SYN Attack Prevention using a Next-Generation Firewall

Sean Batchelder, Ephraim Zimmerman
Advisors: Ali AlSabeh, Jorge Crichigno
Integrated Information Technology Department, College of Engineering and Computing

Abstract

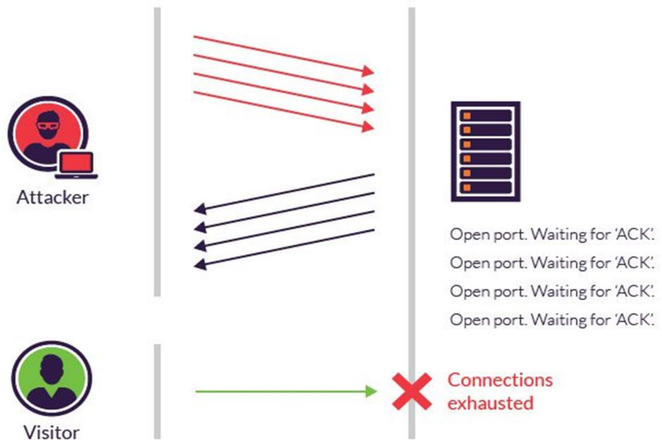
- This project presents SYN attack prevention utilizing Palo Alto, a next-generation Firewall (NGFW).
- Firewalls have evolved beyond simple packet filtering and stateful inspection.
- Many companies are utilizing next-generation firewalls to prevent new threats such as advanced malware and application-layer attacks.
- TCP is the main transport-layer protocol used on the Internet.
- The TCP connection management protocol sets the stage for a Denial of Service (DoS) attack known as the SYN flood attack.
- This Project examines a zone Protection profile with SYN flood protection that is configured to defend an entire ingress zone.
- The NGFW must implement a protection policy against SYN attacks, so that any coordinated or uncoordinated attack must be detected and repelled.
- The network should remain fully operational to legitimate traffic while preventing malicious packets from entering the network.

Project Description

- The handshake process starts when the client sends an initial segment (SYN) to the server, which responds with an acknowledgement segment (SYN, ACK).
- The server awaits an acknowledgement segment (ACK) from the client, which signals the end of the three-way handshake. The connection is then completed.
- In a SYN attack, the attacker sends a large number of TCP SYN segments, without completing the third handshake step.
- With the influx of SYN segments, the server's connection resources become exhausted as they are allocated (but never used) for half-open connections.
- Legitimate clients are then denied service as the server becomes fully allocated.
- The NGFW allows or blocks traffic based on a defined set of security rules.
- The NGFW is located at the edge of a protected network. The NGFW must implement a protection policy against SYN attacks.
- The NGFW must prevent SYN packets from overwhelming the server and allocating all resources.

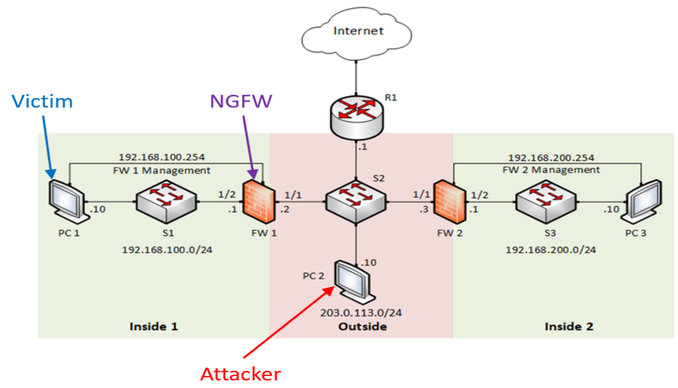
SYN Flood Protection

- A SYN flood is a type of denial-of-service (DDoS) attack which aims to make a server unavailable to legitimate traffic.
- There are multiple type of attacks that can utilize a SYN flood:
  - Direct attack
  - Spoofed attack
  - Distributed attack
- DoS protection profiles protect critical resources from these attacks.
- Aggregate and Classified DoS Protection Profiles:
  - Aggregate - Sets thresholds that apply to the entire group of devices
  - Classified - Sets flood thresholds that apply to each individual device
- SYN Flood protection includes:
  - SYN cookies - Drops traffic that fails the SYN handshake
  - Random early drop – Drops traffic randomly
- For each flood type, you set three thresholds:
  - Alarm Rate - CPS threshold to trigger an alarm
  - Activate - CPS threshold to activate the flood protection
  - Maximum - The max number of CPS to drop when RED is set
- The thresholds are set to default values, due to them being higher and less likely to drop legitimate traffic.



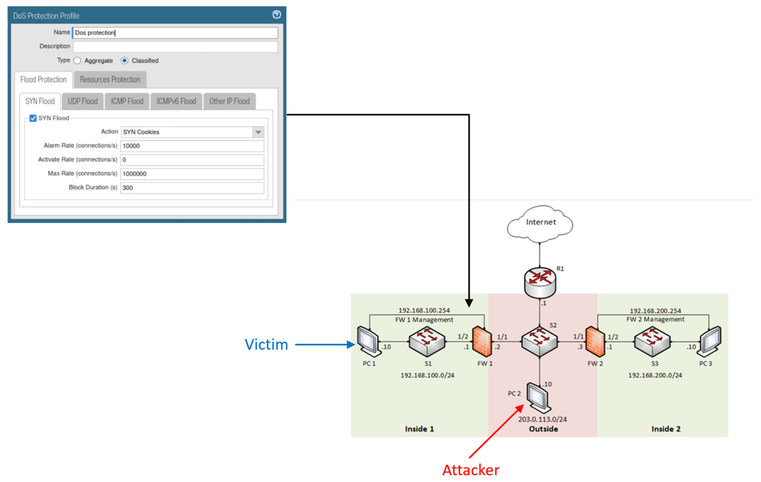
Test System

- The attacker PC2 is placed outside of the network in the "outside zone" while the victim is located inside the network in the "inside 1" zone.
- PC2 will send SYN packets into the network that will attempt to interfere with PC1's ability to access the network.
- A protection policy is implemented and enabled in the NGFW to detect and prevent the SYN flood attack.
- The NGFW FW1 will prevent these SYN packets from entering the network and block the IP address of the attacker, PC2.
- The attack is monitored through Wireshark to determine that the NGFW is effective in its ability to prevent the SYN flood attack.



Experimentation

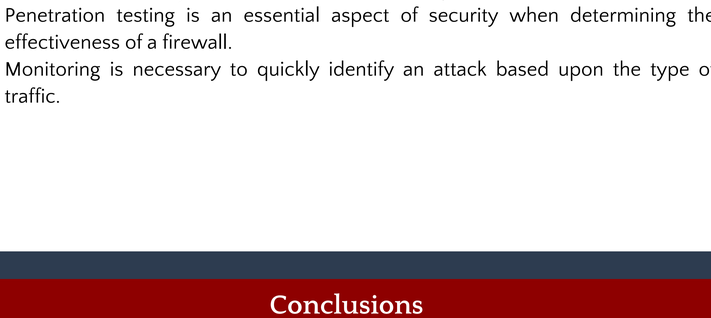
- A webserver using Apache2 is hosted on PC1 to test the connectivity on the network.
- Hping3 is executed within the terminal on PC2 and would administer the SYN flood attack through port 80 and use a spoofed source address.
- The attack is first executed on the network while it was unprotected to ensure the SYN flood is effective.
- Monitoring through Wireshark showed a large flood of TCP traffic entering the network, making it inaccessible to hosts.
- A classified DoS protection profile is utilized with the action set to SYN cookies and default thresholds.
- The DoS protection policy is implemented as a rule with source-IP-only tracking to reduce the number of resources required.
- The DoS protection policy rule is set to "protect" as the action, and the DoS protection profile is applied when the traffic matches the rule.
- The protection policy is implemented and enabled in the NGFW.
- The attack is tested once again while the network is protected.



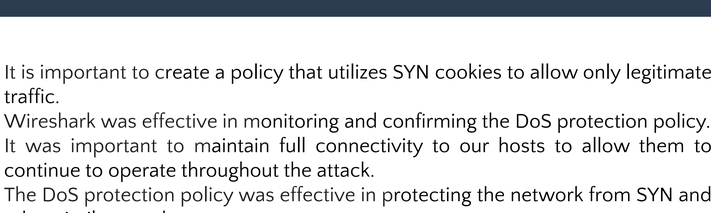
Results

- The classified profile blocks the appropriate source IP that is sending the SYN packets.
- Legitimate requests are allowed through; the illegitimate SYN packets remain blocked.
- Wireshark shows SYN packets are no longer bombarding the network.
- The network remains operational, and all connected hosts have full access to the network.

Policy OFF



Policy ON



Lessons Learned

- Setting the DoS protection rule action to, "protect" is required to implement the DoS protection policy rather than using the action, "deny", which doesn't apply a DoS protection profile.
- Spoofed attacks are far more likely to be utilized to prevent the source IP of the attacker from being shown.
- The key concern is differentiating between legitimate traffic and the illegitimate traffic that is part of an attack.
- Sinkholing and rate limiting are not effective mitigation strategies when compared to a NGFW that has an appropriate DoS protection policy.
- Thresholds will likely need to be adjusted based upon the network environment.
- Penetration testing is an essential aspect of security when determining the effectiveness of a firewall.
- Monitoring is necessary to quickly identify an attack based upon the type of traffic.

Conclusions

- It is important to create a policy that utilizes SYN cookies to allow only legitimate traffic.
- Wireshark was effective in monitoring and confirming the DoS protection policy.
- It was important to maintain full connectivity to our hosts to allow them to continue to operate throughout the attack.
- The DoS protection policy was effective in protecting the network from SYN and other similar attacks.
- Future work is recommended to test the utilization of the NGFW in a larger and more complex environment.
- Future work could adjust the following thresholds to suit the environment:
  - Activate rate
  - Alarm Rate
  - Max rate
- When conducting future work, it will be important to implement further protection against:
  - UDP Floods
  - ICMP Floods
  - ICMPv6 Floods
  - Other types of IP Floods

Acknowledgement

- This work was supported by the Office of Naval Research (ONR) grant N00014-20-1-2797: "Enhancing the Preparation of Next-generation Cyber Professionals"