Comarb
COMISIÓN ARBITRAL DEL CONVENIO MULTILATERAL

CONCURSO DE PRECIOS N° 6/2021

PLIEGO DE BASES Y CONDICIONES GENERALES

1- Normativa aplicable. Para la presente contratación, rigen las disposiciones contenidas en el Pliego de Condiciones Generales, y en el REGLAMENTO PARA LA CONTRATACIÓN DE BIENES, OBRAS Y SERVICIOS aprobado por la COMISIÓN ARBITRAL DEL CONVENIO MULTILATERAL 18.08.77, vigente al momento de inicio del procedimiento de contratación.

2- Objeto. La presente contratación tiene por objeto la adquisición de una Solución de Next Generation Firewall hardware appliance y 75 licencias FortiClient Endpoint Agent para los accesos remotos por VPN, según el Anexo “A” Especificaciones Técnicas, que se adjunta al presente Pliego.

3- Lugares y Plazos. Tanto la recepción de las ofertas como el acto de apertura de los sobres se realizará en la sede de la Comisión Arbitral, departamento de Recursos Humanos y Materiales, sito en Esmeralda 672 piso 3°, Ciudad Autónoma de Buenos Aires.

La recepción de las ofertas será entre las 10:00 y las 11:00 hs del día 8 de junio de 2021.

La apertura de las ofertas se realizará a las 11:15 hs del día 8 de junio de 2021.

4- Requisitos formales para la presentación de las ofertas. Las ofertas deberán cumplir los siguientes requisitos formales:

a. Redactadas en idioma nacional en procesador de texto y/o a máquina, en formularios con membrete de la persona o firma comercial.

b. Firmadas en todas sus hojas por el oferente, representante legal o apoderado debidamente acreditado.

c. Enmiendas y raspaduras en partes esenciales, debidamente salvadas.

d. Todas las fojas (incluida la documentación y folletería que se acompañe) debidamente compaginadas, numeradas y abrochadas o encarpetadas.

e. Por duplicado y presentadas en sobre o paquete cerrado con indicación de número de contratación, fecha y hora de apertura.

f. Se deberá adjuntar toda la documentación presentada en un PEN DRIVE.

g. Tanto las ofertas como los presupuestos, facturas y remitos, deberán cumplir con las normas impositivas y previsionales vigentes.

Las infracciones, errores u omisiones no esenciales no invalidarán la oferta, sin perjuicio de las sanciones que pudiesen corresponder al infractor.

5- Información y documentación que deberá presentarse junto con la Oferta. Se estará a lo dispuesto por el art. 19 del Reglamento para la contratación de bienes, obras y servicios de la Comisión Arbitral. A tal efecto, en el momento de presentar la oferta, se deberá proporcionar la información que en cada caso se indica. En todos los casos deberá acompañarse la documentación respaldatoria y las copias de escrituras, actas, poderes y similares deberán estar autenticadas por Escribano Público:

a- Personas humanas y apoderados:

1- Nombre completo, nacionalidad, profesión, domicilio real y constituido, tipo y número de documento de identidad.

2- Clave Única de Identificación Tributaria (C.U.I.T) y condición frente al Impuesto al Valor Agregado (IVA) y Regímenes de Retención vigentes.

b- Personas jurídicas:

1- Razón Social, domicilio legal y constituido, lugar y fecha de constitución y datos de inscripción registral.

2- Clave Única de Identificación Tributaria (C.U.I.T) y condición frente al Impuesto al Valor Agregado (IVA) y Regímenes de Retención vigentes

c- En todos los casos, con la oferta deberá acompañarse:

1- Copia autenticada del poder, en caso de que quien suscriba la oferta y el resto o parte de la documentación no sea la persona humana o el representante legal respectivo.

2- Declaración Jurada de que ni el oferente, ni los integrantes de los órganos de administración y fiscalización en su caso, se encuentran incursos en ninguna de las causales de inhabilidad para contratar con la Comisión Arbitral.

3- Certificado de inscripción en AFIP, donde se acredite la actividad que desarrolla y cuando corresponda, certificación de condición como "Agente de Retención" y/o certificado de exclusión de retención (Impuesto al valor Agregado, Impuesto a las Ganancias, Sistema Único de Seguridad Social -SUSS-).

4- Constancia de inscripción en el Impuesto a los Ingresos Brutos.

6- Contenido de la oferta. La presentación de las ofertas deberán contemplar la totalidad de los puntos solicitados bastando la falta de alguno de estos para que se desestime la oferta general. La presentación de la oferta significa de parte del oferente el pleno conocimiento del Reglamento de Contrataciones de Bienes, Obras y Servicios de la Comisión Arbitral y la aceptación de las cláusulas que rigen la contratación.

La oferta especificará por cada ítem en relación a la unidad solicitada o su equivalente: precio unitario, precio total; en dólares estadounidenses, con I.V.A. Incluido. El total general de la propuesta será expresado en letras y números con I.V.A. Incluido.

7- Plazo de mantenimiento de la Oferta. El plazo de mantenimiento de la oferta será de siete (7) días, en un todo de acuerdo a lo reglado por el art. 23 del Reglamento para la Contratación de Bienes, Obras y Servicios de la Comisión Arbitral.

8- Efectos de la presentación de la oferta. La presentación de la oferta, importa de parte del oferente el pleno conocimiento de toda la normativa que rige el llamado a contratación, la evaluación de todas las circunstancias, la previsión de sus consecuencias y la aceptación en su totalidad de las bases y condiciones estipuladas, sin que pueda alegar en adelante el oferente su desconocimiento.

9- Análisis de las Ofertas. Las ofertas serán evaluadas por un Comité de Preadjudicación, cuyos integrantes serán designados por el contratante, quienes emitirán el informe de evaluación de las ofertas.

10- Adjudicación. Se adjudica el Concurso de Precios al oferente cuya propuesta se ajuste a lo establecido en el Pliego de Bases y Condiciones Generales, sea satisfactoria la documentación presentada y su oferta económica haya sido evaluada como la más conveniente. Dicha adjudicación se efectuará por monto global.

11- Plazo de entrega. El plazo de entrega será a coordinar con el adjudicatario una vez recibida la orden de compra.

12- Pagos. El pago se efectuará con transferencia bancaria de Banco Nación Argentina Sucursal Plaza de Mayo, en pesos argentinos, una vez recibidos la

totalidad de los ítems y la factura correspondiente. Se tomará el tipo de cambio oficial del Banco Nación Argentina al día anterior a la fecha de pago de la factura.

13- Penalidades y Sanciones. Será de aplicación lo dispuesto por el Capítulo XII del Reglamento para la Contratación de Bienes, Obras y Servicios de la Comisión Arbitral.

14- Impuesto al Valor Agregado. A los efectos de la aplicación del Impuesto al Valor Agregado, la Comisión Arbitral reviste el carácter de consumidor final.

15- Constitución de domicilio. A todos los efectos legales, el oferente deberá constituir domicilio legal en la Ciudad Autónoma de Buenos Aires.

16- Garantía. 1 (un) año.

17- Consultas. A Fernanda González mail fgonzalez@ca.gob.ar

Comarb
COMISIÓN ARBITRAL DEL CONVENIO MULTILATERAL

CONCURSO DE PRECIOS N° 6/2021

ANEXO A ESPECIFICACIONES TÉCNICAS

1 Firewall de Nueva Generación – Fortigate 80F

Descripción

- Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la información perimetral que incluye filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPSec y SSL, IPS, prevención contra amenazas de virus, spyware y malware "Zero Day", bien como controles de transmisión de datos y acceso a internet componiendo una plataforma de seguridad integrada y robusta.
- Por plataforma de seguridad se entiende hardware y software integrados de tipo appliance.
- El soporte y licencias ofrecido por el fabricante de la solución tienen que tener vigencia de 2 (dos) años en la modalidad 7x24.
- En relación al RMA el fabricante debe contar con depósito de partes, o equipos completos con presencia local en el país y poder ofrecer mínimamente reemplazo de partes en el próximo día hábil, conocido por las siglas en inglés NBD (next business day), para poder garantizar el funcionamiento de la solución.
- El fabricante debe estar en el cuadrante de líderes de Gartner para "Enterprise Firewall" o firewalls empresariales en los últimos 6 años.
- El fabricante debe estar certificado para IPv6 en Firewall e IPS por USGv6.
- Las características deben ser confirmadas mediante documentación oficial de acceso público (guías de administración, manuales y/o guías técnicas). No se aceptarán documentos generados expresamente para este proceso (ad-hoc).
- Las soluciones requeridas deben poder interoperar sin necesidad de software o interacción de terceros.

Características del equipamiento

- La solución debe soportar un throughput de por lo menos 7 Gbps con la funcionalidad de firewall habilitada para tráfico UDP de 64 byte.
- La solución debe soportar al menos 1.5 millones de conexiones simultáneas.
- La solución debe soportar al menos 45.000 nuevas conexiones por segundo.
- La solución debe soportar un throughput de al menos 6.5 Gbps de VPN IPSec.
- La solución debe estar licenciada para, o soportar sin necesidad de licencia, 200 túneles de VPN IPSec site-to-site simultáneos.
- La solución debe estar licenciada para, o soportar sin necesidad de licencia, 2.500 túneles de clientes VPN IPSec simultáneos.

- La solución debe soportar un throughput de al menos 950 Mbps de VPN SSL.
- La solución debe soportar al menos 200 clientes de VPN SSL simultáneos en modo túnel.
- La solución debe soportar al menos 1.4 Gbps de throughput de IPS.
- La solución debe soportar al menos 715 Mbps de throughput de Inspección SSL.
- La solución debe soportar al menos 1.8 Gbps de throughput de Application Control.
- La solución debe soportar al menos 1 Gbps de throughput de NGFW.
- La solución debe soportar al menos 900 Mbps de throughput de Threat Protection.
- La solución debe permitir actuar como controlador WIFI, permitiendo que se registren al menos 48 Access Points en modo túnel.
- La solución debe permitir la administración de al menos 16 switches en la misma consola de administración que el firewall.
- La solución debe tener al menos 2 interfaces de 1GE SFP.
- La solución debe tener al menos 8 interfaces de 1GE RJ45.
- La solución debe tener al menos 1 interfaces de 1GE RJ45 para management y alta disponibilidad.
- La solución debe estar licenciada y/o tener incluida sin costo adicional, al menos 10 sistemas virtuales lógicos (contextos) por appliance.
- La solución debe estar licenciada para utilizar funcionalidades de firewall de red.
- La solución debe estar licenciada para utilizar funcionalidades de IPS de red.
- La solución debe estar licenciada para utilizar funcionalidades de antivirus/antimalware de red.
- La solución debe estar licenciada para utilizar un sandbox en la nube del fabricante.
- La solución debe estar licenciada para utilizar funcionalidades de filtrado URL por categorías.

Requerimientos Generales

- La solución debe consistir en una plataforma de protección de red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW).
- Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos.
- La solución debe estar optimizada para análisis de contenido de aplicaciones en capa 7.
- La gestión del equipo debe ser posible a través de la interfaz de administración web disponible localmente en el mismo equipo.
- La solución debe proveerse en modalidad appliance físico. No se aceptarán soluciones virtualizadas.
- La totalidad de las características de SD-WAN y de seguridad (NGFW) solicitadas deben convivir en un mismo y único equipo físico. No se aceptarán opciones virtualizadas.
- La solución deberá brindarse en appliance físico con gestión local, no se aceptarán soluciones de seguridad basadas en administración en la nube.
- La solución debe proveerse con la última versión de software estable disponible.
- La solución debe tener un sistema operativo propietario. Se descartarán las ofertas basadas en sistema operativos Windows, Unix, Solaris, Linux o similar de uso gratuito.
- La solución debe ser compatible con NAT dinámico (1-a-muchos).
- La solución debe soportar NAT estático (1-a-1).

- La solución debe ser compatible con la traducción de puertos (PAT).
- La solución debe ser compatible con NAT Origen.
- La solución debe ser compatible con NAT de destino.
- La solución debe soportar NAT de origen y NAT de destino de forma simultánea.
- La solución debe soportar NAT de origen y NAT de destino en la misma política.
- La solución debe ser compatible con NAT64, NAT46 y NAT66.
- La solución debe soportar la creación de sistemas virtuales en el mismo equipo.
- La solución 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 debe permitir el control, inspección y descifrado de SSL para tráfico entrante y saliente, debe soportar el control de los certificados individualmente dentro de cada sistema virtual, es decir, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos).
- La 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.
- La consola de administración local (GUI) debe soportar como mínimo, inglés, Español y Portugués.
- La consola de administración local (GUI) debe soportar la administración de switches y Access Point.
- La solución debe permitir el monitoreo por 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 del clúster, ataques y estadísticas de uso de las interfaces de red.
- La solución debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF).
- La solución debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL.
- La solución debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes.

Requerimientos de Alta Disponibilidad

- La solución debe soportar la configuración de alta disponibilidad activo/pasivo y activo/activo en modo transparente.
- La solución debe soportar la configuración de alta disponibilidad activo/pasivo y activo/activo en capa 3.
- La solución debe soportar la configuración de alta disponibilidad activo/activo en capa 3 y con al menos 3 dispositivos en el clúster.
- 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 VPN.

- La configuración de alta disponibilidad debe sincronizar: Tablas FIB.
- En modo de alta disponibilidad debe permitir la supervisión de fallos de enlace.
- La solución debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad.

Requerimientos de Networking

- La solución debe soportar 4094 VLANs Tags 802.1q.
- La solución debe soportar agregación de enlaces 802.3ad y LACP.
- La solución debe soportar policy based routing y policy based forwarding.
- La solución debe soportar PIM v2: PIM-SM (RFC 4601), PIM-DM (RFC 3973) y PIM-SSM (RFC 3569).
- La solución debe soportar IGMP v1, IGMP v2, IGMP v3.
- La solución debe tener la habilidad de reenviar tráfico multicast en los modos de implementación transparente y route/NAT L3.
- Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP).
- Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3 y BGP).
- Soportar OSPF graceful restart.
- La solución debe soportar DHCP Relay y DHCP Server.
- La solución debe soportar Jumbo Frames.
- La solución debe soportar subinterfaces Ethernet lógicas.
- La solución debe soportar la utilización de ECMP.
- La solución debe soportar protección contra la suplantación de identidad (anti-spoofing).
- La solución debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red.
- La solución debe soportar modo capa 2 (L2) para la inspección de datos y visibilidad en línea del tráfico.
- La solución debe soportar modo capa 3 (L3) para la inspección de datos y visibilidad en línea del tráfico.
- La solución debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas.
- La solución debe soportar el protocolo estándar de la industria VXLAN.

Requerimientos VPN

- La solución debe soportar VPN de sitio-a-sitio y cliente-a-sitio.
- La solución debe soportar VPN IPSec.
- La solución debe 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 Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14 y Grupo 31.
- La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2).
- La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).

- La solución debe soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec.
- La solución debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting.
- La solución debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL.
- La solución debe soportar autenticación vía AD/LDAP, certificado y base de usuarios local.
- El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.
- La solución debe funcionar como un proveedor de servicios (SP) en una configuración SAML para la autenticación del firewall y del portal web SSL VPN.

Requerimientos de SD-WAN

- La solución debe soportar SD-WAN de forma nativa.
- La solución debe soportar agregar al menos 200 interfaces dentro de SD-WAN.
- La solución debe generar un canal de trasporte a través de una red virtual llamada “Red overlay” la cual debe tener independencia de las redes físicas, las cuales llamaremos “Red underlay”.
- La solución debe realizar cambios automáticamente en el reenvío de trafico de acuerdo con los valores de rendimientos (Latencia, Jitter, Packet Loss).
- La solución debe soportar enrutamiento de paquetes basado en la aplicación y el rendimiento (Latencia, Jitter, Packet Loss) de los enlaces y el estado de la ruta.
- La solución debe soportar la creación de reglas de enrutamiento de enlaces por IP de origen, destino, aplicación, usuarios, grupos de usuarios o servicios conocidos de internet.
- La solución debe permitir definir al menos 4 estrategias de enrutamiento distintas dentro de las reglas de SD-WAN.
- La solución debe soportar balanceo de enlaces 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.
- Las reglas de SD-WAN deben soportar QoS, shaping de tráfico, ruteo por políticas, IPSEC VPN como interfaces miembros.
- La solución debe permitir la utilización de FEC.
- La solución debe permitir el balanceo de tráfico por sesiones.
- La solución debe permitir el balanceo de tráfico por paquetes dentro de túneles IPSec.
- La solución debe permitir la implementación sin asistencia de SD-WAN, es decir, Zero Touch Provisioning.

Requerimientos para el Control de políticas de firewall

- La solución debe permitir construir políticas de seguridad utilizando números de puertos y protocolos.

- La solución debe permitir construir políticas de seguridad utilizando aplicaciones, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones.
- La solución debe permitir construir políticas de seguridad utilizando usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad.
- La solución debe permitir aplicar inspección de control de aplicaciones, antivirus, filtrado DNS, filtrado web, filtrado de archivos e IPS directamente a las políticas de seguridad.
- La solución debe contar con una base de datos actualizada por el fabricante con las direcciones IP de los principales servicios públicos, ej: Microsoft Office 365, Amazon, etc.

Requerimientos para la Identificación de usuarios

- La solución debe permitir de crear políticas basadas en la identidad del usuario a través de la integración con LDAP, Active Directory, E-directorio, RADIUS y base de datos local.
- La solución debe permitir la integración con Microsoft Active Directory para identificar usuarios y grupos.
- La solución debe soportar 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.
- La solución no debe solicitar re-autenticación de usuario para la utilización de los servicios permitidos según las políticas aplicadas (SSO).
- La solución 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.
- La solución debe permitir la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
- La solución debe permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.
- La solución debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación con doble factor.
- La solución debe soportar la autenticación de portal cautivo (red de cortesía) mediante protocolo RADIUS y/o LDAP.

Requerimientos para QoS y Shaping de tráfico

- Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.), se requiere que la solución tenga la capacidad de controlar el ancho de banda máximo utilizado.
- La solución debe soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen.
- La solución debe soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino.
- La solución debe soportar la creación de políticas de QoS y Traffic Shaping por puerto.

- La solución debe soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo.
- La solución debe soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube.
- La solución debe permitir en QoS la definición de tráfico con ancho de banda garantizado.
- La solución debe permitir en QoS la definición de tráfico con máximo ancho de banda utilizado.
- La solución debe permitir en QoS la definición de colas de prioridad.
- La solución debe soportar marcación de paquetes DiffServ, incluso por aplicación.
- La solución debe soportar la modificación de los valores de DSCP para Diffserv.
- La solución debe soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).
- La solución debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.

Requerimientos para Filtro de Archivos

- La solución debe permitir la creación de filtros para archivos predefinidos.
- Los archivos deben ser identificados por tamaño y tipo.
- La solución debe soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos.
- La solución debe soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos.
- La solución debe 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.

Requerimientos para el Control de Aplicaciones

- La solución debe tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo.
- La solución debe detectar miles de aplicaciones en distintas categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico.
- Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, Microsoft teams, Microsoft Office 365.
- La solución debe 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 tráfico 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.
- La solución debe identificar el uso de tácticas evasivas a través de las comunicaciones cifradas.

- La solución debe actualización de la base de firmas de la aplicación de forma automática.
- La solución debe 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 sólo en aplicaciones conocidas.
- La solución debe 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.
- La solución debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo.
- La solución debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo.
- La solución debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat, pero impedir la llamada de video.
- La solución debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.
- La solución debe permitir la creación de grupos dinámicos de aplicaciones, basado en las características de estas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
- La solución debe permitir crear grupos dinámicos de aplicaciones basados en características de estas, tales como: Nivel de riesgo de la aplicación.
- La solución debe permitir crear grupos estáticos de aplicaciones basadas en características de estas, tales como: Categoría de Aplicación.
- Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente.

Requerimientos de IPS

- La solución debe tener módulo IPS integrado en el propio equipo.
- La solución debe incluir firmas de prevención de intrusiones (IPS) y actualización periódica desde una base de datos provista por el fabricante.
- 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.
- La solución 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, usuarios, grupos de usuarios y la combinación de todos estos elementos.
- La solución debe permitir el bloqueo de vulnerabilidades y exploits conocidos.
- La solución debe incluir la protección contra ataques de denegación de servicio.
- La solución debe proteger la arquitectura mediante análisis de decodificación de protocolo.
- La solución debe proteger la arquitectura mediante análisis para detectar anomalías de protocolo.

- La solución debe proteger la arquitectura mediante análisis para detectar malformaciones de paquetes.
- La solución debe ser capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.
- La solución debe detectar y bloquear los escaneos de puertos de origen.
- La solución debe bloquear ataques realizados por gusanos (worms) conocidos.
- La solución debe contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow).
- La solución debe poder crear firmas personalizadas en la interfaz gráfica del producto.
- La solución debe identificar y bloquear la comunicación con redes de bots mediante firmas de IPS y una base de reputación IP provista, mantenida y actualizada periódicamente por el fabricante.
- La solución debe registrar 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.
- La solución debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.
- Los eventos deben identificar el país que origino la amenaza.

Requerimientos de Antivirus

- La solución debe incluir firmas de virus y malware con actualización periódica desde una base de datos provista por el fabricante.
- La solución debe incluir un motor de antivirus heurístico.
- La solución debe permitir realizar escaneos en los siguientes protocolos: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, CIFS.
- La solución debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms).
- La solución debe tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP.
- La solución debe aislar automáticamente las máquinas infectadas de otros segmentos de red.
- La solución debe tener protección contra ataques de día cero a través de una estrecha integración con componentes de Sandbox, en las instalaciones locales y en la nube.

Licenciamiento, soporte y actualizaciones

- El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.

- La vigencia del licenciamiento de funcionalidades de seguridad, soporte para actualizaciones de software, soporte del fabricante y garantía de hardware debe proveerse por 2 años.

- El soporte provisto por el fabricante deberá ser bajo modalidad 24x7 (NBD) y con atención telefónica, mail y web.

2- **Solución de Seguridad de Usuarios/Punto Final (EPP) FORTICLIENT– Cantidad: 75 usuarios concurrentes.**

Funcionalidades generales

1.1 Debe permitir gestión centralizada de 75 endpoints.

1.2 Debe permitir la gestión del cliente de seguridad de endpoint desde una consola central del fabricante

1.3 El licenciamiento debe estar basado en la cantidad de clientes registrados en la consola de gestión central del mismo fabricante

1.4 Debe permitir la copia de seguridad del archivo de configuración del endpoint

1.5 El cliente de seguridad debe poder generar logs sobre las funcionalidades instaladas y configuradas

1.6 Por lo menos los siguientes niveles de log deben estar disponibles: emergencia, alerta, crítico, error, aviso, informativo;

1.7 El cliente de seguridad debe poder enviar los logs a la consola de gestión central

Funcionalidades de Provisionamiento de Clientes

1.8 El fabricante debe proveer un portal para descargar el cliente seguridad y permitir la instalación local

1.9 Debe ser compatible con la instalación vía Active Directory de Microsoft

1.10 La consola de gestión central debe ser capaz de instalar el cliente de seguridad en computadoras Windows asociadas a un dominio Microsoft

Funcionalidades de Antivirus

1.11 El cliente de seguridad debe ser capaz de inspeccionar archivos ejecutables, librerías y drivers en busca de virus

1.12 El cliente de seguridad debe ser capaz de buscar actualizaciones de firmas automáticamente

1.13 El cliente de seguridad debe bloquear canales de comunicación usados por hackers o atacantes

1.14 El cliente de seguridad debe notificar localmente cuando se detecta un virus

1.15 El cliente de seguridad debe permitir que el usuario comience un escaneo bajo demanda

1.16 El cliente de seguridad debe permitir que se comience escaneo de virus de forma automática regularmente

1.17 El cliente de seguridad debe permitir visualizar los archivos puestos en cuarentena

1.18 Debe permitir la configuración del perfil antivirus desde la consola central del mismo fabricante

Funcionalidades de Filtrado de Contenido Web

1.19 Debe permitir la configuración del perfil de filtro de web desde la consola central del mismo fabricante

1.20 El fabricante debe disponibilizar consultas en línea desde el cliente de seguridad sobre la categoría de determinada web (por ej. Interés general, tecnología, hacking, pornografía, etc) para aplicar política de control de acceso a internet

1.21 El cliente de seguridad debe admitir reglas estáticas de acceso a internet basado en expresiones regulares

1.22 Para una URL determinada las acciones deben ser: permitir, bloquear, alertar o monitorar.

Funcionalidades de Firewall de Aplicación

1.23 El cliente de seguridad debe admitir perfiles de Control de Aplicaciones creados centralmente desde la consola de gestión del mismo fabricante

1.24 El fabricante debe disponibilizar consultas en línea desde el cliente de seguridad sobre la categoría de determinada aplicación a modo de ser usada en la política de control de acceso

1.25 Debe ser reconocido más de 2800 aplicaciones por el cliente para ser usadas en reglas de control de acceso

Funcionalidades de VPN SSL

1.26 Debe permitir que el usuario cree nuevas VPN SSL

1.27 Debe permitir que existan varias VPN SSL definidas simultáneamente

1.28 Debe permitir la personalización del puerto TCP en el que funciona la VPN SSL

1.29 Debe permitir la autenticación usando usuario y clave

1.30 Debe permitir la autenticación de dos factores provisto por el mismo fabricante

1.31 Debe permitir la autenticación usando certificados digitales

Funcionalidades de VPN IPSec

1.32 Debe permitir que el usuario cree nuevas VPN IPSEC

1.33 Debe permitir que existan varias VPN IPSEC definidas simultáneamente

1.34 Debe permitir la autenticación usando usuario y clave

1.35 Debe permitir la autenticación usando certificados digitales

1.36 Debe permitir la selección de Modo Main y Agressive;

1.37 Debe permitir la configuración de DHCP sobre IPSec;

1.38 Debe permitir el uso de NAT Traversal;

1.39 Debe permitir la eleccion de grupos Diffie-Hellman (1,2,5 e 14);

1.40 Debe permitir la configuración de expiración de claves IKE;

1.41 Debe permitir el uso de Perfect Forward Secrecy;

1.42 Debe permitir la autenticación de dos factores provisto por el mismo fabricante

Funcionalidades de Scanner de Vulnerabilidades

1.43 El cliente de seguridad debe tener integrado un módulo de búsqueda de vulnerabilidades y permitir la gestión central desde la consola del mismo fabricante

1.44 Debe permitir que el usuario comience un análisis de vulnerabilidades bajo demanda

1.45 Las vulnerabilidades encontradas deben ser mostradas localmente con un vínculo para visualizar información desde una base de datos en internet. Debe tener al menos: nombre, severidad y detalles

Funcionalidades de Gestión

1.46 Debe permitir la instalación sobre Microsoft Windows Server 2008 R2, 2012 o 2012 R2;

1.47 Debe ser entregado en la solución sin costo

1.48 Debe permitir adicionar clientes mediante la adición de licencias

1.49 Debe tener interfaz de gestión gráfica

1.50 Debe tener la funcionalidad de backup

1.51 Debe permitir la creación de usuarios de diferente perfil administrativo

1.52 Debe permitir importar información desde Active Directory mediante LDAP

1.53 El registro manual de estaciones debe permitir el uso de clave

1.54 Debe permitir la creación de grupos de clientes para facilitar la gestión

1.55 Debe permitir la configuración de clientes mediante definición XML

1.56 Debe permitir la importación de configuración de perfiles desde firewall de mismo fabricante

1.57 Debe permitir configuración de diferentes grupos y perfiles para facilitar la administración

1.58 Debe permitir la configuración de perfiles de antivirus, webfilter, control de aplicaciones, scanner de vulnerabilidades y VPN

1.59 Debe permitir habilitar la protección en tiempo real

1.60 Debe permitir configurar la búsqueda de virus y vulnerabilidades de forma programada

1.61 Debe permitir ejecutar escaneo total y escaneo rápido

1.62 Debe permitir configurar filtro de URLs provisto por el fabricante con al menos las siguientes acciones: bloquear, advertir, permitir y monitorar;

1.63 Debe permitir configurar filtro de URLs basado en wildcards o expresiones regulares con las siguientes acciones: bloquear o permitir;

1.64 Debe permitir al usuario configurar VPNs localmente

1.65 Debe permitir al usuario desconectar una VPN

1.66 Debe permitir la conexión de VPN antes de login

1.67 Debe permitir conexión automática de VPN

1.68 Específico y general para VPN IPSec (al menos):

1.69 Uso de certificados o usario y clave para autenticación

1.70 Uso de certificados en smartcard

1.71 Verificación de checksum

1.72 Bloqueo de tráfico IPv6

1.73 Específico a SSL VPN (al menos):

1.74 Especificación de la IP del concentrador

1.75 Especificación del puerto del concentrador

1.76 Opción para que el usuario pueda acceder a la configuración del cliente mediante contraseña

1.77 Envio de logs hacia sistemas de logs externos del mismo fabricante

1.78 Registro junto al sistema de gestión de forma silenciosa (de forma que sea no perceptible para el usuario);

1.79 Instalación de certificado digital en el cliente

1.80 Debe permitir habilitar funcionalidades de Single Sign On

1.81 El sistema de gestión central debe tener disponible información sobre: Cantidad de dispositivos gestionados, Versión de Sistema Operativo, Perfil aplicado, Usuario, Versión de firmas de Antivirus

1.82 Estado del cliente de seguridad: Registrado o no registrado

1.83 Información sobre el sistema operativo en el que está instalado el cliente

1.84 Perfil de seguridad creados y/o aplicados

1.85 Funcionalidades de seguridad aplicadas: antivirus, filtro web, VPN, firewall de aplicaciones.

PLIEGO DE BASES Y CONDICIONES GRALES CP N° 6_2021 FGT80F_y_FORTICLIENT.docx - Documentos de Google

Final Audit Report 2021-05-21

Created:	2021-05-21
By:	Fernanda Gonzalez (fgonzalez@ca.gob.ar)
Status:	Signed
Transaction ID:	CBJCHBCAABAAITBEgBXDGrLovbS3wZsS0IbW8gmSFGhJ

"PLIEGO DE BASES Y CONDICIONES GRALES CP N° 6_2021 FGT80F_y_FORTICLIENT.docx - Documentos de Google" History

Document created by Fernanda Gonzalez (fgonzalez@ca.gob.ar)
2021-05-21 - 7:12:50 PM GMT- IP address: 181.199.156.163

Document emailed to Agustín Domingo (adomingo@ca.gob.ar) for signature
2021-05-21 - 7:14:21 PM GMT

Email viewed by Agustín Domingo (adomingo@ca.gob.ar)
2021-05-21 - 7:25:03 PM GMT- IP address: 66.102.8.29

Document e-signed by Agustín Domingo (adomingo@ca.gob.ar)
Signature Date: 2021-05-21 - 7:25:34 PM GMT - Time Source: server- IP address: 186.141.197.10

Agreement completed.
2021-05-21 - 7:25:34 PM GMT