Trabajo Fin de Grado

Envío de información Difusión Limitada de forma segura mediante tunelización a través de medios no seguros

Aarón Jurado González

Director académico: Jorge Ortín Gracia

Director militar: Tte. Andrés Jesús González Ruiz

Centro Universitario de la Defensa-Academia General Militar

2022

Repositorio de la Universidad de Zaragoza – Zaguan http://zaguan.unizar.es

PÁGINA EN BLANCO

Agradecimientos

Querría agradecer la ayuda y apoyo que me han dado todas aquellas personas que han estado presentes en mi formación y mis años de academia.

En primer lugar quiero agradecer a los componentes de la Compañía de Transmisiones de la Brigada “Aragón I” durante las prácticas externas, en especial al Teniente González Ruiz, quien ha sido mi tutor militar, y al Sargento Alfonso, quien me concedió una entrevista. Ambos me han ayudado enormemente a enfocar el proyecto y a solventar las dudas que me iban surgiendo.

En segundo lugar querría agradecer la labor del profesor Ortín, mi tutor académico, quien me ha ayudado en todo momento con la confección del proyecto.

Finalmente, me gustaría hacer énfasis en mi familia, pareja y amigos, sin los cuales no solo este proyecto, si no mis años de academia hubieran sido muchísimo más difíciles. A mi madre, Ana Belén, y mi hermana Salma, quienes han sido un apoyo constante y que, pese a las dificultades y reveses siempre han estado apoyándome. A mi pareja, Patricia, por darme fuerzas y motivación por mala que fuese la situación, además de ser un referente y hacer que quiera mejorar y crecer a su lado. Y a mis amigos, quienes a pesar de la distancia y las dificultades siempre han estado apoyándome.

A todos, muchas gracias por creer en mi y hacer que llegue hasta aquí.

RESUMEN

La seguridad en las comunicaciones en el ámbito de la Defensa constituye una parte crucial del Esquema Nacional de Seguridad (ENS). Actualmente, en el contexto de un despliegue táctico de una Unidad del ET, esta dispone de medios propios de origen militar que se ven complementados con medios civiles. Esta dualidad en el uso de material militar y civil es motivada por las limitaciones que existen en la velocidad de transferencia de datos y de ancho de banda, siendo estas insuficientes para cumplir con las necesidades de los distintos usuarios de los puestos de mando. Con el objetivo de enmendar esta problemática se recurre a complementar a los medios propiamente militares con medios civiles, con los que satisfacer la demanda de transferencia de datos. Sin embargo, estos medios ajenos al desarrollo militar cuentan con carencias de seguridad que no los hacen apropiados para ser usados para transmitir información clasificada. En este proyecto se ha realizado una investigación cuyo eje central ha sido asegurar las comunicaciones realizadas, cuya información esté clasificada hasta Difusión Limitada, mediante la inclusión de VPNs.

Para la confección de este trabajo se han propuesto una serie de objetivos con los que abordar el tema en cuestión. En primer lugar este proyecto ha buscado conocer el funcionamiento y capacidades que ofrecen las Redes Virtuales, seguidamente ha buscado conocer la viabilidad que tiene la inclusión de VPN como un recurso seguro a la hora de intercambiar información clasificada hasta el nivel Difusión Limitada y, por último, exponer un caso de uso en el que incluir este recurso.

Inicialmente se ha realizado una investigación acerca de la situación actual de una Brigada del ET en el ámbito de las telecomunicaciones. Para ello se ha llevado a cabo una entrevista con personal experto del área de sistemas de información. A raíz de esta entrevista se han identificado los principales problemas relacionados con el intercambio de información entre puestos de mando, de qué medios dispone la Compañía y como opera. Seguidamente se ha realizado un estudio bibliográfico de las VPN, investigando qué tipos hay en función de la capa en la que operen, qué características tienen y realizando una comparación entre ellas. A continuación se ha expuesto un caso de uso en el que la aplicación de este recurso sería beneficioso para el funcionamiento de la Brigada, mejorando las capacidades de esta al contar con un mejor intercambio de información entre centros. Finalmente se han señalado los parámetros de seguridad que debe cumplir un túnel que sea empleado en un contexto táctico como el descrito anteriormente.

Las conclusiones de este proyecto son favorables a la implementación de redes VPN, no obstante hay que recalcar que el uso de este recurso se ve complementado de forma necesaria por equipos y medios certificados o aprobados por el CCN, sin los cuales no es posible asegurar un intercambio de información seguro, objetivo último de este proyecto.

Palabras clave

Difusión Limitada

Redes Privadas Virtuales

Medios no seguros

ABSTRACT

Defense communications security is a crucial part of the National Security Scheme (ENS). At present, in the context of a tactical deployment of a unit of the ET, it has its own military assets complemented by civilian assets. This dual use of military and civilian equipment is motivated by limitations on data transfer speed and bandwidth, which are insufficient to meet the needs of the different users of the command posts. In order to solve this problem, military means are being supplemented by civilian ones, in order to meet the demand for data transfer. However, these non-military means have security deficiencies that make them inappropriate to be used to transmit classified information. In this project, a research project has been carried out whose central axis has been to ensure communications with these means through the inclusion of VPN, using the protection provided by a tunnel through which classified information is passed up to the security level of NATO Restricted.

A number of objectives have been proposed for the preparation of this paper with which to address this subject. First of all, this project has sought to know the functioning and capabilities offered by Virtual Networks, then it has sought to know the viability of including VPN as a secure resource when exchanging classified information up to the level of NATO Restricted and, finally, provide a situation which includes the use of this resource.

Initially, research has been carried out into the current situation of a Land Army Brigade in the field of telecommunications. To this end, an interview was conducted with expert staff in the area of information systems of the transmission company. As a result of this interview, the main problems related to the exchange of information between command posts, the means available to the Company and how it operates under the conditions currently imposed on it were identified. Subsequently, a bibliographic study of the VPNs was carried out, investigating what types of VPN are available depending on the layer in which they operate, what characteristics do they have and comparing them. The following is a case in which the use of this resource would be beneficial to the functioning of the Brigade, enhancing its capabilities through improved exchange of information between centers. Finally, the safety parameters to be met by a tunnel used in a tactical context such as the one described above have been identified.

The conclusions of this project are favorable to the implementation of VPN networks, however it should be stressed that the use of this resource is complemented by equipment and means certified or approved by the CCN, without which it is not possible to ensure a secure exchange of information, the ultimate goal of this project.

KEYWORDS

NATO Restricted / EU Restricted

Virtual Private Network

Unsafe media

INDICE DE CONTENIDO

Agradecimientos.....I

RESUMEN.....II

Palabras clave.....II

ABSTRACT.....III

KEYWORDS.....III

INDICE DE FIGURAS.....VI

INDICE DE TABLAS.....VII

ABREVIATURAS, SIGLAS Y ACRÓNIMOS.....VIII

1 INTRODUCCIÓN.....1

2 OBJETIVOS Y METODOLOGÍA.....3

2.1 OBJETIVOS Y ALCANCE.....3

2.2 METODOLOGÍA.....3

2.2.1 Diagrama de Gantt.....4

2.2.2 Revisión Bibliográfica.....4

2.2.3 Entrevista.....4

2.2.4 Análisis DAFO.....5

3 ANTECEDENTES Y MARCO TEÓRICO.....7

3.1 Niveles de Clasificación.....7

3.2 Medios no seguros.....8

3.3 VPN y tunelización.....9

3.3.1 Tipos de VPN.....9

3.3.2 Ventajas e inconvenientes.....10

4 DESARROLLO: ANÁLISIS Y RESULTADOS.....13

4.1 Red VPN.....13

4.1.1 VPN con protocolo *Secure Shell* (SSH).....13

4.1.2 VPN con protocolo TLS.....14

4.1.3 VPN con estándar IPsec.....15

4.1.4 VPN con estándar MACsec.....16

4.1.5 Comparativa entre distintos tipos de VPN.....17

4.2 Comunicación entre dos puestos de mando a través de los cuales se comparte información del sistema BMS.....20

4.2.1 Comunicación entre centros.....20

4.2.2 Transferencia de datos del sistema BMS.....22

5 CONCLUSIONES.....31

6 REFERENCIAS BIBLIOGRÁFICAS.....32

7 ANEXOS.....35

7.1 ANEXO I: Diagrama de Gantt.....35

7.2 ANEXO II: Entrevista realizada a personal experto en el área de sistemas de información.....37

7.3 ANEXO III: Análisis DAFO.....40

7.4 ANEXO IV: Ubiquiti airGrid M5, modelo AG-HP-5G27.....41

7.5 ANEXO V: Mecanismos de seguridad de los radioenlaces Ubiquiti.....42

7.6 ANEXO VI: Firewall CISCO Firepower Thrat Defense, Firepower 1000 series.....43

7.7 ANEXO VII: DESCRIPCIÓN DEL SISTEMA BMS.....44

7.8 ANEXO IV: Requisitos criptológicos de seguriadad requeridos por un túnel IPsec….46

INDICE DE FIGURAS

Figura 1: *Guía de equivalencias entre grados de clasificación de la información. Fuente: CCN-STIC 001, 2016*.....8

Figura 2: Site-to-site business scenario. Fuente: Cisco, 2007.....10

Figura 3: Remote acces VPN scenario. Fuente: Cisco, 2007.....10

Figura 4: Topología de red con protocolo SSH. Fuente: Burande et al., 2014.....14

Figura 5: CISCO Firepower Threat Defence, Firepower 1000 series. Fuente: Cisco, 2007.....22

Figura 6: Esquema de red en el que se incluye el túnel IPsec. Fuente: Elaboración Propia.....25

Figura 7: Configuración inicial del router. Fuente: elaboración propia.....26

Figura 8: Inclusión de un túnel GRE. Fuente: elaboración propia.....26

Figura 9: Establecimiento del protocolo EIGRP. Fuente: elaboración propia.....27

Figura 10: Adyacencia establecida en el router del puesto de mando avanzado. Fuente: elaboración propia.....27

Figura 11: Configuración de ISAKMP e IPsec Transform-set. Fuente: elaboración propia.....28

Figura 12: Resumen de los protocolos aplicados al túnel. Fuente: elaboración propia.....28

Figura 13: Comprobación de la comunicación entre puestos de mando. Fuente: elaboración propia.....29

Figura 14: Elaboración del Diagrama de Gantt.....35

Figura 15: Especificaciones técnicas antena AG-HP-5G27. Fuente: Ubiquiti Networks, Datasheet AirGrid M5d.....41

Figura 16: Características de los firewall cisco de la serie 1000 auditados por el CCN. Fuente: CCN-STIC 105.....43

INDICE DE TABLAS

Tabla 1: Análisis DAFO. Fuente: elaboración propia.....36

Tabla 2: Protocolos IPsec y ESP. Fuente: CCN-STIC 807, 2022.....42

Tabla 3: Protocolos IKE. Fuente: CCN-STIC 807, 2022.....42

Tabla 4: Grupos Diffie-Hellman. Fuente: CCN-STIC 807, 2022.....43

Tabla 5: Esquema de cifrado. Fuente: CCN-STIC 807, 2022.....45

Tabla 6: Esquema MAC. Fuente: CCN-STIC 807, 2022.....45

Tabla 7: Función PRF en función del protocolo IKE. Fuente: CCN-STIC 807, 2022.....46

Tabla 8: Esquema de firma en función del estándar IKE. Fuente: CCN-STIC 807, 2022.....48

ABREVIATURAS, SIGLAS Y ACRÓNIMOS

AEAD: *Authenticated Encryption with Additional Data*

AES: *Advanced Encryption Standard*

AES- CMAC*: Cipher-based Message Authentication Code*

AH: *Autentication Header*

ATQH: *Satellite At-The-Quick-Halt*

BMS: *Battle Management System*

CCN: Centro Criptológico Nacional

EAP: *Extensible Authentication Protocol.*

ECC: *Elliptic curve cryptography*

ESP: *Encapsulating Security Payload*

ET: Ejército de Tierra

GCM: *Galois/Counter Mode*

GU: Gran Unidad

HF: *High Frecuency*

ICV: Código de verificación de integridad

IKE: *Internet Key Exchange*

IPComp: *Internet Protocol Payload Compression Protocol*

IPsec: *Internet Protocol Security*

IPv4: *Internet Protocol verion 4*

IPv6: *Internet Protocol verion 6*

LAN: *Local Area Network*

MAC: *Media Access Control*

MACsec: *Media Access Control Security*

MC3: Modernización de los sistemas de Mando Control y Comunicaciones

MINSIDEF: Minsterio de Defensa

MTU: *Maximum Transmission Unit*

MODP: *Modular Exponenital*

NAT: *Network Adress Translation*

OTAN: Organización del Tratado del Atlántico Norte

PN: *Packet Number*

PSK: *Pre-Shared Key*

PU: Pequeña Unidad

RRC: Red Radio Combate

RTP.: Red Táctica Principal

SA: Asociación de Seguridad.

SC2NET: Sistema de Mando y Control Nacional del Ejército de Tierra

SMA: *SonicWall Secure Mobile Access*

SSL: *Secure Socket Layer*

STIC*:* Servicio de Tecnologías de la Información y las Comunicaciones

TO: Teatro de Operaciones

TLS: *Transport Layer Security*

UE: Unión Europea

UHF.: *Ultra High Frecuency*

VHF: *Very High Frecuency*

VPN: *Virtual Private Network*

1 INTRODUCCIÓN

Actualmente el Ejército de Tierra (ET) se encuentra desplegado en un gran número de países y se enfrenta a un entorno cambiante, complejo y dispar. Cada misión supone afrontar retos nuevos bajo nuevas condiciones, por lo que tanto material como doctrinalmente el ET ha de ser polivalente y flexible.

Debido a la naturaleza de las operaciones a realizar y la escala de los despliegues se hace imperativo tener un sistema de comunicaciones fiable y seguro, capaz de operar en cualquier ambiente y condición. Para cubrir dichas necesidades el arma de Transmisiones cuenta con diversos medios que se agrupan en tres grandes áreas: Sistemas de Telecomunicaciones, Sistemas de Información y Seguridad de la Información.

Los Sistemas de Telecomunicaciones engloban todos aquellos medios que proporcionan intercambio de voz, datos e imágenes. Dependiendo de la entidad de la unidad y el uso que va a hacer de ellos se clasifican en: Red Radio de Combate (RRC), Red Táctica Principal (RTP) y Comunicaciones Satélite. La RTP es un sistema mallado cuyos nodos están interconectados por radioenlaces, dicha red es a su vez telefónica, telegráfica y ofrece intercambio de datos. La RRC es la red operada por todos aquellos componentes que no pueden estar integrados en la RTP y consiste en una red jerárquica basada en el intercambio de voz que utiliza bandas pertenecientes a HF (*High Frecuency*), VHF (*Very High Frecuency*) y UHF (*Ultra High Frecuency*). La comunicación vía satélite es el soporte principal de las comunicaciones entre PC (Puesto de Mando) de GU (Gran Unidad), dicha comunicación se realiza a través de terminales pertenecientes al Plan MC3[1] (Plan de Modernización de los sistemas de Mando Control y Comunicaciones) tales como el TLB 50-IP (Terminal Ligero Bibanda de alta capacidad y elevadas prestaciones) o el vehículo ATQH (*Satellite At-The-Quick-Halt*).

Atendiendo a la definición dada por el Mando de Adiestramiento y Doctrina (MADOC), los Sistemas de Información son el conjunto de medios para la recogida, almacenamiento y procesamiento de datos para la entrega de información y productos asociados, utilizados para la gestión de las misiones y operaciones. En la actualidad hay dos sistemas que integran dichos Sistemas de Información: SC2NET (Sistema de Mando y Control Nacional del Ejército de Tierra) y BMS (*Battle Management System*). SC2NET es una herramienta que dispone de aplicaciones de gestión táctica, información geográfica, mensajería y otras utilidades que facilitan el mando y control de las unidades, mientras que BMS es un software con capacidad de gestión y seguimiento para las PU (Pequeña Unidad) en TO (Teatro de Operaciones), dicho software integra además capacidades tales como planeamiento, posicionamiento, mensajería y un sistema de navegación entre otros.

Sin embargo, a pesar de la disponibilidad de los distintos sistemas mostrados anteriormente estos presentan limitaciones que pueden ver perjudicada la acción efectiva del mando y control de las unidades en el campo de batalla, como pueden ser la baja capacidad de transferencia de datos de la RRC o la conexión satelital. Entre las diversas soluciones al alcance del ET se encuentra el uso de medios o dispositivos que no sean exclusivos del ámbito militar, tales como una amplia gama de radioenlaces o el uso de Internet. No obstante, dichos medios presentan carencias en el área de la seguridad, ya que son dispositivos que han sido

1 El Plan MC3 tiene por objeto establecer el proceso de modernización de los sistemas de los sistemas de mando y control y comunicaciones del ET.

diseñados para el uso civil y el nivel de amenaza al que se ven expuestos es considerablemente menor comparado con sus homólogos militares.

El desarrollo de nuevos medios que potencien las capacidades actuales de los sistemas ya implementados en el ET, o en su defecto la adquisición de más equipos, supone pasar por un proceso que puede verse enormemente dilatado en el eje temporal y económico. El uso de estos medios comerciales puede suponer un complemento a los medios actuales de los que dispone el ET sin necesidad de desarrollar equipos propios, ya que estos dispositivos se encuentran en el mercado e incluso implementados ya en las unidades, como podría ser el caso de los radioenlaces Ubiquiti. Asimismo, el coste de implementar estos dispositivos es sumamente reducido en contraste con el desarrollo o adquisición de medios propiamente militares.

El caso de uso contemplado consiste en establecer comunicaciones desde un puesto de mando a otro, a través del cual será transportada información con un nivel de protección de Difusión Limitada, como lo es el sistema BMS. Aunque actualmente ya existen medios para dicha comunicación, su capacidad está muy limitada por lo que puede no ser suficiente para cubrir las necesidades de envío de la información del puesto de mando. Por este motivo, en algunos casos sería conveniente contar con capacidad de medios que no son propiamente militares (radioenlaces de marca Ubiquiti, Internet, telefonía pública, etc.). Dado que el empleo de estos medios no garantiza un nivel de seguridad óptimo para las comunicaciones militares, este caso de uso propone el uso de VPN con las que securizar dicho intercambio de información entre los dos centros de mando.

2 OBJETIVOS Y METODOLOGÍA

2.1 OBJETIVOS Y ALCANCE

El objeto de este trabajo es proporcionar una solución basada en la inserción de VPN (*Virtual Private Network*) que habiliten el intercambio de información catalogada como Difusión Limitada de forma segura a través de medios que actualmente no son considerados como tales.

Para la confección de este trabajo se realizarán los siguientes pasos:

1. Explicar los conceptos de VPN y túnel, poniendo de manifiesto sus ventajas e inconvenientes, así como los medios que emplea para que la información que transporta sea segura.
2. Analizar la viabilidad de la inclusión de VPN en los medios actuales de una unidad de Transmisiones del ET cuya información sea hasta Difusión Limitada.
3. Proponer un ejemplo práctico de la mejora en servicios y capacidades que puede ofrecer este protocolo en sistemas ya existentes dentro del ET, en este caso el sistema BMS.

Este trabajo pretende proponer un método viable con el que poder establecer un intercambio de información clasificada como “Difusión Limitada” por medios que actualmente no están catalogados como seguros por el CCN (Centro Criptológico Nacional). Queda fuera del alcance de este trabajo discernir o recomendar un medio concreto con el que realizar dicha comunicación, ya que lo que se propone es independiente de esta.

2.2 METODOLOGÍA

Este trabajo ha sido realizado durante el periodo de Prácticas Externas en la Compañía de Transmisiones 1 del Batallón de Cuartel General de la Brigada Aragón, ubicada en la base “San Jorge”, Zaragoza.

Para la confección de este proyecto se han llevado a cabo tanto técnicas cualitativas como cuantitativas.

Los procedimientos cualitativos empleados consisten, inicialmente, en un estudio bibliográfico en el que se recopila información acerca de las exigencias del CCN respecto a las condiciones impuestas a un medio para que pueda manejar información clasificada, en este caso hasta Difusión Limitada. Posteriormente se llevará a cabo una entrevista a personal experto en el área de sistemas de información, con la que dará una visión más amplia de las necesidades actuales de un puesto de mando desde el punto de vista de las transmisiones. Finalmente se procederá a explicar en qué consiste una VPN, sus tipos, beneficios y desventajas según la capa en la que estas operen.

Los procedimientos cuantitativos que han sido aplicados en este proyecto consisten en:

- Elaboración de un diagrama de Gantt con el que planificar la extensión temporal del proyecto, estableciendo hitos y objetivos intermedios.

- Confección de un análisis DAFO (Debilidades, Amenazas, Fortalezas y Oportunidades) con el que poder valorar la inclusión de estos nuevos medios, securizados mediante VPN.

Finalmente, se ha realizado un estudio de caso de uso con el que ejemplificar la solución propuesta. Para ello se ha diseñado una maqueta con la que simular la comunicación entre dos puestos de mando. En dicha maqueta se ha llevado a cabo la configuración de dos *routers* (uno por puesto de mando), y en la que se muestra la configuración necesaria para implantar el túnel que comunique dichos puestos.

2.2.1 Diagrama de Gantt

En las fases iniciales de la planificación y confección del proyecto resulta sumamente apropiado el uso de un diagrama de Gantt. Gracias al uso de este recurso es posible determinar y acotar en el tiempo la duración de las diversas tareas y objetivos de los que va a consistir el proyecto. Para este proyecto se ha hecho uso de un software libre con el que confeccionar el diagrama llamado *"Project Libre"*.

El Diagrama de Gantt tendrá como fecha de inicio la incorporación a la Compañía de Transmisiones 1 del Batallón de Cuartel General y como fecha final la semana previa a la incorporación en la Academia de Ingenieros, en Hoyo de Manzanares. Las fechas señaladas anteriormente comprenden desde el día 5 de Septiembre de 2022 hasta el 1 de Noviembre de 2022. El diagrama puede ser consultado en el Anexo I.

2.2.2 Revisión Bibliográfica

Durante el proceso de búsqueda de fuentes de información se hará uso de diversos recursos, entre los que destacan:

- Fuentes nacionales de carácter militar. Entre los recursos empleados se hará uso de diversos manuales en los que se detalla el uso del sistema BMS o cuales son los medios actuales del arma de transmisiones, entre otros.

- Guías STIC. Dichas guías son documentos publicados por el CCN con el objetivo de informar y dar recomendaciones en el área de seguridad a los distintos usuarios o unidades que vayan a hacer uso de material informático.

- Fuentes internacionales. Un elemento importante de cara a la obtención de información en este trabajo han sido los memorandos RFC (*Request For Comments*). Los RFC son documentos aprobados por la IETF (*Internet Engerieeng Task Force*). La IETF es una organización internacional sin ánimo de lucro cuyo propósito es la normalización, propuesta y mantenimiento de todos aquellos protocolos que están relacionados con Internet, actualmente es la mayor autoridad en este campo (RFC-3935, 2004).

- Trabajos académicos y de investigación. Finalmente, el uso de trabajos de investigación previos y TFG (Trabajo de Final de Grado), cuyas conclusiones y labores de investigación han sido usadas para confeccionar partes del presente proyecto.

2.2.3 Entrevista

Para la elaboración de la entrevista a personal experto se ha requerido de personal experto en el área de Sistemas de Información de la compañía. En dicha entrevista se han realizado una serie de preguntas orientadas a conocer la situación actual de la problemática, qué necesidades tiene la compañía y cuál sería la más aconsejable y/o factible. La entrevista queda recogida en el Anexo II.

2.2.4 Análisis DAFO

Finalmente, se ha realizado un análisis con el que obtener una visión más completa del proyecto. Se realizará un análisis DAFO. Con el que se evaluarán las debilidades, amenazas, fortalezas y oportunidades que pueda suponer la implementación de la solución propuesta en este proyecto. Dicho análisis queda recogido en el Anexo III.

PÁGINA EN BLANCO

3 ANTECEDENTES Y MARCO TEÓRICO

En este apartado se abordarán cuestiones que es necesario conocer antes de abordar el desarrollo de este proyecto. Puesto que la información que va a ser gestionada por la VPN será catalogada como Difusión Limitada se procederá a explicar los distintos niveles de clasificación de la Información. Posteriormente, se explicará qué es o qué se entiende por medio no seguro, puesto que en este trabajo se propone el uso de estos para conseguir una serie de ventajas a la hora de establecer una comunicación entre centros. Finalmente, se procederá a exponer en qué consiste una red VPN puesto que este es el recurso elegido para garantizar la seguridad de las comunicaciones por medios no seguros.

3.1 Niveles de Clasificación

A lo largo de la historia la información ha sido un bien preciado. Independientemente del ámbito en el que se maneje, su obtención ha supuesto una ventaja competitiva sobre el resto de individuos, organizaciones o Estados. Como consecuencia de esta asimetría en la obtención de información el resto de competidores tratan de hacerse con la información de la que carecen, este fenómeno puede darse en forma de espionaje (entre estados, en el ámbito empresarial, etc.), revelación de secretos o filtraciones[2].

Atendiendo a la sensibilidad de la información que posee el Gobierno de España, este reconoce la necesidad de que parte de esta no sea accesible al conjunto de la sociedad. Por ello establece la existencia de “materias clasificadas” en la Ley 9/68, de 5 de abril sobre secretos oficiales, en las cuales hace distinción entre dos categorías: Secreto y Reservado.

- SECRETO (S): comprende toda aquella información que precise del nivel más alto de protección cuya revelación no autorizada podría conllevar un riesgo a la seguridad o defensa del Estado.

- RESERVADO (R): se aplicará a toda información no catalogada como secreto cuya revelación no autorizada supusiese un riesgo para la seguridad o defensa del Estado.

Posteriormente se consideraron “materias objeto de reserva interna” aquellos datos, documentos objetos o informaciones cuyo conocimiento sin autorización previa pudiera ocasionar un daño o perjuicio al MINISDEF (Ministerio de Defensa). Las dos categorías pertenecientes a este ámbito son: Confidencial y Difusión Limitada.

- CONFIDENCIAL (C): se aplicará a toda aquella información no comprendida en las anteriores categorías y que cuya revelación no autorizada pueda amenazar la seguridad del MINISDEF, perjudicar sus intereses o el cumplimiento de cualquier tarea o misión.

- DIFUSIÓN LIMITADA (DL): se aplicará a toda aquella información no comprendida en

2 Una filtración es una violación de la seguridad en la que información sensible, protegida o confidencial es copiada, transmitida, vista, robada o usada por personal no autorizado.

las categorías anteriores y cuya revelación no autorizada suponga un perjuicio contra los intereses o la misión del MINISDEF.

Finalmente, la información que no está clasificada queda sujeta a dos últimas categorías: USO OFICIAL y USO PÚBLICO.

- USO OFICIAL: Comprende toda aquella información que, a pesar de no ser clasificada, su acceso queda restringido a personal autorizado.
- USO PÚBLICO: Engloba toda aquella información accesible por cualquier individuo, sin restricciones de ningún tipo.

Nacional	UNIÓN EUROPEA	OTAN
SECRETO	TRES SECRET UE /UE TOP SECRET	COSMIC TOP SECRET (CTS)
RESERVADO	SECRET UE / UE SECRET	NATO SECRET (NS)
CONFIDENCIAL	CONFIDENTIEL UE / EU CONFIDENTIAL	NATO CONFIDENTIAL (NC)
DIFUSIÓN LIMITADA	RESTREINT EU / EU RESTRICTED	NATO RESTRICTED (NR)
SIN CLASIFICAR USO OFICIAL USO PÚBLICO	EU SENSITIVE INFORMATION (EUSI) LIMITE PUBLIC	NATO UNCLASSIFIDED (UN) COMMERCIAL-MEDIAL-PERSONAL-PUBLIC- OPEN SOURCE

Figura 1: Guía de equivalencias entre grados de clasificación de la información. Fuente: CCN-STIC 001, 2016.

3.2 Medios no seguros

Un medio no seguro es todo aquel que no cuenta con los estándares o requisitos de seguridad mínimos para poder manejar información clasificada, en este caso hasta el nivel de Difusión Limitada. El objetivo de este trabajo es hacer seguras comunicaciones por medios que actualmente solo pueden ser usados para trabajar con información no clasificada, es decir, que no cuentan con el respaldo ni la certificación del CCN en este ámbito.

Entre los medios empleados por el ET hay algunos cuya información es cifrada por el propio dispositivo, como pueden ser los radioenlaces PR4G o Harris (en sus variantes 5800 y 7800) y otros que no, como pueden ser las comunicaciones vía satélite o los radioenlaces Ubiquiti (actualmente los radioenlaces de esta marca adquiridos por el ET son el AG-HP-5G27 y el Rocket M5. Los medios cuya información no es cifrada por el mismo necesitan un cifrador para poder manejar información clasificada. Sin embargo el número de cifradores es limitado, por lo que supone un recurso crítico. Asimismo, el uso de otros medios como es la comunicación a partir de medios ajenos al desarrollo militar presentan problemas para garantizar la seguridad de la información tratada, por lo que se hace necesaria la búsqueda de otras vías para securizar dichas comunicaciones.

En este trabajo se propone hacer uso de VPNs para proteger las comunicaciones clasificadas hasta Difusión Limitada ya que el nivel de seguridad ofrecido por estas es aceptado por el CCN para este nivel de información. Además, las VPNs suponen un recurso económico, fiable y escalable con el que se habilita el uso de estos medios no seguros para que complementen los medios ya existentes en el ET.

3.3 VPN y tunelización

Actualmente el ET se encuentra desplegado en países con condiciones materiales, geográficas y climáticas sumamente dispares. Desde Letonia hasta Mali, pasando por el Líbano, Turquía o Irak, los contingentes de las fuerzas armadas allí desplegados deben cumplir con misiones de distinta naturaleza, por lo que la capacidad de adaptación al entorno es clave.

Desde el punto de vista de las telecomunicaciones, el ET posee distintos medios para ser autosuficiente en cualquier escenario. No obstante, dichos medios poseen ciertas limitaciones, tales como la limitada capacidad de transferencia de datos de la RRC (expuesta en la introducción de este trabajo) o el elevado coste de obtención y reposición de dicho material de telecomunicaciones.

Con el objetivo de solventar dicha problemática, este trabajo propone hacer uso de medios o infraestructuras catalogados como no seguros. Actualmente la red pública más extendida a lo largo del planeta es Internet, por lo que se hará especial énfasis en dicho recurso. Asimismo, las comunicaciones que harán uso de esta red serán aquellas cuyo grado de confidencialidad no supere el de Difusión Limitada o sus equivalentes de los usados por la OTAN (Organización del Tratado del Atlántico Norte). Como estos medios no tienen las medidas de seguridad apropiadas para este tipo de comunicaciones se propone la implementación de VPNs para subsanar dichas carencias en el área de seguridad. Atendiendo a la definición dada por el Centro Criptológico Nacional (CCN) en su Guía de Seguridad de las TIC, una VPN es

"Una tecnología que establece una conexión virtual segura, conocida como "túnel", construida sobre una red física insegura (normalmente una red pública como Internet). Una VPN proporciona múltiples mecanismos de seguridad para proteger la información transmitida, y para permitir el acceso seguro y controlado a los recursos que protege" (CCN-STIC 836, 2022).

Asimismo, el protocolo de tunelización es definido como

"Un enlace virtual entre dos dispositivos utilizando una infraestructura previa. Hay diferentes técnicas para crear un túnel: encapsular el protocolo, conmutar por etiquetas, o crear circuitos virtuales. El túnel permite que las entidades conectadas utilicen protocolos que soporta la red subyacente." (CCN-STIC 401, 2015).

3.3.1 Tipos de VPN

Las VPN pueden ser diseñadas para responder a diversos tipos de necesidades. Los escenarios más recurrentes son: *site-to-site*, y acceso remoto (Cisco, 2007).

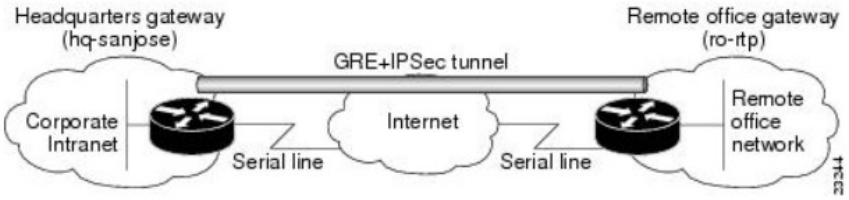
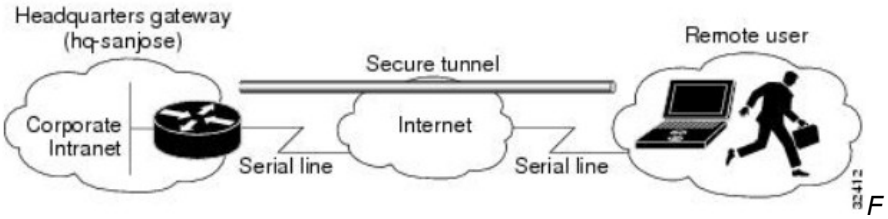


Figura 2: Site-to-site business scenario. Fuente: Cisco, 2007.

- *Site-to-site*: se da cuando dos redes necesitan comunicarse de forma segura. El caso de uso más recurrente es el de una red secundaria que necesita acceder a la estructura y recursos de la red principal.

- Acceso remoto: en este caso de uso un usuario accede a la red interna de la organización. El acceso remoto se habilita cuando desde dicha organización se le incluye dentro de la red virtual, habilitando un túnel que conecte al usuario con la organización.



F igura 3: Remote acces VPN scenario. Fuente: Cisco, 2007.

3.3.2 Ventajas e inconvenientes

La inclusión de redes VPN permite que los usuarios de esta accedan a recursos confidenciales (en este caso hasta el nivel Difusión Limitada o equivalentes) como si estuviesen dentro de una misma red, quedando excluidos el resto.

Entre sus principales ventajas destacan (CCN-STIC 836, 2022):

- Seguridad: emplea mecanismos de cifrado que protegen el flujo de datos. Asegura su integridad al emplear mecanismos de "hasing"[3] así como la autenticación. Finalmente, todo usuario que acceda a la red corporativa se ve sujeto a las mismas medidas de seguridad que aplica esta.

- Bajo coste: al aprovechar la infraestructura ya existente el operador solo debe proporcionar el servidor VPN e instalar el software de cada cliente.

3 Algoritmo matemático que transforma un conjunto de datos de entrada en una salida de longitud fija (CCN-STIC 401, 2015).

- Escalabilidad: en caso de querer aumentar el número de usuarios que hacen uso de la VPN basta con configurar su acceso y sus equipos de forma apropiada, ya que la red de infraestructura necesaria es pública.

No obstante, la implementación de VPN conlleva una serie de riesgos que hay que tener en cuenta, principalmente un mal cifrado de las comunicaciones.

PÁGINA EN BLANCO

4 DESARROLLO: ANÁLISIS Y RESULTADOS

En el siguiente apartado se procederá a exponer los distintos tipos de VPNs disponibles en función de la capa del modelo OSI en el que estas operen, finalizando en una sumarización de los distintos aspectos positivos y negativos de cada una y cuál es la más adecuada para la problemática que se expone en este proyecto. Posteriormente se expondrá un caso de uso en el que se incluye la inclusión de VPNs. Finalmente se realizará una maqueta en la que se incorporan todos los elementos que integran la topología de red del caso de uso propuesto, mostrando la configuración necesaria que debe ser realizada para la inclusión de un túnel IPsec.

4.1 Red VPN

Como hemos visto en apartados anteriores, existen varias formas de clasificar las VPN. Una primera aproximación al diseño de esta puede ser determinar si va a ser una VPN *site-to-site* o si por el contrario va a ser una red de acceso remoto. Con esta distinción definimos qué redes o usuarios van a estar comunicados dentro de esta VPN. Una vez hecho esto falta por saber qué tipo de túnel va a ser implementado para comunicar a las dos partes. Por cada capa del modelo TCP/IP[4] existe al menos un protocolo de tunelización. A continuación, se explicarán dichos protocolos y se determinará cual es el más apropiado para el objetivo de este trabajo.

4.1.1 VPN con protocolo *Secure Shell* (SSH)

El protocolo SSH trabaja en la capa de aplicación (CCN-STIC 836, 2022) Dicho protocolo establece un túnel que protege la información compartida entre dos aplicaciones de software. Un túnel que implemente el protocolo SSH consta de 4 componentes (Burande et al., 2014):

- Buscador web: se trata de la parte interesada en comunicarse con el servidor. Para conseguir comunicarse con el servidor el usuario debe cambiar la configuración del buscador para que este dirija el tráfico al cliente SSH, el cual funciona como un servidor *proxy*[5].

- Cliente SSH: servidor receptor del tráfico del buscador web. Dicho servidor encripta el mensaje y crea un túnel que conecta con el servidor SSH. El cliente SSH tan solo reconoce al servidor SSH que le haya sido indicado, por lo que el túnel que creará para establecer el intercambio de información solo podrá establecerse con dicho servidor.

- Servidor SSH: es el servidor que recibe el mensaje cifrado del cliente SSH a través del túnel. Tras desencriptar el mensaje este es transmitido al servidor web.

- Servidor web: recibe el mensaje y envía información en caso de que esta sea

4 Modelo TCP/IP: conjunto de protocolos que definen la comunicación entre dos dispositivos que se encuentren conectados a la red. Consta de 4 capas: aplicación, transporte, red y enlace/física.

5 Servidor que hace de intermediario entre un cliente y otro servidor.

solicitada. Los pasos a realizar en este nuevo intercambio de información son los análogos a los descritos anteriormente, pero desde el servidor web hacia el cliente SSH.

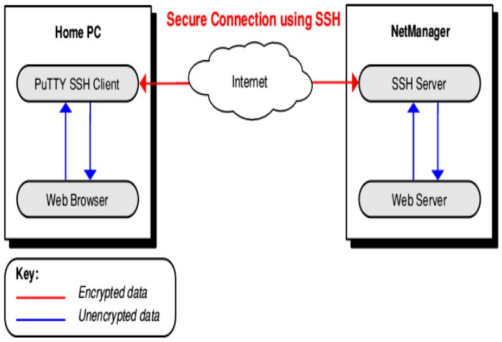


Figura 4: Topología de red con protocolo SSH. Fuente: Burande et al., 2014.

4.1.2 VPN con protocolo TLS

Las VPN que incluyen medidas de seguridad en la fase de intercambio de información entre aplicaciones constituyen las VPN de nivel de transporte (CCN-STIC 836, 2022). El protocolo de seguridad más extendido para este tipo de VPN es el TLS (*Transport Layer Security*), basado en la tercera versión de SSL (*Secure Socket Layer*).

El uso más común de este protocolo consiste en habilitar la conexión remota de un usuario que quiere acceder a una serie de aplicaciones ofrecidas por la red principal de la organización (CCN-STIC 836, 2022). Para acceder a dichas aplicaciones, el usuario debe abrir su navegador web y acceder a la aplicación deseada, por lo que no es necesario que éste instale ningún software.

Las VPN basadas en el protocolo TLS proveen de (RFC-8446, 2018):

- Autenticación: el servidor VPN (localizado en la red principal) siempre debe estar autenticado, el usuario de acceso remoto estará autenticado de forma opcional. Dicha autenticación puede darse por medio de criptografía simétrica[6], como puede ser una clave previamente compartida (PSK) o por criptografía asimétrica[7], usando algoritmos como "*Elliptic Curve Digital Signature Algorithm*" (ECDSA) o "*Edwards-Curve Digital Signature Algorithm* (EdDSA).

6 La criptografía simétrica consiste en el uso de una misma clave o criptografía por ambas partes de la comunicación.

7 La criptografía asimétrica consiste en el uso de distintas claves o parámetros criptográficos entre una parte y otra del túnel.

- Confidencialidad: el protocolo TLS asegura que la información enviada a través del túnel tan solo va a poder ser visualizada por el receptor y el destinatario al que se le ha dado acceso a ella. Sin embargo, el protocolo TLS no oculta la longitud de los paquetes que envía. Para subsanar esta potencial vulnerabilidad, tanto emisor como destinatario de la comunicación tunelizada son capaces de rellenar los paquetes que sean más cortos para que todos tengan la misma longitud.

- Integridad: una vez establecido el túnel la información que fluye por este no puede ser modificada sin que dicho cambio sea detectado.

Los principales componentes del protocolo TLS (RFC-8446, 2018) son:

- *Handshake*: fase inicial que sirve para autenticar a ambas partes, negocia los algoritmos criptográficos que se van a aplicar, establece qué claves se van a usar y proporciona los parámetros de seguridad al "*Record Protocol*".

- *Record Protocol*: transmite el mensaje, divide la información en bloques estándar, protege el flujo de datos y proporciona un resultado. Este protocolo utiliza los parámetros de seguridad establecidos en la fase de *Handshake*.

4.1.3 VPN con estándar IPsec

El estándar IPsec (*Internet Protocol Security*) opera en el nivel de capa de red (CCN-STIC 836, 2022) y es utilizado en configuraciones VPN *site-to-site* y de acceso remoto. IPsec son un conjunto de protocolos diseñados para proporcionar seguridad a los protocolos IPv4 (*Internet Protocol version 4*) e IPv6 (*Internet Protocol version 6*). Las VPN basadas en el estándar IPsec proporcionan acceso completo a la red remota, sin embargo, son difíciles de configurar ya que ofrecen un amplio abanico de opciones entre las que elegir.

- Confidencialidad: ni las cabeceras ni los datos van cifrados, por lo que los paquetes son susceptibles de ser interceptados e inspeccionados.

- Autenticidad: al carecer de protocolos de autenticación se corre el riesgo de que un usuario externo introduzca paquetes propios en el flujo de datos, haciéndolos pasar por propios.

- Integridad: al carecer de protocolos de integridad es posible que un agente externo intercepte y modifique los paquetes que son transportados por el túnel

El estándar IPsec integra varios protocolos con los que proteger las áreas de confidencialidad[8], autenticidad[9] e integridad[10]. Los principales mecanismos que aseguran el intercambio seguro de información (RFC-4301, 2005) son: *Authentication Header* (AH) y

8 Propiedad de la información que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.

9 Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Encapsulating Security Payload (ESP):

- AH: proporciona integridad y autenticación a la información en su origen, así como mecanismos anti-reenvío.

- ESP: proporciona los mismos mecanismos de seguridad que AH pero le añade confidencialidad. Dicha confidencialidad es proporcionada a través de criptografía simétrica usando algoritmos como AES-GCM (CCN-STIC 836, 2022). De acuerdo con el CCN, el uso de ESP es recomendable frente a AH, ya que aporta las mismas medidas de seguridad y además añade confidencialidad.

Ambos protocolos ofrecen control de acceso, aplicado a través de la distribución de claves criptográficas (RFC-4301, 2005) y la gestión del flujo de tráfico dictado por la SPD (*Security Policy Database*). Además de los protocolos ya mencionados, el estándar IPsec integra:

- Protocolo IKE *(Internet Key Exchange*): proporciona autenticación mutua entre origen y destino y establece una Asociación de Seguridad (SA). La SA incluye información secreta cuya función es establecer un AH o un ESP. Asimismo proporciona una serie de algoritmos criptográficos que pueden ser usados por las SA's para proteger el tráfico de red (RFC-7296, 2014).

- Protocolo IPComp (*Internet Protocol Payload Compression Protocol*): reduce el tamaño de los datagramas IP. IPComp mejora la transferencia de datos mediante la compresión de datagramas siempre y cuando los nodos tengan la suficiente capacidad de computación (RFC-3173, 2001).

IPsec cuenta además con dos modos de trabajo: modo túnel y modo transporte (CCN-STIC 836, 2022):

- Modo túnel: se utiliza este modo en escenarios *site-to-site*, es decir, cuando en ambos extremos del túnel se encuentra un servidor. En este modo al paquete se le añade una nueva cabecera IP cuyo objetivo será ocultar la información que viaja a través del túnel, así como proteger el paquete original.

- Modo transporte: este modo se utiliza para conectar dos equipos a través de la VPN de forma nativa. Al paquete original se le añade una cabecera IPsec. Sin embargo la cabecera original se mantiene, por lo que dicha información no está oculta.

4.1.4 VPN con estándar MACsec

Actualmente las VPN de nivel de enlace se basan en el estándar MACsec (*Media Access Control Security*). Dicho protocolo proporciona medidas de seguridad destinadas a la protección de datos en la capa de enlace en redes LAN (*Local Area Network*) y se encuentra definido en

10 Cualidad o condición de la información que garantiza que no ha sido modificada por personas no autorizadas.

IEEE 802.1AE (CCN-STIC 836, 2022).

El estándar MACsec permite que, tanto los dispositivos que se conecten a la red LAN como aquellos que conectan dichas redes, tengan garantizadas la confidencialidad de las tramas que transmitan. Además, permite tomar medidas contra las tramas transmitidas o modificadas por dispositivos no autorizados. MACsec facilita las siguientes utilidades:

- Asegurar el correcto funcionamiento de la red, tanto en el ámbito de la conectividad como en el de los servicios.
- Aislamiento de ataques de denegación de servicio.
- Localización de cualquier fuente de comunicación de red a la LAN de origen.
- Garantizar una comunicación segura entre redes, valiéndose de una LAN de transmisión.

Para hacer seguras las comunicaciones en el entorno LAN en el que está trabajando, el estándar MACsec integra los siguientes servicios de seguridad (CCN-STIC 836, 2022):

- Confidencialidad de datos: para este estándar se hace uso de un cifrado simétrico AES (*Advanced Encryption Standard*) en modo AEAD (*Authenticated Encryption with Additional Data*).
- Protección de la integridad de los datos sin conexión: MACsec utiliza un código de verificación de integridad (ICV) único para cada paquete (sin conexión). Con la implementación de este código cualquier cambio no autorizado en cualquier trama puede ser detectado.
- Autenticidad de datos en origen: con el empleo del código ICV se garantiza la identidad del emisor de la trama.
- Protección anti-reenvíos: al mensaje se le añaden números de secuencia en el campo PN (*Packet Number*).
- Arquitectura segura *hop-by-hop*: en cada nodo que sea gestionado por el estándar MACsec el paquete de información será cifrado y descifrado.
- Límite de retraso de recepción: existe la posibilidad de que algunos paquetes sean interceptados, modificados y posteriormente reenviados haciéndose pasar por propios. Para minimizar este riesgo el estándar MACsec implementa el parámetro "*bounded*", dicho parámetro determina el tiempo límite que debe pasar entre la emisión y la recepción del paquete. Este parámetro se implementa para que, en caso de intercepción, no de tiempo a modificar y reenviar el paquete, ya que quedan descartados todos aquellos que excedan el tiempo especificado en el parámetro "*bound*".

4.1.5 Comparativa entre distintos tipos de VPN

Cada uno de los tipos de VPN expuestos anteriormente aporta soluciones ante distintos tipos de necesidades. Algunas de las variables que afectan a la elección de uso de un tipo de VPN sobre otro son la seguridad, la complejidad de la misma o las necesidades de los clientes que vayan a usarlas.

A continuación, se procederá a comparar los distintos tipos de VPN disponibles, valorando sus ventajas e inconvenientes:

VPN con SSH

- Ventajas: Al ser un modelo de VPN a nivel de aplicación el túnel protege a dicho programa, por lo que cuenta con una gran variedad de opciones con las que configurar la VPN perteneciente a esa aplicación. El modelo SSH cuenta además con un servidor SSH y con otro de cliente, los cuales se comunican con buscador y servidor web respectivamente. Al no comunicarse directamente cliente y servidor añaden un elemento extra de seguridad al sistema (CCN-STIC 836, 2022).

- Inconvenientes: Como trabaja en el nivel de aplicación solo ofrece un túnel seguro por el que intercambiar información en el programa para el que se va a trabajar, por lo que tan solo ese intercambio de información queda protegido. Otra consecuencia de ser un protocolo que trabaja en el nivel de aplicación es que no proporciona protección al flujo de datos que operan en la capa de red (cabeceras IP)(CCN-STIC 836, 2022).

Debido a una mala programación hay ciertos parámetros de seguridad que pueden quedar inhabilitados por el usuario. Entre ellos destaca el modo "*none MAC*" (*Media Access Control*)[11] . Dado el caso de que este modo esté habilitado, todo flujo de datos que atraviese el túnel carecerá de integridad y autenticación (RFC-4251, 2006).

Otro aspecto a tener en cuenta es que, al ser un protocolo en el que interviene un servidor que hace de *proxy*, cabe la posibilidad de que un atacante externo trate de explotar distintas vulnerabilidades en nuestro sistema. Un ejemplo de ataque a la integridad de este sistema es el conocido como "*man in the middle*", mediante el cual un agente externo trata de suplantar la identidad del servidor del cliente con el objetivo de monitorizar el tráfico de datos. Un ataque de estas características se aprovecha de una posible falta de seguridad a la hora de compartir las claves de autenticación que van a ser usadas durante el establecimiento de la conexión SSH (RFC-4251, 2006).

Finalmente, este sistema puede ser apropiado para securizar accesos a información clasificada (hasta DL) realizados por una sola aplicación.

VPN con TLS

- Ventajas: el protocolo TLS ofrece unos mecanismos de seguridad fiables con autenticación de origen y un cifrado robusto de la información (tanto en su versión 1.2 como la 1.3). Además, posee controles de seguridad en *endpoints* y compatibilidad NAT (*Network Adress Translation*).

11 Modo *none Mac* es un modo

- Inconvenientes: el protocolo TLS, al ser estar basado en la capa de transporte, no otorga protección a la información de la capa de red (cabeceras IP). Por la propia arquitectura del protocolo, la autenticación del servidor es obligatoria pero no la del cliente, siendo esta una potencial vulnerabilidad ante un posible agente externo. Finalmente, el protocolo TLS solo protege el intercambio de información entre un usuario y una aplicación del sistema, por lo que tan solo queda protegido ese caso de uso en específico, no la totalidad de las comunicaciones.

Este tipo de VPN que operan en la capa de transporte son apropiadas en el supuesto de que un usuario quiera acceder a un servicio en concreto accesible por internet. Dado el caso una organización como puede ser el MINISDEF, puede optar por tener información clasificada accesible a través de la red pública de internet y que esta sea protegida por un protocolo TLS. El uso de este protocolo garantiza un nivel de seguridad óptimo y una forma fácil de acceso a los usuarios que precisen de dicha información (CCN-STIC 836, 2022).

VPN con IPsec

- Ventajas: Al ser un estándar diseñado para operar en la capa de red, IPsec ofrece protección a todo tráfico IP que pase por él. Asimismo, IPsec integra diversos protocolos que aseguran tanto la integridad del mensaje como la autenticación de las partes (AH), asegurando también su confidencialidad (ESP)(CCN-STIC 836, 2022).

- Inconvenientes: Debido a la flexibilidad que tiene a la hora de ser configurado, el estándar IPsec es complejo de configurar, operar y mantener. Como es un estándar diseñado para operar en el nivel de red no ofrece control de acceso específico a ciertos recursos, sino que son los usuarios quienes gestionan dicho acceso (CCN-STIC 836, 2022).

Por otro lado, el CCN publicó en febrero de 2022 la guía CCN-STIC 105 en la que “tiene como finalidad ofrecer a los organismos de la Administración un conjunto de productos o servicios STIC (Servicio de Tecnologías de la Información y las Comunicaciones) de referencia cuyas funcionalidades de seguridad relacionadas con el objeto de su adquisición han sido certificadas” (CCN-STIC 105, 2022, página 6). En dicha guía se ofrece como producto certificado por el CCN el software para clientes de redes VPN IPsec *Bittium SafeMove VPN Client* (en sus dos variantes: Android y Windows).

Este tipo de redes VPN pueden ser útiles en entornos en los que no tengamos equipos especialmente modernos o con sistemas operativos dispares, ya que este estándar es soportado por la mayoría de ellos.

VPN con MACsec

- Ventajas: las VPN basadas en el estándar MACsec operan en el nivel de enlace, por lo que pueden operar en redes que no estén basadas en el estándar IP. Entre las ventajas del uso de este estándar se encuentra la confidencialidad, asegurada con la inclusión de un cifrado simétrico entre nodos de la misma LAN, la integridad y la autenticación, garantizadas al incluir el protocolo ICV, protección frente a ataques de denegación de servicio y protección anti-reenvíos.

- Inconvenientes: el estándar MACsec, por sus características, tan solo es aplicable a la protección de redes LAN, por lo que la conexión de un único usuario remoto u otras situaciones similares pueden ser ineficientes o incluso no poder llevarse a cabo. Asimismo, requiere de dispositivos específicos que implementen dicho estándar, añadiendo más complejidad a la instalación y mantenimiento de una red de estas características. Finalmente, se puede producir una sobrecarga adicional producida por la inclusión del encabezado MACsec. Esta situación se puede dar siempre y cuando el MTU (*Maximum Transmission Unit*) sea bajo.

MACsec está diseñado tanto para ser implementado en redes LAN como para interconectar a estas, por lo que el uso más adecuado de este estándar podría encontrarse en proporcionar acceso seguro a información clasificada en el que varios dispositivos o usurarios necesiten hacer uso de dicha información, como podría ser una oficina remota (CCN-STIC 836, 2022).

Una vez vistas las ventajas e inconvenientes de cada tipo de VPN es necesario elegir una con la que securizar las comunicaciones entre centros. En el apartado 4.2 en el que se expone la comunicación entre centros se procederá a realizar la elección del tipo de VPN más conveniente para este cometido.

4.2 Comunicación entre dos puestos de mando a través de los cuales se comparte información del sistema BMS

A continuación, se va a presentar el caso de uso planteado en este proyecto, el cual consiste en establecer una comunicación eficaz y fiable entre los dos puestos de mando que componen la maniobra de una brigada tipo. En este intercambio de información se va a proponer transmitir los datos manejados por el sistema BMS, software cuyo nivel de seguridad en el manejo de datos alcanza el nivel de Difusión Limitada (Fernández Rodríguez, 2020). Gracias a este flujo de información tanto el puesto de mando principal como el avanzado dispondrán de la información actualizada que proporciona dicho sistema, así como otras funcionalidades de mensajería y herramientas de mando y control que serán explicadas a continuación.

4.2.1 Comunicación entre centros

En el contexto de un ejercicio táctico a nivel brigada, esta necesita de una compañía de transmisiones que se encuentre organizada en dos centros de mando. Esta duplicidad de puestos de mando viene motivada por la necesidad de realizar saltos[12] a medida que transcurre la maniobra. A pesar de que se den estos saltos, la unidad debe estar siempre liderada por un puesto de mando del que reciba órdenes, por este motivo es necesario que haya dos puestos

12 Un salto es el desplazamiento, en este caso de un puesto de mando, de un lugar a otro en un corto espacio de tiempo. En un ejercicio táctico un puesto de mando puede saltar por diversos motivos, siendo los más comunes el acompañar el avance o repliegue de la unidad propia o modificar su ubicación para no ser detectado.

de mando que alternen las funciones de plataforma de toma de decisiones. En el caso de que la unidad se encuentre estacionada de forma estática en labores defensivas, la configuración de los puestos de mando seguirá manteniéndose como uno principal y otro avanzado. Adicionalmente, en caso de verse comprometido un centro de mando, el restante posee los mismos medios y capacidades, por lo que el general jefe de la brigada puede seguir ejerciendo el mando desde este último.

Al ser dos puestos de mando idénticos e ir turnándose en sus cometidos, estos deben disponer de la misma información en todo momento. Por este motivo es crucial que exista un intercambio de información estable entre ambos centros, con capacidad suficiente como para poder llevar un seguimiento óptimo de la maniobra en tiempo real.

Actualmente los medios disponibles en una compañía de transmisiones de brigada orientados a cumplir con este cometido son dos: la conexión vía satélite y los radioenlaces militares, en este caso radios PR4G y Harris 5800 y 7800 . A pesar de ser medios que actualmente están integrados en la arquitectura de red de cualquier maniobra y cuya fiabilidad ha sido demostrada, ambos adolecen del mismo problema, una velocidad de transmisión de datos muy inferior a la requerida para cumplir con las necesidades de ambos puestos de mando (Entrevista personal experto, Anexo II).

Por los motivos mencionados anteriormente surge la necesidad de resolver esta problemática y satisfacer las necesidades de comunicación entre ambos puestos de mando. El medio elegido para resolver este problema y asegurar una comunicación fluida entre ambos puestos de mando ha sido el uso de radioenlaces de la marca Ubiquiti. El motivo por el que se ha elegido este medio es porque ya se encuentra disponible en las distintas brigadas del ET, además de su elevada capacidad de transferencia de datos, una configuración sencilla y un precio económico si lo comparamos con otras alternativas, como desarrollar o adquirir otros medios militares (Entrevista personal experto, Anexo II).

Los modelos de la marca Ubiquiti que se encuentran disponibles en las unidades de transmisiones son el AG-HP-5G27 y el Rocket M5. La estación Rocket M5 ofrece tasas de transferencia de datos superiores a su contraparte, el modelo AG-HP-5G27. No obstante, ambos radioenlaces son capaces de aumentar considerablemente las capacidades actuales y, tanto en prestaciones de seguridad como en configuración son idénticos. Las características técnicas del radioenlace AG-HP-5G27 pueden ser consultados en el Anexo IV. Los propios radioenlaces Ubiquiti integran una serie de medidas de seguridad, descritas en el Anexo V.

4.2.1.1 Integración de la VPN en las comunicaciones de radioenlaces

Como se ha expuesto anteriormente, existen diversas VPN en función de la capa en la que esta trabaje. En el apartado 4.1 de este trabajo se ha realizado una exposición y valoración de diversas VPN, finalizando en unos pros y contras. Con el objetivo de discernir qué VPN es la más adecuada para ser integrada en un despliegue de una unidad de transmisiones es necesario recurrir a las exigencias impuestas por el CCN en materia de seguridad.

Atendiendo al CCN, este tiene certificados dos tipos de productos relacionados con la implementación de VPN: Firewalls con capacidades VPN de tipo IPsec y el dispositivo SMA (*SonicWall Secure Mobile Access*), el cual habilita y gestiona VPN de tipo SSL (CCN-STIC 105,

2022).

Con el plan MC3 el ET propone que todos sus medios CIS operen haciendo uso del protocolo IP, por lo que la VPN a elegir debe brindar protección en la capa de red. Dado que el CCN certifica dos tipos de productos con capacidad de crear y gestionar VPN las opciones se ven limitadas a la elección de VPN con protocolo TLS (basado en SSL) o estándar IPsec. De estos dos tipos de redes, aquellas que proporcionan protección al tráfico IP son aquellas con el estándar IPsec, por lo que este será el tipo de VPN elegida para proteger el tráfico de datos entre los radioenlaces del centro de mando avanzado y principal.

El CCN certifica una amplia gama de productos con capacidad para gestionar VPN basadas en el estándar IPsec. Dado que actualmente en las brigadas los *routers* son de la marca estadounidense CISCO, el producto más adecuado para llevar a cabo la gestión de dichas VPN son los firewall de esta marca: *Cisco Firepower Threat Defense* (FTD) de la serie *Firepower 1000.* Estos dispositivos cuentan con capacidades *firewall*, VPN e IPS (Sistema de Prevención de Intrusos). La inclusión de estos dispositivos supone añadir un elemento de control y gestión seguro de VPN de tipo IPsec que cuenta con la acreditación del CCN, por lo que las medidas de seguridad implementadas por este están incluidas en el ENS[13] (Esquema Nacional de Seguridad) y entran en la categoría ALTA. La descripción técnica dada por el CCN en su guía CCN-STIC 105 sobre equipos autorizados por el mismo se muestra en el Anexo VI.

Figura 5: CISCO Firepower Threat Defence, Firepower 1000 series. Fuente: Cisco, 2007.

4.2.2 Transferencia de datos del sistema BMS

13 Atendiendo a la definición dada por el Ministerio de Asuntos Económicos y Transformación Digital en la disposición 7191 del BOE del 4 de Mayo de 2022, "e*l ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias"*.

Habiendo elegido el tipo de VPN a aplicar, resulta necesario plantear cómo se va a realizar la transferencia de datos del sistema BMS, explicado con detalle en el Anexo VII.

El sistema BMS recibe la información de las distintas unidades que componen la maniobra a través de la RRC, es decir, haciendo uso de los radioenlaces militares PR4G. En consonancia con el caso de uso propuesto en este trabajo, la información recibida en el puesto de mando avanzado, así como la propia información generada por los usuarios de este (es decir, dentro del propio puesto de mando se encuentran distintos usuarios del sistema BMS que no componen unidades de maniobra, no obstante tienen la posibilitad de mandar mensajes, dibujar líneas de acción, etc.) será transferida al puesto de mando principal.

4.2.2.1 Configuración

Como se ha mencionado anteriormente, el estándar IPsec puede ser configurado en dos modos, túnel y transporte. El modo túnel, desde un punto de vista criptográfico, protege al paquete IP en su totalidad ya que este es encapsulado por el nuevo paquete proporcionado por IPsec. El modo transporte mantiene la cabecera IP original y añade otros campos de seguridad, proporcionado seguridad al *payload*[14] en gran medida. Como conclusión, de cara a la configuración del túnel es preferible establecer el túnel IPsec en modo túnel ya que este proporciona mayor seguridad. No obstante, debido al aumento de tamaño de los paquetes el rendimiento es menor en el modo túnel en comparación con el modo transporte, por lo que las restricciones que imponga la red serán determinantes a la hora de hacer uso de un modo u otro (CCN-STIC 807, 2022).

En el estándar IPsec se dan dos fases diferenciadas a la hora de establecer la comunicación entre las partes y, posteriormente, intercambiar información. El protocolo IKE responde a la necesidad de establecer las claves con las que se va a establecer la comunicación vía túnel y la protección del flujo de datos corre a cargo de los protocolos AH o ESP (CCN-STIC 807, 2022).

- IKE: el protocolo IKE negocia diversos parámetros de conexión, secreto compartido y autenticación mutua de los extremos de comunicación. Actualmente, la versión autorizada es la IKEv2.

  El protocolo IKE negocia unos parámetros criptográficos en la primera conexión que hace cuando se establece el túnel, dichos parámetros reciben el nombre de *Transforms* y constan de:

  - Grupos *Diffie-Hellman*: intervienen en el acuerdo de clave. En el protocolo IKEv2, los parámetros *Diffie-Hellman* se envían de extremo a extremo y, una vez finalizado el acuerdo de clave generan el secreto compartido. Los grupos *Diffie-Hellman* permitidos en las VPN IPsec pueden ser de tipo MODP (*Modular Exponenital*) o de ECC (Curva Elíptica).

  - Función Pseudo-aleatorias: se utilizan para generar valores aleatorios y la derivación

14 El payload o carga útil es aquella parte del mensaje cuya función es la de proporcionar información acerca del propio mensaje para que este llegue a su destino de forma correcta.

del material de claves. Las funciones pseudo-aleatorias aprobadas por el CCN son aquellas basadas en AES-CMAC[15] y HMAC-SHA2[16].

- Algoritmo de encriptación: el algoritmo de encriptación para IKEv2 y ESP puede responder tanto a modelos de cifrado clásico como a esquemas AEAD.

- Algoritmo de integridad y autenticación de origen: la verificación de integridad y autenticación de origen se realizan empleando mecanismos MAC. En el caso de que el algoritmo de encriptación incluya esquemas AEAD no será necesario incluir ninguna medida adicional de protección de integridad o autenticación en el origen. No obstante, en el supuesto de que se esté empleando un mecanismo de cifrado clásico sí que serán necesarias medidas adicionales. Los mecanismos MAC permitidos por el CCN son aquellos basados en esquemas AES-CMAC, AES-GMAC[17] y HMAC-SHA2.

- AH y ESP: como ya se mencionó en el apartado 4.1.3, el protocolo AH garantiza la integridad y la autenticidad del flujo de datos, mientras que ESP ofrece confidencialidad y es capaz de proveer de integridad y autenticidad. Actualmente no se conocen ataques a VPN de tipo IPsec en las que el protocolo AH sea precedido por ESP o en el que este último actúe en solitario, asumiendo las funciones de autenticidad e integridad. Como consecuencia, se recomienda el uso de ESP asumiendo las funciones de proveedor de integridad, autenticidad y confidencialidad.

- Autenticación: la autenticación de ambos extremos de la comunicación se realiza tras finalizar la negociación de los diversos parámetros y material criptográfico que intervienen en la conexión a través de mensajes del tipo IKE_AUTH. El mecanismo de autenticación recomendado por el CCN es la firma electrónica con claves públicas/privadas. Los esquemas de firma electrónica aprobados por el CCN se basan en ECDSA y RSA, siendo señalados de forma más detallada en el Anexo . Finalmente, quedan excluidos como métodos seguros o recomendables el uso de PSK (Claves precompartidas), la no autenticación, o los métodos EAP (*Extensible Authentication Protocol*).

Finalmente, los distintos protocolos mencionados constituyen la configuración óptima impuesta por el CCN para que se pueda establecer una red VPN de tipo IPsec que garantice la seguridad de la información que va a transportar. Los parámetros y protocolos permitidos por el CCN son señalados en el ANEXO VIII de forma más detallada.

---

15 El AES-CMAC es una función de tipo *hash* que se basa en cifrado de bloque de clave simétrica AES (RFC-4493, 2006).

16 El HMAC-SHA2 es un código de autenticación de mensaje que recurre a una función tipo *hash* del tipo 2, que incluye SHA-224, SHA-256, SHA-384 y SHA-512 (RFC-6234, 2011).

17 AES-GCM (*Galois/Counter Mode*) se construye en base a un cifrador de clave simétrica con un tamaño de paquete de 128 bits, valiéndose además de AES (SIST, 2007).

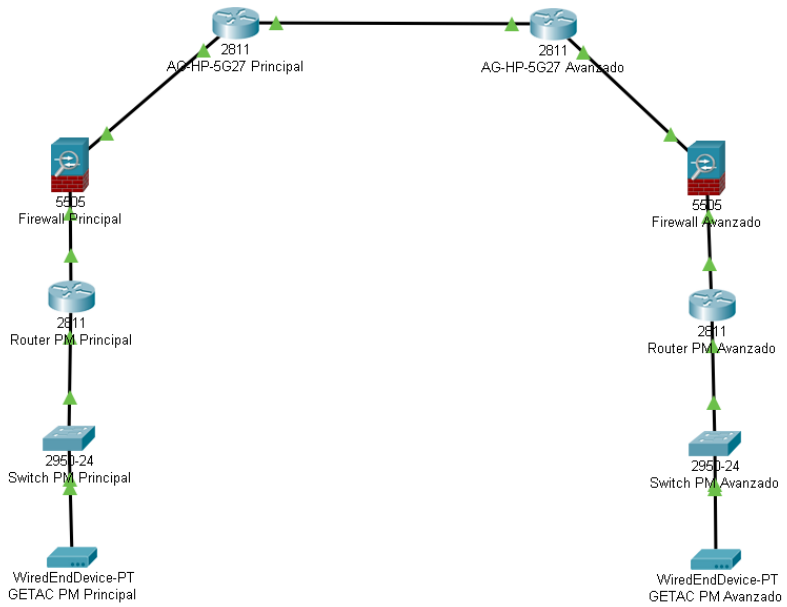


Figura 6: Esquema de red en el que se incluye el túnel IPsec. Fuente: Elaboración Propia

En dicha figura se ve representada de forma esquemática la topología de red aparejada a ambos centros de transmisiones. En dicha maqueta se han incluido dos *routers* como radioenlaces AG-HP-5G27, ya que ambos radioenlaces poseen una dirección IP, dos *firewall*, simulando los *firewall* de la serie 1000 propuestos en el apartado 4.2.1.1, dos *routers* (uno por cada puesto de mando) y un equipo genérico que simula las tablets GETAC con las que se opera el sistema BMS.

Atendiendo a la arquitectura de red expuesta anteriormente se procederá a mostrar la configuración realizada en uno de los *routers* del puesto de mando. La configuración de la red se realiza de forma simétrica en ambos centros.

Paso 0: Configuración inicial

En este paso 0 se realiza una configuración básica del *router*. En dicha configuración se le asigna un nombre, una contraseña con la que acceder a la configuración del mismo, un texto inicial que aparezca en el momento en el que se encienda y el usuario opere con él, etc. En este proceso se le asignan direcciones IP a las distintas bocas que salen del propio *router*, así como una ruta por defecto o un protocolo de enrutamiento. Para la realización de esta maqueta se han configurado los parámetros iniciales concernientes a las direcciones IP y se ha establecido una ruta por defecto.

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/
no]: n


Press RETURN to get started!



Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 19.172.160.2 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 fastethernet 0/0
Router(config)#S
```

Figura 7: Configuración inicial del router. Fuente: elaboración propia.

Paso 1: Configuración del túnel GRE

Una vez realizada la configuración inicial se procede a crear un túnel GRE (*Generic Tunnel Encapsulation*) con el que comunicar de forma directa el *router* del puesto de mando principal y el *router* del puesto de mando avanzado.

```
Press RETURN to get started!



PMPrincipal>enable
PMPrincipal#config t
Enter configuration commands, one per line.  End with CNTL/Z.
PMPrincipal(config)#interface tunnel 1

PMPrincipal(config-if)#
%LINK-5-CHANGED: Interface Tunnel1, changed state to up

PMPrincipal(config-if)#ip address 172.26.5.1 255.255.255.0
PMPrincipal(config-if)#tunnel source fastethernet 0/0
PMPrincipal(config-if)#tunnel destination 205.85.91.2
PMPrincipal(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed
state to up
```

Figura 8: Inclusión de un túnel GRE. Fuente: elaboración propia

Paso 2: Configuración del protocolo de enrutamiento EIGRP y distribución de rutas

Una vez declaradas todas las direcciones IP es necesario incorporar un protocolo de enrutamiento con el que comunicar los *routers*. Gracias a este protocolo de enrutamiento cada *router* conoce no solo las redes a las que está directamente conectado si no aquellas a las que están conectados el resto de *routers* ya que cada *router* comunica al resto cuales son las redes a las que está conectado. En este caso se ha hecho uso del protocolo de enrutamiento EIGRP desarrollado por Cisco, con el que se ha declarado la red perteneciente al túnel que se ha creado en el paso 1.

```
PMPrincipal>enable
PMPrincipal#config t
Enter configuration commands, one per line.  End with CNTL/Z.
PMPrincipal(config)#interface tunnel 1

PMPrincipal(config-if)#
%LINK-5-CHANGED: Interface Tunnel1, changed state to up

PMPrincipal(config-if)#router eigrp 10
PMPrincipal(config-router)#eigrp router-id 1.1.1.1
PMPrincipal(config-router)#network 172.26.5.0 0.0.0.255
PMPrincipal(config-router)#
```

Figura 9: Establecimiento del protocolo EIGRP. Fuente: elaboración propia

Si se accede a la configuración del *router* del puesto avanzado se puede observar que se ha creado una nueva adyacencia, en este caso con la dirección asociada al túnel.

```
Enter configuration commands, one per line.  End with CNTL/Z.
PmAvanzado(config)#ip route 0.0.0.0 0.0.0.0 fastethernet 0/0
PmAvanzado(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed
state to up

%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 172.26.5.1 (Tunnel1) is
up: new adjacency
```

Figura 10: Adyacencia establecida en el router del puesto de mando avanzado. Fuente: elaboración propia

Paso 3: Configuración de ISAKMP e IPsec Transform-set

A continuación se procede a mostrar la configuración del túnel, con el que le se añaden los parámetros necesarios de autenticación y encriptación.

En primer lugar se establece el protocolo IKE, en el que se designa el tipo de encriptación que

se va a usar (AES), el tipo de hash (sha), el método de intercambio de claves, el cual va a ser con claves precompartidas, y el grupo Diffie-Hellman. Posteriormente se establece la clave precompartida y se determina la dirección IP del equipo que va a compartirla. Finalmente se establecen los criterios de seguridad por los cuales se va a regir el túnel, aplicando las transformaciones necesarias para proteger el tráfico de información. En este caso se determina el uso del protocolo ESP y HMAC.

```
PmPrincipal#config t
Enter configuration commands, one per line.  End with CNTL/Z.
PmPrincipal(config)#interface tunnel 1
PmPrincipal(config-if)#crypto isakmp policy 1
PmPrincipal(config-isakmp)#encryption aes
PmPrincipal(config-isakmp)#hash sha
PmPrincipal(config-isakmp)#authentication pre-share
PmPrincipal(config-isakmp)#group 2
PmPrincipal(config-isakmp)#exit
PmPrincipal(config)#crypto isakmp key TFG address 205.85.91.2
PmPrincipal(config)#crypto ipsec transform-set TFG esp-aes esp-
sha-hmac
PmPrincipal(config)#
```

Figura 11: Configuración de ISAKMP e IPsec Transform-set. Fuente: elaboración propia.

Finalmente, con el comando *show crypto aeskmp policy 1* podemos ver de forma resumida los parámetros actuales y los que corresponden por defecto.

```
Global IKE policy
Protection suite of priority 1
        encryption algorithm:   AES - Advanced Encryption
Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard
(56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
PmPrincipal#
```

Figura 12: Resumen de los protocolos aplicados al túnel. Fuente: elaboración propia.

Paso 4: Verificación

Una vez configurado el túnel IPsec falta comprobar si efectivamente existe comunicación entre ambos routers, por ello se hace uso del comando ping, con el que se comprueba la conexión entre dos direcciones IP. En este caso se puede comprobar que la señal ha llegado al router del puesto de mando avanzado y ha regeresado al router del puesto de mando principal de forma satisfactoria.

```
%SYS-5-CONFIG_I: Configured from console by console

PmPrincipal#ping 172.26.5.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.26.5.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1
ms

PmPrincipal#
```

Figura 13: Comprobación de la comunicación entre puestos de mando. Fuente: elaboración propia

PÁGINA EN BLANCO

5 CONCLUSIONES

La motivación de este proyecto ha sido determinar la viabilidad de la implementación de VPN como un método seguro y viable de cara a difundir información clasificada con un grado de protección hasta Difusión Limitada. Los objetivos de los que se ha partido han sido los de explicar los conceptos clave relativos a las VPN, analizar la viabilidad de la inclusión de estas en una Brigada y proponer un ejemplo práctico para su uso.

Atendiendo a la investigación realizada durante este proyecto cabe resaltar varias cuestiones.

En primer lugar se ha comprobado que las VPN suponen un medio seguro por el que, con la configuración adecuada, es factible el intercambio de información clasificada hasta el nivel de seguridad propuesto en este proyecto. No obstante, los medios empleados para la creación y gestión de VPN deben ser acreditados por el CCN por lo que, a falta de una acreditación formal del CCN de unos medios distintos a los que ofrece en su catálogo, es necesario emplear aquellos equipos que vengan recogidos en dicho catálogo. Por este motivo la implantación de una VPN por sí sola, independientemente de los medios usados para crearla y gestionarla, no supone una garantía de seguridad, si no que debe ser complementada con el uso de equipos certificados por el CCN.

Posteriormente, el caso práctico resulta factible desde un punto de vista material y operativo, ya que los medios empleados para llevar a cabo dicho caso ya los posee una Brigada tipo en el ET a excepción del *firewall* certificado. Los beneficios que aporta la comunicación por medios convencionalmente no seguros que han sido securizados gracias a la implementación de VPN son notorios: en primer lugar aseguran poder utilizar una vía que comunicación que hasta ahora quedaba relegada a tareas de menor importancia por no ofrecer las medidas de seguridad adecuadas. Seguidamente brinda la posibilidad de hacer uso de una red de comunicaciones con un ancho de banda considerablemente mayor al que se tiene actualmente haciendo uso de las comunicaciones satélite. Finalmente proporciona otra posibilidad al uso de cifradores, los cuales son un recurso crítico y, a diferencia de estos, la red VPN y los equipos que la componen sí que pueden ser reconfigurados y manipulados con mayor libertad que dichos cifradores, por lo que se le añade un grado más de flexibilidad al despliegue.

En conclusión, el uso de redes VPN es un recurso contemplado en el ENS que ofrece un nivel de seguridad óptimo al nivel de Difusión Limitada. Debido a las características de las VPN, estas ofrecen una gran flexibilidad en su despliegue y gestión, por lo que resultan de gran utilidad en despliegues tácticos en los que se opera en un ambiente complejo y cambiante.

Para finalizar cabe añadir unas líneas de trabajo futuras en las que se contemplan aspectos relevantes del desarrollo del proyecto que, bien por falta de tiempo o medios, no han podido ser llevadas a cabo. En primer lugar no ha sido posible disponer del equipo *firewall* propuesto ya que este no se encuentra entre los medios de dotación en las unidades, por lo que no se han podido realizar pruebas con él ni comprobar sus modos de funcionamiento y capacidades. En segundo lugar, este proyecto ha sido realizado basándose, entre otros, a la información proporcionada por el CCN. No obstante, este organismo es el que, en última instancia, posee la potestad de auditar medios y sistemas en el ámbito de la seguridad, por lo que la solución propuesta debe ser analizada y auditada por dicho organismo.

6 REFERENCIAS BIBLIOGRÁFICAS

RFC-3173, 2001: Internet Engineering Task Force, IP Payload Compression Protocol (IPComp). URL: https://www.rfc-editor.org/rfc/rfc3173. Fecha de la última revisión: 22/11/2022

RFC-3935, 2004: IETF, A mision Statement for the IETF. URL: https://www.rfc-editor.org/rfc/rfc3935. Fecha de la última revisión: 22/11/2022

RFC-4301, 2005: Internet Engineering Task Force, Security Architecture for the Internet Protocol. URL: https://www.rfc-editor.org/rfc/rfc4301#section-4. Fecha de la última revisión: 22/11/2022

RFC-4493, 2006: Internet Engineering Task Force, The AES-CMAC Algorithm. URL: https://www.rfc-editor.org/rfc/rfc4493. Fecha de la última revisión: 22/11/2022.

RFC-4251, 2006: Internet Engineering Task Force, The Secure Shell (SSH) Protocol Architecture. URL: https://www.rfc-editor.org/rfc/rfc4251. Fecha de la última revisión: 22/11/2022.

RFC-6234, 2011: Internet Engineering Task Force, US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF). URL: https://www.rfc-editor.org/rfc/rfc6234. Fecha de la última revisión: 22/11/2022

RFC-7296, 2014: Internet Engineering Task Force, Internet Key Exchange Protocol Version 2 (IKEv2). URL: https://www.rfc-editor.org/rfc/rfc7296.html. Fecha de la última revisión: 22/11/2022.

RFC-8446, 2018: Internet Engineering Task Force, The Transport Layer Security (TLS) Protocol Version 1.3. URL: https://www.rfc-editor.org/rfc/rfc8446. Fecha de la última revisión: 22/11/2022

Arana, 2006: Paul Arana, Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2), 2006. URL: https://cs.gmu.edu/~yhwang1/INFS612/Sample_Projects/Fall_06_GPN_6_Final_Report.pdf . Fecha de la última revisión: 22/11/2022.

Tews, 2007: Erik Tews, Attacks on the WEP protocol, 2007. URL: https://eprint.iacr.org/2007/471.pdf. Fecha de la última revisión: 22/11/2022

SIST, 2007: Morris Dworkin, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, National Institute of Standards and Technology, 2007. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf . Fecha de la última revisión: 22/11/2022

Cisco, 2007: Cisco, Cisco IOS VPN Configuration Guide.

Burande et al., 2014: Aniket Burande, Ankita Pise, Sameer Desai, Yohan Martin, Sejal D'mello, Wireless Network Security by SSH Tunneling, 2014. URL: https://d1wqtxts1xzle7.cloudfront.net/36347164/ijsrp-p2865-with-cover-page-v2.pdf?

Expires=1669820533&Signature=GVvmritk-nA7F5~PG-RXv8~wP0YRhgTyt~VgaBA1gh0lISBGXGe~fqnLHAvozqQneRDccV-AuESlTzFHoeo2rHFBYclQ-bSmHep6oB89Fnk4uymuldxTgfHWwtWZRO12xH9xj7CVi6X7YxaZXvgvSD-9V8X5ngpsBeJr1SUWEMTGcAZX-qLS3Zg0ph~xChfJNZFSliPjGtEiQWyF4Boa97SJgEKqmP6gBGtq11fCPv-mTPvJ2VGKY62nHgMHtpSzm6SNlr3q2Km9JdtZp9oEYHwYL~pQTJXxHb52fp-50RiC58pqMC5T2MkFkvxqCbYKvkNpzmNdkJO~slAhCg4Nsg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Fecha de la última revisión: 22/11/2022

Guonian Lü et al., 2019: Guonian Lü, Michael Batty, Josef Strobl, Hui Lin, A-Xing Zhu & Min Chen, Reflections and speculations on the progress in Geographic Information Systems (GIS): a geographic perspective, International Journal of Geographical Information Science, 2019. URL: https://www.tandfonline.com/doi/pdf/10.1080/13658816.2018.1533136?needAccess=true . Fecha de la última revisión: 22/11/2022

CCN-STIC 401, 2015: Centro Criptológico Nacional, Glosario y Abreviaturas. URL: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html . Fecha de la última revisión: 22/11/2022

CCN-STIC 001, 2016: Centro Criptológico Nacional, Política de seguridad de las TIC. URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1579-ccn-stic-001-informacion-clasificada-en-la-administracion/file.html . Fecha de la última revisión: 22/11/2022

CCN-STIC 807, 2022: Centro Criptológico Nacional, Criptología de empleo en el Esquema Nacional de Seguridad . URL: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html. Fecha de la última revisión: 22/11/2022

CCN-STIC 105, 2022: Centro Criptológico Nacional, Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación. URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html . Fecha de la última revisión: 22/11/2022

CCN-STIC 836, 2022: Centro Criptológico Nacional, Seguridad en Redes Privadas Virtuales. URL: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2299-ccn-stic-836-seguridad-en-vpn-en-el-marco-del-ens/file.html . Fecha de la última revisión: 22/11/2022

XIV JORNADAS STIC CCN-CERT 2020: Protección y ataque en la autenticación criptográfica de información y password hashing. Dr Alfonso Muñoz. URL: https://www.ccn-cert.cni.es/pdf/documentos-publicos/xiv-jornadas-stic-ccn-cert/ponencias-1/5506-s18-d02-02-proteccion-y-ataque-autenticacion-criptografica-de-informacion/file.html Fecha de la última revisión: 27/11/2022.

Fernández Rodríguez, 2022: Integración de diferentes dominios de seguridad: aplicación en sistemas militares. URL: https://zaguan.unizar.es/record/101033/files/TAZ-TFG-2020-4495.pdf

BOE Nº84: Ley 9/1968, de 5 de abril, sobre secretos oficiales URL: https://www.boe.es/buscar/pdf/1968/BOE-A-1968-444-consolidado.pdf Fecha de la última revisión: 27/11/2022.

BOE del 4 de Mayo de 2022, disposición 7191. URL: https://www.boe.es/boe/dias/2022/05/04/pdfs/BOE-A-2022-7191.pdf . Fecha de la última revisión: 27/11/2022.

Ubiquiti Networks Datasheet, AG-HP-5G27. URL: https://dl.ubnt.com/datasheets/airgridm/airGrid_HP.pdf Fecha de la última revisión: 27/11/2022.

7 ANEXOS

7.1 ANEXO I: Diagrama de Gantt

		Nombre	Duracion	Inicio	Terminado	Predecesores	Nombres del Recurso
1		**Planificación**	**4 days?**	**5/09/22 8:00**	**8/09/22 17:00**		
2		Establecimiento de Objetivos	1 day?	5/09/22 8:00	5/09/22 17:00		
3		Elaboración del Índice	1 day?	6/09/22 8:00	6/09/22 17:00	2	
4		Elaboración del Diagrama de Grantt	2 days?	7/09/22 8:00	8/09/22 17:00	3	
5		**Recopilación de Información**	**23 days?**	**9/09/22 8:00**	**11/10/22 17:00**		
6		Antecedentes y Marco Teórico	8 days?	9/09/22 8:00	20/09/22 17:00	4	
7		VPN	10 days?	21/09/22 8:00	4/10/22 17:00	6	
8		BMS	5 days?	5/10/22 8:00	11/10/22 17:00	7	
9		Exposición del caso práctico	9 days?	12/10/22 8:00	24/10/22 17:00	8	
10		Conclusiones	3 days?	25/10/22 8:00	27/10/22 17:00	9	

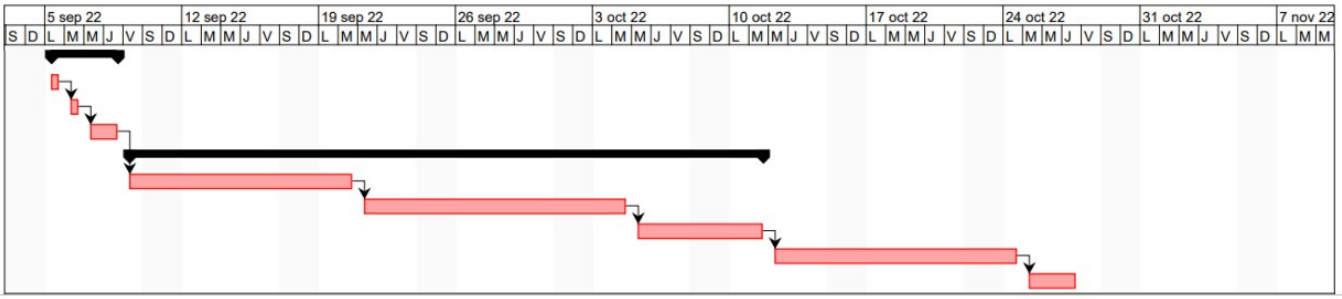


Figura 14: Elaboración del Diagrama de Gantt

PÁGINA EN BLANCO

7.2 ANEXO II: Entrevista realizada a personal experto en el área de sistemas de información

Pregunta 1: ¿Cuáles son los medios actuales de la compañía?

Respecto a los medios físicos de transmisión la Cía cuenta con los siguientes:

- 11 PR4G 9210 de las cuales 4 son SUPERMUX
- 10 Harris 5800
- 5 Spearnet
- 2 PNR 500
- 12 PR4G 9500
- 2 Terminales satélites civiles Began 500
- 1 Terminal satélite Began 325
- Cifradores C, S, TX
- 2 GU de SC2NET

Estos medios físicos se encuentran, algunos de ellos, instalados en diferentes estaciones en función de las necesidades y capacidades de cada una de ellas. Algunas de ellas son las estaciones tipo Mercurio, Soria, Rioja, etc. Adicionalmente, la Compañía posee dos estaciones de Gran Unidad tipo GU de SC2NET, que si bien no tienen medios de transmisión como tal, proporcionan la capacidad de Mando y Control de la Compañía usando los medios de transmisión anteriormente enumerados.

Pregunta 2: Cuando se encuentran realizando un ejercicio táctico, ¿cómo es la comunicación entre centros de mando?¿a qué problemas se enfrenta?

La comunicación entre los centros de mando suele ser llevada a cabo por el terminal satélite, bien el ATQH, que ofrece un mejor ancho de banda para las aplicaciones que son explotadas en los Centros de Mando, o un terminal TLB, usado normalmente como respaldo del anterior.

Pregunta 3: ¿Cuáles son las limitaciones que existen a la hora de establecer dicha comunicación?

La limitación viene determinada por el ancho de banda que ofrece el terminal y la cantidad

de clientes que despliegan en el PC y van a hacer uso de las aplicaciones que corren a través de éstos. En el primer caso, el ATQH ofrece un buen ancho de banda, siendo muy efectiva la comunicación. No ocurre así con el TLB, que en el momento en que el PC tiene un número de usuarios relevante, la comunicación entre los PC se ve ralentizada, especialmente en cuanto al uso de carpetas y recursos compartidos, no así con mensajería a través de *Outlook* (siempre y cuando se trate de texto plano o archivos adjuntos de pequeño tamaño) y *JChat* que sí funcionan con cierta normalidad.

Pregunta 4: ¿Actualmente como solventan estos problemas?

Dependiendo del tipo de ejercicio se puede hacer uso de un enlace a través de antenas omnidireccionales o unidireccionales. En nuestro caso usamos antenas de este tipo de la marca *Ubiquiti*. Si bien, en ejercicios de certificación, como pueden ser los ejercicios tipo Toro, no se puede hacer uso de estos medios no seguros. Para estos casos, la única opción es la limitación a los usuarios de los adjuntos en los correos y los movimientos entre carpetas compartidas entre los PC.

Pregunta 5: ¿Actualmente qué medios catalogados como no seguros están en uso en la compañía?

Las antenas omnidireccionales o unidireccionales anteriormente mencionadas.

Pregunta 6: ¿Qué tipo de información es transmitida por dichos medios?

La información transmitida es toda la que se genera por los usuarios que explotan el PC, a saber; Conjuntos de aplicaciones que forman el sistema de SC2NET (Antares, *Outlook*, *JChat*, carpetas compartidas), aplicaciones de nivel inferior como *BMS* y *TALOS*. Aplicaciones del PC propias como *LOGFAS* para las actuaciones logísticas del PC, *JOWATCH* y *JEEM* para la gestión de incidencias, *SIS* sistema de inteligencia propio de las unidades de inteligencia. Además la aplicación *GESCOM* como gestor de comunicaciones de algunos de los programas referenciados.

Pregunta 7: ¿Han implementado algún método para hacer seguras estas comunicaciones?

Las comunicaciones se envían cifradas a través de cifradores de la propia unidad o los cifradores que traen las propias estaciones ATQH o TLB usadas para la transmisión de los datos entre los PC. Adicionalmente, y a modo de pruebas para propuestas futuras, se han realizado, como parte de una prueba de entidad superior y orquestada por la misma entidad superior, pruebas para escarizar las comunicaciones a través de despliegue de entorno cliente-servidor de *VPN*.

Pregunta 8: ¿Actualmente se emplean VPN o túneles en los ejercicios tácticos de la compañía?, ¿los integrantes de la compañía se encuentran familiarizados con el uso de este recurso?

Actualmente se despliegan túneles entre los PC, configurados directamente en los *Routers* que se encuentran detrás de los cifradores, tanto en la parte roja (la red *LAN* de cada PC) como la parte negra (la red *WAN* a alcanzar por los *Routers*). Sin embargo, no se llevan a cabo el uso de *VPN* en las comunicaciones entre los PC.

La compañía cuenta con personal que se encuentra familiarizado con este recurso, si bien es cierto que está limitado a 3 o 4 personas de toda la Compañía. Se hacen necesarias la asistencia a cursos tipo *CCNA* para poder instruir a más personal en este sentido.

Pregunta 9: ¿Cree factible una solución como la propuesta en este proyecto?

En mi opinión es una solución más que factible; proporciona una comunicación segura independientemente del medio que se vaya a utilizar para la comunicación entre los PC. Es decir, no importa que el medio sea enlace satélite o cableado en un entorno de uso de la red *I3D* o incluso el uso de dispositivos que usen las redes civiles como pudieran ser “pinchos” tipo 4G para la conectividad entre elementos móviles subordinados (como vehículos con capacidad *BMS*). Implementar *VPN* permitiría securizar las comunicaciones con un coste muy pequeño y sin necesidad de dispositivos adicionales tales como cifradores.

7.3 ANEXO III: Análisis DAFO

	FACTORES POSITIVOS	FACTORES NEGATIVOS
FACTORES INTERNOS	**FORTALEZAS**	**DEBILIDADES**
	Protocolos robustos validados por el CCN. No supone un recurso crítico (como lo son los cifradores). Flexibilidad en el despliegue y configuración.	Actualmente el CCN exige el uso de ciertos equipos de tipo firewall para poder usar VPN con seguridad, por lo que es necesaria su adquisición.
FACTORES EXTERNOS	**OPORTUNIDADES**	**AMENAZAS**
	Supone una opción más a la hora de intercambiar información clasificada, pudiendo omitir el uso de cifradores (los cuales suponen un recurso crítico). Gracias al uso de este recurso es posible ampliar el uso de los terminales y medios catalogados como no seguros.	Una mala configuración puede no proporcionar las garantías de seguridad que son requeridas.

Tabla 1: Análisis DAFO. Fuente: elaboración propia.

7.4 ANEXO IV: Ubiquiti airGrid M5, modelo AG-HP-5G27

Specifications

AG-HP-5G27	
Dimensions (Mount Included)	620 x 460 x 360 mm (24.41 x 18.11 x 14.17")
Weight (Mount Included)	2585 g (5.699 lb)
Wind Survivability	200 km/h (125 mph)
Wind Loading	102 N @ 200 km/h (23 lbf @ 125 mph)
Operating Frequency	5725 - 5850 MHz
Max. VSWR	1.5:1
Gain	27 dBi

AG-HP-5G27 Output Power: 25 dBm							
TX Power Specifications				RX Power Specifications			
Modulation	Data Rate	Avg. TX	Tolerance	Modulation	Data Rate	Sensitivity	Tolerance
11a	1 - 24 Mbps	25 dBm	± 2 dB	11a	1 - 24 Mbps	-97 dBm min.	± 2 dB
	36 Mbps	24 dBm	± 2 dB		36 Mbps	-90 dBm	± 2 dB
	48 Mbps	22 dBm	± 2 dB		48 Mbps	-86 dBm	± 2 dB
	54 Mbps	21 dBm	± 2 dB		54 Mbps	-84 dBm	± 2 dB
11n / airMAX	MCS0	25 dBm	± 2 dB	11n / airMAX	MCS0	-97 dBm	± 2 dB
	MCS1	25 dBm	± 2 dB		MCS1	-96 dBm	± 2 dB
	MCS2	25 dBm	± 2 dB		MCS2	-93 dBm	± 2 dB
	MCS3	24 dBm	± 2 dB		MCS3	-91 dBm	± 2 dB
	MCS4	23 dBm	± 2 dB		MCS4	-87 dBm	± 2 dB
	MCS5	22 dBm	± 2 dB		MCS5	-84 dBm	± 2 dB
	MCS6	21 dBm	± 2 dB		MCS6	-78 dBm	± 2 dB
	MCS7	19 dBm	± 2 dB		MCS7	-75 dBm	± 2 dB

Antenna Polar Plots

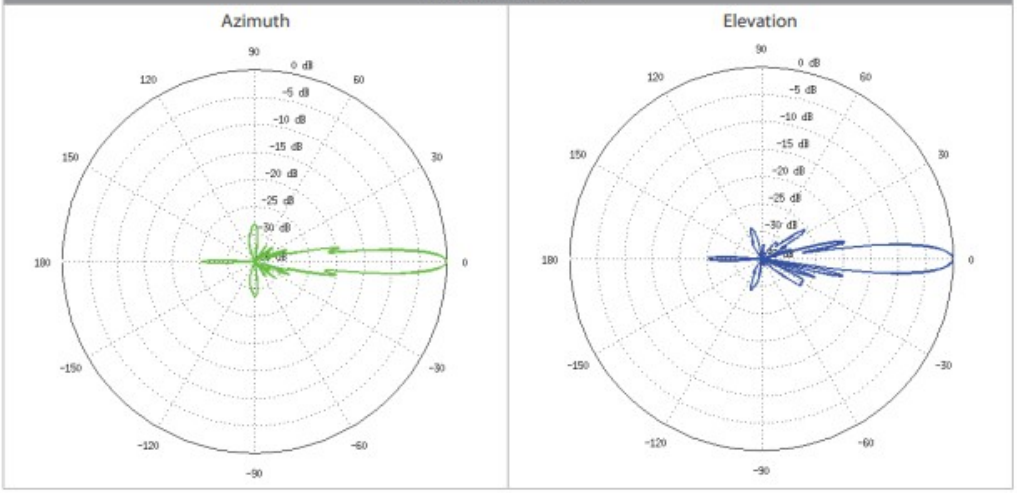


Figura 15: Especificaciones técnicas antena AG-HP-5G27. Fuente: Ubiquiti Networks, Datasheet AirGrid M5d

7.5 ANEXO V: Mecanismos de seguridad de los radioenlaces Ubiquiti

En materia de seguridad, los propios equipos Ubiquiti integran diversos mecanismos con los que proteger sus comunicaciones:

- Cifrado: en el proceso de configuración del equipo este ofrece la opción de cifrar la comunicación inalámbrica entre ambas antenas con diversos protocolos. Entre las opciones disponibles se encuentran los protocolos WEP (*Wired Equivalent Privacy*), WPA (WiFi Protected Access) o WPA2-AES (Segunda verisión del protocolo WPA con cifrado AES).

  - WEP: consiste en un sistema de cifrado incluido en el estándar 802.11, siendo este el primer cifrado en ser implementado dentro del estándar WiFi (CCN-STIC-401, Glosario y Abreviaturas). Actualmente WEP se encuentra en desuso debido a los problemas de seguridad que presenta, tales como problemas de inserción de paquetes, falsa autenticación por parte de terceros, así como la debilidad ante ciertos ataques como el "chop chop" de Korek o el ataque de fragmentación de Bittau (Tews, 2007).

  - WPA: protocolo de seguridad sucesor del protocolo WEP. WPA es un algoritmo que cifra las comunicaciones inalámbricas WiFi con el objetivo de negar el acceso no autorizado por parte de terceros (CCN-STIC 401, 2015).

  - WPA2-AES: protocolo de seguridad sucesor de WEP y WPA. WPA2 hace uso del cifrado AES, el cual supone una alternativa más segura al uso de RC4, método de cifrado usado por los protocolos WEP y WPA a los que sustituye (Arana, 2006).

- Filtrado MAC: método de seguridad consistente en discriminar el acceso de unos equipos a la red en función de su dirección MAC. Con la inclusión de esta medida de seguridad, tan solo los equipos cuya dirección MAC esté permitida podrán acceder a la red.

- Limitación del rango de direcciones IP: durante el proceso de configuración del radioenlace es necesario asignarle una dirección IP. Para poder asignar esta dirección es necesario hacer uso de una dirección de red acompañada de una máscara. Dependiendo de la red y máscara elegida estarán disponibles un número limitado de direcciones IP para ser asignadas a los radioenlaces en cuestión. Como ejemplo, si elegimos una máscara de red /30 habrá un *pool* de 4 direcciones IP, de las cuales una es empleada como dirección de red y otra de *broadcast*, quedando disponibles dos direcciones para ser asignadas a cada uno de los radioenlaces. En el caso de necesitar establecer un relé[18] serían necesarias más direcciones IP, por lo que habría que elegir redes que permitan asignar más direcciones.

---

18 Un relé surje de la necesidad de asegurar la comunicación entre dos radioenlaces que necesitan de una línea de visión directa. En el caso de que esta no pueda darse se recurre a posicionar radioenlaces intermedios que tengan dicha línea de visión directa entre ellos, transportando la señal transmitida desde el emisor hasta el receptor.

7.6 ANEXO VI: Firewall CISCO Firepower Thrat Defense, Firepower 1000 series

En la siguiente imagen extraída de la guía CCN-STIC 105 se muestra la familia de productos Cisco auditada por el CCN. En esta guía se señala el nivel de ENS al que pertenece el producto, versión autorizada, una breve descripción del mismo y dispositivos compatibles.

Cisco Firepower Threat Defense (FTD) en Firepower 1000 Series (FP1010, FP1120 y FP1140) con FMC y FMCv	
Versión	FTD 6.4 y FMC/FCMv 6.4
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/10/2022

Descripción

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).
Compatible con:
-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
-FMCv running on ESXi 6.0 or 6.5 on the Unified Computing System (UCS) UCSB-B200-M4, UCSC-C220-M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Figura 16: Características de los firewall cisco de la serie 1000 auditados por el CCN. Fuente: CCN-STIC 105

7.7 ANEXO VII: DESCRIPCIÓN DEL SISTEMA BMS

El sistema BMS es un software creado por las empresas Thales Group e Indra Sistemas S.A., cuya finalidad es proporcionar un sistema de información para el mando y control de pequeñas unidades. Inicialmente fue concebido para ser empleado en uniades de carros de combate pero su uso se ha extendido a unidades ligeras, con su versión BMS-ET (Fernández Rodríguez, 2020).

La principal aportación del sistema BMS es la de digitalizar el campo de batalla, gracias a ello los usuarios de este son capaces de conocer la localización en tiempo real de las distintas unidades que componen la maniobra.

BMS integra hasta 23 funcionalidades, sin embargo hay algunas que solo son accesibles desde el nivel administrador[19] (ET, 2019. A), entre ellas cabe destacar:

- Administración del Sistema: permite la configuración de este. Desde el nivel administrador se cargan los ficheros de misión[20], cartografía, copias, etc.

- Gestión de datos estáticos: guarda y enlaza los datos cargados tanto en los ficheros de misión como en las plantillas que estos utilizan.

Desde el nivel de usuario se puede acceder a una serie de funciones que podrían ser clasificadas en 3 grupos: funcionalidades SIG[21] (Sistema de Información Geográfica), Mando y Control y Gestión de Telecomunicaciones (ET, 2019. U):

SIG:

- Sistema de Información Geográfica: al ser un sistema SIG permite visualizar mapas, habilita además la creación de capas en las que los usuarios pueden insertar simbología táctica y desarrollar el concepto de la maniobra.

- Navegación: BMS permite el posicionamiento de la plataforma así como la creación o selección de rutas

- Situación Táctica: esta función permite a los usuarios realizar de forma efectiva el mando y control de la operación, ya que establece una organización operativa (cargada desde el fichero de misión), habilita el seguimiento de las unidades propias y ofrece la posibilidad de establecer diversos recursos de planeamiento y conducción de operaciones, como pueden ser la inclusión de medidas de coordinación, instalaciones u obstáculos.

---

19 El nivel administrador en el sistema BMS es un modo de acceso que permite la configuración del sistema.

20 Los ficheros de misión son los archivos en los que viene definida la orgánica de las

21 Los SIG son sistemas de información cuyo propósito es integrar información geográfica, espacial o geoespacial para uso espacio temporal e investigación geográfica (Guonian Lü et al.,

Mando y Control:

- Planeamiento: el sistema BMS posee un registro temporal de los diversos *inputs* y cambios que acontecen a la maniobra. Además de este registro, BMS posee otras herramientas cuyo propósito es facilitar el planeamiento de operaciones. Un ejemplo de dichas herramientas lo encontramos en la inclusión de un subsistema capaz de confrontar líneas de acción (LA), donde se establecen y comparan distintas LA con el objetivo de que el mando escoja la que sea más adecuada según su propósito.

- Apoyo de Fuegos: BMS permite realizar el planeamiento de los fuegos de artillería, en el cual se indica las posiciones desde las que se va a hacer fuego, qué piezas integran el despliegue, los objetivos a abatir, etc. Asimismo, los usuarios tienen la capacidad de realizar una petición de fuegos sobre un objetivo no previsto en dicho plan.

- Apoyo Logístico: esta función se encuentra integrada en el área de mensajería. Gracias a la función de apoyo logístico, los operadores del sistema son capaces de gestionar las necesidades logísticas de las unidades implicadas en el despliegue de forma instantánea, tales como solicitudes de abastecimiento, mantenimiento, transporte o asistencia sanitaria, entre otras.

- Mensajería: gracias a esta función los usuarios de BMS pueden valerse de mensajería instantánea a la que pueden anexar documentos.

- Avisos: permiten mandar un mensaje de forma urgente al jefe de la unidad en el que este es informado de información relevante.

- Alarmas: permiten transmitir información del campo de batalla de especial relevancia con máxima prioridad.

Gestión de Telecomunicaciones

- Gestión de Comunicaciones: permite configurar y supervisar los dispositivos radio encargados de retransmitir la posición de las unidades.

- Difusión de la Información: permite la monitorización de las comunicaciones entre los nodos BMS.

Los usuarios del sistema BMS hacen uso de tablets GETAC, desde las que pueden explotar las distintas funcionalidades del sistema. Además, el sistema BMS se vale de la RRC como soporte físico de las comunicaciones que permiten el intercambio de información. No obstante, hay más elementos que pueden conectarse a GETAC, como pueden ser elementos GPS (Global Positioning System) externos a la tablet.

7.8 ANEXO IV: Requisitos criptológicos de seguriadad requeridos por un túnel IPsec

Las tablas que se adjuntan a continuación describen una serie de parámetros que deben cumplir todos aquellos protocolos que intervienen en el establecimiento de VPNs basadas en el estándar IPsec.

PROTOCOLO	MODO RECOMENDADO	CATEGORÍA
IPsec	Modo túnel	Recomendado
ESP	Confidencialidad & Integridad y Autenticidad	Recomendado

Tabla 2: Protocolos IPsec y ESP. Fuente: CCN-STIC 807, 2022.

PROTOCOLO	MODOS RECOMENDADOS	CATEGORÍA
IKEv1	Main Mode y Quick Mode	Legado
IKEv2	Todos	Recomendado

Tabla 3: Protocolos IKE. Fuente: CCN-STIC 807, 2022.

GRUPO DH	FORTALEZA (BITS)	CATEGORÍA
2048-bit MODP Group	112	L
3072-bit MODP Group	128	R
4096-bit MODP Group	>128	R
6144-bit MODP Group	>128	R
8192-bit MODP Group	>128	R
256-bit random ECP group	128	R
384-bit random ECP group	>128	R
521-bit random ECP group	>128	R
brainpoolP256r1	128	R
brainpoolP384r1	>128	R
brainpoolP512r1	>128	R
x25519	128	R
x448	>128	R

Tabla 4: Grupos Diffie-Hellman. Fuente: CCN-STIC 807, 2022.

ESQUEMA CIFRADO / AEAD	FORTALEZA (BITS)	LONGITUD DE CLAVE (BITS)	CATEGORÍA
ENCR_AES_CBC	128 192 256	128 192 256	R[22]
ENCR_AES_CTR	128 192 256	128 192 256	R
ENCR_AES_CCM_12 (1)	128 192 256	128 192 256	R
ENCR_AES_CCM_16 (1)	128 192 256	128 192 256	R
ENCR_AES_GCM_12 (1) (2)	128 192 256	128 192 256	R
ENCR_AES_GCM_16 (1) (2)	128 192 256	128 192 256	R

22 Siempre y cuando vaya acompañada de un mecanismo de autenticación MAC

ENCR_CHACHA20_POLY 1305 (2)	256	256	R

Tabla 5: Esquema de cifrado. Fuente: CCN-STIC 807, 2022.

ESQUEMA MAC	LONGITUD DE CLAVE (BITS)	FORTALEZA (BITS)	CATEGORÍA
AUTH_HMAC_SHA1_96	160	≥ 128	L
AUTH_HMAC_SHA2_256_128	256	≥ 128	R
AUTH_HMAC_SHA2_384_192	384	≥ 128	R
AUTH_HMAC_SHA2_512_256	512	≥ 128	R
AUTH_AES_CMAC_96	128	128	R
AUTH_AES_GMAC	128 192 256	128 192 256	R

Tabla 6: Esquema MAC. Fuente: CCN-STIC 807, 2022.

FUNCIÓN PRF	ESTÁNDAR IKEV2	LONGITUD DE CLAVE (BITS)	FORTALEZA (BITS)	CATEGORÍA
PRF_HMAC_SHA1	RFC 2104	≥ 100	112	L
PRF_HMAC_SHA2_256	RFC 4868	≥ 100 ≥ 125	112 ≥ 128	L R
PRF_HMAC_SHA2_384	RFC 4868	≥ 100 ≥ 125	112 ≥ 128	L R
PRF_HMAC_SHA2_512	RFC 4868	≥ 100 ≥ 125	112 ≥ 128	L R
PRF_AES128_CMAC	RFC 4615	128	128	R

Tabla 7: Función PRF en función del protocolo IKE. Fuente: CCN-STIC 807, 2022.

ESQUEMA DE FIRMA	ESTÁNDAR IKEV2	LONGITUD CLAVE (BITS)	FORTALEZA (BITS)	CATEGORÍA
RSA Digital Signature (RSASSA-PKCS1-v1_5)	RFC 7296	2048 ≥ 3072	112 ≥ 128	L
RSA Digital Signature (RSASSA-PSS)	RFC 4055	2048 ≥ 3072	112 ≥ 128	L R
ECDSA with SHA-256 on the P-256 curve	RFC 4754	256	128	R
ECDSA with SHA-384 on the P-384 curve	RFC 4754	384	192	R
ECDSA with SHA-512 on the P-521 curve	RFC 4754	512	256	R
ECDSA-256 with BrainpoolP256r1	RFC 7429	256	128	R
ECDSA-384 with BrainpoolP384r1	RFC 7429	384	192	R
ECDSA-512 with BrainpoolP512r1	RFC 7429	512	256	R
ECGDSA-256 with BrainpoolP256r1	RFC 7429	256	128	R
ECGDSA-384 with	RFC 7429	384	192	R

BrainpoolP384r1				
ECGDSA-512 with BrainpoolP512r1	RFC 7429	512	256	R

Tabla 8: Esquema de firma en función del estándar IKE. Fuente: CCN-STIC 807, 2022.