Securing Windows Server 2016, Part 5 of 5: Securing Network Infrastructure

Meet the expert: Patrick Loner has certifications for MCSA, MCSE, MCITP, A+, Network+, Security+, and more. He has been working as a Microsoft Certified Trainer, network administrator, and network consultant for over ten years. He has over a decade of experience working with and teaching about Windows networks with client and server operating systems. He has guided many students toward Microsoft and CompTIA certifications. Most recently, he has worked as a freelance trainer and network consultant specializing in Windows Server 2008 and Microsoft Exchange 2007 and Exchange 2010 implementations, design, and upgrades. Patrick continues to branch out now working with and training on Windows Server 2012, Windows 8, Exchange 2013, and System Center Configuration Manager 2012.

Prerequisites: This is Part 5 of the series

Runtime: 02:10:12

Course description: Securing network Infrastructure is the pathway through all communication. Beginning with firewalls and the Windows firewall with advanced security, this course takes a look at the datacenter firewall especially with multi-tenant environments. Other topics include: IPsec Usage, Authentication methods, DNS security, DNS Policies, RRL, and rounds out with Microsoft Message Analyzer to scan traffic and options for SMB traffic.

Course outline:

Windows Firewall
- Introduction
- Types of Firewalls
- Well-Known Ports
- Host-Based Firewall
- Network Profiles
- Configuring the Windows Firewall
- Demo: Configure the Firewall via Control Panel
- Demo: Windows Firewall with Advanced Security
- Demo: Configure the Firewall via PowerShell
- Demo: Configure the Firewall be GPME
- Summary

Datacenter Firewall
- Introduction
- Network Controller
- Datacenter Firewall
- Network Security Groups
- Scenarios for Datacenter Firewall
- Summary

Utilizing IP Security
- Introduction
- Overview of IP Security
- IPSec Protocols
- IPSec Usage Scenarios
- IPSec Configuration Tools
- Connection Security Rules
- Understanding Rule Types
- Rule Endpoints
- Authentication Settings
- Authentication Methods
- Encryption Settings
- Monitoring Connections
- Demo: Implementing IPSec
- Demo: Protocols
- Summary

Advanced DNS Settings
- Introduction
- Managing DNS Services
- Optimizing DNS Name Resolution
- The GlobalNames Zone
- Implementing DNS Security
- DNS Security (DNSSEC)
- Implementing DNSSEC
- Demo: DNSSEC
- Demo: Validating Responses
- Introducing DNS Policies
- Implementing DNS Policies
- RRL Feature
- Demo: Configure DNS Policies
- Demo: RRL
- Summary

Monitoring Network Traffic
- Introduction
- Microsoft Message Analyzer
- Demo: MMA
- Summary

Securing SMB Traffic
- Introduction
- SMB 3.1.1 Protocol Security
- SMB Encryption Requirements
- Encrypting SMB Shares
- Disabling Support for SMB 1.0
- Summary