DDoS Attack Response Runbook

Enterprise Network Protection & Incident Response

Version:	2.0
Last Updated:	February 2026
Classification:	INTERNAL USE ONLY
Document Owner:	Security Operations Center

Table of Contents

1. Executive Summary

This runbook provides comprehensive guidance for responding to Distributed Denial of Service (DDoS) attacks targeting enterprise networks. It covers detection, mitigation, and recovery procedures using F5 BIG-IP, Fortinet security appliances, ISP coordination, and Splunk-based traffic analysis. This document is designed to ensure rapid, coordinated response to minimize service disruption and protect critical infrastructure.

Key Objectives:

- Detect DDoS attacks within 5 minutes of onset
- Activate mitigation measures within 15 minutes
- Coordinate with ISP within 30 minutes for volumetric attacks
- Maintain service availability for critical systems
- Document all actions for post-incident analysis

2. DDoS Attack Overview

2.1 Attack Types

Attack Type	Description	Primary Impact	Mitigation Layer
Volumetric	UDP/ICMP floods, DNS amplification	Bandwidth saturation	ISP + Edge
Protocol	SYN floods, fragmented packets	State table exhaustion	Firewall + F5
Application	HTTP floods, Slowloris	Application resource exhaustion	F5 + WAF
Reflection	NTP, DNS, SSDP amplification	Bandwidth + target saturation	ISP + Edge

2.2 Common Attack Vectors

Understanding attack vectors enables faster identification and appropriate countermeasures:

- **Layer 3/4 Attacks:** SYN floods, UDP floods, ICMP floods - target network infrastructure
- **Layer 7 Attacks:** HTTP GET/POST floods, Slowloris - target application resources
- **Amplification Attacks:** DNS, NTP, SSDP reflection - leverage misconfigured servers
- **Multi-Vector Attacks:** Combination of volumetric, protocol, and application attacks

3. Detection & Initial Response

3.1 Detection Indicators

- Sudden spike in inbound traffic (>200% baseline)
- Increased connection attempts or half-open connections
- Service degradation or timeouts for legitimate users
- High CPU/memory utilization on firewalls or load balancers
- Alerts from IDS/IPS systems
- Customer complaints about service availability
- Unusual geographic traffic patterns

3.2 Initial Response Checklist (First 5 Minutes)

Step	Action	Responsible	Time
1	Confirm attack vs. legitimate traffic spike	NOC Analyst	2 min
2	Alert Security Operations Center	NOC Analyst	1 min
3	Start incident documentation	SOC Lead	1 min
4	Activate war room bridge	SOC Lead	1 min
5	Begin traffic capture for analysis	Network Engineer	2 min

3.3 Quick Classification

Traffic Volume	Connection Rate	Attack Type	Primary Action
<10 Gbps	Normal	Application Layer	Enable F5 AFM/ASM
<10 Gbps	High (>10k/sec)	Protocol Attack	Enable F5 SYN Cookie
10-50 Gbps	Variable	Volumetric	Activate scrubbing + ISP notify
>50 Gbps	Extremely High	Multi-Vector	ISP immediate + all defenses

4. F5 BIG-IP Mitigation Strategies

4.1 F5 Advanced Firewall Manager (AFM)

AFM provides network firewall capabilities and DDoS protection at layers 3 and 4. Use these procedures to activate protection:

Enable SYN Flood Protection:

```
tmsh modify security firewall global-rules { syn-check enabled syn-cookie-protection
enabled }
```

Configure Rate Limiting:

```
tmsh create security firewall rule-list ddos_protection { rules add {
block_excessive_connections { action drop ip-protocol tcp rate-limit { rate 10000 } } }
}
```

Enable Connection Limits per Source IP:

```
tmsh modify ltm virtual [virtual-server-name] profiles add { ddos-protection { context
clientside } }
```

4.2 F5 Application Security Manager (ASM)

ASM protects against layer 7 application attacks. Deploy these configurations during an attack:

Enable Proactive Bot Defense:

```
tmsh modify asm policy [policy-name] bot-defense { suspicious-browsers enabled
malicious-bots enabled }
```

HTTP Rate Limiting:

```
tmsh create ltm profile http-compression ddos_http_protection { rate-limit 100
rate-limit-mode request rate-limit-source-mask 32 }
```

Enable CAPTCHA Challenge:

```
tmsh modify asm policy [policy-name] captcha-response { enabled true response-type
captcha }
```

4.3 F5 DDoS Hybrid Defender

For dedicated DDoS appliances, activate behavioral analysis and mitigation:

1. Navigate to DoS Protection > Quick Configuration

2. Select protected object (Virtual Server or Network)
3. Enable 'Behavioral & Stress-Based Detection'
4. Set thresholds: Auto (recommended) or Manual based on baseline
5. Enable mitigation modes: Rate Limiting + Packet Filtering
6. Activate TCP SYN Cookie protection
7. Enable HTTP Request Rate Limiting (for Layer 7)
8. Review and apply configuration

4.4 F5 iRules for Custom Protection

Deploy custom iRules for specialized attack patterns:

Example: Block Excessive Requests from Single IP:

```
when CLIENT_ACCEPTED {
  set client_ip [IP::client_addr]
  set req_count [table lookup -subtable ddos_count $client_ip]
  if { $req_count >= 100 } {
    drop
    log local0. "Dropped connection from $client_ip - rate limit exceeded"
  } else {
    table incr -subtable ddos_count $client_ip
    table timeout -subtable ddos_count $client_ip 60
  }
}
```

5. Fortinet FortiDDoS & FortiGate Response

5.1 FortiDDoS Configuration

FortiDDoS provides dedicated DDoS detection and mitigation. Configure protection policies:

Activate Protection Mode:

1. Login to FortiDDoS web interface
2. Navigate to DDoS > Protection Profiles
3. Select appropriate profile (Server, Network, or Custom)
4. Set SPP (Service Protection Profile) to 'High Security'
5. Enable 'Behavioral Analysis' mode
6. Configure thresholds: Packets/sec, Connections/sec, Bandwidth
7. Enable 'Anomaly Detection' for zero-day attacks
8. Activate 'Packet Filtering' and 'Rate Limiting'
9. Apply configuration and monitor Dashboard

CLI Configuration for Emergency Response:

```
config system protection-profile
  edit "emergency_ddos"
    set mode aggressive
    set anomaly-detection enable
    set rate-limit-mode adaptive
    set syn-flood-protection enable
  next
end
```

5.2 FortiGate Firewall DDoS Protection

FortiGate firewalls include DDoS protection capabilities that should be activated:

Enable DoS Policy:

```
config firewall DoS-policy
  edit 1
    set interface "wan1"
    set srcaddr "all"
    set dstaddr "all"
    set service "ALL"
    set anomaly flood tcp-syn-flood
    set anomaly action pass
    set anomaly threshold 10000
  next
end
```

Configure Source IP Rate Limiting:

```
config firewall policy
  edit [policy-id]
    set anti-replay enable
    set per-ip-shaper ddos-shaper
  next
end

config firewall shaper per-ip-shaper
  edit "ddos-shaper"
    set max-bandwidth 10000
  next
end
```

5.3 FortiAnalyzer Integration

Ensure FortiAnalyzer is collecting logs for post-incident analysis:

- Verify log forwarding: config log fortianalyzer setting
- Enable high-volume logging during attack
- Create real-time attack dashboards
- Set up automated reporting for incident documentation
- Archive logs for forensic analysis (minimum 90 days)

6. ISP Coordination Procedures

6.1 When to Engage ISP

Coordinate with Internet Service Provider when on-premises mitigation is insufficient:

- **Volumetric attacks exceeding circuit capacity** (>50% of total bandwidth)
- **Multi-vector attacks** overwhelming edge defenses
- **Attacks lasting more than 30 minutes** despite mitigation efforts
- **Critical service outages** affecting business operations
- **Upstream network congestion** visible in ISP reports

6.2 ISP Contact Procedure

Provider	Contact Method	Account Number	SLA Response
Primary ISP	NOC: [phone/email]	ACCT-XXXX	15 minutes
Secondary ISP	NOC: [phone/email]	ACCT-YYYY	30 minutes
DDoS Scrubbing Provider	Emergency: [phone]	CUST-ZZZZ	5 minutes

IMPORTANT: Customize this table with actual ISP contact information and keep emergency contact cards readily available in the NOC/SOC.

6.3 Information Required for ISP

Prepare the following information before contacting ISP:

- Account number and circuit IDs
- Attack start time and duration
- Attack type (volumetric, protocol, application)
- Target IP addresses and/or prefixes
- Current traffic volume (Gbps, Mpps)
- Source IP addresses or ASNs (if identified)
- Packet captures (PCAP files) - first 1000 packets
- Current business impact (services affected, customer count)
- Requested action: Rate limiting, blackhole, or scrubbing

6.4 BGP Remote Triggered Black Hole (RTBH)

If ISP supports RTBH, use BGP to signal attack targets for upstream filtering:

```
! Cisco IOS Example
ip route [attacked-ip] 255.255.255.255 Null0
router bgp [ASN]
  network [attacked-ip] mask 255.255.255.255
  neighbor [ISP-IP] send-community
!
ip community-list 1 permit [ISP-RTBH-COMMUNITY]
route-map RTBH permit 10
  match community 1
  set community [ISP-RTBH-COMMUNITY]
```

WARNING: RTBH will completely block traffic to the target IP. Use only when service is already unavailable due to attack.

6.5 DDoS Scrubbing Service Activation

For cloud-based scrubbing services, follow these activation steps:

1. Contact scrubbing provider emergency hotline
2. Provide attack details and target networks
3. Request BGP route diversion to scrubbing center
4. Update DNS to point to scrubbing service (if applicable)
5. Verify clean traffic returning via GRE tunnel or direct connection
6. Monitor scrubbing dashboard for attack metrics
7. Coordinate with provider on attack mitigation progress
8. Plan deactivation once attack subsides (minimum 2 hours after last attack traffic)

7. Traffic Analysis with Splunk

7.1 Real-Time Attack Monitoring

Use Splunk to analyze attack patterns and identify attack sources in real-time:

Top Source IPs Query:

```
index=firewall sourcetype=fortinet_traffic action=deny
| stats count by src_ip
| sort -count
| head 100
| eval threat_level=case(count>10000,"Critical", count>5000,"High", count>1000,"Medium",
1=1,"Low")
```

Attack Volume Timeline:

```
index=network sourcetype=netflow
| timechart span=1m sum(bytes) as total_bytes, dc(src_ip) as unique_sources
| eval bytes_gb=total_bytes/1073741824
```

Protocol Distribution:

```
index=network sourcetype=netflow
| stats count by protocol
| eval percentage=round((count/sum(count))*100,2)
```

7.2 Attack Pattern Identification

Identify specific attack patterns to fine-tune mitigation:

SYN Flood Detection:

```
index=firewall sourcetype=f5_ltm tcp_flags="SYN"
| stats count by src_ip, dest_port
| where count > 1000
| sort -count
```

HTTP Flood Detection:

```
index=web sourcetype=access_combined
| stats count by clientip, uri
| where count > 500
| sort -count
| eval requests_per_min=count/5
```

DNS Amplification Detection:

```
index=network sourcetype=dns dest_port=53
| stats avg(response_size) as avg_size, count by src_ip
| where avg_size > 512 AND count > 1000
| sort -count
```

7.3 Geographic Analysis

Identify attack origins by geography to implement geo-blocking if necessary:

```
index=firewall sourcetype=fortinet_traffic
| iplocation src_ip
| stats count by Country, City
| sort -count
| head 20
```

7.4 Splunk Dashboards for DDoS

Create dedicated dashboards for DDoS incident response. Key panels should include:

- Traffic volume timeline (last 24 hours)
- Top 20 source IPs by request count
- Protocol distribution pie chart
- Connection state table (ESTABLISHED, SYN_SENT, etc.)
- Geographic heat map of attack sources
- Targeted services/ports (top 10)
- F5/Fortinet mitigation actions timeline
- Alert timeline with severity levels

7.5 Automated Alerting

Configure Splunk alerts to automatically notify response team:

Alert Name	Condition	Threshold	Action
Traffic Spike	Bandwidth exceeds baseline	+200% for 5 min	Email + PagerDuty
High Connection Rate	New connections/sec	>10,000	Email + Slack
Potential SYN Flood	SYN packets without ACK	>5,000/min	PagerDuty
Geo Anomaly	Traffic from rare countries	>1,000 req	Email

8. Escalation Matrix

8.1 Severity Levels

Level	Criteria	Response Team	Notification
P1 - Critical	Total service outage >50 Gbps attack Revenue impact	Full SOC + NOC Senior Management Vendor TAC	Immediate (SMS + Call)
P2 - High	Degraded service 10-50 Gbps attack Customer impact	SOC Lead + NOC Network Engineering	Within 15 min (Email + Slack)
P3 - Medium	Partial impact <10 Gbps attack Internal systems	SOC Analyst NOC Technician	Within 30 min (Email)
P4 - Low	Blocked at edge No service impact Monitoring only	SOC Analyst	Incident log only

8.2 Contact List

Maintain up-to-date contact information for all response team members:

Role	Primary Contact	Backup Contact	Contact Method
SOC Lead	[Name]	[Name]	Mobile: [number]
Network Engineering Lead	[Name]	[Name]	Mobile: [number]
F5 Administrator	[Name]	[Name]	Mobile: [number]
Fortinet Administrator	[Name]	[Name]	Mobile: [number]
ISP Account Manager	[Name]	[Name]	Direct: [number]
Scrubbing Service TAC	N/A	N/A	24/7: [number]
Executive On-Call	[Name]	[Name]	Mobile: [number]

ACTION REQUIRED: Update this table with actual contact information and review quarterly.

9. Post-Incident Activities

9.1 Attack Deactivation

Do not immediately remove all defenses when attack appears to stop. Follow staged deactivation:

Time After Attack	Action	Monitoring
T+0 hours	Maintain all defenses Continue ISP coordination	Watch for attack resumption
T+2 hours	Reduce rate limiting by 50% Maintain geo-blocks	Monitor traffic patterns
T+4 hours	Disable CAPTCHA challenges Relax connection limits	Check service performance
T+12 hours	Remove geo-blocks (if temporary) Restore normal thresholds	Full traffic analysis
T+24 hours	Deactivate ISP scrubbing Revert to baseline config	Continued monitoring

9.2 Incident Documentation

Complete incident report within 24 hours. Required documentation includes:

- Attack timeline (detection, response actions, resolution)
- Attack classification and peak statistics (Gbps, PPS, connections)
- Affected systems and services with downtime duration
- Mitigation measures deployed and their effectiveness
- ISP coordination details and response times
- Business impact assessment (revenue, customers affected)
- Splunk queries and analysis results
- Packet captures (PCAPs) and traffic samples
- Configuration changes made during incident
- Lessons learned and improvement recommendations

9.3 Post-Incident Review Meeting

Schedule post-incident review within 72 hours. Agenda should cover:

- Incident timeline review and response time analysis
- Effectiveness of detection mechanisms
- Mitigation strategy evaluation (what worked, what didn't)
- Communication effectiveness (internal and external)

- Resource adequacy (staffing, tools, bandwidth)
- Procedural gaps or documentation issues
- Action items for improvement with owners and deadlines
- Budget requests for enhanced defenses if needed

9.4 Defensive Improvements

Based on attack analysis, implement improvements to prevent or mitigate future attacks:

- Update baseline traffic profiles in F5/Fortinet devices
- Add identified attack signatures to IPS/IDS rules
- Implement permanent geo-blocking for confirmed hostile regions
- Adjust rate limiting thresholds based on attack patterns
- Enhance monitoring with new Splunk dashboards and alerts
- Update network capacity planning if attack exceeded current limits
- Review and update ISP coordination procedures
- Conduct tabletop exercise to validate runbook improvements
- Train additional staff on DDoS response procedures

10. Appendices

Appendix A: Quick Reference Command Guide

F5 BIG-IP Commands:

```
# Show current connections per source IP

tmsh show sys connection cs-server-addr

# Display AFM statistics

tmsh show security firewall global-rules-statistics

# Check DoS profile status

tmsh show security dos profile [profile-name]

# View active iRules

tmsh list ltm rule

# Monitor virtual server stats

tmsh show ltm virtual [virtual-name]
```

Fortinet FortiGate Commands:

```
# Show current sessions

diagnose sys session list

# Display DoS policy statistics

diagnose firewall iprope list 100

# Check CPU and memory

get system performance status

# View active DoS sensors

diagnose test application dosd

# Monitor interface traffic

diagnose ip address list
```

Appendix B: Attack Signature Reference

Attack Type	Packet Characteristics	Detection Method
SYN Flood	High SYN, low ACK ratio Same dest port	Connection state analysis SYN/ACK ratio

UDP Flood	High volume UDP Random source ports	PPS threshold Protocol ratio
HTTP GET Flood	Excessive HTTP GET Low payload size	Request rate User-Agent analysis
Slowloris	Slow HTTP headers Incomplete requests	Connection duration Request completion time
DNS Amplification	Large DNS responses Spoofed source IPs	Response size QTYPE = ANY queries
NTP Amplification	Large NTP responses Mode 7 monlist	Packet size >400 bytes Source port 123

Appendix C: Splunk Search Quick Reference

Use Case:

```
Search Query
```

Top Talkers:

```
index=netflow | stats sum(bytes) as total by src_ip | sort -total | head 20
```

Attack Duration:

```
index=firewall action=deny | timechart span=1m count | where count>1000
```

Port Scan Detection:

```
index=firewall | stats dc(dest_port) as ports by src_ip | where ports>100
```

Botnet C2 Detection:

```
index=firewall | stats dc(dest_ip) as unique_dest by src_ip | where unique_dest>50
```

Appendix D: Incident Response Checklist

Phase	Task	Completed
Detection	Confirm attack vs. legitimate traffic spike	■
	Classify attack type and severity	■
	Activate incident response team	■
Initial Response	Enable F5 AFM/ASM protections	■
	Activate Fortinet DoS policies	■
	Start packet capture and logging	■
	Begin Splunk analysis	■

Mitigation	Deploy rate limiting and filtering	■
	Enable CAPTCHA/bot detection (if L7)	■
	Contact ISP if needed	■
	Activate scrubbing service if needed	■
Monitoring	Track attack metrics in real-time	■
	Monitor service availability	■
	Update stakeholders every 30 minutes	■
Recovery	Staged deactivation of defenses	■
	Complete incident documentation	■
	Schedule post-incident review	■
	Implement improvements	■

This runbook should be reviewed and updated quarterly or after each major incident. All personnel involved in DDoS response should be familiar with these procedures and participate in regular tabletop exercises.