ESCUELA SUPERIOR POLITECNICA DEL LITORAL

LINUX REDES Y SEGURIDADES

Xavier Sánchez Granja [(1)]; Marcos Solórzano Cedeño [(2)]
Facultad de Ingeniería en Electricidad y Computación
Campus Gustavo Galindo Velasco, Km 30.5 Vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
xasanhez@fiec.espol.edu.ec (1); jsolorza@fiec.espol.edu.ec [(2)]
Febrero de 2013 – Marzo 2014

Director de Tesis: MSIA Fabián Barboza Gilces, mail rbarboza@espol.edu.ec

RESUMEN

Este proyecto tiene la finalidad de cubrir las necesidades de la empresa PETROGAS EP de acceder remotamente a sus recursos tecnológicos que se encuentran en su infraestructura interna, utilizando como vinculo redes públicas como internet. Para cumplir este objetivo se diseñó una herramienta web que facilita la creación de túneles virtuales para establecer conexiones remotas hacia la infraestructura de red desde cualquier punto con acceso a internet de manera segura, utilizando métodos de encriptación que protegen la información que viaja a través de la red para que no pueda ser alterada o modificada.

Palabras claves: *HTML, CSS, Midleware, Linux, Nodejs, Javascript, Bash, Vpn, OpenVpn, SSH, Certificado Digital, Túnel, Streaming, CENTOS.*

ABSTRACT

This project is intended to meet the needs of the company PETROGAS EP to remotely access their technological resources found in their internal infrastructure, using public networks such as the Internet link. To achieve this goal a web tool that facilitates the creation of virtual tunnels for remote connections to the network infrastructure from anywhere with internet access securely using encryption methods that protect information traveling was designed through network so that it can't be altered or modified.

Keywords: HTML, CSS, Midleware, Linux, Nodejs, Javascript, Bash, Vpn, OpenVpn, SSH, Certificado Digital, Tunel, Streaming, CENTOS.

1. Introducción

Dentro de los últimos años ha existido un enorme crecimiento en lo que corresponde al uso de las tecnologías de redes y transmisión de datos una de ellas son las Redes Privadas Virtuales (VPN), un sistema para construir conexiones seguras a través de la infraestructura de redes públicas, tanto para enlaces punto a punto, como para conectar distintas redes locales entre sí o permitir a un tele-trabajador conectarse a la sede de su empresa desde cualquier lugar con acceso a Internet.

Este sistema permite aprovechar la infraestructura de red de comunicaciones existente (sin la necesidad de alterarla), más la implementación de mecanismos de encriptación y autenticación se consigue un método de comunicación segura que combina un bajo coste con unos altos niveles de privacidad.

Por esta razón se estudia la posibilidad de crear una herramienta web que facilite la instalación, configuración y administración del servicio VPN para la empresa PETROGAS EP.

2. Generalidades.

2.1 Antecedes.

.

PETROGAS al no contar con una infraestructura que permita realizar conexiones remotas decide implementar un sistema de acceso remoto VPN basado en la política control de acceso de la ISO/IEC 27002 por lo cual se propone desarrollar una herramienta que facilite la instalación, configuración y administración del servicio VPN de acceso remoto.

2.2 Objetivo General

Permitir la administración remota de los recursos de la infraestructura de TI mediante un canal de comunicación seguro que garantice el teletrabajo de los empleados de una empresa pública de hidrocarburos.

2.3 Objetivos Específicos

Se especifica a continuación los objetivos específicos planteados para el desarrollo e implementación del proyecto:

- Implementar un canal de comunicación remoto que permita el acceso y transferencia de datos de forma segura.
- Diseñar una aplicación web y un diagrama de red que permita acceso remoto a la infraestructura de TI de la empresa Pública de Hidrocarburos.
- Identificar los requerimientos de la conexión remota para garantizar que se satisfagan las necesidades empresariales.

3. Fundamentación Teórica

En el presente capitulo establecemos una serie de fundamentos teóricos acerca de la tecnología de acceso remoto y el protocolo de seguridad escogido para elaborar el proyecto.

3.1 VPN de acceso remoto.

Provee acceso remoto a la intranet o extranet corporativa a través de una infraestructura pública (Internet), conservando las mismas políticas, como seguridad y calidad de servicio, que en la red privada.

3.2 VPN sobre SSL

Las VPN sobre SSL son basadas a través túneles o puentes que proporcionan autenticación y privacidad entre extremos sobre internet mediante el uso de criptografía.

3.3 Característica principal de la VPN Utilizada

La característica principal es el driver tun/tap utilizado para simular interfaces de red, que se encarga de levantar el túnel y encapsular los paquetes a través del enlace virtual.

Modo Túnel: emplea el driver Tun y es utilizado para crear túneles virtuales operando con el protocolo IP.

Modo Puente: utiliza el driver Tap y es empleado para túneles que encapsulan directamente paquetes Ethernet.

Autenticación: El cliente y el servidor intercambian una clave generada mediante un algoritmo de cifrado como RSA o Diffe-Hellman. Si la clave es correcta se estable un canal de comunicación seguro.

4. Herramientas para el diseño de la solución

Para cumplir las exigencias del proyecto utilizamos herramientas que facilitaron el desarrollo de la página web y la interacción de ésta con el servicio OPENVPN. Luego de un profundo análisis optamos por el uso de la arquitectura cliente servidor, donde la página WEB actúa como cliente y el OpenVpn como Servidor .La estructura de la página está basada en HTML v5 y CSS.

Se utilizó MIDDLEWARE(Node,Js) como agente de interacción entre la página web y el Shell de Linux para poder realizar configuraciones en tiempo real tales como detener o iniciar el servicio de OpenVpn, mostrar reportes de conectividad y permitir la descargas de certificados digitales mediante el uso del streamming.

El objetivo de este capítulo es familiarizar al lector con las herramientas utilizadas para la construcción y simulación del proyecto tanto en la parte de Hardware como en la de Software.

4.1 Especificaciones técnicas

Las características o requerimientos básicos que debe tener el servido para un buen rendimiento y funcionamiento son los siguientes, ver la **Tabla 1.**

No	Dispositivo	Requerimiento	
		Mínimo	Recomendado
1	Procesador	Pentium 4	Quad Core I3
2	RAM	756 MB	2GB
3	Disco Duro	80GB	250 GB
4	Tarjeta de Red	10/100 Mbps	10/100/1000 Mbps

Tabla 1. Características del Servidor

En la **Tabla 2** se presentan los componentes de software.

No	Componente	Nombre
1	Plataforma	Linux
2	Distribución	Centos 6
3	VPN	OpenVpn 2.0.8
4	Servidor Web	Apache
5	Middleware	Node.js 0.10.4
6		Openssl

Tabla2. Componentes del servidor

4.2 Herramientas de propósito General

4.2.1 OpenVpn

Es una solución de conectividad basada en software libre; SSL (Secure Sockets Layer) VPN Virtual Private Network (red virtual privada), OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente

4.2.2 Apache

Apache es un servidor web flexible, rápido y eficiente, continuamente actualizado y adaptado a los nuevos protocolos HTTP.

- Multiplataforma.
- Modular: Puede ser adaptado a diferentes entornos y necesidades, con los diferentes módulos de apoyo que proporciona, y con la API de programación de módulos, para el desarrollo de módulos específicos.

4.2.3 Node.js

Node.js es un entorno de programación en la capa del servidor basado en el lenguaje de programación JavaScript, con I/O de datos en una arquitectura orientada a eventos y basado en el motor Javascript V8. Fue creado con el enfoque de ser útil en la creación de programas de red altamente escalables, como por ejemplo, servidores web.

4.2.4 OpenSSL

OpenSSL consiste en un robusto paquete de herramientas de administración y bibliotecas relacionadas con la criptografía, que suministran funciones criptográficas a otros paquetes como OpenSSH y navegadores web (para acceso seguro a sitios HTTPS), ofrece una capa de cifrado de transporte sobre la capa normal de comunicación, permitiendo la combinación con muchas aplicaciones y servicios de red, además OpenSSL permite crear certificados digitales que pueden aplicarse a un servidor.

4.2.5 HTML

HTML es el lenguaje con el que se definen las páginas web. Básicamente se trata de un conjunto de etiquetas que sirven para definir el texto y otros elementos que compondrán una página web.

4.2.6 GNS3

GNS3 es un simulador grafico de redes del cual hacemos uso para la implementación de este proyecto, con esta herramienta diseñamos fácilmente la topología de red y luego ejecutamos simulaciones en él.

4.2.7 VirtualBox

Herramienta de virtualización la cual hacemos uso para efectos de implementación del proyecto, con esta herramienta montamos nuestro ambiente virtualizado de varios equipos, uno actúa como servidor y el resto como clientes.

5. Diseño e Implementación de la Solución Propuesta

5.1 Arquitectura de la Herramienta Web de Acceso Remoto

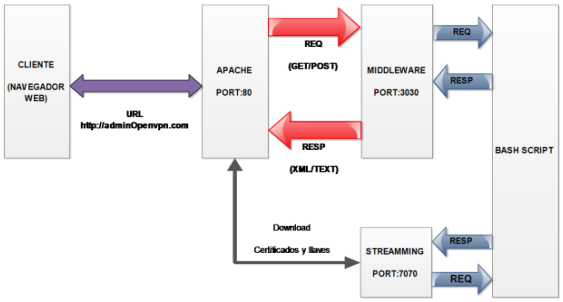

Figura 1. Arquitectura de la herramienta web

El cliente envía peticiones hacia MIDDLEWARE; éste recibe la petición, los procesa y los reenvía hacia el servidor a través de un puerto específico previamente configurado.

5.2 Estructura de la página HTML

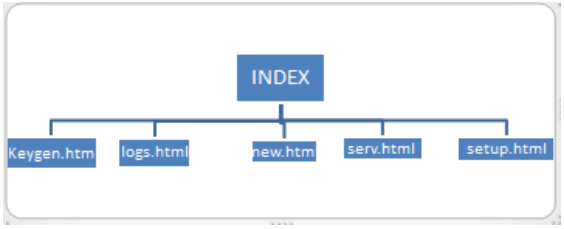

Figura 2. Estructura de la página HTML

La herramienta web está conformada por 5 páginas web, estas están configuradas en un ambiente jerárquico y se ejecutan mediante el accionar de los botones de la página principal.

5.3 Diagrama de Red Utilizado en la Solución propuesta

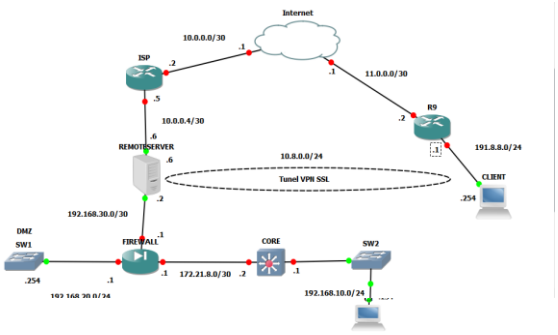

Figura 3. Topología de Red

La red de datos que podemos observar en el grafico es la sugerida a aplicar en PETROGAS, ya que gracias a este diseño tenemos mejor seguridad al momento de acceder a la VPN ya que el tráfico interno es filtrado por el FIREWALL.

6. Conclusiones

- Se ofrece mayor seguridad al momento de realizar conexiones remotas con la ayuda firewall y el uso del protocolo de autenticación/encriptación utilizado.
- Se mejora la productividad de la empresa, debido a que se ofrece facilidades para acceder a los recursos de la red interna desde cualquier punto con acceso a internet.
- Se optimiza los recursos tecnológicos de PETROGAS, al utilizar software libre debido a que nos ofrece seguridad y confiabilidad.

7. Recomendaciones

- Para ofrecer mayor seguridad se recomienda ubicar el servidor detrás del firewall de la infraestructura de red de PETROGAS EP.

- Cuando se agreguen nuevos segmentos a ser visibles en el túnel, especificar los debidos filtros y reglas de nateo en el IPTABLES.

- Cada vez que se realice una configuración adicional en la herramienta, es necesario reiniciar el servicio para que se apliquen los cambios.

8. Referencias

[1] Joel Barrios, Configuración de Servidores con GNU/LINUX, 23 de Agosto del 2012

[2] Scribd, GNS3 simulador de redes, http://es.scribd.com/doc/11840950/GNS3-Simulador-de-Redes-Grafico, Mayo 2013.

[3] Scribd, Virtualización con Virtualbox, http://es.scribd.com/doc/39691787/Virtualizacion-Con-Virtual-Box, Mayo 2013.

[3] monografías.com, Configuración OpenVpn, http://www.monografias.com/trabajos95/configuracion-openvpn/configuracion-openvpn.shtml Junio 2013

[4] recursostic.educacion.ec, Tipos de conexión a internet, http://recursostic.educacion.es/usuarios/web/es/ayudas/54-conexiones-a-internet-bis, junio 2013.

[5] Alcance Libre, VPN en servidor Linux y clientes Windows XP con OpenVpn + Shorewall, http://www.alcancelibre.org/staticpages/index.php/openvpn-clientes-win-linux-shorewall-P1, Julio 2013.

[6] Pello Info, IPTABLES manual práctico, http://www.pello.info/filez/firewall/iptables.html, Octubre 2013.

[7] Wikipedia, OpenVpn, http://es.wikipedia.org/wiki/OpenVPN, Octubre 2013.