IMPORTANCIA DE UNA CONFIGURACIÓN SEGURA DE LAS REDES PRIVADAS VIRTUALES (VPN) PARA LA INDUSTRIA 4.0

Sandra Justiniano
Escuela de Ingeniería en Computación
ITCA-Fepade Técnicos e Ingenieros
San Salvador, El Salvador
justiniano.beatriz@gmail.com

Erick Girón
Tecnologías de la Información
Rulesware
Antiguo Cuscatlán, El Salvador
erick.giron89@gmail.com

***Resumen*— La implementación de nuevas tecnologías hace que la demanda de seguridad en la transferencia de información sensible sea indispensable. Constamente se buscan alternativas para el establecimiento de canales seguros, que permitan conectar, por ejemplo, dos sitios remotos. La documentación técnica para configurar una red privada virtual (VPN) es extensa, existen diversos fabricantes que se permiten incluir en sus equipos, los asistentes de configuración, adicionalmente, en internet se puede encontrar información variada, sin embargo, los parámetros incluidos y las consideraciones sobre los servicios de seguridad que se desean proporcionar, muchas veces no son congruentes. Por lo que en este trabajo se propone una configuración que permita cumplir con los estándares de seguridad requeridos actualmente y además se presenta una comparación de la configuración de una VPN con IPsec y los tiempos que toman el envío de paquetes, gracias a la emulación de equipos en GNS3.**

Palabras clave—Industria, IPsec, Seguridad, VPN.

I. Introducción

El diseño de nuevas tecnologías, la automatización de procesos, los servicios en la nube, han permitido el crecimiento de las organizaciones, pero, en consecuencia, esto ha provocado que estas deban preocuparse de mantener el acceso a la información estableciendo conexiones seguras a los servidores y otros [1].

Dado el contexto, el desarrollo industrial no es la excepción; la industria se apoya de los avances tecnológicos, estos influyen directamente en la oportunidad de optimización de procesos, no obstante, la implementación de nuevas tecnologías genera que cada vez se vuelva más compleja la demanda de seguridad en la transferencia de información sensible del negocio, constamente se buscan alternativas para el establecimiento de canales seguros, que permitan conectar, por ejemplo, dos sitios remotos [1] [2].

Las redes privadas virtuales (VPNs), son parte de las herramientas más oportunas para definir un canal seguro, en general, permiten garantizar la autenticación, la confidencialidad y la integridad de los datos transferidos en la comunicación, las alternativas para configurarlas son variadas; los equipos que soporten características criptográficas, fácilmente podrán incorporar licencias para la configuración de una VPN.

Sin embargo, la problemática actual de las comunicaciones, es que no existe mucho énfasis en la implementación de estos canales seguros, y ya que la información es extensa y existen múltiples consideraciones al momento de seleccionar los parámetros que darán soporte a los servicios de seguridad demandados, en algunas ocasiones podrían no estar configurados de la forma más apropiada, mostrando algunas debilidades para los procesos de autenticación o garantías de cifrado e integridad; por lo cual, desde un análisis criptográfico del marco de trabajo de IPsec se propone una guía concreta para la configuración de una VPN.

II. Preliminares

A. VPN

Red privada virtual, representa una tecnología de red que permite conectarse a través de una red pública como una extensión de la red de área local [3], [4].

B. VPN sitio a sitio

Utilizadas para las empresas que desean tener dos o más sitios conectados de forma segura, a través de la red pública, tradicionalmente se emplean el marco de trabajo IPsec para estas implementaciones [5], [6].

C. VPN de acceso remoto

Algunos usuarios requieren una comunicación desde sus computadoras hasta las sedes de la organización, para estas se pueden emplear diversas tecnologías como IPsec o SSL-VPN, y algunas soluciones de diversos fabricantes [5], [6].

D. Industria 4.0

La cuarta revolución industrial es la industria 4.0 que se refiere a la transformación digital aplicada a la industria de producción; precisamente se enfoca en la digitalización de los procesos productivos en las fábricas por medio de sensores y sistemas de información para la transformación en procesos más eficientes [1].

E. IPsec

Es un marco de trabajo de estándares abiertos que garantiza la privacidad de las comunicaciones en Internet. Proporcionando confidencialidad, integridad y autenticidad en las comunicaciones de datos. La principal característica de IPsec es que el tráfico IP puede ser cifrado y/o autenticado, esto se realiza mediante túneles virtuales seguros entre dos pares (peers), por ejemplo, dos routers [5].

F. Confidencialidad

Consiste en la capacidad de garantizar que la información, almacenada o transmitida por la red, estará disponible únicamente para personas autorizadas [5], [7].

G. Integridad

Consiste en garantizar que los datos no han sido modificados sin autorización, por lo cual se puede reconocer que la información de la que se dispone es válida y consistente [5], [7].

H. Autenticación

Consiste en el proceso que un usuario debe completar para tener acceso a los recursos de un sistema o una red, implica la identificación (quién es el usuario) y autenticación (verificar que el usuario sea quien dice ser) [5], [7].

I. Cifrado

Es la práctica de codificar y decodificar datos, aplicando un algoritmo criptográfico, estos utilizan una clave de longitud de bits variable [4], [7].

III. Estado del Arte

Dentro de las tecnologías que permiten la creación de VPN se encuentran las conexiones SSL, redes MPLS, o los túneles IPsec; elegir una o varias de las tecnologías dependerá de las necesidades específicas de la comunicación a realizar y de los recursos disponibles para la implementación; sin embargo, es importante remarcar, que todas estas tecnologías buscan satisfacer las demandas de las redes empresariales. La documentación técnica para configurar una VPN es extensa, existen diversos fabricantes que se permiten incluir en sus equipos, los asistentes de configuración, adicionalmente, en internet se puede encontrar información variada.

En la configuración de las VPN sitio a sitio, Cisco, para las VPN configuradas en Router, sugiere la utilización del grupo de Diffie-Hellman (DH) 2, algoritmo DES para el cifrado, y para garantizar la integridad MD5 [8]; sin embargo, ofrece también un método más fuerte que implica la utilización de SHA-1 para la integridad, certificados digitales con RSA para la autenticación, el algoritmo AES con clave de 128, 192, o 256 para el cifrado y grupos de DH 14 y 24 [5]; Sonicwall sugiere la utilización del grupo de DH 14, y para los procesos de autenticación y cifrado se utilice el algoritmo AES con llaves de 128, 192 o 256 bits [9]; Checkpoint presenta una guía de configuración en donde se utilizan certificados digitales para la autenticación, el algoritmo AES con clave de 256 bits para el cifrado, y SHA-1 para la integridad [10]; Microsoft Azure, ofrece la orientación para la configuración de las políticas de IPsec utilizando AES con claves de 256 para el cifrado, SHA-256 para la integridad y grupos DH 24 [11], [12]; Fortinet, el asistente de configuración contiene una plantilla predefinida, en donde únicamente se solicitan los parámetros de red para establecer el túnel [13].

Dado que existen múltiples tecnologías para la creación de VPNs, se puede identificar que el marco de trabajo IPsec proporciona flexibilidad al momento de configurar un determinado tipo, y con parámetros que permiten satisfacer las necesidades de seguridad oportunas a la comunicación.

IV. Desarrollo de la Investigación

IPsec emplea diferentes métodos para la protección de los datagramas IP, entre los cuales se identifican: autenticación del origen de datos, autenticación de la integridad de los datos sin conexión, confidencialidad del contenido del datagrama, protección anti-reproducción. De acuerdo ello, IPsec se apoya de diferentes herramientas criptográficas para cumplir con los servicios de seguridad especificados.

- Proveer integridad, por medio de funciones Hash y HMAC.
- Combinación de autenticación y cifrado de datos (algoritmos de cifrado y funciones Hash - HMAC).
- Función de intercambio de claves por medio del protocolo Diffie-Hellman (DH).

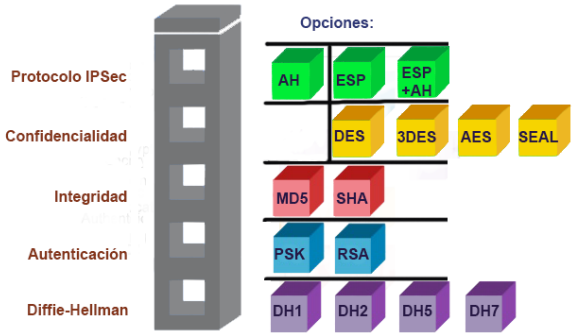

Figura 1. Marco de trabajo IPsec y sus opciones.

Para configurar correctamente una VPN es importante conocer los conceptos asociados a los parámetros que permitirán definir las políticas de seguridad y los mecanismos para el manejo de los paquetes:

- Intercambio de claves de sesión: en el intercambio de las claves de sesión se hace uso del protocolo criptográfico Diffie-Hellman (DH) que permite establecer el *secreto compartido*. DH cuenta con al menos los siguientes grupos: DH1, DH2, DH5, DH14, DH15, DH16, DH19, DH20, DH21, DH24. Los grupos 1, 2 y 5 se considera que no proveen el nivel de seguridad apropiado ante las amenazas más recientes, por tanto, no debe ser utilizado para la protección de información sensible. Si se aplica para la autenticación o cifrado, algoritmos con llaves de 128 bits se utilizan los grupos 5, 14, 19, 20 o 24; si se aplica para la

autenticación o cifrado, algoritmos con llaves de 256 bits o mayores, se utilizan los grupos 21 o 24.

- Integridad y autenticidad de los datos: al garantizar la integridad de los datos se hace uso de los mensajes resumen de los datos del paquete original que viaja con IPsec; estos mensajes se obtienen al aplicar funciones HASH, más específicamente en su construcción con HMAC, pudiendo ser HMAC-MD5 o HMAC-SHA. Por su parte MD5 proporciona un resumen del mensaje con un tamaño de 128 bits, mientras que SHA produce un resumen de 160 bits. MD5 no se considera seguro ya que ha sido vulnerado.
- Método de autenticación de dispositivos: Los extremos involucrados en establecer la comunicación segura por medio de IPsec deben utilizar el protocolo IKE para que, por medio de un proceso de negociación se defina el método para autenticar que se utilizará. Los métodos normalmente aplicados para autenticar son las claves pre-compartidas, haciendo uso de funciones HASH; y la autenticación por medio de firmas RSA, en donde cada extremo firma digitalmente un conjunto de datos, utilizando una autoridad certificadora para otorgar un certificado digital único.
- Cifrado de datos: permite proporcionar confidencialidad, se obtiene empleando algoritmos de cifrado simétricos y claves de sesión. Los algoritmos de cifrados más comunes son: DES, con una clave de 56 bits, 3DES con una clave de 168 bits, y AES con claves de 128, 192 y 256 bits. La seguridad que proporciona un algoritmo recae en la longitud de su clave, por lo cual es recomendable el uso de AES.

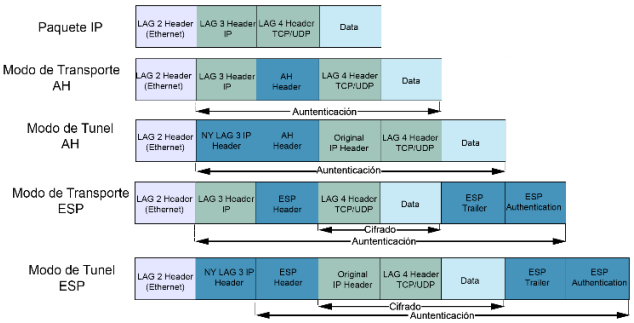

Figura 2. Modos y Encapsulación en IPsec.

Como una guía general, para la definición de una VPN sitio a sitio, se requieren seis pasos.

1) En la fase 1 se requiere crear una política de ISAKMP (Internet Security Association and Key Management Protocol): define los procedimientos de las asociaciones de seguridad (SA – Security Associations), estas contienen la información requerida para la ejecución de servicios de seguridad a nivel de capa de red.
2) Crear llave pre-compartida: es una cadena de texto utilizada en los procesos de autenticación.
3) Crear perfil de ISAKMP: contiene las especificaciones para el manejo de la carga útil del paquete IP.
4) En la fase 2 se requiere definir el set de transformación: contiene la combinación de las transformaciones individuales que tienen lugar en IPsec, cada una para activar las políticas de seguridad específicas para el tráfico.
    a) Un mecanismo para la autenticación de la carga útil (AH transform – permite proveer autenticación e integridad).
    b) Un mecanismo para el cifrado de la carga útil (ESP transform – permite proveer confidencialidad, autenticación e integridad).
    c) Un modo de IPSec, (Modo túnel, se utiliza habitualmente para el cifrado de tráfico en las VPN seguras de IPsec, este modo cifra tanto la carga útil, del paquete, como el encabezado; o Modo transporte, se utiliza únicamente para cifrar la carga útil del paquete, dejando los encabezados intactos).
5) Crear perfil de IPsec.
6) Crear las interfaces túnel y vincular con el perfil de IPsec.

CUADRO I. ALGORITMOS Y FUNCIONES DISPONIBLES PARA ENCABEZADOS DE AH Y ESP

Característica	**AH**	**ESP**
Integridad	MD5 SHA	MD5 SHA
Autenticación	HMAC-MD5 HMAC-SHA1 AES128-XCBC-96	HMAC-MD5 HMAC-SHA HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512 AES-XCBC-MAC
Anti-reproducción	Números de secuencia HMAC-MD5	HMAC-MD5
Confidencialidad	Texto plano	DES 3DES AES AES-CBC AES-CTR
Protección campos de la cabecera	Túnel	Túnel
Modalidad	Túnel Transporte	Túnel Transporte

V. EXPERIMENTOS Y RESULTADOS

Dado que se cuenta con múltiples posibilidades para la configuración de una VPN con IPsec, en diferentes equipos, marcas y asistentes de configuración, se presentan dos

estructuras, en las cuales se han seleccionado determinados algoritmos para los servicios de seguridad especificados, también se muestran los resultados referentes a los tiempos de respuesta de los paquetes; para las pruebas se utilizaron IOS de equipos Cisco emulados en GNS3.

CUADRO II. CONFIGURACIÓN 1

Fase 1					
Autenticación	AES128				
Integridad	MD5				
Grupo Diffie Hellman	14				
Fase 2					
Autenticación	DES	3DES	AES128	AES256	AES256
Integridad	MD5-HMAC	MD5-HMAC	SHA1	SHA256	SHA512
Tiempo Promedio en echo request (ms)	56.2	57.4	55.2	60.2	57.6

CUADRO III. CONFIGURACIÓN 2

Fase 1					
Autenticación	AES256				
Integridad	SHA512				
Grupo Diffie Hellman	24				
Fase 2					
Autenticación	DES	3DES	AES128	AES256	AES256
Integridad	MD5-HMAC	MD5-HMAC	SHA1	SHA256	SHA512
Tiempo Promedio en echo request (ms)	57	58.8	60.8	57.8	60

CUADRO IV. CONFIGURACIÓN RECOMENDADA

Fase 1	
Autenticación	AES256
Integridad	SHA256
Grupo Diffie-Hellman	14
Fase 2	
Autenticación	AES256
Integridad	SHA256

De acuerdo al análisis realizado en las configuraciones de las VPN con los parámetros de los cuadros I y II, y de las características de los algoritmos criptográficos se sugiere la utilización de los parámetros mostrados en el cuadro III, ya que se provee mayor garantía en los procesos de cifrado, autenticación e integridad.

Se sugiere seleccionar modo Túnel, para asegurar todo el contenido del paquete, desde su encabezado; y como protocolo de IPsec ESP, para garantizar el cifrado de la carga útil.

VI. CONCLUSIONES

La robustez de la configuración de una VPN se encuentra directamente vinculada a las características de los principales algoritmos de cifrado, de acuerdo a su modo de operación y la longitud de llaves implementadas; IPsec sugiere el tipo de algoritmos a incluir según el servicio de seguridad que desea gantizarse.

La disponibilidad de ciertos algoritmos y longitudes de llaves están vinculados, también, a las características criptográficas incluidas en los sistemas operativos de los diferentes dispositivos, considerando además las recomendaciones de los fabricantes.

Los resultados del escenario implementado demuestran que las diferencias en RTT (Round-trip time), para los diferentes modos de configuración en la creación de VPNs IPSec entre dos pares, son despreciables así, al contrastar velocidad de cifrado versus fortaleza de los algoritmos a utilizar, es este último factor el más importante a tomar en cuenta al diseñar un túnel VPN IPSec.

Es importante mencionar que la interoperabilidad entre diferentes marcas de equipos conlleva la utilización de diferentes combinaciones de algoritmos y funciones que son parte del marco IPsec, por lo cual es necesario comprender las características principales de cada uno de ellos.

VII. RECOMENDACIONES

Utilizar algoritmos de cifrado y funciones HASH más fuertes y que no hayan sido vulnerados.

Se recomienda la utilización de claves con la mayor longitud posible, para garantizar la fortaleza del cifrado.

Determinar los servicios de seguridad que se requieren garantizar con la configuración de la VPN IPsec, y seleccionar los algoritmos y funciones mas robustos posibles.

Consultar las recomendaciones del fabricante, verificando además las características incluidas en los sistemas operativos de los dispositivos.

Realizar pruebas de la configuración de la VPN con IPsec, e identificar posibles ataques en un entorno controlado, previo a la implementación.

REFERENCIAS

[1] ISOTools, “Industria 4.0: ¿Cuál es la importancia de la estandarización?” Disponible en: https://www.isotools.org/2018/06/13/industria-4-0-estandarizacion/ Junio 2018 [Accedido: Septiembre 29, 2018].

[2] Cluster Industrial, “Ciberseguridad un reto para la Industria 4.0”. Disponible en: https://clusterindustrial.com.mx/post/3566/ciberseguridad-un-reto-para-la-industria-4-0/ Marzo 22, 2018 [Accedido: Septiembre 29, 2018].

[3] L. Cornett, K. Grewal, M. Long, M. Millier, S. Williams, “Network Security: Challenges and Solutions”, Intel® Technology Journal, vol. 14, no. 2, 2009.

[4] W. Odom CCNA, S. Hogg, Routing and Switching, ICND2 200-105 Official Cert Guide, Indianapolis, IN: Cisco Press, 2017.

[5] O. Santos, J. Stuppi, CCNA Security 210-260 Official Cert Guide, Indianapolis, IN: Cisco Press, 2015.

[6] Cisco Networking Academy, “CCNA Routing and Switching: Conexión de Redes v6”, Disponible en: https://www.netacad.com/ 2018 [Accedido: Septiembre 29, 2018].

[7] A. Menezes, P. van Oorschot, S. Vanstone. (1996). Overview of Cryptography. En Handbook of Applied Cryptography(5). CRC Press: CRC Press, Inc.

[8] Cisco Engineers, “Configuration Professional: Site-to-Site IPsec VPN Between Two IOS Routers Configuration Example”. Disponible en:

https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/configuration-professional/113337-ccp-vpn-routerA-routerB-config-00.html/ Noviembre 30, 2011 [Accedido: Agosto, 2018].

[9] Sonicwall, “How to Configure a Site to Site VPN Policy using Main Mode”. Disponible en: https://www.sonicwall.com/en-us/support/knowledge-base/170504380887908/ Mayo 11, 2018 [Accedido: Agosto, 2018].

[10] Checkpoint Software Technologies, “How to Set Up a Site-to-Site VPN with Check Point Gateways Managed by the same Management Server”. Disponible en: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk54060/ Marzo 6, 2018 [Accedido: Agosto 2018].

[11] Microsoft Azure, “Create a Site-to-Site connection in the Azure portal”. Disponible en: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal/ Marzo 4, 2018 [Accedido en: Agosto 2018].

[12] Microsoft Azure, “Configure IPsec/IKE policy for S2S VPN or VNet-to-VNet connections”. Disponible: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-ipsecikepolicy-rm-powershell/ Febrero 13, 2018. [Accedido: Agosto, 2018].

[13] V. Martin, “Site-to-site IPsec VPN with two FortiGates” Disponible en: https://cookbook.fortinet.com/site-site-ipsec-vpn-two-fortigates-56/ Enero 10, 2018. [Accedido: Agosto, 2018].