Funcionalidades Generales Solucion Seguridad Aplicaciones Web

La solución debe de ser del tipo appliance físico/virtual
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.
La solución debe de soportar virtualización en hypervisor VMware
La solución debe de soportar virtualización en hypervisor Microsoft Hyper-V
La solución debe de soportar virtualización en hypervisor Citrix XenServer
La solución debe de soportar virtualización en hypervisor Open Source Xen
La solución debe de soportar virtualización en hypervisor KVM
La solución debe de soportar virtualización en plataformas Docker containers
La solución debe de soportar virtualización en Amazon AWS
La solución debe de soportar virtualización en Microsoft Azure
La solución debe de soportar virtualización en Google Cloud
La solución debe de soportar virtualización en Oracle Cloud
Tener puerto console RS-232 o RJ45, para acceso a la interfaz de linea de comandos

Funcionalidades de Red
Tener LEDs para la indicación del status y actividades de las interfaces
La solución debe permitir implementación en modo Proxy Transparente, Proxy Reverso, Transparente en Línea y Sniffer
La solución debe de ser capaz de ser implementada con protocolo WCCP
Soportar VLANs del estándar IEEE 802.1q.
Debe de implementar el protocolo Link Aggregation Control Protocol (LACP) - IEEE 802.3ad
Soportar direcionamiento IPv4 y IPv6 en las interfaces físicas y virtuales (VLANs).
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 principalpara que quando o principal falhar o tráfego possa continuar sendo processado.
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 própia solución.
La solución debe de soportar enrutamiento por política (policy route)

Funcionalidades de Gestión
El firmware debe soportar interfaz gráfica web para la configuración de las funciones del sistema, utilizando navegadoes 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.
Debe de soportar administración basada en interface web HTTP
Debe de soportar administración basada en interface de línea de comando vía Telnet
Tener la función de auto-completar comandos en la CLI
Tener ayuda contextual en la CLI

La solución debe de tener un Dashboard con información sobre el sistema (información del cluster, hostname, número de série, modo de operación, tiempo en servício, versión de firmware)
Debe de ser posible visualizar a través de la interfaz gráfica de gestión la información de licencia, firmas y contrato de soporte
La solución ofertada deberá de tener acceso a la línea de comando CLI directamente a través de la interfaz gráfica de gestión (GUI)
Debe de proveer, en la interfaz de gestión, las siguientes informaciones del sistema para cada equipo: consumo de CPU y estadísticas de conexión
Debe de ser posible visualizar en la interfaz de gestión la información de consumo de memória
Debe de incluir herramienta dentro de la interfaz gráfica de gestión (dashboard) que permita visualizar los últimos logs de ataques detectados/bloqueados
Dede 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
Tener en la interfaz gráfica estadísticas de conexión concurrente y por segundo, de políticas de seguridad del sistema
Tener un dashboard de visualización con información de las interfaces de red del sistema
La configuración de administración de la solución debe permitir la utilización de perfiles
Debe de ser posible ejecutar y recuperar backup por la interfaz Web (GUI)
Debe de tener la opción de criptografar el backup utilizando algorítmo AES 128-bit o superior
Debe de ser posible ejecutar y recuperar el backup utilizando FTP
Debe de ser posible ejecutar y recuperar el backup utilizando SFTP y TFTP
Debe ser posible probar una nueva versión de firmware en memória RAM, sin instalar en disco, antes de aplicarla
Debe ser posible instalar un firmware alternativo en disco y arrancarlo en caso de fallo del firmware principal
Debe soportar los protocolos de monitoreo SNMP v1, SNMP v2c e SNMP v3
Debe ser capaz de realizar notificación de eventos de seguridad a través de e-mail, traps SNMP y Syslog
La solución deberá de soportar almacenar logs localmente en disco y en servidor externo vía protocolo SYSLOG
Debe tener la capacidad de almacenar los logs en appliance remoto
La solución debe tener la capacidad de enviar alertas por email de los eventos basado en severidad y/o categorías
La solución debe tener datos analíticos conteniendo la localización geográfica de los clientes web
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
Debe tener la capacidad de generar reportes detallados basados en tráfico/acceso/actividades del usuario
Debe soportar RESTful API para gestión de la configuración

Los usuários deben de ser capaces de autenticarse a través del encabezado de autorización HTTP/HTTPS
Los usuários deben de ser capaces de autenticarse a través de formulários HTML embebidos
La solución debe de ser capaz de autenticar los usuários a través de certificados digitales personales
Debe tener base local para almacenamiento y autenticación de los usuários
La solución debe tener la capacidad de autenticar usuários en bases externas remotas LDAP, RADIUS y SAML
La solución debe de ser capaz de autenticar los usuários en base remota vía NTLM
La solución debe de ser capaz de crear grupos de usuários para configurar mecanismos de autenticación por grupos
Debe soportar CAPTCHA y Real Browser Enforcement (RBE)
Debe soportar autenticación de doble factor
Regulamentación y Certificaciones
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
El equipo debe de tener certificación FCC Class A part 15
El equipo debe de tener certificación C-Tick
El equipo debe de tener certificación VCCI
El equipo debe de tener certificación CE
El equipo debe de tener certificación UL/cUL
El equipo debe de tener certificación CB
Funcionalidades de Web Application Firewall
Debe tener soporte nativo de HTTP/2
Dbe soportar traducción de HTTP/2 a HTTP 1.1
Deberá soportar interoperabilidad con OpenAPI 3.0
Debe de ser capaz de identificar y bloquear ataques a través de una base de datos de firmas de vírus y reputación IP, la cual se debe actualizar automáticamente y de manera periódica
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
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
Deberá minimizar la ocurrencia de Falsos Positivos y falsos negativos utilizando Inteligencia Artificial
Tener mecanismo de aprendizaje automático capaz de identificar todos los contenidos de la aplicación, incluyendo URLs, parámetros de URLs, campos de formulários y lo que se espera de cada campo
El perfil aprendido de forma automática debe de poder ser ajustado
Tener la capacidad de creación de firmas de ataques customizables
Tener la capacidad de proteción contra ataques del tipo Adobe Flash binary (AMF) protocol
Tener la capacidad de proteción contra ataques del tipo Botnet
Tener la capacidad de proteción contra ataques del tipo Browser Exploit Against SSL/TLS (BEAST)

La solución debe tener funcionalidad de proteción contra ataques como acceso por fuerza bruta
Debe soportar detección de ataques de Clickjacking
Debe soportar detección de ataques de cambios de cookie
Identificar y proteger contra ataques del tipo Credit Cart Theft
Identificar y proteger contra ataques del tipo Cross Site Request Forgery (CSRF)
La solución debe tener funcionalidad de proteción contra ataques como cross site scripting (XSS)
Debe tener proteción contra ataques de Denial of Service (DoS);
Tener la capacidad de proteción contra ataques del tipo HTTP header overflow
Tener la capacidad de proteción contra ataques del tipo Local File inclusion (FLI)
Tener la capacidad de proteción contra ataques del tipo Man-in-the0middle (MITM)
Tener la capacidad de proteción contra ataques del tipo Remote File Inclusion (RFI)
Tener la capacidad de proteción contra ataques del tipo Server Information Leakage
Proteción contra envíos de comandos SQL ocultos en las requisiciones enviadas a la base de datos (SQL Injection);
Tener la capacidad de proteción contra ataques del tipo Malformed XML
Identificar y prevenir ataques del tipo Low-rate DoS
Prevención contra Slow POST attack
Proteger contra ataques Slowloris
Tener la capacidad de proteción contra ataques del tipo SYN flood
Tener la capacidad de proteción contra ataques del tipo Forms Tampering
La solución debe tener funcionalidad de proteción contra ataques de manipulación de campos ocultos
Tener la capacidad de proteción contra ataques del tipo Directory Traversal
Tener la capacidad de proteción del tipo Access Rate Control
Identificar y proteger contra Zero Day Attacks
Tener la capacidad de configurar proteción del tipo TCP SYN flood-style para prevención de DoS para cualquier política, a través de Syn Cookie y Half Open Threshold
Permitir configurar reglas de bloqueo a métodos HTTP no deseados
Permitir que se configuren reglas de limite de upload por tamaño del archivo
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 direción IP correspondientes a cada país
Debe soportar crear políticas de geo-localización, permitiendo que el tráfico de determinado país sea bloqueado
Permitir configurar listas negras de bloqueo y listas blancas de confianza, basadas en direción IP de origen
Permitir la liberación temporal o definitiva (white-list) de direciones IP bloqueadas por tener originado ataques detectados por la solución
Debe permitir añadir, automaticamente o manualmente, en una lista de bloqueo, las direciones IP de origen, según la base de IP Reputation
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.

Tener la capacidad de prevención contra pérdida de información (DLP), bloqueando la pérdidade información del encabezado HTTP
Tener la funcionalidad de proteger el website contra acciones de defacement, con recuperación automática y rápida del website en caso de fallo
Tener la funcionalidad de antivírus integrada para inspeción de tráfico y archivos, sin la necesidad de instalación de otro equipo
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
Debe se der capaz de hacer aceleración de tráfico SSL basada en hardware
La solución debe de ser capaz de funcionar como terminador de sessión SSL para aceleraración de tráfico
Para SSL/TLS offload soportar al menos SSL 3.0, TLS 1.0, 1.1 e 1.2
La solución debe tener la capacidad de almacenar certificados digitales de CA's
La solución debe de ser capaz de generar CSR para ser firmado por una CA
La solución debe de ser capaz de chequear los certificados válidos y que no fueron revocados por una lista CRL
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 contról de acceso, así como resetear dichas conexiones
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 actualizado automaticamente.
La solución debe de ser capaz de limitar el total de conexiones permitidas hacia cada servidor real de un pool de servidores
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
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).
La solución debe de tener la capacidad de definir restrición a determinados métodos HTTP
La solución debe tener la capacidad de proteger contra detección de campos ocultos
Permitir que se configuren firmas customizadas de ataques y DLP, a través de expresiones regulares
La solución debe permitir la integración con scanners de vulnerabilidades de terceros, tales como Acunetix, IBM AppScan, WhiteHat, etc, para proveer parches virtuales
Debe generar perfil de proteción automaticamente a partir de reporte en formato XML generado por scanner de vulnerabilidade de terceros
Debe permitir programar la verificación de vulnerabilidades
La solución debe generar un reporte de análisis de vulnerabilidades en formato HTML
Soportar redireción y reescritura de requisiciones y respuestas HTTP
Permitir redireción de requisiciones HTTP para HTTPS
Permitir reescribir la línea URL del encabezado de una requisición HTTP
Permitir reescribir el campo HOST del encabezado de una requisición HTTP
Permitir reescribir el campo REFERER del encabezado de una requisición HTTP
Permitir redirigir requisiciones para otro website

Permitir enviar respuesta HTTP 403 Forbidden para requisiciones HTTP
Permitir reescribir el parámetro LOCATION en el encabezado HTTP de una respuesta de redireción HTTP de un servidor web
Permitir reescribir el cuerpo ("body") de una respuesta HTTP de un servidor web
Permitir añadir el campo X-Forwarded-For para identificación de la direción IP real del cliente cuando en modo proxy reverso
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).
La solución debe de soportar combinación de contról 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 usuários de la aplicación
Tener capacidad de caching para aceleración web
La solución debe de ser capaz de enviar archivos para solución de sandboxing del mismo fabricante, a través de una política de restrición de carga del archivo
Debe permitir al administrador crear nuevas firmas y/o cambiar las firmas pre existentes
Funcionalidades de Balanceo de Carga
La solución debe incluir la funcionalidad de balanceo de carga entre servidores web
Debe soportar configurar puertos no estándar para aplicación web HTTP y HTTPS
Soportar balanceo / distribución de tráfico y enrutear el contenido hacia distintos servidores web
La solución debe permitir crear grupos de servidores (Server Farm / Pool) para distribuir las conexiones de los usuários
Soportar el algoritmo Round Robin para balanceo de carga entre servidores
Soportar el algoritmo Weighted Round Robin para balanceo de carga entre servidores
Soportar el algoritmo Least Connection para balanceo de carga entre servidores
La solución debe de soportar creación de servidores virtuales que definan la interfaz de red/bridge y direción IP por donde el tráfico con destino al Server Pool es recibido
Los servidores virtuales deben de entregar el tráfico hacia un único servidor web y tambien incluir la opción de distribuir las sessiones/conexiones entre los servidores web del Server Pool
Debe de ser porible definir el número máximo de conexiones TCP simultáneas hacia un determinado servidor miembro del Server Pool
Permitir prueba de disponibilidad del servidor web a través del método TCP
Permitir prueba de disponibilidad del servidor web a través del método ICMP ECHO_REQUEST (ping)
Permitir prueba de disponibilidad del servidor web a través del método TCP Half Open
Permitir prueba de disponibilidad del servidor web a través del método TCP SSL
Permitir prueba de disponibilidad del servidor web a través del método HTTP
Permitir prueba de disponibilidad del servidor web a través del método HTTPS
En las pruebas de disponibilidad HTTP y HTTPS, permitir indicar la URL exacta a ser probada
En las pruebas de disponibilidad HTTP y HTTPS, permitir eligir entre los métodos HEAD, GET y POST
En las pruebas de disponibilidad HTTP y HTTPS, permitir eligir el nombre del campo HTTP "host" a ser probado

Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Host"
Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "URL"
Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Parâmetro HTTP"
Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Referer"
Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Direción IP de Origen"
Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Encabeçado".
Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Cookie"
Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Valor del campo del Certificado X509"
Implementar Cache de Contenido para HTTP, permitiendo que objectos sean almacenados y requisiciones HTTP sean contestadas directamente por la solución
La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por direción IP de origenendereço IP de origem
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
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
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
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)
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
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
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
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
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
La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por sesión SSL

Requerimientos técnicos de implementación

1- Empresa con técnico certificado en: solución ofertados y CEH, ITIL Foundation y 10 años de experiencia en implementaciones de la solución, Unico ingeniero. (No se permiten certificaciones individuales)
2- Certificación del fabricante de distribución autorizado
3- Servicios técnicos basados en la migración de los equipos actuales y nuevos requerimientos
4- Logística de distribución de equipos en todo el país
5- Precio final debe de incluir viáticos de implementación.