SaaS Platform

Scoping and Requirements Guide

Robin Mordasiewicz

None

Table of Contents

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	___
Total Applications	___

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	
Total	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		
Azure		
Google Cloud		
On-Premises Data Center		
Other Cloud		

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

○ 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		
Per User		
Per API Endpoint		

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
- ○ Sumo 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	
Total API Endpoints	

API Details

For major API services, provide:

API NAME/ SERVICE	BASE PATH	PROTOCOL	AUTH METHOD	DOCUMENTATION
-		□ REST □ GraphQL □ gRPC	□ API Key □ OAuth □ JWT □ None	□ OpenAPI □ None
-		□ REST □ GraphQL □ gRPC	□ API Key □ OAuth □ JWT □ None	□ OpenAPI □ None
-		□ REST □ GraphQL □ gRPC	□ API Key □ OAuth □ JWT □ None	□ OpenAPI □ None
-		□ 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		
Total	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		□ second □ minute □ hour	□ Block □ Throttle
Per User/Token		□ second □ minute □ hour	□ Block □ Throttle
Per Endpoint		□ second □ minute □ hour	□ Block □ Throttle
Per IP Address		□ second □ minute □ hour	□ Block □ Throttle
Global (all traffic)		□ 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

⚠ **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	□	□
O ____	□	□

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%
- ✓ 10-25%
- ✓ 25-50%
- ✓ 50-75%
- ✓ 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.)
- ✓ CDN-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

⚠ 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

5.2 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?
		○ Yes ○ No
		○ Yes ○ No
		○ Yes ○ No
		○ Yes ○ No

Total number of prefixes: ___

5.3 Data Center Infrastructure

Data Centers

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

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

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

METRIC	VALUE
95th Percentile Inbound Bandwidth	s
Peak Inbound Bandwidth	s
Average Inbound Bandwidth	___ s

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	s
Number of ISP connections	
ISP providers	

5.5 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: □

5.6 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.

5.7 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
	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	s
Time to Mitigate	s
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 ○ No
Number of Prefixes	
Number of Data Centers	
Number of Edge Routers	
Clean Bandwidth (95th percentile)	
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	
Total third-party scripts	

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

> **ℹ 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?

- ○ GDPR
- ○ CCPA
- ○ 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
- ✓ F5 XC Console alerts
- ✓ Webhook integration
- ✓ SIEM 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?

○ **Block 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?

○ F5 XC proxy (automatic JavaScript injection)

○ Manual JavaScript tag insertion

○ BIG-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	
Total	

Virtual Host Details

For each application, provide virtual host information:

APPLICATION NAME	DOMAIN(S)	PORT(S)	PROTOCOL
			□ HTTP □ HTTPS □ Both
			□ HTTP □ HTTPS □ Both
			□ HTTP □ HTTPS □ Both
			□ HTTP □ HTTPS □ Both
			□ 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	
Check path (HTTP)	
Expected response code	-
Healthy threshold	
Unhealthy threshold	___

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
- ○ **Mixed** - 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	s
Idle timeout	s
Maximum request body size	___

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

- ☐ IP 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?

- ☐ F5 XC 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)
- ○ Mixed

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	□ TCP Connect □ Custom
Check interval	
Healthy threshold	
Unhealthy threshold	
Timeout	

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	s
Idle timeout	___ s

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	_
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	
Total zones	

> **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		
	□ Primary □ Secondary		
	□ Primary □ Secondary		
	□ Primary □ Secondary		
___	□ Primary □ Secondary	___	___

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)
- ○ CAA (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	
_	□ HTTP □ HTTPS □ TCP □ ICMP	
_	□ HTTP □ HTTPS □ TCP □ ICMP	
___	□ HTTP □ HTTPS □ TCP □ ICMP	___

Total health checks needed: ___

Failover Configuration

PARAMETER	VALUE
Health check interval	
Failure threshold	
Recovery threshold	s
TTL during failover	___

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

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

9.6 Zone Management

Zone Transfer

- ○ Yes - F5 as primary, transfer to secondary
- ○ Yes - 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?

- ☑ F5 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:

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			
(___	___	___	___

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

Bandwidth Requirements

METRIC	VALUE
Total inter-site bandwidth	
Peak inter-site bandwidth	
Average latency requirement	

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
- ✓ **3-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
- ✓ **BGP** - Dynamic routing with BGP
- ✓ **OSPF** - 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?

- ✓ **SNAT** - 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?

- ✓ F5 XC 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	
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	
Total	

11.3 Service Discovery

Service Discovery Requirements

What service discovery mechanisms do you use?

✓ Kubernetes DNS

✓ Consul

✓ DNS-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
- ✓ **Header-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

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)
- ☐ OAuth/OIDC
- ☐ SPIFFE/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
- ✓ DDoS 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)		
JavaScript / CSS		
Video / Media files		
HTML pages		
API responses		s
Documents (PDF, etc.)		
Other: ___	___	___

Content Size

METRIC	VALUE
Total unique content size	
Average object size	
Largest object size	
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?

- ✓ **Honor 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: ☐ eek

12.5 Security Integration

CDN with Security

- ✓ WAF at the edge
- ✓ Bot defense at the edge
- ✓ DDoS protection
- ✓ Rate limiting
- ✓ Geographic 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

- ✓ Image optimization / WebP conversion
- ✓ Minification (JS/CSS/HTML)
- ✓ Compression (Gzip/Brotli)
- ✓ HTTP/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	s
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	
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			
	□ Container □ VM			
	□ Container □ VM			

Workload Scaling

How should workloads scale?

- ✓ixed size - Manual scaling
- ✓lorizontal auto-scaling
- ✓ertical 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		□ Yes □ Limited
	□ Servers □ VMs □ None		□ 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	□
Bandwidth to cloud	□ s
Local network bandwidth	□ ___ ps

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
Standard	8	32GB	80GB	Basic networking/security
App Stack	8	32GB	100GB	+ Container workloads
Large	16	64GB	100GB	High throughput/complex policies

SITE	SIZE	NODES	TOTAL VCPU	TOTAL RAM
	○ Standard ○ App Stack ○ Large	○ 1 ○ 3		
	○ Standard ○ App Stack ○ Large	○ 1 ○ 3		
	○ Standard ○ App Stack ○ Large	○ 1 ○ 3		

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

Traffic Volume Through CE

SITE	REQUESTS/SEC	BANDWIDTH	CONNECTIONS

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

14.9 Operational Requirements

Management Access

How will CE sites be managed?

- ☐ F5 XC Console (required)
- ☐ SSH 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	
	□ Single AZ □ Multi-AZ	
	□ Single AZ □ Multi-AZ	

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

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
- ○ No - 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		
Azure	□ Standard_D4s_v4 □ Standard_D8s_v4 □ Custom		
GCP	□ n1-standard-4 □ n1-standard-8 □ Custom		

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:

```
___
```