Ítem 15. Router principal de distribución

Descripción	Especificar
Marca	Especificar
Fabricante	Especificar
Modelo y/o Número de Parte	Especificar
Origen / Procedencia	Especificar
Cantidad	01 (uno)
Características	**Mínimo Exigido**
Tipo	Next Generation Firewall (NGFW)
Interfaces Requeridas	2 x SFP+ (10GbE) con sus respectivos modulos
	8 x SFP con sus respectivos modulos
	16 x RJ-45 (GbE)
	Puertos de administración: 1 x Puerto de consola, 2 x USB 3.0, 1 x Administración RJ-45 Ethernet, 1 x HA RJ45
Características de desempeño	La Solución de Firewall debe permitir un desempeño ≥ 20 Gbps
	Rendimiento de VPN IPsec: ≥ 6 Gbps
	Túneles Ipsec : ≥ 8.000
	Rendimiento de Antivirus: ≥ 4.8 Gbps
	Rendimiento de IPS ≥ 10 Gbps
	Rendimiento de NGFW (tráfico HTTP, control de Aplicaciones, e IPS habilitado) ≥ 5.5 Gbps
	Rendimiento de Protección contra amenazas (tráfico HTTP, Control de Aplicaciones, IPS, AV y filtrado URL habilitado ≥ 3 Gbps
	Sesiones concurrentes: ≥ 2 millones
	Nuevas sesiones / seg: ≥ 140.000
	Políticas de Firewall: ≥ 20.000
	Número de instancias virtuales soportados ≥: 30
	Inspección SSL TLSv 1.3 soportado
	Factor de forma: ≤ 2RU
	AC Power: al menos 2 fuentes de alimentación 220Vac 50Hz.

Características de Hardware	Almacenamiento interno: ≥ 8 GB y adicionalmente deberá permitir la ampliación de esta capacidad con unidades SSD de 1.8 TB o superior
	Rango de temperatura de operación: 0°C a +40°C o rango superior
Seguridad de datos	La solución propuesta debe tener control de la transferencia de archivos en función de su tipo, tamaño y nombre
	La solución propuesta debe contar con identificación del protocolo de archivos, incluyendo HTTP, FTP, SMTP, POP3 y SMB
	La solución propuesta debe contar con identificación de firmas y sufijos de archivos para más de 100 tipos de archivos
	La solución propuesta debe contar con filtrado de contenidos para los protocolos HTTP-GET, HTTP-POST, FTP y SMTP
	La solución propuesta debe contar con identificación de MI y auditoría del comportamiento de la red
	La solución propuesta debe filtrar los archivos transmitidos por HTTPS mediante el proxy SSL y SMB
Firewall	La solución propuesta debe soportar los siguientes modos de funcionamiento: NAT/ruta, transparente (bridge) y mixto
	La solución propuesta debe soportar objetos de política: predefinidos, personalizados, políticas agregadas, agrupación de objetos
	La solución propuesta debe soportar políticas de seguridad basada en la aplicación, la función y la geolocalización
	La solución propuesta debe soportar puertas de enlace a nivel de aplicación y soporte de sesiones: MSRCP, PPTP, RAS, RSH,
	SIP, FTP, TFTP, HTTP, dcerpc, dns- tcp, dns-udp, H.245 0, H.245 1, H.323
	La solución propuesta debe tener soporte de NAT y ALG: NAT46, NAT64, NAT444, SNAT, DNAT, PAT,
	Full Cone NAT, STUN
	La solución propuesta debe contar con configuración de NAT: por política y tabla central de NAT
	La solución propuesta debe soportar VoIP: SIP/H.323/SCCP NAT traversal, RTP pin holing
	La solución propuesta debe contar con vista de la gestión global de las políticas
	La solución propuesta debe contar con inspección de redundancia de políticas de seguridad, grupo de políticas, reversión de la configuración de políticas, políticas agregadas
	La solución propuesta debe contar con asistente de políticas para facilitar el despliegue de políticas detalladas
	La solución propuesta debe contar con análisis de políticas y limpieza de políticas inválidas
	La solución propuesta debe contar con política global de DNS
	La solución propuesta debe contar con horarios: únicos y recurrentes

	La solución propuesta debe contar con apoyo a la importación y exportación de políticas
Conectividad y sistema de ruteo	La solución propuesta debe soportar enrutamiento dinámico (OSPF, BGP, RIPv2).
	La solución propuesta debe soportar enrutamiento estático y por políticas.
	La solución propuesta debe soportar rutas controladas por la aplicación.
	La solución propuesta debe soportar DHCP, NTP, servidor DNS y proxy DNS integrados
	La solución propuesta debe soportar modo Tap - se conecta al puerto SPAN
	La solución propuesta debe soportar los siguientes modos de interfaz: sniffer, puerto agregado, loopback, VLANs (802.1Q y Trunking)
	La solución propuesta debe soportar conmutación y enrutamiento de capa 2 y capa 3
	La solución propuesta debe soportar multidifusión (PIM-SSM)
	La solución propuesta debe soportar el despliegue de cable virtual (capa 1) transparente en línea
	La solución propuesta debe soportar VPN Ipsec y sus siguientes funcionalidades:
	Modo IPsec Fase 1: modo de protección de ID agresivo y principal
	Opciones de aceptación de pares: cualquier ID, ID específico, ID en el grupo de usuarios de acceso telefónico
	Soporta IKEv1 e IKEv2 (RFC 4306)
	Método de autenticación: certificado y clave precompartida
	Soporte de configuración del modo IKE (como servidor o cliente)
	DHCP sobre IPsec
	Caducidad de la clave de cifrado IKE configurable, frecuencia de mantenimiento de la vida de la NAT
	Fase 1/Fase 2 Propuesta de encriptación: DES, 3DES, AES128, AES192, AES256
	Autenticación de la propuesta de la fase 1/fase 2: MD5, SHA1, SHA256, SHA384, SHA512
	IKEv1 soporta los grupos DH 1,2,5,19,20,21,24
	IKEv2 soporta los grupos DH 1,2,5,14,15,16,19,20,21,24
	XAuth como modo de servidor y para usuarios de acceso telefónico
	Detección de pares muertos
	Detección de repeticiones
	Autokey keep-alive para la Fase 2 SA
	La solución propuesta debe soportar la compatibilidad con el ámbito de VPN IPsec: permite múltiples inicios de sesión de VPN SSL personalizados asociados a grupos de usuarios (rutas de URL, diseño)

VPN	La solución propuesta debe soportar las opciones de configuración de VPN IPsec: basadas en rutas o en políticas
	La solución propuesta debe soportar los siguientes modos de implementación de VPN IPsec: puerta de enlace a puerta de enlace, malla completa, hub-and- spoke, túnel redundante, terminación de VPN en modo transparente
	La solución propuesta debe soportar el inicio de sesión único evita los inicios de sesión simultáneos con el mismo nombre de usuario
	La solución propuesta debe tener limitación de usuarios concurrentes en el portal SSL
	La solución propuesta debe tener un módulo de reenvío de puertos SSL VPN cifra los datos del cliente y los envía al servidor de aplicaciones
	La solución propuesta debe admitir clientes que funcionan con iOS, Android y Windows XP/Vista, incluido el sistema operativo Windows de 64 bits
	La solución propuesta debe tener comprobación de la integridad del host y del sistema operativo antes de las conexiones del túnel SSL
	La solución propuesta debe tener comprobación de host MAC por portal
	La solución propuesta debe tener la opción de limpieza de la caché antes de finalizar la sesión de SSL VPN
	La solución propuesta debe tener modo cliente y servidor L2TP, L2TP sobre IPsec y GRE sobre IPsec
	La solución propuesta debe poder ver y gestionar las conexiones IPsec y SSL VPN
	La solución propuesta debe poder realizar PnPVPN
Clientes SSL VPN	Deberá incluir al menos 6 licencias de clientes SSL VPN y soportar 3500 usuarios con licencias adicionales en caso de ser necesario.
Control de aplicaciones	Debe poseer una base de datos de más 6.000 aplicaciones diferentes verificables por medio de la interface gráfica de un equipo de la Línea ofertada (que no sea superior al modelo ofertado), donde las aplicaciones que pueden filtrarse por nombre, categoría, subcategoría, tecnología y riesgo. Deberán poder ser actualizadas vía web
	Debe tener aplicación que contenga una descripción, factores de riesgo, dependencias, puertos típicos utilizados y URLs para referencias adicionales
	Debe soportar las siguientes acciones: bloquear, restablecer la sesión, monitoreo y traffic shapping
	Debe proporcionar supervisión y estadísticas multidimensionales para las aplicaciones en la nube, incluyendo la categoría de riesgo y las características
	La solución propuesta debe tener túneles de ancho de banda máximo/garantizado o base de IP/usuario

Traffic Shaping / QoS	La solución propuesta debe tener asignación de túneles basada en el dominio de seguridad, la interfaz, la dirección, el usuario/grupo de usuarios, el servidor/grupo de servidores, la aplicación/grupo de aplicaciones, TOS, VLAN
	La solución propuesta debe asignar el ancho de banda por tiempo, por prioridad o por reparto equitativo del ancho de banda
	La solución propuesta debe soportar Tipo de Servicio (TOS) y Servicios Diferenciados (DiffServ)
	La solución propuesta debe tener asignación prioritaria del ancho de banda restante
	La solución propuesta debe tener máximas conexiones simultáneas por IP
	La solución propuesta debe poder asignar el ancho de banda en función de la categoría de la URL
	La solución propuesta debe limitar el ancho de banda retrasando el acceso para el usuario o la IP
	La solución propuesta debe realizar la limpieza automática de la caducidad y limpieza manual del tráfico utilizado por el usuario
Carga del servidor	La solución propuesta debe soportar hashing ponderado, conexión mínima ponderada y round-robin ponderado
	La solución propuesta debe soportar protección de la sesión, persistencia de la sesión y control del estado de la sesión
	La solución propuesta debe contar con comprobación del estado del servidor, supervisión de la sesión y protección de la sesión
Server load sharing	La solución propuesta debe contar con equilibrio de la carga
	de los enlaces bidireccionales
	La solución propuesta debe contar con equilibrio de la carga de los enlaces salientes: enrutamiento basado en políticas, incluyendo ECMP, tiempo, ponderado y enrutamiento ISP integrado; detección activa y pasiva de la calidad del enlace en tiempo real y selección de la mejor ruta
	La solución propuesta debe soportar el equilibrio de carga de los enlaces entrantes y ser compatible con SmartDNS y la detección dinámica
	La solución propuesta debe soportar la conmutación automática de enlaces en función del ancho de banda, la latencia, el jitter, la conectividad, la aplicación, etc.
	La solución propuesta debe soportar la inspección del estado del enlace con ARP, PING y DNS
	La solución propuesta debe soportar la identificación de aplicaciones para el tráfico cifrado SSL
	La solución propuesta debe contar con habilitación de IPS para el tráfico cifrado SSL
	La solución propuesta debe contar con habilitación de AV para el tráfico cifrado SSL

Descifrado SSL	La solución propuesta debe contar con filtro de URL para el tráfico cifrado SSL
	La solución propuesta debe soportar lista blanca de tráfico cifrado SSL
	La solución propuesta debe soportar el modo de descarga del proxy SSL
	La solución propuesta debe soportar la identificación de aplicaciones, DLP, sandbox IPS, AV para el tráfico descifrado del proxy SSL de SMTPS/POP3S/IMAPS
Autenticación	Debe soportar base de datos local de usuarios
	Debe soportar la autenticación remota de usuarios: TACACS+, LDAP, Radius, Active Directory
	Debe soportar el inicio de sesión único: Windows AD
	Debe soportar la autenticación de 2 factores: Soporte de terceros, servidor de tokens integrado con físico y SMS
	Debe soportar políticas basadas en usuarios y dispositivos
	Debe soportar la sincronización de grupos de usuarios basada en AD y LDAP
	Debe tener soporte para 802.1X, SSO Proxy
	Debe contar con WebAuth: personalización de la página, prevención de grietas forzadas, soporte de IPv6
	Debe tener autenticación basada en la interfaz
	Debe contar con ADSSO sin agente (sondeo AD)
	Debe poder utilizar la sincronización de la autenticación basada en el monitor SSO
	Debe admitir la autentificación de usuarios basada en IP y en MAC
	Debe soportar que el servidor Radius emite la política de seguridad del usuario a través de un mensaje CoA
Antivirus	La solución propuesta debe tener actualizaciones de firmas manuales, automáticas, push y pull
	La solución propuesta debe añadir o eliminar manualmente la firma MD5 en la base de datos AV
	La solución propuesta debe de soportar firma MD5 cargando a la nube sandbox, y añadiendo o eliminando manualmente en la base de datos local
	La solución propuesta debe de soportar antivirus basado en flujo: los protocolos incluyen HTTP, SMTP, POP3, IMAP, FTP/SFTP, SMB
	La solución propuesta debe soportar análisis de virus de archivos comprimidos
Administración	La solución propuesta debe tener acceso de gestión: HTTP/HTTPS, SSH, telnet, consola
	La solución propuesta debe de tener integración de sistemas: SNMP, syslog, alianzas
	La solución propuesta debe tener despliegue rápido: Auto instalación USB, ejecución local y remota de scripts

	La solución propuesta debe contar con un tablero de control dinámico en tiempo real y widgets de seguimiento de la información.
	La solución propuesta debe tener soporte de idiomas: inglés o español como mínimo
Estadísticas y control	Debe poder tener instalaciones de registro: almacenamiento local 8 GB o superior; deberá permitir extender a 6 meses de almacenamiento de registros con almacenamiento de expansión (disco duro SSD), servidor syslog
	Debe tener el registro cifrado e integridad de los registros con carga programada de registros por lotes de administrador de Logs
	Debe tener el registro fiable mediante la opción TCP (RFC 3195)
	Debe tener los registros de tráfico detallados: reenviados, sesiones violadas, tráfico local, paquetes no válidos, URL, etc.
	Debe tener registros completos de eventos: auditorías de la actividad del sistema y de la administración, enrutamiento y redes, VPN, autenticaciones de usuarios, eventos relacionados con Wi-Fi
	Debe tener la opción de resolución de nombres de IP y puertos de servicio
	Debe tener la opción de formato de registro de tráfico breve
	Debe contar con al menos tres informes predefinidos: Informes de seguridad, de flujo y de red
	Debe permitir informes definidos por el usuario
	Debe tener los informes para exportar en PDF, Word y HTML por correo electrónico y FTP
Estadísticas y control	Debe soportar las estadísticas y seguimiento de aplicaciones, URL y eventos de amenazas
	Debe soportar las estadísticas y análisis de tráfico en tiempo real
	Debe proporcionar la información del sistema, como la sesión simultánea, el CPU, la memoria y la temperatura
	Debe proporcionar las estadísticas y supervisión del tráfico iQOS, supervisión del estado de los enlaces
	Debe tener el soporte de colección de información del tráfico y reenvío vía Netflow (v9.0)
Filtrado de URLs	La solución propuesta debe de contar con inspección de filtrado web basada en el flujo
	La solución propuesta debe tener filtrado web definido manualmente basado en la URL, el contenido web y el encabezado MIME
	La solución propuesta debe tener filtrado web dinámico con base de datos de categorización en tiempo real basada en la nube: más de 140 millones de URL con 64 categorías (8 de ellas relacionadas con la seguridad)
	Anulación del perfil de filtrado web: permite al administrador asignar temporalmente diferentes perfiles al usuario/grupo/IP

	Filtro web de categorías locales y anulación de la clasificación de categorías
	Admite la lista de direcciones permitidas y la lista de bloqueadas
IPS	Debe contar con detección de anomalías en los protocolos, detección basada en la velocidad, firmas personalizadas, actualizaciones de firmas manuales o automáticas push o pull, con enciclopedia de amenazas integrada
	Debe contar con acciones del IPS: por defecto, supervisar, bloquear, restablecer (IP del atacante o IP de la víctima, interfaz de entrada) con tiempo de caducidad
	Debe contar con opción de registro de paquetes
	Debe incluir una base de datos de firmas de IPS con por lo menos
	12.000 firmas verificables en la interface gráfica de un equipo de la Línea ofertada (que no sea superior al ofertado), y que pueden ser ampliables vía web
	Debe contar con selección basada en filtros: gravedad, objetivo, sistema operativo, aplicación o protocolo
	Debe contar exención de IP de firmas específicas de IPS
	Debe contar con modo sniffer IDS
	Debe Protección DoS basadas en la tasa de IPv4 e IPv6 con ajustes de umbral contra la inundación de TCP Syn, el escaneo de puertos TCP/UDP/SCTP, el barrido ICMP, la inundación de sesiones TCP/UDP/ SCIP/ICMP (origen/destino)
	Debe contar con bypass activo con interfaces de bypass
	Debe contar con configuración de prevención predefinida
	Debe poder realizar captura de paquetes de amenazas IPS (sólo con almacenamiento de expansión)
Alta disponibilidad	El equipo propuesto, debe soportar operación en Alta Disponibilidad con interfaces redundantes del tipo Heart beat
	El equipo propuesto debe soportar los modos Activo/Pasivo, Activo/Activo
	El equipo propuesto debe soportar la sincronización de sesiones independientes
	El equipo propuesto debe poseer Interfaz de gestión reservada para HA
	El equipo propuesto debe soportar la conmutación por error:
	Monitorización de puertos, enlaces locales y remotos
	Conmutación por error de estado
	Recuperación en menos de un segundo
	Notificación de fallos
	La solución propuesta debe soportar las siguientes opciones de despliegue:
	HA con agregación de enlaces
	Malla completa HA
	HA geográficamente dispersa

Reputación IP	El equipo propuesto debe identificar y filtrar el tráfico procedente de las direcciones IPs de riesgo, como hosts de botnets, spammers, nodos Tor, hosts vulnerados y ataques de fuerza bruta.
	El equipo propuesto debe soportar el registro, eliminación de paquetes o bloqueo de diferentes tipos de tráfico IP de riesgo
	El equipo propuesto debe soportar la actualización periódica de la base de datos de firmas de reputación IP
Sandbox	La solución propuesta debe soportar la subida de los archivos maliciosos a la sandbox de la nube para su análisis
	La solución propuesta debe soportar protocolos como HTTP/HTTPS, POP3, IMAP, SMTP, FTP y SMB
	La solución propuesta debe soportar tipos de archivos como PE, ZIP, RAR, Office, PDF, APK, JAR,
	SWF y Script
	La solución propuesta debe tener dirección de la transferencia de archivos y control del tamaño de estos
	Proporcionar un informe completo de análisis del comportamiento de los archivos maliciosos
	Intercambio de información sobre amenazas a nivel mundial, bloqueo de amenazas en tiempo real
	La solución propuesta debe soportar el modo solo detección sin subir archivos
	Configuración de la lista de URLs permitidas/bloqueadas
Prevención de Command and Control de botnet	Debe descubrir el host de la red de bots de la intranet mediante la supervisión de las conexiones de C&C y bloquear otras amenazas avanzadas como la red de bots y el ransomware
	Debe actualizar periódicamente las direcciones de los servidores de la red de bots
	Debe tener prevención para IP y el dominio del C&C
	Debe admitir la detección de tráfico TCP, HTTP y DNS
	Debe permitir lista de permisos y bloqueos basada en la dirección IP o el nombre de dominio
	Debe soportar la detección de DNS sinkhole y DNS tunneling
	Debe soportar la detección de la DGA
Endpoint Control	Debe tener soporte para identificar la IP del punto final, la cantidad de puntos finales, el tiempo en línea, el tiempo fuera de línea y la duración en línea
	Debe soportar 10 sistemas operativos incluyendo Windows, iOS, Android, etc.
	Debe admitir la consulta basada en la IP, la cantidad de puntos finales, la política de control y el estado, etc.
	Debe soportar la identificación de la cantidad de puntos finales a los que se accede a través de la capa 3, el registro y la interferencia en la IP sobrepasada
	Debe soportar la visualización de la página de redireccionamiento después de la operación de interferencia personalizada

	Debe admitir operaciones de bloqueo en IP sobrepasadas
	Debe soportar la visualización de la página de redireccionamiento después de la operación de interferencia personalizada
	Debe admitir operaciones de bloqueo en IP sobrepasadas
	Debe soportar la identificación de usuarios y control del tráfico para los servicios de escritorio remoto de Windows Server
Defense Attack	La solución propuesta debe de contar con defensa contra ataques de protocolos anormales
	Debe contar con defensa contra ataques de inundación, incluyendo inundación ICMP, inundación UDP, inundación de consulta DNS, inundación de consulta DNS recursiva, inundación de respuesta DNS, inundación SYN
	Debe contar con defensa contra la falsificación de ARP y la falsificación de ND
	Debe contar con defensa contra el escaneo y la suplantación de identidad, incluida la suplantación de direcciones IP, el barrido de direcciones IP y el escaneo de puertos
	Debe contar con defensa DoS/DDoS, incluyendo el ataque de ping de la muerte, el ataque de lágrima, el fragmento IP, la opción IP, el ataque pitufo o frágil, el ataque de tierra, el paquete ICMP grande, el ataque WinNuke
	Debe contar con lista de permisos para la dirección IP de destino
ZTNA	Debe soportar el acceso de usuarios basado en el principio ZTNA con licencias adicionales en caso de ser requerido
	Debe soportar configuración de políticas Zero Trust basado en etiquetas ZTNA y recursos de aplicación, con protección de seguridad y seguridad de dato
	Debe soportar administración de recursos de aplicación y configuración de recursos de aplicación basado en nombre de dominio
	Etiquetas ZTNA debe soportar password de cuentas y estado de terminal
	Debe soportar publicación de aplicación, y despliegue de aplicaciones autorizadas para usuarios terminales sobre portal ZTNA
	Debe soportar transición suave desde una SSL VPN a una solución ZTNA
	Debe soportar administración ZTNA centralizada incluyendo monitoreo y estadísticas de datos
Nube	Debe poseer una plataforma en la nube que permita el registro del equipo, para monitoreo remoto y estadísticas con una antigüedad mínima de 7 días.

Licenciamiento y actualizaciones	El licenciamiento de todas las funcionalidades debe ser ilimitado en cuanto a usuarios, cajas de correo, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La vigencia de las actualizaciones para los servicios de IPS, Antivirus (AV), Filtrado URL, QoS, Reputación IP, C2, Anti-Spam, y Sandbox debe proveerse por el periodo mínimo de un (1) año. El servicio de conectividad de la red deberá continuar en funcionamiento al término de dicho periodo de vigencia de las actualizaciones.
Instalación	Se requiere la instalación y montaje de la solución. Se deberán realizar todas las configuraciones en el equipo conforme requerimientos de la convocante, asegurando que el equipo esté listo para usar
ISO	ISO 9001, ISO14001, ISO27001 o similares de la marca ofertada, Certificación ICSA labs.
Certificación	IPV6 ready Phase 1 y Phase 2, Cumplimiento CVE
Autorización	El oferente deberá ser representante o distribuidor autorizado de los bienes ofertados. Se deberá presentar una Autorización del Fabricante para presentar oferta. Esta Autorización podrá ser reemplazada por la documentación vigente que pruebe fehacientemente que el Oferente es Representante o Distribuidor y Servicio Técnico Autorizado de la marca del bien ofertado.
Garantía de fábrica	El equipo ofertado deberá contar con una garantía de fábrica de al menos dos (2) años. Esta garantía permite el acceso a las actualizaciones de firmware del equipo sin costo para la convocante durante el periodo de garantía.
Técnicos certificados	El oferente deberá contar con al menos 2 (dos) técnicos certificados en fábrica para la instalación y configuración de los equipos ofertados (podrán ser subcontratistas)
Documentaciones	Catálogos y Especificaciones originales del Equipo Ofertado. Se considerarán catálogos y especificaciones originales del equipo ofertado todo material que pueda descargarse de la web del fabricante.