

# Web Application Firewall (WAF) Sizing

The F5 Distributed Cloud WAF provides comprehensive protection against web application attacks including OWASP Top 10 vulnerabilities, injection attacks, cross-site scripting, and advanced threats.

## Application Inventory

### Application Count

How many web applications require WAF protection?

CATEGORY	COUNT
Production Applications	<div>Enter value</div>
Staging/QA Applications	<div>Enter value</div>
Development Applications	<div>Enter value</div>
Total Applications	<div>Enter value</div>

### Application Details

For each major application, provide the following:

APPLICATION NAME	DOMAIN/FQDN	ENVIRONMENT	PROTOCOL	CRITICALITY
<input type="text" value="Enter value"/>	<input type="text" value="Enter value"/>	<input type="checkbox"/> Prod <input type="checkbox"/> Stage <input type="checkbox"/> Dev	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS	<input type="checkbox"/> Critical <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low
<input type="text" value="Enter value"/>	<input type="text" value="Enter value"/>	<input type="checkbox"/> Prod <input type="checkbox"/> Stage <input type="checkbox"/> Dev	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS	<input type="checkbox"/> Critical <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low
<input type="text" value="Enter value"/>	<input type="text" value="Enter value"/>	<input type="checkbox"/> Prod <input type="checkbox"/> Stage <input type="checkbox"/> Dev	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS	<input type="checkbox"/> Critical <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low
<input type="text" value="Enter value"/>	<input type="text" value="Enter value"/>	<input type="checkbox"/> Prod <input type="checkbox"/> Stage <input type="checkbox"/> Dev	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS	<input type="checkbox"/> Critical <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low
<input type="text" value="Enter value"/>	<input type="text" value="Enter value"/>	<input type="checkbox"/> Prod <input type="checkbox"/> Stage <input type="checkbox"/> Dev	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS	<input type="checkbox"/> Critical <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low

### Additional Applications

If you have more than 5 applications, please attach a separate spreadsheet with complete details.

## Application Architecture

What types of applications are you protecting?

- ☒ Traditional web applications (server-rendered HTML)
  - ☒ Single Page Applications (SPA) - React, Angular, Vue
  - ☒ Mobile application backends
  - ☒ API-only services (covered in API Security section)
  - ☒ Legacy applications
  - ☒ Microservices
  - ☒ Other: \_\_\_\_
- 

## Traffic Volume

### Request Volume

Provide estimated request volumes:

METRIC	AVERAGE	PEAK
Requests per Second (RPS)	<input type="text" value="Enter value"/>	<input type="text" value="Enter value"/>
Requests per Day	<input type="text" value="Enter value"/>	<input type="text" value="Enter value"/>
Requests per Month	<input type="text" value="Enter value"/>	<input type="text" value="Enter value"/>

### Base Package Includes

Standard tier includes 30 million requests per month from Regional Edges.

Bandwidth

Metric	Value	Unit
Average Inbound Bandwidth	<div>Enter value</div>	Mbps
Peak Inbound Bandwidth	<div>Enter value</div>	Mbps
Average Response Size	<div>Enter value</div>	KB

Geographic Distribution

Where are your users located?

Region	Percentage of Traffic
North America	<div>Enter value</div> %
Europe	<div>Enter value</div> %
Asia-Pacific	<div>Enter value</div> %
South America	<div>Enter value</div> %
Middle East / Africa	<div>Enter value</div> %
Total	100%

## WAF Features Required

### Core Protection

Which attack types do you need to protect against?

- ☒ SQL Injection
- ☒ Cross-Site Scripting (XSS)
- ☒ Cross-Site Request Forgery (CSRF)
- ☒ Remote File Inclusion (RFI)
- ☒ Local File Inclusion (LFI)
- ☒ Command Injection
- ☒ XML External Entity (XXE)
- ☒ Server-Side Request Forgery (SSRF)
- ☒ HTTP Protocol Violations
- ☒ HTTP Request Smuggling
- ☒ All OWASP Top 10

### Advanced Features

Do you require the following advanced features?

FEATURE	REQUIRED	NOTES
Automatic Signature Tuning	<input type="checkbox"/> Yes <input type="checkbox"/> No	Reduces false positives automatically
Threat Campaigns	<input type="checkbox"/> Yes <input type="checkbox"/> No	Advanced tier - vetted attack signatures
Malicious User Detection	<input type="checkbox"/> Yes <input type="checkbox"/> No	Advanced tier - behavioral scoring
Data Masking	<input type="checkbox"/> Yes <input type="checkbox"/> No	Mask sensitive data in logs
Custom Rules	<input type="checkbox"/> Yes <input type="checkbox"/> No	Organization-specific signatures

## Operating Mode

What WAF operating mode do you prefer?

- ☒ **Blocking Mode** - Block malicious requests immediately
- ☒ **Monitoring Mode** - Log but don't block (for initial deployment)
- ☒ **Start in Monitoring, transition to Blocking** after tuning period

Tuning period preference: \_\_\_\_ days/weeks

---

## Origin Infrastructure

### Origin Server Locations

Where are your application origin servers hosted?

LOCATION	COUNT	PROVIDER
<b>AWS</b>	<input type="text" value="Enter value"/>	Region(s): <input type="text" value="Enter value"/>
<b>Azure</b>	<input type="text" value="Enter value"/>	Region(s): <input type="text" value="Enter value"/>
<b>Google Cloud</b>	<input type="text" value="Enter value"/>	Region(s): <input type="text" value="Enter value"/>
<b>On-Premises Data Center</b>	<input type="text" value="Enter value"/>	Location(s): <input type="text" value="Enter value"/>
<b>Other Cloud</b>	<input type="text" value="Enter value"/>	Provider: <input type="text" value="Enter value"/>

## Origin Connectivity

How will F5 XC connect to your origin servers?

- ☒ Public Internet (origin servers have public IPs)
- ☒ Private connectivity via Customer Edge sites
- ☒ Direct cloud connectivity (AWS Direct Connect, Azure ExpressRoute, etc.)
- ☒ VPN tunnels

## High Availability

Do you have multiple origin servers per application?

- ☒ Yes - Active/Active load balancing
- ☒ Yes - Active/Standby failover

☒ No - Single origin server

Number of origin servers per application: \_\_\_\_

## TLS/SSL Configuration

### Certificate Management

How do you want to manage TLS certificates?

- ☒ **Automatic** - F5 XC provisions and manages certificates
- ☒ **Custom** - We will provide our own certificates
- ☒ **Mixed** - Automatic for some, custom for others

### Certificate Details (if Custom)

DOMAIN	CERTIFICATE TYPE	EXPIRATION	NOTES
<input type="text" value="Enter value"/>	<input type="checkbox"/> Single <input type="checkbox"/> Wildcard <input type="checkbox"/> SAN	<input type="text" value="Enter value"/>	<input type="text" value="Enter value"/>
<input type="text" value="Enter value"/>	<input type="checkbox"/> Single <input type="checkbox"/> Wildcard <input type="checkbox"/> SAN	<input type="text" value="Enter value"/>	<input type="text" value="Enter value"/>
<input type="text" value="Enter value"/>	<input type="checkbox"/> Single <input type="checkbox"/> Wildcard <input type="checkbox"/> SAN	<input type="text" value="Enter value"/>	<input type="text" value="Enter value"/>

### TLS Requirements

- Minimum TLS version required: ☐ TLS 1.2 ☐ TLS 1.3
- Do you require mTLS (Mutual TLS)? ☐ Yes ☐ No



- Cipher suite requirements: \_\_\_\_

## Service Policies

### Access Control Requirements

- ☒ IP Allowlisting (only allow specific IPs)
- ☒ IP Denylisting (block specific IPs)
- ☒ Geographic restrictions (block certain countries)

Number of IP prefixes to manage: \_\_\_\_

### Rate Limiting

- ☒ Yes
- ☒ No

If yes, provide requirements:

SCOPE	LIMIT	TIME WINDOW
Per IP Address	<div>Enter value</div> requests	<div>Enter value</div> seconds
Per User	<div>Enter value</div> requests	<div>Enter value</div> seconds
Per API Endpoint	<div>Enter value</div> requests	<div>Enter value</div> seconds

### Geographic Blocking (OFAC Compliance)

- ☒ Yes - OFAC sanctioned countries

☒ Yes - Custom country list

☒ No

Countries to block: \_\_\_\_

---

## Logging and Observability

### Log Requirements

What logging capabilities do you need?

☒ Security event logging (blocked requests)

☒ All request logging

☒ Performance metrics

☒ Custom log formats

### Log Destinations

Where should logs be sent?

☒ F5 XC Console (included)

☒ Splunk

☒ Datadog

☒ AWS S3

☒ Azure Blob Storage

☒ Sumo Logic

☒ Other SIEM: \_\_\_\_

### Retention Requirements

Log retention period required: \_\_\_\_ days

---

## Support and Management

## Support Requirements

What level of support do you need?

- ☒ **Standard** - Business hours support
- ☒ **Enhanced** - 24x7 support with named resources
- ☒ **Enhanced Plus** - 24x7 support with dedicated resources + SOC

## Managed Services

Do you want F5 to manage WAF policies?

- ☒ **Self-Service** - We will manage policies ourselves
- ☒ **Managed** - F5 SOC manages policies with our input
- ☒ **Hybrid** - Shared responsibility

## Summary: WAF Requirements

REQUIREMENT	VALUE
Number of Applications	<input type="text" value="Enter value"/>
Estimated Monthly Requests	<input type="text" value="Enter value"/>
Tier Required	<input type="checkbox"/> Standard <input type="checkbox"/> Advanced
Support Level	<input type="checkbox"/> Standard <input type="checkbox"/> Enhanced <input type="checkbox"/> Enhanced Plus
Primary Deployment Region	<input type="text" value="Enter value"/>

Additional notes or special requirements:



