**ANEXO TÉCNICO**

**CONTRATAR LA COMPRA E INSTALACIÓN DE UNA SOLUCION DE SEGURIDAD PERIMETRAL PARA LA AGENCIA NACIONAL DE INFRAESTRUCTURA – ANI**

1. **Denominación del bien o servicio:**
   Solución de seguridad perimetral para la Agencia Nacional de Infraestructura – ANI.

2. **Unidad de medida**
   1 UTM (sistema de seguridad informática perimetral)

## 2.1. Descripción técnica

## SOLUCION DE SEGURIDAD PERIMETRAL PARA DE LA AGENCIA NACIONAL DE INFRAESTRUCTURA – ANI

| Ítem | Requerimiento Técnico Mínimo (de obligatorio cumplimiento) |
|---|---|
| 1.1 | **Generalidades.**<br><br>Adquisición de un (1) sistema de seguridad informática perimetral que sea del tipo Administración Unificada de Amenazas (UTM por sus siglas en inglés) o Firewall de Nueva Generación, donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que se detallan en el presente documento.<br><br>• Todos los componentes del sistema: procesador, tarjeta principal y en general el conjunto electrónico debe ser de propósito específico.<br>• Para el firewall, NO se aceptan sistemas de propósito general (PCs o servidores) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.<br>• El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red. |
| 1.2 | **Rendimiento**<br><br>El equipo deberá cumplir con las siguientes características MINIMAS de desempeño:<br><br>• Rendimiento de Firewall 16 Gpbs<br>• Rendimiento de IPS 4 Gpps<br>• Rendimiento IPSec y VPN 8 Gbps<br>• Rendimiento Antivirus (Flow Based) de 2,8 Gbps<br>• Soporte de 3.000.000 sesiones concurrentes<br>• Soporte de 10.000 políticas de firewall<br>• Soporte a 5000 usuarios VPN SSL |
| 1.3 | **Conectividad**<br><br>El equipo deberá contar con las siguientes interfaces electrónicas de conexión:<br><br>• Minimo 16 interfaces 10/100/1000 cobre |
| 1.4 | **Protocolos soportados.**<br><br>• IPv4 e IPv6<br>• DHCP cliente, servidor, relay |
| 1.5 | **Certificaciones y estándares soportados.**<br><br>El sistema completo deberá estar certificado en:<br><br>• FIPS NIVEL 2<br>• ICSA LABS Firewall and VPN<br>• ICSA LABS IPS<br>• ICSA LABS Gateway AV<br>• IPv6 Ready Logo Phase 2 |
| 1.6 | **Address Traslation**<br><br>• NAT y PAT<br>• NAT estático<br>• NAT: destino, origen<br>• NAT, NAT64 persistente |
| 1.7 | **Manejo de tráfico y calidad de servicio.** |

| | |
|---|---|
| | • Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall<br>• Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión<br>• Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.<br>• Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo<br>• Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo<br>• Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia |
| 1.8 | **Funciones básicas de Firewall**<br><br>• Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.<br>• Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.<br>• Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario),<br>• La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP.<br>• La solución será capaz de habilitar o deshabilitar el paso de trafico a través de procesadores de propósito especifico, si el dispositivo cuenta con estos procesadores integrados dentro del mismo<br>• El dispositivo será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico<br>• Tendrá la capacidad de hacer escaneo a profundidad de trafico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis<br>• La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.<br>• La solución soportará políticas basadas en dispositivo. Esto Signfica que podrán definirse políticas de seguridad de acuerdo al dispositivo (movil, laptop) que tenga el usuario. |
| 1.9 | **Conectividad y Enrutamiento**<br><br>• Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.<br>• Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.<br>• Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.<br>• Soporte a políticas de ruteo (policy routing)<br>• Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP<br>• Soporte a ruteo dinámico RIPng, OSPFv3<br>• La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes.<br>• Soporte de ECMP (Equal Cost Multi-Path)<br>• Soporte a ruteo de multicast<br>• La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.<br>• La solución podrá habilitar políticas de ruteo en IPv6<br>• La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6 |
| 1.10 | **VPN IPSEC**<br>El equipo deberá soportar las siguientes características:<br>• Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)<br>• Soporte para IKEv2 y IKE Configuration Method<br>• Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES<br>• Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits<br>• Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.<br>• Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.<br>• Posibilidad de crear VPN's entre gateways y clientes con IPSec. Estoes, VPNs IPSeC site-to-site y VPNs IPSec client-to-site.<br>• La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN)<br>• En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall. |

| | |
|---|---|
| | **VPN SSL**<br>• Capacidad de realizar SSL VPNs.<br>• Soporte a certificados PKI X.509 para construcción de VPNs SSL.<br>• Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.<br>• Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.<br>• Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.<br>• Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning)<br>• La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS<br>• Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL<br>• Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente<br>• Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.<br>• Los portales personalizados deberán soportar al menos la definición de:<br>Widgets a mostrar:<br>Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC<br>o Soporte para Escritorio Virtual<br>o Política de verificación de la estación de trabajo.<br>• La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información. |
| 1.11 | **Autenticación**<br>El dispositivo deberá manejar los siguiente tipos de autenticación:<br>• Capacidad de integrarse con Servidores de Autenticación RADIUS.<br>• Capacidad incluida, al integrarse con Microsoft Windows Active Directory, de autenticar transparentemente usuarios sin preguntarles username o password,aprovechando las credenciales del dominio de Windows bajo un concepto "Single-Sign-On"<br>• Soporte de doble Factor de autenticación para reglas de firewall o VPN.<br>• Soporte de Token Físicos o mobile sobre smartphone basado en IOS o Android. |
| 1.12 | **Módulos de Seguridad** |
| 1.12.1 | **Antivirus**<br>• Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.<br>• El Antivirus deberá poder configurarse en modo Proxy como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruídos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente.<br>• Antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor **o** appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.<br>• El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.<br>• La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso.<br>• El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging).<br>• Se debe incluir protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats). Dentro de estos controles se debe incluir: |

| | |
|---|---|
| | 1. Protección contra botnets: Se deben bloquear intentos de conexión a servidores de Botnets, para ello se debe contar con una lista de los servidores de Botnet más utilizado. Dicha lista debe actualizarse de forma periodica por el fabricante<br><br>2. Sandboxing: La funcionalidad de Sandbox hace que el archivo sea ejecutado en un ambiente seguro para analizar su comportamiento y, a base del mismo, tomar una acción sobre el mismo. |
| 1.13.2 | **Filtrado WEB**<br><br>• Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.<br>• Debe poder categorizar contenido Web requerido mediante IPv6.<br>• La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión (modo proxy) como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación (modo flujo).<br>• Capacidad de filtrado de scripts en páginas web (JAVA/Active X).<br>• La solución de Filtraje de Contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta<br>• funcionalidad se soportará al menos para Google, Yahoo! y Bing. |
| 1.13.3 | **Protección contra Intrusos IPS**<br><br>• El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror.<br>• Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6.<br>• Capacidad de detección de más de 4000 ataques.<br>• El detector y preventor de intrusos deberá soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / misuse detection).<br>• Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.<br>• Actualización automática de firmas para el detector de intrusos<br>• Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP. |
| 1.13.4 | **Control de Aplicaciones**<br><br>• Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.<br>• La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.<br>• La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante.<br>• El listado de aplicaciones debe actualizarse periódicamente.<br>• Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.<br>• Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.<br>• Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de trafficshaping. |

| | |
|---|---|
| | • Preferentemente deben soportar mayor granularidad en las acciones. |
| 1.13.5 | **Inspección de Contenido SSL**<br>• La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.<br>• La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle).<br>• El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS |
| | **álisis de Vulnerabilidades:**<br>- La solucion debera Permitir hacer análisis de vulnerabilidades y generarar un reporte de cuáles vulnerabilidades fueron encontradas. No deberá tener límite de equipos a analizar. |
| 1.14 | **Alta disponibilidad.**<br>• El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6<br>• Debe soportar Alta Disponibilidad en modo Activo-Pasivo<br>• Debe soportar Alta Disponibilidad en modo Activo-Activo<br>• Debe soportar Posibilidad de definir al menos dos interfaces para sincronía<br>• El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red.<br>• Deberá Ser posible definir interfaces de gestión independientes para cada miembro en un clúster. |
| 1.15 | **Virtualización**<br>• La solucion ofertada debera tener como minimo 10 firewalls virtuales incluidos.<br>• El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”,“Virtual Firewalls” o “Virtual Domains”<br>• Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red<br>• Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual |
| 1.16 | **Cliente de VPN**<br>• Se debe suministrar el software de cliente para VPN.<br>• La solución debe estar licenciada para cinco mil (5000) usuarios de VPN SSL dinámicos, externos o móviles.<br>• El cliente debe permitir la autenticación por dos factores. |
| | |

➢ **CONDICIONESMÍNIMASGENERALES**

El contratista deberá ejecutar el objeto del contrato cumpliendo cada una de las especificaciones técnicas y requerimientos mínimos de los ítems anteriores.

Se debe instalar, configurar y dejar en correcto funcionamiento la solución brindada.

La garantía de los equipos deberá ser por un periodo mínimo de 12 Meses.

El contratista se compromete con la Entidad, a suministrar todos los equipos certificados y garantizados de fábrica, cumpliendo las Normas técnicas vigentes nacionales e internacionales.

El proponente debe comprometerse a entregar los reportes de los mantenimientos o reparaciones técnicas realizadas en el equipo o equipos en el periodo de garantía.

El contratista deberá explicar claramente la metodología que se debe seguir para solicitar y prestar el servicio

de garantía y mantenimiento aun número único al cual se solicitará el soporte a través de unhelp desk, sin costo para la Entidad.

Las partes que sean remplazadas en los mantenimientos correctivos realizados durante el término de duración de la garantía, deben ser originales y deben estar homologadas por el fabricante del equipo.

La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS y URLF iltering debe proveerse por al menos un (1) año.

➢**SOPORTETECNICO**

**El soporte debe estar orientado presencialmente en modalidad (7x 24 x 4)** a los funcionarios que la Oficina de Tecnología e Información designe como contactos autorizados. El proveedor atenderá los requerimientos de soporte a los equipos reportados y efectuará la asistencia técnica ante la presencia de fallas.

De requerirse un técnico en la oficina de la entidad, este arribará para atender los eventos reportados, de acuerdo al horario de cubrimiento y tiempos de respuesta solicitados, siempre y cuando la solución del problema reportado no se pueda realizar mediante las conexiones remotas que actualmente la entidad tiene configuradas.

Los gastos de transporte del personal ajeno a la entidad deben correr por cuenta del proveedor y no deben generar ningún costo adicional para la entidad.

El soporte debe brindarse en forma proactiva y preventiva con el fin de evitar la interrupción al máximo del servicio, garantizando la operación correcta y permanente de la plataforma:

- 1 Nivel : Soporte técnico del proveedor
- 2 Nivel : Soporte técnico especilizado.
- 3 Nivel: Soporte técnico fabricante

El soporte técnico presencial se debe brindar en las instalaciones de la entidad en la ciudad de Bogotá.

El soporte técnico debe garantizar una adecuada operación de los productos ofrecidos, de conformidad con las especificaciones técnicas y de funcionalidades señaladas en la documentación para la operación de los productos por el fabricante.

El contratista debe entregar informes o documentación detallada de todos los procedimientos realizados después de los mantenimientos preventivos y soporte por problemas presentados, actualizaciones, asimismo se debe detallar en el informe las causas, procedimientos preventivos y soluciones futuras inmediatas a los problemas o daños presentados en cualquiera de las herramientas.

# I. Servicios Asociados:

**Atención en Sitio:** Cuando se haya determinado el problema y no se encuentre la solución telefónica o remota, el proveedor debe asignar un ingeniero para que se desplace a las oficinas de la entidad, en un tiempo no mayor de cuatro (4) horas.

**Mantenimiento Correctivo:**

Vigencia doce (12) meses. Se deberá realizar cuantas veces la entidad lo requiera en modalidad de (7 x 24) con un tiempo de respuesta no mayor a cuatro (4) horas y deberá prestarse en las instalaciones en donde se encuentre instalada la solución de seguridad propuesta.

Los repuestos que sean necesarios para efectuar la reparación y dejar en perfecto funcionamiento cualquiera de los elementos de los equipos o partes cubiertos correrán por cuenta del proveedor con el apoyo del fabricante.

En caso de determinarse una falla de Hardware sobre la solución ofrecida, que no pueda ser resuelta dentro de las 8 horas hábiles siguientes al reporte de la misma, el contratista debe reemplazar el equipo averiado con un equipo de su propiedad dentro de las siguientes veinticuatro horas contadas a partir del reporte de la falla. Este equipo debe ser de características idénticas o superiores al que presenta la falla y debe ser instalado temporalmente en el sitio, en calidad de soporte mientras se dá la solución definitiva.

Los repuestos empleados para remplazar elementos defectuosos serán de la misma calidad existente y se realizara su remplazo previa autorización de la Oficina de Tecnología e Información de la entidad.

**Soporte Técnico Especializado**

El contratista en caso de falla, deberá atender los requerimientos de soporte de los elementos objeto del contrato, en la modalidad 7x24, incluyendo 10 horas de asesoría para gestión remota.

- **GARANTÍA**

El contratista debe otorgar un año (1) de garantía para todos y cada uno de los componentes de hardware, software y/o equipos o dispositivos que se ofrecen.

- **CAPACITACION**

El contratista debe realizar una capacitación certificada por el fabricante para un funcionario de la entidad por un mínimo de 16 horas

- **CERTIFICACIÓN DEL FABRICANTE.**

El proponente debe proporcionar la certificación del fabricante vigente, como distribuidor autorizado.

- **INSTALACIÓN**

El contratista deberá instalar la solución de seguridad en el Datacenter de la Entidad y dejar en perfecto funcionamiento, previa presentación del plan de trabajo e implementación