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 00178

0027

EXPEDICION DEL CDP: 2015/01/28

SECCIONAL MANIZALES

OBJETO: SUMINISTRO Y CONFIGURACION ELEMENTOS - IMPLEMENTACION VPN

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	24,000,000
TOTAL DISPONIBILIDAD PRESUPUESTAL		**24,000,000**

DIEGO IVAN LOPEZ LARGO

Jefe Seccion Presupuesto

Recibí mercancía 9 28-01-2015

Código F-GC-01 Versión: 5 Diciembre 18 de 2013	EMPOCALDAS S.A E.S.P GESTION CONTRATACIÓN ANÁLISIS DE CONVENIENCIA Y OPORTUNIDAD	

Ciudad y Fecha: Manizales, 5/01/2015

Dependencia o Seccional:	Sección sistemas	Código	SI
		Consecutivo	007

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

Una red privada virtual (VPN) es una red privada construida dentro de una infraestructura de red pública, tal como la red mundial de Internet. Las empresas pueden usar redes privadas virtuales para conectar en forma segura oficinas y usuarios remotos a través de accesos a Internet económicos proporcionados por terceros, en vez de enlaces WAN dedicados o enlaces de marcación remota de larga distancia.

Las organizaciones pueden usar redes privadas virtuales para reducir los costos de ancho de banda de redes WAN, y a la vez aumentar las velocidades de conexión a través de conectividad a Internet de alto ancho de banda, tal como DSL, Ethernet o cable.

Las redes privadas virtuales proporcionan el mayor nivel posible de seguridad mediante seguridad IP (IPsec) cifrada o túneles VPN de Secure Sockets Layer (SSL) y tecnologías de autenticación. Estas tecnologías protegen los datos que pasan por la red privada virtual contra accesos no autorizados. Las empresas pueden aprovechar la infraestructura estilo Internet de la red privada virtual, cuya sencillez de abastecimiento permite agregar rápidamente nuevos sitios o usuarios. También pueden aumentar drásticamente el alcance de la red privada virtual sin expandir significativamente la infraestructura.

Las redes privadas virtuales extienden la seguridad a los usuarios remotos

Las redes VPN SSL y VPN IPsec se han convertido en las principales soluciones de redes privadas virtuales para conectar oficinas remotas, usuarios remotos y partners comerciales, porque:

Proporcionan comunicaciones seguras con derechos de acceso adaptados a usuarios

individuales, tales como empleados, contratistas y partners

Aumentan la productividad al ampliar el alcance de las redes y aplicaciones empresariales

Reducen los costos de comunicación y aumentan la flexibilidad

Los dos tipos de redes virtuales privadas cifradas:

VPN IPsec de sitio a sitio: Esta alternativa a Frame Relay o redes WAN de línea arrendada permite a las empresas extender los recursos de la red a las sucursales, oficinas en el hogar y sitios de los partners comerciales.

VPN de acceso remoto: Esto extiende prácticamente todas las aplicaciones de datos, voz o video a los escritorios remotos, emulando los escritorios de la oficina central. Las redes VPN de acceso remoto pueden desplegarse usando redes VPN SSL, IPsec o ambas, dependiendo de los requisitos de implementación.

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.

Características básicas de la seguridad

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autentificación

Autentificación y autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.

Integridad: de que los datos enviados no han sido alterados. Para ello se utiliza funciones de Hash. Los algoritmos de hash más comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).

Confidencialidad/Privacidad: Dado que sólo puede ser interpretada por los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).

No repudio: es decir, un mensaje tiene que ir firmado, y quien lo firma no puede negar que

envió el mensaje.

Control de acceso: Se trata de asegurar que los participantes autenticados tiene acceso únicamente a los datos a los que están autorizados.

Auditoria y registro de actividades: Se trata de asegurar el correcto funcionamiento y la capacidad de recuperación.

Calidad del servicio: Se trata de asegurar un buen rendimiento, que no haya una degradación poco aceptable en la velocidad de transmisión.

Requisitos básicos

Identificación de usuario: las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.

Cifrado de datos: los datos que se van a transmitir a través de la red pública (Internet), antes deben ser cifrados, para que así no puedan ser leídos si son interceptados. Esta tarea se realiza con algoritmos de cifrado como DES o 3DES que sólo pueden ser leídos por el emisor y receptor.

Administración de claves: las VPN deben actualizar las claves de cifrado para los usuarios.

Nuevo algoritmo de seguridad SEAL.

Tipos de VPN

Básicamente existen tres arquitecturas de conexión VPN:

VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las

conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.

Tunneling

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU (unidades de datos de protocolo) determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc.

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil. En escenarios de IP móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil.

VPN over LAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

Otro ejemplo es la conexión a redes Wi-Fi haciendo uso de túneles cifrados IPSec o SSL que además de pasar por los métodos de autenticación tradicionales (WEP, WPA, direcciones MAC, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN interna o externa.

La Sección Sistemas de **EMPOCALDAS S.A E.S.P** conocedora en lo necesaria que es la conexión con nuestras sedes remotas por medio de VPN recomienda hacer la adquisición de los elementos que permita brindar con dichos servicios.

La solución debe tener las siguientes características:

Specifications	**Description**
Standards	IEEE 802.11n, 802.11g, 802.11b, 802.3, 802.3u, 802.1D, 802.1p, 802.1w (Rapid Spanning Tree) 802.1X (security authentication), 802.1Q (VLAN), 802.11i (Wi-Fi Protected Access [WPA2] security), 802.11e (wireless QoS), IPv4 (RFC 791), IPv6 (RFC 2460), Routing Information Protocol (RIP) v1 (RFC 1058), RIP v2 (RFC 1723)
Ports	LAN, WAN, USB
Switch	Power button (on/off)
Buttons	Reset
Cabling Type	Category 5e or better

LEDs	Power, VPN, USB, WAN, Wireless, LAN (ports 1-4)
Operating System	Linux
Network	
Network Protocols	• Dynamic Host Configuration Protocol (DHCP) server • Point-to-Point Protocol over Ethernet (PPPoE) • Point-to-Point Tunneling Protocol (PPTP) • Layer 2 Tunneling Protocol (L2TP) • DNS proxy • DHCP relay agent • IGMP proxy and multicast forwarding • Rapid Spanning Tree Protocol (RSTP) • Dynamic Domain Name System (TZO, DynDNS, 3322.org, NOIP) • Network Address Translation (NAT), Port Address Translation (PAT) • One-to-One NAT • Port management • Port mirroring • Software configurable DMZ to any LAN IP address • Session Initiation Protocol (SIP) Application Layer Gateways (ALG)
LAN	• Four (4) 10/100/1000 Mbps Gigabit LAN ports with managed switch
WAN	• Single (1) 10/100/1000 Mbps Gigabit WAN port
WLAN	• Built-in high-speed 802.11n wireless access point
Routing Protocols	• Static routing • Dynamic routing • RIP v1 and v2 • Inter-VLAN routing
Network Address Translation (NAT)	Port Address Translation (PAT), Network Address Port Translation (NAPT) protocol
VLAN Support	Port-based and 802.1Q tag-based VLANs
Number of VLANs	5 active VLANs (3-4096 range)
IPv6	• Dual-stack IPv4 and IPv6 • 6to4 tunneling • Stateless address auto-configuration • DHCPv6 Server for IPv6 Clients on LAN • DHCP v6 client for WAN connectivity

	• Internet Control Message Protocol (ICMP) v6 • Static IPv6 Routing • Dynamic IPv6 Routing with RIPng
Network Edge (DMZ)	Software configurable to any LAN IP address
Layer 2	802.1Q-based VLANs, 5 active VLANs
Security	
Firewall	Stateful packet inspection (SPI) firewall, port forwarding and triggering, denial-of-service (DoS) prevention, software-based DMZ DoS Attacks Prevented: • SYN Flood Detect Rate • Echo Storm • ICMP Flood • UDP Flood • TCP Flood Block Java, Cookies, Active-X, HTTP Proxy
Access Control	IP access control lists; MAC-based wireless access control
Content Filtering	Static URL blocking or keyword blocking
Secure Management	HTTPS, username/password complexity
WPS	Wi-Fi Protected Setup
User Privileges	2 levels of access: admin and guest
VPN	
Gateway-to-gateway IPsec VPN	10 gateway-to-gateway IPSec tunnels
Client-to-gateway IPsec VPN	10 client-to-gateway IPsec tunnels using TheGreenBow and ShrewSoft VPN client
PPTP VPN	10 PPTP tunnels for remote client access
Encryption	Triple Data Encryption Standard (3DES)

Authentication	MD5/SHA1
VPN Pass-through	IPsec/PPTP/Layer 2 Tunneling Protocol (L2TP) pass-through
Quality of Service	
QoS	• 802.1p port-based priority on LAN port, application-based priority on WAN port • 3 queues • Differentiated Services Code Point support (DSCP) • Class of Service (CoS) • Bandwidth Management for service prioritization
Jumbo Frame	Supports Jumbo Frame on Gigabit ports - at least 1536B
Performance	
NAT Throughput	800 Mbps
Concurrent Sessions	12,000
IPsec VPN Throughput (3DES/AES)	50 Mbps
Configuration	
Web User Interface	Simple, browser-based configuration (HTTP/HTTPS)
Management	
Management Protocols	Web browser, Simple Network Management Protocol (SNMP) v3, Bonjour, Universal Plug and Play (UPnP)
Event Logging	Local, syslog, email alerts
Network Diagnostics	Ping, Traceroute, and DNS Lookup
Upgradability	Firmware upgradable through web browser, imported/exported configuration file
System Time	Supports NTP, Day Light Savings, Manual entry

Languages	GUI supports English, French, Italian, German, and Spanish
Wireless	
Radio and modulation type	802.11b: direct sequence spread spectrum (DSSS), 802.11g: orthogonal frequency division multiplexing (OFDM), 802.11n: OFDM
WLAN	2.4GHz IEEE 802.11n standard-based access point with 802.11b/g compatibility
Operating channels	11 North America, 13 most of Europe, auto channels selection
Wireless isolation	Wireless isolation between clients
External antennas	2 fixed antennas
Antenna gain in dBi	2 dBi
Transmit power	802.11b: 16.5 dBm +/- 1.5 dBm; 802.11g: 15 dBm +/- 1.5 dBm; 802.11n: 12.5 dBm +/- 1.5 dBm
Receiver sensitivity	-87 dBm at 11 Mbps, -71 dBm at 54 Mbps, -68 dBm at mcs15, HT20, -66 dBm at mcs15, HT40
Radio Frequency	Single-band, works on 2.4GHz
Wireless Domain Service (WDS)	Allows wireless signals to be repeated by up to 4 compatible devices
Operating Modes	Multifunction device-wireless router, access point mode with WDS, Point-to-Point Bridge mode with WDS, Point-Multi Point Bridge mode with WDS, Repeater mode with WDS
Active WLAN clients	Support up to 64 concurrent clients in wireless router mode and wireless Access Point mode
Multiple SSIDs	Supports multiple Service Set Identifiers (SSIDs), up to 4 separate virtual networks
Wireless VLAN map	Supports SSID to VLAN mapping with wireless client isolation

WLAN security	Wired Equivalent Privacy (WEP), WPA, WPA2-PSK, WPA2-ENT, 802.11i
Wi-Fi Multimedia (WMM)	WMM, WMM power save (WMM-PS)
Environmental	
Power	12V 2A
Certifications	FCC class B, CE, IC, Wi-Fi
Operating temperature	0° to 40°C (32° to 104°F)
Storage temperature	-20° to 70°C (-4° to 158°F)
Operating humidity	10 to 85 percent noncondensing

Se debe incluir la instalación, configuración y todos los elementos que se requieran para el adecuado funcionamiento de la solución ofrecida.

Los equipos serán configurados en la sede principal e implementados por el personal de sistemas en las sedes remotas que hacen parte de la infraestructura de EMPOCALDAS.

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 deberá garantizar un tiempo máximo de reposición de 3 horas para los equipos router que serán utilizados en las sedes remotas.

El suministro debe hacerse antes del 10 de Febrero del año en curso.

OBLIGACIONES DEL FUTURO CONTRATO:

- Suministro solución
- Instalación de la solución

NOMBRE Y ESPECIFICACIONES DEL OBJETO DEL CONTRATO	CANT	UND	VR. UNIT	VR. TOTAL
Multifunction Wireless-N VPN Router (Soporta 10 VPN, 64 clientes concurrentes WIFI, Puertos Lan(4 Puertos a GB), Wan(1 Puerto GB), Wlan (Support up to 64 concurrent clients in wireless router mode and wireless Access Point mode), Supports multiple Service Set Identifiers (SSIDs), up to 4 separate virtual networks, Soporte Usb, soporta 5 vlan, Soporte capa 2, Firewall Basico, control IP access control lists; MAC-based wireless access control, Soporta calidad QoS, soporte de trafico Nat 800 MBS, Configuración basada en Web con contrato de servicios RV130W-A-K9-NA CON-SBS-SVC2	25			
Servicio de implementación y soporte en sitio por 12 meses directamente por el proveedor.	1			

2. CONDICIONES DEL FUTURO CONTRATO

Objeto: Suministro equipos para la implementación de VPN

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

Sitio de entrega: Manizales

Valor estimado: $ 24.000.000

Rubro presupuestal: 23010201 $ 24.000.000

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.

Código F-GC-01 Versión: 5 Diciembre 18 de 2013	EMPOCALDAS S.A E.S.P GESTION CONTRATACIÓN ANÁLISIS DE CONVENIENCIA Y OPORTUNIDAD	

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