GERENCIA DE TECNOLOGÍA INFORMÁTICA
ESPECIFICACIONES TÉCNICAS
Actualización de la infraestructura de Firewall

1. OBJETIVO

Proveer una solución de seguridad de Firewall que incluya equipos (Hardware), instalación, garantías, mantenimiento, actualización y soporte técnico.

2. ALCANCE

a. El dispositivo debe ser un equipo de propósito específico.
b. La solución deberá ser de un mismo fabricante
c. La solución debe tener la capacidad de gestionar accesos por usuarios y niveles según perfiles.
d. El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red
e. En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP
f. El equipo Firewall deberá contar con fuentes redundantes a 120/225V AC
g. El equipo deberá soportar un mínimo de 500 sesiones concurrentes con un mínimo de 100 sesiones nuevas por segundo
h. La solución deberá tener Alta disponibilidad con capacidad de balancear la carga entre ambos Equipos
i. El equipo debe soportado actualizaciones de sistema operativo del fabricante mínimo 5 años
j. La solución de seguridad de Firewall deberá ser ofertada con licenciamiento, garantías, mantenimiento, actualización y soporte técnico del fabricante para al menos un (3) año en todos sus componentes
k. La solución de seguridad de Firewall deberá ser ofertada con licenciamiento, garantías, mantenimiento, actualización y soporte técnico del fabricante para al menos un (3) año en todos sus componentes
l. Como requisito “mínimo”, La solución debe contar con los siguientes componentes.
    - Componente de gestión, administración y operación de la solución.
    - Componente de correlación de eventos y/o log’s “en tiempo real”.
    - Componente de reportes.
    - Componente de auditoría y análisis de eventos.
m. la solución deberá incluir soporte, administración y monitoreo por el periodo de 3 años, deberá ser de lunes a domingo 24 horas al día 7 días a la semana, incluyendo días feriados

.

3. Especificaciones Técnicas del Firewall

a. El equipo deberá contar con al menos 15 GBS de Firewall throughput.
b. Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
c. Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.
d. Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.
e. Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando
f. Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.
g. Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo.
h. Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año)
i. Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.
j. Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP)
k. Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.
l. Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.
m. 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),
n. La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas.
o. En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID
p. En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.
q. El equipo deberá permitir la creación de políticas de tipo Firewall con capacidad de seleccionar campos como dirección, identificador de usuarios o identificador de dispositivos para el caso de dispositivos móviles como smartphones y tabletas.
r. El equipo deberá permitir la creación de políticas de tipo VPN con capacidad de seleccionar campos como IPSEC o SSL según sea el tipo de VPN
s. La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP.
t. La solución de seguridad deberá permitir la creación de servicios de Firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada
u. La solución será capaz de integrar los servicios dentro de las categorías de Firewall predefinidas o personalizadas y ordenarlos alfabéticamente
v. El dispositivo de seguridad podrá determinar accesos y denegación a diferentes tipos de tráfico predefinidos dentro de una lista local de políticas
w. La solución será capaz de habilitar o deshabilitar el paso de tráfico a través de procesadores de propósito específico, si el dispositivo cuenta con estos procesadores integrados dentro del mismo
x. La solución podrá crear e implementar políticas de tipo Multicast y determinar el sentido de la política, así como también la habilitación del NAT dentro de cada interface del dispositivo

y. El dispositivo de seguridad será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces.
z. El dispositivo de generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS
aa. La solución de seguridad permitirá configurar el mapeo de protocolos a puertos de manera global o especifica
bb. La solución capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos.
cc. El dispositivo integrara la inspección de tráfico tipo SSL y SSH bajo perfiles predefinidos o personalizados
dd. El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico
ee. Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis
ff. La solución permitirá bloquear o monitorear toda la actividad de tipo Exec, Port-Forward, SSH-Shell, y X-11 SSH

3.1 Conectividad y Sistema de ruteo.

a. El equipo deberá contar con 16 interfaces de red, puertos SPF.
b. Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.
c. Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.
d. Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
e. Soporte a políticas de ruteo (policy routing).
f. El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace
g. Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS
h. Soporte a ruteo dinámico RIPng, OSPFv3
i. La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes.
j. Soporte de ECMP (Equal Cost Multi-Path)
k. Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador.
l. Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa.
m. Soporte a ruteo de multicast
n. La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.
o. La solución podrá habilitar políticas de ruteo en IPv6
p. La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6
q. La solución deberá soportar la creación de políticas de tipo Firewall y VPN y subtipo por dirección IP, tipos de dispositivo y por usuario, con IPv6
r. La solución será capaz de habilitar funcionalidades de UTM (Antivirus, Filtrado Web, Control de Aplicaciones, IPS,Filtrado de correo, DLP, ICAP y VoIP) dentro de las políticas creadas con direccionamiento IPv6
s. El dispositivo debe integrar la autenticación por usuario o dispositivo en IPv6
t. El dispositivo deberá soportar la inspección de tráfico IPv6 en modo proxy explicito
u. Deberá ser capaz de integrar políticas con proxy explícito en IPv6

v. La solución podrá restringir direcciones IPv6 en modo proxy explicito
w. Deberá hacer NAT de la red en IPv6
x. La solución será capaz de comunicar direccionamiento IPv6 a servicios con IPv4 a través de NAT
y. Como dispositivo de seguridad deberá soportar la inspección de tráfico IPv6 basada en flujo
z. La solución deberá ser capaz de habilitar políticas de seguridad con funcionalidades IPS, Filtrado Web, Control de Aplicaciones, Antivirus y DLP, para la inspección de tráfico en IPv6 basado en flujos
aa. La solución contara con una base de administración de información interna generada por sesiones sobre IPv6
bb. Deberá ser capaz de habilitar la funcionalidad de Traffic Shaper por IP dentro de las políticas creadas en IPv6
cc. El dispositivo podrá tener la capacidad de transmitir DHCP en IPv6
dd. La solución tendrá la funcionalidad de habilitar DHCP en IPv6 por interface
ee. La solución deberá contar con soporte para sincronizar por sesiones TCP en IPv6 entre dispositivos para intercambio de configuración en Alta Disponibilidad
ff. El dispositivo podrá ser configurado mediante DHCP en IPv6 para comunicarse con un servidor TFTP donde se encontrará el archivo de configuración
gg. El dispositivo podrá hacer la función como servidor DHCP IPv6
hh. La solución será capaz de configurar la autenticación por usuario por interface en IPv6
ii. La solución deberá poder balancer varios enlaces hacia el Internet para aumentar el ancho de banda y proveer de funcionalidad fail over en caso de caida de un enlace.
jj. La solución deberá manejar los siguientes algoritmos de balanceo: Bandwidth, Sessions, Spillover, Source-Destination-IP

3.2 VPN IPSec/L2TP/PPTP.

a. El equipo deberá contar con al menos 6 Gbps de capacidad para VPN IPSec (throughput)
b. Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)
c. Soporte para IKEv2 y IKE Configuration Method
d. Debe soportar la configuración de túneles PPTP
e. Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.
f. Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits
g. Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.
h. Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.
i. Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site.
j. La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN)
k. 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.
l. Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.

3.3 VPN SSL.

a. El equipo deberá contar con al menos 5 Gbps de capacidad para VPN SSL (throughput)
b. Capacidad de realizar SSL VPNs.
c. Soporte a certificados PKI X.509 para construcción de VPNs SSL.
d. 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.
e. Soporte de renovación de contraseñas para LDAP y RADIUS.

f. Soporte a asignación de aplicaciones permitidas por grupo de usuarios
g. Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.
h. 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.
i. Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning)
j. 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
k. Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL
l. Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente
m. 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.
n. Los portales personalizados deberán soportar al menos la definición de:
o. Widgets a mostrar
p. Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC
q. Esquema de colores
r. Soporte para Escritorio Virtual
s. Política de verificación de la estación de trabajo.
t. 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.
u. Para la configuración de cluster, en caso de caída de uno de los dispositivos, la VPN SSL que estuviera establecida, debe restablecerse en el otro dispositivo sin solicitar autentificación nuevamente.

3.4 Traffic Shapping / QoS.

a. Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall
b. Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión
c. 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.
d. Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo
e. Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo
f. Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia

3.5 Autenticación y Certificación Digital.

a. Capacidad de integrarse con Servidores de Autenticación RADIUS.
b. Capacidad nativa de integrarse con directorios LDAP
c. Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”
d. Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet.

e. Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet.
f. Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)
g. La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.
h. Deben poder definirse usuarios y grupos en un repositorio local del dispositivo.
i. Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo:
j. Longitud mínima permitida
k. Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc.
l. Expiración de contraseña.
m. Debe poder limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP.

3.6 Antivirus.

a. 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.
b. 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.
c. 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.
d. El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.
e. 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.
f. El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad.
g. El appliance deberá de manera opcional poder inspeccionar por todos los virus conocidos.
h. El Antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos http, FTP, IMAP, POP3, SMTP
i. El Antivirus integrado tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus.
j. El Antivirus deberá incluír capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red.
k. El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger.
l. El antivirus deberá ser capaz de filtrar archivos por extensión
m. El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo
n. Capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo “Push” (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo “pull” (Consultar los centros de actualización por versiones nuevas)
o. El antivirus deberá poder integrarse con un Sandbox en modo nube o local.

3.4 AntiSpam

a. La capacidad antispam incluída deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.
b. La capacidad AntiSpam incluída deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address).
c. La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como mecanismos para detección de SPAM
d. En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.

3.5 Filtraje de URLs (URL Filtering)

a. 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.
b. Debe poder categorizar contenido Web requerido mediante IPv6.
c. Filtrado de contenido basado en categorías 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.
d. Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso.
e. Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida
f. 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).
g. Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables. Estos mensajes de remplazo deberán poder aplicarse para conexiones http y https, tanto en modo proxy como en modo flujo.
h. Los mensajes de remplazo deben poder ser personalizados por categoría de filtrado de contenido.
i. Capacidad de filtrado de scripts en páginas web (JAVA/Active X).
j. 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 funcionalidad se soportará al menos para Google, Yahoo! y Bing.
k. Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.
l. Será posible exceptuar la inspección de HTTPS por categoría.
m. Debe contar con la capacidad de implementar el filtro de Educacion de Youtube por Perfil de Filtro de Contenido para tráfico HTTP, garantizando de manera centralizada, que todas

las sesiones aceptadas por una política de seguridad con este perfil, van a poder acceder solamente a contenido de tipo Educativo en Youtbube, bloqueando cualquier tipo de contenido no Educativo.

n. El sistema de filtrado de URLs debe tener al menos 3 métodos de inspección:
   - Modo de Flujo: La página es inspeccionada paquete a paquete sin reconstruir la página completa.
   - Modo Proxy: La página es reconstruida completamente para ser analizada a profundidad.
   - Modo DNS: La inspección se basa únicamente en la categorización del dominio accesado
o. Se debe incluir la funcionalidad de reputación basada en filtrado de URLs.
p. La funcionalidad de reputación busca que, al acceder a páginas de contenido no deseado (tales como Malware, pornografía, consumo de ancho de banda excesivo, etc) se asigne un puntaje a cada usuario o IP cada vez visita una página de esta índole. De acuerdo a esto se extrae los usuarios que infringen las políticas de filtrado con más frecuencia con el fin de detectar zombies dentro de la red.l sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido.
q. Se debe incorporar la funcionalidad de filtrado educativo de Youtube (Youtube Education Filter)
r. En dicho sistema cada organismo obtiene un ID de Youtube para habilitar el contenido educativo del mismo. Se deberá insertar dicho codigo en la configuración de filtrado de URLs del equipo para poder habilitar unicamente el contenido educativo de Youtube.

3.6 Protección contra intrusos (IPS).

a. El equipo deberá contar con un mínimo de 8 Gbps de capacidad de IPS (throughput).
b. 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.
c. Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.
d. Capacidad de detección de más de 4000 ataques.
e. Capacidad de actualización automática de firmas IPS mediante tecnología de tipo “Push” (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo “pull” (Consultar los centros de actualización por versiones nuevas)
f. El detector y preventor de intrusos deberá estar 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 prevención de intrusos. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.
g. 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).
h. Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.
i. Actualización automática de firmas para el detector de intrusos
j. El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.
k. Métodos de notificación:
l. Alarmas mostradas en la consola de administración del appliance.

m. Alertas vía correo electrónico.
n. Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado.
o. La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma “indefinida”, hasta que un administrador tome una acción al respecto.
p. 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.
q. Se debe incluir protección contra amenzas avanzadas y persistentes (Advanced Persistent Threats). Dentro de estos controles se debe incluir:
    - 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.
    - 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 accion sobre el mismo.
r. La solución deberá poder bloquear Botnets conocidas.

3.7 Prevención de Fuga de Información (DLP)

a. La solución debe ofrecer la posibilidad de definir reglas que permitan analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial.
b. La funcionalidad debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos.
c. Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.
d. Ante la detección de una posible fuga de información deben poder aplicarse el menos las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la dirección IP de origen, registrar el evento,
e. En caso del bloqueo de usuarios, la solución debe permitir definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción.
f. La solución debe soportar la capacidad de guardar una copia del archivo identificado como posible fuga de información. Esta copia podría ser archivada localmente o en otro dispositivo.
g. La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares.
h. Se debe proveer la funcionalidad de filtrado de fuga de información. Dentro de las técnicas de detección se debe considerar como mínimo las siguientes:
    - Filtrado por tipo de archivo
    - Filtrado por nombre de archivo
    - Filtrado por expresiones regulares: Se detectarán los archivos según las expresiones regulares que se encuentren dentro de los mismos.
i. Fingerprinting: Se tomará una muestra del archivo que se considere como confidencial. Según esto se bloquearán archivos que sean iguales a esta muestra.
j. Watermarking: Se insertará un "sello de agua" dentro del archivo considerado como confidencial. De acuerdo a esto se analizarán los archivos en busca de este sello de agua, este se detectará incluso si el archivo sufrió cambios.

3.8 Control de Aplicaciones

a. Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
b. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.
c. La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante.
d. El listado de aplicaciones debe actualizarse periódicamente.
e. Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.
f. Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.
g. Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.
h. Preferentemente deben soportar mayor granularidad en las acciones.
i. La solución deberá hacer inspección de nubes públicas como Dropbox, Youtube, Amazon, etc, deberá proveer control granular para bloquear subidas, descargas o loging.

3.9 Inspección de Contenido SSL

a. 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.
b. La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle).
c. La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.
d. Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.
e. 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

3.10 Optimización WAN y Web Caching.

a. La solución deberá permitir la creación de perfiles para la aplicación de Optimización WAN e indicar bajo que protocolos se ejecutará. Deberá ser capaz de activar en modo transparente dentro de los perfiles de Optimización WAN y seleccionar un determinado grupo de usuarios para autenticación de acceso
b. El dispositivo deberá soportar la desfragmentación dinámica de paquetes para detectar fragmentos persistentes de distintos archivos o datos adjuntos dentro del trafico bajo protocolos desconocidos
c. La solución debe ser capaz de generar y aplicar perfiles de Optimización WAN para los usuarios
d. El dispositivo de seguridad podrá integrar contenido de inspección dentro de sus políticas de seguridad con Optimización WAN. La solución integrará dentro de cada interface la capacidad de hacer túneles de Optimización WAN Deberá ser capaz de configurar Optimización WAN en modo Activo/Pasivo
e. Solución capaz de aplicar web cache a tráfico HTTP y HTTPS dentro de las políticas de seguridad incluyendo también Optimización WAN y web proxy cache Dispositivo capaz de habilitar el almacenamiento en caché web tanto en el lado del cliente y del lado de la solución.

f. La solución podrá recibir el tráfico HTTPS en nombre del cliente, abrirá y extraerá el contenido del tráfico cifrado para inspeccionar y almacenar en cache para el envío al usuario final.
g. El dispositivo tendrá la opción de integrar un certificado SSL determinado para la recifrado de tráfico.
h. La solución capaz de configurar el cache de tráfico HTTP y HTTPS bajo distintos puertos a los predeterminados (80 y 443).
i. La solución debe ser capaz de habilitar opciones para depurar la funcionalidad de Web Cache a determinadas URL.

3.11 Alta Disponibilidad

a. 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
b. Alta Disponibilidad en modo Activo-Pasivo
c. Alta Disponibilidad en modo Activo-Activo
d. Posibilidad de definir al menos dos interfaces para sincronía
e. El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red
f. Será posible definir interfaces de gestión independientes para cada miembro en un clúster.

3.12 Características de Administración

a. Interfase gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfase debe soportar SSL sobre HTTP (HTTPS)
b. La interfase gráfica de usuario (GUI) vía Web deberá poder estar en español y en inglés, configurable por el usuario.
c. Interfase basada en línea de comando (CLI) para administración de la solución.
d. Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interfase gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet)
e. El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales.
f. Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.
g. El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet,http o HTTPS.
h. El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.
i. Soporte de SNMP versión 2
j. Soporte de SNMP versión 3
k. Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos
l. Soporte para almacenamiento de eventos en un repositorio que pueda consultarse luego con SQL.
m. Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.
n. Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.

o. Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.
p. Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica.
q. Contar con facilidades de administración a través de la interfaz gráfica como listas de edición a través de click derecho.
r. Contar con facilidades de administración a través de la interfaz gráfica como ayudantes de configuración (setup wizard).
s. Contar con la posibilidad de agregar una barra superior (Top Bar) cuando los usuarios estén navegando con información como el ID de usuario, cuota de navegación utilizada, y aplicaciones que vayan en contra de las políticas de la empresa.
t. Contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.

3.13 Actualizaciones de plataforma

a. La solución contara con el servicio de actualización de firmas para dispositivos sobre BYOD
b. El dispositivo tendrá la opción de conectarse a los servidores NTP de los Laboratorios de Investigación y Actualización propietarios del mismo fabricante para actualización del horario de sistema local
c. Sera capaz de hacer consultas a los servidores DNS de los Laboratorios de Investigación y Actualización del mismo fabricante para resolución y categorización de sitios web dentro de los perfiles para Filtrado Web
d. Tendrá la capacidad de hacer consultas a los servidores DNS de los Laboratorios de investigación y Actualización mismos del fabricante sobre reputación de direcciones IP

3.14 Licenciamiento y actualizaciones

a. El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, cajas de correo, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.
b. La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS y URL Filtering debe proveerse por al menos 3año.

4. Monitoreo, administración y Soporte.

El servicio propuesto debe contener como mínimo lo detallado continuación:

4.1. **Monitorización**: El servicio de monitorización persigue:
   a. Prevenir los problemas detectando anomalías en su fase inicial.
   b. Alertar de los problemas en el mismo momento que ocurran para permitir una resolución más rápida
   c. Verificar el correcto funcionamiento de todos los servicios
   d. ofrecer en modalidad 24x7 para garantizar una actuación totalmente pro-activa.
   e. Las alertas deben ser verificadas por el personal técnico para evitar falsos positivos y los tiempos de notificación de incidentes reales estén reducidos al máximo.
   f. Se debe enviar un informe diario con todas las alertas reportadas en las 24 horas anteriores.

g. Informe mensual de Alertas, Incidentes y disponibilidad.

4.2. Administración:

a. El servicio debe incluir la operación y administración de dispositivos y aplicaciones, así como la gestión de cambios e incidentes. Delegar la gestión de las soluciones de parte de ENSA en manos del proveedor en cada una de las tecnologías, con el objetivo de garantizar tanto la disponibilidad del servicio como el funcionamiento más óptimo, seguro y eficiente.
b. El servicio debe incluir, pero no limitarse a:
   - Actualizaciones, backup y mantenimiento básico al día.
   - Ejecución de las acciones correctoras o recomendaciones pertinentes.
   - La realización de cambios en configuraciones de toda índole sobre lo existente.
   - Minimizar el impacto producido por un incidente de seguridad restableciendo el servicio lo antes posible.
   - Administración y creación de usuarios bajo SLA acordado con el contratista.
   - Administración de reglas para puesta en producción de aplicaciones bajo SLA acordado con el contratista.
   - Establecerse como un interlocutor único en la gestión de incidentes de cara a otros proveedores en nombre del cliente.

4.3. Deberán entregar cuadro de escalamiento ante algún incidente presentado.

4.4. Soporte Técnico remoto

Deberán atender Incidencias técnicas ocurridas con los dispositivos:

- Fallo de operación
- Consultas telefónicas acerca de nuevas tecnologías o configuraciones.
- Problemas de operación del producto
- Recuperación de la solución.

5. CONSIDERACIONES

a. El proponente debe tener presencia local.
b. Carta del distribuidor autorizado emitida por el fabricante que certifique la trayectoria de los productos o servicios ofertados y que cuenta con los derechos de comercialización. La carta debe indicar que el proponente tiene más de 5 años de representar la marca en el país.
c. El prominente deberá presentar mínimo 2 cartas de referencia donde haga constar que ha realizado a satisfacción la implementación del producto ofertado.
d. El proponente deberá presentar mínimo 2 cartas de referencia donde haga constar que brinda el servicio de soporte, monitoreo y administración de la solución ofertada.
e. El proponente deberá ser 1 sola empresa o en su defecto bajo la figura de Contratista Primario (Prime Contractor) para garantizar la uniformidad de la solución a entregar y la responsabilidad completa en el proyecto.
f. Para constatar la experiencia solicitada, el proveedor deberá presentar constancia y/o detalle de las referencias de los trabajos o proyectos realizados, para cada uno de los casos, para lo cual se debe detallar los datos de contacto que incluyen: Nombre de la empresa, persona de contacto, correo electrónico, teléfono, año en que se realizó el

servicio, generales de los proyectos implementados. Si las referencias no se pueden validar, no se tomarán como válidas.

g. Se requiere que el personal técnico o consultores que proponga el proveedor, tengan mínimo cinco (5) años de experiencia en la implementación de la solución ofertada y que dominen el idioma español.
h. El proveedor, deberá entregar como mínimo la siguiente documentación:

- Plan de trabajo.
- Cronograma de actividades: y actualización del mismo semanalmente.
- Acta de alcance.
- Diagrama de la solución implementada.
- Documentación Técnica de la solución implementada.

i. Tiempo de entrega de equipos no mayor a 35 días.
j. Se debe capacitar al menos 2 técnicos de ENSA en la solución instalada.
k. EL proponente deberá entregar plan detallado de la implementación.