Funcionalidades EndPoint Protecction.

La solucion propuesta debe permitir la gerencia de cliente de seguridad a partir de un sistema centralizado de gerencia del mismo fabricante.
La solucion propuesta debe poder utilizar multiples perfiles de configuracion de acuerdo al segmento de red donde la misma se encuentre
"Debe ser compatible con los siguientes sistemas operativos:
Microsoft Windows: 7 (32 y 64 bits)
Microsoft Windows: 8 (32 y 64 bits)
Microsoft Windows: 8.1
Microsoft Windows:10 (32 y 64 bits);
Microsoft Windows Server: 2008 R2
Microsoft Windows Server:2012
Microsoft Windows Server: 2012 R2;
Microsoft Windows Server: 2016
Mac OS X: v10.8 (León de montaña),
Mac OS X: v10.9 (Mavericks),
Mac OS X:v10.10 (Yosemite),
Mac OS X:v10.11 (El Capitán)
Linux OS
Ubuntu 16.04+
Red Hat 7.4+
CentOS 7.4+ "
"Debe ser compatible con los siguientes sistemas operativos moviles:
IOS 5.1+
Adroid 4.4.4+"
La solución debe permitir realizar un backup y restauración del archivo de configuración del cliente de seguridad
La solucion propuesta debe ser capaz de generar registros (logs) relacionados con: red privada virtual (VPN), firewall de aplicación, actividades de antivirus, actividades de filtros web, Actividad de búsqueda de vulnerabilidades;
Al menos los siguientes niveles de registro deben estar disponibles: emergencia, alerta, crítico, error, aviso, informativo;
El cliente de seguridad debe ser capaz de enviar la información de los logs a los sistemas de administración e informes del mismo fabricante a través de la red IP;
La solución propuesta debe permitir la configuración de parámetros del sistema vía XML (eXtensible Markup Language);
La solución propuesta debe permitir la integración con sistemas de Sandboxing del mismo fabricante;
La solución debe permitir el control de dispositivos de medios extraíbles como unidades USB. El cliente puede Permitir, Bloquear o Monitorizar el acceso a dispositivos de medios extraíbles.
La solución propuesta debe permitir que durante la instalacion se elija cuales componentes de la misma seran ejecutadas

El fabricante debe poseer portal para descargar el cliente de seguridad e instalación directa en los sistemas operativos;
Debe ser compatible con posibles instalaciones a través del servidor de directorio activo de Microsoft;
El sistema de gestión centralizada debe ser capaz de instalar el cliente de seguridad en equipos con sistema operativo Windows en un dominio de Windows;
El cliente de seguridad debe ser capaz de comprobar archivos, archivos ejecutables, archivos DLL y drivers que buscan los virus informáticos;
El cliente de seguridad debe buscar actualizaciones periódicas y automáticas en los sistemas del fabricante disponibles en Internet, incluyendo comprobaciones en tiempo real;
El cliente de seguridad debe ser capaz de enviar archivos al sistema de Sandboxing del mismo fabricante para que sean analizados;
El cliente de seguridad debe bloquear el acceso a los canales de comunicación de los hackers / atacantes;
El cliente de seguridad debe proporcionar notificaciones cuando se detectan virus informáticos;
El cliente de seguridad debe permitir que el usuario o el sistema de administración inician la exploración de la búsqueda de virus en el equipo donde está instalado el cliente;
El cliente de seguridad debe permitir la programación de barrido indicando frecuencia (diaria, semanal o mensual) con horario de inicio y tipo de barrido;
El cliente de seguridad debe ser capaz de mostrar los archivos colocados en cuarentena por el subsistema antivirus;
Debe permitir la configuración de diferentes perfiles de cliente de seguridad definidos del sistema de gestión centralizada;
El cliente de seguridad debe aceptar perfiles de filtrado de sitios web creados desde el sistema de administración centralizada del mismo fabricante;
El fabricante deberá poner a disposición en Internet la clasificación de las paginas web que puede utilizarse en la definición de reglas que se aplicar al cliente de seguridad;
El cliente de seguridad debe permitir la configuración de reglas estáticas de acceso desde el sistema de administración centralizada del mismo fabricante. Debe permitirse la creación de reglas basadas en expresiones regulares y / o Wildcard
Para una determinada URL las posibles acciones realizadas por el sistema de gestión deben ser: permitir, bloquear, alertar o monitorear;
El cliente de seguridad debe aceptar perfiles para el control de applicaciones creados desde el sistema de administración centralizada del mismo fabricante. Estos perfiles deben permitir el bloqueo, la supervisión o permitir la aplicación;
El fabricante deberá poner a disposición en Internet la clasificación de las aplicaciones que puede utilizarse en la definición de reglas que se pueden aplicar al cliente de seguridad;
Deberán reconocerse al menos 2800 aplicaciones para la definición de reglas de acceso desde el cliente de seguridad (configuración desde el sistema de gestión centralizada del mismo fabricante);
Debe permitir al usuario crear nuevas conexiones SSL VPN;
Debe permitir la configuración de varios puntos de acceso VPN (diversos concentradores de acceso a la red);
Debe permitir la personalización de puerto TCP que se utilizará para la conexión SSL

Debe permitir la autenticación por nombre de usuario y contraseña;
Debe permitir la autenticación de dos factores a través de sistemas adicionales proporcionados por el fabricante;
Debe permitir el uso de certificados para la autenticación para el acceso SSL;
Debe permitir al usuario crear nuevas conexiones con VPN IPSec;
Debe permitir la configuración de varios puntos de acceso (diversos concentradores de acceso a la red);
Debe permitir la autenticación de nombre de usuario y contraseña;
Debe permitir métodos de autenticación basados en certificados X.509 y Pre-Shared Key;
Debe permitir la selección de modo principal y agresivo;
Debe permitir la configuración de DHCP sobre IPSec;
Debe permitir la selección de NAT Traversal;
Debe permitir la selección de grupos Diffie-Hellman (1,2,5 y 14);
Debe permitir la configuración de caducidad de claves IKE;
Debe permitir el uso de Perfect Forward Secrecy;
Debe permitir la autenticación de dos factores a través de sistemas adicionales proporcionados por el fabricante;
El cliente de seguridad debe tener un sistema de búsqueda de vulnerabilidades conocidas en equipo donde el cliente está instalado, configurable por el sistema de gestion centralizada
El cliente de seguridad debe permitir que el usuario inicie el proceso de exploración para encontrar vulnerabilidades;
Las vulnerabilidades encontradas por el cliente de seguridad se deben presentar en el propio sistema y tener acceso (a través de direcciones URL) a un banco de vulnerabilidades proporcionado por el fabricante en Internet. Este banco debe proveer al menos: nombre de la vulnerabilidad, grado de severidad y detalles sobre la misma;
El cliente de seguridad debe permitir la remediacion de las vulnerabilidades dectectadas
Debe permitir la instalación en Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016
La gerencia sobre clientes de seguridad debe estar incluida en el mismo licenciamiento del del cliente de seguridad.
Debe poseer interfaz de gestión vía web browser;
Debe poseer funcionalidad de copia de seguridad de la base de datos;
Debe permitir la creación de usuarios con diferentes derechos de administración;
Debe posibilitar la importación de información de usuario y su ordenador desde el servidor de Directorio Activo con servicios LDAP o STARTTLS;
Debe permitir la creación de grupos de clientes de seguridad para facilitar la gestión del medio ambiente;
Debe permitir la configuración de los perfiles de los clientes de seguridad vía XML;
Debe posibilitar la importación de perfil de configuración de firewalls del mismo fabricante;
Debe permitir la configuración de diferentes perfiles y diferentes grupos de clientes de seguridad para facilitar la gestión del conjunto de clientes de seguridad instalados;
Debe permitir la creación de perfiles de cliente de seguridad incluyendo antivirus, filtro web, firewall de aplicación y red privada virtual (VPN);
La solucion debe poder gestionar la protección en tiempo real de los clientes instalados
La solucion debe poder gestionar el escaneo programado: diario, semanal o mensual;

La solucion debe poder gestionar el tipo de barrido: completas o parciales;
La solucion debe poder gestionar la clasificación de sitios web proporcionada por el fabricante y disponibles en la herramienta y sus posibles acciones: bloquear, avisar, permitir y monitorear;
La solucion debe poder gestionar la clasificación de sitios web a través de comodines o expresiones regulares y sus posibles acciones: bloquear o permitir;
La solucion debe poder gestionar el permiso para que los usuarios realicen la configuración de las VPN;
La solucion debe poder gestionar el permiso de desconexión de VPN;
La solucion debe poder gestionar el permitir la conexión antes del inicio de sesión de Windows;
La solucion debe poder gestionar la auto conexión de VPN en el cliente
La solucion debe poder gestionar la opción para que el usuario tenga acceso a la configuración del cliente de seguridad por contraseña solamente;
La solucion debe poder gestionar le enrutamiento de registros (logs) para sistemas de gestión y / o informes del mismo fabricante;
La solucion debe poder gestionar la instalación junto al sistema de gestión de forma silenciosa (de forma que no sea perceptible para el usuario);
La solucion debe poder gestionar la Instalación de certificados en el cliente (copia local al sistema de gestión centralizado);
La solucion debe poder gestionar la habilitación de funcionalidad de inicio de single sign on mobility agent
"Debe estar disponible un Dasbboard en el sistema de gestión centralizada para proporcionar información sobre:
Cantidad de dispositivos administrados,
Versión del sistema operativo,
Perfil de instalación, Usuario,
Versión de firma de antivirus."
"Debe estar disponible un Dashboard en el sistema de gestion centralizada para proporcionar informacion sobre:
Estado del cliente de seguridad
registrado o no registrado;"
"Debe estar disponible un Dashboard en el sistema de gestion centralizada para proporcionar informacion sobre:
Información sobre el sistema operativo donde está instalado el cliente de seguridad;"
"Debe estar disponible un Dashboard en el sistema de gestion centralizada para proporcionar informacion sobre:
Perfil de cliente de seguridad;"
"Debe estar disponible un Dashboard en el sistema de gestion centralizada para proporcionar informacion sobre:
Funciones de seguridad habilitadas en el cliente de seguridad: antivirus, filtro web, VPN, firewall de aplicación;"
"Debe estar disponible un Dashboard en el sistema de gestion centralizada para proporcionar informacion sobre:
Vulnerabilidades detectadas"

La solucion debe poder gestionar la integracion con un firewall de la misma marca del fabricante para establecer reglas de compliance
La solucion debe poder gestionar los clientes localizados tanto en una red LAN local como a travez de Internet
La solucion debe poder enviar correos electronico cuando ocurra una alerta definida
La solucion debe poder gestionar el parchado de vulnerabilidades detectadas
La solucion propuesta debe licenciarse basado en la cantidad de numero de clientes

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
4- Logística de distribución de equipos en todo el país
5- Precio final debe de incluir viáticos de implementación.