

DDoS Readiness 2026 Checklist

Three attack categories. Upstream defenses. Practiced response.

Know the Category — Know the Defense

VOLUMETRIC

L3/4 • Gbps-Tbps

Techniques:

UDP flood, DNS/NTP/Memcached amp

Defense:

Cloud scrubbing

PROTOCOL

L3/4 • Packets/sec

Techniques:

SYN flood, Smurf, Ping of Death

Defense:

SYN cookies + firewall

APPLICATION

L7 • Requests/sec

Techniques:

HTTP flood, Slowloris, endpoint spam

Defense:

WAF + rate limiting

Amplification Factors — Block These Protocols Outbound

DNS

60B in
~5KB out
50-100x

NTP

60B in
~30KB out
500x

SSDP

70B in
~30KB out
~30x

CharGen

20B in
~7KB out
~350x

Memcached

15B in
~750KB out
50,000x+

LDAP

50B in
~2KB out
~46x

Detection Signals to Monitor

VOLUME

- 10x-100x bandwidth spike
- Sustained (not burst)
- ISP alerts you
- Users report slow/down

SOURCES

- Unfamiliar IP ranges
- Unusual geography
- Cloud provider IPs
- Botnet fingerprints

PROTOCOL

- Half-open TCP conns
- Connection table full
- SYN with no ACK
- TCP retransmits climbing

APP LAYER

- Endpoint response times up
- Same URL hit repeatedly
- Pool exhaustion
- CDN sees it first

Defense Stack — Filter Upstream

- ☐ **Cloud DDoS Protection**
Cloudflare / AWS Shield / Akamai / Google Cloud Armor in front of everything public
- ☐ **CDN + Anycast**
Distribute origin — attackers can't easily focus fire on one node
- ☐ **Web Application Firewall**
Rate limits, bot detection, JS challenges. Modern behavioral analysis.
- ☐ **App-Tier Rate Limits**
Per-IP caps, expensive endpoints get stricter limits than static content
- ☐ **BGP Blackhole Routing**
Emergency null-route. You go dark, but the attack stops. Last resort.
- ☐ **DDoS Runbook**
Provider contacts, comms templates, escalation paths. Tabletop it.

When It Hits — First 30 Minutes

Verify

Confirm attack — check monitoring, ISP, edge provider

Classify

Which category? (Volume / Protocol / App). Which endpoints?

Engage

Call cloud DDoS provider. Enable emergency mitigation.

Watch

Look for exfil / lateral movement — DDoS may be a distraction

Communicate

Status page. Customer comms. Executive brief.

Watch the full breakdown → youtube.com/@nasscybercorner

© Nas's Cyber Corner • ATK-04