ESPECIFICACIONES TECNICAS

DESCRIPCIÓN	ESPECIFICACIONES TECNICAS MINIMAS
Marca	Especificar
Modelo	Especificar
Cantidad	1 (uno)
Características Generales	La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo
	Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos
	Las funcionalidades de protección de red que conforman la plataforma de seguridad, pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación
	La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7
	La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red
	Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP
	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding
	Los dispositivos de proteccion de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM)
	Los dispositivos de protección de red deben soportar DHCP Relay
	Los dispositivos de protección de red deben soportar DHCP Server
	Los dispositivos de protección de red deben soportar sFlow
	Los dispositivos de protección de red deben soportar Jumbo Frames
	Los dispositivos de protección de red deben soportar sub-interfaces Ethernet Lógicas
	Debe ser compatible con NAT dinámica (varios-a-1)
	Debe ser compatible con NAT dinámica (muchos-a-muchos)
	Debe soportar NAT estática (1-a-1)
	Debe admitir NAT estática (muchos-a-muchos)
	Debe ser compatibles con NAT estático bidireccional 1-a-1
	Debe ser compatibles con la traducción de puertos (PAT)
	Debe ser compatible con NAT Origen
	Debe ser compatible con NAT de destino

	Debe soportar NAT de origen y NAT de destino de forma simultanea
	Debe soportar NAT de origen y NAT de destino en la misma política
	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico
	Debe ser compatibles con NAT64 y NAT46
	Debe implementar el protocolo ECMP
	Debe soportar SD-WAN de forma nativa
	Debe soportar el balanceo de enlace hash por IP de origen
	Debe soportar el balanceo de enlace por hash de IP de origen y destino.
	Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces
	Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales
	Debe soportar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales
	Debe permitir el monitoreo de SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado de clúster, ataques y estadísticas de uso de las interfaces de red
	Enviar logs a sistemas de gestión externos simultáneamente
	Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL
	Debe soportar protección contra la suplantación de identidad (anti-spoofing)
	Implementar la optimización del tráfico entre dos dispositivos
	Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP)
	Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3)
	Soportar OSPF graceful restart
	Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red
	Debe soportar modo capa - 2(L2) para la inspección de datos y visibilidad en línea del trafico
	Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del trafico
	Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas
	Soportar la configuración de alta disponibilidad activo/pasivo y activo/activo: En modo transparente
	Soportar la configuración de alta disponibilidad activo/pasivo y activo/activo: En capa 3

	Soportar configuración de alta disponibilidad activo/pasivo y activo/activo: En la capa 3 y con al menos 3 dispositivos en el cluster.
	La configuración de alta disponibilidad debe sincronizar: Sesiones
	La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red
	La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad de VPN
	La configuración de alta disponibilidad debe sincronizar: Tablas FIB
	En modo HA (modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace
	Debe soportar la creación de sistemas virtuales en el mismo equipo
	Para una alta disponibilidad, el uso del clusters virtuales debe ser posibles, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos
	Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales
	La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso
	Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos)
Performance	Soportar al menos 1.5 millones de conexiones simultaneas
	Soportar al menos 55.000 nuevas conexiones por segundo
	Soportar al menos 11 Gbps Throughput de VPN IPSec
	Soportar al menos 2.000 túneles de VPN IP Sec site-to-site simultáneos
	Soportar al menos 15.000 túneles de clientes VPN IPSec simultáneos
	Soportar al menos 900 Mbps Throughput de VPN SSL
	Soportar al menos 500 clientes de VPN SSL simultáneos
	Soportar al menos 2.5 Gbps de throughput de IPS
	Soportar al menos 900 Mbps de throughput de Inspeccion SSL
	Soportar al menos 2.1 Gbps de throughput de Application Control
	Soportar al menos 1.6 Gbps de throughput de NGFW
	Soportar al menos 900 Mbps de Protection de Amenazas

Interfaces	Tener al menos 12 interfaces 1Gbps RJ45
	Tener al menos 2 interfaces 1Gbps SFP
	Tener al menos 2 interfaces 10 Gbps SFP+
	Tener al menos 1 interfaces USB
	Fuente Redundante
Requisitos Mínimos de Funcionalidad	
Control por Política de Firewall	Debe soportar controles de zona de seguridad
	Debe contar con políticas de control por puerto y protocolo
	Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones
	Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad
	Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad
	Además de las direcciones y servicios de destino, los objetos de servicio de internet deben poder agregarse directamente a las políticas de firewall
	Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenSrack, Cisco ACI, Nuage y Kubernetes
	Debe soportar el protocolo estándar de la industria VXLAN
	La solución debe permitir la implementación sin asistencia de SD-WAN
	En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN
	La solución debe soportar la integración nativa como solución de sandboxing, protección de correo electrónico, cache y Web application firewall
Control de Aplicación	Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo
	Detección de miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, video, Proxy, mensajería instantánea, compartición de archivos, correo electrónico
	Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, Skype, Facebook chat, Gmail chat, WhatsApp, 4shared, Dropbox, Google Drive, Skydrive, db2, mysql, Oracle, active directory, kerberos, Idap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, Evernote, Google-docs.
	Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con

	tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor.
	Para trafico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante
	Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas
	Actualización de la base de firmas de la aplicación en forma automática
	Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos
	Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no solo en aplicaciones conocidas
	Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante.
	El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos
	Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc.) permitiendo granularidad de control/reglas para el mismo
	Debe permitir la diferenciación de trafico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo
	Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat pero impedir la llamada de video
	Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo
	Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Base, Network Protocol, etc.)
	Debe ser posibles crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación
	Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de aplicación
Prevención de Amenazas	Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo.
	Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware)
	Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no

	exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante.
	Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad
	Debe 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 elementos
	Debe permitir el bloqueo de vulnerabilidades y exploits conocidos
	Debe incluir la protección contra ataques de denegación de servicio
	Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo
	Debe tener los siguientes mecanismos de inspección de IPS: Análisis para detectar anomalías de protocolo
	Debe tener los siguientes mecanismos de inspección de IPS: Desfragmentación IP
	Debe tener los siguientes mecanismos de inspección de IPS: Re ensamblado de paquetes TCP
	Debe tener los siguientes mecanismos de inspección de IPS: Bloqueo de paquetes con formato incorrecto (malformed packets)
	Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.
	Detectar y bloquear los escaneos de puertos de origen
	Bloquear ataques realizados por gusanos (worms) conocidos
	Contar con firmas específicas para la mitigación de ataques DoS y DDoS
	Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow)
	Debe poder crear firmas personalizadas en la interfaz gráfica del producto
	Identificar y bloquear la comunicación con redes de bots
	Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo
	Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación
	Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos
	Los eventos deben identificar el país que origino la amenaza
	Debe incluir protección contra virus HTML y Javascript, software espía (spyware) y gusanos (worms)
	Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP

	Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basado en usuario, grupos de usuarios, origen, destino, zonas de seguridad
	En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (Laptop, Desktop, etc.) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles
Filtrado de URL	Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o periodo determinado (día, mes, año, día de la semana, hora)
	Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quien está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explicito
	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL
	Debe tener la base de datos de URLs en cache en el equipo o en la nube del fabricante, evitando retrasos de comunicación/validación de direcciones URL
	Tener por lo menos 75 categorías de URL
	Debe tener la funcionalidad de exclusión de URLs por categoría
	Permitir página de bloqueo personalizada
	Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio)
Identificación de Usuarios	Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quien está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directory y base de datos local
	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas/control basados en usuarios y grupo de usuarios
	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc.
	Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad/control basados en usuarios y grupos de usuarios

	Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la política/control basados en usuarios y grupos de usuarios
	Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo)
	Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios
	Debe de implementar la creación de grupos de usuarios en el firewall, basada en atributos de LDAP/AD
QoS	Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto en audio como de video streaming
	Soportar la creación de políticas QoS y Traffic Shaping por dirección de origen
	Soportar la creación de políticas QoS y Traffic Shaping por dirección de destino
	Soportar la creación de políticas QoS y Traffic Shaping por usuario y grupo
	Soportar la creación de políticas QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube
	Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto
	En QoS debe permitir la definición de tráfico con ancho de banda garantizada
	En QoS debe permitir la definición de tráfico con máximo ancho de banda
	En QoS debe permitir la definición de colas de prioridad
	Soportar marcación de paquetes DiffServ, incluso por aplicación
	Soportar la modificación de los valores de DSCP para DiffServ
	Soportar priorización de trafico utilizando información de Tipo de Servicio (Type of Service)
	Debe soportar QoS (traffic shaping) en las interface agregadas o redundantes
Filtro de Datos	Permite la creación de filtros para archivos y datos predefinidos
	Los archivos deben ser identificados por tamaño y tipo
	Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones

	Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos
	Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de ese tipo de archivos
	Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares
Geo Localización	Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto país/países
	Debe permitir la visualización de los países de origen y destino en los registros de acceso
	Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas
VPN	Soporte VPN de sitio-a-sitio y cliente-a-sitio
	Soportar VPN IPSec
	Soportar VPN SSL
	La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512
	La VPN IPSec debe ser compatible con Diffir-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14
	La VPN IPSec debe ser compatible con Internet Key Exchanfe (IKEv1 y v2)
	La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard)
	Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall
	Soportar VPN par IPv4 e IPv6, asi como el tráfico IPv4 dentro de túneles IPv6 IPSec
Licenciamiento, Garantía	El plazo de duración de los servicios y garantía de Hardware será de 36 meses, en la modalidad de 24x7 incluyendo el reemplazo de partes y/o del equipo en caso de fallas no atribuibles a la convocante. La garantía deberá ser expedida por el fabricante del equipo.
Soporte Técnico	Por lo menos 2 (dos) contratos de servicios que demuestren su capacidad de brindar el servicio 24x7 con soporte técnico especializado capaz de dar asistencia remota en línea
Idoneidad, Instalación, Configuración	El oferente deberá montar, instalar y configurar el equipo; dejando totalmente operativo todos los servicios con que cuenta la convocante