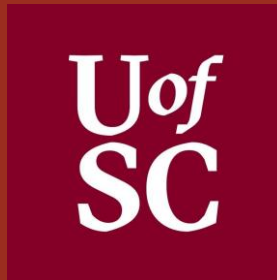


Protection Against Brute-Force Attacks



Lauren Waddell and Brendan Curran
University of South Carolina



Integrated Information Technology Department
USC ROTC

December 1, 2020

Agenda

- Overview
- Motivation
 - Advantages of NGFW
- Objectives
- Custom Scenario
- Mitigation
- Results
- Conclusion

Overview

A brute force attack uses a large volume of requests/responses from the same source or destination IP address to break into a system.

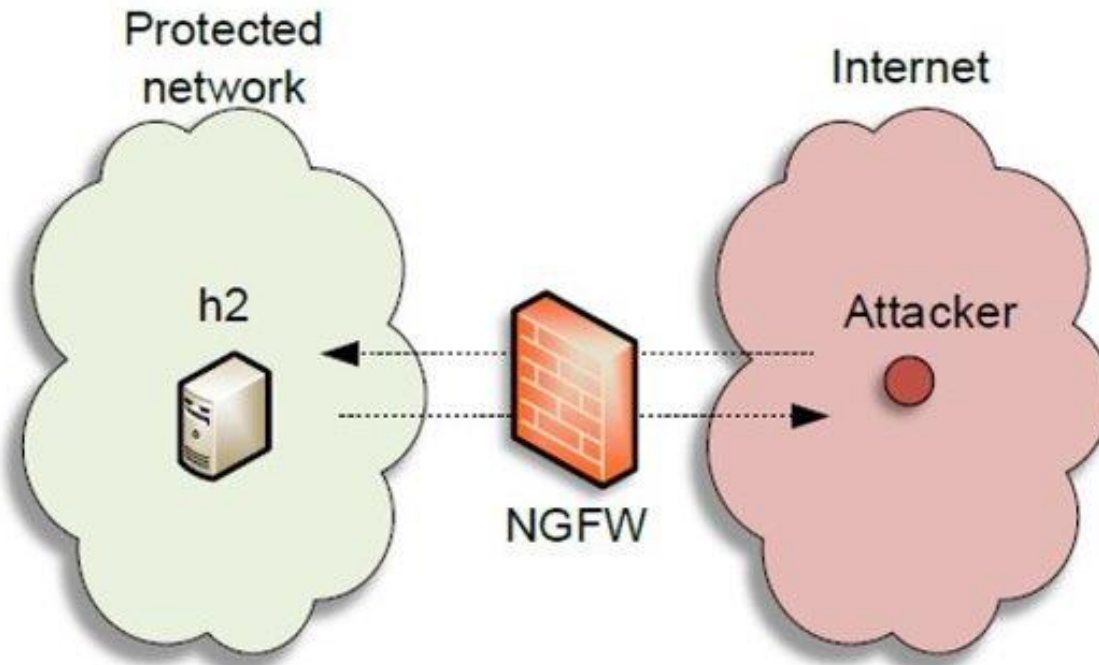
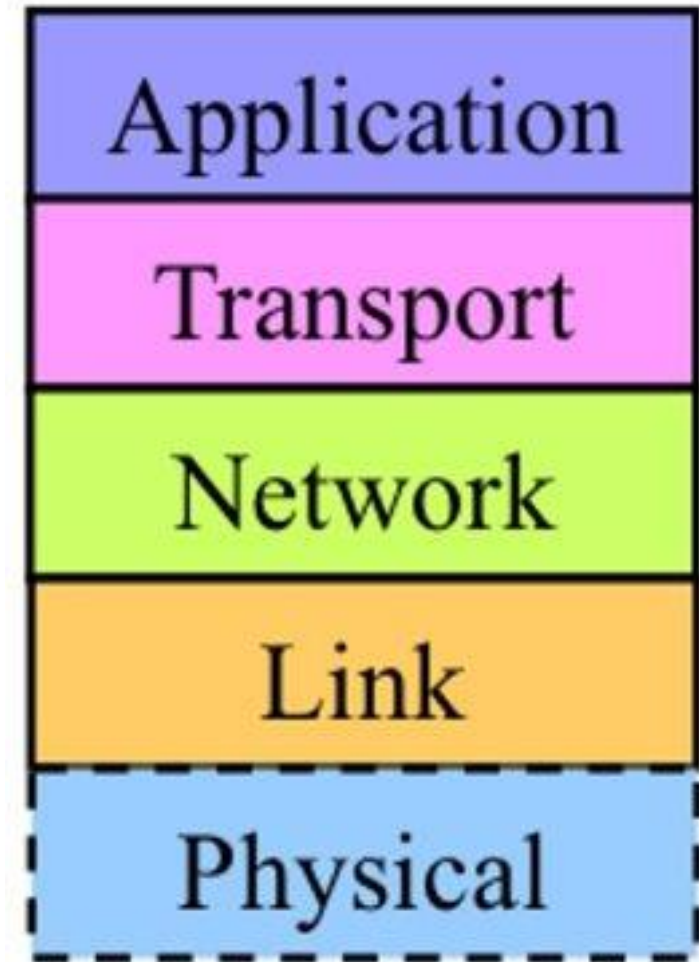


Figure 1. Network topology.

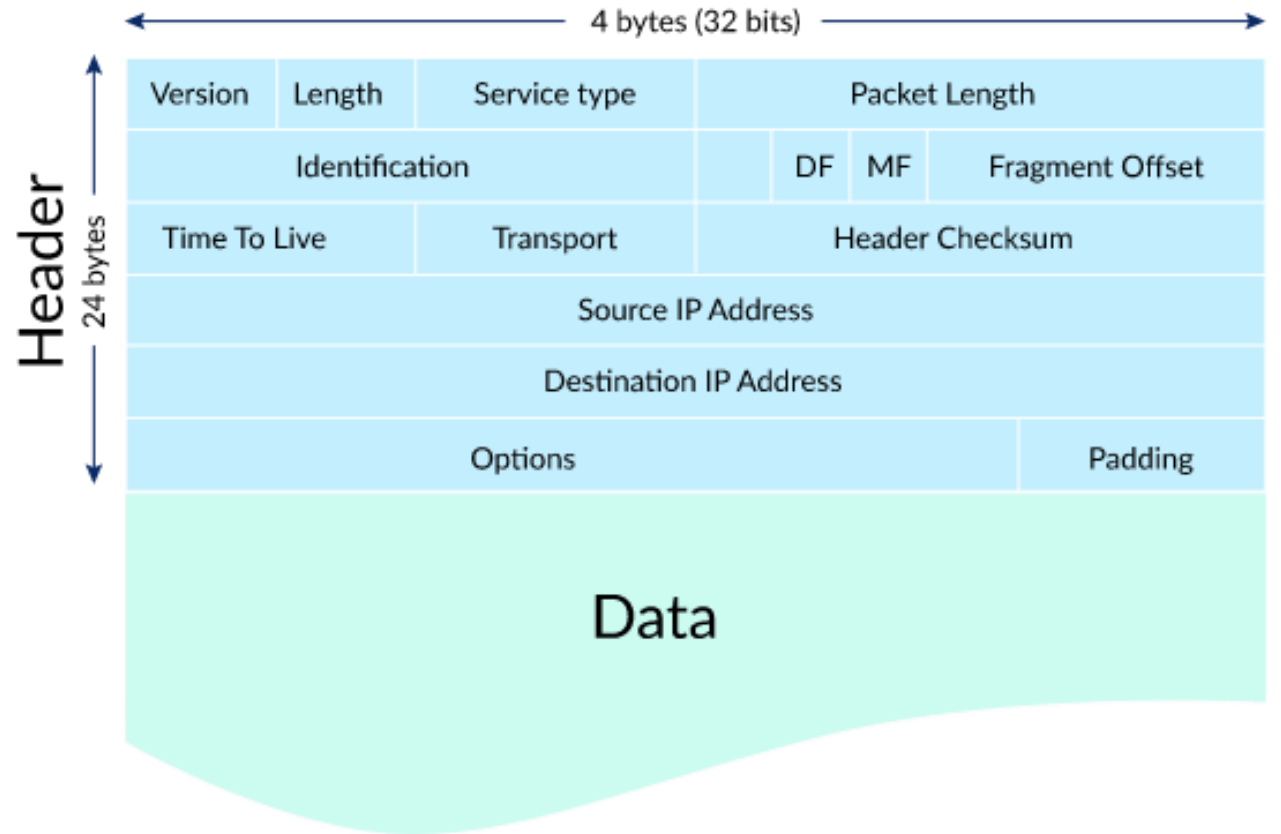
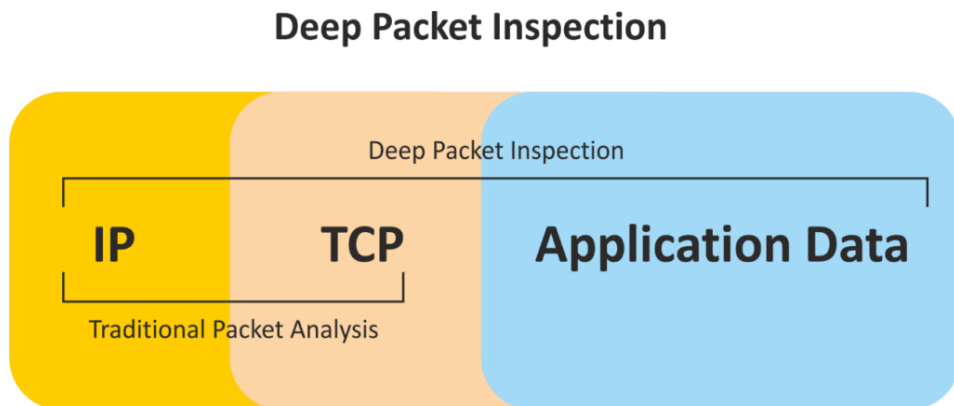
Motivation

- Test the ability of Next Generation Firewalls (NGFWs) to mitigate the effectiveness of a brute force attack on a network.
- Firewall- network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- Two types:
 - Traditional Stateful
 - NGFW



Advantages of NGFW

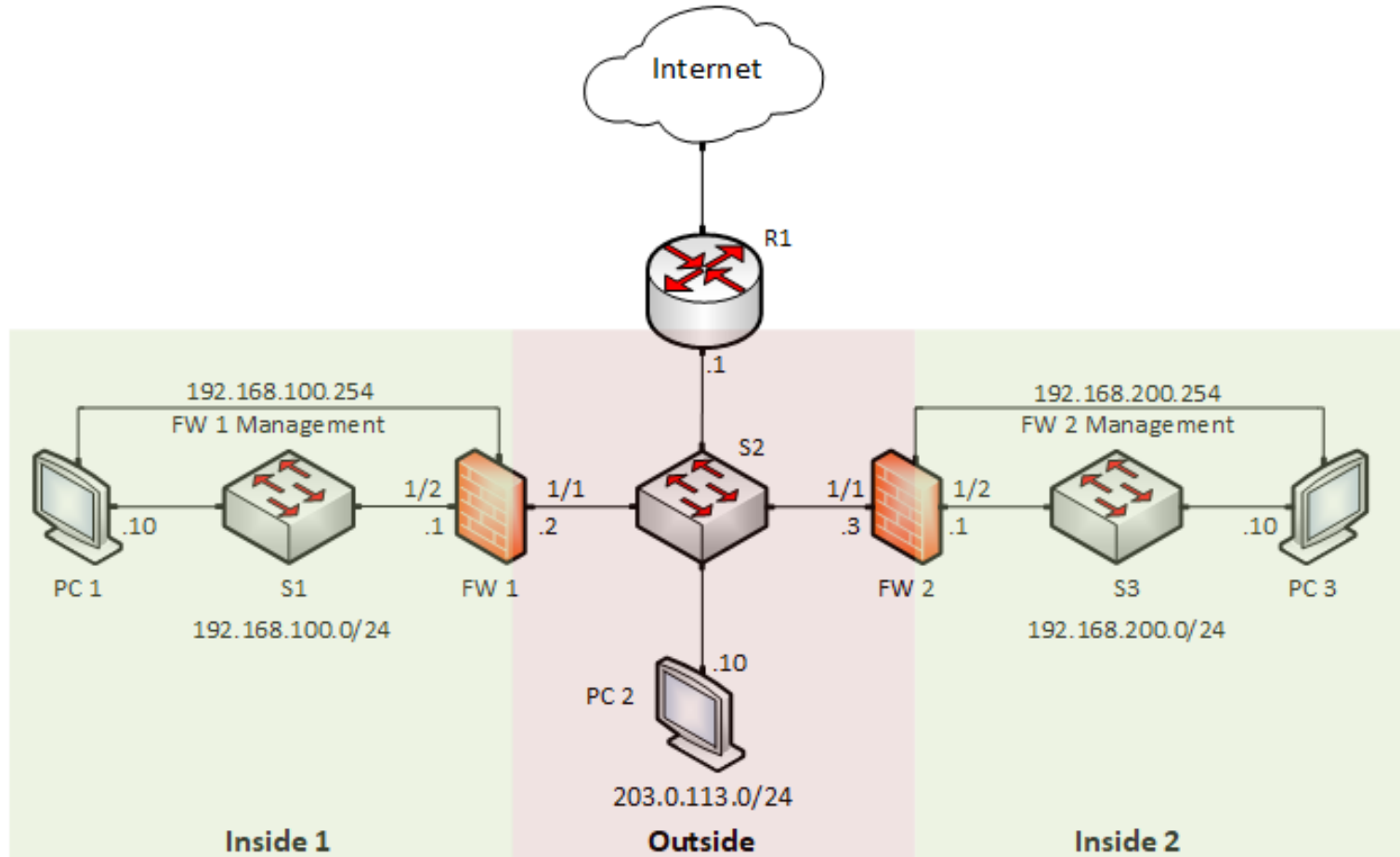
- Set Application layer specific rules
- Deep Packet Inspection
 - See full content of packet header
- NGFW powerful scanner



Objectives

- The goal of this project is:
 - To determine the effectiveness of a modern Next-generation Firewall (NGFW) to detect brute-force attacks
 - To provide best practices when deploying a NGFW to prevent such attacks.
- Use Ncrack(an open-source tool) to understand the anatomy of brute-force attacks
- Implement a brute-force protection policy
 - Protect the network against attacks to well-known services such as SSH and FTP.

NetLab Custom Scenario



Mitigation

- Security Policy to allow Traffic to flow between zones
- Vulnerability Profile (VP)
 - Brute Force Signatures Detected
- Attach VP to security rule

The screenshot shows a 'Vulnerability Protection Profile' configuration window. The 'Name' field is set to 'lab-vp'. The 'Rules' tab is selected, and a search for 'brute force' has been performed, resulting in 3 items. The table below lists these items:

Enable	ID	Threat Name	IP Address Exemptions	Rule	C...	Host	Category	Severity	Action	Packet Capture
<input checked="" type="checkbox"/>	40...	FTP: login Brute Force attempt		brute-force-rule		server	brute-force	high	block-ip (source,300)	disable
<input checked="" type="checkbox"/>	40...	Telnet Authentication Brute Force Attempt		brute-force-rule		server	brute-force	high	block-ip (source,300)	disable
<input checked="" type="checkbox"/>	40...	SSH User Authentication Brute Force Attempt		brute-force-rule		server	brute-force	high	block-ip (source,300)	disable

At the bottom of the window, there is a 'Show all signatures' checkbox, a page indicator 'Page 1 of 1', and a status message 'Displaying 1 - 3/ 3 threats'. 'OK' and 'Cancel' buttons are located at the bottom right.

Results

Monitor Threat Log

	Dashboard	ACC	Monitor	Policies	Objects	Network	Device		Comr			
	Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
	11/20 13:52:00	vulner...	FTP: login Brute Force attempt	Outside	Inside 1	203.0.113.10		192.168.1...	21	ftp	block-ip	high

Conclusion

- Security engineers must develop skills to analyze network traffic.
- Threat logs are essential tools for traffic analysis, for identifying cyber attacks, and for mitigating them.
- NGFWs are effective to mitigate brute force attacks on a network.