Understanding, Detecting, and Mitigating Denial-of-Service Attacks Using Next-Generation Firewalls

Brian Nelson, Dakota McDaniels

Department of Integrated Information Technology
University of South Carolina

December 1st, 2020

Agenda

- Purpose
- Introduction
- Problem description
- Background information
  - Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
  - Next-generation Firewalls (NGFWs)
- Proposed solution and implementation
- Conclusion

Purpose

- Understand DoS/DDoS
- Understand mitigation of DoS/DDoS
- Implement mitigation practices
- Observe mitigation in effect

Introduction

- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) are a leading threat to many businesses, government entities, and citizens
- Characteristics of DoS attacks
  - Simple to complete
  - Effective against small networks/ single target
  - Detection is not difficult
  - Damage/risk potential is low
- Characteristics of DDoS attacks
  - Require multiple attackers
    - Usually a botnet
  - Effective against small or large networks
  - Detection is not difficult
  - Mitigation can be complicated
  - Damage/risk potential is high

Problem Description

- Volatile network connectivity
- Random disruptions of services
- Suspected malicious activity

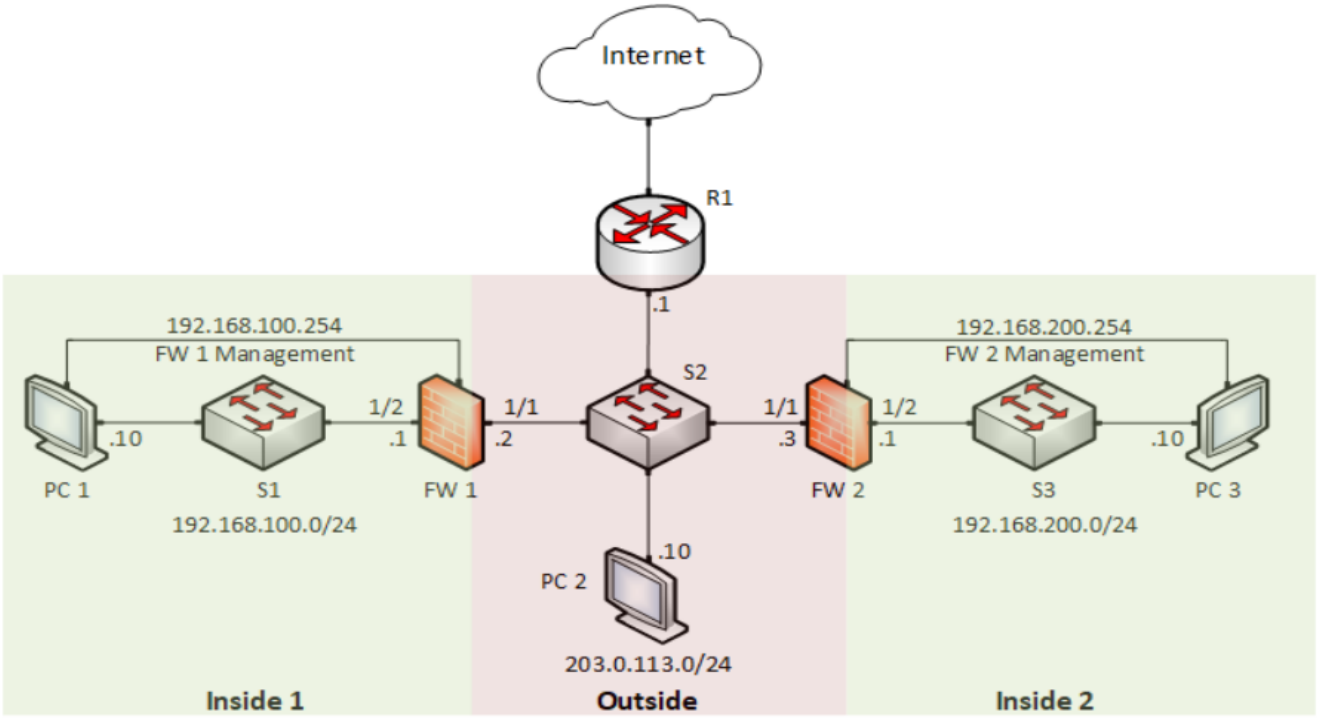

Figure 1. *Effectiveness of DDoS Filtering on Next-Generation Firewalls - Topology*

- Currently, there are no measures taken for threat detection and mitigation

Background Information

- Next-Generation firewalls
  - Configuration
  - Objects
  - Policies
- TCP/IP and OSI model

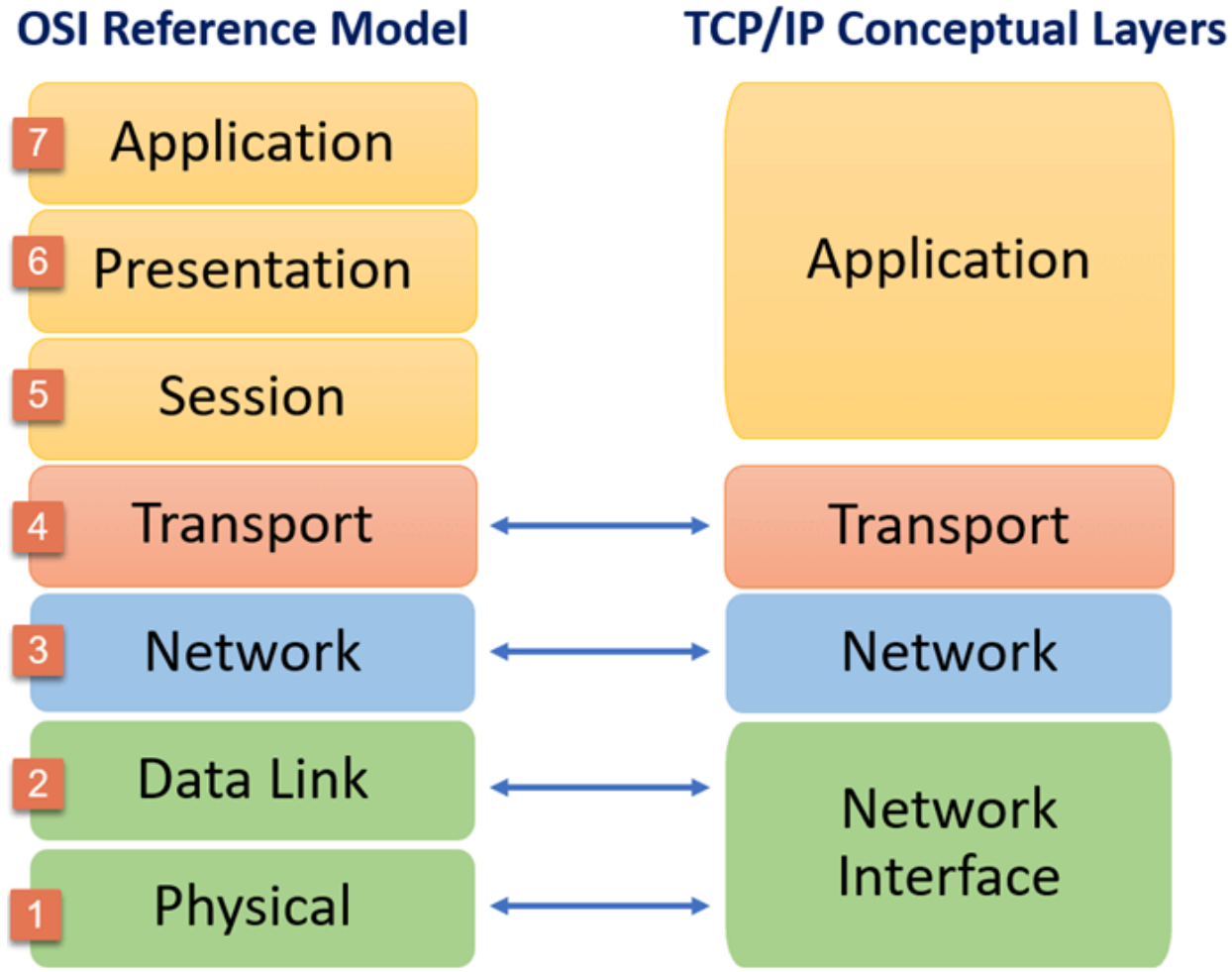

Figure 2. *TCP/IP Model: Layers & Protocol: What is TCP IP Stack? (n.d.). Retrieved November 12, 2020, from https://www.guru99.com/tcp-ip-model.html.*

Proposed Solution and Implementation

PaloAlto Next-Generation Firewall

Configure detection methods

- View and understand logs

Configure the firewall mitigation measures

- Configure DoS Protection Object and Policy
- View mitigation
  - Logs
  - Hands-on exercise

Conclusion

- Why is this work important?
- Future projects/concepts with this knowledge
- Questions?
- Thank you for listening and watching