S. E. CASA DE MONEDA

PLIEGO DE ESPECIFICACIONES TECNICAS Y PARTICULARES

Firewall + AP

S. E. CASA DE MONEDA

Contenido

S. E. CASA DE MONEDA

OBJETO

Este pliego tiene por objeto establecer los requisitos mínimos y lineamientos para la provisión, instalación y soporte de un sistema de seguridad (Next Generation Firewall) con capacidad para implementar gestión unificadas de amenazas (UTM) destinado a controlar el tráfico cursado desde y hacia las redes externas a la institución junto con la gestión de conectividad inalámbrica. Se deberán proveer (4) Firewalls de Próxima Generación y 80 antenas.

De lo solicitado dos (2) firewalls serán instalados en la Sede de Retiro y otros dos (2) en la Sede Don Torcuato, en cuanto a las antenas ser instaladas 60 en la Sede de Retiro y 20 en la Sede Don Torcuato.

CONDICIONES GENERALES

CONSIDERACIONES Y REQUERIMIENTOS GENERALES

1.1. Todos los requerimientos técnicos de los equipos y software objeto de este pliego, deben ser considerados mínimos, pudiendo el Oferente presentar ofertas cuyas características superen o mejoren las aquí solicitadas.

1.2. Todas las facilidades solicitadas para los equipos y software, incluidas las ampliaciones y capacidades de expansión, deberán estar disponibles a la fecha de apertura de la presente licitación. Se considera “estar disponible” el haber sido liberado al mercado mundial en forma oficial por la empresa fabricante del equipo o desarrolladora del software.

1.3. No se aceptarán (serán consideradas como no presentadas) facilidades y/o expansiones no soportadas por la versión actual del software y hardware (la vigente a la fecha de apertura de la presente licitación).

1.4. Se proveerán todos los cables necesarios para las interconexiones de los equipos.

1.5. Todos los equipos deberán operar con una alimentación 220 VCA 50Hz, monofásico con conectores C13-C14 o C19-C20 sin el uso de transformadores externos. Como máximo los equipos firewall ocuparán 1 unidad de Rack de altura.

1.6. Todos los requerimientos técnicos y funcionalidades esperadas de acuerdo a lo solicitado en el presente pliego, deben operar tanto en forma independiente unas de otras como en forma totalmente integrada y/o simultánea, sin limitación alguna.

1.7. Los elementos, unidades funcionales, dispositivos y accesorios estarán constituidos por unidades nuevas, sin uso previo y en perfecto estado de conservación y funcionamiento (se entiende por nuevo y sin uso, a que S.E. Casa de Moneda será el primer usuario de los equipos desde que estos salieron de fábrica).

1.8. Todos los sistemas ofrecidos deberán cumplir con las especificaciones en materia de regulación de seguridad eléctrica, emisión de radiofrecuencia, emisión electromagnética y emisión de radiación, emitidas por los organismos competentes.

1.9 Todos los equipos a proveer de un mismo tipo (Equipos que poseen las mismas características técnicas y funcionales, y están destinados a satisfacer una misma necesidad según la especificación particular de cada uno dada en el documento de licitación) deberán ser del mismo modelo.

1.10 Los equipos a proveer deberán estar vigentes y no poseer fecha de discontinuidad de fabricación a la fecha de presentación de la oferta.

1.11 Todos los appliances a proveer deberán operar con corriente alterna de 220 V, 50 Hz, con conexión a tierra, sin posibilidad de conmutar manualmente a otro voltaje/frecuencia.

1.12 Todos los equipos ofrecidos deberán operar en rangos de temperatura ambiente desde 0 a 40 grados centígrados, sin necesidad de acondicionamiento especial.

1.13 Todo el equipamiento deberá entregarse con todos los accesorios necesarios para su correcta instalación y funcionamiento, entiéndase por esto fuentes de alimentación, cables de conexión, y drivers de software.

CONDICIONES DE LAS OFERTAS

Los oferentes deberán presentar en su oferta: folletos, documentación técnica, manual de especificaciones y facilidades del equipamiento ofrecido. No se admitirá especificar simplemente “según pliego” como identificación del equipamiento ofrecido.

La contestación a los puntos del pliego deberá hacerse punto por punto en castellano indicando en qué parte de la documentación presentada se especifica el cumplimiento de los mismos.

La instalación de los equipos ofrecidos será realizada por la Adjudicataria. Los detalles de la instalación deberán ser detallados claramente en ítem separado.

CARACTERISTICAS GENERALES DEL EQUIPAMIENTO

El equipamiento deberá poseer como mínimo las siguientes características técnicas de las prestaciones requeridas:
Poseerá compatibilidad con todos y cada uno de los siguientes estándares:
Ethernet IEEE 802.3, Fast Ethernet IEEE 802.3u, Gigabit Ethernet IEEE 802.3z, 10 Gigabit Ethernet IEEE 802.3ae.

Los cuatro equipos deberán poder operar en alta disponibilidad, en modalidad activo-activo y activo-pasivo. Cada uno de los equipos deberá tener la posibilidad de agregado de fuentes redundantes del tipo hot swap. El sistema deberá poder operar en modo Router (permitiendo el envío de paquetes en L2 y L3) como así también en modo transparente.

Deberá permitir la creación de al menos 10 sistemas virtuales dentro del mismo equipo, sin necesidad de hardware o licencias adicionales. Cada sistema virtual podrá operar en modo Router o Transparente sin limitaciones en forma simultánea sobre cada sistema virtual.

El sistema deberá permitir la definición de interfaces virtuales (VLANs) las que podrán estar asignadas a diferentes interfaces físicas en diferentes sistemas virtuales. Deberá soportar el etiquetado de los paquetes según IEEE 802.1Q utilizando cualquier ID (1-4095). Asimismo, deberá contar con soporte de VXLAN.

El mecanismo de control de filtrado utilizado por el engine del firewall deberá estar basado en técnicas “statefull inspection” que crean conexiones virtuales, incluso para los protocolos connection-less como UDP y RPC.

El Firewall deberá poseer las configuraciones localmente, no dependiendo su funcionamiento de otros productos, servicios o herramientas de gestión centralizadas.

Las reglas deben permanecer en medio físico, no volátil. Estas reglas deberán poder definirse, diferenciando protocolo, IP destino/origen, puerto destino/origen y geolocalización utilizando rangos horarios.

El dispositivo deberá soportar al menos la generación de 10.000 políticas de firewall.

El dispositivo deberá soportar SNAT, DNAT y PAT. Será posible la aplicación de SNAT y DNAT y PAT en forma simultánea sobre una misma conexión.

Deberá soportar NAT estático y dinámico y PAT sobre cualquier tipo de conexión, tanto para IPv4 como IPv6. Deberá soportar NAT46 y NAT64 sobre la totalidad de las políticas de firewall.

Deberá soportar la configuración de NAT estático sobre todas las interfaces físicas y lógicas utilizando direcciones IP virtuales, que no sean las propias IP declaradas en las interfaces del firewall.

Cada Firewall deberá permitir el uso de objetos dinámicos aplicables a todo tipo de regla, definiendo las propiedades de los mismos sobre cada Firewall en particular. Los objetos deben poder referenciar servidores, redes, direcciones basadas en ubicación geográfica y servicios como mínimo.

Cada Firewall deberá poseer capacidad de manejo de apertura de puertos dinámicos en base a protocolos de uso común (HTTP, SMTP, FTP, H323, SIP) y posibilidad de crear sesiones personalizadas que manejen dicho comportamiento.

El equipo deberá permitir la implementación de políticas de calidad de servicio y Traffic Shaping soportando al menos:

- Puertos físicos e interfaces agregadas o redundantes.
- Políticas de QoS y Traffic Shaping por dirección de origen y destino, usuario y grupo.
- La definición de tráfico con ancho de banda garantizado.
- La definición de tráfico con máximo ancho de banda.
- La definición de colas de prioridad.
- La priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.
- El etiquetado de paquetes DiffServ, incluso por aplicación.
- La modificación de los valores de DSCP para Diffserv.
- La priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).

El equipo deberá poseer la capacidad de entregar direcciones IP a los hosts conectados en sus interfaces LAN por medio del protocolo DHCP (DHCP server).

Cada Firewall deberá además soportar las siguientes funcionalidades:

- Autenticación de usuarios en forma local y remota por medio de los protocolos RADIUS y LDAP, debiendo ser totalmente compatible con Active Directory.
- Soporte de IPSec NAT Traversal.

El equipo deberá permitir la terminación de túneles VPN.
El Firewall deberá soportar túneles utilizando protocolo IPSEC estándar o a través de SSL. Para el caso de VPNs SSL, el equipo debe soportar que el usuario pueda realizar la conexión a través de un cliente VPN instalado en el sistema operativo de su máquina o a través de una interface web.

El equipo, con su funcionalidad de Next Generation Firewall activa deberá soportar el throughput requerido medido con tráfico real con las siguientes funcionalidades habilitadas simultáneamente:
Clasificación y control de aplicaciones, IPS, Control de navegación por URL, Antivirus y Antispyware, Control de amenazas avanzadas de día cero (Sandboxing). Para todas las firmas que la plataforma de seguridad posea totalmente activadas, actualizadas al día y con el mayor

nivel de seguridad posible; considerando múltiples políticas de seguridad y que tengan habilitado la generación de Logs y NAT aplicado a todas las reglas.

El Control de Amenazas avanzadas (Sandboxing) deberá ser provisto en la solución. El mismo deberá estar disponible durante el período de garantía.

El Firewall deberá soportar la activación y desactivación de la funcionalidad de IPS, detección de anomalías y anti-malware para los protocolos soportados.

- Deberá realizar el análisis de IPS basado en firmas las cuales se deberán poder agrupar para aplicar a las reglas.
- Deberá permitir armar firmas propias de IPS.
- Deberá realizar la actualización de firmas de IPS en forma automática y periódica, durante el periodo de garantía.
- Deberá poseer una base de conocimiento que detalle la definición de la regla.
- Deberá ante un ataque de IPS responder con una notificación o un bloqueo del tráfico.
- Deberá poseer la capacidad de excluir para una regla específica, una firma en particular; sin que ello implique deshabilitar por completo la utilización de esa firma en las demás reglas.
- El motor de IPS deberá soportar el agregado de firmas específicas para ambientes industriales a los fines de interpretar los protocolos específicos de esos ambientes.

El Firewall deberá identificar potenciales vulnerabilidades y sugerir las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de la solución. La información podrá brindarse mediante la GUI o vía reportes.

El Firewall deberá funcionar como proxy web explícito (validación en Active Directory o por medio del protocolo LDAP) y como proxy transparente.

El Firewall deberá incorporar funcionalidades para SD-WAN. Si fuese necesario el agregado de licencias adicionales indicar cómo se aplican las mismas.

Capacidades de SD-WAN a soportar en el firewall:

- Balanceo de vínculos a Internet, VPNs y enlaces WAN (ej: MPLS)
- Balanceo Round Robin, Balanceo por peso, cantidad de sesiones, ancho de banda y derrame.
- Definición de políticas de SDWAN por Aplicación, Servicio de internet, usuarios, IPs o Interfaces/zonas.
- Soporte a más de 5 vínculos a Internet.
- Debe contar con un mecanismo por el cual se puedan recuperar los datos enviados sin necesidad de recurrir a las retransmisiones de protocolo TCP y que permita la reconstrucción del stream en el lado receptor.

El Firewall deberá soportar la activación y desactivación de técnicas de detección y evasión de ataques de DOS (Denegación de Servicio).

Cada Firewall deberá soportar la activación y desactivación de técnicas de protección de ataques de generación masiva de conexiones (SYN attack) permitiendo su configuración para una dirección IP en particular.

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.

Deberá tener la posibilidad de aplicar la funcionalidad de antivirus por regla sobre conexiones HTTP, FTP, SMTP, POP3, IMAP y túneles VPN encriptados establecidas a través del equipo.

Deberá tener la funcionalidad de filtrado de contenidos Web.

- Deberá permitir o bloquear el acceso de los usuarios a diferentes sitios web considerados o no maliciosos.
- Deberá permitir el 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).
- Deberá permitir la actualización automática de la base de filtrado de contenidos durante el transcurso del período de garantía.
- Deberá soportar al menos sesenta (60) categorías en la base de filtrado.
- Deberá tener la funcionalidad para detectar aplicaciones. Para ello el equipo deberá:
    - Inspeccionar el contenido del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas, independiente de puerto y protocolo que utilicen.
    - Deberá reconocer al menos 3000 aplicaciones diferentes, permitiendo agrupar las mismas en al menos 16 categorías y aplicar políticas de seguridad a las mismas.
    - Debe permitir la creación de firmas de aplicación manuales.
- Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo.
- Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.
- Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos.

Deberá soportar la inspección de sesiones que atraviesan el firewall y utilizan el protocolo SSL (Secure Sockets Layer) para encriptación, incluyendo el protocolo HTTPS.

El equipo deberá proveerse con los servicios de actualización de firmas para los motores de filtrado descriptos en los puntos anteriormente mencionados por el término de 12 meses.

Debe permitir la administración del equipo por medio de los protocolos HTTP/HTTPS, Telnet/SSH y SNMP v1/v2.

Deberá permitir el registro local y remoto de eventos utilizando servidores syslog.

Controlador de puntos de conexión inalámbricos o WIFI. Dicha función deberá estar integrada dentro de la solución de firewall requerida.

En el caso de requerir una licencia específica para la funcionalidad de Controlador WIFI especificarlo.

Debe permitir la conexión de dispositivos inalámbricos que implementen los estándares IEEE 802.11a / b / g / n / ac y que transmitan tráfico IPv4 e IPv6 a través del controlador.

La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor.

El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS.

La solución debe optimizar el rendimiento y la cobertura inalámbrica (RF) en los puntos de acceso administrados por ella, realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados. La solución debe permitir además deshabilitar el ajuste automático de potencia y canales cuando sea necesario.

Permitir programar día y hora en que ocurrirá la optimización del aprovisionamiento automático de canales en los Access Points.

El encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser tuneleados hasta el controlador inalámbrico.

Cuando tuneleado, el tráfico debe ser encriptado a través de DTLS o IPSEC.

Debe permitir la administración de puntos de acceso conectados remotamente a través de WAN. En este escenario el encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe ocurrir de forma distribuida (local switching), o sea, el tráfico debe ser cambiado localmente en la interfaz LAN del punto de acceso y no necesitará de tunelamiento hasta el controlador inalámbrico.

Cuando el tráfico se conmuta directamente en los puertos Ethernet de los puntos de acceso (local switching) y la autenticación sea WPA/WPA2-Personal (PSK), en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica.

La solución debe permitir definir qué redes serán tuneleadas hasta la controladora y qué redes serán conmutadas directamente por la interfaz del punto de acceso.

La solución debe soportar el recurso de Split-Tunneling de forma que sea posible definir, a través de las subredes de destino, qué paquetes serán tuneleados hasta el controlador y cuáles serán conmutados localmente en la interfaz del punto de acceso.

La solución debe permitir el equilibrio de carga de los usuarios conectados a la infraestructura inalámbrica de forma automática. La distribución de los usuarios entre los puntos de acceso cercanos debe ocurrir sin intervención humana y basada en criterios como número de dispositivos asociados en cada punto de acceso.

La solución debe tener mecanismos para detectar y mitigar los puntos de acceso no autorizados, también conocidos como Rogue AP. La mitigación debe realizarse de forma automática y batida en criterios tales como: intensidad de señal o SSID. Los puntos de acceso administrados por la solución deben evitar la conexión de clientes en puntos de acceso no autorizados.

La solución debe mostrar información sobre los dispositivos conectados a la infraestructura inalámbrica e informar al menos la siguiente información: Nombre de usuario conectado al dispositivo, Fabricante y sistema operativo del dispositivo, Dirección IP, SSID al que está conectado, Punto de acceso al que está conectado, Canal al que está conectado, Banda transmitida y recibida (en Kbps), intensidad de la señal considerando el ruido en dB (SNR), capacidad MIMO y horario de la asociación.

La solución debe implementar reglas de firewall (stateful) para controlar el tráfico permitiendo o descartando paquetes de acuerdo con la política configurada, reglas que deben utilizar como criterio de interfaz de origen el SSID de la red WIFI.

La solución debe monitorear y clasificar el riesgo de las aplicaciones accesadas por los clientes inalámbricos.

Permitir configurar el bloqueo en la comunicación entre los clientes inalámbricos conectados a un SSID.

Debe implementar la autenticación administrativa a través del protocolo RADIUS.

En combinación con los puntos de acceso, la solución debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES).

En combinación con los puntos de acceso, la solución debe ser compatible e implementar el método de autenticación WPA3.

La solución debe permitir la configuración de múltiples claves de autenticación PSK para su uso en un SSID determinado.

Cuando se utiliza la función de múltiples claves PSK, la solución debe permitir la definición de límite en cuanto al número de conexiones simultáneas para cada clave creada.

La solución debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios basados en los atributos proporcionados por los servidores RADIUS.

La solución debe implementar el mecanismo de cambio de autorización dinámica a 802.1X, conocido como RADIUS CoA (Change of Authorization) para autenticaciones 802.1X.

La solución debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP.

La solución debe implementar la característica de autenticación de los usuarios a través de la página web HTTPS, también conocido como Captive Portal. La solución debe limitar el acceso de los usuarios mientras éstos no informen las credenciales válidas para el acceso a la red.

La solución debe permitir el hospedaje del captive portal en la memoria interna del controlador inalámbrico.

La solución debe permitir la personalización de la página de autenticación, de forma que el administrador de red sea capaz de cambiar el código HTML de la página web con formato de texto e insertar imágenes.

La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red.

La solución debe permitir que la página de autenticación se quede alojada en un servidor externo.

La solución debe permitir el registro de cuentas para usuarios visitantes en la memoria interna. La solución debe permitir que sea definido un período de validez para la cuenta creada.

La solución debe garantizar que los usuarios se autentiquen en el portal cautivo que utilice la dirección IPv6.

La solución debe tener interfaz gráfica para administrar y gestionar las cuentas de usuarios visitantes, no permitiendo acceso a las demás funciones de administración de la solución.

Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado.

La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes.

La solución debe identificar automáticamente el tipo de equipo y sistema operativo utilizado por el dispositivo conectado a la red inalámbrica.

La solución debe permitir que los usuarios puedan acceder a los servicios disponibles a través del protocolo Bonjour (L2) y que estén alojados en otras subredes, como AirPlay y Chromecast. Debe ser posible especificar en qué VLANs el servicio estará disponible.

La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog.

La solución debe permitir ser administrada a través del protocolo SNMP (v1, v2c y v3), además de emitir notificaciones a través de la generación de traps.

La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP.

La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB).

La solución debe presentar gráficamente la topología lógica de la red, representar los elementos de la red gestionados, además de información sobre los usuarios conectados con la cantidad de datos transmitidos y recibidos por ellos.

La solución debe permitir la adición de controlador redundante operando en N + 1. En este modo, el controlador redundante debe monitorear la disponibilidad y sincronizar la configuración del principal, además de asumir todas las funciones en caso de error del controlador principal. De esta forma, todos los puntos de acceso deben asociarse automáticamente al controlador redundante que pasará a tener función de primario de forma temporal.

La solución debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red. Debe ser posible especificar en qué puntos de acceso o grupos de puntos de acceso que cada dominio estará habilitado.

La solución debe garantizar al administrador de la red determinar los horarios y días de la semana que las redes (SSID) estarán disponibles para los usuarios.

La solución debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming.

La solución debe implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute la itinerancia.

La solución debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente conectado mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos.

La solución debe implementar el estándar IEEE 802.11w para prevenir ataques a la infraestructura inalámbrica.

La solución debe soportar priorización a través de WMM y permitir la traducción de los valores a DSCP cuando los paquetes se destinan a la red de cableado.

La solución debe permitir la configuración del valor de Short Guard Interval para 802.11n y 802.11ac en 5GHz.

La solución provista debe tener la capacidad de hacer Reporting, Análisis y guardar logs. Esta solución deberá ser de la misma marca que los equipos propuestos.
• Deberá poder ser desplegado como una Máquina Virtual (VM) sobre infraestructura KVM o VMWare.
• El sistema deberá analizar los registros provenientes de múltiples dispositivos, por usuario o por grupo de usuarios
• Deberá generar una variedad de reportes que permiten a los administradores de red asegurar las redes de manera proactiva conforme se presentan las amenazas, evitando los abusos de red.
• El sistema deberá permitir la visualización de registros o cualquier mensaje o archivo de registro desde los dispositivos registrados. Deberá implementar filtros que permitan navegar sobre los registros de forma simple y amigable.
• El sistema deberá implementar reportes que permitan a los administradores conocer al menos:
• Ataques: por unidad, por hora del día, por categoría, y por fuentes de los ataques.
• Virus: principales virus detectados en la red y detectados por Protocolo.
• Eventos: Por Firewall, eventos en general, eventos de seguridad desencadenados y eventos desencadenados por el día de la semana.
• Utilización de la Red: Principales usuarios de la Red y principales clientes intentando acceder a sitios bloqueados.
• Ancho de banda: Principales usuarios de ancho de banda.
Ancho de banda por día, por hora y utilización de ancho de banda por familia de protocolos.
• Protocolos: los principales protocolos utilizados, usuarios FTP y usuarios de Telnet.
• El sistema deberá implementar análisis forenses de forma que se pueda rastrear las actividades de un usuario.
• El sistema deberá ser administrable vía Web utilizando HTTPs.
Los administradores podrán ser por dominio y deberá poder asignarse de qué equipos (por dirección IP y máscara) puede el administrador conectarse.
• El sistema deberá soportar al menos dos niveles de administración: Lectura/Escritura (Read/Write) y Sólo Lectura (Read-Only).
• Debe contar con reporte de AP´s y SSID´s autorizados, así como clientes WIFi.

La solución provista deberá contar con el espacio para el almacenamiento permanente de los logs y espacio para el guardado de los logs diarios que se utilizarán para la Analítica.

Debe soportar servicio de Indicadores de Compromiso del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.

La solución provista deberá tener no menos de 3 TB de Almacenamiento permanente de logs y 6 Gbps para Analítica de logs diarios.

IV: ESPECIFICACIONES PARTICULARES

IV.a) Firewall de Próxima Generación Sede Retiro. Cantidad 2

Número de Interfaces Requeridas	8x GE RJ45 8x GE SFP (Bahias) 2x GE SFP+ (Bahias) 2 x GE RJ45 Puertos administrativos
Throughput de Firewall (con paquetes de 512 Bytes)	36 Gbps
Latencia de firewall (con paquetes de 64 byte)	2 µs
Throughput de VPN IPSec (con paquetes de 512 byte)	20 Gbps
Throughput de NGFW	9 Gbps
Throughput de Inspección SSL	8 Gbps
Políticas de Firewall admitidas	10.000
Túneles IPsec gateway to gateway	2.000
Túneles IPsec client to gateway	50.000
Túneles SSL	5.000
Throughput VPN SSL	7 Gbps
Sesiones Concurrentes	7 Millones

Sesiones SSL Concurrentes	800.000
Nuevas sesiones / segundo	430.000
Nuevas sesiones SSL / segundo	5.000
Puntos acceso soportados en modo túnel	512
Sistemas Virtuales incluidos	10

IV.b) Firewall de Próxima Generación Sede Don Torcuato. Cantidad 2

Número de Interfaces Requeridas	16x GE RJ45 4x GE SFP (Bahias) 2 x GE RJ45 Puertos administrativos
Throughput de Firewall (con paquetes de 512 Bytes)	20 Gbps
Latencia de firewall (con paquetes de 64 byte)	3 µs
Throughput de VPN IPSec (con paquetes de 512 byte)	7 Gbps
Throughput de NGFW	1.5 Gbps
Throughput de Inspección SSL	800 Mbps
Políticas de Firewall admitidas	10.000
Túneles IPsec gateway to gateway	2.000
Túneles IPsec client to gateway	10.000
Túneles SSL	500
Throughput VPN SSL	900 Mbps
Sesiones Concurrentes	2 Millones
Sesiones SSL Concurrentes	240.000
Nuevas sesiones / segundo	130.000

Nuevas sesiones SSL / segundo	1.000
Puntos acceso soportados en modo túnel	128
Sistemas Virtuales incluidos	10

IV. c) Puntos de conexión inalámbricos

Cantidad de dispositivos Access Point sede Retiro: 60

Cantidad de dispositivos Access Point sede Don Torcuato: 20

Tipo	Indoor
Throughput	800 Mbps
Nro. Máximo de Clientes por radio	512
Tecnología 802.11 a/b/g/n/ac	SI
Cantidad de **Puertos Ethernet**	2
Frecuencias de Radios	2.4 y 5 GHz
MIMO	2x2
802.11ac Wave2	SI
Potencia Máx de Transmisión	24 dBm
Spatial Stream	2
Antenas Internas	4
Ganancias de Antenas por radio	2.4 GHz: 4dBi ; 5 GHz: 5 dBi
Capacidad BLE	SI
Interfaces ethernet 1x 10/100/1000 Base-T RJ45	1
IEEE 802.3az	SI
SSIDs Simultáneos	16
Tipos EAP	EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST
Estandares IEEE	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3az
Transmit Beam Forming (TxBF)	SI
Maximum Likelihood Demodulation (MLD)	SI

Maximum Ratio Combining (MRC)	SI
A-MPDU and A-MSDU Packet Aggregation	SI
MIMO Power Save	SI
Short Guard Interval	SI
Rogue Scan Radio Modes	SI
WIPS / WIDS Radio Modes	SI
Spectrum Analyzer	SI
Peso Max.	500 gramos
Consumo Max.	12.5 Watts
Alimentación POE	SI
Accesorios incluídos para su instalación y fijación.	SI

V: INSTALACION

La adjudicataria deberá estar presente a través de sus representantes autorizados en el momento de la instalación de los equipos en el destino que esta S.E. Casa de Moneda le indique.

A los fines precedentemente señalados, la adjudicataria coordinará con personal de S.E. Casa de Moneda día y horario para realizar las tareas.

Los oferentes deberán especificar claramente en la oferta las condiciones ambientales que deberán ser cumplidas por S.E. Casa de Moneda para la correcta instalación de los equipos:

- Tipo de alimentación y potencia eléctrica requerida por las unidades ofrecidas, aclarando si es necesaria la instalación de un estabilizador externo para prever anomalías de la red domiciliaria de alimentación o si es suficiente con el estabilizador propio de la fuente de alimentación del equipo.
- Superficie propia ocupada por los equipos incluyendo puertas o paneles abiertos para su mantenimiento y espacio destinado a la operación de los mismos, si fuera necesario.
- Otras características que deban ser tenidas en cuenta para la instalación.

Si el oferente no suministra las especificaciones de la instalación física, se entenderá que no es imputable la falla al mal uso de los equipos por parte del usuario y por lo mismo las eventuales fallas estarán sujetas a reparación dentro de la cobertura que ofrece la garantía.

VI: GARANTIA

El adjudicatario deberá proveer, a partir de la fecha de instalación y puesta en funcionamiento y por el período de cinco (5) años, un servicio de garantía integral (partes, mano de obra y reemplazo inmediato de partes dañadas) para todo el hardware ofertado, con atención en el lugar de instalación incluyendo repuestos, traslados y mano de obra.

La garantía de funcionamiento comprenderá el servicio de reparación con provisión de repuestos y/o cambio de las partes que sean necesarias sin cargo alguno para S.E. Casa de Moneda. El proveedor garantizará que el servicio técnico será brindado por personal especializado de la empresa fabricante de los productos ofrecidos, o en su defecto por su propio plantel especializado el que deberá estar debidamente autorizado por los fabricantes de los productos ofrecidos.

Los materiales y repuestos a emplear deberán ser originales de fábrica o de calidad similar, nuevos y sin uso, debiendo presentarse la documentación que respalde las citadas características.

La propiedad de los repuestos que se instalen será de S.E. Casa de la Moneda. La propiedad de las partes reemplazadas será del proveedor.

La relación para el cumplimiento de la garantía será directamente entre el representante del oferente y el responsable de la S.E. Casa de Moneda.

Los oferentes que consideren necesaria la realización de mantenimiento preventivo durante el período de garantía solicitado deberán incluir un plan a efectos de coordinar con la S.E. Casa de Moneda las fechas y horarios en que serán llevados a cabo. De no ser presentado se interpretará que la firma oferente no considera necesario el mismo.

Los siguientes criterios son aplicables al equipamiento solicitado:
• El servicio de garantía deberá estar disponible en la modalidad de 7x24.
• El tiempo de respuesta a los llamados deberá ser en la modalidad de 7x24.
• El tiempo máximo para la reparación o reemplazo de los equipos será de 48hs. de efectuarse el llamado (considerando solo días hábiles).

Cuando la magnitud de la avería requiera el traslado del equipamiento para su reparación en laboratorio, el mismo será por cuenta y responsabilidad del adjudicatario y no generará ningún costo adicional para S.E. Casa de Moneda. Sólo se aceptará que los equipos sean retirados de las oficinas de S.E. Casa de Moneda para su reparación si previamente:
• El proveedor lo reemplaza por otro equipo de idénticas características.
•S.E. Casa de la Moneda autoriza en forma explícita el retiro de los equipos.

Si hubiera elementos o situaciones para los cuales no fuera aplicable la garantía, éstos y éstas deberán estar detallados en forma clara y explícita en la oferta. NO se aceptarán descripciones

ambiguas como ser “mal uso del equipamiento”. No se aceptarán posteriores adiciones a la lista explícita de elementos y/o situaciones no cubiertas por la garantía.

El costo del servicio de garantía deberá estar incluido en el precio de los equipos.

Todas las características del servicio ofrecido se deberán encontrar operativas al día de la apertura de esta licitación.

Los oferentes deberán especificar claramente las condiciones ambientales para que la garantía cubra cualquier eventualidad incluyendo:
• Tipo de alimentación y potencia eléctrica requerida por las unidades ofrecidas, aclarando si es necesaria la instalación de un estabilizador externo para prever anomalías de la red domiciliaria de alimentación o si es suficiente con el estabilizador propio de la fuente de alimentación del equipo.
• Superficie propia ocupada por los equipos incluyendo puertas o paneles abiertos para su mantenimiento y espacio destinado a la operación de los mismos, si fuera necesario.

VII: LUGAR Y PLAZO DE ENTREGA

Los equipos serán entregados por cuenta del adjudicatario en:
Sede Retiro
Av. Antártida Argentina 2085, Ciudad Autónoma de Buenos Aires. Código postal C1104ACH
Dos (2) equipos

Sede Don Torcuato
Ruta Panamericana 24500 Don Torcuato, Prov. Buenos Aires. Código postal B1611KRN
Dos (2) equipos

Se deberá realizar la entrega del total adjudicado dentro de los ……30…. días hábiles, contados a partir de la notificación de la orden de compra.

VIII: CONDICIONES DEL SERVICIO DE SEGURIDAD Y VIGILANCIA

La Adjudicataria deberá proporcionar antes del inicio de su actividad una nómina de la dotación que concurrirá a esta S. E. CASA DE MONEDA, detallando: Apellido y nombre, Tipo y Número de Documento de Identidad, Fecha de nacimiento, Nacionalidad, Domicilio, Teléfono (si lo tuviese).

Dicha nómina deberá ser actualizada con suficiente anticipación en caso de reemplazos y/o ampliaciones.

La Adjudicataria cumplirá y hará cumplir a todo su personal las normas y procedimientos de Seguridad que le exija S. E. CASA DE MONEDA.

Asimismo, presentará una nómina pormenorizada de las herramientas y/o maquinaria que ingresará a esta S. E. CASA DE MONEDA para realizar las tareas.

IX: CONDICIONES DE HIGIENE Y SALUBRIDAD

La Adjudicataria deberá generar y preservar a su costo las condiciones de higiene y salubridad requeridas para cumplir con las regulaciones vigentes y con los requerimientos solicitados por S. E. CASA DE MONEDA, referentes a documentación a presentar para ingreso a la Planta, desenvolvimiento de trabajos en obra y Normas de Seguridad, para todo su personal durante la ejecución de los trabajos.

La Adjudicataria deberá especificar por nota, en forma previa a la iniciación de los trabajos, los encuadramientos que dentro de las actividades a desarrollar se aplicarán dentro del marco normativo vigente y conforme a las condiciones de riesgo que, como resultado de los trabajos a efectuar, puedan originar situaciones de peligro para las instalaciones y/o personal de S. E. CASA DE MONEDA.

La Adjudicataria deberá designar un responsable de la aplicación, control y desarrollo de las medidas de Seguridad surgidas del ítem precedente, el cual deberá contactarse con los responsables del Servicio de Higiene y Seguridad de S. E. CASA DE MONEDA al correo electrónico: seguridadehigiene@casademoneda.gob.ar, en forma previa a la iniciación de las tareas, con el fin de garantizar el normal cumplimiento de las actividades.

X: SEGURO- CERTIFICADO DE COBERTURA

La Adjudicataria presentará en forma mensual y durante la extensión del contrato y/o ampliaciones, el Certificado de Cobertura emitido por la Aseguradora de Riesgos del Trabajo (ART) que tiene contratada para su personal en relación de dependencia o, en su defecto, el pago mensual de la Póliza de Accidentes Personales para el personal que reviste en otra modalidad de prestación.

Deberá informar de igual modo, el procedimiento a seguir en caso de accidente de trabajo de su personal.

XI: CUADRO DE CUMPLIMIENTO TECNICO

Se detalla a continuación cuadro con las características de prestaciones requeridas a fin de que el oferente indique en el mismo las características de lo cotizado:

Características	Especificación requerida	Especificación ofrecida	Observaciones
PRESTACIONES			
Poseerá compatibilidad con todos y cada uno de los siguientes estándares: Ethernet IEEE 802.3, Fast Ethernet IEEE 802.3u, Gigabit Ethernet IEEE 802.3z, 10 Gigabit Ethernet IEEE 802.3ae.	SI		
Los equipos deberán poder operar en alta disponibilidad (2 en sede retiro y 2 en sede Don Torcuato), en modalidad activo-activo y activo-pasivo. Cada uno de los equipos deberá tener la posibilidad de agregado de fuentes redundantes del tipo hot swap. El sistema deberá poder operar en modo Router (permitiendo el envío de paquetes en L2 y L3) como así también en modo transparente.	SI		
Deberá permitir la creación de al menos 10 sistemas virtuales dentro del mismo equipo, sin necesidad de hardware o licencias adicionales. Cada sistema virtual podrá operar en modo Router o Transparente sin limitaciones en forma simultánea sobre cada sistema virtual.	SI		
El sistema deberá permitir la definición de interfaces virtuales (VLANs) las que podrán estar asignadas a diferentes interfaces	SI		

físicas en diferentes sistemas virtuales. Deberá soportar el etiquetado de los paquetes según IEEE 802.1Q utilizando cualquier ID (1-4095). Asimismo deberá contar con soporte de VXLAN.			
El mecanismo de control de filtrado utilizado por el engine del firewall deberá estar basado en técnicas “statefull inspection” que crean conexiones virtuales, incluso para los protocolos connection-less como UDP y RPC.	SI		
El Firewall deberá poseer las configuraciones localmente, no dependiendo su funcionamiento de otros productos, servicios o herramientas de gestión centralizadas.	SI		
Las reglas deben permanecer en medio físico, no volátil. Estas reglas deberán poder definirse, diferenciando protocolo, IP destino/origen, puerto destino/origen y geolocalización utilizando rangos horarios.	SI		
El dispositivo deberá soportar al menos la generación de 10.000 políticas de firewall.	SI		
El dispositivo deberá soportar SNAT, DNAT y PAT. Será posible la aplicación de SNAT y DNAT y PAT en forma simultánea sobre una misma conexión.	SI		
Deberá soportar NAT estático y dinámico y PAT sobre cualquier tipo de conexión, tanto para IPv4 como IPv6. Deberá soportar NAT46 y NAT64 sobre la totalidad de las políticas de firewall.	SI		

Deberá soportar la configuración de NAT estático sobre todas las interfaces físicas y lógicas utilizando direcciones IP virtuales, que no sean las propias IP declaradas en las interfaces del firewall.	SI		
Cada Firewall deberá permitir el uso de objetos dinámicos aplicables a todo tipo de regla, definiendo las propiedades de los mismos sobre cada Firewall en particular. Los objetos deben poder referenciar servidores, redes, direcciones basadas en ubicación geográfica y servicios como mínimo.	SI		
Cada Firewall deberá poseer capacidad de manejo de apertura de puertos dinámicos en base a protocolos de uso común (HTTP, SMTP, FTP, H323, SIP) y posibilidad de crear sesiones personalizadas que manejen dicho comportamiento.	SI		
El equipo deberá permitir la implementación de políticas de calidad de servicio y Traffic Shaping soportando al menos: • Puertos físicos e interfaces agregadas o redundantes. • Políticas de QoS y Traffic Shaping por dirección de origen y destino, usuario y grupo. • La definición de tráfico con ancho de banda garantizado. • La definición de tráfico con máximo ancho de banda. • La definición de colas de prioridad. • La priorización de protocolo en tiempo real de voz (VoIP)	SI		

como H.323, SIP, SCCP, MGCP y aplicaciones como Skype. • El etiquetado de paquetes DiffServ, incluso por aplicación. • La modificación de los valores de DSCP para Diffserv. • La priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).			
El equipo deberá poseer la capacidad de entregar direcciones IP a los hosts conectados en sus interfaces LAN por medio del protocolo DHCP (DHCP server).	SI		
Cada Firewall deberá además soportar las siguientes funcionalidades: • Autenticación de usuarios en forma local y remota por medio de los protocolos RADIUS y LDAP, debiendo ser compatible con Active Directory. • Soporte de IPSec NAT Traversal.	SI		
El equipo deberá permitir la terminación de túneles VPN. • El Firewall deberá soportar túneles utilizando protocolo IPSEC estándar o a través de SSL. Para el caso de VPNs SSL, el equipo debe soportar que el usuario pueda realizar la conexión a través de un cliente VPN instalado en el sistema operativo de su máquina o a través de una interface web.	SI		
El equipo, con su funcionalidad de Next Generation Firewall activa deberá soportar un throughput requerido medido con tráfico real con la funcionalidad de control de	SI		

aplicaciones habilitada, para todas las firmas que el fabricante posea actualizadas con la última actualización disponible.			
El equipo, con su funcionalidad de Next Generation Firewall activa deberá soportar el throughput requerido medido con tráfico real con las siguientes funcionalidades habilitadas simultáneamente: Clasificación y control de aplicaciones, IPS, Control de navegación por URL, Antivirus y Antispyware, Control de amenazas avanzadas de día cero (Sandboxing). Para todas las firmas que la plataforma de seguridad posea totalmente activadas, actualizadas al día y con el mayor nivel de seguridad posible; considerando múltiples políticas de seguridad y que tengan habilitado la generación de Logs y NAT aplicado a todas las reglas.	SI		
El Control de Amenazas avanzadas (Sandboxing) deberá ser provisto en la solución. El mismo deberá estar disponible durante el período de garantía.	SI		
El Firewall deberá soportar la activación y desactivación de la funcionalidad de IPS, detección de anomalías y anti-malware para los protocolos soportados. • Deberá realizar el análisis de IPS basado en firmas las cuales se deberán poder agrupar para aplicar a las reglas. • Deberá permitir armar firmas propias de IPS.	SI		

• Deberá realizar la actualización de firmas de IPS en forma automática y periódica, durante el periodo de garantía. • Deberá poseer una base de conocimiento que detalle la definición de la regla. • Deberá ante un ataque de IPS responder con una notificación o un bloqueo del tráfico. • Deberá poseer la capacidad de excluir para una regla específica, una firma en particular; sin que ello implique deshabilitar por completo la utilización de esa firma en las demás reglas. • El motor de IPS deberá soportar el agregado de firmas específicas para ambientes industriales a los fines de interpretar los protocolos específicos de esos ambientes.			
El Firewall deberá identificar potenciales vulnerabilidades y sugerir las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de la solución. La información podrá brindarse mediante la GUI o vía reportes.	SI		
El Firewall deberá funcionar como proxy web explícito y como proxy transparente.	SI		
El Firewall deberá incorporar funcionalidades para SD-WAN. Si fuese necesario el agregado de licencias adicionales indicar cómo se aplican las mismas.	SI		
Capacidades de SD-WAN a soportar en el firewall:	SI		

• Balanceo de vínculos a Internet, VPNs y enlaces WAN (ej: MPLS) • Balanceo Round Robin, Balanceo por peso, cantidad de sesiones, ancho de banda y derrame. • Definición de políticas de SDWAN por Aplicación, Servicio de internet, usuarios, IPs o Interfaces/zonas. • Soporte a más de 5 vínculos a Internet. • Debe contar con un mecanismo por el cual se puedan recuperar los datos enviados sin necesidad de recurrir a las retransmisiones de protocolo TCP y que permita la reconstrucción del stream en el lado receptor.			
El Firewall deberá soportar la activación y desactivación de técnicas de detección y evasión de ataques de DOS (Denegación de Servicio).	SI		
Cada Firewall deberá soportar la activación y desactivación de técnicas de protección de ataques de generación masiva de conexiones (SYN attack) permitiendo su configuración para una dirección IP en particular.	SI		
Debe tener la función de protección a través de la resolución de	SI		

direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos.			
Deberá tener la posibilidad de aplicar la funcionalidad de antivirus por regla sobre conexiones HTTP, FTP, SMTP, POP3, IMAP y túneles VPN encriptados establecidas a través del equipo.	SI		
Deberá tener la funcionalidad de filtrado de contenidos Web. • Deberá permitir o bloquear el acceso de los usuarios a diferentes sitios web considerados o no maliciosos. • Deberá permitir el 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). • Deberá permitir la actualización automática de la base de filtrado de contenidos durante el transcurso del período de garantía. • Deberá soportar al menos sesenta (60) categorías en la base de filtrado.	SI		
Deberá tener la funcionalidad para detectar aplicaciones. Para ello el equipo deberá: • Inspeccionar el contenido del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas,	SI		

independiente de puerto y protocolo que utilicen. • Deberá reconocer al menos 3000 aplicaciones diferentes, permitiendo agrupar las mismas en al menos 16 categorías y aplicar políticas de seguridad a las mismas. Debe permitir la creación de firmas de aplicación manuales. • Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo. • Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo. • Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos.			
Deberá soportar la inspección de sesiones que atraviesan el firewall y utilizan el protocolo SSL (Secure Sockets Layer) para encriptación, incluyendo el protocolo HTTPS.	SI		
El equipo deberá proveerse con los servicios de actualización de firmas para los motores de filtrado descriptos en los puntos anteriormente mencionados por el término de 60 meses.	SI		
Debe permitir la administración del equipo por medio de los protocolos	SI		

HTTP/HTTPS, Telnet/SSH y SNMP v1/v2.			
Deberá permitir el registro local y remoto de eventos utilizando servidores syslog.	SI		
Controlador de puntos de conexión inalámbricos o WIFI. Dicha función deberá estar integrada dentro de la solución de firewall requerida (sede Retiro: 60 dispositivos y sede Don Torcuato: 20 dispositivos).	SI		
En el caso de requerir una licencia específica para la funcionalidad de Controlador WIFI especificarlo.	SI		
Debe permitir la conexión de dispositivos inalámbricos que implementen los estándares IEEE 802.11a / b / g / n / ac y que transmitan tráfico IPv4 e IPv6 a través del controlador;	SI		
La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor;	SI		
El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS	SI		
La solución debe optimizar el rendimiento y la cobertura inalámbrica (RF) en los puntos de acceso administrados por ella, realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados. La solución debe permitir además deshabilitar el ajuste automático de potencia y canales cuando sea necesario	SI		

Permitir programar día y hora en que ocurrirá la optimización del aprovisionamiento automático de canales en los Access Points	SI		
El encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser tuneleados hasta el controlador inalámbrico	SI		
Cuando tuneleado, el tráfico debe ser encriptado a través de DTLS o IPSEC	SI		
Debe permitir la administración de puntos de acceso conectados remotamente a través de WAN. En este escenario el encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe ocurrir de forma distribuida (local switching), o sea, el tráfico debe ser cambiado localmente en la interfaz LAN del punto de acceso y no necesitará de tunelamiento hasta el controlador inalámbrico;	SI		
Cuando el tráfico se conmuta directamente en los puertos Ethernet de los puntos de acceso (local switching) y la autenticación sea WPA/WPA2-Personal (PSK), en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse	SI		

la conexión de nuevos usuarios a la red inalámbrica			
La solución debe permitir definir qué redes serán tuneleadas hasta la controladora y qué redes serán conmutadas directamente por la interfaz del punto de acceso;	SI		
La solución debe soportar el recurso de Split-Tunneling de forma que sea posible definir, a través de las subredes de destino, qué paquetes serán tuneleados hasta el controlador y cuáles serán conmutados localmente en la interfaz del punto de acceso	SI		
La solución debe permitir el equilibrio de carga de los usuarios conectados a la infraestructura inalámbrica de forma automática. La distribución de los usuarios entre los puntos de acceso cercanos debe ocurrir sin intervención humana y basada en criterios como número de dispositivos asociados en cada punto de acceso	SI		
La solución debe tener mecanismos para detectar y mitigar los puntos de acceso no autorizados, también conocidos como Rogue AP. La mitigación debe realizarse de forma automática y batida en criterios tales como: intensidad de señal o SSID. Los puntos de acceso administrados por la solución deben evitar la conexión de clientes en puntos de acceso no autorizados	SI		
La solución debe mostrar información sobre los dispositivos conectados a la infraestructura	SI		

inalámbrica e informar al menos la siguiente información: Nombre de usuario conectado al dispositivo, Fabricante y sistema operativo del dispositivo, Dirección IP, SSID al que está conectado, Punto de acceso al que está conectado, Canal al que está conectado, Banda transmitida y recibida (en Kbps), intensidad de la señal considerando el ruido en dB (SNR), capacidad MIMO y horario de la asociación			
La solución debe implementar reglas de firewall (stateful) para controlar el tráfico permitiendo o descartando paquetes de acuerdo con la política configurada, reglas que deben utilizar como criterio de interfaz de origen el SSID de la red WIFI	SI		
La solución debe monitorear y clasificar el riesgo de las aplicaciones accesadas por los clientes inalámbricos	SI		
Permitir configurar el bloqueo en la comunicación entre los clientes inalámbricos conectados a un SSID	SI		
Debe implementar la autenticación administrativa a través del protocolo RADIUS	SI		
En combinación con los puntos de acceso, la solución debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES)	SI		
En combinación con los puntos de acceso, la solución debe ser compatible e implementar el método de autenticación WPA3	SI		

La solución debe permitir la configuración de múltiples claves de autenticación PSK para su uso en un SSID determinado	SI		
Cuando se utiliza la función de múltiples claves PSK, la solución debe permitir la definición de límite en cuanto al número de conexiones simultáneas para cada clave creada	SI		
La solución debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios basados en los atributos proporcionados por los servidores RADIUS	SI		
La solución debe implementar el mecanismo de cambio de autorización dinámica a 802.1X, conocido como RADIUS CoA (Change of Authorization) para autenticaciones 802.1X	SI		
La solución debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP	SI		
La solución debe implementar la característica de autenticación de los usuarios a través de la página web HTTPS, también conocido como Captive Portal. La solución debe limitar el acceso de los usuarios mientras éstos no informen las credenciales válidas para el acceso a la red	SI		
La solución debe permitir el hospedaje del captive portal en la memoria interna del controlador inalámbrico	SI		
La solución debe permitir la personalización de la página de	SI		

autenticación, de forma que el administrador de red sea capaz de cambiar el código HTML de la página web con formato de texto e insertar imágenes			
La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red	SI		
La solución debe permitir que la página de autenticación se quede alojada en un servidor externo	SI		
La solución debe permitir el registro de cuentas para usuarios visitantes en la memoria interna. La solución debe permitir que sea definido un período de validez para la cuenta creada	SI		
La solución debe garantizar que los usuarios se autentiquen en el portal cautivo que utilice la dirección IPv6	SI		
La solución debe tener interfaz gráfica para administrar y gestionar las cuentas de usuarios visitantes, no permitiendo acceso a las demás funciones de administración de la solución	SI		
Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado	SI		
La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes	SI		
La solución debe identificar automáticamente el tipo de equipo y sistema operativo	SI		

utilizado por el dispositivo conectado a la red inalámbrica			
La solución debe permitir que los usuarios puedan acceder a los servicios disponibles a través del protocolo Bonjour (L2) y que estén alojados en otras subredes, como AirPlay y Chromecast. Debe ser posible especificar en qué VLANs el servicio estará disponible	SI		
La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog	SI		
La solución debe permitir ser administrada a través del protocolo SNMP (v1, v2c y v3), además de emitir notificaciones a través de la generación de traps	SI		
La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP	SI		
La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB)	SI		
La solución debe presentar gráficamente la topología lógica de la red, representar los elementos de la red gestionados, además de información sobre los usuarios conectados con la cantidad de datos transmitidos y recibidos por ellos	SI		
La solución debe permitir la adición de controlador redundante operando en N + 1. En este modo, el controlador redundante debe monitorear la disponibilidad y sincronizar la configuración del principal,	SI		

además de asumir todas las funciones en caso de error del controlador principal. De esta forma, todos los puntos de acceso deben asociarse automáticamente al controlador redundante que pasará a tener función de primario de forma temporal			
La solución debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red. Debe ser posible especificar en qué puntos de acceso o grupos de puntos de acceso que cada dominio estará habilitado	SI		
La solución debe garantizar al administrador de la red determinar los horarios y días de la semana que las redes (SSID) estarán disponibles para los usuarios	SI		
La solución debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming	SI		
La solución debe implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute la itinerancia	SI		
La solución debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente	SI		

conectada mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos			
La solución debe implementar el estándar IEEE 802.11w para prevenir ataques a la infraestructura inalámbrica	SI		
La solución debe soportar priorización a través de WMM y permitir la traducción de los valores a DSCP cuando los paquetes se destinan a la red de cableado	SI		
La solución debe permitir la configuración del valor de Short Guard Interval para 802.11n y 802.11ac en 5GHz	SI		
La solución provista debe tener la capacidad de hacer Reporting, Análisis y guardar logs. Esta solución deberá ser de la misma marca que los equipos propuestos. • Deberá poder ser desplegado como una Máquina Virtual (VM) sobre infraestructura KVM o VMWare. • El sistema deberá analizar los registros provenientes de múltiples dispositivos, por usuario o por grupo de usuarios • Deberá generar una variedad de reportes que permiten a los administradores de red asegurar las redes de manera proactiva conforme se presentan las amenazas, evitando los abusos de red. • El sistema deberá permitir la visualización de registros o	SI		

cualquier mensaje o archivo de registro desde los dispositivos registrados. Deberá implementar filtros que permitan navegar sobre los registros de forma simple y amigable. • El sistema deberá implementar reportes que permitan a los administradores conocer al menos: • Ataques: por unidad, por hora del día, por categoría, y por fuentes de los ataques. • Virus: principales virus detectados en la red y detectados por Protocolo. • Eventos: Por Firewall, eventos en general, eventos de seguridad desencadenados y eventos desencadenados por el día de la semana. • Utilización de la Red: Principales usuarios de la Red y principales clientes intentando acceder a sitios bloqueados. • Ancho de banda: Principales usuarios de ancho de banda. Ancho de banda por día, por hora y utilización de ancho de banda por familia de protocolos. • Protocolos: los principales protocolos utilizados, usuarios FTP y usuarios de Telnet. • El sistema deberá implementar análisis forenses de forma que se pueda rastrear las actividades de un usuario. • El sistema deberá ser administrable vía Web utilizando HTTPs.			

Los administradores podrán ser por dominio y deberá poder asignarse de qué equipos (por dirección IP y máscara) puede el administrador conectarse. • El sistema deberá soportar al menos dos niveles de administración: Lectura/Escritura (Read/Write) y Sólo Lectura (Read-Only). • Debe contar con reporte de AP´s y SSID´s autorizados, así como clientes WIFi			
La solución provista deberá contar con el espacio para el almacenamiento permanente de los logs y espacio para el guardado de los logs diarios que se utilizarán para la Analítica.	SI		
Debe soportar servicio de Indicadores de Compromiso del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.	SI		
La solución provista deberá tener no menos de 3 TB de Almacenamiento permanente de logs y 6 Gbps para Analítica de logs diarios.	SI		
GARANTIA integral por el término de cinco (5) años.	SI		

XII: PRUEBAS Y COMPROBACIONES

- S.E. CASA DE MONEDA se reserva el derecho de solicitar al oferente, cuando este lo requiera, ponga a su disposición, un equipo de idénticas características al que cotiza en la oferta, de manera de poder verificar que responde al modelo ofertado con las características solicitadas y poder realizar sobre el mismo las pruebas de performance.

- Estas pruebas y comprobaciones no implicarán reconocimiento de gasto por parte de S.E. CASA DE MONEDA y el material necesario para la misma será facilitado sin cargo por el oferente.

- La fecha y lugar de aplicación de las pruebas serán convenidos entre el S.E. CASA DE MONEDA y el oferente a efecto de que las mismas se realicen dentro de los 10 (diez) días hábiles siguientes a la apertura de las ofertas. Con tal fin el oferente deberá disponer de los elementos ofrecidos a las 48hs. contadas a partir de su notificación por parte de S.E. CASA DE MONEDA.

- No se aceptará probar equipamiento cuyas características, marca y/o modelo no se correspondan exactamente con la oferta.

XIII: VISITA DE OBRA

A los fines de la exacta apreciación de las características de los trabajos, sus dificultades y sus costos, el oferente deberá efectuar una visita (obligatorio) a los lugares de emplazamiento de los trabajos, a fin de examinar por su cuenta las condiciones en que recibirá las instalaciones, previo a la presentación de la oferta.

Al momento de la visita se le extenderá un certificado de visita de obra, que deberá ser presentado junto con la oferta. Las visitas podrán efectuarse hasta 96 hs. antes de la fecha de apertura de ofertas, en el horario de 10:00hs. a 16:00hs. y deberán coordinarse en tecnologia@casademoneda.gob.ar.

El no cumplimiento de la inspección puede ser causa de desestimación de la oferta, al sólo y exclusivo juicio de Casa de Moneda, no dará derecho a reclamo alguno a los oferentes por desconocimiento de las instalaciones.