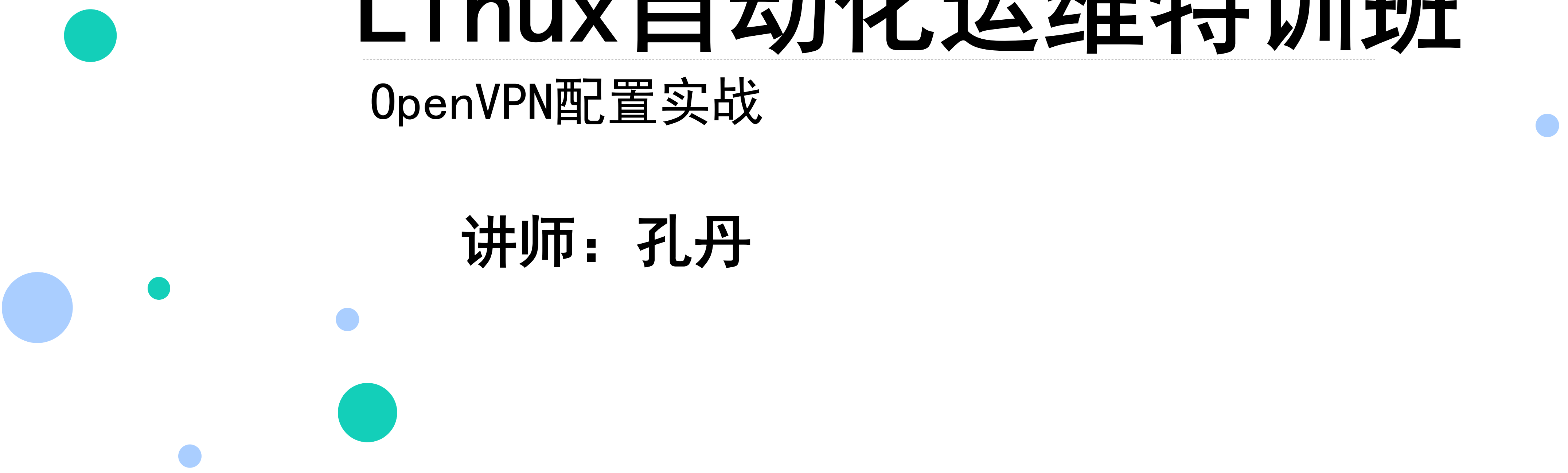


Linux自动化运维特训班

PPTP-VPN配置实战

讲师：孔丹



大纲

- VPN简介
- VPN分类
- PPTP VPN简介
- PPTP VPN配置

版权所有，侵权必究

VPN简介

- VPN概述

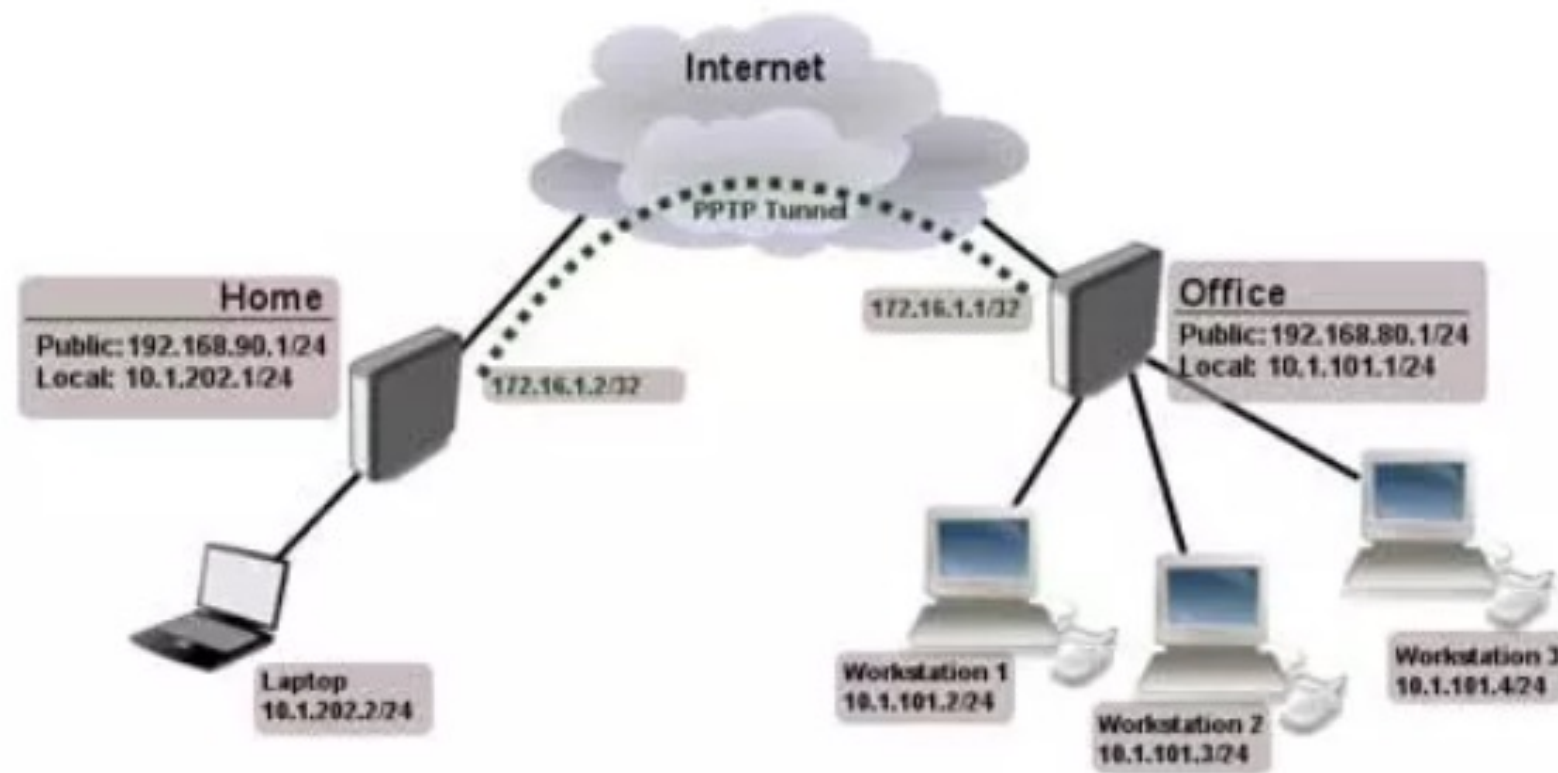
- VPN（Virtual Private Network，虚拟专用网）。“虚拟”（Virtual）指的是一种逻辑连接，“专用或私有”（Private）指的是排他性的连接，“网络”（Network）指按某种协议进行通信的计算机集合。

- 虚拟专用网络可以实现不同网络的组件和资源之间的相互连接。虚拟专用网络能够利用Internet或其它公共互联网络的基础设施为用户创建隧道，并提供与专用网络一样的安全性和功能保障。

- VPN是对在公共通信基础设施上构建的“虚拟专用或私有网”连接技术的总称。VPN与真实网络的差别在于VPN以隔离方式通过公用网，VPN外的节点不能与VPN内的节点通信

VPN分类

□ PPTP

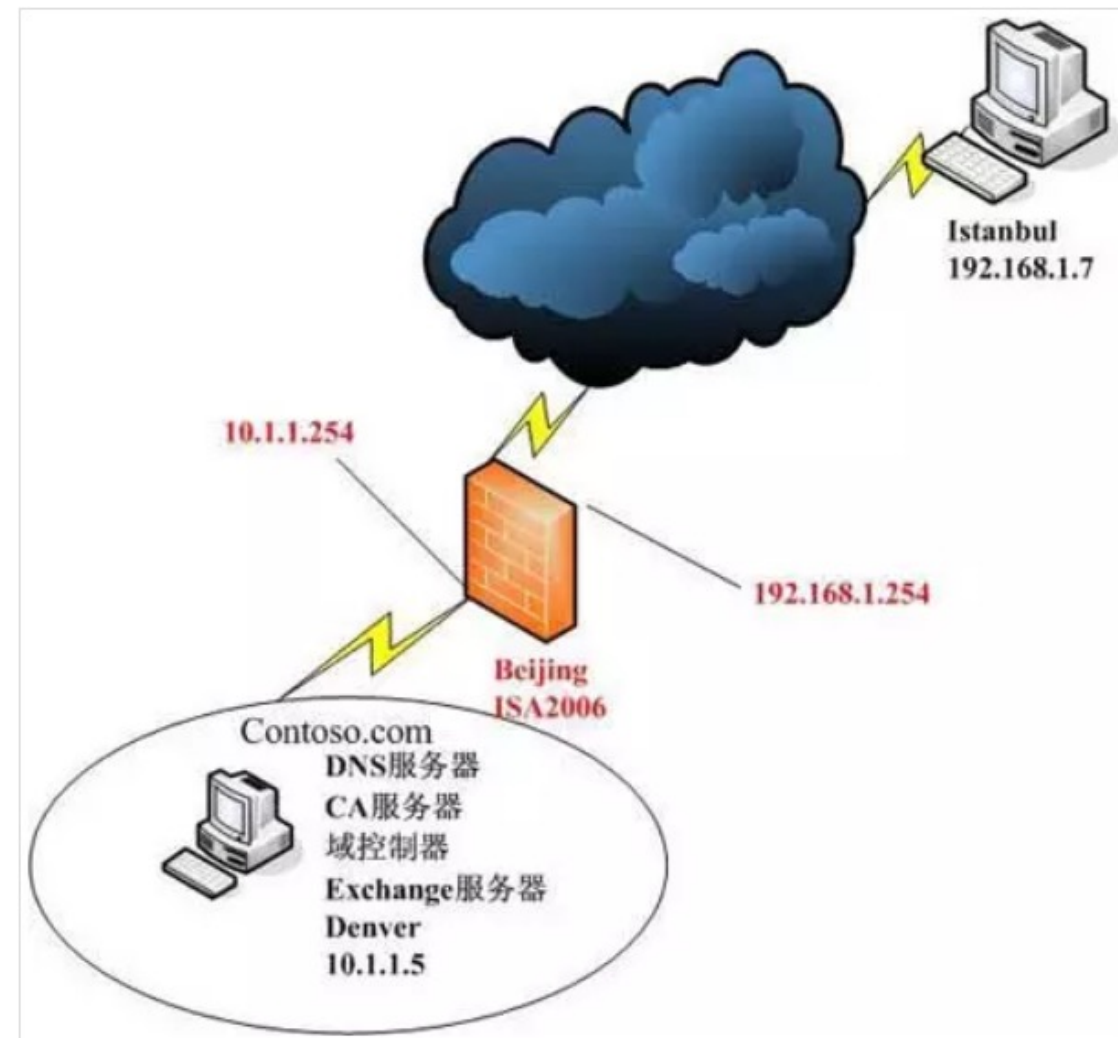


- 点对点隧道协议 (PPTP) 是由包括微软和3Com等公司组成的PPTP论坛开发的一种点对点隧道协，基于拨号使用的PPP协议使用PAP或CHAP之类的加密算法，或者使用Microsoft的点对点加密算法MPPE。其通过跨越基于TCP/IP的数据网络创建VPN实现了从远程客户端到专用企业服务器之间数据的安全传输。PPTP支持通过公共网络(例如Internet)建立按需的、多协议的、虚拟专用网络。PPTP允许加密IP通讯，然后在要跨越公司IP络或公共IP网络(如Internet)发送的IP头中对其进行封装。

版权所有，侵权必究

VPN分类

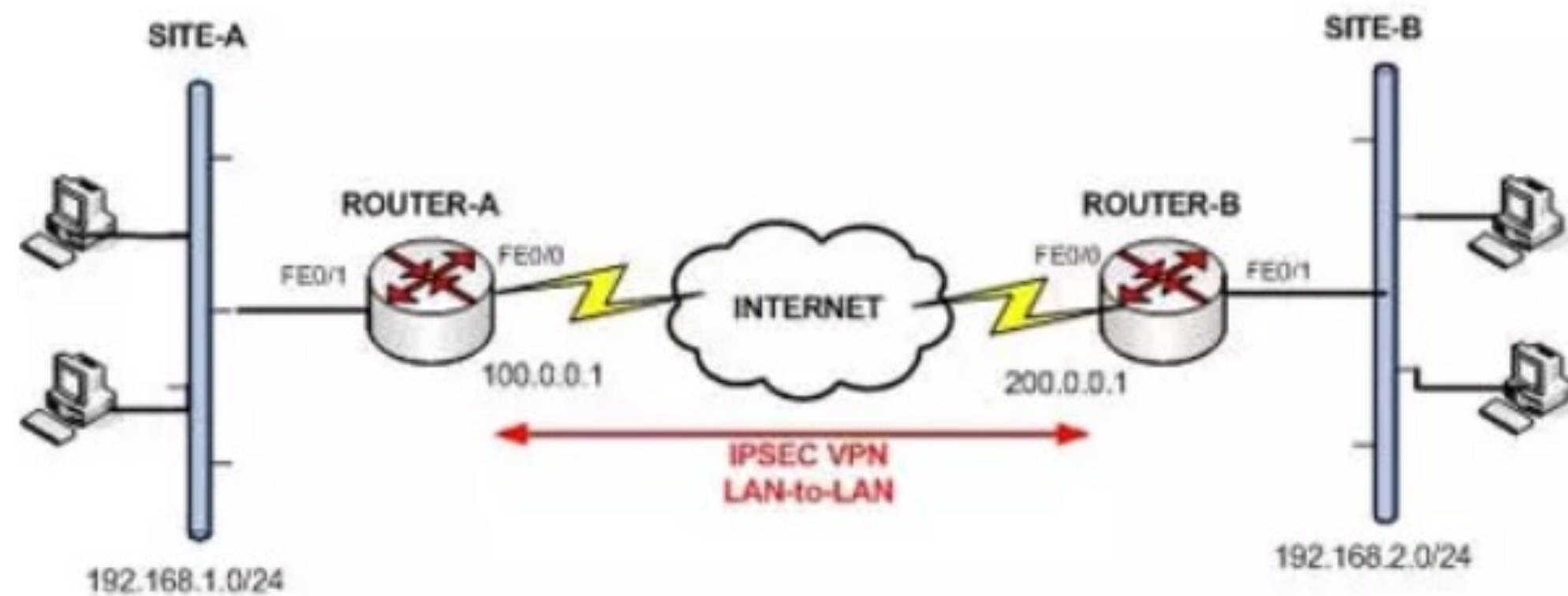
□ L2TP



- 第2层隧道协议 (L2TP) 是IETF基于L2F (Cisco的第二层转发协议) 开发的PPTP的后续版本。是一种工业标准Internet隧道协议，其可以为跨越面向数据包的媒体发送点到点协议 (PPP) 框架提供封装。PPTP和L2TP都使用PPP协议对数据进行封装，然后添加附加包头用于数据在互联网上的传输。PPTP只能在两端点间建立单一隧道。L2TP支持在两端点间使用多隧道，用户可以针对不同的服务质量创建不同的隧道。L2TP可以提供隧道验证，而PPTP则不支持隧道验证。但是当L2TP或PPTP与IPSEC共同使用时，可以由IPSEC提供隧道验证，不需要在第2层协议上验证隧道使用L2TP。PPTP要求互联网络为IP网络。L2TP只要求隧道媒介提供面向数据包的点对点的连接，L2TP可以在IP (使用UDP)，帧中继永久虚拟电路 (PVCs)，X.25虚拟电路 (VCs) 或ATM VCs网络上使用。

VPN分类

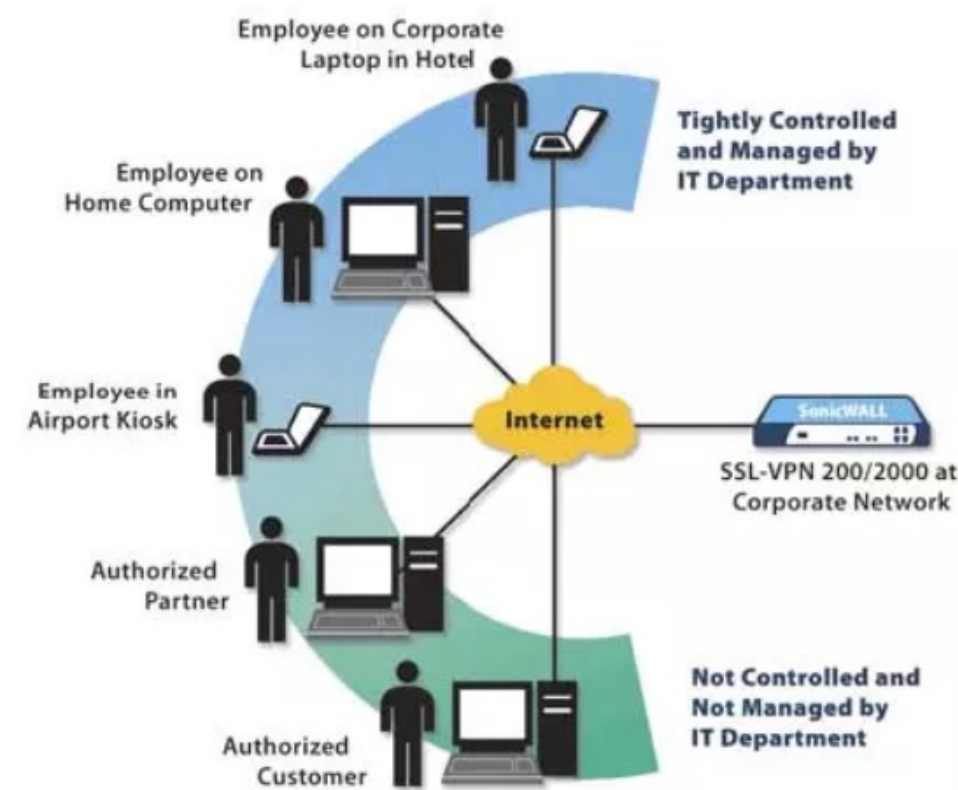
□ IPSec



- IPSec的隧道是由封装、路由与解封装组成整个过程。隧道将原始数据包隐藏(或封装)在新的数据包内部。该新的数据包可能会有新的寻址与路由信息，从而使其能够通过网络传输。隧道与数据保密性结合使用时，在网络上窃听通讯的人将无法获取原始数据包数据(以及原始的源和目标)。封装的数据包到达目的地后，会删除封装，原始数据包头用于将数据包路由到最终目的地。

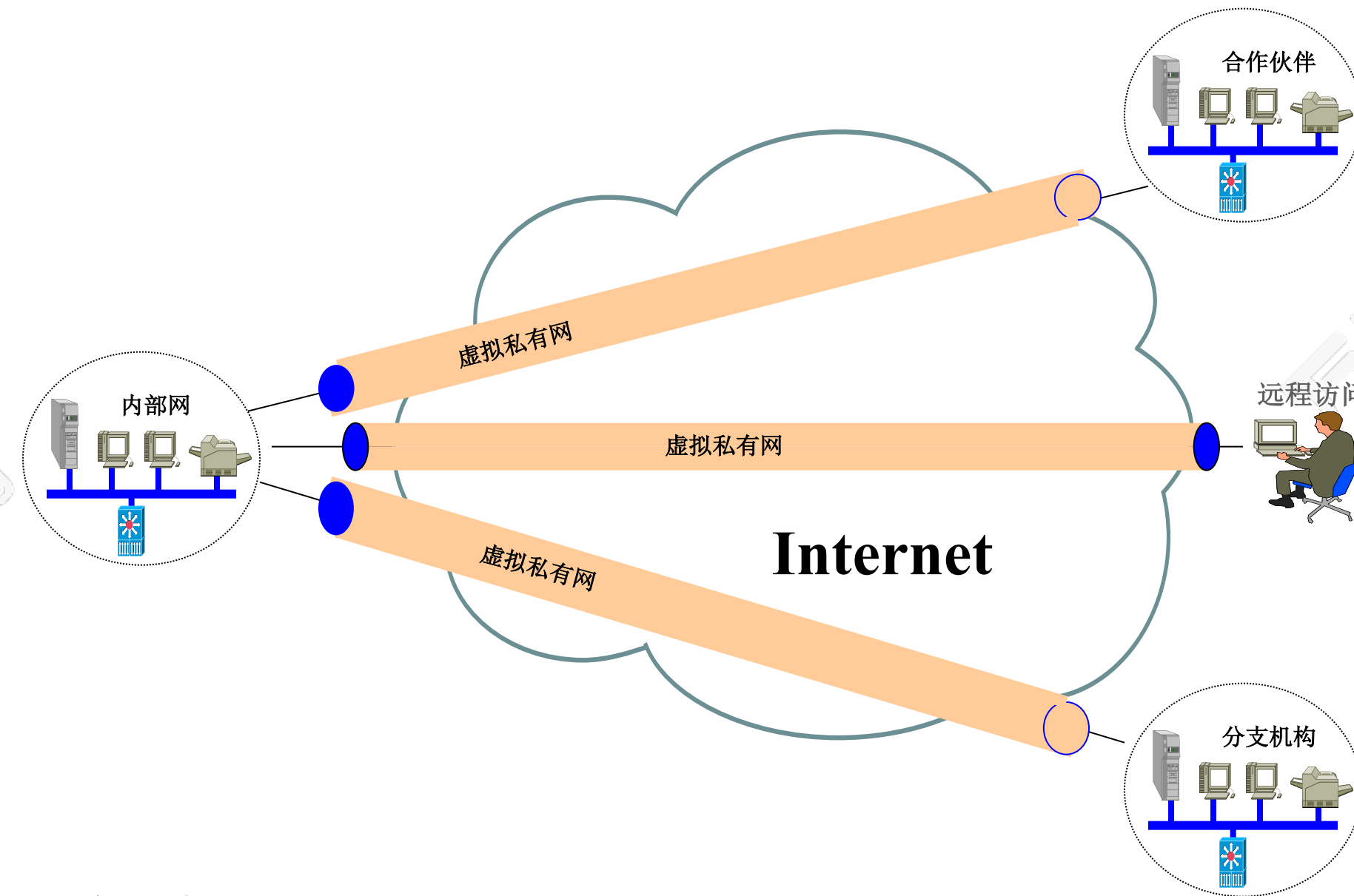
VPN分类

□ SSLVPN



- SSL协议提供了数据私密性、端点验证、信息完整性等特性。SSL协议由许多子协议组成，其中两个主要的子协议是握手协议和记录协议。握手协议允许服务器和客户端在应用协议传输第一个数据字节以前，彼此确认，协商一种加密算法和密码钥匙。在数据传输期间，记录协议利用握手协议生成的密钥加密和解密后来交换的数据。
- SSL独立于应用，因此任何一个应用程序都可以享受它的安全性而不必理会执行细节。SSL置身于网络结构体系的传输层和应用层之间。此外，SSL本身就被几乎所有的Web浏览器支持。这意味着客户端不需要为了支持SSL连接安装额外的软件。这两个特征就是SSL能应用于VPN的关键点。

VPN的典型应用



❑ 远程访问VPN (Access VPN)

远程访问VPN适用于企业内部人员流动频繁或远程办公的情况，出差员工或在家办公的员工利用当地Internet服务提供商 (ISP) 就可以和企业的VPN网关建立私有的隧道连接

❑ 内联网VPN (Intranet VPN)

如果要进行企业内部异地分支机构的互联，可以使用内联网VPN (Intranet VPN) 方式

❑ 外联网VPN (Extranet VPN)

与合作伙伴企业网构成Extranet，将一个公司与另一个公司的资源进行连接。

VPN特点

□ 成本低

由于VPN建立在物理连接基础之上，使用Internet、帧中继或ATM等公用网络设施，不需要租用专线，可以节省购买和维护通讯设备的费用。

□ 安全保障

VPN使用Internet等公用网络设施，提供了各种加密、认证和访问控制技术来保障通过公用网络平台传输数据的安全性，以确保数据不被攻击者窥视和篡改，并且防止非法用户对网络资源或私有信息的访问。

□ 服务质量保证

不同的用户和业务对服务的质量保证有着不同的要求。所有VPN应提供相应的不同等级的服务质量保证(Quality ofService, QoS)

□ 可管理性

VPN实现简单、方便、灵活，同时具有安全管理、设备管理、配置管理、访问控制列表管理、QoS管理等内容，方便用户和运营商管理和维护。

□ 可扩展性

VPN设计易于增加新的网络节点，并支持各种协议，如RSIP

IPv6、MPLS、SNMPv3，满足同时传输IP语音、图像和IPv6数据等新应用对高质量传输以及带宽增加的需求。

VPN关键技术

□ 隧道技术（Tunneling Protocol）

- 隧道技术是将分组封装（ Capsule ） 的技术， 它是VPN实现以内部网地址通信与多协议通信的重要功能， PPTP、L2TP、 IPSec、 GRE和GTP被广泛采用。

□ 认证协议

- 在远程访问VPN中 ， 使用了用户名及口令， 它们被用来判断用户名是否有权访问。 PPP采用了PAP（ Password Authentication Protocol ） 及CHAP（ Challenge Handshake Authentication Protocol ） 等规程进行认证。 PPTP及L2TP等隧道协议采用这种PPP的认证协议。

□ 加密技术

- 加密技术由IPSec ESP（ Encapsulating Security Payload ）。

PPTP VPN简介

- ❑ 点对点隧道协议（Point to Point Tunneling Protocol，缩写为PPTP）是实现虚拟专用网（VPN）的方式之一。PPTP使用传输控制协议（TCP）创建控制通道来发送控制命令，以及利用通用路由封装（GRE）通道来封装点对点协议（PPP）数据包以发送数据。这个协议最早由微软等厂商主导开发，但因为它的加密方式容易被破解，微软已经不再建议使用这个协议。
- ❑ PPTPD（Point-to-Point Tunneling Protocol Daemon）是VPN（Virtual Private Network）服务器，PPTP（Point-to-Point Tunneling Protocol）是VPN客户端。PPTPD和PPTP都是通过PPP（Point to Point Protocol）来实现VPN功能的。MPPE模块是用来支持Linux与Windows之间连接的。如果不需要Windows电脑参与连接，则不需要可以这安装MPPE模块。PPTPD、PPTP和MPPE Module一起统称Poptop。Poptop官方网站上的定义是The PPTP Server for Linux，就是利用PPTP（Point to Point Tunneling Protocol，点到点隧道协议）通过Internet访问VPN（Virtual Private Network，虚拟局域网）。

版权所有，侵权必究

PPTP VPN配置

□ 环境规划

主机名	网卡	默认网关	用途
VPN Server	192.168.150.11（ens33，内网卡） 200.1.1.1（ens37，外网卡）	192.168.150.2	VPN Server
FTP Server	192.168.150.12	192.168.150.2	内网FTP Server
Remote Client	200.1.1.10		模拟外网测试客户机

说明：

VPN Server采用双网卡，网关指向192.168.150.2。

Remote Client 远程拨入VPN Server后要能访问内网

FTP Server资源。

Remote Client拨号地址为200.1.1.1（模拟外网IP）

版权所有，侵权必究

PPTP VPN配置

- PPTP的配置主要有下面五个步骤
 - 验证内核是否加载了MPPE模块
 - 安装所需的软件包
 - 配置PPP和PPTP的配置文件
 - 打开内核的IP转发功能
 - 启动pptpd守护进程
 - 配置iptables防火墙放行和转发规则

PPTP VPN配置

❑ 1、验证内核是否加载了MPPE模块

```
[root@node1 ~]# modprobe ppp-compress-18 && echo MPPE  
is ok
```

MPPE is ok

❑ 2、检查PPP是否支持MPPE

```
[root@node1 ~]# yum install ppp -y  
[root@node1 ~]# strings '/usr/sbin/pppd' | grep -i  
mppe | wc -l
```

43

若结果显示0则表示不支持，而30或更大的数字就表示支持。

❑ 3、安装pptpd

```
[root@node1 ~]# yum install  
http://rpmfind.net/linux/epel/7/x86_64/Packages/p/  
pptpd-1.4.0-2.el7.x86_64.rpm -y
```


PPTP VPN配置

- ❑ 1、编辑/etc/pptpd.conf设置VPN内网IP段

localip 192.168.0.1

remoteip 192.168.0.101-238, 192.168.0.200

- ❑ 2、编辑/etc/ppp/options.pptpd

1>更改DNS项

ms-dns 223.5.5.5

ms-dns 8.8.8.8

2>修改日志记录

nologfd

logfile /var/log/pptpd.log

- ❑ 3、编辑/etc/ppp/chap-secrets设置VPN账号密码

用户名 pptpd 密码 *//每个字段之间用tab键隔开 *表示用任意

IP连接VPN都可以

[root@node1 ~]# tail -3 /etc/ppp/chap-secrets

client server secret IP addresses

user1pptpd 123456 *

user2pptpd 123456 192.168.0.168

版权所有，侵权必究

PPTP VPN配置

□ 4、开启路由转发

编辑/etc/sysctl.conf修改内核参数支持内核转发

```
net.ipv4.ip_forward=1
```

输入命令生效：`sysctl -p`

□ 5、启动服务

```
[root@node1 ~]# systemctl start pptpd
```

```
[root@node1 ~]# systemctl enable pptpd
```

□ 6、准备内网ftp服务器

注意：网关指向VPN Server内网卡地址

```
[root@node1 ~]# yum install vsftpd -y
```

```
[root@node1 ~]# systemctl start vsftpd
```

PPTP VPN配置

测试：

本文使用win7测试，查看IP

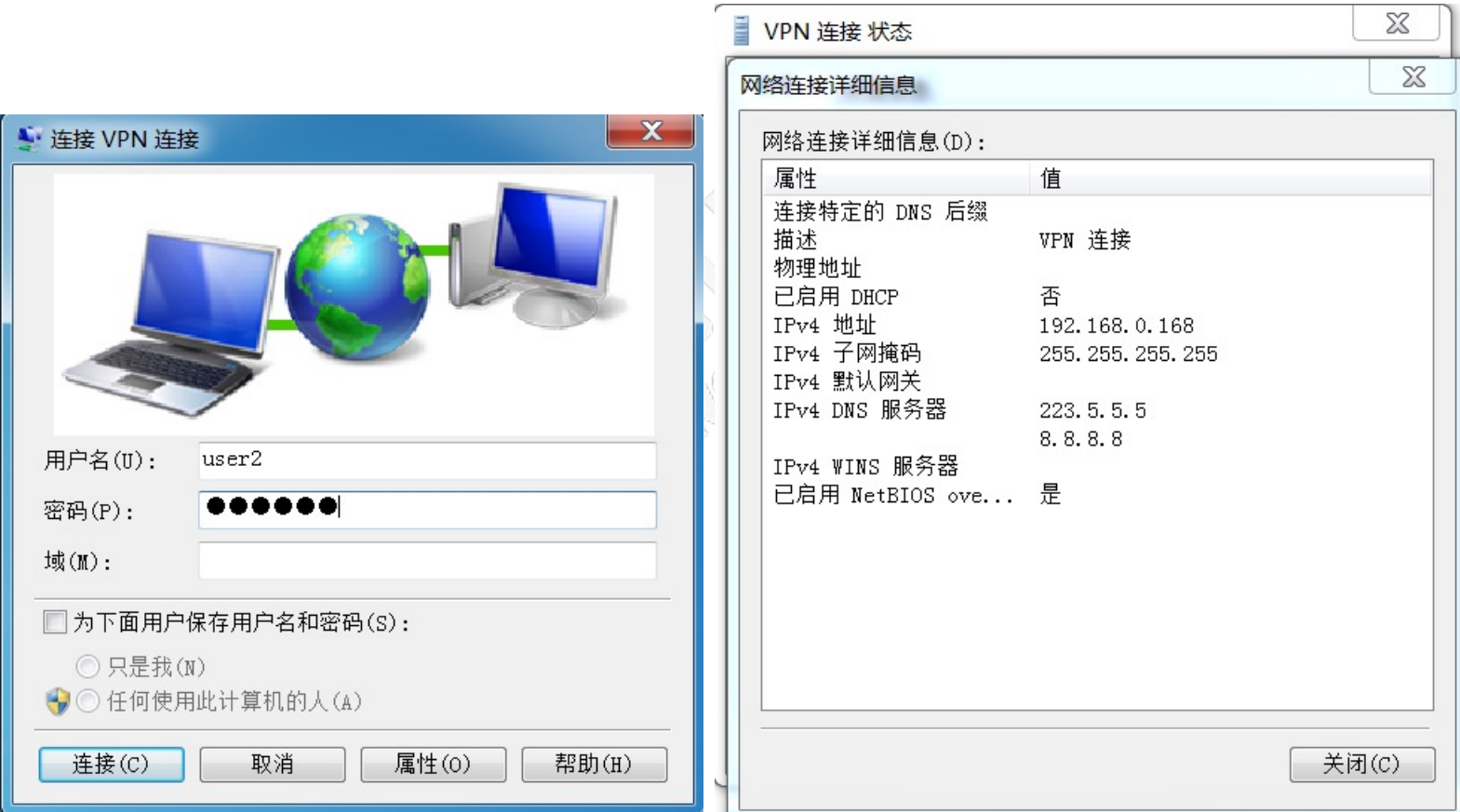
C:\Users\Administrator>ipconfig

Windows IP 配置

以太网适配器 本地连接:

连接特定的 DNS 后缀 :
本地连接 IPv6 地址. fe80::505f:7380:e20c:58e0%11
IPv4 地址 : 200.1.1.2
子网掩码 : 255.255.255.0
默认网关. :

拨号成功后再次查看：



PPTP VPN配置

□ 测试：

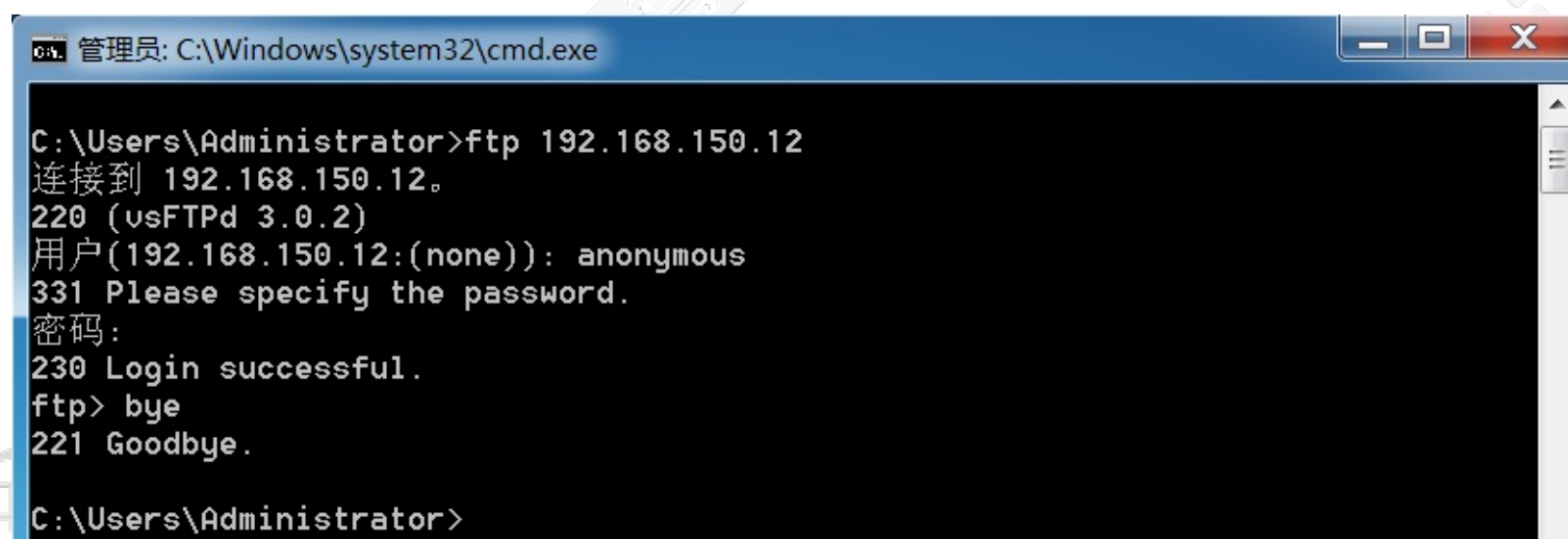
访问ftp服务器测试：

```
C:\Users\Administrator>ping 192.168.150.12
正在 Ping 192.168.150.12 具有 32 字节的
来自 192.168.150.12 的回复: 字节=32 时间
来自 192.168.150.12 的回复: 字节=32 时间
来自 192.168.150.12 的回复: 字节=32 时间
来自 192.168.150.12 的回复: 字节=32 时间
```

192.168.150.12 的 Ping 统计信息：

数据包：已发送 = 4，已接收 = 4，丢失
往返行程的估计时间(以毫秒为单位)：

最短 = 1ms，最长 = 3ms，平均 = 2ms



```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ftp 192.168.150.12
连接到 192.168.150.12。
220 (vsFTPd 3.0.2)
用户(192.168.150.12:(none)): anonymous
331 Please specify the password.
密码:
230 Login successful.
ftp> bye
221 Goodbye.
C:\Users\Administrator>
```

PPTP VPN配置

□ 测试:

VPN服务器查看:

```
[root@node1 ~]# last | head -1
```

```
user2      ppp0      200.1.1.2
```

```
Sun Dec  1 20:25      still
```

```
logged in
```

查看日志:

```
[root@node1 ~]# tail /var/log/pptpd.log
```

```
Modem hangup
```

```
Connection terminated.
```

```
Plugin /usr/lib64/pptpd/pptpd-logwtmp.so loaded.
```

```
Using interface ppp0
```

```
Connect: ppp0 <--> /dev/pts/1
```

```
peer from calling number 200.1.1.2 authorized
```

```
MPPE 128-bit stateless compression enabled
```

```
Cannot determine ethernet address for proxy ARP
```

```
local  IP address 192.168.0.1
```

```
remote IP address 192.168.0.168
```

版权所有，侵权必究

总结

- VPN简介
- VPN分类
- PPTP VPN简介
- PPTP VPN配置

版权所有，侵权必究



谢谢观看

更多好课，请关注万门大学APP

