UNIVERSAL POSTAL UNION

NON-BINDING REQUEST FOR INFORMATION

Web Application Firewall, Network Load Balancer and Access Policy Gateway

Issue Date: 5 April 2024

CONTENTS

Definitions

In this Non-Binding Request for Information, the following terms shall have the following definitions, unless otherwise stated:

- “Designated Operator” means any governmental or non-governmental entity/entities officially designated by a UPU member country to operate postal services and to fulfil the related obligations arising out of the Acts of the UPU on its territory;
- "Respondent" means any entity expressing its interest in the project for the Web Application Firewall (WAF), Network Load Balancer (NLB) and Access Policy Gateway (APG) within the UPU and providing a response to any or all of the areas of information requested by this RFI;
- “RFI” means this document, which is intended to gather information in order to assist the Universal Postal Union in chosing the right technology/product for the WAF/NLB/APG; to assist the Universal Postal Union in establishing the necessary parameters upon which future procurement processes might be issued; and to identify the universe of entities which might be interested in participating in the potential implementation of the WAF/NLB/APG infrastructure and its related services by the Universal Postal Union;
- "RFI Response" means any document lodged by a Respondent in response to this RFI;
- "UPU" means the Universal Postal Union, an intergovernmental organization and specialized agency of the United Nations whose main aim is to secure the organization and improvement of the postal services and to promote in this sphere the development of international collaboration;

Important Notice and Disclaimer

This RFI and any of its parts, as well as any information, advice or data subsequently provided to the Respondent whether orally or in writing by or on behalf of the UPU, shall be subject to the terms and conditions set out in this RFI or any other specific agreement entered into by the Respondent and the UPU. Therefore, upon having access and receiving any or all of the information contained herein by any means of communication, the Respondent agrees to comply with all the terms and conditions contained herein; the Respondent further acknowledges and agrees that all information contained herein may not be used, copied, reproduced or distributed to any other person for any purpose whatsoever without the prior written consent of the UPU.

This RFI does not constitute an offer nor is it an invitation or solicitation for any Respondent or any other person to become a provider of products or services to the UPU or its member countries. Each Respondent shall make its own independent assessment and investigation of the information contained herein, and should not rely on any statement or on the significance, adequacy or accuracy of any information contained in this RFI.

Furthermore, the information contained herein does not purport to contain all of the data that a Respondent may deem necessary to provide its RFI Response. The information contained herein may not be deemed adequate or appropriate for all prospective Respondents, and it is not possible for the UPU to have regard to the objectives, financial situation and particular needs of each Respondent having access to the information contained herein. Some Respondents may have a better knowledge of, or access through their own business activities to, more information concerning the information requested by this RFI than other Respondents. In all cases, before acting in reliance on any of the information contained herein, the Respondent should conduct its own investigation and analysis in relation to this RFI, as well as to its accuracy, completeness and reliability; in case of doubt, the Respondent should strive to obtain independent and specific assistance from appropriate professional advisers.

In that regard, the UPU makes no representation or warranty as to the accuracy, completeness, reliability and timeliness of any information contained in this RFI. The UPU and any of its agents, employees and consultants shall incur no liability for any statements, opinions, information or matters, expressed or implied, arising out of, contained in or derived from, or any omissions from, the information contained in this RFI except in so far as liability under any statute cannot be excluded. The UPU shall not be responsible for, nor shall it pay for, any costs, expenses or losses which may be incurred by a Respondent or its representatives in conducting their review and evaluation of this RFI, in expressing interest or submitting an RFI Response, or in any other way arising from, or connected with, this RFI.

The information contained in this RFI is of a preliminary nature and subject to clarification and change. The UPU may, at its absolute discretion, update, amend or supplement the information contained in this RFI. The UPU may also, at its absolute discretion, amend or discontinue this RFI or any future procurement processes potentially related thereto at any time and without further notice. All costs related to RFI Responses shall be borne by the Respondents. All references to currency shall be in Swiss Francs (CHF) unless expressly stated otherwise. References to years concern calendar years starting on 1 January and ending on 31 December, unless otherwise stated. No representation made by or on behalf of UPU in relation to this RFI or its contents shall be binding on the UPU unless that representation is made in writing and incorporated into contractual documents to be formed on the basis of this RFI or any subsequent procurement processes issued by the UPU, as the case may be.

Nothing in or relating to this RFI shall be deemed a waiver, express or implied, of any of the privileges and immunities of the UPU.

Background Information

1.1 Introduction

The UPU is interested in researching the market for potential solution providers of Web Application Firewall, Network Load Balancer and Access Policy Gateway functionalities.

The UPU aims to identify solutions, either on-premise or in the cloud, that could combine above-mentioned services into one product/solution.

1.2 The UPU

The postal sector plays a key role in the economic and social development of many countries and continues to provide services critical to the global economy. Indeed, the postal sector globally employs more than five million people and has more than 642,000 retail points across the globe in locations, ranging from major cities to some of the remotest locations on the planet. This represents one of the largest networks in the world.

The UPU, established in 1874 with its headquarters in Berne, Switzerland, is the primary forum for cooperation between postal sector players and helps to ensure a truly universal network of up-to-date international postal products and services. With 193 member countries, this specialized agency of the United Nations fulfils an advisory, liaison and regulatory role and renders technical assistance where needed. It sets the rules for international mail exchanges and makes recommendations to stimulate growth in mail volumes and to improve the quality of service for customers. As an intergovernmental institution, the UPU is called upon to play an important leadership role in promoting the continued revitalization of postal services.

1.3 Scope of the request for information

The UPU is launching this Request for Information (RFI) to identify potential solution providers to combine Web Application Firewall (WAF), Network Load Balancer (NLB) and Access Policy Gateway (APG) into one product or service to enable threat and security protection of on-premise and cloud web applications and APIs.

The total number of web applications (including APIs) to be protected by the solution:

On-premise:	200-250
Cloud (Azure/AWS):	30-50

The major web platforms used by the web applications are:

- IIS
- SharePoint (2016/2019)
- Apache (Apache Tomcat)

The total number of users accessing web applications:

- 300-350 internal users
- up to 10,000 external users

After analysis of the answers to this RFI the UPU may decide to launch a formal Call for Tender (CFT).

Providers interested in this RFI are asked to provide answers according to the structure given in section 2.1. Answers to sections 3.4 (pricing and costs) and 2.3 (technical description of the solution) do not impose a specific format.

2. Main Requirements of the RFI

2.1 Core Requirements

Area	Requirement	Covered?
Technical Web Application Firewall (WAF)	Support various deployment options, including on-premise, cloud-based or hybrid deployment models	
	Compatibility with major cloud platforms such as Azure, AWS and Google Cloud Platform	
	Ability to handle increasing traffic loads and scale horizontally to accommodate growing web application demands (including occasional spikes)	
	Dynamic scaling based on traffic patterns	
	Protection against common web attacks such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and remote file inclusion (RFI)	
	Support for OWASP (Open Web Application Security Project) top 10	
	Integration with threat intelligence feeds to identify and block known malicious IPs, domains, and URLs	
	Ability to identify and mitigate automated attacks by bots and other attack tools	
	Ability to perform protocol validation, data validation, and content inspection to prevent attacks	
	Behavioral and automatic protection against L7 DDoS attacks by analyzing traffic behavior using machine learning and data analyses	
	Support of X-Forwarded-For header insertion	
	Support for SSL/TLS termination and inspection to detect and prevent encrypted attacks	
	Minimal impact on the performance of web applications	
	Ability to handle high volumes of HTTP/HTTPS traffic efficiently	
	Low latency in processing requests and responses	
	Built-in redundancy and failover mechanisms to ensure high availability	
	Comprehensive logging capabilities including request/response logging, security events, and policy violations	
	The ability to capture and log web requests and responses, including post data	
	Real-time monitoring and alerting mechanisms for security incidents and breaches	
	Customizable dashboards and reports for various audience (technical, executive, operational)	
	Compliance with major industry standards such as PCI DSS, HIPAA, GDPR, etc.	
	Ability to generate compliance reports and assist in meeting regulatory requirements	
	Integration with security information and event management (SIEM) systems for centralized logging and analysis	
Technical Network Load Balancer (NLB)	Support various deployment options, including on-premise, cloud-based or hybrid deployment models	
	Compatibility with major cloud platforms such as Azure, AWS and Google Cloud Platform	
	Ability to handle high volumes of traffic and distribute it evenly across backend servers	
	Compatibility with a wide range of application protocols including HTTP(S), TCP, UDP, FTP, etc.	
	Support for integration with common application servers, web servers, and database servers	
	Support for horizontal scaling	
	Support for backend servers that are not exposed publicly via IPSec/VPN connectivity to the on-premise environment	

Area	Requirement	Covered?
	Support for various load balancing algorithms such as Round Robin, Least Connections, Weighted Round Robin, Least Response Time and etc	
	Customizable algorithm selection based on specific application requirements	
	Mechanisms for monitoring the health and availability of backend servers	
	Support for configurable health checks to verify server status based on protocols like HTTP, TCP, ICMP, etc.	
	Automatic detection and removal of failed or degraded servers from the pool	
	Ability to prioritize traffic based on criteria such as URL path, source IP, session persistence, etc.	
	Support of X-Forwarded-For header insertion	
	Support for content-based routing and traffic redirection based on specific application requirements	
	SSL/TLS termination and offloading capabilities	
	Built-in redundancy and failover mechanisms to ensure continuous availability	
	Support for active-passive and active-active clustering configurations	
	Seamless failover without disruption to ongoing sessions or transactions	
	Protection against common network attacks such as DDoS (Distributed Denial of Service), SYN flood, and DNS reflection attacks	
	Support for IP whitelisting/blacklisting and access control lists (ACLs) to restrict certain traffic	
	Intuitive and centralized management interface for configuring and monitoring load balancing policies	
	Real-time analytics and reporting capabilities to track traffic patterns, server health, and performance metrics	
	Customizable dashboards and reports for various audience (technical, executive, operational)	
	Integration with security information and event management (SIEM) systems for centralized logging and analysis	
Technical Access Policy Gateway (APG)	Support for various authentication methods including username/password, multi-factor authentication (MFA), SAML, OAuth, LDAP, etc.	
	Granular access control policies based on user roles, groups, attributes, and contextual information	
	Integration with identity providers (IdPs) for centralized authentication and user provisioning	
	SSO support for classic authentication (Kerberos, header-based, etc.), credential caching, OAuth 2.0, SAML 2.0, and FIDO2 (U2F)	
	Seamless integration with popular SSO solutions such as Okta, Azure AD, Ping Identity, etc.	
	Credential caching and proxy for SSO	
	Ability to federate identities across multiple applications and services for simplified user access	
	Bridging modern authentication and authorization (SAML, OAuth/OIDC) and classic authentication and authorization methods	
	API protection and authorization	
	Secure authentication for REST APIs and integration of OpenAPI or “swagger” files to ensure appropriate authentication actions	

2.2 Optional Requirements

N/A

2.3 Technical Specifications

Describe in this section the architecture of the solution, the technology stack, and in the case of hosting in UPU premises give the minimum technical requirements for hosting the solution.

3. Conditions of Response and Rules Governing the Submission of RFI Responses

3.1 Process overview

This RFI may, at the sole discretion of the UPU, be followed by Requests for Proposal relating to a Web Application Firewall (WAF), Network Load Balancer (NLB) and Access Policy Gateway (APG) solution/service.

The submission of a RFI Response may lead to additional clarifications to be requested from the Responder.

The UPU may seek for additional clarifications, demos or Proof of Concepts from the Responder.

3.2 Contact details for inquiries related to this RFI

Respondents shall send their respective RFI responses and related enquires by **19 April 2024** to the following contact person:

Secretary of the Tenders and Procurements Committee
Universal Postal Union
International Bureau
Weltpoststrasse 4
3015 BERNE
SWITZERLAND

E-mail: caa@upu.int

Any other communication (including unsolicited submissions or promotional and advertising activities) between Respondents and the staff of the International Bureau of the UPU concerning this RFI process shall not be allowed except with the prior written consent of the contact person specified above. Any such unauthorized communication with the UPU may lead to disqualification of a Respondent from further participation in the WAF/NLB/APG project.

As the case may be, Respondents may be individually contacted by the UPU to answer specific questions and to discuss materials/technology submitted. In addition, they may be invited to give a presentation to the UPU at its headquarters located in Berne, Switzerland.

PLACE FOR LODGEMENT: All RFI Responses, on an exceptional basis, be submitted to the UPU by e-mail (electronic format) **ONLY** at caa@upu.int with "**WAF/NLB/APG Project**" as the subject line, and in conformity with the format and conditions of the RFI Response as detailed below.

ISSUE DATE: 5 April 2024

CLOSING TIME AND DATE: 19 April 2024 at 17.00 CEST.

The UPU shall not take into consideration any responses received after this date and time.

Furthermore, it shall not accept any responses sent to any e-mail address other than that specified above or sent by any other means. There shall be no charge to the UPU for the preparation and submission of responses to this RFI.

3.3 Contents and documents contained in the RFI Response

The RFI Response shall be submitted electronically via email in the English language only, in Word (.doc) or PDF formats, and be structured in the following manner:

- A cover letter including a brief summary of the RFI Response, including a clear indication of the specific areas being approached in the RFI Response, as well as a detailed list and description of all supporting documentation included in the RFI Response;
- The main RFI Response, covering any or all of the areas of information requested by this RFI.

Respondents are requested to provide information on any past experiences and references in the areas covered by the "Web Application Firewall (WAF), Network Load Balancer (NLB) and Access Policy Gateway (APG)" solution; this should include if possible the reference information of the customer.

Any RFI Response received by the UPU shall be treated as a public document and be shared with UPU member countries and their Designated Operators. In case the Respondent sends any proprietary or copyrighted material as part of its RFI Response to the UPU (indicated as such), the Respondent acknowledges and agrees that the UPU shall be granted a non-exclusive, unrestricted, gratuitous and worldwide license for use of any such material by the UPU for the purposes of this RFI or other related UPU procurement processes, including without limitation the right to use, publish, reproduce, distribute and incorporate the contents of any RFI Response in future UPU documents or procurement processes related to the "Web Application Firewall (WAF), Network Load Balancer (NLB) and Access Policy Gateway (APG)" project. The Respondent shall also specify the conditions under which any proprietary or copyrighted material contained and duly specified in its RFI Response may be used for any other purposes by the UPU.

3.4 Costs and Preparation of the RFI response

Respondents are required to provide the pricing model and fees for:

- Using the solution in UPU premises;
- Accessing and using the solution in the cloud (SaaS for example);
- Identification of additional costs for integration (deployment phase).

All pricing information should be provided **exclusively in Swiss Francs (CHF)**.

The UPU shall neither be responsible for, nor pay for, any expense or loss which may be incurred by Respondents in the preparation and submission of their RFI Response. Respondents shall be responsible for fully informing themselves in relation to all matters arising from this RFI.

3.5 Acceptance Conditions

The UPU shall not be bound to accept any RFI Response nor consider it for future UPU procurement processes.

3.6 Tentative Follow-up Schedule

Conclusion of review of RFI Responses	**26 April 2024**
Follow-up with selected Responders (as the case may be)	**May-July 2024**

Note: The UPU reserves the right to change any date in this RFI at its absolute discretion.