



Microsoft

MCSA

Windows Server 2016实现和管理

程尊华



Module 8

实施VPN

模块概述

- 规划VPN
- 实施VPN



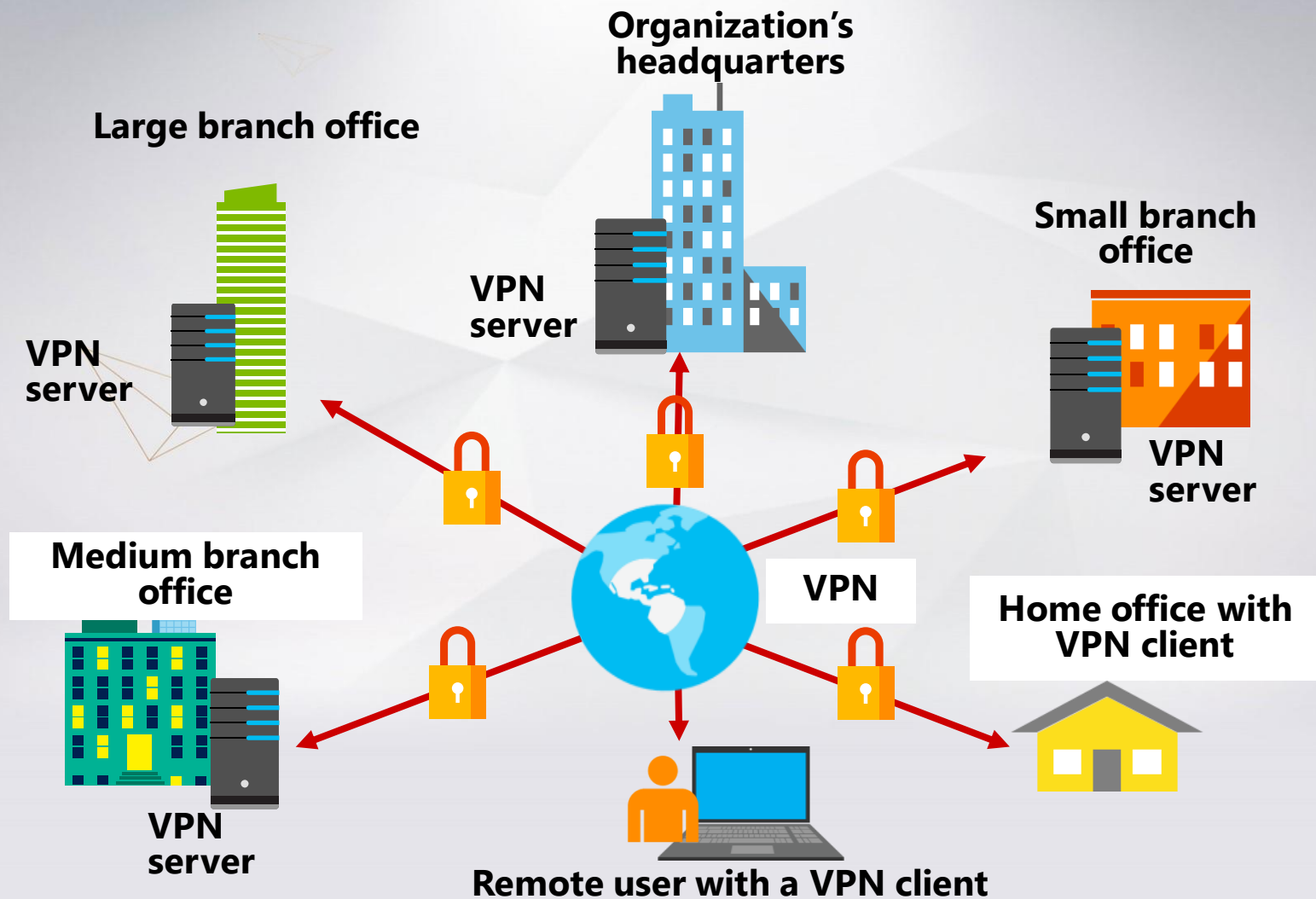
第1课：规划VPN

- VPN方案
- 站点到站点VPN
- VPN隧道协议选项
- VPN认证选项
- 什么是VPN重新连接？
- 应用触发的VPN功能



VPN方案

VPN通过使用诸如Internet的公共网络来提供专用网络组件之间的点对点连接



站点到站点VPN

- 连接私有网络的两个部分
- 呼叫路由器（VPN客户端）将身份验证到应答路由器（VPN服务器）
- 需要创建一个请求拨号界面
- 您可以创建三种类型的站点到站点VPN
 - PPTP
 - L2TP
 - IKEv2
- 可以持续或按需
- 您可以使用IP需求拨号过滤器或拨出过滤器来控制流量




VPN隧道协议选项

Windows Server 2016支持四种VPN隧道协议

隧道协议	防火墙访问	描述
PPTP	TCP端口1723	提供数据机密性，但不提供数据完整性或数据认证
L2TP / IPsec	UDP端口500，UDP端口1701，UDP端口4500和IP协议ID 50	使用证书或预共享密钥进行身份验证；我们推荐证书认证
SSTP	TCP端口443	使用SSL提供数据机密性，数据完整性和数据认证
IKEv2	UDP端口500	支持最新的IPsec加密算法，提供数据机密性，数据完整性和数据认证



VPN认证选项

协议	描述	安全级别
pap	使用明文密码 如果远程访问客户端和远程访问服务器无法协商更安全的验证形式，则通常使用它。	最不安全的认证协议。 不能防止重播攻击，远程客户端模拟或远程服务器模拟。
chap	一种使用行业标准md5散列方案的质询 - 响应认证协议。 	对pap的改进是因为密码不是通过ppp链路发送的。 需要密码的明文版才能验证挑战响应。 不能防止远程服务器模拟。
ms-chapv2	升级ms-chap。 提供双向认证，也称为相互认证。 远程访问客户端接收验证，即远程访问服务器其所在到有权访问用户的密码拨号。	提供比chap更强的安全性。
eap	允许通过使用认证方案（称为eap类型）对远程访问连接进行任意身份验证。	通过提供最大的灵活性来提供最强的安全性。



什么是VPN重新连接？

- VPN Reconnect维护网络中断时的连接
- VPN重新连接：
 - 提供无缝连贯的VPN连接
 - 使用IKEv2技术
 - 连接可用时自动重新建立VPN连接
 - 如果用户在不同网络之间移动，则维护连接
 - 为用户提供透明的连接状态



应用触发的VPN功能

- 应用程序触发的VPN使应用程序能够自动触发VPN配置文件
- 您可以通过使用
AddVpnConnectionTriggerApplication
PowerShell命令 配置的应用程序触发的VPN
- 域成员计算机不支持应用程序触发的VPN
- 应用程序触发的VPN要求您为VPN配置文件启用拆分隧道



第2课：实施VPN

- 使用入门向导配置VPN
- 修改VPN配置的选项
- 演示：配置VPN
- 什么是Connection Manager管理工具包？
- 演示：创建连接配置文件
- 分发VPN配置文件



使用入门向导配置VPN

- 使用远程访问管理控制台中的入门向导配置VPN
- VPN服务器配置的要求包括：
 - 两个网络接口（公共和私有）
 - IP地址分配（静态池或DHCP）
 - 验证提供商（NPS / RADIUS或VPN服务器）
 - DHCP中继考虑事项
 - 在本地管理员组或同级成员身份



修改VPN配置的选项

要配置您的VPN解决方案，您可能需要：

- 配置静态包过滤器
- 配置服务和端口
- 调整路由协议的日志级别
- 配置可用VPN端口的数量
- 为用户创建一个Connection Manager配置文件
- 添加AD CS
- 增加远程访问安全性
- 增加VPN安全性
- 实施VPN重新连接



演示：配置VPN

- 在此演示中，您将学习如何：
 - 验证IKEv2和SSTP的证书要求
 - 查看默认VPN配置
 - 配置远程访问策略



什么是Connection Manager管理工具包？

- CMAK：
 - 允许您自定义用户 的 远程连接
通过创建预定义连接的经验
远程服务器和网络
 - 创建可以在客户端计算机上运行以建立您设计的网络连接的
的可执行文件
- 您可以使用以下方式将CMAK配置文件分发到客户端
计算机：
 - 操作系统映像
 - 可移动媒体
 - 软件分发工具，如SCCM



演示：创建连接配置文件

- 在此演示中，您将学习如何：
 - 安装CMAK
 - 创建连接配置文件
 - 检查配置文件



分发VPN配置文件


- 您可以使用以下方式创建和分发VPN配置文件：
 - SCCM
 - Intune
 - 组策略
 - 脚本



实验：实施VPN

- 练习1：实施VPN
- 练习2：验证VPN部署
- 练习3：对VPN访问进行故障排除

登录信息

虚拟机: **20741B-LON-DC1**
20741B-EU-RTR
20741B-LON-CL1
用户名:  **Adatum\Administrator**
密码: **Pa55w.rd**

虚拟机: **20741B-INET1**
用户名: **Administrator**
密码: **Pa55w.rd**

预计时间: 60 minutes



实验场景

DirectAccess部署工作非常好。但是，部署在A. Datum的几台计算机无法使用DirectAccess连接到组织的网络。例如，一些家庭用户正在使用不属于Adatum.com域的成员的计算机。其他用户正在运行不支持DirectAccess的操作系统版本。要启用这些计算机的远程访问，您必须部署VPN解决方案。

此外，您必须调查Logan无法连接到A. Datum VPN的原因。



实验回顾

- 在实验室中，您通过使用动态主机配置协议（DHCP）配置VPN服务器来分配IPv4地址。是否有任何其他选项分配IPv4地址到客户端？
- 在练习1，任务3，您配置了允许IT组的成员连接到A.基准的VPN服务器的网络策略。如果您没有创建该策略，您是否可以连接？
- 在故障排除练习中，您将AdatumCA根证书手动导入受信任的根证书颁发机构存储
- LON-CL1。是否可以自动化此过程？



模块回顾和作业

- 复习题
- 工具
- 最佳实践



- 感谢大家！
- 也欢迎大家加入我们的技术交流群，我会定时将课程资料下发到群里，供大家下载学习。
- 也请大家持续关注我们的公众号！
- 最后祝大家学习顺利！再次感谢！

