ANEXO II

PLIEGO DE ESPECIFICACIONES TÉCNICAS

1. DESCRIPCION

- 1.1. Adquisición de una solución de protección de redes con características de NextGeneration 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 deberá ser en el formato Appliance.
- 1.3. El soporte y licencias ofrecido por el fabricante de la solución tienen que tener vigencia de 3 (tres) años en la modalidad 7x24.
- 1.4. El fabricante debe estar en el cuadrante de líderes de Gartner para “Enterprise Firewall” o firewalls empresariales en los últimos 6 años.
- 1.5. El fabricante debe estar como líder en el informe de Forrester de “Zero Trust eXtended (ZTX) EcosystemProviders.
- 1.6. El fabricante debe estar certificado para IPv6 en Firewall e IPS por NIST USGv6.
- 1.7. No se aceptarán soluciones UTM ya que estas están orientadas al segmento SMB.
- 1.8. 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).
- 1.9. Las soluciones ofrecidas tienen que ser de un mismo fabricante y tener la posibilidad de orquestrarlas entre sí y compartir una misma base de inteligencia, se no acepta soluciones que no se orquestren o con bases de firmas de terceras partes.

2. CARACTERISTICAS GENERALES DEL VIRTUAL APPLIANCE

- 2.1. El Virtual Appliance debe ser compatible con los siguientes entornos de nube y virtualización: VMware NSX, ESXi, vCloud Air, Citrix Netscaler SDX, Microsoft Azure e Hyper-V, Amazon® Web Services, Google Cloud, KVM/MyOpenStack.
- 2.2. El licenciamiento debe ser independiente del entorno de virtualización o nube. Pudiendo mover el Virtual Appliance entre cualquiera de los entornos mencionados en el punto anterior

3. CAPACIDAD

- 3.1. La plataforma de seguridad debe poseer las capacidades y características mínimas siguientes:
 - 3.1.1. Throughput de 4Gbps medido con tráfico real (no es válido 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.
 - 3.1.2. Throughput de 2Gbps medido con tráfico de real (no es válido 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.

- 3.1.3. Soporte a, como mínimo, 800.000 conexiones simultaneas con todos los modulos de seguridad de capa 7 habilitados simultáneamente, en el mayor nivel de seguridad posible;
 - 3.1.4. Soporte a, como mínimo, 30.000 nuevas conexiones por segundo;
 - 3.1.5. Capacidad de Descripción de SSL de al menos 15.000 sesiones simultaneas.
 - 3.1.6. Soporte a, como mínimo, 10 (diez) ruteadores virtuales;
 - 3.1.7. Soporte a, como mínimo, 40 (cuarenta) zonas de seguridad;
 - 3.1.8. Estar licenciada para soportar sin uso de licenciamiento, 2.000 (mil) clientes de VPN SSL y IPSec simultáneos del estilo cliente-servidor;
 - 3.1.9. Estar licenciada para soportar sin uso de licenciamiento, 2.000 (dos mil) túneles de VPN IPSEC simultáneos del estilo sitio-a-sitio;
- 3.2. Por el equipamiento que componen la plataforma de seguridad, se entiende como Virtual Appliance y licenciamiento de software necesarios para su funcionamiento;
- 3.3. Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados en el sitio del fabricante como listas de end-of-life y end-of-sale.

4. CARACTERÍSTICAS GENERALES

- 4.1. La solución debe consistir de Virtual Appliances de seguridad de red con funcionalidades de Next Generation Firewall (NGFW), y consola de administración y monitoreo;
- 4.2. Por funcionalidades de NGFW se entiende: reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
- 4.3. La plataforma debe ser optimizada para análisis de contenido de aplicaciones en Capa 7;
- 4.4. El software que ejecuten las funcionalidades de seguridad de red y de administración y monitoreo, deben ser de tipo Virtual Appliance. No serán aceptados equipamientos servidores y sistema operacional de uso genérico;
- 4.5. El software deberá ser ofrecido en su versión más estable y/o más avanzada;
- 4.6. Los dispositivos de seguridad de red deben poseer por lo menos las siguientes funcionalidades:
 - 4.6.1. Soporte de 4094 VLAN Tags 802.1q, tanto por dispositivo como en una sola interfaz;
 - 4.6.2. Agregación de links 802.3ad;
 - 4.6.3. Policy based routing o policy based forwarding;
 - 4.6.4. Ruteo multicast (PIM-SM);
 - 4.6.5. DHCP Relay;
 - 4.6.6. DHCP Server;

- 4.6.7. Jumbo Frames;
- 4.6.8. Soporte a creación de objetos de red que puedan ser utilizados como dirección IP de interfaces L3;
- 4.7. Soportar sub-interfaces ethernet lógicas.
- 4.8. Debe soportar los siguientes tipos de NAT:
 - 4.8.1. Nat dinámico (Many-to-1);
 - 4.8.2. Nat dinámico (Many-to-Many);
 - 4.8.3. Nat estático (1-to-1);
 - 4.8.4. NAT estático (Many-to-Many);
 - 4.8.5. Nat estático bidireccional 1-to-1;
 - 4.8.6. Traducción de porta (PAT);
 - 4.8.7. NAT de Origen;
 - 4.8.8. NAT de Destino;
 - 4.8.9. Soportar NAT de Origen y NAT de Destino simultáneamente;
 - 4.8.10. Enviar log para sistemas de monitoreo externos, simultáneamente;
 - 4.8.11. Debe tener la opción de enviar logs para los sistemas de monitoreo externos vía protocolo TCP y SSL;
 - 4.8.12. Debe permitir configurar certificado caso necesario para autenticación del sistema de monitoreo externo de logs;
 - 4.8.13. Seguridad contra anti-spoofing;
 - 4.8.14. Para IPv4, debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2);
 - 4.8.15. Debe soportar MP-BGP
 - 4.8.16. Para IPv6, debe soportar enrutamiento estático y dinámico (OSPFv3);
 - 4.8.17. Soportar OSPF *graceful restart*;
 - 4.8.18. 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...)
 - 4.8.19. Soportar BFD (bidirectional forward detection)
 - 4.8.20. Soportar LACP/LLDP Pre-negotiation
 - 4.8.21. 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), Descripción 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;
 - 4.8.22. Debe contar con una herramienta para poder optimizar políticas de seguridad, detectar cuáles no se estén 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.
 - 4.8.23. El fabricante de la solución seleccionada, debe contar con una herramienta que convierta desde múltiples fabricantes de firewall (por lo menos: Juniper, Checkpoint, Palo Alto Networks, Cisco, Fortinet, etc) al formato de la solución adquirida, y además optimice las políticas para poder convertir las reglas de origen, destino y puerto en reglas de NGFW basadas en aplicación aprendiendo del tráfico de la red.
 - 4.8.24. Los dispositivos de seguridad deben tener la capacidad de operar de forma simultánea 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;

- 4.8.24.1. Modo Sniffer, para inspección de tráfico de datos de la red;
- 4.8.24.2. Modo Capa – 2 (L2), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación;
- 4.8.24.3. 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;
- 4.8.24.4. Modo Transparente, para poder inspeccionar de datos en línea y tener visibilidad del control de tráfico en nivel de aplicación sobre 2 puertos en modo bridge/Transparente.
- 4.8.25. Modo mixto de trabajo Sniffer, Transparente, L2 e L3 simultáneamente en diferentes interfaces físicas del mismo equipo;
- 4.8.26. En el modo Transparente, debe poder soportar al menos 256 interfaces (físicas y/o virtuales) sobre cada sistema virtual lógico (Contexto).
- 4.9. Soporte a configuración de alta disponibilidad Activo/Pasivo e Activo/Activo:
 - 4.9.1. En modo transparente;
 - 4.9.2. En layer 3;
- 4.10. La configuración en alta disponibilidad debe sincronizar:
 - 4.10.1. Sesiones;
 - 4.10.2. Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QOS y objetos de red;
 - 4.10.3. Certificados de descifrado;
 - 4.10.4. Asociaciones de Seguridad de las VPNs;
 - 4.10.5. Tablas FIB;
 - 4.10.6. El HA (modo de Alta-Disponibilidad) debe posibilitar monitoreo de fallo de link.
- 4.11. 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.
- 4.12. Debe poder inspeccionar protocolos como:
 - 4.12.1. GRE
 - 4.12.2. IPSEC no encriptado (NULL o AH)
 - 4.12.3. GPRS para GTP-U

5. CONTROL POR POLÍTICA DE FIREWALL

- 5.1. Deberá soportar controles por zona de seguridad
- 5.2. Controles de políticas por puerto y protocolo.
- 5.3. 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.
- 5.4. Control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad.

- 5.5. Control de políticas por código de País (Por ejemplo: AR, BR, USA, UK, RUS).
- 5.6. Control, inspección y desenscripción de SSL por política para tráfico de entrada (Inbound) y Salida (Outbound).
- 5.7. Debe soportar offload de certificado en inspección de conexiones SSL de entrada (Inbound);
- 5.8. Capacidad de Desenscripción de SSL de al menos 15.000 sesiones simultáneas.
- 5.9. Debe descriptar tráfico Inbound y Outbound en conexiones negociadas con TLS 1.2;
- 5.10. Debe descriptar tráfico que use certificados ECC (como ECDSA)
- 5.11. Control de inspección y desenscripción de SSH por política;
- 5.12. La plataforma de seguridad debe implementar copia del tráfico desenscriptado (SSL y TLS) para soluciones externas de análisis (Forense de red, DLP, Análisis de Amenazas, entre otras);
- 5.12.1. Se permite el uso de appliance externo, específico para la desenscripción de (SSL y TLS), con copia del tráfico desenscriptado tanto para el firewall, como para otras soluciones de análisis externas.
- 5.13. Bloqueos de los siguientes tipos de archivos: bat, cab, dll, exe, pif, yreg
- 5.14. Traffic shaping QoS basado en políticas (Prioridad, Garantía y Máximo)
- 5.15. QoS basado en políticas para marcación de paquetes (diffserv marking), inclusive por aplicaciones.
- 5.16. Soporte a objetos y Reglas IPV6.
- 5.17. Soporte a objetos y Reglas multicast.
- 5.18. Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.

6. CONTROL DE APLICACIONES

- 6.1. Los dispositivos de seguridad de red deberán poseer la capacidad de reconocer aplicaciones, independiente del puerto y protocolo, con las siguientes funcionalidades:
 - 6.1.1. Debe ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación de puertos y protocolos.
 - 6.1.2. 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;
 - 6.1.3. 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, rcover http, gotomeeting, webex, evernote, google-docs, etc;
 - 6.1.4. 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 limitado a RDP en el puerto 80 en vez del 389;
 - 6.1.5. 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;

- 6.1.6. Identificar el uso de tácticas evasivas, o sea, de 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.
- 6.1.7. Para tráfico Cifrado (SSL y SSH), debe permitir la descifrado de paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante;
- 6.1.8. 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. La decodificación de protocolo también debe identificar funcionalidades específicas dentro de una aplicación. También debe detectar el archivo y otros contenidos que deben ser inspeccionados de acuerdo a las Reglas de seguridad implementadas;
- 6.1.9. Debe Identificar el uso de tácticas evasivas vía comunicaciones cifradas;
- 6.1.10. Debe Actualizar la base de firmas de aplicaciones automáticamente;
- 6.1.11. Debe Reconocer aplicaciones en IPv6;
- 6.1.12. Limitar el ancho de banda (download/upload) usado por aplicaciones (trafficshaping), basado en IP de origen, usuarios y grupos del LDAP/AD;
- 6.1.13. Los dispositivos de seguridad de red deben poseer la capacidad de identificar al usuario de red con integración Microsoft Active Directory, sin la necesidad de instalación de agente en el Domain Controller, ni en las estaciones de los usuarios;
- 6.1.14. 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;
- 6.1.15. Debe soportar múltiples métodos de identificación y clasificación de las aplicaciones, por lo menos chequeo de firmas, decodificación de protocolos y análisis heurístico;
- 6.1.16. Para mantener la seguridad de la red eficiente, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas;
- 6.1.17. 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;
- 6.1.18. 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:
 - 6.1.18.1. HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP y File body.
- 6.1.19. El fabricante debe permitir la solicitud de inclusión de aplicaciones en la base de firmas de aplicaciones;
- 6.1.20. Debe alertar al usuario cuando una aplicación fuera bloqueada
- 6.1.21. Debe posibilitar que el control de puertos sea aplicado para todas las aplicaciones;
- 6.1.22. Debe posibilitar la diferenciación de tráfico Peer2Peer (Bittorrent, emule, neonet, etc.) proveyendo granularidad de control/políticas para los mismos;
- 6.1.23. Debe posibilitar la diferenciación de tráfico de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) proveyendo granularidad de control/políticas para los mismos;

- 6.1.24. 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);
- 6.1.25. Debe posibilitar la diferenciación de aplicaciones Proxies (ghostsurf, freegate, etc.) proveyendo granularidad de control/políticas para los mismos;
- 6.1.26. Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como:
 - 6.1.26.1. Tecnología utilizada en las aplicaciones (Client-Server, BrowseBased, Network Protocol, etc).
 - 6.1.26.2. Nivel de riesgo de las aplicaciones.
 - 6.1.26.3. Categoría y sub-categoría de aplicaciones.
 - 6.1.26.4. Aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda, etc.
- 6.1.27. Debe poder monitorear aplicaciones SaaS (Software as a service) tanto via GUI como en reporte predefinido

7. PREVENCIÓN DE AMENAZAS

- 7.1. Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS, Antivirus y Anti-Spyware integrados en el propio Virtual Appliance de Firewall
- 7.2. Debe incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti-Spyware);
- 7.3. 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.
- 7.4. Debe sincronizar las firmas de IPS, Antivirus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo e Activo/pasivo;
- 7.5. 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-Virus y Anti-spyware habilitadas simultáneamente.
- 7.6. Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo;
- 7.7. Excepciones por IP de origen o de destino deben ser posibles en las Reglas, de forma general y firma por firma;
- 7.8. 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.
- 7.9. Debe permitir el bloqueo de vulnerabilidades.
- 7.10. Debe permitir el bloqueo de exploits conocidos.
- 7.11. Debe incluir seguridad contra ataques de negación de servicios.
- 7.12. Deberá poseer los siguientes mecanismos de inspección de IPS:
 - 7.13. Análisis de parones de estado de conexiones;
 - 7.14. Análisis de decodificación de protocolo;
 - 7.15. Análisis para detección de anomalías de protocolo;
 - 7.16. Análisis heurístico;
 - 7.17. IP Defragmentation;
 - 7.18. Re ensamblado de paquetes de TCP;
 - 7.19. Bloqueo de paquetes malformados.

- 7.20. Ser inmune y capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, etc;
- 7.21. Detectar y bloquear el origen de portscans;
- 7.22. Bloquear ataques efectuados por worms conocidos, permitiendo al administrador añadir nuevos patrones;
- 7.23. 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, reensamblado de paquetes de TCP y bloqueo de paquetes malformados;
- 7.24. Poseer firmas específicas para la mitigación de ataques DoS;
- 7.25. Poseer firmas para bloqueo de ataques de buffer overflow;
- 7.26. Poseer firmas de C2 (Comando y control) generadas de forma automática.
- 7.27. Deberá permitir la creación de firmas customizadas por la interfaz gráfica del producto.
- 7.28. Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 7.29. Soportar bloqueo de archivos por tipo;
- 7.30. Identificar y bloquear comunicaciones como botnets;
- 7.31. Debe soportar varias técnicas de prevención, incluyendo Drop y TCP-RST (Cliente, Servidor y ambos);
- 7.32. Debe soportar referencia cruzada como CVE;
- 7.33. La solución 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.
- 7.34. 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.
- 7.35. Registrar en la consola de monitoreo las siguientes informaciones sobre amenazas identificadas:
- 7.36. Debe soportar la captura de paquetes (PCAP), por firma de IP y Antispyware;
- 7.37. Debe permitir que en la captura de paquetes por firmas de IP y Antispyware sea definido el número de paquetes a ser capturados. Esta captura debe permitir seleccionar, como mínimo, 50 paquetes;
- 7.38. Debe poseer la función de resolución de direcciones vía DNS, para que conexiones como destino a dominios maliciosos sean resueltas por el Firewall como direcciones (IPv4 e IPv6), previamente definidas;
- 7.39. Permitir el bloqueo de virus, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 7.40. Los eventos deben identificar el país de donde partió la amenaza;
- 7.41. Debe incluir seguridad contra virus en contenido HTML y JavaScript, software espía (spyware) y worms.
- 7.42. Seguridad contra downloads involuntarios usando HTTP de archivos ejecutables maliciosos.
- 7.43. Rastreo de virus en pdf.
- 7.44. Debe permitir la inspección en archivos comprimidos que utilizan o algoritmo deflate (zip, gzip, etc.)

- 7.45. Debe ser posible la configuración de diferentes políticas de control de amenazas y ataques basadas 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.

8. ANALISIS DE MALWARE MODERNO

- 8.1. Poseer la capacidad de análisis de amenazas no conocidas;
- 8.2. Debido a los Malware hoy en día se debe ser muy dinámico y un antivirus común no es capaz de detectar los mismos a la misma velocidad que sus variaciones son creadas, la solución ofertada debe poseer funcionalidades para análisis de Malware no conocidos incluidas en la propia herramienta
- 8.3. 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;
- 8.4. Seleccionar a través de la política de Firewall que tipos de archivos sufrirán este análisis;
- 8.5. Soportar el análisis de por lo menos 60 (sesenta) tipos de comportamientos maliciosos para el análisis de la amenaza no conocida;
- 8.6. Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP y Windows 7;
- 8.7. 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;
- 8.8. 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);
- 8.9. 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;
- 8.10. 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;
- 8.11. Debe permitir la descarga de los malware identificados a partir de la propia interfaz de administración;
- 8.12. Debe permitir visualizar los resultados de los análisis de malware de día Zero en los diferentes sistemas operacionales soportados;
- 8.13. 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.
- 8.14. Soportar el análisis de archivos ejecutables, DLLs, ZIP y encriptados en SSL en el ambiente controlado;
- 8.15. Soportar el análisis de archivos del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), email link, flash, archivos de MacOSX (mach-o, dmg, pkg) y Android APKs en el ambiente controlado;
- 8.16. Poseer SLA de, como máximo, 5 minutos para actualización de la base de vacunas contra malware desconocidos identificados en el ambiente controlado;

- 8.17. Permitir el envío de archivos para análisis en el ambiente controlado vía web y de forma automática vía API.
- 8.18. Debe poder dar veredictos distintos, como mínimo:
 - 8.18.1. Malicioso
 - 8.18.2. Grayware
 - 8.18.3. Benigno
 - 8.18.4. Phishing
- 8.19. En caso de detectar una forma de evasión de máquina virtual, debe poder enviar de forma automática a revisión en modo Bare Metal (máquinas físicas)

9. FILTRO DE URL

- 9.1. La plataforma de seguridad debe poseer las siguientes funcionalidades de filtro de URL
 - 9.1.1. Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)
 - 9.1.2. Debe ser posible crear políticas por usuario, grupo de usuario, ips, redes y zonas de seguridad
 - 9.1.3. Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y contra de quien está utilizando cuáles URLs a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, E-Directory y base de datos local
 - 9.1.4. 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
 - 9.1.5. Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL
 - 9.1.6. Debe bloquear el acceso a sitios de búsqueda (Google, Bing y Yahoo!) en el caso de que la opción de SafeSearch esté deshabilitada. Debe en ese caso exhibir una página de bloqueo dando instrucciones al usuario de cómo habilitar dicha función
 - 9.1.7. Debe soportar una caché local de URL en el Virtual Appliance, evitando el delay de comunicación/validación de las URLs
 - 9.1.8. Debe poseer al menos 60 categorías de URLs
 - 9.1.9. Debe soportar la creación de categorías URL custom
 - 9.1.10. Debe soportar la exclusión de URLs del bloqueo por categoría
 - 9.1.11. Debe permitir la customización de la página de bloqueo
 - 9.1.12. Debe permitir o bloquear y continuar (habilitando que el usuario acceda a un sitio potencialmente bloqueado informándole del bloqueo y habilitando el botón de "continuar" para permitirle seguir a ese sitio)
 - 9.1.13. Debe soportar la inclusión de los logs del producto de las informaciones de las actividades de los usuarios
 - 9.1.14. 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 páginas web (estas categorías podrían ser: phishing, 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.
 - 9.1.15. Debe poder actualizar de forma automática en 5 minutos o menos las categorías de malware, command and control y phishing.

10. PROTECCION AVANZADA DE DNS

- 10.1. 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.
- 10.2. La protección de DNS debe ser alimentada exponencialmente por un servicio de inteligencia global.
- 10.3. El servicio de protección de DNS debe alimentarse de telemetría provista por clientes a nivel mundial y más de 30 fuentes de inteligencia de amenazas de terceros.
- 10.4. La solución debe ser capaz de predecir y detener dominios maliciosos de malware basados en algoritmos de generación de dominio (por sus siglas en inglés conocido como DGA – DomainGenerationAlgorithm).
- 10.5. Aprendizaje automático para detectar dominios DGA nuevos y nunca antes vistos mediante el análisis de las consultas de DNS a medida que se realizan.
- 10.6. Debe utilizar machine learning o inteligencia artificial para detectar nuevos dominios nunca antes vistos autogenerados por algoritmos DGA.
- 10.7. Debe poseer políticas para bloquear dominios DGA o interrumpir las consultas de DNS a dichos dominios.
- 10.8. Debe detectar e interrumpir robo de datos ocultos o enviados mediante túneles en tráfico DNS.
- 10.9. 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.

11. IDENTIFICACION DE USUARIOS

- 11.1. Debe incluir la 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.
- 11.2. 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.
- 11.3. Debe poseer integración con Radius para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.
- 11.4. Debe poseer integración con TACACS+
- 11.5. Debe poseer integración con ldap para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en Usuarios y Grupos de usuarios.
 - 11.5.1.1. 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
- 11.6. Debe permitir el control, sin instalación de cliente de software, de 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).
- 11.7. Soporte a autenticación Kerberos.
- 11.8. Soporte SAML 2.0
- 11.9. La solución ofrecida debe soportar e incluir múltiples factores de autenticación (como por ejemplo usuario y password + 2FA hardtoken + 2FA

softtoken + portal cautivo) para poder utilizarlo tanto en aplicación web como en aplicaciones cliente servidor.

- 11.10. Debe poseer Soporte a identificación de múltiples usuarios conectados en un mismo 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
- 11.11. Debe poseer Soporte a identificación de múltiples usuarios conectados en un mismo dirección IP en servidores accedidos remotamente, incluso que no sean servidores Windows.

12. QOS

- 12.1. 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, deba 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.
- 12.2. Soportar la creación de políticas de QoS por:
 - 12.2.1. Dirección de origen
 - 12.2.2. Dirección de destino
 - 12.2.3. Por usuario y grupo de LDAP/AD.
 - 12.2.4. Por aplicaciones, incluyendo, más no limitando a Skype, Bittorrent, YouTube y Azureus;
 - 12.2.5. Por puerto;
- 12.3. El QoS debe permitir la definición de clases por:
 - 12.3.1. Ancho de Banda garantizado
 - 12.3.2. Ancho de Banda Máximo
 - 12.3.3. Cola de prioridad.
- 12.4. Soportar priorización Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.
- 12.5. Soportar marcación de paquetes Diffserv, inclusive por aplicaciones;
- 12.6. Disponer de estadísticas Real Time para clases de QoS.
- 12.7. Deberá permitir el monitoreo del uso que las aplicaciones hacen por bytes, sesiones y por usuario.

13. FILTRO DE DATOS

- 13.1. Permite la creación de filtros para archivos y datos predefinidos;
- 13.2. Los archivos deben ser identificados por extensión y firmas;
- 13.3. Permite identificar y opcionalmente prevenir la transferencia de varios tipos de archivos (MS Office, PDF, etc) identificados sobre aplicaciones (P2P, Instant Messaging, SMB, etc);
- 13.4. Soportar la identificación de archivos compactados y las aplicaciones de políticas sobre el contenido de esos tipos de archivos;
- 13.5. Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, más no limitando al número de tarjetas de crédito, permitiendo la creación de nuevos tipos de datos vía expresión regular;
- 13.6. Permitir listar el número de aplicaciones soportadas para control de datos;
- 13.7. Permitir listar el número de tipos de archivos soportados para el control de datos;
- 13.8. Debe poder integrarse con soluciones de punto final de terceros para mejorar la política de DLP.

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

14. GEO-LOCALIZACION

- 14.1. Soportar la creación de políticas por Geo localización, permitiendo que el tráfico de determinado País/Países sean bloqueados.
- 14.2. Debe permitir la visualización de los países de origen y destino en los logs de acceso.
- 14.3. Debe permitir la creación de regiones geográficas desde la interfaz gráfica y crear políticas utilizando las mismas.

15. VPN

- 15.1. Soportar VPN Site-to-Site y Cliente-To-Site;
- 15.2. Soportar IPsec VPN;
- 15.3. Soportar SSL VPN;
- 15.4. La VPN IPsec debe soportar:
 - 15.4.1. DES y 3DES;
 - 15.4.2. Autenticación MD5 e SHA-1;
 - 15.4.3. Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
 - 15.4.4. Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
 - 15.4.5. AES 128, 192 e 256 (Advanced Encryption Standard)
 - 15.4.6. Debe permitir SSO via Kerberos
 - 15.4.7. Autenticación vía certificado IKE PKI.
 - 15.4.8. Debe ser compatible con la Suite B de protocolos de NSA
- 15.5. Debe poseer interoperabilidad con los siguientes fabricantes:
 - 15.5.1. Cisco;
 - 15.5.2. Checkpoint;
 - 15.5.3. Juniper;
 - 15.5.4. Palo Alto Networks;
 - 15.5.5. Fortinet;
 - 15.5.6. Sonic Wall
- 15.6. Las VPN SSL deben soportar:
 - 15.6.1. Permitir que el usuario realice la conexión por medio de cliente instalado en el sistema operativo o por medio de interfaz WEB;
 - 15.6.2. Las funcionalidades de VPN SSL deben ser atendidas con o sin el uso de agente;
 - 15.6.3. La asignación de dirección IP en los clientes remotos de VPN;
 - 15.6.4. La asignación de DNS en los clientes remotos de VPN;
 - 15.6.5. Debe haber la opción de ocultar el agente de VPN instalado en el cliente remoto, tornando el mismo invisible para el usuario;
 - 15.6.6. Debe permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN SSL;
 - 15.6.7. Las VPN SSL deben soportar proxy y el uso de interfaces PPPoE;
 - 15.6.8. Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
 - 15.6.9. 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 con las herramientas de Windows-logon;
 - 15.6.10. Soporte de lectura y verificación de CRL (certificate revocation list);
 - 15.6.11. Permite la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles SSL;
 - 15.6.12. El agente de VPN a ser instalado en los equipos 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;
- 15.6.13. El agente deberá comunicarse con el portal para determinar las políticas de seguridad del usuario,
 - 15.6.14. Debe permitir que las conexiones como VPN SSL sean establecidas de las siguientes formas:
 - 15.6.14.1. Antes del usuario autenticarse en la estación;
 - 15.6.14.2. Después de la autenticación del usuario en la estación;
 - 15.6.14.3. Bajo demanda del usuario;
 - 15.6.15. Deberá mantener una conexión segura con el portal durante la sesión.
 - 15.6.16. 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
 - 15.6.17. 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
 - 15.6.18. 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.
 - 15.6.19. Debe poseer la capacidad de identificar el origen de conexión de VPN si es interna o externa
 - 15.7. Debe soportar VPN SSL sin el uso de cliente
 - 15.7.1. Esta función no debe estar basada en Java
 - 15.8. Debe poder integrarse con soluciones MDM de terceros (por ejemplo, AirWatch)

16. CONSOLA DE ADMINISTRACION y MONITOREO

- 16.1. La administración de la solución debe soportar acceso vía SSH, cliente WEB (HTTPS) y API abierta;
- 16.2. 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;
- 16.3. La administración debe permitir/hacer:
 - 16.3.1. Creación y administración de políticas de firewall y control de aplicaciones;
 - 16.3.2. Creación y administración de políticas de IPS y Anti-Spyware;
 - 16.3.3. Creación y administración de políticas de filtro de URL
 - 16.3.4. Monitoreo de logs;
 - 16.3.5. Herramientas de investigación de logs;
 - 16.3.6. Debugging;
 - 16.3.7. Captura de paquetes.
 - 16.3.8. Debe permitir el acceso concurrente de administradores;
 - 16.3.9. Debe tener un mecanismo de búsqueda de comandos de administración vía SSH, facilitando la localización de los comandos;
 - 16.3.10. Debe permitir usar palabras clave y distintos tags de colores para facilitar la identificación de Reglas;
 - 16.3.11. 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;
 - 16.3.12. Debe permitir el bloqueo de alteraciones, en el caso de acceso simultáneo de dos o más administradores;

- 16.3.13. 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;
- 16.3.14. Debe permitir la autenticación integrada con Microsoft Active Directory y servidor Radius;
- 16.3.15. Debe permitir la localización de donde están siendo utilizados objetos en: Reglas, dirección IP, Rango de IPs, subredes u objetos
- 16.3.16. Debe poder atribuir secuencialmente un número a cada regla de firewall, NAT, QOS y Reglas de DOS;
- 16.3.17. Debe permitir la creación de Reglas que estén activas en un horario definido;
- 16.3.18. Debe permitir la creación de Reglas con fecha de expiración;
- 16.3.19. Debe poder realizar un backup de las configuraciones y rollback de configuración para la última configuración salvada;
- 16.3.20. Debe soportar el Rollback de Sistema operativo para la última versión local;
- 16.3.21. Debe poseer la habilidad del upgrade vía SCP, TFTP e interfaz de administración;
- 16.3.22. Debe poder validar las Reglas antes de las aplicaciones;
- 16.3.23. Debe permitir la validación de las políticas, avisando cuando haya Reglas que ofusquen o tengan conflicto con otras (shadowing);
- 16.3.24. Debe posibilitar la visualización y comparación de configuraciones actuales, la configuración anterior y configuraciones más antiguas.
- 16.3.25. Debe posibilitar la integración con otras soluciones de SIEM del mercado (third-party SIEM vendors)
- 16.3.26. Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó y el horario de la alteración;
- 16.3.27. 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;
- 16.3.28. Debe permitir la generación de mapas geográficos en tiempo real para la visualización de orígenes y destinos del tráfico generado en la institución;
- 16.3.29. 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;
- 16.3.30. La administración de la solución debe posibilitar la recolección de estadísticas de todo el tráfico que pasa por los dispositivos de seguridad;
- 16.3.31. Debe proveer resúmenes de utilización de los recursos por aplicaciones, amenazas (IPS, Anti-Spyware y antivirus de la solución), etc;
- 16.3.32. Debe proveer de una visualización sumariada de todas las aplicaciones, amenazas (IPS, Antivirus e Anti-Spyware) y URLs que pasan por la solución;
- 16.3.33. Debe poseer un mecanismo "Drill-Down" para navegación por los resúmenes en tiempo real;
- 16.3.34. En las listas de "Drill-Down", debe ser posible identificar el usuario que ha determinado el acceso;
- 16.3.35. Debe ser posible exportar los logs en CSV;
- 16.3.36. 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.
- 16.3.37. Debe tener rotación de logs;

- 16.3.38. Debe tener presentaciones de las siguientes informaciones, de forma histórica y en tiempo real (actualizado de forma automática y continua cada 1 minuto):
- 16.3.39. Debe mostrar la situación del dispositivo y del cluster;
- 16.3.40. Debe poder mostrar las principales aplicaciones;
- 16.3.41. Debe poder mostrar las principales aplicaciones por riesgo;
- 16.3.42. Debe poder mostrar los administradores autenticados en la plataforma de seguridad;
- 16.3.43. Debe poder mostrar el número de sesiones simultaneas;
- 16.3.44. Debe poder mostrar el estado de las interfaces;
- 16.3.45. Debe poder mostrar el uso de CPU;
- 16.4. Generación de reportes. Como mínimo los siguientes reportes deben poder ser generados:
 - 16.4.1. Resumen gráfico de las aplicaciones utilizadas;
 - 16.4.2. Principales aplicaciones por utilización de ancho de banda de entrada y salida;
 - 16.4.3. Principales aplicaciones por tasa de transferencia en bytes;
 - 16.4.4. Principales hosts por número de amenazas identificadas;
 - 16.4.5. 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;
 - 16.4.6. Debe permitir la creación de reportes personalizados;
- 16.5. 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;
- 16.6. Generar alertas automáticas vía:
 - 16.6.1. Email;
 - 16.6.2. SNMP;
 - 16.6.3. Syslog;
- 16.7. El equipo deberá soportar el envío de logs a un servidor externo syslogsegún RFC 3164.
- 16.8. La plataforma de seguridad debe permitir a través de API-XML (ApplicationProgram 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.

17. MIGRACIÓN E IMPLEMENTACIÓN

- 17.1. Implementación básica de Firewall a adquirir.
- 17.2. Configuración de networking y cambio de topología actual.
- 17.3. Migración de reglas de firewall al nuevo equipo desde diferentes tecnologías de firewall y proxys.
- 17.4.
 - Configuración de reglas de firewall.
- 17.5.
 - Configuración de NATs.
- 17.6.
 - Configuración de VPNsIPSec.
- 17.7.
 - Configuración de VPN SSL para acceso de los usuarios.
- 17.8.
 - Integración con Active Directory.
- 17.9.
 - Configuración de reglas de URL Filter.
- 17.10.
 - Configuración de reglas de Application Control.
- 17.11.
 - Configuración de reglas de AntiVirus.

- 17.12. • Configuración de reglas de IPS.

18. CAPACITACIÓN

18.1. Se deberá brindar una capacitación para todo el personal de redes, el mismo deberá contemplar todos los conocimientos de las diferentes funcionalidades requeridas en la solución. Se deberán entregar los certificados correspondientes de la capacitación avalados por el oferente.
en este punto se observa que deberá requerir adicionalmente lo siguiente:

- i. Carga horaria de la capacitación: No debera ser con una carga horaria menor a 2 hs durante una semana
- ii. Cantidad de participantes: 3 (tres)
- iii. Domicilio de dictado: Se dictara en el organismo

19. SERVICIOS DE SOPORTE PARA EL FIREWALL

- 19.1. Soporte Técnico para la tecnología ofrecida.
- 19.2. Soporte y seguimiento de incidentes.
- 19.3. Upgrades de Sistemas Operativos.
- 19.4. Mejora continua en seguridad.
- 19.5. Apertura y seguimiento de casos con el fabricante.

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 en donde se cumplen cada una de las especificaciones solicitadas en el pliego. Serán desestimadas todas las propuestas técnicas que no cumplan con lo anteriormente solicitado.

Los oferentes deberán ser canales certificados de las casas matrices.

Garantía de buen funcionamiento de los equipos y la configuración solicitada.

Servicio de soporte técnico, mantenimiento correctivo y/o preventivo (de corresponder), Indicando los horarios de atención, plazos máximos de respuesta y reparación de los Incidentes que puedan suscitarse.

El equipamiento cotizado se entregará con un servicio de soporte y mantenimiento (upgrade) por un período de 1 (un) año a partir de la entrega.

El soporte técnico del mismo debera esta disponible de lunes a viernes de 8 a 18 hs. El tiempo de respuesta a losllamadosdeberá ser de 2 hs. como máximo

vi. el adjudicatario en ningun momento deberá tener acceso a los servidores o informacion crítica y confidencial.

En caso de tener que acceder a los mismos deberá respetar las Confidenciales de los datos que se encuentren almacenados en los servidores que se pretende redundar.

Solicitar Garantía Técnica del firewall a proveer, indicando el alcance y las condiciones de la misma.

vii. Los adjudicatarios deberán proveer, a partir de la fecha de recepción y por el período mínimo de 1 (un) año, un servicio de garantía integral (partes, mano de obra y reemplazo inmediato de partes dañadas) para todo el bien o servicio ofertado

(entendiéndose por “recepción” no su simple entrega, sino instalados y funcionando debiendo extenderse la correspondiente constancia con indicación de lugar, fecha y firma del funcionario receptor), con atención en el lugar de instalación incluyendo repuestos, traslados y mano de obra.