FORTINET

FortiADC

Feature Guide

Overview

FortiADC is an advanced Application Delivery Controller (ADC) that provides a comprehensive set of capabilities across application delivery, security, access, and system operations. By combining load balancing, traffic optimization, and integrated security features, FortiADC helps organizations deliver reliable and secure application experiences.

This guide will introduce FortiADC features from the following aspects:

- Application Availability – Health Check, SSL Offloading, Content Routing, Scripting, Global Sever Load Balancing (GSLB), DNS Service and Security, Compression, Caching, Page Speed Optimization.
- Application Security – WAF, DoS Protection, Antivirus (AV), Intrusion Prevention System (IPS), Geo IP Protection, IP Reputation.
- Agentless Application Gateway (AAG)
- System and Operations – VDOMs and ADOMs, FortiAI Assistant, Automation Stitches, FortiView

Application Availability

Application Load Balancing

- L7 HTTP & HTTPS LB
- Advanced Health Check
- SSL Offloading and Inspection

Scripting & Automation

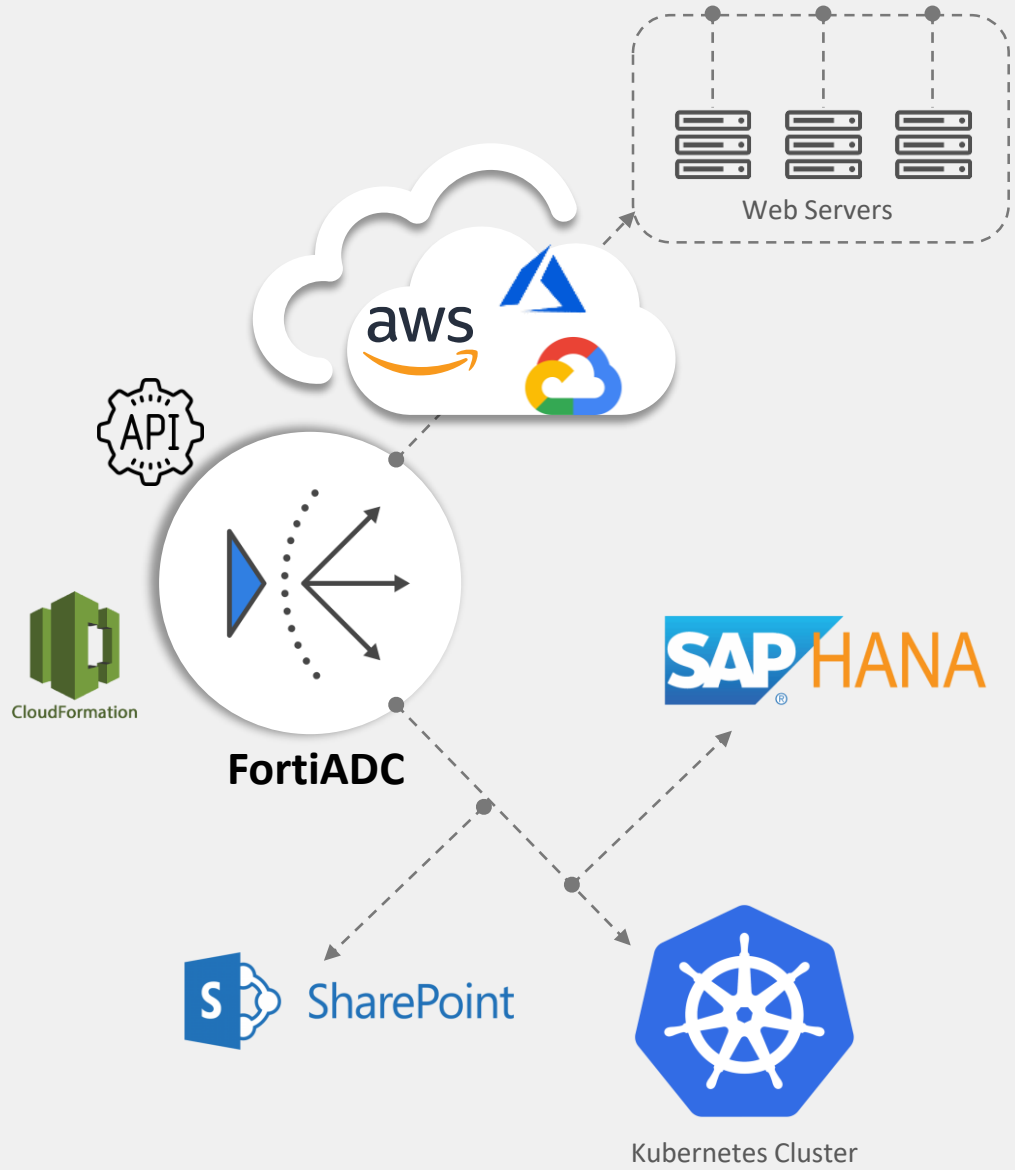
- Support any customer requirements
- React to real-time events via Automation

Global LB

- Ensuring Business Continuity
- Support traffic rerouting based on health checks, Geolocation, and application RTT

Optimization

- Improve User Quality of Experience
- Provide website performance enhancement tools



Back to Overview

Application Security

Web Application and API Protection

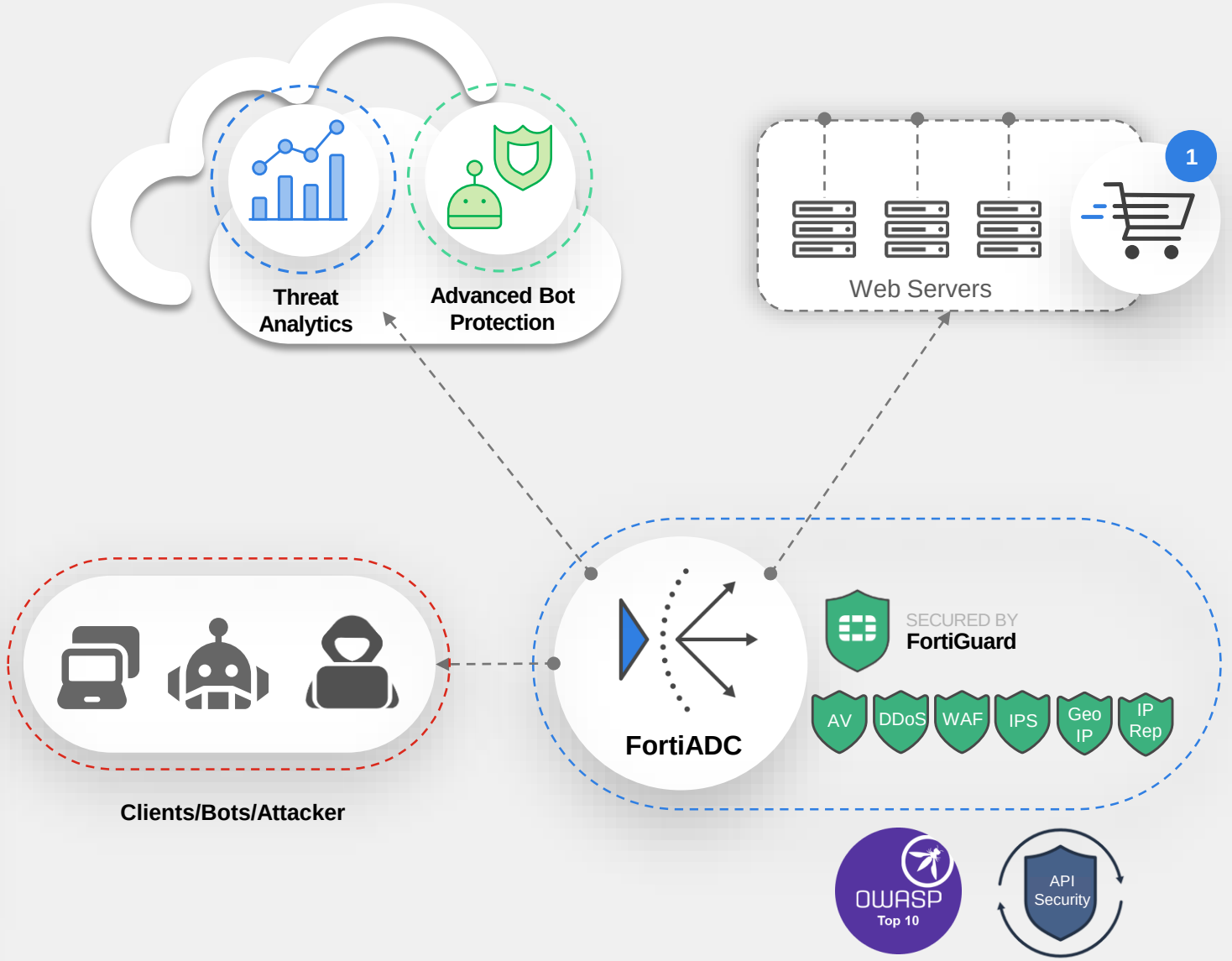
- Protects against common web threats, including SQL injection, XSS, and other OWASP Top 10 risks
- Adaptive traffic learning for continuous threat detection and response
- Monitors and controls API traffic to prevent data breaches and unauthorized access

Bot Protection

- ML-driven, biometric, and behavior-based detection of malicious bots to protect online services and free up network resources

Threat Analytics

- Reduces alert fatigue by speeding up incident investigation and provides SOC analysts with insights to prioritize mitigations and workload



Back to Overview

Application Access

Agentless Application Gateway

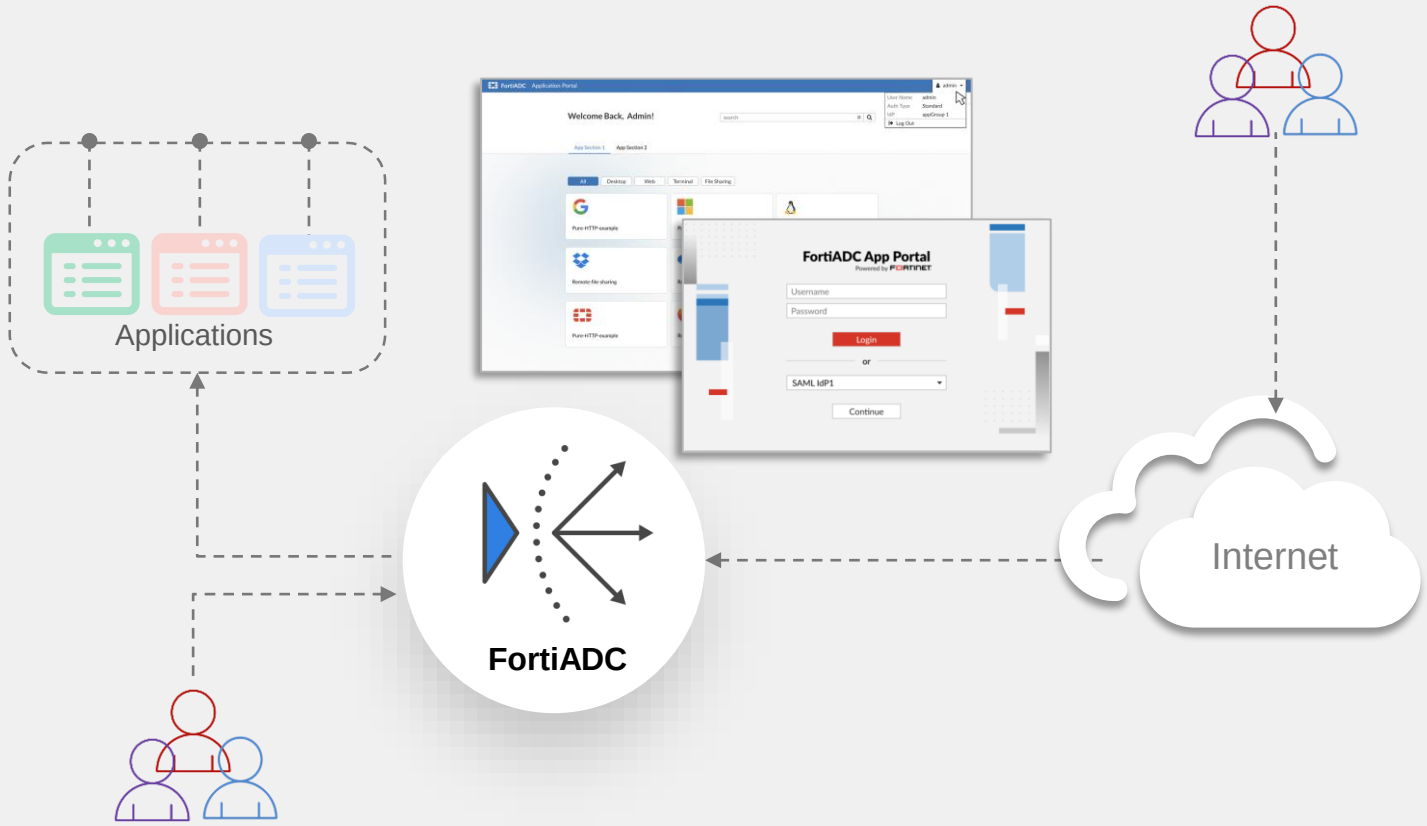
- Access internal applications with **no client-side agents**
- secure access to corporate resources from **any location,** enabling a global workforce to work efficiently and securely
- Publish RDP, VNC, Telnet, SSH, and web applications through a centralized portal

Strong Security & Authentication

- Support multi-factor authentication (MFA) and SSO
- Enforce granular user access policies for enhanced security

Real-Time Visibility & Control

- Monitor user sessions and application access



Back to Overview

Application Automation

Automation Stitches

- Ensure application automation and application security using automation stitches.
- An event triggers the predefined condition on the FortiADC that activates the action. (For example, a failed login attempt).
- FortiADC then acts in response to the trigger. (For example, changing the configuration).

Back to Overview

Application Availability

Application Availability

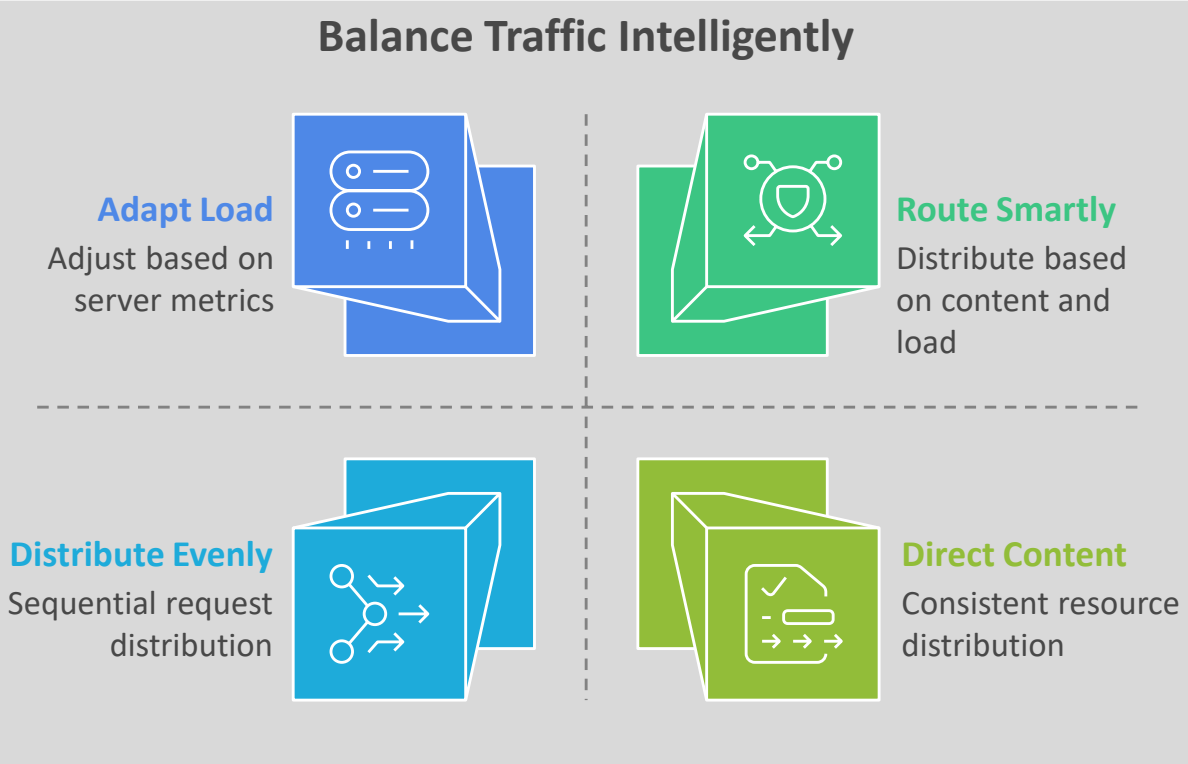
Application Availability focuses on ensuring that applications are available, responsive, and efficiently delivered to users.

- Server Load Balancing
- Health Check
- SSL Offloading
- Content Routing
- Scripting
- Global Sever Load Balancing (GSLB)
- DNS Service and Security
- Compression
- Caching
- Page Speed Optimization

Back to Overview

Server Load Balancing

-Application Availability



Server Load Balancing (SLB) is a technique that distributes incoming client requests across multiple backend servers to ensure high availability, optimal performance, and efficient resource utilization.

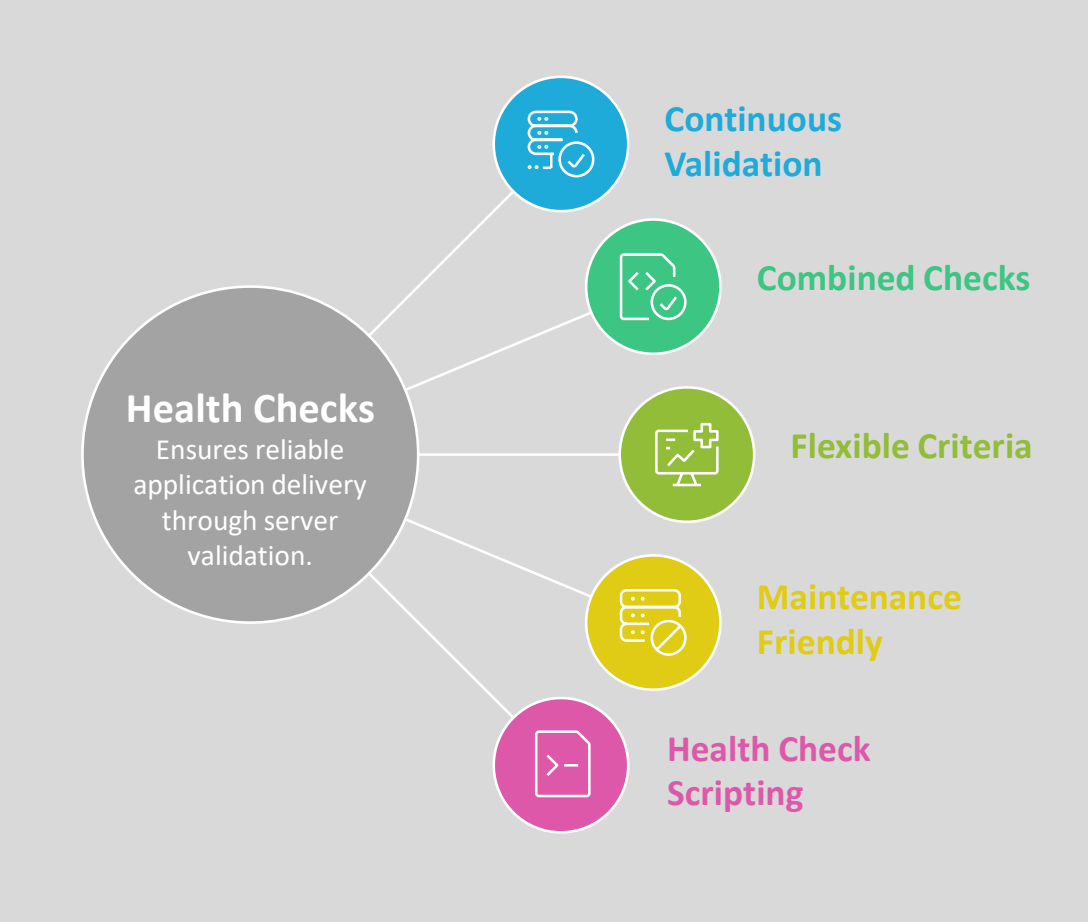
FortiADC supports both connection-based and content-aware load-balancing methods for Layer 7 traffic, including:

- **Round Robin / Least Connection** – Evenly distributes requests across servers or sends traffic to the server with the fewest active connections
- **Fastest Response** – Chooses the quickest server (health check latency)
- **URI / Host Hash** – Ensures consistent routing for same resource or domain
- **Dynamic Load** – Adjusts traffic using real-time server metrics (CPU, memory, SNMP)

Back to Overview

Health Check

-Application Availability



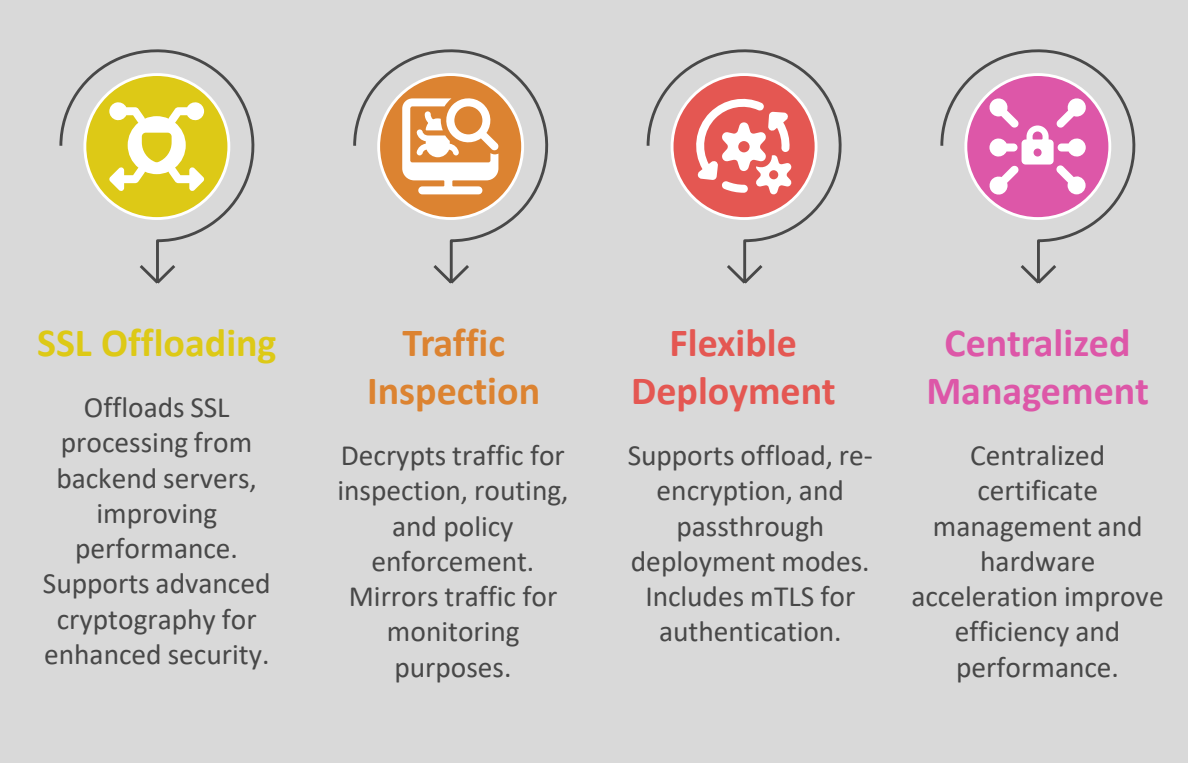
FortiADC uses health checks to monitor backend server availability and responsiveness, ensuring that traffic is directed only to healthy servers and enabling reliable application delivery.

- **Continuous validation** – Polls servers to ensure services are up before forwarding traffic.
- **Combined checks –** Multiple dependencies (e.g., web + RADIUS) must all pass.
- **Flexible criteria –** Configure interval, timeout, retries, URL, and response validation (content/status code).
- **Maintenance friendly –** Manually disable servers to stop checks during downtime.
- **Customizable checks** – Supports scripting-based health checks for advanced, customer-defined validation logic.

Back to Overview

SSL Service

-Application Availability



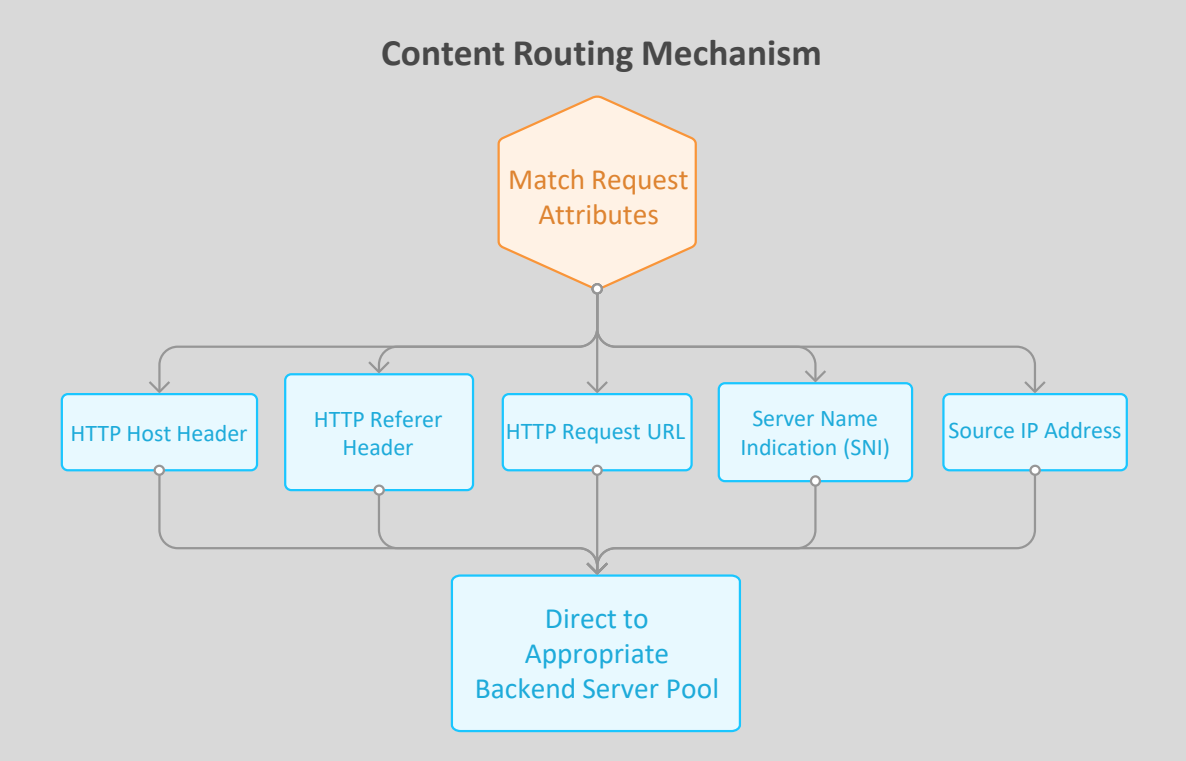
FortiADC provides comprehensive SSL services, including offloading, inspection, and traffic mirroring, to improve performance, visibility, and control.

- **Performance optimization** – Offloads SSL/TLS processing from backend servers
- **Advanced cryptography** – Supports QPC for enhanced security
- **Inspection & control** – Decrypts traffic for inspection, routing, and policy enforcement
- **Traffic mirroring** – Mirrors decrypted traffic for monitoring and analysis
- **Flexible deployment** – Supports offload, re-encryption, or passthrough modes
- **mTLS support** – Enables client certificate authentication
- **Centralized management** – Simplifies certificate handling on FortiADC
- **Hardware acceleration** – Improves performance on supported models

Back to Overview

Content Routing

-Application Availability



FortiADC uses content routing to **direct client requests to the appropriate backend server pool based on attributes in the HTTP request**.

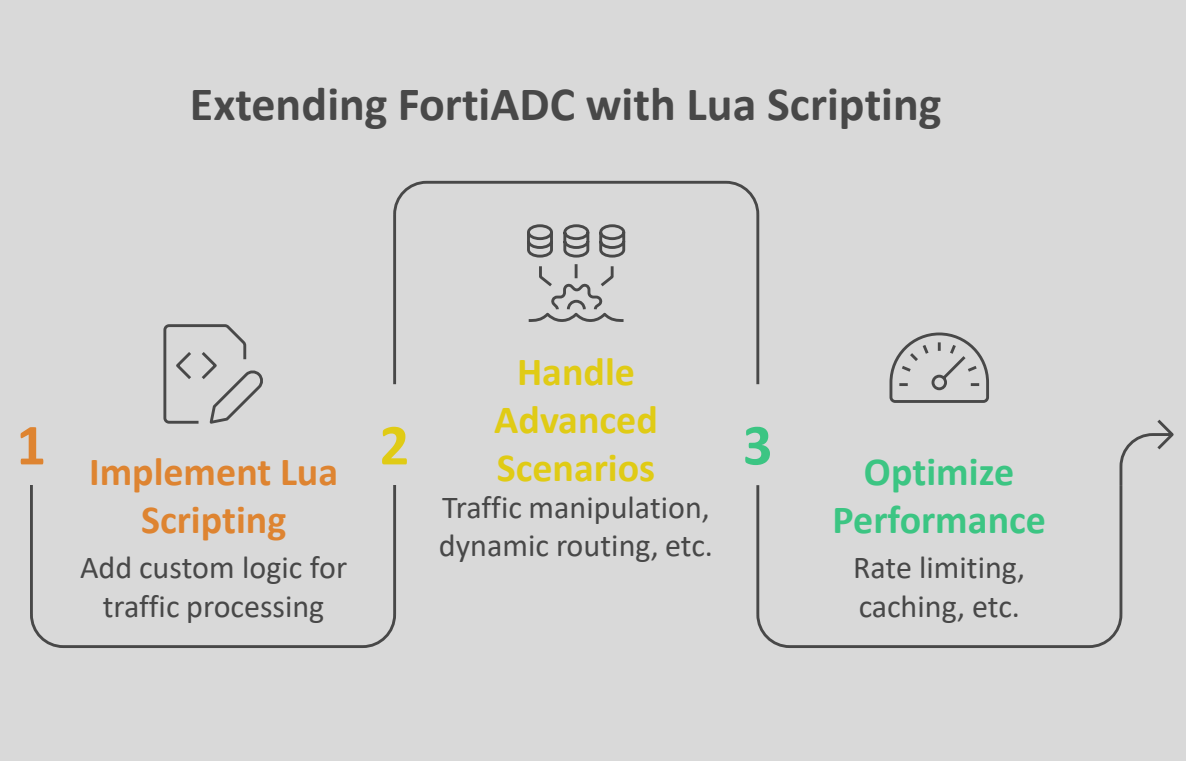
Content routing supports matching based on:

- **HTTP Host header** – for domain-based routing
- **HTTP Referer header** – for request origin-based routing
- **HTTP request URL** – for path-based routing
- **Server Name Indication (SNI)** – for HTTPS virtual hosting
- **Source IP address** – for client-based routing

Back to Overview

Scripting

-Application Availability



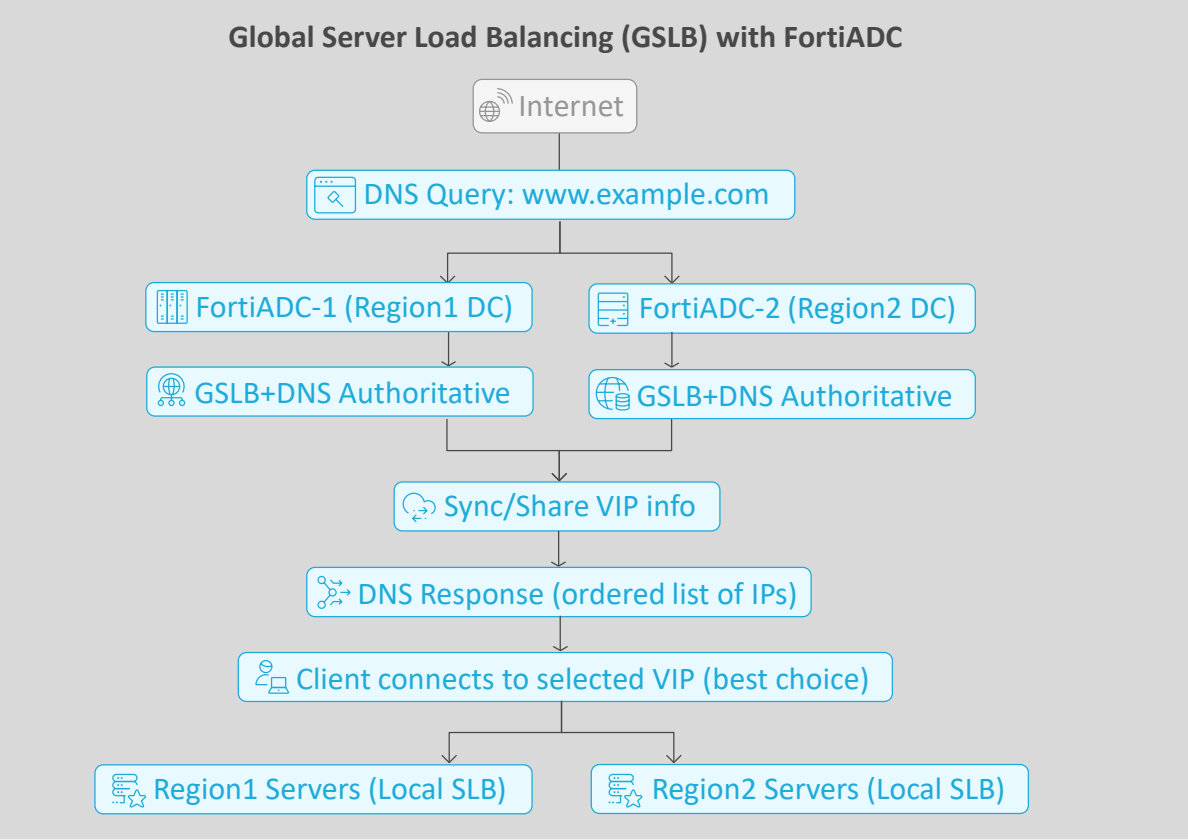
When built-in features are not sufficient, FortiADC supports Lua scripting to extend traffic processing with custom logic.
Use scripting for advanced scenarios such as:

- **Traffic manipulation** beyond standard rewriting
- **Dynamic routing** based on complex conditions
- **Custom redirection logic**
- **Advanced authentication flows**
- **Performance optimization** (e.g., rate limiting, caching)
- **Protocol handling** for special or legacy cases

Back to Overview

Global Sever Load Balancing (GSLB)

-Application Availability



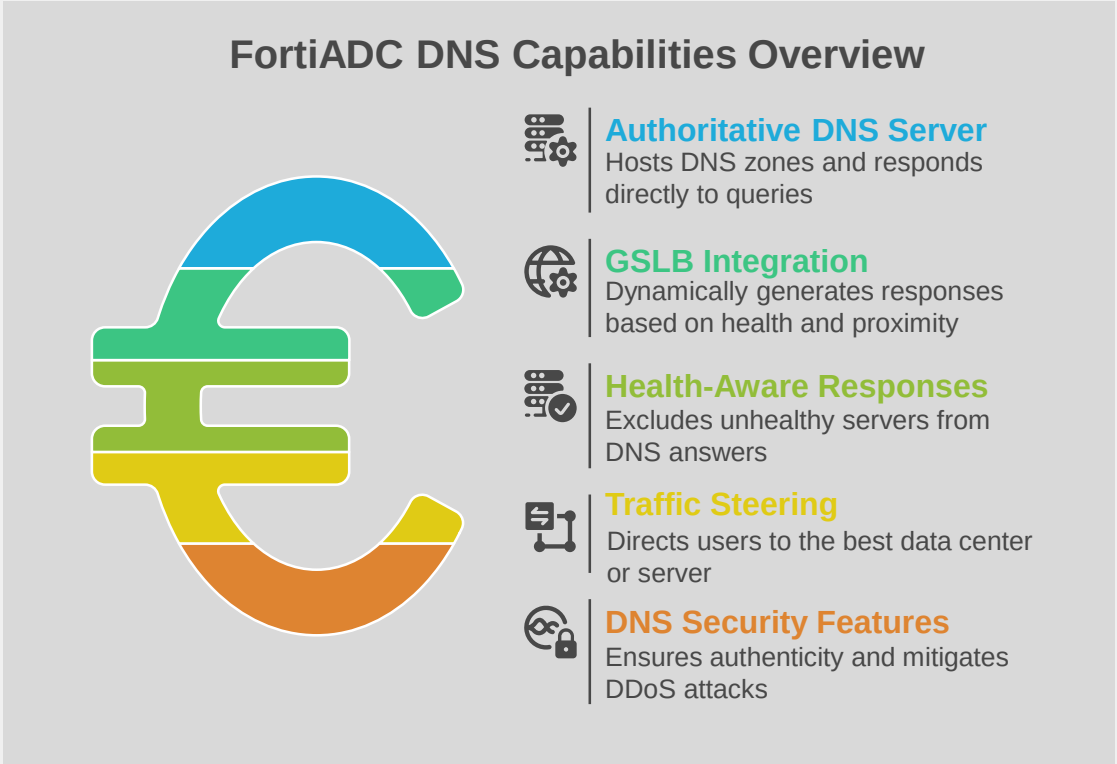
Global Load Balancing ensures that **users are directed to the best available application instance across multiple geographic locations**.
When a client accesses an application (for example, www.example.com), FortiADC uses DNS-based logic to return the most appropriate server IP based on:

- **Availability** – Only healthy data centers are selected
- **Proximity** – Users are directed to the closest location to reduce latency
- **Performance** – Traffic is routed to the best-performing server
- **Failover** – If a local site is unavailable, traffic is redirected to a backup site

Back to Overview

DNS Service and Security

-Application Availability



FortiADC includes a built-in DNS service that allows it to act as an authoritative DNS server for your domains. This DNS capability is tightly integrated with its load balancing features, especially Global Server Load Balancing (GSLB).

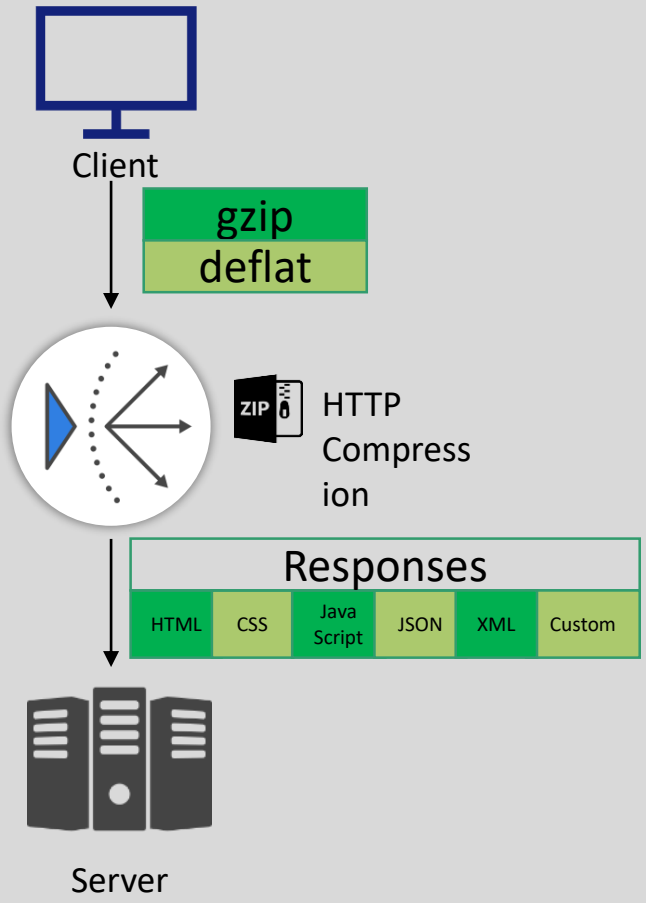
Instead of just resolving domain names to IP addresses, FortiADC's DNS service:

- Answers DNS queries for your application domains (e.g., www.example.com)
- Returns intelligent, ordered IP addresses (VIPs)
- Directs users to the best available application endpoint

Back to Overview

Compression

-Application Availability



Compression is an application-layer optimization that **reduces the size of data transmitted between the server and the client**.

In FortiADC, responses are compressed after they are generated by the backend server and before they are sent to the client, improving load time and reducing bandwidth usage.

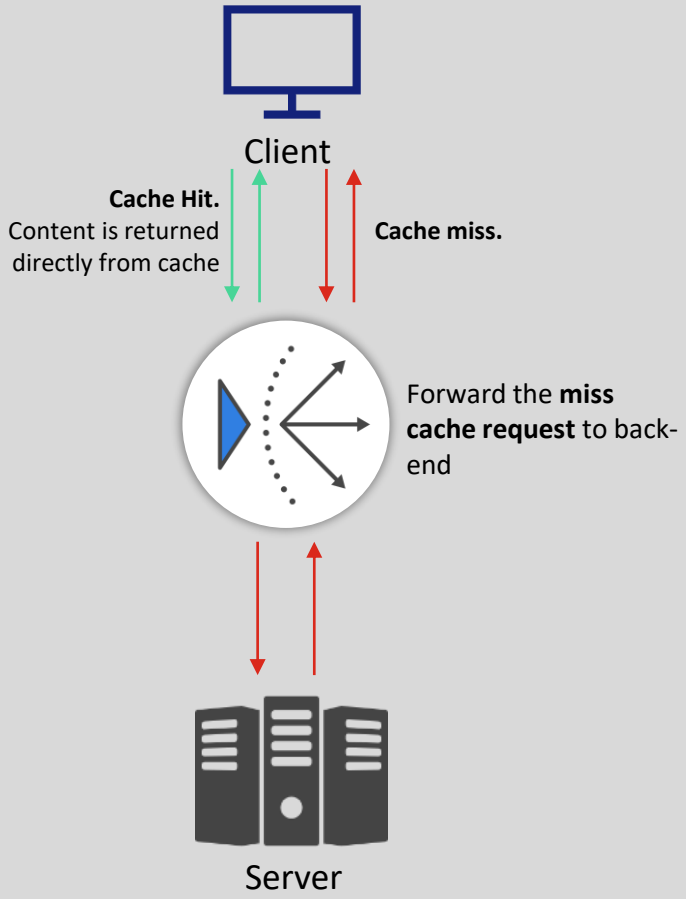
Benefits:

- Faster content delivery
- Reduced bandwidth consumption
- Improved user experience

Back to Overview

Caching

-Application Availability



Caching is an application delivery optimization that stores previously retrieved content so it can be reused for future requests without contacting the backend server.

In FortiADC, eligible HTTP responses are stored in RAM and served directly to clients, reducing backend load, network traffic, and response time.

How it works

- **Cache Miss** → Forward request to backend, store response
- **Cache Hit** → Serve content directly from cache

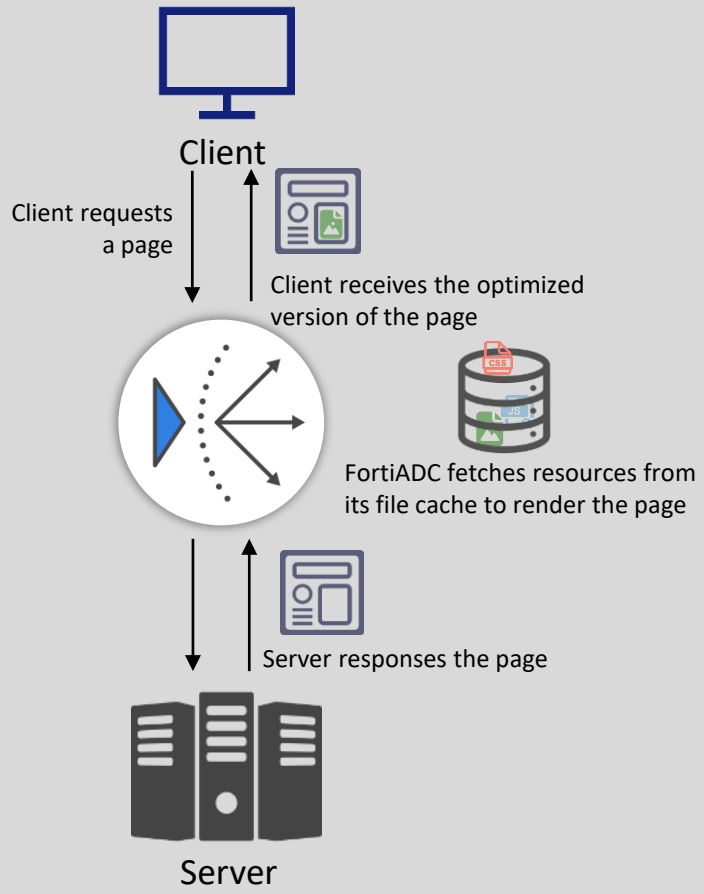
Benefits

- Faster response time
- Reduced backend load
- Lower network traffic

Back to Overview

Page Speed

-Application Availability



Page Speed Control is an application-layer optimization feature that **improves web page load performance** by rewriting and optimizing HTML pages and their referenced resources (such as JavaScript, CSS, and images) as traffic passes through FortiADC.

How it works

- Select pages by URI (include / exclude)
- Analyze HTML and referenced resources
- Apply optimizations (minify, combine, rewrite)
- Optimize resource delivery paths

Benefits

- Faster page rendering
- Reduced browser load time
- Improved user experience

Back to Overview

Application Security

Application Security

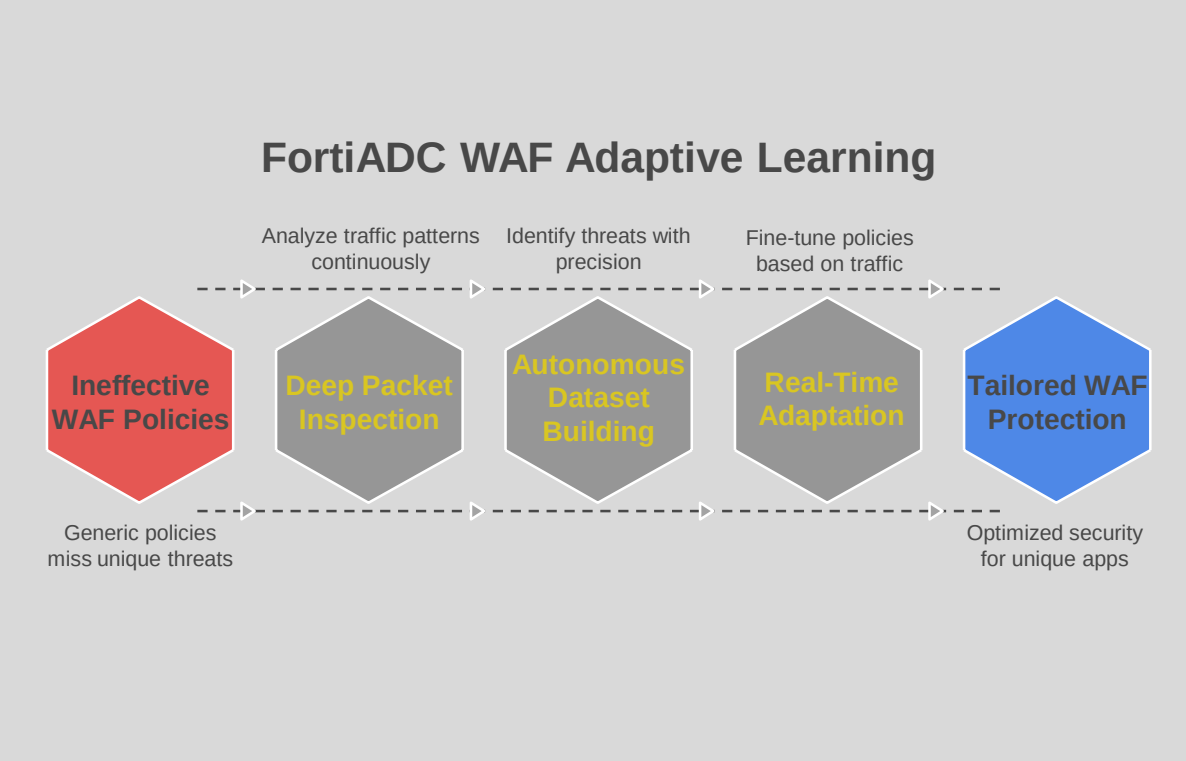
FortiADC provides multi-layered security to protect applications from modern threats.

- WAF
  - Adaptive Learning
  - OWASP Top 10 Protection
  - Web Signature
  - API Security
- DoS Protection
- Antivirus (AV)
- Intrusion Prevention System (IPS)
- Geo IP Protection
- IP Reputation

Back to Overview

WAF – Adaptive Learning

-Application Security



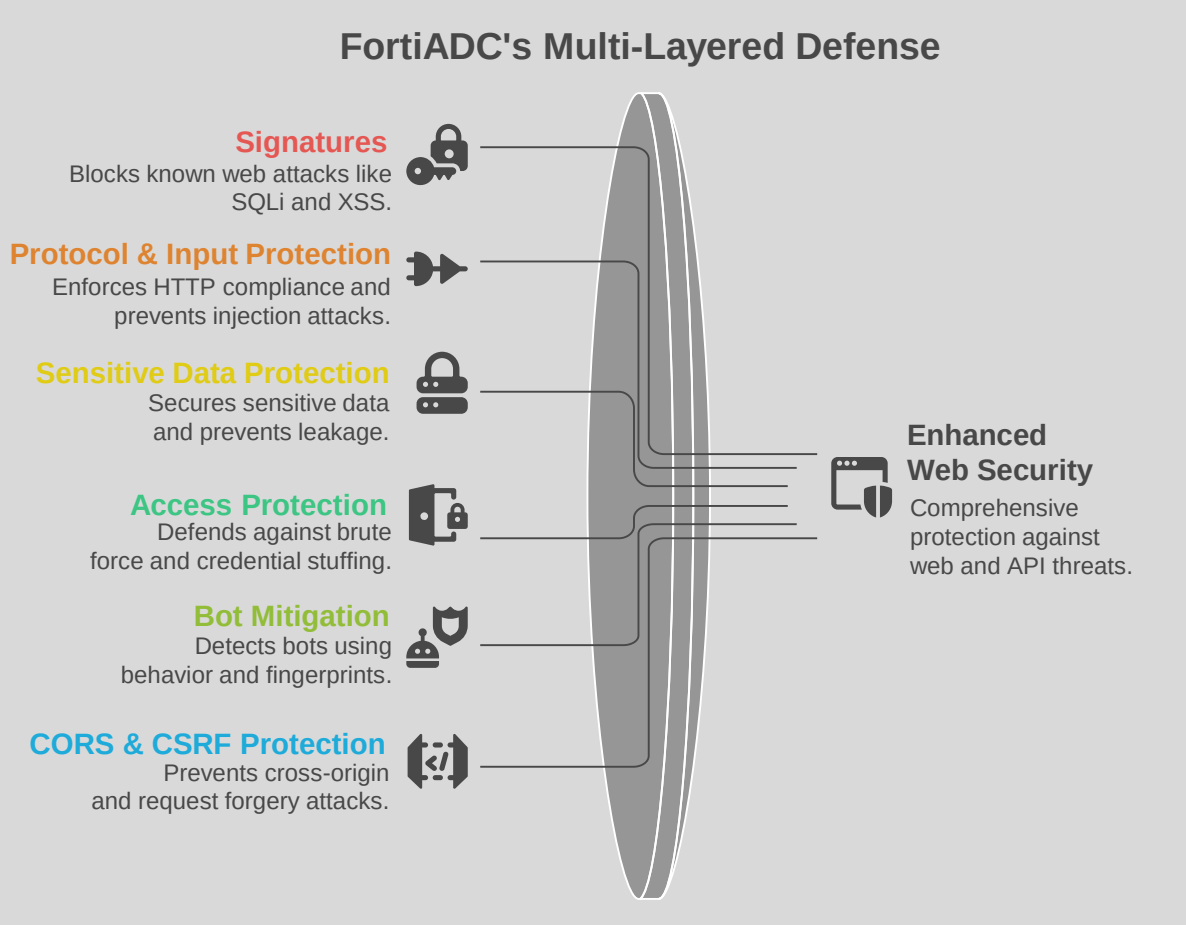
FortiADC's WAF Adaptive Learning feature uses continuous deep packet inspection and traffic analysis to dynamically generate tailored recommendations for refining WAF protection policies.

- Uses traffic analysis and deep inspection to learn application behavior
- Automatically generates policy recommendations
- Builds datasets from real traffic patterns
- Enables precise, application-specific protection

Back to Overview

WAF – OWASP Top 10 Protection

-Application Security



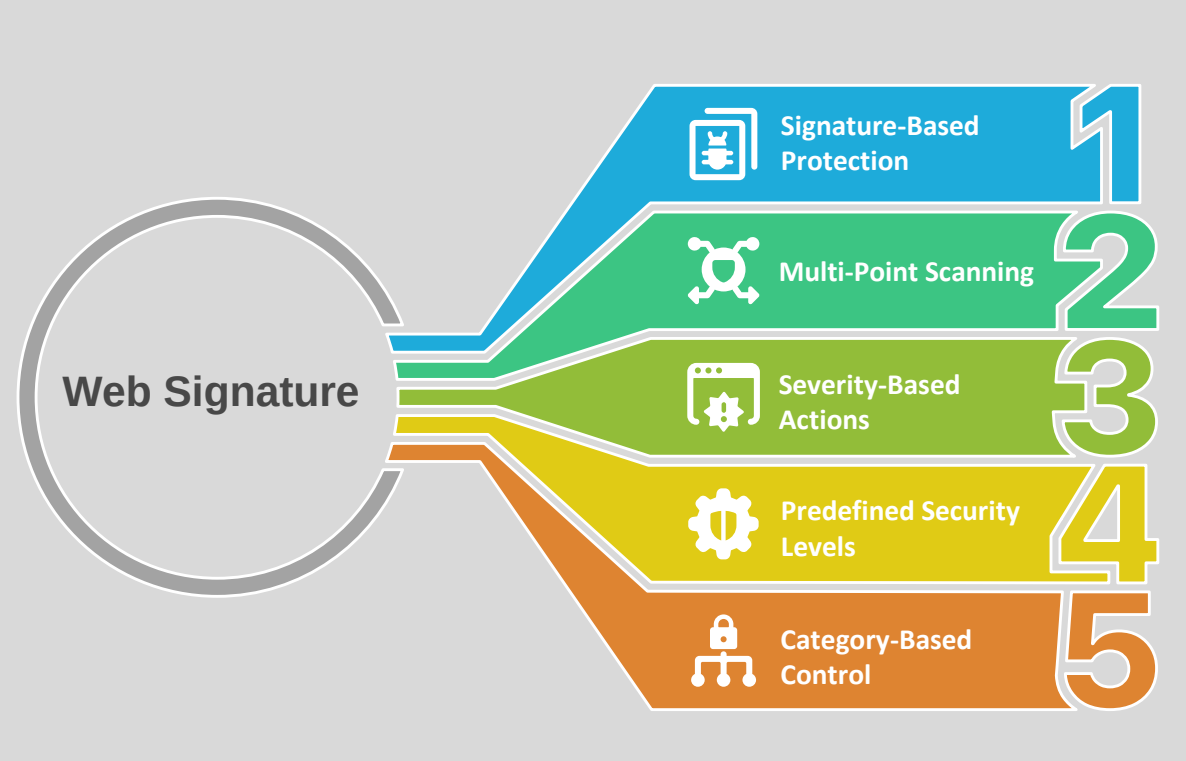
FortiADC delivers multi-layered protection against OWASP Top 10 risks across web and API applications. Its key capabilities include:

- **Signatures** – Blocks known web attacks (e.g., SQLi, XSS)
- **Protocol & Input Protection** – Enforces HTTP compliance and prevents SQL/XSS injection
- **Sensitive Data Protection** – Secures cookies, headers, and prevents data leakage
- **Access Protection** – Defends against brute force and credential stuffing
- **CORS & CSRF Protection** – Prevents cross-origin and request forgery attacks
- **Advanced Protection** – Detects complex and emerging threats
- **Bot Mitigation –** Detects bots using behavior, thresholds, and fingerprints

Back to Overview

WAF – Web Signature

-Application Security



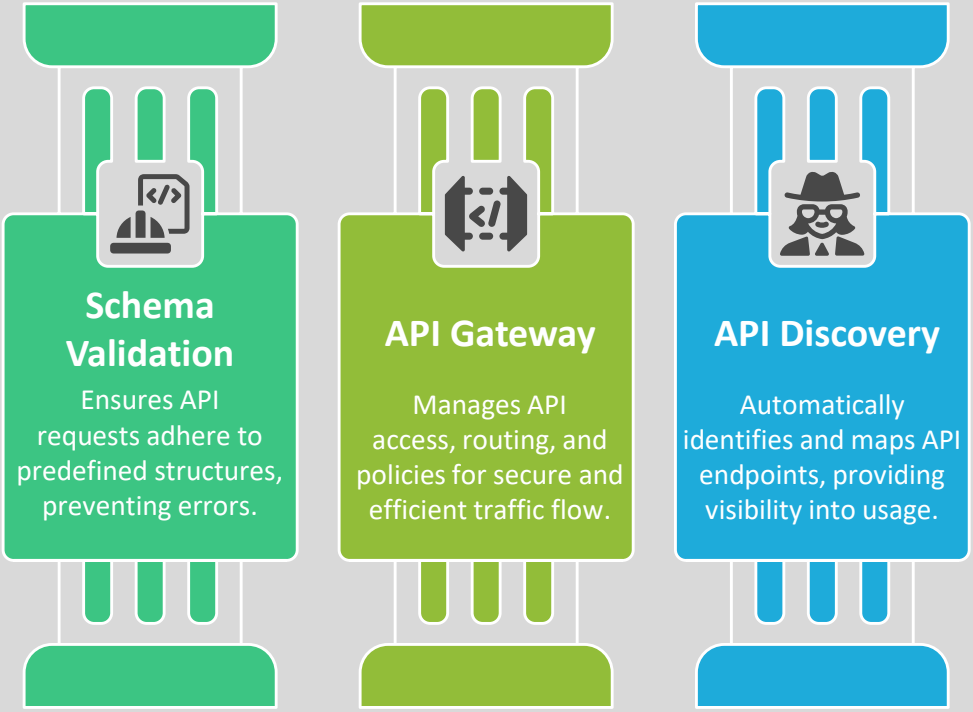
FortiADC delivers signature-based protection against known attacks with flexible scanning and severity-based actions.

- Uses FortiGuard signature database to detect known web attacks (e.g., SQLi, XSS)
- Multi-point scanning:
  - HTTP headers (always enabled)
  - Request and response body (optional for performance)
- Severity-based actions:
  - High → Deny
  - Medium → Deny or Alert
  - Low → Allow + Log
- Predefined security levels (High / Medium / Alert-only) for easy deployment
- Category-based control to enable/disable specific attack types

Back to Overview

WAF – API Security

-Application Security



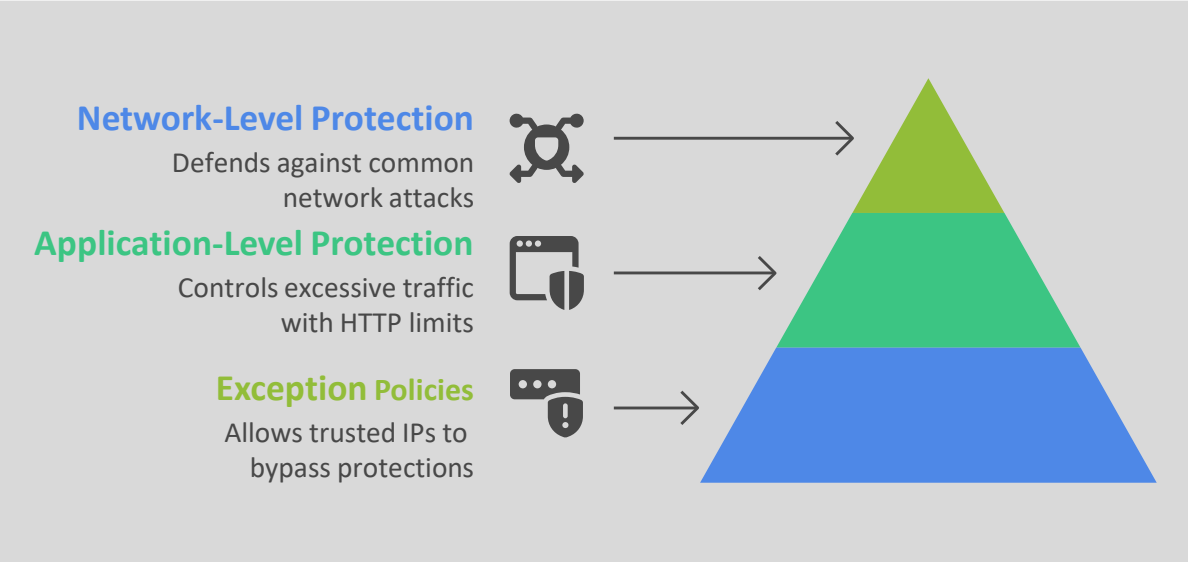
FortiADC provides comprehensive API security and management through:

- Schema Validation
  - Supports JSON, XML, and OpenAPI validation
  - Enforces API structure and detects malformed requests
- API Gateway
  - Controls API access, routing, and policies
  - Manages users and rules for API traffic
- API Discovery
  - Automatically identifies API endpoints
  - Builds visibility into API usage and behavior

Back to Overview

DoS Protection

-Application Security



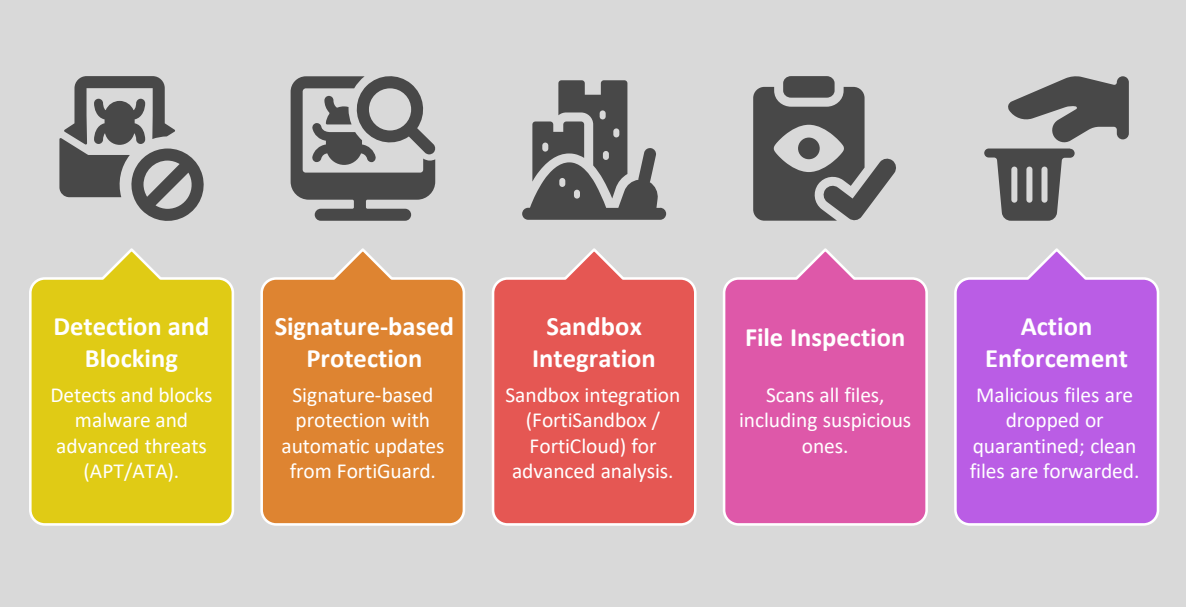
DoS Protection FortiADC provides multi-layered protection against denial-of-service (DoS) attacks across both application and network layers:

- **Application-Level Protection** controls excessive traffic with HTTP access limits. It detects and mitigates:
  - HTTP connection floods
  - HTTP request floods
  - DNS query and reverse floods
- **Network-Level Protection** defends against common network attacks:
  - TCP SYN floods
  - TCP connection floods
  - TCP slow data (slowloris) attacks
  - IP fragmentation attacks
- Exception policies allow trusted source IP addresses to bypass DoS protections

Back to Overview

Antivirus (AV)

-Application Security



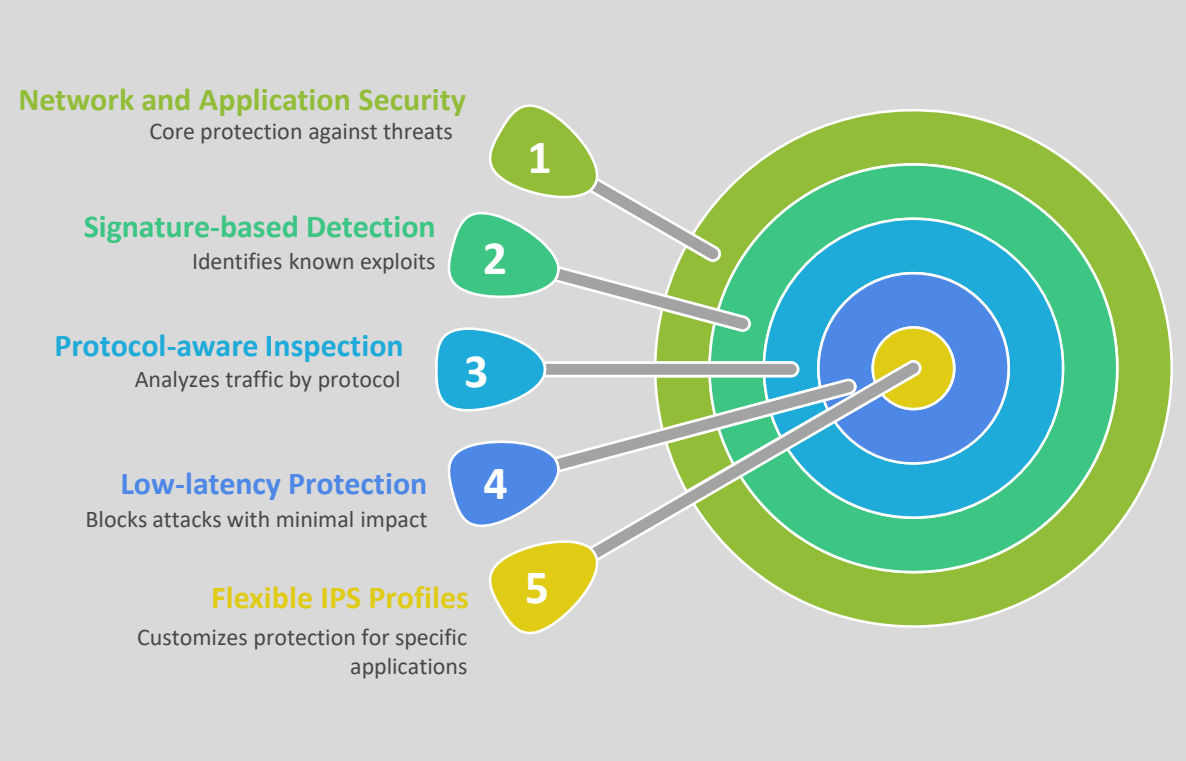
FortiADC provides integrated malware and Advanced Persistent Threats (APT) protection using the FortiOS AV engine:

- **Detects and blocks** malware and advanced threats (APT/ATA)
- **Signature-based protectio**n with automatic updates from FortiGuard
- **Sandbox integration** (FortiSandbox / FortiCloud) for advanced analysis
- **File inspection** – scans all files, including suspicious ones
- **Action enforcement** – malicious files are dropped or quarantined; clean files are forwarded

Back to Overview

Intrusion Prevention System (IPS)

-Application Security



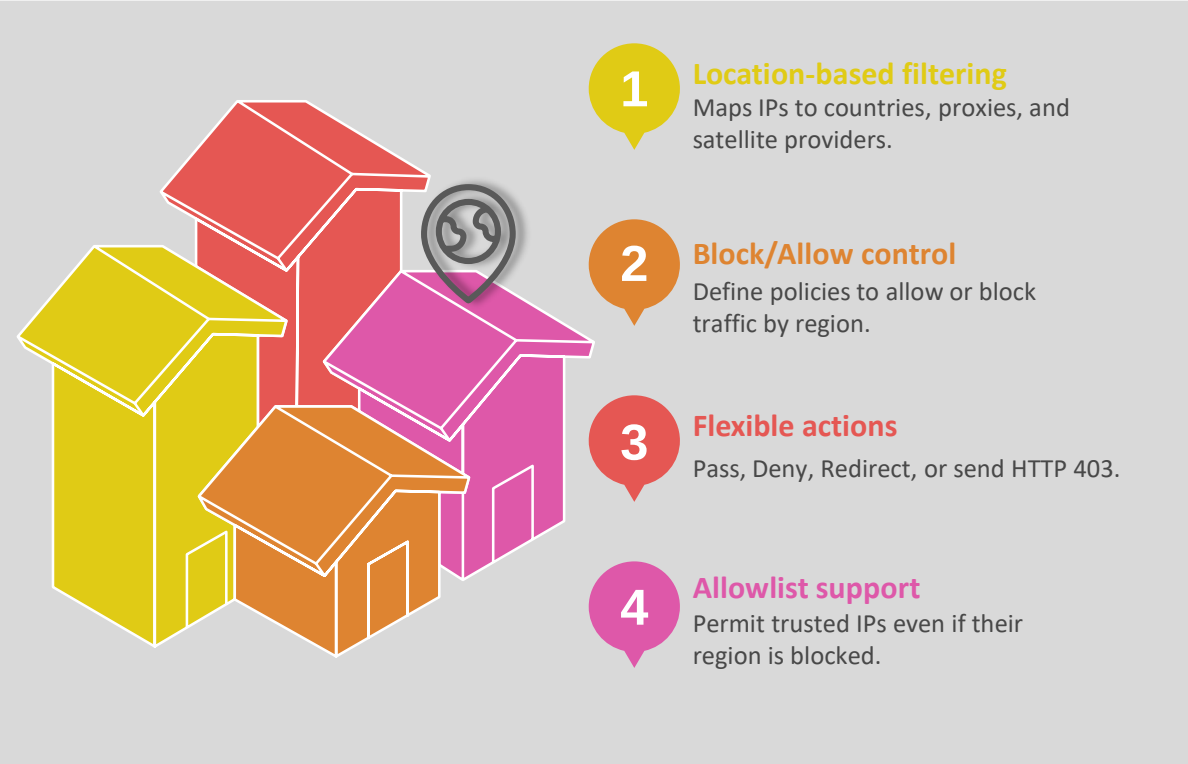
FortiADC provides an Intrusion Prevention System (IPS) to protect network and application services from known exploits and malicious traffic.

- **Signature-based detection** – Identifies known exploits using FortiGuard threat intelligence
- **Protocol-aware inspection** – Analyzes traffic by protocol for efficient and accurate detection
- **Low-latency protection** – Blocks attacks with minimal impact on performance
- **Flexible IPS profiles** – Apply predefined or custom profiles to protect specific applications
- **Automatic updates** – Continuously updated signatures for new and zero-day threats

Back to Overview

Geo IP Protection

-Application Security



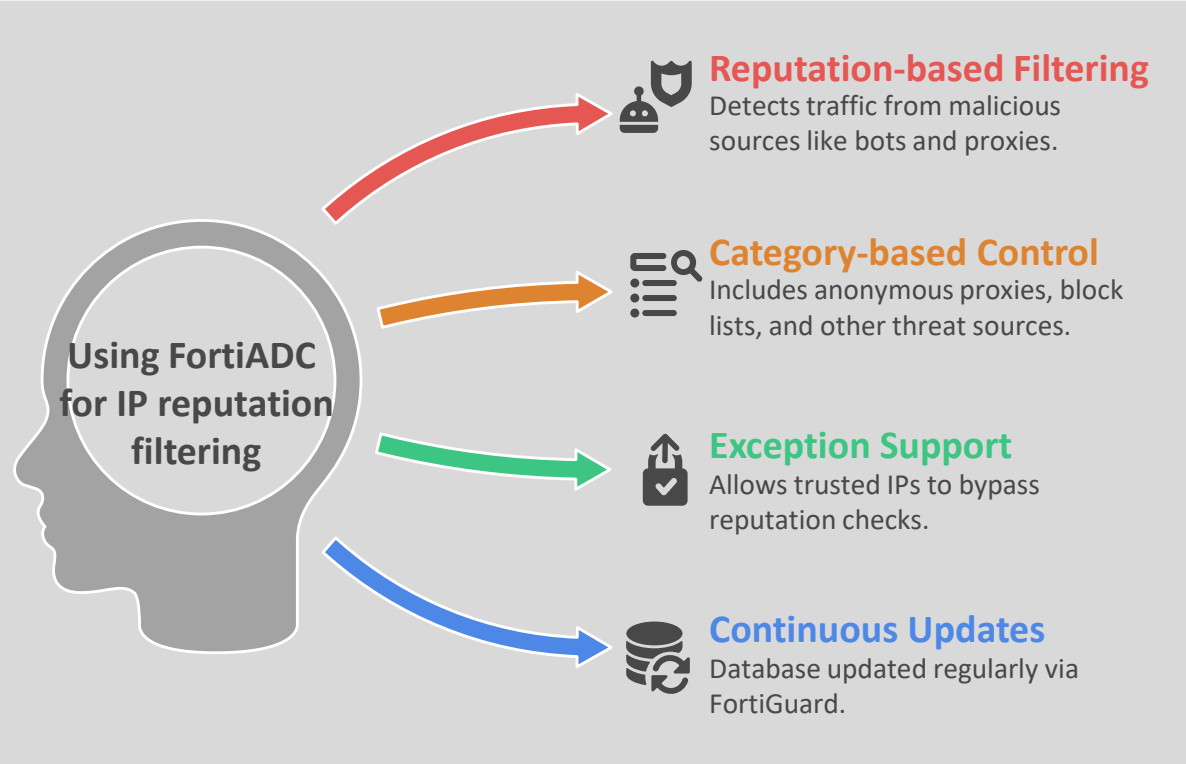
FortiADC uses the FortiGuard Geo IP database to control traffic based on geographic location.

- **Location-based filtering** – Maps IPs to countries, proxies, and satellite providers
- **Block/Allow control** – Define policies to allow or block traffic by region
- **Flexible actions** – Pass, Deny, Redirect, or send HTTP 403
- **Allowlist support** – Permit trusted IPs even if their region is blocked

Back to Overview

IP Reputation

-Application Security



FortiADC uses the FortiGuard IP Reputation database to identify and control traffic from known malicious or compromised IP addresses.

- **Reputation-based filtering** – Detects traffic from malicious sources (e.g., bots, proxies)
- **Category-based control** – Includes anonymous proxies, block lists, and other threat sources
- **Exception support** – Allows trusted IPs to bypass reputation checks
- **Continuous updates** – Database updated regularly via FortiGuard

Back to Overview

Application Access

Agentless Application Gateway (AAG)

FortiADC Agentless Application Gateway (AAG) is an agentless remote access gateway built on FortiADC's Layer-7 reverse-proxy engine.

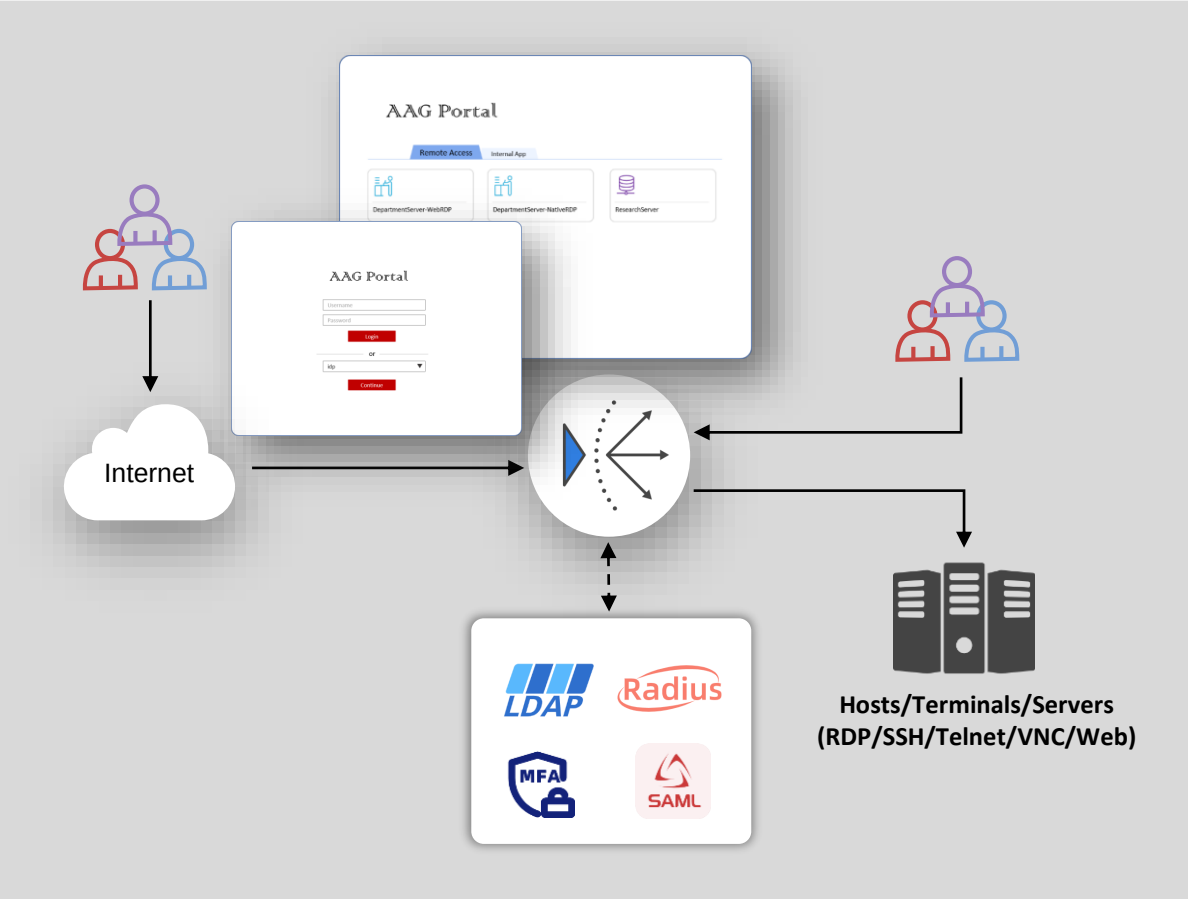
Its key capabilities include:

- Application Portal
- Site and Application Publishing
- Application Authentication

Back to Overview

Application Portal

-AAG



The AAG Portal in FortiADC is a web-based access portal that provides users with secure, centralized access to remote desktop or terminals as well as internal web Apps—without requiring a VPN or client software.

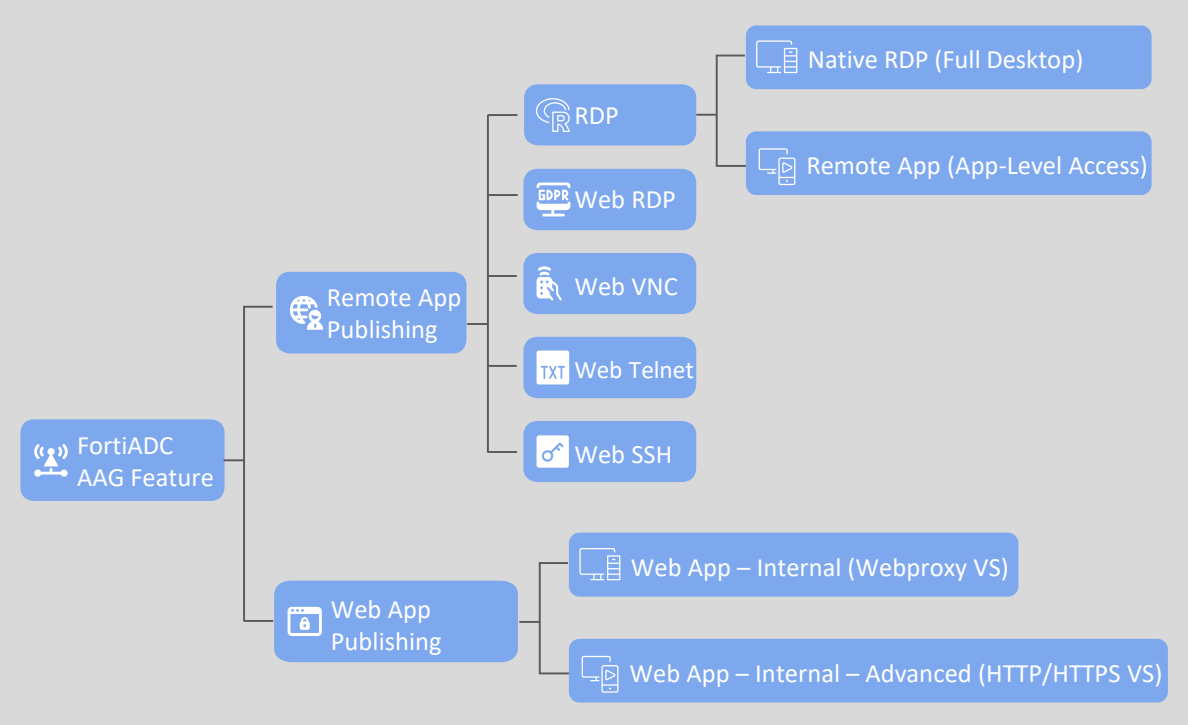
Users from both the Internet and internal network can access the AAG portal through the following process:

1. Users enter the AAG portal URL in their browser.
2. FortiADC validates user credentials through remote authentication servers or identity providers (IdPs).
3. After authentication, users see the AAG portal with the applications assigned to them.
4. When a user clicks an application, FortiADC connects the user to the corresponding backend RDP, SSH, Telnet, VNC, or web server.

Back to Overview

Site and Application Publishing

-AAG



FortiADC enables secure access to backend systems through both browser-based and native client connections.

Remote Hosts & Terminals

- Native RDP (full desktop) and Remote App (app-level)
- Browser-based access: RDP, VNC, Telnet, SSH

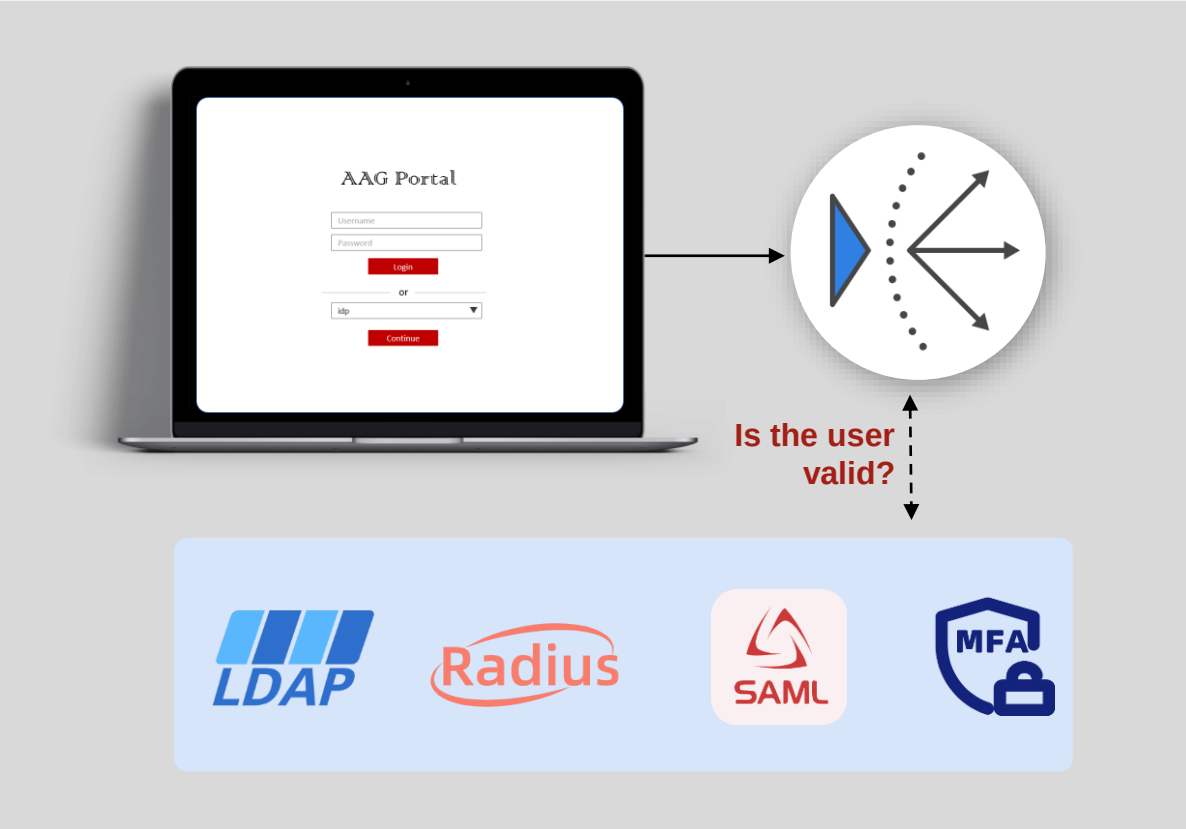
Internal Web Applications

- Published through the AAG portal instead of directly exposing to the Internet
- Portal acts as a secure access gateway

Back to Overview

Application Authentication

-AAG



FortiADC provides secure and flexible user authentication and access control through the AAG portal.

- **Centralized Authentication & Policy Enforcement**
  - Defines authentication, authorization, and session behavior
  - Supports LDAP, RADIUS, and SAML-based identity providers
- **Federated Authentication (SAML 2.0)**
  Integrates with external IdPs (e.g., FortiAuthenticator, Microsoft Entra ID)
- **Multi-Factor Authentication (MFA)**
  Adds an extra layer of verification for enhanced security

Back to Overview

System & Operations

System and Operations

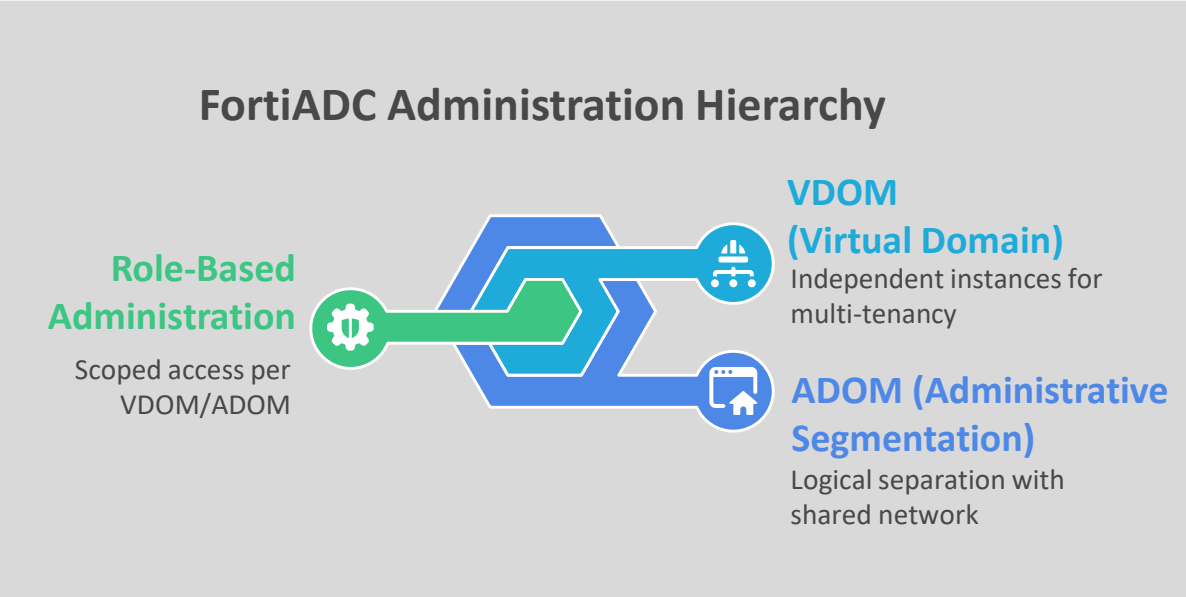
FortiADC provides system-level features for scalability, automation, and visibility.

- VDOMs and ADOMs
- FortiAI Assistant
- Automation Stitches
- FortiView

Back to Overview

VDOMs and ADOMs

-System and Operations



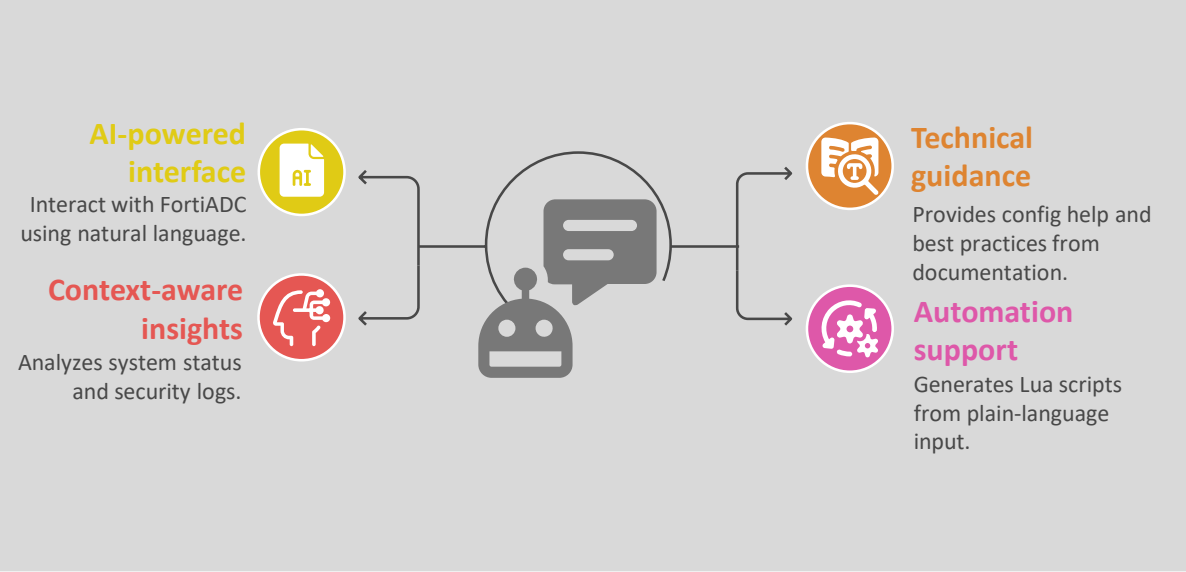
FortiADC supports multi-tenancy and administrative separation through Virtual Domains (VDOMs) and Administrative Domains (ADOMs).

- **VDOM (Virtual Domain)**
  - Multiple independent FortiADC instances on one device
  - Separate configs for **multi-tenant deployments**
  - Supports **independent or shared** networking modes
- **ADOM (Administrative Segmentation)**
  - Logical separation with **shared network and routing**
  - Restricts admin access to specific resources
- **Role-Based Administration**
  - Scoped admin access per VDOM/ADOM
  - Global admins manage all domains

Back to Overview

FortiAI Assist

-System and Operations



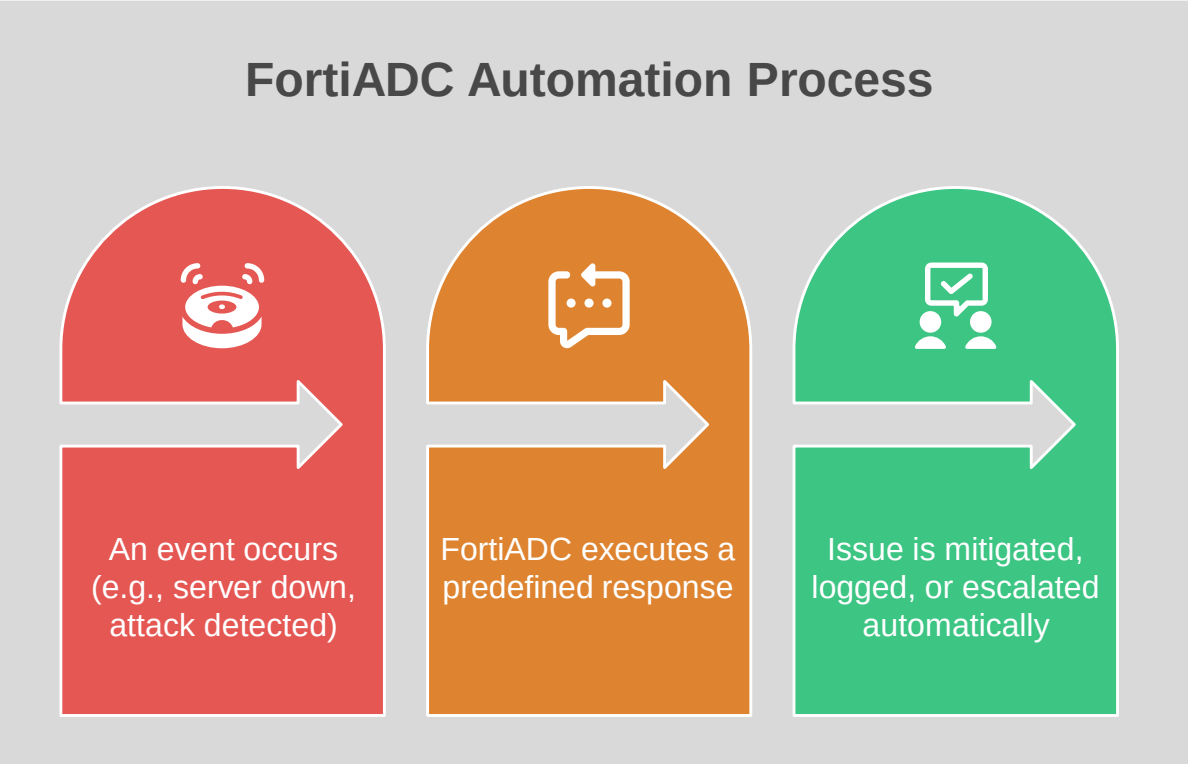
FortiAI Assist is available in GUI (Ask FortiAI panel). It simplifies configuration, troubleshooting, and automation with AI-driven assistance.

- **AI-powered interface** – Interact with FortiADC using natural language
- **Technical guidance** – Provides config help and best practices from documentation
- **Context-aware insights** – Analyzes system status and security logs
- **Automation support** – Generates Lua scripts from plain-language input

Back to Overview

Automation Stitches

-System and Operations



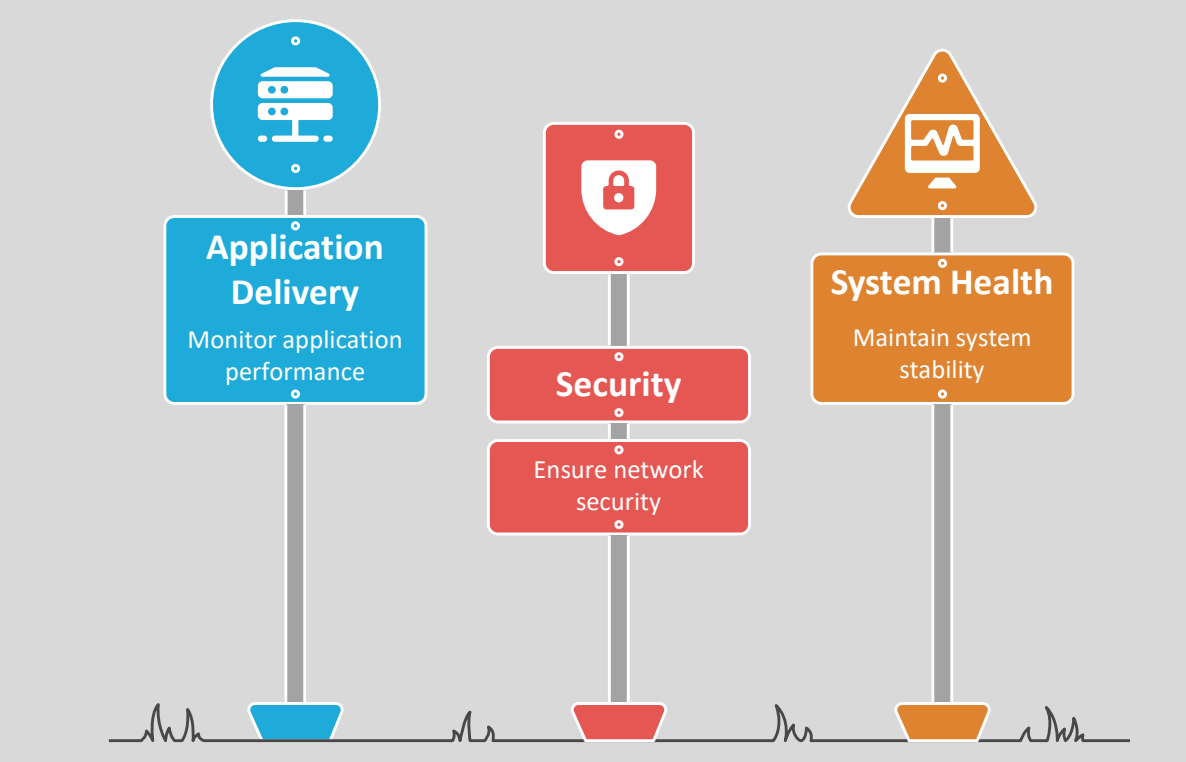
FortiADC Automation Stitches enables event-driven workflows that automatically respond to system, application, and security events without manual intervention.

- **Event-driven response**
  Reacts to system, network, and security events in real time
- **Automated mitigation**
  Takes actions such as blocking IPs, running scripts, or limiting traffic
- **Alerting & notification**
  Sends alerts via email, SNMP, or syslog
- **System integration**
  Connects with external systems using webhooks or FortiGate integration
- **Operational efficiency**
  Reduces manual effort and speeds up troubleshooting and response

Back to Overview

FortiView

-System and Operations



FortiView provides real-time visibility and analytics for your FortiADC, helping you monitor application delivery, security, and system health from a centralized dashboard.

- **Logical Topology** – End-to-end application flow and relationships
- **Server Load Balance** – Traffic distribution and server performance
- **Security** – Threats, attacks, and protection status
- **System** – Events, alerts, and operational status
- **Global Load Balance** – Cross-region traffic and availability
- **Link Load Balance** – WAN/link utilization and performance
- **ZTNA Endpoints** – Visibility into client access (FortiClient)
- **AAG User Sessions** – Real-time view of active user sessions

Back to Overview

Conclusion

FortiADC delivers a comprehensive platform that combines application delivery, security, access, and automation.
By integrating intelligent load balancing, advanced threat protection, performance optimization, and AI-driven operations, FortiADC ensures applications are always available, secure, and high-performing.
With its unified capabilities, organizations can simplify management, improve user experience, and respond to challenges with greater efficiency and confidence.


FORTINET