Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i1.278

Seguridad con IP seguro en internet (IPSEC)

Internet Secure IP Security (IPSEC)

Segurança IP segura na Internet (IPSEC)

Viviana Vanessa Aparicio-Izurieta
Universidad Técnica Luis Vargas Torres de Esmeraldas, Ecuador
viviana.aparicio@utelvt.edu.ec
https://orcid.org/0000-0002-1417-2036

RESUMEN

Antes de IPSec, las soluciones disponibles en el mercado para lograr una transmisión segura de datos a través de Internet sobre IP dependían de la aplicación del fabricante; En otras palabras, son decisiones aisladas. Aunque generalmente funcionan bien, tienen el problema de que los protocolos estables de diferentes fabricantes no son compatibles entre sí o son difíciles de conciliar; Si la organización y todos los actores con los que interactúa están utilizando la misma solución tecnológica, no debería haber ningún problema. Sin embargo, el punto común es que existe algún tipo de heterogeneidad relacionada con los dispositivos de comunicación, sistemas operativos, facilidades de transmisión de datos, etc., lo que significa que utilizar una solución de estabilización propietaria no es muy conveniente.IPSec, publicado en 1994 en RFC 1636, ha superado ingeniosamente esta incompatibilidad, ya que se basa en estándares, lo que supone una ventaja a su favor. Su diseño es completamente independiente del sistema operativo, plataforma informática y tecnologías subyacentes utilizadas, por lo que la interoperabilidad está garantizada. Además, está lo suficientemente abierto para incorporar los desarrollos tecnológicos y criptográficos necesarios en el futuro. Tanto es así que está incluido en el marco íntegramente en IPv6.

PALABRAS CLAVES: protocolo, seguridad, confidencialidad, TCP, UDP, red de comunicación, integridad, disponibilidad, cifrado, paquete IP, encapsulado, técnicas seguras, encriptación

ABSTRACT

Before IPSec, the solutions available on the market for secure transmission of data over the Internet over IP depended on the manufacturer's application; In other words, they are isolated decisions. Although they work well, they have the problem that stable protocols from different manufacturers are not compatible with each other or are difficult to reconcile; If the organization and all the actors it interacts with are using the same technology solution, there should be no problem. However, the common point is that there is some kind of heterogeneity related to communication devices, operating systems, data transmission facilities, etc., which means that using a proprietary stabilization solution is not very convenient. IPSec, published in 1994 in RFC 1636, has ingeniously overcome this incompatibility, as it is based on standards, which is an advantage in its favor. Its design is completely independent of the operating system, computing platform and underlying technologies used, so interoperability is guaranteed. In addition, it is open enough to incorporate the necessary technological and crypto developments in the future. So much so that it is included in the framework entirely in IPv6.

KEY WORDS: protocol, security, confidentiality, TCP, UDP, communication network, integrity, availability, encryption, IP packet, encapsulation, secure techniques, encryption.

INTRODUCCIÓN

Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i1.278

Si bien esto es cierto hoy en día, vivimos en un mundo donde prevalece la necesidad del intercambio constante de información a través de Internet e intranet, muchas veces más esta información debe mantenerse confidencial, por lo que se debe proporcionar un medio para garantizar la seguridad de su transmisión.

De tal manera que en el presente artículo se desarrolla un estudio de la Seguridad con IP seguro en Internet (IPSec), el cual tiene muchas características y cualidades que satisfacen las obligaciones de protección, confidencialidad y autenticidad de la información en la red.

El fin de este análisis es que, utilizando ayudas instructivas, permita facultar el estudio y la comunicación del protocolo IPSec en internet, permitiendo proteger la comunicación en las organizaciones y evitar eventuales riesgos a los sistemas de información y de esa manera asegurar la pureza de la información de las diferentes entidades, a través del estudio y análisis de dicho protocolo.

Es de vital importancia indicar que cuando se habla de la palabra “seguro”, no se refiere solo de la confidencialidad de las comunicaciones, sino también de la integridad de los datos, que es específica de muchas empresas y entornos de comercio, que puede ser una preocupación importante, donde los requisitos son más críticos que la confidencialidad. De modo que, es fundamental conservar la solidez y seguridad de los sistemas, porque los efectos de un ataque informático pueden comprometer con la integridad de la información.

El problema inicial no solo se trata en el ámbito técnico, sino la conciencia de los peligros latentes en la transferencia de la información con el proceso de las comunicaciones a través de la red y la carencia del entendimiento de los varios ataques informáticos a las entidades. Se podría determinar que la información es de la parte más importante a la hora de tomar decisiones en una entidad. De ahí el valor de proteger las comunicaciones y los sistemas de información para estos sujetos. Con el transcurso del tiempo, se detectan muchas vulnerabilidades con potencial de ser atacadas, y son pocos los responsables de TI que comprenden la importancia de la ciberseguridad para las organizaciones. Como si eso no fuera suficiente, la falta de entendimiento para tratar esta grave situación que se desarrolla por medio de las vulnerabilidades que dan oportunidad a un agresor quebrantar la seguridad de las comunicaciones de una entidad y así tomar esa información para perpetrar delitos.

La metodología de este trabajo es teórica - analítica, la cual se basa en la recopilación de información, de diferentes fuentes bibliográficas que conceptualizan al protocolo IPSec y su importancia a la hora de proteger las comunicaciones sobre el Protocolo de Internet (IP), en la red.

IPSec desarrolla servicios de protección en la capa IP y todos los protocolos IP superiores (TCP y UDP, entre otros) y llena los vacíos de seguridad del protocolo IP. Estos defectos son muy graves, como se ha observado en los últimos años, y afectan la infraestructura de las redes IP. En la actualidad los protocolos apoyados en IP son omnipresentes en las redes de telecomunicaciones, desde cualquier red local normal hasta la propia Internet, confían en este protocolo para funcionar.

La mayoría de los demás protocolos de seguridad funcionan en la capa de aplicación para las comunicaciones de red, mientras que IPsec, dado que funciona a nivel de red en lugar de a nivel de aplicación, puede cifrar todo el paquete IP. Gracias al enfoque dual, IPSec es uno de los métodos más garantizados a la hora de cifrar datos, en tanto que sistemas como SSL funcionan a

Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i1.278

nivel de aplicación, SSL requiere cambios en aplicaciones individuales, pero IPSec solo requiere cambios en el sistema operativo.

La información recolectada del protocolo IPSec, nos permite plantear la problemática del acceso no autorizado a las comunicaciones a traves de internet, tanto desde una perspectiva preventiva con las medidas adecuadas. Con el conocimiento que se ha adquirido tiene una cierta superioridad para hacer frente a la problemática que enfrenta todos los días cuando se trata de seguridad informática.

IPSec se está convirtiendo rápidamente en el protocolo preferido para las entidades, al combinar muchas funciones de cifrado y seguridad juntas, puede garantizar el más alto nivel de privacidad, con el tiempo IPSec parece ser hoy en día, aún más seguro y se ha convertido en el estándar de la industria para la seguridad.

Este trabajo está justificado por la naturaleza y la particularidad del valor de la seguridad informática, donde la labor es proteger las comunicaciones sobre el Protocolo de Internet (IP), y lo fundamental de establecer una formación de seguridad informática corporativa.

Podemos ver la gran importancia de IPSec, así como la forma en que ha sabido combinar características muy importantes para poder brindar seguridad, autenticidad y seguridad en la red.

IPSec, publicado en 1994 en RFC 1636, ha superado ingeniosamente esta incompatibilidad, ya que se basa en estándares, lo que supone una ventaja a su favor. Su diseño es completamente independiente del sistema operativo, plataforma informática y tecnologías subyacentes utilizadas, por lo que la interoperabilidad está garantizada. Además, está lo suficientemente abierto para incorporar los desarrollos tecnológicos y criptográficos necesarios en el futuro.

METODOLOGÍA

La metodología de la investigación son las técnicas y métodos que se aplican en una investigación, para obtener los datos de forma segura y real, en base al estudio y comparación de estos se podrá llegar a una conclusión y resolver la problemática principal de la investigación.

En el presente artículo de acuerdo al objetivo principal se aplica una investigación teórica, en donde sin importar la aplicación práctica o experimental, se recolectan diferentes datos, para generar y fortalecer conceptos. Se ha investigado en diferentes fuentes la funcionalidad y la definición del protocolo IPSec, y como usarlo cuando se trata de las comunicaciones a través de la red. Si nuestra investigación es teórica, la recolección de datos es netamente cualitativa, siendo este otro método de investigación; que proporciona información a base de conceptos y datos cualitativos que permiten profundizar la investigación con casos actuales a los que se enfrentan y están en riesgo las organizaciones y las personas en general.

De acuerdo con el nivel de profundización, la investigación se vuelve explicativa, la cual establece la importancia de implementar el uso de este protocolo en nuestras comunicaciones para la protección de la información, ya que así nos genera un campo de seguridad a favor. Tal es el caso, con el avance tecnológico existen diferentes delitos informáticos, que se aprovechan con las vulnerabilidades que existe en la red de comunicación, como códigos maliciosos, hackers entre otros que son las causas de la problemática (Ataques informáticos); mientras que los

Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i1.278

efectos y consecuencias son las pérdidas financieras, de tiempo, de materiales y entre otras que ocasionan y obstaculizan el cumplimiento de metas institucionales.

Cuando se empieza de conceptos y leyes generales que van a lo mínimo o particular, estamos hablando de una investigación deductiva por el tipo de inferencia que se realiza; este método es aplicado en esta investigación empezando del concepto del protocolo IPSec, los servicios que ofrece IPSec, protocolos que forman parte de IPSec; de estas definiciones se desprenden todas los conceptos y funcionalidades que forman parte del protocolo seguro.

Finalmente, para concluir la investigación se aplica el método de investigación analítico, en donde se descomponen los datos y generalidades, para analizar su naturaleza, causas y efectos y con ello establecer las conclusiones.

TEORIZACIÓN

El Protocolo IPSec

Se define al protocolo IPSec como, "un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado". (Universidad Politecnica de Madrid, 2021)

IPSec es un estándar muy útil que brinda funciones de seguridad en redes IP de todo tipo, compuesto por un grupo de estándares de Internet Engineering Task Force (IETF) que brindan en conjunto servicios de seguridad en la capa IP de los dispositivos de comunicación de sistemas electrónicos, así como todos los los protocolos de nivel superior basados en IP (TCP, UDP, ICMP, etc).

Hoy en día, los protocolos basados en IP son omnipresentes en las redes de telecomunicaciones. Desde cualquier red local normal hasta la propia Internet, confían en este protocolo para funcionar. El problema que afronta IP es la dificultad de asegurar las conexiones. Con la palabra "seguro" se refiere no solo a la seguridad de los sistemas de acceso (que suele ser lo primero que se nos viene a la cabeza), sino también a la creación de medios de comunicación que se pueden prevenir, interceptación y procesamiento de información, también como garantizar la confidencialidad de los datos intercambiados.

Otro punto importante es que las aplicaciones y dispositivos que ni siquiera son compatibles con IPSec en la práctica pueden protegerse, debido a la protección dada en las capas inferiores de OSI.

Aunque muchos administradores de sistemas aún no lo utilizan, hoy IPSec está presente en prácticamente todos los dispositivos de comunicación, sistemas operativos modernos como Windows y otros sistemas operativos como Solaris 10, Linux o MacOS.

Servicios de Seguridad Ofrecidos por IPSec

IPsec es capaz de admitir tareas relacionadas con la seguridad, asumiendo que gestionar todos o solo algunos según las necesidades de cada nodo; por ejemplo:

Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i1.278

- **Control de acceso:** en esta parte se mencionan dos partes fundamentales, autenticación y autorización. La primera parte se utiliza para garantizar que las personas sean correctas en lo que dicen y donde se supone que deben estar.

Por otro lado, la autorización significa que incluso si el interlocutor se autentica, puede acceder a los recursos de la red IP que solicite. Como ejemplo de lo anterior, es posible que un empleado tenga una identificación para acceder a la empresa para la que trabaja, pero esta identificación no es válida para ciertas áreas restringidas a los empleados anteriores. Lo que brinda es semejante o parecido a un firewall con filtrado de paquetes, y se pueden calcular para generar problemas como el protocolo, el puerto, las direcciones IP emisoras y receptoras, así como otras especificaciones para los paquetes.

- **Confidencialidad:** proporciona que se cifre el tráfico de datos y oculte los tipos de comunicaciones. En otras palabras, los datos se transforman carácter a carácter para que un intruso no pueda interpretarlos. Esto asegura que incluso si alguien intercepta la comunicación entre los dos nodos, no podrá descifrar su contenido, lo que incluye la conversión carácter por carácter a través del cifrado.

- **Autenticación e integridad:** si bien ocultar información es importante, la comunicación no es muy eficaz si alguien puede interceptar y modificar paquetes, o los envía fingiendo ser otra persona que no quiere. IPSec permite confirmar que las personas involucradas en la comunicación son en realidad quienes están invitadas. Además, tiene la tarea de afianzar la integridad de los datos, es decir, si alguien los cambia durante la transmisión entre dos partes, los cambios serán identificados y no se les permitirá hacer trampa.

- **Detección redundante**: existe un patrón de ataque que faculta a un delincuente cibernético capturar paquetes (incluso si están debidamente autenticados) y enviarlos varias veces al receptor para su aceptación y, por lo tanto, perturbar la transmisión del mensaje.

Para evadir este tipo de intentos, IPSec integra un sistema de detección de paquetes duplicados. Para hacer esto, utiliza un número de serie que se adjunta al encabezado del paquete y está protegido por la integridad del sistema para que los piratas informáticos no puedan cambiarlo.

Protocolos Básicos de IPSec

IPSec consiste en un conjunto de estándares de cifrado que le otorgan propiedades específicas. Hace uso de algoritmos de passwords públicas como RSA, algoritmos de análisis digital (SHA1 y MD5), certificados digitales X509 y algoritmos de cifrado de password simétrica como DES, IDEA, Blowfish o AES. Todos estos componentes vienen hacer parte de IPSec como pequeñas partes que pueden comunicarse entre sí sin afectarse entre sí. Esto hace posible utilizar todo tipo de algoritmos que existen hoy o en el futuro.

Sin embargo, para lograr la mayor interoperabilidad, las aplicaciones IPSec deben proporcionar al menos algunos elementos estándar que siempre deben ser compatibles. En particular, los algoritmos de cálculo de huellas dactilares (hash) MD5 y SHA-1 y los algoritmos DES y DES triple para el cifrado simétrico utilizando la clave privada seguirán estando disponibles.

El funcionamiento de IPSec depende de la presencia de dos elementos muy importantes:

Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i1.278

- **Un protocolo de gestión de claves denominado IKE (Internet Key Exchange)**, que se encarga de negociar todas las transacciones de seguridad y comunicación necesarias, incluidas, como su nombre lo indica, las claves utilizadas para transferir datos criptográficos.
- **Protocolo de seguridad.** La función principal de este protocolo es proteger el tráfico IP.

El modelo determina dos protocolos de seguridad que se pueden usar con IPSec: **Authentication Header (AH) y Encapsulating Security Payload (ESP)**.

Aquí hay una rápida argumentación de ambos. Es aceptable tener en cuenta que el segundo es más completo y ofrece más funciones que el primero, pero AH a veces es una buena opción si no se necesita privacidad.

El Protocolo de Gestión de Claves

La repartición segura de claves es esencial para el funcionamiento de IPSec, porque si las claves son pirateadas, la seguridad de todas las conexiones se romperá y estarán en manos de cualquier pirata informático. De tal manera es por eso que la durabilidad del mecanismo de intercambio es la base del sistema, antes de analizar el protocolo IKE, es imprescindible aclarar un concepto importante en importante en IPSec: correlación Asociación de Seguridad (SA), SA es un conducto de comunicación que conecta dos puntos, que por medio de ellos se transfiere datos protegidos por cifrado en una dirección.

Es importante enfatizar que SA solo maneja datos en una sola dirección, es decir, de un nodo al otro al que está conectado, y no al revés. Esto significa que cuando establece una relación IPSec protegida entre dos puntos, obtendrá dos tipos de SA, uno para cada dirección.

El protocolo de control IKE es responsable de intercambiar claves entre nodos, acordar qué algoritmos criptográficos y parámetros de control utilizar y establecer enlaces seguros (uno en cada dirección). IKE no es específico de IPSec, pero es un protocolo de administración de claves estándar que se utiliza en otros lugares.

Las negociaciones de comunicación entre dos nodos que utilizan IKE se llevan a cabo en dos etapas. Inicialmente, se crea un canal seguro y los dos nodos se autentican entre sí. Este canal se logra mediante una serie de códigos de cifrado simétrico y una serie de códigos de autenticación de mensajes. La autenticación mutua se logra de dos formas posibles:

1. **Utilización secretos compartidos.** En este caso, los dos nodos que intentan comunicarse deben conocer una determinada secuencia de caracteres que componen el secreto compartido. Mediante funciones de mensajes digitales (hash), cada nodo le manifiesta al otro que tiene presente el secreto sin tener que transmitirlo a través de la red. Para ejecutar este método de autenticación débil, cada par de puntos IPSec debe generar un secreto distinto. Por esta razón, en configuraciones grandes con una gran cantidad de nodos, las claves no se pueden administrar con este sistema y se deben utilizar métodos de autenticación más sólida.

2. **Utilización de certificados digitales.** El uso de un certificado X509v3 permite una distribución de confianza de la clave pública de diferente nodo y resuelve el problema del método anterior cuando están activos múltiples nodos de comunicación segura. Al usar criptografía de clave pública y tener un certificado digital en cada punto o parte, es posible verificar la identidad de uno de ellos usando un par de claves pública / privada. El inconveniente de este planteamiento es que se necesita una infraestructura de clave pública (PKI) para respaldarlo, aunque no es un problema muy complejo de resolver.

Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i1.278

La segunda etapa de las negociaciones de conexión es responsable, después de asegurar el canal seguro IKE y la autenticación, de los factores de seguridad propios que se utilizarán para el resto de la conexión (recuerde que IKE es un protocolo de inicio de sesión común que protege el establecimiento de la conexión con el protocolo de seguridad subyacente, en este caso IPSec). El nodo que inicia la conexión informa al otro nodo de todas las opciones de conexión disponibles (algoritmos criptográficos, sus parámetros, etc.), en orden de prioridad que se haya establecido. Posteriormente, el destinatario acepta automáticamente las primeras opciones proporcionadas por el remitente, correspondientes a las que tiene a su disposición. De ese modo queda establecida la sesión IPSec.

Protocolo de Seguridad AH

El protocolo de encabezado de autenticación (AH) se utiliza cuando es suficiente para garantizar la autenticidad e integridad de los paquetes IP intercambiados en la conexión. En otras palabras, le asegura a la parte receptora que la información que recibió provino de la fuente esperada y que no fue alterada de ninguna manera durante la transmisión. Sin embargo, este protocolo no crea herramientas para garantizar la confidencialidad de los datos, que podrían ser leídos por cualquiera que los intercepte. En algunos casos, esta puede ser una situación aceptable, con total integridad y autenticación de origen. De esta manera, las computadoras que usan IPSec no se sobrecargan al añadir cifrado de datos si no es necesario.

Como sugiere el nombre, AH confía en su trabajo basado en la presencia de la dirección la autenticación se inserta entre la dirección IP estándar y los datos enviados, ya sea TCP, UDP, etc. Su funcionamiento es bastante sencillo, utilizando un algoritmo de validación de mensajes. Es decir, lo que realiza es calcular la huella dactilar o hash de una combinación de una clave, así como el mensaje enviado. Esta huella dactilar identifica de forma exclusiva y sincrónica tanto al mensaje como al remitente, ya que es la única huella dactilar, además del destinatario, que reconoce la password utilizada. Esta contraseña se negocia en el Protocolo de control IKE.

El mensaje resultante o la extracción digital se incluye en el encabezado de verificación que se envía con la información. El punto que recibe, realiza el mismo cálculo en el otro extremo de la conexión porque tiene suficientes elementos para hacerlo (la clave está estandarizada en IKE y el mensaje se envía claramente). Si el extractor (o huella digital) resultante coincide con el encabezado de autenticación, esto significa que el paquete o contenido no se ha modificado en tránsito, ya que solo la forma de conseguirlo es utilizar elementos y claves que solo conocen los dos nodos implicados en la conexión.

Protocolo de Seguridad ESP

El protocolo ESP (Encapsulating Security Payload) aporta seguridad de la que carece el protocolo AH: la confidencialidad. Para eso, se pacta en IKE cómo proteger los datos transmitidos y cómo incluir esta información en los paquetes que se entregan. Como ventaja adicional, ESP puede combinar servicios de integración con autenticación nativa, utilizando tecnología muy similar a la tecnología de protocolo AH.

Este es claramente un protocolo más compuesto que el anterior. Encapsula los paquetes IP enviados utilizando listas y encabezados IP muy complejos, estos elementos contienen los datos que se transmiten y cifran internamente.

La seguridad de la información en ESP se logra mediante un algoritmo de cifrado simétrico (que es menos costoso que los algoritmos de clave pública). Lo más común es utilizar

Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i1.278

un cifrado en bloque como DES o Triple-DES, por lo que el mensaje cifrado debe ser múltiplo del tamaño de bloque mencionado anteriormente. Este hecho a veces te obliga a completar la carta en consecuencia, en este caso, esto también oculta su longitud real antes del cifrado, lo que dificulta el análisis del tráfico.

Este proceso es similar al anterior, dos nodos conectados conocen a uno de ellos la clave que acordaron de antemano. Esto se usa como clave para el algoritmo que encripta los datos antes de que se envíen, y también se usa para generar el encabezado de autenticación. En el lado receptor, se utiliza la misma clave acordada para descifrar el paquete cifrado y verificar la dirección.

Cabe señalar que todo el sistema se bloqueará si no hay forma de intercambiar claves de forma segura. Todos los componentes de IPSec trabajan juntos para lograr un resultado final altamente seguro, aunque cada uno tiene una funcionalidad autónoma que se puede reutilizar en otros momentos.

Modos de Funcionamiento de IPSec

Los protocolos de seguridad estudiados entregan dos modos de operación seleccionables para AH y ESP.

- **Modo transporte** Este modo de operación posibilita la conexión punto a punto entre las partes que desea conectar a IPSec. Se utiliza cuando ambas partes pueden utilizar el protocolo IPSec directamente.

- **Modo túnel**. Este modo se hace uso cuando uno de los dispositivos conectados (uno o ambos) no es responsable de realizar las funciones IPSec.

Este es el método de operación más común cuando se utilizan enrutadores que aíslan las redes privadas de las redes públicas, centralizando todo el proceso del tráfico IPSec en una parte tal cual, por ejemplo, no es necesario implementar o comprender los equipos locales en la red de área local y sus aplicaciones, IPSec, Se comunican normalmente (sin ninguna protección) con el nodo de procesamiento IPSec, y el nodo es responsable de realizar las funciones para todos, conectándose con otro host IPSec en el otro lado o extremo.

Esto protege las direcciones privadas, centraliza la gestión de los protocolos de seguridad en un solo punto e IPSec se puede utilizar en sistemas que inicialmente no están listos para su uso una de las primordiales aplicaciones del modo túnel son crear de forma fácil y económica una red privada virtual (o VPN) en redes públicas, esto permite la comunicación entre ellos, ya sea a través de Internet, una red de área local o computadoras aisladas de ellos, la seguridad garantiza que si están en una red privada, incluso si están usando una dirección IP internamente, no lo harán validas en la red.

Aplicaciones de IPSec en el Día a Día

Una vez que lea este documento, podrá pensar en una gran cantidad de aplicaciones prácticas para IPSec.

Entre ellos:

- **Control de acceso y autorización de comunicaciones**. Con el filtrado IPSec, puede especificar exactamente cómo comunicarse a través de IP con cualquier protocolo de alto nivel. Si los protocolos también son TCP o UDP, es factible inspeccionar lo que se hace con el tráfico

Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i1.278

en función de la dirección IP, los puertos de origen y destino. Obtiene casi las mismas capacidades que los firewalls (ahorro de distancia).

- **Oficinas conectadas de forma segura y creación de intranets distribuidas.** Con IPSec, es posible ejecutar diferentes sucursales y oficinas de una empresa a través de líneas ADSL o ISDN como si estuvieran de hecho en la misma red de área local física y sin la necesidad de una línea punto a punto dedicada: directamente a través de la línea Internet y garantía total. Esto significa un gran ahorro de costes con una gran comodidad.

- **Relaciones seguras con proveedores, distribuidores, socios y otros actores ambientales.** Para el canje de información comercial y técnica, difusión electrónica de datos (EDI) y comercio electrónico entre empresas.

- **Tele trabajo y acceso de viajantes y personal desplazado.** Los empleados que viajen o trabajen desde casa podrán acceder de forma segura a la red de la empresa para buscar en determinadas bases de datos, enviar solicitudes e informes, consultar su correo o calendario interno o visitar el sitio web interno.

DISCUSIÓN

Tras la investigación y en el contexto de la ciberseguridad, se puede acotar que el uso generalizado de Internet y la creciente diversidad de usuarios ha llevado a la necesidad de proteger los tipos de información que circulan en la red. Existen muchas propuestas y alternativas para garantizar la seguridad y confiabilidad de todos los paquetes que pasan por la red. La expansión del mundo de Internet, así como los mecanismos de cifrado disponibles, sin duda facilitarán el desarrollo de nuevas aplicaciones como el comercio electrónico o cualquier actividad doméstica que requiera seguridad como el acceso a datos bancarios, etc.

Por otro lado, se concuerda con el análisis y desarrollo de varios autores, descritos en este artículo, quienes describen el protocolo IPSec, en el cual se aplican una serie de mecanismos de seguridad a la capa IP y se denominan IPSec: Authentication Header (AH: Authentication Header), Encapsulación de seguridad de carga útil (ESP), así como su integración, también protocolos, negociación e intercambio de claves para dos mecanismos de seguridad (enlace de seguridad e intercambio de una llave).

CONCLUSIONES

Este artículo presentó el protocolo IPSec desde una manera teórica y funcional, como también ejemplos de su funcionalidad en el mundo real, se pudo comprobar la gran importancia que tiene IPSec, así como la forma en que logra integrar propiedades que son muy importantes para poder brindar seguridad, confiabilidad e integridad en la red. De la misma forma, que se puede resumir antes y después de la existencia de IPSEC, se puede reconocer que la tecnología ha traído mejoras en la seguridad porque se basa en estándares, es decir, en su diseño independientemente del sistema operativo, de la computadora y las tecnologías subyacentes utilizadas, para garantizar la interoperabilidad.

Estamos en el inicio de la era en la que Internet jugará un papel muy importante en la sociedad y por tanto la seguridad que pueda tener será uno de los principales factores decisivos

Recebido: 03/02/2021
Aceito: 15/02/2021
Disponível: 15/02/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i1.278

porque la mayoría de aplicaciones serán posibles completar datos personales, algunos de los cuales son muy importantes o para realizar transacciones bancarias de gran trascendencia, y saber que existe un protocolo que protege este tipo de transmisión de información promoverá el desarrollo de nuevas aplicaciones y dará prioridad a aplicaciones existentes aquellas que necesitan seguridad y confiabilidad al 100%.

IPSec aún está en proceso de crecimiento y, de esa manera, los mecanismos de seguridad están sujetos a cambios, el futuro de estos mecanismos de seguridad es bastante incierto, con la posibilidad de que nunca se utilicen realmente porque tienden a proporcionar seguridad a nivel de aplicación, donde la seguridad se proporciona de forma transparente a los usuarios.

REFERENCIAS

CactusVPN. (1 de Diciembre de 2021). *CactusVPN*. Obtenido de CactusVPN: https://www.cactusvpn.com/es/la-guia-para-principiantes-de-vpn/que-es-ipsec/

Cysco Systems. (4 de Diciembre de 2021). *Cysco Systems*. Obtenido de Cysco Systems: https://www.cisco.com/

Kent, S. a. (1998). *Security Architecture for the Internet Protocol.* Valencia: RFC 2401.

Kent, S. a. (2021). *IP Encapsulating Protocol* . Valencia: RFC 2406.

Stallings, W. (1995.). *Network and Internetwork Security, principIes and practice.* . New York: Ed. Prentice Hall.

UCL. (10 de Diciembre de 2021). *UCL*. Obtenido de UCL: http://www.cs.ucl.ac.uk/staffIJ/

Universidad Politecnica de Madrid. (4 de Diciembre de 2021). *Universidad Politecnica de Madrid*. Obtenido de Universidad Politecnica de Madrid: https://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec

Anexo 1: