DDOS Defense using Next Generation Firewalls

Jacob Sherer, Matthew Kleeman
Advisors: Ali Mazloum, Jorge Crichigno

Department of Integrated Information Technology
University of South Carolina

December 2023

Agenda

Background Information

Project Objective

Solutions

Conclusion

Background Information

A **Denial of Service** (DoS) attack renders a target computer unavailable for legitimate users by utilizing all the resources of a device.

DoS attacks have multiple forms including:

- **TCP SYN** flood: Use the TCP three-way handshake to start many connections but never closing the connections.
- **ICMP** flood: Use the ICMP protocol, generally many pings, to overwhelm the target's resources.
- **UDP** flood: Send many UDP packets to a targeted server with the aim of overwhelming that device’s ability to process and respond.

Background Information

Firewalls are network devices meant to protect the network through monitoring the inbound and outbound packets.

Firewalls are classified as either:

- **Stateless firewalls:** Only consider packet headers while filtering the traffic.
- **Stateful firewalls:** Consider the state of the flows besides the packet headers in the filtering process.

Next-generation Firewalls (NGFW) are stateful firewalls that have more advanced capabilities that can be used to protect a network against the previously mentioned attacks. Palo Alto NGFW are used in this scenario.

Project Objective

Goal: Use a Palo Alto NGFW to protect a network against various types of DoS attacks.

- TCP SYN flood attacks
- ICMP flood attacks
- UDP flood attacks

Solutions

Palo Alto NGFW has multiple ways to protect against these types of DoS attacks. This project focused on 2, **Zone Protection Profiles**, and **DoS Protection Profiles.**

These methods allow the firewall to detect, log, and block TCP SYN flood, ICMP flood, and UDP flood attacks.

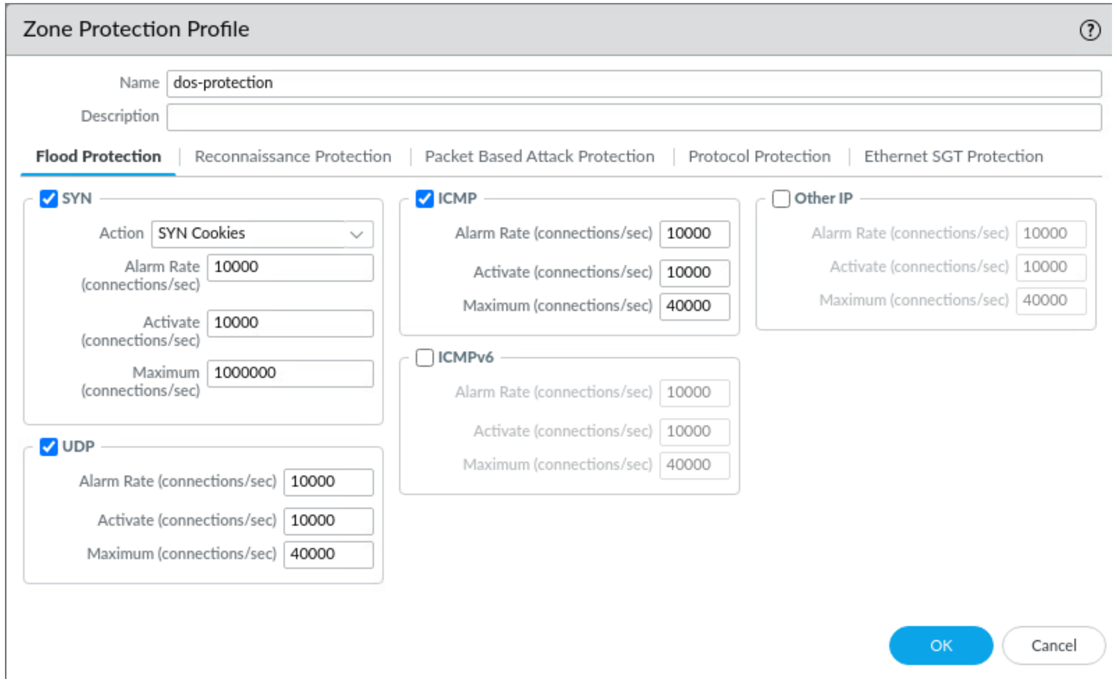
The logs include information about the attacks like time, type, source and destination addresses, the action took, and more.

Solutions cont.

Zone Protection Profiles are the security rules assigned to the various security zones defined by the Palo Alto NGFW.

The configurable parameters are:

- **Alarm Rate:** How many connections/second need to occur before being logged as a flood.
- **Activate:** When the chosen action is enabled to block subsequent connections.
- **Maximum:** How many connections can be initiated before the rest are dropped.



Zone Protection Profile
?
Flood Protection | Reconnaissance Protection | Packet Based Attack Protection | Protocol Protection | Ethernet SGT Protection
OK
Cancel

Name: dos-protection

Description:

☑ SYN

Action: SYN Cookies

Alarm Rate (connections/sec): 10000

Activate (connections/sec): 10000

Maximum (connections/sec): 1000000

☑ UDP

Alarm Rate (connections/sec): 10000

Activate (connections/sec): 10000

Maximum (connections/sec): 40000

☑ ICMP

Alarm Rate (connections/sec): 10000

Activate (connections/sec): 10000

Maximum (connections/sec): 40000

□ ICMPv6

Alarm Rate (connections/sec): 10000

Activate (connections/sec): 10000

Maximum (connections/sec): 40000

□ Other IP

Alarm Rate (connections/sec): 10000

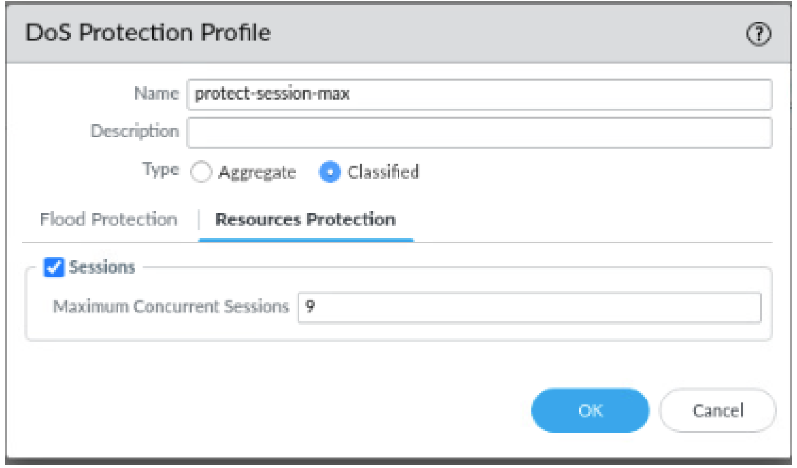
Activate (connections/sec): 10000

Maximum (connections/sec): 40000

Solutions cont.

DoS Protection Profile are specialized security policies with more granular control to mitigate DoS attacks on specific systems.

An example of the added granularity is in classifying based on the source or destination addresses or users.



DoS Protection Profile

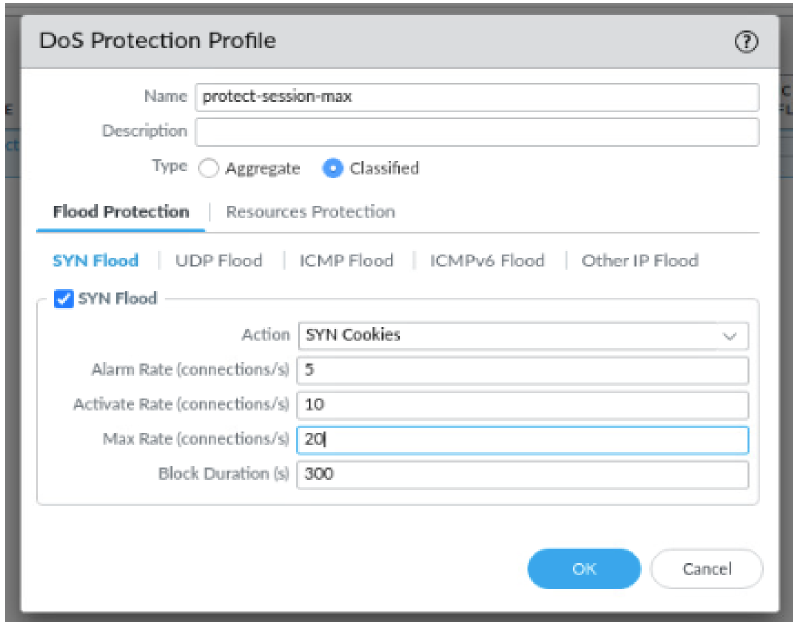
Name: protect-session-max

Description:

Type: ○ Aggregate ● Classified

☑ Sessions

Maximum Concurrent Sessions: 9



DoS Protection Profile

Name: protect-session-max

Description:

Type: ○ Aggregate ● Classified

☑ SYN Flood

Action: SYN Cookies

Alarm Rate (connections/s): 5

Activate Rate (connections/s): 10

Max Rate (connections/s): 20

Block Duration (s): 300

Conclusion

- DoS attacks aim at overwhelming a target machine’s resources.
- NGFW provide the means of defense against these attacks.
- The two utilized ways in this project are:
  - Zone protection profiles
  - DoS protection profiles
- By the end of the project, we were able to detect, log, and block TCP SYN floods, ICMP floods, and UDP floods.