بسم الله الرحمن الرحيم

Information Sheet

Web Application Firewall

Supply, Install, Configure and Integration for Application Delivery Controller with Web Application Firewall

1. Product:
   - Product Name: Fortinet FortiADC Virtual Appliance
   - Product Description: A comprehensive virtual application delivery controller (ADC) solution designed to optimize the delivery, security, and performance of web applications.
   - Virtualization Platforms: VMware, Microsoft Hyper-V, KVM
2. Throughput Capacity:
   - High-performance ADC with a throughput capacity of 2Gbps to handle heavy traffic loads and ensure seamless application delivery.
3. Load Balancing:
   - Load balancing methods include round-robin, weighted round-robin, least connections, and source IP-based persistence.
4. SSL/TLS Offloading:
   - SSL/TLS offloading capabilities to relieve backend servers from the resource-intensive task of encrypting and decrypting SSL/TLS traffic.
   - Enhances server performance and scalability while ensuring secure communication with clients.
5. Application Acceleration:
   - Advanced features such as HTTP/2 optimization, caching, compression, and content routing to accelerate application performance and improve user experience.
   - Acceleration techniques optimize application delivery, reduce latency, and enhance overall responsiveness.
6. Web Application Firewall (WAF):
   - Integrated web application firewall (WAF) functionality to protect against common web-based attacks, including SQL injection, cross-site scripting (XSS), and remote file inclusion.
   - Offers customizable security policies, predefined rules, web application signatures, and HTTP parameter protection to safeguard web applications from threats.
7. High Availability (HA):
   - Shall support Active-active or active-passive high availability configurations for continuous availability of web services.
8. Scalability:
   - Shall be scalable architecture to accommodate growing traffic demands and evolving business requirements.

9. Security Fabric Integration:
    - Shall support seamless integration with the Fortinet Security Fabric, enabling unified visibility, control, and management across the entire security infrastructure.
    - Shall support Integration with existing FortiGate firewalls, FortiManager, and FortiAnalyzer for coordinated security policies, centralized logging, and analysis.
10. Support and Maintenance:
    - Comprehensive support and maintenance services, including technical assistance, firmware updates, and access to Fortinet's customer portal for resources and documentation.
    - Shall include 1 Year Standard Bundle (FortiCare Premium plus IP Reputation and FortiADC WAF Security Service).

Installation, Configuration, Integration and Training Service

Overview

The purpose of this project is to implement a comprehensive Fortinet FortiADC Virtual Appliance solution, including web application firewall (WAF) capabilities, to optimize the delivery, security, and performance of our web applications. The project aims to enhance application availability, scalability, and user experience while ensuring seamless integration with our existing Fortinet Security Fabric. The scope of work includes the following tasks:

Installation and Configuration:

- Deployment Planning: Conduct a thorough assessment of the client's network infrastructure, requirements, and objectives to develop a comprehensive deployment plan.
- Installation: Install and deploy the FortiADC Virtual Appliance on the designated virtualization platform (VMware) as per the manufacturer recommended specifications.
- Configuration: Configure the FortiADC Virtual Appliance to align with the client's network architecture, load balancing requirements, SSL/TLS settings, and security policies.
- Performance Optimization: Fine-tune the configuration to optimize the performance of the FortiADC solution, ensuring efficient traffic distribution and application acceleration.

Web Application Firewall (WAF) Configuration:

- Requirement Gathering: Collaborate with the client to understand their specific web application security requirements, including the desired security policies, threat vectors, and application-specific rules.
- WAF Policy Development: Develop a comprehensive WAF policy tailored to the client's web applications, utilizing the available features and capabilities of the FortiADC Virtual Appliance.
- Predefined Rule Customization: Customize and fine-tune the predefined rules provided by the FortiADC WAF to align with the client's security needs and web application characteristics.
- Web Application Signatures: Enable and configure the use of web application signatures to detect and block common attack patterns, such as SQL injection, cross-site scripting (XSS), and remote file inclusion.
- HTTP Parameter Protection: Configure the FortiADC WAF to protect web applications against attacks targeting HTTP parameters by validating and sanitizing user input.

- Session Protection: Implement session protection mechanisms, such as session tracking and cookie security, to prevent session hijacking and enforce secure session management.
- Rate Limiting: Enable rate limiting settings in the FortiADC WAF to mitigate the impact of excessive traffic or potential denial-of-service (DoS) attacks.
- Geolocation-based Access Control: Utilize the geolocation capabilities of the FortiADC Virtual Appliance to restrict access to web applications based on the geographical location of the clients.
- Web Application Security Monitoring: Configure logging and alerting mechanisms within the FortiADC Virtual Appliance to monitor web application security events, detect anomalies, and generate alerts.
- Ongoing Maintenance: Ensure regular updates of the FortiADC WAF's security rules, signatures, and policies to address emerging threats and vulnerabilities.

Integration with Existing Fortinet Security Fabric:

- FortiGate Firewall Integration: Integrate the FortiADC Virtual Appliance with the existing FortiGate firewalls to ensure seamless traffic flow and coordinated security policies.
- FortiManager Integration: Configure the integration between the FortiADC Virtual Appliance and the FortiManager system to enable centralized management and monitoring of the ADC solution.
- FortiAnalyzer Integration: Set up the integration between the FortiADC Virtual Appliance and the FortiAnalyzer system for centralized logging, reporting, and analysis of ADC-related data.
- Security Fabric Integration: Establish integration between the FortiADC solution and the client's existing Fortinet Security Fabric, enabling unified visibility, control, and management across the entire security infrastructure.

Testing and Validation:

- Functional Testing: Perform comprehensive functional testing to ensure the proper functioning of the FortiADC Virtual Appliance, including load balancing, SSL/TLS offloading, and application acceleration.
- Integration Testing: Validate the integration between the FortiADC solution, FortiGate firewalls, FortiManager, and FortiAnalyzer to ensure smooth interoperability and seamless data exchange.

Knowledge Transfer and Documentation:

- Training: Provide training sessions to 2 members of the IT team, covering the management, administration, and monitoring of the FortiADC Virtual Appliance and its integration with the Fortinet Security Fabric.
- Documentation: Prepare comprehensive documentation, including installation guides, configuration instructions, integration procedures, and troubleshooting guidelines.