Microsoft® Official Course

Module10

Implementing Network Security

Microsoft®

Module Overview

- Overview of Network Security
- Implementing Firewalls
- Internet Protocol Security

Lesson 1: Overview of Network Security

- Network Security Threats
- Mitigating Network Security Threats

Network Security Threats

- There are a variety of network security threats, but they fall into a number of categories
- Common network-based security threats include:
  - Eavesdropping
  - Denial-of-service
  - Port scanning
  - Man-in-the-middle
  - Replay Attacks
- Hacking is a generic term that means any type of network attack

Mitigating Network Security Threats

- It is important to implement a holistic approach to network security to ensure that one loophole or omission does not result in another

Attack	Mitigation
Eavesdropping	IPsec, VPNs, intruder detection
Denial-of-service	Firewalls, perimeter networks, IPsec, server hardening
Port scanning	Server hardening, firewalls
Man-in-the-middle	IPsec
Replay Attacks	IPsec, Session tokens, One-Time Passwords,

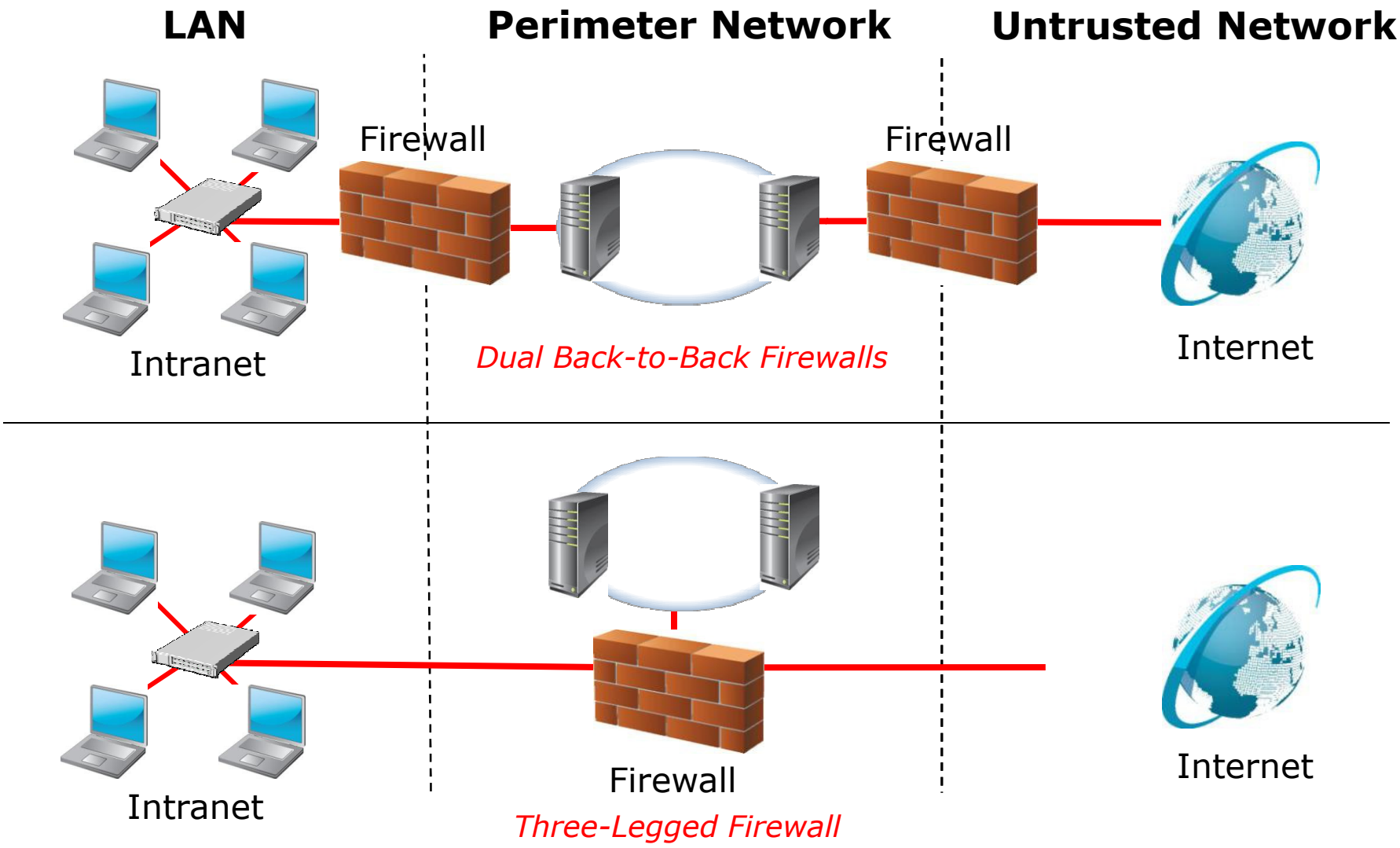
Lesson 2: Implementing Firewalls

- Firewall Types
- What Is a Perimeter Network?
- What Is Windows Firewall?
- Network Location-Aware Profiles
- Configuring Windows Firewall with Advanced Security
- Demonstration: How to Use Windows Firewall to Manage Inbound Network Traffic

Firewall Types

- Firewalls can be installed on hosts, such as Windows Server, or implemented as software in devices such as routers
- There are different types of firewalls:
  - Application-layer gateways
  - Circuit-level gateways
  - Packet filters
  - Stateful multilayer inspection

What Is a Perimeter Network?



What Is Windows Firewall?

- Windows Firewall is a host-based, stateful firewall that provides:
  - Management via:
    - Control Panel
    - Windows Firewall with Advanced Security management console
    - Group Policy
    - Windows PowerShell “NetSecurity” module
  - Network location-aware profiles
  - Granular configuration through inbound and outbound rules
  - IPsec integration

Network Location-Aware Profiles

- The first time that your server connects to a network, you must select a network location
- There are three network profiles:
  - Domain networks
  - Private networks
  - Public networks
- It is also possible to create and join Homegroups to allow the sharing of files and printers between computers and devices on a private home network

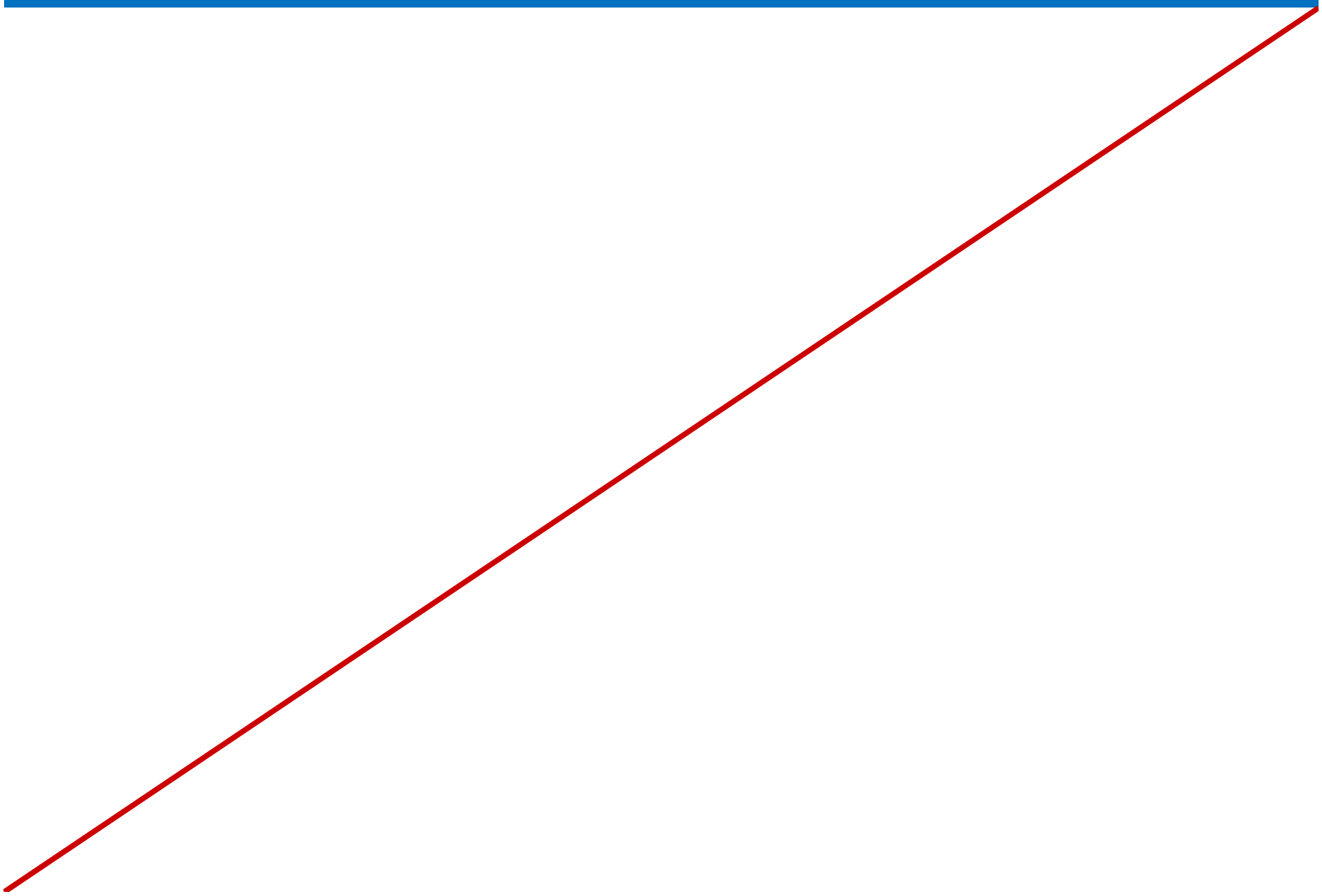
Configuring Windows Firewall with Advanced Security

- Inbound and outbound rules define which traffic you will allow, block, or secure
- There are four types of rules:
  - Program rules
  - Port rules
  - Predefined rules
  - Custom rules
- Connection security rules complement the firewall rules

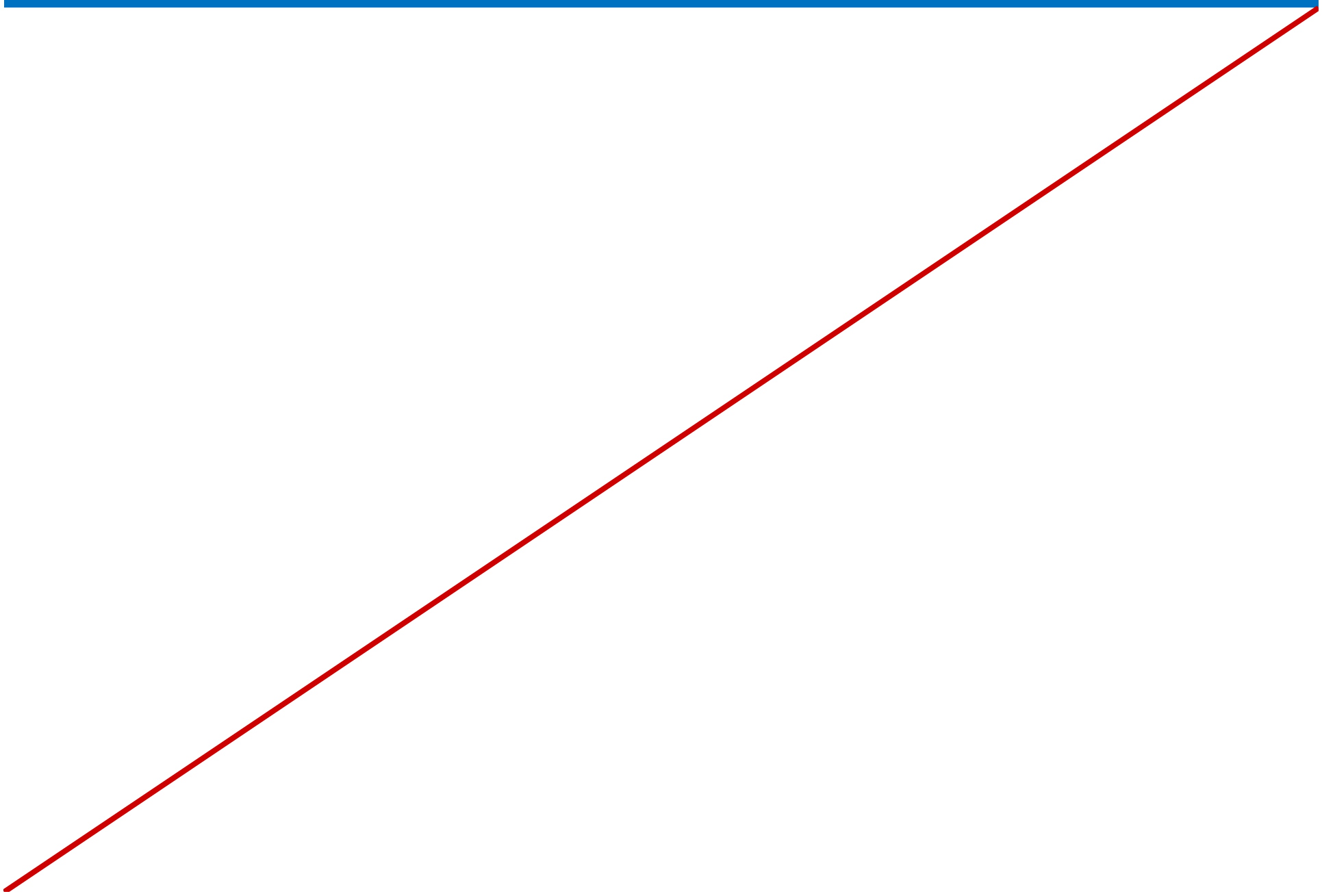
Demonstration: How to Use Windows Firewall to Manage Inbound Network Traffic

- In this demonstration, you will see how to create and test an inbound firewall rule

Notes Page Over-flow Slide. Do Not Print Slide.



Notes Page Over-flow Slide. Do Not Print Slide.



Lesson 3: Internet Protocol Security

- What Is IPsec?
- Implementing IPsec
- Connection Security Rules
- Managing IPsec
- Demonstration: Create Server to Server Connection Security Rule

What Is IPsec?

- IPsec is a suite of protocols that allows secure, encrypted communication between two computers over an unsecured network
- IPsec provides:
  - Network-level peer and data origin authentication
  - Data integrity and confidentiality
  - Protection from replay attacks

- IPsec policies define the type of traffic that IPsec examines, how that traffic is secured and encrypted and how IPsec peers are authenticated

Implementing IPsec

- Implementing IPsec can provide:
  - Packet Filtering
  - Security for host to host traffic
  - Security for traffic to servers
  - Secure VPNs
  - Site to site tunneling
  - Server/Domain isolation
- IPsec should not be used for:
  - Securing communication between domain member and Domain Controllers
  - Securing All network traffic

Connection Security Rules

Rule Type	Description
Isolation	• Restricts connections based on authentication criteria that you define
Authentication Exemption	• Exempts specific computers, or a group or range of IP addresses, from being required to authenticate • Grants access to those infrastructure computers with which this computer must communicate before authentication occurs
Server-to-Server	• Authenticates two specific computers, two groups of computers, two subnets, or a specific computer and a group of computers or subnet
Tunnel	• Provides secure communications between two peer computers through tunnel endpoints (VPN or L2TP IPsec tunnels)
Custom	• Enables you to create a rule with special settings

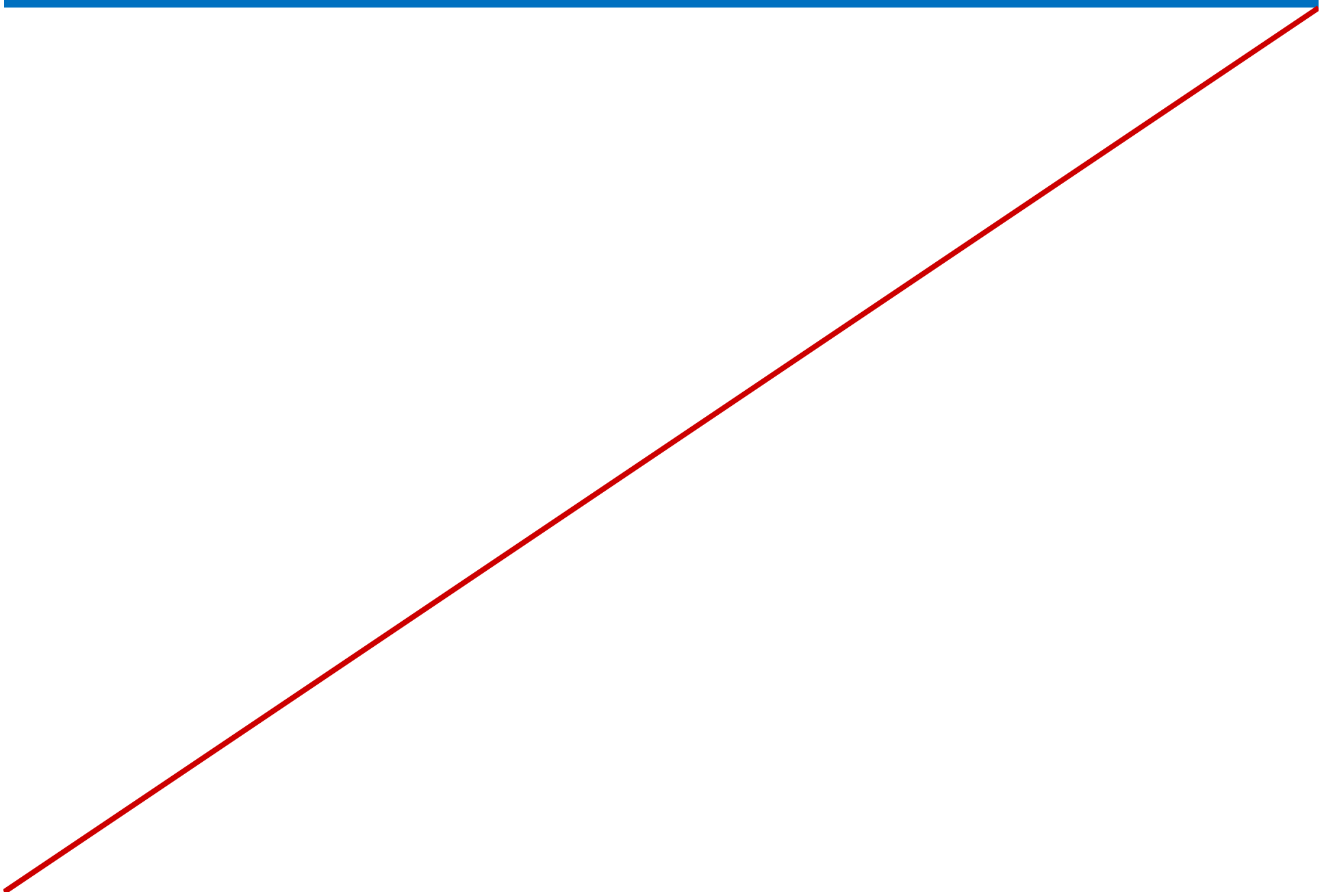
Managing IPsec

- Windows Firewall with Advanced Security
  - Configuration of Firewall rules and IPsec settings in a single interface
- IPsec Policy mmc snap-in
  - Used for mixed environments where there are legacy versions if Windows present i.e. pre Windows Server 2008
- Windows PowerShell
  - Allows for granular and automated management for local and remote computers

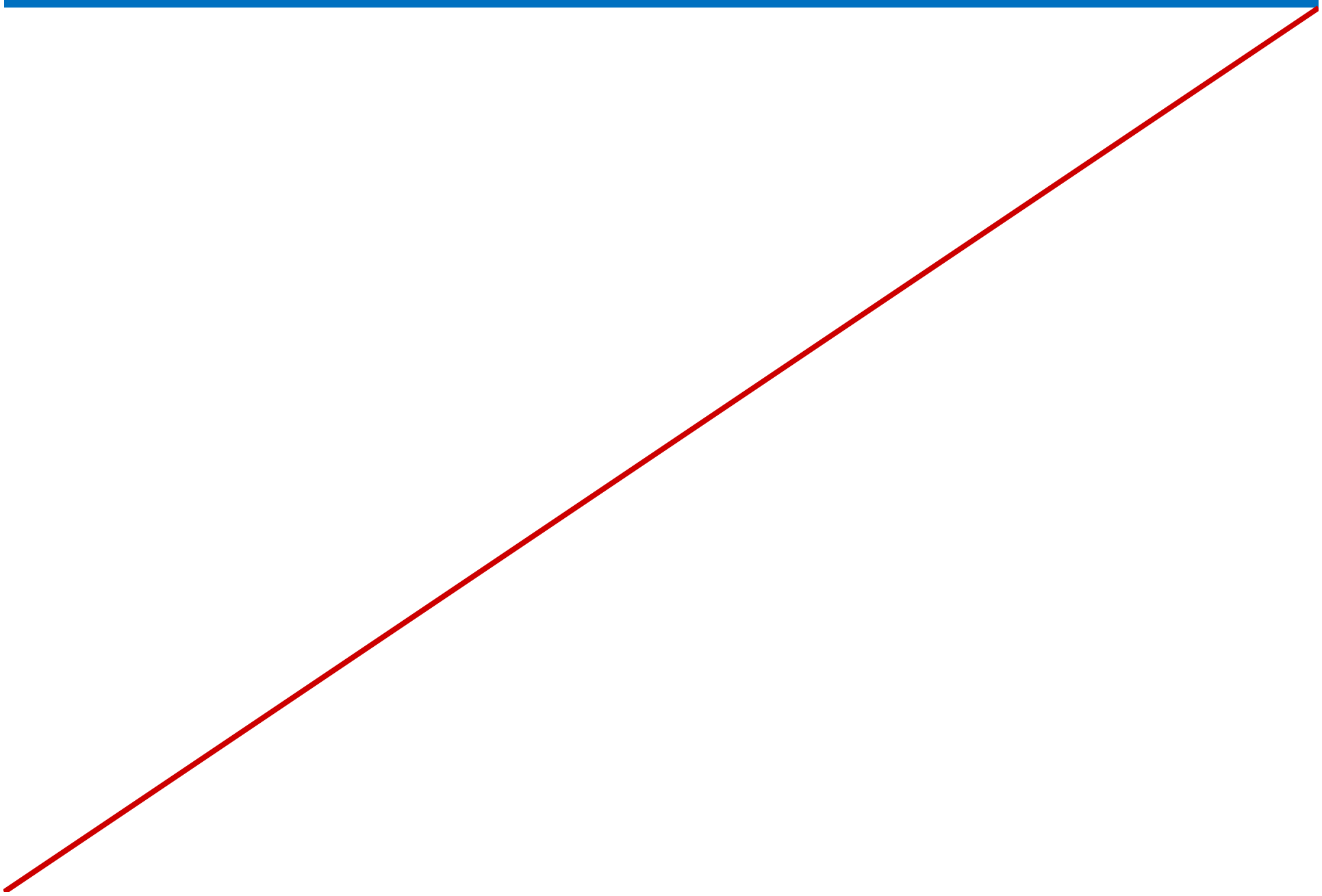
Demonstration: Create Server to Server Connection Security Rule

- In this demonstration, you will see how to create an Server to Server connection security rule

Notes Page Over-flow Slide. Do Not Print Slide.



Notes Page Over-flow Slide. Do Not Print Slide.



Lab: Implementing Network Security

- Exercise 1: Configuring Windows Firewall with Advanced Security
- Exercise 2: Create a Server to Server Connection Security Rule

Logon Information
Virtual Machines: 10967A-LON-DC1, 10967A-LON-SVR1 and 10967A-LON-CL1
User Name: ADATUM\Administrator
Password: Pa$$w0rd

Estimated Time: 60 minutes

Lab Scenario

Ed Meadows is looking to make available the Intranet web site for project queries. He has asked you to test the configuration and to create Firewall rules to make sure that access can be granted and blocked if needed. He has supplied the requirements in an email message. You must read the requirements and then implement them on a client computer.

Lab Review

- If you wanted to make sure that only domain computers could communicate with other domain computers, how could you easily achieve this with Windows Firewall?

Module Review and Takeaways

- Review Questions
- Tools
- Best Practice