CONVOCATORIA

PROYECTO "WAF"

Implementación de Web Application Firewall (WAF) para el Ámbito Universitario

La **ARIU** (Asociación de Redes de Interconexión Universitaria) invita al personal de las áreas de Tecnologías de la Información (TI) de las Universidades Nacionales a presentar propuestas para el desarrollo y ejecución del proyecto **"WAF"**. Este proyecto busca diseñar e implementar una solución de Web Application Firewall utilizando herramientas de código abierto, capaz de proteger el conjunto de aplicaciones web típicas del ecosistema universitario argentino y que sirva como implementación de referencia reutilizable por otras instituciones.

1. Objetivo del Proyecto

Diseñar e implementar una solución WAF de código abierto que opere como proxy inverso con terminación TLS, protegiendo simultáneamente múltiples aplicaciones web universitarias con perfiles de tráfico heterogéneos. La solución debe ser desplegable en producción y estar acompañada de una metodología documentada de configuración y ajuste de reglas que permita a cualquier universidad adoptarla independientemente del estado de despliegue de sus propias aplicaciones.

La arquitectura, las herramientas y la estrategia de configuración forman parte de la solución a presentar y serán evaluadas por el comité técnico. Los equipos deberán justificar técnicamente sus decisiones de diseño.

Los lineamientos del proyecto para la formulación de la propuesta se encuentran en el Anexo 1.

1.1 Entregables

Se espera que el equipo entregue una solución completa, lista para su despliegue en producción, compuesta por:

Despliegue del servidor:

1. Contenedor Docker con la implementación completa.
2. VM para Proxmox con la implementación completa.

3. Instalación mediante scripts parametrizados sobre GNU/Linux (al menos Debian y Ubuntu, última versión estable).

Configuración por perfil de aplicación:

4. Configuración WAF funcional y probada para cada uno de los perfiles de aplicación definidos en el Anexo 1, con las exclusiones documentadas y justificadas.
5. Plantillas de configuración reutilizables por perfil, adaptables a distintas instancias de las mismas aplicaciones.

Documentación:

6. Metodología de tuning: guía general para configurar y ajustar el WAF ante nuevas aplicaciones no contempladas en el proyecto, incluyendo el proceso de identificación y corrección de falsos positivos.
7. Informe técnico con análisis de herramientas evaluadas, justificación de decisiones de diseño, resultados de las pruebas de seguridad y análisis de falsos positivos por perfil.
8. Repositorio con guía paso a paso para el despliegue y la administración del sistema completo.

2. Composición de los Equipos

- Equipos **de un mínimo de 2 y máximo de 5 personas**.
- Los integrantes pueden pertenecer a la misma Universidad Nacional o a distintas instituciones.

3. Financiamiento e Infraestructura

Financiamiento: Para el desarrollo de la propuesta elegida se destinarán $30.000.000 (treinta millones de pesos). Este monto se dividirá en 4 fases (25%) de revisión de avance del plazo total del proyecto.

Cumplida cada revisión de las 4 fases, se realizarán los desembolsos de manera proporcional a cada miembro del equipo de trabajo.

Infraestructura: Toda la infraestructura tecnológica necesaria para el desarrollo y despliegue del proyecto será soportada y provista por la ARIU, según se acuerde con el equipo y en función de las imputaciones previstas.

Soporte y mantenimiento del producto: Una vez finalizada la etapa de desarrollo y entrega del proyecto, la ARIU podrá, si lo considera necesario, solicitar la contratación de un servicio de

soporte y mantenimiento evolutivo y/o correctivo. Dicho servicio podrá comprender, entre otras actividades, la actualización de imágenes Docker, máquinas virtuales y scripts ante nuevas versiones del sistema operativo base o de las dependencias del sistema; la actualización del conjunto de reglas WAF conforme evolucionen los estándares de referencia adoptados; la verificación de compatibilidad y adecuación de las configuraciones por perfil frente a nuevas versiones de las aplicaciones contempladas en el proyecto (SIU, Moodle y DSpace); y la elaboración de guías de migración que faciliten la actualización de las instalaciones existentes.

La eventual contratación de este servicio no forma parte del alcance obligatorio del presente proceso y quedará sujeta a la evaluación técnica y presupuestaria que realice ARIU, así como a la disponibilidad de recursos y a los términos y condiciones que oportunamente acuerden las partes.

4. Criterios de Evaluación

Las propuestas serán evaluadas por un comité técnico bajo los siguientes puntajes:

1) Por cada uno de los miembros:

- **Antecedentes Laborales Relacionados (15%):** Experiencia comprobable en administración de servidores web, seguridad informática y gestión de infraestructura en el ámbito universitario. Se valorará especialmente la experiencia con herramientas WAF, análisis de tráfico HTTP/S y administración de servidores en entornos GNU/Linux, para no menos de un integrante del equipo.

- **Antecedentes Académicos (15%):** Formación de pregrado, grado o posgrado, certificaciones técnicas y participación en investigaciones relacionadas con ciberseguridad, seguridad en aplicaciones web o infraestructura de redes, a cumplir por no menos de uno de los integrantes del equipo.

2) Por grupo de trabajo:

- **Desarrollo de la Propuesta (40%):** Calidad y coherencia del plan de trabajo, solidez en la justificación técnica de las herramientas y arquitectura elegidas, tratamiento de los distintos perfiles de aplicación y viabilidad de los plazos propuestos para el prototipo y el producto final.

- **Entrevista (30%):** Se realizará una entrevista al grupo que presente cada propuesta con el fin de evaluar la factibilidad del proyecto presentado.

5. Requisitos de Presentación

Los interesados deberán entregar:

1. **Plan de Trabajo y Cronograma:** Indicando plazos para el **prototipo** y el **producto final**, tomando en cuenta las 4 fases de revisión.

2. **Aval Institucional:** Firmado por el/la/los **Rectores/Rectoras** de las universidades de origen de cada integrante.

3. **Currículum Vitae:** De cada integrante para la evaluación de antecedentes.

4. Al momento de realizar el desembolso, cumplida y aprobada la revisión de la primera fase, cada integrante del equipo de trabajo deberá presentar la constancia de inscripción en el monotributo y deberá facturar el monto percibido a la ARIU. El mismo mecanismo se utilizará para las 3 fases restantes.

6. Propiedad Intelectual

Todo el desarrollo deberá realizarse bajo **licencias libres** que permitan la reutilización y auditoría por parte de otras Universidades Nacionales. El equipo final deberá entregar un informe detallado y un repositorio con la guía paso a paso para el despliegue de la solución.

7. Cronograma y Fechas Clave

- **Periodo de Presentación:** Desde el **13 de julio** hasta el **20 de agosto**.

- **Plazos de la Propuesta:** El equipo deberá indicar en su plan de trabajo el tiempo estimado para la entrega de los siguientes entregables:

    - Un **prototipo** funcional con al menos un perfil de aplicación configurado.
    - El **producto final** con los cuatro perfiles de aplicación configurados, incluyendo documentación técnica y repositorio.
    - El **informe final** con las conclusiones solicitadas.

- El **plazo máximo** de financiamiento del proyecto será de 12 meses.

8. Entrega y Recepción de Propuestas

- **Medio de envío:** Las propuestas deben enviarse por correo electrónico a: **proyectos@riu.edu.ar**.

- **Modalidad:** Para facilitar la gestión, **solo un miembro del equipo** deberá enviar la documentación requerida de todos los integrantes y la propuesta técnica.

Los resultados de la convocatoria serán publicados en la página web de ARIU.

ANEXO 1

Proyecto de Implementación de Web Application Firewall (WAF) con Código Abierto

Objetivo General

El objetivo de este proyecto es diseñar e implementar, utilizando exclusivamente herramientas de código abierto, una solución WAF que opere como proxy inverso con terminación TLS y proteja simultáneamente múltiples aplicaciones web universitarias. La solución debe ser desplegable en producción y estar acompañada de una metodología de configuración y ajuste de reglas que permita a cualquier institución adoptarla independientemente del estado de despliegue de sus propias aplicaciones.

La arquitectura, las herramientas y la estrategia de configuración no están prescritas. Su selección y justificación forman parte del trabajo a desarrollar y serán evaluadas como parte de la propuesta.

Dirigido a

Personal de las áreas de Tecnologías de la Información (TI) de las Universidades Nacionales.

I. Contexto y Alcance

Las aplicaciones web universitarias son vectores frecuentes de ataque: portales de autogestión académica, aulas virtuales y repositorios institucionales exponen interfaces públicas que deben resistir inyecciones SQL, cross-site scripting, inclusión de archivos y otras amenazas del OWASP Top 10. Un WAF operando como proxy inverso con terminación TLS permite centralizar esta protección: intercepta todo el tráfico HTTPS entrante, lo inspecciona en capa de aplicación antes de reenviarlo al backend, y gestiona los certificados TLS de los dominios protegidos. Las aplicaciones del backend reciben tráfico HTTP desde la red interna, sin necesidad de ser modificadas.

El desafío principal de un WAF en producción no es detectar ataques evidentes, sino **configurar reglas que protejan sin interrumpir el funcionamiento legítimo de cada aplicación**. Aplicaciones distintas generan perfiles de tráfico distintos: lo que es tráfico normal en un editor de contenido enriquecido puede parecer un ataque XSS para un conjunto de reglas genéricas. Por eso, el entregable central de este proyecto no es solo una instalación funcional, sino una **metodología de tuning documentada** que otras universidades puedan aplicar a sus propios entornos.

II. Arquitectura y Requisitos de Seguridad

II.1. Modelo de despliegue

Los posibles modelos de despliegue son:

Modo standalone: El WAF opera como proxy inverso con terminación TLS. En este caso:

- El WAF recibe las conexiones HTTPS de los usuarios y termina la sesión TLS.
- Inspecciona el tráfico HTTP en claro en la capa de aplicación.
- Reenvía las solicitudes al backend correspondiente, opcionalmente con re-cifrado si la red interna lo requiere.
- Gestiona los certificados TLS de los dominios protegidos, con soporte para certificados emitidos por Let's Encrypt u otras autoridades de certificación.

Modo HA (alta disponibilidad): Un balanceador de carga externo opera como endpoint TLS y distribuye el tráfico entre múltiples instancias WAF. En este caso:

- El balanceador termina la sesión TLS, lo que le permite operar en capa de aplicación (L7) y tomar decisiones de enrutamiento basadas en contenido HTTP, gestionar sesiones persistentes y realizar health checks sobre las instancias WAF.
- El balanceador reenvía el tráfico en claro (o re-cifrado internamente) a las instancias WAF.
- Cada instancia WAF inspecciona el tráfico de forma independiente.
- La propuesta debe contemplar la gestión del estado de sesión entre instancias WAF (por ejemplo, mediante sesiones persistentes en el balanceador o un mecanismo de estado compartido) para garantizar la coherencia de la inspección.
- Los requisitos de protocolo TLS descritos en la sección II.2 se aplican al balanceador como punto de entrada del sistema.

La solución propuesta debe soportar el modo standalone, pero se considerará en la evaluación de la propuesta si ambos modos de despliegue son soportados.

La documentación deberá cubrir los modos de despliegue implementados y especificar los requisitos que debe cumplir el balanceador externo en el modo HA.

La solución debe soportar la protección simultánea de múltiples aplicaciones en distintos dominios o subdominios, con conjuntos de reglas configurables de forma independiente por aplicación.

II.2. Requisitos de protocolo TLS y HTTP

El punto de entrada del sistema expuesto a internet —el WAF en modo standalone, o el balanceador en modo HA— debe cumplir los siguientes requisitos de protocolo:

- **TLS 1.3 como versión mínima requerida.** TLS 1.2 debe estar deshabilitado por defecto; su habilitación como excepción para dispositivos legacy debe estar explícitamente documentada y justificada.
- **Soporte para intercambio de claves híbrido post-cuántico.** El sistema debe soportar grupos de intercambio de claves híbridos que combinen un algoritmo clásico (como X25519) con ML-KEM, según los esquemas que está estandarizando el IETF para TLS 1.3. Este requisito es alcanzable hoy con las bibliotecas TLS modernas y es consistente con el soporte que los navegadores actuales ya negocian con los servidores.
- **Soporte dual-stack IPv4/IPv6.** El WAF debe aceptar conexiones entrantes y establecer conexiones hacia los backends en ambas familias de direcciones. La solución no debe requerir IPv4 como condición para funcionar ni degradar el soporte IPv6 a un modo secundario.
- **HTTP/2 como versión mínima del protocolo de aplicación.**
- **Soporte para HTTP/3 (QUIC) como característica deseable.** Dado que el soporte HTTP/3 en herramientas WAF de código abierto se encuentra en distintos grados de madurez, no se exige como requisito obligatorio. La propuesta deberá indicar si el diseño lo soporta o contempla una hoja de ruta para incorporarlo, y este aspecto será valorado positivamente en la evaluación.

II.3. Reglas y estándares

El equipo deberá seleccionar y justificar el motor WAF y el conjunto de reglas a utilizar. El conjunto de reglas debe basarse en estándares reconocidos de la industria —como el OWASP Core Rule Set (CRS) u equivalentes— y debe cubrir al menos las vulnerabilidades del OWASP Top 10.

Los equipos deberán evaluar el estado de mantenimiento y la trayectoria de las herramientas candidatas, ya que el ecosistema de WAFs de código abierto ha experimentado cambios significativos de mantenimiento en los últimos años.

II.4. Gestión de falsos positivos

El ajuste de reglas para minimizar falsos positivos es un componente central del proyecto. La propuesta deberá describir la metodología que el equipo utilizará para:

- Identificar bloqueos de tráfico legítimo durante la fase de configuración.
- Construir exclusiones quirúrgicas que corrijan el falso positivo sin debilitar la protección general.
- Documentar cada exclusión con su justificación técnica, de modo que sea auditable y reutilizable.

III. Perfiles de Aplicación a Proteger

La solución debe estar configurada y probada para los siguientes cuatro perfiles de aplicación, que representan el ecosistema web típico de una universidad nacional argentina. Las instancias de prueba serán provistas o acordadas con ARIU durante el desarrollo del proyecto.

III.1. Aplicaciones SIU

Las aplicaciones del consorcio SIU (Guaraní, Pilagá, Mapuche, Diaguita, Huarpe y similares) son sistemas de gestión académica y administrativa con formularios estructurados y parámetros de valores predecibles y acotados. Este perfil admite una configuración de reglas relativamente estricta.

Características a contemplar en la configuración:

- Parámetros con tipos de dato definidos (fechas, identificadores numéricos, cadenas cortas).
- Autenticación centralizada y gestión de sesiones.
- Múltiples aplicaciones SIU con estructura similar pero distintas rutas y endpoints.
- La configuración para una aplicación SIU debe ser adaptable a las demás con cambios mínimos.

III.2. Aulas Virtuales (Moodle)

Moodle presenta el perfil de tráfico más complejo por la presencia de un editor de contenido enriquecido que permite a los usuarios enviar HTML y recursos embebidos de forma legítima. Este perfil requiere exclusiones cuidadosas para no romper la funcionalidad de edición.

Características a contemplar en la configuración:

- Editor de contenido que genera parámetros POST con HTML complejo.

- Carga de archivos de múltiples tipos (documentos, imágenes, videos, archivos comprimidos).
- API REST para interacciones dinámicas desde el navegador.
- Distinción entre la interfaz de los estudiantes (más restringida) y la interfaz de los docentes y administradores (que requiere las exclusiones del editor).

III.3. Repositorio Institucional (DSpace)

DSpace expone una interfaz de búsqueda con operadores complejos y una API de interoperabilidad, además de permitir la carga de archivos académicos en formatos variados.

Características a contemplar en la configuración:

- Consultas de búsqueda con operadores booleanos y sintaxis que puede asemejarse a inyecciones.
- Carga de archivos en formatos académicos (PDF, XML, Dublin Core, MARC).
- API OAI-PMH para cosecha de metadatos por sistemas externos.
- Interfaz de administración para la gestión de colecciones.

III.4. Sitio Web Institucional

El sitio web institucional tiene el perfil de tráfico más simple: mayormente contenido estático o semi-estático con formularios de contacto básicos. Si incluye un área de administración con CMS, esa sección requiere un tratamiento similar al del editor de Moodle.

Características a contemplar en la configuración:

- Contenido estático (HTML, CSS, JS, imágenes) sin procesamiento de parámetros complejos.
- Formularios de contacto con campos de texto libre acotado.
- Área de administración del CMS (si aplica) con editor de contenido.
- Protección especial contra ataques de fuerza bruta sobre el panel de administración.

IV. Requisitos de Pruebas de Seguridad

Las pruebas deben demostrar tanto la efectividad del WAF para detectar ataques como su capacidad para no interrumpir el tráfico legítimo de cada perfil.

IV.1. Pruebas de detección de ataques

Se deberán simular ataques basados en el OWASP Top 10 contra cada perfil de aplicación, incluyendo al menos:

- Inyección SQL (SQLi)
- Cross-Site Scripting (XSS)
- Inclusión de archivos (Local File Inclusion — LFI)
- Traversal de directorios
- Fuerza bruta sobre formularios de autenticación

IV.2. Pruebas de evasión

Se deberán probar técnicas de evasión orientadas a sortear las reglas WAF, incluyendo al menos:

- Codificación de payloads (URL encoding, doble encoding, Unicode encoding).
- Fragmentación y ofuscación de ataques.
- Variaciones de capitalización y espaciado.

El informe deberá documentar qué técnicas de evasión fueron detectadas y cuáles, si las hubiera, lograron evadir la detección, con el análisis correspondiente.

IV.3. Pruebas de tráfico legítimo

Para cada perfil de aplicación se deberán documentar los escenarios de tráfico legítimo que inicialmente generaron falsos positivos y las exclusiones implementadas para resolverlos. Esta sección es tan importante como las pruebas de ataque: una configuración que bloquea ataques pero interrumpe el uso normal de la aplicación no es apta para producción.

IV.4. Impacto en rendimiento

Se deberá medir el impacto en latencia introducido por el WAF con y sin inspección activa, bajo carga representativa, para al menos uno de los perfiles de aplicación.

V. Requisitos de Despliegue

La solución del lado servidor debe poder desplegarse en las siguientes plataformas a partir de los artefactos entregados:

- Contenedor Docker.
- Máquina virtual para Proxmox.
- Instalación directa mediante scripts parametrizados sobre GNU/Linux (Debian y Ubuntu, última versión estable).

La propuesta deberá contemplar además:

- **Gestión de certificados TLS:** El sistema debe incluir un mecanismo para la emisión y renovación automática de certificados para los dominios protegidos.
- **Configuración por perfil:** La arquitectura debe permitir aplicar conjuntos de reglas distintos por dominio o aplicación, sin que los cambios en un perfil afecten a los demás.
- **Monitoreo y registro:** El sistema debe generar registros de eventos de seguridad (ataques detectados, bloqueos) y de acceso, con indicación de la regla que motivó cada bloqueo.
- **Actualización de reglas:** El diseño debe contemplar un mecanismo para actualizar el conjunto de reglas base sin interrumpir el servicio.

VI. Plan de Implementación

El proyecto se dividirá en cuatro fases, alineadas con los hitos de revisión y desembolso:

1. **Fase 1 — Diseño:** Análisis y selección de herramientas (motor WAF, conjunto de reglas, servidor web proxy). Diseño de la arquitectura de despliegue y de la estrategia de configuración por perfil. Entrega: documento de diseño con todas las decisiones técnicas justificadas.

2. **Fase 2 — Implementación base y primer perfil:** Despliegue funcional del WAF con terminación TLS y configuración completa para el perfil SIU, incluyendo pruebas de ataque, pruebas de tráfico legítimo y documentación de exclusiones. Entrega: prototipo funcional con el primer perfil configurado y probado.

3. **Fase 3 — Perfiles restantes:** Configuración y pruebas para los perfiles Moodle, DSpace y sitio web institucional. Entrega: solución completa con los cuatro perfiles configurados y probados.

4. **Fase 4 — Metodología, hardening y entrega final:** Redacción de la metodología de tuning generalizada, revisión de seguridad de la configuración, corrección de vulnerabilidades detectadas y producción del repositorio de despliegue. Entrega: producto final listo para producción con documentación completa.

VII. Documentación y Recursos

El equipo deberá producir los siguientes entregables de documentación:

- **Informe técnico:** Descripción de las herramientas evaluadas y la justificación de la selección, arquitectura implementada, resultados de las pruebas de seguridad y evasión por perfil, análisis de falsos positivos y exclusiones aplicadas, y recomendaciones para la adopción institucional.

- **Metodología de tuning:** Guía general, independiente de las aplicaciones específicas del proyecto, que documente el proceso para configurar el WAF ante una nueva aplicación: cómo habilitar el modo detección, cómo analizar los logs para identificar falsos positivos, cómo construir exclusiones y cómo validar que la protección se mantiene. Esta guía es el entregable de mayor valor para la reutilización institucional.

- **Repositorio de despliegue:** Guía paso a paso para la instalación y configuración del sistema, incluyendo scripts, archivos de configuración comentados por perfil y procedimientos de mantenimiento (actualización de reglas, renovación de certificados, rotación de logs).

- **Revisión final con ARIU:** Para la aprobación del hito final, el equipo realizará una demostración del sistema ante el equipo técnico de ARIU, que incluirá la detección de al menos un ataque y la verificación de que el tráfico legítimo de al menos dos perfiles de aplicación no es bloqueado.

Perfil del Postulante

El equipo en su conjunto deberá acreditar experiencia en las siguientes áreas. No se requiere que todos los integrantes cubran la totalidad de los puntos, pero sí que el equipo los cubra colectivamente:

- Administración de servidores web en entornos GNU/Linux (Nginx, Apache u otros).
- Conocimiento de los mecanismos de ataque cubiertos por el OWASP Top 10 y experiencia en herramientas de pruebas de penetración web.
- Familiaridad con WAFs de código abierto y el OWASP Core Rule Set o equivalentes.
- Experiencia en configuración y operación de proxies inversos con terminación TLS.
- Manejo de entornos de contenedores y virtualización (Docker, Proxmox).
- Conocimiento de las aplicaciones del ecosistema universitario argentino (SIU, Moodle, DSpace) o capacidad demostrable para analizar su comportamiento HTTP.
- Capacidad para producir documentación técnica clara, orientada a la adopción por parte de administradores de otras instituciones.