BOLSA MERCANTIL DE COLOMBIA

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

Nombre del Bien/Producto/Servicio (SIBOL)	DISPOSITIVO DE SEGURIDAD PERIMETRAL PARA REDES DE DATOS LICENCIAMIENTO DE SOFTWARE
Código SIBOL	43314 43007
Nombre Comercial del Bien/Producto/Servicio (Opcional)	Solución de seguridad Perimetral Nueva Generación de Firewall – NGFW.
Calidad	*Debe cumplir con todos los requisitos establecidos en la presente ficha técnica, de acuerdo con las especificaciones requeridas.*
Requisitos Específicos	**Ítem** **Solución Nueva Generación de Firewall - NGFW**

Características del hardware:

Arquitectura de Doble Procesador: Tecnología de procesamiento multinúcleo - x86 AMD CPU & Xstrewam Flow Processor (Marvell NPU)

- Factor de forma (Tamaño) : Desktop/1U/2U Rackmount
- Puertos Ethernet Incluídos: 8 puertos Gbe, cobre + modulo spf+
- Cantidad de Slots de Expansión : 1
- Pantalla : Módulo LCD multifunción
- Fuente de alimentación: Estandar de corriente alterna (AC)
- Certificaciones de productos (Safety, EMC): CB, CE, FCC Clase A, CTick, IC, VCCI, RCM, UL, CCC

Rendimiento de seguridad

- Firewall Throughput : 39000 Mbps.
- Firewall IMIX : 20000 Mbps.
- IPS throughput : 7000 Mbps
- Threat Protection throughput : 1500 Mbps
- NGFW : 6300 Mbps.
- IPsec VPN throughput : 20500 Mbps.
- IPsec VPN concurrent tunnels: 5000
- SSL VPN concurrent tunnels : 2500
- Conexiones simultáneas : 6500000

- Nuevas conexiones/seg : 148000
- SSL/TLS Inspection throughput : 1450 Mbps
- Conexiones simultaneas de SSL/TLS advanced: 18432
- Soporte modulo alimentacion externa
- Dencidad máxima de puertos: 18
- Puerto de administracion consola
- Puertos USB: 2
- Puerto micro usb: 1
- Cable de consola incluido

Características del firewall base

Administración General

- Interfaz de usuario optimizada y especialmente diseñada y administración de reglas de firewall para grandes conjuntos de reglas con agrupación con características de reglas de un vistazo e indicadores de aplicación
- Compatibilidad con autenticación de dos factores (contraseña de un solo uso) para acceso de administrador, portal de usuario, IPSec y SSL VPN
- Sistema de menú de autodocumentación / Ayuda
- Herramientas avanzadas de resolución de problemas / Troubleshooting en GUI (por ejemplo, captura de paquetes)
- Interfaz de línea de comandos (CLI) completa accesible desde GUI
- Administración basada en roles
- Notificación de actualización de firmware automatizada con un proceso de actualización automatizado sencillo y funciones de reversión
- Definición de objetos reutilizables para redes, servicios, hosts, períodos de tiempo, usuarios y grupos, clientes y servidores
- Portal de autoservicio
- Seguimiento de cambios de configuración
- Control flexible de acceso a dispositivos para servicios por zonas
- Opciones de notificación de captura snmp o correo electrónico
- Soporte SNMP v3 y Netflow
- Soporte de administración central a través de la consola unificada basada en la nube
- Notificaciones automáticas por correo electrónico para cualquier evento importante
- Configuraciones de backup y restauración: localmente, a través de FTP, correo electrónico, desde la plataforma de administración Cloud; bajo demanda, diaria, semanal o mensualmente
- Mejoras en el proceso de restauración de copias de Seguridad
- API para la integración con terceros

BOLSA MERCANTIL DE COLOMBIA

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

- Guias de administración en video integradas en Links en el FW
- Opción de acceso remoto al firewall de manera nativa del fabricante
- Soporte técnico de Syslog
- Cambio de nombre de la Interfaz
- La consola de administración Cloud debe tener capacidades de agrupar FWs, generar Backups y hacer deployments zero touch
- Desde la consola de administración cloud se debe poder generar reportes centralizados.

Administración centralizada

- La gestión e informes basados en la nube Central para varios Firewalls ofrece gestión de políticas de grupo y una única consola para todos sus productos de seguridad informática.
- La gestión de políticas de grupo permite que los objetos, la configuración y las políticas se modifiquen una vez y se sincronicen automáticamente en todos los Firewalls que pertenecen al mismo grupo.
- Contar con un Administrador de tareas proporciona una pista de auditoría histórica completa y una supervisión del estado de los cambios en las políticas de grupo
- La gestión de copias de seguridad de firmware debe tener la opción de almacenar los últimos cinco archivos de copia de seguridad de configuración de cada Firewall registrado con uno que se puede anclar para un almacenamiento permanente y un acceso sencillo.
- La programación de actualizaciones de firmware permite aplicar fácilmente actualizaciones automatizadas en cualquier momento
- El despliegue sin intervención (Zero-touch) permite realizar la configuración inicial en la central y luego exportarla para cargarla en el dispositivo desde una unidad flash al arrancar, conectando automáticamente el dispositivo al firewall central
- Gestión de firewalls de grupo a través del Partner Dashboard
- Informes de varios firewalls a través de grupos de firewalls.

Firewall, Networking & Routing

Firewall de inspección profunda de paquetes (Stateful deep Packet)

- Modelo de políticas unificada que permite gestionar las directivas en una sola pantalla
- la arquitectura de procesamiento de paquetes de contar con niveles extremos de visibilidad, protección y rendimiento mediante el procesamiento de paquetes basado en flujos
- Herramienta de simulador de pruebas de políticas para habilitar la regla de firewall y la web

BOLSA MERCANTIL DE COLOMBIA

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

	• simulación de políticas y pruebas por usuario, IP y hora del día • Inspección TLS con alto rendimiento, soporte para TLS 1.3 sin degradación, puerto • independientes, políticas de nivel empresarial, visibilidad única del panel y solución de problemas de compatibilidad • Motor DPI proporciona protección de escaneado de flujo para IPS, AV, Web, App Control e inspección TLS en un único motor de alto rendimiento. • Acelera el tráfico SaaS, SD-WAN y en la nube, como VoIP, video y otras aplicaciones confiables a través de FastPath (Aceleración de tráfico) • Network Flow FastPath ofrece automáticamente una aceleración inteligente y basada en políticas del tráfico de confianza • debe ofrecer aceleración del tráfico cifrado TLS • Políticas basadas en usuarios, grupos, tiempos o redes • Políticas de acceso delimitadas por tiempo por usuario/grupo • Habilitar políticas por zonas, redes o por tipo de servicio • Aislamiento de zonas y soporte de políticas basadas en zonas • Zonas predeterminadas para LAN, WAN, DMZ, LOCAL, VPN y WiFi • Zonas personalizadas para LAN o DMZ • Políticas NAT personalizables con enmascaramiento de IP • soporte completo de objetos para redirigir o reenviar múltiples servicios en una sola regla con un conveniente asistente de reglas NAT para crear rápida y fácilmente reglas NAT complejas con solo unos pocos clics • Soporte completo de VLAN • Nat de origen • Nat de destino • Renombrar Interfaces • Protección contra inundaciones: DoS, DDoS y portscan blocking • Bloqueo por geo-IP • Enrutamiento avanzado: estático, multidifusión (PIM-SM) y dinámico (RIP, BGP, OSPF, OSPF v3) con soporte completo de VLAN 802.1Q y multicast (PIM-SM y IGMP) • Enrutamiento de multidifusión independiente del protocolo con snooping IGMP • Soporte de Bridging con STP y ARP broadcast forwarding • Balanceo de enlaces WAN: Multiples conexiones a Internet, auto-link health check, failover automático, balanceo automático y por peso, reglas granulares multipath • Compatibilidad con WAN inalámbrica • Soporte de link aggregation 802.3ad • Configuración completa de DNS, DHCP y NTP • DNS dinámico (DDNS) • Enrutamiento mullticast independiente de protocolo con IGMP Snooping

BOLSA MERCANTIL DE COLOMBIA

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

- Compatibilidad con IPv6 con soporte de tunelización 6in4, 6to4, 4in6 e implementación rápida de IPv6 (6rd) a través de IPSec de acuerdo con el RFC 5969
- Soportar IPv6 DHCP Prefix Delegation
- Soportar BGPv6
- Compatibilidad con Wilcards para objetos host de nombre de dominio
- Soporte y etiquetado DHCP VLAN
- Soporte de Multiple bridge

Inspección SSL en todos los Puertos

Soportar Inspección SSL sin comprometer el rendimiento de la red o la experiencia del usuario. Ofrecer soporte de alto rendimiento y alta capacidad para TLS 1.3 y todos los conjuntos de cifrado modernos que proporcionan un rendimiento de inspección SSL extremo en todos los puertos, protocolos y aplicaciones.

Ítem
SD-WAN

- Debe tener tecnología de conectividad SD-WAN
- Integración de SD-WAN de terceros con redes troncales de Cloudflare, Akamai y Azure
- La funcionalidad SD-WAN debe ser compatible con la conectividad a Secure SD-WAN que se ofrece en el servicio Microsoft Azure Virtual WAN
- Debe admitir perfiles SD-WAN para balancear la carga de las conexiones entre interfaces
- Debe tener métodos de Balanceo: round-robin y persistencia de sesiones con las siguientes opciones:
  - ✓ Por conexión
  - ✓ IP de Origen
  - ✓ IP de destino
  - ✓ IP de Origen y Destino
- Los enlaces se pueden ponderar para determinar cómo se distribuye el tráfico entre ellos, y el SLA se puede usar para seleccionar qué enlaces serán incluidos para balancear carga.
- Debe soportar la configuración de nivel de calidad (SLA)mínimo (latencia, jitter y pérdida de paquetes) para que SDWAN elija un enlace determinado.
- Debe soportar el uso de al menos 4 (cuatro) enlaces de Internet / MPLS

	• Soporte para múltiples opciones de enlace WAN, incluyendo VDSL, DSL, cable y celular 3G / 4G / LTE con monitoreo esencial, balanceo, conmutación por error • Los perfiles SD-WAN admiten varias opciones de enlace WAN, como VDSL, DSL, cable, LTE/celular y MPLS. • Debe soportar el uso de enlaces de interfaz física, subinterfaces VLAN lógicas y túneles IPSec • Debe generar un Log de eventos que registre los cambios en el estado de los enlaces SD-WAN, monitoreados por el estado de salud de los enlaces • La solución debe ser capaz de medir el estado de salud del enlace en base a criterios mínimos de: Latencia, Jitter y Pérdida de Paquetes, donde es posible configurar un valor Theshold para cada uno de estos ítems, el cual será utilizado como factor de decisión en las reglas SD-WAN • La solución SD-WAN debe poder presentar gráficamente todos los datos de análisis del estado del enlace, que contenga gráficos que presenten al menos los criterios descritos anteriormente. • Los gráficos deben presentarse en tiempo real y permitir una visualización histórica de al menos 24 horas, 48 horas, 1 semana y 1 mes • La verificación del estado de salud debe admitir el marcado de paquetes con DSCP, para una evaluación más precisa de los enlaces que tienen QoS configurado • La solución debe tener funcionalidad para crear la malla SD-WAN en varios firewalls en un solo concentrador • Esta funcionalidad debería facilitar la configuración SD-WAN de múltiples firewalls, creando automáticamente toda la información necesaria para que SD-WAN suceda, como al menos, pero no limitado a: creación de rutas, reglas de firewall, objetos y túneles VPN necesarios. • La misma consola del concentrador SD-WAN debe monitorear los enlaces de cada dispositivo implementado, lo que garantiza una vista única de todos los dispositivos implementados. • Selección y enrutamiento de rutas de aplicaciones, que se utiliza para garantizar la calidad y minimizar la latencia para aplicaciones de misión crítica como VoIP • SD-WAN sincronizada, una función de seguridad sincronizada que aprovecha la claridad y confiabilidad adicionales de la identificación de aplicaciones que viene con el intercambio de información de control de aplicaciones sincronizadas entre los puntos finales administrados y el firewall • Enrutamiento sincronizado de aplicaciones SD-WAN a través de enlaces preferidos a través de reglas de firewall o enrutamiento basado en políticas

BOLSA MERCANTIL DE COLOMBIA

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

- Soporte VPN robusto que incluye IPSec y SSL VPN
- Orquestación VPN centralizada
- Túnel ÚNICO RED Layer 2 con enrutamiento
- Integración con Azure Virtual WAN para una red de superposición SD-WAN completa

Terminales brutas para conectividad VPN en oficinas remotas de pocos usuarios

- El comitente vendedor debe proveer una terminal que no contenga todas las capacidades del FW de nueva generación y que sea mucho más económica y que sea de la misma línea de marca del firewall para levantar VPNs para oficinas remotas de pocos usuarios que no necesiten tener un FW dedicado.
- 850 Mbps.4 x10/100/1000, puerto compartido wan1 con SFP. 1x fibra sfp. 2 Puertos PoE (potencia total 30 w). Modulo Wi-fi opcional: 802.11a/b/g/n/ac Wave 1 (Wifi-5) de doble banda 2x2 mimo. 2 antenas. 2xUSB 3.0 (frontal - trasero
- Zero Touch: se conecta automáticamente a través de un servicio de aprovisionamiento basado en la nube
- Túnel cifrado seguro con certificados digitales X.509 y cifrado AES256-
- Interfaz Ethernet virtual para una transferencia fiable de todo el tráfico entre ubicaciones
- Administración de direcciones IP con configuración de servidor DHCP y DNS definida de forma centralizada
- Desautorizar remotamente los dispositivos después de un período selecto de inactividad
- Compresión del tráfico del túnel
- Opciones de configuración del puerto VLAN

Traffic Shaping & Quotas

- Para controlar las aplicaciones y el tráfico cuyo consumo puede ser excesivo y tener un alto consumo de ancho de banda, se requiere que la solución, además de poder permitir o denegar este tipo de aplicaciones, debe tener la capacidad de controlarlas mediante políticas de ancho de banda máximo cuando lo requieran diferentes usuarios o aplicaciones
- La solución debe soportar Traffic Shaping (Qos) y la creación de políticas basadas en categoría web y aplicación por: dirección de origen; dirección de destino; Usuario y grupo LDAP/AD
- La configuración del tráfico (QoS) se basará en la red o en el usuario
- Establecer cuotas de tráfico basadas en usuario, carga/descarga, tráfico total, cíclico o no cíclico

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

- Debe permitir aplicar prioridad incluso después del enrutamiento, utilizando el protocolo DSCP
- Soportar la priorización en tiempo real de los protocolos de voz (VoIP).

Protección y Control Wireless

- Implementación sencilla plug-and-play de puntos de acceso inalámbricos (APX): deben visualizarse automáticamente en un centro de control nativo de APs en el FW
- Supervisar y administrar centralmente todos los dispositivos APX y clientes inalámbricos a través del controlador inalámbrico incorporado
- Capacidad de mapiar APs a LAN, VLAN, o una zona separada con las opciones de aislamiento de cliente
- Soporte de SSID múltiple por radio incluyendo SSID ocultos
- Soporte de opciones de cifrado y seguridad más recientes, incluyendo WPA2 Personal y Enterprise
- Soporte de IEEE 802.1X (Autenticación RADIUS)
- Soporte de 802.11r (fast transition)
- Soporte de Hotspot para vouchers personalizados, contraseña del día o aceptación de T&C
- Acceso inalámbrico a Internet para invitados con opciones de Walled Garden
- Acceso a la red inalámbrica basada en el tiempo
- Modo de red mallado de repetición y puente inalámbrico con Aps compatibles
- Optimización automática de selección de canales en background
- Soporte para inicio de sesión HTTPS

Autenticación

- Debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién usa qué aplicaciones a través de la integración con los servicios de directorio, la autenticación a través de LDAP, Active Directory, Azure AD, Radius, eDirectory, TACACS+ y a través de la base de datos local, para la identificación de usuarios y grupos que permiten granularidad de control/políticas basadas en usuarios y grupos de usuarios
- Debe soportar la identificación de múltiples usuarios conectados a la misma dirección IP en ambientes Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que se encuentran en estos servicios
- Debe permitir la autenticación en los modos: transparente, autenticación proxy (explícita, NTLM y Kerberos) y autenticación vía

BOLSA MERCANTIL DE COLOMBIA

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

clientes en estaciones de trabajo con sistemas operativos Windows, macOS y Linux 32/64
- Al usar la opción de proxy explícito, se debe permitir la autenticación para cada conexión, a fin de garantizar que el Firewall identifique correctamente a los usuarios que iniciaron sesión en servidores multisesión, incluso cuando se usa solo 1 IP de origen
- Debe ser compatible con la configuración de inicio de sesión único para que los administradores inicien sesión en la consola web mediante Azure AD
- Debe tener autenticación de inicio de sesión único para al menos Active Directory, Azure AD y sistemas de directorio de eDirectory
- Autenticación vía: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
- Agentes de autenticación de servidor para SSO, STAS, SATC de Active Directory
- Tiempo de espera de radio con autenticación de dos factores (2FA)
- Agentes de autenticación de cliente para Windows, Mac OS X, Linux 32/64
- Certificados de autenticación para iOS y Android
- Single sign-on: Active directory, eDirectory
- Servicios de autenticación para IPSec, L2TP, PPTP, SSL
- Compatibilidad con la creación de usuarios con formato UPN para la autenticación RADIUS
- Debe permitir el control, sin necesidad de instalar un software cliente, de los dispositivos que soliciten salida a internet para que antes de iniciar la navegación se amplíe un portal de autenticación residente en el firewall (Portal Cautivo).

Portal de Autoservicio de usuario

- Descarga de cliente de autenticación - Authentication Client
- Descargar cliente de acceso remoto SSL (Windows) y archivos de configuración para otros SO's
- Información de acceso al hotspot
- Cambiar el nombre de usuario y la contraseña
- Ver el uso personal de Internet
- Acceder a mensajes en cuarentena y administre listas de remitentes de bloqueo/permiso basadas en el usuario (requiere protección de correo electrónico)

Opciones de VPN

- La solución de Firewall deberá permitir crear túneles VPN IPSec y SSL ilimitados
- Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

- La VPN IPsec debe admitir: Autenticación DES, 3DES, GCM, Suite-B, MD5 y SHA-1, Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14; algoritmo de intercambio de claves de Internet (IKE); AES 128, 192 y 256 (Estándar de cifrado avanzado); SHA 256, 384 y 512; Autenticación mediante certificado PKI (X.509) y clave precompartida (PSK).
- L2TP y PPTP
- Deberá permitir las VPN basada en rutas
- Remote access: SSL, IPsec, iPhone/iPad/ Cisco/Andriod VPN client
- Deberá brindar soporte al protocolo IKEv2 que se utiliza para negociar una asociación de seguridad al principio de una sesión
- La solución deberá permitir la aplicación de TLS 1.2 para túneles VPN de acceso remoto y sitio a sitio SSL
- Debe tener opción IPSEC VPN con cliente nativo del fabricante
- Cliente SSL para Windows & descarga de configuración a través del portal de usuarios
- Debe contar con un portal encriptado basado en HTML5 para soportar al menos: RDP, SSH, Telnet y VNC, sin necesidad de instalar clientes VPN en las estaciones de acceso
- Debe permitir la creación de políticas de control de aplicaciones, IPS, Antivirus, Anti-Malware y filtrado de URL para el tráfico de clientes remotos conectados a la VPN SSL.
- Debe soportar de forma nativa la integración con Amazon para establecer un túnel seguro entre los dispositivos y AWS VPN

- Permita establecer un túnel VPN SSL con una solución de autenticación a través de LDAP, Active Directory, Azure AD, Radius, eDirectory, TACACS+ y a través de una base de datos local.

Cliente IPSec

- Autenticación: Pre-Shared Key (PSK), PKI (X.509), Smartcards, Token y XAUTH
- Cifrado: AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (up to 2048 Bit), Grupos DH 1/2/5/14, MD5 y SHA-256/384/512
- Soportar autentición via AD/LDAP, Token y base datos de usuarios locales
- Split-tunneling inteligente para un enrutamiento de tráfico óptimo
- Soporte de NAT-transversal
- Monitor de cliente para una visión general gráfica del estado de la conexión
- Multilenguaje

BOLSA MERCANTIL DE COLOMBIA

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

CARACTERISTICAS LICENCIAMIENTO FIREWALL

Intrusion Prevention Systems (IPS)

Licenciamiento capaz de gestionar VPN site to site, y VPN ssl, cubrimiento y protección de redes, Protección web con control de aplicaciones, segmentación de tráfico, que contenga espacios seguros con machine learning para la aplicación de día cero, orquestador SD WAN, y cubrimiento de RMA.

Motor de inspección profunda de paquetes IPS de próxima generación y alto rendimiento con patrones IPS selectivos que se pueden aplicar sobre la base de reglas de firewall para obtener el máximo rendimiento y protección.

Ítem
Licencia Advanced firewall NG

- Interfaz de usuario optimizada y especialmente diseñada y administración de reglas de firewall para grandes conjuntos de reglas con agrupación con características de reglas de un vistazo e indicadores de aplicación
- Compatibilidad con autenticación de dos factores (contraseña de un solo uso) para acceso de administrador, portal de usuario, IPSec y SSL VPN
- Sistema de menú de autodocumentación / Ayuda
- Herramientas avanzadas de resolución de problemas / Troubleshooting en GUI (por ejemplo, captura de paquetes)
- Interfaz de línea de comandos (CLI) completa accesible desde GUI
- Administración basada en roles
- Notificación de actualización de firmware automatizada con un proceso de actualización automatizado sencillo y funciones de reversión
- Definición de objetos reutilizables para redes, servicios, hosts, períodos de tiempo, usuarios y grupos, clientes y servidores
- Portal de autoservicio
- Seguimiento de cambios de configuración
- Control flexible de acceso a dispositivos para servicios por zonas
- Opciones de notificación de captura snmp o correo electrónico
- Soporte SNMP v3 y Netflow
- Soporte de administración central a través de la consola unificada basada en la nube
- Notificaciones automáticas por correo electrónico para cualquier evento importante

BOLSA MERCANTIL DE COLOMBIA

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

- Configuraciones de backup y restauración: localmente, a través de FTP, correo electrónico, desde la plataforma de administración Cloud; bajo demanda, diariamente, semanalmente o mensualmente
- Mejoras en el proceso de restauración de copias de Seguridad
- API para la integración con terceros
- Guias de administración en video integradas en Links en el FW
- Opción de acceso remoto al firewall de manera nativa del fabricante
- Soporte técnico de Syslog
- Cambio de nombre de la Interfaz
- La consola de administración Cloud debe tener capacidades de agrupar FWs, generar Backups y hacer deployments zero touch
- Desde la consola de administración cloud se debe poder generar reportes centralizados.

Ítem
Solución Endpoint

Protección avanzada contra amenazas y respuesta aut. a incidentes-ENDPOINT.

- Protección avanzada contra Malware: utiliza tecnologías de detección tanto tradicionales como de última generación, incluyendo inteligencia artificial y aprendizaje automático, para identificar y neutralizar amenazas, como virus, ransomware y otros tipos de malware. detener automáticamente procesos maliciosos y aislamiento de dispositivos comprometidos para evitar propagación de amenazas en la red.
- Debe realizar una inspección profunda de paquetes para la prevención de intrusiones (IPS) y debe incluir firmas de prevención de intrusiones.
- Las firmas de prevención de intrusiones (IPS) deben poder personalizarse.
- Protección avanzada contra amenazas (Detectar y bloquear el tráfico de red con servidores de comando y control mediante DNS multicapa, AFC y firewall)
- Visibilidad instantánea sobre el estado de amenaza de los endpoints, con la opción mediante el aislamiento de los sistemas infectados tanto para tráfico en el mismo dominio de broadcast como para otros segmentos de red sin que haya ningún tipo de intervención o cambios realizados por el administrador.
- Proporcionar visibilidad de los usuarios de mayor riesgo, aplicaciones desconocidas, amenazas avanzadas y payloads sospechosos.
- Los filtros inteligentes de directiva IPS habilitan directivas dinámicas que se actualizan automáticamente a medida que se agregan nuevos patrones.
- Solicitar información de aplicaciones al Endpoint para el tráfico que no coincida con ninguna firma de control de aplicaciones.

- not match any application control signature.
- Capacidades forenses y de análisis profundas en usuarios, amenazas, aplicaciones, uso web y otras actividades en la red.
- Limitar el acceso a los recursos de red o aislar completamente los sistemas comprometidos hasta que se mitigue completamente el riesgo o se elimine la amenaza
- Tener la capacidad de compartir telemetría y el estado de salud entre el Endpoint y el firewall para proporcionar una respuesta automática y adaptativa ente una amenaza de seguridad.

CARACTERISTICAS PROTECCION WEB

Protección y Control Web

- Proxy totalmente transparente para antimalware y filtrado web
- Protección avanzada mejorada contra amenazas
- Debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién usa qué URL a través de la integración con servicios de directorio, autenticación a través de LDAP, Active Directory, Azure AD, Radius, E-directory y base de datos local.
- Permitir llenar todos los registros de URL con información de usuario como se describe en Integración de servicios de directorio
- La solución deberá proveer una base de datos de filtrado de URL con millones de sitios en 92 categorías respaldados por OEMLabs
- Debe poder categorizar URL desde la base o caché de URL locales o mediante consultas dinámicas en la nube del fabricante, independientemente del método de clasificación, la categorización no debe causar demoras en la comunicación visibles para el usuario.
- Debe soportar la creación de categorías de URL personalizadas
- Políticas de tiempo de cuota de navegación por usuario/grupo
- Políticas de acceso por tiempo para usuario/grupo
- Debe tener la capacidad para que algunos usuarios seleccionados previamente eludan temporalmente la política de bloqueo actual
- Análisis de malware: bloquee todas las formas de virus, malware web, troyanos y spyware en HTTP/S, FTP y correo electrónico basado en la web
- Protección avanzada contra malware web con emulación JavaScript
- Live Protection búsquedas en tiempo real en la nube para la última inteligencia de amenazas
- Segundo motor de detección de malware independiente para el doble análisis
- Escaneo en tiempo real o en modo por lotes
- Protección de Pharming
- Análisis HTTP y HTTPS por usuario o política de red con reglas y excepciones personalizables

- Detección y enforcement de túneles SSL
- Supervisión y aplicación de palabras claves en navegación para bloquear o permitir sitios que contengan dicho contenido.
- Validación de certificados
- Almacenamiento en caché de contenido web de alto rendimiento
- Almacenamiento en caché forzado para actualizaciones de Endpoint
- Filtrado de tipos de archivo por tipo de mimo, extensión y tipos de contenido activo (por ejemplo, Activex, applets, cookies, etc.)
- Soporte de SafeSearch (basada en DNS) para los principales motores de búsqueda por política (usuario/grupo)
- Monitoreo y aplicación de palabras clave web para registrar, informar o bloquear palabras clave coincidentes con contenido web listas con la opción de subir listas de aduanas
- Bloquear aplicaciones potencialmente no deseadas (PUAs)
- Debe permitir especificar la política de navegación Web por tiempo, es decir, definir reglas para un día de la semana determinado y hora de inicio y fin, permitiendo agregar múltiples días y horas en una misma definición de política por tiempo. Esta regla de tiempo puede ser recurrente o única.
- Opción de anulación de directivas web para que los profesores o el personal permitan temporalmente el acceso a sitios o categorías bloqueados que son totalmente personalizables y administrables por usuarios seleccionados
- Aplicación de políticas de usuario/grupo en Google Chromebooks
- Filtrado web automático de sitios identificados por Internet Watch Foundation (IWF) que contienen abuso sexual infantil

Protección y control de aplicaciones

Control mejorado de aplicaciones con firmas y patrones de Capa 7 para miles de aplicaciones

Los dispositivos de protección de red deben tener la capacidad de reconocer aplicaciones por firmas y capa 7, utilizando puertos estándar (80 y 443), puertos no estándar, salto de puerto y tunelización a través de tráfico SSL encriptado.

Debe ser posible inspeccionar paquetes cifrados con algoritmos SSL 2.0, SSL 3.0, TLS 1.2 y TLS 1.3

El motor de análisis de tráfico cifrado debe reconocer, entre otros, al menos los siguientes algoritmos: curvas elípticas (ECDH, ECDHE, ECDSA), DH, DHE, Autenticación, RSA, DSA, ANON, Bulk ciphers,

	RC4, 3DES, IDEA, AES128, AES256, Camelia, ChaCha20-Poly1305, GCM, CCM, CBC, MD5, SHA1, SHA256, SHA384 El motor de inspección de paquetes cifrados debe ser configurable y permitir definir acciones como no descifrar, denegar el paquete y cifrar para determinadas conexiones cifradas Reconocer al menos 2300 aplicaciones diferentes clasificadas por nivel de riesgo, características y tecnología, incluido, entre otros, el tráfico relacionado con peer-to-peer, redes sociales, acceso remoto, actualización de software, servicios de red, VoIP, transmisión de medios, proxy y tunelización. mensajería instantánea, uso compartido de archivos, correo electrónico web y actualizaciones de software Reconocer al menos las siguientes aplicaciones: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, base de datos Oracle, descarga de archivos RAR, Redtube Streaming, RPC sobre HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing and File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer y WhatsApp Web Debe escanear y controlar la microaplicación que incluye, entre otros: Facebook (aplicaciones, chat, comentarios, eventos, juegos, complemento Me gusta, mensaje, descarga y carga de fotos, complemento, adjunto de publicación, publicación, preguntas, actualización de estado, chat de video, video reproducción, carga de video, sitio web), Freegate Proxy, Gmail (aplicación de Android, archivo adjunto), Google Drive (base, descarga de archivos, carga de archivos), aplicación de Google Earth, Google Plus, LinkedIN (búsqueda de empresa, redacción de correo web, búsqueda de empleo, correo Bandeja de entrada, actualización de estado), carga y descarga de archivos de SkyDrive, Twitter (mensaje, actualización de estado, carga, sitio web), Yahoo (correo web, archivo adjunto de correo web) y Youtube (búsqueda de video, transmisión de video, carga, sitio web)

BOLSA MERCANTIL DE COLOMBIA

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

Para el tráfico cifrado SSL, debe descifrar los paquetes para poder leer la carga útil para verificar las firmas de las aplicaciones conocidas por el fabricante.

Reconocimiento de Aplicaciones en IPv6

Control de aplicaciones basado en categorías, características (por ejemplo, consumo de ancho de banda y productividad), tecnología (por ejemplo, P2P) y nivel de riesgo

El medidor de riesgo de aplicaciones proporciona un factor de riesgo general basado en el nivel de riesgo de las aplicaciones de la red

Identificar, clasificar y controlar aplicaciones previamente desconocidas activas en la red a través de integración Nativa con solución de Endpoint

Identificar, clasificar y controlar automáticamente todas las aplicaciones en la red incluyendo las desconocidas o para las que no se tengan firmas a través de integración nativa con solución de XDR garantizando la identificación y control del 100% de las aplicaciones que generan tráfico dentro de la organización

Debe permitir el uso individual de diferentes aplicaciones para usuarios pertenecientes a un mismo grupo de usuarios, sin necesidad de cambiar de grupo o crear uno nuevo. Otros usuarios de este mismo grupo que no tengan acceso a estas aplicaciones deberán tener bloqueado su uso

Aplicación de directivas de control de aplicaciones por usuario o regla de red

Visibilidad de Aplicaciones Cloud

- El widget Centro de control muestra la cantidad de datos cargados y descargados en aplicaciones en la nube categorizados como nuevos, sancionados, no autorizados o tolerados
- Poder descubrir Shadow IT en un vistazo
- Desglose para obtener detalles sobre los usuarios, el tráfico y los datos

BOLSA MERCANTIL DE COLOMBIA

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

- Filtrar el uso de aplicaciones en la nube por categoría o volumen
- Informe detallado de uso de aplicaciones en la nube personalizable para obtener informes históricos completos

Configuración del tráfico de Web & App

Opciones de modelado de tráfico personalizado (QoS) por categoría web o aplicación para limitar o garantizar la carga/descarga o la prioridad total del tráfico y la velocidad en bits individualmente o compartidas

CARATERISTICAS SANDBOXSING

Protección de Sandbox contra amenazas de día cero

- El appliance de seguridad ofertado debe poder habilitar el servicio de Sandboxing en la nube para análisis y detonación de malware potencial, de igual manera sincronizar firewall-nube-antivirus sobre la misma línea de marca.
- Inspeccionar ejecutables y documentos que contengan contenido ejecutable
- Inspecciona ejecutables y documentos que contienen contenido ejecutable (incluidos .exe, .com y .dll, .doc, .docx, docm y .rtf y PDF) y archivos que contienen cualquiera de los tipos de archivo enumerados anteriormente (incluidos ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)
- Inspeccionar documentos de Word (incluyendo .doc, .docx, docm and .rtf)
- Detonar PDF
- Informes de archivos maliciosos en profundidad y capacidad de liberación de archivos de panel
- El sanbox debe realizar análisis dinámico de comportamiento de malware y deep learning (si un pc es infectado debe quedar aislado de la red para no propagar el virus a la red)
- Análisis en menos de 120 segundos
- Reportes detallados conteniendo inteligencia de amenaza: Composición del archivo, patrones de ejecución, similitud con otros códigos, etc.

Características de ZTNA

- Protección Zero Trus Network Access
- Firewall deberá poderse integrar con Zero Trust Network Access (ZTNA) para ofrecer una forma segura y sencilla para que los

BOLSA MERCANTIL DE COLOMBIA

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

usuarios se conecten de forma segura a aplicaciones y datos importantes
- Integración del Gateway de ZTNA en el Firewall
- Deberá conectar de forma segura a los usuarios a las aplicaciones
- Soportar aplicaciones en la nube y locales
- Acceso remoto de los usuarios desde cualquier lugar
- El estado del dispositivo se integra con la seguridad sincronizada

Ítem
Solución Endpoint Advanced

Protección completa de SMTP y POP contra correo no deseado, pesca de información y fuga de datos con protección todo en uno que combina cifrado de correo electrónico basado en políticas con DLP y anti-spam, mayor seguridad al sincronizar con el firewall.

- Análisis de correo electrónico con soporte SMTP, POP3 e IMAP
- Reglas de flujo de correo Microsoft 365
- Protección de post entrega para Microsoft 365
- Protección contra phishing de suplantación de identidad
- Comprobación contra dominios de imitación
- Soporte completo de almacenamiento y reenvío de MTA
- Servicio de reputación con monitoreo de brotes de spam basado en la tecnología patentada De detección de patrones recurrentes
- Bloquear el spam y el malware durante la transacción SMTP
- Segundo motor de detección de malware independiente (Avira) para escaneo dual
- Protección antispam DKIM y BATV
- Búsquedas en la nube en tiempo real de Live Protection para obtener la inteligencia de amenazas más reciente
- Actualizaciones automáticas de firmas y patrones
- Detección/bloqueo/escaneo de archivos adjuntos de tipo de archivo
- Aceptar, rechazar o quitar mensajes de gran tamaño
- Detecta URL de phishing dentro de correos electrónicos
- Usar reglas de análisis de contenido predefinidas o crear sus propias reglas personalizadas basadas en una variedad de criterios
- Soportar cifrado TLS para SMTP, POP e IMAP
- Verificación del destinatario
- Anexar firma automáticamente a todos los mensajes salientes
- Greylisting
- Capacidad de Outbound email relay
- Capacidad de operar como archivador de correo electrónico
- Las listas de remitentes individuales basadas en el usuario se bloquean y permiten mantener a través del portal de usuarios.

BOLSA MERCANTIL DE COLOMBIA

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

DETECCION Y RESPUESTA EXTENDIDA (XDR)

Visibilidad completa

- Monitoreo continuo y visibilidad en endpoints, servidores y otras areas.
- Protección contra Ransomware, detección de archivos malicioso y restauración.
- Aislar el equipo de la red al ser infectado.
- Deep learning, detección y bloqueo de malware antes de ejecutarse.
- Security adavanced: sincronización de seguridad entre firewall y Endpoint.

Email Quarantine Management

- Opciones de resumen y notificaciones de cuarentena no deseado
- Cuarentenas de malware y spam con opciones de búsqueda y filtro por fecha, remitente, destinatario, asunto y motivo con opción de liberar y eliminar mensajes
- Portal de usuario de autoservicio para ver y liberar mensajes en cuarentena

Cifrado de correo electrónico y DLP

- Soportar cifrado de mensajes unidireccionales
- Auto registro del destinatario y contraseñas de cifrado
- Añadir archivos adjuntos a correos de respuestas cifradas
- Completamente transparente, no se requiere software o cliente adicional
- Listas de control de contenido (CCL) de tipo de datos confidenciales preempaquetadas para PII, PCI, HIPAA y más, mantenidas Inteligencia de Amenazas del Fabricante

LOGGING Y REPORTERIA

Reporteador de Firewall (Gestión centralizada)

- Múltiples informes integrados con opciones de informe personalizados y flexibles
- Dashboards de tráfico, Seguridad y Amenazas de Usuario

BOLSA MERCANTIL DE COLOMBIA

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

- Informe de aplicaciones (riesgo de aplicaciones, aplicaciones bloqueadas, usos web, motores de búsqueda, servidores web, FTP),
- Informe de Amenazas de Red (IPS, ATP, Wireless, Respuesta a incidentes),
- Reportes de VPN
- Reportes de protección y uso de Correo Electrónico
- Informes de cumplimiento (HIPAA, GLBA, SOX, FISMA, PCI-DSS, NERC CIP v3 y CIPA)
- Supervisión de actividad actual: estado del sistema, usuarios activos, conexiones IPsec, usuarios remotos, conexiones en vivo, clientes inalámbricos, cuarentena y ataques DoS
- Reportar anonimización
- Programación de informes a varios destinatarios por grupo de informes con opciones de frecuencia flexibles
- Opciones de registro estándar y granular
- Exportar informes como HTML, PDF, Excel (XLS)
- Informe de auditoría de seguridad
- Informe de contenido de palabras clave web
- Almacenamiento en la nube de 7 días para informes de Central Firewall
- Reportar marcadores
- Visor de registro completo con personalización de retención por categoría
- todos los anteriores en una sola consola.

Especificación de almacenamiento de reportes

- Informes agregados de múltiples firewalls
- Guardar plantillas de informe personalizadas
- Programación de informes a varios destinatarios por grupo de informes con opciones de frecuencia flexibles
- Exportar informes en formato PDF, CFV o HTML
- Posibilidad de tener desde 30 días hasta 1 año de almacenamiento de datos por firewall en la consola Centralizada.
- Contar con el conector XDR/MTR
- Búsqueda y visualización de Syslog
- Informes bajo demanda.

On-Box Reporting

Cientos de informes en la caja con opciones de informes personalizados: paneles (tráfico, seguridad y cociente de amenazas del usuario), aplicaciones (riesgo de aplicaciones, aplicaciones bloqueadas, aplicaciones sincronizadas, motores de búsqueda,

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

servidores web, coincidencia de palabras clave web, FTP), redes y amenazas (IPS, ATP, inalámbrico, security heartbeat, sandstorm), VPN, correo electrónico, cumplimiento (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)

- Almacenamiento integrado en la serie XGS para un almacenamiento ilimitado de datos de registro para informes históricos
- Monitoreo de actividad actual: estado del sistema, usuarios en vivo, conexiones IPSec, usuarios remotos, conexiones en vivo, clientes inalámbricos, cuarentena y ataques DoS
- Anonimización de informes
- Programación de informes a varios destinatarios por grupo de informes con opciones de frecuencia flexibles
- Exportar informes como HTML, PDF, Excel (XLS)
- Personalización de la retención de registros por categoría
- Soporte de Syslog
- Visor de registros en vivo con todas las funciones con vista de columna y vista detallada con potentes opciones de filtro y búsqueda, ID de regla con hipervínculos y personalización de la vista de datos

Ítem
Solución Endpoint Server

Protección Web Application Firewall

- Proxy Reverso
- Motor de endurecimiento de URL con enlace profundo y prevención de recorrido de directorios
- Motor de endurecimiento de formularios
- Protección contra la inyección SQL
- Protección contra Cross-site scripting
- Debe contar con un motor de antivirus Dual, tener dos diferentes fuentes de definiciones
- Offloading cifrado HTTPS (SSL)
- Firma de cookies con firmas digitales
- Enrutamiento Path-based
- Soporte de Outlook anywhere
- Autenticación inversa (descarga) para la autenticación básica y basada en formularios para el acceso al servidor
- Abstracción de servidores virtuales y servidores físicos
- Balanceador de carga integrado para distribuir a los visitantes entre varios servidores
- Omita los cheques individuales de manera granular según sea necesario

BOLSA MERCANTIL DE COLOMBIA

Calle 113 N° 7 – 21 Torre A, Piso 15
Edificio Teleport Business Park
PBX: 629 2529
Bogotá D.C.
www.bolsamercantil.com.co – Documento público

	• Coincidir con las solicitudes de las redes de origen o las direcciones URL de destino especificadas • Soporte para operadores lógicos y/o • Ayudar a la compatibilidad con varias configuraciones e implementaciones no estándar • Opciones para cambiar los parámetros de rendimiento de WAF • Opción de límite de tamaño de escaneo • Permitir/Bloquear rangos IP • Soporte de Wildcards para paths de servidores • Anexar automáticamente un prefijo/sufijo para la autenticación. **Ítem** **Instalación e implementación** Se debe asignar un (1) Ingeniero Sistemas para la puesta (configuración de firewall) e instalación de los equipos en sede, previamente con estudio de la topología en detalle de la organización. Migración e Implementación de Ipv6 (dual stack). **Ítem** **Soporte y mesa de ayuda x 36 meses** Soporte técnico con línea de atención, email, generación de tickets **Ítem** **Soporte fabrica x 36 meses** Soporte 24/7 en ingles por medio de chat o tickets, por parte del fabricante, actualizaciones de funciones (Firmware), garantía de equipos (hardware) durante la vigencia del licenciamiento.
Empaque y rotulado (Aplica para productos)	Cajas con dispositivos de Hardware tipo Appliance que incluyan manual de usuarios y las especificaciones del producto.
Presentación (Aplica para productos)	*Unidad.*

Nota. *Las cantidades requeridas por ítem están incluidas en la Ficha Técnica de Negociación.*

YANNNY LUGDY CARRIÓN PEDRAZA
Directora Administrativa Y Financiera
Empresa Férrea Regional S.A.S.

Elaboró: Ronal Giovanni Quecan – Contratista Dirección Administrativa y Financiera
Darío Sotelo – Profesional Dirección Administrativa y Financiera