REVIEW LESSON

MTA Course: 98-367 Security Fundamentals
Lesson name: Understand Network Security
Topic: Understand dedicated firewalls
(One 50-minute class period)
File name: SecurityFund_RL_3.1

Lesson Objective

3.1: Understand dedicated firewalls. *This objective may include, but is not limited to:* types of firewalls and their characteristics, when to use a hardware firewall instead of software firewall, stateful vs. stateless inspection.

Preparation Details

Instructor preparation activities

- Make copies of Student Activity SecurtyFund_SA_3.1.

Resources, software, and additional files needed for this lesson

- SecurityFund_PPT_3.1
- SecurityFund_SA_3.1
- SecurityFund_SA_3.1_Key

Teaching Guide

Essential Vocabulary

application firewall—in the context of computer networking, an application-level gateway (also known as ALG or application layer gateway) consists of a security component that augments a firewall or NAT employed in a computer network. It allows customized NAT traversal filters to be plugged into the gateway to support address and

port translation for certain application layer "control/data" protocols such as FTP, Bit Torrent, SIP, RTSP, file transfer in IM applications, etcetera.

firewall—a security system intended to protect an organization's network against external threats, such as hackers, coming from another network, such as the Internet. Usually a combination of hardware and software, a firewall prevents computers in the organization's network from communicating directly with computers external to the network and vice versa.

gateway—a device that connects networks using different communications protocols so that information can be passed from one to the other. A gateway both transfers information and converts it to a form compatible with the protocols used by the receiving network.

packet filtering—the process of controlling network access based on IP addresses. Firewalls will often incorporate filters that allow or deny users the ability to enter or leave a local area network. Packet filtering is also used to accept or reject packets such as e-mail, based on the origin of the packet, to ensure security on a private network

proxy server—a firewall component that manages Internet traffic to and from a local area network (LAN) and can provide other features, such as document caching and access control. A proxy server can improve performance by supplying frequently requested data, such as a popular Web page, and can filter and discard requests that the owner does not consider appropriate, such as requests for unauthorized access to proprietary files.

Lesson Sequence

Activating prior knowledge/lesson staging (Anticipatory Set: 10 minutes)

1. Windows® Firewall (see PowerPoint slide 3)
    a. Have students open Control Panel.
    b. Click on Security Settings
    c. Click on Firewall to open
    d. Click on "How does a firewall protect my computer?"
    e. Close window and then click on Windows Firewall at the bottom of the open window.
    f. What is the current setting?
2. Give students a few minutes to research and respond, allowing them to work until they have finished.
3. As time permits, call on a few students to report to the group with their findings.

Lesson activity (40 minutes, slides 4–10) (Student handout – SecurityFund_SA_3.1)

1. Teacher Instruction (20 minutes)
   - Use the included PowerPoint® slideshow to review the advantages and disadvantages of hardware and software firewalls.
   - (Student handout – SecurityFund_SA_3.1) At the end of the slideshow, ask the students to research how to:
     - Identify the features necessary in your perimeter firewall.
     - Classify firewall products.
     - Select the best firewall product for your perimeter firewall.
   - Give the students 5 to 10 minutes to discuss findings with a partner.
   - Finally, have each pair of students share their findings with the whole group.
2. Guided Practice (20 minutes) Datamation: Security/Firewalls – Product Listing and Comparisons *(http://products.datamation.com/security/firewalls/)*
   - Ask students to do some research on low-cost firewalls suited for home and small businesses. Identify which of these have NAT functions.
   - If time allows, you may review all or part of the information, discussing student responses to the research.

Assessment/lesson reflection (10 minutes)

1. The last slide in the PowerPoint facilitates this exercise (slide 14).
2. On a piece of paper, tell students to summarize why a firewall should be a part of an overall security plan, not the ONLY form of protection for a LAN.
   - Be sure to give ample time for students to write their summaries.
   - If time allows, pick a few students to read their summaries.
3. At the bottom of the page, tell students to write any questions they have or any topics about which they would like more assistance
4. After class, look through the student responses and follow up with any student requiring additional help.

Microsoft® resources and Web links

- **Understanding Windows Firewall**
  http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx
- **TechNet: Perimeter Firewall Design**
  http://technet.microsoft.com/en-us/library/cc700828.aspx
- **TechNet: Firewalls**
  http://technet.microsoft.com/en-us/library/cc700820.aspx
- **Datamation: Security/Firewalls – Product Listing and Comparisons**
- *http://products.datamation.com/security/firewalls/*