

Mitigating SYN Attacks with NGFWs

Jesse Leonard and Cameron McDuffie

Advisors: Jorge Crichigno, Ali Mazloun, Jose Gomez



Department of Integrated Information Technology
University of South Carolina

December 2nd, 2021



Agenda

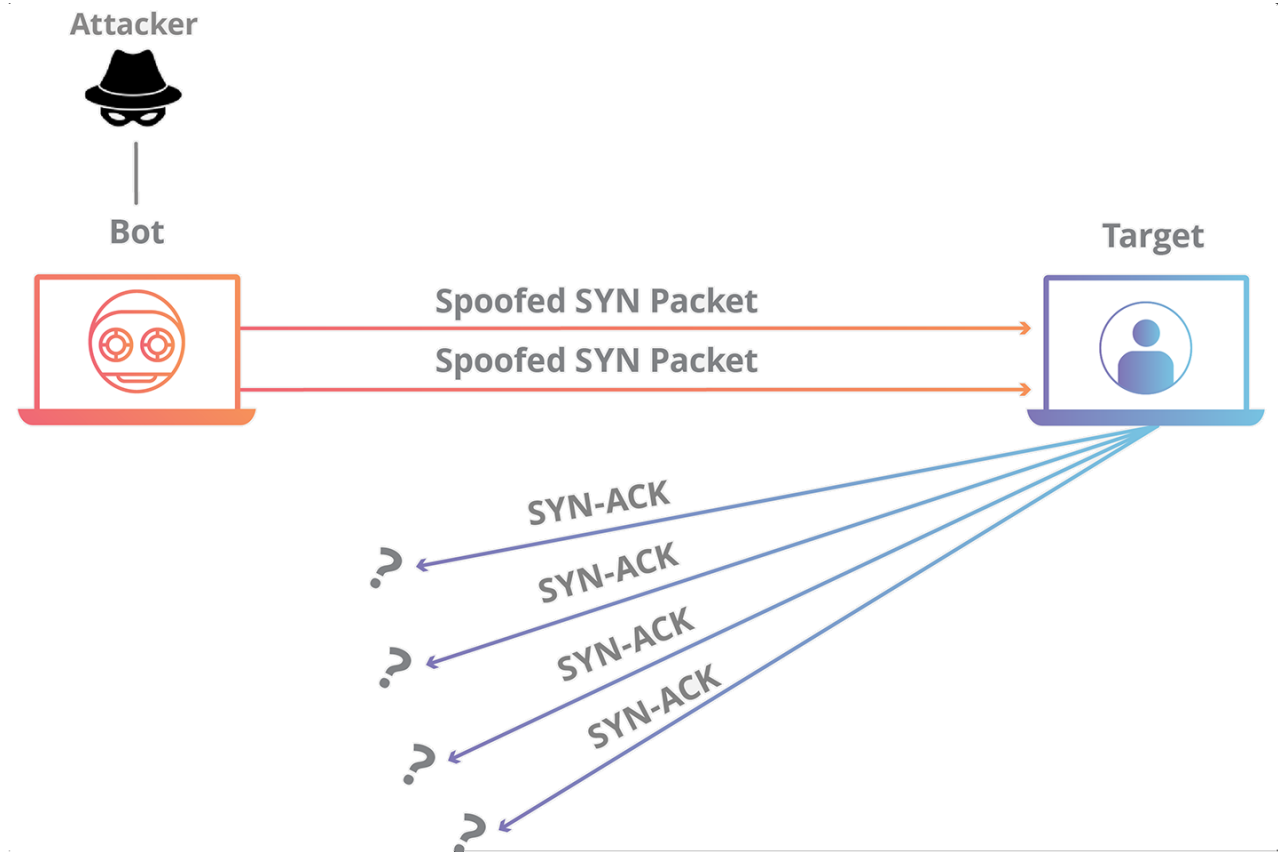
- Purpose
- Introduction
- Problem Description
- Background Information
- Proposed Solution
- Analyzing SYN Packets
- Conclusion

Purpose

- Understand the TCP handshake
- Understand SYN flood attacks
- Understand NGFW's abilities and configurations
- Mitigate Denial of Service (via SYN flood) using a NGFW
- Find a balanced solution between protection and resource allocation

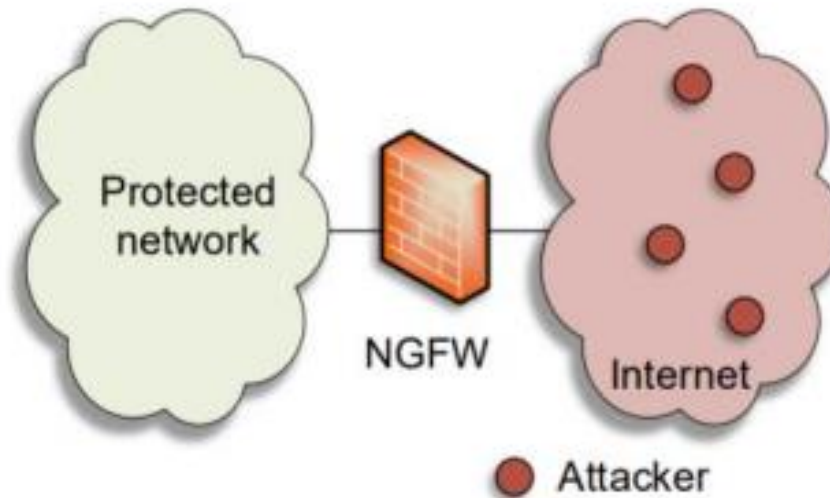
Introduction

- SYN Flood – Type of DDoS (Denial of Service) Attack
- Utilizes TCP three-way handshake
- Three types of attacks
 - I. Direct
 - II. Spoof
 - III. Distributed



Problem Description

- Protect a network against SYN attacks using a NGFW
- Implement a protection policy
- Server is unable to respond to legitimate traffic, policy prevents this



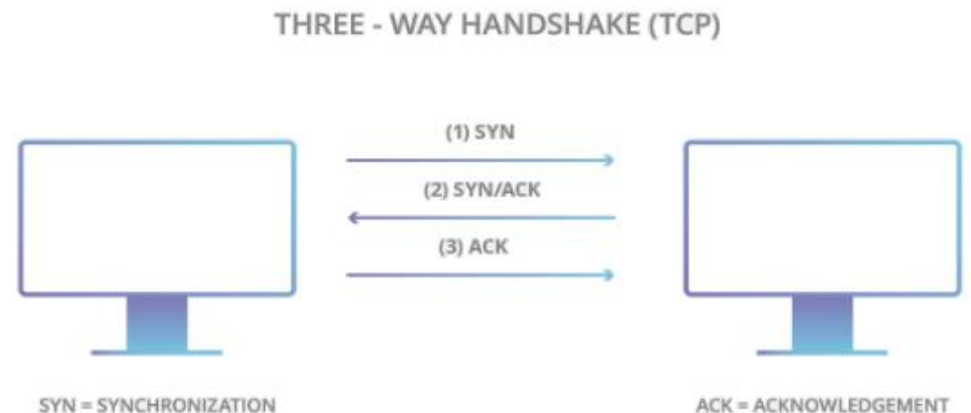
Background Information

- Traditional Firewalls

- I. Identify traffic based on protocol, IP address, and port number
- II. Attacks pass through open firewall ports intended for legitimate traffic

- TCP

- I. Main transport-layer protocol used on the internet
- II. Establishes connections to take place between devices



Proposed Solution

- Filtered traffic is monitored via wireshark, only TCP SYN packets will show
- DoS protection profile allows the firewall to block illegitimate traffic
- Firewall generates SYN cookies to understand what traffic is legitimate
- If a client does not return a cookie with the ACK packet, it is dropped

Analyzing SYN Packets

The screenshot shows a Wireshark capture of normal traffic on the ens160 interface. The display filter is set to `tcp.port == 80 || udp.port == 80`. The packet list shows a mix of TCP and HTTP traffic. Packet 174 is highlighted, showing a SYN packet from 203.0.113.10 to 192.168.100.10 on port 80. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol layers. The hex and ASCII views are visible at the bottom.

No.	Time	Source	Destination	Protocol	Length	Info
174	196.708189462	203.0.113.10	192.168.100.10	TCP	74	41370 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
175	196.708237700	192.168.100.10	203.0.113.10	TCP	74	80 → 41370 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460
176	196.708400067	203.0.113.10	192.168.100.10	TCP	66	41370 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2705442374
177	196.709006733	203.0.113.10	192.168.100.10	HTTP	544	GET /index.html HTTP/1.1
178	196.709048309	192.168.100.10	203.0.113.10	TCP	66	80 → 41370 [ACK] Seq=1 Ack=479 Win=64768 Len=0 TSval=80763416
179	196.710192972	192.168.100.10	203.0.113.10	HTTP	580	HTTP/1.1 200 OK (text/html)
180	196.711214411	203.0.113.10	192.168.100.10	TCP	66	41370 → 80 [ACK] Seq=479 Ack=515 Win=64128 Len=0 TSval=270544
193	201.711846386	203.0.113.10	192.168.100.10	TCP	66	41370 → 80 [FIN, ACK] Seq=479 Ack=515 Win=64128 Len=0 TSval=2
194	201.711998429	192.168.100.10	203.0.113.10	TCP	66	80 → 41370 [FIN, ACK] Seq=515 Ack=480 Win=64768 Len=0 TSval=8
195	201.712209592	203.0.113.10	192.168.100.10	TCP	66	41370 → 80 [ACK] Seq=480 Ack=516 Win=64128 Len=0 TSval=270544

Normal Traffic

The screenshot shows a Wireshark capture of SYN attack traffic on the ens160 interface. The display filter is set to `Apply a display filter ... <Ctrl-/>`. The packet list shows a series of RST packets from 203.0.113.10 to 192.168.100.10 on port 80. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol layers. The hex and ASCII views are visible at the bottom.

No.	Time	Source	Destination	Protocol	Length	Info
867168	4.282432202	203.0.113.10	192.168.100.10	TCP	60	44564 → 80 [RST] Seq=1 Win=0 Len=0
867169	4.282432233	203.0.113.10	192.168.100.10	TCP	60	44560 → 80 [RST] Seq=1 Win=0 Len=0
867170	4.282432261	203.0.113.10	192.168.100.10	TCP	60	44554 → 80 [RST] Seq=1 Win=0 Len=0
867171	4.282432292	203.0.113.10	192.168.100.10	TCP	60	44556 → 80 [RST] Seq=1 Win=0 Len=0
867172	4.282432321	203.0.113.10	192.168.100.10	TCP	60	44571 → 80 [RST] Seq=1 Win=0 Len=0
867173	4.282432350	203.0.113.10	192.168.100.10	TCP	60	44575 → 80 [RST] Seq=1 Win=0 Len=0

SYN Attack Traffic

Conclusion

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