Solución de seguridad avanzada, protección de endpoint, detección y respuesta.

1. Solución de seguridad avanzada, protección de endpoint, detección y respuesta.

1.1. OBJETIVOS

Se pretende una solución de seguridad avanzada con detección, prevención y bloqueo post infección en tiempo real de malware. Mediante esto desactivar amenazas potenciales en tiempo real y automatizar los procedimientos de respuesta y remediación con playbooks personalizables.

1.2. ALCANCE DE LA SOLUCIÓN

El presente Pliego deberá incluir la provisión, configuración, instalación y puesta en marcha, contemplando el esquema actual y Tunning post instalación, garantizando los objetivos planteados.

1.3. CARACTERÍSTICAS PARTICULARES DE LO SOLICITADO.

1.3.1. Requerimientos del Agente

1.3.1.1. La solución propuesta debe ser compatible con los siguientes sistemas operativos:

- Windows (32-bit & 64-bit versiones) XP SP2/SP3, 7, 8, 8.1 y 10.
- Windows Server 2003 R2 SP2, 2008 R1 SP2, 2008 R2, 2012, 2012 R2, 2016 y 2019.
- MacOS Versiones: Yosemite (10.10), El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) y Catalina (10.15).
- Linux Versiones: RedHat Enterprise Linux y CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 y 7.7 y Ubuntu LTS 16.04.5, 16.04.6, 18.04.1 y 18.04.2 server, 64-bit. Ambientes Virtual Desktop Infrastructure (VDI) en VMware Y Citrix. VMware Horizons 6 y 7, y Citrix XenDesktop 7.

1.3.1.2. Debe tener un consumo máximo de 120MB de memoria RAM, un consumo promedio de menos de 2% de uso de CPU y un consumo menor a 20MB de espacio en disco.

1.3.1.3. Debe soportar el despliegue masivo a través de herramientas como MS System Center, JAMF, y Satellite.

1.3.1.4. Debe tener la habilidad de actualizar el Endpoint sin interacción por parte del usuario y sin requerimiento de reinicio.

1.3.1.5. Debe tener protección "Anti-Tamper" en el Agente.

1.3.1.6. Debe trabajar sin depender de firmas hash locales conocidas para la detección de archivos maliciosos.

1.3.1.7. Debe poder registrar en tiempo real información del proceso e informaciones adicionales tal como conocer el usuario asociado con los eventos.

1.3.1.8. Debe contar con la opción de establecer contraseña para desinstalar el agente en el endpoint.

1.3.1.9. El collector a ser instalado en los endpoint de la solución propuesta debe poder trabajar detrás de un proxy.

1.3.2. Detección de Malware

1.3.2.1. La solución propuesta debe poder:

1.3.2.2. funcionar en modalidad "offline" fuera de línea sin que el Agente se encuentre conectado a la red empresarial.

- Detectar procesos en ejecución, inicios de procesos, paradas de procesos e interacciones entre procesos.
- Detectar cambios realizado por procesos maliciosos en el registro de las PC.
- Detectar solicitudes DNS enviadas desde el dispositivo.
- Detectar conexiones de red desde el dispositivo.
- Detectar actividad sospechosa asociada con archivos DLL.
- Incorporar inteligencia de amenazas en el esquema de detección.
- Incorporar las técnicas de MITRE ATT&CK en el esquema de -detección.
- Identificar actividad maliciosa conocida.
  - Debe tener la capacidad de recibir actualizaciones diarias de inteligencia.
  - Debe tener la capacidad de categorizar los eventos detectados en diferentes categorías (Ej: Malicioso, Sospechoso, No concluyente, Probablemente Seguro).

1.3.3. Prevención de Malware

La solución propuesta debe tener la capacidad de prevención de ejecución de archivos maliciosos.

Debe incorporar un motor de antivirus de última generación (NGAV) basado en el kernel con capacidad de "Machine Learning".

Debe tener capacidad de controlar dispositivos USB.

Debe poder bloquear tráfico malicioso de exfiltración de datos, debe poder bloquear tráfico malicioso de comunicación hacia C&C (Command & Control).

Debe poder frenar brechas de seguridad e intentos de ransomware en tiempo real.

Debe poder evitar cifrados de disco causado por ransomware y modificación de archivos o registro de los dispositivos.

Debe poder ser configurada en modo de simulación donde no se realicen bloqueos, pero toda actividad maliciosa es registrada.

Debe poder permitir la modificación de las reglas de detección de eventos maliciosos para que estas reglas solo almacenen un registro o estén en modo bloqueo.

Debe poder permitir la realización de escaneos periódicos de los archivos contenidos en los dispositivos con el Agente instalado.

1.3.4. Difusión (Post-infección)

La solución propuesta debe permitir el bloqueo automático de un dispositivo donde se ha encontrado una actividad causada por malware. Debe permitir el bloqueo de las actividades realizadas por parte de archivos maliciosos.

Debe tener la capacidad de creación de WhiteList/Blacklist para los archivos basados en su hash: MD5, SHA1 y SHA256. Debe tener la capacidad de creación de WhiteList/Blacklist para los archivos basados en el nombre de estos. Debe tener la

capacidad de creación de WhiteList/Blacklist para los archivos basados en la localización de este (File Path). Debe tener la capacidad de creación de WhiteList/Blacklist para las aplicaciones basada en el nombre, versión y proveedor de estas.

Debe tener la capacidad de reclasificar los falsos positivos de forma manual para marcar la actividad como falso positivo y evitar que ocurran detecciones similares. Debe tener la capacidad de recalificar automáticamente la actividad como falso positivo y evitar que ocurran detecciones similares.

Debe permitir la creación de excepciones de eventos basados en direcciones IP, aplicaciones y protocolos.

1.3.5. Respuesta a Incidentes

La solución propuesta debe permitir la integración con plataformas SIEMs (Security Information and Event Management) a través de un syslog.

Debe tener la capacidad:

- de abrir tickets en plataformas de gestión tales como ServiceNow y JIRA.
- para terminar un proceso basado en la clasificación de este.
- para eliminar un archivo basado en la clasificación de este.
- para restaurar la configuración base basada en la clasificación de actividad predefinida.
- para aislar dispositivos infectados de la red.
- para restringir el acceso del dispositivo a la red de forma automática según la clasificación de actividad detectada.

Debe obtener visibilidad completa de la cadena de ataque y cambios maliciosos.

Debe permitir la limpieza automática de los dispositivos y revertir los cambios maliciosos mientras mantiene el tiempo de disponibilidad del dispositivo.

Debe permitir la suscripción de servicios opcionales de detección y respuesta a incidentes (Ej: Servicios gestionados de detección y respuesta).

Debe permitir el envío de ejecutables para su análisis a un sandbox, con la finalidad de determinar si son maliciosos o inofensivos.

Debe proporcionar múltiples mecanismos de protección, incluida como la terminación de un proceso, eliminación de un archivo malicioso, el bloqueo de una conexión de red.

1.3.6. Control de Vulnerabilidades y Comunicación

La solución propuesta debe tener la capacidad para descubrir aplicaciones vulnerables que se estén comunicando a través de la red.

Debe tener la capacidad para realizar un parche virtual, a través de la restricción de los accesos de comunicación en aquellas aplicaciones que sean vulnerables.

Debe permitir la reducción de las superficies de ataque utilizando políticas proactivas de comunicación basadas en el riesgo de acuerdo con CVE y la calificación o reputación que puede tener una aplicación.

Debe tener la capacidad para prevenir la comunicación a través de la red de cualquier aplicación no autorizada.

Debe tener la capacidad para crear políticas que tengan la capacidad de prevenir la comunicación de aplicaciones de acuerdo con la versión de la aplicación instalada.

Debe poder detectar e identificar todas las aplicaciones en los dispositivos que se comunican en la red.

Debe poder visualizar y entregar información sobre el uso de aplicaciones en red mostrando información como los IP destinos y cuales dispositivos generan tráfico.

1.3.7. Escenarios de ataque

La solución propuesta debe identificar y prevenir los intentos de estalación de privilegios.

Debe bloquear ataques de ransomware conocido.

Debe detectar malware desconocidos como RAT (Remote Access Trojan) a través de las actividades del malware y no una firma.

Debe proteger contra Scripts de Powershell maliciosos.

Debe proteger contra Scripts de CScript maliciosos.

Debe proteger contra macros de Office maliciosos.

Debe tener control sobre dispositivos USB.

1.3.8. Consola de administración

La solución propuesta debe cumplir con el estándar GDPR

La consola de administración de la solución propuesta debe poder integrarse con:

- Soluciones de NGFW existentes en el mercado para suspender o bloquear la IP del endpoint luego de un evento de seguridad.
- Soluciones de NAC existentes en el mercado para la instrucción de cuarentena del endpoint luego de un evento de seguridad.
- Soluciones de sandboxing on premise o en la nube existentes en el mercado para permitir el análisis de archivos sospechosos y así proteger a los endpoints de ataques de día cero mediante esta tecnología.

Debe permitir la integración con "Active Directory" para garantizar el cumplimiento de los requisitos de la política de contraseñas de la empresa.

Debe permitir:

- El uso de autenticación de doble factor (2FA) para acceder a la misma
- El uso de roles granulares para los administradores
- La gestión para ambientes Multi-inquilinos.
- La gestión a través de Full Restful API

La solución propuesta debe poder ser gestionada completamente en nube sin requerimiento de servicios en las premisas

Debe poder ser gestionada en una arquitectura hibrida utilizando servicios en las premisas complementadas con otras en nube.

Debe permitir ser gestionada en una arquitectura totalmente en las premisas del cliente.

La solución propuesta debe soportar la integración con la base de inteligencia en la nube del fabricante para actualización de inteligencia de malware y amenazas.

La consola de administración de la solución propuesta debe permitir la:

- visualización de los eventos registrados en los dispositivos que requieran atención.
- visualización la salud de los Agentes instalados.
- desinstalación remota del Agente instalado en los dispositivos.
- desactivación/activación remota del Agente instalado en los dispositivos.
- actualización remota del Agente instalado en los dispositivos.
- creación de reportes ejecutivo conteniendo un resumen que describe los eventos de seguridad y el estado del sistema.
- creación de grupos organizativos de dispositivos en los cuales cada grupo podrá tener reglas de protección independiente de los demás.
- exportación de bitácoras locales generadas por los Agentes desde la misma consola.
- creación de reportes de inventario sobre los Agentes desplegados conteniendo información como: Dirección IP, Hostname, Sistema Operativo, Dirección MAC, Versión de Agente instalada, Estado del Agente, Último día visto por la consola.
- integración de un SMTP externo para el envío de alertas a través de correo electrónico.
- La consola de administración de la solución propuesta debe permitir las auditorías de cambios realizados por los administradores/operadores.

La consola de administración de la solución propuesta debe proporcionar la visibilidad de eventos generados por los dispositivos o eventos de acuerdo con el proceso ejecutado.

La consola de administración de la solución propuesta debe permitir las auditorías de cambios realizados por los administradores/operadores.

1.4. CAPACITACIÓN

Se deberá poner a disposición de ATER una capacitación para un grupo de hasta X usuarios a fin de permitir la incorporación del conocimiento necesario para la gestión de las funcionalidades de la solución.

2. Provisión, instalación y configuración de equipamiento de seguridad perimetral para Segmentación de la red LAN de Servidores

2.1. OBJETIVOS

La presente solicitud intenta dar solución a las siguientes problemáticas que ATER deberá enfrentar a corto plazo:

- Ampliar la capacidad y performance de sus redes de núcleo y centro de datos, para resolver limitaciones en el respaldo de la información crítica y la sincronización de los sistemas de contingencia.
- Elevar niveles de seguridad en la red LAN, frente a la obsolescencia tecnológica de los dispositivos de seguridad actuales.
- Implementar mecanismos de protección sobre los activos de información, con el objetivo de mitigar parcialmente los riesgos de ataques y explotación de vulnerabilidades, tanto desde Internet como desde las redes internas de la Organización (LAN y WAN).

Se pretende una solución de seguridad integral que permita proteger los activos de información de los potenciales ataques desde las redes internas donde se encuentran expuestos y al mismo tiempo permita el acceso seguro y controlado a los mismos.

Además, como la arquitectura actual de la red de datos de ATER es una red plana en una velocidad de 1Gb, se pretende migrar a una velocidad para sus Servers de 10Gb y segmentar la red para ampliar la capacidad y performance de las redes de núcleo y centro de datos. Para esto se quiere implementar un clúster de switches que permitan llevar a 10Gbps la velocidad mínima para los enlaces de distribución y servidores, y a 25Gbps la performance del núcleo en el centro de datos. A su vez que trabajará para incorporar las mejores prácticas actuales y los beneficios disponibles en la tecnología del tipo NGFW (Next Generation Firewall).

Esta alternativa permitirá una evolución gradual de la red, incorporando estas capacidades en los nuevos servidores y activos de red, como así también dotar de funciones de protección e información de control sobre eventos que podrían afectar a la seguridad de la red de datos. También se busca una relación costo/beneficio al considerar el estado actual de las tecnologías 10GE que permitirá evolucionar el núcleo en el futuro, llevando estos equipos a la capa de distribución con enlaces de distribución en 25Gbps.

2.2. GENERALIDADES.

Se deberá incluir la instalación, configuración, puesta en marcha, migración (de ser necesario) del esquema actual a la nueva plataforma, y tunning post instalación, garantizando los objetivos planteados.

Se aclara especialmente, que las tecnologías, protocolos, normas, estándares, nomenclaturas, etc., que puedan estar mencionadas son indicativas y orientativas. ATER analizará las soluciones tecnológicas que se propongan para logar el objetivo planteado por lo que "EL OFERENTE" podrá cotizar otras tecnologías, normas y estándares, cuya debida fundamentación deberá formar parte de la OFERTA.

Todas las especificaciones, calidades y cantidades detalladas se deberán entender como los **requerimientos mínimos pretendidos**, debiendo adicionalmente explicitarse todas aquellas ventajas y/o facilidades que el sistema propuesto presente por sobre las especificaciones solicitadas.

2.3. CARACTERÍSTICAS GENERALES DE LO SOLICITADO.

Es necesario implementar una solución de hardware y software que contemple la protección de los sistemas centrales (manejo unificado de amenazas), a través de una consola de administración consolidada con acceso a todas las configuraciones, monitoreo y manejo de todas las funciones disponibles.

La solución deberá soportar la política de seguridad del organismo, para lo cual se pretende contar con las funcionalidades necesarias para enfrentar la problemática de seguridad de una manera comprensiva, atendiendo la totalidad de las diferentes tecnologías que pueden suponer un peligro potencial; y al mismo tiempo contar con un nivel de granularidad tal que permita aplicar las reglas de esa política de seguridad a nivel de grupo de usuarios y/o servicios.

La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo. Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos.

Las funcionalidades de protección de red que conformarán la plataforma de seguridad, podrán ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación. La plataforma deberá estar optimizada para análisis de contenido de aplicaciones en capa 7.

La gestión de los equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red.

Deberá existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi.

La consola de administración deberá soportar como mínimo, inglés, Español y Portugués, como así también tendrá que soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad.

Respecto de la consola de monitoreo y control central, deberá poseer las siguientes características:

- Tener capacidad de recibir al menos 5 GB de logs diarios

- Contar con las actualizaciones, indicadores de compromiso y demás servicios en línea para contar con la funcionalidad plena de la herramienta por 36 meses.

2.3.1. Funcionalidades Generales de la consola de monitoreo y control central

Si la solución es virtualizada, debe ser compatible con los siguientes ambientes:

- VMware ESXi 5.0/5.1/5.5/6.0/6.5/6.7;
- Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2/2016
- Citrix XenServer 6.0+
- Open Source Xen 4.1+
- KVM on Redhat 6.5+ and Ubuntu 17.04
- Nutanix AHV (AOS 5.10.5)
- Amazon Web Services (AWS)
- Microsoft Azure.
- Google Cloud (GCP)
- Oracle Cloud Infrastructure (OCI)
- Alibaba Coud (AliCloud)

Además, no debe haber límites a la cantidad de múltiples vCPU ni para la expansión de memoria RAM

- Debe soportar acceso vía SSH, WEB (HTTPS) para la gestión de la solución

- Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interfaz gráfica (GUI) como vía línea de comandos en consola de gestión.

- Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.

- Soporte SNMP versión 2 y 3

- Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.

- Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución, como así también permitir activar y desactivar para cada interfaz de la plataforma, los permisos de acceso HTTP, HTTPS, SSH

- Autenticación de usuarios de acceso a la plataforma vía LDAP, Radius y TACACS+.

- Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos, burbuja y tabla.

- Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.

- Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la

dirección IP, usuario y contraseña de este.

- Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado

- Contar con mecanismos de borrado automático de logs antiguos.

- Permitir la importación y exportación de reportes

- Debe contar con la capacidad de crear informes en formato HTML, PDF, XML y CSV. Debe permitir exportar los logs en formato CSV

- Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora de este. Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.

- La solución debe contar con reportes predefinidos

- Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución

- Debe ser posible la duplicación de reportes existentes para su posterior edición. Debe tener la capacidad de personalizar la portada de los reportes obtenidos.

- Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.

- Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.

- Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas

- Debe poseer mecanismo de “Drill-Down” para navegar en los reportes de tiempo real.

- Debe permitir descargar de la plataforma los archivos de logs para uso externo.

- Tener la capacidad de generar y enviar reportes periódicos automáticamente.

- Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.

- Permitir el envío por email de manera automática de reportes. Debe permitir que el reporte a enviar por email sea al destinatario específico.

- Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.

- Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado. Debe permitir el uso de filtros en los reportes.

Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros. Permitir especificar el idioma de los reportes creados

- Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.

- Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.

- Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.

- Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.

- Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de estos.

- Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.

- Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.

- Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.

- Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.

- Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos

- Debe permitir visualizar en tiempo real los logs recibidos. Debe permitir el reenvío de logs en formato syslog. Debe permitir el reenvío de logs en formato CEF (Common Event Format).

- Debe incluir dashboard para operaciones SOC para monitorear lo siguiente:

    - las principales amenazas de seguridad para la red.
    - comprometimiento de usuarios y uso sospechoso de la web en la red.
    - el tráfico en la red.
    - el tráfico de aplicaciones y sitios web en la red
    - detecciones de amenazas de día cero en la red (sandboxing).
    - actividad de endpoints en la red.

- actividad VPN ren la red.
- puntos de acceso WiFi y SSIDs
- rendimiento de recursos local de la solución (CPU, Memoria)

- Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC

- Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3

- Debe permitir generar alertas de eventos a partir de logs recibidos. Debe permitir crear incidentes a partir de alertas de eventos para endpoint

- Debe permitir la integración al sistema de tickets ServiceNow

- Debe soportar servicio de Indicadores de Compromiso (IoC) 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.

- Debe permitir respaldar logs en nube publica de Amazon S3, en la nube publica de Microsoft Azure y en la de Gooogle Cloud

- Debe soportar el estándar SAML para autenticación de usuarios administradores

2.3.2. Reportes de Firewall

- Debe contar con reportes de:
  - Cumplimiento de PCI DSS
  - Utilización de aplicaciones SaaS
  - Prevención de perdida de datos (DLP)
  - VPN
  - Sistema de prevención de intrusos (IPS)
  - Reputación de cliente
  - Análisis de seguridad de usuario
  - Análisis de amenaza cibernética
  - Breve resumen diario de eventos e incidentes de seguridad
  - Tráfico DNS
  - Tráfico de correo electrónico
  - Top 10 de Aplicaciones utilizadas en la red

- Top 10 de Websites utilizadas en la red
- Uso de redes sociales
- Evaluación de riesgo para correo electrónico
- Cumplimiento PCI de Wireless.
- AP´s y SSID´s autorizados, así como clientes WIFi
- Vulnerabilidades de solución gestionada de seguridad de equipo terminal.
- Aplicaciones web

2.4. CARACTERÍSTICAS PARTICULARES DE LO SOLICITADO.

- Se pretende contar con un clúster de equipos del tipo NGFW en el centro de datos y sendos clústers de Switches tanto en el Centro de Datos de ATER como en el sitio de Disaster Recovery ubicado en el Data Center del Gobierno de Entre.

- Los equipos a proveer deberán soportar la funcionalidad de Statefull Firewall basado en políticas que permitan la discriminación de tráfico en base a interfaces, direcciones IP, puertos TCP/UDP, rango horario e identidad del usuario.

- Funcionalidad de control de aplicaciones que complemente la función de los filtros de contenido.

- Para cada una de las funcionalidades avanzadas de seguridad detalladas, deberá ser posible mantener múltiples perfiles de configuración y aplicarlos independientemente siguiendo la granularidad solicitada precedentemente.

- La solución deberá posibilitar la selección de pares de interfaces físicas para implementar funcionalidades de IPS puro, donde se analizan los flujos de tráfico sin tener presencia de red ni interferir con la arquitectura de nivel superior.

- La solución deberá brindar un mecanismo para el análisis de contenido cifrado SSL para detectar potenciales amenazas que de otro modo pasarían inadvertidas.

- La solución debe permitir la implementación de SD-WAN

- La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;

- Deberá soportar la capacidad de integrar la plataforma de seguridad perimetral con el esquema de autenticación de usuarios interno basado en MS Active Directory de forma tal de evitar la creación y mantenimiento de usuarios/password locales.

- Deberán permitir la segmentación de la red de datos de tal manera de separar los Servers de los equipos de la red.

- La solución debe soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.

- En este sentido, deberá tener la capacidad para autorizar usuarios activos del dominio sin solicitarles el reingreso de usuario y contraseña.

- Adicionalmente, deberá soportar los protocolos de enrutamiento dinámico avanzados OSPFv2 y BGP-4+.

- Deberá permitir la implementación de traffic shaping con el nivel de granularidad indicado en el presente apartado.

- La información de las funcionalidades dinámicas (patrones IPS, firmas AV, categorías de filtrado de contenido, etc.) deberán mantenerse actualizadas en forma automática sin implicar interrupción del servicio.

- El equipamiento principal deberá contemplar la redundancia y disponibilidad que evite un punto único de falla (Alta disponibilidad - HA)

2.5. EQUIPAMIENTO MINIMO SOLICITADO.

La solución, al menos, deberá componerse de dos (2) dispositivos de estado sólido tipo appliance, con características de NGFW, cada uno con al menos:

- Throughput de por lo menos 70 Gbps con la funcionalidad de firewall habilitada para tráfico UDP IPv4 y IPv6, independientemente del tamaño del paquete.

- Soporte de por lo menos 7.8M conexiones simultáneas. Soporte de por lo menos 550K nuevas conexiones por segundo.

- Throughput de al menos 55 Gbps de VPN IPSec

- Estar licenciado para, o soportar sin necesidad de licencia, 2K túneles de VPN IPSec site-to-site simultáneos. Estar licenciado para, o soportar sin necesidad de licencia, 50K túneles de clientes VPN IPSec simultáneos

- Throughput de al menos 4,3Gbps de VPN SSL

- Soportar al menos 2500 clientes de VPN SSL simultáneos

- Soportar al menos 14Gbps de throughput de IPS

- Soportar al menos 9Gbps de throughput de Inspección SSL

- Soportar al menos 11.5Gbps de throughput de NGFW, entendido como la aplicación concurrente de las funciones de Statefull Firewall, IPS y Application control, con registro de eventos habilitado.

- Soportar al menos 10.5Gbps de throughput de Threat Protection, entendido como la aplicación concurrente de las funciones de Statefull Firewall, IPS, Application control y Malware protection, con registro de eventos habilitado.

- Incluir funciones de controlador inalámbrico con capacidad instalada para gestionar al menos 512 Access Points en modo tunelizado

- Incluir funciones de controlador de los switches incluidos en la propuesta, con capacidad instalada para gestionar al menos 96 switches.

- Tener al menos 16 interfaces 1GE/RJ45 y 8 slots GE/SFP

- Tener al menos 4 slots 10GE/SFP+ y 4 slots 25GE/SFP28

- Incluir la capacidad para implementar al menos 10 contextos o sistemas virtuales lógicos.

- Incluir la capacidad para implementar un clúster de alta disponibilidad con 2 equipos iguales.

- Incluir doble fuente de alimentación en configuración redundante 1+1

- Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q; deben soportar agregación de enlaces 802.3ad y LACP, Policy based routing y policy based forwarding, encaminamiento de multicast (PIM-SM y PIM-DM), soportar DHCP Relay, soportar DHCP Server, sFlow, Jumbo Frames. Deben soportar sub-interfaces Ethernet lógicas. Debe ser compatible con NAT dinámica (varios-a-1 y muchos-a-muchos). Debe soportar NAT estática (1-a-1). Debe admitir NAT estática (muchos-a-muchos). Debe ser compatible con NAT estático bidireccional 1-a-1. Debe ser compatible con la traducción de puertos (PAT). Debe ser compatible con NAT Origen y con NAT de destino. Debe soportar NAT de origen y NAT de destino de forma simultánea. Debe soportar NAT de origen y NAT de destino en la misma política.

- Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico.

- Debe ser compatible con NAT64 y NAT46. Debe implementar el protocolo ECMP.

- Debe soportar SD-WAN de forma nativa

- Debe soportar el balanceo de enlace hash por IP de origen. Debe soportar el balanceo de enlace por hash de IP de origen y destino;

- Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces. Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales.

- Debe 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. Enviar logs a sistemas de gestión externos simultáneamente. Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL.

- Debe soportar protección contra la suplantación de identidad (anti-spoofing)

- Implementar la optimización del tráfico entre dos dispositivos

- Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP). Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3). Soportar OSPF

graceful restart.

- Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;

- Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico.

- Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico. Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas.

- Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente.

- Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3.

- Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster.

- La configuración de alta disponibilidad debe sincronizar: Sesiones y 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 y Tablas FIB

- En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace

- Debe soportar la creación de sistemas virtuales en el mismo equipo

- Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos

- Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;

- Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);

- Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red. El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red.

- Debe soportar controles de zona de seguridad. Debe contar con políticas de control por puerto y protocolo

- Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones. Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad.

- Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad. Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall.

- Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.

- Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF)

- Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes

- Debe soportar el protocolo estándar de la industria VXLAN

- En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN

- Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo. Detección de miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, 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;

- 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;

- Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas.

- Actualización de la base de firmas de la aplicación de forma automática.

- Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos. Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas.

- Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;

- El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos. Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo. Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo. Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video. Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.

- Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc), Nivel de riesgo de la aplicación, Categoría de Aplicación, etc.

- Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente.

- Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo. Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware). Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante. Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad. Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos. Deber permitir el bloqueo de vulnerabilidades y exploits conocidos. Debe incluir la protección contra ataques de denegación de servicio. Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo. Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo. Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP, Re ensamblado de paquetes TCP, Bloqueo de paquetes con formato incorrecto (malformed packets). Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc.

- Detectar y bloquear los escaneos de puertos de origen. Bloquear ataques realizados por gusanos (worms) conocidos. Contar con firmas específicas para la mitigación de ataques DoS y DDoS. Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);

- Debe poder crear firmas personalizadas en la interfaz gráfica del producto;

- Identificar y bloquear la comunicación con redes de bots.

- Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo.

- Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.

- Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos. Los eventos deben identificar el país que origino la amenaza. Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms). Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP.

- Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;

- En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles. Proporcionar protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube).

- Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc.

- Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios. Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios.

- Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix, Horizon y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;

- Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;

- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma. Debe incluir al

menos dos tokens de forma nativa, lo que permite la autenticación de dos factores.

- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen. Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino. Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo. Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube. Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto. En QoS debe permitir: la definición de tráfico con ancho de banda garantizado, permitir la definición de tráfico con máximo ancho de banda y permitir la definición de colas de prioridad.

- Soportar marcación de paquetes DiffServ, incluso por aplicación. Soportar la modificación de los valores de DSCP para Diffserv. Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service). Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.

- Permitir la creación de filtros para archivos y datos predefinidos. Los archivos deben ser identificados por tamaño y tipo. Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones. Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos. Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos. Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares.

- Soporte VPN de sitio-a-sitio y cliente-a-sitio. Soportar VPN IPSec. Soportar VPN SSL.

- La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512. La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14. 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). Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall. Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec. Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting. Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy.

- Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;

- Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.

- El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos

Windows y Mac OS.

Por otro lado, se deberán proveer 4 (cuatro) switches de Core. Dos (2) para el centro de datos principal y dos (2) para el sitio de contingencia, de acuerdo a los siguientes parámetros:

- Mínimo de 24 puertos SFP+ capaces de configurarse como interfaces 1GE y 10GE. Mínimo de 2 puertos de cuatro canales integrados QSFP+/QSFP28, capaces de configurarse para permitir vínculos de 40GE y 100GE.
- Tener 1 puerto 1GE de gestión dedicado. Tener interfaz de consola RJ-45
- Form Factor del tipo 1 RU
- Capacidad de conmutación dúplex de 880 Gbps. Soportar 1309 Mpps. MAC address storage mínimo de 96 K. Tabla de enrutamiento de 16K entradas. Host Table de 24K entradas
- Soportar protocolos de enrutamiento dinámico OSPFv2, RIPv2, VRRP, BGP, ISIS
- Latencia máxima menos a 2µs
- Soportar Link Aggregation Groups con hasta 48 elementos. Soportar al menos 24 Link Aggregation Groups. Packet buffers de al menos 8 MB
- Memoria DRAM de al menos 8 GB
- Doble fuente y alimentación AC, redundante y reemplazable en caliente (hot swap)
- MTBF superior a 140 mil horas
- Temperatura de operación al menos en el rango 0-40 ºC
- Deberá suportar Split Port en los puertos Q*, a través del uso de cable breakout, permitiendo múltiples enlaces independientes: 4x10GE, 4x25GE y 2x50GE.
- Deberá aceptar actualizaciones de firmware, soportar detección y notificación de conflictos de direcciones IP, administración en la nube, administración por IPv4 y IPv6, Telnet / SSH para acceso a consola, soportar HTTP / HTTPS, SNMP v1/v2c/v3, permitir configuración de servidor NTP, contar con una interface de línea de comando y una interface de configuración web, soportar actualizaciones de Software por TFTP/FTP/GUI, deberá suportar HTTP REST API para configuración y monitorización.
- Deberá soportar Multi-Chassis LAG (MCLAG) y STO sobre Multi-Chassis LAG (MCLAG)
- Soportar priorización de tráfico basado en 802.1p, priorización de tráfico basado en IP TOS/DSCP, marcación de tráfico con 802.1p y/o IP TOS/DSCP. Link Aggregation estático, LACP, Spanning Tree, Jumbo Frames, negociación automática de puertos y de Duplex, IEEE 802.1D MAC Bridging/STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), STP Root Guard, STP BPDU Guard, Edge Port / Port Fast, IEEE 802.1Q

VLAN Tagging, Private VLAN, IEEE 802.3ad Link Aggregation com LACP, deberá ser capaz de balancear tráfico Unicast/Multicast en un mismo puerto Trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac, IEEE 802.1AX Link Aggregation, Spanning Tree (MSTP/CST), IEEE 802.3x Flow Control con Back-pressure, IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3z 1000Base-SX/LX, IEEE 802.3ab 1000Base-T, IEEE 802.3 CSMA/CD, Storm Control, creación de VLANS por MAC, IP y Ethertype-based, Virtual-Wire, Time-Domain Reflectometer (TDR), 4094 VLANS simultáneas, IGMP Snooping, IGMP Proxy y querier, emergency location identifier numbers (ELINs) no LLDP-MED, deberá ser posible limitar la cantidad de MACs aprendidos por puerto, permitir un mínimo de 15 instancias de MSTP, Storm Control de broadcast de forma independiente en cada puerto, detección y prevención de loops, VLAN Stacking (QinQ), SPAN, RSPAN e ERSPAN, soportar enrutamiento estático, RIP v2, OSPF v2, VRRP, IS-IS, BGP, protocolos de enrutamiento multicast, Equal Cost Multipath Routing (ECMP), Bidirectional Forwarding Detection (BFD), DHCP Relay, deberá soportar DHCP Server, RFC 2571 referente a arquitectura de SNMP, soportar DHCP Client, RFC 854 que especifica el protocolo TELNET, RFC 2865 referente a RADIUS, RFC 1643 que posee las definiciones de objetos gerenciados para interfaces Ethernet-like, soportar RFC 1213 referente a MIB-II, soportar la RFC 1354 - IP Forwarding Table MIB, RFC 2572 referente al procesamiento y envío de mensajes SNMP, soportar la RFC 1573 SNMP MIB II, soportar a RFC 1157 SNMPv1/v2c, soportar a RFC 2030 SNTP.

- Deberá soportar Port Mirroring, Autenticación admin por la RFC 2865 RADIUS, IEEE 802.1x authentication port-based, IEEE 802.1x authentication MAC-based, IEEE 802.1x Guest and Fallback VLAN, IEEE 802.1x MAC Access Bypass (MAB), IEEE 802.1x Dynamic VLAN Assignment, soportar Radius CoA (Change of Authority), IEEE 802.1ab Link Layer Discovery Protocol (LLDP), IEEE 802.1ab LLDP-MED, soportar Radius Accounting, EAP pass-through, detección de dispositivos, MAC-IP binding, Sflow, Flow Export, ACLs, múltiples ACLs de entrada, planificación de ACLs, soportar DHCP Snooping, soportar listas de servidores DHCP permitidos, soportar bloqueo de DHCP, deberá permitir Dynamic ARP Inspection (DAI), permitir Access VLANs, permitir tagging de tráfico con VLAN ID por medio de ACLs, soportar Syslog.

- Debe contener un sensor de temperatura interno. Debe permitir monitorear la temperatura del dispositivo

- Debe soportar QSFP+ low-power mode, Energy-Efficient Ethernet (EEE), QSFP+ low-power mode y Energy-Efficient Ethernet (EEE)

Todos los equipos proporcionados deben ser adecuados para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación.

La solución deberá incluir una suscripción de servicios por 36 meses que provea actualizaciones automáticas para soportar las funcionalidades de IPS y Protección de malware avanzado (Antivirus, Botnet, Mobile Malware, Outbreak prevention, cloud sandbox), actualizaciones de firmware y reemplazo avanzado de hardware.

Además se deberán proveer los cables y transceptores de acuerdo al alcance del proyecto, el equipamiento a conectar y las capacidades de estos para responder a los requerimientos de alta disponibilidad, según detalle:

- 10GE SFP+ Passive Direct Attach Cable, 3 m for Systems with SFP+ and SFP/SFP+

slots

- 10GE SFP+ Passive Direct Attach Cable, 5 m for Systems with SFP+ and SFP/SFP+ slots
- 10GE SFP+ Passive Direct Attach Cable, 7 m for Systems with SFP+ and SFP/SFP+ slots
- 10GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots
- 10GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots
- 40GE QSFP+ Passive Direct Attach Cable, 3 m for Systems with QSFP+ slots

El Oferente deberá presentar un plan de trabajo junto con el alcance de los servicios ya que se trata de un proyecto “llave en mano”. Se deberá incluir la propuesta con los servicios de despliegue de la solución, transferencia de conocimientos, soporte correctivo y adaptativo y un acompañamiento más allá del período de implementación.

La solución provista deberá asegurar las funcionalidades activas y actualizadas, las nuevas versiones de software y el reemplazo avanzado del hardware por un período no menor a 36 meses respaldado por el fabricante.

3. ANTECEDENTES DE LOS OFERENTES:

El Implementador de las tareas descriptas, deberá acreditar probados antecedentes y experiencia en proyectos similares a los descriptos en el presente pliego. El mismo, deberá adjuntar un "Curriculum Vitae", el cual se constituirá en elemento de valoración en el estudio de las respectivas propuestas.

El equipo técnico propuesto para participar del proyecto deberá contar con al menos 2 personas con certificaciones técnicas vigentes del fabricante de los productos ofertados.

El implementador será el responsable de la configuración y tunning de los equipos ofrecidos en la solución propuesta.

El oferente deberá presentar una nómina de Organismos públicos o privados donde se hayan realizado tareas similares a las solicitadas, indicando claramente, Nombre, Dirección, Teléfono y Contacto, preferentemente en la Pcia. de Entre Ríos.

4. HARDWARE, SOFTWARE, Y LICENCIAS:

Tanto el Hardware como el Software deberán encontrarse vigentes de comercialización y no discontinuados, ni ser discontinuado durante el presente año.

Asimismo, se pretende una solución integrada, por lo que no serán aceptadas ofertas que propongan una solución con materiales de distintos proveedores en sus partes esenciales (equipamiento de networking), debiendo presentar uniformidad en cuanto al modelo y la marca de los equipos ofrecidos.

Todos los elementos ofertados deberán ser nuevos y sin uso.

Todas las Licencias de Software serán provistas a nombre de Administradora Tributaria de Entre Ríos (ATER).

Será responsabilidad del proveedor la entrega de la constancia documental (COA Certificado de Autenticidad), correspondiente según la modalidad de comercialización a los Estado Provinciales, que utilicen los productores de dicho software (licencia escrita, sticker, manual con holograma, etc...).

Las actualizaciones de software, firmware y base de datos de firmas de antivirus deberán estar incluidas por un periodo no menor a tres años.

El proveedor deberá hacer constar, en el remito de entrega o en la factura de venta, el software y hardware entregado con todos sus datos (nombre y versión, cantidad de licencias, números de serie, costos etc...).

El software provisto con el/los equipos, deberá ser únicamente el/los solicitados en el presente pliego; todo otro software adicional que se ofrezca, deberá ser entregado con las licencia legales correspondientes.

5. CAPACITACION

Se deberá incluir en la cotización una capacitación orientada a la administración y configuración del equipamiento adquirido, contemplando específicamente conexionado de hardware y administración y configuración de software/firmware. La capacitación será brindada en las instalaciones de la ATER para un mínimo de 4 personas, y la cantidad de horas será acordada entre el adjudicatario y el personal de la Dirección General de Sistemas Informáticos de ATER, de acuerdo a las necesidades de la implementación.

El proveedor deberá realizar transferencia de conocimientos durante todo el proceso de instalación, y un informe detallado sobre el estado final de la misma, revisando y analizando las configuraciones y los mecanismos para mantener y expandir los servicios implementados y la asistencia remota durante los 60 días posteriores a la finalización del despliegue con asistencia on-site el último día de ese período.

6. CONTRATACION

El equipamiento a incorporar es totalmente importado, por lo cual se podrá realizar la adquisición del mismo, por el proceso de compra o leasing, a conveniencia de ATER, en dólares, pagaderos al dólar oficial del día anterior a la presentación de la factura correspondiente.

7. ADJUDICACION:

Para la adjudicación se tendrá especialmente en cuenta las propuestas que presenten equipos cuya marca reconocida, presencia y permanencia en el mercado nacional e internacional, ofrezcan al sólo criterio de ATER, garantías en su funcionamiento, calidad y soporte técnico.

Las ofertas deberán contemplar la posibilidad de realizar, a solicitud del Estado Provincial, y durante el período de análisis de ofertas, pruebas y demostraciones de los equipos ofrecidos, visitas a instalaciones similares efectuadas en las provincias de Entre Ríos, Santa Fé o donde el proveedor haya realizados instalaciones similares, en un radio no mayor a 600

km , consultas sobre todo tipo de dudas que requieran aclaraciones, incluyendo la provisión de documentación técnica adicional, sin que esto signifique, para el Estado Provincial, costo alguno o causal de demanda.

8. IMPUGNACIONES:

El tiempo establecido para recibir las impugnaciones de las ofertas presentadas, será de cuarenta y ocho horas (48hs) a partir del horario establecido para la apertura de los sobre de la presente licitación.

9. INSTALACION:

Todos los equipos deben entregarse instalados y en funcionamiento, para lo cual el adjudicatario deberá proveer todos los insumos o cableados necesarios para integrarlos a la red existente. De ser necesaria la instalación de soportes, kits de Rackeo, o cualquier otro elemento necesario para la implementación, deberá ser provisto por el Adjudicatario y estar incluido en los costos de instalación.
Se deberá proveer la totalidad de cables, conectores y demás elementos accesorios necesarios para la correcta instalación y funcionamiento, debiendo consensuar el modo de hacerlo con el personal de la Dirección de Sistemas Informáticos de ATER.

El plazo de instalación no deberá superar los noventa (90) días contados desde recepción de la Orden de Compra respectiva...

9.1. Tareas mínimas a realizar en esta Instalación:

La solución solicitada en el presente prevé se entregue la totalidad de la misma en pleno funcionamiento, para lo cual deberán considerarse:

- Consultoría para la revisión de la política de seguridad del organismo, para lo cual se deberá trabajar en conjunto con los responsables del área y redactar un documento que contenga los lineamientos resultantes, contemplando las reglas actualmente en vigencia y las nuevas que surjan de este estudio.
- Implementar un esquema de Single-Sign-On sobre la solución provista de tal manera que la autenticación se apoye exclusivamente sobre base de usuarios de Active Directory existente, evitando la necesidad de múltiples claves para un mismo usuario.
- Implementar las funcionalidades de protección IPS para los servicios publicados en Internet, ajustando sus características a cada escenario para optimizar la utilización de los recursos.
- Implementar funciones de control interno, hasta el punto que no interfiera en la performance, sobre el tráfico originado desde áreas de la LAN/MAN no controladas y con el objetivo primario de obtener información sobre el comportamiento actual de la red.

10. GARANTIA Y SERVICIO TECNICO:

El oferente indicará claramente el período de garantía (mínimo dos años), en el cual se hará cargo del correcto funcionamiento del/los elementos cotizados, como así también de la provisión de repuestos y disponibilidad de servicio técnico sin cargo.

La garantía alcanzará a los repuestos que fueren necesarios para la reparación de los elementos, como así también la mano de obra, la movilidad, permanencia y horas de trabajo.

11. RECEPCION E INSTALACION:

Los equipos deben ser entregados en las oficinas del Organismo Solicitante o donde este determine. Serán probados por personal técnico de la Dirección General de Informática de la Provincia de Entre Ríos, según las especificaciones de la Orden de Compra respectiva y del Pliego de Condiciones Técnicas correspondiente.

Dado que el proyecto es considerado una solución integral a pleno funcionamiento, se dará la recepción definitiva, una vez que el o los dispositivos, se encuentren instalados, configurados y funcionando en un todo de acuerdo al presente Pliego, autorizando la presentación de la correspondiente factura.