信息系统安全

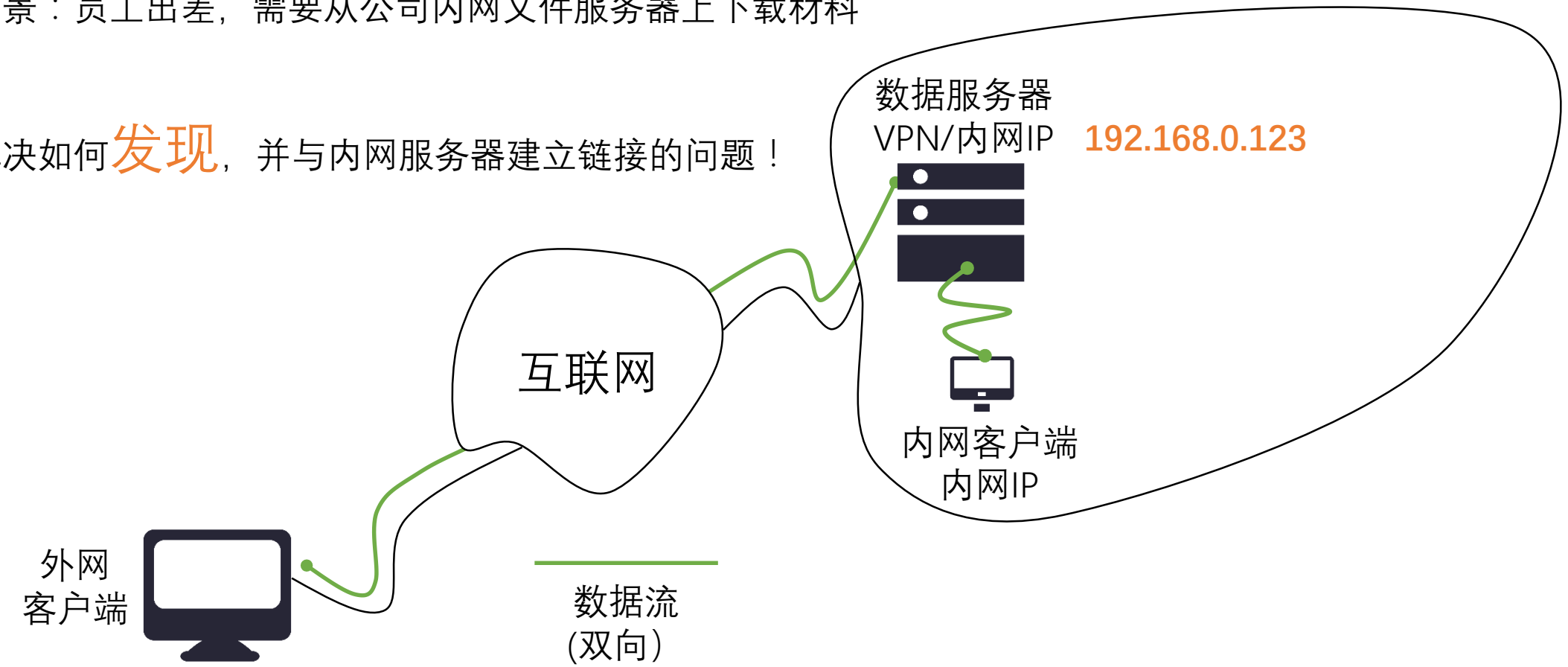
实验 4 虚拟局域网与反向代理技术

School of Software Engineering
South China University of Technology
Dr. Chunhua Chen
chunhuachen@scut.edu.cn
2016 Spring

问题-背景

运用网络与安全技术解决一个实际的问题

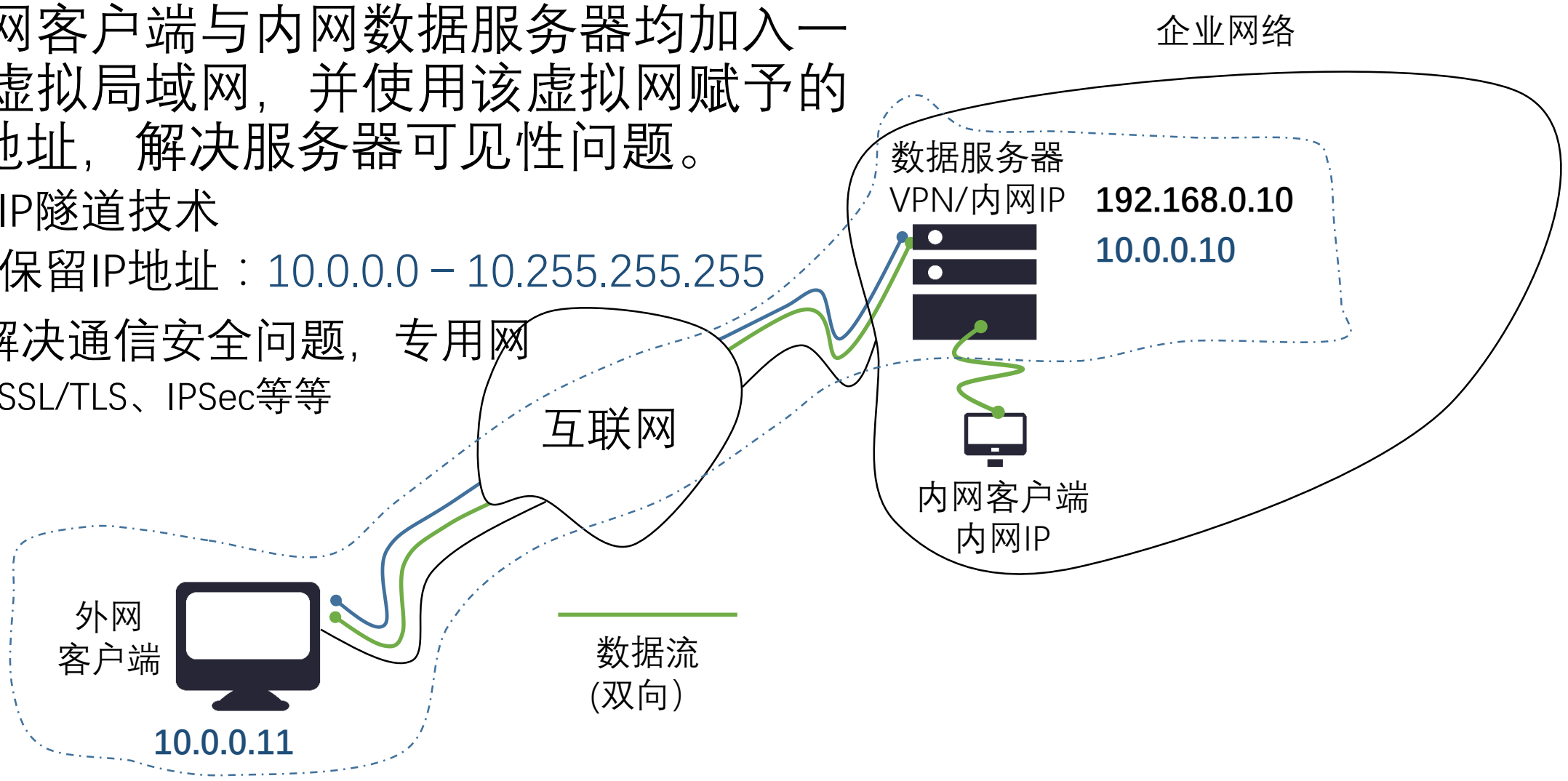
- 外网客户端如何使用企业内部网络的服务，比如下载文件等等
  - 场景：员工出差，需要从公司内网文件服务器上下载材料
- 需要解决如何发现，并与内网服务器建立链接的问题！



方案: 企业虚拟专用网 (Virtual Private Network)

在IP网络上构建虚拟专用网络 (VPN): 虚拟局域网(Virtual Local Area Network, VLAN)+安全信道

- 外网客户端与内网数据服务器均加入一个虚拟局域网，并使用该虚拟网赋予的IP地址，解决服务器可见性问题。
  - IP隧道技术
  - 保留IP地址：10.0.0.0 – 10.255.255.255
- 还解决通信安全问题，专用网
  - SSL/TLS、IPSec等等

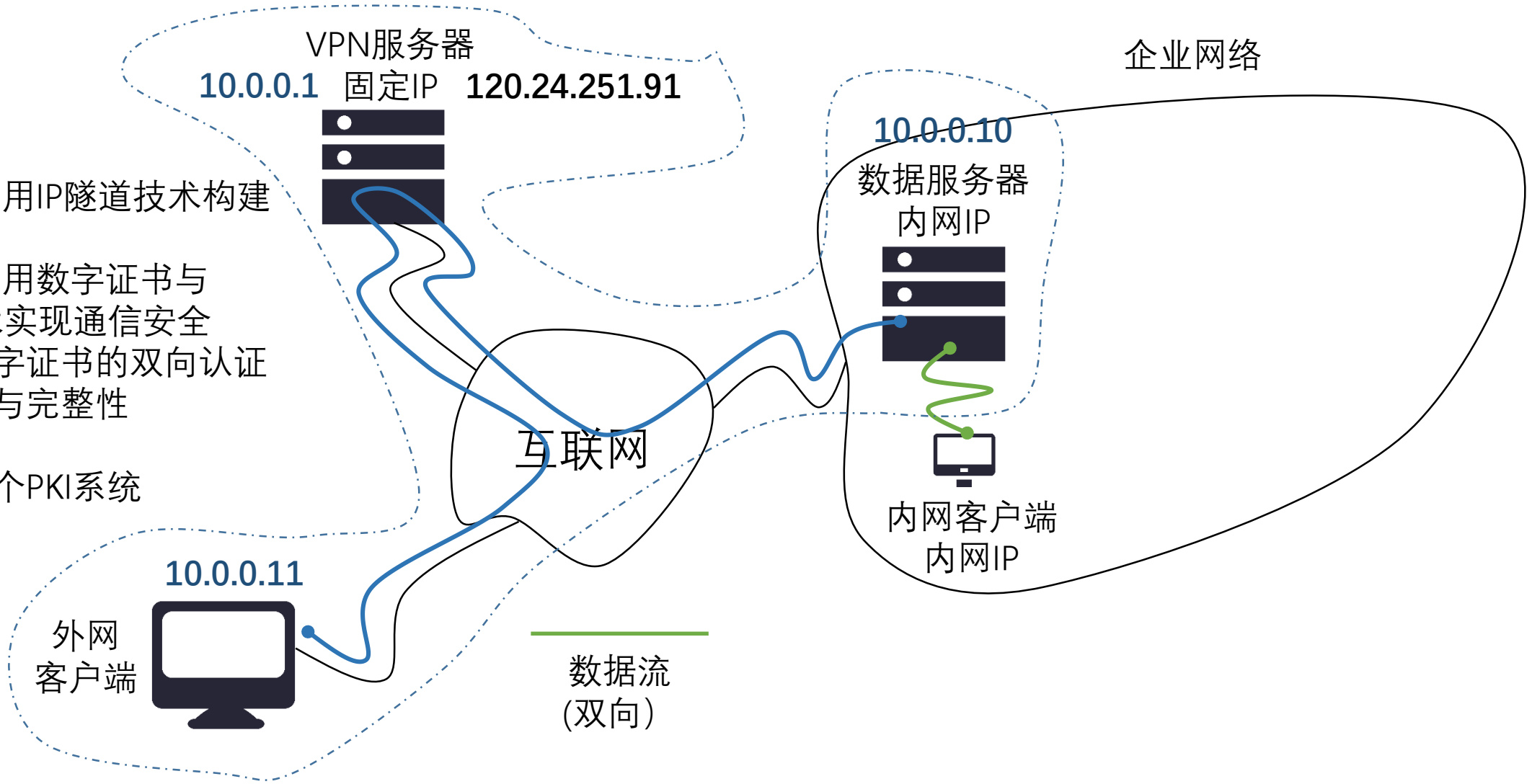


使用OpenVPN来构建VPN

OpenVPN是开源的, 但是 www.openvpn.net 需要翻墙访问

- OpenVPN使用IP隧道技术构建VLAN
- OpenVPN使用数字证书与SSL/TLS技术实现通信安全
  - 基于数字证书的双向认证
  - 保密性与完整性

- 必须构建一个PKI系统



步骤1 为OpenVPN构建一个PKI系统

安全的基石: 数字证书与PKI使用公钥密码学，回忆SSL/TLS协议吧

- 创建CA, 公私钥对与数字证书 （1）
- 创建OpenVPN服务器的公私钥对与数字证书（1）
- 为客户端创建公私钥对与数字证书 （N）
  - 2份，外网客户端与内网服务器

- 在后续部署虚拟局域网网络时，使用这些秘钥与证书，实现通信安全，即专用网络。

- **工具: EasyRSA2 (https://github.com/OpenVPN/easy-rsa)**

步骤 2 创建OpenVPN服务器

- 部署 OpenVPN 服务器
  - 使用自己的阿里云服务器，参加文档使用CentOS 7 操作系统
- 1. 规划IP使用(10.0.0.*/24, OpenVPN服务器默认使用10.0.0.1)
- 2. 配置OpenVPN配置文件
  - 使用CA公钥证书，服务器公私钥与数字证书
- 3. 启动OpenVPN服务器

- 工具: OpenVPN 服务器端程序
  - https://github.com/OpenVPN

步骤 3 创建OpenVPN客户端

外网客户端，内网服务器

- 1. 配置OpenVPN客户端配置文件
  - 使用CA公钥证书，客户端公私钥与数字证书
- 2. 启动OpenVPN客户端
  - 向OpenVPN服务器注册信息该客户端的网络信息，包括建立并维持一个长链接，作为后续通信的通道
  - OpenVPN服务器给客户端分配VLAN网络配置，IP等

- 工具: OpenVPN 客户端程序
  - https://github.com/OpenVPN

步骤4 测试连通状态

Ping: ICMP 服务(注意打开)

- OpenVPN服务器10.0.0.1，ping从客户端10.0.0.11
- OpenVPN服务器10.0.0.1，数据服务器10.0.0.10
- 从客户端10.0.0.11，ping OpenVPN服务器10.0.0.1
- 从客户端10.0.0.11，ping 数据服务器10.0.0.10
- 从数据服务器10.0.0.10，ping OpenVPN服务器10.0.0.1
- 从数据服务器10.0.0.10，ping 客户端10.0.0.11

- 在数据服务器10.0.0.10中启动Tomcat 7,提供Web服务，然后从客户端10.0.0.11访问Tomcat管理系统
  - http:// 10.0.0.10:8080

其他

- OpenVPN安装后，在其文件夹中有服务器端配置文件与客户端配置文件的模板
  - /usr/share/doc/openvpn-*/sample/sample-config-files/

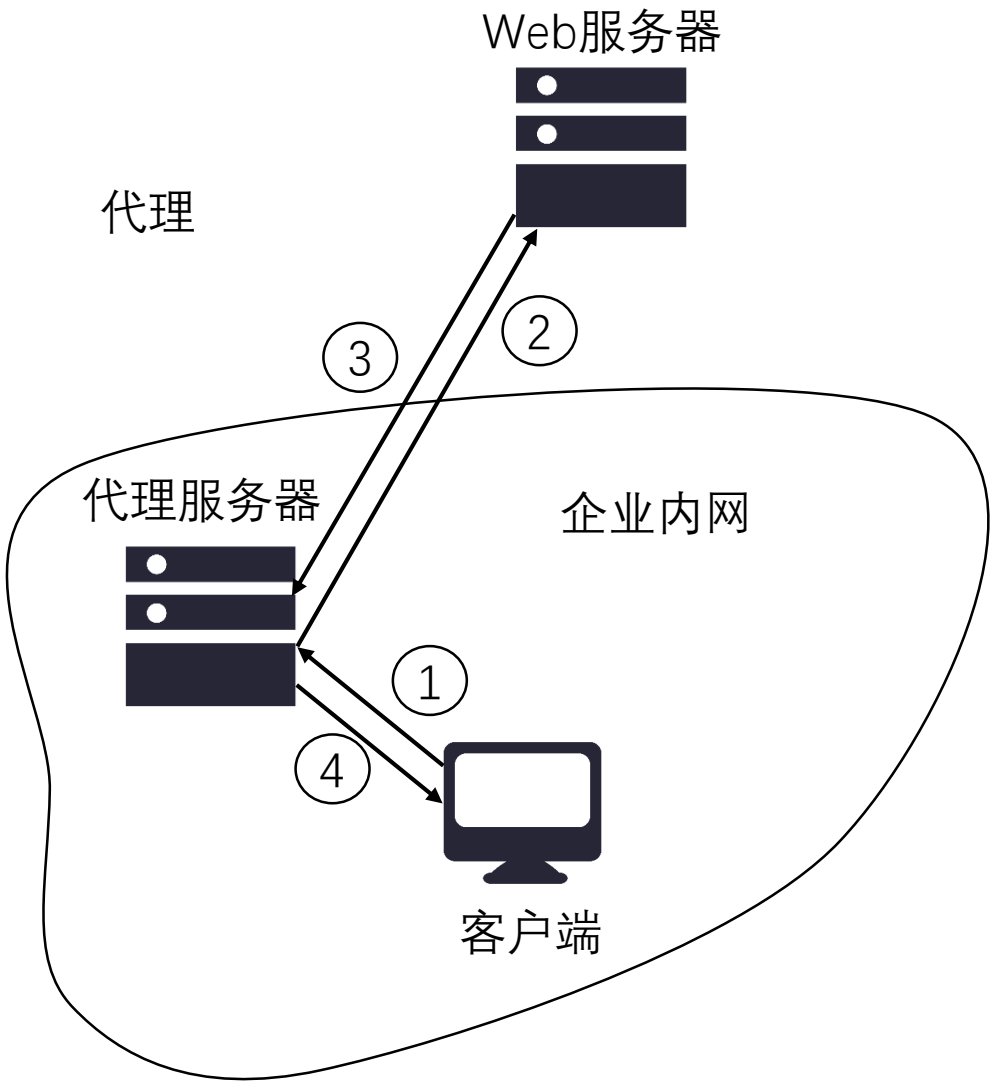
思考: 如何更安全地提供服务

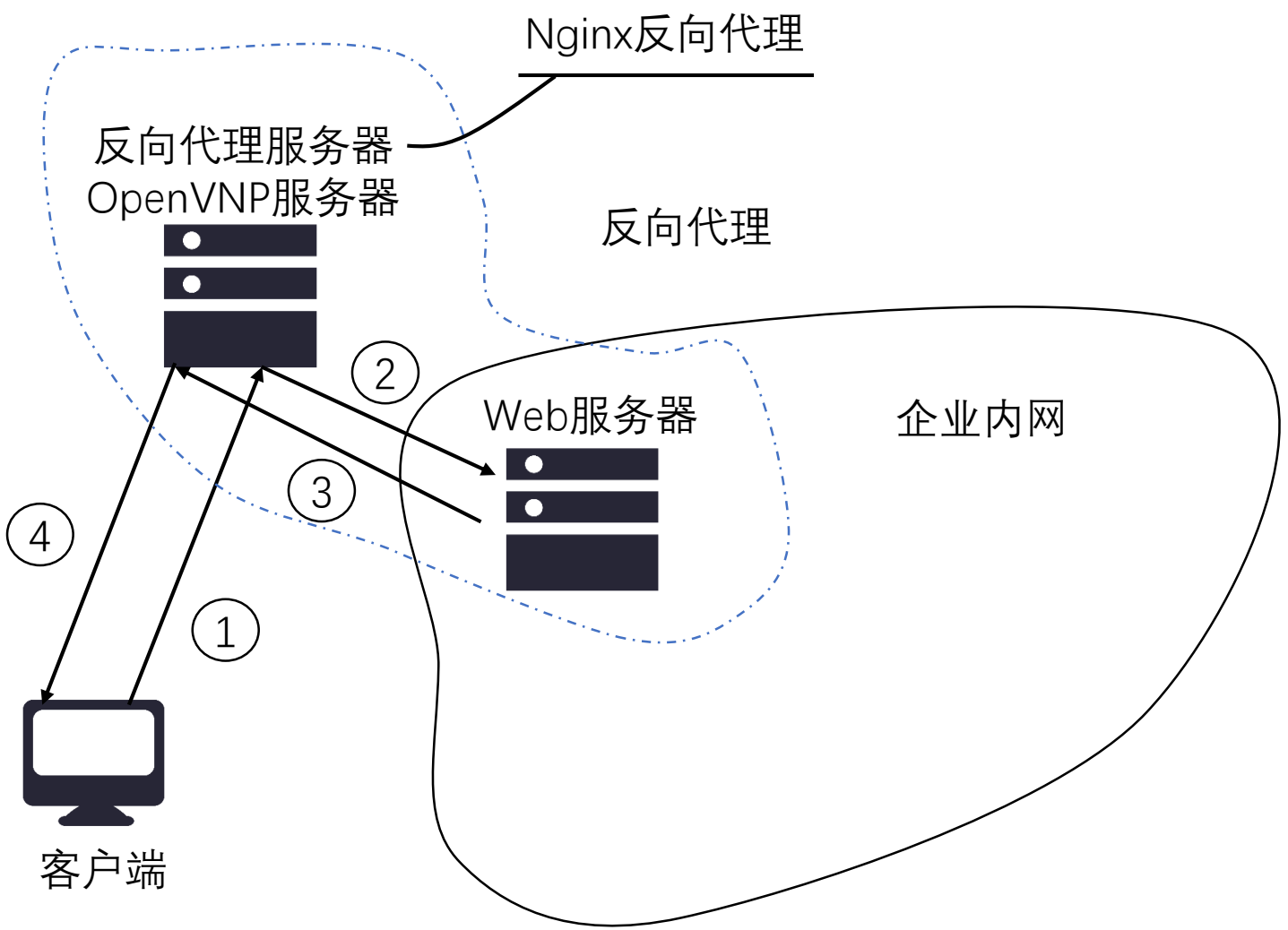
以Web服务为例子

- 如果有一个客户端，不是本企业的员工，仍需要使用数据服务器中的Web服务呢？
  - 允许该外单位客户端加入VPN网络吗？
    - 安全隐患哪里？网络层连通，攻击者实施攻击的关键！

- 不在网络层连通，如何解决可见性问题？
  - IP不可见，解决Web服务可见！！这个是应用层的问题！
  - 使用反向代理技术！

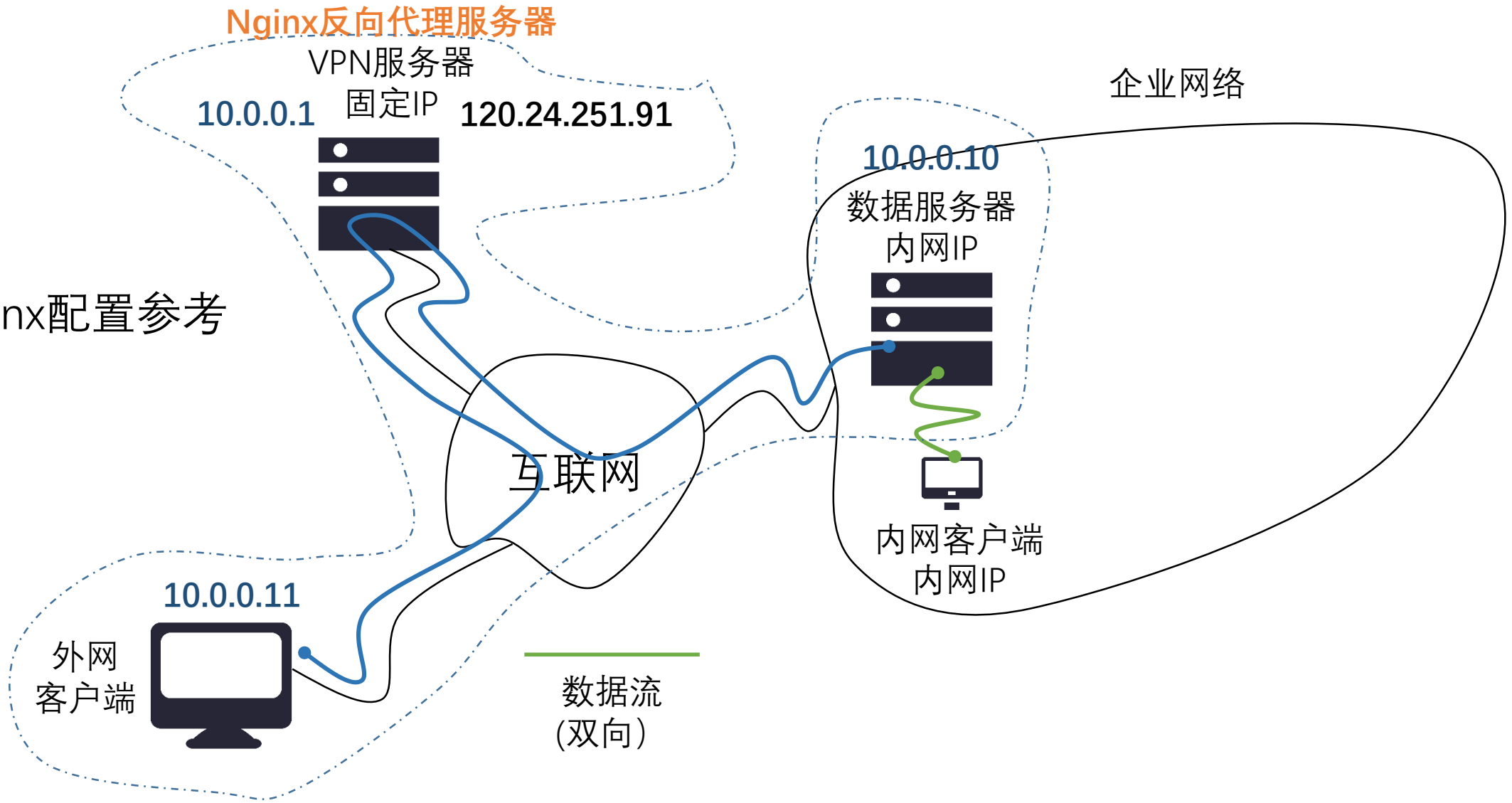
方案: 代理与反向代理 (应用层HTTP代理)





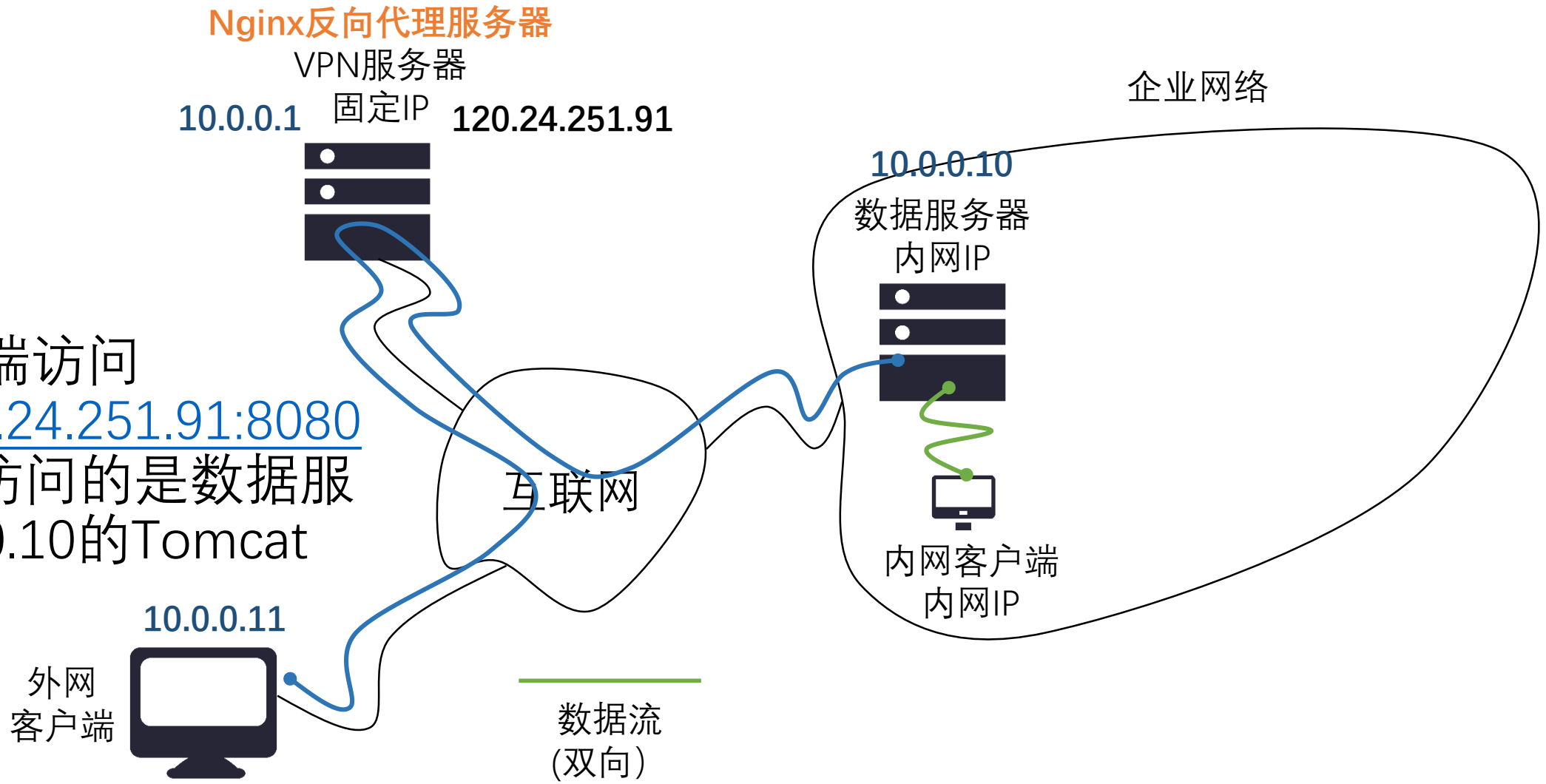
使用Nginx创建HTTP反向代理服务器

- 参考: Nginx配置参考



测试Web的访问性

- 任何客户端访问 http://120.24.251.91:8080/, 实际上访问的是数据服务中10.0.0.10的Tomcat web服务



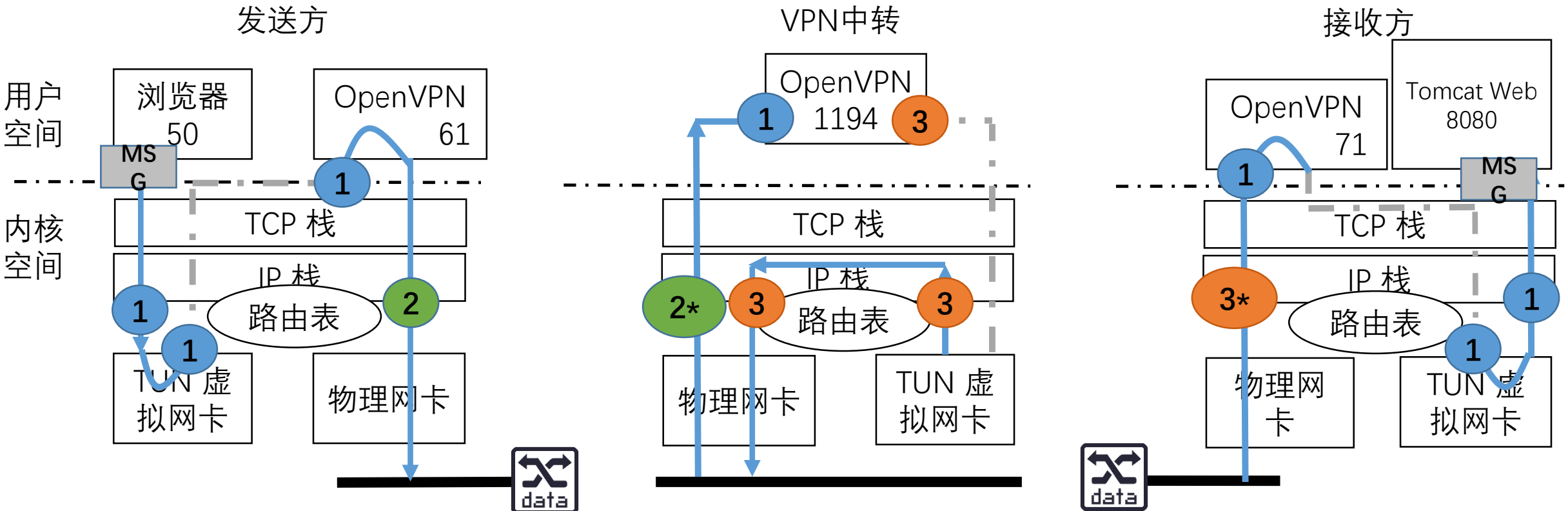
研究: OpenVPN的基本原理

- IP隧道技术
- SSL技术
  - 基于数字证书的认证
  - SSL安全通道

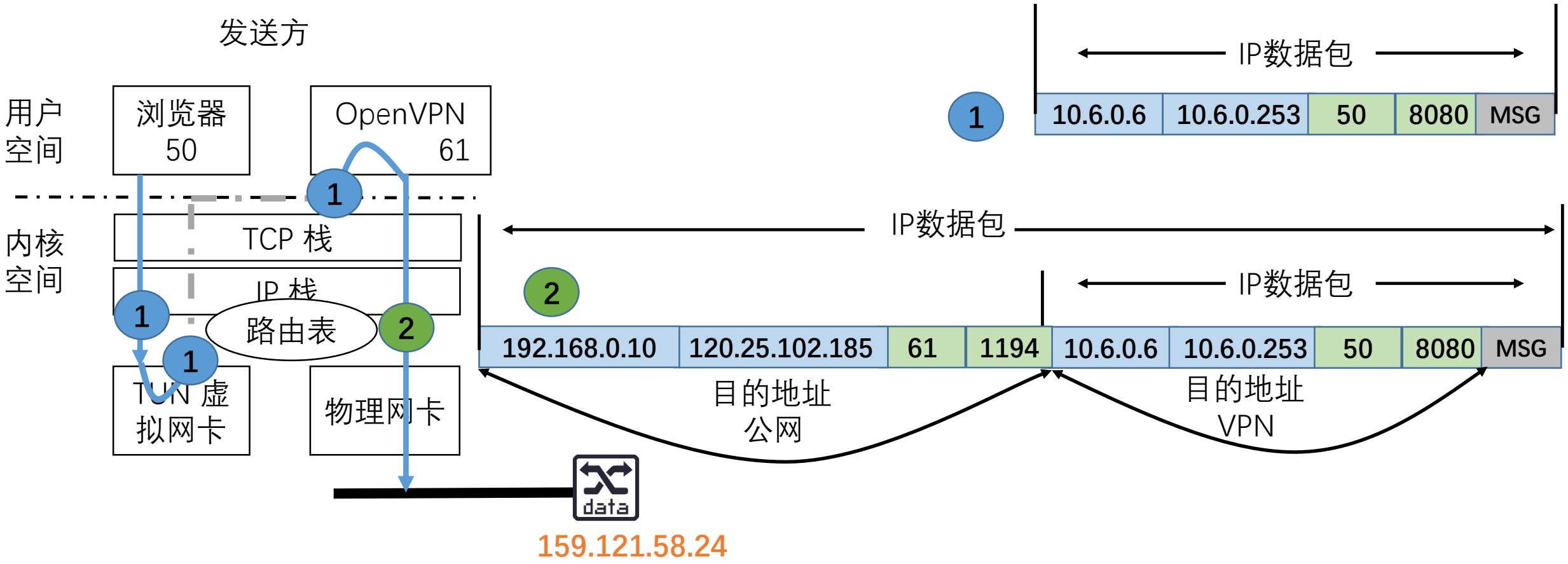
附录: OpenVPN基本原理

OpenVPN 原理

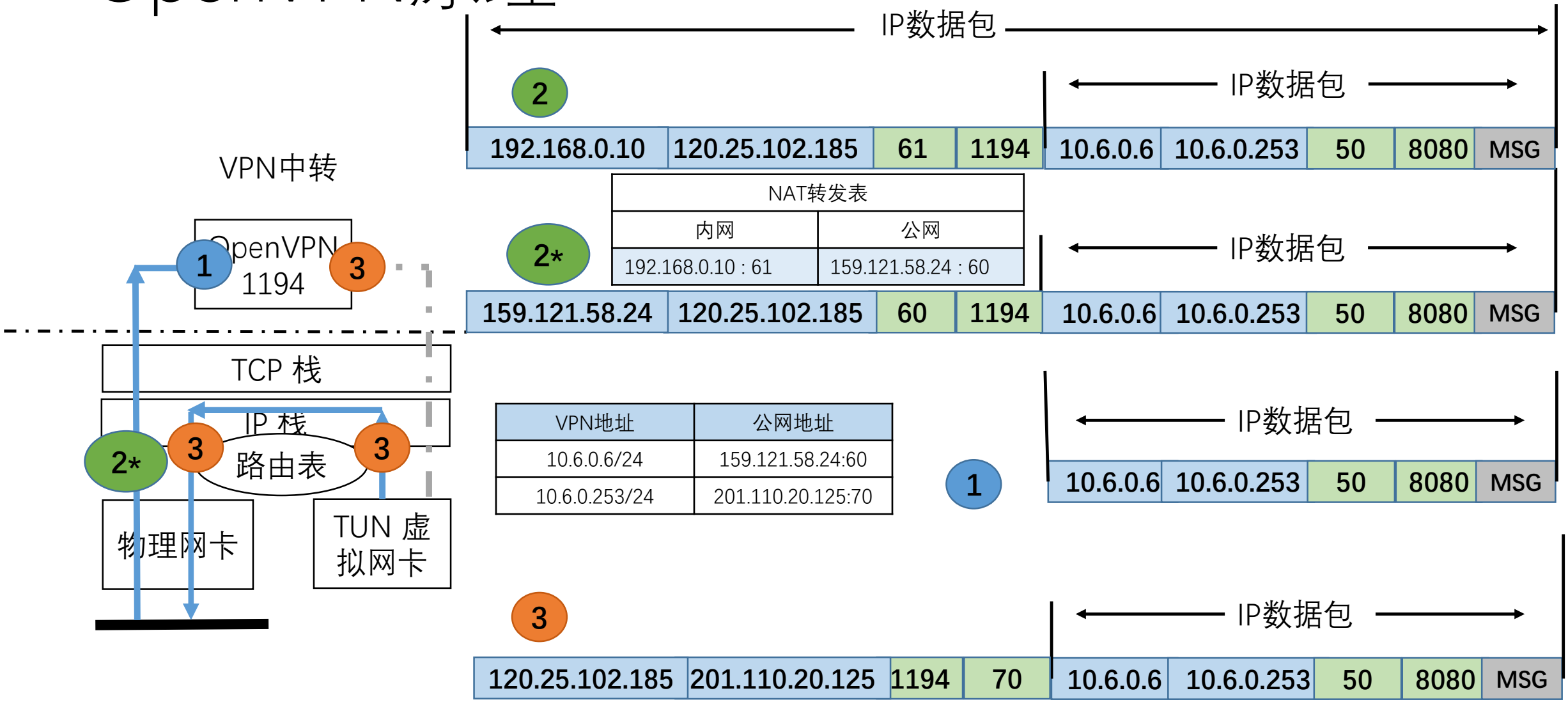
- TUN 虚拟网卡设备
- IP 通道：封装与解封，转发 ~



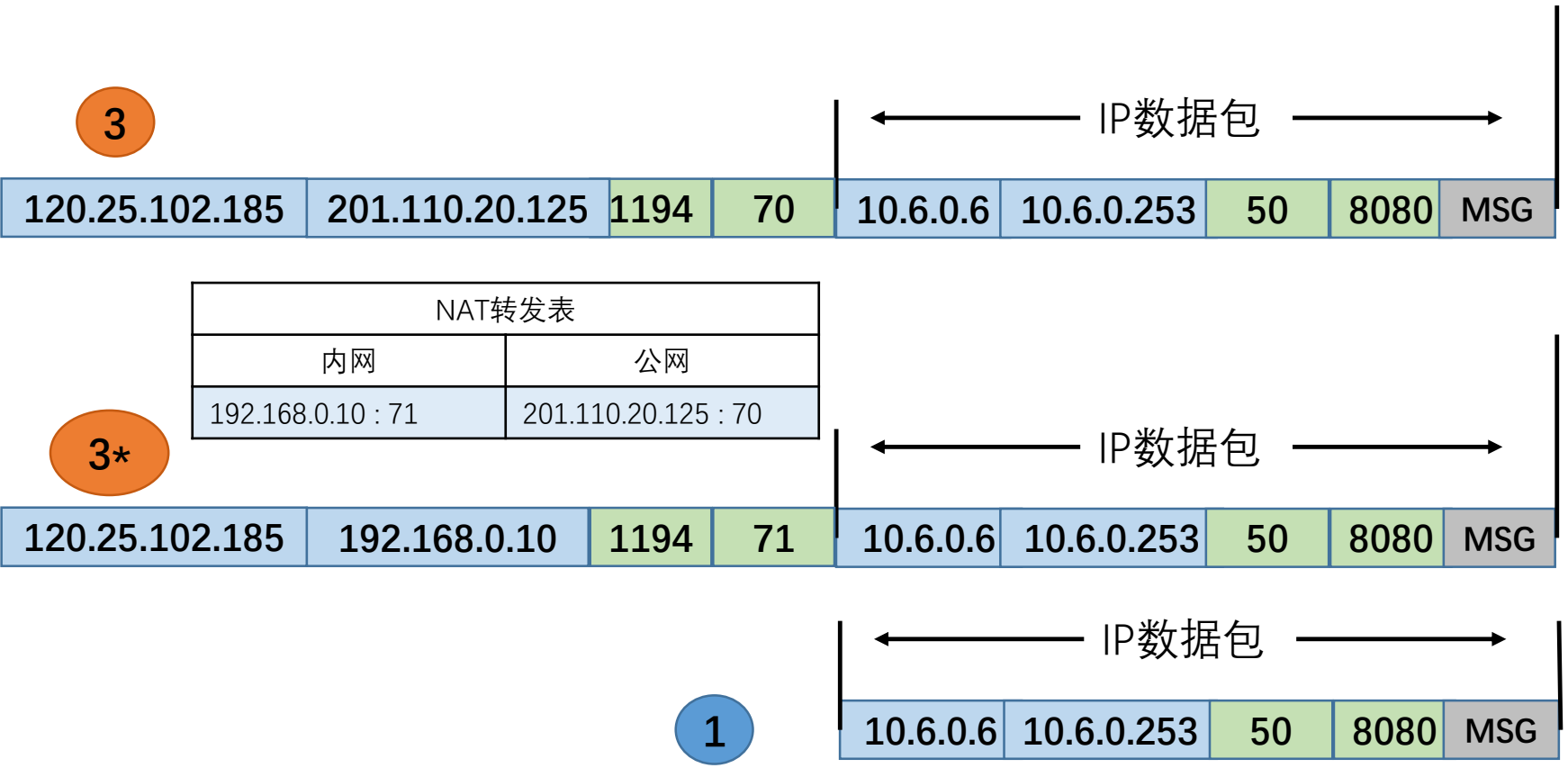
OpenVPN原理

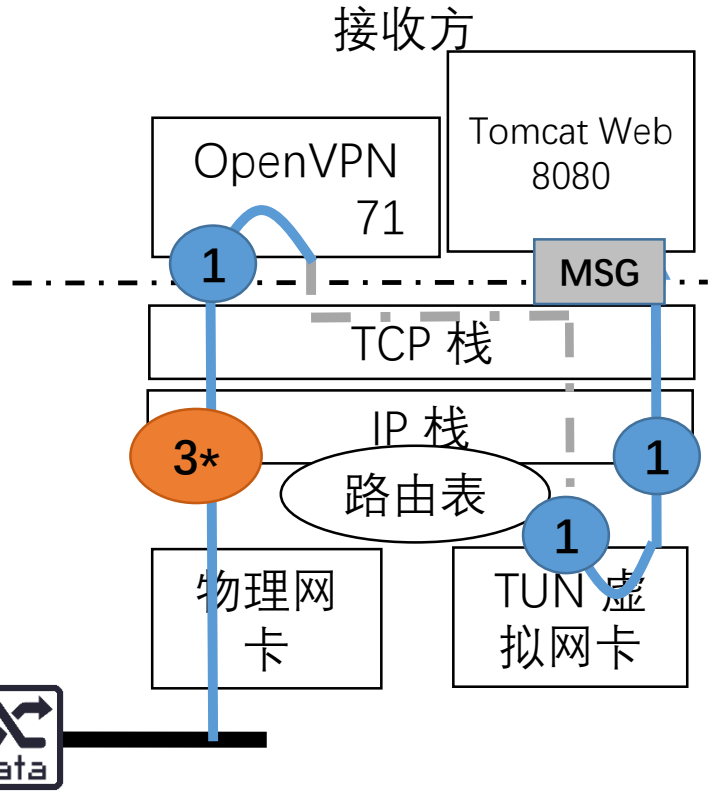

发送方
用户空间
浏览器
50
OpenVPN
61
内核空间
TCP 栈
IP 栈
路由表
TUN 虚拟网卡
物理网卡
1
2
IP数据包
10.6.0.6
10.6.0.253
50
8080
MSG
192.168.0.10
120.25.102.185
61
1194
目的地址
公网
目的地址
VPN
data
159.121.58.24

OpenVPN原理


IP数据包
IP数据包
2
192.168.0.10
120.25.102.185
61
1194
10.6.0.6
10.6.0.253
50
8080
MSG
VPN中转
OpenVPN
1194
1
3
NAT转发表
内网
公网
192.168.0.10 : 61
159.121.58.24 : 60
2*
IP数据包
159.121.58.24
120.25.102.185
60
1194
10.6.0.6
10.6.0.253
50
8080
MSG
TCP 栈
IP 栈
2*
3
路由表
3
VPN地址
公网地址
10.6.0.6/24
159.121.58.24:60
10.6.0.253/24
201.110.20.125:70
1
IP数据包
10.6.0.6
10.6.0.253
50
8080
MSG
物理网卡
TUN 虚拟网卡
3
IP数据包
120.25.102.185
201.110.20.125
1194
70
10.6.0.6
10.6.0.253
50
8080
MSG

OpenVPN原理



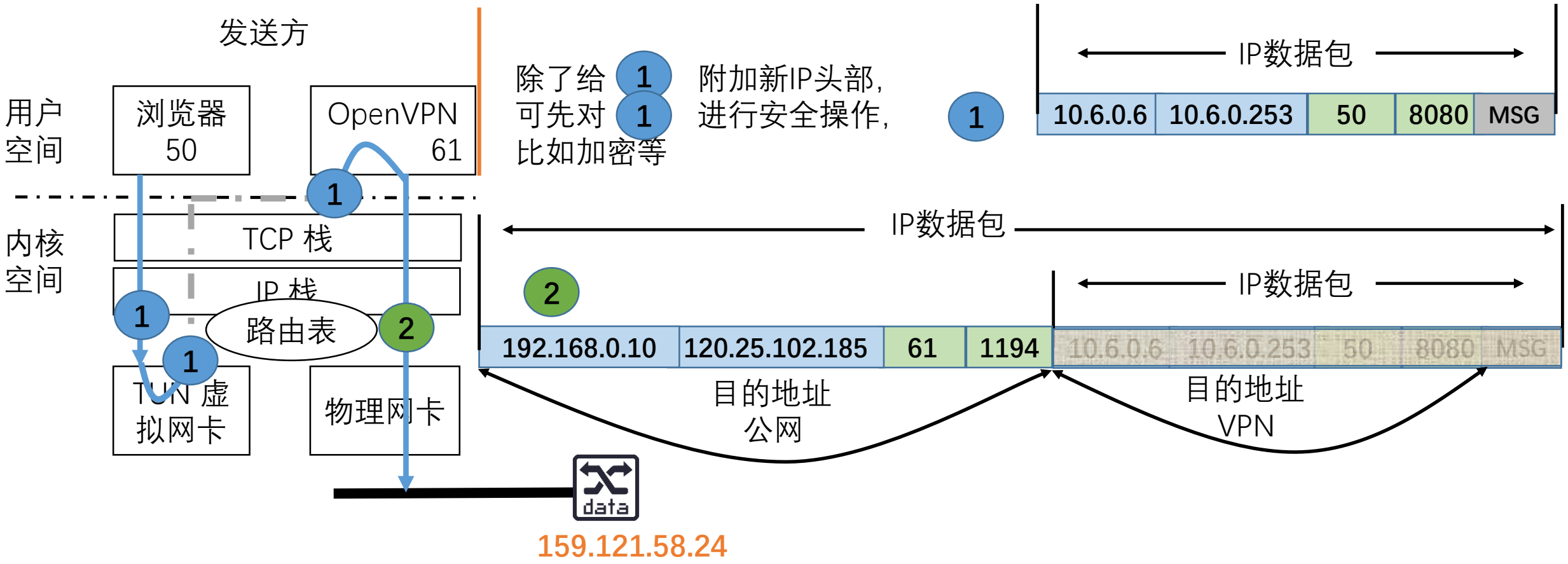


201.110.20.125

OpenVPN原理: 路由表

- 理解OpenVPN服务器端与客户端的路由表非常关键！
  - IP隧道，本质是转发
- 学习CentOS 7中的路由表与Windows中的路由表

OpenVPN安全


发送方
用户空间
浏览器 50
OpenVPN 61
内核空间
TCP 栈
IP 栈
路由表
TUN 虚拟网卡
物理网卡
data
159.121.58.24
除了给可先对比如加密等
1
1
附加新IP头部，进行安全操作，
1
IP数据包
10.6.0.6
10.6.0.253
50
8080
MSG
IP数据包
2
IP数据包
192.168.0.10
120.25.102.185
61
1194
10.6.0.6
10.6.0.253
50
8080
MSG
目的地址 公网
目的地址 VPN

参考

[1] OpenVPN, www.openvpn.net

[2] Jie Qian and Ben Smeets. *IPsec and OpenVPN worked-out examples.* http://ipseclab.eit.lth.se/tiki-index.php

[3]Tunneling protocol, https://en.wikipedia.org/wiki/Tunneling_protocol

[4] IP Tunnel, https://en.wikipedia.org/wiki/IP_tunnel

[5] IP in IP, https://en.wikipedia.org/wiki/IP_in_IP

[6] Nginx, www.nginx.org