# DDoS Protection Sizing

F5 Distributed Cloud DDoS Mitigation provides multi-terabit protection against L3/L4 volumetric attacks and L7 application-layer attacks with always-on or on-demand deployment options.

---

## DDoS Requirements Assessment

### DDoS Attack History

Have you experienced DDoS attacks in the past?

- Yes - Frequent attacks (monthly or more)
- Yes - Occasional attacks (quarterly)
- Yes - Rare attacks (annually or less)
- No - But we want proactive protection
- Unknown

If yes, describe recent attacks:

| DATE | ATTACK TYPE | PEAK SIZE | DURATION | IMPACT |
|---|---|---|---|---|
| Enter valu | Enter valu | Enter valu Gbps | Enter valu min | Enter valu |
| Enter valu | Enter valu | Enter valu Gbps | Enter valu min | Enter valu |
| Enter valu | Enter valu | Enter valu Gbps | Enter valu min | Enter valu |

---

## Network Infrastructure

### Customer ASN

Does your company have an Autonomous System Number (ASN) assigned by an Internet Authority?

- **YES** - ASN: _____
- **NO**

> **⚠ No ASN**
>
> If you do not have an Autonomous System Number, please inform your F5 Sales Specialist immediately as this affects BGP-based DDoS mitigation options.

### BGP Network Prefix

Have you been assigned a network prefix by your ISP or Internet authority to announce via BGP using your ASN?

- **YES**
- **NO**

> **✎ Prefix Size Requirements**
>
> The network prefix size must be a /24 or shorter (/23, /22, /21, etc.). If you do not have a network prefix assigned and under control of your ASN, please inform your F5 Sales Specialist immediately.

If yes, list your network prefixes:

| PREFIX (CIDR) | SIZE | ANNOUNCED VIA BGP? |
|---|---|---|
| Enter value | / Enter value | ◯ Yes ◯ No |
| Enter value | / Enter value | ◯ Yes ◯ No |
| Enter value | / Enter value | ◯ Yes ◯ No |
| Enter value | / Enter value | ◯ Yes ◯ No |

Total number of prefixes:

## Data Center Infrastructure

### Data Centers

How many data centers do you need to protect from DDoS attacks?

| DATA CENTER LOCATION | PROVIDER | ROUTER COUNT |
|---|---|---|
| Enter value | ○ On-Prem ○ Colo ○ Cloud | Enter value |
| Enter value | ○ On-Prem ○ Colo ○ Cloud | Enter value |
| Enter value | ○ On-Prem ○ Colo ○ Cloud | Enter value |
| Enter value | ○ On-Prem ○ Colo ○ Cloud | Enter value |

**Total Data Centers:**

## Edge Routers

How many EDGE/CORE/BORDER routers do you want F5 to monitor for DDoS attack detection?

| ROUTER LOCATION | ROUTER TYPE | VENDOR/MODEL |
|---|---|---|
| Enter value | ○ Edge ○ Core ○ Border | Enter value |
| Enter value | ○ Edge ○ Core ○ Border | Enter value |
| Enter value | ○ Edge ○ Core ○ Border | Enter value |
| Enter value | ○ Edge ○ Core ○ Border | Enter value |

**Total Edge Routers:**

## Bandwidth Requirements

### Clean Bandwidth

Please provide the amount of **CLEAN BANDWIDTH** utilized by the network prefixes you would like to protect:

| METRIC | VALUE |
| --- | --- |
| **95th Percentile Inbound Bandwidth** | Enter value Mbps |
| **Peak Inbound Bandwidth** | Enter value Mbps |
| **Average Inbound Bandwidth** | Enter value Mbps |

> **Measurement**
>
> The bandwidth measurement should be provided in Mbps, calculated using 95th percentile usage, for **INBOUND TRAFFIC ONLY**.

### Current Internet Connectivity

What is your total internet connectivity capacity?

| METRIC | VALUE |
| --- | --- |
| **Total uplink capacity** | Enter value Gbps |
| **Number of ISP connections** | Enter value |
| **ISP providers** | Enter value |

---

## Protection Mode

### Mode of Protection

Please select your preferred protection mode:

- **CONTINUOUS (Always On)**
- All traffic routed through F5 at all times
- Zero detection/mitigation delay
- Best for high-value, frequently-targeted assets
- **ON-DEMAND (Always Available)**
- Traffic routes normally until attack detected
- Mitigation activates upon detection
- Cost-effective for less frequently attacked assets

### Activation Method (On-Demand Only)

If On-Demand, how should mitigation be activated?

- Automatic (F5 detects attack and activates)
- Manual (Customer initiates activation)
- Hybrid (Auto-detect with manual confirmation)

Acceptable time to mitigate after detection:

## Attack Types

### L3/L4 Volumetric Attacks

Attack types to protect against:

- UDP Floods
- TCP SYN Floods
- TCP ACK Floods
- ICMP Floods
- DNS Amplification
- NTP Amplification
- SSDP Amplification
- Memcached Amplification
- Fragmentation Attacks
- Teardrop Attacks
- Smurf Attacks

### L7 Application-Layer Attacks

- Yes - Requires Advanced tier or WAF
- No

Attack types to protect against:

- HTTP Floods
- Slowloris
- Slow POST
- DNS Query Floods
- SSL/TLS Exhaustion
- API Abuse
- Login Page Attacks

> ⚠ **L7 DDoS**
>
> Layer 7 DDoS mitigation with ML-based anomaly detection requires the Advanced WAAP tier.

---

## Detection and Alerting

### Detection Requirements

How should DDoS attacks be detected?

- [ ] Traffic analysis on edge routers (NetFlow/sFlow)
- [ ] Inline detection (Always On mode)
- [ ] External monitoring integration

### Alerting Requirements

How do you want to be notified of attacks?

- [ ] Email alerts
- [ ] SMS/Text alerts
- [ ] Phone call (24x7 SOC)
- [ ] Webhook/API integration
- [ ] SIEM integration

Alert contacts:

| NAME | ROLE | EMAIL | PHONE |
|---|---|---|---|
| Enter value | Primary | Enter value | Enter value |
| Enter value | Secondary | Enter value | Enter value |
| Enter value | Escalation | Enter value | Enter value |

### Reporting Requirements

What DDoS reporting do you need?

- Real-time attack dashboard
- Post-attack reports
- Monthly summary reports
- Custom reporting

---

## Integration Requirements

### BGP Integration

Will you establish BGP sessions with F5 for traffic diversion?

- Yes - Direct BGP peering
- Yes - Through IX (Internet Exchange)
- No - DNS-based diversion only

BGP session details (if applicable):

| PEER LOCATION | YOUR ROUTER IP | F5 PEER IP |
|---|---|---|
| Enter value | Enter value | TBD |
| Enter value | Enter value | TBD |

### GRE Tunnel Requirements

- Yes - GRE tunnels to our routers
- No - Direct routing

Number of GRE tunnel endpoints:

### Existing DDoS Solutions

Do you have existing DDoS protection?

| SOLUTION | PROVIDER | REPLACE OR LAYER? |
|---|---|---|
| Enter value | Enter value | ○ Replace<br>○ Layer |

---

## Service Level Requirements

### SLA Requirements

What SLA requirements do you have?

| METRIC | REQUIREMENT |
| --- | --- |
| **Time to Detect** | < Enter value minutes |
| **Time to Mitigate** | < Enter value minutes |
| **Uptime SLA** | Enter value % |
| **False Positive Rate** | < Enter value % |

### Support Level

What level of DDoS support do you need?

- **Standard** - Business hours support
- **Enhanced** - 24x7 SOC monitoring
- **Enhanced Plus** - Dedicated SOC resources

---

## Summary: DDoS Protection Requirements

| REQUIREMENT | VALUE |
| --- | --- |
| **Customer ASN** | ◯ Yes ◯ No |
| **Number of Prefixes** | Enter value |
| **Number of Data Centers** | Enter value |
| **Number of Edge Routers** | Enter value |
| **Clean Bandwidth (95th percentile)** | Enter value Mbps |
| **Protection Mode** | ◯ Always On ◯ On-Demand |
| **L3/L4 Protection** | ◯ Yes ◯ No |
| **L7 Protection** | ◯ Yes ◯ No |
| **Support Level** | ◯ Standard ◯ Enhanced ◯ Enhanced Plus |

Network diagram attached: ☐ Yes ☐ No

Additional notes or special requirements: