CARACTERÍSTICAS TÉCNICAS POR EQUIPO
Firewall throughput de mínimo 50 Gbps
Throughput IPS mínimo 10 Gbps
Sesiones concurrentes mínimo 20.000.000
Soportar mínimo 200.000 nuevas sesiones/segundo
VPN throughput 5.5 GB
Antivirus throughput (proxy) 7 GB
Mínimo 6 puertos 10 GbE SFP+
Mínimo 8 puertos de cobre GbE
2 puertos USB 3.0
1 puerto COM (RJ45)
Fuente de poder redundante
La fecha de lanzamiento del producto no debe ser anterior a primero de enero del 2017
Con la licencia disponible el dispositivo deberá tener habilitados los módulos o funcionalidades de: protección de red(firewall), protección web, protección de correo electrónico, protección de servidor web (WAF), soporte de fábrica 24x7.
El fabricante del Firewall debe estar posicionado como líder en el cuadrante Gartner en el año 2018 para Unified Threat Management (SMB Multifunction Firewalls)
El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución.
La solución debe presentarse en un appliance hardware de propósito específico.
El dispositivo debe estar catalogado como un Firewall UTM.
Debe estar licenciado para operar en alta disponibilidad activo-activo.
Debe soportar alta disponibilidad activo-activo en modo transparente.
Protección de servidores por vulnerabilidades conocidas
Debe actualizar de manera automática las firmas para el sistema de detección de intrusos
Controlar el ancho de banda por usuario y/o por aplicación.
El Antivirus deberá incluir capacidades de detección y bloqueo de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red. Deberá tener la capacidad de escanear de virus los protocolos HTTP, HTTPS, FTP, SMTP, POP3, IMAP y además de filtrar los mismos en Túneles de VPN de tal forma que la información que se transmite por este túnel sea libre de malware.
Debe permitir identificar y bloquear conexiones hacia servidores de Centro de Control de Botnets.
El dispositivo deberá de contar con protección contra ataques persistentes (ATP)
Bloqueo de página por URL o Categoría.
Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida.
La solución deberá poder ofrecer una plataforma de reportes ejecutivos adicionales a la solución de Firewall
Deberá soportar Cifrado TLS para los protocolos SMTP, IMAP y POP
Deberá incluir motor DLP con escaneo automático de correos y adjuntos para restringir él envió de información sensible.
Debe contar con módulo de reporteo integrado que permita conocer de modo gráfico y detallado las operaciones, sin depender de algún equipo adicional.

CARACTERÍSTICAS TÉCNICAS	

940

Compras y Contratación

Universidad de Nariño

Fecha: 9-Mayo-19 Hora: 8:38am Firma:

Deberá incluir la funcionalidad integrada de VPN en SSL (Secure Socket Layer) en el mismo dispositivo.

- Soporte a Protocolos TCP&UDP sobre el Túnel.
- Autenticación puede ser vía: Directorio Activo, LDAP, RADIUS, TACACS+, Local.
- Autenticación Multinivel para el cliente a través de Certificados, Usuario y Contraseña.
- Asignación de Políticas por usuario y/o grupo
- Acceso a Red de forma: Total o Parcial.
- Acceso al cliente basado en Web a través de un Portal.
- Cliente ligero para acceso a través del Túnel.
- Acceso granular a los recursos de la Red.
- Controles y Administración de: Sesión timeout, Dead Peer Detección, Personalización del Portal de acceso.
- Acceso basado en aplicaciones TCP, entre las cuales debe de incluir: HTTP, HTTPS, RDP, TELNET, SSH, FTP, IBM Server Terminal, FTPS, SFTP, SMB y VNC

Deberá soportar los diferentes estándares para túneles de VPN:

- Encripción - 3DES, DES, AES, Twofish, Blowfish, Serpent
- Hash Algorithms - MD5, SHA-1
- Authentication - Preshared key, Digital certificates
- IPSec NAT Traversal
- Soporte a Dead peer detection y PFS
- Diffie Hellman Grupos - 1,2,5,14,15,16
- Soporte a entidades de una Autoridad Certificadora.
- Soporte a PPTP, L2TP.
- Soporte a Exportar configuraciones de Conexiones de tipo Cliente IPSec
  Soporte a las diferentes Plataformas:
  WinXP 32/64- bit, Windows Server 2008/2012, Windows Vista,7, 8/8.1 y 10 ya sea a 32/64-bits
- Soporte de Túneles a usuarios finales por Nombre Dominio
- Conexión Redundante de VPN
- Failover de enlaces MPLS a través de VPN IPSec
- Soporte de Overlapping
- Soporte de VPN Hub & Spoke

Deberá de contar también con un dispositivo para establecer VPNs de forma automática hacia el sitio central, este dispositivo no deberá de contar con alguna interface de configuración local, sino que toda la configuración de este dispositivo será realizada de forma centralizada en el equipo central, dicho dispositivos deberá de soportar

- Administración Centralizada de estos dispositivos desde el NGFW principal
- Sin configuración necesario en el dispositivo, toda configuración se tomará automáticamente por medio de un cloud de aprovisionamiento
- Túnel encriptado y seguro utilizando Certificados X.509 y encriptación AES256
- Estos tuneles de VPN se deberán de reflejar como una interface más de red en el NGFW central de tal forma que toda la asignación de permisos incluso DHCP y DNS deber de ser de forma centralizada
- Soporte a configuración de VLANs
- Compresión del tráfico enviado por el túnel de VPN.
- Desautorización remota de estos dispositivos después de un periodo de tiempo de inactividad configurable

El dispositivo debe ser capaz de realizar shaping de tráfico y QoS:

- Implementación flexible de QoS por usuario o por red.
- Configurar quotas de tráfico basadas en usuario en upload/download, Tráfico total, cíclico y no cíclico.
- Optimización de VoIP en tiempo real.
- Configuración de QoS avanzada por categoría Web o por aplicaciones para limitar o garantizar prioridades de trafico de upload/download, total, individual o compartido.

Deberá ofrecer la siguiente funcionalidad en el mismo Dispositivo. Web Application Firewall (WAF)

- Detección Intuitiva de amenazas y ataques para el Portal WEB (www).
- Protección contra Robo de Identidades de Sesión, Cross-site Scripting, Inyecciones de SQL, Envenenamiento de Cookies.
- Re direccionamiento de páginas web en base a los encabezados HTTP
- Soporte a protocolo Outlook anyware
- Autenticación reversa en base a formas web o autenticación básica web
- Motor para endurecimiento de formas web
- Escaneo dual de Antivirus
- Exclusiones/Bloqueos en base a IP o rangos de IP's
- Soporte al protocolo HTTP0.9/1.0/1.1
- Servicio de Registro y reportes extenso.
- Soporte a la detección de ataques Top 10 declarado por OWASP.

Deberá brindar la funcionalidad de Aplicar políticas por usuario, donde se le asigne de forma granular lo siguiente (Criterio de Control de Acceso):

- Ancho de banda asignado
- Filtrado de Aplicaciones Web
- Filtrado de Contenido vía HTTP y HTTPS
- Prevención de Intrusos
- Anti-Spam
- Zona Destino
- Direccion Fisica (MAC Address)
- IP Fuente
- IP Destino
- Servicio Calendarizado

Deberá ofrecer un filtrado para Prevención de intrusos el cual deberá de poder detectar y bloquear de forma enunciativa mas no limitativa el siguiente tipo de tráfico:

- Protocol Anomaly Detection Block
- Actividad de tipo "Phone home"
- Keylogger
- Mapa Geografico de tráfico (origen y destino de paquetes)
- Capacidad de Generacion de reportes limitada (visibilidad de tráfico, pero no de su origen) via los privilegios de administrador y totalmente abierta (visibilidad de Trafico con sus origenes) mediante las credenciales de un usuario adicional. Esto con el fin de preserver de inicio un nivel de confidencialidad para el usuario.

CARACTERÍSTICAS TÉCNICAS

El equipo deberá ofrecer como característica el Servicio de correlacionador de eventos en el mismo dispositivo de forma embebida, sin incurrir en un costo adicional. Este Servicio deberá contar con:

- Más de 1200+ reportes.
- Reportes Historicos
- Busqueda de Reportes
- Reportes Personalizados
- Reportes Incluidos de: Seguridad, Spam, Virus, Trafico, Bloqueos
- Más de 45 Reportes que cumplen con alguna norma o estándar de Seguridad.
- Todos los reportes exportables a archivos de tipo PDF y Excel.
- Reporte del nivel de riesgo por usuario, calificando dicho nivel de riesgo en base al comportamiento en Internet del usuario, y al estar ligado a la autenticación, debe poder mostrar el detalle de la información del usuario y su actividad.

Deberá Contar con analizador de tráfico en tiempo real.

- Registros en Tiempo real
- Notificación de estos reportes Vía email, de Virus y ataques
- Prevención de Intrusos
- Violaciones de Políticas
- Filtrado Web por uso de categorías
- Palabras buscadas en un search engine o buscador
- Información transferida (Por Host, Grupo y Direcciones IP)
- Incidencias de Virus por usuario y por dirección IP