



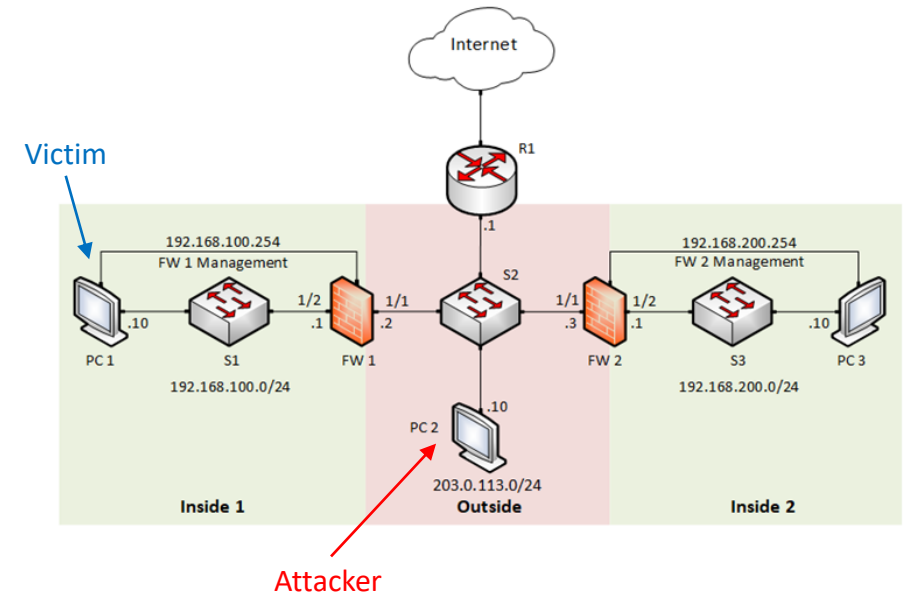
SYN Attack Prevention

Sean Batchelder and Ephraim Zimmerman
Advisor: Ali AlSabeH

Department of Integrated Information Technology
University of South Carolina

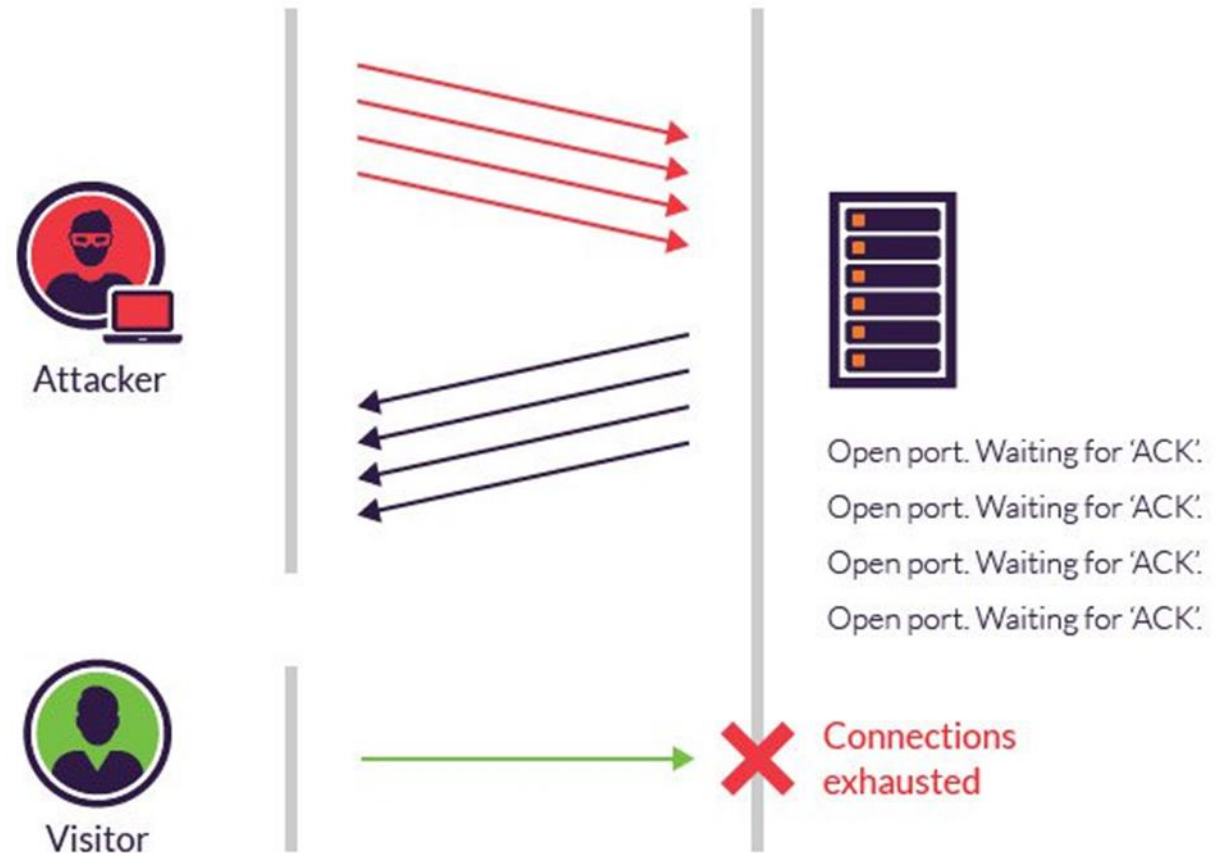
Objective

- Understand and utilize a next-generation Firewall
- Implement a protection policy against SYN attacks
- Protect a network against SYN and similar attacks



SYN Flooding

A SYN flood is a type of denial-of-service (DDoS) attack which aims to make a server unavailable to legitimate traffic.



Types of SYN Floods

Direct Attack

Attacker does not mask their IP address

Spoofed Attack

IP address is masked to hide the attacker's identity

Distributed Attack

Attack created using a botnet

Flood Protection

SYN Cookies

Drops only traffic that fails the SYN handshake

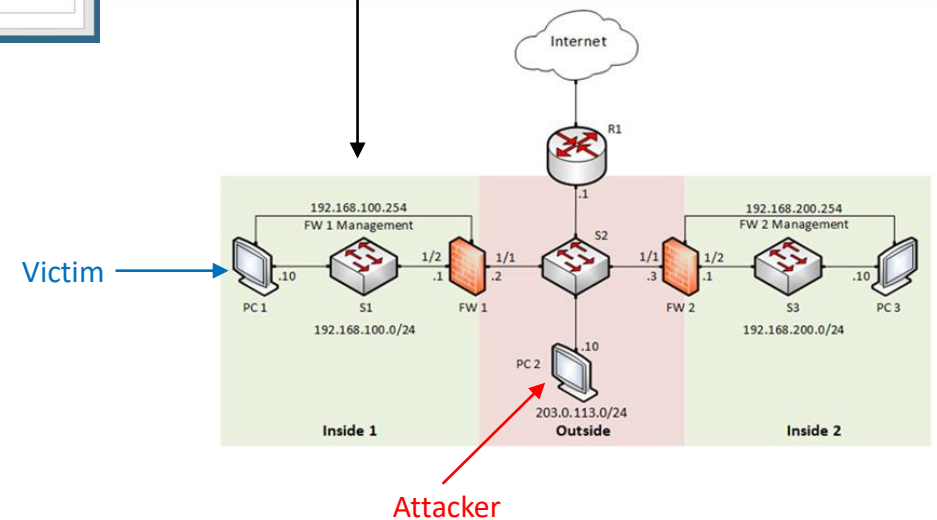
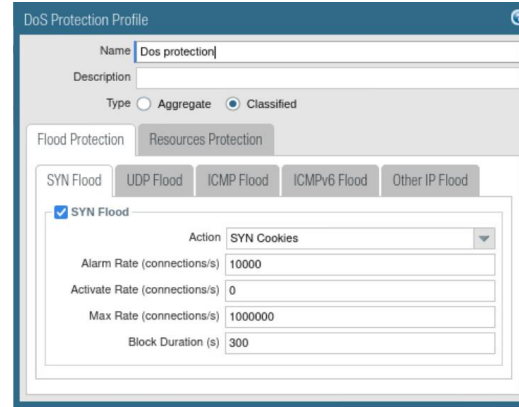
Random Early Drop

Drops all traffic randomly

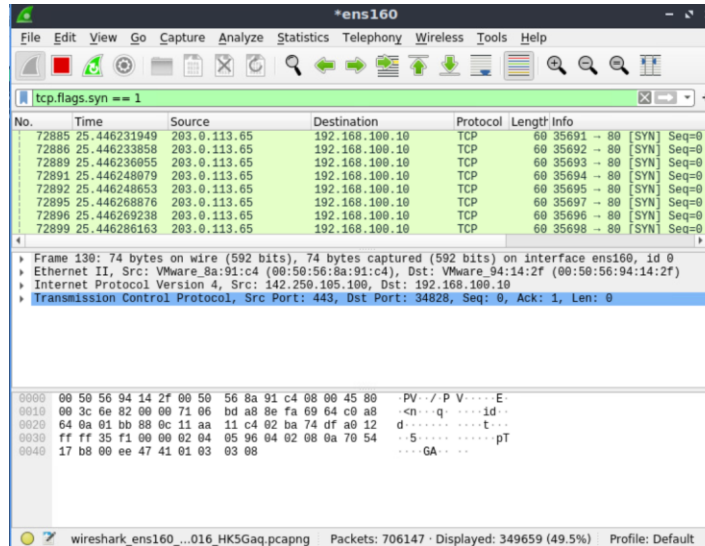


Solution

- Classified DoS protection is used with source-IP-only tracking to reduce resources
- Set the action to SYN cookies
- Implement the profile into the security policy to block PC2



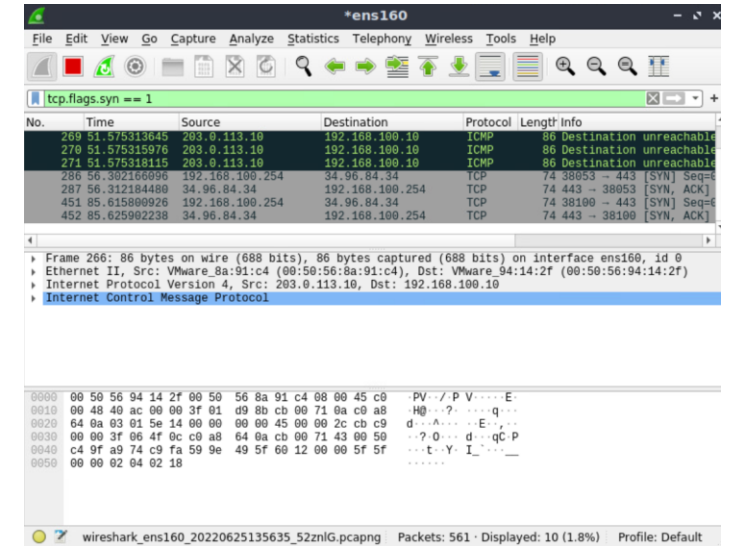
Policy OFF



No.	Time	Source	Destination	Protocol	Length	Info
72885	25.446231949	203.0.113.65	192.168.100.10	TCP	60	35691 → 80 [SYN] Seq=0
72886	25.446233858	203.0.113.65	192.168.100.10	TCP	60	35692 → 80 [SYN] Seq=0
72889	25.446236955	203.0.113.65	192.168.100.10	TCP	60	35693 → 80 [SYN] Seq=0
72891	25.446248079	203.0.113.65	192.168.100.10	TCP	60	35694 → 80 [SYN] Seq=0
72892	25.446248653	203.0.113.65	192.168.100.10	TCP	60	35695 → 80 [SYN] Seq=0
72895	25.446268876	203.0.113.65	192.168.100.10	TCP	60	35697 → 80 [SYN] Seq=0
72896	25.446269238	203.0.113.65	192.168.100.10	TCP	60	35696 → 80 [SYN] Seq=0
72899	25.446286163	203.0.113.65	192.168.100.10	TCP	60	35698 → 80 [SYN] Seq=0

Frame 130: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface ens160, id 0
 Ethernet II, Src: VMware 8a:91:c4 (00:50:56:8a:91:c4), Dst: VMware 94:14:2f (00:50:56:94:14:2f)
 Internet Protocol Version 4, Src: 142.250.105.100, Dst: 192.168.100.10
 Transmission Control Protocol, Src Port: 443, Dst Port: 34828, Seq: 0, Ack: 1, Len: 0

Policy ON



No.	Time	Source	Destination	Protocol	Length	Info
269	51.575313645	203.0.113.10	192.168.100.10	ICMP	86	Destination unreachable
270	51.575315976	203.0.113.10	192.168.100.10	ICMP	86	Destination unreachable
271	51.575318115	203.0.113.10	192.168.100.10	ICMP	86	Destination unreachable
286	56.392166996	192.168.100.254	34.96.84.34	TCP	74	38053 → 443 [SYN] Seq=0
287	56.312184480	34.96.84.34	192.168.100.254	TCP	74	443 → 38053 [SYN, ACK]
451	85.615800926	192.168.100.254	34.96.84.34	TCP	74	38100 → 443 [SYN] Seq=0
452	85.625902238	34.96.84.34	192.168.100.254	TCP	74	443 → 38100 [SYN, ACK]

Frame 266: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface ens160, id 0
 Ethernet II, Src: VMware 8a:91:c4 (00:50:56:8a:91:c4), Dst: VMware 94:14:2f (00:50:56:94:14:2f)
 Internet Protocol Version 4, Src: 203.0.113.10, Dst: 192.168.100.10
 Internet Control Message Protocol

Results

- The classified profile blocks the appropriate source IP
- Wireshark and Palo monitors show the network is protected
- PC1 can access the network

Conclusion

- Create a policy utilizing SYN cookies to allow legitimate traffic
- Protect a network against SYN and similar attacks
- Effectively prevented the SYN attack
- Future Work