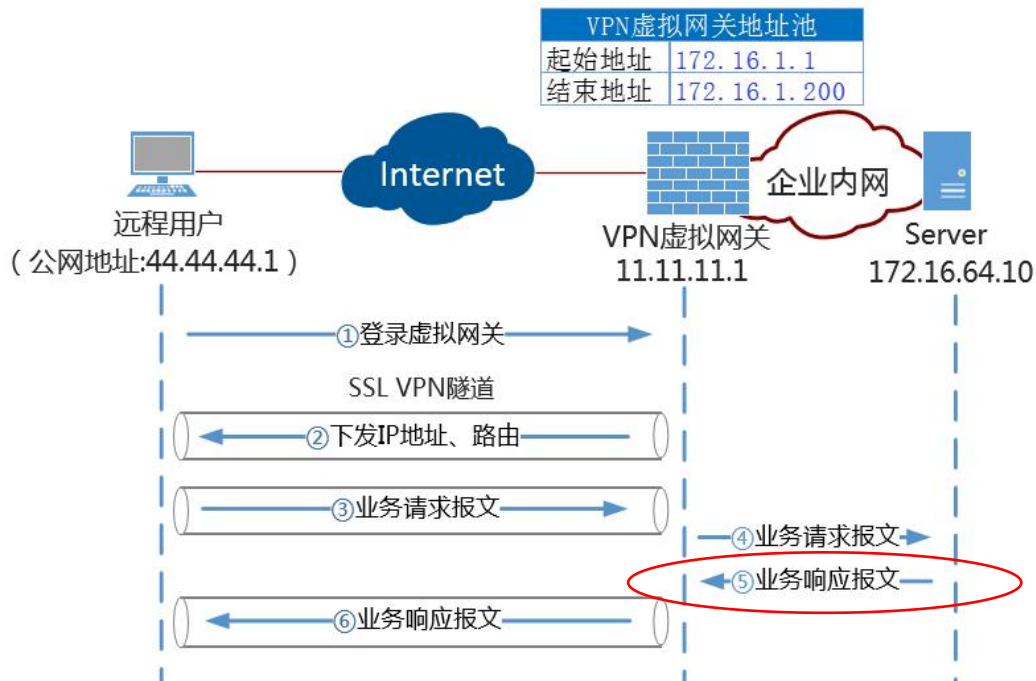
- 虚拟网关对收到的报文进行解封装，并将解封装后的原始业务请求报文（首部地址中源IP是172.16.1.1，目的IP是172.16.64.10）发送给内网Server。
- 思考：如何路由可达？
- 注意，此时报文是不加密的！



## ➤ 案例1：SSL VPN应用

### □ 步骤5：内网Server响应远程用户的业务请求

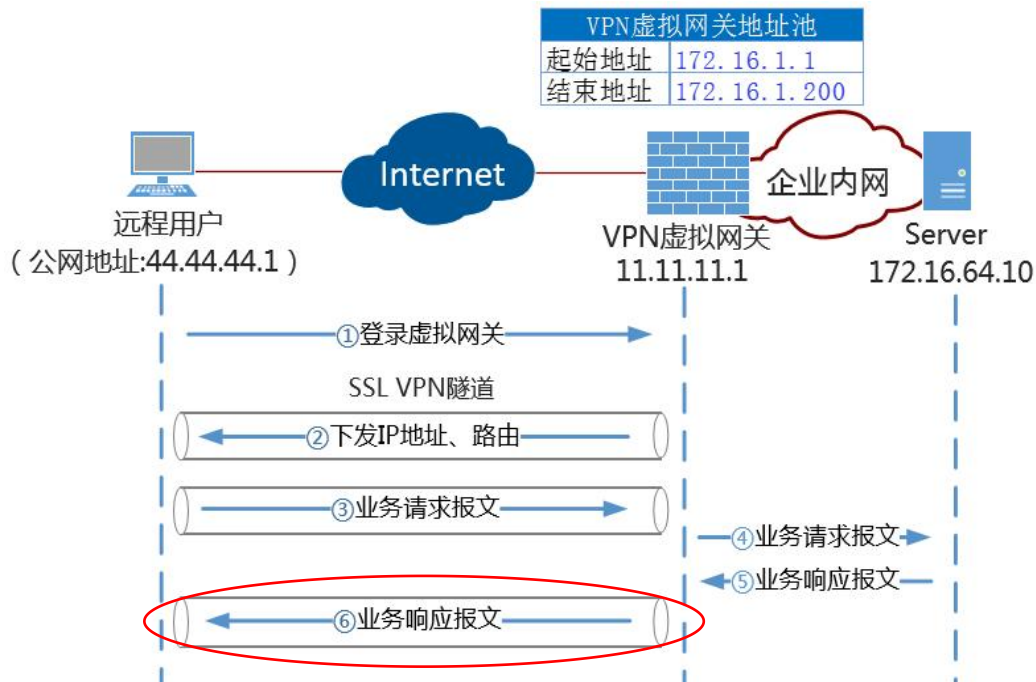
- 内网Server响应远程用户的业务请求报文。该报文是不加密的。
- 首部地址中源IP是172.16.64.10, 目的IP是172.16.1.1
- 该报文会先到VPN虚拟网关。



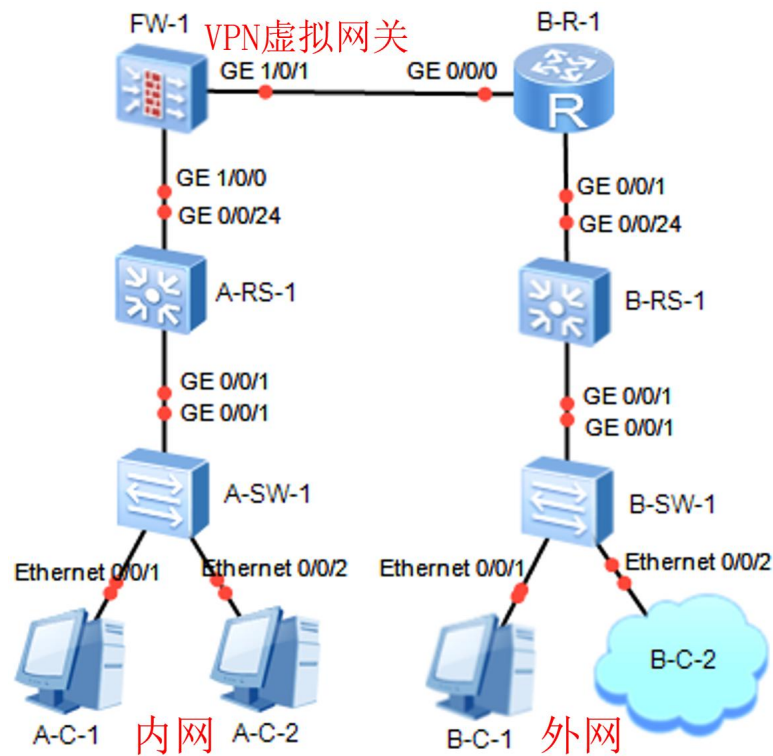
## ➤ 案例1：SSL VPN应用

### □ 步骤6：虚拟网关转发业务响应报文给远程用户

- 此处VPN虚拟网关对收到的业务响应报文进行加密，并重新封装。
- 封装后的报文首部源IP是11.11.11.1，目的IP是44.44.44.1
- 该报文被加密并重新封装，如同在一条专用隧道中传输，最后到达远程用户。
- 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



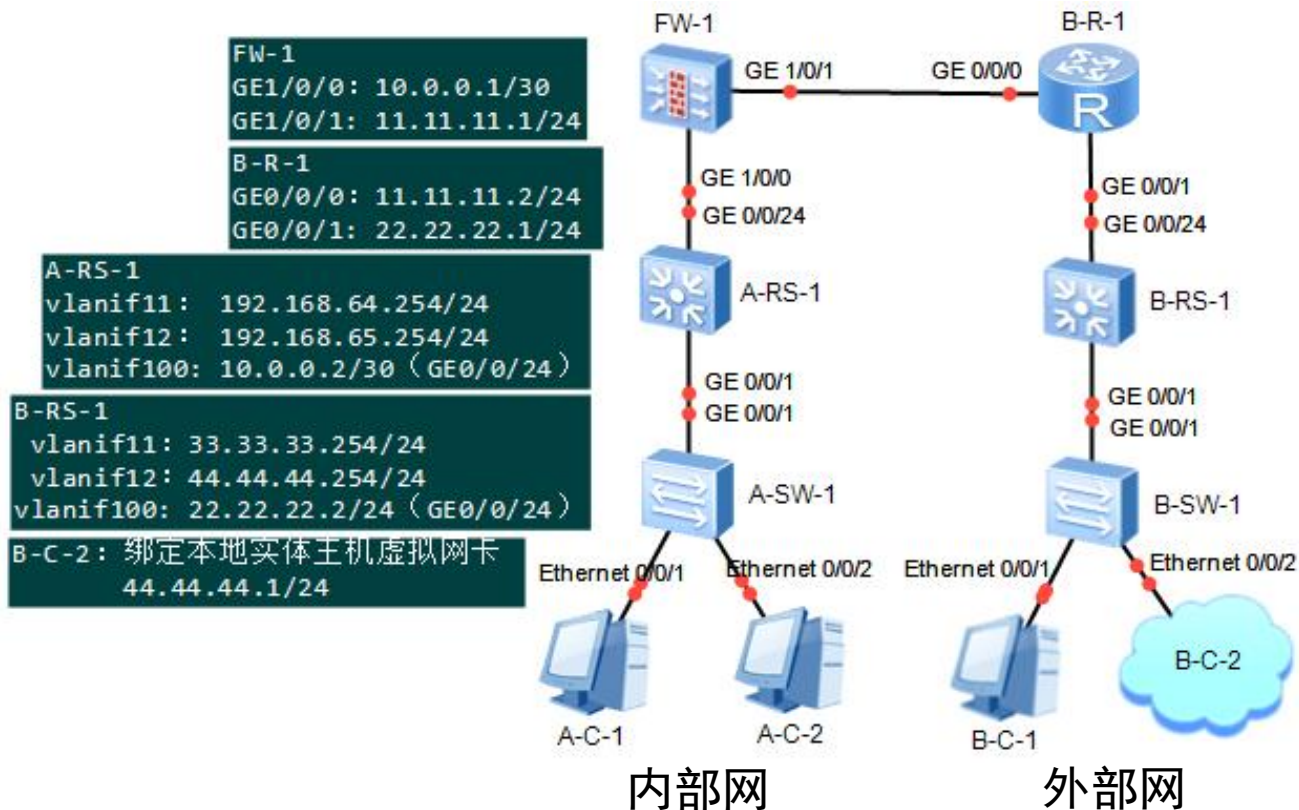
## 案例2：SSL VPN应用



## 案例2:

### ▣ 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2:

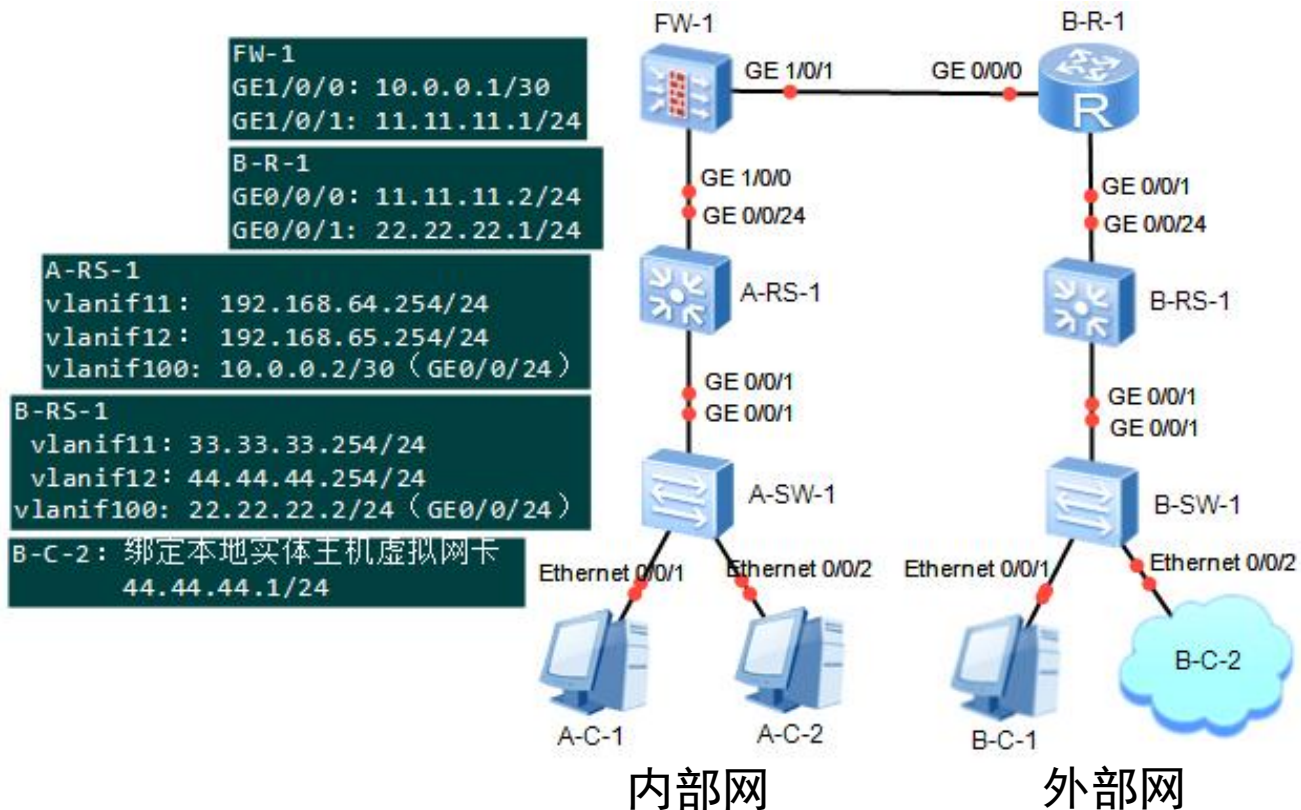
### □ IP分析

### □ 内部网

- 192.168.64.0/23

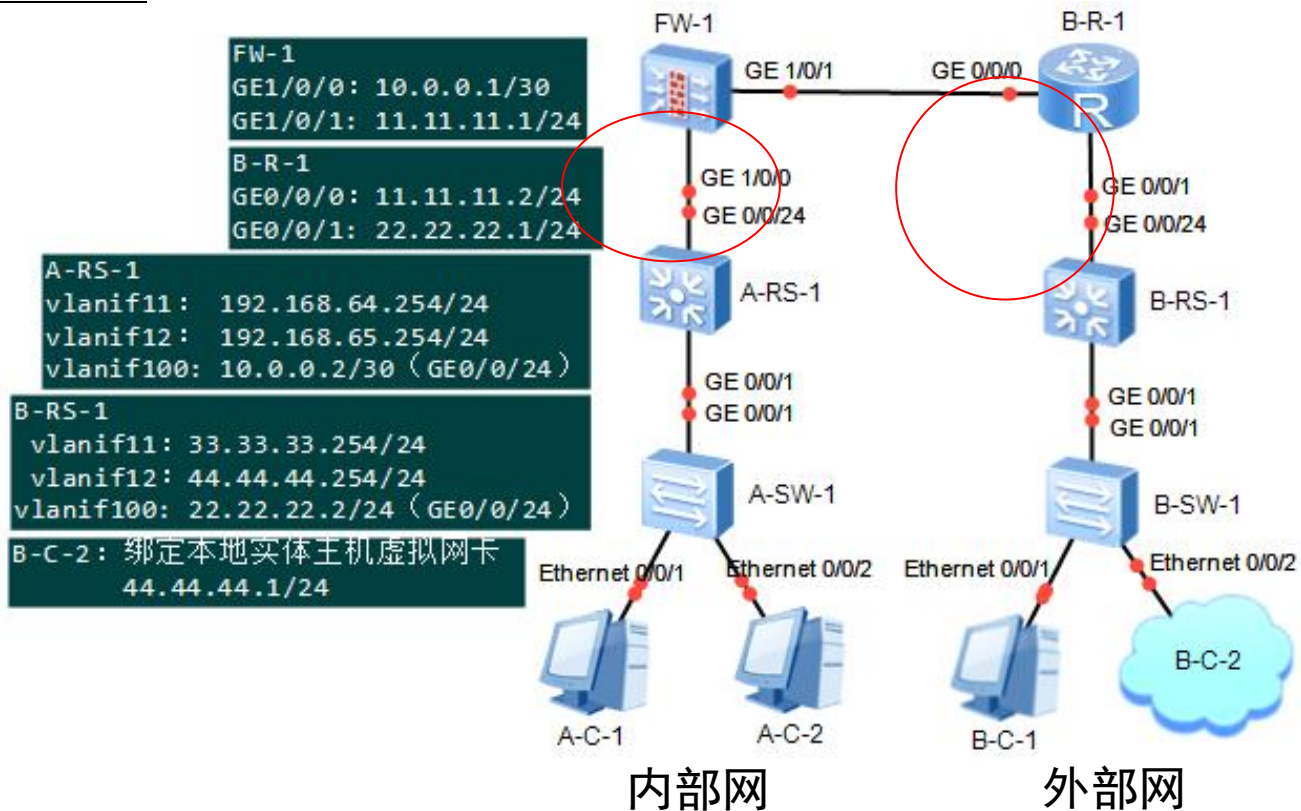
### □ 外部网

- 11.11.11.0/24
- 22.22.22.0/24
- 33.33.33.0/24
- 44.44.44.0/24



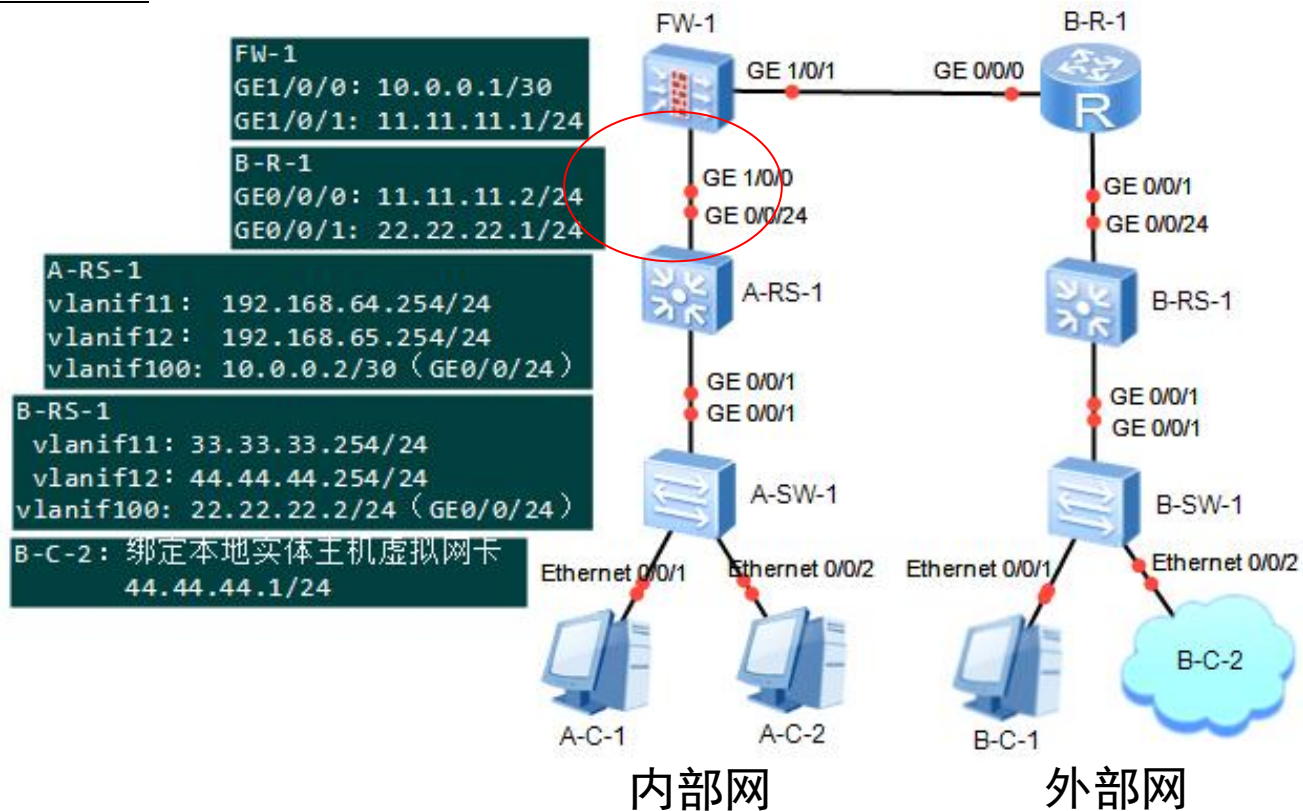
## 案例2:

- 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2:

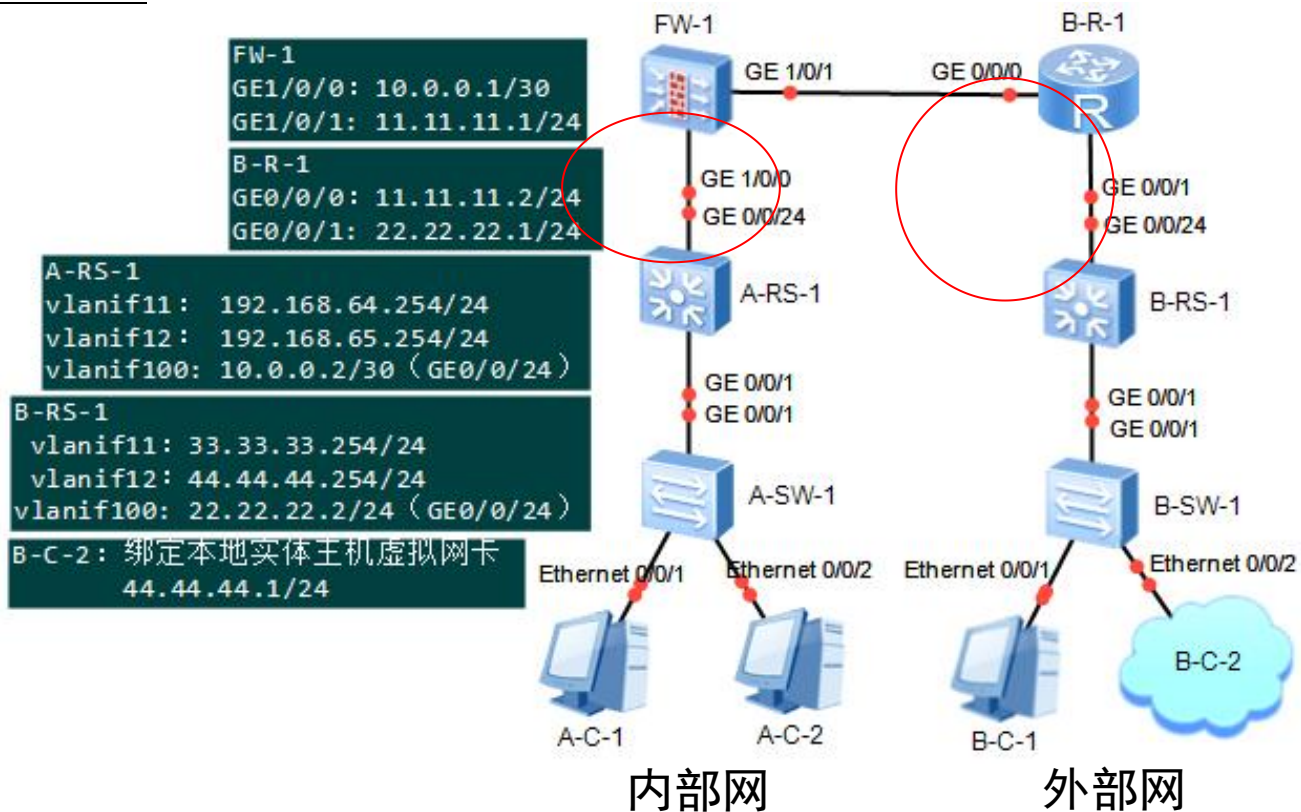
### □ 步骤1: 实现内部网通信



## 案例2:

### □ 步骤2: 实现外部网通信

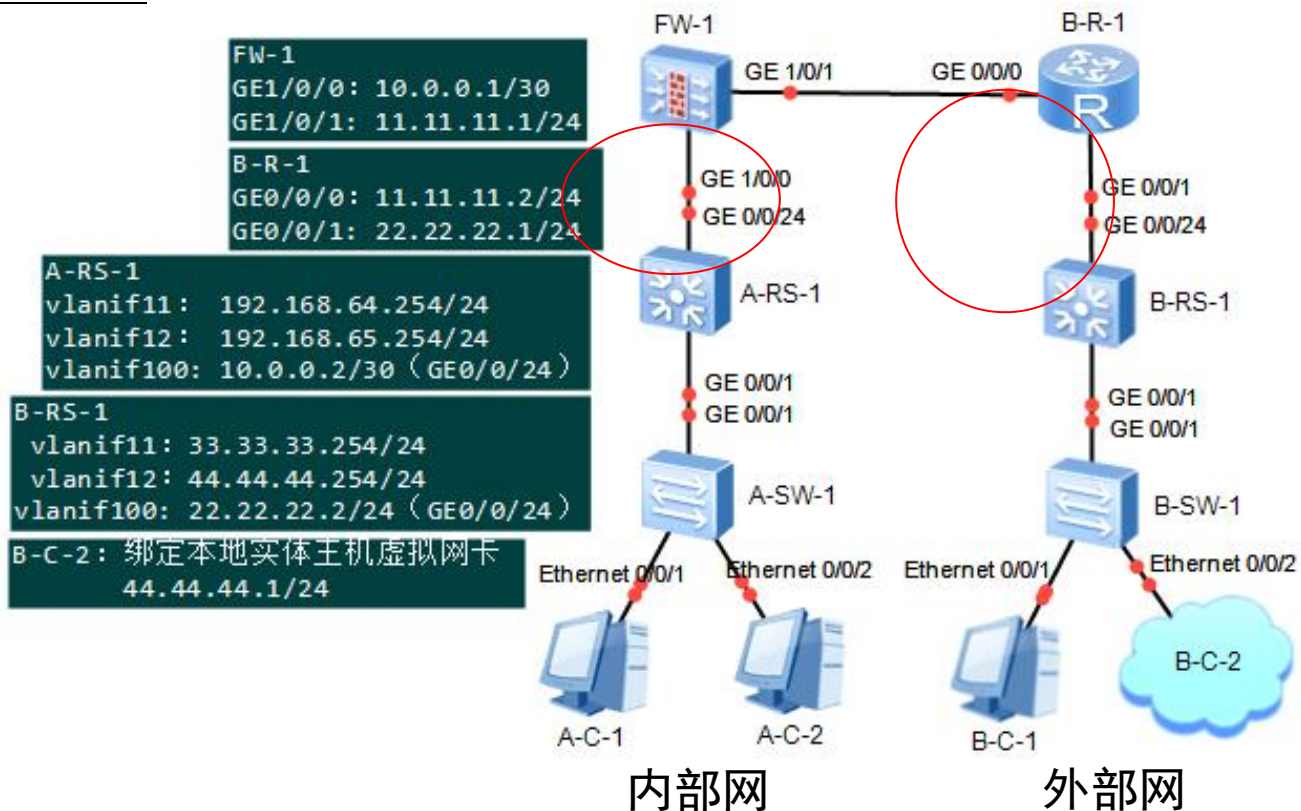
- B-C-1能否ping通FW-1的GE1/0/1口?



## 案例2:

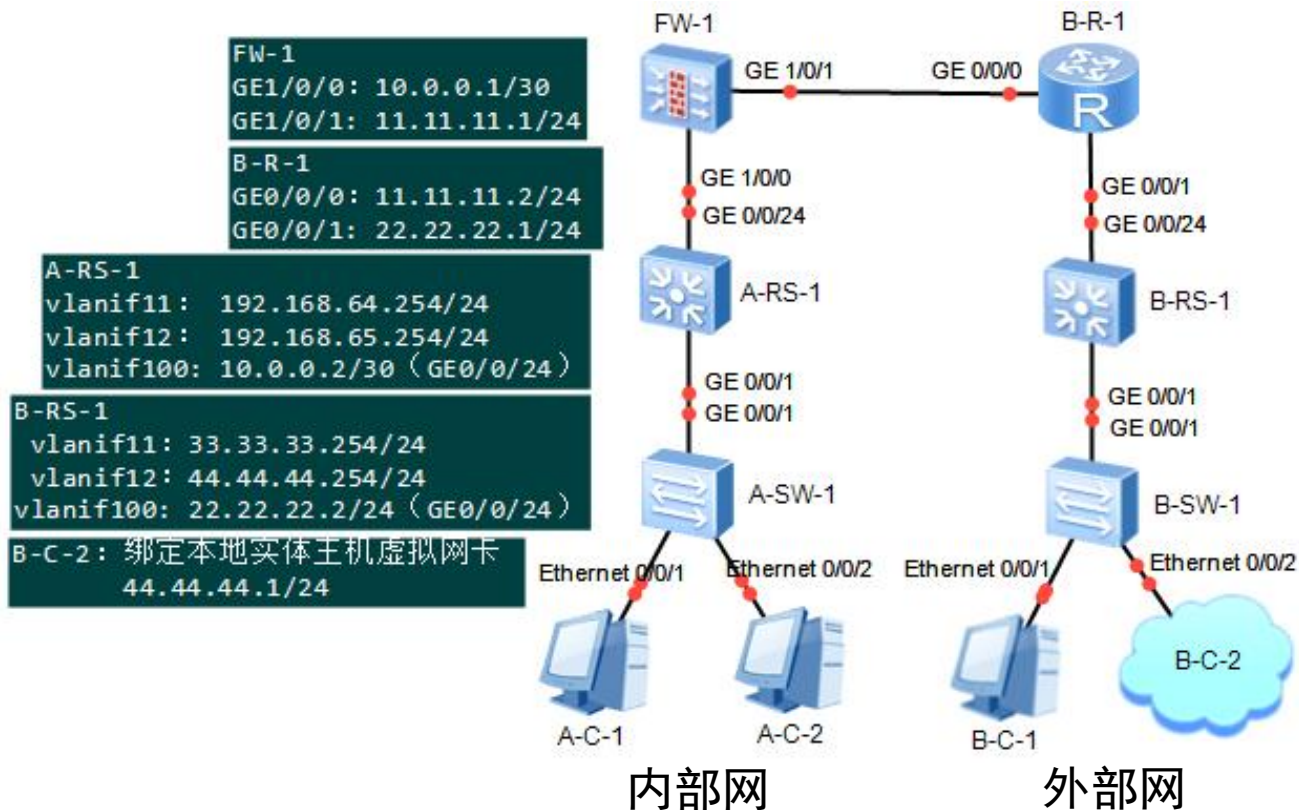
### □ 步骤3: 内部网用户NAT访问外部网

- FW-1中的缺省路由
- Default-route-advertise always//在ospf中引入缺省路由



## 案例2:

- 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2:

### □ 步骤5: 外网用户登录认证

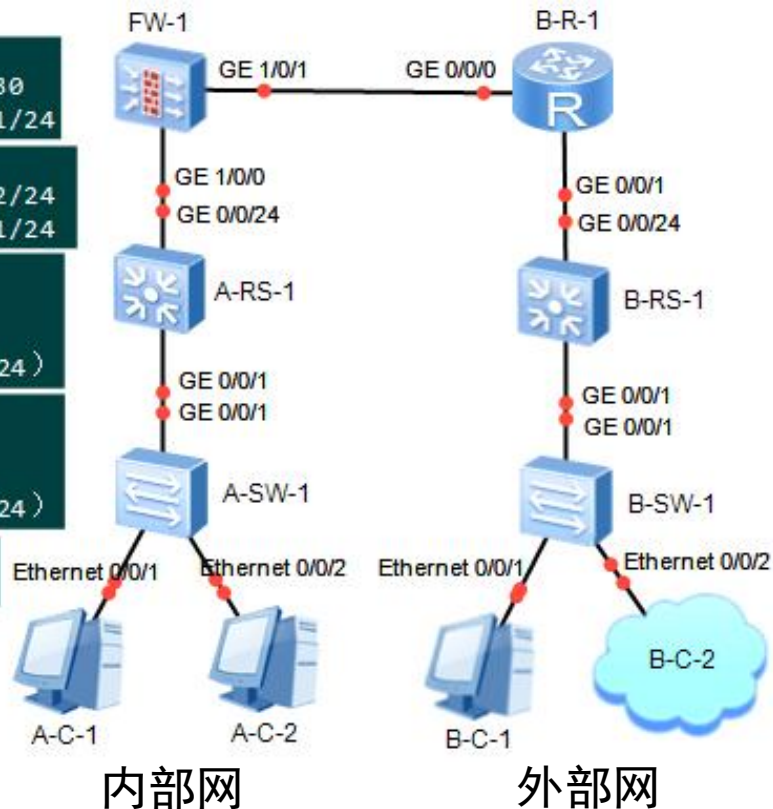
```
FW-1
GE1/0/0: 10.0.0.1/30
GE1/0/1: 11.11.11.1/24
```

```
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2:

## □ 步骤5: 外网用户登录认证

```
C:\Windows\system32>ipconfig

Windows IP 配置

以太网适配器 本地连接 2:

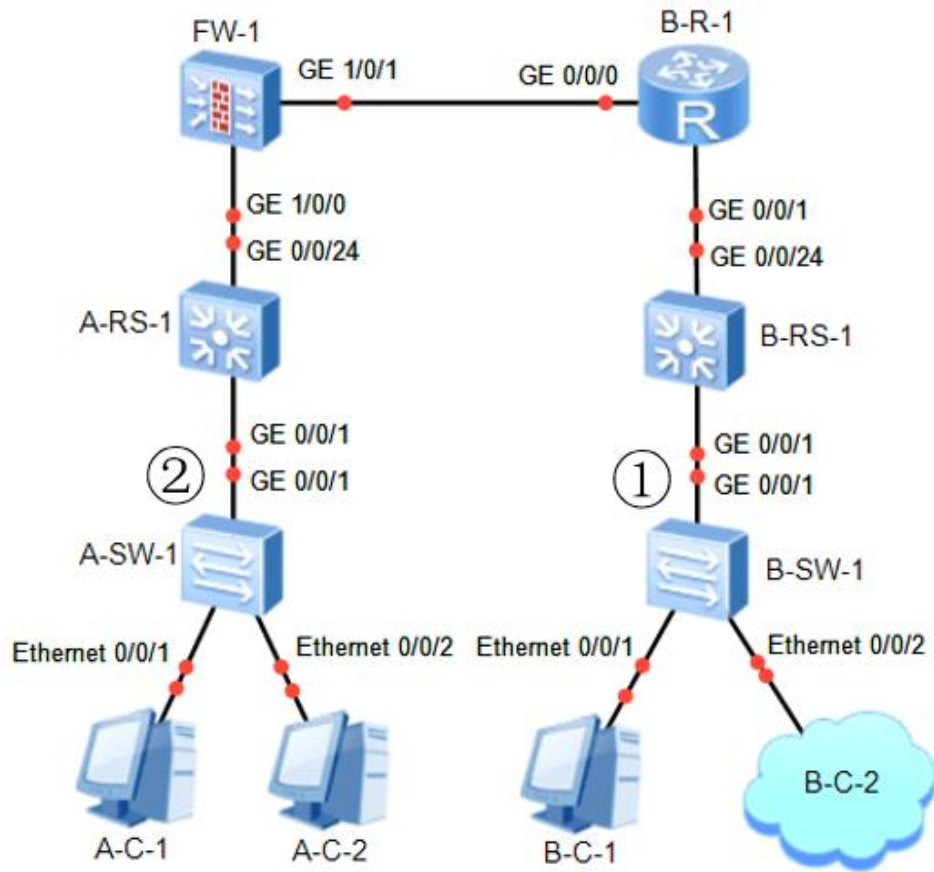
    连接特定的 DNS 后缀 . . . . . : 
    本地链接 IPv6 地址 . . . . . : fe80::a0b0:91b4:a6
    IPv4 地址 . . . . . : 172.16.1.1
    子网掩码 . . . . . : 255.255.255.255
    默认网关 . . . . . :
```



## 案例2:

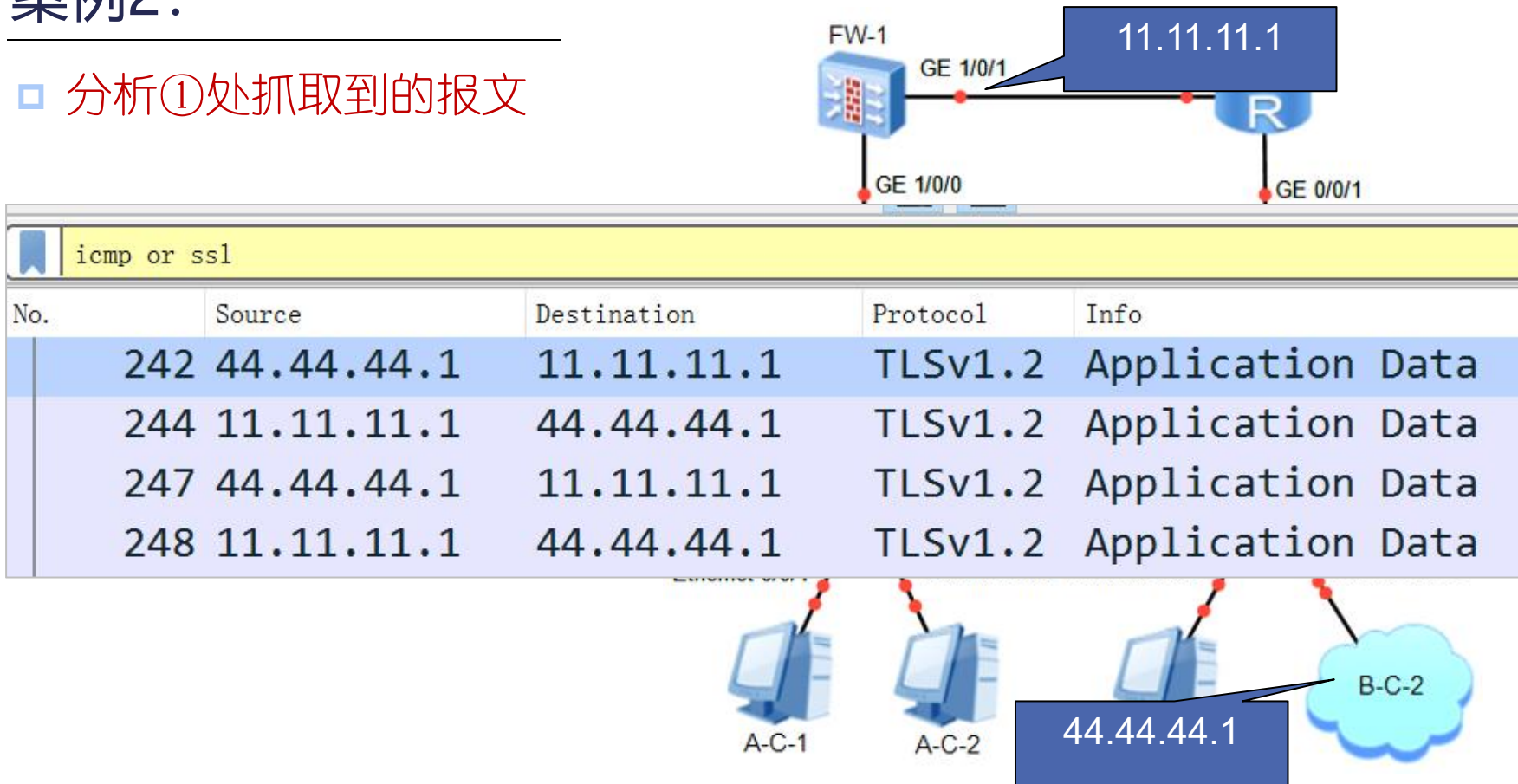
### □ 步骤6: 外网用户访问内网服务器

- 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2:

### □ 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）。

| 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。

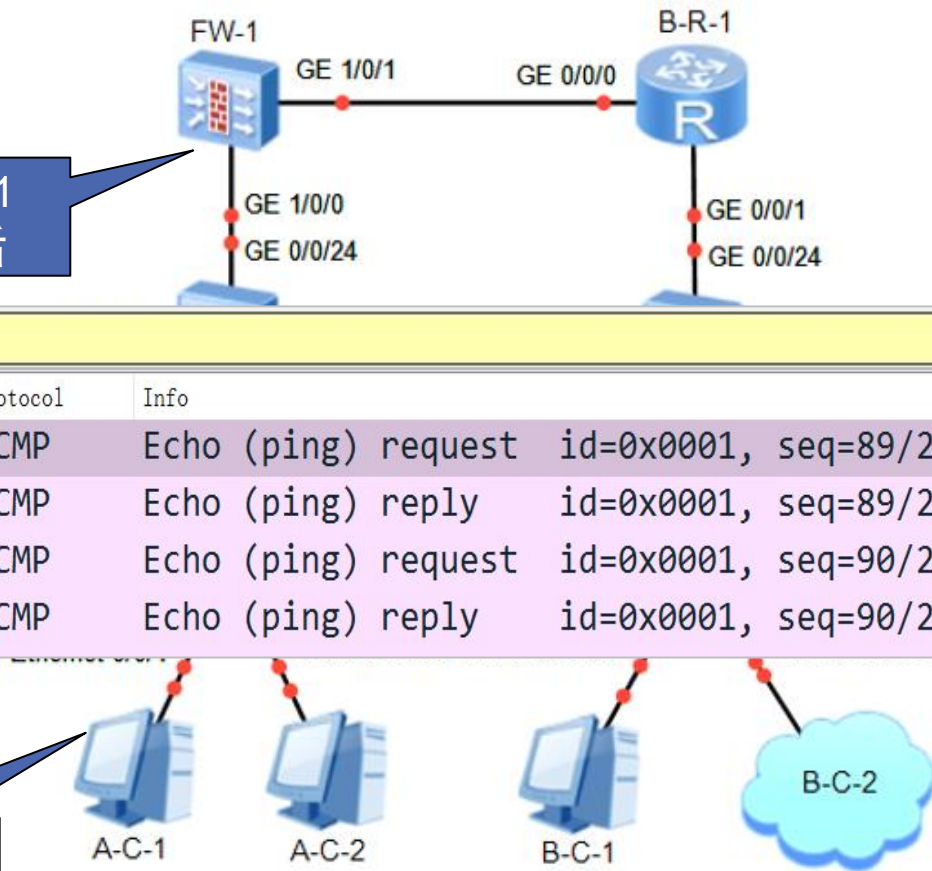
## 案例2:

### 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: 6162636465666768696a6b6c6d6e6f707172737475767761...
  [Length: 32]
```



**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，

# 第12讲 VPN实现安全通信

## (完)