Universidad Nacional de La Matanza

ANEXO CONVOCATORIA

32/2019

RENGLONES

Renglón	Especificación Técnica	Imagen
	La solución de seguridad deberá brindarse en Hardware dedicado, para ello se deberán proveer 2 Firewalls en Alta Disponibilidad (HA) los cuales deberán cumplir con las siguientes especificaciones: 1- Desempeño / Conectividad • Cantidad de equipos 2 (en HA) • Número de Interfaces Gigabit Ethernet RJ45 8 • Número de Interfaces / slots SFP 8 • Número de Interfaces 10 Gigabit Ethernet SFP+ 2 • Número de Interfaces Management 1 • Número de Interfaces HA 1 • Puerto de Consola 1 • Throughput de Firewall (con paquetes de 1518/512/64 byte) 36/36/27 Gbps • Latencia de firewall (con paquetes de 64 byte, UDP) 2 s • Paquetes por Segundo procesados por el Firewall 40,5 Mpps • Throughput de VPN IPSec (con paquetes de 512 byte) 20 Gbps • Throughput de NGFW 9,5 Gbps • Throughput de IPS (HTTP/Enterprise Mix) 10 Gbps • Throughput de Inspección SSL (Promedio HTTPS) 8 Gbps • Políticas de Firewall admitidas 10.000 • Túneles gateway to gateway 2.000 • Túneles client to gateway 50.000 • Throughput VPN SSL 7 Gbps • Sesiones Concurrentes 8 millones • Nuevas sesiones / segundo 450.000 • Capacidad para gestionar Switchs 64 • Capacidad para gestionar Access Point 512 • Incluir SFP+ en Cobre (10Gbps) 8 • Incluir cables cat 6a (4 de 1,5 mts + 4 de 12 mts) 8 2- Funcionalidades y Características del Sistema Características del dispositivo • El dispositivo debe ser un equipo de propósito específico. • Basado en tecnología ASIC y que sea capaz de brindar una solución de “Complete Content Protection”. Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux • Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC) • Capacidad de reensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC) • El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red • En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP • El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local consultas de acuerdo a la configuración del administrador • El equipo de seguridad debe soportar el uso del protocolo ICAP con el fin de poder delegar tareas a equipos terceros con el fin de liberar procesamiento de este • Debe contar con fuentes redundantes internas o externas para asegurar el funcionamiento ante posibles cortes de energía • La solución proporcionada debe contar con un formato rackeable Firewall	

Universidad Nacional de La Matanza

Renglón	Especificación Técnica	Imagen
	• Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs • El Firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino • Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino • Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando • Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico origen, puerto físico destino, direcciones IP origen, dirección IP destino • Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo • Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos • Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP) • Capacidad de hacer traslación de direcciones estático, uno a uno, NAT y PAT • Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Interfaz de línea de comando) como por GUI (Interfaz Gráfica de Usuario) • La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas • En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID • En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible • El equipo deberá permitir la creación de políticas de tipo Firewall con capacidad de seleccionar campos como dirección, identificador de usuarios o identificador de dispositivos para el caso de dispositivos móviles como smartphone y tabletas • El equipo deberá permitir la creación de políticas de tipo VPN con capacidad de seleccionar campos como IPSEC o SSL según sea el tipo de VPN • La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP • La solución de seguridad deberá permitir la creación de servicios de Firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada • La solución será capaz de integrar los servicios dentro de las categorías de Firewall predefinidas o personalizadas y ordenarlos alfabéticamente • El dispositivo de seguridad podrá determinar accesos y denegación a diferentes tipos de tráfico predefinidos dentro de una lista local de políticas • La solución será capaz de habilitar o deshabilitar el paso de tráfico a través de procesadores de propósito específico, si el dispositivo cuenta con estos procesadores integrados dentro del mismo • La solución podrá crear e implementar políticas de tipo Multicast y determinar el sentido de la política, así como también la habilitación del NAT dentro de cada interfaz del dispositivo • El dispositivo de seguridad será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces • El dispositivo debera generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS • La solución de seguridad permitirá configurar el mapeo de protocolos a puertos de manera global o especifica • La solución capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos. • El dispositivo integrara la inspección de tráfico tipo SSL y SSH bajo perfiles predefinidos o personalizados • El dispositivo será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico • Tendrá la capacidad de hacer escaneo a profundidad de trafico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis • La solución permitirá bloquear o monitorear toda la actividad de tipo Exec, Port-Forward, SSH-Shell, y X-11 SSH Conectividad y Sistema de ruteo • Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP • Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs	

Universidad Nacional de La Matanza

Renglón	Especificación Técnica	Imagen
	• Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas • Soporte a políticas de ruteo (policyrouting) • El soporte a políticas de ruteo deberá permitir que, ante la presencia de dos enlaces a Internet, se pueda decidir cuál tráfico sale por un enlace y qué tráfico sale por otro enlace • Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS • Soporte a ruteo dinámico RIPng, OSPFv3 • La configuración de BGP debe soportar AutonomousSystemPath (AS-PATH) de 4 bytes • Soporte de ECMP (EqualCostMulti-Path) • Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas, pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador • Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa • Soporte a ruteo de multicast • La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow • La solución podrá habilitar políticas de ruteo en IPv6 • La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6 • La solución deberá soportar la creación de políticas de tipo Firewall y VPN y subtipo por dirección IP, tipos de dispositivo y por usuario, con IPv6 • La solución será capaz de habilitar funcionalidades de UTM (Antivirus, Filtrado Web, Control de Aplicaciones, IPS,Filtrado de correo, DLP, ICAP y VoIP) dentro de las políticas creadas con direccionamiento IPv6 • El dispositivo debe integrar la autenticación por usuario o dispositivo en IPv6 • El dispositivo deberá soportar la inspección de tráfico IPv6 en modo proxy explicito • Deberá ser capaz de integrar políticas con proxy explícito en IPv6 • La solución podrá restringir direcciones IPv6 en modo proxy explicito • Deberá hacer NAT de la red en IPv6 • La solución será capaz de comunicar direccionamiento IPv6 a servicios con IPv4 a través de NAT • Como dispositivo de seguridad deberá soportar la inspección de tráfico IPv6 basada en flujo • La solución deberá ser capaz de habilitar políticas de seguridad con funcionalidades IPS, Filtrado Web, Control de Aplicaciones, Antivirus y DLP, para la inspección de tráfico en IPv6 basado en flujos • La solución contara con una base de administración de información interna generada por sesiones sobre IPv6 • Deberá ser capaz de habilitar la funcionalidad de TrafficShaper por IP para el tráfico en IPv6 • El dispositivo podrá tener la capacidad de transmitir DHCP en IPv6 • La solución tendrá la funcionalidad de habilitar DHCP en IPv6 por interface • La solución deberá contar con soporte para sincronizar por sesiones TCP en IPv6 entre dispositivos para intercambio de configuración en Alta Disponibilidad • El dispositivo podrá ser configurado mediante DHCP en IPv6 para comunicarse con un servidor TFTP donde se encontrará el archivo de configuración • El dispositivo podrá hacer la función como servidor DHCP IPv6 • La solución será capaz de configurar la autenticación por usuario por interface en IPv6 VPN IPSec/L2TP/PPTP • Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site) • Soporte para IKEv2 y IKE ConfigurationMethod • ¬Debe soportar la configuración de túneles PPTP • Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES. • Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits • Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14. • Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256. • Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNsIPSeCsite-to-site y VPNsIPSecclient-to-site • La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN) • En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall • Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de	

Universidad Nacional de La Matanza

Renglón	Especificación Técnica	Imagen
	túneles nativos de Windows y MacOS X VPN SSL • Capacidad de realizar SSL VPNs. • Soporte a certificados PKI X.509 para construcción de VPNs SSL. • Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN. • Soporte de renovación de contraseñas para LDAP y RADIUS. • Soporte a asignación de aplicaciones permitidas por grupo de usuarios • Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet. • Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL. • Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning) • La VPN SSL integrada deberá soportar a través de algunplug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS • Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL • Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente • Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios • VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información • Para la configuración de cluster, en caso de caída de uno de los dispositivos, la VPN SSL que estuviera establecida, debe restablecerse en el otro dispositivo sin solicitar autentificación nuevamente Traffic Shaping / QoS • Capacidad de poder asignar parámetros de trafficshaping • Capacidad de poder asignar parámetros de trafficshaping diferenciadas para el tráfico en distintos sentidos de una misma sesión • Capacidad de definir parámetros de trafficshaping que apliquen para cada dirección IP en forma independiente • Capacidad de poder definir ancho de banda garantizado • Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) • Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia Autenticación y Certificación Digital • Capacidad de integrarse con Servidores de Autenticación RADIUS • Capacidad nativa de integrarse con directorios LDAP • Capacidad incluida, al integrarse con Microsoft Windows Active Directory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On” • Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Deberá poseer solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet • Debe ser posible definir puertos alternativos de autenticación para los protocolos HTTP, FTP y Telnet • Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site) • La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios • Deben poder definirse usuarios y grupos en un repositorio local del dispositivo • Debe poder limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP Antivirus • Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP • El Antivirus deberá poder configurarse en modo Proxy como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruídos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente • Antivirus en tiempo real, integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto	

Universidad Nacional de La Matanza

Renglón	Especificación Técnica	Imagen
	externo o software adicional para realizar la categorización del contenido • El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6 • La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso • El appliance deberá de manera opcional poder inspeccionar todos los virus conocidos • El Antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos HTTP, FTP, IMAP, POP3, SMTP • El Antivirus integrado tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus • El Antivirus deberá incluir capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red • El antivirus deberá ser capaz de filtrar archivos por extensión • El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo • Capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo “Push” (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo “pull” (Consultar los centros de actualización por versiones nuevas) AntiSpam • La capacidad AntiSpam deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje • La capacidad AntiSpamincluída deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address) • La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como mecanismos para detección de SPAM • En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje Filtrado de URLs (URL Filtering) • Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos • Debe poder categorizar contenido Web requerido mediante IPv6 • Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido • Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso • Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo del origen de la conexión o grupo de usuario al que pertenezca. • La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión (modo proxy) como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación (modo flujo) • Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables. Estos mensajes personalizados deberán poder aplicarse para conexiones http y https, tanto en modo proxy como en modo flujo • Capacidad de filtrado de scripts en páginas web (JAVA/Active X) • Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos • Será posible exceptuar la inspección de HTTPS por categoría. • El sistema de filtrado de URLs debe tener al menos 3 métodos de inspección: • Modo de Flujo: La página es inspeccionada paquete a paquete sin reconstruir la página completa • Modo Proxy: La página es reconstruida completamente para ser analizada a	

Universidad Nacional de La Matanza

Renglón	Especificación Técnica	Imagen
	profundidad • Modo DNS: La inspección se basa únicamente en la categorización del dominio accesado • Se debe incluir la funcionalidad de reputación basada en filtrado de URLs • La funcionalidad de reputación busca que, al acceder a páginas de contenido no deseado (tales como Malware, pornografía, consumo de ancho de banda excesivo, etc) se asigne un puntaje a cada usuario o IP cada vez que visita una página de esta índole. De acuerdo a esto se extrae los usuarios que infringen las políticas de filtrado con más frecuencia con el fin de detectar zombies dentro de la red • El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido Protección contra intrusos (IPS) • El IPS debe poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en spam o mirror • Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6 a través de sensores • Capacidad de detección de más de 4000 ataques • Capacidad de actualización automática de firmas IPS mediante tecnología de tipo “Push” (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo “pull” (Consultar los centros de actualización por versiones nuevas) • El IPS deberá estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. • Deberá soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signaturebased / misusedetection). • Basado en análisis de firmas en el flujo de datos en la red, deberá permitir configurar firmas nuevas para cualquier protocolo. • Actualización automática de firmas para el detector de intrusos • El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios • Métodos de notificación: • Alarmas mostradas en la consola de administración del appliance • Alertas vía correo electrónico • Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado • La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma “indefinida”, hasta que un administrador tome una acción al respecto • Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP • Se debe incluir protección contra amenazas avanzadas y persistentes (AdvancedPersistentThreats). Dentro de estos controles se debe incluir: • Protección contra botnets: Se deben bloquear intentos de conexión a servidores de Botnets, para ello se debe contar con una lista de los servidores de Botnet más utilizado. Dicha lista debe actualizarse de forma periódica por el fabricante. • Sandboxing: La funcionalidad de Sandbox hace que el archivo sea ejecutado en un ambiente seguro para analizar su comportamiento y, a base del mismo, tomar una acción sobre el mismo. Prevención de Fuga de Información (DLP) • La solución debe ofrecer la posibilidad de definir reglas que permitan analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial • La funcionalidad debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos • Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP • Ante la detección de una posible fuga de información deben poder aplicarse el menos las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la	

Universidad Nacional de La Matanza

Renglón	Especificación Técnica	Imagen
	dirección IP de origen, registrar el evento, • En caso del bloqueo de usuarios, la solución debe permitir definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción • La solución debe soportar la capacidad de guardar una copia del archivo identificado como posible fuga de información. Esta copia podría ser archivada localmente o en otro dispositivo • La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares • Se debe proveer la funcionalidad de filtrado de fuga de información. Dentro de las técnicas de detección se debe considerar como mínimo las siguientes: • Filtrado por tipo de archivo • Filtrado por nombre de archivo • Filtrado por expresiones regulares: Se detectarán los archivos según las expresiones regulares que se encuentren dentro de los mismos • Fingerprinting: Se tomará una muestra del archivo que se considere como confidencial. Según esto se bloquearán archivos que sean iguales a esta muestra • Watermarking: Se insertará un "sello de agua" dentro del archivo considerado como confidencial. De acuerdo a esto se analizarán los archivos en busca de este sello de agua, este se detectará incluso si el archivo sufrió cambios Control de Aplicaciones • Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo • La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico • La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante • El listado de aplicaciones debe actualizarse periódicamente • Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log • Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log • Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de trafficshaping • Preferentemente deben soportar mayor granularidad en las acciones Inspección de Contenido SSL • La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S • La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In TheMiddle) • La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario • Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado • El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS • Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log Controlador Inalámbrico (Wireless Controller) • El dispositivo debe tener la capacidad de funcionar como Controlador de Wireless • En modo de Controlador de Wireless tendrá la capacidad de configurar múltiples puntos de acceso (Access Points: APs) reales de forma tal de que se comporten como uno solo. Cómo mínimo deberá controlar los SSID, roaming entre APs, configuraciones de cifrado, configuraciones de autenticación • Debe soportar la funcionalidad de detección y mitigación de puntos de acceso (APs). Rogue Access Point Detection • El controlador de Wireless tendrá la capacidad de configurar la asignación de direcciones IP mediante DHCP a las estaciones de trabajo conectadas a los APs • Deberá tener la capacidad de monitorear las estaciones de trabajo, clientes wireless, conectadas a alguno de los APs • La solución debe contar con la funcionalidad de WIDS (Wireless IDS), la capacidad de monitorear el trafico wireless para detectar y reportar posibles intentos de intrusión • Debe contar con un sistema de aprovisionamiento de usuarios invitados para red wifi, que permita la creación sencilla de accesos para invitados, por medio de un portal independiente	

Universidad Nacional de La Matanza

Renglón	Especificación Técnica	Imagen
	• El equipo debe tener capacidad de que estos usuarios invitados con acceso inalámbrico, tengan la opción de colocar o no contraseña, con tiempo limitado y configurable para la expiración de la cuenta • El controlador inalámbrico deberá tener la capacidad de balancear la carga entre los puntos de acceso (Access Points) soportando por lo menos los siguientes métodos de balanceo: Access Point Hand-off, Frequency Hand-off • Debe contar con la capacidad de realizar Bridge SSID, permitiendo que una red inalámbrica y un segmento cableado LAN pertenezcan a la misma rubred • El dispositivo deberá ser capaz de administrar los dispositivos wireless AP de la misma plataforma, tanto en consola CLI como a través de una interfaz gráfica (GUI) • El dispositivo debe tener la capacidad de controlar varios puntos de acceso de la misma plataforma de forma remota. • El dispositivo debe poder cifrar la información que se envía hacia los puntos de acceso de la misma plataforma, sobre los cuales se esté teniendo control y gestión. • El dispositivo debe permitir la administración y manejo tanto de redes cableadas como inalámbricos dentro del mismo segmento de red. • El equipo debe tener la capacidad de reconocer y monitorear diferentes tipos de dispositivos de comunicación móvil como Smartphones Androide, Blackberry y Iphone y diferentes tipos de tabletas con SO Android o tabletas IPad • El equipo debe tener la capacidad de controlar el acceso a la red de los diferentes dispositivos antes mencionados a través de ACLs por MAC • El equipo deberá permitir el crear diferentes niveles de acceso a la red en función del tipo de dispositivo que se conecte, siendo estos: Smartphones, Tabletas, Laptops, PCs (tanto en Windows como en Linux) • El equipo debe permitir la separación de redes al menos entre usuarios internos e invitados, permitiendo la colocación de reglas en función de los dispositivos móviles conectados. Controlador Switchs (SwitchController) El dispositivo debe tener la capacidad de funcionar como Controlador de Switchs El equipo deberá tener la capacidad de aplicar segmentación por Vlan El equipo deberá tener la capacidad de aplicar Vlan a puertos específicos de los Switchs controlados por el Deberá tener la capacidad de monitorear las estaciones de trabajo, conectadas a los Switchs El equipo debe tener la capacidad de controlar el acceso a la red de los diferentes dispositivos antes mencionados a través de ACLs por MAC Filtrado de tráfico VoIP, Peer-to-Peer y Mensajería instantánea • Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time StreamingProtocol (RTSP). • El dispositivo deberá poseer técnicas de detección de P2P y programas de archivos compartidos (peer-to-peer) • En el caso de los programas para compartir archivos (peer-to-peer) deberá poder limitar el ancho de banda utilizado por ellos, de manera individual. • La solución debe contar con un ALG (ApplicationLayer Gateway) de SIP • Debe poder hacerse inspección de encabezados de SIP • Deben poder limitarse la cantidad de requerimientos SIP que se hacen por segundo. Esto debe poder definirse por cada método SIP. • La solución debe soportar SIP HNT (Hosted NAT Transversal). • La solución deberá integrar la inspección de tráfico basado en flujo utilizando un motor de IPS dentro del mismo dispositivo para escaneo de paquetes • Deberá ser capaz de hacer inspección tráfico SSH en modo proxy explicito • La solución de seguridad podrá hacer inspección de tráfico HTTP, HTTPS y FTP sobre HTTP en modalidad proxy explicito con las funcionalidades de IPS, Antivirus, Filtrado Web, Control de Aplicaciones y DLP, todo en un mismo dispositivo • El dispositivo tendrá la opción para configurar sus interfaces integradas en modo Sniffer con funcionalidades de Filtrado Web, Control de Aplicaciones, Antivirus e IPS Optimización WAN y Web Caching • La solución deberá permitir la creación de perfiles para la aplicación de Optimización WAN e indicar bajo que protocolos se ejecutará • Deberá ser capaz de activar en modo transparente dentro de los perfiles de Optimización WAN y seleccionar un determinado grupo de usuarios para autenticación de acceso • El dispositivo deberá soportar la desfragmentación dinámica de paquetes para detectar fragmentos persistentes de distintos archivos o datos adjuntos dentro del trafico bajo protocolos desconocidos • La solución debe ser capaz de generar y aplicar perfiles de Optimización WAN para los usuarios • El dispositivo de seguridad podrá integrar contenido de inspección dentro de sus políticas de seguridad con Optimización WAN	

Universidad Nacional de La Matanza

Renglón	Especificación Técnica	Imagen
	• La solución integrará dentro de cada interface la capacidad de hacer túneles de Optimización WAN • Deberá ser capaz de configurar Optimización WAN en modo Activo/Pasivo • Solución capaz de aplicar web cache a tráfico HTTP y HTTPS dentro de las políticas de seguridad incluyendo también Optimización WAN y web proxy cache • Dispositivo capaz de habilitar el almacenamiento en caché web tanto en el lado del cliente y del lado de la solución • La solución podrá recibir el tráfico HTTPS en nombre del cliente, abrirá y extraerá el contenido del tráfico cifrado para inspeccionar y almacenar en cache para el envío al usuario final • El dispositivo tendrá la opción de integrar un certificado SSL determinado para la recifrado de tráfico • La solución deberá ser capaz de configurar el cache de trafico HTTP y HTTPS bajo distintos puertos a los predeterminados (80 y 443) • La solución debe ser capaz de habilitar opciones para depurar la funcionalidad de Web Cache a determinadas URL Alta Disponibilidad • El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6 • Alta Disponibilidad en modo Activo-Pasivo • Alta Disponibilidad en modo Activo-Activo • Posibilidad de definir al menos dos interfaces para sincronía • El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red • Será posible definir interfaces de gestión independientes para cada miembro en un clúster Características de Administración • Interfase gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfase debe soportar SSL sobre HTTP (HTTPS) • Interfase basada en línea de comando (CLI) para administración de la solución. • Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto. • Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interfase gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet) • El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales. • Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar. • El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet,http o HTTPS. • El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional. • Soporte de SNMP versión 2 y versión 3 • Soporte para almacenamiento de eventos en un repositorio que pueda consultarse luego con SQL. • Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall. • Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red. • Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión. • Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica. • Contar con facilidades de administración a través de la interfaz gráfica como ayudantes de configuración (setupwizard). • Contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard) Virtualización • El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual	

Universidad Nacional de La Matanza

Renglón	Especificación Técnica	Imagen
	Systems", "Virtual Firewalls" o "Virtual Domains" • La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus • Se debe incluir la licencia para al menos 10 (diez) instancias virtuales dentro de la solución a proveer. • Cada instancia virtual debe poder tener un administrador independiente • La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales. • Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red • Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual • Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual. • Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual. • Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el trafico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente. Análisis de Seguridad y Almacenamiento de Logs en la Nube • La solución de seguridad debe contar con una solución en la nube que permita centralización de reportes, análisis de tráfico, administración de configuraciones, y almacenamiento de logs sin la necesidad de software o hardware adicional para esta función. • Contar con funcionalidad de Análisis de archivos sospechosos en la nube en caso que no se cuente con suficiente información en la solución de seguridad para calificar el tráfico como legitimo o ilegitimo, por medio de técnicas de Caja de Arena o Sandboxing. • Almacenamiento de Logs hasta 1 Giga por equipo incluido con capacidad de crecimiento en caso de requerirse. • Debe permitir administración centralizada de todos los equipos de la solución de seguridad perimetral desde una misma interfaz. • Permitir Monitoreo y alertas en tiempo real. • Debe contar con Reportes predefinidos y la opción de personalización, así como contar con herramientas de análisis. • Debe permitir visualizar de manera sencilla que todos los equipos de seguridad perimetral gestionados cuenten con la misma versión de firmware o sistema operativo para garantizar la homogeneidad en la red. 3- Licenciamiento y actualizaciones * Característicasdel licenciamiento El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, casillas de correo, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. * Vigencia de actualización dela licencia La vigencia de las actualizaciones para los servicios de Antivirus, Antispam, IPS, Application Control y URL Filtering debe proveerse por al menos 1 año. 4- Migración e Implementación • Implementación básica de Firewall a adquirir. • Configuración de Alta Disponibilidad. • Configuración de networking y cambio de topología actual. • Migración de reglas de firewall al nuevo equipo desde diferentes tecnologías de firewall y proxys. • Migración de reglas de control de ancho de banda desde equipamiento Exinda. • Configuración de reglas de firewall. • Configuración de NATs. • Configuración de VPNsIPSec. • Configuración de VPN SSL para acceso de los usuarios. • Integración con Active Directory. • Configuración de reglas de URL Filter. • Configuración de reglas de Application Control. • Configuración de reglas de AntiVirus. • Configuración de reglas de IPS. • Integración con WAF. 5- Capacitación Firewall Infrastructure: • Routing • WAN (SD-WAN) definida por Software • Dominios Virtuales • Layer 2 Switching	

Universidad Nacional de La Matanza

Renglón	Especificación Técnica	Imagen
	• VPN con IPSecsite-to-site • Alta Disponibilidad • Single Sign-On • Proxy Web • Diagnóstico Firewall Seguridad: • Introducción a firewall y la protección (respuesta rápida y unificada ante amenazas) • Políticas del Firewall. • Network AddressTranslation (NAT) • Autenticación del Firewall • Revisión de logs y monitoreo de uso • Operaciones Certificadas • Filtros Web • Control de Aplicaciones • Antivirus • Prevención de intrusiones y de Ataques DDoS(Denial of Service) • SSL VPN • VPN IPSEC via Dial Up • Prevención de pérdida de datos (Data LeakPrevention - DLP) Se deberá brindar una capacitación para todo el personal (7 personas) del Centro de Tecnología Informática y Seguridad Informática, 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 6- Servicios de Soporte para el Firewall • Soporte Técnico para la tecnología ofrecida. o Soporte y seguimiento de incidentes. o Upgrades de Sistemas Operativos. o Mejora continua en seguridad. • Apertura y seguimiento de casos con el fabricante. • El proveedor debe tener una herramienta para el manejo y seguimiento de incidentes. • El soporte deberá estar disponible de lunes a viernes de 8 a 22 horas. La UNLaM ponderara positivamnete toda oferta que reuniendo los requisitos tecnicos minimos establecidos por este pliego resulte favorable en condiciones tecnicas y/o economicas. 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 y deberán acreditar al menos tres años en esa situación.	
2	Se debera proveer 10 (diez) placas Fiber Channel para servidores DL380 Gen9 con las siguientes caracteristicas • P9D94A -- HPE StoreFabric SN1100Q 16Gb Dual Port Fibre Channel Host Bus Adapter • Placa controladora HBA de 2 canales, de 16 Gbps por canal. • Conexión PCI Express 3.0 de 8X • De bajo perfil. • Conexión LC • 25 CORDON DUPLEX CONECTORIZADO OM3 LC-UPC/LC-UPC 5M La UNLaM ponderara positivamnete toda oferta que reuniendo los requisitos tecnicos minimos establecidos por este pliego resulte favorable en condiciones tecnicas y/o economicas. 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 y deberán acreditar al menos tres años en esa situación.	

Universidad Nacional de La Matanza

Firma del Responsable de Contrataciones