F5 U.S. FEDERAL LIST OF CAPABILITIES

F5 SOLUTIONS DEPLOYMENTS

- All 15 executive departments of the U.S. cabinet
- 48 of the Fortune 50 companies
- 8 of the top 10 U.S. securities companies

At F5, our mission is rooted in the fact that businesses depend on apps. F5 solutions give you the ability to deploy compliant, secure, automated, and scalable applications in a federal setting, across both cloud and on-premises environments.

APPLICATION SECURITY

Layer 7 application protection
Advanced web application firewall
OWASP Top 10 protection
AI / ML (behavioral) for increased security and improved user experience
Bot/Automation protection
Post-authentication automation protection (after CAC malware)
Fraud protection
Leaked credential protection
MiTB protection
Available in cloud, on-prem, hardware/software
Available as a managed service or SaaS offering
WAF can help meet the DMZ STIG
Security scanner integration (Nessus, WhiteHat Sentinel, Qualys)

ZERO TRUST

F5 can be a PEP (policy enforcement point) and a PDP (policy decision point)
VPN-less secure access
Identity Aware Proxy—using per-request policies
Step-up authentication
Third-party telemetry integration
Trust scoring algorithm

F5 HAS PARTNERSHIPS WITH ALL MAJOR FEDERAL GOVERNMENT SYSTEM INTEGRATORS.

ACCESS MANAGEMENT

CAC authentication
Authentication bridging (legacy to modern)
Multi-factor authentication integration (Duo, RSA, Okta, Azure)
Use BIG-IP as a SP or IdP for SAML
Invisible MFA
VPN and per-app VPN
Integration with MDM like Intune and MobileIron
Remote access (RDP gateway)
Per-session and per-request access policies
Attribute-based authentication
Directory integration – Active Directory, LDAP
SSO (single sign-on)—SAML, Kerberos, NTLM, etc.
Client-side endpoint checks
VDI Support—authentication and reduction in infrastructure (PCoIP, VMware, Citrix)
Privileged User Access—ephemeral passwords for PKI
Webtop portal—VPN-less secure application portal for users
Modern authentication—SAML, JWT, OIDC

DNS

DNSSEC
Complete DNSSEC signing
Centralized DNSSEC key management
ICSA Labs certified as a firewall
DNS attack protection
Hardened F5 DNS code base (not BIND protocol)
Can be deployed in the DMZ
IP Anycast
Global server load balancing
Automated DNS failover
Location-based routing
Intelligent load balancing
Persistence
Topology mapping for improved user experience
Infrastructure monitoring
Caching, resolving
Available in cloud, VE, hardware
Protect existing DNS infrastructure with DNS Express
Programmatic functionality with iRules

AUTOMATION

- AS3 Declarative Interface
- iControl Rest
- Ansible
- Terraform
- Cloud Templates

CLOUD

- AWS GovCloud
- Azure Government
- Google Cloud for Government

CONTRACTING VEHICLES

- GSA Schedule #: GS
- 35F 0119Y

NETWORKING

ICSA-certified network firewall—Advanced Firewall Manager

Assured resilient communication

Multi-tenant support

On-board HSM and support for third-party external HSM

Full proxy—forward & reverse

IPv6 and IP Anycast

HTTP/2 and TLS 1.3 support

SFlow, SNMP, Syslog support

Protocol transformation (i.e., HTTP/2 to HTTP 1.1)

IP intelligence

IDS / IPS

IPSEC

SSL offloading

Application acceleration—compression, caching, WAN/LAN optimization

Advanced routing support: BGP, OSPF, IS-IS

Fully extensible via iRulesLX using node.js libraries

Intelligent server load balancing

Ability to scale for 100K(s)+ users across 100s of sites

Traffic shaping

All capabilities available in both hardware & software platforms

Templates for common deployments like SharePoint and Exchange

Automation and orchestration with well-known configuration management tools like Ansible and with F5's own automation toolchain, AS3 and DO

IoT MQTT protection, API security & gateway, and proxy

5G

CLOUD

F5 satisfies the SCCA (Secure Cloud Computing Architecture)

Multi-cloud availability

AWS, Azure, GCP deployment templates

Proven production deployments

IaC and configuration management integration (Terraform, Ansible)

SECURITY

- Application Security OWASP
- Top 10 App Transport Security
- SSL/TLSSSL/TLS Visibility

DEVOPS & DEVSECOPS

Open Source (NGINX)—lightweight web server, load balancer

Centralized management platform

Web Application Firewall with bot and threat campaign protection

Lightweight service mesh

API security & management

Kubernetes ingress controllers

Service mesh complex Istio K8s deployments

Programmability/DevOps focused API first

Automation tool chain

Integration with many A/O tools (Ansible, Terraform)

Traditional F5 hardware and VE capable of integrating with the ecosystem of automation, orchestration tools

IoT MQTT protection, API security & gateway, and proxy

SSL BREAK & INSPECT / VISIBILITY

SSL visibility or break and inspect

URL filtering

Industry-leading cryptographic hardware performance

Single decryption and re-encryption point

Dynamic service chaining

Contextual based routing—bypass decryption for sensitive traffic flows

Granular control—rewrite headers, port translation, ciphers, and protocol translation

Multiple topologies supported—inline layer 3, inline layer 2, explicit and transparent forward proxy

Support for all inspection devices—inline layer 2/3, ICAP services, receive-only (TAP)

Extensive Logging Integration—ArcSight, Splunk, and others

Easily scale out security devices in the inspection zone

No single point of failure as the service chains are dynamic and not traditional daisy chained

Intuitive GUI that simplifies a traditionally complex deployment

Secure Web Gateway

"F5 SOLUTIONS ENABLED US TO DELIVER HIGHER LEVELS OF APPLICATION AVAILABILITY AND PERFORMANCE IN A STANDARD MANNER—WITHOUT EXTENSIVE CUSTOM ENGINEERING FOR EACH PARTICULAR APPLICATION."
IT Architect, large enterprise aerospace & defense company

F5 AS A SERVICE

Behavioral application protection

Managed WAF, DDoS and AI/ML protection—24x7 SOC

Next-gen bot protection

Large-scale volumetric DDoS attack protection

Global server load balancing

Advanced fraud and automation protection

Application monitoring (Beacon)

CENTRALIZED MANAGEMENT

A centralized management platform for BIG-IP

Manage over 1,000 BIG-IP's from a single cluster

Manage licenses for over 5,000 devices

Logging, dashboards, auditing

Automate backups

Automate upgrades

Granular RBAC access controls

Automation with F5's automation tool chain

Key management and integration with Venafi and Let's Encrypt

Security management to include WAF policies, Access policies, firewall and SSL orchestration

CERTIFICATIONS

Common Criteria certification

CSfC (Commercial Solutions for Classified) traffic filtering firewall

DoDIN APL

FedRamp in process

FIPS 140-2 level 1, 2 & 3

ICSA certifications

IPv6

JITC (Joint Interoperability Test Command) PKE (Public Key Enabled)

NIST 800-53

TIC 3.0

UC-APL

USGv6

RESOURCES

- F5 U.S. Federal Solutions
- F5 Labs
- DevCentral
- F5 Certifications