Esquema de accesibilidad a servicios digitales del ITC mediante una red virtual privada con seguridad

Julio Armando Asato España
Instituto Tecnológico de Celaya
julio.asato@itcelaya.edu.mx

Juan Ignacio Cerca Vázquez
Instituto Tecnológico de Celaya
nacho@itcelaya.edu.mx

José Jesús Sánchez Farías
Instituto Tecnológico de Celaya
jesus.sanchez@itcelaya.edu.mx

Mayra Ortiz Nava
Instituto Tecnológico de Celaya
mayra.ortiz100@hotmail.com

Resumen

En el presente artículo se sintetiza el proceso y resultados del trabajo desarrollado en el marco de proyecto de investigación titulado “Presentación de un esquema de accesibilidad a servicios digitales del ITC mediante una red virtual privada con seguridad“, con clave de registro CLY-ISC-2013-635. El cual ofrece una alternativa tecnológica para acceder a recursos digitales, controlados mediante direcciones IP (Protocolo de Internet), de una manera regulada y segura. A lo largo de este documento se abordará inicialmente la oportunidad del trabajo a distancia mediante el uso de recursos digitales, así como la problemática de control que esto representa;

posteriormente se tratará sobre la manera en que fue abordado el proyecto y el método empleado para su desarrollo; posteriormente está la propuesta funcional que fue considerada para la instrumentación de las acciones, seguida de los resultados operativos obtenidos y las conclusiones a las que se llegó respecto a la experiencia adquirida en el desarrollo de estos trabajos.

Palabra(s) Clave(s): redes de computadoras, VPN, seguridad, conectividad.

1. Introducción

El trabajo a distancia es una oportunidad que hace referencia a realizar actividades mediante una conexión al lugar de trabajo desde una ubicación remota con la ayuda de las TICs (Tecnologías de la Información y Comunicación). Esto es técnicamente posible debido a las conexiones de Internet de banda ancha, redes privadas virtuales (VPN por sus siglas en inglés) y tecnologías más avanzadas, incluidas la de voz sobre IP y las videoconferencias, de manera que ya no es obligado estar físicamente en un lugar para poder participar activamente.

Cualquier solución de conexión a distancia mencionada permite ahorrar dinero que, de otro modo, se gastaría en viajes, infraestructura y soporte de instalaciones, lo que permite aprovechar las oportunidades de conectividad de las herramientas tecnológicas existentes, en horarios que resulten apropiados para las actividades que deben realizarse (Odom, 2008).

Con los diferentes esquemas de trabajo a distancia se tienen las siguientes ventajas organizacionales:

- Continuidad de las operaciones.
- Mayor capacidad de respuesta.
- Acceso a la información en forma segura y confiable.
- Integración económica de datos, voz, video y aplicaciones.
- Nuevas oportunidades de productividad.
- Satisfacción y retención de empleados.

Todas estas ventajas representan beneficios directos importantes para las organizaciones de carácter industrial y comercial, sin embargo, también las instituciones

de educación superior (IES) así como los centros de investigación y desarrollo tecnológico pueden beneficiarse con el uso de estas tecnologías.

Como parte esencial de su quehacer, el Instituto Tecnológico de Celaya (ITC) forma parte del Consorcio Nacional de Recursos de Información Científica y Tecnológica (CONRICYT), lo que le permite tener acceso a los materiales y publicaciones de las más de treinta casas editoriales inscritas en el consorcio, la cuales incorporan información científica de actualidad, bases de datos y revistas científicas reconocidas en el circuito científico mundial.

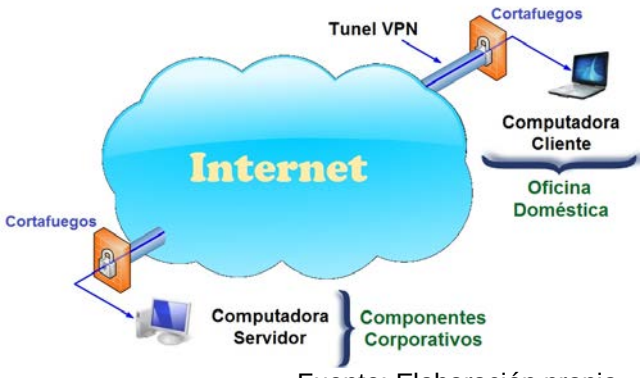
Sin embargo y por razones de seguridad, en diferentes instancias editoriales se establecen restricciones de acceso adicionales al tradicional registro de usuarios, de manera que el permiso de acceso a los materiales publicados está limitado a ingresos desde las direcciones IP del ITC, de manera que se requiere que el investigador se encuentre físicamente en el Instituto para poder establecer una conexión con los portales de algunas casas editoriales. Sin embargo, mediante recursos tecnológicos como la VPN es posible que de una manera segura y controlada, sea posible establecer un enlace desde una localización remota al ITC para poder trabajar como si se estuviera en el Instituto. La VPN es una tecnología de red que permite crear una extensión de una red local sobre una red pública no controlada como lo es la Internet. Para hacerlo posible de manera segura es necesario contar con una serie de elementos que permitan garantizar lo siguiente (Ferrer, 2004):

- Autenticación y autorización: Es tener la certeza de quién es el usuario o equipo que se encuentra al otro lado de la conexión y determinar qué nivel de acceso debe tener.
- Integridad: Es la garantía de que los datos enviados no han sido alterados deliberada o accidentalmente en el trayecto.
- Confidencialidad: Como los datos viajan a través de un medio incierto como lo es la Internet, los mismos son susceptibles de ser interceptados, por eso es fundamental el cifrado de los datos. De este modo aunque sea interceptada la información, esta no podrá ser interpretada más que por los legítimos destinatarios de la misma.

Para poder conectarse efectivamente a la red objetivo, los usuarios de una VPN necesitan dos conjuntos de componentes clave, los componentes de la oficina doméstica y los componentes corporativos:

- Componentes de la oficina doméstica: Son una computadora personal, acceso de banda ancha a internet, servicio de cortafuegos y un enrutador VPN o bien software cliente de VPN instalado en la computadora, un componente adicional podría ser un punto de acceso inalámbrico. Durante los viajes, los usuarios a distancia necesitan una conexión a Internet y un cliente VPN para conectarse a la red corporativa por medio de cualquier conexión de banda ancha, red o acceso telefónico disponible.
- Componentes corporativos: los componentes corporativos son enrutadores y concentradores con capacidad de VPN, cortafuegos u otras aplicaciones de seguridad, componentes de autenticación y dispositivos de administración central para la unificación y la terminación flexible de las conexiones VPN.

Con estos elementos la tecnología VPN permite que las organizaciones creen redes privadas en la infraestructura de Internet pública con un alto nivel de confidencialidad y seguridad, los datos transmitidos están encriptados y ninguna persona que no esté autorizada puede descifrarlos. Las VPN permiten acceder a datos de servidores remotos hasta el cortafuego local con los mismos niveles de acceso como si estuvieran en una oficina corporativa, como puede apreciarse en la figura 1.



Fuente: Elaboración propia.

Figura 1 Esquema de operación de una VPN.

Las organizaciones usan las redes VPN para proporcionar una infraestructura de red de área amplia virtual que conecta sus sucursales, oficinas domésticas, oficinas de socios comerciales y trabajadores a distancia con la red corporativa, de esta manera se benefician con el aumento en la flexibilidad de las operaciones y la productividad resultante. Los sitios remotos y los usuarios a distancia pueden conectarse de manera segura a la red corporativa desde casi cualquier lugar.

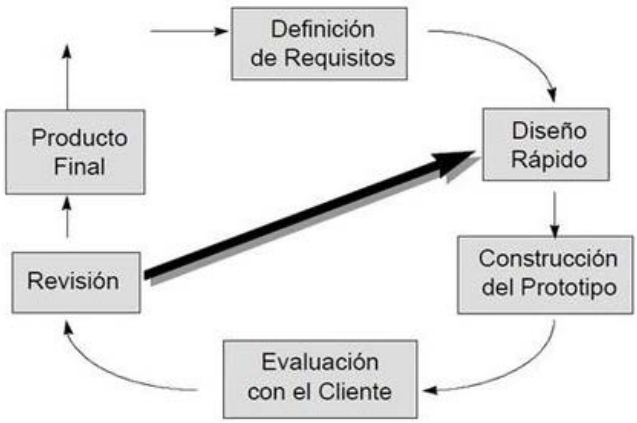
En el caso particular del ITC la construcción de una VPN permitirá que la comunidad tecnológica participe en los beneficios de las suscripciones del CONRICYT, a las bibliotecas en trabajos colaborativos y en segunda instancia, permitirá fortalecer los servicios de comunicaciones que demandan los tiempos actuales.

2. Método

En este proyecto lo que se busca es la integración y evaluación de diversos elementos tecnológicos existentes, el método aplicado es el denominado “Construcción de Prototipos”, el cual es una forma práctica para identificar y atender con rapidez necesidades específicas. El prototipo es un modelo susceptible a ser evaluado u operado a fin de avanzar gradualmente bajo circunstancias donde la información disponible sobre el asunto a tratar no ha sido definida o probada en su totalidad. Al ser un método iterativo es posible repetir las labores de diseño, construcción, prueba y evaluación las veces que sea necesario hasta alcanzar a obtener un producto satisfactorio (Frey y otros, 2014). Como se observa en la figura 2, los pasos para el método de prototipos implican las siguientes actividades:

1. Definición de requisitos y características necesarias que deberá tener el sistema a desarrollar.
2. Diseño de un prototipo que satisfaga aspectos esenciales identificados en los requisitos. A partir de un segundo ciclo, podrán satisfacerse aspectos secundarios además de mejorar las características previamente atendidas.
3. Construcción del prototipo funcional, el cual no necesariamente deberá tener todas las características indicadas en los requisitos en una primera instancia.
4. Prueba del prototipo de acuerdo a las características implementadas, esta etapa deberá realizarse en coordinación con el cliente o usuario.

5. Evaluación del prototipo a fin de definir las nuevas características a considerar, tras lo cual se regresa al paso dos para un nuevo ciclo; o bien si ya cumple con lo establecido, se continúa en la etapa seis.
6. Entrega del producto final, verificando con el cliente las características solicitadas y su debido cumplimiento en el producto, así como las actividades para la formalización de la entrega final.



Fuente: Frey y otros (2014).
Figura 2 Esquema del método de construcción de prototipos.

Este proceso resulta aplicable en situaciones donde los requisitos iniciales están definidos pero no con un nivel de detalle suficiente para completar el desarrollo en un solo ciclo, habiendo casos donde es necesario evaluar un resultado antes de definir, diseñar e implementar el paso siguiente. Otra alternativa de aplicación de este método es cuando el proyecto implica pruebas sucesivas sobre características que deben cubrirse de manera progresiva. De manera particular, en este proyecto se realizaron tres ciclos sobre los siguientes aspectos:

- Ciclo 1: Establecimiento de conectividad entre el cliente y el servidor.
- Ciclo 2: Verificación de la seguridad del enlace.
- Ciclo 3: Evaluación operativa de la conexión VPN de acuerdo al propósito deseado.

Cabe señalar que en todo momento las actividades se realizaron en estrecha colaboración con nuestro cliente, que en este caso se trató del Departamento de Centro

de Cómputo del Instituto Tecnológico de Celaya, quien a final de cuentas ofertará y coordinará la implantación de este servicio.

3. Propuesta

Los accesos a los servicios Institucionales para el trabajo a distancia mediante una VPN ofrecen a los usuarios del ITC la disponibilidad de enriquecer su quehacer de forma constante, las VPN proporcionan algunas de las características deseables para realizar desde ubicaciones remotas diferentes actividades de la gestión basada en web. Para la implementación práctica de este servicio deberán tenerse las siguientes consideraciones:

- La creación y gestión redes virtuales mediante solicitud, según se necesite y sea autorizado, ya que este recurso evidentemente no será proporcionado de manera masiva.
- Procedimientos de distribución centralizada de software para evitar situaciones de descarga de versiones no probadas, con problemas de compatibilidad o con seguridad comprometida por la potencial presencia de software malicioso.
- Ágiles métodos de instalación del software para la oficina doméstica, bastará con enviar a los usuarios finales un vínculo para que descarguen e instalen el software del cliente, además de los archivos de acceso para participar en una red virtual específica.
- Gestión y restauración de redes virtuales para usuarios, desde cualquier sitio a través de la web, a fin de proporcionar soporte técnico, verificar vigencia y resolver problemas operativos.
- Establecimiento de un conjunto de políticas que regulen el control de acceso a los recursos privados en la red local del ITC. Una vez que un usuario sea registrado se definirá a qué recursos de la red puede tener acceso. La VPN gestionará la sesión del usuario, permite el acceso a los recursos autorizados, así también impide el acceso a los recursos no autorizados.
- Administración de claves para asegurar la integridad de una clave pública, ésta es proporcionada al usuario junto con un certificado, que es una estructura de

datos firmada digitalmente por una organización conocida como Autoridad de Certificación (CA por sus siglas en inglés). Una CA firma su certificado con su clave privada. Un usuario que utiliza la clave pública de la CA podrá comprobar que el certificado le pertenece a dicha CA y por lo tanto, la clave pública es válida y aceptada.

- Administración del ancho de banda que se hace con el fin de que el tráfico de la red fluya de forma eficiente. Para esto se utiliza un software específico llamado EXINDA, garantizando al usuario que el acceso a los recursos de la red privada sea de forma eficiente y controlada.

La construcción del prototipo se realizará con el software de administración de VPN llamado OpenVPN, el cual es una solución de conectividad basada en software que ofrece conectividad punto-a-punto con validación jerárquica de clientes y servidores conectados remotamente. El software OpenVPN es buena opción en tecnologías Wi-Fi (redes inalámbricas) y soporta una amplia configuración como el balanceo de cargas. También significa que es capaz de enlazar un nodo A (servidor) conectado a una red privada y a Internet, con un nodo B en cualquier otra parte del mundo con conexión a Internet, de forma que parezca que están en la misma red privada.

Esta tecnología ha sido desarrollada por la organización OpenVPN Technologies Inc. Bajo la modalidad de software libre y es distribuida mediante los términos de Licencia Pública General de GNU, siendo una solución de costo cero (para adquisición) la cual ha sido mejorada desde su primer lanzamiento en el año 2001. Por la manera en que ha sido desarrollado el software OpenVPN, es posible conectarse al servidor de VPN desde clientes con sistema operativo Linux, así como de Microsoft Windows.

4. Resultados

Se realizó el análisis técnico del requerimiento planteado y se evaluaron diferentes tecnologías disponibles para su implementación, dentro de esta etapa se cubrieron los tres ciclos considerados en el método de trabajo para establecer la conectividad, evaluar la seguridad y probar la funcionalidad de la propuesta. Para ésta última etapa las verificaciones realizadas contemplaron los siguientes aspectos:

- Realizar una prueba de conexión desde una ubicación con internet doméstico.
- Realizar una prueba desde un lugar con internet abierto (sitio público).
- Realizar una prueba desde un lugar con internet controlado (con servidor proxi o cortafuegos), ajeno al ITC.

En todos los casos se verificó que pudiera establecerse de la conexión y se tuviera acceso seguro a recursos restringidos por dirección IP. Para efecto de documentar los resultados del proceso se desarrollaron los siguientes manuales:

- Creación del certificado de cliente VPN para el servidor OpenVPN: Este manual es para uso exclusivo del Departamento de Centro de Cómputo, quien tiene la función de ser un CA. En el documento se explica la manera en cómo se hace el registro de un cliente autorizado a utilizar la VPN así como la obtención de su certificado y llave de acceso.
- Instalación del cliente: En este documento se explica la manera de instalar el software del lado del cliente, utilizando el software OpenVPN versión 2.3.0-I004, la instalación del certificado proporcionado por la instancia administradora de la red y la configuración del enlace VPN.
- Manual de usuario VPN: Es un documento de ayuda general para la operación del esquema de la red privada virtual, en él se explican aspectos operativos de la implementación.

Aunque la propuesta tecnológica ya fue integrada y probada, es conveniente puntualizar que la operación de este servicio en particular está sujeto a las políticas y reglas que a ella correspondan, las cuales son competencia del Departamento de Centro de Cómputo del ITC, sin dejar de lado que la idea básica aquí planteada puede replicarse en otros lugares bajos sus propias necesidades.

5. Discusión

Al implementar una solución de red remota, el Instituto ahora cuenta con un medio de acceso controlado a los recursos y a la información, permitiendo la libertad a los usuarios remotos para que accedan a los recursos institucionales de la red local, así

como permitir que las oficinas remotas se conecten entre sí para compartir recursos e información. La solución garantiza la privacidad e integridad de los datos al viajar a través de internet público, así como a través de la red local institucional.

Con la tecnología VPN también será posible establecer canales de acceso controlados y seguros para efecto de actividades de investigación y desarrollo tecnológico ligadas a empresas, ya que los investigadores y profesores sólo necesitarán contar con un cliente de conexión VPN en su equipo portátil para poder compartir información, servicios y aplicaciones como si estuvieran en un aula del instituto, lo cual aplica para proyectos desarrollados con empresas con las que se tienen convenios, trabajos de residencias profesionales, entre otras actividades de docencia, vinculación e investigación.

Otra aplicación potencial es el uso de los equipos de videoconferencia institucionales en donde se puede aprovechar la VPN para implementar telepresencia entre grupos disciplinarios de investigación sin importar el campus donde se encuentren, eventualmente pudiendo realizarse desde el mismo domicilio de los investigadores.

Sin embargo aunque la tecnología y resultados están desarrollados, es ahora turno de los interesados generar propuestas de aplicación del servicio, de manera que los usos potenciales que aquí se han presentado puedan materializarse en beneficios tangibles para la comunidad tecnológica del ITC.

Bibliografía

[1] AENOR (2010). Norma UNE 166000: Terminología y definiciones de las actividades de I+D+i. Asociación Española de Normalización y Certificación. España: http://www.aenor.es/aenor/normas/buscadornormas/buscadornormas.asp

[2] FERRER, DAMIÁN. (2004). VPN, Una introducción a las redes privadas virtuales. Kriptópolis, Revista electrónica de criptografía y seguridad. España: http://www.kriptopolis.com/.

[3] FREY, ADAM y otros. (2014). Método de construcción de prototipos. Wikispace soportado por Tangient LLC: http://metodologiasistemasinf.wikispaces.com/M%C3%A9todo+de+construcci%C3%B3n+de+prototipos.

[4] PLAZA GARCÍA, INMACULADA. (2010). *Calidad en actividades de I+D+i. Aplicación en el Sector TIC*. México. Alfa Omega Grupo Editor.

[5] TOBÓN, SERGIO y otros. (2006). *Manual para el diseño del plan docente acorde con el EEES*. Universidad Complutense de Madrid. España.

[6] ODOM, WENDELL. (2008). *CCNA ICND2 Official Exam Certification Guide.* Segunda Edición. Cisco Press.