

Week #4 – Firewalls

Overview of the week's objectives

Networked computers are under constant threat from unauthorized users, rogue programs, and malicious scripts intent on exploiting holes in the network, protocol, or computer systems. One tool that system administrators use to help with network security is a firewall. Understanding firewalls and the rules that allow them to be effective is a necessary skill for any aspiring administrator. A misconfigured firewall can block legitimate traffic. Conversely, a well-configured firewall can minimize risks. In this lesson, you will learn to use and configure a firewall securely.

Please refer to “Week #2’s Overview PDFs” for details / advice relating to, or concerning, each of the tasks detailed in the remainder of this overview. You are responsible for recommendations or instructions noted in ALL PREVIOUS WEEK’s OVERVIEWS! Do review them!

TODO List

Please refer to “Week #2’s Overview PDF” for details / advice about each of the tasks detailed in the remainder of this overview. While we focus on instructions specific to this week’s material herein, previous instructions still apply.

Learning Activity			Time in hours		Points
			Expected	Spent	
Reading Assignments	O5L8	Online Module Guides & Videos	2		
Practice Assignments	O5L8-PQ	Taking Practice Quizzes	1		
	W4-PA	Working on PAs & Participating to PA forums	8		
Graded Assignments	W4-GQ	Taking Graded Quiz	1		2
		Participating to Discussion forums			1
			12		3

Task #1 – Reading Assignments

You will find one “[online module guide](#)” document in this week’s folder per module.

Refer to “Week #2’s Overview PDF” for detailed instructions on how to use [online module guides](#), [practice quizzes](#) and our [support forum](#) while working on this task.

Task #2 – Practice Assignments

Refer to “ALL PREVIOUS WEEK’s Overview PDF” files for detailed instructions applying to all Practice Assignments.

These activities were designed to help you think critically about the topics covered in this lesson and to assess whether your knowledge and application of the content meets the stated objectives. You will need to research each topic and complete the assignment as instructed. Do not rely only on the contents of this lesson or on Wikipedia to complete these assignments.

PA #1 : Report – Types of Firewalls (C5L8A1)

Write a compare/contrast paper that explores four different types of firewalls and the application of each. Use Internet references as your sources. Do not use Wikipedia or blogs as sources. Be sure it is your own work! Take notes, reorganize them, and present a written report in your own words and even include a few paragraphs in your report of your own personal interpretation based on the factual information.

Upload to the drop box using standard naming conventions for credit.

PA #2 : Lab – Firewall Form Lesson (C5L8A2)

Setup a network layer firewall using the exact instructions provided in this lesson. After creating your firewall, use NMAP to check your firewall settings and security.

Take a screen capture showing the use of NMAP to test your firewall.

Gather the following two files:

- **rc.firewall**
- **/etc/sysconfig/iptables**

Combine the two files (above) and the screen capture into a tar.bz2 archive.

Upload this archive file to the drop box using the standard naming convention of: *firstname_lastname_course5_lesson8_lab1.tar.bz2* to receive credit.

PA #3 : Lab – Allow Incoming Traffic to Apache Server (C5L8A3)

Change your firewall to allow incoming traffic to your test machine's web server (Apache). Start your web server and capture the screen showing you browsing to it from another machine.

Create a tar.bz2 archive with this screen shot, an NMAP port scan, and the **/etc/sysconfig/iptables** file.

Upload this file using standard naming convention of:
firstname_lastname_course5_lesson8_lab2.gpg to receive credit.

PA#4 : Lab – Allow All Outbound Traffic (C5L2F2)

Change your firewall to allow ALL outbound traffic.
Leave the inbound traffic the same as Lab 2.
Capture the screen of you browsing to it from another machine.
Create a tar.bz2 archive with this screen shot, an NMAP port scan, and the **/etc/sysconfig/iptables** file.

Upload this file using standard naming convention of:
firstname_lastname_course5_lesson8_lab3.tar.bz2 to receive credit.

Task #3 – Use the “Support forum”

Refer to “Week #2’s Overview PDF” and “ALL PREVIOUS WEEK’s Overview PDF” for detailed instructions applying to all discussion forums assignments.

PA #5 : Forum – Extreme Firewall Settings (C5L8F1)

Is it possible for a system administrator to lock down a firewall too much? For example, could an administrator make it too difficult for users to get work done?

Give some examples of firewall settings that make it difficult to get work done.

Once you have responded to the question, respond constructively to two comments from your classmates.

PA #6 : Forum – Bypassing Firewalls (C5L8F2)

In what ways can a hacker get around a firewall and do damage to a machine?

Suggest two methods hackers may use and provide a solution, user Internet resources for your response.

Once you have responded to the question, respond constructively to two of your classmates.

Task #4 – Graded quizzes

Refer to “Week #2’s Overview PDF” and “ALL PREVIOUS WEEK’s Overview PDF” for detailed instructions applying to all graded quizzes.