**ESPECIFICACIONES BÁSICAS**

**- GESTION UNIFICADA DE AMENAZAS EN CAPA 7 –**

1. **DESCRIPCIÓN (SE DEBE CONTEMPLAR PARA CORFERIAS Y UNA SUCURSAL – dos soluciones-)**

|  |  |  |
| --- | --- | --- |
|  |  | Cumple / no cumple |
| 1.1 | Adquisicion de dos solucciones de proteccion de red con características de Next Generation Firewall (NGFW) en alta disponibilidad marca Paloalto Networks para la seguridad de la informacion perimetral que incluye control de aplicaciones, administracion de ancho de banda (QoS), VPN IPSec y SSL, IPS, prevencion contra amenazas de vírus, spyware y malware “Zero Day”, bien como controles de transmision de datos y acceso a internet comoponiendo una plataforma de seguridwad integrada y robusta. |  |
| 1.2 | Por plataforma de seguridad se entiende hardware y software integrados de tipo appliance. |  |
| 1.3 | El fabricante debe estar en el cuadrante de lideres de Gartner para “Enterprise Firewall” o firewalls empresariales en los últimos 4 años |  |
| 1.4 | El fabricante debe estar certificado para IPv6 en Firewall e IPS por USGv6 |  |
| 1.5 | Debe encontrarse como líderes en el reporte de Forrester del 2016 para Automated Malware Analysis (AMA) |  |
| 1.6 | No se aceptaran soluciones UTM ya que estas estan orientadas al segmento Pyme. |  |
| 1.7 | Las características deben ser confirmadas mediante documentacion oficial de acceso publico (guias de administracion, manuales y/o guias técnicas). No se aceptaran documentos generados expresamente para este processo (ad-hoc).  |  |

1. **CAPACIDAD Y CANTIDADES**

|  |  |  |
| --- | --- | --- |
|  |  | **Cumple / no cumple** |
| **2.1** | La plataforma de seguridad debe poseer las capacidades y características siguientes (Informacion por cada una de las dos maquinas): |  |
| **2.1.1** | Throughput de 18.5 Gbps con la funcionalidad de control de aplicaciones habilitada para todas las firmas que el fabricante posea; |  |
| **2.1.2** | Throughput de 9.2 Gbps con las siguientes funcionalidades habilitadas simultaneamente para todas las firmas que la plataforma de seguridad posea debidamente activadas y actuando: control de aplicaciones, IPS, Antivírus e Antispyware;  |  |
| **2.1.3** | Soporte a, como mínimo, 4.000.000 de conexiones simultaneas;  |  |
| **2.1.4** | Soporte a, como mínimo, 169.000 nuevas conexiones por segundo;  |  |
| **2.1.5** | Fuente 120/240 AC o DC, redundante y hot-swappable; |  |
| **2.1.6** | Disco Solid State Drive (SSD) de, como mínimo, 240 GB en RAID 1, para almacenamiento del sistema. |  |
| **2.1.7** | Unidades de Disco duro (HDD) de, como mínimo, 2TB, en RAID 1 para almacenamiento de Logs; |  |
| **2.1.8** | 4 (cuatro) interfaces de red 100/1000/10000 base-TX;  |  |
| **2.1.9** | 16 (dieciseis) interfaces de red 1G/10G Gbps SFP/SFP+; incluir en la oferta dos módulos transeiver SFP+ SR 10GigE transceiver (PA-7000 series, PA-5060, PA-5050, PA-3060) por maquina para un total de 4; |  |
| **2.1.10** | 4 (cuatro) interfaces de red 40G (QSFP+); |  |
| **2.1.11** | 2 (dos) interfaces dedicadas para alta disponibilidade a 1 Gbps; |  |
| **2.1.12** | 1 (una) interfaz dedicada para alta disponibilidade a 40 Gbps; |  |
| **2.1.13** | 1 (una) interfaz de red 1 Gbps dedicada para administracion; |  |
| **2.1.14** | 1 (una) interfaz de tipo consola o similar; |  |
| **2.1.15** | Soporte a, como mínimo, 20 (veinte) ruteadores virtuales; |  |
| **2.1.16** | Soporte a, como mínimo, 80 (ochenta) zonas de seguridad; |  |
| **2.1.17** | Estar licenciada para soportar sin uso de licenciamiento, 15.000 (quince mil) clientes de VPN SSL simultaneos;  |  |
| **2.1.18** | Estar licenciada para soportar sin uso de licenciamiento, 10.000 (diez mil) tuneles de VPN IPSEC simultaneos; |  |
| **2.2** | Debe tener posibilidad de virtualizar, al menos, 10 sistemas de firewall sin necesidad de licencia alguna |  |
| **2.3** | Debe permitir expansion futura a hasta 20 sistemas virtuales lógicos (Contextos) en el firewall Físico; |  |
| **2.4** | Los contextos virtuales deben las funcionalidades nativas del gateway de seguridad incluyendo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de Datos, VPN, Control de Aplicaciones, QOS, NAT e Identificacion de usuarios; |  |
| **2.5** | Por el equipamento que comopone la plataforma de seguridad, se entiende como hardware y licenciamiento de software necesarios para su funcionamento; |  |
| **2.6** | Por consola de administracion y monitoreo, se entiende el licenciamento de software necesario para las dos funcionalidades, tambien como hardware dedicado para el funcionamento de las mismas. |  |
| **2.7** | La consola de administracion 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 funcion; |  |
| **2.8** | Para efectos de la propuesta, ninguno de los modelos ofertados podran estar listados en el site del fabricante como listas de end-of-life y end-of-sale. |  |

1. **CARACTERÍSTICAS GENERALES**

|  |  |  |
| --- | --- | --- |
|  |   | **cumple no cumple** |
| **3.1** | La solucion debe consistir de un appliance de seguridad de red con funcionalidades de Next Generation Firewall (NGFW), y consola de administracion y monitoreo; |   |
| **3.2** | Por funcionalidades de NGFW se entiende: reconocimiento de aplicaciones, prevencion de amenazas, identificacion de usuarios y control granular de permisos; |   |
| **3.3** | La plataforma debe ser optimizada para analisis de contenido de aplicaciones en Capa 7; |   |
| **3.4** | El hardware y software que ejecuten las funcionalidades de seguridad de red y de administracion y monitoreo, deben ser de tipo appliance. No seran acceptados equipamentos servidores y sistema operacional de uso genérico; |   |
| **3.5** | Todos los equipamentos ofrecidos deben ser adecuados para montaje en rack 19” |   |
| **3.6** | El software deberá ser ofrecido en su version mas estable y/o mas avanzada; |   |
| **3.7** | Los dispositivos de seguridad de red deben poseer por lo menos las siguientes funcionalidades:  |   |
| **3.8** | Soporte a 4094 VLAN Tags 802.1q;  |   |
| **3.9** | Agregacion de links 802.3ad; Policy based routing o policy based forwarding; Ruteo multicast (PIM-SM); DHCP Relay; DHCP Server;Jumbo Frames; Soporte a creacion de objetos de red que puedan ser utilizados como direccion IP de interfaces L3;Soportar sub-interfaces ethernet logicas.Debe soportar los siguientes tipos de NAT:Nat dinamico (Many-to-1);Nat dinamico (Many-to-Many);Nat estático (1-to-1);NAT estático (Many-to-Many);Nat estático bidirecional 1-to-1;Traduccion de porta (PAT);NAT de Origen;NAT de Destino;Soportar NAT de Origen y NAT de Destino simultaneamente;Enviar log para sistemas de monitoreo externos, simultaneamente; Debe tener la opcion de enviar logs para los sistemas de monitoreo externos via protocolo TCP y SSL;Debe permitir configurar certificado caso necesario para autenticacion del sistema de monitoreo externo de logs;Seguridad contra anti-spoofing; Para IPv4, debe soportar enrutamiento estático y dinamico (RIPv2, BGP y OSPFv2);Para IPv6, debe soportar enrutamiento estático y dinamico (OSPFv3);Soportar OSPF *graceful restart*;Debe ser capaz de balancear vários enlaces de internet sin el uso de politicas especificas, permitiendo aplicar una variedad de algoritmos distintos (round Robin, weighted...).Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificacion 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, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, Activo/Activo, Activo/Pasivo, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones;Los dispositivos de seguridad deben tener la capacidad de operar de forma simultanea mediante el uso de sus interfaces físicas en los siguientes modos: Modo sniffer (monitoreo y analisis del trafico de red), Capa 2 (l2) y Capa 3 (l3);Modo Sniffer, para inspeccion via puerto espejo del trafico de datos de la red;Modo Capa – 2 (L2), para inspeccion de datos en linea y tener visibilida del control del trafico en nível de aplicacion;Modo Capa – 3 (L3), para inspeccion de datos en linea y tener visibilida del control del trafico en nível de aplicacion operando como default gateway de las redes protegidas;Modo mixto de trabajo Sniffer, L2 e L3 en diferentes interfaces físicas; |   |
| **3.10** | Soporte a configuracion de alta disponibilidad Activo/Pasivo e Activo/Activo:En modo transparente;En layer 3; |   |
| **3.11** | La configuracion en alta disponibilidad debe sincronizar:Sesiones;Configuraciones, incluyendo, mas no limitado a políticas de Firewall, NAT, QOS y objetos de red; Certificados de-criptografados;Asociaciones de Seguridad de las VPNs;Tablas FIB;El HA (modo de Alta-Disponibilidad) debe posibilitar monitoreo de fallo de link. |   |
| **3.12** | Las funcionalidades de control de aplicaciones, VPN IPSec y SSL, QOS, SSL y SSH Decryption y protocolos de enrutamiento dinamico deben operar en caracter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe derecho de recibir actualizaciones o que no haya contrato de garantia de software con el fabricante. |   |
| **3.13** | La identificacion de usuarios, el control de aplicaciones, filtro de datos, VPN, QoS, NATs, GeoLocalizacion debe de estar embebido en el sistema operativo, sin necesidad de una licencia que active las mismas. No se aceptaran soluciones que se tengan que licenciar o renovar anualmente alguna de estas funcionalidades. |   |

1. **CONTROL POR POLÍTICA DE FIREWALL**

|  |  |  |
| --- | --- | --- |
|  |   | **cumple no cumple** |
| **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 dinamicos de aplicaciones (baseados en características y comoportamento de las aplicaciones) y categorias 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: BR, USA, UK, RUS). |   |
| **4.6** | Control, inspeccion y desencripción de SSL por política para trafico de entrada (Inbound) y Salida (Outbound). |   |
| **4.7** | Debe soportar offload de certificado en inspeccion de conexiones SSL de entrada (Inbound); |   |
| **4.8** | Debe desencriptar trafico Inbound y Outbound en conexiones negociadas con TLS 1.2; |   |
| **4.9** | Control de inspeccion y desencripción de SSH por política; |   |
| **4.10** | La plataforma de seguridad debe implementar espejamiento de trafico desencripcióndo (SSL e TLS) para soluciones externas de analisis (Forense de red, DLP, Analisis de Amenazas, entre otras); |   |
| **4.11** | Es permitido el uso de appliance externo, específico para la desencripción de (SSL y TLS), con espejamiento de copia del trafico desencripcióndo tanto para el firewall, como para las soluciones de analisis. |   |
| **4.12** | Bloqueos de los siguientes tipos de archivos: bat, cab, dll, exe, pif, e reg  |   |
| **4.13** | Traffic shaping QoS baseado en Políticas (Prioridad, Garantia y Máximo) |   |
| **4.14** | QoS baseado en políticas para marcacion de paquetes (diffserv marking), inclusive por aplicaciones. |   |
| **4.15** | Soporte a objetos y Reglas IPV6. |   |
| **4.16** | Soporte a objetos y Reglas multicast. |   |
| **4.17** | Soportar los atributos de agendamento de las políticas con el objetivo de habilitar y desabilitar políticas en horários predefinidos automaticamente. |   |
| **4.18** | Permitir la detección de portales de phishing estableciendo políticas que eviten el envío de credenciales válidas de usuarios a sitiosno autorizadas. |   |
| **4.19** | Creación de políticas que soliciten un segundo factor de autenticación basadas en el origen (Usuario / Zona / Direcciones) y destino del tráfico (Aplicativos / Zonas / IP) |   |
| **4.20** | Aplicación de etiqueta de manera automática a una IP origen (o destino) cuando un log es generado en el firewall, y que la etiqueta pueda formar parte de políticas existentes que puedan aplicar controles de manera dinámica |   |

1. **CONTROL DE APLICACIONES**

|  |  |  |
| --- | --- | --- |
|  |   | **cumple no cumple** |
| **5.1** | Los dispositivos de seguridad de red deberan poseer la capacidad de reconocer aplicaciones, independente del puerto y protocolo, con las siguientes funcionalidades:  |   |
| **5.2** | Debe ser posible la liberacion y bloqueo solamente de aplicaciones sin la necesidad de liberacion de puertos y protocolos. |   |
| **5.3** | Reconocer por lo menos 2000 aplicaciones diferentes, incluyendo, mas no limitado: el trafico relacionado a peer-to-peer, redes sociales, acesso remoto, update de software, protocolos de red, voip, áudio, vídeo, proxy, mensajeria instantanea, comoparticion de archvos, e-mail; |   |
| **5.4** | 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; |   |
| **5.5** | Debe inspecionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independente del puerto y protocolo. El chequeo de firmas tambien debe determinar si una aplicacion está utilizando su puerto default o no, incluyendo, mas no limitando a RDP en el puerto 80 en vez del 389; |   |
| **5.6** | Debe aplicar analisis heuristico a fin de detectar aplicaciones a través de analisis comoportamental del trafico observado, incluyendo, mas no limitado a Encrypted Bittorrent y aplicaciones VOIP que utilizan criptografia proprietária; |   |
| **5.7** | Identificar el uso de tacticas evasivas, o sea, debe tener la capacidad de visualizar y controlar las aplicaciones y los ataques que utilizan táticas evasivas via comounicaciones criptografiadas, tales como Skype y ataques mediante el puerto 443. |   |
| **5.8** | Para trafico criptografado (SSL y SSH), debe desencripciónr paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante; |   |
| **5.9** | Debe realizar decodificacion de protocolos con el objetivo de detectar aplicaciones encapsuladas dentro del protocolo y validar si el trafico corresponde con la especificacion del protocolo, incluyendo, mas no limitado a Yahoo Instant Messenger usando HTTP. La decodificacion de protocolo tambien debe identificar funcionalidades especificas dentro de una aplicacion, incluyendo, mas no limitado a la comoparticion de archivos dentro de Webex. Tambien debe detectar el archivo y otros contenidos que deben ser inspecionados de acuerto a las Reglas de seguridad implementadas; |   |
| **5.10** | Debe Identificar el uso de táticas evasivas via comounicaciones criptografiadas; |   |
| **5.11** | Debe Actualizar la base de firmas de aplicaciones automaticamente;  |   |
| **5.12** | Debe Reconocer aplicaciones en IPv6;  |   |
| **5.13** | Limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos del LDAP/AD; |   |
| **5.14** | Los dispositivos de seguridad de red deben poseer la capacidad de identificar al usuário de red con integracion al Microsoft Active Directory, sin la necesidad de instalacion de agente en el Domain Controller, ni en las estaciones de los usuarios;  |   |
| **5.15** | Debe ser posible adicionar control de aplicaciones en todas las Reglas de seguridad del dispositivo, o sea, no limitandose solamente a la posiblidad de habilitar control de aplicaciones en algumas Reglas; |   |
| **5.16** | Debe soportar múltiples métodos de identificacion y clasificacion de las aplicaciones, por lo menos chequeo de firmas, decodificacion de protocolos y analisis heurístico; |   |
| **5.17** | Para mantener la seguridad de la red eficiente, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas; |   |
| **5.18** | Permitir nativamente la creacion de firmas personalizadas para reconocimiento de aplicaciones proprietárias en la própria interface gráfica de la solucion, sin la necesidad de accion por parte del fabricante, manteniando la confidencialidad de las aplicaciones del organo; |   |
| **5.19** | La creacion de firmas personalizadas debe permitir el uso de expresiones regulares, contexto (sesiones o transacciones), usando la posicion en el payload de los paquetes TCP y UDP y usando decoders de por lo menos los siguientes protocolos:  |   |
| **5.20** | HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP y File body. |   |
| **5.21** | El fabricante debe permitir la solucitud de inclusion de aplicaciones en la base de firmas de aplicaciones; |   |
| **5.22** | Debe alertar al usuário cuando una aplicaciones fuera bloqueada |   |
| **5.23** | Debe posibilitar que el control de puertos sea aplicado para todas las aplicaciones; |   |
| **5.24** | Debe posibilitar la diferenciacion de traficos Peer2Peer (Bittorrent, emule, neonet, etc.) proveyendo granularidad de control/politicas para los mismos; |   |
| **5.25** | Debe posibilitar la diferenciacion de traficos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) proveyendo granularidad de control/politicas para los mismos; |   |
| **5.26** | Debe posibilitar la diferenciacion y control de partes de las aplicaciones como por ejemplo permitir Gtalk chat y bloquear la transferência de l; |   |
| **5.27** | Debe posibilitar a diferenciacion de aplicaciones Proxies (ghostsurf, freegate, etc.) proveyendo granularidad de control/politicas para los mismos; |   |
| **5.28** | Debe ser posible la creacion de grupos estáticos de aplicaciones y grupos dinamicos de aplicaciones baseados en características de las aplicaciones como: |   |
| **5.29** | Tecnologia utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc). |   |
| **5.30** | Nível de resgo de las aplicaciones. |   |
| **5.31** | Categoria y sub-categoria de aplicaciones. |   |
| **5.32** | Aplicaciones que usen técnicas evasivas, utilizadas por malwares, como transferência de archivos y/o uso excesivo de ancho de banda, etc. |   |

1. **PREVENCION DE AMENAZAS (Esta suscripcion se debe incluir por un año)**

|  |  |  |
| --- | --- | --- |
|  |   | **cumple no cumple** |
| **6.1** | Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS, Antivírus y Anti-Spyware integrados en el próprio appliance de Firewall  |   |
| **6.2** | Debe incluir firmas de prevencion de intrusos (IPS) y bloqueo de archivos maliciosos (Antivírus y Anti-Spyware);  |   |
| **6.3** | Las funcionalidades de IPS, Antivírus 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 garantia de software con el fabricante. |   |
| **6.4** | Debe sincronizar las firmas de IPS, Antivírus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo e Activo/pasivo; |   |
| **6.5** | Cuando se utilicen las funciones de IPS, Antivírus y Anti-spyware, el equipamento 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 simultaneamente. |   |
| **6.6** | Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo;  |   |
| **6.7** | Exenciones por IP de origen o de destino deben ser posibles en las Reglas, de forma general y firma a firma;  |   |
| **6.8** | Debe soportar granularidad en las politicas de IPS Antivírus y Anti-Spyware , permitiendo la creacion de diferentes politicas por zona de seguridad, direccion de origen, direccion de destino, servicio y la combinacion de todos esos items.  |   |
| **6.9** | Debe permitir el bloqueo de vulnerabilidades.Debe permitir el bloqueo de vulnerabilidades.Debe permitir el bloqueo de exploits conocidos.Debe incluir seguridad contra ataques de negacion deservicios.Deberá poseer los siguientes mecanismos de inspeccion de IPS:Analisis de parones de estado de conexiones;Analisis de decodificacion de protocolo; Analisis para deteccion de anomalias de protocolo;Analisis heurístico; IP Defragmentation;Reensamblado de paquetes de TCP;Bloqueo de paquetes malformados.Ser imune y capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc; Detectar y bloquear el origen de portscans; Bloquear ataques efectuados por worms conocidos, permitindo al administrador adicionar nuevos patrones; Soportar los siguientes mecanismos de inspeccion contra amenazas de red: analisis de patrones de estado de conexiones, analisis de decodificacion de protocolo, analisis para deteccion de anomalias de protocolo, analisis heuristico, IP Defragmentation, reensamblado de paquetes de TCP y bloqueo de paquetes malformados; Posea firmas específicas para la mitigacion de ataques DoS;Posea firmas para bloqueo de ataques de buffer overflow;Deberá posibilitar la creacion de firmas customizadas por la interfaz gráfica del producto.Permitir el bloqueo de vírus y spywares en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3;Soportar bloqueo de archivos por tipo;  |   |
| **6.10** | Los eventos deben identificar el país de donde partio la amenaza;  |   |
| **6.11** | Debe incluir seguridad contra vírus en contenido HTML y javascript, software espia (spyware) y worms. |   |
| **6.12** | Seguridad contra downloads involuntários usando HTTP de archivos ejecutables. maliciosos.  |   |
| **6.13** | Rastreamento de vírus en pdf. |   |
| **6.14** | Debe permitir la inspeccion en archivos comprimidos que utilizan o algoritmo deflate (zip, gzip, etc.) |   |
| **6.15** | Debe ser posible la configuracion de diferentes políticas de control de amenazas y ataques basados en politicas del firewall considerando Usuarios, Grupos de usuarios, origen, destino, zonas de seguridad, etc, o sea, cada politica de firewall podrá tener una configuracion diferente de IPS, siendo esas politicas por Usuarios, Grupos de usuário, origen, destino, zonas de seguridad. |   |

1. **ANALISIS DE MALWARES MODERNOS**

|  |  |  |
| --- | --- | --- |
|  |   | **cumple no cumple** |
| **7.1** | Poseer la capacidad de analisis de amenazas no conocidas; |   |
| **7.2** | Debido a los Malwares hoy en dia hay que ser muy dinamicos y un antivírus comun no es capaz de detectar los mismos a la misma velocidad que sus variaciones son creadas, la solucion ofertada deber poseer funcionalidades para analisis de Malwares no conocidos incluídas en la própria ferramenta  |   |
| **7.3** | El dispositivo de seguridad debe ser capaz de enviar archivos transferidos de forma automática para analisis "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 sufriran este analisis; |   |
| **7.5** | Soportar el analisis como por lo menos 60 (sesenta) tipos de comportamentos maliciosos para el analisis de la amenaza no conocida; |   |
| **7.6** | Soportar el analisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP y Windows 7; |   |
| **7.7** | Debe soportar el monitoreo de archivos transferidos por internet (HTTP, FTP, HTTP, SMTP) como tambien archivos transferidos internamente en los servidores de archivos usando SMB; |   |
| **7.8** | El sistema de analisis “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 infeccion, detectar aplicaciones no confiables utilizadas por el Malware, generar firmas de Antivírus y Anti-spyware automaticamente, definir URLs no confiables utilizadas por el nuevo Malware y proveer informaciones sobre el usuário infectado (su direccion ip y su login de red); |   |
| **7.9** | El sistema automático de analisis "In Cloud" o local debe emitir relacion para identificar cuales soluciones de antivírus existentes en el mercado poseen firmas para bloquear el malware; |   |
| **7.10** | Debe permitir exportar el resultado de los analisiss de malwares de dia Zero en PDF y CSV a partir de la própria interfaz de administracion; |   |
| **7.11** | Debe permitir la descarga de los malwares indentificados a partir de la própria interfaz de administracion; |   |
| **7.12** | Debe permitir visualizar los resultados de los analisis de malware de dia 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 analisis de malwares de dia Zero a partir de la própria interfaz de administracion. |   |
| **7.14** | Soportar el analisis de archivos ejecutables, DLLs, ZIP y criptografiados en SSL en el ambiente controlado;  |   |

1. **IDENTIFICACION DE USUARIOS**

|  |  |  |
| --- | --- | --- |
|  |   | **cumple no cumple** |
| **8.1** | Debe incluir a capacidad de creacion de políticas baseadas en la visibilidad y control de quien está utilizando cuales aplicaciones a través de la integracion como servicios de directorio, autenticacion via ldap, Active Directory, E-directory y base de datos local.  |   |
| **8.2** | Debe poseer integracion con Microsoft Active Directory para identificacion de usuarios y grupos permitiendo la granularidad de control/politicas baseadas en usuarios y grupos de usuarios. |   |
| **8.3** | Debe poseer integracion con Radius para identificacion de usuarios y grupos permitiendo la granularidad de control/politicas baseadas en usuarios y grupos de usuarios. |   |
| **8.4** | Debe posea integracion con Ldap para identificacion de usuarios y grupos permitiendo la granularidad de control/politicas baseadas en Usuarios y Grupos de usuarios. |   |
| **8.5** | Debe soportar la recepcion de eventos de autenticacion de controladoras wireless, dispositivos 802.1x y soluciones NAC via syslog, para la identificacion de direcciones IP y usuarios |   |
| **8.6** | Debe permitir el control, sin instalacion de cliente de software, en equipamentos que soliciten salida a internet para que antes de iniciar la navegacion, se muestre un portal de autenticacion residente en el firewall (Captive Portal). |   |
| **8.7** | Soporte a autenticacion Kerberos. |   |
| **8.8** | Debe poseer Soporte a identificacion de multiples usuarios conectados en una misma direccion IP en ambientes Citrix y Microsoft Terminal Server, permitindo visibilidad y control granular por usuário sobre el uso de las aplicaciones que tiene estos servicios |   |
| **8.9** | Debe poseer Soporte a identificacion de multiples usuarios conectados en una misma direccion IP en servidores accedidos remotamente, incluso que no sean servidores Windows. |   |

1. **QOS**

|  |  |  |
| --- | --- | --- |
|  |   | **cumple no cumple** |
| **9.1** | Como la finalidad de controlar aplicaciones y trafico cuyo consumo pueda ser excesivo, (como youtube, ustream, etc) y tener un alto consumo de ancho de banda, se requiere que la solucion, a la ves 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 áudio como de vídeo streaming.  |   |
| **9.2** | Soportar la creacion de políticas de QoS por: |   |
| **9.3** | Direccion de origen |   |
| **9.4** | Direccion de destino |   |
| **9.5** | Por usuário y grupo de LDAP/AD. |   |
| **9.6** | Por aplicaciones, incluyendo, mas no limitando a Skype, Bittorrent, YouTube y Azureus; |   |
| **9.7** | Por puerto; |   |
| **9.8** | El QoS debe permitir la definicion de clases por: |   |
| **9.9** | Ancho de Banda garantizado |   |
| **9.10** | Ancho de Banda Máximo |   |
| **9.11** | Cola de prioridad. |   |
| **9.12** | Soportar priorizacio RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype. |   |
| **9.13** | Soportar marcacion de paquetes Diffserv, inclusive por aplicaciones; |   |
| **9.14** | Disponer de estatísticas RealTime para clases de QoS. |   |
| **9.15** | Deberá permitir el monitoreo del uso que las aplicaciones hacen por bytes, sesiones y por usuário.  |   |

1. **FILTRO DE DATOS**

|  |  |  |
| --- | --- | --- |
|  |   | **cumple no cumple** |
| **10.1** | Permite la creacion de filtros para archivos y datos prédefinidos; |   |
| **10.2** | Los archivos deben ser identificados por extension y firmas; |   |
| **10.3** | Permite identificar y opcionalmente prevenir la transferência de vários tipos de archivos (MS Office, PDF, etc) identificados sobre aplicaciones (P2P, InstantMessaging, SMB, etc); |   |
| **10.4** | Soportar la identificacion de archivos compactados y las aplicaciones de politicas sobre el contenido de esos tipos de archivos; |   |
| **10.5** | Permitir identificar y opcionalmente prevenir la transferência de informaciones sensibles, incluyendo, mas no limitando al número de tarjetas de crédito, permitiendo la creacion de nuevos tipos de datos via expresion regular; |   |
| **10.6** | Permitir listar el número de aplicaciones soportadas para control de datos; |   |
| **10.7** | Permitir listar el número de tipos de archivos soportados para el control de datos; |   |
| **10.8** | Permitir la detección de portales de phishing estableciendo políticas que eviten el envío de credenciales válidas de usuarios a sitiosno autorizadas.  |   |
| **10.9** | Creación de políticas que soliciten un segundo factor de autenticación basadas en el origen (Usuario / Zona / Direcciones) y destino del tráfico (Aplicativos / Zonas / IPs) |   |
| **10.10** | Aplicación de etiqueta de manera automática a una IP origen (o destino) cuando un log es generado en el firewall, y que la etiqueta pueda formar parte de políticas existentes que puedan aplicar controles de manera dinámica |   |

1. **GEO-LOCALIZACION**

|  |  |  |
| --- | --- | --- |
|  |   | **cumple no cumple** |
| **11.1** | Soportar la creacion de politicas por Geo localizacion, permitiendo que el trafico de determinado Pais/Países sean bloqueados. |   |
| **11.2** | Debe posibilitar la visualizacion de los países de origen y destino en los logs de acceso. |   |
| **11.3** | Debe posibilitar la creacion de regiones geográficas desde la interfaz gráfica y crear politicas utilizando las mismas.  |   |

1. **VPN**

|  |  |  |
| --- | --- | --- |
|  |   | **cumple no cumple** |
| **12.1** | Soportar VPN Site-to-Site y Cliente-To-Site; |   |
| **12.2** | Soportar IPSec VPN; |   |
| **12.3** | Soportar SSL VPN; |   |
| **12.4** | La VPN IPSEc debe soportar: |   |
| **12.5** | 3DES; |   |
| **12.6** | Autenticacion MD5 e SHA-1;  |   |
| **12.7** | Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;  |   |
| **12.8** | Algoritmo Internet Key Exchange (IKEv1 & IKEv2); |   |
| **12.9** | AES 128, 192 e 256 (Advanced Encryption Standard) |   |
| **12.10** | Autenticacion via certificado IKE PKI. |   |
| **12.11** | Debe ser compatible con la Suite B de protocolos de NSA |   |
| **12.12** | Debe poseer interoperabilidade como los siguientes fabricantes:Cisco;Checkpoint;Juniper;Palo Alto Networks;Fortinet;Sonic Wall |   |
| **12.13** | Las VPN SSL deben soportar: |   |
| **12.14** | Permitir que el usuário realice la conexion por medio de cliente instalado en el sistema operacional del equipamento o por medio de interfaz WEB; |   |
| **12.15** | Las funcionalidades de VPN SSL deben ser atendidas con o sin el uso de agente; |   |
| **12.16** | La asignacion de direccion IP en los clientes remotos de VPN; |   |
| **12.17** | La asignacion de DNS en los clientes remotos de VPN; |   |
| **12.18** | Debe haber la opcion de ocultar el agente de VPN instalado en el cliente remoto, tornando el mismo invisible para el usuário; |   |
| **12.19** | Deber permitir criar políticas de control de aplicaciones, IPS, Antivírus, Antipyware para trafico de los clientes remotos conectados en la VPN SSL; |   |
| **12.20** | Las VPN SSL deben soportar proxy arp y el uso de interfaces PPPOE; |   |
| **12.21** | Soportar autenticacion via AD/LDAP, Secure id, certificado y base de usuarios local; |   |
| **12.22** | Permite establecer un túnel VPN client-to-site del cliente a la plataforma de seguridad, proveyendo una solucion de single-sign-on a los usuarios, integrandose como las herramientas de Windows-logon; |   |
| **12.23** | Soporte de lectura y verificacion de CRL (certificate revocation list); |   |
| **12.24** | Permite la aplicacion de políticas de seguridad y visibilidade para las aplicaciones que circulan dentro de los tuneles SSL; |   |
| **12.25** | El agente de VPN a ser instalado en los equipamentos desktop y laptops, debe ser capaz de ser distribuído de manera automática via Microsoft SMS, Active Directory y ser descargado directamente desde su propio portal, en el cual residirá el centralizador de VPN; |   |
| **12.26** | El agente deberá comunicarse con el portal para determinar las políticas de seguridad del usuário,  |   |
| **12.27** | Debe permitir que las conexiones como VPN SSL sean estrablecidas de las siguientes formas: |   |
| **12.28** | Antes del usuário autenticarse en la estacion; |   |
| **12.29** | Despues de la autenticacion del usuário en la estacion; |   |
| **12.30** | Bajo demanda del usuário; |   |
| **12.31** | Deberá mantener una conexion segura con el portal durante la sesion. |   |
| **12.32** | El agente de VPN SSL client-to-site debe ser compatible al menos con: Windows XP, Vista, Windows 7, Windows 8; |   |
| **12.33** | El portal de VPN debe enviar al cliente remoto la lista de gateways VPN activos para el establecimiento de la conexion, los cuales deben poder ser administrados centralizadamente |   |
| **12.34** | Debe haber una opcion en el cliente remoto de escojer manualmente el gateway de VPN y de forma automática a traves de la mejor respuesta entre los gateways disponibles con base al mas rápido. |   |
| **12.35** | Debe poseer la capacidade de identificar el origen de conexion de VPN si es interna o externa |   |

1. **CONSOLA DE ADMINISTRACION y MONITOREO**

|  |  |  |
| --- | --- | --- |
|  |   | **cumple no cumple** |
| **13.1** | Debe centralizar la administracion de Reglas y políticas del cluster, usando una única interfaz de administracion  |   |
| **13.2** | La administración de la solucion debe soportar acesso via SSH, cliente WEB (HTTPS) y API abierta; |   |
| **13.3** | En el caso de que sea necessária la instalacion de cliente para administracion de la solucion, el mismo debe ser compatible con sistemas operacionales Windows y Linux; |   |
| **13.4** | La administracion debe permitir/hacer:Creacion y administracion de políticas de firewall y control de aplicaciones;Creacion y administracion de políticas de IPS y Anti-Spyware;Creacion y administracion de politicas de filtro de URLMonitoreo de logs;Herramientas de investigacion de logs;Debugging;Captura de paquetes |   |
| **13.4** | Debe permitir el acceso concurrente de administradores; |   |
| **13.5** | Debe tener un mecanismo de busqueda de comandos de administracion via SSH, facilitando la localizacion de los comandos; |   |
| **13.6** | Debe permitir usar palabras clave y distintos tags de colores para facilitar la identificacion de Reglas;  |   |
| **13.7** | Debe permitir monitorear via SNMP fallas en el hardware, insercion o remocion de fuentes, discos y ventiladores, uso de recursos por número elevado de sesiones, número de tuneles establecidos de VPN cliente-to-site, porcentaje de utilizacion en referencia al número total soportado/licenciado y número de sesiones establecidas;  |   |
| **13.8** | Debe permitir el bloqueo de alteraciones, en el caso de acesso simultaneo de dos o mas administradores;  |   |
| **13.9** | Debe permitir la definicion de perfiles de acesso a la consola con permisos granulares como: acceso de escritura, acceso de lectura, creacion de usuarios, alteracion de configuraciones; |   |
| **13.10** | Debe permitir la autenticacion integrada con Microsoft Active Directory y servidor Radius; |   |
| **13.11** | Debe permitir la localizacion de donde estan siendo utilizados objetos en: Reglas ,direccion IP, Rango de IPs, subredes u objetos  |   |
| **13.12** | Debe poder atribuir sequencialmente un número a cada regla de firewall, NAT, QOS y Reglas de DOS; |   |
| **13.13** | Debe permitir la creacion de Reglas que esten activas en un horário definido; |   |
| **13.14** | Debe permitir la creacion de Reglas con fecha de expiracion; |   |
| **13.15** | Debe poder realizar un backup de las configuraciones y rollback de configuracion para la última configuracion salvada; |   |
| **13.16** | Debe soportar el Rollback de Sistema operativo para la ultima version local; |   |
| **13.17** | Debe poseer la habilidad del upgrade via SCP, TFTP e interfaz de administracion; |   |
| **13.18** | Debe poder validar las Reglas antes de las aplicaciones; |   |
| **13.19** | Debe permitir la validacion de las políticas, avisando cuando haya Reglas que ofusquen o tengan conflicto con otras (shadowing); |   |
| **13.20** | Debe posibilitar la visualizacion y comparacion de configuraciones actuales, la configuracion anterior y configuraciones mas antiguas. |   |
| **13.21** | Debe posibilitar la integracion con otras soluciones de SIEM del mercado (third-party SIEM vendors) |   |
| **13.22** | Debe permitira la generacion de logs de auditoria detallados, informando de la configuracion realizada, el administrador que la realizo y el horário de la alteracion;  |   |
| **13.23** | Deberá tener la capacidad de generar un grafico que permita visualizar los cambios en la utilizacion 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 relacion al pasado; |   |
| **13.24** | Debe permitir la generacion de mapas geográficos en tiempo real para la visualizacion de origenes y destinos del trafico generado en la institucion; |   |
| **13.25** | Debe proveer resumenes con la vista correlacionada de aplicaciones, amenazas (IPS, AntiSpware) URLs y filtro de archivos, para un mejor diagnóstico y respuesta a incidentes; |   |
| **13.26** | La administracion de la solucion debe posibilitar la recoleccion de estadísticas de todo el trafico que pasa por los dispositivos de seguridad; |   |
| **13.27** | Debe proveer resumenes de utilizacion de los recursos por aplicaciones, amenazas (IPS, Anti-Spware y antivirus de la solucion), etc; |   |
| **13.28** | Debe proveer de una visualizacion sumarizada de todas las aplicaciones, amenazas (IPS, Antivírus e Anti-Spware) y URLs que pasan por la solucion; |   |
| **13.29** | Debe poseer un mecanismo "Drill-Down" para navegacion por los resumenes en tempo real; |   |
| **13.30** | En las listas de "Drill-Down", debe ser posible identificar el usuário que ha determinado el acesso; |   |
| **13.31** | Debe ser posible exportar los logs en CSV; |   |
| **13.32** | Deberá ser posible acceder al equipamento a aplicar configuraciones durante momentos donde el trafico sea muy alto y la CPU y memória del equipamento este siendo totalmente utilizada. |   |
| **13.33** | Debe tener rotacion de logs;  |   |
| **13.34** | Debe tener presentaciones de las siguientes informaciones, de forma histórica y en tiempo real (actualizado de forma automática y contínua cada 1 minuto): Debe mostrar la situacion del dispositivo y del cluster;Debe poder mostrar las principales aplicaciones;Debe poder mostrar las principales aplicaciones por riesgo;Debe poder mostrar los administradores autenticados en la plataforma de seguridad;Debe poder mostrar el número de sesiones simultaneas;Debe poder mostrar el estado de las interfaces;Debe poder mostrar el uso de CPU; |   |
| **13.35** | Generacion de reportes. Como mínimo los siguientes reportes deben poder ser generados: Resumen gráfico de las aplicaciones utilizadas; Principales aplicaciones por utilizacion de ancho de banda de entrada y salida;Principales aplicaciones por tasa de transferencia en bytes;Principales hosts por número de amenazas identificadas; Actividades de un usuário específico y grupo de usuarios del AD/LDAP, incluyendo aplicaciones accedidas y amenazas (IPS, y Anti-Spware), de red vinculadas a este trafico; Debe permitir la creacion de reportes personalizados;  |   |
| **13.36** | En cada critério de busqueda del log debe ser posible incluir multiples entradas (ej. 10 redes e IP’s distintas; servicios HTTP, HTTPS y SMTP), excepto en el campo horário, donde debe ser posible definir un rango de tiempo como critério de busqueda;  |   |
| **13.37** | Generar alertas automáticas via:Email;SNMP;Syslog; |   |
| **13.38** | La plataforma de seguridad debe permitir a través de API-XML (Application Program Interface) la integracion con sistemas existentes en el ambiente de contratacion de forma que posibilite que aplicaciones desarrolladas por el cliente puedan interactuar en tempo real con la solucion permitiendo asi que Reglas y políticas de seguridad puedan ser modificadas por estas aplicaciones con la utilizacion de scripts en lenguajes de programacion como Perl o PHP. |   |

**ESPECIFICACIONES BÁSICAS**

**- BALANCEO DE SERVIDORES WEB SOLAMENTE PARA CORFERIAS -**

1. **DESCRIPCIÓN**

|  |  |  |
| --- | --- | --- |
|  |  | Cumple / no cumple |
| **1.1** | El equipo ofertado debe ser una plataforma de hardware de propósito específico denominado “appliance” marca F5. |  |
| **1.2** | El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de Balanceo de Carga de Servicios y Aplicaciones basadas en IP (TCP/UDP) y servicios web. |  |
| **1.3** | Los valores de desempeño solicitados deberán ser logrados por el equipo “appliance” como un sistema independiente y autónomo que cumpla el desempeño exigido y no como la suma o agregación de varios "appliance" que logren sumar el valor solicitado. |  |
| **1.4** | Se debe ofrecer dos (2) equipos en Alta disponibilidad funcionando en configuración de Par Activo. Por razones de eficiencia de uso de la energía, la climatización, uso de espacio en rack, administración y facilidad de configuración, no se aceptará soluciones basadas en cluster virtual de múltiples equipos.  |  |
| **1.5** | Cada equipo debe cumplir con las siguientes características: * La solución debe soportar un Throughput en L4 de al menos 10 Gbps
* La solución debe soportar un Throughput en L7 de al menos 10 Gbps
* La solución debe soportar al menos 14 Millones de conexiones simultáneas
* La solución debe soportar al menos 120.000 conexiones por segundo en L4
* La solución debe soportar al menos 600.000 HTTP Requests por Segundo
 |  |
| **1.6** | Cada equipo debe soportar al menos las siguientes Interfaces de red:* Al menos 4 puertos SFP, con opción de conectividad de 1 Gbps cobre o fibra
* Al menos 1 puertos SFP+ de 10 Gbps
 |  |
| **1.7** | Cada equipo debe contar con fuentes de poder redundantes AC, entradas de voltaje de 110 a 220 VAC que se puedan remover en caliente (hot-swap) y certificadas “80 Plus Platinum” para eficiencia energética.  |  |
| **1.8** | Los equipos deberán ser instalados en rack estándar de 19”, máximo 1RU. |  |
| **1.9** | Los equipos deben tener la característica de soportar alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual. La Solución debe tener la capacidad de recuperar las sesiones del sistema en forma inmediata y automática, en caso de fallo de un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico. |  |
| **1.10** | Cada equipo debe incluir 16 Gb de Memoria RAM mínimo  |  |
| **1.11** | Cada equipo debe incluir mínimo un Disco duro de 500 Gb |  |
| **1.12** | Debe soportar cluster Activo/Activo entre dos o más plataformas, soportando diferentes modelos de hardware (no solamente del mismo modelo). |  |
| **1.13** | La solución debe permitir configurar cluster entre más de dos equipos y permitir que sean plataformas no necesariamente idénticas (como equipos appliance físico, chasis o virtuales) con el fin de contar con un sistema a futuro altamente escalable y en demanda |  |
| **1.14** | Para mejorar el rendimiento de la sincronización de configuración deberá poder sincronizar la configuración de manera incremental. |  |
| **1.15** | Ante la necesidad de conmutar el tráfico a otros dispositivos del grupo, el sistema deberá poder realizar cálculos para determinar el mejor dispositivo basado en: recursos, capacidad, carga de tráfico en cada dispositivo. Identificando la mejor opción cuando el ambiente sea heterogéneo en cuanto se refiere a plataformas. |  |
| **1.16** | La configuración será sincronizada entre todos los dispositivos del grupo pudiendo escoger si la sincronización se realiza de manera automática o manual.  |  |
| **1.17** | Los equipos deben tener hardware acelerador FPGA personalizables y programables para varias funciones como protección DDoS, protocolos SDN y manejo de trafico UDP |  |

1. **CAPACIDADES Y CANTIDADES**

|  |  |  |
| --- | --- | --- |
|  |  | **cumple no cumple** |
| **2.1** | La solución debe realizar funciones de balanceo de tráfico a aplicaciones basadas en TCP/UDP, incluidos servicios web. |  |
| **2.2** | La solución debe permitir la definición de dirección IP y puerto virtual para la prestación de un servicio, que permita atenderlo mediante una granja de servidores identificados mediante una dirección IP y un puerto del servicio igual o diferente del presentado al público. |  |
| **2.3** | La solución debe tener arquitectura Full-Proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado del servidor o los recursos.  |  |
| **2.4** | La solución ofertada debe ser capaz de soportar balanceo amortiguado de los servidores que se agreguen nuevos, para prevenir la saturación de conexiones. De manera que servidores que se agregan al grupo de balanceo, reciban al inicio menos cantidad de peticiones por un tiempo determinado, hasta ser capaz de recibir la misma cantidad de peticiones que los que ya estaban en el grupo. |  |
| **2.5** | Deberá permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones |  |
| **2.6** | La solución debe permitir hacer control de balanceo de tráfico según se defina entre uno o varios tipos de algoritmos especializados de balanceo. Estos métodos deben realizarse de manera nativa y no por medio de configuración por scripting:* Round Robin
* Proporcional (Ratio)
* Proporcional dinámico
* Respuesta más rápida
* Conexiones mínimas
* Menor número de sesiones
* Tendencia de menor cantidad de conexiones
* Tendencia de desempeño
 |  |
| **2.7** | Debe permitir balancear a una granja de servidores y seleccionar el destino basado en la carga de estos, como memoria/RAM |  |
| **2.8** | El equipo debe no tener restricciones en el número de servicios virtuales que se pueden configurar (Virtual Servers, Virtual IP, granjas) |  |
| **2.9** | El sistema debe ser capaz de identificar fallos en servicios para redundancia de las aplicaciones. |  |
| **2.10** | La solución debe tener reglas que permitan el control de ancho de banda de manera dinâmica |  |
| **2.11** | La solución debe realizar monitoreo de la salud de los Servidores que gestione el equipo de Balanceo de tráfico, por medio de:* Ping.
* Chequeo a nivel de TCP y UDP a puertos específicos
* Monitoreo http y https
* Monitoreo del hardware y software mediante Windows Management Instrumentation (WMI) o mediante un sistema similar reconocido y aprobado por Microsoft.
* Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos.
* Ejecución de scripts para determinar la respuesta emulando un cliente.
* Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red.
* Monitoreos en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma
* Monitoreo de aplicaciones de mercado:
	+ LDAP
	+ FTP
	+ SMTP
	+ IMAP/POP3
	+ Oracle
	+ MSSQL
	+ MySQL
	+ RADIUS
	+ SIP
	+ Protocolo SASP
	+ SOAP
	+ WMI
	+ SNMP
 |  |
| **2.12** | Debe poder realizar todos estos métodos de persistencia de las conexiones:* Dirección IP origen
* Dirección IP destino
* Cookies
* Hash
* SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia
* Sesiones SSL
* Microsoft Remote Desktop
 |  |
| **2.13** | Debe Permitir crear persistencia por cualquier valor del paquete por medio de reglas. |  |
| **2.14** | Debe garantizar afinidad del servidor, de tal forma que una solicitud de un cliente y cada solicitud posterior se dirijan al mismo servidor de la granja. |  |
| **2.15** | El sistema debe ser capar de realizar un método secundario de persistencia, en caso de que el primer método no pueda ejecutarse por factores externos a la plataforma. |  |
| **2.16** | Soporte de API para construir aplicaciones de administración o monitoreo personalizadas:* Soporte de SOAP/XML, que sea base del Sistema Operativo. Que permita la integración con aplicaciones como VMWare vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), Soporte de Java, .NET, PERL, PHP, PowerShell y Python. Las interfaces de control deben ser accesibles por conexiones SSL con requerimientos de autenticación vía http básica, para evitar accesos no autorizados.
 |  |
| **2.17** | Soporte de RESTful API |  |
| **2.18** | Deberá ser posible modificar el contenido HTML utilizando objetos de configuración y sin necesidad de generar scripts. |  |
| **2.19** | Debe soportar el protocolo TDS para balanceo de MSSQL |  |
| **2.20** | Debe soportar el protocolo MQTT para administración de tráfico desde dispositivos IoT. Debe permitir identificar mensajes dentro del protocolo MQTT, proveer estadísticas y exponer API para acceder a la información de los mensajes MQTT |  |
| **2.21** | El sistema deberá soportar scripts de programación basados en un lenguaje estructurado (TCL) que permita crear funcionalidades que por defecto no se encuentren en el menú de configuración u opciones y debe soportar la creación de Procedimientos o funciones que pueden ser utilizadas desde cualquier otro script. |  |
| **2.22** | La solución debe permitir configuración de scripts basados en Node.js con el fin de brindar además del TCL, el acceso a paquetes de npm para facilitar la escritura y el mantenimiento del código.  |  |
| **2.23** | El equipo debe ser compatible con tráfico IPSEC y ser certificado por ICSA Labs como dispositivo IPSEC 1.3 |  |
| **2.24** | Debe soportar e incluir Geolocalización, de manera que pueda tomar decisiones basado en una base de datos de continentes, países y de direcciones IP.La Base de datos de geolocalización debe incluir los países de América Latina y estar disponible en el mismo equipo sin necesidad de acceso a Internet (offline). |  |

1. **CARACTERISTICAS GENERALES DE SEGURIDAD**

|  |  |  |
| --- | --- | --- |
|  |  | **cumple no cumple** |
| **3.1** | Cada equipo debe soportar seguridad SSL con las siguientes características:* Incluir el soporte de Aceleración SSL usando Hardware Dedicado
* Incluir mínimo 2500 Transacciones por segundo SSL (RSA 2K Keys)
* Incluir mínimo 2100 Transacciones por segundo SSL (ECDSA P-256)
* Soportar al menos 5 Gbps SSL Bulk Encryption (Thoughput SSL)
* Soporte de llaves SSL RSA de 1024, 2048 y 4096 bits
 |  |
| **3.2** | La solución debe soportar mirroring de sesiones SSL. Sin el equipo primario falla el equipo secundario debe mantener la sesión SSL |  |
| **3.3** | El Stack TLS del equipo debe soportar las siguientes funcionalidades/características* Session ID
* Session Ticket
* OCSP Stapling (on line certificate status protocol)
* Dynamic Record Sizing
* ALPN (Application Layer Protocol Negotiation)
* Forward Secrecy
 |  |
| **3.4** | La solución debe manejar AES, AES-GCM, SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman, Digital Signature Algorithm (DSA) y Elliptic Curve Cryptography (ECC) |  |
| **3.5** | Debe soportar algoritmos de cifrado Camellia |  |
| **3.6** | El equipo o sistema operativo debe estar certificado por ICSA Labs como Firewall de Red (Corporate Firewall) |  |
| **3.7** | El equipo o sistema operativo debe estar certificado por ICSA Labs como Web Application Firewall |  |
| **3.8** | Firmado criptográfico de cookies para verificar su integridad. |  |
| **3.9** | Capacidad de integración con dispositivos HSM externos. Deberá soportar al menos Thales nShield Y Safenet (Gemalto) Luna. |  |
| **3.10** | La solución debe permitir la funcionalidad Proxy SSL, esta funcionalidad permite que sesión SSL se establezca directamente entre el usuario y el servidor final, sin embargo el equipo balanceador debe ser capaz de desencriptar, optimizar y reencriptar el trafico SSL sin que el balanceador termine la sesión SSL. |  |
| **3.11** | Se requiere que soporte la extensión STARTTLS para el protocolo SMTP de manera de poder cambiar una conexión en texto plano a una conexión encriptada sin necesidad de cambiar el puerto. |  |
| **3.12** | Debe soportar HSTS (HTTP Strict Transport Security) |  |
| **3.13** | Debe soportar por medio de agregación de subscripción a futuro, un sistema de reputación IP para prevenir conexiones bidireccionales (entrantes y salientes) a direcciones IP no confiables y agrupadas en categorías.* Scanners
* Exploits Windows
* Denial of Service
* Proxies de Phishing
* Botnets
* Proxies anónimos
 |  |

1. **ESTANDARES DE RED**

|  |  |  |
| --- | --- | --- |
|  |  | **cumple no cumple** |
| **4.1** | Soporte VLAN 802.1q, Vlan tagging |  |
| **4.2** | Soporte de 802.3ad para definición de múltiples troncales |  |
| **4.3** | Soporte de NAT, SNAT |  |
| **4.4** | Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente. |  |
| **4.5** | Soporte de Rate Shapping. |  |
| **4.6** | Soporte de dominios de Enrutamiento, donde cada uno pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento.  |  |
| **4.7** | Debe soportar VXLAN, VXLAN Gateway, NVGRE y Transparent Ethernet Bridging para entornos de redes virtualizadas. |  |
| **4.8** | Debe soportar protocolos de enrutamiento BGP, RIP, OSPF, IS-IS |  |

1. **ADMINISTRACION DEL SISTEMA**

|  |  |  |
| --- | --- | --- |
|  |  | **cumple no cumple** |
| **5.1** | La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, interfaz de administración gráfica basada en Web seguro (HTTPS) |  |
| **5.2** | La solución debe integrarse con Directorio Activo Windows 2003 o superior, para la autenticación de usuarios para gestión de la herramienta. |  |
| **5.3** | La solución debe integrarse con LDAP, para la autenticación de usuarios para gestión de la herramienta. |  |
| **5.4** | La solución debe integrarse con RADIUS y TACACS+ para la autenticación de usuarios para gestión de la herramienta. |  |
| **5.5** | La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales |  |
| **5.6** | La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante:* Protocolo SysLog
* Notificación vía SMTP
* SNMP versión.2.0 o superior.
 |  |
| **5.7** | El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico. |  |
| **5.8** | El equipo debe contar con un módulo de administración tipo lights out que permita encender/apagar el sistema de manera remota y visualizar el proceso de arranque. |  |
| **5.9** | La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real |  |
| **5.10** | Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, URLs más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos. |  |
| **5.11** | Debe Contar con plantillas para la implementación rápida de aplicaciones de mercado conocidas (ej, Oracle, Microsoft, SAP, IBM) y permitir crear plantillas personalizadas que puedan ser actualizadas/exportadas entre equipos. |  |

1. **SERVICIOS**

|  |  |  |
| --- | --- | --- |
|  |   | **cumple no cumple** |
| **14.1** | Se debe incluir servicio de montaje implementacion configuracion y puesta en marcha de la solución completa. En el caso de Paloalto incluir el servicio de migración de la plataforma actual a nível ferias y a nível administrativo |   |
| **14.2** | Se debe oferecer garantía (premium support del fabricante) por 1 año a nível de suscripciones garantias y software. |   |
| **14.3** | Se debe oferecer soporte del partner en sitio 24x7 para atender cualquier falla en la plataforma, por un año. |   |