Comarb
COMISIÓN ARBITRAL DEL CONVENIO MULTILATERAL

CONCURSO DE PRECIOS N° 4/2021

PLIEGO DE BASES Y CONDICIONES GENERALES

1- Normativa aplicable. Para la presente contratación, rigen las disposiciones contenidas en el Pliego de Condiciones Generales, y en el REGLAMENTO PARA LA CONTRATACIÓN DE BIENES, OBRAS Y SERVICIOS aprobado por la COMISIÓN ARBITRAL DEL CONVENIO MULTILATERAL 18.08.77, vigente al momento de inicio del procedimiento de contratación.

2- Objeto. La presente contratación tiene por objeto la adquisición de una solución de Firewall de Aplicaciones Web virtual marca Fortinet, según el Anexo "A" Especificaciones Técnicas, que se adjunta al presente Pliego.

3- Lugares y Plazos. Tanto la recepción de las ofertas como el acto de apertura de los sobres se realizará en la sede de la Comisión Arbitral, departamento de Recursos Humanos y Materiales, sito en Esmeralda 672 piso 3°, Ciudad Autónoma de Buenos Aires.

La recepción de las ofertas será entre las 10:00 y las 11:00 hs del día 8 de Junio de 2021.

La apertura de las ofertas se realizará a las 11:45 hs del día 8 de Junio de 2021.

4- Requisitos formales para la presentación de las ofertas. Las ofertas deberán cumplir los siguientes requisitos formales:

a. Redactadas en idioma nacional en procesador de texto y/o a máquina, en formularios con membrete de la persona o firma comercial.

b. Firmadas en todas sus hojas por el oferente, representante legal o apoderado debidamente acreditado.

c. Enmiendas y raspaduras en partes esenciales, debidamente salvadas.

d. Todas las fojas (incluida la documentación y folletería que se acompañe) debidamente compaginadas, numeradas y abrochadas o encarpetadas.

e. Por duplicado y presentadas en sobre o paquete cerrado con indicación de número de contratación, fecha y hora de apertura.

f. Se deberá adjuntar toda la documentación presentada en un PEN DRIVE.

g. Tanto las ofertas como los presupuestos, facturas y remitos, deberán cumplir con las normas impositivas y previsionales vigentes.

Las infracciones, errores u omisiones no esenciales no invalidarán la oferta, sin perjuicio de las sanciones que pudiesen corresponder al infractor.

5- Información y documentación que deberá presentarse junto con la Oferta. Se estará a lo dispuesto por el art. 19 del Reglamento para la contratación de bienes, obras y servicios de la Comisión Arbitral. A tal efecto, en el momento de presentar la oferta, se deberá proporcionar la información que en cada caso se indica. En todos los casos deberá acompañarse la documentación respaldatoria y las copias de escrituras, actas, poderes y similares deberán estar autenticadas por Escribano Público:

a- Personas humanas y apoderados:

1- Nombre completo, nacionalidad, profesión, domicilio real y constituido, tipo y número de documento de identidad.

2- Clave Única de Identificación Tributaria (C.U.I.T) y condición frente al Impuesto al Valor Agregado (IVA) y Regímenes de Retención vigentes.

b- Personas jurídicas:

1- Razón Social, domicilio legal y constituido, lugar y fecha de constitución y datos de inscripción registral.

2- Clave Única de Identificación Tributaria (C.U.I.T) y condición frente al Impuesto al Valor Agregado (IVA) y Regímenes de Retención vigentes

c- En todos los casos, con la oferta deberá acompañarse:

1- Copia autenticada del poder, en caso de que quien suscriba la oferta y el resto o parte de la documentación no sea la persona humana o el representante legal respectivo.

2- Declaración Jurada de que ni el oferente, ni los integrantes de los órganos de administración y fiscalización en su caso, se encuentran incursos en ninguna de las causales de inhabilidad para contratar con la Comisión Arbitral.

3- Certificado de inscripción en AFIP, donde se acredite la actividad que desarrolla y cuando corresponda, certificación de condición como “Agente de Retención” y/o certificado de exclusión de retención (Impuesto al valor Agregado, Impuesto a las Ganancias, Sistema Único de Seguridad Social -SUSS-).

4- Constancia de inscripción en el Impuesto a los Ingresos Brutos.

6- Contenido de la oferta. La presentación de las ofertas deberán contemplar la totalidad de los puntos solicitados bastando la falta de alguno de estos para que se desestime la oferta general. La presentación de la oferta significa de parte del oferente el pleno conocimiento del Reglamento de Contrataciones de Bienes, Obras y Servicios de la Comisión Arbitral y la aceptación de las cláusulas que rigen la contratación.

La oferta especificará por cada ítem en relación a la unidad solicitada o su equivalente: precio unitario, precio total; en dólares estadounidenses, con I.V.A. Incluido. El total general de la propuesta será expresado en letras y números con I.V.A. Incluido.

7- Plazo de mantenimiento de la Oferta. El plazo de mantenimiento de la oferta será de siete (7) días, en un todo de acuerdo a lo reglado por el art. 23 del Reglamento para la Contratación de Bienes, Obras y Servicios de la Comisión Arbitral.

8- Efectos de la presentación de la oferta. La presentación de la oferta, importa de parte del oferente el pleno conocimiento de toda la normativa que rige el llamado a contratación, la evaluación de todas las circunstancias, la previsión de sus consecuencias y la aceptación en su totalidad de las bases y condiciones estipuladas, sin que pueda alegar en adelante el oferente su desconocimiento.

9- Análisis de las Ofertas. Las ofertas serán evaluadas por un Comité de Preadjudicación, cuyos integrantes serán designados por el contratante, quienes emitirán el informe de evaluación de las ofertas.

10- Adjudicación. Se adjudica el Concurso de Precios al oferente cuya propuesta se ajuste a lo establecido en el Pliego de Bases y Condiciones Generales, sea satisfactoria la documentación presentada y su oferta económica haya sido evaluada como la más conveniente. Dicha adjudicación se efectuará por monto global.

11- Plazo de entrega. El plazo de entrega será a coordinar con el adjudicatario una vez recibida la orden de compra.

12- Pagos. El pago se efectuará con transferencia bancaria de Banco Nación Argentina Sucursal Plaza de Mayo, en pesos argentinos, una vez recibidos la totalidad de los ítems y la factura correspondiente. Se tomará el tipo de cambio oficial del Banco Nación Argentina al día anterior a la fecha de pago de la factura.

13- Penalidades y Sanciones. Será de aplicación lo dispuesto por el Capítulo XII del Reglamento para la Contratación de Bienes, Obras y Servicios de la Comisión Arbitral.

14- Impuesto al Valor Agregado. A los efectos de la aplicación del Impuesto al Valor Agregado, la Comisión Arbitral reviste el carácter de consumidor final.

15- Constitución de domicilio. A todos los efectos legales, el oferente deberá constituir domicilio legal en la Ciudad Autónoma de Buenos Aires.

16- Garantía. 1 (un) año.

17- Consultas. A Fernanda González mail fgonzalez@ca.gob.ar

Comarb
COMISIÓN ARBITRAL DEL CONVENIO MULTILATERAL

Anexo “A” Especificaciones Técnicas

1- Firewall de Aplicaciones Web- Modalidad virtual - Cantidad: 1

1. Características Equipo tipo 1 (1 unidad).

   1.1.Throughput mínimo para HTTP de 500 Mbps

2. Requisitos Mínimos de Funcionalidad.

   Funcionalidades generales

   2.1. La solución debe de ser del tipo appliance físico/virtual.

   2.2. Cada equipo (appliance físico o virtual) debe de tener un firmware específico destinado a la finalidad de Firewall de Aplicación Web (WAF –Web Application Firewall), así como las licencias necesarias para su funcionamiento y protección de servidores y aplicaciones Web.

   2.3. La solución debe de soportar virtualización en hypervisor VMware

   2.4. La solución debe de soportar virtualización en hypervisor Microsoft Hyper-V

   2.5. La solución debe de soportar virtualización en hypervisor Citrix XenServer

   2.6. La solución debe de soportar virtualización en hypervisor Open Source Xen

   2.7. La solución debe de soportar virtualización en hypervisor KVM

   2.8. La solución debe de soportar virtualización en plataformas Docker containers

   2.9. La solución debe de soportar virtualización en Amazon AWS

   2.10. La solución debe de soportar virtualización en Microsoft Azure

   2.11. La solución debe de soportar virtualización en Google Cloud

   2.12. La solución debe de soportar virtualización en Oracle Cloud

   Funcionalidades de red

   2.13. La solución debe permitir implementación en modo Proxy Transparente, Proxy Reverso, Transparente en Línea y Sniffer

   2.14. La solución debe de ser capaz de ser implementada con protocolo WCCP

   2.15. Soportar VLANs del estándar IEEE 802.1q.

   2.16. Debe de implementar el protocolo Link Aggregation Control Protocol (LACP) - IEEE 802.3ad

   2.17. Soportar direccionamiento IPv4 y IPv6 en las interfaces físicas y virtuales (VLANs).

   2.18. La solución debe de soportar y brindar cluster de alta disponibilidad entre dos equipos en modo Activo-Pasivo y Activo-Activo, de forma que el tráfico siga siendo procesado en

caso de fallo del equipo principal para que quando o principal falhar o tráfego possa continuar sendo processado.

2.19. La solución debe de soportar la sincronización de configuración entre dos appliances del mismo tipo, con el objetivo de operar en modo activo-activo, con la distribución de tráfico siendo realizada por balanceador de tráfico externo o por la propia solución.

2.20. La solución debe de soportar enrutamiento por política (policy route)

Funcionalidades de Gestión

2.21. El firmware debe soportar interfaz gráfica web para la configuración de las funciones del sistema, utilizando navegadores disponibles gratuitamente y protocolo HTTPS, y también por CLI (interface de línea de comando), accediendo localmente al equipo por puerto de console, o remotamente via SSH.

2.22. Debe de soportar administración basada en interface web HTTP

2.23. Debe de soportar administración basada en interface de línea de comando vía Telnet

2.24 Tener la función de auto-completar comandos en la CLI

2.25. ener ayuda contextual en la CLI

2.26. La solución debe de tener un Dashboard con información sobre el sistema (información del cluster, hostname, número de série, modo de operación, tiempo en servicio, versión de firmware)

2.27. Debe de ser posible visualizar a través de la interfaz gráfica de gestión la información de licencia, firmas y contrato de soporte

2.28. La solución ofertada deberá de tener acceso a la línea de comando CLI directamente a través de la interfaz gráfica de gestión (GUI)

2.29. Debe de proveer, en la interfaz de gestión, las siguientes informaciones del sistema para cada equipo: consumo de CPU y estadísticas de conexión

2.30. Debe de ser posible visualizar en la interfaz de gestión la información de consumo de memória

2.31. Debe de incluir herramienta dentro de la interfaz gráfica de gestión (dashboard) que permite visualizar los últimos logs de ataques detectados/bloqueados

2.32. Debe proveer las siguientes informaciones en la interfaz gráfica de gestión: estadísticas de throughput HTTP en tiempo real, estadísticas de eventos de ataques detectados/bloqueados, estadísticas de requisición HTTP en tiempo real y los últimos logs de eventos del sistema

2.33. Tener en la interfaz gráfica estadísticas de conexión concurrente y por segundo, de políticas de seguridad del sistema

2.34. Tener un dashboard de visualización con información de las interfaces de red del sistema

2.35. La configuración de administración de la solución debe permitir la utilización de perfiles

2.36. Debe de ser posible ejecutar y recuperar backup por la interfaz Web (GUI)

2.37. Debe de tener la opción de criptografar el backup utilizando algorítmo AES 128-bit o superior

2.38. Debe de ser posible ejecutar y recuperar el backup utilizando FTP

2.39. Debe de ser posible ejecutar y recuperar el backup utilizando SFTP y TFTP

2.40. Debe ser posible probar una nueva versión de firmware en memória RAM, sin instalar en disco, antes de aplicarla

2.41. Debe ser posible instalar un firmware alternativo en disco y arrancarlo en caso de fallo del firmware principal

2.42. Debe soportar los protocolos de monitoreo SNMP v1, SNMP v2c e SNMP v3

2.43. Debe ser capaz de realizar notificación de eventos de seguridad a través de e-mail, traps SNMP y Syslog

2.44. La solución deberá de soportar almacenar logs localmente en disco y en servidor externo vía protocolo SYSLOG

2.45. Debe tener la capacidad de almacenar los logs en appliance remoto

2.46. La solución debe tener la capacidad de enviar alertas por email de los eventos basado en severidad y/o categorías

2.47. La solución debe tener datos analíticos conteniendo la localización geográfica de los clientes web

2.48. La solución debe tener datos analíticos, siendo posible visualizar el total de ataques y porcentaje de cada país de origen, el volumen total de tráfico en bytes y porcentaje de cada país de origen, y el total de accesos (hits) y porcentaje de cada país de origen

2.49. Debe tener la capacidad de generar reportes detallados basados en tráfico/acceso/actividades del usuario

2.50. Debe soportar RESTful API para gestión de la configuración

Funcionalidades de autenticación

2.51. Los usuarios deben de ser capaces de autenticarse a través del encabezado de autorización HTTP/HTTPS

2.52. Los usuarios deben de ser capaces de autenticarse a través de formularios HTML embebidos

2.53. La solución debe de ser capaz de autenticar los usuarios a través de certificados digitales personales

2.54. Debe tener base local para almacenamiento y autenticación de los usuários

2.55. La solución debe tener la capacidad de autenticar usuarios en bases externas remotas LDAP, RADIUS y SAML

2.56. La solución debe de ser capaz de autenticar los usuarios en base remota vía NTLM

2.57. La solución debe de ser capaz de crear grupos de usuários para configurar mecanismos de autenticación por grupos

2.58. Debe soportar CAPTCHA y Real Browser Enforcement (RBE)

2.59. Debe soportar autenticación de doble factor

Reglamentación y Certificaciones

2.60. La solución debe de soportar el modelo de seguridad positiva definido por OWASP y proteger contra el Top 10 de ataques a aplicaciones definido por OWASP

2.61. El equipo debe de tener certificación FCC Class A part 15

2.62. El equipo debe de tener certificación C-Tick

2.63. El equipo debe de tener certificación VCCI

2.64. El equipo debe de tener certificación CE

2.65. El equipo debe de tener certificación UL/cUL

2.66. El equipo debe de tener certificación CB

Funcionalidades de Web Application Firewall

2.67. Debe tener soporte nativo de HTTP/2

2.68. Debe soportar traducción de HTTP/2 a HTTP 1.1

2.69. Deberá soportar interoperabilidad con OpenAPI 3.0

2.70. Debe de ser capaz de identificar y bloquear ataques a través de una base de datos de firmas de virus y reputación IP, la cual se debe actualizar automáticamente y de manera periódica

2.71. La solución debe permitir eligir entre utilizar la base de datos completa o solamente la base de datos que contiene los últimos y más peligrosos vírus

2.72. Deberá tener algoritmos para detección de amenazas avanzadas basados en aprendizaje de máquina con Inteligencia Artificial (AI) para detectar anomalías y aprender si se trata de ataques o no

2.73. Deberá minimizar la ocurrencia de Falsos Positivos y falsos negativos utilizando Inteligencia Artificial

2.74. Tener mecanismo de aprendizaje automático capaz de identificar todos los

contenidos de la aplicación, incluyendo URLs, parámetros de URLs, campos de formularios y lo que se espera de cada campo

2.75. El perfil aprendido de forma automática debe de poder ser ajustado

2.76. Tener la capacidad de creación de firmas de ataques customizables

2.77. Tener la capacidad de protección contra ataques del tipo Adobe Flash binary (AMF) protocol

2.78. Tener la capacidad de protección contra ataques del tipo Botnet

2.79. Tener la capacidad de protección contra ataques del tipo Browser Exploit Against SSL/TLS (BEAST)

2.80. La solución debe tener funcionalidad de protección contra ataques como acceso por fuerza bruta

2.81. Debe soportar detección de ataques de Clickjacking

2.82. Debe soportar detección de ataques de cambios de cookie

2.83. Identificar y proteger contra ataques del tipo Credit Cart Theft

2.84. Identificar y proteger contra ataques del tipo Cross Site Request Forgery (CSRF)

2.85. La solución debe tener funcionalidad de protección contra ataques como cross site scripting (XSS)

2.86. Debe tener protección contra ataques de Denial of Service (DoS);

2.87. Tener la capacidad de protección contra ataques del tipo HTTP header overflow

2.88. Tener la capacidad de protección contra ataques del tipo Local File inclusion (FLI)

2.89. Tener la capacidad de protección contra ataques del tipo Man-in-the0middle (MITM)

2.90. Tener la capacidad de protección contra ataques del tipo Remote File Inclusion (RFI)

2.91. Tener la capacidad de protección contra ataques del tipo Server Information Leakage

2.92. Protección contra envíos de comandos SQL ocultos en las requisiciones enviadas a la base de datos (SQL Injection);

2.93. Tener la capacidad de protección contra ataques del tipo Malformed XML

2.94. Identificar y prevenir ataques del tipo Low-rate DoS

2.95. Prevención contra Slow POST attack

2.96. Proteger contra ataques Slowloris

2.97.Tener la capacidad de protección contra ataques del tipo SYN flood

2.98. Tener la capacidad de protección contra ataques del tipo Forms Tampering

2.99. La solución debe tener funcionalidad de protección contra ataques de manipulación de campos ocultos

2.101. Tener la capacidad de protección contra ataques del tipo Directory Traversal

2.102. Tener la capacidad de protección del tipo Access Rate Control

2.103. Identificar y proteger contra Zero Day Attacks

2.104. Tener la capacidad de configurar protección del tipo TCP SYN flood-style para prevención de DoS para cualquier política, a través de Syn Cookie y Half Open Threshold

2.105. Permitir configurar reglas de bloqueo a métodos HTTP no deseados

2.106. Permitir que se configuren reglas de límite de upload por tamaño del archivo

2.107. Debe permitir que el administrador bloquee el tráfico de entrada o salida en base a países, sin la necesidad de gestionar manualmente los rangos de dirección IP correspondientes a cada país

2.108. Debe soportar crear políticas de geo-localización, permitiendo que el tráfico de determinado país sea bloqueado

2.109. Permitir configurar listas negras de bloqueo y listas blancas de confianza, basadas en direción IP de origen

2.110. Permitir la liberación temporal o definitiva (white-list) de direcciones IP bloqueadas por tener originado ataques detectados por la solución

2.111. Debe permitir añadir, automáticamente o manualmente, en una lista de bloqueo, las direcciones IP de origen, según la base de IP Reputation

2.112. Tener la capacidad de conectarse a una base de datos en Internet para validar que las credenciales que usan los usuarios para acceder a algún sistema no sean credenciales robadas.

2.113. Tener la capacidad de prevención contra pérdida de información (DLP), bloqueando la pérdida de información del encabezado HTTP

2.114. Tener la funcionalidad de proteger el website contra acciones de defacement, con recuperación automática y rápida del website en caso de fallo

2.115. Tener la funcionalidad de antivirus integrada para inspección de tráfico y archivos, sin la necesidad de instalación de otro equipo

2.116. Tener la capacidad de investigar y analizar todo el tráfico HTTP para validar si cumple con el RFC del protocolo HTTP o si ha sufrido alguna alteración y debe ser bloqueado

2.117. Debe se der capaz de hacer aceleración de tráfico SSL basada en hardware

2.118. La solución debe de ser capaz de funcionar como terminador de sesión SSL para aceleración de tráfico

2.119. Para SSL/TLS offload soportar al menos SSL 3.0, TLS 1.0, 1.1 e 1.2

2.120. La solución debe tener la capacidad de almacenar certificados digitales de CA's

2.121. La solución debe de ser capaz de generar CSR para ser firmado por una CA

2.122. La solución debe de ser capaz de chequear los certificados válidos y que no fueron revocados por una lista CRL

2.123. La solución debe contener las firmas de robôs conocidos como link checkers, indexadores de web, search engines, spiders y web crawlers que puedan ser añadidos a los perfiles de control de acceso, así como resetear dichas conexiones

2.124. La solución debe de tener un sistema de bloque con base en la reputación de direcciones IP públicas conocidas. La lista de IPs con mala reputación debe de ser actualizada automáticamente.

2.125. La solución debe de ser capaz de limitar el total de conexiones permitidas hacia cada servidor real de un pool de servidores

2.126. La solución debe permitir la customización o reenvío de solicitaciones y respuestas HTTP en el HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body y HTTP Location

2.127. La solución debe permitir crear reglas definiendo el orden con que las páginas deben de ser accedidas para prevenir ataques como cross-site request forgery (CSRF).

2.128. La solución debe de tener la capacidad de definir restricción a determinados métodos HTTP

2.129. La solución debe tener la capacidad de proteger contra detección de campos ocultos

2.130. Permitir que se configuren firmas customizadas de ataques y DLP, a través de expresiones regulares

2.131. La solución debe permitir la integración con scanners de vulnerabilidades de terceros, tales como Acunetix, IBM AppScan, WhiteHat, etc, para proveer parches virtuales

2.132. Debe generar perfil de protección automáticamente a partir de reporte en formato XML generado por scanner de vulnerabilidade de terceros

2.133. Debe permitir programar la verificación de vulnerabilidades

2.134. La solución debe generar un reporte de análisis de vulnerabilidades en formato HTML

2.135. Soportar redirección y reescritura de requisiciones y respuestas HTTP

2.136. Permitir redirección de requisiciones HTTP para HTTPS

2.137. Permitir reescribir la línea URL del encabezado de una requisición HTTP

2.138. Permitir reescribir el campo HOST del encabezado de una requisición HTTP

2.139. Permitir reescribir el campo REFERER del encabezado de una requisición HTTP

2.140. Permitir redirigir requisiciones para otro website

2.141. Permitir enviar respuesta HTTP 403 Forbidden para requisiciones HTTP

2.142. Permitir reescribir el parámetro LOCATION en el encabezado HTTP de una respuesta de redirección HTTP de un servidor web

2.143. Permitir reescribir el cuerpo ("body") de una respuesta HTTP de un servidor web

2.144. Permitir añadir el campo X-Forwarded-For para identificación de la dirección IP real del cliente cuando en modo proxy reverso

2.145. La solución debe de soportar reglas para definir si las requisiciones HTTP serán aceptadas en función de la URL y origen de la petición y, si necesario, aplicar una tasa específica de velocidad (rate limit).

2.146. La solución debe de soportar combinación de control de acceso y autenticación utilizando mecanismos como HTML Form, Basic y soporte a SSO, métodos como LDAP y RADIUS para consultas y integración de los usuarios de la aplicación

2.147. Tener capacidad de caching para aceleración web

2.148. La solución debe de ser capaz de enviar archivos para solución de sandboxing del mismo fabricante, a través de una política de restricción de carga del archivo

2.149. Debe permitir al administrador crear nuevas firmas y/o cambiar las firmas pre existentes

Funcionalidades de Balanceo de carga

2.150. La solución debe incluir la funcionalidad de balanceo de carga entre servidores web

2.151. Debe soportar configurar puertos no estándar para aplicación web HTTP y HTTPS

2.152. Soportar balanceo / distribución de tráfico y enrutar el contenido hacia distintos servidores web

2.153. La solución debe permitir crear grupos de servidores (Server Farm / Pool) para distribuir las conexiones de los usuários

2.154. Soportar el algoritmo Round Robin para balanceo de carga entre servidores

2.155. Soportar el algoritmo Weighted Round Robin para balanceo de carga entre servidores

2.156. Soportar el algoritmo Least Connection para balanceo de carga entre servidores

2.157. La solución debe de soportar creación de servidores virtuales que definen la interfaz de red/bridge y dirección IP por donde el tráfico con destino al Server Pool es recibido

2.158. Los servidores virtuales deben de entregar el tráfico hacia un único servidor web y también incluir la opción de distribuir las sesiones/conexiones entre los servidores web del Server Pool

2.159. Debe de ser posible definir el número máximo de conexiones TCP simultáneas hacia un determinado servidor miembro del Server Pool

2.160. Permitir prueba de disponibilidad del servidor web a través del método TCP

2.161. Permitir prueba de disponibilidad del servidor web a través del método ICMP ECHO_REQUEST (ping)

2.162. Permitir prueba de disponibilidad del servidor web a través del método TCP Half Open

2.163. Permitir prueba de disponibilidad del servidor web a través del método TCP SSL

2.164. Permitir prueba de disponibilidad del servidor web a través del método HTTP

2.165. Permitir prueba de disponibilidad del servidor web a través del método HTTPS

2.166. En las pruebas de disponibilidad HTTP y HTTPS, permitir indicar la URL exacta a ser probada

2.167. En las pruebas de disponibilidad HTTP y HTTPS, permitir elegir entre los métodos HEAD, GET y POST

2.168. En las pruebas de disponibilidad HTTP y HTTPS, permitir elegir el nombre del campo HTTP "host" a ser probado

2.169. Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Host"

2.170. Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "URL"

2.171. Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Parâmetro HTTP"

2.172. Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Referer"

2.173. Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Dirección IP de Origen"

2.174. Soportar el ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Encabeçado".

2.175. Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Cookie"

2.176. Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Valor del campo del Certificado X509"

2.177. Implementar Cache de Contenido para HTTP, permitiendo que objetos sean almacenados y requisiciones HTTP sean contestadas directamente por la solución

2.178. La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por dirección IP de origenendereço IP de origen

2.179. La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por análisis de cualquier parámetro del header HTTP

2.180. La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por análisis de la URL accedida

2.181. La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por cookie – método cookie insert y cookie rewrite

2.182. La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por embedded cookie (cookie original seguido de porción aleatoria)

2.183. La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en Reescritura del Cookie

2.184. La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en Cookie Persistente

2.185. La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en ASP Session ID

2.186. La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en PHP Session ID

2.187. La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en JSP Session ID

2.188. La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por sesión SSL

PLIEGO DE BASES Y CONDICIONES GRALES CP N° 4_2021 (1).docx - Documentos de Google

Final Audit Report 2021-05-21

Created:	2021-05-21
By:	Fernanda Gonzalez (fgonzalez@ca.gob.ar)
Status:	Signed
Transaction ID:	CBJCHBCAABAASaQK4gioSWoan7mdTw0DduIsb1gvlh_r

"PLIEGO DE BASES Y CONDICIONES GRALES CP N° 4_2021 (1).docx - Documentos de Google" History

Document created by Fernanda Gonzalez (fgonzalez@ca.gob.ar)
2021-05-21 - 8:18:36 PM GMT- IP address: 181.199.156.163

Document emailed to Agustín Domingo (adomingo@ca.gob.ar) for signature
2021-05-21 - 8:23:01 PM GMT

Email viewed by Agustín Domingo (adomingo@ca.gob.ar)
2021-05-21 - 8:26:50 PM GMT- IP address: 66.102.8.9

Document e-signed by Agustín Domingo (adomingo@ca.gob.ar)
Signature Date: 2021-05-21 - 8:28:04 PM GMT - Time Source: server- IP address: 45.176.89.54

Agreement completed.
2021-05-21 - 8:28:04 PM GMT