

# F5 Distributed Cloud

---

## Scoping and Requirements Guide

*F5 Networks*

*None*

## Table of Contents

---

1. F5 Distributed Cloud Sizing Guide	3
2. Web Application Firewall (WAF) Sizing	4
3. API Security Sizing	14
4. Bot Defense Sizing	24
5. DDoS Protection Sizing	34
6. Client-Side Defense Sizing	45
7. HTTP Load Balancer Sizing	53
8. TCP Load Balancer Sizing	63
9. DNS Services Sizing	69
10. Multi-Cloud Networking Sizing	78
11. App Connect Sizing	87
12. CDN Sizing	94
13. Edge Compute Sizing	101
14. Customer Edge Sites Sizing	106
15. Cloud Sites Sizing	114

# 1. F5 Distributed Cloud Sizing Guide

---

Welcome to the **F5 Distributed Cloud Customer Scoping and Requirements Guide**. This comprehensive questionnaire will help accurately evaluate your environment prior to deploying F5 Distributed Cloud solutions.

## 2. 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.

### 2.1 Application Inventory

#### Application Count

How many web applications require WAF protection?

Category	Count
Production Applications	_____
Staging/QA Applications	_____
Development Applications	_____
<b>Total Applications</b>	_____

## Application Details

For each major application, provide the following:

Application Name	Domain/ FQDN	Environment	Protocol	Criticality
_____	_____	[ ] Prod [ ] Stage [ ] Dev	[ ] HTTP [ ] HTTPS	[ ] Critical [ ] High [ ] Medium [ ] Low
_____	_____	[ ] Prod [ ] Stage [ ] Dev	[ ] HTTP [ ] HTTPS	[ ] Critical [ ] High [ ] Medium [ ] Low
_____	_____	[ ] Prod [ ] Stage [ ] Dev	[ ] HTTP [ ] HTTPS	[ ] Critical [ ] High [ ] Medium [ ] Low
_____	_____	[ ] Prod [ ] Stage [ ] Dev	[ ] HTTP [ ] HTTPS	[ ] Critical [ ] High [ ] Medium [ ] Low
_____	_____	[ ] Prod [ ] Stage [ ] Dev	[ ] HTTP [ ] HTTPS	[ ] Critical [ ] High [ ] Medium [ ] 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: \_\_\_\_\_

## 2.2 Traffic Volume

### Request Volume

Provide estimated request volumes:

Metric	Average	Peak
Requests per Second (RPS)	____	____
Requests per Day	____	____
Requests per Month	____	____

#### Base Package Includes

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

### Bandwidth

Metric	Value	Unit
Average Inbound Bandwidth	____	Mbps
Peak Inbound Bandwidth	____	Mbps
Average Response Size	____	KB

## Geographic Distribution

Where are your users located?

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

## 2.3 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	[ ] Yes [ ] No	Reduces false positives automatically
Threat Campaigns	[ ] Yes [ ] No	Advanced tier - vetted attack signatures
Malicious User Detection	[ ] Yes [ ] No	Advanced tier - behavioral scoring
Data Masking	[ ] Yes [ ] No	Mask sensitive data in logs
Custom Rules	[ ] Yes [ ] 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

---

## 2.4 Origin Infrastructure

### Origin Server Locations

Where are your application origin servers hosted?

Location	Count	Provider
AWS	____	Region(s): _____
Azure	____	Region(s): _____
Google Cloud	____	Region(s): _____
On-Premises Data Center	____	Location(s): _____
Other Cloud	____	Provider: _____

### 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: \_\_\_\_\_

## 2.5 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
_____	[ ] Single [ ] Wildcard [ ] SAN	---	---
_____	[ ] Single [ ] Wildcard [ ] SAN	---	---
_____	[ ] Single [ ] Wildcard [ ] SAN	---	---

### TLS Requirements

- Minimum TLS version required: [ ] TLS 1.2 [ ] TLS 1.3
- Do you require mTLS (Mutual TLS)? [ ] Yes [ ] No
- Cipher suite requirements: \_\_\_\_\_

## 2.6 Service Policies

### Access Control Requirements

- Allowlisting (only allow specific IPs)
- 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	_____ requests	_____ seconds
Per User	_____ requests	_____ seconds
Per API Endpoint	_____ requests	_____ seconds

## Geographic Blocking (OFAC Compliance)

Yes - OFAC sanctioned countries

Yes - Custom country list

No

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

## 2.7 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
- Lumo Logic
- Other SIEM: \_\_\_\_\_

## Retention Requirements

---

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

---

## 2.8 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
-

## 2.9 Summary: WAF Requirements

Requirement	Value
Number of Applications	_____
Estimated Monthly Requests	_____
Tier Required	[ ] Standard [ ] Advanced
Support Level	[ ] Standard [ ] Enhanced [ ] Enhanced Plus
Primary Deployment Region	_____

Additional notes or special requirements:

-----  
-----  
-----

# 3. API Security Sizing

F5 Distributed Cloud API Security provides comprehensive protection for your APIs including automatic discovery, schema validation, rate limiting, and behavioral analysis.

## 3.1 API Inventory

### API Discovery Requirements

Do you have complete documentation of all your APIs?

- Yes - All APIs are documented with OpenAPI/Swagger specs
- Partial - Some APIs are documented
- No - We need to discover our API landscape

#### Shadow API Discovery

F5 XC can automatically discover APIs in your traffic, including

undocumented "shadow" APIs that may pose security risks.

### Known API Count

If you know your API landscape, provide details:

Category	Count
Public APIs (internet-facing)	_____
Partner APIs (B2B)	_____
Internal APIs	_____
<b>Total API Endpoints</b>	_____

## API Details

For major API services, provide:

API Name/ Service	Base Path	Protocol	Auth Method	Documentation
——	/api/v1/...	[ ] REST [ ] GraphQL [ ] gRPC	[ ] API Key [ ] OAuth [ ] JWT [ ] None	[ ] OpenAPI [ ] None
——	/api/v1/...	[ ] REST [ ] GraphQL [ ] gRPC	[ ] API Key [ ] OAuth [ ] JWT [ ] None	[ ] OpenAPI [ ] None
——	/api/v1/...	[ ] REST [ ] GraphQL [ ] gRPC	[ ] API Key [ ] OAuth [ ] JWT [ ] None	[ ] OpenAPI [ ] None
——	/api/v1/...	[ ] REST [ ] GraphQL [ ] gRPC	[ ] API Key [ ] OAuth [ ] JWT [ ] None	[ ] OpenAPI [ ] None

## 3.2 API Traffic Volume

### Request Volume

Metric	Average	Peak
API Requests per Second	——	——
API Requests per Day	——	——
API Requests per Month	——	——

#### Base Package

Standard includes up to 500,000 API requests per month for API protection.

## API Consumer Distribution

Who consumes your APIs?

Consumer Type	Percentage	Estimated Daily Requests
Web Applications (browsers)	_____%	_____
Mobile Applications	_____%	_____
Partner Integrations (B2B)	_____%	_____
Internal Services (M2M)	_____%	_____
Third-Party Developers	_____%	_____
<b>Total</b>	100%	_____

## 3.3 API Security Features Required

### API Discovery

- Yes - **Critical** - We need to discover all APIs in our traffic
- Yes - **Nice to have** - We have docs but want validation
- No - We have complete API documentation

Discovery scope:

- Production traffic only
- All environments (Prod, Stage, Dev)

### API Schema Validation

- Yes - Enforce requests match OpenAPI specification

If yes, what actions should be taken on violations?

Violation Type	Action
Unknown endpoints	[ ] Block [ ] Log Only [ ] Allow
Invalid request parameters	[ ] Block [ ] Log Only [ ] Allow
Invalid request body	[ ] Block [ ] Log Only [ ] Allow
Missing required fields	[ ] Block [ ] Log Only [ ] Allow
Wrong data types	[ ] Block [ ] Log Only [ ] Allow

## API Rate Limiting

Yes

No

If yes, provide requirements:

Rate Limit Type	Limit	Time Window	Action
Per API Key	_____ requests	[ ] second [ ] minute [ ] hour	[ ] Block [ ] Throttle
Per User/Token	_____ requests	[ ] second [ ] minute [ ] hour	[ ] Block [ ] Throttle
Per Endpoint	_____ requests	[ ] second [ ] minute [ ] hour	[ ] Block [ ] Throttle
Per IP Address	_____ requests	[ ] second [ ] minute [ ] hour	[ ] Block [ ] Throttle
Global (all traffic)	_____ requests	[ ] second [ ] minute [ ] hour	[ ] Block [ ] Throttle

## Sensitive Data Protection

Yes

No

If yes, what data types need detection?

- Credit Card Numbers (PCI-DSS)
- Social Security Numbers
- Email Addresses
- Phone Numbers
- Healthcare Data (HIPAA)
- Custom Patterns: \_\_\_\_\_

What action should be taken when sensitive data is detected?

- Block the request/response
  - Mask the data in transit
  - Log and alert only
  - Allow (detection only)
- 

## 3.4 API Authentication and Authorization

### Authentication Methods

What authentication methods do your APIs use?

- API Keys (header or query parameter)
- OAuth 2.0 / OpenID Connect
- JWT (JSON Web Tokens)
- Basic Authentication
- Mutual TLS (mTLS)
- Custom authentication
- No authentication (public APIs)

## JWT Validation

If using JWT, do you need F5 XC to validate tokens?

- Yes - Validate JWT signatures
- Yes - Validate JWT claims (expiration, audience, etc.)
- No - Application handles JWT validation

JWT issuer (if applicable): \_\_\_\_\_

## Authorization Requirements

- Yes - Enforce role-based access to API endpoints
  - No - Application handles authorization
- 

## 3.5 API Security Threats

### OWASP API Security Top 10

Which API-specific threats are you concerned about?

- API1 - Broken Object Level Authorization
- API2 - Broken Authentication
- API3 - Broken Object Property Level Authorization
- API4 - Unrestricted Resource Consumption
- API5 - Broken Function Level Authorization
- API6 - Unrestricted Access to Sensitive Business Flows
- API7 - Server Side Request Forgery (SSRF)
- API8 - Security Misconfiguration
- API9 - Improper Inventory Management
- API10 - Unsafe Consumption of APIs

## Historical API Attacks

Have you experienced any API-specific attacks?

- API scraping / data harvesting
- Credential stuffing on login APIs
- Abuse of business logic
- Inventory/pricing manipulation
- Enumeration attacks
- None / Unknown

Describe any specific concerns:

---

---

## 3.6 OpenAPI Specification Import

### Existing Specifications

Do you have OpenAPI/Swagger specifications for your APIs?

- Yes - OpenAPI 3.x
- Yes - OpenAPI 2.0 (Swagger)
- Partial - Some APIs only
- No - We need to generate specs

### Specification Management

How will you manage API specifications?

- Upload static files to F5 XC
- Automatic sync from API gateway/management platform
- Generate from live traffic discovery
- CI/CD pipeline integration

Number of specification files: \_\_\_\_\_

## Specification Source

Where are your API specifications stored?

- Git repository
- API management platform (Apigee, Kong, etc.)
- Internal documentation system
- AWS API Gateway
- Azure API Management
- Other: \_\_\_\_\_

## 3.7 Advanced API Security (Advanced Tier)

### Behavioral API Security

- Yes - Detect anomalies in API usage patterns
- No - Schema validation is sufficient

#### **A**Advanced Tier Required

Behavioral API security with ML-based anomaly detection requires the

Advanced tier.

### API Posture Management

- Yes - Score APIs based on security risk
- No

### Data Intelligence Tier

What level of data intelligence do you need?

- Basic - Standard PII detection
- Advanced - Custom patterns + compliance data types
- Premium - Full data classification + custom policies

## 3.8 Integration Requirements

### Existing API Infrastructure

Do you have existing API management infrastructure?

Platform	In Use	Integration Needed
AWS API Gateway	[ ]	[ ]
Azure API Management	[ ]	[ ]
Google Apigee	[ ]	[ ]
Kong	[ ]	[ ]
MuleSoft	[ ]	[ ]
Other: ____	[ ]	[ ]

### CI/CD Integration

- Yes - Scan API specs before deployment
- Yes - Security gates in deployment pipeline
- No

CI/CD platforms in use:

- Jenkins
- GitHub Actions
- GitLab CI
- Azure DevOps
- Other: \_\_\_\_\_

## 3.9 Summary: API Security Requirements

Requirement	Value
Number of API Endpoints	—
API Discovery Required	[ ] Yes [ ] No
Estimated Monthly API Requests	—
Schema Validation Required	[ ] Yes [ ] No
Sensitive Data Protection Required	[ ] Yes [ ] No
Tier Required	[ ] Standard [ ] Advanced

Additional notes or special requirements:

---

---

---

# 4. Bot Defense Sizing

F5 Distributed Cloud Bot Defense provides AI/ML-powered protection against automated threats including credential stuffing, account takeover, content scraping, and other bot attacks.

## 4.1 Bot Defense Requirements Assessment

### Current Bot Challenges

What bot-related challenges are you experiencing?

- Credential stuffing attacks
- Account takeover (ATO)
- Content scraping / price scraping
- Inventory hoarding / scalping
- Gift card fraud
- fake account creation
- Spam / form abuse
- Ad fraud / click fraud
- API abuse by bots
- Competitive intelligence bots
- None currently, but want proactive protection

Describe specific bot challenges:

---

---

## 4.2 Application Scope

### Applications Requiring Bot Defense

Which applications need bot protection?

Application/ Domain	Critical Pages	Platform
_____	[ ] Login [ ] Registration [ ] Checkout [ ] Search	[ ] Web [ ] Mobile [ ] API
_____	[ ] Login [ ] Registration [ ] Checkout [ ] Search	[ ] Web [ ] Mobile [ ] API
_____	[ ] Login [ ] Registration [ ] Checkout [ ] Search	[ ] Web [ ] Mobile [ ] API

### FQDNs to Protect

List the fully qualified domain names requiring bot defense:

FQDN	Environment
_____	[ ] Production [ ] Staging
_____	[ ] Production [ ] Staging
_____	[ ] Production [ ] Staging
_____	[ ] Production [ ] Staging

#### Standard Tier

Standard Bot Defense includes protection for 2 FQDNs. Additional FQDNs

require add-ons.

## Mobile Applications

Do you have mobile applications requiring bot protection?

- Yes - iOS applications
- Yes - Android applications
- Yes - Both iOS and Android
- No - Web only

If yes, provide mobile app details:

App Name	Platform	Downloads (est.)
_____	[ ] iOS [ ] Android	_____
_____	[ ] iOS [ ] Android	_____

## 4.3 Traffic Volume

### Transaction Volume

Provide estimated transaction volumes:

Metric	Daily Volume
Total page views / transactions	_____
Login attempts	_____
Registration attempts	_____
Checkout / purchase attempts	_____
Search queries	_____
API calls	_____

### Tier Entitlements

- Standard: Up to 500,000 transactions/day
- Advanced: Up to 1,000,000 transactions/day
- Additional capacity available as add-ons

## Peak Traffic

Metric	Peak Value	When
Peak transactions per day	—	—
Peak transactions per hour	—	—
Seasonal peaks (e.g., Black Friday)	—	—

## Current Bot Traffic Estimate

What percentage of your traffic do you estimate is bot traffic?

- 10%
- 0-25%
- 5-50%
- 0-75%
- 75%
- Unknown - need visibility

## 4.4 Bot Defense Features

### Detection Method

What level of bot detection do you need?

- Signature-Based** (Standard) - Detect known bot frameworks and tools
- Behavioral** (Advanced) - AI/ML analysis of device signals and behavior
- Both** - Maximum protection

## Mitigation Actions

What actions should be taken when bots are detected?

Detection Confidence	Action
High confidence bot	[ ] Block [ ] Challenge [ ] Log only
Medium confidence bot	[ ] Block [ ] Challenge [ ] Log only
Low confidence bot	[ ] Block [ ] Challenge [ ] Log only

Challenge types acceptable:

- JavaScript challenges
- CAPTCHA (as last resort)
- Custom challenge pages

## Specific Bot Types to Address

Which automated threat categories are priorities?

OWASP Automated Threat	Priority	Notes
Credential Stuffing	[ ] Critical [ ] High [ ] Medium [ ] Low [ ] N/A	
Account Takeover	[ ] Critical [ ] High [ ] Medium [ ] Low [ ] N/A	
Carding	[ ] Critical [ ] High [ ] Medium [ ] Low [ ] N/A	
Scraping	[ ] Critical [ ] High [ ] Medium [ ] Low [ ] N/A	
Scalping	[ ] Critical [ ] High [ ] Medium [ ] Low [ ] N/A	
Spamming	[ ] Critical [ ] High [ ] Medium [ ] Low [ ] N/A	
Denial of Inventory	[ ] Critical [ ] High [ ] Medium [ ] Low [ ] N/A	
Sniping	[ ] Critical [ ] High [ ] Medium [ ] Low [ ] N/A	

## 4.5 Integration Requirements

### Deployment Method

How will Bot Defense be deployed?

- F5 XC as reverse proxy (traffic flows through F5)
- JavaScript tag injection only
- Both (recommended for full protection)

### JavaScript Integration

For web applications, how will the Bot Defense JavaScript be injected?

- F5 XC automatic injection (proxy mode)
- Manual insertion in page templates
- Tag manager (Google Tag Manager, etc.)
- DN-based injection

### Mobile SDK Integration

For mobile applications, can you integrate the F5 Mobile SDK?

- Yes - We can add SDK to our mobile apps
- No - Mobile integration not possible
- N/A - No mobile applications

### Existing Bot Solutions

Do you have existing bot management solutions?

Solution	Replace or Integrate
_____	[ ] Replace [ ] Integrate
_____	[ ] Replace [ ] Integrate

## 4.6 Advanced Features (Advanced Tier)

### Device Fingerprinting

Yes - Identify devices across sessions

No

### Content Scraping Protection

Yes - Protect proprietary content, pricing, inventory

No

### Managed Threat Intelligence

Yes - 24x7 SOC monitoring for bot threats

Yes - Custom detection rules developed by F5

Yes - Regular threat briefings

No - Self-service is sufficient

#### A Advanced/Premium Tier

Managed threat intelligence requires Advanced or Premium tier.

## 4.7 Reporting and Analytics

### Visibility Requirements

What bot visibility do you need?

Real-time dashboard of bot activity

Automated threat summaries (monthly)

Detailed attack attribution

Custom reports

## Integration with SIEM/Analytics

Yes - Send to SIEM (Splunk, etc.)

Yes - Send to data lake (S3, etc.)

No - F5 console is sufficient

Target system: \_\_\_\_\_

---

## 4.8 Geographic Distribution

### Bot Engine Regions

Where do you need bot detection infrastructure?

Region	Required
North America	[ ] Yes [ ] No
Europe	[ ] Yes [ ] No
Asia-Pacific	[ ] Yes [ ] No
South America	[ ] Yes [ ] No

#### Tier Entitlements

- Standard: 1 production region, 1 QA region
- Advanced: 6 bot engines across regions
- Premium: Unlimited bot engines

## 4.9 Support Requirements

### Support Level

What level of bot defense support do you need?

- Self-Service** - Manage bot policies yourself
- Enhanced** - 24x7 support with named resources
- Enhanced Plus** - Dedicated resources + managed service

### Onboarding Support

- Yes - Full onboarding support
- Yes - Integration assistance only
- No - Self-service deployment

## 4.10 Summary: Bot Defense Requirements

Requirement	Value
Number of FQDNs	_____
Estimated Daily Transactions	_____
Mobile SDK Required	[ ] Yes [ ] No
Detection Method	[ ] Signature [ ] Behavioral [ ] Both
Tier Required	[ ] Standard [ ] Advanced [ ] Premium
Support Level	[ ] Self-Service [ ] Enhanced [ ] Enhanced Plus

Primary bot threats to address:

1. \_\_\_\_\_
  2. \_\_\_\_\_
  3. \_\_\_\_\_

Additional notes or special requirements:

---

---

---

# 5. 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.

## 5.1 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
____	____	____ Gbps	____ min	____
____	____	____ Gbps	____ min	____
____	____	____ Gbps	____ min	____

## 5.2 Network Infrastructure

### Customer ASN

#### What is an ASN?

An Autonomous System Number (ASN) is a unique identifier assigned by an

Internet authority that identifies a collection of IP networks under a single administrative domain.

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

### What is a Network Prefix?

A network prefix is a range of network addresses (e.g., 192.0.2.0/24)

assigned by your ISP or Internet authority that you can announce via BGP.

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?
____/____	/____	[ ] Yes [ ] No
____/____	/____	[ ] Yes [ ] No
____/____	/____	[ ] Yes [ ] No
____/____	/____	[ ] Yes [ ] No

Total number of prefixes: \_\_\_\_\_

---

## 5.3 Data Center Infrastructure

### Data Centers

#### What is a Data Center?

For DDoS protection sizing, F5 XC quantifies a data center as a physical or

virtual hosting location with a minimum of one to two routers.

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

Data Center Location	Provider	Router Count
_____	[ ] On-Prem [ ] Colo [ ] Cloud	_____
_____	[ ] On-Prem [ ] Colo [ ] Cloud	_____
_____	[ ] On-Prem [ ] Colo [ ] Cloud	_____
_____	[ ] On-Prem [ ] Colo [ ] Cloud	_____

**Total Data Centers:** \_\_\_\_\_

## Edge Routers

### What is an Edge Router?

Edge/Core/Border routers are the routers at the edge of your network that F5

will monitor for DDoS attack detection.

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

Router Location	Router Type	Vendor/Model
_____	[ ] Edge [ ] Core [ ] Border	_____
_____	[ ] Edge [ ] Core [ ] Border	_____
_____	[ ] Edge [ ] Core [ ] Border	_____
_____	[ ] Edge [ ] Core [ ] Border	_____

Total Edge Routers: \_\_\_\_\_

## 5.4 Bandwidth Requirements

### Clean Bandwidth

### What is Clean Bandwidth?

Clean bandwidth is the amount of legitimate traffic (after DDoS mitigation)

that flows to your network prefixes. Measured using 95th percentile for INBOUND TRAFFIC ONLY.

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

Metric	Value
95th Percentile Inbound Bandwidth	_____ Mbps
Peak Inbound Bandwidth	_____ Mbps
Average Inbound Bandwidth	_____ 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	_____ Gbps
Number of ISP connections	_____
ISP providers	_____

## 5.5 Protection Mode

### Mode of Protection

#### Protection Modes

- **ALWAYS ON (Continuous)**: All traffic continuously routes through F5

scrubbing infrastructure. Immediate protection with no detection delay. - **ALWAYS AVAILABLE (On-Demand)**: Protection activates when attacks are detected. Traffic diverts to F5 scrubbing during attacks.

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: \_\_\_\_\_ minutes

---

## 5.6 Attack Types

### L3/L4 Volumetric Attacks

---

Attack types to protect against:

- DDoS Floods
- TCP SYN Floods
- TCP ACK Floods
- ICMP Floods
- NS Amplification
- UDP Amplification
- SDP 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

### DDoS

Layer 7 DDoS mitigation with ML-based anomaly detection requires the

Advanced WAAP tier.

## 5.7 Detection and Alerting

### Detection Requirements

How should DDoS attacks be detected?

- Traffic analysis on edge routers (NetFlow/sFlow)
- Online 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
- IEM integration

Alert contacts:

Name	Role	Email	Phone
_____	Primary	_____	_____
_____	Secondary	_____	_____
_____	Escalation	_____	_____

## Reporting Requirements

What DDoS reporting do you need?

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

## 5.8 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
_____	_____	TBD
_____	_____	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?
_____	_____	[ ] Replace [ ] Layer

---

## 5.9 Service Level Requirements

### SLA Requirements

What SLA requirements do you have?

Metric	Requirement
Time to Detect	< ____ minutes
Time to Mitigate	< ____ minutes
Uptime SLA	____ %
False Positive Rate	< ____ %

### Support Level

What level of DDoS support do you need?

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

## 5.10 Summary: DDoS Protection Requirements

Requirement	Value
Customer ASN	[ ] Yes: <input type="text"/> [ ] No
Number of Prefixes	<input type="text"/>
Number of Data Centers	<input type="text"/>
Number of Edge Routers	<input type="text"/>
Clean Bandwidth (95th percentile)	<input type="text"/> 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:

---



---



---

# 6. Client-Side Defense Sizing

---

F5 Distributed Cloud Client-Side Defense provides protection against Magecart, formjacking, digital skimming, and other malicious JavaScript supply chain attacks.

---

## 6.1 Requirements Assessment

### Client-Side Security Concerns

What client-side threats are you concerned about?

- Magecart attacks** - Credit card skimming via JavaScript
- Formjacking** - Credential theft from forms
- Digital skimming** - PII harvesting
- Supply chain attacks** - Compromised third-party scripts
- Data exfiltration** - Unauthorized data transmission
- Page tampering** - Unauthorized DOM modifications

Have you experienced client-side attacks?

- Yes - Describe: \_\_\_\_\_
  - No
  - Unknown
-

## 6.2 Application Scope

### Pages Requiring Protection

Which pages handle sensitive data and require protection?

Page Type	URL Pattern	Sensitive Data Type
Login pages	_____	[ ] Credentials
Registration forms	_____	[ ] PII
Checkout/Payment	_____	[ ] Payment card data
Account settings	_____	[ ] PII [ ] Financial
Contact forms	_____	[ ] PII
Other: _____	_____	_____

### Transaction Volume

Estimated monthly transactions on protected pages:

Metric	Monthly Volume
Total page views (protected pages)	_____
Form submissions	_____
Payment transactions	_____

#### Base Package

Client-Side Defense includes 1 million transactions in the base package.

## 6.3 JavaScript Environment

### Third-Party Scripts

How many third-party JavaScript resources are loaded on your pages?

Category	Estimated Count
Analytics (Google Analytics, etc.)	_____
Marketing/Advertising	_____
Social media widgets	_____
Chat/Support widgets	_____
Payment processors	_____
A/B testing tools	_____
Other third-party scripts	_____
<b>Total third-party scripts</b>	_____

### Script Sources

Where do your JavaScript resources come from?

- First-party (your own domains)
- CDN-hosted (cdnjs, jsdelivr, etc.)
- Direct third-party domains
- Tag managers (Google Tag Manager, etc.)

List critical third-party script sources:

Script Purpose	Source Domain	Critical?
_____	_____	[ ] Yes [ ] No
_____	_____	[ ] Yes [ ] No
_____	_____	[ ] Yes [ ] No
_____	_____	[ ] Yes [ ] No

## Content Security Policy (CSP)

Do you currently have a Content Security Policy?

- Yes - Strict CSP
  - Yes - Reporting-only mode
  - No - No CSP implemented
  - Unknown
- 

## 6.4 Compliance Requirements

### PCI-DSS Requirements

Are you subject to PCI-DSS compliance?

- Yes - PCI-DSS Level 1
- Yes - PCI-DSS Level 2
- Yes - PCI-DSS Level 3-4
- No

#### PCI-DSS 4.0

PCI-DSS 4.0 includes requirements (6.4.3 and 11.6.1) for monitoring and

controlling client-side scripts on payment pages.

### Other Compliance

Which other compliance frameworks apply?

- DPR
- CPA
- HIPAA
- SOC 2
- Other: \_\_\_\_\_

## 6.5 Detection and Alerting

### Detection Capabilities

What detection capabilities do you need?

- Script behavior monitoring** - Detect changes in script behavior
- Network request monitoring** - Detect unauthorized data exfiltration
- Form field monitoring** - Detect unauthorized form reads
- DOM manipulation detection** - Detect unauthorized page changes
- Page tamper detection** - Detect payment page modifications

### Alerting Requirements

How should you be notified of detected threats?

- Email alerts
- SIEM Console alerts
- Webhook integration
- IEM integration

Alert severity thresholds:

Alert Type	Severity
New third-party script detected	[ ] Critical [ ] High [ ] Medium [ ] Low
Script behavior change	[ ] Critical [ ] High [ ] Medium [ ] Low
Data exfiltration attempt	[ ] Critical [ ] High [ ] Medium [ ] Low
Page tampering detected	[ ] Critical [ ] High [ ] Medium [ ] Low

## 6.6 Mitigation Actions

### Response Actions

What actions should be taken when threats are detected?

Threat Type	Action
Malicious script detected	[ ] Block [ ] Alert only
Data exfiltration attempt	[ ] Block [ ] Alert only
Unauthorized form access	[ ] Block [ ] Alert only
Page tampering	[ ] Block [ ] Alert only

### Blocking Method

If blocking, how should blocking be implemented?

- lock network calls** - Prevent exfiltration to malicious domains
  - remove malicious script** - Strip script from page
  - redirect to safe page** - Show user a warning
- 

## 6.7 Integration

### Deployment Method

How will Client-Side Defense be deployed?

- CSC proxy (automatic JavaScript injection)**
- Manual JavaScript tag insertion**
- IG-IP integration (iApp or native module)**
- CDN integration**

## Existing BIG-IP

Do you have F5 BIG-IP that could integrate with Client-Side Defense?

Yes - BIG-IP version: \_\_\_\_\_

No

---

## 6.8 Page Tamper Protection

### Payment Page Monitoring

If yes, provide payment page URLs:

Payment Page URL	Expected Update Frequency
_____	[ ] Rarely [ ] Monthly [ ] Weekly [ ] Daily
_____	[ ] Rarely [ ] Monthly [ ] Weekly [ ] Daily

## Baseline Management

How often do your payment pages legitimately change?

Rarely (quarterly or less)

Monthly

Weekly

Frequently (daily or more)

---

## 6.9 Summary: Client-Side Defense Requirements

Requirement	Value
Number of Protected Pages	_____
Estimated Monthly Transactions	_____
Third-Party Scripts to Monitor	_____
PCI-DSS Compliance Required	[ ] Yes [ ] No
Page Tamper Protection Required	[ ] Yes [ ] No
Detection Mode	[ ] Monitor [ ] Block

Critical pages requiring protection:

- 1. \_\_\_\_\_
- 2. \_\_\_\_\_
- 3. \_\_\_\_\_

Additional notes or special requirements:

- 
- 
-

# 7. HTTP Load Balancer Sizing

---

F5 Distributed Cloud HTTP Load Balancer provides global application delivery with intelligent routing, health checks, TLS termination, and integration with security services.

---

## 7.1 Load Balancer Requirements

### Application Inventory

How many HTTP/HTTPS applications need load balancing?

Environment	Application Count
Production	_____
Staging/QA	_____
Development	_____
<b>Total</b>	_____

### Virtual Host Details

For each application, provide virtual host information:

Application Name	Domain(s)	Port(s)	Protocol
_____	_____	[ ] 80 [ ] 443 [ ] Other: _____	[ ] HTTP [ ] HTTPS [ ] Both
_____	_____	[ ] 80 [ ] 443 [ ] Other: _____	[ ] HTTP [ ] HTTPS [ ] Both
_____	_____	[ ] 80 [ ] 443 [ ] Other: _____	[ ] HTTP [ ] HTTPS [ ] Both
_____	_____	[ ] 80 [ ] 443 [ ] Other: _____	[ ] HTTP [ ] HTTPS [ ] Both
_____	_____	[ ] 80 [ ] 443 [ ] Other: _____	[ ] HTTP [ ] HTTPS [ ] Both

### Base Package

The base package includes 1 load balancer. Additional load balancers are

available as add-ons.

## 7.2 Traffic Volume

### Request Metrics

Metric	Average	Peak
Requests per second	—	—
Concurrent connections	—	—
Bandwidth (Mbps)	—	—

### Traffic Patterns

What are your traffic patterns?

- steady throughout the day
- business hours peaks
- seasonal peaks (specify): \_\_\_\_\_
- event-driven spikes
- unpredictable

Geographic distribution of users:

Region	Traffic Percentage
North America	_____ %
Europe	_____ %
Asia-Pacific	_____ %
South America	_____ %
Other	_____ %

---

## 7.3 Origin Pool Configuration

### Origin Server Details

For each application, describe origin servers:

Application	Origin Type	Count	Location
_____	[ ] IP [ ] FQDN [ ] K8s Service	_____	_____
_____	[ ] IP [ ] FQDN [ ] K8s Service	_____	_____
_____	[ ] IP [ ] FQDN [ ] K8s Service	_____	_____

### Origin Connectivity

How will F5 XC reach your origin servers?

- **Public Internet** - Origins have public IP addresses
- **Customer Edge** - Via F5 CE deployed in your environment
- **Cloud Site** - Via F5 site in AWS/Azure/GCP
- **Private Link** - Direct cloud connectivity

## Origin Protocol

What protocol to use when connecting to origins?

Application	Origin Protocol	Origin Port
_____	[ ] HTTP [ ] HTTPS	_____
_____	[ ] HTTP [ ] HTTPS	_____
_____	[ ] HTTP [ ] HTTPS	_____

## 7.4 Load Balancing Configuration

### Load Balancing Algorithm

Preferred load balancing algorithm:

- Round Robin** - Distribute evenly across origins
- Least Connections** - Send to origin with fewest active connections
- Random** - Random selection
- Source IP Hash** - Consistent routing based on client IP
- Ring Hash** - Consistent hashing for cache efficiency

### Session Persistence

- Yes - Source IP based
- Yes - Cookie based
- Yes - Header based
- No - Stateless application

Persistence timeout: \_\_\_\_\_ seconds

## Health Checks

Health check requirements:

Parameter	Value
Health check type	[ ] HTTP [ ] HTTPS [ ] TCP
Check interval	_____ seconds
Check path (HTTP)	_____
Expected response code	[ ] 200 [ ] 2xx [ ] Custom: _____
Healthy threshold	_____ consecutive checks
Unhealthy threshold	_____ consecutive checks

## 7.5 TLS Configuration

### TLS Termination

Where should TLS be terminated?

- At F5 XC** - F5 terminates TLS, connects to origin over HTTP/HTTPS
- End-to-End** - F5 terminates and re-encrypts to origin
- Pass-Through** - TLS passes through to origin (TCP LB only)

### Certificate Management

How will TLS certificates be managed?

- Automatic** - F5 XC provisions via Let's Encrypt
- Custom** - We provide our own certificates
- Fixed** - Different per application

Custom certificate details:

Domain	Certificate Type	Key Type
_____	[ ] Single [ ] Wildcard [ ] SAN	[ ] RSA 2048 [ ] RSA 4096 [ ] ECC
_____	[ ] Single [ ] Wildcard [ ] SAN	[ ] RSA 2048 [ ] RSA 4096 [ ] ECC

## TLS Requirements

Requirement	Value
Minimum TLS version	[ ] TLS 1.2 [ ] TLS 1.3
Cipher suite preference	[ ] Default [ ] Custom
HSTS enabled	[ ] Yes [ ] No
HTTP to HTTPS redirect	[ ] Yes [ ] No

## Mutual TLS (mTLS)

Do you require mTLS client authentication?

Yes - Clients must present certificates

No

If yes:

- Client CA certificate source: \_\_\_\_\_
- XFCC header forwarding needed: [ ] Yes [ ] No

---

## 7.6 Traffic Management

### Routing Rules

**Path-based routing** - Route based on URL path

**Header-based routing** - Route based on HTTP headers

**Query parameter routing** - Route based on query strings

### **Method-based routing** - Route based on HTTP method

Example routing requirements:

Condition	Destination
Path: /api/*	API origin pool
Header: X-Version: v2	V2 origin pool
—	—

## Traffic Policies

- Request header insertion/modification
- Response header insertion/modification
- URL rewriting
- Request body buffering
- Response compression

## Timeouts and Limits

Parameter	Value
Request timeout	____ seconds
Idle timeout	____ seconds
Maximum request body size	____ MB

## 7.7 High Availability

### Multi-Region Deployment

- Yes - Active/Active across regions
- Yes - Active/Standby failover
- No - Single region

Regions required:

- North America
- Europe
- Asia-Pacific
- South America

## Origin Failover

---

Do you have multiple origin pools for failover?

- Yes - Automatic failover between pools
- No - Single origin pool

Failover configuration:

Primary Pool	Secondary Pool	Failover Condition
_____	_____	[ ] Health check [ ] Manual

---

## 7.8 Security Integration

### WAF Integration

---

Should WAF be enabled on this load balancer?

- Yes - Apply WAF policy
- No - Load balancing only

### Bot Defense Integration

---

Should Bot Defense be enabled?

- Yes - Apply bot defense
- No

## Service Policies

- Allowlist/denylist
- Geo-blocking
- Rate limiting
- Custom rules

Number of service policy rules: \_\_\_\_\_

---

## 7.9 Observability

### Logging Requirements

What logging do you need?

- Access logs (all requests)
- Security event logs
- Error logs only
- Custom log format

### Log Destinations

Where should logs be sent?

- SXC Console (default)
- External SIEM: \_\_\_\_\_
- Cloud storage (S3, etc.): \_\_\_\_\_

## Metrics and Monitoring

What metrics do you need?

- Request rate
  - Response time / latency
  - Error rates
  - Origin health status
  - Bandwidth utilization
- 

## 7.10 Summary: HTTP Load Balancer Requirements

Requirement	Value
Number of Load Balancers	_____
Total Applications	_____
Estimated Peak RPS	_____
TLS Certificate Management	[ ] Automatic [ ] Custom [ ] Mixed
WAF Integration	[ ] Yes [ ] No
Multi-Region	[ ] Yes [ ] No
Session Persistence	[ ] Yes [ ] No

Additional notes or special requirements:

# 8. TCP Load Balancer Sizing

---

F5 Distributed Cloud TCP Load Balancer provides Layer 4 load balancing for non-HTTP protocols including databases, gaming servers, mail servers, and custom TCP/UDP applications.

---

## 8.1 TCP Load Balancer Requirements

### Application Inventory

What TCP/UDP applications need load balancing?

Application	Protocol	Port(s)	Use Case
_____	[ ] TCP [ ] UDP	_____	[ ] Database [ ] Gaming [ ] Mail [ ] SSH [ ] Custom
_____	[ ] TCP [ ] UDP	_____	[ ] Database [ ] Gaming [ ] Mail [ ] SSH [ ] Custom
_____	[ ] TCP [ ] UDP	_____	[ ] Database [ ] Gaming [ ] Mail [ ] SSH [ ] Custom
_____	[ ] TCP [ ] UDP	_____	[ ] Database [ ] Gaming [ ] Mail [ ] SSH [ ] Custom

### Port Configuration

- Single port per load balancer
  - Multiple specific ports: \_\_\_\_\_
  - Port range: \_ to \_\_\_\_\_
-

## 8.2 Traffic Volume

### Connection Metrics

Metric	Average	Peak
Connections per second	_____	_____
Concurrent connections	_____	_____
Bandwidth (Mbps)	_____	_____
Average connection duration	_____ seconds	_____

### Connection Patterns

What are your connection patterns?

- Short-lived connections (request/response)
  - Long-lived connections (persistent)
  - Fixed
- 

## 8.3 Origin Configuration

### Origin Servers

Application	Origin Type	Count	Ports
_____	[ ] IP [ ] FQDN	_____	_____
_____	[ ] IP [ ] FQDN	_____	_____
_____	[ ] IP [ ] FQDN	_____	_____

## Origin Connectivity

How will F5 XC reach TCP origins?

- Public Internet
  - Customer Edge site
  - Cloud Site (AWS/Azure/GCP)
  - Private connectivity
- 

## 8.4 Load Balancing Configuration

### Load Balancing Algorithm

- Round Robin
- Least Connections
- Source IP Hash (session persistence)
- Random

### Health Checks

Health check configuration:

Parameter	Value
Health check type	<input type="checkbox"/> TCP Connect <input type="checkbox"/> Custom
Check interval	_____ seconds
Healthy threshold	_____ checks
Unhealthy threshold	_____ checks
Timeout	_____ seconds

### Session Persistence

- Yes - Source IP based
- No - Connections can go to any origin

## 8.5 TLS Configuration

### TLS Requirements

- TLS Termination** - F5 terminates TLS
- TLS Pass-Through** - Pass encrypted traffic to origin
- No TLS** - Unencrypted TCP

### Certificate Configuration

If TLS termination:

Parameter	Value
Certificate source	[ ] Automatic [ ] Custom
Minimum TLS version	[ ] TLS 1.2 [ ] TLS 1.3
mTLS required	[ ] Yes [ ] No

## 8.6 Timeouts and Limits

### Connection Timeouts

Parameter	Value
Connection timeout	_____ seconds
Idle timeout	_____ seconds

### Connection Limits

Parameter	Value
Max connections per client IP	_____
Max total connections	_____

## 8.7 Use Case Specific

### Database Load Balancing

If load balancing databases:

Parameter	Value
Database type	[ ] MySQL [ ] PostgreSQL [ ] MongoDB [ ] Redis [ ] Other: __
Read/Write splitting needed	[ ] Yes [ ] No
Connection pooling	[ ] Yes [ ] No

### Gaming/Real-Time

If gaming or real-time applications:

Parameter	Value
UDP support needed	[ ] Yes [ ] No
Latency sensitivity	[ ] Critical [ ] Important [ ] Normal
Geographic proximity required	[ ] Yes [ ] No

## 8.8 Summary: TCP Load Balancer Requirements

Requirement	Value
Number of TCP Load Balancers	__
Protocols	[ ] TCP [ ] UDP [ ] Both
Port(s)	__
Peak Connections per Second	__
TLS Required	[ ] Yes [ ] No
Session Persistence	[ ] Yes [ ] No

**Additional notes:**

-----  
-----

# 9. DNS Services Sizing

F5 Distributed Cloud DNS provides geo-distributed DNS services with global server load balancing (GSLB), automatic failover, health checking, and DDoS protection.

## 9.1 DNS Requirements Assessment

- Yes - Primary DNS hosting
- Yes - Secondary DNS (backup)
- Yes - DNS Load Balancing (GSLB) only

## Current DNS Provider

Who is your current DNS provider?

Current Provider	Keep or Migrate
_____	[ ] Migrate to F5 [ ] Keep as primary [ ] Keep as secondary

## 9.2 DNS Zone Configuration

### Zone Count

How many DNS zones do you need?

Zone Type	Count
Primary zones	_____
Secondary zones	_____
<b>Total zones</b>	_____

#### Base Package

Standard includes 250 primary or secondary zones.

## Zone Details

List your primary domains/zones:

Domain	Zone Type	Records (est.)	Query Volume
_____	[ ] Primary [ ] Secondary	_____	_____ qps
_____	[ ] Primary [ ] Secondary	_____	_____ qps
_____	[ ] Primary [ ] Secondary	_____	_____ qps
_____	[ ] Primary [ ] Secondary	_____	_____ qps
_____	[ ] Primary [ ] Secondary	_____	_____ qps

## Record Types

What DNS record types do you use?

- A (IPv4 address)
- AAAA (IPv6 address)
- CNAME (Canonical name)
- MX (Mail exchange)
- TXT (Text records)
- SRV (Service records)
- NS (Nameserver)
- AAA (Certificate Authority Authorization)
- PTR (Reverse DNS)
- Other: \_\_\_\_\_

Total estimated DNS records: \_\_\_\_\_

## 9.3 DNS Load Balancing (GSLB)

- Yes - Distribute traffic across multiple locations
- No - Basic DNS hosting only

### Base Package

Standard includes 50 DNS load balancer records and 200 health checks.

## Load Balancing Use Cases

What DNS load balancing capabilities do you need?

- Geographic proximity** - Route users to nearest data center
- Active/Standby failover** - Automatic failover to backup site
- Weighted distribution** - Distribute traffic by percentage
- Performance-based** - Route based on health/latency
- Disaster recovery** - Manual failover capability

## DNS Load Balancer Records

How many DNS load balancer records do you need?

Record/Domain	Type	Locations
_____	[ ] Geo [ ] Failover [ ] Weighted	_____
_____	[ ] Geo [ ] Failover [ ] Weighted	_____
_____	[ ] Geo [ ] Failover [ ] Weighted	_____
_____	[ ] Geo [ ] Failover [ ] Weighted	_____

Total DNS LB records needed: \_\_\_\_\_

## 9.4 Health Checking

### Health Check Requirements

- Yes
- No

Health check details:

Target	Check Type	Interval
_____	[ ] HTTP [ ] HTTPS [ ] TCP [ ] ICMP	_____ sec
_____	[ ] HTTP [ ] HTTPS [ ] TCP [ ] ICMP	_____ sec
_____	[ ] HTTP [ ] HTTPS [ ] TCP [ ] ICMP	_____ sec
_____	[ ] HTTP [ ] HTTPS [ ] TCP [ ] ICMP	_____ sec

Total health checks needed: \_\_\_\_\_

## Failover Configuration

Parameter	Value
Health check interval	_____ seconds
Failure threshold	_____ consecutive failures
Recovery threshold	_____ consecutive successes
TTL during failover	_____ seconds

## 9.5 DNS Security

### DNSSEC

Yes - Sign DNS responses cryptographically

No

#### DNSSEC

DNSSEC provides authentication of DNS responses, preventing DNS spoofing and

cache poisoning attacks.

## DNS DDoS Protection

- Yes - Standard DNS DDoS protection (included)
- Yes - Advanced DNS DDoS protection
- No

Have you experienced DNS attacks?

- Yes - DNS floods
- Yes - DNS amplification
- Yes - NXDOMAIN attacks
- No

## Access Control

- SIG authentication for zone transfers
- IP-based access restrictions
- Rate limiting per client

## 9.6 Zone Management

### Zone Transfer

- F5 as primary, transfer to secondary
- External primary, F5 as secondary
- No

External DNS servers for zone transfer:

Server	IP Address	Direction
_____	_____	[ ] To F5 [ ] From F5
_____	_____	[ ] To F5 [ ] From F5

## Zone Import

Do you have existing zone files to import?

- Yes - Standard zone file format
- Yes - BIND format
- No - Creating zones from scratch

Number of zone files to import: \_\_\_\_\_

## DNS Management Integration

How will DNS be managed?

- GUI XC Console (UI)
  - Terraform / Infrastructure as Code
  - API integration
  - CI/CD pipeline
- 

## 9.7 Query Volume

### DNS Query Metrics

Metric	Value
Average queries per second	_____
Peak queries per second	_____
Daily query volume	_____
Monthly query volume	_____

## Query Sources

Where do DNS queries originate?

Region	Percentage
North America	_____ %
Europe	_____ %
Asia-Pacific	_____ %
South America	_____ %
Other	_____ %

## 9.8 Advanced Features

### Split-Horizon DNS

- Yes - Different responses for internal vs external
- No

### Dynamic DNS

- Yes - Programmatic record updates
- No

### GeoDNS Customization

- Yes - By country
- Yes - By region/continent
- Yes - By ASN (ISP)
- Yes - By client subnet
- No - Standard geo-proximity

## 9.9 Domain Delegation

### Domain Registrar

Will you delegate domains to F5 nameservers?

Yes - Update NS records at registrar

No - Using F5 as secondary only

Current registrar: \_\_\_\_\_

### Nameserver Configuration

Nameserver preference:

F5 provided nameservers

Custom/vanity nameservers: \_\_\_\_\_

## 9.10 Summary: DNS Requirements

Requirement	Value
Total DNS Zones	_____
Primary Zones	_____
Secondary Zones	_____
DNS LB Records	_____
Health Checks	_____
Estimated QPS	_____
DNSSEC Required	[ ] Yes [ ] No
Tier Required	[ ] Standard [ ] Advanced

Domains to migrate:

1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_

Additional notes:

-----  
-----

# 10. Multi-Cloud Networking Sizing

---

F5 Distributed Cloud Network Connect provides secure, encrypted connectivity between public clouds, on-premises data centers, and edge sites with centralized management and observability.

---

## 10.1 Multi-Cloud Networking Requirements

- Yes - Connect multiple cloud environments
- Yes - Connect cloud to on-premises
- Yes - Connect distributed edge sites

### Current Multi-Cloud Challenges

---

What networking challenges are you experiencing?

- Complex cloud-specific networking configurations
  - Inconsistent security policies across clouds
  - Limited visibility across environments
  - High latency between sites
  - Difficult troubleshooting
  - Manual configuration overhead
  - Other: \_\_\_\_\_
-

## 10.2 Site Inventory

### Cloud Environments

What cloud environments need connectivity?

Cloud Provider	Regions	VPCs/VNets	Workloads
AWS	_____	_____	_____
Azure	_____	_____	_____
Google Cloud	_____	_____	_____
Other: _____	_____	_____	_____

### On-Premises Data Centers

Data Center Location	Network Connectivity	Workloads
_____	[ ] Internet [ ] MPLS [ ] Direct Connect	_____
_____	[ ] Internet [ ] MPLS [ ] Direct Connect	_____
_____	[ ] Internet [ ] MPLS [ ] Direct Connect	_____

### Edge/Branch Sites

Site Type	Count	Connectivity
Branch offices	_____	[ ] Internet [ ] MPLS
Retail locations	_____	[ ] Internet [ ] MPLS
Manufacturing sites	_____	[ ] Internet [ ] MPLS
Remote workers	_____	[ ] Internet [ ] VPN
Other: _____	_____	_____

Total sites to connect: \_\_\_\_\_

## 10.3 Connectivity Requirements

### Site-to-Site Connectivity

What site-to-site connectivity patterns do you need?

- Full Mesh** - Every site connects to every other site
- Hub and Spoke** - Sites connect through central hubs
- Partial Mesh** - Specific site-to-site connections

Diagram your connectivity requirements:

[Draw or describe your target topology]

---



---



---

### Traffic Patterns

What traffic flows between sites?

Source	Destination	Traffic Type	Bandwidth
_____	_____	_____	_____ Mbps
_____	_____	_____	_____ Mbps
_____	_____	_____	_____ Mbps
_____	_____	_____	_____ Mbps

### Bandwidth Requirements

Metric	Value
Total inter-site bandwidth	_____ Mbps
Peak inter-site bandwidth	_____ Mbps
Average latency requirement	< _____ ms

## 10.4 Customer Edge Deployment

### CE Site Deployment

Where will F5 Customer Edge (CE) nodes be deployed?

Site	Deployment Type	Node Count	Size
_____	[ ] Physical [ ] VM [ ] Cloud	_____	[ ] Small [ ] Medium [ ] Large
_____	[ ] Physical [ ] VM [ ] Cloud	_____	[ ] Small [ ] Medium [ ] Large
_____	[ ] Physical [ ] VM [ ] Cloud	_____	[ ] Small [ ] Medium [ ] Large
_____	[ ] Physical [ ] VM [ ] Cloud	_____	[ ] Small [ ] Medium [ ] Large

#### CE Node Sizes

- **Small:** 8 vCPU, 32GB RAM, 80GB disk
- **Medium:** 8 vCPU, 32GB RAM, 100GB disk (App Stack)
- **Large:** 16 vCPU, 64GB RAM, 100GB disk

### High Availability

CE high availability requirements:

- **Single node** - Development/non-critical
- **2-node cluster** - Production HA (recommended)

# 10.5 Network Configuration

## IP Addressing

Provide subnet information for connected networks:

Site	Inside Subnet (CIDR)	Outside Subnet (CIDR)	Gateway
---	---/---	---/---	---
---	---/---	---/---	---
---	---/---	---/---	---

## Routing Requirements

What routing is required?

- Static routing** - Manually configured routes
- GP** - Dynamic routing with BGP
- SPF** - Dynamic routing with OSPF (via BGP redistribution)

BGP requirements (if applicable):

Parameter	Value
Local ASN	---
Peer ASN(s)	---
Advertised prefixes	---

## NAT Requirements

What NAT is required?

- NAT** - Source NAT for outbound traffic
- No NAT** - Direct routing between sites

# 10.6 Security Features

## Network Firewall

Yes - L3/L4 firewall policies

No

Firewall requirements:

Source	Destination	Protocol	Port	Action
_____	_____	_____	_____	[ ] Allow [ ] Deny
_____	_____	_____	_____	[ ] Allow [ ] Deny
_____	_____	_____	_____	[ ] Allow [ ] Deny

Number of firewall rules: \_\_\_\_\_

## Micro-Segmentation

Yes - Segment traffic within sites

No

## Forward Proxy

Yes - HTTP/HTTPS inspection

Yes - URL filtering

No

## Service Insertion

Yes - F5 BIG-IP integration

Yes - Palo Alto Networks

Yes - Other: \_\_\_\_\_

No

# 10.7 Cloud Integration

## AWS Connectivity

If connecting AWS:

Parameter	Value
AWS regions	_____
VPCs to connect	_____
Transit Gateway integration	[ ] Yes [ ] No
Direct Connect	[ ] Yes [ ] No

## Azure Connectivity

If connecting Azure:

Parameter	Value
Azure regions	_____
VNets to connect	_____
Virtual WAN integration	[ ] Yes [ ] No
ExpressRoute	[ ] Yes [ ] No

## GCP Connectivity

If connecting Google Cloud:

Parameter	Value
GCP regions	_____
VPCs to connect	_____
Cloud Interconnect	[ ] Yes [ ] No

## 10.8 Observability

### Visibility Requirements

What network visibility do you need?

- Site-to-site tunnel status
- Latency monitoring
- Bandwidth utilization
- Flow logs / traffic analysis
- Security event logging

### Integration

Where should network telemetry be sent?

- NXC Console only
  - SIEM integration: \_\_\_\_\_
  - Network monitoring tool: \_\_\_\_\_
- 

## 10.9 Advanced Features (Advanced Tier)

### Advanced Network Connect Features

- Anomaly detection - ML-based traffic analysis
- Integrated WAF/DDoS/Bot - Security at network edge
- Advanced service chaining - Complex traffic flows

### Site Mesh Groups

- Full mesh - Direct connectivity between all sites
  - Hub-spoke mesh - Connectivity through hub sites
  - No site mesh required
-

## 10.10 Summary: Multi-Cloud Networking Requirements

Requirement	Value
Total Sites to Connect	_____
Cloud Environments	_____
On-Premises Data Centers	_____
Edge/Branch Sites	_____
Total Inter-Site Bandwidth	_____ Mbps
CE Nodes Required	_____
Network Firewall Rules	_____
Tier Required	[ ] Standard [ ] Advanced

Network topology diagram attached: [ ] Yes [ ] No

Additional notes:

---



---



---

# 11. App Connect Sizing

---

F5 Distributed Cloud App Connect provides service mesh capabilities with app-to-app connectivity, service discovery, and centralized orchestration across distributed environments.

---

## 11.1 App Connect Requirements

### Use Cases

What App Connect capabilities do you need?

- Service discovery** - Discover services across environments
  - Service mesh** - Secure service-to-service communication
  - App migration** - Migrate apps between environments
  - Kubernetes networking** - Connect K8s clusters
  - Legacy integration** - Connect legacy and modern apps
- 

## 11.2 Application Environment

### Application Architecture

What type of applications do you have?

- Monolithic applications
- Microservices
- Hybrid (monolith + microservices)
- Serverless / Functions
- Legacy applications

## Kubernetes Deployments

Do you have Kubernetes clusters?

Yes

No

If yes:

Cluster Name	Location	Distribution	Services
_____	_____	[ ] EKS [ ] AKS [ ] GKE [ ] OpenShift [ ] Other	_____
_____	_____	[ ] EKS [ ] AKS [ ] GKE [ ] OpenShift [ ] Other	_____
_____	_____	[ ] EKS [ ] AKS [ ] GKE [ ] OpenShift [ ] Other	_____

Total Kubernetes clusters: \_\_\_\_\_

## Service Inventory

How many services need connectivity?

Environment	Service Count
Production	_____
Staging	_____
Development	_____
<b>Total</b>	_____

## 11.3 Service Discovery

### Service Discovery Requirements

---

What service discovery mechanisms do you use?

- Kubernetes DNS
- Consul
- NS-based
- static configuration
- Other: \_\_\_\_\_

### Cross-Environment Discovery

---

Do services need to discover services in other environments?

- Yes - Cross-cluster Kubernetes
  - Yes - Kubernetes to VM-based
  - Yes - Cloud to on-premises
  - No - Single environment only
- 

## 11.4 Traffic Management

### Load Balancing

---

What load balancing is needed between services?

- Round robin
- Least connections
- Weighted distribution
- Geographic / Proximity-based

### Advanced Traffic Management

---

- A/B testing - Route percentage to different versions
- Canary deployments - Gradual rollout

- **Blue-green deployments** - Switch between versions
- **Leader-based routing** - Route based on headers
- **Fault injection** - Test resilience

## Traffic Patterns

Describe service-to-service traffic patterns:

Source Service	Destination Service	RPS	Latency Requirement
_____	_____	_____	< _____ ms
_____	_____	_____	< _____ ms
_____	_____	_____	< _____ ms

## 11.5 Security

### Service-to-Service Security

What security is required between services?

- **MTLS** - Mutual TLS authentication
- **Service policies** - Allow/deny between services
- **Encryption** - Encrypt all service traffic

## Policy Requirements

Source	Destination	Action	Notes
_____	_____	[ ] Allow [ ] Deny	_____
_____	_____	[ ] Allow [ ] Deny	_____
_____	_____	[ ] Allow [ ] Deny	_____

## Identity Integration

What identity systems need integration?

- Service accounts (Kubernetes)
  - Auth/OIDC
  - PIFFE/SPIRE
  - Custom certificates
  - None
- 

## 11.6 Observability

### Service Observability

What service observability do you need?

- Request tracing
- Service dependency mapping
- Traffic flow visualization
- Error rate monitoring
- Latency metrics

### Distributed Tracing

Do you use distributed tracing?

- Yes - Jaeger
  - Yes - Zipkin
  - Yes - Other: \_\_\_\_\_
  - No
-

## 11.7 Migration Use Cases

### Application Migration

Are you migrating applications?

- Yes - Cloud to cloud
- Yes - On-premises to cloud
- Yes - Monolith to microservices
- No

Migration details:

Application	From	To	Timeline
_____	_____	_____	_____
_____	_____	_____	_____

### Hybrid Operation

- Yes - Active/Active across locations
- Yes - Active/Standby failover
- No

## 11.8 Integration

### Existing Service Mesh

Do you have an existing service mesh?

- Yes - Istio
- Yes - Linkerd
- Yes - Consul Connect
- Yes - Other: \_\_\_\_\_
- No

If yes, will you:

- Replace with F5 App Connect
- Integrate/coexist
- Migrate gradually

## F5 BIG-IP Integration

Do you have F5 BIG-IP to integrate?

- Yes - Discover BIG-IP services
  - Yes - Extend BIG-IP functionality
  - No
- 

## 11.9 Summary: App Connect Requirements

Requirement	Value
Total Services	_____
Kubernetes Clusters	_____
Cross-Environment Discovery	[ ] Yes [ ] No
mTLS Required	[ ] Yes [ ] No
Advanced Traffic Management	[ ] Yes [ ] No
Service Migration	[ ] Yes [ ] No
Tier Required	[ ] Standard [ ] Advanced

Service mesh diagram attached: [ ] Yes [ ] No

Additional notes:

---



---

# 12. CDN Sizing

---

F5 Distributed Cloud CDN provides global content delivery with intelligent caching, reducing latency and bandwidth costs while integrating with F5's security services.

---

## 12.1 CDN Requirements

### CDN Goals

What are your primary CDN goals?

- Improve user experience / reduce latency
  - Reduce origin server load
  - Reduce bandwidth/egress costs
  - Global content distribution
  - DoS protection at the edge
  - Other: \_\_\_\_\_
-

## 12.2 Content Profile

### Content Types

What content will be cached?

Content Type	Percentage	Cache TTL
Static images (jpg, png, gif, svg)	____%	____ hours
JavaScript / CSS	____%	____ hours
Video / Media files	____%	____ hours
HTML pages	____%	____ hours
API responses	____%	____ seconds
Documents (PDF, etc.)	____%	____ hours
Other: _____	____%	____

### Content Size

Metric	Value
Total unique content size	____ GB/TB
Average object size	____ KB
Largest object size	____ MB
Total number of unique objects	____

### Content Origin

Where is your origin content hosted?

Origin Location	Provider	Percentage
_____	[ ] AWS [ ] Azure [ ] GCP [ ] On-Prem [ ] Other	____%
_____	[ ] AWS [ ] Azure [ ] GCP [ ] On-Prem [ ] Other	____%

## 12.3 Traffic Volume

### Request Metrics

Metric	Average	Peak
Requests per second	_____	_____
Requests per month	_____	_____
Bandwidth (Gbps)	_____	_____

### Regional Distribution

Where are your users located?

Region	Traffic Percentage
North America	_____ %
Europe	_____ %
Asia-Pacific	_____ %
South America	_____ %
Other	_____ %

#### Regional Pricing

CDN data transfer and request pricing varies by region.

## 12.4 Caching Configuration

### Cache Policy

How should content be cached?

- Follow origin headers** - Respect Cache-Control headers
- Override with custom TTL** - Set custom cache times
- Query string handling:** [ ] Include [ ] Ignore [ ] Selective

### Cache Key Configuration

What should be included in cache keys?

- URL path
- Query string parameters
- Specific headers: \_\_\_\_\_
- Cookies: \_\_\_\_\_

### Cache Purge Requirements

How will you purge cached content?

- Manual purge via console
- API-based purge
- Tag-based purge
- Path-based purge
- Full cache purge

Estimated purge frequency: \_\_\_\_\_ per day/week

## 12.5 Security Integration

### CDN with Security

- WAF at the edge

- ⚡ot defense at the edge
- ⚡DoS protection
- ⚡ate limiting
- ⚡eographic restrictions

## TLS Configuration

Parameter	Value
TLS termination at edge	[ ] Yes [ ] No
Minimum TLS version	[ ] TLS 1.2 [ ] TLS 1.3
Custom certificates	[ ] Yes [ ] No
HTTP to HTTPS redirect	[ ] Yes [ ] No

## 12.6 Advanced Features

### Dynamic Content Optimization

- mage optimization / WebP conversion
- linification (JS/CSS/HTML)
- mpression (Gzip/Brotli)
- TTP/2 / HTTP/3 support

### Custom Rules

URL Pattern	Cache Behavior	TTL
/api/*	[ ] Cache [ ] Bypass	—
/static/*	[ ] Cache [ ] Bypass	—
*.css	[ ] Cache [ ] Bypass	—
—	[ ] Cache [ ] Bypass	—

## 12.7 Performance Metrics

### Expected Cache Performance

Metric	Target
Target cache hit ratio	> ____ %
Target TTFB from edge	< ____ ms
Acceptable origin load reduction	____ %

### Monitoring Requirements

What CDN metrics do you need?

- Cache hit/miss ratios
- Bandwidth by region
- Request counts
- Error rates
- Origin response times
- Popular content reports

## 12.8 Summary: CDN Requirements

Requirement	Value
Domains to CDN	____
Monthly Requests	____
Monthly Data Transfer	____ GB
Primary Regions	____
Security Integration	[ ] Yes [ ] No
Custom Cache Rules	[ ] Yes [ ] No

**Additional notes:**

-----  
-----

# 13. Edge Compute Sizing

---

F5 Distributed Cloud provides edge compute capabilities through Customer Edge sites and App Stack, enabling you to run application logic closer to users.

---

## 13.1 Edge Compute Requirements

### Edge Compute Use Cases

What are your edge compute requirements?

- API processing** - Process API requests at the edge
  - Data transformation** - Transform data before reaching origin
  - Authentication** - Edge authentication/authorization
  - Content personalization** - Personalize content at the edge
  - IoT processing** - Process IoT data locally
  - Machine learning inference** - Run ML models at the edge
  - Real-time analytics** - Process analytics locally
  - Other: \_\_\_\_\_
- 

## 13.2 Workload Profile

### Workload Types

What types of workloads will run at the edge?

- Containers (Docker/Kubernetes)
- Virtual machines
- Serverless functions
- Custom applications

## Workload Details

Workload Name	Type	CPU	Memory	Storage
_____	[ ] Container [ ] VM	_____ cores	_____ GB	_____ GB
_____	[ ] Container [ ] VM	_____ cores	_____ GB	_____ GB
_____	[ ] Container [ ] VM	_____ cores	_____ GB	_____ GB

## Workload Scaling

How should workloads scale?

- Fixed size - Manual scaling
- Horizontal auto-scaling
- Vertical scaling

## 13.3 Edge Locations

### Edge Site Locations

Where do you need edge compute?

Location	Site Type	Workloads
_____	[ ] Data Center [ ] Branch [ ] Retail [ ] Other	_____
_____	[ ] Data Center [ ] Branch [ ] Retail [ ] Other	_____
_____	[ ] Data Center [ ] Branch [ ] Retail [ ] Other	_____

Total edge compute locations: \_\_\_\_\_

## Edge Infrastructure

What infrastructure is available at edge locations?

Location	Compute Available	Network	Power/Cooling
_____	[ ] Servers [ ] VMs [ ] None	_____ Mbps	[ ] Yes [ ] Limited
_____	[ ] Servers [ ] VMs [ ] None	_____ Mbps	[ ] Yes [ ] Limited

## 13.4 App Stack Requirements

### App Stack Deployment

Yes - Managed K8s at the edge

No - Using existing infrastructure

### Container Requirements

If using containers:

Parameter	Value
Total containers	_____
Container registry	[ ] Docker Hub [ ] Private [ ] AWS ECR [ ] Azure ACR [ ] GCR
Container sizes needed	[ ] Tiny [ ] Medium [ ] Large

#### Container Sizes

- **Tiny:** 0.25 vCPU, 0.5GB RAM
- **Medium:** 1 vCPU, 2GB RAM
- **Large:** 2 vCPU, 4GB RAM

## 13.5 Networking

### Edge Network Requirements

How do edge workloads need to communicate?

- With origin/cloud services
- With other edge sites
- With local devices (IoT, sensors)
- With external APIs

### Network Performance

Requirement	Value
Latency to local users	< ____ ms
Bandwidth to cloud	____ Mbps
Local network bandwidth	____ Mbps

## 13.6 Data Management

### Data at the Edge

What data will be processed at the edge?

- User data / PII
- IoT sensor data
- Transaction data
- Log data
- Media / video

## Data Residency

Are there data residency requirements?

Yes - Data must stay in specific regions

No

Regions with data residency requirements: \_\_\_\_\_

## Edge Storage

Yes - \_\_\_\_\_ GB per site

No - Stateless workloads only

## 13.7 Summary: Edge Compute Requirements

Requirement	Value
Edge Compute Locations	_____
Total Workloads	_____
App Stack (Managed K8s)	[ ] Yes [ ] No
Container Count	_____
Persistent Storage	[ ] Yes [ ] No

Primary edge compute use case:

-----

-----

# 14. Customer Edge Sites Sizing

---

Customer Edge (CE) sites are F5 software deployments in your environment that provide private connectivity, local security enforcement, and edge compute capabilities.

---

## 14.1 CE Site Requirements

### CE Use Cases

Why do you need Customer Edge sites?

- Private connectivity** - Access applications on private networks
  - Local security enforcement** - WAF/security at the edge
  - Multi-cloud networking** - Site-to-site connectivity
  - Edge compute** - Run workloads locally
  - Low latency** - Local processing requirements
  - Data residency** - Keep data local
  - Other: \_\_\_\_\_
- 

## 14.2 Site Inventory

### Site Locations

Where will CE sites be deployed?

Site Name	Location	Environment	Purpose
_____	_____	[ ] DC [ ] Branch [ ] Edge [ ] Cloud	_____
_____	_____	[ ] DC [ ] Branch [ ] Edge [ ] Cloud	_____
_____	_____	[ ] DC [ ] Branch [ ] Edge [ ] Cloud	_____
_____	_____	[ ] DC [ ] Branch [ ] Edge [ ] Cloud	_____
_____	_____	[ ] DC [ ] Branch [ ] Edge [ ] Cloud	_____

Total CE sites: \_\_\_\_\_

## Site Criticality

Site	Criticality	High Availability Required
_____	[ ] Critical [ ] High [ ] Medium [ ] Low	[ ] Yes (3-node) [ ] No (1-node)
_____	[ ] Critical [ ] High [ ] Medium [ ] Low	[ ] Yes (3-node) [ ] No (1-node)
_____	[ ] Critical [ ] High [ ] Medium [ ] Low	[ ] Yes (3-node) [ ] No (1-node)

## 14.3 Infrastructure Requirements

### Deployment Platform

How will CE sites be deployed?

Site	Platform	Hypervisor/OS
_____	[ ] VM [ ] Bare Metal [ ] Cloud VM	_____
_____	[ ] VM [ ] Bare Metal [ ] Cloud VM	_____
_____	[ ] VM [ ] Bare Metal [ ] Cloud VM	_____

### Node Sizing

What size CE nodes do you need?

## CE Node Size Reference

Size	vCPU	RAM	Disk	Use Case
<b>Standard</b>	8	32GB	80GB	Basic networking/security
<b>App Stack</b>	8	32GB	100GB	+ Container workloads
<b>Large</b>	16	64GB	100GB	High throughput/complex policies

Site	Size	Nodes	Total vCPU	Total RAM
_____	[ ] Standard [ ] App Stack [ ] Large	[ ] 1 [ ] 3	_____	_____ GB
_____	[ ] Standard [ ] App Stack [ ] Large	[ ] 1 [ ] 3	_____	_____ GB
_____	[ ] Standard [ ] App Stack [ ] Large	[ ] 1 [ ] 3	_____	_____ GB

## High Availability Configuration

For production sites, 3-node clusters are recommended:

Site	HA Mode	Nodes	Notes
_____	[ ] Single [ ] 3-node HA	_____	_____
_____	[ ] Single [ ] 3-node HA	_____	_____

## 14.4 Network Configuration

### Network Interfaces

How many network interfaces per CE node?

- Single interface (on-a-stick)** - Simplified deployment
- Dual interface** - Inside and outside networks
- Multiple interfaces** - Complex routing

### IP Addressing

Site	Interface	Subnet	Gateway	DHCP or Static
_____	Outside	_____/__	_____	[ ] DHCP [ ] Static
_____	Inside	_____/__	_____	[ ] DHCP [ ] Static
_____	Outside	_____/__	_____	[ ] DHCP [ ] Static
_____	Inside	_____/__	_____	[ ] DHCP [ ] Static

### DNS Configuration

Site	DNS Servers
_____	_____
_____	_____

### Internet Connectivity

How do CE sites connect to F5 Regional Edges?

Site	Internet Access	Proxy Required
_____	[ ] Direct [ ] NAT [ ] Proxy	[ ] Yes [ ] No
_____	[ ] Direct [ ] NAT [ ] Proxy	[ ] Yes [ ] No

## 14.5 Workload Configuration

### Services at CE Sites

What services will run at CE sites?

Site	Services
___	[ ] HTTP LB [ ] TCP LB [ ] WAF [ ] Network Firewall [ ] App Stack
___	[ ] HTTP LB [ ] TCP LB [ ] WAF [ ] Network Firewall [ ] App Stack
___	[ ] HTTP LB [ ] TCP LB [ ] WAF [ ] Network Firewall [ ] App Stack

### Origin Servers Behind CE

What applications/services are behind each CE?

Site	Applications	Servers/IPs
___	___	___ servers
___	___	___ servers
___	___	___ servers

### Traffic Volume Through CE

Site	Requests/sec	Bandwidth	Connections
___	___	___ Mbps	___
___	___	___ Mbps	___
___	___	___ Mbps	___

## 14.6 Security Configuration

### Network Firewall at CE

Yes - Ingress filtering

- Yes - Egress filtering
- Yes - East-West filtering
- No

Estimated firewall rules per site: \_\_\_\_\_

## Forward Proxy at CE

---

- Yes - For outbound internet access
- No

## Network Policies

---

What network policies are needed?

- Allow/deny lists
  - Geographic restrictions
  - Rate limiting
  - Custom L3/L4 rules
- 

## 14.7 Multi-Cloud Connectivity

### Site Mesh

---

Will CE sites participate in site mesh?

- Yes - Full mesh with other CEs
- Yes - Hub-spoke topology
- No

### Tunnel Configuration

---

Site	Connects To	Tunnel Type
_____	_____	[ ] IPsec [ ] SSL VPN
_____	_____	[ ] IPsec [ ] SSL VPN

---

## 14.8 App Stack (Optional)

### App Stack Required

Yes - Run container workloads

No - Networking/security only

If yes:

Site	Containers	Storage	Registry
___	___	___ GB	___
___	___	___ GB	___

## 14.9 Operational Requirements

### Management Access

How will CE sites be managed?

5 XC Console (required)

SH access for troubleshooting

Local console access

### Monitoring

What monitoring is required?

Infrastructure health (CPU/Memory/Disk)

Network metrics (throughput/latency)

Application metrics

Security events

## Maintenance Windows

Site	Maintenance Window	Change Control
_____	_____	[ ] Standard [ ] Expedited [ ] Emergency only
_____	_____	[ ] Standard [ ] Expedited [ ] Emergency only

## 14.10 Summary: Customer Edge Requirements

Requirement	Value
Total CE Sites	_____
HA Sites (3-node)	_____
Single Node Sites	_____
Total CE Nodes	_____
Total vCPU Required	_____
Total RAM Required	_____ GB
App Stack Sites	_____

Site deployment timeline:

Site	Target Deployment Date
_____	_____
_____	_____
_____	_____

Additional notes:

-----

-----

# 15. Cloud Sites Sizing

---

Cloud Sites are F5-managed deployments in public cloud providers (AWS, Azure, GCP) that provide cloud-native integration and connectivity.

---

## 15.1 Cloud Site Requirements

### Cloud Site Use Cases

Why do you need Cloud Sites?

- Cloud-native apps** - Protect cloud workloads
  - VPC/VNet connectivity** - Connect to private cloud networks
  - Multi-cloud networking** - Bridge multiple clouds
  - Cloud egress** - Secure internet access from cloud
  - Service mesh** - Connect cloud-based services
  - Other: \_\_\_\_\_
- 

## 15.2 Cloud Provider Inventory

### AWS Sites

Yes

No

If yes:

AWS Region	VPCs to Connect	Workloads	Node Size
_____	_____	_____	[ ] Standard [ ] Large
_____	_____	_____	[ ] Standard [ ] Large
_____	_____	_____	[ ] Standard [ ] Large

AWS integration requirements:

- AWS Transit Gateway integration
- AWS Direct Connect integration
- VPC peering
- PrivateLink endpoints

## Azure Sites

---

- Yes
- No

If yes:

Azure Region	VNets to Connect	Workloads	Node Size
---	---	---	[ ] Standard [ ] Large
---	---	---	[ ] Standard [ ] Large
---	---	---	[ ] Standard [ ] Large

Azure integration requirements:

- Azure Virtual WAN integration
- Azure ExpressRoute integration
- VNet peering
- Private Endpoint

## Google Cloud Sites

---

- Yes
- No

If yes:

GCP Region	VPCs to Connect	Workloads	Node Size
---	---	---	[ ] Standard [ ] Large
---	---	---	[ ] Standard [ ] Large
---	---	---	[ ] Standard [ ] Large

GCP integration requirements:

- Cloud Interconnect integration
  - Shared VPC support
  - Private Service Connect
- 

## 15.3 Cloud Network Configuration

### Deployment Mode

How should Cloud Sites be deployed?

- Ingress/Egress Gateway - Single interface, simplified
- Ingress Gateway - Internet-facing only
- Workload - Full routing capability

### IP Addressing

Cloud Site	Site Network CIDR	Inside Subnets	Outside Subnets
---	---/---	---	---
---	---/---	---	---
---	---/---	---	---

## VPC/VNet Connectivity

What cloud networks need connectivity?

Cloud Network	Cloud Provider	CIDR	Connect To
_____	[ ] AWS [ ] Azure [ ] GCP	____/____	_____
_____	[ ] AWS [ ] Azure [ ] GCP	____/____	_____
_____	[ ] AWS [ ] Azure [ ] GCP	____/____	_____

## 15.4 High Availability

### HA Configuration

What availability is required?

Cloud Site	HA Mode	Availability Zones
_____	[ ] Single AZ [ ] Multi-AZ	____ AZs
_____	[ ] Single AZ [ ] Multi-AZ	____ AZs
_____	[ ] Single AZ [ ] Multi-AZ	____ AZs

## Node Count

Cloud Site	Master Nodes	Worker Nodes (if App Stack)
_____	[ ] 1 [ ] 3	_____
_____	[ ] 1 [ ] 3	_____
_____	[ ] 1 [ ] 3	_____

## 15.5 Services at Cloud Sites

### Services Required

What services will run at Cloud Sites?

Cloud Site	Services
_____	[ ] HTTP LB [ ] TCP LB [ ] WAF [ ] Network Connect [ ] App Stack
_____	[ ] HTTP LB [ ] TCP LB [ ] WAF [ ] Network Connect [ ] App Stack
_____	[ ] HTTP LB [ ] TCP LB [ ] WAF [ ] Network Connect [ ] App Stack

### Traffic Volume

Cloud Site	Expected Throughput	Connections
_____	_____ Mbps	_____
_____	_____ Mbps	_____
_____	_____ Mbps	_____

## 15.6 Cloud Credentials

### Cloud Account Access

How will F5 XC access your cloud accounts?

Cloud Provider	Access Method	Account/Subscription ID
AWS	[ ] IAM Role [ ] Access Key	_____
Azure	[ ] Service Principal	_____
GCP	[ ] Service Account	_____

## Permissions Required

Have you reviewed F5 XC required cloud permissions?

- Yes - AWS IAM policy reviewed
  - Yes - Azure RBAC permissions reviewed
  - Yes - GCP IAM roles reviewed
  - To - Need to review
- 

## 15.7 Cost Optimization

### Instance Types

Preferred cloud instance types:

Cloud Provider	Instance Type	vCPU	Memory
AWS	[ ] t3.xlarge [ ] m5.xlarge [ ] m5.2xlarge [ ] Custom	____	____ GB
Azure	[ ] Standard_D4s_v4 [ ] Standard_D8s_v4 [ ] Custom	____	____ GB
GCP	[ ] n1-standard-4 [ ] n1-standard-8 [ ] Custom	____	____ GB

### Cost Considerations

- Use spot/preemptible instances where possible
  - Use reserved capacity for steady workloads
  - Optimize for specific regions with lower costs
-

## 15.8 Summary: Cloud Sites Requirements

Requirement	Value
AWS Cloud Sites	_____
Azure Cloud Sites	_____
GCP Cloud Sites	_____
Total Cloud Sites	_____
Multi-AZ Deployments	_____
App Stack Sites	_____

Cloud regions to deploy:

AWS: \_\_\_\_\_  
Azure: \_\_\_\_\_  
GCP: \_\_\_\_\_

Additional notes:

-----  
-----