



# Microsoft

MCSA

Windows Server 2016实现和管理

程尊华



# Module 6

Windows Server 2016的远程访问

# 模块概览

- 远程访问概述
- 实施Web应用程序代理



# 第1课：远程访问概述

- 讨论：何时使用远程访问
- 远程访问选项
- 在Windows Server 2016中管理远程访问
- 演示：安装和管理远程访问服务器角色
- 什么是网络策略服务器？
- 网络策略服务器策略
- 演示：配置网络策略服务器策略
- 部署用于远程访问的PKI的注意事项
- 配置路由和NAT与远程访问角色



# 讨论：何时使用远程访问

- 您是否允许用户远程连接到您的网络资源？如果是这样，怎么办？
- 您使用远程访问的业务需求是什么？



10 minutes



# 远程访问选项

- DirectAccess
- VPN
- 路由
- Web应用程序代理



# 在Windows Server 2016中管理远程访问

您可以使用以下方式来管理远程访问服务器角色：

- 远程访问管理控制台
- 路由和远程访问控制台
- Windows PowerShell命令：
  - **Set-DAServer**
  - **Get-DAServer**
  - **Set-RemoteAccess**
  - **Get-RemoteAccess**



# 演示：安装和管理远程访问服务器角色

- 在此演示中，您将看到如何：
  - 安装远程访问服务器角色
  - 管理远程访问服务器角色





# 什么是网络策略服务器？

- Windows Server 2016中的网络策略服务器提供以下功能：
  - RADIUS服务器。网络策略服务器对无线，认证交换机，拨号和VPN连接进行集中连接认证，授权和计费
  - RADIUS代理。您配置连接请求策略，指示网络策略服务器将转发到其他RADIUS服务器的哪些连接请求以及要转发连接请求的RADIUS服务器

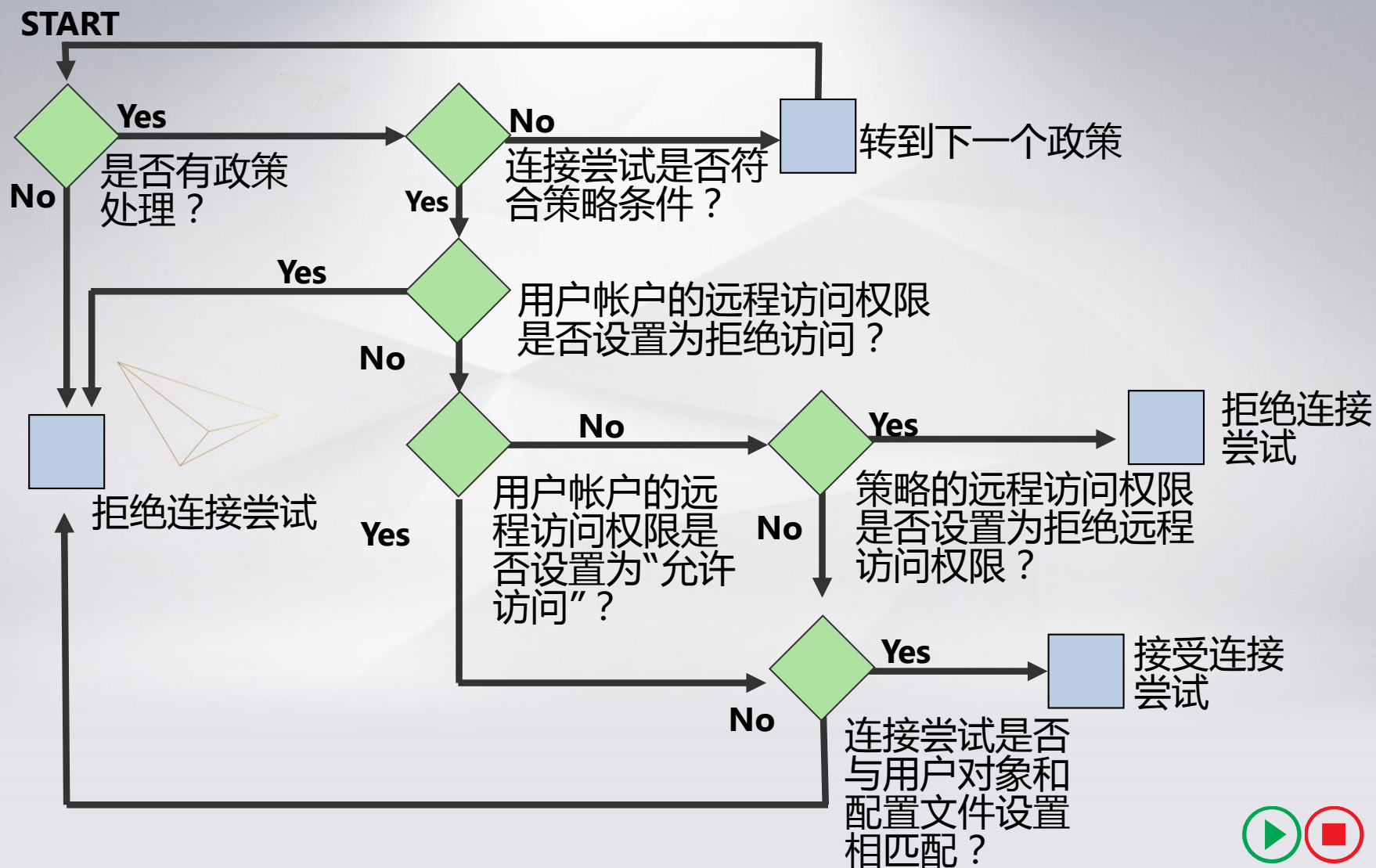


# 网络策略服务器策略

- 网络策略服务器支持管理和控制来自远程访问客户端的连接的策略
- 存在两种类型的策略：
  - 连接请求策略：
    - 当网络策略服务器作为RADIUS服务器或RADIUS代理时使用
  - 网络政策：
    - 用于认证和授权连接尝试
- 您设置条件和约束来控制访问
- 首次部署网络策略服务器时，远程访问被拒绝，您必须至少配置一个策略以允许访问



# 网络策略服务器策略



# 演示：配置网络策略服务器策略

在此演示中，您将看到如何配置远程访问策略



# 部署用于远程访问的PKI的注意事项

- 您是否会使用PKI加密数据和流量？
- 您是否会使用PKI不仅用于加密，还可用于验证用户及其计算机？
- 您是否会使用自签名证书，内部私人CA或外部公共CA提供的证书？



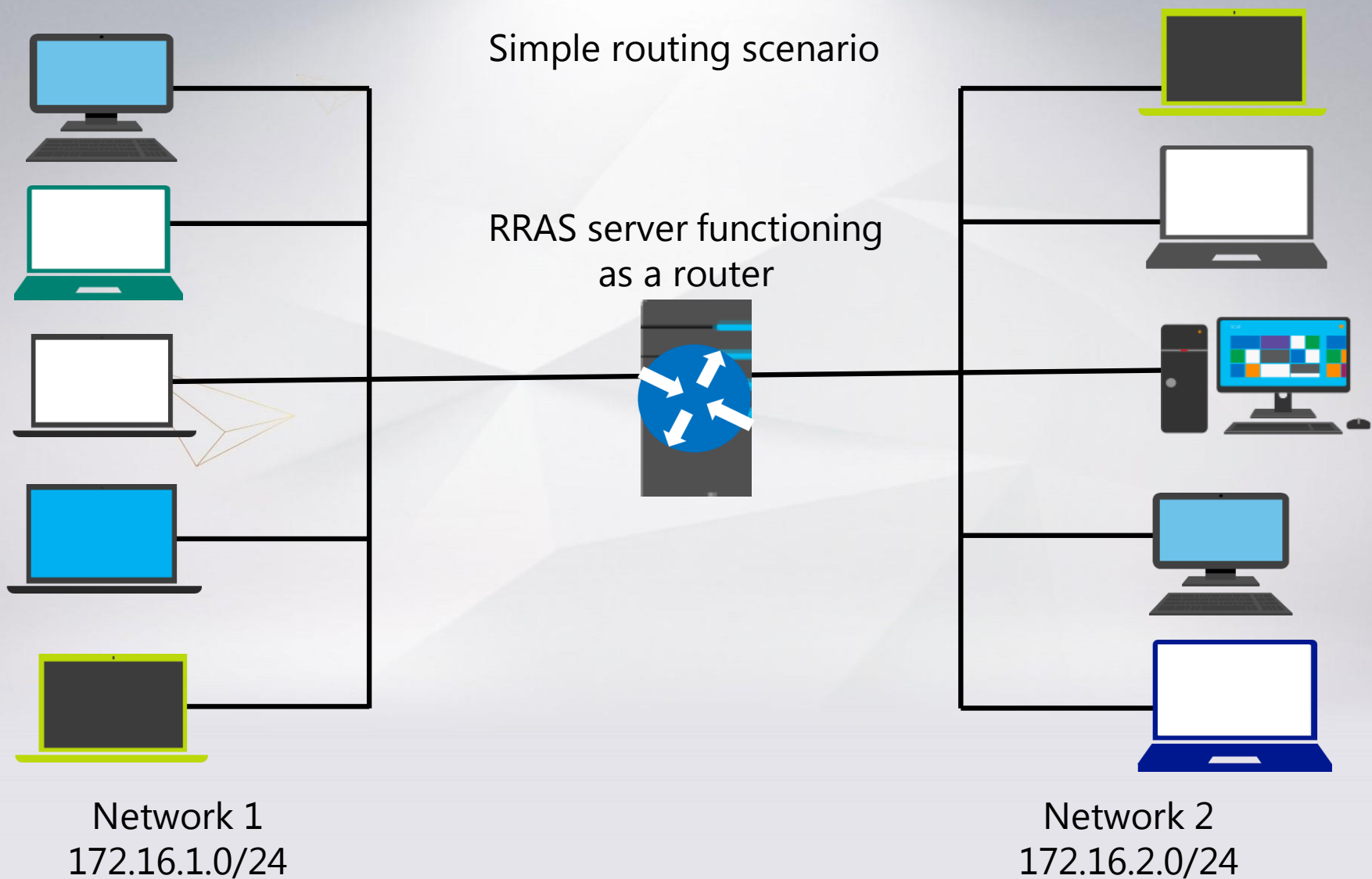
# 配置路由和NAT与远程访问角色

## RRAS路由：

- RRAS是基于软件的路由器
- 可以路由LAN到LAN，LAN到WAN，请求拨号和NAT流量
- 支持以下类型的路由：
  - 静态路由（IPv4 / IPv6）
  - IGMP（IPv4）
  - RIP（IPv4）
  - NAT（IPv4）
- 是在一个中小型网络实施简单网络通讯路由的选项

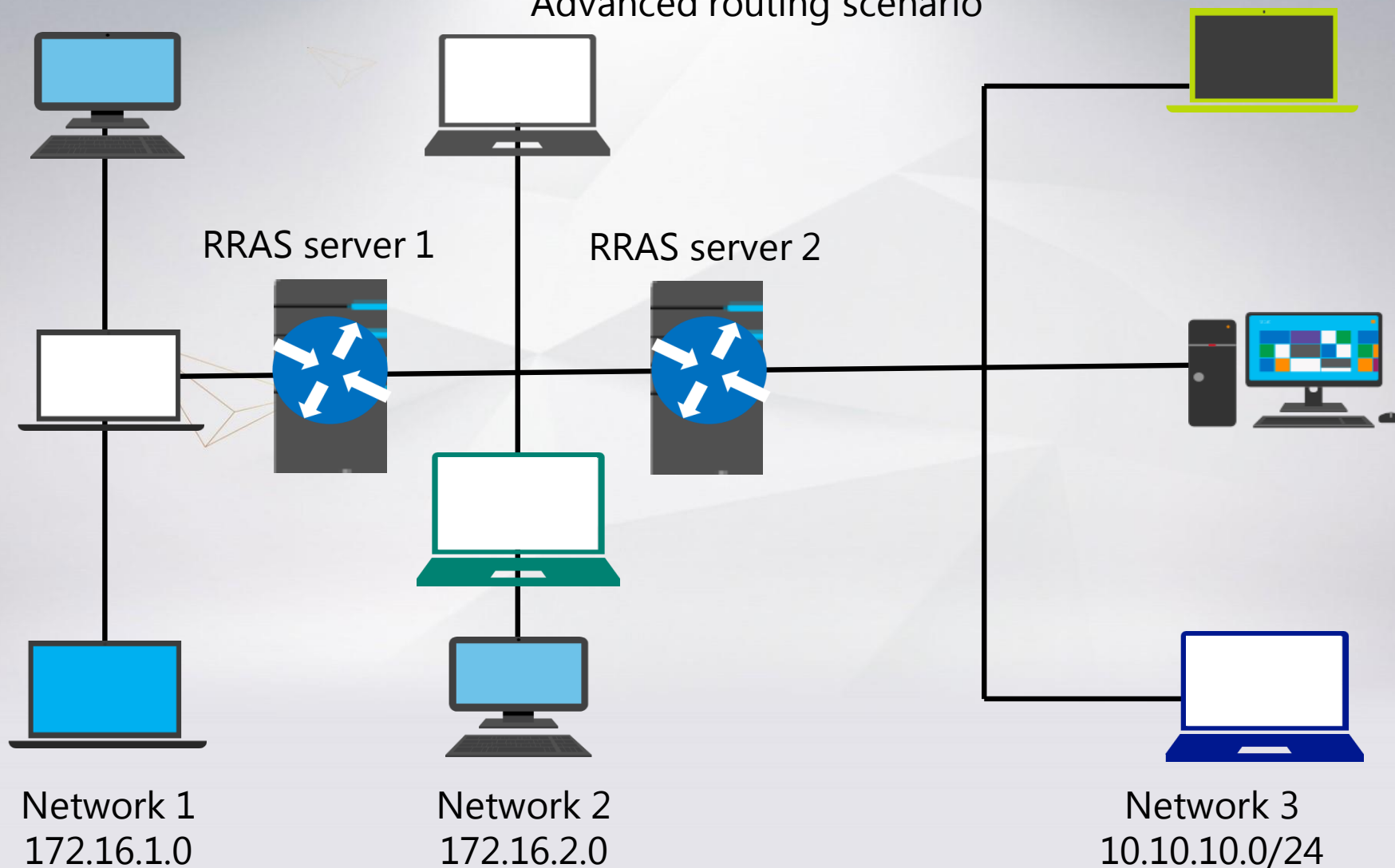


# 配置路由和NAT与远程访问角色



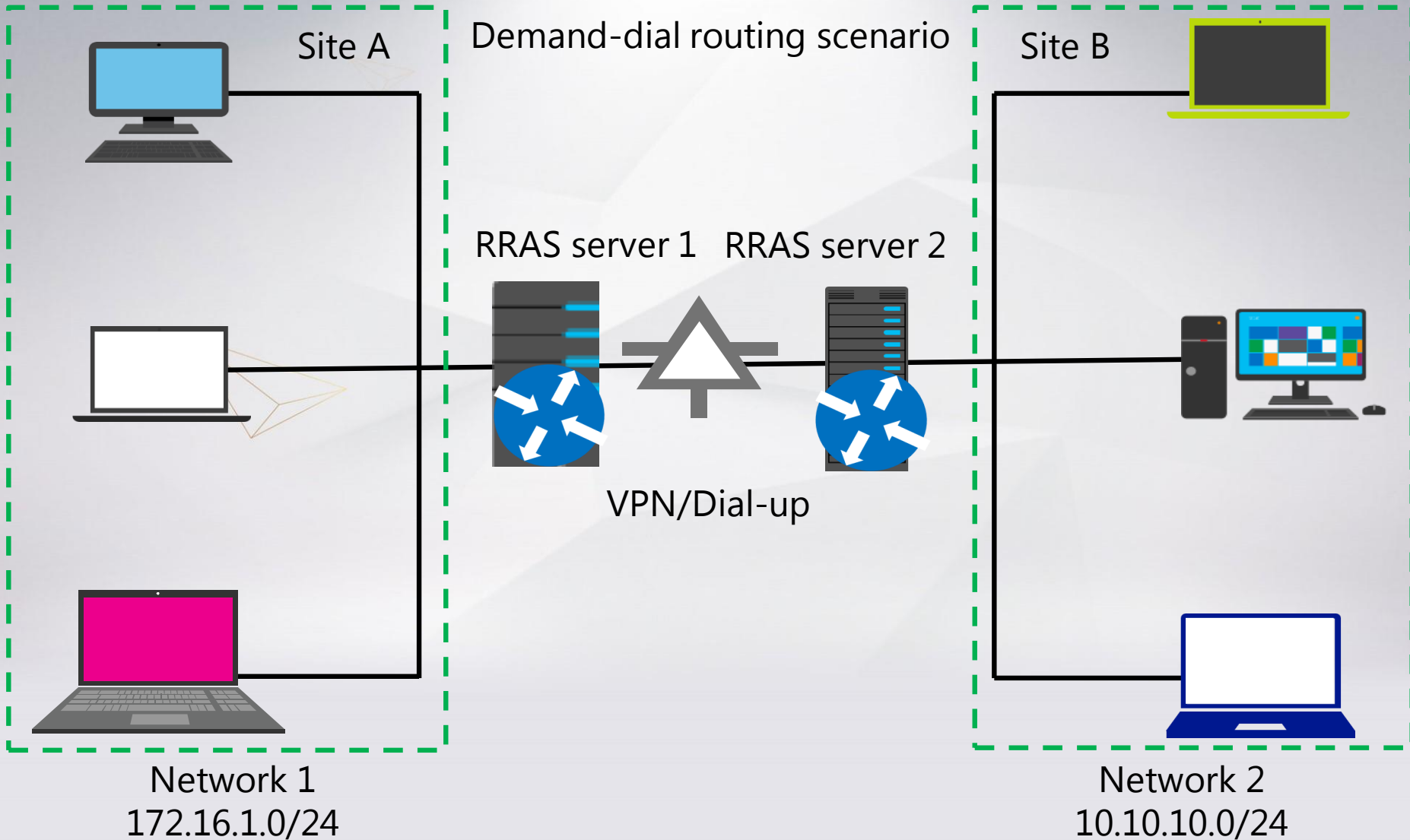
# 配置路由和NAT与远程访问角色

Advanced routing scenario

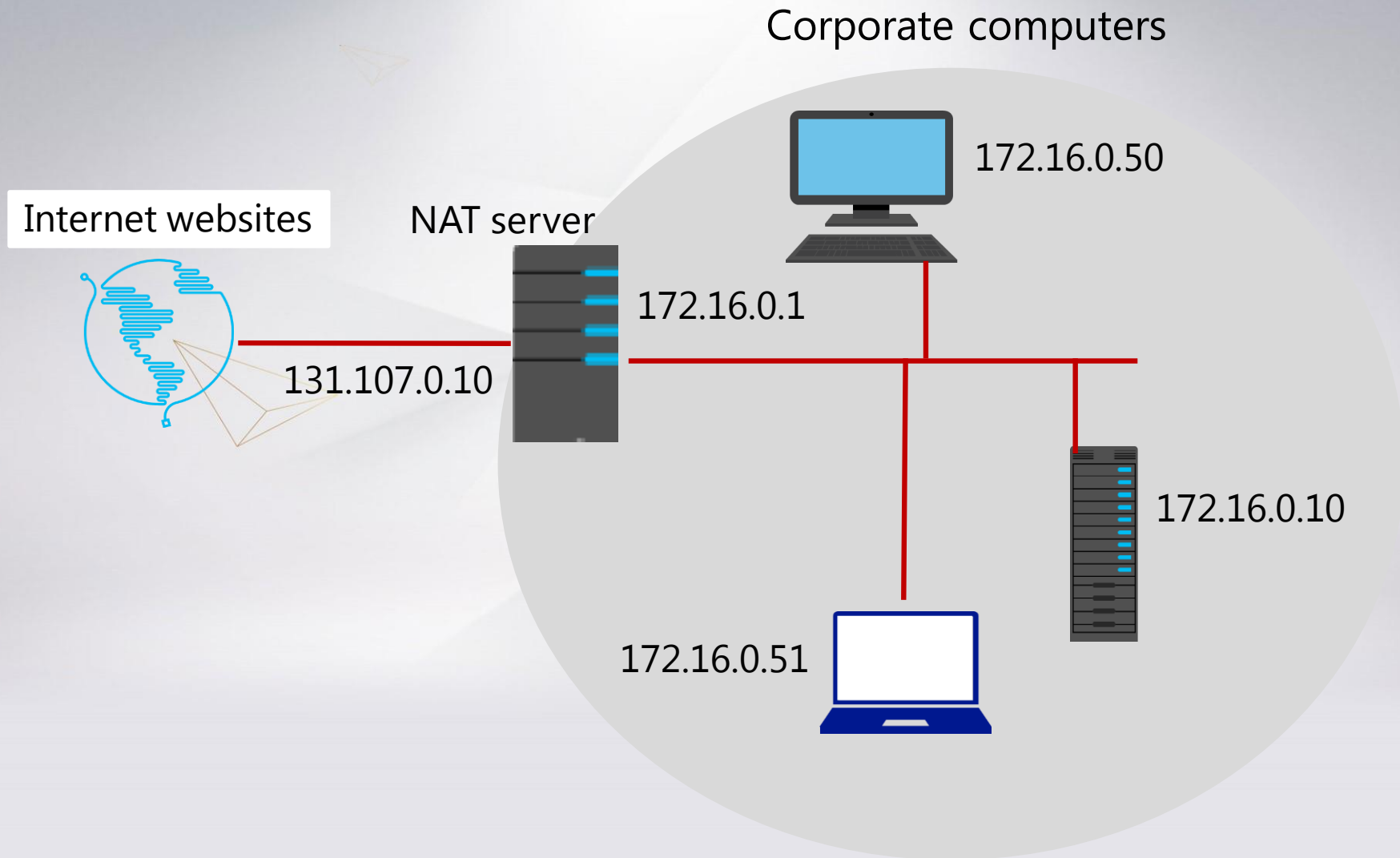




# 配置路由和NAT与远程访问角色



# 配置路由和NAT与远程访问角色



## 第2课：实施Web应用程序代理

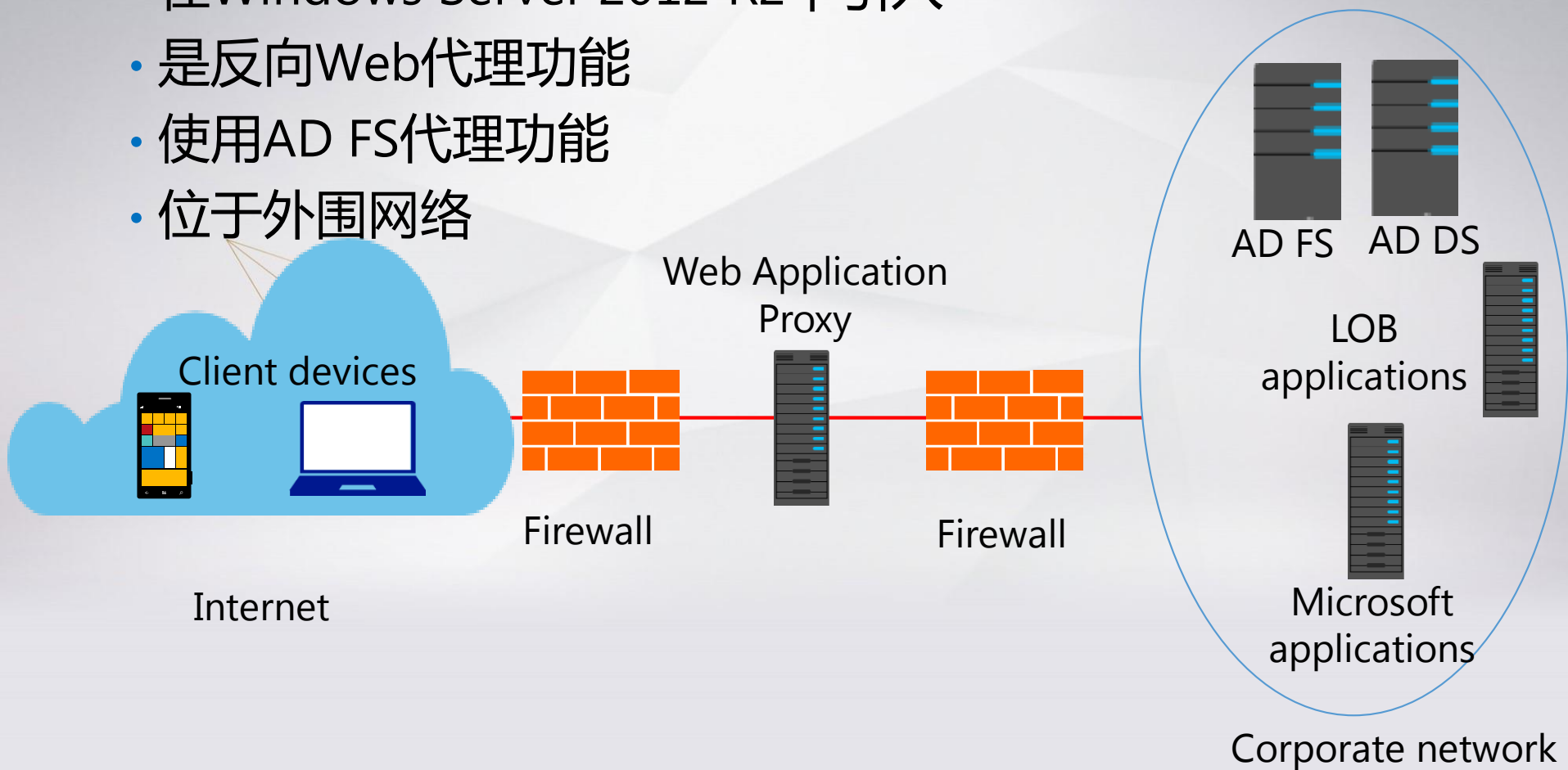
- 什么是Web应用代理？
- Web应用程序代理的验证选项
- 使用Web Application Proxy发布应用程序
- 演示：发布安全网站



# 什么是Web应用代理？

## Web应用代理：

- 在Windows Server 2012 R2中引入
- 是反向Web代理功能
- 使用AD FS代理功能
- 位于外围网络



# Web应用程序代理的验证选项

- 用户认证：
  - AD FS预认证
  - 传递预认证
- AD FS优点：
  - Workplace join
  - SSO
  - 多重认证
  - 多因素访问控制



# 使用Web Application Proxy发布应用程序

- 配置Web应用程序代理设置：

- AD FS服务器名称
- AD FS管理员凭据
- AD FS证书



# 使用Web Application Proxy发布应用程序

- 发布Web应用程序：
  - 预认证的类型 - 例如，直通
  - 将被发布的应用程序
  - 应用程序的外部URL - 例如，https://lon-svr1.adatum.com/
  - 证书，其主题名称涵盖了外部URL - 例如，lon-svr1.adatum.com
  - 后端服务器的URL



# 使用Web Application Proxy发布应用程序

- 发布远程桌面网关：
  - 预认证的类型 - 例如，直通
  - 将被发布的应用程序
  - 应用程序的外部URL - 例如，<https://rdgw.adatum.com/>
  - 证书，其主题名称涵盖了外部URL - 例如，[rdgw.adatum.com](https://rdgw.adatum.com/)
  - 后端服务器的URL





# 演示：发布安全网站

- 在此演示中，您将学习如何：
  - 安装Web应用程序代理角色服务
  - 配置对内部网站的访问
  - 验证从客户端计算机访问内部网站



# 实验：实现Web应用程序代理

- 练习1：实现Web应用程序代理
- 练习2：验证Web应用程序代理部署

## 登录信息

虚拟机:



**20741B-LON-DC1**

**20741B-LON-SVR1**

**20741B-LON-SVR2**

**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: 70 minutes



# 实验场景

远程访问部署在A.基准公司运作良好，但IT管理还希望能够访问一些内部应用程序合作伙伴公司的用户。这些用户不应该访问任何内部资源除了指定的应用程序。您必须实现和测试Web应用程序代理为这些用户。此外，在由A. Datum管理员应该能够尽可能以最安全的方式来远程管理内部网络中的服务器。



# 实验回顾

- 应该在哪里部署Web应用程序代理服务器？
- 客户访问发布的Web应用程序需要什么？



# 模块回顾和作业

- 最佳实践
- 复习题
- 工具



- 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！

