Requisitos Mínimos de Funcionalidad de Reportería y Administración Centralizada

Funcionalidades Generales

Si la solución es virtualizada, no debe haber límites a la cantidad de múltiples vCPU
Si la solución es virtualizada, no debe haber límites a la expansión de memoria RAM
Debe soportar acceso vía SSH, WEB (HTTPS) para la gestion de la solución
Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía linea de comandos en consola de gestión.
Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
Soporte SNMP versión 2 y 3
Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH
Autenticación de usuarios de acceso a la plataforma via LDAP
Autenticación de usuarios de acceso a la plataforma via Radius
Autenticación de usuarios de acceso a la plataforma via TACACS+
Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos
Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.
Generación de informes en tiempo real de tráfico, en formato de gráfica tabla
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.
Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.
Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado
Contar con mecanismos de borrado automático de logs antiguos.
Permitir la importación y exportación de reportes
Debe contar con la capacidad de crear informes en formato HTML
Debe contar con la capacidad de crear informes en formato PDF
Debe contar con la capacidad de crear informes en formato XML
Debe contar con la capacidad de crear informes en formato CSV
Debe permitir exportar los logs en formato CSV

Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.
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.
La solución debe contar con reportes predefinidos
Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución

Debe ser posible la duplicación de reportes existentes para su posterior edición.
Debe tener la capacidad de personalizar la portada de los reportes obtenidos.
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.
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.
Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas
Debe poseer mecanismo de "Drill-Down" para navegar en los reportes de tiempo real.
Debe permitir descargar de la plataforma los archivos de logs para uso externo.
Tener la capacidad de generar y enviar reportes periódicos automáticamente.
Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
Permitir el envío por email de manera automática de reportes.
Debe permitir que el reporte a enviar por email sea al destinatario específico.
Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.
Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.
Debe permitir el uso de filtros en los reportes.
Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.
Permitir especificar el idioma de los reportes creados
Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.
Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.
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.
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.
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.

Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.
Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.
Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.
Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos
Debe permitir visualizar en tiempo real los logs recibidos.
Debe permitir el reenvío de logs en formato syslog.
Debe permitir el reenvío de logs en formato CEF (Common Event Format).
Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red

Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en su red.
Debe incluir dashboard para operaciones SOC que monitorea el tráfico en su red.
Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en su red
Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en su red (sandboxing).
Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en su red.
Debe incluir dashboard para operaciones SOC que monitorea actividad VPN ren su red.
Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs
Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria)
Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC
Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3
Debe permitir generar alertas de eventos a partir de logs recibidos
Debe permitir crear incidentes a partir de alertas de eventos para endpoint
Debe permitir la integración al sistema de tickets ServiceNow
Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, 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.
Debe permitir respaldar logs en nube publica de Amazon S3
Debe permitir respaldar logs en nube publica de Microsoft Azure
Debe permitir respaldar logs en nube publica de Goooogle Cloud
Debe soportar el estándar SAML para autenticación de usuarios administradores

Reportes de Firewall
Debe contar con reporte de cumplimiento de PCI DSS
Debe contar con reporte de utilización de aplicaciones SaaS
Debe contar con reporte de prevención de perdida de datos (DLP)
Debe contar con reporte de VPN
Debe contar con reporte de Sistema de prevención de intrusos (IPS)
Debe contar con reporte de reputación de cliente
Debe contar con reporte de análisis de seguridad de usuario
Debe contar con reporte de análisis de amenaza cibernética
Debe contar con reporte de breve resumen diario de eventos e incidentes de seguridad
Debe contar con reporte de tráfico DNS
Debe contar con reporte tráfico de correo electrónico
Debe contar con reporte de Top 10 de Aplicaciones utilizadas en la red
Debe contar con reporte de Top 10 de Websites utilizadas en la red
Debe contar con reporte de uso de redes sociales

Reportes de Fabric

Debe contar con reporte de evaluación de riesgo para correo electrónico

Reportes de Wireless

Debe contar con reporte de cumplimiento PCI de Wireless.

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

Reportes de Endpoint

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

Reportes de WAF

Debe contar con reporte de aplicaciones web, si se cuenta con plataforma de seguridad web

Soporte para la administración centralizada de toda la solución incluido soporte de hasta 110 dispositivos.

Requerimientos técnicos de implementación

1- Empresa con técnico certificado en: solución ofertados y CEH, ITIL Foundation y 10 años de experiencia en implementaciones de la solución, Unico ingeniero. (No se permiten certificaciones individuales)
2- Certificación del fabricante de distribución autorizado
3- Servicios técnicos basados en la migración de los equipos actuales y nuevos requerimientos