

ANEXO 1 AL CONTRATO N° 12/2.025 ADQUISICIÓN DE EQUIPO
DE FIREWALL.

ESPECIFICACIONES TÉCNICAS REQUERIDAS

Los bienes y/o servicios deberán cumplir con las siguientes especificaciones técnicas y normas:

Características	Mínimo Exigido
Marca: Fortinet	Exigido
Modelo: FortiGate 200F	Exigido
Procedencia: EEUU	Exigido
Cantidad: 2 (Dos)	Exigido
La solución ofertada deberá tener la característica de soportar a futuro, alta disponibilidad y ser tolerante a fallos sin interrupción de los servicios de red.	Exigido
La validez de las Licencias, como del soporte de fábrica de la solución tendrá una vigencia de 2 (dos) años.	Exigido
El equipo ofertado debe ser una plataforma de hardware de propósito específico denominado appliance. No serán admitidos servidores genéricos con un sistema de seguridad virtualizado o instalado sobre este servidor genérico.	Exigido
Deberá contar con un Throughput Firewall de al menos 10 Gbps.	Exigido
Deberá contar Threat Protection Throughput de al menos 2.5 Gbps.	Exigido
Deberá contar con Intrusión Prevention Throughput de al menos 4.5 Gpbs.	Exigido
Deberá contar con NGFW Throughput de al menos 3 Gpbs.	Exigido
Deberá contar con la funcionalidad de control de aplicaciones (AVC), Intrusion Prevention System (IPS), Control de navegación, User, Antispam Antivirus/ Antimalware con Sandboxing.	Exigido
Deberá soportar como mínimo 2.800.000 sesiones TCP por segundo.	Exigido
Deberá soportar como mínimo 250.000 nuevas sesiones TCP por segundo.	Exigido
Deberá soportar un Throughput para VPN IPsec de 12 Gbps.	Exigido
Deberá soportar una cantidad de túneles IPsec Gateway-to-Gateway no menor a 1.800.	Exigido
Deberá soportar una cantidad de túneles IPsec Client-to-Gateway no menor a 15.000.	Exigido
Por razones de eficiencia de uso de energía, los equipos deberán contar con fuente de energía redundantes 100240VAC (5060Hz).	Exigido
Deberá contar con soporte mínimo de al menos 4 interfaces de SFP+ de 10Gb.	Exigido
El equipo ofertado deberá contar con al menos 6 interfaces SFP de 1Gb.	Exigido

El equipo ofertado deberá contar con al menos 12 interfaces de cobre RJ45 de 1Gb.	Exigido
El equipo ofertado deberá contar con 1 interfaz de red de 1 Gbps dedicada para administración.	Exigido
El equipo ofertado deberá contar con 1 interfaz de tipo consola o similar RJ45, 1 USB port o 1 micro-USB.	Exigido
Deberá contar con reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos.	Exigido
La plataforma deberá realizar análisis de contenido de aplicaciones en Capa 7.	Exigido
El equipo ofertado deberá de contar con el software en su última versión estable esta información deberá ser corroborada con documentación oficial en el site del fabricante.	Exigido
Soporte multicast (PIM-SM).	Exigido
Soporte de 4094 VLAN Tags 802.1q.	Exigido
Deberá soportar creación de objetos de red que puedan ser utilizados como dirección IP de interfaces L3.	Exigido
Deberá contar con la funcionalidad de DHCP Relays.	Exigido
Deberá contar con soporte de DHCP Server.	Exigido
El equipo ofertado deberá soportar sub-interfaces ethernet lógicas.	Exigido
El equipo ofertado deberá soportar traducción de IP Puertos Network Address Translation (NAT).	Exigido
El equipo ofertado deberá soportar Nat dinámico (Many-to-1).	Exigido
El equipo ofertado deberá soportar Nat estático bidireccional 1-to-1.	Exigido
Soportar NAT de Origen y NAT de Destino simultáneamente.	Exigido
El equipo ofertado deberá contar con la capacidad de enviar log para sistemas de monitoreo externos denominados comúnmente como SIEM (Security Information and Event Management), simultáneamente.	Exigido
El equipo ofertado deberá de contar con funcionalidades de seguridad contra anti-spoofing.	Exigido
El equipo ofertado deberá soportar enrutamiento estático y dinámico (RIP, BGP y OSPFv2) para IPv4.	Exigido
Para IPv6, debe soportar enrutamiento estático y dinámico (OSPFv3).	Exigido
El equipo ofertado deberá de soportar OSPF graceful restart.	Exigido
Deberá contar con funcionalidad NAT64.	Exigido
Deberá contar con la funcionalidad de Identificación de usuarios a partir de LDAP/AD.	Exigido

Deberá contar con reglas de seguridad contra DoS (Denial of Service).	Exigido
Deberá contar con descriptión SSL y SSH.	Exigido
Deberá contar con QoS, DHCPv6 Relay.	Exigido
Deberá contar con las funcionalidades de Simple Network Management Protocol (SNMP) Network Time Protocol (NTP).	Exigido
Deberá contar con NTP autenticado.	Exigido
Deberá contar con SYSLOG.	Exigido
Deberá contar con Domain Name System (DNS).	Exigido
Deberá contar con control de aplicaciones.	Exigido
Los dispositivos de seguridad deben tener la capacidad de operar de forma simultánea mediante el uso de sus interfaces físicas en los siguientes modos dentro del mismo firewall, sin necesidad de tener que hacer uso de contextos virtuales: Modo sniffer (monitoreo y análisis del tráfico de red), Capa 2 (L2), Capa 3 (L3) y modo Transparente.	Exigido
Modo Sniffer, para inspección vía puerto espejo del tráfico de datos de la red.	Exigido
Modo Capa 2 (L2), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación.	Exigido
Modo Capa 3 (L3), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación operando como default Gateway de las redes protegidas.	Exigido
Modo Transparente, para poder inspeccionar de datos en línea y tener visibilidad del control de tráfico en nivel de aplicación sobre 2 puertos en modo bridge/Transparente.	Exigido
Modo mixto de trabajo Sniffer, Transparente, L2 e L3 simultáneamente en diferentes interfaces físicas del mismo equipo.	Exigido
El equipo ofertado deberá soportar a futuro la configuración de alta disponibilidad Activo/Pasivo y Activo/Activo.	Exigido
El equipo ofertado deberá poder sincronizar las configuraciones cuando esté implementado en alta disponibilidad tanto en modo transparente (Modo Firewall) o en modo Layer 3 (Modo Route).	Exigido
Sesiones TCP/IP.	Exigido
Sesiones VPNs.	Exigido
Políticas de Firewall.	Exigido
Configuraciones de NATs.	Exigido
Entradas de NATs.	Exigido
Configuraciones de QOS.	Exigido

Objetos de Red.	Exigido
Certificados para desencripción.	Exigido
Los equipos ofertados en modo de Alta-Disponibilidad (HA) deberá de contar con mecanismos de monitoreo de fallo de link.	Exigido
El equipo ofertado deberá de soportar controles por zona de seguridad.	Exigido
El equipo ofertado deberá de soportar inspección de protocolos IPSEC.	Exigido
El equipo ofertado deberá de contar con controles de políticas por puerto y protocolo.	Exigido
Control de políticas por aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.	Exigido
Control de políticas, IPs, redes y zonas de seguridad.	Exigido
Control de políticas por País.	Exigido
Control, inspección y desencripción de tráfico SSL con capacidad mínima 280.000 de sesiones SSL concurrentes.	Exigido
Debe desencriptar tráfico Inbound y Outbound en conexiones negociadas con TLS 1.2.	Exigido
Debe desencriptar tráfico que use certificados ECC (como ECDSA).	Exigido
Deberá permitir Traffic shaping QoS basado en políticas (Prioridad, Garantía y Máximo).	Exigido
Soporte a objetos y Reglas IPV6.	Exigido
Soporte a objetos y Reglas multicast.	Exigido
Deberá poseer la capacidad de reconocer aplicaciones, independiente del puerto y protocolo.	Exigido
Reconocimiento de aplicaciones diferentes, incluyendo, más no limitado: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e- mail.	Exigido
Deberá inspeccionar el payload (carga útil) del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo.	Exigido
El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no.	Exigido
Deberá identificar el uso de tácticas evasivas, o sea, debe tener la capacidad de visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas vía comunicaciones cifradas, como ataques mediante el puerto 443.	Exigido

Para tráfico Cifrado (SSL y SSH), debe permitir la descricpción de paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante.	Exigido
Deberá Actualizar la base de firmas de aplicaciones automáticamente.	Exigido
Deberá poder limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos del LDAP/AD.	Exigido
Deberá soportar múltiples métodos de identificación y clasificación de las aplicaciones, por lo menos chequeo de firmas, decodificación de protocolos y análisis heurístico.	Exigido
Deberá poseer módulo de IPS, Antivirus y Anti-Spyware integrados en el propio appliance de Firewall.	Exigido
Deberá incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti- Spyware).	Exigido
Las funcionalidades de IPS, Antivirus y Anti-Spyware deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.	Exigido
Debe sincronizar las firmas de IPS, Antivirus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo y Activo/pasivo.	Exigido
Deberá soportar granularidad en las políticas de IPS Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos esos ítems.	Exigido
Debe permitir el bloqueo de vulnerabilidades.	Exigido
Deberá permitir el bloqueo de exploits conocidos.	Exigido
Deberá incluir seguridad contra ataques de denegación de servicios.	Exigido
Deberá ser inmune y capaz de impedir ataques básicos como Synflood.	Exigido
Deberá ser inmune y capaz de impedir ataques básicos como ICMPflood.	Exigido
Deberá ser inmune y capaz de impedir ataques básicos como UDPfloof.	Exigido
Deberá posar firmas específicas para la mitigación de ataques DoS.	Exigido
Deberá posar firmas específicas para la mitigación de ataques buffer overflow.	Exigido
Deberá permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3.	Exigido
Deberá identificar y bloquear comunicaciones generadas por botnets.	Exigido
Deberá registrar en la consola de monitoreo las siguientes informaciones sobre amenazas identificadas.	Exigido
Deberá permitir Captura de paquetes (PCAP).	Exigido

Deberá poseer la función resolución de direcciones vía DNS, para que conexiones como destino a dominios maliciosos sean resueltas por el Firewall como direcciones (IPv4 e IPv6), previamente definidos.	Exigido
Los eventos deberán identificar el país de donde partió la amenaza.	Exigido
Deberá ser posible la configuración de diferentes políticas de control de amenazas y ataques basados en políticas del firewall considerando:	Exigido
Usuarios	Exigido
Grupos de usuarios,	Exigido
Origen	Exigido
Destino	Exigido
Zonas de seguridad	Exigido
Deberá Soportar la creación de políticas de QoS por:	Exigido
Dirección de origen	Exigido
Dirección de destino	Exigido
por puertos	Exigido
por aplicaciones	Exigido
Ancho de Banda garantizado	Exigido
Ancho de Banda Máximo	Exigido
por cola de prioridad	Exigido
Soportar la creación de políticas por Geolocalización, permitiendo que el tráfico de determinados País/Países sean bloqueados.	Exigido
Soportar VPN Site-to-Site y Client-To-Site.	Exigido
Soportar IPSec VPN.	Exigido
Soportar SSL VPN.	Exigido
La VPN IPSEc deberá soportar:	Exigido
DES y 3DES.	Exigido
Autenticación MD5 e SHA-1.	Exigido
Diffie-Hellman Group 1, Group 2, Group 5 y Group 14.	Exigido
Algoritmo Internet Key Exchange (IKEv1 & IKEv2).	Exigido
AES 128, 192 e 256 (Advanced Encryption Standard).	Exigido
Autenticación vía certificado IKE PKI.	Exigido
El agente de VPN SSL client-to-site debe ser compatible con sistemas operativos windows, linux actuales.	Exigido

Debe proteger implementaciones de VoIP.	Exigido
Debe permitir la aceleración de tráfico conocido, sin agregar herramientas de terceros o servidores separados.	Exigido
La solución de VPN debe soportar la conectividad de Smart Phones, al menos las siguientes plataformas, iPhone, iPad y Android. Permitiendo que todas las aplicaciones nativas puedan ser accedidas por clientes remotos desde el smart phone.	Exigido
La solución de VPN debe soportar la integración con los siguientes protocolos de autenticación: Lightweight Directory Access Protocol (LDAP) Servers Remote Authentication Dial-in User Service (RADIUS) ACE Management Servers (SecurID) Client certificates, authenticated by trusted CAs.	Exigido
La solución deberá proveer funcionalidad de autenticación de usuarios y equipos en el dominio Single Sign On.	Exigido
El Firewall Web debe tener la capacidad de identificar y bloquear herramientas de proxy bypass sobre protocolos estándar y no estándar (sin la necesidad de instalar un agente en los hosts o licencias adicionales).	Exigido
La solución debe controlar (traffic shapping) el ancho de banda de las aplicaciones por regla, horario.	Exigido
La solución debe permitir la creación de objetos de tiempo por aplicación o grupo de aplicaciones en las reglas, para que una acción definida se cumpla sólo durante tiempos especificados.	Exigido
Se deberán presentar catálogos y especificaciones del equipo ofertado.	Exigido
Certificados Internacionales exigido al oferente: Certificación ISO 9001/2015 o superior, la certificación superior debe basarse en los mismos criterios que solicita o certifica la norma ISO 9001/2015 con respecto a la calidad de la gestión de procedimientos de Provisión e integración de bienes y/o servicios. Certificación ISO 27001/2022 o superior, la certificación superior debe basarse en los mismos criterios que solicita o certifica la norma ISO 27001/2013 con respecto a la gestión de la seguridad, confidencialidad e integridad de los datos.	Exigido
Deberá incluir en su oferta todas las actividades de montaje, instalación en general, configuración y puesta en funcionamiento del equipo.	Exigido
El oferente deberá realizar una capacitación de al menos 40 horas al equipo técnico designado posterior al proceso de instalación.	Exigido