VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

MAESTRÍA EN GERENCIA DE SISTEMAS

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN GERENCIA DE SISTEMAS

TEMA "DISEÑO E IMPLEMENTACIÓN DE ENCRIPTACIÓN DE LOS DATOS DE COMUNICACIÓN DE UNA ENTIDAD FINANCIERA ECUATORIANA SOBRE EQUIPOS FORTIGATE"

AUTOR: OJEDA BÁEZ, BYRON FERNANDO

DIRECTOR: ING. SALAZAR CHACÓN, GUSTAVO DAVID

SANGOLQUÍ

2019

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, ***"DISEÑO E IMPLEMENTACIÓN DE ENCRIPTACIÓN DE LOS DATOS DE COMUNICACIÓN DE UNA ENTIDAD FINANCIERA ECUATORIANA SOBRE EQUIPOS FORTIGATE"*** fue realizado por el señor ***Ojeda Báez, Byron Fernando***, el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 13 de agosto de 2019

Firma:

.....

Gustavo David Salazar Chacón

C.C.: 1716104797

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORÍA DE RESPONSABILIDAD

Yo, ***Ojeda Báez, Byron Fernando***, con cédula de ciudadanía n° 1722334149, declaro que el contenido, ideas y criterios del trabajo de titulación: ***"Diseño e implementación de encriptación de los datos de comunicación de una Entidad Financiera Ecuatoriana sobre equipos FortiGate"*** es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas. Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, 13 de agosto de 2019

Firma:

.....

Byron Fernando Ojeda Báez

C.C.: 1722334149

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN

Yo, ***Ojeda Báez, Byron Fernando*** autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: ***"Diseño e implementación de encriptación de los datos de comunicación de una Entidad Financiera Ecuatoriana sobre equipos FortiGate"*** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 13 de agosto de 2019

Firma:

.....

Byron Fernando Ojeda Báez

C.C.: 1722334149

DEDICATORIA

Dedico el presente trabajo a mi amado hijo Joaquín que a su corta edad me ha brindado los mejores momentos de mi vida y enseñado que los logros se consiguen con sacrificio y perseverancia, es mi gran inspiración.

A mi esposa Soledad que con su preocupación, amor y dedicación hemos logrado este gran éxito para nuestra familia.

A mi madre que, con su amor, buen ejemplo y apoyo incondicional ha logrado guiarme de forma acertada en cada una de las etapas de mi vida personal y profesional.

A mi padre, por su comprensión y consejos que me orientaron a tomar las mejores decisiones y por creer en mí, y sobre todo por su amor que me brinda.

A mis hermanas y mi sobrino Jhosue, por su gran amor y apoyo en los buenos y malos momento de mi vida.

A mis abuelitas, que desde el cielo guían el rumbo de mi vida, sus enseñanzas siempre serán de ayuda para enfrentar el día a día.

AGRADECIMIENTO

A Dios, por bendecir cada día a mi familia y permitirme disfrutar de este logro junto a ellos.

Un sincero agradecimiento a Gustavo, por toda la guía brindada en la elaboración de este proyecto, así como los conocimientos y experiencia compartida.

A mis compañeros de trabajo por compartir su valioso conocimiento que fue de gran ayuda en el desarrollo de este proyecto

A mis familiares directos y políticos por la motivación que me dieron para finalizar esta meta en mi vida.

ÍNDICE DE CONTENIDOS

ESTADO DEL ARTE

CAPITULO IV

CAPÍTULO V

IMPLEMENTACIÓN DE LA SOLUCIÓN

CAPITULO VI

RESULTADOS

CAPITULO VII

CONCLUSIONES, RECOMENDACIONES

REFERENCIAS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En la actualidad, la encriptación de datos es un tema muy importante para considerar en la red de datos de una empresa, esto debido a que se tiene el temor que esta pueda ser vulnerable a diversos ataques informáticos. Las Entidades Financieras son las más vulnerables, ya que están directamente relacionadas con pérdidas económicas y de confidencialidad tanto para la Empresa como para sus clientes. En la actualidad las Entidades Financieras ofrecen diversos servicios a sus clientes acorde a las nuevas tecnologías como por ejemplo banca electrónica, aplicaciones móviles para realizar diferente tipo de transacciones, por ello se vuelve indispensable robustecer la seguridad en las diferentes comunicaciones que se realicen. En este proyecto se plantea implementar VPNs IPSec en los equipos FortiGate mediante un canal de datos dedicado, con la consideración de que la latencia de la red no se vea afectada. Para desarrollar el presente proyecto se utilizó una metodología aplicada, ya todo el estudio realizado se refleja en una implementación final. Los medios utilizados serán de carácter documental, la recolección de información será de fuentes primarias y secundarias, considerando la confiabilidad de esta, principalmente de artículos científicos, libros, trabajos de titulación y documentación propia de los proveedores de servicios de Seguridad. La implementación de este proyecto ha permitido generar un canal de comunicación seguro (encriptado) en la red de datos de la Entidad Financiera, con una latencia que asegura el correcto funcionamiento de las aplicaciones que posee esta.

PALABRAS CLAVE:

- **ALGORTIMOS DE ENCRIPTACIÓN**
- **REDES PRIVADAS VIRTUALES**
- **IPSEC**
- **ENTIDADES FINANCIERAS**
- **ENCRIPTACIÓN**

ABSTRACT

Currently, data encryption is a very important issue to consider in a company's data network, this is because there is a fear that it may be vulnerable to various computer attacks. Financial Entities are the most vulnerable, since they are directly related to economic losses and confidentiality for both the Company and its customers. Currently, the Financial Institutions offer various services to their customers according to new technologies such as electronic banking, mobile applications to perform different types of transactions, so it becomes essential to strengthen security in the different communications that are made. This project plans to implement IPSec VPNs on FortiGate devices through a dedicated data channel, with the consideration that network latency is not affected. To develop this project an applied methodology was used, and the entire study is reflected in a final implementation. The means used will be of a documentary nature, the collection of information will be from primary and secondary sources, considering its reliability, mainly of scientific articles, books, degree papers and documentation of the Security service providers. The implementation of this project has allowed the generation of a secure (encrypted) communication channel in the Financial Entity's data network, with a latency that ensures the proper functioning of the applications that it has.

KEY WORDS:

- **ENCRYPTION ALGORITHMS**
- **VIRTUAL PRIVATE NETWORS**
- **IPSEC**
- **FINANCIAL ENTITIES**
- **ENCRYPTION**

CAPÍTULO I

INTRODUCCIÓN

1.1. Planteamiento del problema

En la actualidad los ataques informáticos a redes corporativas son cada vez más comunes, sofisticados y de mayor impacto, especialmente a Entidades Financieras, debido al giro de negocio que manejan. Estos ataques se producen por vulnerabilidades que se encuentran presentes en la red de datos, comprometiendo la integridad, confidencialidad e incluso la disponibilidad de la información.

Los ataques pueden ser prevenidos o tratados de forma oportuna, pero para ello es necesario que la Empresa destine los recursos necesarios para contar con una infraestructura robusta y altamente escalable a nivel de hardware y software, así como la implementación de estándares de seguridad vigentes.

El desconocimiento sobre seguridad de la información por parte de los Administradores de Red debe ser corregido de forma permanente, basándose en las nuevas tendencias. Es muy común que las Empresas tengan software y hardware de seguridad obsoletos, generando diferentes vulnerabilidades que son fácilmente aprovechados por los atacantes Informáticos.

De acuerdo con la evolución tecnológica de las Entidades Bancarias, tales como comercio electrónico, aplicaciones móviles, sitios web para realizar transacciones, entre otros, surge la necesidad de garantizar la seguridad en la red de datos con una baja

latencia, ya que el impacto ante cualquier ataque informático o degradación del servicio es muy alto.

Debido a que la red de datos cuenta con equipos FortiGate, se planteó la necesidad de realizar la encriptación de los datos de comunicación mediante la configuración de IPSec en cada una de las sedes, considerando el crecimiento que se tendrá a mediano plazo.

1.2. Justificación

Las Entidades Financieras debido a la criticidad de la información que manejan, requieren que su red garantice confidencialidad, disponibilidad e integridad en la comunicación que se tiene entre sus diferentes sedes con Matriz. A esto se suma que se debe cumplir con la norma de control de las seguridades en el uso de transferencias electrónicas SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103, específicamente con el punto que indica que la Cooperativa debe *contar con una plataforma tecnológica que permita una encriptación sólida* (Superintendencia de Economía Popular y Solidaria, 2017).

La Entidad Financiera asociada a este proyecto tiene implementado en su red, equipos FortiGate como CPEs (Customer Premises Equipment) sin configuraciones que garanticen la seguridad en las comunicaciones, para ello se propuso que las mismas sean mediante redes privadas virtuales IP (IP VPN), con la cual se encriptan los datos que se intercambian en la red de datos.

1.3. Hipótesis

La hipótesis que se plantea se basa en la siguiente pregunta:

¿Qué solución se puede implementar en la red de datos de una Entidad Financiera para asegurar la seguridad en la comunicación de los datos?

Debido a que la red de datos tiene implementado en su red equipos FortiGate, es necesario buscar una configuración que sea soportada en los mismos y asegure la seguridad de la comunicación de datos, buscando una mínima inversión de hardware o software, pero con una alta escalabilidad.

¿Es posible encriptar de forma adecuada los datos en tránsito?

IPSec brinda seguridad al momento de encriptar los datos en tránsito, esto se validará mediante la captura y análisis de este.

1.4. Objetivos

1.4.1. Objetivo General

Implementar una solución de encriptación de datos en una Entidad Financiera Ecuatoriana, mediante la configuración de VPNs, para robustecer la seguridad en la comunicación de datos.

1.4.2. Objetivos Específicos

- Realizar un análisis de la situación actual y revisión sistemática de literatura básica sobre las herramientas de hardware y software para encriptación en canales de comunicación de datos.
- Diseñar la solución de encriptación de datos.
- Implementación de la solución de encriptación de datos

- Capturar el tráfico de la comunicación de datos para obtener la encriptación de estos.
- Realizar pruebas de conectividad para obtener tiempos de respuesta adecuados a la tecnología de última milla.

CAPÍTULO II

MARCO TEÓRICO

2.1. Seguridad de la Información

La información es uno de los recursos más importantes para todo tipo de empresa, ya que ayuda a la toma de decisiones oportunas y adecuadas, la misma es propia de cada una, por ende, cuidar de ella se convierte en algo indispensable ya que los datos son cada vez más importantes tanto para las compañías como para sus clientes.

La información que manejan las entidades financieras es mucho más crítica ya que está de por medio transacciones y consultas de dinero. En la actualidad debido a las nuevas tendencias como banca móvil entre otros, es necesario que las entidades financieras refuercen el tema de la seguridad de la información.

El concepto de seguridad de la información significa proteger la información y los sistemas de información de un acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados**.** Los principales objetivos de la seguridad de la Información son asegurar la confidencialidad, disponibilidad e integridad de la información.

Confidencialidad: únicamente las personas o entes autorizados pueden acceder a una información específica.

Disponibilidad: la información debe estar accesible cuando se la necesite.

Integridad: la información debe ser fiable, es de decir únicamente las personas o entes autorizados pueden modificarla (Soriano) (Oficina de la Seguridad para las Redes Informáticas) (Instituto Nacional de Ciberseguridad). Este objetivo se enfoca en que el canal de comunicación utilizado para las transacciones que realizan los clientes de las Entidades Financieras sea seguro (encriptado), por ello es necesario encriptar el mismo y tiene una estrecha relación con la confidencialidad de la información.

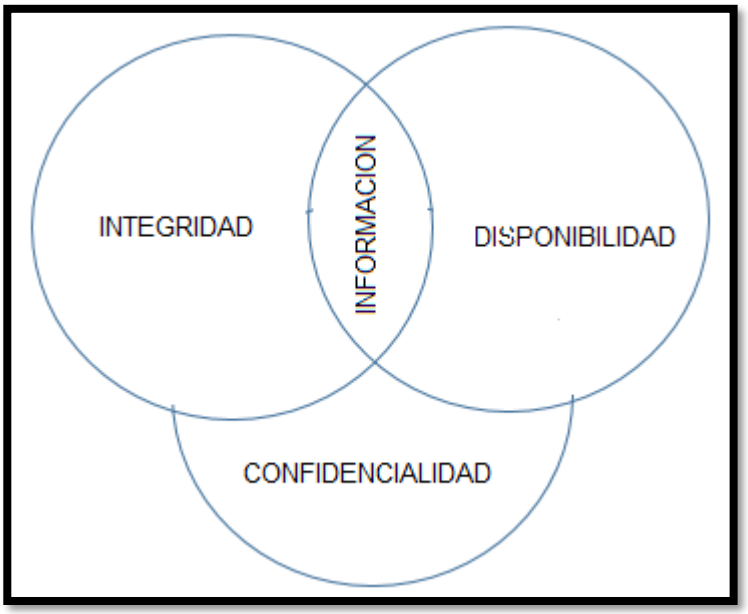

Figura 1. Objetivos Seguridad de la Información
Fuente: (Ribera, 2019)

2.2. Encriptación de Datos

Del griego criptos (oculto) y logos (tratado), la criptología se puede definir como la ciencia que estudia las bases teóricas y las implementaciones prácticas para garantizar la privacidad en el intercambio de información. Desde el origen de las comunicaciones se ha utilizado la encriptación, en los años 100 a.C uno de los primeros métodos de

encriptación fue el cifrado de Cambio de César que surgió con la necesidad de ocultar información escrita en latín por parte del Ejército de Julio César. Consistía en sustituir cada una de las letras del mensaje por aquella que ocupaba tres posiciones más en el alfabeto, debido a su baja complejidad se crearon otros métodos, por ejemplo, tatuar las claves del cifrados en los esclavos (Instituto Nacional de Ciberseguridad) (Alvarez D.) (Alvarez & Solares, 2005) (Damico, 2009).

La criptografía se clasifica históricamente en clásica y moderna:

Clásica: Fue utilizada hasta la mitad del siglo XX y hace referencia a la criptografía no digitalizada. Perdieron su eficacia debido a que son fácilmente criptoanalizables por los ordenadores, todos los algoritmos clásicos son simétricos.

Moderna:

Es importante mencionar los principales beneficios que ofrece la encriptación (ESET).

- Proteger la información confidencial de una organización:
- Proteger la imagen y el prestigio de una organización:
- Proteger las comunicaciones de una organización:
- Proteger dispositivos móviles e inalámbricos:

En la actualidad, para la mayoría de Empresas la encriptación se ha convertido en un proceso esencial en sus actividades diarias, y mucho más para las que brindan servicios financieros, según estudios, las Entidades Financieras gastas tres veces más en seguridad informática que otras organizaciones de otros sectores, ya que se

encuentran bajo presión para robustecer la seguridad debido a las nuevas tendencias como la banca móvil que aumentan el riego de ataques cibernéticos (Kaspersky, 2017) (INTECO).

La encriptación de datos puede realizarse en datos en reposo (guardados en medios físicos) y en datos en tránsito que son los que se encuentran recorriendo una red, el presente estudio se enfoca en este último.

2.3. Algoritmos de Cifrado

Los algoritmos de cifrado modifican la información para asegurar integridad, confidencialidad y autenticación de esta, los mismos se clasifican en:

- **Simétricos**: llamados como algoritmos de clave privada, es decir que encriptan y desencriptan con una única clave secreta, compartida entre emisor y destinatario.

Figura 2. Algoritmo de cifrado simétrico

Fuente: (González, 2006)

- **Asimétricos:** llamados como algoritmos de clave pública, es decir se encriptan con una clave y desencriptan con otra, el emisor y destinatario tiene acceso a la clave pública y cada uno de ellos tiene su propia clave privada

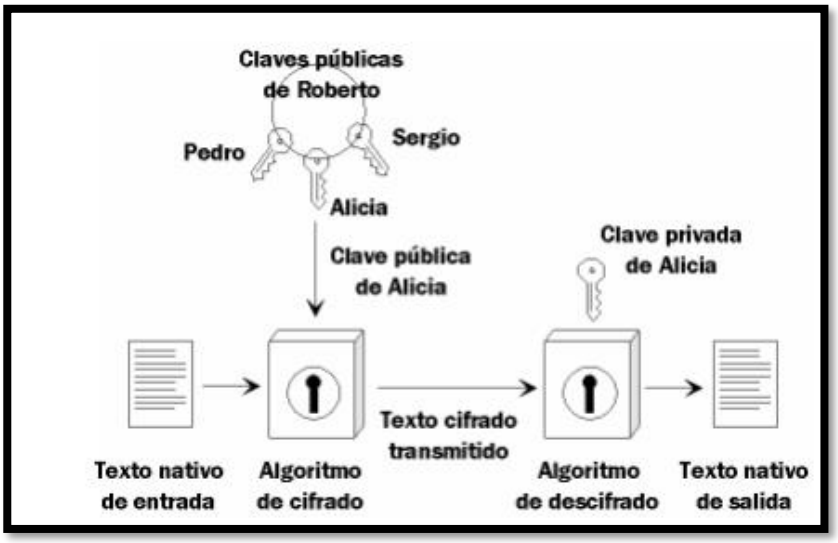

Figura 3. Algoritmo de cifrado asimétrico
Fuente: (González, 2006)

2.4. Redes Privadas Virtuales (VPN)

Muchas empresas tienen sucursales en varias ciudades de un país en inclusive en otros países, en el pasado era común usar canales dedicados (red privada) para conectar los sitios, es decir alquilaban a diferentes compañías telefónicas, en la actualidad todavía se hace uso de estas. Las redes privadas ofrecen una seguridad robusta, pero con costos muy elevados, por ello surge la necesidad de utilizar una red pública para comunicar diversos sitios de una empresa sin descuidar la seguridad informática. Esta necesidad llevó a la invención de las Redes Privadas Virtuales (VPN) que son redes que tienen la apariencia y características similares a las de un canal dedicado, esto debido a que virtualmente se tiene una conexión punto a punto entre el equipo (cliente VPN) y el

servidor de la organización (servidor VPN), pero en realidad se encuentra sobre una red pública.

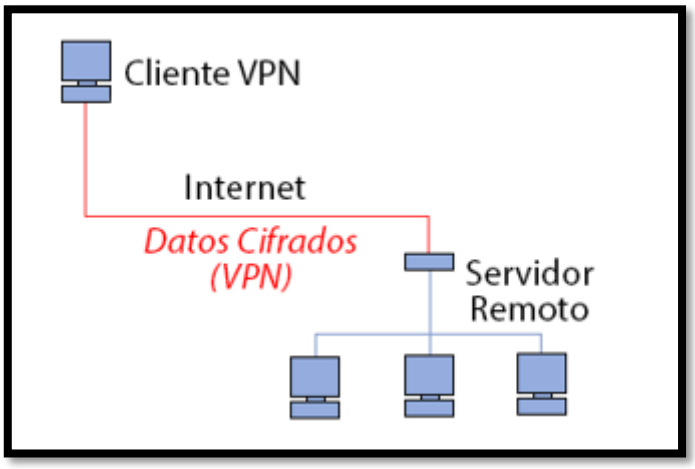

Figura 4. Red Privada Virtual (VPN)

Entre las principales prestaciones que brinda la VPN se tienen las siguientes (Cisco, s.f.).

- Confiabilidad
- Capacidad de conversión a escala
- Administración de la red
- Administración de políticas
- Autenticación
- Encriptación de datos
- Costo menor con respecto a canales dedicados
- Acceso fácil desde cualquier lugar
- Garantiza integridad, confidencialidad y disponibilidad de los datos

Las VPNs acorde a su implementación se clasifican de la siguiente manera (Alonso, Fernández, Figuerola, & Zazo, 2006).

- **Basada en hardware:** el proceso de encriptación lo realiza un equipo dedicado, es decir tiene la VPN incorporada (algoritmos necesarios), brindando mayor facilitad al momento de configurar y gestionar la misma, pero con tecnología externa y cerrada por parte del fabricante, entre los principales podemos mencionar Ovislink, Zyxel Guard.
- **Basada en software:** surge con la necesidad de las Empresas de tener una mayor escalabilidad a un menor costo, así como una mayor gama de opciones con grandes prestaciones.

A continuación, se detalla las VPNs basadas en software más comunes:

SSL (Secure Sockets Layer) /TLS (Transport Layer Security): Ofrece autenticación y privacidad de la información de extremo a extremo sobre internet, son protocolos que se encuentran sobre la capa de transporte. La autenticación se realiza tanto en el cliente como en el servidor, usando claves públicas y certificados digitales que proporciona comunicación segura mediante el cifrado de la información entre emisor y receptor.

Se compone de cuatro protocolos (Tomás & Malgosa, 2008) (Hayoz, 2003) (Cisco Systems, Inc).

- **Protocolo Handshake:** inicia la conexión SSL, siempre el cliente se autentica al servidor, ya sea mediante web o aplicación cliente, este protocolo se encarga de gestionar la negociación de los algoritmos de cifrado y la autenticación entre cliente y

servidor. Define las claves de sesión utilizadas para cifrar. Se podría decir que es un protocolo de autenticación.

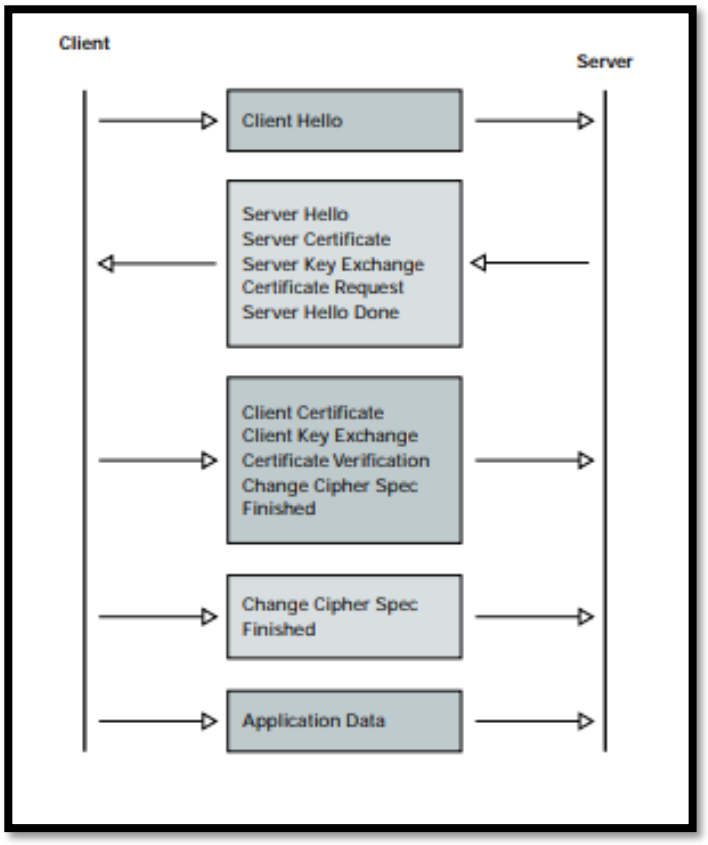

Figura 5. Protocolo Handshake
Fuente: (Cisco, s.f.)

- **Protocolo Change Cipher Spec:** es un mensaje de un byte para notificar

cambios en la estrategia de cifrado, la funcionalidad de este protocolo se usa en la fase final del protocolo handshake, es decir indica que los siguientes mensajes se cifraran con los nuevos parámetros de seguridad establecidos.

Figura 6. Protocolo Change Cipher Spec
Fuente: (Gordon, 2011)

- **Alert Protocol:** señaliza alertas y errores en la sesión establecida, es decir maneja excepciones para las conexiones seguras SSL. los mensajes constan de dos bytes, el primero indica la gravedad de una alerta y el segundo contiene el código de alerta. El valor del primer byte es 1 o 2, donde 1 significa que el mensaje es una advertencia (conexión restringida) y un valor de 2, que es una alerta fatal. Al recibir una alerta de fatal, la conexión debe ser terminada inmediatamente y la sesión actual no puede ser reanudada, el formato del protocolo es el siguiente:

Figura 7. Protocolo Alert
Fuente: (Tomás & Malgosa, 2008)

- **Record Protocol:** encapsula los protocolos de nivel más alto y construye un canal de comunicaciones seguro. Hace referencia a un protocolo de transporte, fragmenta el flujo de datos en una serie de registros protegidos de manera individual y los envía de forma independiente a través del canal.

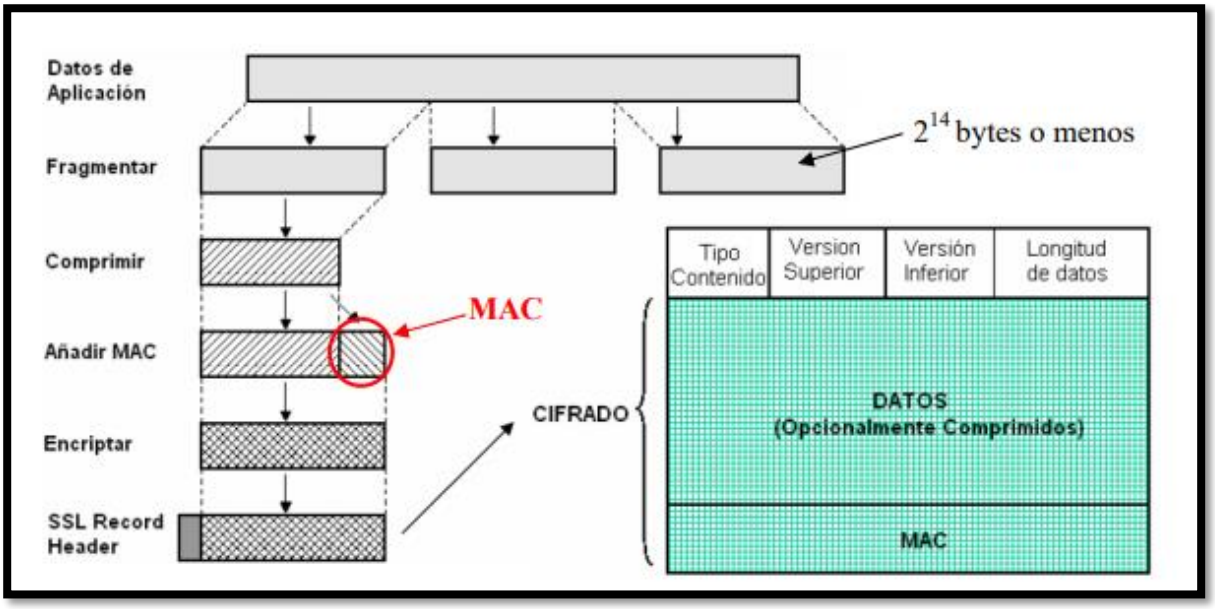

Figura 8. Cifrado y Formato de Datos de Aplicación con Record Protocol
Fuente: (Tomás & Malgosa, 2008)

Es importante tener claro el concepto y diferencia entre conexión y sesión SSL.

Sesión SSL: asociación entre cliente y servidor creada por el protocolo handshake y definida por un conjunto de parámetros de seguridad. Una sesión puede tener varias conexiones, evitando innecesarias negociaciones de parámetros de seguridad para cada conexión.

Conexión SSL: es un enlace de comunicación transitoria y está asociada con una única sesión.

A continuación, se presenta la arquitectura SSL/TLS

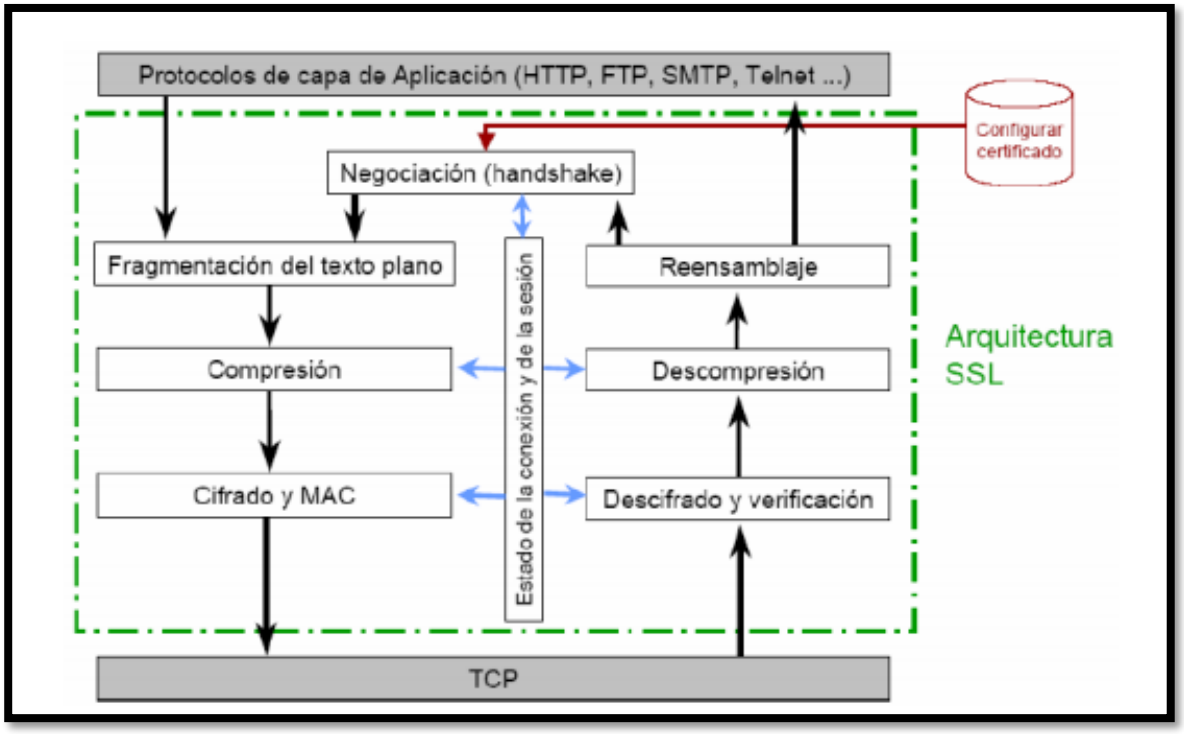

Figura 9. Arquitectura SSL/TLS
Fuente: (Tomás & Malgosa, 2008)

IPSEC (Internet Protocol Security). Es un conjunto de estándares y protocolos que se integran para brindar seguridad criptográfica al protocolo de Internet (IP) y capas superiores, es decir brindando confidencialidad, integridad y autenticidad cada paquete IP en flujo de datos, actualmente se encuentra implementado para IPV4 e IPV6 (obligatorio). Esto se logra mediante la combinación de tecnologías de claves públicas, algoritmos de cifrado, algoritmos de hash y certificados digitales tal y como se observa en la siguiente figura. El uso actual más común es brindar una VPN ya sea entre dos

ubicaciones o entre usuario y red empresarial (Internet Engineering Task Force (IETF) , 2011) (Pérez, 2001).

Figura 10. Tecnologías utilizadas en IPSec
Fuente: (Pérez, 2001)

IPSec brinda las siguientes características de una conexión segura (Cisco Systems, Inc).

Autenticación de pares: Los puntos finales verifican la identidad de cada uno antes de establecer la VPN.

Confidencialidad de los datos: Los puntos finales usan el cifrado para evitar la visualización no autorizada de la información.

Integridad de datos: El punto final de destino confirma que los paquetes recibidos del origen son idénticos a los paquetes que fueron transmitidos.

Autenticación de los datos origen: El punto final de destino confirma que los datos recibidos se originaron a partir del punto final de origen.

IPSec utiliza dos protocolos para proteger los paquetes IP, Authentication Header (AH) y Encapsulated Security Payload (ESP) y uno de gestión de claves Key Exchange (IKE).

PROTOCOLO AH: Garantiza la integridad y autenticación de los datos en tránsito y en casi todos los campos de la cabecera IP (reduce ataques de spoofing), excluyendo aquellos que se modifican en tránsito tales como TTL, TOS, Header Checksum, Flags y Fragment Offset, tal y como se visualiza en la ***Figura 11*** **¡Error! No se encuentra el origen de la referencia.** AH no garantiza confidencialidad, es decir la información puede ser vista por un tercero, ya que no realiza encriptación. El IANA asignó a este protocolo el número 51, es decir el campo protocolo de la cabecera IP es 51. AH se base en el algoritmo HMAC (Hashed Message Authentication Codes), que es un código de autenticación de mensajes que utiliza funciones hash de un solo sentido. HMAC usa una clave secreta para generar el valor del hash que es llamado *extracto*, evitando que un tercero altere el paquete y vuelva a calcular el hash correcto. HMAC utiliza algoritmos de resumen como MD5 y SHA. La seguridad del protocolo HA se fundamenta en el cálculo del extracto, que es imposible saberlo sin conocer la clave (Luján, 2005), (Pérez, 2001), (Cisco Systems, Inc, 2016). En la siguiente figura se describe el funcionamiento del protocolo AH

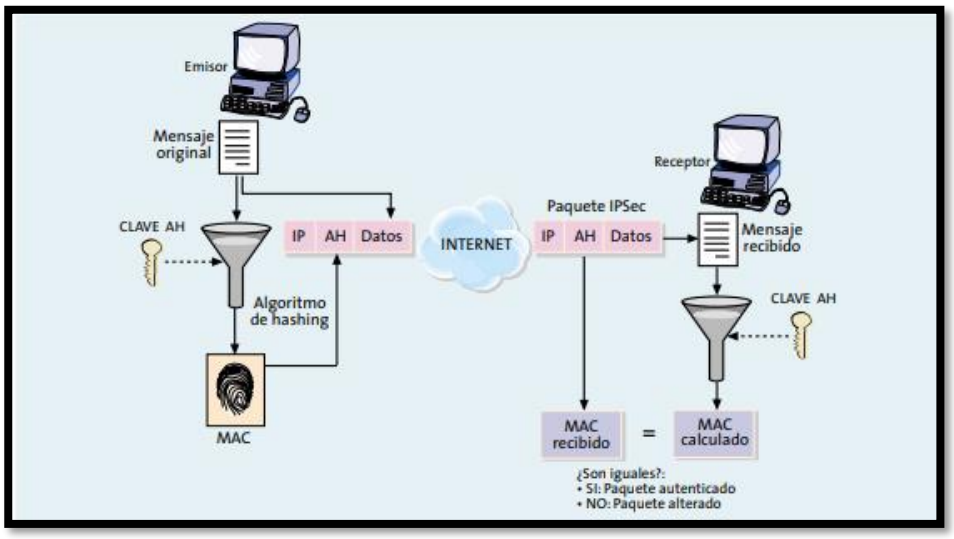

Figura 11. Funcionamiento Protocolo AH
Fuente: (Pérez, 2001)

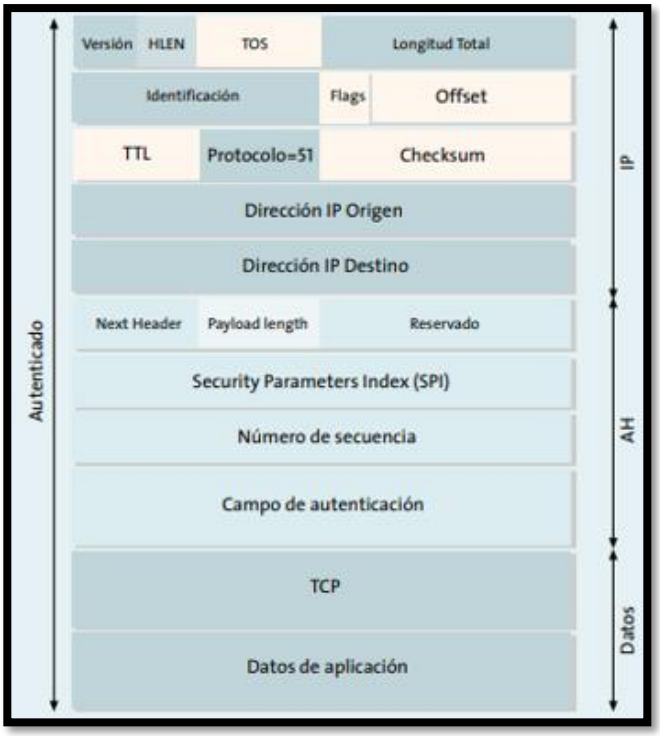

Figura 12. Estructura datagrama Header (AH)
Fuente: (Pérez, 2001)

PROTOCOLO ESP: asignado con el número 50, el objetivo principal del mismo es brindar confidencialidad, es decir asegurar la privacidad de los datos en tránsito usando

técnicas criptográficas, se puede decir que es el core del protocolo IPSec. Puede operar de distintas formas de sólo cifrado, sólo autentificación o ambas, las utilizada es la última por la seguridad que brinda. El cifrado de ESP se realiza con un algoritmo de clave simétrica, en la Figura 13 se muestra la estructura de un datagrama ESP, que es mucho más complejo que el de AH por la funciones que brinda (Araya, Carvajal, & Llico), (Pérez, 2001), (Cisco Systems, Inc, 2016).

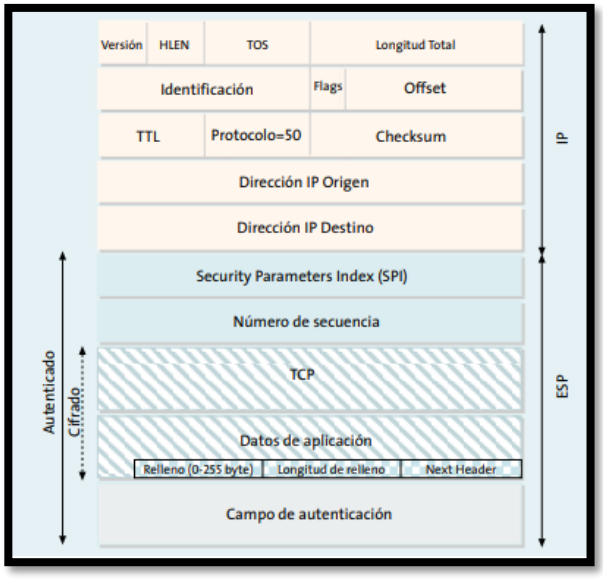

Figura 13. Estructura Datagrama ESP
Fuente: (Pérez, 2001)

En la siguiente figurar se puede visualizar como el protocolo ESP envía datos en tránsito de forma confidencial. La seguridad de este protocolo está ligada a la robustez del algoritmo de cifrado.

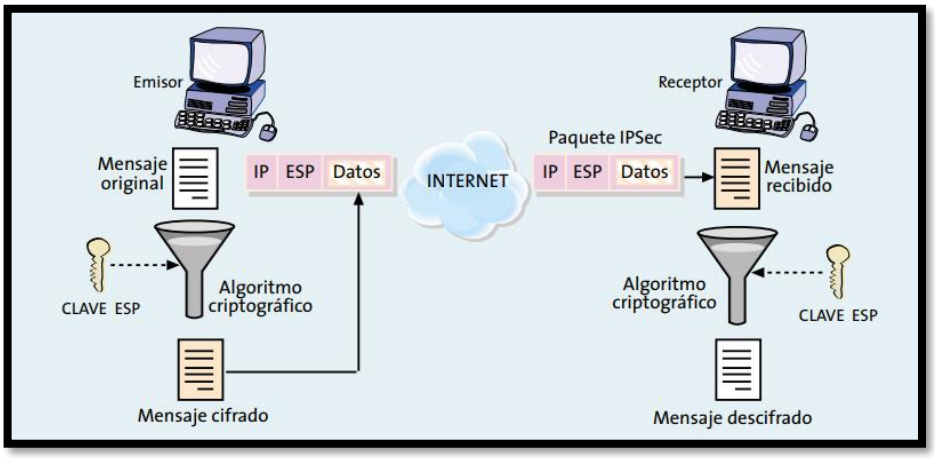

Figura 14. Funcionamiento protocolo ESP
Fuente: (Pérez, 2001)

Es importante mencionar el concepto de asociación de seguridad (SA), que es un conjunto de parámetros de seguridad para la autenticación y el cifrado utilizados por un túnel. Cualquier implementación de AH o ESP debe soportar el concepto de SA.

PROTOCOLO IKE: para la implementación de una VPN con cifrado es necesario cambiar periódicamente las claves de cifrado de la sesión. Si no se cambian estas claves, la VPN puede sufrir ataques de descifrado por fuerza bruta, el protocolo IKE ayuda a resolver este problema. IKE indica mecanismos necesarios que establecen las SA necesarias para asegurar los paquetes entre los dos pares IPSec. El protocolo IKE autentica al peer y luego negocia una política de seguridad compatible antes de establecer el túnel de datos. IKE resulta de la combinación de dos protocolos ISAKMP (RFC 2408) y Oakley, ISAKMP define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE y Oakley especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente. La operación de este protocolo conste de dos fases:

Fase 1: en esta fase se establece un canal seguro y autenticado y se generan claves compartidas para proteger los mensajes del protocolo IKE. Adicional se negocia entre los pares los SA de IKE, que sirven para proteger la comunicación posterior entre los pares.

Cuando se autentica los interlocutores criptográficos acuerdan el algoritmo de cifrado, el método hash y otros parámetros descritos en la Figura 15 (Inside Secure), (Cisco Systems, Inc, 2006), (Rodriguez, 2011).

Parámetro	Valor Aceptado	Keyword	Por Defecto
Algoritmo de Cifrado	DES 3DES AES	des 3des aes	Des
Algoritmo de Integración de Mensajes (hash)	SHA-1 MD5	sha md5	sha-1
Método de Autenticación	Claves precompartidas RSA Firmas RSA	pre-share rsa-encr rsa-sig	Firmas RSA
Parámetros de Intercambio de Claves	Diffie-Hellman 768 bits Diffie-Hellman 1024 bits	1 2	Diffie-Hellman 768 bits
Tiempo de Vida AS	Se puede especificar un numero en segundos		86400 Segundos

Figura 15. Parámetros IPSec
Fuente: (Rodriguez, 2011)

Fase 2: Después de que las negociaciones de la Fase 1 de IPsec finalicen con éxito, comienza la Fase 2. Se puede configurar los parámetros de la Fase 2 para definir los

algoritmos que el equipo puede usar para cifrar y transferir datos durante el resto de la sesión. Durante la Fase 2, selecciona asociaciones de seguridad IPsec específicas necesarias para implementar servicios de seguridad y establecer un túnel.

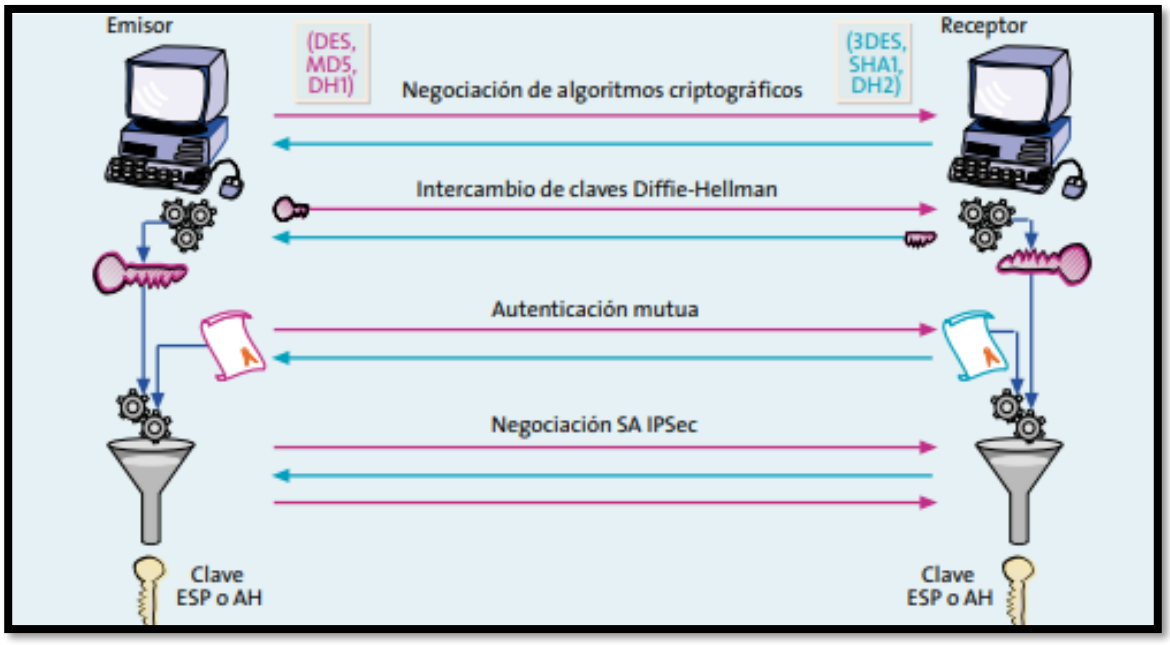

Figura 16. Funcionamiento Protocolo IKE
Fuente: (Pérez, 2001)

Modos de Operación IPSec

Modo Transporte: brinda una conexión segura entre dos puntos finales, ya que encapsula la carga útil de IP (los datos que se transfieren), la cabecera IP no se modifica. En este modo se inserta el encabezado ESP o AH entre el encabezado IP y el siguiente protocolo o la capa de transporte del paquete (Cisco Systems, Inc, 2006), (Inside Secure).

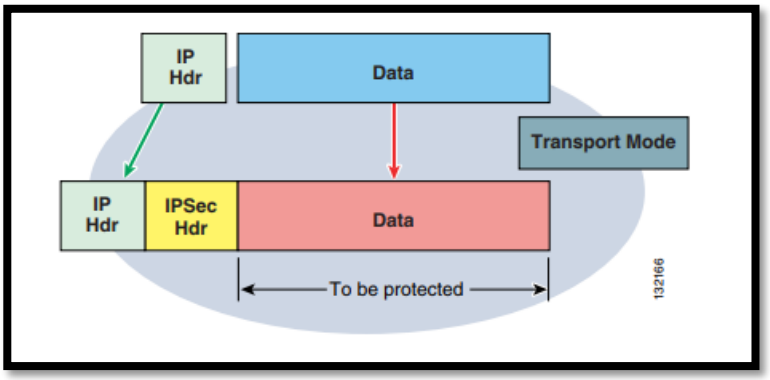

Figura 17. IPSec Modo Transporte
Fuente: (Cisco Systems, Inc, 2006)

Modo Túnel: utilizado para brindar seguridad de datos entre dos redes, los paquetes IP completos se encapsulan dentro de otro y se envían al destino. Encapsula el encabezado IP completo, así como la carga útil. Este modo es mucho más seguro y flexible que el modo transporte. Este modo cifra las direcciones IP de origen y destino del paquete original y oculta esa información de la red no protegida (Cisco Systems, Inc, 2006), (Cisco Systems, Inc, 2016), (Newport Networks, 2006).

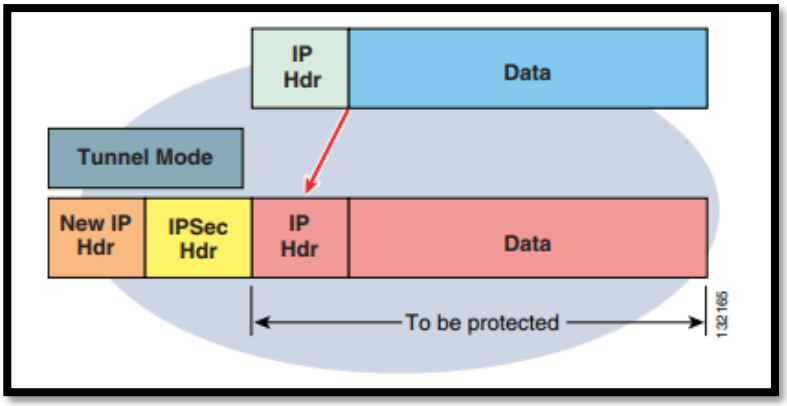

Figura 18. IPSec Modo Túnel
Fuente: (Cisco Systems, Inc, 2006)

Lo referente a IPSec para equipos Fortinet se detalla en el siguiente capítulo, es importante mencionar que la Entidad Financiera asociada a este proyecto utiliza equipos

FortiGate como CPEs, a su vez se indicará características importantes de otros fabricantes de equipos de seguridad.

El diseño de este proyecto está basado en equipos FortiGate que actualmente se encuentran en operación en la red de la Entidad Financiera, pero sin ninguna configuración de seguridad, por ello se implementó VPN IPSec sobre estos equipos.

CAPITULO III

ESTADO DEL ARTE

Gartner Inc.

Es una empresa estadounidense de investigación y análisis de TI fundada en 1979, sus dos principales herramientas que ofrece son: el cuadrante mágico de Gartner y el ciclo de exageraciones:

Ciclo de exageraciones: es una representación gráfica de las etapas del ciclo de vida que una tecnología atraviesa desde la concepción hasta la madurez y la adopción generalizada, es publicada de manera anual y las empresas la utilizan como guía para reducir el riesgo en la toma de decisiones de inversión tecnológica.

Cuadrante mágico de Gartner: es una metodología de investigación y herramienta de visualización para monitorear y evaluar el progreso y las posiciones de los proveedores de tecnología. Utiliza una matriz bidimensional para ilustrar los puntos fuertes y las diferencias entre las empresas. Los informes de investigación generados ayudan a los inversionistas a encontrar compañías que se ajustan a sus necesidades y ayudan a las empresas a comparar competidores en su mercado. Se clasifica en cuatro tipos de proveedores de TI.

- Los líderes se ejecutan bien contra su visión actual y están bien posicionados para el futuro, poseen un portafolio extenso y completo de productos con capacidad de adaptarse a los cambios del mercado.

- Los visionarios entienden a dónde va el mercado o tienen una visión para cambiar las reglas del mercado, pero aún no soporta necesidad a nivel global.
- Los jugadores de nicho se enfocan con éxito en un segmento pequeño, o están fuera de foco y no superan o innovan a otros.
- Los retadores se ejecutan bien hoy o pueden dominar un segmento grande, pero no demuestran una comprensión total de la dirección del mercado (Gartnet Inc, 2019) (Rouse, 2019) (gbadvisors, 2019).

En lo referente a seguridad se tiene el cuadrante mágico de Gartner (septiembre 2018) enfocado a equipos firewalls de red empresarial.

- **Líderes:** Palo Alto Networks, Fortinet, Cisco y Check Point Software Technologies
- **Retadores:** Huawei
- **Visionarios:** Forcepoint
- **Jugadores de nicho:** Sophos, Juniper Network, Barracuda, Sangfor, Hillstone, WatchGuard, AhnLab, SonicWall, Stormshield, New H3C Group.

Para este proyecto se consideró el grupo de líderes del cuadrante.

Figura 19. Cuadrante de Gartner 2018 Firewall
Fuente: (Gartner, 2018)

Palo Alto: Soporta IPSec para poder tener acceso seguro a la información entre dos o más sitios, para ello es necesario los siguientes componentes (Palo Alto Networks, 2019).

- IKE Gateway: Los dispositivos inician y terminan las conexiones VPN a través de dos redes denominadas IKE Gatewasy
- Tunnel Interface: interface lógica que se utiliza para entregar tráfico entre dos puntos finales.

- Tunnel Monitoring: Permite verificar la conectividad (usando ICMP) a una dirección IP de destino o al siguiente salto en un intervalo de sondeo específico, y especificar una acción en caso de no acceder a la dirección IP monitoreada.
- Internet Key Exchange (IKE) for VPN: permite a los pares VPN en ambos extremos del túnel cifrar y descifrar paquetes utilizando claves o certificados acordados mutuamente y un método de cifrado.

IKEv2: proporciona los siguientes beneficios sobre IKEv1:

- Los puntos finales del túnel intercambian menos mensajes para establecer un túnel. IKEv2 usa cuatro mensajes; IKEv1 usa nueve mensajes (en modo principal) o seis mensajes (en modo agresivo).
- La funcionalidad NAT-T incorporada mejora la compatibilidad entre proveedores.
- La comprobación de estado incorporada restablece automáticamente un túnel si se cae. La verificación de vida reemplaza la Detección de pares muertos utilizados en IKEv1.
- Soporta selectores de tráfico (uno por intercambio). Los selectores de tráfico se utilizan en las negociaciones de IKE para controlar qué tráfico puede acceder al túnel.
- Admite el intercambio de hash y URL para reducir la fragmentación.
- Capacidad de resistencia contra ataques DoS con validación de pares mejorada.

Los equipos Palo Alto soportan los siguientes algoritmos de encriptación.

Tabla 1
Algoritmos de encriptación Palo Alto

Algoritmo	Descripción
3des	Triple estándar de cifrado de datos (3DES) con una seguridad de 112 bits
aes-128-cbc	Estándar de cifrado avanzado (AES) utilizando encadenamiento de bloques de cifrado (CBC) con una seguridad de 128 bits
aes-192-cbc	AES utilizando CBC con una seguridad de 192 bits.
aes-256-cbc	AES utilizando CBC con una seguridad de 256 bits.
aes-128-ccm	AES utiliza el contador con CBC-MAC (CCM) con una seguridad de 128 bits
aes-128-gcm	AES que utiliza Galois / Counter Mode (GCM) con una seguridad de 128 bits
aes-256-gcm	AES utilizando GCM con una seguridad de 256 bits.
des	Estándar de cifrado de datos (DES) con una seguridad de 56 bits

Cisco: según este fabricante IPSec brinda los siguientes beneficios:

- Incrementa la productividad de los empleados: permite el acceso seguro en cualquier momento y lugar a la red corporativa.
- Controlar el acceso a los recursos de la empresa: proporciona un control de acceso basado en identidad, evitando accesos no autorizados a la información.
- Admite necesidades empresariales acorde a tendencias actuales: admite aplicaciones de datos, voz, video y multimedia con la extensión de nuevas aplicaciones a ubicaciones remotas.
- Brindar altos niveles de seguridad a través de cifrado y autenticación.

- Reduce los costos de implementación y administración, ya que utiliza una solución de comunicaciones segura, única, fácil de instalar y fácil de usar (Cisco Systems, Inc, 2019).

Cisco maneja los siguientes algoritmos de encriptación, hace referencia a equipos power fire versión 6.2 (Cisco Systems, Inc, 2018).

AES-GCM— (solo IKEv2). El Estándar de cifrado avanzado en el Modo Galois / Contador es un modo de operación de cifrado por bloques que proporciona confidencialidad y autenticación de origen de datos, y brinda mayor seguridad que AES. AES-GCM ofrece tres fortalezas de clave diferentes: claves de 128, 192 y 256 bits. Una clave más larga proporciona mayor seguridad, pero una reducción en el rendimiento. GCM es un modo de AES que se requiere para ser compatible con NSA Suite B. NSA Suite B es un conjunto de algoritmos criptográficos que los dispositivos deben admitir para cumplir con los estándares federales de resistencia criptográfica.

AES-GMAC: (solo las propuestas IKEv2 IPsec). El Código de autenticación de mensajes de Galois estándar de cifrado avanzado es un modo de operación de cifrado de bloque que proporciona solo la autenticación de origen de datos. Es una variante de AES-GCM que permite la autenticación de datos sin cifrar los datos. AES-GMAC ofrece tres fortalezas de claves diferentes: claves de 128, 192 y 256 bits.

AES: Advanced Encryption Standard es un algoritmo de cifrado simétrico que proporciona mayor seguridad que DES y es computacionalmente más eficiente que 3DES. AES ofrece tres fortalezas de clave diferentes: claves de 128, 192 y 256 bits. Una clave más larga proporciona mayor seguridad, pero una reducción en el rendimiento.

3DES: Triple DES, que encripta tres veces con claves de 56 bits, es más seguro que DES porque procesa cada bloque de datos tres veces con una clave diferente. Sin embargo, utiliza más recursos del sistema y es más lento que DES.

DES: el estándar de cifrado de datos, que se encripta con claves de 56 bits, es un algoritmo de bloque de clave secreta simétrico. Es más rápido que 3DES y utiliza menos recursos del sistema, pero también es menos seguro. Si no necesita una confidencialidad de datos sólida, y si los recursos o la velocidad del sistema son una preocupación, elija DES.

Nulo: un algoritmo de cifrado nulo proporciona autenticación sin cifrado. Esto se suele utilizar para fines de prueba solamente.

Es importante mencionar que Cisco hace uso de IPSec para los sistemas IOT, ya que a medida que crece la necesidad de conectar varios tipos de dispositivos localizados en diferentes ubicaciones, se vuelve indispensable brindar una seguridad integral a estas conexiones, para ello Cisco brinda la solución Cisco Remote and Mobile Assets, que de manera general es la combinación de Cisco Kinetic - Módulo Management Gateway (GMM) y Cisco Routers industriales (IRS), cuyas características de arquitectura son las siguientes (Cisco Systems, Inc, 2019).

- **Enrutadores industriales:** Capacidades de red integrales en un factor de forma resistente.
- **Gestión basada en la nube:** Seguridad, política y operaciones unificadas utilizando el personal existente.

- **Múltiples opciones de conectividad:** Optimizar el uso de backhaul y presupuestos disponibles.
- **Seguridad y controles empresariales:** seguridad de borde y rendimiento superior de VPN con el software Cisco IOS.

Esta solución está diseñada por bloques, en donde el Túnel IPSec cifrado para aprovisionar y administrar las puertas de enlace de borde.

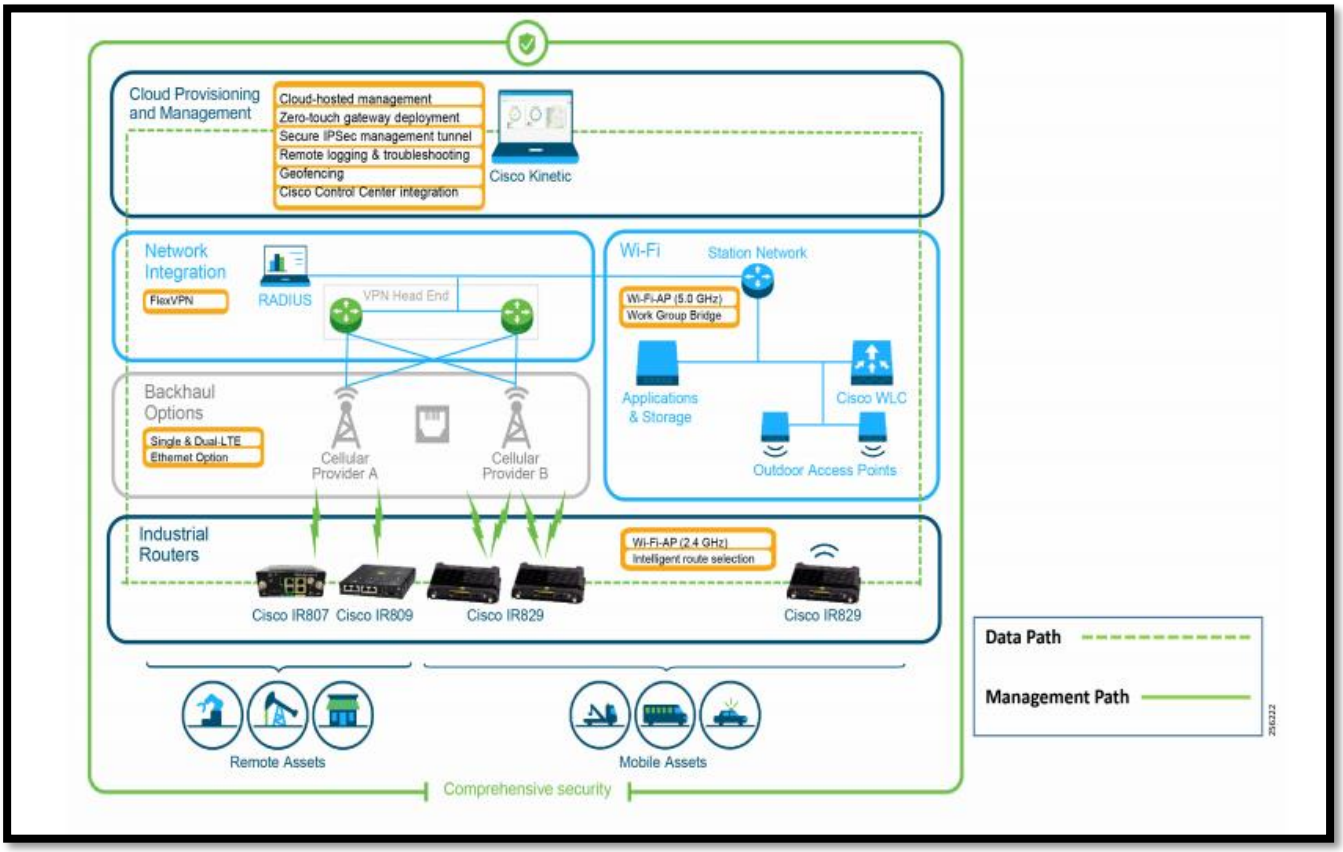

Figura 20. Bloques de construcción de activos remotos y móviles de Cisco
Fuente: (Cisco Systems, Inc, 2019)

En 2016 Cisco lanzó su firewall de última generación denominado *FirePower*, cuyas principales ventajas son: detener más amenazas, obtener más

información, detectar antes y actuar más rápido. Cisco Firepower NGFW ofrece protección frente a amenazas avanzadas antes y después de un ataque, así como durante este.

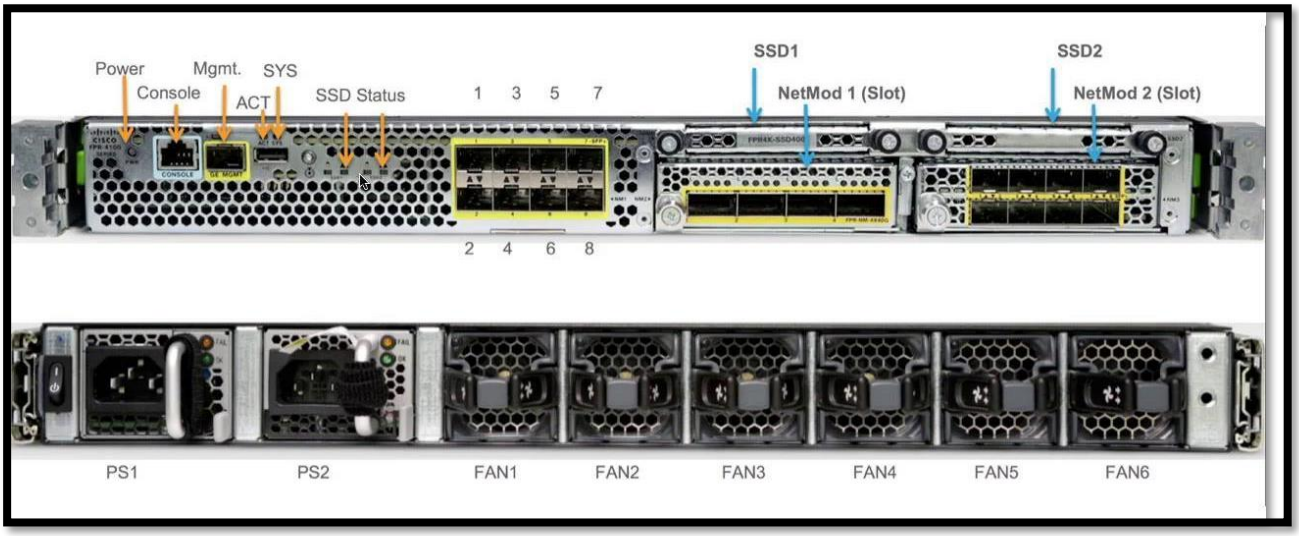

Figura 21. Cisco Firepower serie 4100
Fuente: (Cisco Systems, Inc)

Check Point: Este fabricante provee conectividad segura a redes corporativas a usuarios remotos y móviles, la seguridad se garantiza al integrar control de acceso, autenticación y cifrado, resalta los siguientes beneficios:

Conectividad VPN segura para usuarios remotos y móviles, sucursales:

- Administración simple y centralizada de acceso remoto y VPN de sitio a sitio
- Seguridad mejorada contra ataques de denegación de servicio (DoS)
- La política de seguridad se puede aplicar en diversos grados según el nivel de cifrado

Flexibilidad para construir la solución VPN que satisfaga sus necesidades específicas

- Múltiples modos de conectividad VPN de acceso remoto
- Conjunto completo de alternativas de clientes VPN de acceso remoto
- Múltiples métodos de creación de VPN, incluyendo VPN basadas en rutas y basadas en dominios

Integrado en la arquitectura de Check Point Infinity

- Active IPSec VPN en cualquier punto de seguridad de Check Point
- Registro e informes centralizados a través de una única consola

La VPN de IPsec de Check Point admite la creación de VPN a través de múltiples métodos:

VPN basadas en rutas: los administradores establecen reglas de VPN para definir qué tráfico debe cifrarse, lo que permite la creación de VPN complejas de gran escala de sitio a sitio en entornos dinámicos. Las VPN basadas en ruta también admiten la extensión de enrutamiento dinámico y comunidades de multidifusión a través de VPN.

VPN basadas en dominio: los administradores identifican los recursos detrás de la puerta de enlace para los cuales se debe cifrar el tráfico VPN.

IPSec de Check Point está integrada en la Arquitectura Infinita de Check Point, que el mismo fabricante lo define como una arquitectura de seguridad cibernética totalmente consolidada que proporciona una protección sin precedentes contra los mega

ciberataques de Gen V, así como también las futuras amenazas cibernéticas en todas las redes, puntos finales, nube y dispositivos móviles. La arquitectura está diseñada para resolver las complejidades de la creciente conectividad y la seguridad ineficiente (Check Point Software Technologies Ltd), (Check Point Software Technologies Ltd, 2019)

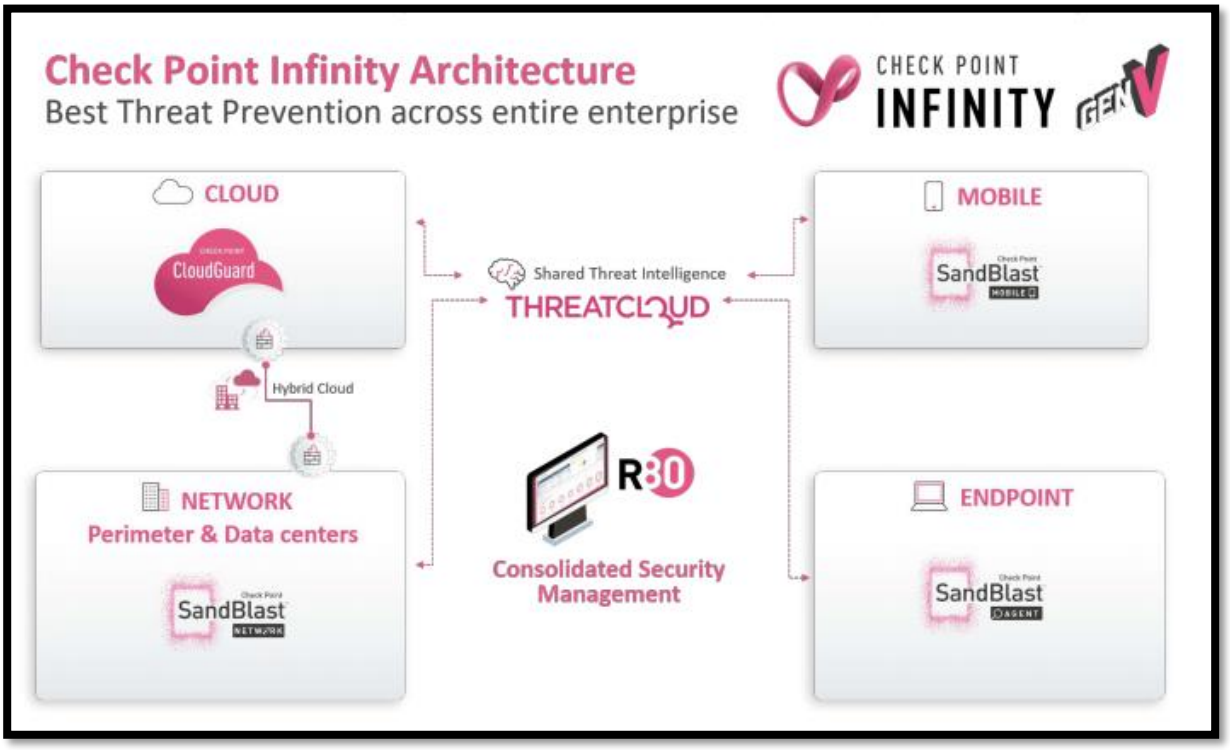

Figura 22. Arquitectura Infinita de Check Point
Fuente: (Check Point Software Technologies Ltd)

Check Point soporta los siguientes métodos de encriptación e integridad, así como los grupos del protocolo Diffie Hellman.

Parameter	IKE Phase 1 (IKE SA)	IKE PHASE 2 (IPSec SA)
Encryption	▪ AES-128 ▪ AES-256(default) ▪ 3DES ▪ DES ▪ CAST (IKEv1 only)	▪ AES-128 (default) ▪ AES-256 ▪ 3DES ▪ DES ▪ DES-40CP (IKEv1 only) ▪ CAST (IKEv1 only) ▪ CAST-40 (IKEv1 only) ▪ NULL ▪ AES-GCM-128 ▪ AES-GCM-256
Integrity	▪ MD5 ▪ SHA1 (default) ▪ SHA -256 ▪ AES-XCBC ▪ SHA -384	▪ MD5 ▪ SHA1 (default) ▪ SHA -256 ▪ AES-XCBC ▪ SHA -384

Figura 23. Métodos de encriptación en integridad
Fuente: (Check Point Software Technologies Ltd, 2019)

Parameter	IKE Phase 1 (IKE SA)	IKE Phase 2 (IPSec SA)
Diffie Hellman Groups	▪ Group2 (1024 bits) (default) ▪ Group1 (768 bits) ▪ Group5 (1536 bits) ▪ Group14 (2048 bits) ▪ Group19 (256-bit ECP) ▪ Group20 (384-bit ECP)	▪ Group2 (1024 bits) (default) ▪ Group1 (768 bits) ▪ Group5 (1536 bits) ▪ Group14 (2048 bits) ▪ Group19 (256-bit ECP) ▪ Group20 (384-bit ECP)

Figura 24. Grupos del protocolo Diffie Hellman IPSec Check Point
Fuente: (Check Point Software Technologies Ltd, 2019)

Fortinet: este fabricante en su versión Fortios 6.0 introduce las siguientes novedades (Fortinet , 2019).

Soporte OCVPN (One Click VPN) en FortiOS 6.0.2. es una solución basada en la nube que simplifica significativamente el aprovisionamiento y configuración de una VPN IPSec. El administrador habilita la opción OCVPN con un solo clic, agrega las subredes

necesarias y luego se completa la configuración. La OCVPN actualiza cada FortiGate automáticamente a medida que los dispositivos se unen a la VPN, a medida que se agregan / eliminan las subredes, cuando cambian las IP externas dinámicas (por ejemplo, DHCP / PPPoE), y cuando cambian los enlaces de la interfaz WAN (como en el caso de redundancia de WAN dual). Los cambios de configuración y los eventos se propagan automáticamente a través de los nodos participantes sin la intervención del usuario, por lo que, en cierto sentido, la VPN se administra a sí misma como una unidad con solo la mínima entrada del usuario. El usuario especifica qué subredes participar en la VPN. Todo lo demás pasa de forma transparente al usuario (Fortinet , 2019).

Esta nueva solución presenta las siguientes limitaciones:

- El FortiGate debe estar registrado con una licencia válida de Soporte de FortiCare.
- Solo se admiten las configuraciones VPN de malla completa que utilizan la criptografía PSK.
- Se deben usar direcciones IP públicas (FortiGates detrás de NAT no puede participar).
- VDOM no root y máquinas virtuales FortiGate no son compatibles.
- Se pueden agregar hasta 16 nodos a la nube OCVPN, cada uno con un máximo de 16 subredes.

En FortiOS 6.01 se tienen las siguientes novedades (Fortinet , 2019).

- **Actualizaciones del soporte de IPsec para el cifrado AEAD de ChaCha20 / Poly1305:** En IKEv2, para admitir *RFC 7634*, los algoritmos criptográficos ChaCha20 y

Poly1305 se pueden usar juntos como un cifrado AEAD de modo combinado (como aes-gcm) en el nuevo *crypto_ftnt cipher in cipher_chacha20poly1305.c*

- **Soporte IPsec para AES-GCM para IKEv2 Fase 1:** En IKEv2, para admitir *RFC 5282*, el algoritmo AEAD AES-GCM ahora es compatible, con variantes de 128 y 256 bits.

Fortinet enfatiza que sus soluciones son ideales para instituciones financieras, con seguridad de alto rendimiento y máxima calificación respaldada por la última inteligencia de amenazas de FortiGuard Labs, según el fabricante 9 de los 10 bancos más importantes del mundo utilizan sus servicios.

Es importante mencionar que Fortinet cuenta con la herramienta FortiManager, cuyas principales características son las siguientes (Fortinet, Inc, 2019).

- Gestión centralizada: Proporciona un amplio conjunto de herramientas para administrar de forma centralizada más de 100,000 dispositivos, como firewalls, switches y puntos de acceso desde una única consola.
- Alta disponibilidad: Realiza automáticamente copias de respaldo de la base de datos de FortiManager en hasta cinco nodos en un clúster que puede estar geográficamente disperso para la recuperación de desastres
- Automatización de seguridad: Reduce la complejidad y el costo, aprovechando la automatización habilitada a través de la API REST, los scripts, los conectores y los puntos de automatización.

CAPITULO IV

4.1. Situación actual

La entidad financiera asociada al presente proyecto al momento opera con los siguientes enlaces a nivel nacional, sin realizar encriptación en los datos en tránsito entre matriz hacia las agencias y ATMs, en la Tabla 2 un detalle.

Tabla 2

Detalle enlaces Entidad Financiera

Tipo	Número	Ancho de banda promedio	Tipo de última milla	Modelo equipo FortiGate	Tipo de servicio
Agencias	26	4.5 Mbps	Fibra óptica y microonda	FortiGate-30E	IP VPN
Cajeros (ATMs)	103	256-512 Kbps	Fibra óptica, microonda y satelital (difícil acceso)	FortiGate-30E	IP VPN
Bodegas	1	2 Mbps	Fibra óptica	FortiGate-30E	IP VPN
Matriz	2	120 Mbps	Fibra óptica	FortiGate-900D	IP VPN
Total	132				

En la Tabla 3, se brinda las principales características de los equipos FortiGate utilizados en la solución.

Tabla 3

Principales características equipos FortiGate

FortiGate	Firewall Throughput	IPsec VPN Throughput	Switch Ports GE	WAN Ports GE	Hardward Accelerated Ports GE
30E	950 Mbps	75 Mbps	4	1	-
900D	52 Gbps	25 Gbps	-	-	16

Fuente: (Fortinet, Inc, 2019)

Figura 25. FortiGate 30E
Fuente: (Fortinet, Inc, 2019)

Figura 26. FortiGate 900D
Fuente: (Fortinet, Inc, 2018)

4.2. Diseño de la solución

La solución planteada en el presente trabajo es la encriptación de datos en la red de comunicaciones de una Entidad Financiera que brinda un proveedor de servicios a través de MPLS entre matriz y todas las sucursales, incluyendo ATMs (automated teller machine). Al momento el cliente tiene implementado canales, cuyo diagrama general se detalla en la Figura 27, el CPE en cada uno de los

puntos como se indicó en capítulos anteriores es Fortinet, el cliente optó por este fabricante debido al costo-beneficio que se tiene, en la

Tabla **4** se muestra una comparativa entre Fortinet y Cisco.

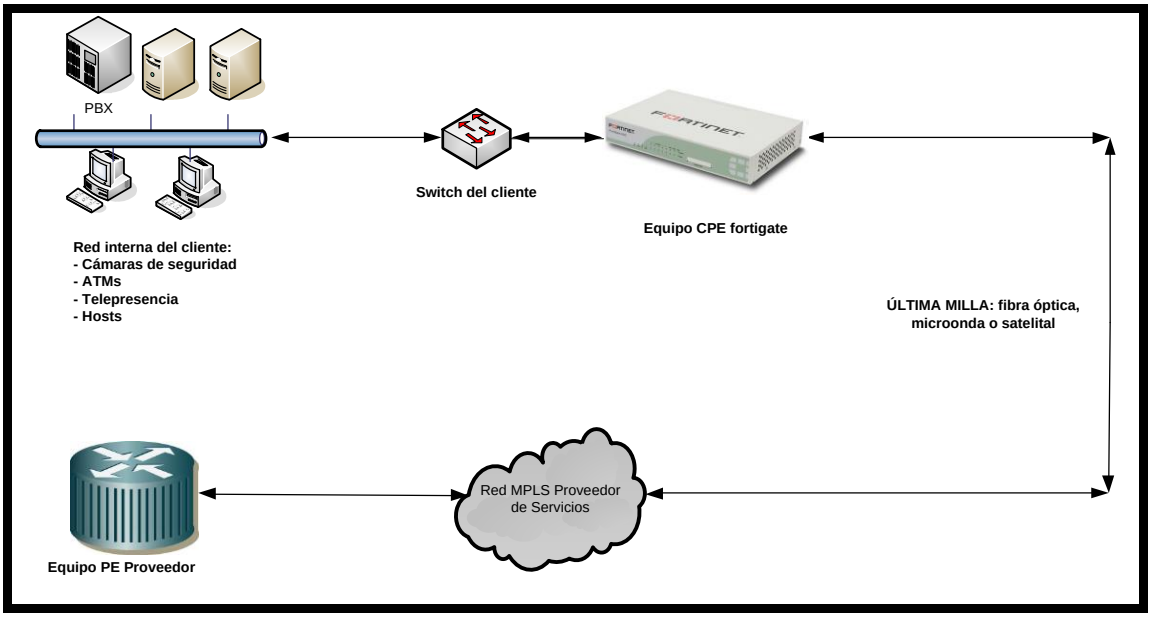

Figura 27. Diagrama general de los enlaces del cliente

Tabla 4

Comparación FortiGate vs Cisco

	FortiGate	Cisco
Configuración	La interfaz es fácil de configurar. Incluye una línea de comandos disponibles para administradores de alto nivel, suelen ser de muy bajo mantenimiento y fáciles de actualizar.	El equipo es robusto y confiable. Tiene gran flexibilidad en las configuraciones y es totalmente escalable en potencia y funcionalidades en relación con las necesidades de cada empresa
Soluciones	Es una gran solución VPN, puerta de enlace de correo, dispositivos de enrutamiento y por supuesto, dispositivo firewall. Tiende a ser ideal para empresas medianas y grandes de 500 o más usuarios. Igualmente, los FortiGates en entornos pequeños y medianos con múltiples ubicaciones también funcionan muy bien	Las soluciones firewall ASA tienden a ser ideales para pequeñas empresas. (Sin dejar de lado las grandes) Integran un firewall de hardware con controles de software en una solución de seguridad integral que incluye soporte de red privada virtual **(**VPN**)**, antivirus, antispam, antispywarey capacidades de filtrado de contenido.
Restricciones de VPN	Los números de VPN están limitados únicamente por la fabricación del chasis de hardware.	Tiene numerosos modelos de licencia, esto limita el número de pares independientemente del tipo: clientless vs client, sslvpn**,** ipsec**,** l2tp-ipsec**.**
Rendimiento	Todas las funciones habilitadas en el firewall generan poco o hasta incluso ningún impacto en el rendimiento.	Tiene la capacidad de integrarse con otras tecnologías de seguridad críticas para ofrecer soluciones integrales que satisfacen las necesidades de seguridad.

Fuente: (Nsit, 2019)

Luego de haber revisado en capítulos anteriores lo referente a VPN, se tiene que la encriptación de datos que se necesita realizar es mediante la implementación de VPN IPSec modo túnel, ya que brinda los niveles de seguridad y flexibilidad necesarios al momento de encriptar los datos en tránsito, esto se validará mediante la captura y análisis de este.

4.3. Diagrama General

En la Figura 29 muestra el diagrama general de la solución de encriptación que se va a implementar en el presente proyecto, los ATMs y agencias levantan una VPN IPsec contra la sede matriz para garantizar seguridad de los datos en tránsito, en estos datos se incluyen las transacciones financieras que realizan los clientes ya sea mediante ventanilla, apps, web site u otros. Como parte final de la implementación se añadirá cada uno de los equipos FortiGate a la herramienta de administración Fortimanager con el appliance 2000e, cuyo objetivo principal es la administración simplificada de implementaciones y configuraciones futuras de hasta 1200 dispositivos (licencia a adquirir). No se puede agregar desde un inicio debido a que la compra de licencias de la herramienta está prevista realizar en un par de meses por temas de presupuesto. Es importante mencionar que la administración de los equipos FortiGate la realiza el Centro de Operaciones de Seguridad SOC del proveedor de servicios del cliente, para ello se trabajará en conjunto con dicho personal para el tema de accesos y permisos correspondientes.

Figura 28. FortiManager 2000e

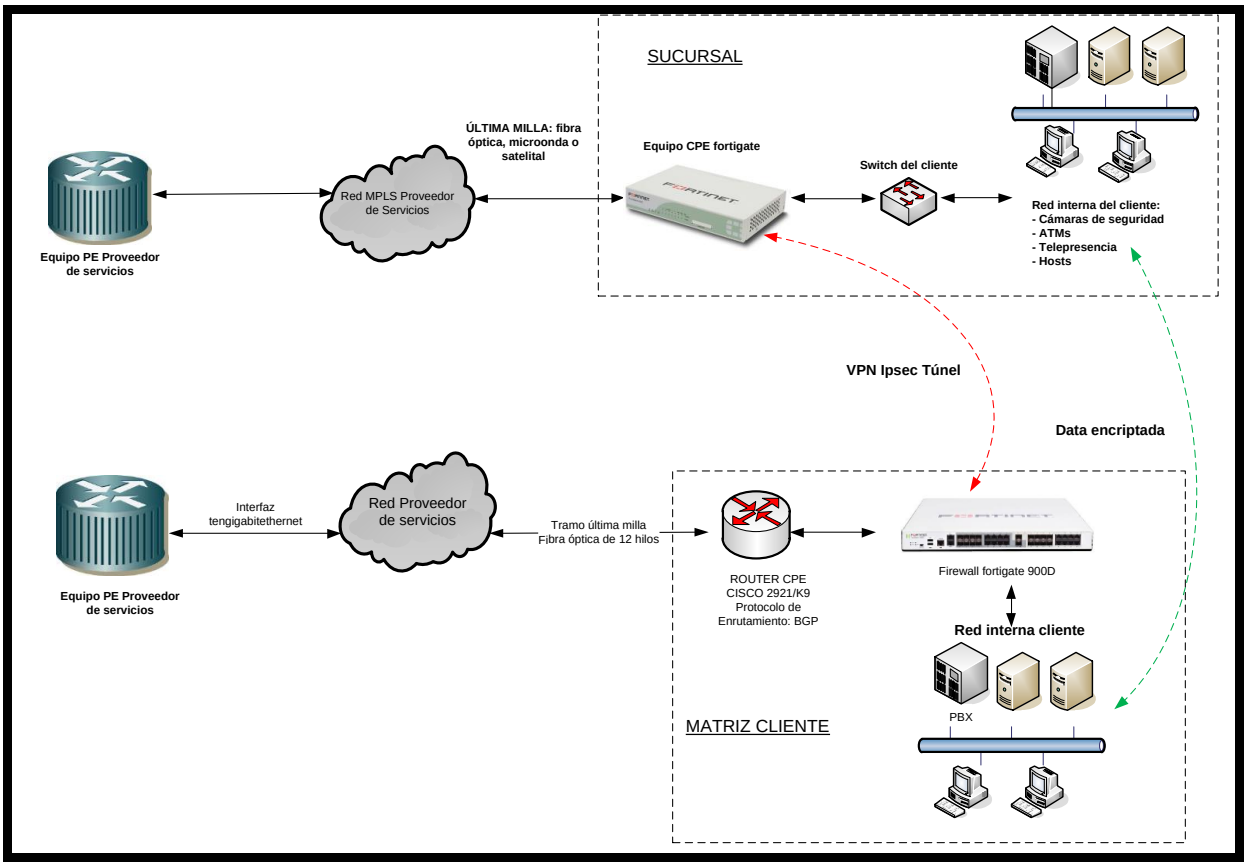

Figura 29. Solución general de encriptación

4.4. Validación conexión remota segura a los equipos FortiGate

Para iniciar con las configuraciones es necesario contar con una conexión remota, vía ssh y https.

Con el fin de gestionar la conexión remota a los equipos FortiGate vía ssh se utilizará la herramienta SecureCRT de VanDyke, en donde se validará si la conexión https se encuentra, habilitada, para ello se tiene los siguientes pasos a ejecutar.

- Obtener IPs Loopback de monitoreo de cada uno de los enlaces, a través de un reporte de la herramienta Orion.
- Validar conectividad y acceso ssh/https desde la red del servidor Orion del proveedor de servicios hacia los enlaces del cliente a través de la IP Loopback.
- Crear sesiones ssh en la herramienta SecureCRT.

Figura 30. Herramienta SecureCRT

4.5. Respaldo de configuraciones de los equipos FortiGate

Debido a que se van a realizar cambios en producción, es necesario respaldar la configuración, para ello se utilizará el módulo NCM de la herramienta de monitoreo Orion.

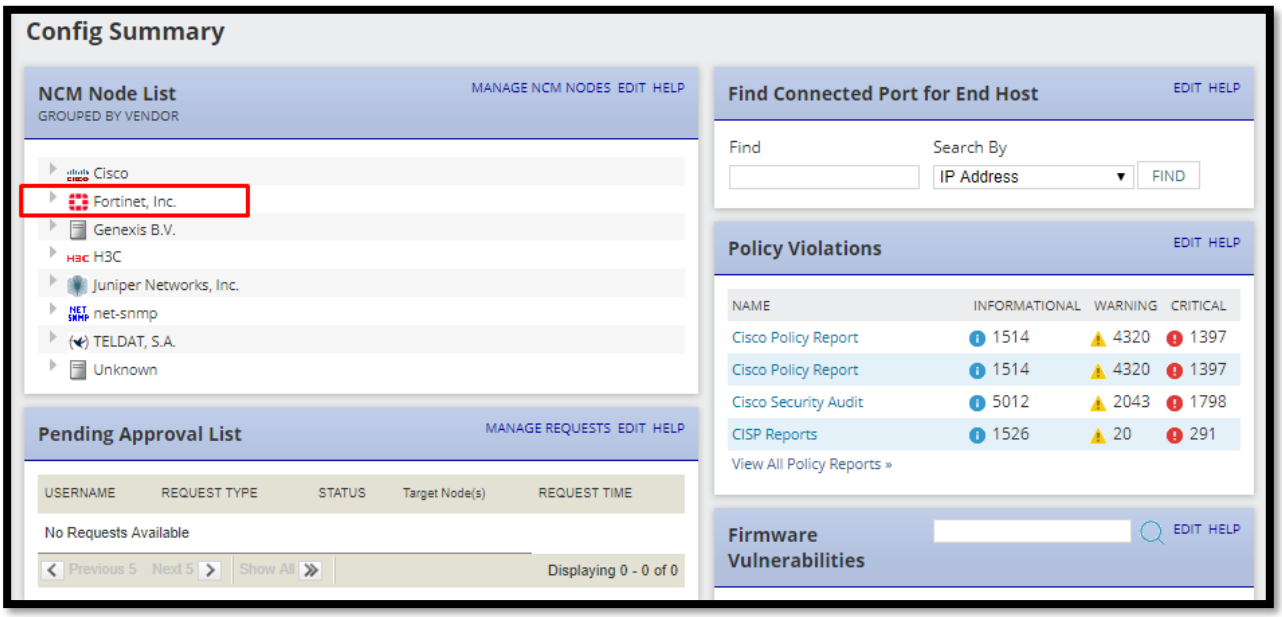

Figura 31. Módulo NCM herramienta Orion

4.6. Configuración IPSec en los equipos FortiGate

A continuación, los pasos a seguir para levantar el túnel Ipsec entre cada una de las sedes y matriz.

- Configurar fase 1
- Configurar fase 2
- Validar que el túnel IPsec se levante
- Creación de las direcciones IP del servidor remoto y del enlace local
- Configuración de las políticas de acceso
- Validar tráfico sobre el túnel IPsec

4.6.1. Parámetros de configuración fase 1

Nombre: VPN_nombre_enlace/ATM

Local Gateway: Static IP address, corresponde a la dirección IP configurada en el FortiGate dentro del segmento LAN, es único para cada punto.

Remote Gateway: Static IP address, será la misma dirección IP para todas las VPNs que se levante, ya que se trata de la IP del concentrador de VPNs que se encuentra en la oficina matriz.

Local Interface: Interface WAN por la que se alcanza el peer remoto x.x.x.x, en caso de que se utilice una vlan sobre la interface WAN debe especificarse interface tipo vlan.

Preshared Key: Se utilizará la misma clave para todos los enlaces.

Peer options: opción *any peer,* debido a que el método de autenticación es con clave compartida.

Adicional se debe deshabilitar la opción de IPsec Interface Mode para configurar una VPN IPSEC del tipo Policy / Tunnel Mode

4.6.2. Parámetros de configuración fase 2

Name: Utilizar el formato VPN_nombre_cajero

Phase 1: Colocar el nombre de la fase 1 creada.

Local Address: Escoger el tipo IP Address e ingresar la dirección IP del ATM, en algunos puntos el cliente cuenta con más de 1 ATM, para ello se realizará la configuración de fase dos para cada uno.

Remote Address: Escoger el tipo IP Address e ingresar la dirección IP del servidor. Siempre será esta dirección IP ya que pertenece al servidor de transacciones del cajero.

CAPÍTULO V

IMPLEMENTACIÓN DE LA SOLUCIÓN

5.1. Conexión remota segura a los equipos FortiGate

Para iniciar con la implementación es necesario contar con una data actualizada de las IPs de monitoreo que serán usadas para la conexión remota hacia cada uno de los equipos, ejecutaremos la siguiente consulta sql sobre la base de datos de la herramienta Orion.

```
SELECT Nodes.Caption AS NodeName, Nodes.IP_Address AS IP_Address
 FROM Nodes
 WHERE
(
  (Nodes.Caption LIKE 'NOMBRE_ENTIDAD_FINANCIERA%') AND
  (Nodes.MachineType = 'Fortinet, Inc.')
)
```

A continuación, un detalle de la información obtenida del reporte.

Tabla 5

Resumen de puntos de datos del cliente

	Agencia	Cajero	Total
Total	26	103	129

Con la data de direcciones IP de monitoreo actualizada, a través de cada una de ellas se procede a validar la conexión ssh versión 2 a los diferentes puntos desde la red del servidor Orion utilizando la herramienta licenciada SecureCRT. Las credenciales de acceso han sido proporcionadas por el Centro de Operaciones de Seguridad (SOC) del proveedor, las mismas son genéricas para todos los puntos y poseen permisos de lectura y escritura de manera temporal. En SecureCRT se ha creado una sesión por cada punto del cliente, es decir 129, en la Figura 32 se visualiza la información requerida para la creación.

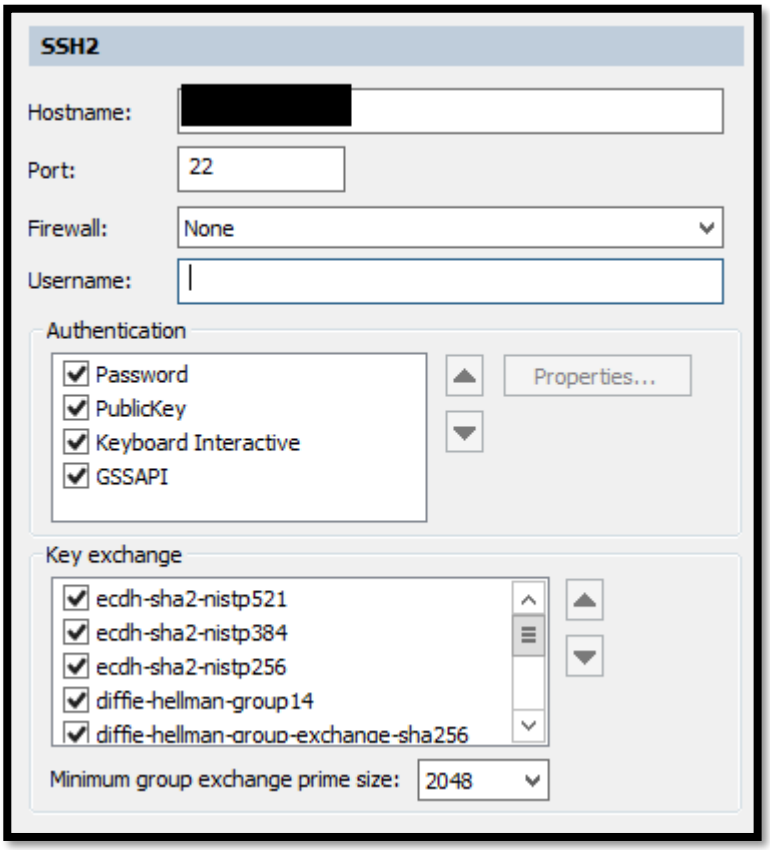

Figura 32. Creación nueva conexión remota

Las sesiones se dividieron en cajeros y agencias y estas a su vez clasificadas por regiones. Se valida el correcto acceso remoto a cada uno de los puntos.

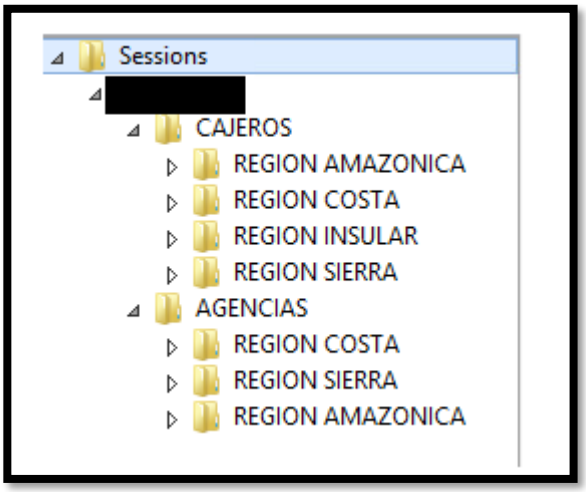

Figura 33. Creación sesiones remotas

Con el objetivo de habilitar y validar el acceso remoto por https, se configura de forma remota en cada uno de los equipos FortiGate el comando *set allowaccess ping https ssh snmp http telnet fgfm* en la interfaz de management (loopack),

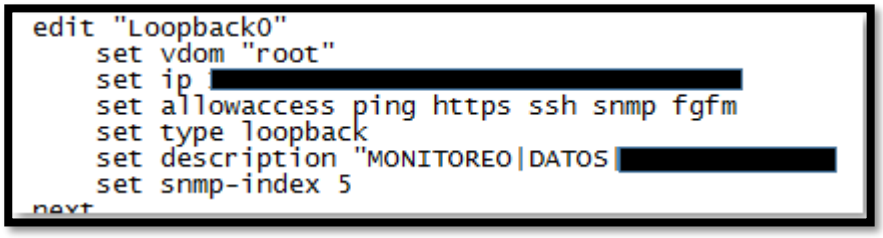

Figura 34. Configuración de permisos de acceso remoto

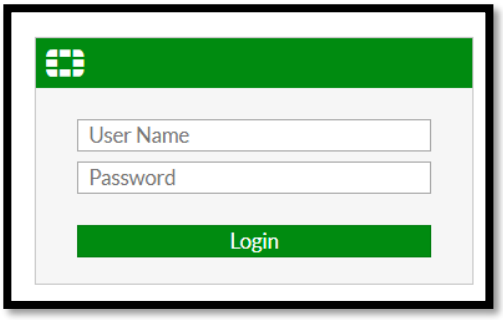

Figura 35. Acceso remoto vía https

5.2. Respaldo de configuraciones de los equipos FortiGate

Una vez validado el acceso mediante ssh/https se realiza el respaldo de configuración de cada uno de los equipos mediante el módulo NCM de la herramienta Orion, con el objetivo de tener un punto de restauración en caso de inconvenientes que puedan presentarse, para lo cual se ha realizado lo siguiente:

- Validar que los equipos se encuentren monitoreados mediante snmp con una comunidad escritura/lectura (WR), se realiza un test de comprobación.

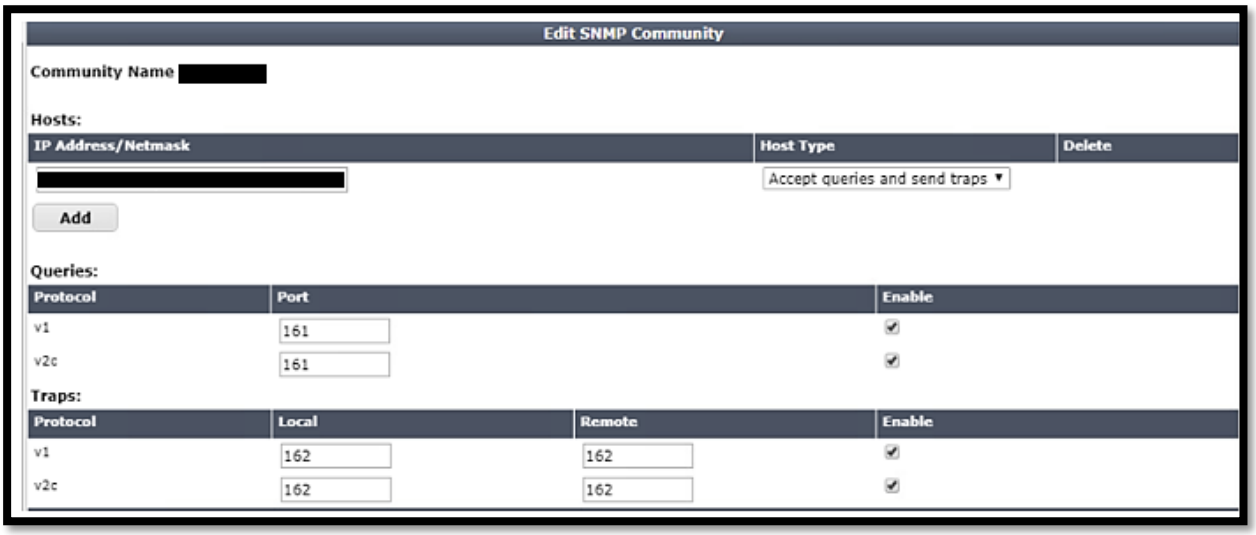

Figura 36. Configuración SNMP en equipo FortiGate

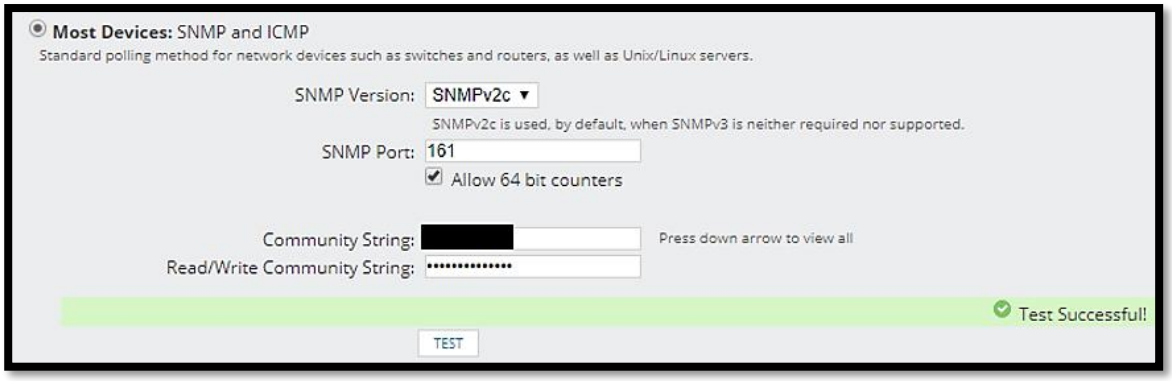

Figura 37. Test de conexión vía snmp desde Orion

- Agregar los equipos FortiGate en el módulo NCM
- Creación de un usuario genérico con privilegios de administrador para poder acceder a los equipos mediante el módulo NCM, por tema de seguridad las credenciales únicamente las conoce el Centro de Operaciones de Seguridad del proveedor de servicios, se realiza un test de comprobación en cada equipo.

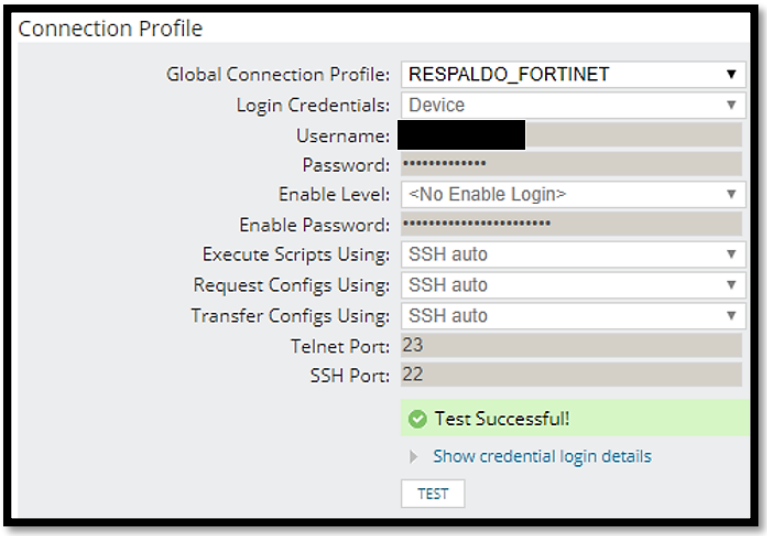

Figura 38. Test de conexión remota ssh

- Descarga de la configuración de cada uno de los equipos de forma masiva.

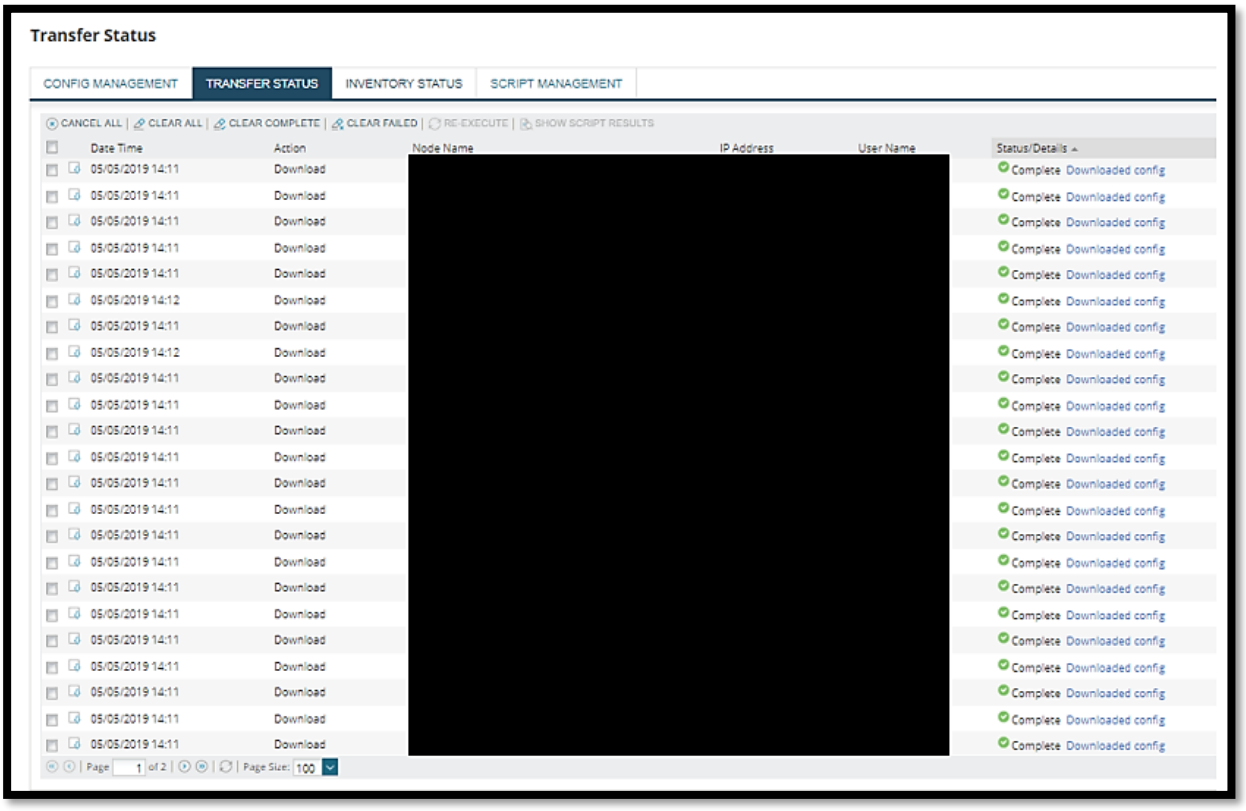

Figura 39. Descarga configuraciones equipos FortiGate en Orion

Para tener un respaldo actualizado de las configuraciones se creó un job que descarga automáticamente las mismas cada miércoles a las 02h00, adicional valida cambios con respecto a la última configuración.

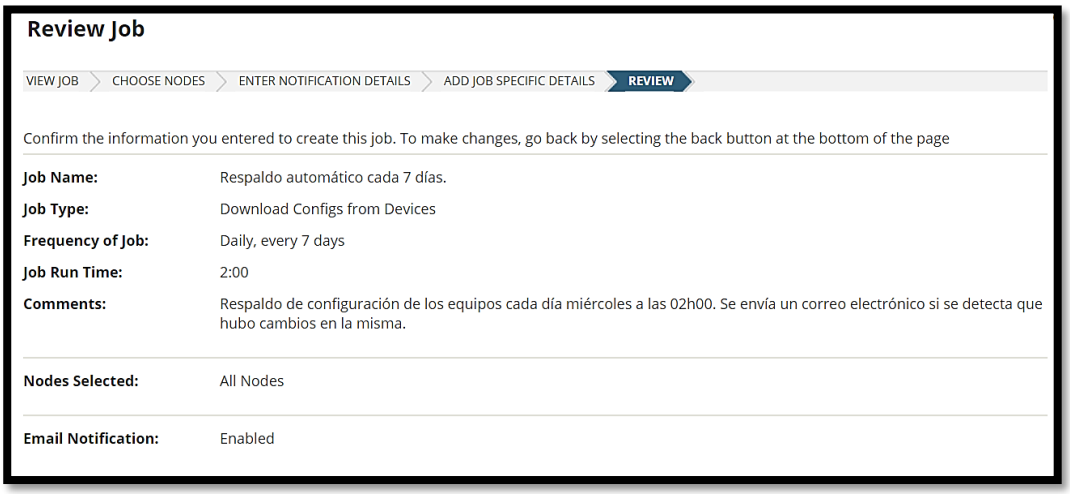

Figura 40. Respaldo automático de configuración de los equipos FortiGate

Una vez que se tiene un respaldo actualizado de las configuraciones de cada uno de los puntos se inicia con las configuraciones necesarias para levantar el túnel Ipsec.

5.3. Configuración Ipsec en equipos FortiGate 30e & 900D

Fase 1: para levantar la fase 1 se ha elaborado el siguiente script acorde a lo detallado en el capítulo 4, es importante mencionar que se ha configurado tanto del lado del CPE como de matriz considerando los cambios necesarios en cada caso con respecto a las direcciones IP.

```
config vpn ipsec phase1
    edit "VPN_NOMBRE_AGENCIA/ATM"
        set interface "nombre_interfaz_wan/vlan"
        set local-gw x.x.x.x
        set peertype any
        set remote-gw x.x.x.x
        set psksecret xxxxxxx
    next
end
```

Fase 2: para levantar la fase 2 se ha elaborado el siguiente script acorde a lo detallado en el capítulo 4.

```
config vpn ipsec phase2
```

```
    edit "VPN_NOMBRE_AGENCIA/ATM "
        set phase1name "NOMBRE_VPN_FASE_1"
        set src-addr-type ip
        set dst-addr-type ip
        set src-start-ip x.x.x.x
        set dst-start-ip x.x.x.x
    next
end
```

Con respecto a las configuraciones de autenticación y encriptación se han tomado las que vienen por defecto, que consiste en una tabla que asocia la primera coincidencia encontrada, las mismas cumplen con los requisitos de seguridad necesarios sin descuidar el rendimiento del equipo, el análisis se realizó en el capítulo 2.

```
set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1 3des-sha1
```

Figura 41. Configuración de autenticación y encriptación fase 1 Ipsec vía CLI

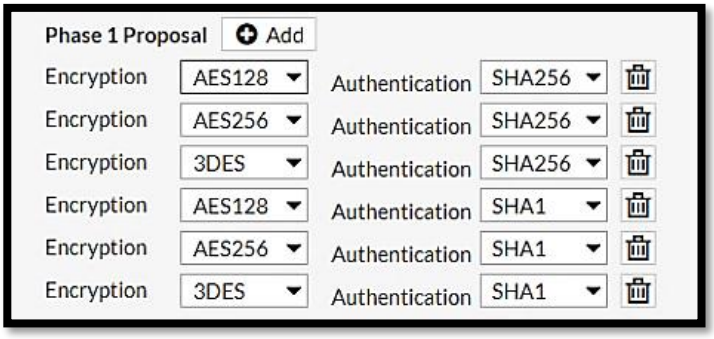

Figura 42. Configuración fase 1 Ipsec vía web

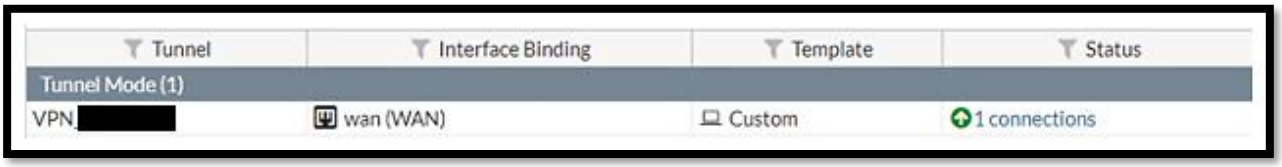

Figura 43. Estado VPN Ipsec lado remoto

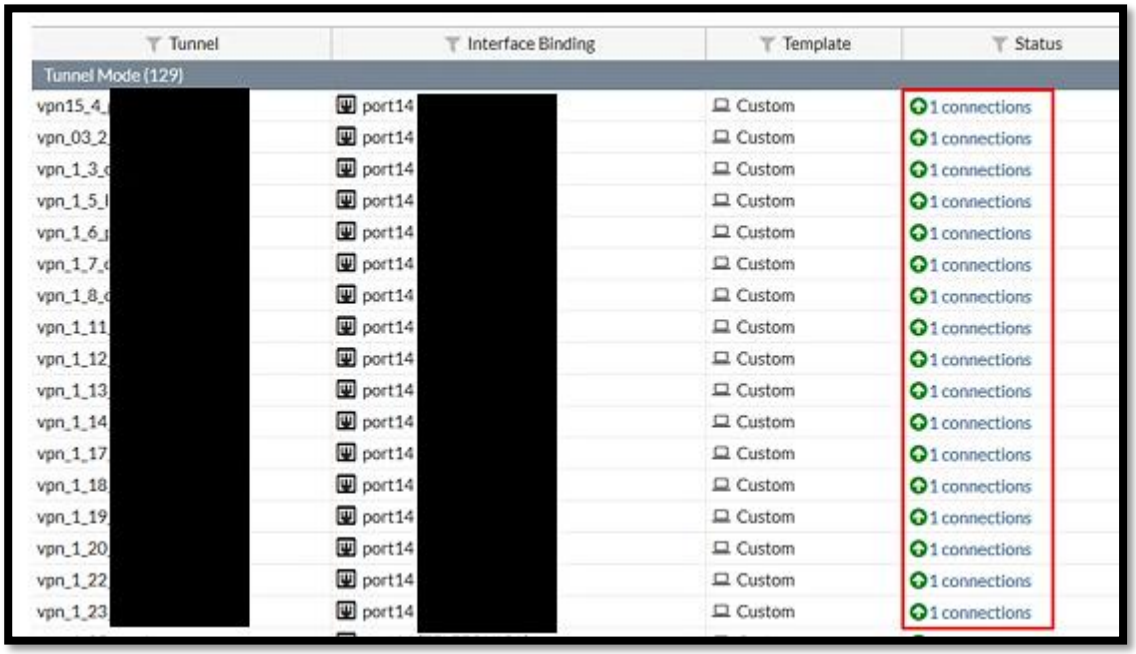

Figura 44. Estado VPNs matriz

Luego de haber validado que el túnel se encuentra Up se procede con la creación de las direcciones IP del servidor remoto y del enlace local, para ello se creó el siguiente script.

```
config firewall address
    edit "ATM"
        set subnet x.x.x.x 255.255.255.255
    next
end
config firewall address
```

```
    edit "NOMBRE_DIRECCION_IP_SERVIDOR_TRANSACCIONES"
        set subnet x.x.x.x 255.255.255.255
    next
end
```

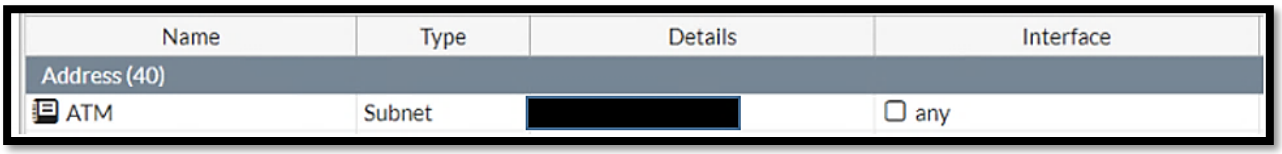

Figura 45. Dirección IP ATM

Con las direcciones IP creadas se procede con la configuración de la política que permita el tráfico entre el ATM y matriz, el script elaborado es el siguiente.

```
config firewall policy
    edit 9
        set name "vpn_out"
        set srcintf "nombre_interfaz_lan/servidor"
        set dstintf "nombre_interfaz_wan/vlan "
        set srcaddr "ATM/Servidor_transacciones"
        set dstaddr "ATM/Servidor_transacciones"
        set action ipsec
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set inbound enable
        set outbound enable
```

set vpntunnel " *VPN_NOMBRE_AGENCIA/ATM* "

next

end

5.4. Configuración de equipos FortiGate en herramienta FortiManager

Para agregar un equipo a la herramienta Fortimanager es necesario que exista conectividad origen-destino, para esto se usa la que ya existe entre Orion y cada uno de los CPEs mediante la IP Loopback de monitoreo, a continuación, los pasos a seguir.

1) Ingreso al FortiManager

2) Seleccionar la opción “Device Manager”

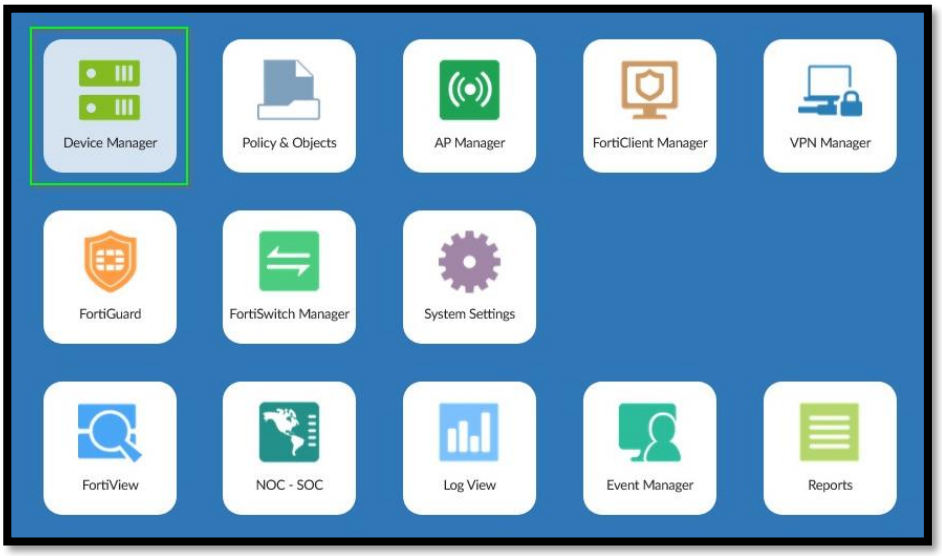

Figura 46. Opción Device Manager

3) Seleccionar el ADOM del cliente

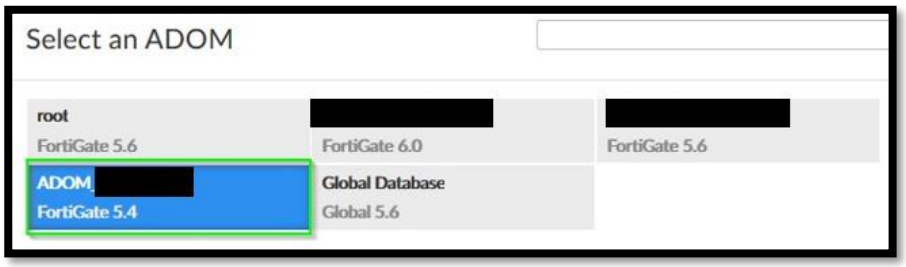

Figura 47. ADOM cliente

4) Seleccionar opción para agregar un nuevo dispositivo.

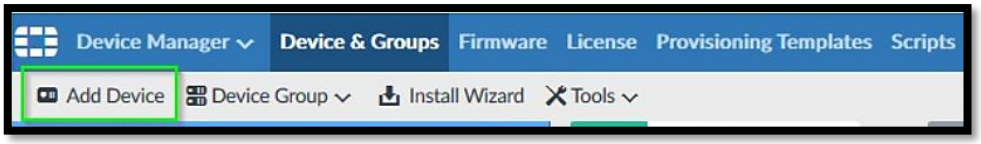

Figura 48. Opción de agregar nuevo equipo

5) Ingreso de credenciales para acceso remoto al equipo

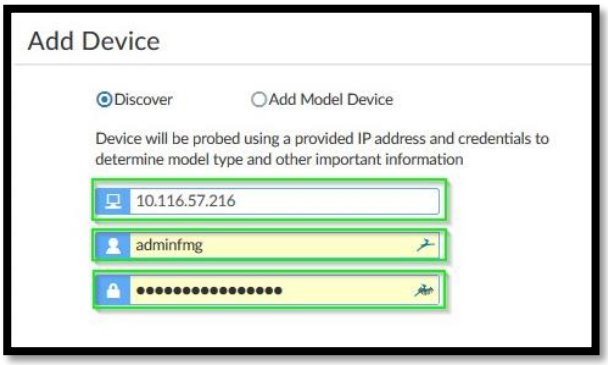

Figura 49. Credenciales de acceso remoto

Figura 50. Descubrimiento del equipo

6) Luego de haber descubierto el equipo se visualiza la información tomada de forma remota.

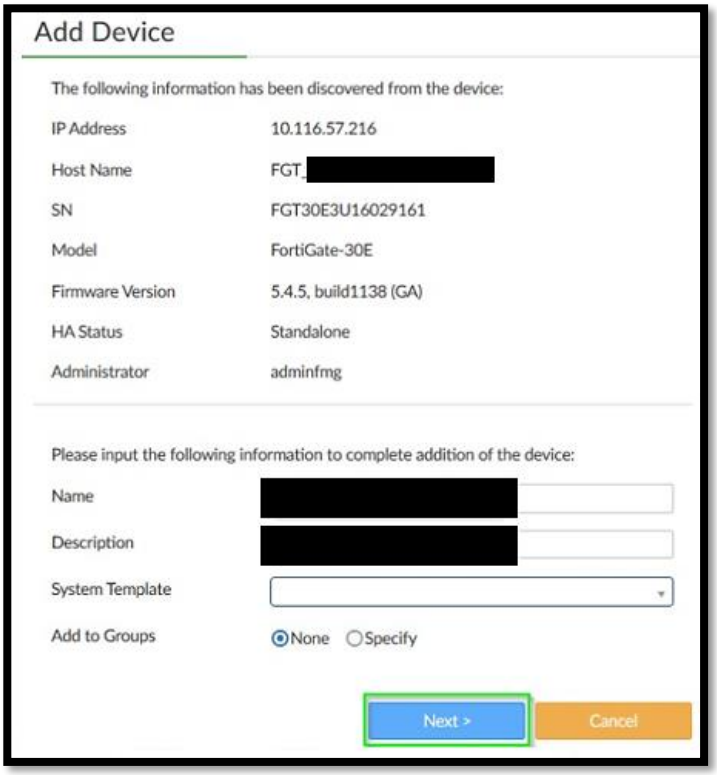

Figura 51. Información del equipo remoto

7) Con la información del descubrimiento validada se procede a la creación de estructura de alojamiento del equipo en la herramienta.

Figura 52. Creación de estructura de alojamiento del equipo

Figura 53. Estructura de alojamiento completada

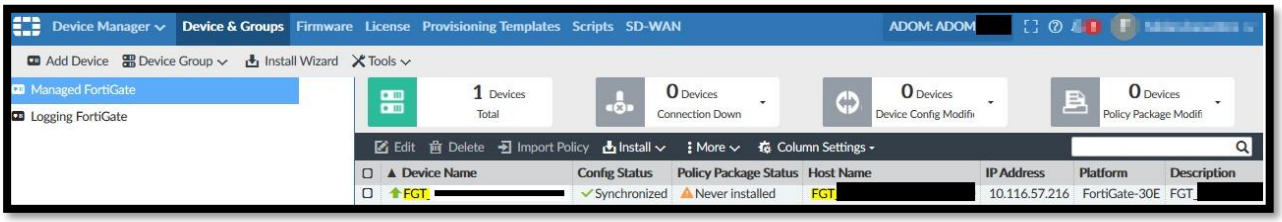

Figura 54. Equipo agregado al FortiManager

8) Con el mismo procedimiento anterior se agrega al resto de equipos FortiGate a la herramienta.

Figura 55. Equipos FortiGate agregados al FortiManager

CAPITULO VI

RESULTADOS

6.1. Validación funcionamiento túnel IPsec

Una vez realizadas las configuraciones sobre los equipos FortiGate tanto del lado del ATM como de matriz, se valida lo siguiente:

6.2. Estado VPN

Figura 56. Estado VPN Ipsec vía web

Figura 57. Estado VPN vía CLI

Como se puede observar en la Figura 56 y Figura 57 el túnel Ipsec se encuentra levantado y existe tráfico sobre la política creada (Figura 59).

Figura 58. Política IPsec

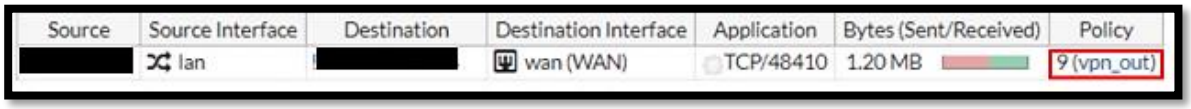

Figura 59. Tráfico sobre la política Ipsec

6.3. Datos en tránsito encriptados

Para validar que los datos en tránsito se encuentren encriptados se toma capturas de tráfico de diferentes puntos. En algunos puntos del cliente debido a la tecnología y

proveedor de última milla existe un equipo Mikrotik antes del CPE FortiGate, tal y como se visualiza en la Figura 60.

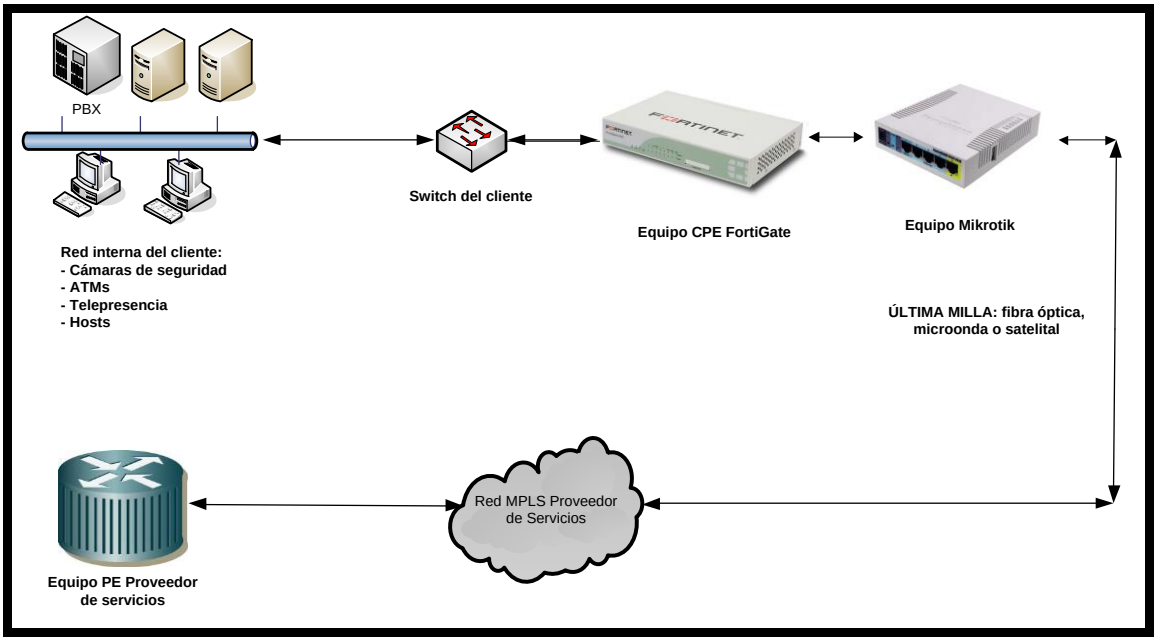

Figura 60. Diagrama enlace cliente con equipo Mikrotik

Se captura el tráfico sobre el equipo Mikrotik validando que el mismo se encuentra encriptado tal y como se observa en la Figura 61.

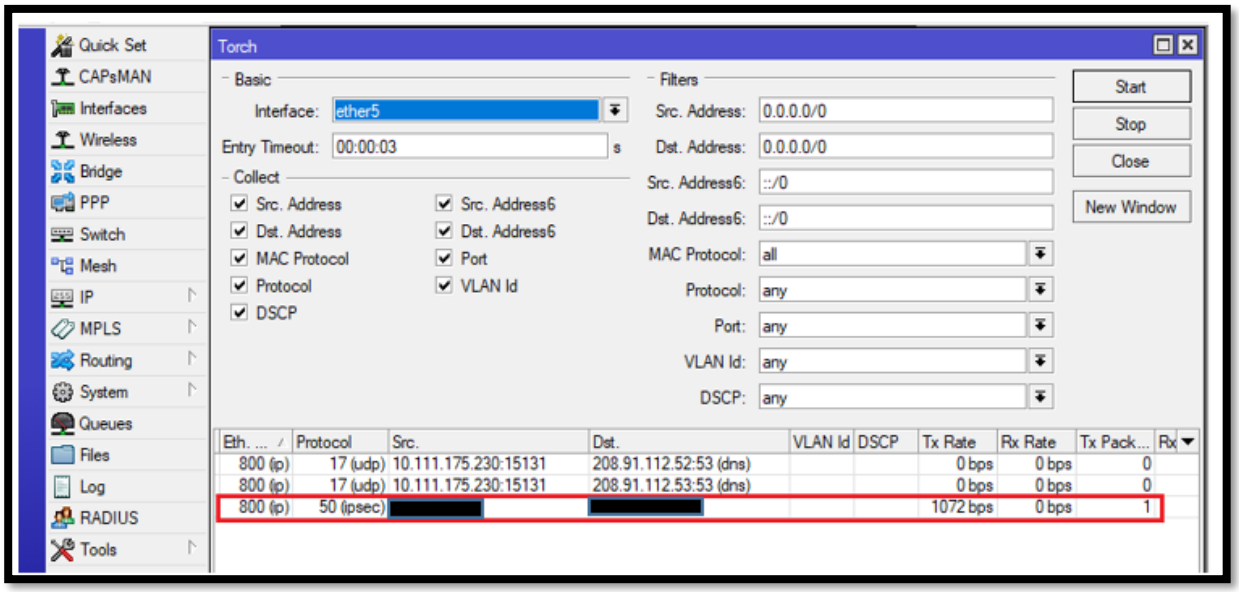

Figura 61. Captura tráfico equipo Mikrotik

6.4. Latencia

Una vez validado que los datos se encuentran encriptados es necesario validar si la latencia está acorde a la necesidad de la conexión, la misma dependerá de la tecnología de última milla de matriz (fibra óptica) y del punto remoto (fibra óptica, radio enlace o satelital) El parámetro será medido desde matriz hacia el punto remoto.

Fibra óptica: Se valida que la latencia promedio es de 2 ms, la misma se encuentra dentro de los valores normales.

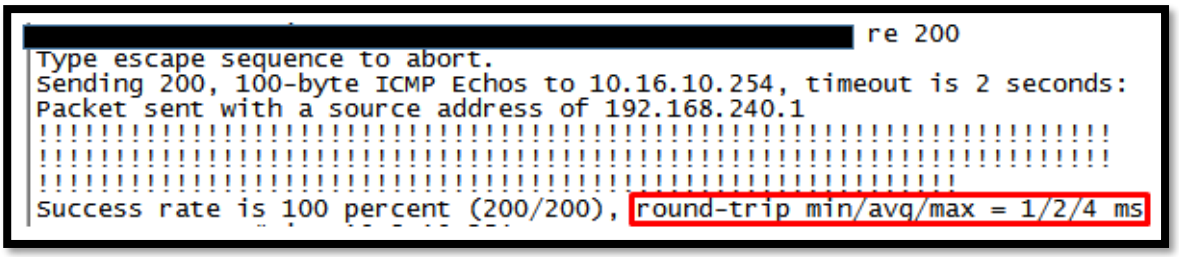

Figura 62. Conectividad matriz - sitio remoto (fibra óptica)

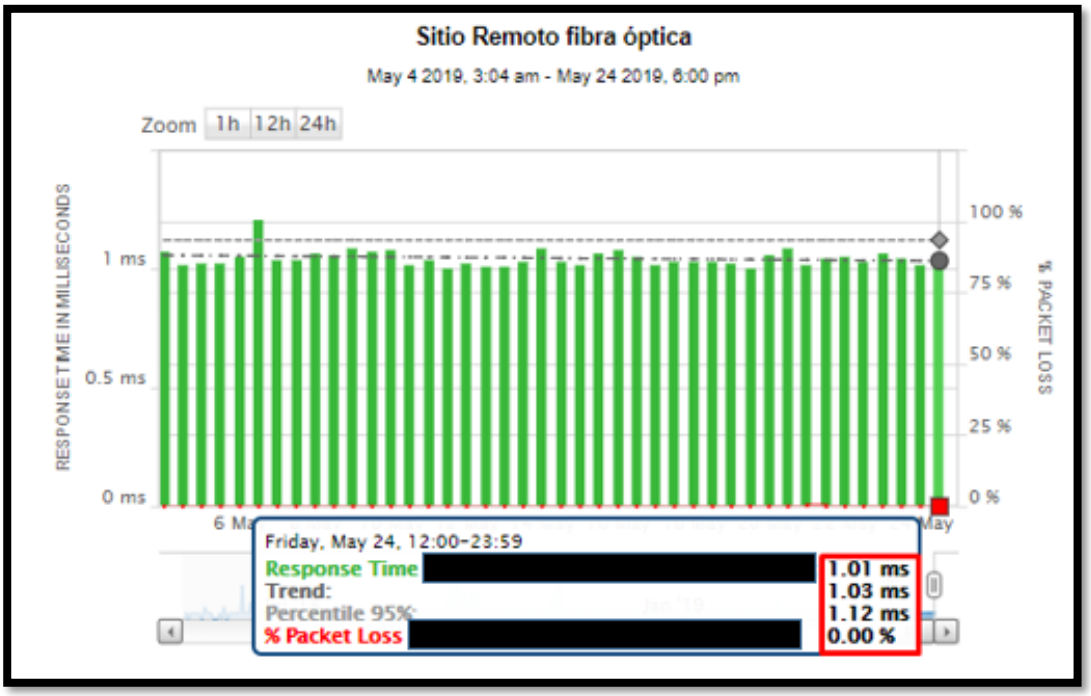

Figura 63. Medición de latencia desde Orion hacia sitio remoto (fibra óptica)

Radio enlace: Se valida que la latencia promedio es de 23 ms, la misma se encuentra dentro de los valores normales.

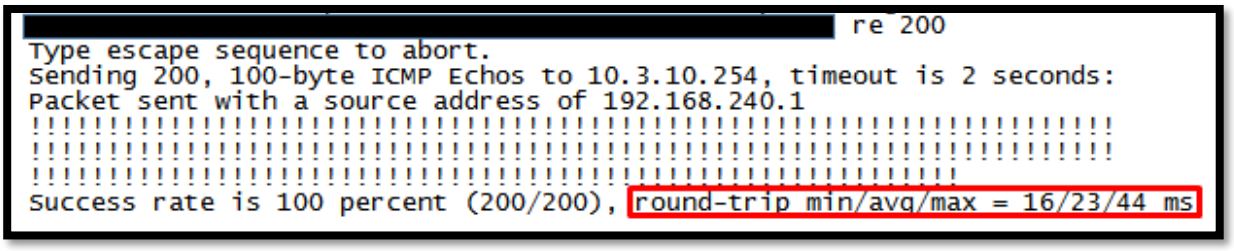

Figura 64. Conectividad matriz - sitio remoto (radio enlace)

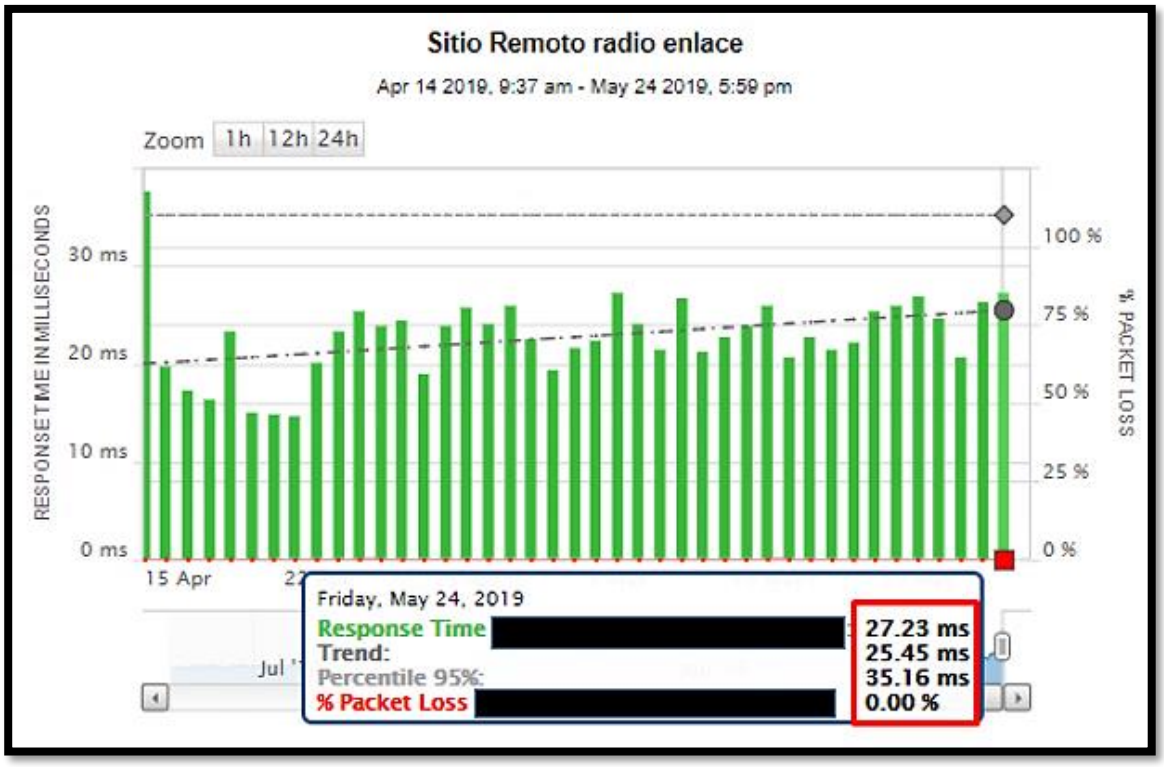

Figura 65. Medición de latencia desde Orion hacia sitio remoto (radio enlace)

Satelital: Se valida que la latencia promedio es de 652 ms, la misma se encuentra dentro de los valores normales. Debido a que esta tecnología tiene una alta latencia en comparación a fibra óptica y radio enlace, surge la necesidad de asegurar que la

comunicación no tenga inconvenientes, para ello se configura QoS en la comunicación, tal y como se muestra en la

```
CPN_MATRIZ_UIO#ping 10.7.1.254 source 192.168.240.1 re 200
Type escape sequence to abort.
Sending 200, 100-byte ICMP Echos to 10.7.1.254, timeout is 2 seconds:
Packet sent with a source address of 192.168.240.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (200/200), round-trip min/avg/max = 556/652/1032 ms
```

Figura 66. Conectividad matriz - sitio remoto (satelital)

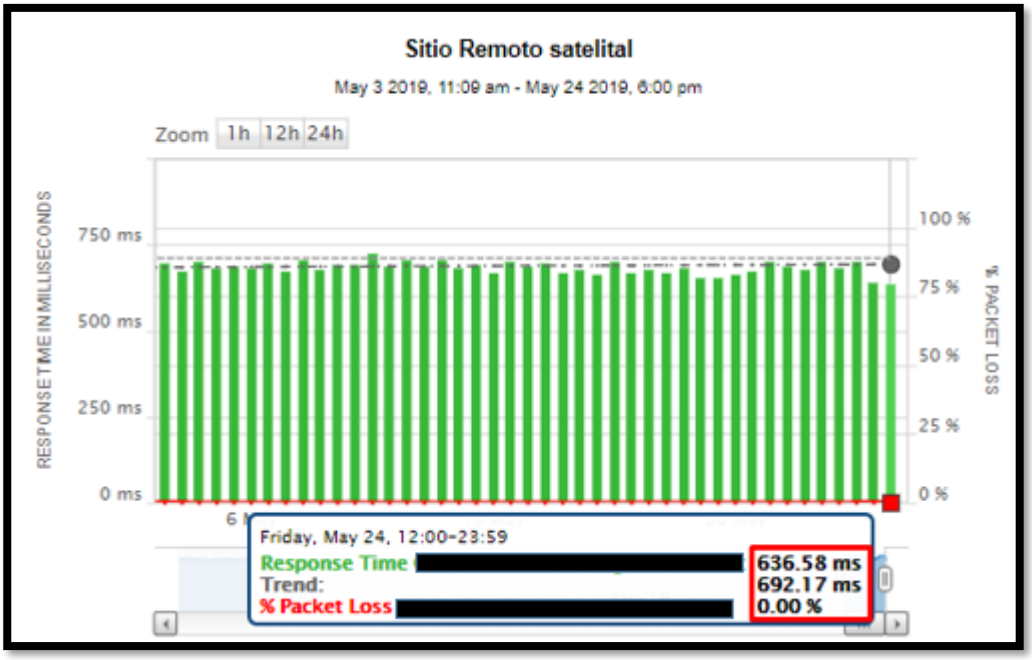

Figura 67. Medición de latencia desde Orion hacia sitio remoto (satelital)

6.5. Costos del Proyecto

A continuación, se presenta la propuesta económica en la cual se basó el presente proyecto, se contempla un valor recurrente por la prestación del servicio de encriptación para cada sitio donde se requiere aplicar dicha funcionalidad y un valor único de instalación y configuración inicial. El cliente final optó por esta modalidad debido a que el

proveedor de servicios incluye el servicio de encriptación, la gestión de los equipos FortiGate a través de su Centro de Operaciones de Seguridad, la atención de requerimientos e incidencias por el Centro de Soporte de Datos y el costo de renta del CPE, los costos detallados a continuación incluyen descuentos que el proveedor ha contemplado, considerando todos los servicios de datos fijos, móvil y digital que tiene contratado el cliente y precios preferenciales por ser partner directo de Fortinet

Tabla 6

Costo recurrente mensual del proyecto

Descripción	Cantidad	Costo Unitario	Costo Total Mensual (USD)	Precio Total Anual (USD)
Equipos para encriptación agencias y ATMs	129	45	5805	69.660

Tabla 7

Costo único de instalación y configuración inicial

Descripción	Cantidad	Precio Unitario	Precio Total Mensual (USD)
Instalación y configuración del servicio de encriptación	129	50	6450

A continuación, se realiza una comparación de costos entre la modalidad renta y compra en un plazo de 5 años, que es el tiempo del ciclo de vida de los equipos Fortinet.

Los costos en renta son los que actualmente el cliente ha empezado a facturar de forma recurrente, y los en modo compra han sido tomado de los precios de lista del fabricante Fortinet (el costo del servicio de encriptación es el mismo en los dos modos).

Tabla 8

Costo del Proyecto modo compra

Descripción	Precio
Costo de compra de equipo con soporte de 5 años	1.828,00
Costo servicio encriptación mensual por equipo	27,00
Costo servicio encriptación 5 años por equipo	1.620,00
Costo total de la solución por 5 años por equipo	3.448,00
Costo total de la solución de 129 equipos por 5 años	444.792,00

Tabla 9

Costo del Proyecto modo renta

Descripción	Precio
Costo renta de equipo mensual con soporte 5 años	18,00
Costo servicio encriptación mensual por equipo	27,00
Costo total mensual de la solución por equipo	45,00
Costo total de la solución por 5 años por equipo	2.700,00
Costo total de la solución de 129 equipos por 5 años	348.300,00

Como se puede verificar existe una diferencia a favor del modo renta de **$ 96.492** sobre el modo compra, lo que refleja un ahorro directo en 5 años en comparación de contratar el servicio con otro proveedor, adicional en modo renta el proveedor es quien asume el costo de reemplazo de equipo en caso de avería de este.

Figura 68. Ciclo de vida equipos Fortinet

Concretamente en el apartado del firmware se definen dos fechas distintas: End Of Engineering Support (EOES) y End Of Support (EOS). La primera fecha (EOES) se refiere a: pasada la fecha definida, el personal de soporte continuará resolviendo tickets para dicha versión de firmware, pero no se desarrollarán más parches para la misma incluso en el caso en el que se detectara algún bug desconocido. En cambio, al alcanzar la fecha definida en la columna EOS, el departamento de soporte no atenderá más tickets que se abran con dicha versión de firmare.

CAPITULO VII

CONCLUSIONES Y RECOMENDACIONES

7.1. Conclusiones

- Se implementó de manera exitosa la solución de encriptación de datos en una Entidad Financiera Ecuatoriana, mediante la configuración de VPNs IPsec entre matriz y los diferentes sitios que cuentan con un ATM, el funcionamiento fue validado por los responsables del área de TI de la Empresa.
- La configuración de las VPNs Ipsec se realizó mediante CLI, debido a que la latencia en los enlaces satelitales dificultaba el acceso vía https.
- Se validó que el tráfico en tránsito capturado en la comunicación entre el ATM y la sede de matriz se encuentra encriptado. Cumpliendo con la norma de control de las seguridades en el uso de transferencias electrónicas SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103, específicamente con el punto que indica que la Cooperativa debe *contar con una plataforma tecnológica que permita una encriptación sólida*
- Se verifica que la latencia en la comunicación entre los diferentes ATMs y la sede matriz se encuentra dentro de los parámetros normales, la misma se encuentra estrechamente relacionada con la tecnología de última milla utilizada (fibra óptica, radio enlace y satelital). Únicamente en el caso satelital se tuvo que configurar QoS para asegurar una comunicación adecuada.

- La seguridad en la comunicación se robustece al encriptar los datos en tránsito y tener canales dedicados de datos exclusivos para la Entidad Financiera desde matriz hacia cada uno de los ATMs.
- Considerando el análisis costo vs beneficio de los diferentes fabricantes de equipos firewall, la Entidad Financiera optó por Fortinet, en el capítulo 3 se brinda un mayor detalle.
- La herramienta de monitoreo Orion de Solarwinds fue de gran ayuda para tener una gestión centralizada de todos los equipos FortiGate, se logró respaldar configuración, obtener parámetros de desempeño de red de cada uno de los enlaces y ejecución de scripts en los mismos.
- Como alcance adicional al proyecto se logró agregar los equipos FortiGate a la herramienta Forti Manager, esto debido a que usa para la conexión las mismas IP de gestión de Orion. La herramienta será de gran ayuda para la gestión centralizada de los equipos, considerando que la Entidad Financiera prevé un crecimiento del 4% con respecto al número de agencias/ATMs a nivel nacional.

7.2. Recomendaciones

- Se recomienda realizar una revisión a detalle sobre el consumo de ancho de banda de cada uno de los enlaces, esto debido a que se detectó saturación en varios de ellos.
- Debido a que se prevé un crecimiento a mediano plazo en el número de agencias y cajeros de la Entidad Financiera, se recomienda completar y afinar la utilización de la herramienta FortiManager que ayuda a una gestión centralizada de los equipos FortiGate, que al momento ya se encuentran agregados.
- Los ciberataques a entidades financieras representan pérdidas cercanas al 9% de sus ingresos netos. El dato surge de una investigación publicada por el Fondo Monetario Internacional (FMI) en la que se analiza el riesgo que representan los ciberataques para el sector financiero a nivel global, por lo que se recomienda validar opciones de seguridad en el resto de la red de datos cuyo costo de implementación o mantenimiento se encuentra plenamente justificado.
- Se recomienda apoyar al proceso de control de cambios interno mediante la unificación del firmware de cada uno de equipos FortiGate.

REFERENCIAS

Alonso, J., Fernández, J., Figuerola, C., & Zazo, A. (2006). Redes Privadas Virtuales. *Departamento de Informática y Automática- Univesidad de Salamanca*, 106.

Alvarez, D. (s.f.). Enciptación. *Univesidad Católica "Nuestra Señora de la Asunción"*, 18.

Alvarez, L., & Solares, P. (2005). Seguridad Informática (Auditoría de Sistemas). *Universidad Iberoamericana*, 117.

Araya, S., Carvajal, C., & Llico, A. (s.f.). Utilización y Aplicación de Túneles IPsec en ambiente de VPN empresarial. *Universidad Técnica Federico Santa María*, 6.

Check Point Software Technologies Ltd. (01 de 03 de 2019). *Check Point IPSec VPN Software Blade*. Obtenido de https://www.checkpoint.com/products/ipsec-vpn-software-blade/

Check Point Software Technologies Ltd. (s.f.). Check point infinity architecture-the cyber security architecture of the future. *Check point software technologies ltd*, 20.

Cisco. (s.f.). *Cisco*. Recuperado el 20 de 01 de 2018, de https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.pdf

Cisco Systems, Inc. (2006). IPsec VPN WAN Design Overview. *Cisco*, 52.

Cisco Systems, Inc. (2016). IPSec Reference, StarOS Release 20. *Cisco*, 166.

Cisco Systems, Inc. (2018). *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.2.* San José.

Cisco Systems, Inc. (24 de 02 de 2019). *Cisco Systems, Inc*. Obtenido de https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-ipsec/index.html

Cisco Systems, Inc. (2019). Remote and Mobile Assets Design and Implementation Guide. *Cisco Systems, Inc*, 120.

Cisco Systems, Inc. (s.f.). Introduction to Secure Sockets Layer. *Cisco*, 12.

Cisco Systems, Inc. (s.f.). IPSec, VPN, and Firewall Concepts. *Cisco*, 14.

Damico, T. (2009). *Inquiries Journal*. Recuperado el 06 de 01 de 2019, de http://www.inquiriesjournal.com/articles/1698/a-brief-history-of-cryptography

ESET. (s.f.). Cifrado de la Información. *ESET*, 26.

Fortinet . (02 de 03 de 2019). *Fortinet*. Obtenido de Actualizaciones del soporte de IPsec para el cifrado aead de ChaCha20 / Poly1305

Fortinet, Inc. (2018). Fortigate 900D. *Fortinet, Inc*, 6.

Fortinet, Inc. (2019). FortiGate/FortiWiFi 30E. *Fortinet, Inc*, 6.

Fortinet, Inc. (2019). FortiGate/FortiWiFi 50E Series. *Fortinet, Inc*, 6.

Fortinet, Inc. (23 de 03 de 2019). *Fortinet*. Obtenido de https://www.fortinet.com/products/management/fortimanager.html

Gartnet Inc. (28 de 07 de 2019). *Gartner*. Obtenido de https://www.gartner.com/en/about

gbadvisors. (28 de 07 de 2019). *gbadvisors*. Obtenido de https://www.gb-advisors.com/es/cuadrante-de-gartner/

González, A. (2006). Redes Privadas Virtuales. *Universidad Autónoma del Estado de Hidalgo*, 202.

Gordon, M. (16 de 02 de 2011). *Micrium, Inc.* Obtenido de https://www.embedded.com/print/4213208

Hayoz, M. (2003). Introducing SSL The Secure Sockets Layer Protocol. *University of Freiburg i. Ue., Switzerland*, 19.

Inside Secure. (s.f.). Internet protocol security (ipsec) guide. *Inside Secure*, 12.

Instituto Nacional de Ciberseguridad. (s.f.). Protección de la Información. *Instituto Nacional de Ciberseguridad*, 23.

INTECO. (s.f.). La Criptografía desde la antigua Grecia hasta la máquina Enigma. *Instituto Nacional de Tecnología de la Comunicación - España*, 12.

Internet Engineering Task Force (IETF) . (2011). IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. *RFC 6071*, 63.

Kaspersky. (09 de 03 de 2017). *Kaspersky*. Recuperado el 13 de 01 de 2019, de https://latam.kaspersky.com/about/press-releases/2017_los-bancos-gastan-tres-veces-mas-en-seguridad-informatica

Luján, E. F. (2005). Seguridad en ip con el protocolo ipsec para IPV6. *Universidad de San Carlos de Guatemala*, 158.

Newport Networks. (2006). IPsec in VoIP Networks . *Newport Networks Ltd*, 5.

Nsit. (10 de 03 de 2019). *Nsit*. Obtenido de fortinet vs cisco: ¿cuál es la mejor opción?: https://www.nsit.com.co/fortinet-vs-cisco-cual-es-la-mejor-opcion/

Oficina de la Seguridad para las Redes Informáticas. (s.f.). Metodología para la Gestión de la Seguridad Informática. *Oficina de la Seguridad para las Redes Informáticas*, 68.

Palo Alto Networks. (2019). Pan-os administrator's guide. *Palo Alto Networks*, 976.

Pérez, S. (2001). Análisis del protocolo IPSec: el estándar de seguridad en IP. *Comunicaciones de Telefónica I+D* , 14.

Ribera, G. (05 de 01 de 2019). *Objetivos de la seguridad informática*. Obtenido de https://infosegur.wordpress.com/tag/disponibilidad/

Rodriguez, C. (2011). Vpns a través del protocolo ipsec y administración de seguridad en routers cisco. *Universidad libre*, 106.

Rouse, M. (28 de 07 de 2019). *WhatIs*. Obtenido de https://whatis.techtarget.com/definition/Gartner

Soriano, M. (s.f.). Seguridad en redes y seguridad de la información. *IMPROVET*, 80.

Superintendencia de Economía Popular y Solidaria. (23 de noviembre de 2017). *Superintendencia de Economía Popular y Solidaria.* Obtenido de Superintendencia de Economía Popular y Solidaria: https://www.seps.gob.ec/documents/20181/25522/Resolucio%CC%81n%20No.%20SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103.pdf/dfb837e2-31e1-498d-badf-430ad0dd1c4b

Tanenbaum, A. (2012). *Redes de Computadoras.* Estado de Mexico: Pearson.

Tomás, J., & Malgosa, J. (2008). Servicio VPN de acceso remoto basado en SSL mediante Openvpn. *Universidad politécnica de cartagena* , 167.