Trade Up Equipos Fortinet

FortiGate 600C **Serial** FG600C3914800775

FortiGate 600C **Serial** FG600C3913800889

Documentación técnica de los reemplazos.

TERMINOS DE REFERENCIAS FAZ-200E

1) **Solución de Reportes tipo 1 (1 unidades)**

1.1) Debe soportar recibir logs de al menos 150 dispositivos

1.2) Tener capacidad de recibir al menos 100 GBytes de logs diarios

1.3) Soportar al menos 3000 logs/segundo de forma contínua

1.4) Tener al menos TB de espacio en disco

1.5) Tener al menos 2 interfaces de 1Gbps RJ-45

2) **Requisitos Mínimos de Funcionalidad**

Funcionalidades Generales

2.1) Debe soportar acceso vía SSH, WEB (HTTPS) y Telnet para la gestión de la solución

2.2) Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía línea de comandos en consola de gestión.

2.3) Permitir acceso simultaneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.

2.4) Soporte SNMP versión 2 y 3

2.5) Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.

2.6) Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.

2.7) Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH y Telnet.

2.8) Autenticación de usuarios de acceso a la plataforma vía Radius

2.9) Generación de informes en tiempo real de tráfico, ya sea en mapas geográficos y en tablas.

2.10) Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.

2.11) Autenticación de usuarios de acceso a la plataforma vía Microsoft Active Directory

2.12) Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.

2.13) Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.

2.14) Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado

2.15) Contar con mecanismos de borrado automático de logs antiguos.

2.16) Permitir la importación y exportación de reportes

2.17) Debe contar con la capacidad de crear informes en formato HTML

2.18) Debe contar con la capacidad de crear informes en formato PDF

2.19) Debe contar con la capacidad de crear informes en formato XML

2.20) Debe contar con la capacidad de crear informes en formato CSV

2.21) Debe permitir exportar los logs en formato CSV

2.22) Generación de logs de auditoria, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.

2.23) Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.

2.24) La solución debe contar con reportes predefinidos

2.25) Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución

2.26) Debe ser posible la duplicación de reportes existentes para su posterior edición.

2.27) Debe tener la capacidad de personalizar la portada de los reportes obtenidos.

2.28) Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.

2.29) Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.

2.30) Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas

2.31) Debe poseer mecanismo de "Drill-Down" para navegar en los reportes de tiempo real.

2.32) Debe permitir descargar de la plataforma los archivos de logs para uso externo.

2.33) Tener la capacidad de generar y enviar reportes periódicos automáticamente.

2.34) Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.

2.35) Permitir el envío por email de manera automática de reportes.

2.36) Debe permitir que el reporte a enviar por email sea al destinatario especifico.

2.37) Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.

2.38) Debe ser posible visualizar gráficamente en tiempo real el consumo de disco y la tasa de generación de logs por cada dispositivo gestionado.

2.39) Debe permitir el uso de filtros en los reportes.

2.40) Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.

2.41) Permitir que los reportes creados sean en idioma español

2.42) Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.

2.43) Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.

2.44) Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para su en gráficas y tablas en reportes.

2.45) Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.

2.46) Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.

2.47) Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.

2.48) Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.

2.49) La solución debe servir como un servidor Syslog y aceptar logs de diferentes fabricantes

2.50) Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.

2.51) Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.

2.52) Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos

2.53) Debe permitir visualizar en tiempo real los logs recibidos

Reportes

2.54) Debe permitir la creación de Dashboards personalizados para visualizar tráfico de aplicaciones, categorías de URL, amenazas, servicios, países, origen y destino.

2.55) Debe contar con un Indicar de Comprometimiento (IoC), que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.

2.56) Debe contar con reporte de cumplimiento de PCI DSS

2.57) Debe contar con reporte de utilización de aplicaciones SaaS

2.58) Debe contar con reporte de prevención de perdida de datos (DLP)

2.59) Debe contar con reporte de VPN

2.60) Debe contar con reporte de Sistema de prevención de intrusos (IPS)

2.61) Debe contar con reporte de reputación de cliente

2.62) Debe contar con reporte de análisis de seguridad de usuario

2.63) Debe contar con reporte de análisis de amenaza cibernética

Reportes

2.64) Debe contar con reporte de cumplimiento PCI de Wireless.

2.65) Debe contar con reporte de AP´s y SSID´s autorizados, así como clientes WIFi

Reportes

2.66) Debe contar con reporte de vulnerabilidades de solución gestionada de seguridad de equipo terminal.

Reportes

2.67) Debe contar con análisis de seguridad y uso de web, si se tiene plataforma de Cache

Reportes

TERMINOS DE REFERENCIAS DE FORTIGATE 500E

1) Solución UTM/NGFW tipo 1 (2 unidades)

1.1) Throughput de por lo menos 22 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6, independiente del tamaño del paquete

1.2) Soporte a por lo menos 8M conexiones simultaneas

1.3) Soporte a por lo menos 300K nuevas conexiones por segundo

1.4) Throughput de al menos 20 Gbps de VPN IPSec

1.5) Estar licenciado para, o soportar sin necesidad de licencia, 2K túneles de VPN IPSec site-to-site simultáneos

1.6) Estar licenciado para, o soportar sin necesidad de licencia, 10K túneles de clientes VPN IPSec simultáneos

1.7) Throughput de al menos 5 Gbps de VPN SSL

1.8) Soportar al menos 500 clientes de VPN SSL simultáneos

1.9) Soportar al menos 5 Gbps de throughput de IPS

1.10) Soportar al menos 5 Gbps de throughput de Inspección SSL

1.11) Throughput de al menos 4.5 Gbps con las siguientes funcionalidades habilitadas simultáneamente para todas las firmas que la solución de seguridad tenga debidamente activadasy operativas: control de aplicaciones, IPS, Antivirus y Antispyware. Caso el fabricante tenga publicado múltiples números de desempeño para cualquiera de las funcionalidades, solamente el de valor más pequeño será aceptado.

1.12) Permitir gestionar al menos 256 Access Points

1.13) Tener al menos 18 interfaces 1Gbps

1.15) Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance

1.16) Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance

2) Requisitos Mínimos de Funcionalidad

Características Generales

2.1) La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.;

2.2) Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;

2.3) Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;

2.4) La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;

2.5) Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación;

2.6) La gestión de los equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;

2.7) Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;

2.8) Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;

2.9) Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;

2.10) Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);

2.11) Los dispositivos de protección de red deben soportar DHCP Relay;

2.12) Los dispositivos de protección de red deben soportar DHCP Server;

2.13) Los dispositivos de protección de red deben soportar sFlow;

2.14) Los dispositivos de protección de red deben soportar Jumbo Frames;

2.15) Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;

2.16) Debe ser compatible con NAT dinámica (varios-a-1);

2.17) Debe ser compatible con NAT dinámica (muchos-a-muchos);

2.18) Debe soportar NAT estática (1-a-1);

2.19) Debe admitir NAT estática (muchos-a-muchos);

2.20) Debe ser compatible con NAT estático bidireccional 1-a-1;

2.21) Debe ser compatible con la traducción de puertos (PAT);

2.22) Debe ser compatible con NAT Origen;

2.23) Debe ser compatible con NAT de destino;

2.24) Debe soportar NAT de origen y NAT de destino de forma simultánea;

2.25) Debe soportar NAT de origen y NAT de destino en la misma política

2.26) Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;

2.27) Debe ser compatible con NAT64 y NAT46;

2.28) Debe implementar el protocolo ECMP;

2.29) Debe soportar el balanceo de enlace hash por IP de origen;

2.30) Debe soportar el balanceo de enlace por hash de IP de origen y destino;

2.31) Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;

2.32) Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;

2.33) Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;

2.34) Enviar logs a sistemas de gestión externos simultáneamente;

2.35) Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;

2.36) Debe soporta protección contra la suplantación de identidad (anti-spoofing);

2.37) Implementar la optimización del tráfico entre dos dispositivos;

2.38) Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);

2.39) Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);

2.40) Soportar OSPF graceful restart;

2.41) Los dispositivos de protección deben tener la capacidad de operar simultáneamente en una única instancia de servidor de seguridad, mediante el uso de sus interfaces físicas en los siguientes modos: modo sniffer (monitoreo y análisis de tráfico de red), capa 2 (L2) y capa 3 (L3);

2.42) Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;

2.43) Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;

2.44) Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;

2.45) Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;

2.46) Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;

2.47) Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;

2.48) Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;

2.49) La configuración de alta disponibilidad debe sincronizar: Sesiones;

2.50) La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;

2.51) La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;

2.52) La configuración de alta disponibilidad debe sincronizar: Tablas FIB;

2.53) En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;

2.54) Debe soportar la creación de sistemas virtuales en el mismo equipo;

2.55) Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;

2.56) Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;

2.57) La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;

2.58) Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);

2.59) Debe soportar un tejido de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;

2.60) El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;

2.61) Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi;

Control por Política de Firewall

2.62) Debe soportar controles de zona de seguridad;

2.63) Debe contar con políticas de control por puerto y protocolo;

2.64) Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;

2.65) Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;

2.66) Firewall debe poder aplicar la inspección UTM (control de aplicaciones y filtrado web como mínimo) directamente a las políticas de seguridad en vez de usar perfil obligatoriamente;

2.67) Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;

2.68) Debe soportar el almacenamiento de bitácoras (logs) en tiempo real tanto para entorno de la nube como entorno local (on-premise);

2.69) Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);

2.70) Debe existir una manera de evitar que el almacenamiento de logs en tiempo real no superen la velocidad de subida de los mismos (upload);

2.71) Debe soportar el protocolo estándar de la industria VXLAN;

Control de Aplicación

2.72) Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;

2.73) Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos;

2.74) Reconocer al menos 1.700 aplicaciones diferentes, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;

2.75) Reconocer al 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;

2.76) Debe inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo;

2.77) Debe detectar aplicaciones a través del análisis del comportamiento del tráfico observado, incluyendo, pero no limitado a las aplicaciones de VoIP que utilizan cifrado propietario y BitTorrent;

2.78) Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;

2.79) Para trafico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;

2.80) Debe hacer decodificación de protocolos con el fin de detectar aplicaciones encapsuladas dentro del protocolo y validar que el tráfico corresponde a la especificación del protocolo, incluyendo, pero no limitado a Yahoo Instant Messenger utilizando HTTP. La decodificación de protocolo también debe identificar las características específicas dentro de una aplicación, incluyendo, pero no limitado al intercambio de ficheros dentro de Webex;

2.81) Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;

2.82) Actualización de la base de firmas de la aplicación de forma automática;

2.83) Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos;

2.84) Los dispositivos de protección de red deben tener la capacidad de identificar al usuario de la red con la integración de Microsoft Active Directory sin necesidad de instalación del agente en el controlador de dominio, o en estaciones de trabajo de usuario;

2.85) Debe ser posible añadir múltiples reglas de control de aplicaciones, es decir, no debe limitar habilitar el control de aplicaciones de control solamente en algunas reglas;

2.86) Debe ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación;

2.87) Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;

2.88) Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;

2.89) La creación de firmas personalizadas debe permitir el uso de expresiones regulares, el contexto (sesiones o transacciones), utilizando la posición en el payload de paquetes TCP y UDP, y el uso de decodificadores de al menos los siguientes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, SSL y RTSP;

2.90) El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;

2.91) Debe alertar al usuario cuando sea bloqueada una aplicación;

2.92) Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;

2.93) Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;

2.94) Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;

2.95) Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;

2.96) Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc);

2.97) Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;

2.98) Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;

2.99) Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente.

Prevención de Amenazas

2.100) Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;

2.101) Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);

2.102) Las características de IPS, antivirus y anti-spyware deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;

2.103) Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;

2.104) Debe implementar los siguientes tipos de acciones a las amenazas detectadas por IPS: Permitir, permitir y generar registro, bloquear, bloquear IP del atacante durante un tiempo y enviar tcp-reset;

2.105) Las firmas deben ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo;

2.106) Debe ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad;

2.107) Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas;

2.108) Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;

2.109) Deber permitir el bloqueo de vulnerabilidades;

2.110) Debe permitir el bloqueo de exploits conocidos;

2.111) Debe incluir la protección contra ataques de denegación de servicio;

2.112) Debe tener los siguientes mecanismos de inspección IPS: Análisis de patrones de estado de las conexiones;

2.113) Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;

2.114) Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;

2.115) Debe tener los siguientes mecanismos de inspección IPS: Análisis heurístico;

2.116) Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;

2.117) Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;

2.118) Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);

2.119) Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;

2.120) Detectar y bloquear los escaneos de puertos de origen;

2.121) Bloquear ataques realizados por gusanos (worms) conocidos;

2.122) Contar con firmas específicas para la mitigación de ataques DoS y DDoS;

2.123) Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);

2.124) Debe poder crear firmas personalizadas en la interfaz gráfica del producto;

2.125) Debe permitir utilizar operadores de negación en la creación de firmas personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración;

2.126) Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3;

2.127) Soportar el bloqueo de archivos por tipo;

2.128) Identificar y bloquear la comunicación con redes de bots;

2.129) Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;

2.130) Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;

2.131) Debe permitir la captura de paquetes por tipo de firma IPS y definir el número de paquetes capturados o permitir la captura del paquete que dio lugar a la alerta, así como su contexto, facilitando el análisis forense y la identificación de falsos positivos;

2.132) Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;

2.133) Los eventos deben identificar el país que origino la amenaza;

2.134) Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);

2.135) Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;

2.136) Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;

2.137) El Firewall debería permitirle analizar la implementación del tejido de seguridad para identificar posibles vulnerabilidades y resaltar las mejores prácticas que podrían utilizarse para mejorar la seguridad y el rendimiento general de su red;

2.138) En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;

2.139) Los recursos de postura de seguridad deben existir para permitir que el software de seguridad de endpoint aplique protección en tiempo real, antivirus, filtrado de Web y control de aplicaciones en el punto final;

2.140) Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);

Filtrado de URL

2.141) Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);

2.142) Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad;

2.143) Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio Active Directory y la base de datos local;

2.144) Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;

2.145) Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;

2.146) Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL;

2.147) Tener por lo menos 60 categorías de URL;

2.148) Debe tener la funcionalidad de exclusión de URLs por categoría;

2.149) Permitir página de bloqueo personalizada;

2.150) Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);

2.151) Además del Explicit Web Proxy, soportar proxy web transparente;

Identificación de Usuarios

2.152) Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;

2.153) Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios;

2.154) Debe tener integración y soporte para Microsoft Active Directory para los siguientes sistemas operativos: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2;

2.155) Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no

debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;

2.156) Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios;

2.157) Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/control basados en usuarios y grupos de usuarios;

2.158) Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);

2.159) Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;

2.160) Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;

2.161) Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;

2.162) Proporcionar al menos un token de forma nativa, lo que permite la autenticación de dos factores;

QoS Traffic Shaping

2.163) Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;

2.164) Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;

2.165) Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;

2.166) Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;

2.167) Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;

2.168) Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;

2.169) En QoS debe permitir la definición de tráfico con ancho de banda garantizado;

2.170) En QoS debe permitir la definición de tráfico con máximo ancho de banda;

2.171) En QoS debe permitir la definición de colas de prioridad;

2.172) Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype;

2.173) Soportar marcación de paquetes DiffServ, incluso por aplicación;

2.174) Soportar la modificación de los valores de DSCP para Diffserv;

2.175) Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);

2.176) Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shaping;

2.177) Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;

Filtro de Datos

2.178) Permite la creación de filtros para archivos y datos predefinidos;

2.179) Los archivos deben ser identificados por tamaño y tipo;

2.180) Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.);

2.181) Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;

2.182) Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;

2.183) Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares;

Geo Localización

2.184) Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;

2.185) Debe permitir la visualización de los países de origen y destino en los registros de acceso;

2.186) Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;

VPN

2.187) Soporte VPN de sitio-a-sitio y cliente-a-sitio;

2.188) Soportar VPN IPSec;

2.189) Soportar VPN SSL;

2.190) La VPN IPSec debe ser compatible con 3DES;

2.191) La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1;

2.192) La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;

2.193) La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);

2.194) La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);

2.195) La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI;

2.196) Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

2.197) Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;

2.198) Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;

2.199) La VPN SSL debe soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web;

2.200) Las características de VPN SSL se deben cumplir con o sin el uso de agentes;

2.201) Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;

2.202) Asignación de DNS en la VPN de cliente remoto;

2.203) Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;

2.204) Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;

2.205) Suportar lectura y revisión de CRL (lista de revocación de certificados);

2.206) Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;

2.207) Debe permitir que la conexión a la VPN se establezca de la siguiente manera: Antes de que el usuario se autentique en su estación;

2.208) Debe permitir que la conexión a la VPN se establezca de la siguiente manera: Después de la autenticación de usuario en la estación;

2.209) Debe permitir que la conexión a la VPN se establezca de la siguiente manera: Bajo demanda de los usuarios;

2.210) Deberá mantener una conexión segura con el portal durante la sesión;

2.211) El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows 7 (32 y 64 bits), Windows 8 (32 y 64 bits), Windows 10 (32 y 64 bits) y Mac OS X (v10.10 o superior).

Wireless Controller

2.212) Deberá gestionar de manera centralizada puntos de acceso del mismo fabricante de la solución ofertada;

2.213) Soportar servicio de servidor DHCP por SSID para proporcionar direcciones IP a los clientes inalámbricos;

2.214) Soporte IPv4 e IPv6 por SSID;

2.215) Permitir elegir si el tráfico de cada SSID se enviará a la controladora o directamente por la interfaz de punto de acceso en una determinada VLAN;

2.216) Permitir definir qué redes se acceden a través de la controladora y que redes serán accedidas directamente por la interfaz del Access Point;

2.217) Soportar monitoreo y supresión de puntos de acceso indebidos;

2.218) Proporcionar autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS;

2.219) Permitir autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows;

2.220) Permitir la visualización de los dispositivos inalámbricos conectados por usuario;

2.221) Permitir la visualización de los dispositivos inalámbricos conectados por IP;

2.222) Permitir la visualización de los dispositivos inalámbricos conectados por tipo de autenticación;

2.223) Permitir la visualización de los dispositivos inalámbricos conectados por canal;

2.224) Permitir la visualización de los dispositivos inalámbricos conectados por ancho de banda usado;

2.225) Permitir la visualización de los dispositivos inalámbricos conectados por potencia de la señal;

2.226) Permitir la visualización de los dispositivos inalámbricos conectados por tiempo de asociación;

2.227) Debe soportar Fast Roaming en autenticación con portal cautivo;

2.228) Debe soportar configuración de portal cautivo por SSID;

2.229) Permitir bloqueo de tráfico entre los clientes conectados a un SSID y AP específico;

2.230) Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y / o TKIP;

2.231) Debe ser compatible con el protocolo 802.1x RADIUS;

2.232) La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal;

2.233) La controladora deberá permitir métodos de descubrimiento de puntos de acceso de manera automática;

2.234) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por IP estática;

2.235) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DHCP;

2.236) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DNS;

2.237) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por Broadcast;

2.238) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por Multicast;

2.239) La controladora inalámbrica deberá suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue);

2.240) La controladora deberá contar con protección contra ataques ARP Poisoning en el controlador inalámbrico;

2.241) La controladora deberá contar con mecanismos de protección de tramas de administración de acuerdo a las especificaciones de la alianza Wi-Fi y estándar 802.11ac;

2.242) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo ASLEAP;

2.243) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Association Frame Flooding;

2.244) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Authentication Frame Flooding;

2.245) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Broadcasting De-authentication;

2.246) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo EAPOL Packet flooding;

2.247) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Invalid MAC OUI;

2.248) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Long Duration Attack;

2.249) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Null SSID probe response;

2.250) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Spoofed De-authentication;

2.251) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Weak WEP IV Detection;

2.252) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Wireless Bridge;

2.253) Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas;

2.254) Permitir seleccionar el día y hora en que se producirá la optimización de aprovisionamiento automática de canales en los puntos de acceso;

2.255) La controladora inalámbrica debe permitir agendar horarios para determinar en qué momento la red inalámbrica (SSID) se encuentra disponible;

2.256) La controladora inalámbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario;

2.257) Permitir configurar el número máximo de clientes que pueden ser permitidos por SSID;

2.258) Permitir configurar el número máximo de clientes que pueden ser permitidos por punto de acceso;

2.259) Permitir configurar el número máximo de clientes que pueden ser permitidos por Radio;

2.260) La controladora debe permitir crear, administrar y autorizar las redes inalámbricas mesh;

2.261) Ofrecer un mecanismo de creación automática y/o manual de usuarios visitantes y contraseñas, que puedan ser enviados por correo electrónico o SMS a los usuarios, con ajuste de tiempo de expiración de la contraseña;

2.262) La comunicación entre la controladora y el punto de acceso inalámbrico pueda ser realizada de forma cifrada utilizando protocolo DTLS;

2.263) Debe tener un mecanismo de ajuste automático de potencia de la señal con el fin de reducir la interferencia entre canales entre dos puntos de acceso administrados;

2.264) Ofrecer un mecanismo de balanceo de trafico/usuarios entre Puntos de acceso;

2.265) Proporcionar un mecanismo de balanceo de trafico/usuarios entre frecuencias y/o radios de los Puntos de Acceso;

2.266) Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualización a través de la interfaz gráfica;

2.267) Permitir que sean deshabilitados clientes inalámbricos que tengan baja tasa de transmisión;

2.268) Permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados;

2.269) La controladora debe permitir configurar el valor de Short Guard Interval para 802.11n y 802.11ac en 5 GHz;

2.270) Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados;

2.271) Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID especifico mediante protocolo RADIUS;

2.272) Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID especifico mediante vlan pooling;

2.273) Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalámbrico;

2.274) La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en aplicaciones;

2.275) La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en dirección de destino;

2.276) La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en amenaza;

2.277) La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en sesiones;

2.278) la controladora inalámbrica debe soportar una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de tráfico;

2.279) El controlador inalámbrico debe tener interface de administración integrado en el mismo equipo;

2.280) El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el nodo secundario y nodos principales;

2.281) La controladora inalámbrica deberá soportar aceleración de tráfico del protocolo CAPWAP a través de un procesador de red de propósito específico;

2.282) La controladora inalámbrica deberá soportar aceleración de túnel de tráfico de puente inalámbrico a través de un procesador de red de propósito específico;

2.283) La controladora inalámbrica debe soportar protocolo LLDP;

2.284) Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC exacta;

2.285) Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC adyacente;

2.286) Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos;

2.287) La controladora inalámbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado;

2.288) La controladora inalámbrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas;

2.289) La controladora inalámbrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada;

2.290) Deberá soportar la conversión de Multicast a Unicast para mejorar el rendimiento del tiempo de aire;

2.291) En el entorno de alta disponibilidad, debe existir el concepto de controladores primarios y secundarios en la unidad AP, permitiendo que la unidad decida el orden en el que el AP selecciona una unidad controlador y cómo la unidad AP se conecta a un controlador de backup en el caso de que el controlador primario falle;

2.292) Debe proporcionar la capacidad de crear varias claves pre-compartidas de acceso protegido WiFi (WPA-PSK) para que no sea necesario compartir PSK entre dispositivos;