Incident Response Report - DoS Attack from PC1 to WebServer1

Incident Response Document
Incident Title: Denial-of-Service (DoS) Attack from PC1 to WebServer1
Environment: Cisco Packet Tracer Simulation
Detected By: ASA Firewall - High Connection Count

1. Executive Summary

A DoS attack was detected targeting WebServer1 within the simulated network topology. The attack originated from internal client PC1, flooding WebServer1 with excessive connection attempts. The ASA firewall triggered an alert due to an abnormal spike in connection counts, initiating the incident response process.

2. Incident Timeline

14:05 - ASA firewall detects high connection count from PC1 to WebServer1
14:07 - Initial triage begins by Tier 1 analyst
14:10 - PC1 isolated from the network
14:15 - Firewall logs reviewed and archived
14:20 - Attack confirmed as internal DoS
14:30 - Incident escalated to Tier 2 and root cause analysis initiated
15:00 - IR write-up completed and systems restored

3. Triage Summary

Indicators of Compromise (IoCs):
- ASA connection logs show >500 simultaneous connections from 192.168.1.10 (PC1) to 192.168.1.100
(WebServer1)
- CPU spike on WebServer1
- No external IPs involved - internal threat vector
Affected Systems:
- WebServer1 (192.168.1.100)
- ASA Firewall (connected to internal and DMZ segments) - PC1 (192.168.1.10)
Priority Level: High
Reason: Critical internal asset under denial-of-service, affecting availability.

4. Incident Response Playbook

Phase 1 - Preparation

- Network logging enabled on ASA firewall
- ACLs in place to restrict external traffic
- Syslog server monitoring firewall and endpoints

Phase 2 - Identification

- ASA firewall logs flagged high connection count:

show conn | include 192.168.1.10

- WebServer1 logs show service saturation

Phase 3 - Containment

- PC1 isolated via switch port shutdown:

interface FastEthernet0/1

shutdown

- Temporary ASA rule added to drop traffic from 192.168.1.10

Phase 4 - Eradication

- PC1 analyzed for malicious script or user behavior
- Suspicious DoS script found in PC1 background tasks and removed
- ACL updated to block unnecessary outbound connections

Phase 5 - Recovery

- WebServer1 rebooted and monitored
- ASA connection tables cleared:

clear conn address 192.168.1.10Phase 6 - Lessons Learned

- Internal access monitoring enhanced
- Host-based IDS/IPS considered for future simulation

5. Technical Investigation

ASA Firewall Log Output:

show conn address 192.168.1.10

TCP inside 192.168.1.10:12345 DMZ 192.168.1.100:80 idle 0:00:01 Bytes 0

... (repeated hundreds of times)

Packet Tracer Observation:

- Continuous ping/flood script from PC1
- WebServer1 unresponsive due to exhausted resources

Root Cause:

- Unauthorized script execution from PC1
- No internal traffic rate-limiting in place

6. Write-Up / Incident Summary

Title: Internal DoS from PC1

Summary: PC1 generated a denial-of-service flood targeting WebServer1, which overwhelmed services. The ASA firewall detected and helped isolate the attack. The root cause was unauthorized internal traffic generation.

Actions Taken: Host isolation, traffic filtering, script removal.

Next Steps: Implement traffic shaping, user monitoring, host firewall rules.

7. Escalation Path

Tier 1 - Helpdesk Analyst - Initial detection

Tier 2 - Network Admin - Attack confirmation

Tier 3 - Security Officer - If DoS persists or spreads

Exec - IT Manager - If uptime SLA is breached