ANEXO II ESPECIFICACIONES TECNICAS

RENGLON 1 - UPS

1. CODIGO ETAP: UPS-SRV-RACK - UNIDAD DE ENERGÍA ININTERRUMPIDA PARA SERVIDORES Y/O RACKS DE COMUNICACIONES

1.1 DETALLE TÉCNICO / FUNCIONAL

a) Las Unidades de Potencia Ininterrumpida (UPS) deberán ser de tecnología:

De Línea Interactiva

b) Rango de Potencia no inferior a: (1)

3000 VA

c) Autonomía a plena carga no menor a:

30 minutos.

d) Tensión de entrada:

200-260 VAC / 50 Hz (+-)5 %.

e) Tensión de salida:

220 VAC (+-)5 % (apropiada para cargas de 220-240 VAC).

f) Frecuencia de salida en línea:

Sincronizada dentro de 50 Hz (+-)3 % y 50 Hz (+-)1 % en batería.

g) Forma de onda de salida:

Senoidal o cuasi-senoidal.

h) Eficiencia mayor al 90 % a plena carga (para disminuir la disipación de calor).

i) Tomas de salida mínimas:

Entre 1501 y 4999VA: al menos 8 tomas de salida

j) Gabinete con conexión a tierra.

k) Indicación:

Luminosa de encendido (on/off), señalización de pérdida de energía primaria y en batería acústica y luminosa.

Estado de carga de batería y consumo

l) Protección:

Totalmente protegidas contra sobrecarga y con reposición manual de la protección sin necesidad de abrir el equipo.

m) Baterías:

Herméticas, sin mantenimiento y cambiables por el usuario.

En caso de que el proveedor realice el recambio de baterías durante la etapa de garantía u obsolescencia (con soporte) del UPS, sea esto a solicitud explícita del organismo o debido al alcance previsto en el servicio de mantenimiento, el proveedor será responsable de la deposición de las mismas, de acuerdo a la normativa vigente.

n) Puertos:

Puerto para conexión con software para cierre automático y ordenado de aplicaciones y sistema operativo, monitoreo de tensión de alimentación y salida, consumo total, estado de carga de la batería, posibilidad de registro de eventos, variables, etc.

(1) Para especificar el rango de potencia deberá considerarse la sumatoria del consumo de la totalidad de los equipos conectados a la UPS más un margen de seguridad del orden de 15%.

RENGLON 2 - SERVIDORES

Codigo ETAP : SR-X86-STD Servidores de Red Genéricos - Arquitectura basada en X86/64 Bit

Características Generales

Deberá ser totalmente compatible con Arquitectura X86.

Deberá poseer setup residente en ROM, CD-ROM o DVD-ROM con password de ingreso y encendido.

Deberá poseer control de booteo residente en ROM, con posibilidad de booteo desde CD-ROM y/o DVD-ROM.

Deberá poseer reloj en tiempo real con batería y alarma audible.

Deberán indicarse otros controles adicionales que posea.

Detalle Técnico / Funcional

a) **Unidad Central De Proceso**

"INTEL Xeon" de al menos 2,20Ghz de frecuencia y cache de al menos 24,75MB, o rendimiento superior compatible con arquitectura X86.

Compatible con sistemas de virtualización, es decir, Intel VT o AMD-Vi/VT-d.

Del tipo "16 cores" (16 núcleos) o superior

Cantidad de sockets a proveer (cada socket soportará la instalación de 1 CPUs **del tipo seleccionado):** al menos 2

Cantidad de CPU a proveer instaladas (para el tipo seleccionado): al menos 2

b) **Memoria Ram A Proveer Y Su Escalabilidad**

Tipo de memoria: Tipo: DDR4 de 2933Mhz o rendimiento superior con corrección de errores (ECC).

Capacidad: A continuación se detalla la capacidad a proveer inicialmente y la capacidad máxima instalable en el equipo.

Memoria inicial a proveer: al menos 512GB.

Memoria final a alcanzar: al menos 2TB.

La capacidad máxima de RAM instalable debe poder alcanzarse mediante el sólo agregado o reemplazo de módulos de RAM.

No se admitirá que la ampliación de la RAM inicial requiera la instalación o recambio de las CPU originales por otros modelos de CPU.

c) **Puertos Incorporados**

Se deberán proveer los siguientes puertos:

1 Port para monitor
Al menos 3 puerto USB (Universal Serial Bus) versión 3.0

d) **Networking Y Comunicaciones**

En la tabla de abajo se indican las interfases de red que se deberán proveer:

Tipo de Interfaz	Cant. de Puertos (mínimo)
Puertos Gigabit Ethernet en cobre (RJ45)	4
Puertos SFP 10/25 Gigabit Ethernet	2

Almacenamiento Extraible

Medios ópticos:

Lectora de DVD-ROM de 6X o superior.

e) **Bus De E/S Y Expansión**

Bus de E/S:

Deberá soportar mínimamente los estándares PCI 2.1/2.2, PCI-X y PCI-E.
- Los slots PCI-X deberán permitir alcanzar una tasa de transferencia sincrónica no inferior a 1GB/seg y los slots PCI-E, deberá poseer una tasa de transferencia no inferior a 250 MB/s por LANE.

Expansión: Luego de instaladas todas las placas PCI necesarias para cubrir las características del equipo solicitado, deberán quedar:

Al menos 1 slot PCI-E de 4 LANEs (x4) libre para futuras ampliaciones.

f) **Adaptador De Video**

VGA o superior con 8MB de memoria mínimo para soporte de las interfaces gráficas de los sistemas operativos existentes en el mercado.

g) Opciones para servidores rackeables

Debe ser Rackeable, incluyendo todos los accesorios, tornillos y elementos necesarios para ser alojado en un rack de 19" estándar.

No debe ocupar más de 2 unidades de Rack.

h) **Almacenamiento Masivo Interno**

Característica de la Controladora de Discos Duros:

-Tipo:

SAS o superior: El conjunto formado por las controladoras de disco y las unidades de discos, deberán transferir hacia el canal SAS a una tasa sincrónica no inferior a:

600 MB/s (6.0 Gbps).

HOT-SWAP: La controladora de discos duros, así como los discos usados en la implementación del sistema de almacenamiento masivo deberán soportar capacidad Hot-Swap de los discos.

- Configuraciones RAID soportadas:

Configuración RAID 0,1 o 0+1 por hardware en todos los canales.

Configuración RAID 5 por hardware en todos los canales.

Discos duros que componen el almacenamiento interno:

Los discos provistos deben ser capaces de transferir en ráfaga, a una velocidad no inferior a:

600 MB/s (6.0 Gbps)

Los discos provistos deben tener una velocidad de rotación no inferior a:

10000 RPM

Configuración del almacenamiento interno:

Configuración RAID a proveer en el conjunto de discos:

RAID 5 (Data Stripping with parity)

Capacidad:

8 (ocho) Discos **SAS**: capacidad por unidad no inferior a: 2,4TB de 10.000 (diez mil) RPM.

i) **Fuente De Alimentación**

Deberá poder conectarse directamente a la red de suministro de energía eléctrica de 220 V - 50 Hz, además de tener conexión a tierra.

Deberá ser redundante

j) **La Sistema Operativo Sin Sistema Operativo**

La marca Deberá garantizar que el producto soporte virtualización con Proxmox (open sourse) por escrito.

Condiciones:

El equipamiento propuesto deberá ser nuevo y sin uso, de la misma marca con números de partes de todos sus componentes del mismo fabricante.

Los equipos deberán tener instaladas las últimas versiones liberadas de firmware, drivers y de software embebido a la fecha de su entrega definitiva.

Debe poseer garantía de 3 años onsite y reposición o reparación de componentes.

Requisitos:

La propuesta técnica de los oferentes no solo deberá ser la simple entrega de los folletos y hojas de datos de los equipos, sino que se deberá describir lo que se ofrece para cada ítem solicitado. Asimismo, se deberá indicar la hoja de la propuesta donde se hace referencia a cada una de las especificaciones solicitadas en el pliego. Serán desestimadas todas las propuestas técnicas que no cumplan con lo anteriormente solicitado.

RENGLON 3 – DRONE

Con Cámara, Resolución de la cámara: 4K

Velocidad mínima: 70 km/h

Cantidad de baterías: 1

Tiempo mínimo de vuelo: 30m

Cantidad de motores: 4

Con Gps

Con función de auto retorno

Con retención de altitud

Con función de seguimiento

Con control remoto

RENGLON 4 – PROYECTOR

PROYECTORES DE VIDEO; BRILLO: 5200 LM, RESOLUCION VIDEO: 1920 X 1200 PXL, PROYECCION DIAGONAL: 20 A 300 pulg

Tamaño de la imagen: 20 "- 316" Con Wi-Fi: Sí Conexiones de entrada: HDMI, miniplug, VGA Fuentes de luz: Fósforo láser Tecnología de proyección: DLP Brillo de 5200 lúmenes ANSI y resolución WXGA Entrada 4K UHD HDR con HDMI 2.0 (HDCP 2.2) Vida útil de la fuente de luz hasta 30.000 horas

RENGLON 5 – NOTEBOOKS

PC-007 - COMPUTADORA PORTÁTIL AVANZADA

1.2 CARACTERÍSTICAS GENERALES

Consideraciones Especiales para PC definidas en **CESP-001, CESP-002, CESP-005,** y de corresponder **CESP-006.**

Computadora portátil del tipo “Notebook” optimizada para alto rendimiento operativo.

Arquitectura X86 de 64 bits con soporte USB 3.0 (Universal Serial Bus versión 3.0).

Setup residente en ROM con password de booteo y setup.

Con contraseña de encendido por BIOS activable y configurable.

Peso: menor a 1.5 kg

1.3 UNIDAD DE PROCESAMIENTO (CPU)

- Rendimiento medio:

Si oferta procesador marca "INTEL":

El rendimiento deberá ser NO inferior a **"Core i7 mobile"**, como mínimo de doble núcleo.

Si oferta procesador marca "AMD":

El rendimiento deberá ser NO inferior a **"Ryzen 7 mobile"**, como mínimo de doble núcleo.

Sin importar la marca o modelo ofertado, el CPU tendrá una antigüedad de lanzamiento al mercado internacional no mayor a 18 meses.

1.4 MEMORIA

Tipo:

- Tipo: DDR4-2400 o superior.

Capacidad:

- **8 GB** mínimo ampliable a **16 GB** sin cambiar la memoria inicialmente provista

1.5 DISCO DURO

Tipo y capacidad:

- SSD 480 GB.

1.6 VIDEO

Controladora de vídeo SVGA/XGA o superior, con las siguientes características mínimas:

Soporte de resoluciones no inferiores a 1920x1080 (Full HD).

Color de 32 bits.

Acceso a no menos de 512MB de RAM de video.

1.7 AUDIO

Placa de Sonido (o chipset integrado) con las siguientes características:

Grabación/Reproducción de audio: 16 bits mínimo.

Rango de Grabación/Reproducción: 8 - 44.1 KHz, estéreo.

Conectores para línea de entrada, micrófono y salida para auricular / bocinas externas.

Bocinas internas 1 (UNA) como mínimo.

1.8 NETWORKING Y COMUNICACIONES

Interfaz de Red interna Gigabit Ethernet mínimo.

Interfaz de Red WiFi (WLAN) interna con antena integrada, compatible con el estándar:

- IEEE 802.11ac (450 Mbps o más).

1.9 DISPOSITIVOS DE INTERFAZ HUMANA

Cámara Web incorporada.

Teclado: tipo QWERTY en idioma español latinoamericano, que incluya función numérica.

Dispositivo de señalamiento incorporado del tipo mouse o similar (trackball, trackpoint, touchpad, mini-joystick, etc.).

1.10 PANTALLA

Tipo: Color LCD, o TFT, o LED

Resolución:

- No inferior a WXGA (Wide XGA) de 1280 x 800 pixels para relación de aspecto 16:10, ó 1366x768 para relación de aspecto 16:9.

Tamaño diagonal de pantalla:

- No inferior a 14"

1.11 PUERTOS INCORPORADOS

Deberá contar con:

Puertos USB 2.0 de alta velocidad:

- Al menos 2 puertos.

Puertos USB 3.0:

- Al menos 1 puerto.

Puertos adicionales:

- ✓ Puerto HDMI (High Definition Multimedia Interface)

1.12 SISTEMA OPERATIVO

- **Windows 10 Professional (x64) o superior, en español con licencia original..**

A fin de garantizar la compatibilidad del hardware ofertado con el sistema operativo solicitado, la estación de trabajo deberá acreditar haber pasado favorablemente los test de compatibilidad de “Certifiedfor Microsoft Windows 10 Clientfamily, x64”, no aceptando partes o componentes de los mismos, sino la estación en su totalidad. Para ello los oferentes deberán detallar en la oferta el SUBMISSION ID junto al “Windows Logo VerificationReport” el cual deberá haber resultado aprobado (approved).

1.13 ALIMENTACIÓN, PORTABILIDAD Y AHORRO DE ENERGÍA

Alimentación por baterías recargables de níquel-hidruro metálico (NiMH), Li-Ion o similar, y directamente del suministro de red pública (a través del alimentador/cargador), automático 110/240 V – 50/60 Hz.

Si la pantalla es mayor de 14.0” en diagonal, deberá cumplir con:

Peso: no superior a 2,8 Kg (no incluyendo la batería y el transformador).

Duración de la batería: superior a 4 horas (en condiciones de uso permanente).

Deberá contar con configuración para programar el apagado automático de pantalla, disco duro y otros dispositivos, transcurrido un tiempo sin actividad determinable por el operador.

Deberá contar con características de modo de suspensión y/o backup automático de los archivos abiertos transcurrido un cierto tiempo sin actividad determinable por el operador, y/o cuando el nivel de batería haya descendido a niveles peligrosos.

Se deberá indicar toda otra característica adicional de ahorro de energía.

1.14 CARACTERÍSTICAS ADICIONALES QUE COMPLETAN LA PORTABILIDAD

Un (1) alimentador para recarga de baterías y conexión directa a la red de suministro, con capacidad de detectar automáticamente las características de la corriente alterna (voltaje y frecuencia).

RENGLON 6 – ACCES POINT

LAN-018 - ACCESS POINT (PUNTO DE ACCESO INALÁMBRICO)

1.15 DETALLE TÉCNICO / FUNCIONAL

Punto de acceso inalámbrico a la red (WLAN) con las siguientes características:

o) Compatibilidad

IEEE 801.11ac (Wifi 5G), IEEE 802.11n, IEEE 802.11g y IEEE 802.11b

Interfaz de aire: DSSS (IEEE 802.11b/g) y OFDM (IEEE 802.11g/n)

Frecuencia de operación: 2.4 ó 5 GHz, a un ancho de banda de 20, 40 u 80 MHz por canal.

Velocidad de transmisión (máx):

Fallback automático a 11 Mbps para compatibilidad con IEEE 802.11b.

Fallback automático a 54 Mbps para compatibilidad con IEEE 802.11g.

Fallback automático a 150 Mbps para compatibilidad con IEEE 802.11n.

Para el estándar IEEE 802.11n, deberá garantizar un ancho de banda de:

- 450 Mbps (3 o más radios).

Para el estándar IEEE 802.11ac, deberá garantizar un ancho de banda de:

- 1.3 Gbps (3 o más radios).

Deberá contar con “dual stack” IPV4/IPV6

p) Antena

Debe estar incluida teniendo la capacidad de funcionar en los rangos de frecuencia de 2.4 GHz y 5 GHz.

Debe incluir la cantidad de elementos necesarios para garantizar el ancho de banda solicitado.

- ✓ Soporte de calibración automática del radio transmisor.

Soporte de multiplexación espacial múltiple (MIMO):

- ✓ Debe soportar al menos MIMO 3x3 (3 antenas emisoras y 3 receptoras).

Soportará funcionamiento como accesspoint (punto de acceso a la red) y como access bridge (puente entre redes inalámbricas de características diferentes).

q) Estándares de seguridad soportados:

IEEE 802.11i para Acceso Wi-Fi Protegido WPA y WPA2 (seguridad en WLAN).

Protocolos de autenticación extensibles (EAP)

IEEE 802.1X para autenticación basada en el usuario.

Estándares de encripción:

Protocolo de Integridad de Clave Temporal (TKIP) para encripción WPA.

Estándar de Encripción Avanzada (AES) para encripción WPA2

r) Debe soportar claves de acceso WEP IEEE 802.11 de 40 y 128 bits de longitud.

Debe soportar WiFi Multimedia (WMM) y calidad de servicio (QoS) compatible con IEEE 802.11e

s) Puertos LAN

Deberá incorporar al menos 2 puertos Ethernet IEEE 10/100/1000BaseT con conector del tipo RJ45.

t) Concurrencia de conexiones

Debe soportar una concurrencia de usuarios no menor a 250 Usuarios.

u) Administración

Capacidad de centralización de la gestión de los APsvia plataforma de management.

- ✓ Capacidad de distribución inteligente del tráfico WiFi, mediante IEEE 802.11k
- ✓ Soporte de configuración remota de dispositivos conectados, mediante IEEE 802.11v

v) Alimentación

- ✓ Los equipos deberán soportar alimentación PoE, compatible con IEEE 802.3af.

w) Manuales y documentación

Cada unidad deberá ser entregada con 1 (un) juego de manuales de configuración de hardware y software.

Los manuales podrán ser entregados como original en papel, en medios digitales o mediante descarga web.

x) Ciclo de vida de los equipos ofertados:

La fecha mínima de EOL de los equipos ofertados, no debe ser inferior a 5 años.

En caso de existir, los oferentes deben informar:

- Fecha de finalización de soporte por parte del fabricante.
- Fecha de fin de venta (EOS - End Of Sale) por parte del fabricante.

Fecha de fin de vida útil (EOL - End Of Life) por parte del fabricante.

RENGLON 7 – FIREWALL

ESPECIFICACIONES BÁSICAS

Especificaciones Técnicas para la adquisición 5 (cinco) soluciones de **Next Generation Firewall (NGFW)** para 5 (cinco) Institutos Pertenecientes a esta ANLIS. Cada una de ellas debe cumplir con los siguientes requerimientos:

1. DESCRIPCION

1.1. Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la información perimetral que incluye filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPSec y SSL, IPS, prevención contra amenazas de virus, spyware y malware “Zero Day”, bien como controles de transmisión de datos y acceso a internet componiendo una plataforma de seguridad integrada y robusta.

1.2. Por plataforma de seguridad se entiende hardware y software integrados de tipo appliance.

1.3. El soporte y licencias ofrecido por el fabricante de la solución tienen que tener vigencia de 1 (un) año en la modalidad 7x24.

1.4. En relación al RMA el fabricante debe contar con depósito de partes, o equipos completos con presencia local en el país y poder ofrecer mínimamente remplazo de partes en el próximo dia hábil, conocido por las siglan en ingles NBD (next business day), para poder garantizar el funcionamiento de la solución.

1.5. El fabricante debe estar en el cuadrante de líderes de Gartner para “Enterprise Firewall” o firewalls empresariales en los últimos 6 años.

1.6. El fabricante debe estar como líder en el informe de Forrester 2016 para soluciones de protección avanzada.

1.7. El fabricante debe estar como líder en el informe de Forrester de “Zero Trust eXtended (ZTX) Ecosystem Providers.

1.8. El fabricante debe estar certificado para IPv6 en Firewall e IPS por NIST USGv6.

1.9. No se aceptarán soluciones UTM ya que estas están orientadas al segmento SMB.

1.10. Las características deben ser confirmadas mediante documentación oficial de acceso público (guías de administración, manuales y/o guías técnicas). No se aceptarán documentos generados expresamente para este proceso (ad-hoc).

1.11. Las soluciones requeridas deben poder interoperar sin necesidad de software o interaccion de terceros.

1.12. Las soluciones ofrecidas tienen que ser de un mismo fabricante y tener la posibilidad de orquestrarlas entre si y compartir una misma base de inteligencia, se no acepta soluciones que no se orquestren o con bases de firmas de terceras partes.

2. CAPACIDAD

2.1. Cada appliance de la plataforma de seguridad debe poseer las capacidades y características minimas siguientes:

2.1.1. Throughput de 2,4 Gbps medido con trafico real (no es valido tomar mediciones ideales o de laboratorio) con la funcionalidad de control de aplicaciones habilitada, para todas las firmas que el fabricante posea actualizadas con la última actualización disponible y log habilitado.

2.1.2. Throughput de 1 Gbps medido con tráfico de real (no es valido tomar mediciones ideales o de laboratorio), con las siguientes

funcionalidades habilitadas simultáneamente: Clasificación y control de aplicaciones, IPS, Control de navegación por URL, Antivirus y Antispyware, Control de amenazas avanzadas de día cero (Sandboxing). Para todas las firmas que la plataforma de seguridad posea totalmente activadas, actualizadas al día y con el mayor nivel de seguridad posible; considerando múltiples políticas de seguridad (por lo menos 100 políticas de seguridad aplicadas), y que tengan habilitado la generación de Logs y NAT aplicado a todas las reglas.

2.1.3. Soporte a, como mínimo, 200.000 de conexiones simultaneas con todos los modulos de seguridad de capa 7 habilitados simultáneamente, en el mayor nivel de seguridad posible;

2.1.4. Soporte a, como mínimo, 39.000 nuevas conexiones por segundo;

2.1.5. Capacidad de Desencripción de SSL de al menos 25.600 sesiones simultaneas.

2.1.6. Fuente de energia de 240 AC; con posibilidad de tener fuente redundante sobre el mismo equipo.

2.1.7. Alamcenamiento de, como mínimo, 128 GB para el sistema y uso de la solución con el objetivo de que pueda guardar logs y reportes localmente cada equipo.

2.1.8. A continuación, se detallan las Interfaces de red requeridas:

2.1.8.1. Minimo 8 (ocho) interfaces de red 10/100/1.000 sobre interfaces de cobre, con puerto RJ45

2.1.9. Minimo 1 (una) interface de red 1 Gbps dedicada para administración;

2.1.10. Minimo 1 (una) interface de tipo consola o similar;

2.1.11. Soporte a, como mínimo, 3 (tres) ruteadores virtuales;

2.1.12. Soporte a, como mínimo, 50 (cincuenta) zonas de seguridad;

2.1.13. Estar licenciada para soportar sin uso de licenciamiento adicional, 1.000 (mil) clientes de VPN SSL y IPSec simultáneos del estilo cliente-servidor;

2.1.14. Estar licenciada para soportar sin uso de licenciamiento adicional, 2.800 (dos mil ochocientos) túneles de VPN IPSEC simultáneos del estilo sitio-a-sitio;

2.2. Por el equipamiento que compone la plataforma de seguridad, se entiende como hardware y licenciamiento de software necesarios para su funcionamiento;

2.3. Por consola de administración y monitoreo, se entiende el licenciamiento de software necesario para las dos funcionalidades, también como hardware dedicado para el funcionamiento de las mismas.

2.4. La consola de administración y monitoreo puede residir en el mismo appliance de seguridad de red, desde que posea recurso de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función;

2.5. Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados en el site del fabricante como listas de end-of-life y end-of-sale.

3. CARACTERÍSTICAS GENERALES

3.1. La solución debe consistir en appliances de seguridad de red con funcionalidades de Next Generation Firewall (NGFW), y consola de administración y monitoreo;

3.2. Por funcionalidades de NGFW se entiende: reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;

3.3. La plataforma debe ser optimizada para análisis de contenido de aplicaciones en Capa 7;

3.4. El hardware y software que ejecuten las funcionalidades de seguridad de red y de administración y monitoreo, deben ser de tipo appliance. No serán aceptados equipamientos servidores y sistema operacional de uso genérico;

3.5. Todos los equipamientos ofrecidos deben ser adecuados para montaje en rack 19”

3.6. El software deberá ser ofrecido en su versión más estable y/o más avanzada;

3.7. La arquitectura de procesadores utilizado por la solucion tiene que ser procesadores reprogramables, tipo FPGA, para garantizar que con futuras actualizaciones el equipo no quede obsoleto.

3.8. Los dispositivos de seguridad de red deben poseer por lo menos las siguientes funcionalidades:

3.8.1. Soporte de 4094 VLAN Tags 802.1q, tanto por dispositivo como en una sola interfaz;

3.8.2. Agregación de links 802.3ad;

3.8.3. Policy based routing o policy based forwarding;

3.8.4. Ruteo multicast (PIM-SM);

3.8.5. DHCP Relay;

3.8.6. DHCP Server;

3.8.7. Jumbo Frames;

3.8.8. Soporte a creación de objetos de red que puedan ser utilizados como dirección IP de interfaces L3;

3.9. Soportar sub-interfaces ethernet lógicas.

3.10. Debe soportar los siguientes tipos de NAT:

3.10.1. Nat dinamico (Many-to-1);

3.10.2. Nat dinámico (Many-to-Many);

3.10.3. Nat estático (1-to-1);

3.10.4. NAT estático (Many-to-Many);

3.10.5. Nat estático bidireccional 1-to-1;

3.10.6. Traducción de porta (PAT);

3.10.7. NAT de Origen;

3.10.8. NAT de Destino;

3.10.9. Soportar NAT de Origen y NAT de Destino simultáneamente;

3.10.10. Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.

3.10.11. Enviar log para sistemas de monitoreo externos, simultáneamente;

3.10.12. Debe tener la opción de enviar logs para los sistemas de monitoreo externos vía protocolo TCP y SSL;

3.10.13. Debe permitir configurar certificado caso necesario para autenticación del sistema de monitoreo externo de logs;

3.10.14. Seguridad contra anti-spoofing;

3.10.15. Para IPv4, debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2);

3.10.16. Debe soportar MP-BGP
3.10.17. Para IPv6, debe soportar enrutamiento estático y dinámico (OSPFv3);
3.10.18. Soportar OSPF *graceful restart*;
3.10.19. Debe ser capaz de balancear varios enlaces de internet sin el uso de políticas específicas, permitiendo aplicar una variedad de algoritmos distintos (round Robin, weighted...)
3.10.20. Soportar BFD (bidirectional forward detection)
3.10.21. Soportar LACP/LLDP Pre-negotiation
3.10.22. Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Desencripción SSL y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, Activo/Activo, Activo/Pasivo, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones;
3.10.23. Debe contar con una herramienta para poder optimizar políticas de seguridad, detectar cuáles no se esten usando y por cuánto tiempo; poder aprender de las políticas aplicadas y sugerir que aplicaciones deberían aplicarse a las políticas en el NGFW. Dar estadísticas de uso, ancho de banda por aplicación, último hit de las aplicaciones, sobre cada política, con el objetivo de optimizar y mejorar la configuración del NGFW.
3.10.24. El fabtricante de la solucion seleccionada, debe contar con una herramienta que convierta desde multiples fabricantes de firewall (por lo menos: Juniper, Checkpoint, Palo Alto Networks, Cisco, Fortinet, etc) al formata de la solucion adquirida, y ademas optimice las políticas para poder convertir las reglas de origen, destino y puerto en reglas de NGFW basadas en aplicación aprendiendo del trafico de la red.
3.10.25. Los dispositivos de seguridad deben tener la capacidad de operar de forma simultanea mediante el uso de sus interfaces físicas en los siguientes modos dentro del mismo firewall, sin necesidad de tener que hacer uso de contextos virtuales: Modo sniffer (monitoreo y análisis del tráfico de red), Capa 2 (L2), Capa 3 (L3) y modo Transparente;

3.10.25.1. Modo Sniffer, para inspección vía puerto espejo del tráfico de datos de la red;

3.10.25.2. Modo Capa – 2 (L2), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación;

3.10.25.3. Modo Capa – 3 (L3), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación operando como default Gateway de las redes protegidas;

3.10.25.4. Modo Transparente, para poder inspeccionar de datos en línea y tener visibilidad del control de trafico en nivel de aplicación sobre 2 puertos en modo bridge/Transparente.

3.10.26. Modo mixto de trabajo Sniffer, Transparente, L2 e L3 simultaneamente en diferentes interfaces físicas del mismo equipo;

3.10.27. En el modo Transparente, debe poder soportar al menos 256 interfaces (fisicas y/o virtuales) sobre cada sistema virtual lógico (Contexto).

3.11. Soporte a configuración de alta disponibilidad Activo/Pasivo e Activo/Activo:

3.11.1. En modo transparente;

3.11.2. En layer 3;

3.12. La configuración en alta disponibilidad debe sincronizar:

3.12.1. Sesiones;

3.12.2. Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QOS y objetos de red;

3.12.3. Certificados de desencripción;

3.12.4. Asociaciones de Seguridad de las VPNs;

3.12.5. Tablas FIB;

3.12.6. El HA (modo de Alta-Disponibilidad) debe posibilitar monitoreo de fallo de link.

3.13. Las funcionalidades de control de aplicaciones, VPN IPSec y SSL, QOS, SSL y SSH Decryption y protocolos de enrutamiento dinámico deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.

3.14. Debe poder inspeccionar protocolos como:

3.14.1. GRE

3.14.2. IPSEC no encriptado (NULL o AH)

3.14.3. GPRS para GTP-U

4. CONTROL POR POLÍTICA DE FIREWALL

4.1. Deberá soportar controles por zona de seguridad

4.2. Controles de políticas por puerto y protocolo.

4.3. Control de políticas por aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.

4.4. Control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad.

4.5. Control de políticas por código de País (Por ejemplo: AR, BR, USA, UK, RUS).

4.6. Control, inspección y desencripción de SSL por política para tráfico de entrada (Inbound) y Salida (Outbound).

4.7. Debe soportar offload de certificado en inspección de conexiones SSL de entrada (Inbound);

4.8. Debe desencriptar tráfico Inbound y Outbound en conexiones negociadas con TLS v1.1, v1.2 y v1.3;

4.9. Debe desencriptar tráfico que use certificados ECC (como ECDSA)

4.10. Control de inspección y desencripción de SSH por política;

4.11. La plataforma de seguridad debe implementar copia del tráfico desencriptado (SSL y TLS) para soluciones externas de análisis (Forense de red, DLP, Análisis de Amenazas, entre otras);

4.11.1. Se permite el uso de appliance externo, específico para la desencripción de (SSL y TLS), con copia del tráfico desencriptado tanto para el firewall, como para otras soluciones de análisis externas.

4.12. La solución tiene que contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL / TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de trafico, el mismo tiene que tener varios estados de trobleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del trafico (ej: informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexion por parte del cliente, entre otros).
4.13. Bloqueos de los siguientes tipos de archivos: bat, cab, dll, exe, pif, y reg
4.14. Traffic shaping QoS basado en políticas (Prioridad, Garantía y Máximo)
4.15. QoS basado en políticas para marcación de paquetes (diffserv marking), inclusive por aplicaciones.
4.16. Permitir añadir un comentario de auditoria cada vez que se haga un cambio o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada.
4.17. Al crear o editar politicas de seguridad, se debe poder forzar el uso de una descripcion, tag o comentario de auditoria. Esto con el fin de garantizar buenas practicas de documentacion, organizacion y auditoria.
4.18. Soporte a objetos y Reglas IPV6.
4.19. Soporte a objetos y Reglas multicast.
4.20. Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.

5. CONTROL DE APLICACIONES

5.1. Los dispositivos de seguridad de red deberán poseer la capacidad de reconocer aplicaciones, independiente del puerto y protocolo, con las siguientes funcionalidades:
5.1.1. Debe ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación de puertos y protocolos.
5.1.2. Reconocer por lo menos 2500 aplicaciones diferentes, incluyendo, más no limitado: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail;
5.1.3. Reconocer por lo 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, etc;
5.1.4. Debe inspeccionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, incluyendo, más no limitando a RDP en el puerto 80 en vez del 389;
5.1.5. Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis comportamental del tráfico observado, incluyendo, más no limitado a Encrypted Bittorrent y aplicaciones VOIP que utilizan cifrado propietario;

5.1.6. Identificar el uso de tácticas evasivas, o sea, debe tener la capacidad de visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas vía comunicaciones cifradas, tales como Skype y ataques mediante el puerto 443.
5.1.7. Para tráfico Cifrado (SSL y SSH), debe permitir la desencripción de paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante;
5.1.8. Debe realizar decodificación de protocolos con el objetivo de detectar aplicaciones encapsuladas dentro del protocolo y validar si el tráfico corresponde con la especificación del protocolo, incluyendo, más no limitado a Yahoo! Instant Messenger usando HTTP. La decodificación de protocolo también debe identificar funcionalidades específicas dentro de una aplicación, incluyendo, más no limitado a la compartición de archivos dentro de Webex. También debe detectar el archivo y otros contenidos que deben ser inspeccionados de acuerdo a las Reglas de seguridad implementadas;
5.1.9. Debe Identificar el uso de tácticas evasivas vía comunicaciones cifradas;
5.1.10. Debe Actualizar la base de firmas de aplicaciones automáticamente;
5.1.11. Debe Reconocer aplicaciones en IPv6;
5.1.12. Limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos del LDAP/AD;
5.1.13. Los dispositivos de seguridad de red deben poseer la capacidad de identificar al usuario de red con integración al Microsoft Active Directory, sin la necesidad de instalación de agente en el Domain Controller, ni en las estaciones de los usuarios;
5.1.14. Debe ser posible adicionar control de aplicaciones en todas las Reglas de seguridad del dispositivo, o sea, no limitándose solamente a la posibilidad de habilitar control de aplicaciones en algunas Reglas;
5.1.15. Debe soportar múltiples métodos de identificación y clasificación de las aplicaciones, por lo menos chequeo de firmas, decodificación de protocolos y análisis heurístico;
5.1.16. Para mantener la seguridad de la red eficiente, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas;
5.1.17. Permitir nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interface gráfica de la solución, sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones de la empresa;
5.1.18. La creación de firmas personalizadas debe permitir el uso de expresiones regulares, contexto (sesiones o transacciones), usando la posición en el payload de los paquetes TCP y UDP y usando decoders de por lo menos los siguientes protocolos:
5.1.18.1. HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP y File body.
5.1.19. El fabricante debe permitir la solicitud de inclusión de aplicaciones en la base de firmas de aplicaciones;
5.1.20. Debe alertar al usuario cuando una aplicación fuera bloqueada
5.1.21. Debe posibilitar que el control de puertos sea aplicado para todas las aplicaciones;
5.1.22. Debe posibilitar la diferenciación de tráficos Peer2Peer (Bittorrent, emule, neonet, etc.) proveyendo granularidad de control/políticas para los mismos;
5.1.23. Debe posibilitar la diferenciación de tráficos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) proveyendo granularidad de control/políticas para los mismos;
5.1.24. Debe posibilitar la diferenciación y control de partes de las aplicaciones como por ejemplo permitir Gtalk chat y bloquear la transferencia de IM (mensajería instantánea);

5.1.25. Debe posibilitar a diferenciación de aplicaciones Proxies (ghostsurf, freegate, etc.) proveyendo granularidad de control/políticas para los mismos;
5.1.26. Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como:
5.1.26.1. Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
5.1.26.2. Nivel de riesgo de las aplicaciones.
5.1.26.3. Categoría y sub-categoría de aplicaciones.
5.1.26.4. Aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda, etc.
5.1.27. Debe poder monitorear aplicaciones SaaS (Software as a service) tanto via GUI como en reporte predefinido.
5.1.28. Las politicas de seguridad tienen que poder ser creadas en base a las aplicaciones y no en base a puertos TCP/UDP.
5.1.29. La aplicacion de seguridad tienen que ser 100% en base a aplicaciones pudiendo aplicar reglas especificas a cada aplicacion, ejemplo si dos aplicaciones utilizan el mismo puerto de comunicaciones, se tienen que poder crear 2 politicas de seguridad en las cuales se apliquen controles de seguridad diferentes a cada aplicacion.
5.1.30. Al crear politicas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz grafica debe sugerir y permitir agregar las politicas dependientes de la seleccionada, para poder permitir el uso correcto de la aplicación.

6. PREVENCION DE AMENAZAS

6.1. Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS, Antivirus y Anti-Spyware integrados en el propio appliance de Firewall
6.2. Debe incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti-Spyware);
6.3. Las funcionalidades de IPS, Antivirus y Anti-Spyware deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.
6.4. Debe sincronizar las firmas de IPS, Antivirus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo e Activo/pasivo;
6.5. Cuando se utilicen las funciones de IPS, Antivirus y Anti-spyware, el equipamiento debe entregar el mismo performance (no degradar) entre tener 1 única firma de IPS habilitada o tener todas las firmas de IPS, Anti-Vírus y Antispyware habilitadas simultáneamente.
6.6. Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo;
6.7. Excepciones por IP de origen o de destino deben ser posibles en las Reglas, de forma general y firma por firma;
6.8. 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 esos ítems.
6.9. Debe permitir el bloqueo de vulnerabilidades.
6.10. Debe permitir el bloqueo de exploits conocidos.
6.11. Debe incluir seguridad contra ataques de negación de servicios.
6.12. Deberá poseer los siguientes mecanismos de inspección de IPS:
6.13. Análisis de parones de estado de conexiones;

6.14. Análisis de decodificación de protocolo;
6.15. Análisis para detección de anomalías de protocolo;
6.16. Análisis heurístico;
6.17. IP Defragmentation;
6.18. Re ensamblado de paquetes de TCP;
6.19. Bloqueo de paquetes malformados.
6.20. Ser inmune y capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;
6.21. Detectar y bloquear el origen de portscans;
6.22. Bloquear ataques efectuados por worms conocidos, permitiendo al administrador adicionar nuevos patrones;
6.23. Soportar los siguientes mecanismos de inspección contra amenazas de red: análisis de patrones de estado de conexiones, análisis de decodificación de protocolo, análisis para detección de anomalías de protocolo, análisis heurístico, IP Defragmentation, re ensamblado de paquetes de TCP y bloqueo de paquetes malformados;
6.24. Posea firmas específicas para la mitigación de ataques DoS;
6.25. Posea firmas para bloqueo de ataques de buffer overflow;
6.26. Posea firmas de C2 (Comando y control) generadas de forma automática.
6.27. Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
6.28. Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3;
6.29. Soportar bloqueo de archivos por tipo;
6.30. Identificar y bloquear comunicaciones como botnets;
6.31. Debe soportar varias técnicas de prevención, incluyendo Drop y tcp-rst (Cliente, Servidor y ambos);
6.32. Debe soportar referencia cruzada como CVE;
6.33. La solucion ofrecida a partir de los logs debe poder generar indicadores “tags” para IP de equipos a partir de las detecciones de amenazas con el objetivo de poder utilizar los mismos en grupos dinámicos y aplicarlos a otras políticas. Esta funcionalidad tiene que poder efectuarse localmente en el mismo NGFW o bien poder una vez detectado generar el Tag en un firewall remoto o en la consola de gestión para poder aplicar los grupos dinámicos local, remoto o a todos los NGFW de la organización.
6.34. La funcionalidad de Indicadores/Tags mencionada en el punto anterior tiene que poder utilizarse para poder agregar o quitar tags a la IP de origen o destino de una detección efectuada.
6.35. Registrar en la consola de monitoreo las siguientes informaciones sobre amenazas identificadas:
6.36. Debe soportar la captura de paquetes (PCAP), por firma de IPS y Antispyware;
6.37. Debe permitir que en la captura de paquetes por firmas de IPS y Antispyware sea definido el número de paquetes a ser capturados. Esta captura debe permitir seleccionar, como mínimo, 50 paquetes;
6.38. Debe poseer la función resolución de direcciones vía DNS, para que conexiones como destino a dominios maliciosos sean resueltas por el Firewall como direcciones (IPv4 e IPv6), previamente definidos;
6.39. Permitir el bloqueo de virus, por al menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3;
6.40. Los eventos deben identificar el país de donde partió la amenaza;
6.41. Debe incluir seguridad contra virus en contenido HTML y JavaScript, software espía (spyware) y worms.
6.42. Seguridad contra downloads involuntarios usando HTTP de archivos ejecutables. maliciosos.

6.43. Rastreo de virus en pdf.
6.44. Debe permitir la inspección en archivos comprimidos que utilizan o algoritmo deflate (zip, gzip, etc.)
6.45. Debe ser posible la configuración de diferentes políticas de control de amenazas y ataques basados en políticas del firewall considerando Usuarios, Grupos de usuarios, origen, destino, zonas de seguridad, etc, o sea, cada política de firewall podrá tener una configuración diferente de IPS, siendo esas políticas por Usuarios, Grupos de usuario, origen, destino, zonas de seguridad.
6.46. Capacidad de poder redireccionar el trafico de consultas de DNS a un servidor del tipo sinkhole para poder identificar equipos comprometidos con spyware o actividad de command and control dentro de la red corporativa.

7. ANALISIS DE MALWARE MODERNO

7.1. Poseer la capacidad de análisis de amenazas no conocidas;
7.2. Debido a los Malware hoy en día se debe ser muy dinámicos y un antivirus común no es capaz de detectar los mismos a la misma velocidad que sus variaciones son creadas, la solución ofertada deber poseer funcionalidades para análisis de Malware no conocidos incluidas en la propia herramienta
7.3. El dispositivo de seguridad debe ser capaz de enviar archivos transferidos de forma automática para análisis "In Cloud" o local, donde el archivo será ejecutado y simulado en un ambiente controlado;
7.4. Seleccionar a través de la política de Firewall que tipos de archivos sufrirán este análisis;Mo
7.5. Soportar el análisis de por lo menos 60 (sesenta) tipos de comportamientos maliciosos para el análisis de la amenaza no conocida;
7.6. Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows 7;
7.7. Debe soportar el monitoreo de archivos transferidos por internet (HTTP, FTP, HTTP, SMTP) como también archivos transferidos internamente en los servidores de archivos usando SMB;
7.8. El sistema de análisis “In Cloud” o local debe proveer informaciones sobre las acciones del Malware en la máquina infectada, informaciones sobre cuales aplicaciones son utilizadas para causar/propagar la infección, detectar aplicaciones no confiables utilizadas por el Malware, generar firmas de Antivirus y Anti-spyware automáticamente, definir URLs no confiables utilizadas por el nuevo Malware y proveer informaciones sobre el usuario infectado (su dirección ip y su login de red);
7.9. El sistema automático de análisis "In Cloud" o local debe emitir relación para identificar cuales soluciones de antivirus existentes en el mercado poseen firmas para bloquear el malware;
7.10. Debe permitir exportar el resultado de los análisis de malware de día Zero en PDF y CSV a partir de la propia interfaz de administración;
7.11. Debe permitir la descarga de los malware identificados a partir de la propia interfaz de administración;
7.12. Debe permitir visualizar los resultados de los análisis de malware de día Zero en los diferentes sistemas operacionales soportados;
7.13. Debe permitir informar al fabricante cuando haya una sospecha de falso-positivo y falso-negativo en el análisis de malware de día Zero a partir de la propia interfaz de administración.
7.14. Soportar el análisis de archivos ejecutables, DLLs, ZIP y encriptados en SSL en el ambiente controlado;

8. FILTRO DE URL

8.1. La plataforma de seguridad debe poseer las siguientes funcionalidades de filtro de URL

8.1.1. Permite especificar la política por tempo, horario o determinado período (día, mes, año, día de la semana y hora)

8.1.2. Debe ser posible crear políticas por usuario, grupo de usuario, ips, redes y zonas de seguridad

8.1.3. Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y contra de quien está utilizando cual URLs a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, E-Directory y base de datos local

8.1.4. Debe permitir poder publicar los logs de URL con la información de los usuarios conforme a lo descrito en la integración con servicios de directorio

8.1.5. Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL

8.1.6. Debe bloquear el acceso a sitios de búsqueda (Google, Bing y Yahoo!) en el caso de que la opción de Safe Search este deshabilitada. Debe en ese caso exhibir una página de bloqueo dando instrucciones al usuario de como habilitar dicha función

8.1.7. Debe soportar una cacheé local de URL en el appliance, evitando el delay de comunicación/validación de las URLs

8.1.8. Debe poseer al menos 60 categorías de URLs

8.1.9. Debe soportar la creación de categorías URL custom

8.1.10. Debe soportar la exclusión de URLs del bloqueo por categoría

8.1.11. Debe permitir la customización de la página de bloqueo

8.1.12. Debe permitir o bloquear y continuar (habilitando que el usuario acceso a un sitio potencialmente bloqueado informándole del bloqueo y habilitando el botón de “continuar” para permitirle seguir a ese site)

8.1.13. Debe soportar la inclusión de los logs del producto de las informaciones de las actividades de los usuarios

8.1.14. Debe evitar la fuga de credenciales desde o hacia sitios web, pudiendo tener granularidad en la configuración, es decir poder permitir o no el uso de credenciales de red internas en diferentes categorías de paginas web (estas categorías podrían ser: phising, redes sociales, foros, o categorías personalizadas por el cliente, etc), en incluso el uso indebido de los mismos dentro de la red del cliente. El objetivo de este requerimiento, es evitar que credenciales internas de la red sean publicadas en sitios de internet, inclusive sitios categorizados como desconocidos por el motor de categorización de filtros de URL.

8.1.15. Debe poder actualizar de forma automática en 5 minutos o menos las categorías de malware, command and control y phising.

8.1.16. Capacidad de poder aplicar técnicas de aprendizaje de maquina (Machine Learning) localmente sobre los NGFW para poder identificar nuevos sitios de phishing, con la capacidad de poder bloquear los mismos.

8.1.17. Debe contar con multi categorías de URL, que permita que un sitio web pertenezca a dos categorías distintas.

9. PROTECCION AVANZADA DE DNS

9.1. La solución debe ser capaz de proteger contra decenas de millones de dominios maliciosos identificados con análisis en tiempo real sin depender de firmas estáticas.

9.2. La protección de DNS debe ser alimentada exponencialmente por un servicio de inteligencia global.

9.3. El servicio de proteccion de DNS debe alimentarse de telemetria provista por clientes a nivel mundial y más de 30 fuentes de intelifgencia de ameanzas de terceros.
9.4. La solucion debe ser capaz de predecir y detener dominios malicosos de malware basados en algoritmos de geneneración de dominio (por sus siglas en ingles conocido como DGA – Domain Generation Algoritm).
9.5. Aprendizaje automático para detectar dominios DGA nuevos y nunca antes vistos mediante el análisis de las consultas de DNS a medida que se realizan.
9.6. Debe utilizar machine learning o inteligencia artificial para detectar nuevos dominios nunca antes vistos autogenerados por algoritmos DGA.
9.7. Debe poseer políticas para bloquear dominios DGA o interrumpir las conusltar de DNS a dichos dominios.
9.8. Debe detectar e interrumpir robo de datos ocultos o enviados mediante tuneles en trafico DNS.
9.9. Debe analizar las consultas de DNS, incluyendo las tasas de consultas y patrones, entropía, frecuencia, análisis de dominios, etc. para detectar posibles intentos de tunelización de DNS.

10. IDENTIFICACION DE USUARIOS

10.1. Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de quien está utilizando cuales aplicaciones a través de la integración como servicios de directorio, autenticación vía ldap, Active Directory, E-directory y base de datos local.
10.2. Debe poseer integración con Microsoft Active Directory para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.
10.3. Debe poseer integración con Radius para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.
10.4. Debe poseer integración con TACACS+
10.5. Debe posea integración con Ldap para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en Usuarios y Grupos de usuarios.
10.5.1.1. Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x y soluciones NAC vía syslog, para la identificación de direcciones IP y usuarios
10.6. Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal).
10.7. Soporte a autenticación Kerberos.
10.8. Soporte SAML 2.0
10.9. La solucion ofrecida debe soportar e incluir múltiples factores de autenticación (como por ejemplo usuario y password + 2FA hard token + 2FA soft token + portal cautivo) para poder utlizarlo tanto en aplicación web como en aplicaciones cliente servidor.
10.10. Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que tiene estos servicios
10.11. Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en servidores accedidos remotamente, incluso que no sean servidores Windows.

11. QOS

11.1. Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube, ustream, etc) y tener un alto consumo de ancho de banda, se requiere que la solución, a la vez de poder permitir o negar ese tipo de aplicaciones, debe tener la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones, tanto de audio como de vídeo streaming.

11.2. Soportar la creación de políticas de QoS por:

11.2.1. Dirección de origen

11.2.2. Dirección de destino

11.2.3. Por usuario y grupo de LDAP/AD.

11.2.4. Por aplicaciones, incluyendo, más no limitando a Skype, Bittorrent, YouTube y Azureus;

11.2.5. Por puerto;

11.3. El QoS debe permitir la definición de clases por:

11.3.1. Ancho de Banda garantizado

11.3.2. Ancho de Banda Máximo

11.3.3. Cola de prioridad.

11.4. Soportar priorización Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.

11.5. Soportar marcación de paquetes Diffserv, inclusive por aplicaciones;

11.6. Disponer de estadísticas Real Time para clases de QoS.

11.7. Deberá permitir el monitoreo del uso que las aplicaciones hacen por bytes, sesiones y por usuario.

12. FILTRO DE DATOS

12.1. Permite la creación de filtros para archivos y datos predefinidos;

12.2. Los archivos deben ser identificados por extensión y firmas;

12.3. Permite identificar y opcionalmente prevenir la transferencia de varios tipos de archivos (MS Office, PDF, etc) identificados sobre aplicaciones (P2P, InstantMessaging, SMB, etc);

12.4. Soportar la identificación de archivos compactados y las aplicaciones de políticas sobre el contenido de esos tipos de archivos;

12.5. Permitir identificar y opcionalmente prevenir la transferencia de informaciones sensibles, incluyendo, más no limitando al número de tarjetas de crédito, permitiendo la creación de nuevos tipos de datos vía expresión regular;

12.6. Permitir listar el número de aplicaciones soportadas para control de datos;

12.7. Permitir listar el número de tipos de archivos soportados para el control de datos;

12.8. Debe poder integrarse son soluciones de punto final de terceros para mejorar la política de DLP.

12.9. Debe traer por efecto al menos dos perfiles de bloqueo predefinidos.

13. GEO-LOCALIZACION

13.1. Soportar la creación de políticas por Geo localización, permitiendo que el tráfico de determinado País/Países sean bloqueados.

13.2. Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.

13.3. Debe posibilitar la creación de regiones geográficas desde la interfaz gráfica y crear políticas utilizando las mismas.

14. VPN

14.1. Soportar VPN Site-to-Site y Cliente-To-Site;

14.2. Soportar IPSec VPN;
14.3. Soportar SSL VPN;
14.4. La VPN IPSEc debe soportar:
14.4.1. DES y 3DES;
14.4.2. Autenticación MD5 e SHA-1;
14.4.3. Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
14.4.4. Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
14.4.5. AES 128, 192 e 256 (Advanced Encryption Standard)
14.4.6. Debe permitir SSO via Kerberos
14.4.7. Autenticación vía certificado IKE PKI.
14.4.8. Debe ser compatible con la Suite B de protocolos de NSA
14.5. Debe poseer interoperabilidad como los siguientes fabricantes:
14.5.1. Cisco;
14.5.2. Checkpoint;
14.5.3. Juniper;
14.5.4. Palo Alto Networks;
14.5.5. Fortinet;
14.5.6. Sonic Wall
14.6. Las VPN SSL deben soportar:
14.6.1. Permitir que el usuario realice la conexión por medio de cliente instalado en el sistema operacional del equipamiento o por medio de interfaz WEB;
14.6.2. Las funcionalidades de VPN SSL deben ser atendidas con o sin el uso de agente;
14.6.3. La asignación de dirección IP en los clientes remotos de VPN;
14.6.4. La asignación de DNS en los clientes remotos de VPN;
14.6.5. Debe haber la opción de ocultar el agente de VPN instalado en el cliente remoto, tornando el mismo invisible para el usuario;
14.6.6. Deber permitir criar políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN SSL;
14.6.7. Las VPN SSL deben soportar proxy arp y el uso de interfaces PPPOE;
14.6.8. Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
14.6.9. Permite establecer un túnel VPN client-to-site del cliente a la plataforma de seguridad, proveyendo una solución de single-sign-on a los usuarios, integrándose como las herramientas de Windows-logon;
14.6.10. Soporte de lectura y verificación de CRL (certificate revocation list);
14.6.11. Permite la aplicación de políticas de seguridad y visibilidades para las aplicaciones que circulan dentro de los túneles SSL;
14.6.12. El agente de VPN a ser instalado en los equipamientos desktop y laptops, debe ser capaz de ser distribuido de manera automática vía Microsoft SMS, Active Directory y ser descargado directamente desde su propio portal, en el cual residirá el centralizador de VPN;
14.6.13. El agente deberá comunicarse con el portal para determinar las políticas de seguridad del usuario,
14.6.14. Debe permitir que las conexiones como VPN SSL sean establecidas de las siguientes formas:
14.6.14.1. Antes del usuario autenticarse en la estación;
14.6.14.2. Después de la autenticación del usuario en la estación;
14.6.14.3. Bajo demanda del usuario;
14.6.15. Deberá mantener una conexión segura con el portal durante la sesión.
14.6.16. El agente de VPN SSL client-to-site debe ser compatible al menos con: Windows XP, Vista, Windows 7, Windows 8, Windows 10, MacOS X; Apple iOS, Android, Linux, Windows 10 UWP y Google Chrome OS 45 superior

14.6.17. El portal de VPN debe enviar al cliente remoto la lista de gateways VPN activos para el establecimiento de la conexión, los cuales deben poder ser administrados centralizadamente
14.6.18. Debe haber una opción en el cliente remoto de escoger manualmente el Gateway de VPN y de forma automática a través de la mejor respuesta entre los gateways disponibles con base al más rápido.
14.6.19. Debe poseer la capacidad de identificar el origen de conexión de VPN si es interna o externa
14.7. Debe soportar VPN SSL sin el uso de cliente
14.7.1. Esta función no debe estar basada en Java
14.8. Debe poder integrarse con soluciones MDM de terceros (por ejemplo, AirWatch).
14.9. Debe permitir configurar Split Tunel inteligente, que permita seleccionar el tráfico a enrutar en base a la aplicación y dominio de internet. Por ejemplo, la navegación a Salesforce que viaje por el túnel VPN, pero no todo el resto de tráfico de internet.
14.10. Debe permitir aislar el dispositivo de la red y mantenerlo en cuarentena de forma dinámica, en caso se detecte alguna actividad maliciosa
14.11. Debe permitir la configuración de políticas de seguridad de VPN basado en las características del equipo, por lo menos se deberá recopilar las siguientes características: sistema operativo, dominio de red, versión de parche, software antivirus, software DLP y software de cifrado de disco. De tal forma que si el equipo no cumple cierta condición basado en esas características (Perfilamiento y Postura), no permita el acceso a la VPN o le otorgue acceso de mayores restricciones.
14.12. El Perfilamiento y postura mencionado en el punto anterior, tiene que poder efectuarse inclusive dentro de la red, entre dos o mas segmentos de red que controle el firewall, sin necesidad de armar un túnel de VPN, sino solamente utilizando el perfilamiento y postura del equipo de punto final sobre las políticas de seguridad del NGFW.

15. CONSOLA DE ADMINISTRACION y MONITOREO

15.1. La administración de la solución debe soportar acceso vía SSH, cliente WEB (HTTPS) y API abierta;
15.2. En el caso de que sea necesaria la instalación de cliente para administración de la solución, el mismo debe ser compatible con sistemas operacionales Windows y Linux;
15.3. La administración debe permitir/hacer:
15.3.1. Creación y administración de políticas de firewall y control de aplicaciones;
15.3.2. Creación y administración de políticas de IPS y Anti-Spyware;
15.3.3. Creación y administración de políticas de filtro de URL
15.3.4. Monitoreo de logs;
15.3.5. Herramientas de investigación de logs;
15.3.6. Debugging;
15.3.7. Captura de paquetes.
15.3.8. Debe permitir el acceso concurrente de administradores;
15.3.9. Debe tener un mecanismo de búsqueda de comandos de administración vía SSH, facilitando la localización de los comandos;
15.3.10. Debe permitir usar palabras clave y distintos tags de colores para facilitar la identificación de Reglas;
15.3.11. Debe permitir monitorear vía SNMP fallas en el hardware, inserción o remoción de fuentes, discos y ventiladores, uso de recursos por número elevado de sesiones, número de túneles establecidos de VPN cliente-to-site,

porcentaje de utilización en referencia al número total soportado/licenciado y número de sesiones establecidas;

15.3.12. Debe permitir el bloqueo de alteraciones, en el caso de acceso simultaneo de dos o más administradores;

15.3.13. Debe permitir la definición de perfiles de acceso a la consola con permisos granulares como: acceso de escritura, acceso de lectura, creación de usuarios, alteración de configuraciones;

15.3.14. Debe permitir la autenticación integrada con Microsoft Active Directory y servidor Radius;

15.3.15. Debe permitir la localización de donde están siendo utilizados objetos en: Reglas, dirección IP, Rango de IPs, subredes u objetos

15.3.16. Debe poder atribuir secuencialmente un número a cada regla de firewall, NAT, QOS y Reglas de DOS;

15.3.17. Debe permitir la creación de Reglas que estén activas en un horario definido;

15.3.18. Debe permitir la creación de Reglas con fecha de expiración;

15.3.19. Debe poder realizar un backup de las configuraciones y rollback de configuración para la última configuración salvada;

15.3.20. Debe soportar el Rollback de Sistema operativo para la última versión local;

15.3.21. Debe poseer la habilidad del upgrade vía SCP, TFTP e interfaz de administración;

15.3.22. Debe poder validar las Reglas antes de las aplicaciones;

15.3.23. Debe permitir la validación de las políticas, avisando cuando haya Reglas que ofusquen o tengan conflicto con otras (shadowing);

15.3.24. Debe posibilitar la visualización y comparación de configuraciones actuales, la configuración anterior y configuraciones más antiguas.

15.3.25. Debe posibilitar la integración con otras soluciones de SIEM del mercado (third-party SIEM vendors)

15.3.26. Debe permitirá la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo y el horario de la alteración;

15.3.27. Deberá tener la capacidad de generar un gráfico que permita visualizar los cambios en la utilización de aplicaciones en la red en lo que se refiere a un período de tiempo anterior, para permitir comparar los diferentes consumos realizados por las aplicaciones en el tiempo presente con relación al pasado;

15.3.28. Debe permitir la generación de mapas geográficos en tiempo real para la visualización de orígenes y destinos del tráfico generado en la institución;

15.3.29. Debe proveer resúmenes con la vista correlacionada de aplicaciones, amenazas (IPS, Antispyware) URLs y filtro de archivos, para un mejor diagnóstico y respuesta a incidentes;

15.3.30. La administración de la solución debe posibilitar la recolección de estadísticas de todo el tráfico que pasa por los dispositivos de seguridad;

15.3.31. Debe proveer resúmenes de utilización de los recursos por aplicaciones, amenazas (IPS, Anti-Spyware y antivirus de la solución), etc;

15.3.32. Debe proveer de una visualización sumarizada de todas las aplicaciones, amenazas (IPS, Antivirus e Anti-Spyware) y URLs que pasan por la solución;

15.3.33. Debe poseer un mecanismo "Drill-Down" para navegación por los resúmenes en tiempo real;

15.3.34. En las listas de "Drill-Down", debe ser posible identificar el usuario que ha determinado el acceso;

15.3.35. Debe ser posible exportar los logs en CSV;

15.3.36. Deberá ser posible acceder al equipamiento a aplicar configuraciones durante momentos donde el tráfico sea muy alto y la CPU y memoria del equipamiento este siendo totalmente utilizada.
15.3.37. Debe tener rotación de logs;
15.3.38. Debe tener presentaciones de las siguientes informaciones, de forma histórica y en tiempo real (actualizado de forma automática y continua cada 1 minuto):
15.3.39. Debe mostrar la situación del dispositivo y del cluster;
15.3.40. Debe poder mostrar las principales aplicaciones;
15.3.41. Debe poder mostrar las principales aplicaciones por riesgo;
15.3.42. Debe poder mostrar los administradores autenticados en la plataforma de seguridad;
15.3.43. Debe poder mostrar el número de sesiones simultaneas;
15.3.44. Debe poder mostrar el estado de las interfaces;
15.3.45. Debe poder mostrar el uso de CPU;
15.4. Generación de reportes. Como mínimo los siguientes reportes deben poder ser generados:
15.4.1. Resumen gráfico de las aplicaciones utilizadas;
15.4.2. Principales aplicaciones por utilización de ancho de banda de entrada y salida;
15.4.3. Principales aplicaciones por tasa de transferencia en bytes;
15.4.4. Principales hosts por número de amenazas identificadas;
15.4.5. Actividades de un usuario específico y grupo de usuarios del AD/LDAP, incluyendo aplicaciones accedidas y amenazas (IPS, y Anti-Spyware), de red vinculadas a este tráfico;
15.4.6. Debe permitir la creación de reportes personalizados;
15.5. En cada criterio de búsqueda del log debe ser posible incluir múltiples entradas (ej. 10 redes e IP's distintas; servicios HTTP, HTTPS y SMTP), excepto en el campo horario, donde debe ser posible definir un rango de tiempo como criterio de búsqueda;
15.6. Generar alertas automáticas vía:
15.6.1. Email;
15.6.2. SNMP;
15.6.3. Syslog;
15.7. El equipo deberá soportar el envío de logs a un servidor externo syslog según RFC 3164.
15.8. La plataforma de seguridad debe permitir a través de API-XML (Application Program Interface) la integración con sistemas existentes en el ambiente de contratación de forma que posibilite que aplicaciones desarrolladas por el cliente puedan interactuar en tiempo real con la solución permitiendo así que Reglas y políticas de seguridad puedan ser modificadas por estas aplicaciones con la utilización de scripts en lenguajes de programación como Perl o PHP.

ALCANCE DE LA IMPLEMENTACION

ETAPA 1 - Primeros Pasos:

- Verificación visual de los equipos.
- Etiquetado de equipos.

- Montaje físico del equipamiento en el Datacenter del Cliente.

ETAPA 2 - Configuración Base:

- Configuración de DNS Server.
- Creación de nuevo usuario ‘Superadmin’.
- Configuración de NTP.
- Configuración de Login Banner.
- Configuración de HA.

ETAPA 3 - Configuración Inicial de Conectividad:

- Configuración de Interfaces.
- Definición y Configuración de Zonas.
- Configuración de Virtual Routers (VR).
- Configuración de la política de NAT y Seguridad para la navegación.

ETAPA 4 - Licenciamiento y Firmware:

- Registro y Activación de Licencias.
- Actualización de Content-ID (Dependiendo de las licencias adquiridas).
- Actualización de firmware a la última versión estable.

ETAPA 5 - Integraciones:

- Integración con Active Directory (AD).
- Herramienta de Backups Automáticos vía API.
- Integración de EDLs con MineMeld.

ETAPA 6 - Configuración de Políticas de Seguridad:

- Creación de hasta 100 políticas de Firewall con App-ID y User-ID.

- Creación de hasta 10 perfiles de filtros custom (Dependiendo de las licencias adquiridas).
- Creación de hasta 50 reglas de protección de DoS.

ETAPA 7 - Túneles VPN:

- Creación de hasta 20 túneles VPN IPSec.
- Creación de Túneles para conectividad remota con cliente GlobalProtect o Clientless.

Importante: una vez finalizada la implementación el cliente tiene un mes de Soporte ante los incidentes que se puedan generar post puesta en producción del equipo.

La oferta debe incorporar la capacitación de 5 Agentes de Informática de esta ANLIS, (no menor a 24hs de capacitación)-modalidad Virtual.