TDR Adquisición de
Adquisición de Licenciamientos de Monitoreo, Seguridad y Equipo Firewall Para el Centro de Datos Del Estado Dominicano.

Razón de ser de la adquisición del del Servicio.

Actualmente el Centro de Datos Del Estado Dominicano requiere de una solución que ofrezca una administración de registros, análisis y plataforma de informes, proporcionando a la institución un panel único de orquestación, automatización y respuesta para una seguridad simplificada, operaciones, identificación proactiva, remediación de riesgos, y visibilidad completa de toda la superficie de ataque.

Con esta adquisición se pretende contar con una solución tecnológica vigente que garantice la prevención y detección temprana de cualquier tipo de amenaza cibernética, que puedan afectar las operaciones del centro de datos del estado y de los servicios ofrecidos.

Envista de las altas demandas y necesidades presentadas por las instituciones gubernamentales de los servicios ofertados por el Centro de Datos del Estado Dominicano, para continuar brindando los servicios de infraestructura, surgió una gran necesidad de solicitar la actualización de nuestros equipos Firewalls, con la finalidad de seguir cumpliendo con los requerimientos con alto volumen y flujo de solicitudes de servicios ofrecidos a las siguientes instituciones del estado.

- INSTITUCION
- DIGEIG
- SUPERINTENDENCIA DE SEGURO
- DIGEPRES
- IDECOOP
- INFOTEP
- INAGUJA
- MEPYD
- CSIRT
- ONDA
- HACIENDA
- CAASD
- PRESIDENCIA
- SALUD PUBLICA
- PLANSOCIAL DE LA PRESIDENCIA
- CONADIS
- CORAASAN
- PROINDUSTRIA
- MINISTERIO DE LA JUVENTUD
- BANCO AGRICOLA
- INAFOCAM
- LOTERIA NACIONAL
- CENPA
- UAF

Debido a la alta demanda de nuevos proyectos de conectividad que estamos realizando en el Centro De Datos del Estado Dominicano, adicionalmente sumando el proyecto de la red estatal. Los requerimientos por parte de las instituciones alojadas en las instalaciones del Centro de Datos, nos vemos en la necesidad de fortalecer la estructura y así poder contar con una arquitectura de telecomunicaciones, seguridad eficientes y redundantes que permitan escalar:

- Mejora de la arquitectura de telecomunicaciones para recibir las conectividades de las redes del estado.
- Fortalecer arquitectura de Centro de Datos. El mismo debe incluir los equipos adecuados para soportar el crecimiento proyectado, esto incluye routers, Firewall, Switches de accesos, Switches Core, Switches WAN e Infraestructura de Seguridad, para mitigar los ataques que se presentan cada día a la arquitectura de las redes del estado.
- Mejora al actual esquema de seguridad que nos ayude a tener mayor visibilidad y control para proteger las bases de datos y servidores de los ataques constantes.
- Establecer un esquema segmentado con certificados que ayude a mitigar cualquier ataque que se pueda presentar en la red interna hacia los servidores.
- Implementar arquitectura para mitigación de ataques de día cero que se puedan dar a las redes del estado.
- Mejorar la solución para protección de las aplicaciones WEB que se publican al internet.
- Mejorar el centro de operaciones de Red, NOC (Network Operation Center) y SOC, quien será responsable del monitoreo operacional de la infraestructura y servicios. Su función es asegurar la red al identificar, investigar, priorizar, resolver/escalar incidentes que pueden o que están afectando la disponibilidad o el desempeño de la plataforma.

Alcance

A través de la adquisición de Licenciamientos de Monitore, Seguridad y Equipo Firewall Para el Centro de Datos Del Estado Dominicano fortaleceremos el proyecto de conectividad de la red estatal, logrando interconectar las instituciones gubernamentales y fortalecer los siguientes puntos:

- Identifica miles de aplicaciones dentro del tráfico de red para una inspección profunda y aplicación de políticas rigurosas.
- Protege contra malware, exploits y sitios web maliciosos en tráfico cifrado y no cifrado.
- Prevenir y detectar ataques conocidos y desconocidos utilizando inteligencia artificial.
- Mejorar el rendimiento de protección contra amenazas y latencia especialmente diseñado.
- Proporcionar un rendimiento y protección para el tráfico cifrado SSL.
- Mejoras de capacidades de red avanzadas que se integran perfectamente con la seguridad avanzada de capa 7 y los dominios virtuales (VDOM).

Detalles

La adquisición consiste en la instalación de un equipo el cual ofrecen protección contra amenazas de alto rendimiento e inspección SSL para grandes empresas y proveedores de servicios, con la flexibilidad de implementarse en el borde de la empresa/nube, en el núcleo del centro de datos o segmentos internos. Las múltiples interfaces de alta velocidad, la eficacia de seguridad superior y el alto rendimiento de estas series mantienen la red conectada y segura.

Especificaciones del servicio:

LICENCIAS	
DESCRIPCION DEL ITEM	CANTIDAD
LOTE 1	
Analyzer	
• La solución debe ser compatible con la tecnología Security Fabric Analytics. • La solución debe tener la capacidad de realizar correlación de eventos en tiempo real, detección en todos los registros, con Indicadores de compromiso (IOC) servicio y detección de amenazas avanzadas. • La solución debe poder integrarse con FortiGate NGFW, FortiClient, FortiSandbox, FortiWeb, FortiMail y otros, para visibilidad más profunda y crítica de la red. • La solución debe contar la disponibilidad para automatizar copia de seguridad de base de datos, (hasta clúster de cuatro nodos) que puede ser segregado geográficamente para recuperación de desastres. • La solución debe contar con la capacidad de automatización de la seguridad para reducir complejidad, aprovechando REST, API, scripts, conectores, y puntadas de automatización para acelerar la respuesta de seguridad y reducir el tiempo de detección. • La solución debe contar con la capacidad de multiusuario con gestión de cuotas. • La solución debe contar con la capacidad de separar los datos del cliente, administrar dominios para eficacia operativa y cumplimiento. • La solución debe contar con opciones de implementación flexibles como dispositivo, VM, alojado o nube pública. Utilice AWS, Azure, o Google para la nube secundaria almacenamiento de archivos. • Suscripción por 3 años 50gb por día. • Soporte 24/7 IOC, SOC y nube.	1
Web Application Firewall	
• VM Appliance Virtual • Soporte para 4 x vCPU core • Soporte por 3 años 24x7 • Antivius • IP Reputation • Servicios de Seguridad • Sandboxing cloud • Credential Stuffing Defense Service • Funcionalidades Generales Solucion Seguridad Aplicaciones Web • La solución debe de ser del tipo appliance virtual	1

• 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.	

Equipo	
DESCRIPCION DEL ITEM	CANTIDAD
LOTE 2	
Equipo Firewalls	
• 2200 4 x 40GE QSFP+ slots, 20 x 10GE SFP+ slots (including 18x ports, 2x HA ports), 14 x GE RJ45 ports (including 12 x ports, 2 x management ports), SPU NP6 and CP9 hardware accelerated, and dual AC power supplies • Next Generation Firewall • Segmentation • Secure Web Gateway • IPS • Mobile Security • Soporte del fabricante de 36 meses. • Servicios de configuración e implementación.	1

PLAZO DE EJECUCIÓN

Una vez seleccionado el proveedor de esta aplicación tenemos un plazo de 4 semanas para la implementación por el nivel de urgencia que se requiere.

CONDICIONES DE GARANTIA DEL SERVICIO

Soporte de fabricante por 3 años
Acceso permanente al Centro de asistencia técnica, soporte 24/7-365, además de acceso a la comunidad de la aplicación seleccionada, supervisada de forma activa por los especialistas. gestionar todos los recursos incluidos en la asistencia técnica básica y en la asistencia técnica por e-mail.

SERVICIOS DE CONFIGURACIÓN E IMPLEMENTACIÓN.

El oferente deberá entregar mínimo 3 meses de soporte y servicio post implementación donde ejecutará cualquier petición solicitada y documentada por la institución.

La Adjudicación será decidida a favor del Oferente/Proponente cuya propuesta cumpla con todos los requisitos exigidos (técnicos y económicos) logrando cumplir con los Criterios de Evaluación y haya presentado el menor precio ofertado.

Para la implementación del Firewall el oferente deberá presentar certificaciones en las que especifique las siguientes características: 1. NSE4, NSE7, ITIL y CEH para el ingeniero Senior. (Adjuntar certificaciones de los ingenieros avalada por la entidad competente y que la misma pueda ser validada).