Ciudad y Fecha: Manizales, 5/01/2015

Dependencia o Seccional:	Sección sistemas	Código	SI
		Consecutivo	005

En cumplimiento a los principios generales de la contratación y lo ordenado por la Gerencia, se adelanta el siguiente análisis de conveniencia y oportunidad:

1. DEFINICIÓN DE LA NECESIDAD

Con la interconexión de equipos informáticos en red, la especialización de algunos de ellos en determinados servicios y, la conexión de éstos a Internet para ofrecerlos a cualquier usuario, ha avivado la necesidad de proteger las redes privadas ante posibles intentos de infiltración externos y, por extensión también los internos.

Una de las principales tareas, desde el punto de vista preventivo, que se va a encontrar es el diseño y configuración de la llamada seguridad perimetral, cuya definición más inmediata indica que no es más que el establecimiento de un perímetro de seguridad que proteja y aísle la red local interna y la red local de servicios de las entradas externas, definiendo, al estilo de las estrategias militares, un perímetro de seguridad mediante el uso de equipamiento específico configurado para realizar determinados filtros a los paquetes de datos y, en definitiva, manejar y controlar el acceso a la red interna de la organización.

Elementos de la seguridad perimetral

Para el diseño y, posterior implementación de una protección perimetral, se debe tener en cuenta las distintas posibilidades que se nos ofrece, dependiendo de los diferentes elementos que utilicemos para desarrollar los controles de acceso.

El primer control de acceso que se puede aplicar en una red es la segmentación de los dominios de colisión y difusión. Por tanto, los switchs y routers, encargados los primeros de la segmentación del dominio de colisión y los segundos, además, de la segmentación del dominio permiten definir qué equipos se ven sin necesidad de filtrar, simplemente segmentando y definiendo las tablas de rutas.

El filtrado de paquetes se puede realizar a distintos niveles de la pila TCP/IP, con elementos y características diferentes por nivel. Así, a nivel de red, se encuentran los llamados router de selección que son, básicamente, equipos de red que tienen la capacidad de encaminar y filtrar paquetes. En un nivel más elevado, se distinguen, como principales elementos, los proxys, socks y las envolventes.

Switch

Desde el punto de vista de la seguridad preventiva, el primer paso que se da implícitamente es en el diseño de la red local de una organización con la segmentación de la red en diferentes subredes y la definición de las tablas de rutas de los diferentes encaminadores. La posibilidad introducida por los switchs de aislar el tráfico en diferentes redes, incluso dentro de un mismo elemento de red con la tecnología de VLANS, introduce implícitamente características de confidencialidad, como mínimo, al no poder, desde una subred dada, acceder al tráfico de otra.

Esta seguridad, además, es la más eficiente ya que no introduce carga extra al sistema como el caso de la encriptación (procesos que consumen muchos ciclos de CPU) o el filtrado (aplicar regla a TODOS los paquetes que circulan por la red puede suponer, dependiendo del número de filtros y la cantidad de paquetes a procesar, un exceso de computación).

Por tanto, los switchs se pueden considerar como elementos de seguridad ya que permiten la segmentación del dominio de colisión, e incluso, con las tecnologías de VLANS, de difusión, ayudando, por tanto a prevenir posibles amenazas contra la confidencialidad e integridad de los datos que circulan por la red.

Además, existen switchs de alto nivel que permiten, incluso, controlar a nivel de enlace a qué equipos permitimos conectarse a la red. Las configuraciones, en cuanto a nivel de comprobación, pueden variar desde simplemente permitir determinadas MAC, hasta con el uso del protocolo 802.1X, que sólo equipos donde los usuarios que están autenticados y autorizados puedan utilizar la red, introduciendo así, la característica de autentificación.

Router de selección

Un router o encaminador es un dispositivo de red encargado redirigir paquetes desde una interfaz a otra utilizando para ellos las reglas de encaminamiento que se le indican por configuración (encaminamiento estático), o por un proceso que aprende dichas reglas (encaminamiento dinámico). En definitiva, segmentan el dominio de difusión y, por extensión, el de colisión, permitiendo además que unas redes se comuniquen con otras mediante la característica de encaminar paquetes.

Como se ha comentado anteriormente, en el diseño y con la decisión de permitir que los routers dirijan paquetes o no de una red a otra, se está introduciendo cierta seguridad preventiva. Con el encaminamiento clásico en el que la redirección de paquetes se basa en reglas que sólo tienen en cuenta el destino se estaba más limitado a la hora de gestionar seguridad a este nivel. Sin embargo, se han introducido dos características adicionales que muchos routers presentan -sobre todo la primera, que prácticamente todos disponen de ella-: filtrado de paquetes y encaminamiento regulado. Con el encaminamiento regulado, podemos introducir reglas de rutas basadas en más parámetros que la simple dirección de destino, lo que introduce más versatilidad y más control de qué paquetes se redirigen y, por tanto, de qué redes se pueden interconectar.

Los routers con filtrado de paquetes reciben el nombre de routers de selección y suelen ser el elemento principal de casi todas las configuraciones de seguridad perimetral. Consiste en definir reglas de control de acceso para permitir o denegar, en su concepción más básica, la redirección de paquetes, aunque las tablas de encaminamiento permitan mandarlos. Normalmente, dichas reglas se aplican en el orden en el que han sido guardadas y, en cuanto un paquete cumple las condiciones de una regla, se aplica ésta, interrumpiéndose el análisis del resto y permitiendo o denegando el paquete, según lo que indique la regla. Si no se cumple ninguna, se suele disponer de una acción por defecto que significa:

- Todo lo que no está permitido explícitamente, está prohibido
- Todo lo que no está prohibido explícitamente, está permitido

Desde el punto de vista de la seguridad, parece mejor opción la primera, ya que se es más restrictivo y, en el caso de que exista un error y algo que debiera estar permitido, no sea así, seguro que algún usuario avisa al administrador. Por el contrario, con la segunda opción, si se nos olvida alguna regla y dejamos abierto algún servicio, es muy poco probable que un usuario avise del problema.

Las acciones que puede realizar un router de selección con filtrado de paquetes son:

- Enviar el paquete
- Eliminar el paquete sin avisar al destinatario
- Rechazar el paquete devolviendo un error
- Guardar un registro del evento
- Activar una alarma
- Modificar el paquete cambiando direcciones o puertos de origen o destino del paquete realizando la llamada Network Translation Address (NAT).

Su principal ventaja es que, sobre todo cuando se habla de hardware dedicado, son más rápidos y eficientes a la hora de manejar grandes volúmenes de datos. Por el contrario, son menos versátiles, no permitiendo, en la mayoría de los casos, comprobaciones a nivel de usuario y análisis de contenido de los paquetes.

NAT

La modificación de los paquetes por parte de los routers de selección para cambiar las direcciones y/o puertos de origen o destino, recibe el nombre de Network Translation Address (NAT). Esta técnica se puede utilizar, además de para la optimización de las direcciones IP, para aislar el tráfico de entrada y/o salida ocultando la configuración interna de la red.

El cambio puede ser estático, una IP se sustituye por otra fija, o dinámico con la que la información de estado no siempre está disponible. Además, NAT puede interferir con algunos sistemas de encriptación y autentificación; también con el sistema de registro de

eventos ya que, por ejemplo, si se realiza NAT para la red Interna de una organización, todos los ordenadores que se conecten a un servidor Web externo lo harán con la misma IP y, por tanto, podría tomarse como el mismo equipo. Además, el NAT de puertos podría interferir con el propio sistema de filtrado de paquetes, por lo que se debe ser muy cauteloso con su uso e integración con el resto de los mecanismos de prevención.

Proxy

Los proxys se ejecutan en el nivel de aplicación. Por tanto, son aplicaciones que, ante requerimientos de los usuarios de equipos internos de la red de una organización para conectarse a servicios de Internet, actúan de intermediario, de tal forma que las peticiones desde el cliente interno van al Proxy y éste las redirige al servidor destino, siendo la dirección de la interfaz externa del proxy la que ve el servidor final.

Este tipo de aplicación presenta la ventaja de que se dispone de mayor control que con NAT, permitiendo filtros más inteligentes. Se pueden establecer reglas en función del usuario y contenido, por ejemplo, que actualmente muy pocos routers de selección con NAT disponen.

Además, también puede proporcionar mecanismos de caché que optimiza el uso de la red, aunque por el contrario, los router de selección son más eficientes y permiten manejar mayor cantidad de paquetes -presentan mayor ancho de banda-.

Como principal inconveniente, además del menor ancho de banda con respecto al NAT, es que dependen del servicio. Por lo tanto, debe existir un Proxy por cada servicio al que queramos conectarnos.

Como solución a este problema se creó socks. Socks es una aplicación independiente del servicio que realiza la misma función que los Proxy y cuyo principal inconveniente es que exige modificar las aplicaciones utilizando librerías específicas que conecten con el servidor de socks.

Cortafuegos

Se entiende por cortafuegos a una arquitectura de seguridad de red en la que se sitúan diversos elementos para controlar el tráfico de entrada y salida a una organización.

Antes de entrar en detalle con las arquitecturas existentes de cortafuegos, se va a describir tres de los elementos que intervienen en ellas, además de los routers de selección y los proxys:

- Host bastión. Equipo de la red que realiza filtros de paquetes, como los routers de selección, es utilizado como intermediario en las comunicaciones y, por tanto, debe estar especialmente protegido, ya que puede ser objeto de ataques al ser un equipo visible desde el exterior.

- Host de base dual. Equipo que dispone de dos interfaces de red -con más de dos recibe el nombre de host de base múltiple- por lo general, cada una conectada a una red diferente.

- Red perimetral o zona neutra. Red añadida entre dos redes para proporcionar mayor protección a una de ellas.

Arquitectura de cortafuegos

Cuando una organización conecta su red local a Internet, deja abierto el acceso a todos los equipos de su red desde el exterior. La posibilidad de proteger los equipos de forma individual causa pavor entre los administradores de sistemas por el excesivo trabajo que puede llevar, proporcional al número de equipos; la complejidad que supone el mantenimiento y la fiabilidad de los sistemas, por la posible heterogeneidad de los clientes, tanto en software como hardware que puede no soportar determinada aplicación de filtrado, el trato que los usuarios de los equipos puedan realizar, etc. En definitiva, para proteger a todos los equipos de una red, la solución debe ser global y enfocarse como un problema de red, aunque se pueda realizar filtros en los equipos finales.

Una arquitectura de cortafuegos debería diseñarse y planificarse, idealmente, cuando se diseña la estructura de la red. Un cortafuegos no deja de ser un diseño de red en el que se emplean determinados componentes, de los descritos en el apartado anterior, cuya finalidad es la de canalizar el tráfico por los elementos apropiados y permitir o denegar según las reglas introducidas.

Existen varias arquitecturas de cortafuegos desde la más sencilla que utiliza simplemente un router de selección hasta otras más complejas basadas en varios routers de selección, proxys y redes perimetrales. El tipo de arquitectura se debe elegir en función a las necesidades de seguridad y a la disponibilidad económica de la organización.

Router de protección

Es la configuración más simple consistente en el empleo de un router de selección para filtrar el tráfico de entrada y salida a la red local. El encaminador se sitúa en la conexión con la red externa y se encarga de canalizar, además del filtrado, los paquetes entre la red interna y externa.

Es una arquitectura barata y simple, toda la seguridad de la red reside en un único punto: el router de selección.

La Sección Sistemas de **EMPOCALDAS S.A E.S.P** entendida en lo necesaria que es proveer con seguridad perimetral y con un sistema de conexión entre las sedes por medio de VPN recomienda hacer la adquisición de una herramienta que permita brindar con dichos servicios.

La solución debe tener las siguientes características:

Características	Descripción
Maximum application control (AVC) throughput	500 Mbps
Maximum application control (AVC) and IPS throughput	250 Mbps

Maximum concurrent sessions	250,000
Maximum New Connections per second	15,000
Application control (AVC) or IPS sizing throughput [440 byte HTTP]*	150 Mbps
Supported applications	More than 3,000
URL categories	80+
Number of URLs categorized	More than 280 million
Centralized configuration, logging, monitoring, and reporting	Multi-device Cisco Security Manager and Cisco Management Center opción hardware ó software.
Market-leading NGIPS	Superior threat prevention and mitigation for both known and unknown threats
Advanced malware protection	Detection, blocking, tracking, analysis, and remediation to protect the enterprise against targeted and persistent malware attacks
Full contextual awareness	Policy enforcement based on complete visibility of users, mobile devices, client-side applications, communication between virtual machines, vulnerabilities, threats, and URLs
Application control and URL filtering	Application-layer control (over applications, geolocations, users, websites) and ability to enforce usage and tailor detection policies based on custom applications and URLs
Enterprise-class management	Dashboards and drill-down reports of discovered hosts, applications, threats, and indications of compromise for comprehensive visibility
Streamlined operations automation	Lower operating cost and administrative complexity with threat correlation, impact assessment, automated security policy tuning, and user identification
Purpose-built, scalable	Highly scalable security appliance architecture that performs at up to multigigabit speeds; consistent and robust security across branch, Internet edge, and data centers in physical and virtual environments
Third-party technology ecosystem	Open API that enables the third-party technology ecosystem to integrate with existing customer work streams
Integration with Snort and OpenAppID	Open source security integration with Snort and OpenAppID for access to community resources and ability to easily customize security to address new and specific threats and applications

	quickly
Collective Security intelligence (CSI)	Globally acclaimed security and web reputation intelligence for real-time security protection
Proven firewall	Rich routing, stateful firewall, Network Address Translation,
Next-generation firewall	Industry's first threat-focused NGFW; provides firewall functionality, advanced threat protection, and advanced breach detection and remediation combined in a single device

El sistema debe:

- Ser un Firewall de clase empresarial con VPN de acceso remoto y clustering avanzado para acceso de alto rendimiento de alta seguridad y alta disponibilidad para ayudar a garantizar la continuidad del negocio. Debe ser capaz de verificar tanto interna como externamente la red, analizando cada capa de la misma, no solo a nivel de puertos de servicios, blindando los segmentos definidos por el equipo IT, obteniendo seguridad inteligente, debe hacer revisión de los ataques y comportamientos no habituales dentro de cada red que se proteja, adicional mostrar en el tiempo los comportamientos de los ataques granularmente y emitir alertas para tomar medidas, esto genera continuidad en la empresa, no solo revisar dispositivos de red comunes como equipos pc, debe ser capaz de analizar máquinas virtuales (Vmware, Xen), dispositivos móviles, diferentes sistemas operativos, impresoras, routers y switch, sistemas de Telefonía (ejemplo avaya, polycom…), sistemas de servidores (Apache, ISS4), protocolos de aplicaciones http, ssh, smtp, en los usuarios Ad, Ldap, Pop3, en aplicaciones web (Ebay, Facebook, etc..). Debe permitir generar alertas y recibir alertas a nivel de bases de datos en común a nivel mundial, debe ser capaz de analizar un comportamiento sencillo como un malware detrás de un archivo temporal.

- Contener una aplicación visibilidad granular y control (AVC) compatible con más de 3000 capas de aplicación y controles basados en el riesgo que puede invocar el sistema de prevención de intrusiones (IPS) a la medida de las políticas de detección de amenazas para optimizar la eficacia de la seguridad.

- La solución debe incluir la nueva generación IPS (NGIPS) que ofrece prevención muy eficaz contra amenazas y la conciencia contextual completa de los usuarios, la

infraestructura, las aplicaciones y el contenido para detectar amenazas multivectoriales y automatizar la respuesta de defensa.

- El sistema debe incluir un sistema para el Filtrado de URL basado en reputación, y basado en categorías de alertas y debe ofrecer un amplio control sobre el tráfico web sospechoso y hacer cumplir las políticas en cientos de millones de URLs en más de 80 categorías.

- El sistema debe ofrecer una avanzada protección contra malware con comprobada eficacia, debe ser líder en la industria de detección de incumplimiento, con un TCO bajo, y el valor de protección superior que le ayuda a descubrir, entender, y detener el malware y las amenazas emergentes perdidas por otras capas de seguridad.

- La solución tiene que proporcionar a los equipos de seguridad una visibilidad completa y control sobre la actividad dentro de la red. Dicha visibilidad incluye usuarios, dispositivos de comunicación entre máquinas virtuales, las vulnerabilidades, las amenazas, las aplicaciones del lado del cliente, archivos y sitios web. Holísticos, las indicaciones exigibles de compromiso (IOC) se correlacionan red y evento del objetivo obtener información detallada y proporcionar más visibilidad en las infecciones de malware.

- El sistema de Centro de Gestión debe proporcionar un conocimiento de contenido con trayectoria de archivos de malware que ayude detener la infección y a detectar la causa raíz para acelerar el tiempo de solución.

- El aplicativo administrador del sistema debe estar en capacidad de proporcionar la visión de las operaciones de la red y permitir la gestión de flujo de trabajo de manera escalable y centralizada. Asimismo, debe integrar un potente conjunto de capacidades; incluidas la política y la gestión de objetos, gestión de eventos, presentación de informes y resolución de problemas para las funciones de servidor de seguridad del dispositivo. Para pequeña escala y despliegues simples, el Administrador de dispositivos que incluya debe estar en capacidad de proporcionar en el dispositivo, la gestión de operaciones de red de firewall basada en GUI.

- El Sistema debe estar especialmente diseñado para ser altamente escalable, alcanzar velocidades de hasta multigigabit, y proporciona seguridad coherente y sólida en toda la rama, con el borde de Internet y centros de datos en entornos físicos y virtuales.

- El sistema de gestión debe analizar líneas corrientes para correlacionar las amenazas, evaluar su impacto, de forma automática la política de seguridad se debe ajustar e detectar las identidades de los usuarios que ocasionan los eventos de seguridad. El sistema debe continuamente monitorear la red y como cambia con el tiempo. Las nuevas amenazas deben ser evaluadas automáticamente para determinar lo que puede afectar al negocio.

Se debe incluir todos los elementos que se requieran para el adecuado funcionamiento de la solución ofrecida.
El proveedor de la solución debe tener relacionamiento directo con el fabricante, donde debe definirse mínimo como canal Cisco Select, y debe tener soporte en sitio, suministrando apoyo de ingeniería con personal certificado CCNA1, IT, cableado estructurado en varios fabricantes.
El proveedor debe implementar sobre una máquina virtual en VMWare los servicios de administración del firewall.
El suministro del elemento debe hacerse antes del 31 de Enero del año en curso.

OBLIGACIONES DEL FUTURO CONTRATO:

- Suministro equipo de seguridad perimetral
- Instalación de la solución

NOMBRE Y ESPECIFICACIONES DEL OBJETO DEL CONTRATO	CANT	UND	VR. UNIT	VR. TOTAL
NGFW 6GE AC 3DES/AES SSD con Contrato de Servicios 1Y ASA5500-x Licencias Management para su administración, licencias de seguridad IPS, con soporte URL y análisis malware. El Firewall debe contar con contrato de servicio	1			

smartnet 8x5NBD, actualización de software, acceso al Tac 24x7 Soporte, acceso a recurso técnicos en línea, contrato renovable durante un (1) año.				
Servicio de implementación y soporte en sitio por 12 meses directamente por el proveedor.	1			

2. CONDICIONES DEL FUTURO CONTRATO

Objeto: Adquisición de equipo de seguridad perimetral

Plazo de entrega o ejecución requerido: 15 días desde el acta de inicio

Sitio de entrega: Manizales

Valor estimado: $ 32.000.000

Rubro presupuestal: 23010201 $ 32.000.000

Centro de costos:_____ Código del procedimiento:

Cuando el plazo exceda el 31 de diciembre del año en curso se debe solicitar autorización a la Junta Directiva

Clase de contrato											
Suministros	X	Obra		Prestación de Servicio		Interventoría		Compra Venta		Orden de compra	
Convenio Inter-Administrativo		Contrato Inter-Administrativo		Otro		Cual:					

Si selecciona la respuesta "Prestación de Servicio" en la definición de la necesidad deberá sustentar que dentro de la planta de personal no existe persona idónea o suficiente para desempeñar dichas tareas, o determinar si se trata de una tarea especializada que amerita realizar la contratación.

Tipo de contratación							
Directa		Invitación	x	Invitación Pública		Otros	

Corresponde a una orden judicial?	SI		NO	x

Si selecciona la respuesta "SI" deberá anexar copia simple de la parte resolutiva de la providencia.

Tipo de Acción							
Acción de Tutela		Acción Popular		Otro		Cual:	
Nombre del Despacho Judicial que profirió la providencia:							

3. RIESGOS QUE DEBE AMPARAR EL CONTRATISTA

Amparo	

Anticipo	
Cumplimiento	
Salarios, prestaciones sociales e indemnización de personal	
Estabilidad y calidad de la obra	
Responsabilidad civil extracontractual	
Calidad y correcto funcionamiento de bienes y equipos suministrados	
Calidad	

4. INTERVENTOR SUGERIDO PARA EL CONTRATO
JEFE SECCION SISTEMAS

De acuerdo con lo establecido en el manual de contratación de la Empresa y la Ley 142 de 1994, se hace necesario realizar el citado contrato, cumpliendo con los parámetros legales señalados en las normas anteriormente citadas y las demás complementarias.

SE CONSIDERA OPORTUNA Y LEGAL LA CELEBRACIÓN DE ESTE CONTRATO.

Solicitado por:

Nombre	CARLOS ANDRES MARQUEZ MEJIA
Firma	
Cargo	JEFE SECCION SISTEMAS

FIRMA JEFE DEL AREA

17
5 015

EMPRESA DE OBRAS SANITARIAS DE CALDAS S.A. E.S.P

EMPOCALDAS S.A. E.S.P

NIT. 890.803.239-9

CERTIFICADO DE DISPONIBILIDAD PRESUPUESTAL

NUMERO 00024

EXPEDICION DEL CDP: 2015/01/05

SECCIONAL MANIZALES

OBJETO: ADQUISICION EQUIPO SEGURIDAD PERIMETRAL

EL SUSCRITO JEFE DE LA SECCION DE PRESUPUESTO

CERTIFICA

Que en el presupuesto de Gastos para la vigencia 2015, existe saldo disponible y no comprometido en el (o los) siguientes rubro(s) de apropiacion:

RUBRO APROPIACION	DESCRIPCION	VALOR
23010202	Adquisicion y Mantenimiento Hardware - equipos y R	32,000,000
TOTAL DISPONIBILIDAD PRESUPUESTAL		**32,000,000**

DIEGO IVAN LOPEZ LARGO

Jefe Seccion Presupuesto