Universidad Zaragoza
1542

Trabajo Fin de Grado

EMPLEO DE UN SERVIDOR VPN PARA IMPLEMENTAR UN SISTEMA DE MANDO Y CONTROL EN UNA BRIGADA A TRAVÉS DE UNA ARQUITECTURA DE RED EXTERNA

Autor

D.A.C. Laura Herranz López

Directores

Director académico: Dra. Noelia Marcano Aguado

Director militar: Cap. Javier Fernández González

Centro Universitario de la Defensa-Academia General Militar

2021

Agradecimientos

Transmitir mi más sincero agradecimiento a todos aquellos que me han ayudado a lo largo de esta etapa y han colaborado en esta investigación.

En primer lugar, a los miembros de la Compañía de Transmisiones de la Brigada Ligera Aerotransportable Galicia VII por haber formado parte de mi aprendizaje, en especial al Capitán Don Javier Fernández González, al Teniente Don Juan Ignacio Olivares González y al Sargento Primero Don Adolfo López Ardura.

Me gustaría agradecer el seguimiento continuo recibido por parte de mi tutora la Doctora Doña Noelia Marcano Aguado. Su ayuda ha hecho posible finalizar este proyecto.

Por último, agradecer el cariño y el apoyo incondicional de mis padres y hermana que siempre me han acompañado en todos los objetivos que me he propuesto en mi vida.

RESUMEN

Cuando los usuarios abandonan la base en la que se encuentra su Unidad, dejan de poder tener acceso a la información y a sus servicios. Para estos casos las VPN permiten a los usuarios acceder desde un punto remoto al servidor de su organización a través de la infraestructura de encaminamiento que proveen las redes públicas.

Cada día es más necesario implementar políticas de teletrabajo dentro de las Unidades del Ejército de Tierra (ET) para un acceso seguro de los recursos compartidos tanto en ejercicios de instrucción como en Zona de Operaciones (ZO).

Este proyecto surge de la necesidad de dotar de mayores ventajas al sistema de mando y control de las Unidades del ET. Para ello, el presente proyecto consiste en el análisis, y posterior implementación de una red privada virtual (VPN) con la finalidad de que todos los usuarios puedan conectarse remotamente de forma segura.

En este estudio se plantea, en primer lugar, un trabajo de investigación a través de la recogida de información en publicaciones, recomendaciones y manuales proporcionados por el Ministerio de Defensa y el Centro Criptológico Nacional (CCN) sobre los sistemas de información de acceso remoto y su seguridad. En segundo lugar, se ha puesto en práctica la configuración de la arquitectura de red VPN en los equipos de los usuarios haciendo un estudio exhaustivo de lo que se está usando en la actualidad y cómo gestionar el proyecto en base a los riesgos. El principal objetivo conseguido ha sido la configuración de los equipos del ET con la implementación de comandos capaces de permitir el acceso a los servicios e información del ET.

El trabajo desarrollado se trata de un primer estudio que da lugar a un nuevo tipo de enlace a través de un medio público seguro. Los resultados han evidenciado la necesidad de implementar este tipo de redes en las Unidades del ET como medio para obtener mayor rendimiento y escalabilidad en las comunicaciones y traspaso de información.

Palabras clave

VPN, INTERNET, IPSEC

ABSTRACT

When users leave the base where their Unit is located, they will no longer be able to access the information and its services. For these cases, VPNs allow users to access their organization's server from a remote point through the routing infrastructure provided by public networks.

Every day it is more necessary to implement telework policies within the Spanish Army (ET) for a secure access to shared resources both in training exercises and in the Area of Operation.

This project arises from the need to provide greater advantages to the command and control system of the ET Units. For this, this project consists of the analysis and subsequent implementation of a virtual private network (VPN) in order that all users can connect remotely in a secure way.

In this study, a research work is proposed, in the first place, through the collection of information in publications, recommendations and manuals provided by the Ministry of Defense and the National Cryptological Center (CCN) on remote access information systems and your safety. Second, the configuration of the VPN network architecture has been put into practice on the users' computers, making a thorough study of what is currently being used and how to manage the project based on risks. The main objective obtained has been the configuration of the ET equipment with the implementation of commands capable of allowing access to the ET services and information.

The work developed is a first study that gives rise to a new type of link through a secure medium. The results have shown the need to implement this type of network in the ET Units to obtain greater performance and scalability in communications and information transfer.

Keywords

VPN, INTERNET, IPSEC

INDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ABREVIATURAS, SIGLAS Y ACRÓNIMOS

TFG	Trabajo Fin de Grado
CUD	Centro Universitario de la Defensa
AGM	Academia General Militar
BRILAT	Brigada de Infantería Ligera Aerotransportable
ET	Ejército de Tierra
VPN	Virtual Private Network
ZO	Zona de Operaciones
BMS	Battle Management System
ATAK	Android Tactical Assault Kit
OSI	Organización Internacional de Estándares
CCN	Centro Criptológico Nacional
ISP	Internet Service Provider
LAN	Local Area Network
PDU	Protocol Data Unit
MD	Message Digest
SHA	Secure Hash Algorithm
IPSEC	Internet Protocol SECurity
PPTP	Point to Point Tunneling Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
SSH	Secure SHell
TIC	Tecnologías de la Información y la Comunicación
CNI	Centro Nacional de Inteligencia
STIC	Servicio de Tecnologías de la Información y las Comunicaciones

PDCIS	Plan Director de Sistemas de Información y Telecomunicaciones
RSA	Algoritmo de Cifrado creado por Rivest, Shamir y Adleman
QoS	Quality of Service
WAN	Wide Area Network
WAN C2	Red para Mando y Control
WAN PG	Red de Propósito General
AGE	Administración General del Estado
CA	Autoridad Certificadora
DNS	Domain Name Sytem
URL	Uniform Resource Locator
CRL	Certificate Revocation List
TCP	Transmission Control Protocol
IP	Internet Protocol
NHRP	Next Hop Resolution Protocol
IKE	Internet Key Exchange
OSPF	Open Shortest Path First
EIGRP	Enhanced Interior Gateway Routing Protocol
LTE	Long Term Evolution

1 INTRODUCCIÓN

La siguiente memoria expone la información recopilada y los procedimientos realizados durante el Trabajo Fin de Grado (TFG) correspondiente al Grado de Ingeniería de Organización Industrial impartido por el Centro Universitario de la Defensa (CUD) en la Academia General Militar (AGM) de Zaragoza. Para la realización del proyecto se trabajó en colaboración con la Compañía de Transmisiones de la Brigada de Infantería Ligera Aerotransportable (BRILAT) ‘Galicia’ VII localizada en la provincia de Pontevedra donde se desarrollaron las prácticas externas.

Este proyecto surge de la necesidad de dotar de mayores ventajas al sistema de mando y control de las Unidades del Ejército de Tierra (ET), para ello, el presente proyecto consiste en el análisis, y posterior implementación de una red privada virtual (VPN) con la finalidad de que todos los usuarios puedan conectarse remotamente de forma segura.

1.1 MOTIVACIÓN

El desarrollo de una Fuerza con horizonte en el año 2035 se debe a factores que originan cambios principalmente en el entorno de Seguridad y Defensa (Ministerio de Defensa, 2019). En este entorno, la tecnología y la competición geopolítica están cambiando el carácter de la guerra y, por ende, de las comunicaciones a través de las redes de información.

Cada día es más necesario implementar políticas de teletrabajo dentro de las Unidades del ET para un acceso seguro de los recursos compartidos tanto dentro como en territorio internacional Por una parte, ha sido evidente durante la pandemia Covid-19 la importancia de poder trabajar a distancia lejos del perímetro donde puede ubicarse la Unidad. Y lo mismo ocurre en Zona de Operaciones (ZO), donde es necesario mantener el enlace con Unidades desplegadas lejos del Puesto de Mando. Estas situaciones son solamente algunas de las razones por las que el Ministerio de Defensa se propone dar acceso desde el exterior a sus recursos internos por medio del Nodo Extranet. Un nuevo concepto que permite el uso de una red pública para el envío y recepción de información clasificada, entre otros muchos recursos. Para ello resulta imprescindible un acceso securizado para así disponer de una fuerza plenamente operativa, es decir, una fuerza capaz de desarrollar todas sus misiones y proyectos propuestos.

A menudo la información debe atravesar una infraestructura de redes públicas como podría ser Internet, lo que la hace vulnerable a los ataques de usuarios ajenos o mal intencionados. Ante este peligro potencial, una solución utilizada hasta el momento para evitar este problema han sido las redes privadas. Sin embargo, este tipo de comunicación se está abandonando debido al alto coste y la baja escalabilidad que produce una conexión entre largas distancias.

Como solución más eficiente surgen las Redes Privadas Virtuales (VPN) que permiten complementar a las redes de comunicación comunes y proteger el contenido de dicho tráfico, para asegurar tanto su privacidad como la integridad de la información que pasa por ellas.

El presente proyecto consiste en el análisis, y posterior implementación de una VPN dentro del ámbito militar, concretamente en los sistemas de mando y control de las Unidades del ET con la finalidad de que todos los usuarios puedan conectarse remotamente de forma segura a dichos servicios. Por ejemplo, dando servicio de geolocalización a las unidades tácticas para que el puesto de mando de su Brigada sea capaz de conocer su posición en un tiempo que no ponga en riesgo el cumplimiento de la misión. Este servicio de localización tiene capacidad de proporcionarlo el Sistema de Gestión de la Batalla, o BMS (Battle Management System). Sin embargo, tiene como servidumbre depender de un alcance relativamente corto si se compara con las posibilidades que ofrecería su transmisión por medio de VPN.

El fin último de este trabajo ha sido la creación de un servidor VPN para la Compañía de Transmisiones de la Brigada de Infantería Ligera Aerotransportable (BRILAT) 'Galicia VII' localizada en la provincia de Pontevedra (ver escudo en la Figura 1) encuadrada dentro del Ministerio de Defensa (Anexo I).

En la memoria se presentan inicialmente los conceptos teóricos de las redes de comunicación utilizadas en la actualidad dentro de la Compañía de Transmisiones, centrándose en la explicación de las Redes Virtuales Privadas (VPN) junto con sus tipos, arquitectura de red, características de seguridad y ventajas y servidumbres que presentan. Seguidamente se describe el proceso de implementación de las VPN y los requisitos de configuración de su arquitectura de red.

En la parte práctica, se pretende implementar el servidor VPN para mejorar el sistema de mando y control de las Brigadas y así poder dar servicio de BMS, localizando a las unidades de una forma segura. En el apartado de verificación y validación se tratará de justificar su implementación exponiendo las reflexiones de expertos y posibles usuarios. También se estudiará el caso del sistema Android Team Awareness Kit (ATAK), una aplicación de localización similar a Battle Management System o BMS y cuya configuración ya permite la transmisión de información de forma segura por medio de VPN.

Por último, se expondrán las conclusiones generales que se extraen del trabajo realizado y se destacarán posibles líneas futuras a estudiar.

Figura 1. Escudo BRILAT. Fuente: Ministerio de Defensa

2 OBJETIVOS Y METODOLOGÍA

2.1 OBJETIVOS

El objetivo principal de este trabajo es analizar la viabilidad de emplear un servidor de acceso remoto VPN para el mando y control de una unidad táctica a nivel Brigada.

El empleo del servidor VPN persigue los siguientes cuatro objetivos:

- Facilitar la movilidad de las Unidades del ET de forma integrada, independientemente de la ubicación de los usuarios.

- Proporcionar al usuario facilidad de uso y eficiencia.

- Constituir un único punto de acceso para todos los servicios, aplicaciones y recursos que el usuario requiera.

- Proporcionar seguridad tanto a la información intercambiada con el usuario, como a los recursos accedidos, sin poner en riesgo el resto de los recursos de las redes privadas.

En este sentido, para alcanzar los objetivos marcados durante el desarrollo del trabajo se han seguido las siguientes fases:

- Analizar el estado actual de las redes internas y las posibles arquitecturas de acceso remoto.

- Identificar las necesidades y capacidades operativas de mando y control de una unidad táctica a nivel Brigada.

- Estudiar la normativa vigente y recomendaciones sobre protocolos de seguridad dentro del ámbito del ET.

- Analizar riesgos y beneficios de implementación de un servidor VPN dentro de una Brigada.

- Realizar pruebas de implementación de un servidor VPN capaz de prestar los servicios necesarios para el mando y control a una Brigada.

- Analizar los resultados de las pruebas.

- Obtener conclusiones sobre la viabilidad del empleo del servidor VPN.

- Mencionar las posibles líneas de estudio futuras.

2.2 METODOLOGÍA

En el desarrollo del trabajo se han utilizado diferentes herramientas en función de la fase abordada.

En la fase inicial se ha llevado a cabo un exhaustivo trabajo de investigación a través de la recogida de información en Publicaciones Doctrinales del Ejército de Tierra y recomendaciones del Centro Criptológico Nacional (CCN). Asimismo, se han consultado manuales de VPN así como de Antivirus y cifrados de datos. Con todo ello se realizará una valoración del tipo de acceso actual a la red interna.

En lo relativo a la fase de investigación se han realizado entrevistas tanto a personal experto de la BRILAT, como a posibles futuros usuarios recopiladas en el Anexo II, con el fin de obtener información de gran utilidad para identificar potenciales riesgos y amenazas que pudiera presentar el proyecto.

Para analizar los riesgos y beneficios de la implementación de un servidor VPN se ha decidido hacer uso de las herramientas estudiadas durante el Grado de Ingeniería de Organización Industrial:

Análisis DAFO, que permite identificar las debilidades y fortalezas del empleo de un servidor VPN en un sistema de Mando y Control a nivel Brigada y las diferentes oportunidades y amenazas que se presentarían.

Análisis de Riesgos, que permite analizar el impacto, probabilidad y el efecto de los mismos en el proyecto. De este análisis se obtendrán posibles soluciones y alternativas que consigan minimizar esos efectos y por lo tanto, garanticen la viabilidad del proyecto.

Matriz interés-poder, que permite realizar un análisis estratégico del proyecto, ya que permite diseñar estrategias dirigidas a facilitar sus relaciones con los grupos de interés.

Diagrama de Gantt para gestionar el tiempo del proyecto.

En la fase experimental, se ha llevado a cabo la implementación de un servidor VPN que permita alcanzar una comunicación eficiente entre las distintas Unidades de forma segura mediante el uso de los sistemas de mando y control BMS y ATAK.

3 ANTECENDENTES Y MARCO TEÓRICO (ESTADO DEL ARTE)

3.1 REDES DE COMUNICACIÓN

Tradicionalmente, las redes de las organizaciones se encontraban dentro de la ubicación física de dicha organización. Hoy en día, este perímetro es mucho más amplio y es necesario el acceso remoto por parte de los usuarios.

Permitir acceso remoto a los recursos profesionales conlleva riesgos de seguridad inherentes que deben ser mitigados por las soluciones que se implementen. El objetivo del acceso seguro es proporcionar protección *Zero Trust*. Se trata de facilitar accesos simples y efectivos a la información, aplicaciones y servicios de la organización, sin compromiso de la seguridad (Centro Criptológico Nacional). El modelo Zero Trust asume que nada fuera o dentro de la organización es confiable, y que se debe identificar y autenticar a cualquier persona o entidad que intente conectarse, antes de permitir su acceso.

A continuación, se presentan las principales arquitecturas de acceso remoto existentes en la actualidad.

3.1.1 Historia

La comunicación virtual se inicia cuando aparece Internet cuya arquitectura de red se desarrolla en el Anexo III y que se define como una red global de redes que permitió la primera comunicación virtual en la década de los setenta. Con su nacimiento se iniciaron conexiones internacionales de acceso universal. Fue necesario un acuerdo en cuanto al protocolo a utilizar para un desarrollo de sistemas totalmente compatibles. (Janet Abbate, 2009)

A mediados de los setenta el Comité Consultor sobre Telegrafía y Telefonía Internacional del Sindicato Internacional de Telecomunicaciones desarrolló un protocolo estándar de conmutación de paquetes llamado X.25. Este protocolo proporcionaba una conexión fiable, conocida como circuito virtual, entre dos puntos de una red, permitiendo a los usuarios de las distintas terminales acceder a recursos en línea sin necesidad de instalar un complejo software específico. Aunque el X.25 fue más tarde reemplazado por otras tecnologías tales como la transmisión de tramas o *frame relay,* proporcionó la base para el rápido desarrollo de redes públicas en todo el mundo.

Otro influyente esfuerzo de estandarización ocurrido a finales de la década fue el modelo de Interconexión de sistemas abiertos (*Open Systems Interconnection*) creado por la OSI (Organización Internacional de Estándares). Dicho modelo definía las funciones de siete modelos de proceso, desde conexiones básicas entre hardware hasta aplicaciones e interfaces de usuario (Janet Abbate, 2009).

Las redes públicas de datos supusieron el primer acceso online para gran parte de la población mundial. Las sedes de las organizaciones empezaron a interconectar mediante líneas con anchos de banda fijos independientes para voz y datos. Hasta la actualidad, se ha producido un aumento continuado en la demanda de la transmisión de datos a mayores velocidades. Así, se detectado la necesidad de interconectar las distintas redes de áreas local (LAN) y dotarlas de una mayor capacidad de procesamiento de datos mediante un sistema de procesamiento de paquetes que dividía la información en tramas, cada una de las cuales transportaba su dirección utilizada por los conmutadores para determinar su destino final.

3.1.2 Actualidad

A continuación, la figura 2 y 3 representan, respectivamente, un esquema y un diagrama de las principales arquitecturas de acceso remoto que existen en la actualidad y que serán abordadas a lo largo de este apartado.

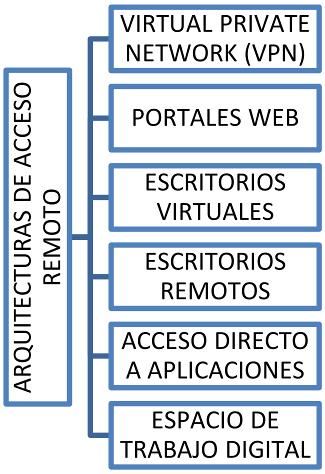

Figura 2. Esquema de las arquitecturas de acceso remoto. Fuente: elaboración propia.

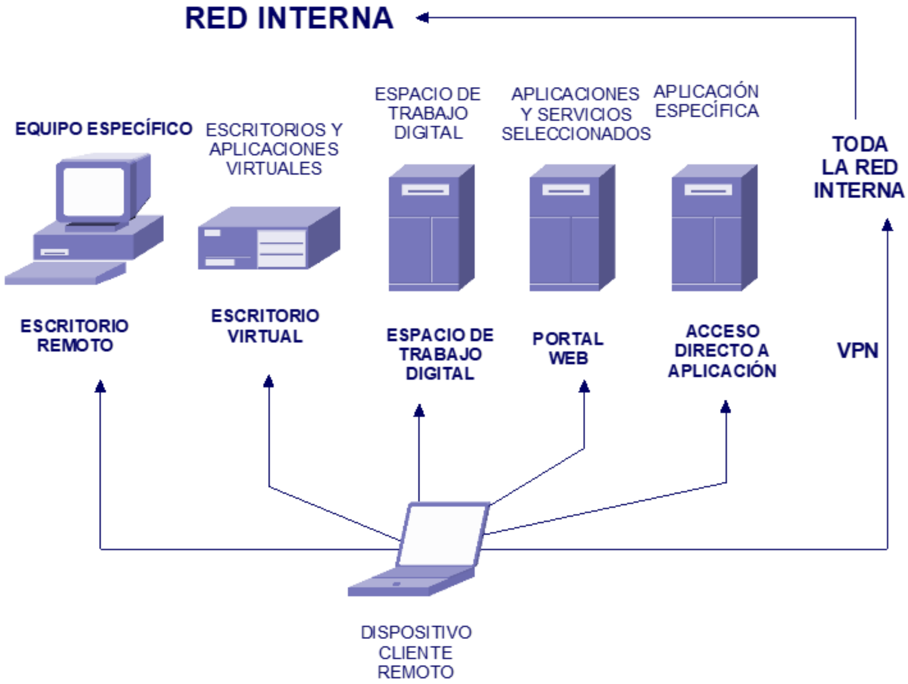

Figura 3. Diagrama de las arquitecturas de acceso remoto. Fuente: elaboración propia.

Cuando un cliente no tiene acceso remoto a todos los recursos de la red interna sino a un conjunto determinado de contenido o servicios se hace uso de los **Portales Web** (ver figura 4). Estos ofrecen una interfaz web centralizada con acceso como, por ejemplo, a información sobre clientes, carpetas compartidas, noticias o correo a través de la ejecución de una serie de aplicaciones cliente que establecen conexiones a los servidores, bases de datos y repositorios internos. De este modo, el portal hace la función de capa de presentación ante los usuarios (Centro Criptológico Nacional, 2021).

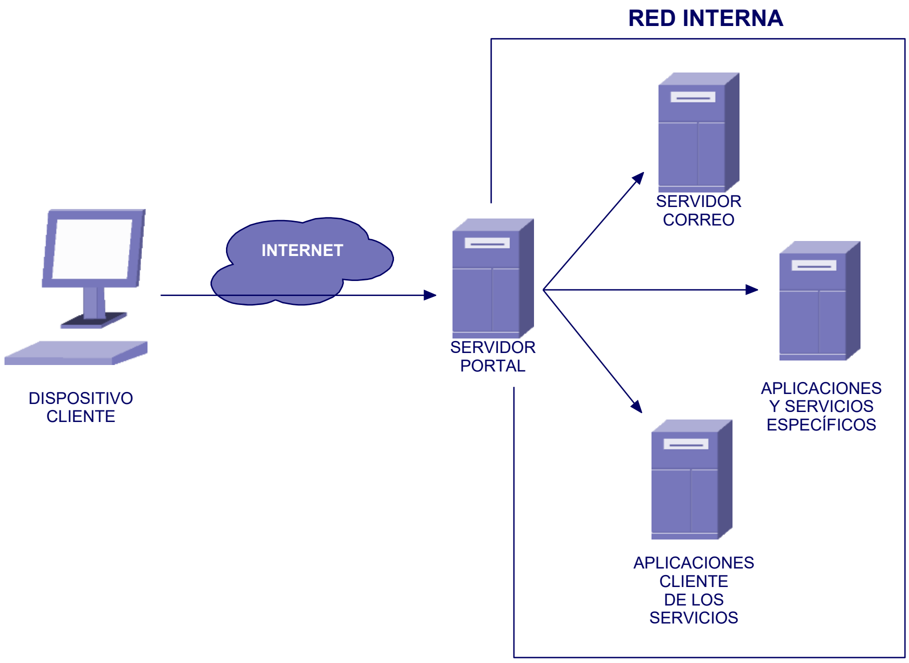

Figura 4. Arquitectura Portales Web. Fuente: elaboración propia.

Otra forma de que el cliente tenga acceso es mediante la implementación de un **acceso directo a las aplicaciones** desde el exterior, de forma que la aplicación pueda autentificar al usuario y proteger la comunicación. El usuario puede necesitar un software cliente o directamente usar el navegador ya que suelen ser aplicaciones basadas en web, como por ejemplo el web mail.

Por otro lado, los **escritorios virtuales** son una opción que permite a los usuarios el acceso remoto a un entorno de escritorio completo con las aplicaciones y recursos que necesitan. La tecnología de escritorio virtual se basa en que los recursos hardware y software que soportan y ejecutan los escritorios virtuales se encuentran en servidores en el centro de datos de la organización (ver figura 5). El usuario accede desde su dispositivo cliente a estos servidores, los cuales le asignan un recurso de escritorio y le envían su información gráfica y multimedia. El procesamiento se produce, por lo tanto, en los servidores. El almacenamiento de datos se produce en los servidores remotos, de forma que el cliente no almacena ningún dato sensible en su dispositivo.

Figura 5. Arquitectura escritorio virtual. Fuente: elaboración propia.

La tecnología de **Escritorio Remoto** (*Remote Desktop*) permite al usuario controlar de forma remota un equipo de la organización, normalmente el suyo (ver figura 6). El usuario tiene el control del teclado y el ratón del ordenador remoto y ve su pantalla en el dispositivo cliente. El escritorio remoto permite al usuario acceder a todas las aplicaciones, datos y otros recursos que normalmente están disponibles desde su equipo en la oficina. Se suele utilizar para labores de mantenimiento.

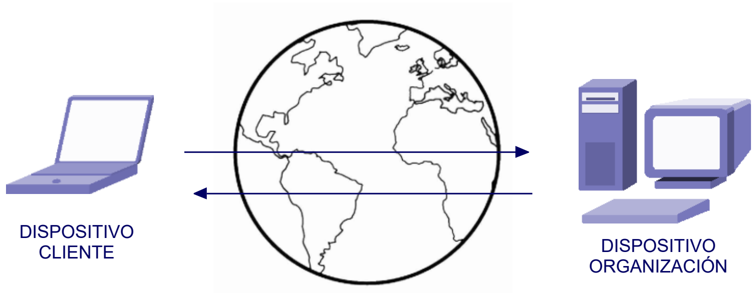

Figura 6. Escritorio remoto. Fuente: elaboración propia.

Un **espacio de trabajo digital** (*Digital Workspace*) es un marco de trabajo o *framework*, que integra varias tecnologías para entregar a los usuarios aplicaciones, datos y escritorios virtuales de forma unificada en un único espacio de trabajo.

Tras explicar los tipos de acceso remoto más importantes, en los apartados siguientes se explicará el acceso al servidor por parte de clientes conectados a través de internet por medio de las **Redes Privadas Virtuales.**

3.2 REDES PRIVADAS VIRTUALES

3.2.1 Introducción a las VPN

Una Red Privada Virtual (VPN, *Virtual Private Network*) es una red construida sobre una infraestructura de red pública, que permite establecer una conexión segura denominada "túnel" mediante datos cifrados para que no se puedan interceptar las comunicaciones dentro de un medio inseguro como es Internet.

- Virtual: no se trata de unir A y B mediante un cable físico, sino virtual a través de Internet.

- Privada: el acceso al propio recurso es dado por el creador de la red.

- Network: al unir A y B se genera una red entre ambas.

Las VPN permiten a los usuarios acceder desde un punto remoto al servidor de su organización a través de la infraestructura de encaminamiento que proveen las redes públicas. Así, este tipo de conexión permite a los usuarios una conexión punto a punto entre su ordenador personal, por ejemplo, y el servidor de su organización de la que quieren obtener sus recursos.

La infraestructura VPN está normalmente formada por dos elementos principales: el servidor o gateway y el cliente. El servidor VPN es el encargado de establecer las conexiones seguras a través del túnel VPN con los dispositivos del usuario, el cliente VPN, es decir, el software que debe instalarse en los dispositivos de usuario para poder establecer la conexión segura con el servidor VPN (ver Figura 7).

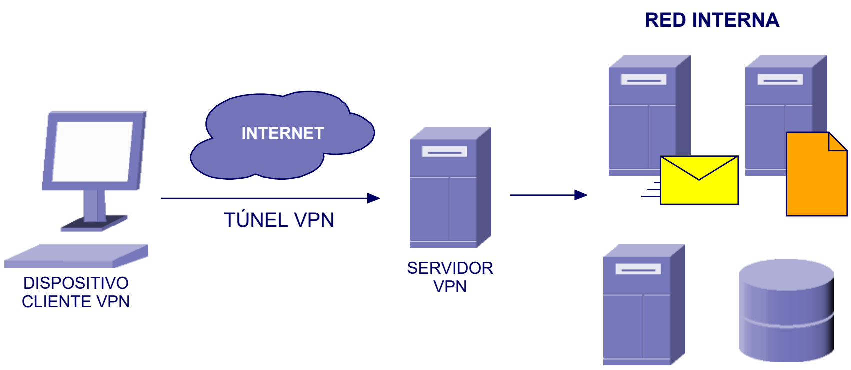

Figura 7. Arquitectura VPN. Fuente: elaboración propia.

3.2.2 Tipos de arquitectura VPN

<u>VPN de acceso remoto</u>

Es el modelo más utilizado y consiste en usuarios o proveedores que se conectan con la organización desde sitios remotos (como podrían ser la oficina, los cuarteles, los domicilios, incluso los hoteles) utilizando Internet como vínculo de acceso. Una vez autenticados, estos usuarios tienen un nivel de acceso muy similar al que tienen en la red local de la propia organización.

Un ejemplo de este tipo de VPN es VPN sobre LAN (*Local Area Network*). Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la LAN de la empresa. Esto permite aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes WiFi.

<u>VPN punto a punto</u>

Este esquema es el más utilizado para conectar organizaciones remotas con la organización central. Los servidores VPN, que poseen un vínculo permanente a Internet, aceptan las conexiones vía Internet provenientes de los sitios y establece los túneles VPN. Los servidores de las oficinas remotas se conectan a Internet utilizando los servicios de su ISP (*Internet Service Provider*) local, lo que permite eliminar los costosos vínculos tradicionales punto a punto (realizados por lo general mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales.

La tecnología más común es el *tunneling*. Esta técnica consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador, ver en Anexo IV) creando un túnel dentro de una red de computadoras (Militarpedia, 2016). El establecimiento de dicho túnel se implementa incluyendo una PDU (*Protocol Data Unit*) dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada (Ortín, 2020/2021). De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes.

3.2.3 Tipos de conexión

Conexión de acceso remoto: Una conexión de acceso remoto es realizada por un cliente o un usuario de un equipo que se conecta a una red privada. Los paquetes enviados a través de la conexión VPN son originados en el cliente de acceso remoto que se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente (Militarpedia, 2016).

Conexión VPN router a router: Una conexión VPN router a router (ver Figura 8) es realizada por uno de ellos que se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentifica ante el que responde y éste a su vez se autentica ante el que realiza la llamada.

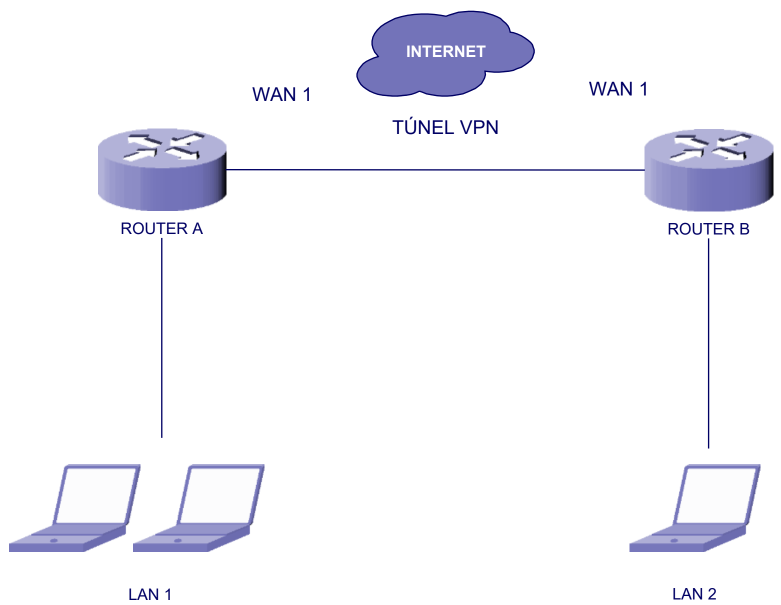

Figura 8. Conexión entre routers. Fuente: elaboración propia.

Conexión VPN firewall a firewall: Una conexión VPN *firewall* a *firewall* es realizada por uno de ellos, y éste a su vez se conecta a una red privada (ver Figura 9). En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El *firewall* que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.

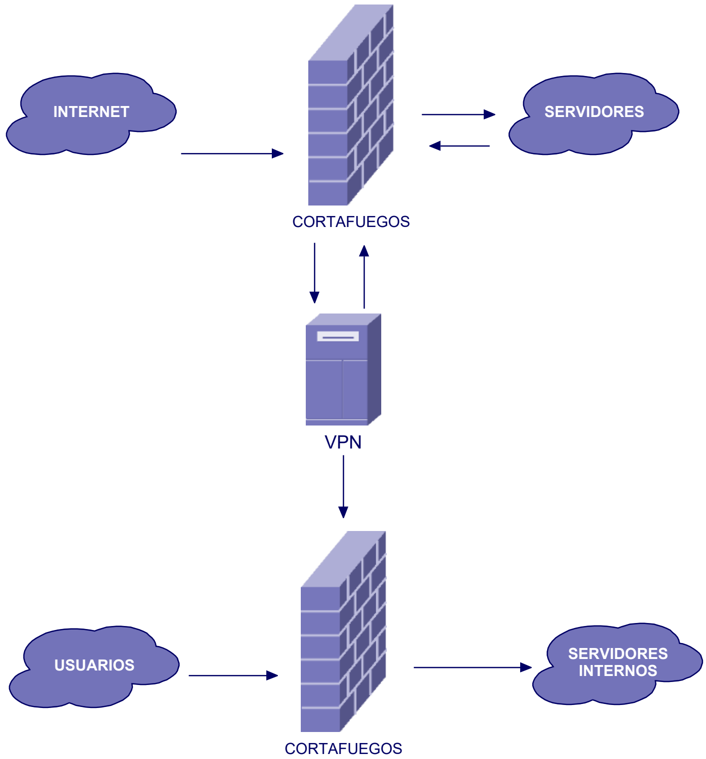

Figura 9. Conexión entre firewalls. Fuente: elaboración propia.

3.2.4 Implementaciones

Los protocolos de comunicación comúnmente utilizados son el IPSEC (*Internet Protocol SECurity*), PPTP (*Point to PointTunneling Protocol*), L2F (*Layer 2 Forwarding*), L2TP (*Layer 2 Tunneling Protocol*), SSL/TLS (*Secure SocketsLayer/Transport Layer Security*), SSH (*Secure Shell*) entre otros. Cada protocolo tiene sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados. El protocolo estándar, es decir, el más utilizado es el IPSEC a pesar de que actualmente hay una línea de investigación en crecimiento relacionada con el protocolo SSL/TLS que intenta hacer más amigable la configuración con nuevas soluciones a los problemas. Cabe señalar que para la implementación de túneles VPN para dar servicio a una Brigada se va a configurar mediante el protocolo IPSEC.

Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software. Dentro de esta familia se encuentran los productos de Fortinet, SonicWall, WatchGuard, Nortel, Cisco, Linksys, Netscreen (JuniperNetworks), Symantec, Nokia.

Las aplicaciones VPN por software son las más configurables y son ideales cuando surgen problemas de interoperabilidad entre los modelos anteriores. Obviamente el rendimiento es menor y la configuración más delicada puesto que se suma el sistema operativo y la seguridad del equipo en general. En este caso Linux puede ser ejemplo como posible solución, así como productos de código abierto como OpenSSH, OpenVPN y FreeS/Wan, a disposición de todo el mundo de forma gratuita.

Independientemente de la implementación adoptada (*hardware* o *software*) se pueden utilizar en ambos casos soluciones de firewall obteniendo un nivel de seguridad alto por la protección que brindan, aunque por supuesto en detrimento del rendimiento.

3.2.5 Amenazas de seguridad

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciber amenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f) (Jefatura del Estado, 2022).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas (Ministerio de Defensa, 2004).

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información, que, como se puede ver en la Tabla 1, puede ser de dos tipos: clasificada o sensible. (Ministerio de la Presidencia, 2010).

Precisamente el Real Decreto 3/2010 de 8 de enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

A continuación, se ofrece un listado de productos STIC (Figura 10) de referencia con el propósito de satisfacer las necesidades y demandas actuales de empleo de productos seguros en las redes del Ministerio de Defensa dentro de entornos clasificados dónde se maneje información clasificada y en entornos sensibles. El CCN publicó este pasado mes de diciembre el catálogo de productos y servicios de seguridad de las Tecnologías de la Información y la Comunicación (CCN, 2021)

TIPO DE PRODUCTO	INFORMACIÓN QUE MANEJA
APROBADO	CLASIFICADA
CUALIFICADO	SENSIBLE

Tabla 1. Tipos de productos seguros. Fuente: elaboración propia

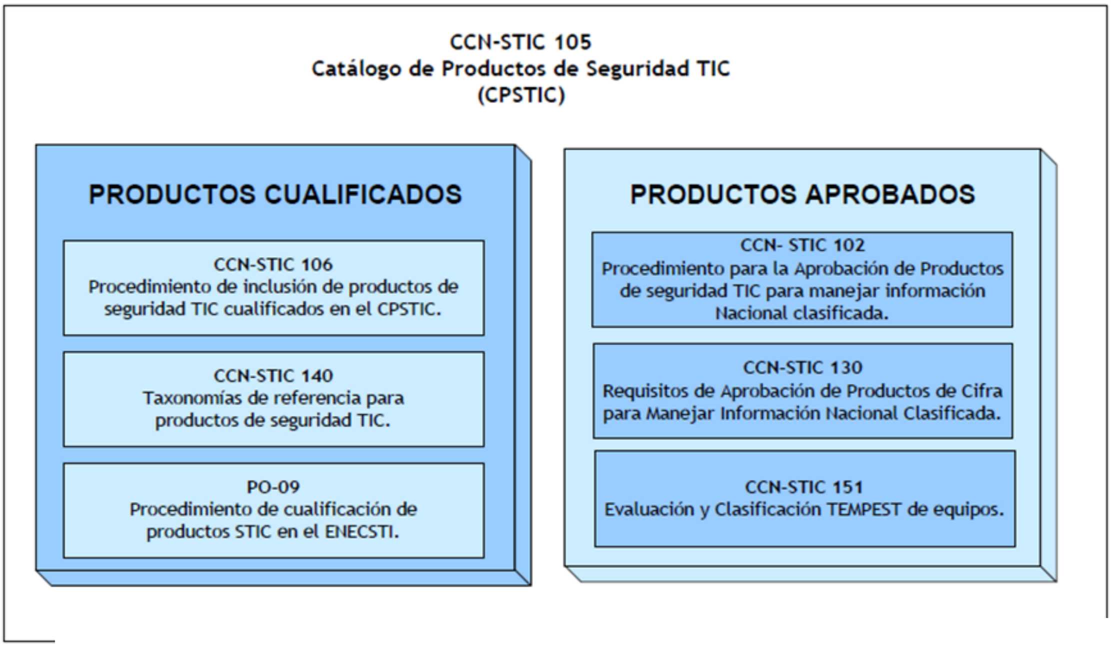

Figura 10. Protocolos de seguridad STIC. Fuente: CCN

3.2.6 VPN: Ventajas e inconvenientes

Como ya se ha mencionado, las redes privadas virtuales intentan dar soluciones principalmente a problemas tales como:

− El acceso remoto a la red de la organización.

− La interconexión de múltiples sitios remotos.

− Establecimiento de conexiones seguras.

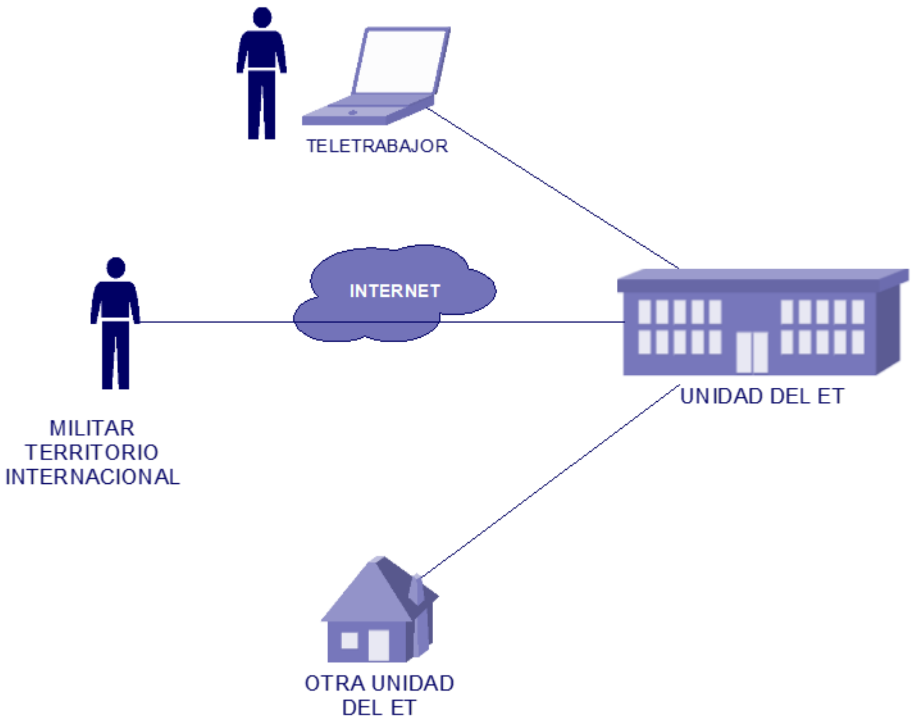

Figura 11. Ventajas que presenta el uso de VPN. Fuente: elaboración propia.

Las principales ventajas de su uso son la posibilidad de visitar cualquier página web desde cualquier lugar, así como proporcionar cualquier servicio evitando restricciones geográficas o que sigan el rastro de la huella digital del usuario.

Aunque las VPN presentan ventajas tales como el ahorro de costes, la flexibilidad y la escalabilidad, la implementación de una VPN acompaña consigo los siguientes problemas:

− Seguridad: las VPN requieren con mucha frecuencia de un gran esfuerzo de gestión relativa a la seguridad ya que requieren de la gestión de claves, conexiones, control de acceso…

− Compatibilidad: la mayoría de los protocolos que se utilizan para crear túneles y dotar de seguridad a la VPN no son compatibles entre ellos por ahora, por lo que es complicado seleccionar un único protocolo que satisfaga todas las necesidades.

− Fiabilidad y Rendimiento: las VPN sobre Internet dependen de la infraestructura pública de Internet y experimentan los mismos problemas que ésta. Además, a menudo las organizaciones necesitan que se les garantice una calidad de servicio (QoS).

− Cuellos de Botella Potenciales: el cifrado y descifrado o el encapsulado y desencapsulado de paquetes son acciones que requieren una gran capacidad de procesado y que hacen que aumenten el tamaño de los paquetes.

Esto mismo es lo que se pretende implementar en las Brigadas con la dificultad de trabajar con servidores creados por y para el ET, sin depender de aplicaciones de empresas privadas o de terceros. Por otro lado, la tecnología VPN permitiría al Ministerio de Defensa conectar con las Unidades del Ejército de Tierra desplegadas en territorio internacional a través de redes públicas ofreciendo comunicaciones seguras a largas distancias. Con la seguridad de estar enlazado dentro de una red como si fuese privada.

Tal como se puede apreciar en la Figura 11, las ventajas de implementar este sistema dentro del ET se encuentran clasificadas en tres niveles: Ministerio de Defensa, Brigadas y usuarios.

Cada uno de estos grupos, a pesar de presentar una serie de debilidades y fortalezas específicas, al formar parte de un mismo engranaje, todas las partes se enfrentan a las mismas amenazas y oportunidades.

A nivel del Ministerio de Defensa, implementar un servidor VPN en las Brigadas le posicionaría un lugar óptimo por las mejoras tecnológicas que implica y la seguridad que ofrece en Zona de Operaciones cuando se trata de la transmisión de información clasificada con el Territorio Nacional como destinatario. Como debilidad, se presenta la necesidad de expertos a nivel de configuración de equipos capaces de implementar servidores y equipos VPN innovadores para el ET.

A nivel Brigada, se estaría ofreciendo un alto nivel de operatividad a nivel táctico debido a la facilidad del mando y control por parte del Puesto de Mando cuando tiene a sus Unidades desplegadas. Sin embargo, haría falta personal técnico desplegado en la propia misión que fuese capaz de resolver incidencias muy específicas a nivel de red.

A nivel usuario, las VPN les ofrecen los servicios de su Unidad en cualquier lugar que presente redes públicas y un fácil manejo del dispositivo, como puede ser su propio teléfono móvil, para acceder a la información del equipo del despacho de su Unidad.

Como ya se ha mencionado, el puesto de mando tiene una serie de oportunidades con dicha implementación del sistema como puede ser la exclusividad del servidor VPN para dentro del Ministerio de Defensa, así como el control de diferentes Unidades desplegadas en diferentes zonas también.

DEBILIDADES	***AMENAZAS***
- Producto innovador dentro de las Unidades del ET sin referencias previas. *- Dependencia de personal cualificado*	*- Uso de información confidencial* *- Desconocimiento de la herramienta*
FORTALEZAS	***OPORTUNIDADES***
- Posicionamiento del ET en un lugar óptimo internacionalmente *- Facilidad mando y control* *- Fácil manejo*	*- Personalización del servidor y exclusividad* *- Mejoras tecnológicas* *- Monitorización de grupos de trabajo diferentes*

Tabla 2. Análisis DAFO (Elaboración propia). Fuente: opinión de expertos y pruebas propias.

No hay que ignorar las amenazas externas en medio del ciberespacio y el tipo de información clasificada que se maneja en la transmisión y recepción de datos a nivel de red. La tabla 2 recoge el análisis DAFO llevado a cabo sobre el uso de las VPN en las Brigadas. Este análisis ha sido realizado en base a la información recabada en la documentación consultada y la obtenida en las entrevistas con el personal experto (Anexo II). Para este caso se ha contado con le colaboración de un Teniente del Arma de Transmisiones desplegado en misiones internacionales, con cinco años de experiencia en una Brigada del ET. De acuerdo con el análisis realizado, el aspecto más favorable a destacar sobre la implementación de un servidor VPN, es la facilidad para el mando y control de las Unidades a nivel Brigada, teniendo en cuenta el tiempo que se necesita al principio para la instrucción de los usuarios en su manejo.

3.3 TIPOS DE ACCESO REMOTO DEL MINISTERIO DE DEFENSA

Dentro de los modos de acceso a los recursos internos del ET que ha mencionado el Ministerio de Defensa se encuentra la posibilidad de conectarse a la red interna por medio de redes públicas como es Internet. Este escenario, objetivo del futuro, podrá conseguir avances en lo referido a los recursos de mando y control dentro de las Unidades.

Una vez mencionados los conceptos más teóricos sobre la implementación VPN, en este apartado se tratará de explicar los objetivos que el Ministerio de Defensa se ha propuesto y cómo ponerlos en práctica dentro las Brigadas del ET.

3.3.1 Arquitectura I*Net

En la actualidad, por parte del Ministerio de Defensa se ha establecido una política respecto a las Tecnologías de la Información y las Comunicaciones aprobada en una Orden Ministerial por parte del Plan Director de Sistemas de Información y Telecomunicaciones (PDCIS) donde se estipulan dos redes de área extensa (WAN1) que dan soporte a los sistemas de información del Ministerio: WAN para Mando y Control Militar (WAN C2) y WAN Corporativa de Propósito General (WAN PG). Esta última conexión a la intranet del ET por parte de todos los usuarios pertenecientes al Ministerio de Defensa necesita la implementación y despliegue de una nueva arquitectura de acceso a Internet, denominada I*Net.

Este modelo de arquitectura de red ofrece los recursos internos de la Red de Área Extensa de Propósito General (WAN PG) a determinados equipos normalizados que tienen como objetivo proporcionar al usuario servicios como intercambio de mensajería interpersonal no oficial con el exterior mediante correo electrónico, denominado Correo Corporativo, así como servicios de navegación o publicación de información accesible por Internet. El acceso y manejo de esta información depende de sus grados de clasificación: sin clasificar, limitada o *nato restricted*.

Los servicios que se proporcionan al exterior es el acceso tanto de redes locales como la Red de Propósito General en el extranjero, así como la interconexión entre la WAN PG y la red de la Administración General del Estado (Intranet Administrativa de la AGE).

Todos estos servicios se agrupan en cuatro nodos en función de las características y origen de la conexión, siendo éstos:

- *Nodo de Internet Corporativa.*

- *Nodo de Redes Remotas.*

- *Nodo de Servicios Web.*

- *Nodo Extranet.*

De acuerdo con los nodos de interconexión en los que se agrupan los diferentes servicios de Internet del Ministerio de Defensa, se presenta el esquema de arquitectura final representado en la Figura 12 (Ministerio de Defensa, 2006).

---

[1] Una Red de Área Amplia (Wide Area Network o WAN, del inglés), es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 km hasta unos 1.000 km.

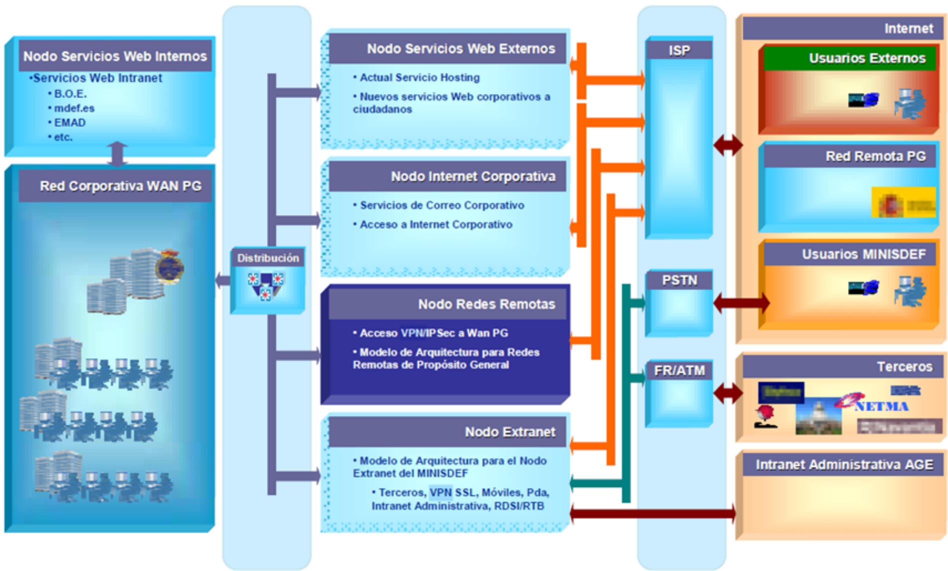

Figura 12. Modelo Arquitectura nodo acceso a Internet. Fuente: Ministerio de Defensa.

El modelo establece tres capas:

- La capa interior, que se corresponde con el interior del Ministerio de Defensa (red corporativa del Ministerio de Defensa, WAN PG).

- Una capa intermedia, la cual es la capa de servicios Internet/Extranet.

- La capa externa que se corresponde con el exterior de la ubicación física de la Unidad.

La capa externa representa los elementos de acceso al Ministerio de Defensa, que son los siguientes:

- A través de Internet: usuarios externos, redes remotas de propósito general y usuarios del Ministerio de Defensa.

- Entidades privadas y organismos nacionales e internacionales.

- Administraciones públicas a través de la Intranet Administrativa de la Administración General del Estado (AGE).

Los elementos de acceso anteriores podrán interconectarse a la capa de servicios Internet/Extranet del Ministerio de Defensa mediante proveedores de servicios de Internet (ISPs), líneas dedicadas (FR / ATM, *Frame Relay / Asynchronous Transfer Mode*) y líneas de telefonía PSTN (*Public Switched Telephone Network*).

Como se ha visto, el objetivo de la creación del Nodo Extranet por parte del Ministerio de Defensa es proporcionar acceso desde el exterior a los recursos internos de la Red de Área Extensa de Propósito General (WAN PG) al personal capaz de manejar información sin clasificar de forma inmediata o de difusión limitada por medio de líneas dedicadas por terceros, por Internet o también por servicios de correo y navegación. Se han detectado seis tipos de acceso identificados que podrían permitir el acceso a dicha información como marca la Figura 13 (Ministerio de Defensa, 2006).

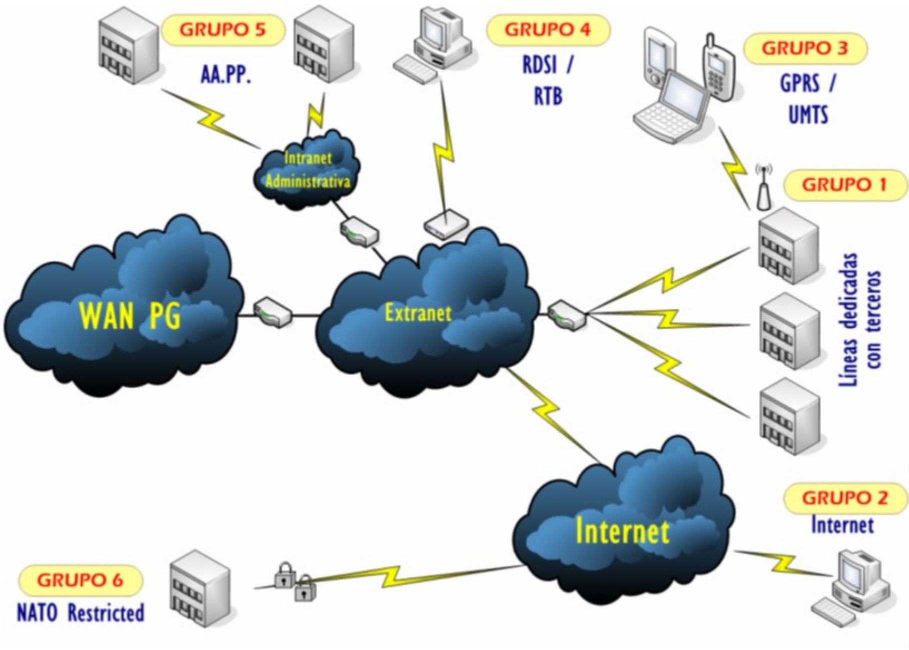

Figura 13. Grupos de acceso. Fuente: Ministerio de Defensa.

Como se ha mencionado, uno de los objetivos actuales propuestos por el Ministerio de Defensa es el acceso a los recursos internos por medio de Internet. En base a este objetivo, y de acuerdo a los grupos de acceso identificados presentados en la Figura 13, en el presente trabajo se va a tratar de implementar un túnel VPN a través del grupo de acceso número dos (Ministerio de Defensa, 2006).

Para llevarlo a cabo, se deben cumplir unos requisitos de seguridad específicos. En particular, se han de utilizar certificados emitidos por la Autoridad Certificadora (CA) del Ministerio de Defensa para la creación de los túneles VPN y para la autenticación de usuarios del Departamento.

El Modelo de Arquitectura del nodo de interconexión Extranet debe cumplir con los requisitos de seguridad para poder manejar información con un grado de clasificación nacional de DIFUSIÓN LIMITADA y cumplir los requisitos de la normativa del Centro Criptológico Nacional del Centro Nacional de Inteligencia (CCN/CNI) al respecto. En concreto, los que se describen en las siguientes normas:

- Instrucción Técnica CCN-STIC-301 Requisitos INFOSEC.

- Instrucción Técnica CCN-STIC-302 Interconexión de CIS.

- Guía de Seguridad CCN-STIC-408 Herramientas de Seguridad.

Se establecen unos requerimientos vistos en el anexo V para el funcionamiento del Nodo Extranet.

Para un acceso remoto de usuarios a los recursos internos por medio de Internet como medio de transmisión, se necesita un esquema de arquitectura basado en un dispositivo dedicado en exclusiva para ese uso y con capacidades de Red Privada Virtual (VPN). Los usuarios podrán tener acceso desde un puesto conectado a Internet de la manera explicada en el anexo VI.

Se implementará el escenario de acceso remoto mediante un producto que provea de capacidades VPN SSL según la arquitectura reflejada en el esquema de la Figura 14 (Centro Criptológico Nacional, 2021).

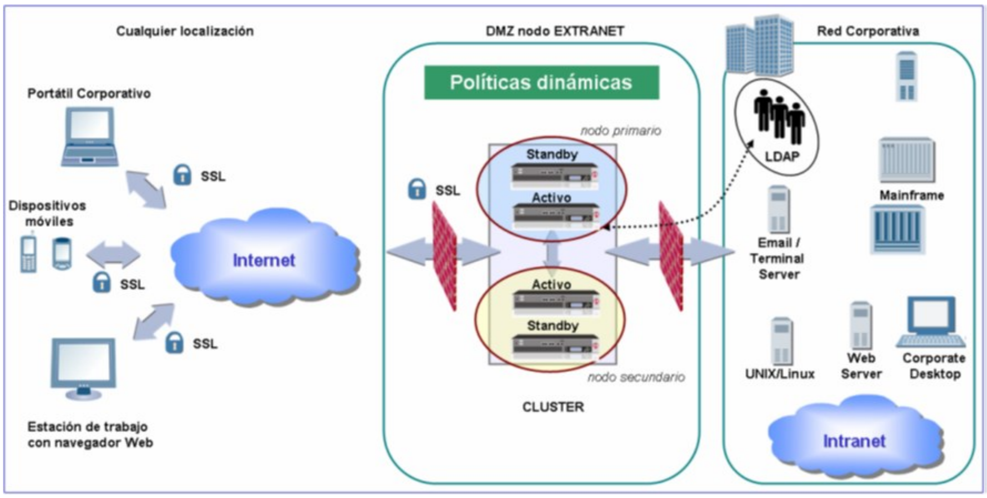

Figura 14. Arquitectura Internet por VPN. Fuente: CCN

A pesar de que esto se desarrolló teóricamente por parte del Ministerio de Defensa, también es cierto que el resto de las Brigadas no se está poniendo en práctica este recurso. A continuación, se procederá a desarrollar los criterios necesarios para un traspaso de información de manera segura.

3.3.2 Requisitos de seguridad

Para hacer posible el uso de una red privada de forma segura existen algoritmos matemáticos que garantizan la autentificación e integridad en la comunicación como puede verse algunos ejemplos en el anexo VII.

Para ello se necesita seguridad por parte de los usuarios en el manejo de sus equipos e información. Por parte del Ministerio de Defensa, se han publicado una serie de boletines de concienciación en ciberdefensa, que dejo uno de ellos en el Anexo VIII a modo de ejemplo. Por parte de los usuarios, se busca la autentificación, lo que permite el control de acceso a sus equipos. También se requiere la integridad del enlace, es decir, la garantía de que la información intercambiada a través del túnel VPN no ha sido alterada por equipos intermedios. Para este caso se utilizan algoritmos como el MD5 (*Message Digest*) o SHA (*Secure Hash Algorithm*).

Para cerciorarse de que el enlace no presenta repudio, los mensajes deben estar **firmados digitalmente** por el usuario que confirma ser el remitente y autor del propio mensaje. Por último, se debe garantizar la confidencialidad de la información como garantía de que solo ha sido gestionada por los destinatarios correctos. En este caso, se hace uso de algoritmos de encriptación con clave simétrica como el DES (*Data Encryption Standard*), 3DES y AES (*Advanced Encryption Standard*).

Por ello, los requerimientos básicos necesarios son:

- Identificación de usuario: las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentran autorizados.

- Codificación de datos: los datos que se van a transmitir a través de una red pública (Internet), deben de ser cifrados previamente de modo que no puedan ser leídos. Esto se consigue con algoritmos de cifrado como DES o 3DES que sólo pueden ser leídos por el emisor y el receptor de los datos.

- Administración de claves: las VPN deben actualizar las claves de cifrado para los usuarios.

Existen diferentes mecanismos de cifrado para proteger la privacidad de la información a través de Internet, como son la firma digital, el mecanismo de un solo sentido o la clave simétrica.

Firma digital.

- Consiste en enviar información a un destinatario, de modo que éste pueda comprobar dos cosas: *i)* Que ha sido el usuario quien ha generado la información,y *ii)* Que dicha información no ha sido modificada durante el tránsito.

- Consiste en calcular el "*hash*"[2] de la información a enviar, y cifrarlo con la clave privada. El resultado se añadirá a la información a enviar. El Hash son los bits obtenidos como resultado de aplicar una función resumen a unos datos (Centro Criptológico Nacional, 2021)

- El receptor descifrará el *hash* con la clave pública y la comparará con el "hash" que calcule él mismo a partir de la información recibida. Rechazará el paquete en caso de que no sean iguales.

- La información se puede enviar cifrada o no, con una clave simétrica. Si se hiciera, el destinatario debe conocer esa clave simétrica para poder descifrarla y acceder a la información y calcular posteriormente su "*hash*".

Mecanismo de un solo sentido (*one-way hash*).

- Es un algoritmo público, que se utiliza para producir una "digestión", que consiste en una "firma" no descifrable. No sirve, por tanto, para enviar información cifrada, sino como "*checksum*"[3] de la información que acompaña.

- Propiedades: El hash resultante varía al modificar el texto de entrada, aunque sea sólo un byte (dispersión). Existen "colisiones", textos completamente distintos que producen la misma firma.

- La longitud de la firma es una constante del método matemático, independiente de la longitud del texto al que se aplica el cálculo de hash.

- El equipo receptor compara este "*hash*" recibido con el que calcula él mismo (no necesita clave). Rechazará el paquete si no son iguales.

Clave simétrica.

- Es cuando un algoritmo de cifrado utiliza la misma clave tanto para cifrar como descifrar.

- La transferencia entre dos equipos exige que ambos hayan acordado, mediante un medio seguro, una clave simétrica común.

---

[2] Es un algoritmo matemático denominado Secure Hash Algorithm capaz de transformar cualquier bloque arbitrario de datos en una nueva cadena única de caracteres con una longitud fija.

[3] El checksum, o suma de comprobación, es el resultado de la ejecución de un algoritmo dentro de un archivo único. Comparar el checksum que se genera del archivo provisto por la fuente y el generado por la versión del nuevo, representa una ayuda para asegurarse una copia libre de errores.

4 DESARROLLO: ANÁLISIS Y RESULTADOS

4.1 REQUISITOS PARA LA INFRAESTRUCTURA DE RED

A continuación se describe la práctica donde se llevan a cabo las pruebas de implementación de un servidor de acceso remoto VPN para el mando y control de una unidad táctica a nivel Brigada, en concreto, la BRILAT ‘Galicia VII’ donde se llevaron a cabo las Prácticas Externas. El propósito de esta práctica es implementar la securización y fiabilidad que nos proporciona el túnel VPN para un sistema de mando y control que haga la labor del mando más eficiente en zona de operaciones.

Para ello se ha intentado implementar el sistema BMS (Battlefield Management System), explicado en el anexo IX, a través de un túnel VPN. Esto requiere que uno de los equipos actúe como servidor VPN y el otro como cliente VPN, según marcan los modos de autentificación IPSec y las estructuras y encapsulamientos de sus paquetes desarrollado en el anexo X. Para el diseño de la infraestructura de la red se configuró el servidor VPN en el sistema operativo haciendo uso de un equipo con Windows 10. El mismo sistema operativo es el que se necesita para configurar el acceso del equipo del cliente.

Esta práctica se ha desarrollado en base al Acuerdo de Diffie-Hleman (Anexo VII), que consiste en la distribución de claves, es decir, generar en dos equipos la misma clave simétrica a partir de intercambiar información en texto claro sin ser utilizado para cifrar o descifrar. En primer lugar, se comienza intercambiando números primos grandes para factorizarlos. Cada uno genera una clave privada. Pero para generar la clave pública se utiliza un algoritmo en el que intervienen los números intercambiados previamente además de la clave privada local.

En definitiva, las claves públicas se transmiten al otro equipo, pero no son independientes entre sí debido al modo en que han sido generadas. La propiedad que tienen es que cada equipo puede generar, por separado, la misma clave simétrica a partir de su privada y la pública del otro.

4.1.1 Comprobación túnel seguro

Existen tres mecanismos para comprobar que detrás de la dirección IP del otro extremo del túnel seguro se encuentra el destinatario correcto:

1. Claves compartidas o *Pre-shared*.

2. Algoritmo de cifrado RSA.

Intercambio de claves públicas. Las claves privadas son inaccesibles para el propio administrador mientras que la pública se puede leer para poder enviarla al administrador del otro equipo. Es decir, permite al remitente conservar la confidencialidad de la información cuando es transmitida a través de equipos terceros. Se puede utilizar el método de autentificación RSA en VPN IPSec usando SSH *(Secure Shell)* o contactando con un servidor de certificados digitales.

3. Certificado Digital (estructura PKI).

Una vez se hayan se haya realizado la autenticación de los certificados digitales de ambos extremos, es decir que hayan obtenido ambos previamente el certificado digital del servidor, se comprueba su autentificación. En base a la capacidad de identificar falsificaciones si ambos están firmados digitalmente por la misma entidad emisora.

4.1.2 Servidor de Certificados Digitales

Los equipos clientes (router, PC) solicitan un certificado digital de un CA (*Certification Authority*) server, para ser utilizado como medio de autentificación al negociar la transmisión de información a través del VPN IPSec (Cisco, 2017).

Los pasos a realizar son:

1. La generación de una pareja de claves asimétricas, para poder hablar en modo seguro con el CA server. En el momento de contactar, el CA server y el equipo cliente se intercambian dinámicamente las claves públicas. Los certificados, al tener hora de emisión y caducidad, deben estar sincronizados. Así mismo, también se debe configurar la información DNS, de ese modo, el CA Server accede mediante URL.

2. Se genera en el router o en el pc una petición de certificado. Es un documento electrónico normalizado PKSxx.

3. Esta petición se envía en modo seguro al CA server. Se obtiene la clave pública de este CA para encriptar la petición.

4. El administrador del CA server decide concederlo. Para la prueba en la Brigada Galicia VII la concesión puede ser automática. En un ejercicio real, sin embargo, se necesita un trámite administrativo que puede demorar varios días la concesión para conseguir el certificado (formato X.509x) que incluye la información del usuario y de la autoridad emisora, número de serie, fechas de expedición y caducidad, punto de distribución de certificados revocados, la clave pública y la firma digital.

4.1.3 Autentificación mediante certificados

En la negociación de plantillas de IKE phase 1, se acuerda la autentificación por certificados emitidos por una autoridad certificadora común. A continuación, se intercambian los certificados ambos extremos entre sí. Como los certificados están firmados digitalmente por el CA servidor, y su clave pública es conocida por los extremos, ambos pueden detectar falsificaciones comprobando las fechas de emisión, caducidad e identidad del otro extremo.

También se comprueba si el número de serie del certificado aportado por el otro extremo no está incluido en la lista CRL (Certificate Revocate List), publicada por la autoridad emisora del mismo, como se ve en la Tabla 3. En dicha tabla se muestra el orden de aparición de los datos de ambos extremos, tanto el algoritmo que utilizan para transmitir la información, como la autoridad que certifica su validez, así como su periodo, etc.

	VERSIÓN DEL CERTIFICADO
	NÚMERO DE SERIE
INDENTIFICADOR DEL ALGORITMO PARA FIRMAR EL PAQUETE X.509.	Algoritmo Parámetros
AUTORIDAD CERTIFICADORA	ENTIDAD EMISORA
PERIODO DE VALIDEZ	No antes de... No después de...
PROPIETARIO DE LA CLAVE PÚBLICA QUE SE ESTÁ FIRMANDO	USUARIO
CLAVE PÚBLICA DEL USUARIO PARA IDENTIFICAR EL ALGORITMO UTILIZADO	Algoritmo Parámetros LLave
FIRMA DIGITAL CON CLAVE PRIVADA DE UNA UNIDAD CERTIFICADORA	FIRMA

Tabla 3. Autenticación mediante certificados. Fuente: elaboración propia.

4.1.4 Estructura PKI

Consiste en que los ordenadores cliente obtienen certificados de otro ordenador del nivel superior PKI. El equipo cliente conectado al recibir su certificado personal, recibe también la cadena de certificados del ordenador servidor a dos niveles:

- *Root certificate*: Certificado expedido del ordenador servidor.

- *Identity certificate*: Certificado del ordenador cliente que valida su identidad.

De esta manera, dos equipos distintos que hayan obtenido sus certificados del mismo servidor pueden verificar la autenticidad de sus certificados a partir del certificado *Root.*

4.1.5 Fases de las VPN IPSec

1. Configurar IKE (Internet Key Exchange)

Ambos extremos del túnel deben coincidir en el tipo de tráfico que van a intercambiar mediante la VPN. Así, cuando uno de los extremos recibe un paquete IP dirigido al otro que debe ser cifrado pero no tiene ningún túnel seguro en ese momento, iniciará la construcción del mismo. Es lo que se denomina túneles bajo demanda.

Para esta parte se configura lo siguiente:

- Encryption (Valor por default: DES)

- Hash (Valor por default: SHA)

- Authentication (Valor por default: RSA-SIG)

- Group (Valor por default: 1)

- Lifetime (Valor por default: 1 día, es decir, 86400 segundos)

Hay que tener en cuenta que mientras más bits agreguemos a los algoritmos de cifrado y mientras utilicemos algoritmos más complejos, entonces más CPU se necesitará; por esta razón es importante definir cuáles son las limitaciones de hardware de los equipos antes de pasar a la configuración.

2. IKE phase 1. El objetivo es crear un túnel seguro, denominado **de control, para negociar** los túneles para el tráfico de usuario. Se realiza en tres pasos (separados si se hace en modo "*main mode* (MM)", o juntos si se hace en "*agressive mode* (AM)".

Primero intercambian plantillas de configuración para encontrar una común. Seguidamente ejecutan el acuerdo Diffie-Helman. En este momento el túnel es seguro (cifrado). Y después realizan la autentificación.

3. IKE phase 2. El objetivo es crear un túnel seguro, denominado **de producción para el tráfico** de información. Se realiza en un sólo paso (QM "*quick mode*"). Intercambian plantillas de configuración para encontrar una común en una combinación concreta de algoritmos.

Las plantillas de ambas fases IKE se encuentran desarrolladas en el Anexo XI.

Para representar una política de seguridad de tráfico se debe definir una combinación de transformaciones IPSEC de forma individual. Nuevamente los pares definen parámetros específicos.

4. Se utiliza el túnel anterior para **enviar el tráfico** interesante en modo túnel o transporte.

5. Al dejar de transmitir información, el túnel finaliza. Para renovar las claves debido a que se ha superado el tiempo de uso o el volumen de tráfico, se sustituye el túnel por otro.

4.1.6 Configuración para la seguridad del túnel VPN

A continuación, se describen los comandos necesarios para la configuración de un túnel VPN en el sistema operativo de cualquier equipo de la Brigada para el mando y control de la Unidad.

IPsec es un conjunto de protocolos para autenticar y cifrara todo el tráfico de IP entre dos ubicaciones. Permite que los datos fiables pasen a través de redes que de lo contrario se considerarían no seguras. Los puntos finales de los túneles IPsec pueden estar ubicados en cualquier lugar y aun así proporcionan acceso a toda su red privada o a las redes que especifique. Los túneles IPsec son incompatibles si se utiliza una zona, o los puntos finales del servicio de nube.

El acceso VPN de IBM Cloud permite a los usuarios gestionar todos los servidores de forma remota y segura en la red privada de IBM Cloud. Una conexión VPN desde su ubicación a la red privada permite la gestión fuera de banda y el rescate de servidor a través de un túnel VPN cifrado. Con el acceso VPN, puede:

- Establecer una conexión VPN en la red privada mediante SSL o IPsec.

- Acceder al servidor con la dirección IP 10.x.x.x privada mediante SSH o RDP.

- Conectarse a la dirección IP de IPMI del servidor para otras tareas de rescate y gestión de servidores.

<u>0. Planificación y comprobación de la red.</u>

Se definen los parámetros de negociación necesarios para una conexión VPN.: Dirección IP estática para el punto final de VPN, clave precompartida (contraseña), algoritmo de cifrado (DES, 3DES, AES128, AES192, AES256), de autenticación (MD5, SHA1, SHA256)…- Se comprueba que la red IP de tránsito permite el tráfico IPSec: Paquetes en texto claro UDP dirigidos al puerto 500 (protocolo ISAKMP), Paquetes AH (protocolo 50) y Paquetes ESP (protocolo 51).

1. Identidad del otro extremo y clave compartida.

crypto isakmp enable

crypto isakmp identity address | *name*

crypto isakmp key CLAVE address x.x.x.x.x (si la autentificación es pre-shared)

Se visualiza con el comando: *show crypto isakmp key*

2. Autentificación".

authentication pre-share (claves compartidas)

authentication rsa-sig (certificados)

authentication rsa-encr (claves asimétricas)

- Encriptación: DES, 3DES, AES.

- Grupo de Diffie-Helman: 1, 2.

- Hash: MD5, SHA-1.

- Tiempo de vida. (tiempo en segundos, se elige el número menor propuesto por ambos extremos).

Se visualiza con el comando: **show crypto isakmp policy**

Una vez configurados ambos extremos siguiendo los pasos anteriores, se asegura un correcto traspaso de información a través de la conexión de ambos extremos conectados a Internet.

4.2 CONFIGURACIÓN DE VPN IPSEC

Para la realización de la práctica dentro de la Compañía de la Brigada Galicia VII, con el objetivo de poder transmitir información de la propia Unidad a través de Internet se propuso implementar el siguiente esquema de red de la Figura 15:

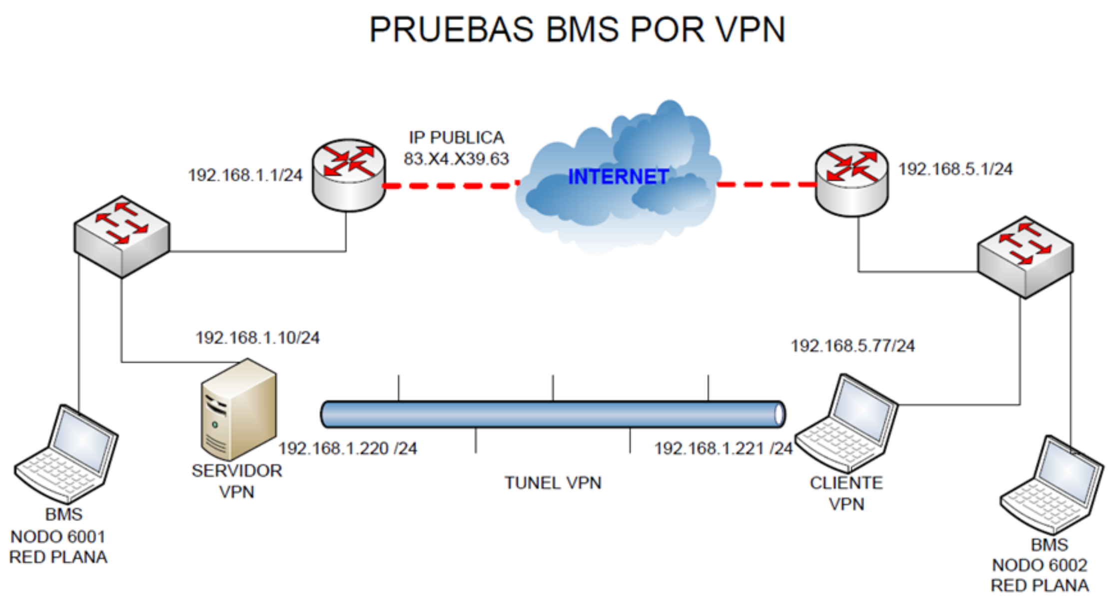

Figura 15.Esquema de red objeto. Fuente: elaboración propia

Una manera sencilla de entender la práctica, más concretamente, entender la configuración de los equipos sería explicando el siguiente esquema de red mostrado gráficamente en la Figura 16:

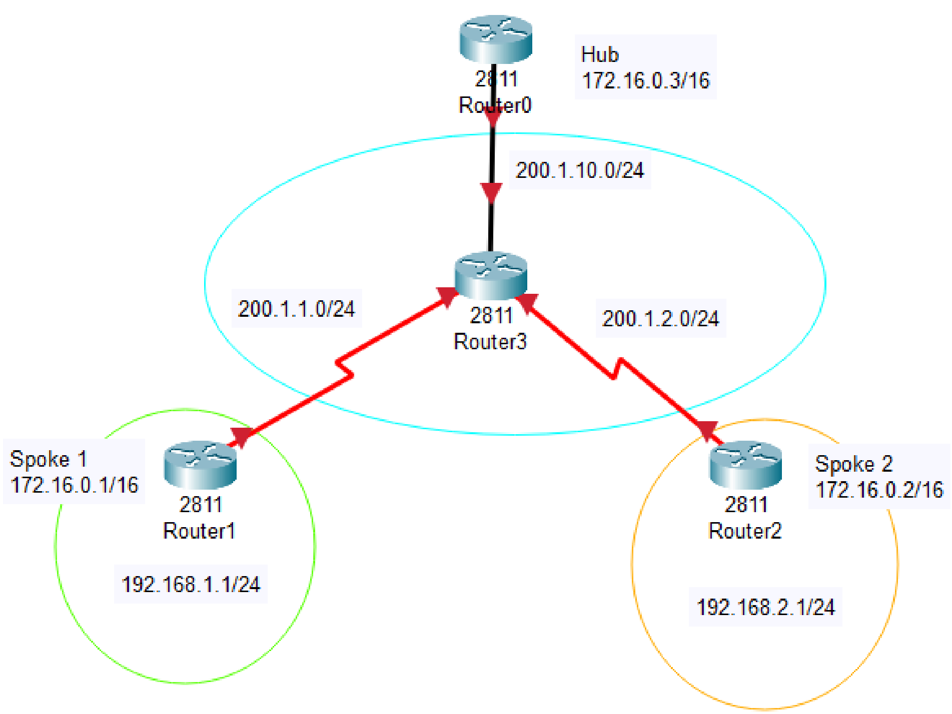

Figura 16. Esquema red DMVPN. Fuente: elaboración propia.

Esta arquitectura de red está formada por un Switch Central L3 y tres routers que se localizan uno de ello en la zona del acuartelamiento y otros dos más de los extremos de la arquitectura de red de la Figura 16 que corresponden a los usuarios conectados a través de cable Ethernet a sus respectivos equipos portátiles.

La VPN que se monta es de tipo SITE TO SITE entre los router de los emplazamientos fijos y desplegables.

Se complica un poco ya que parece el concepto de Hub como concentrador de VPN, con el concepto DMVPN, que no es otra cosa que llevar la VPN al novel de interconexión múltiple.

En el esquema de la figura 16, la zona pública representaría, por ejemplo, Internet y por lo tanto se necesita que todos los *routers* puedan alcanzarse entre sí. R3 representa la red pública. En la Brigada se hizo la práctica con un Switch Central L3 (Figura 17) (Cisco, 2021) configurado con varios interfaces IP. La configuración queda desarrollada en el Anexo XII.

Para la creación de túneles GRE cuya configuración se desarrolla en el Anexo XIII, se deben crear a través de la Red Pública, especificando que el túnel es Multipoint. Se debe especificar un nuevo direccionamiento privado para la red multipunto que creará los túneles.

Figura 17. Switch Central L3. Fuente: Cisco

Los *routers* situados en los extremos de la Figura 16, deben definir el origen del túnel y el destino mediante el protocolo de resolución del siguiente salto NHRP que se desarrolla en el Anexo XIV.

El comando ip nhrp map “ip-privada” “ip-pública” hace un mapeo de la dirección del túnel hacia la dirección ip que es pública. Cuando los router de los extremos quieren enviar información nhrp deben encapsularla a través de la dirección IP Pública.

El comando ip nhrp nhs “ip-privada” es para indicar donde está el servidor NHRP, y averiguar las direcciones de los demás routers y así crear los túneles GRE de forma automática.

El comando ip nhrp map multicast ip-pública sirve para encapsular el tráfico multicast con la dirección pública del Router-HUB

El comando ip nhrp map multicast dynamic es para que el Router Central, “hub” pueda construir la tabla en base a los mensajes unicast que llegan al Router hub que han sido previamente reencapsulados.

Esto es muy importante todo si se ejecutan protocolos de enrutamiento dinámicos como OSPF[4] o EIGRP[5], ya que éstos utilizan direccionamiento Multicast. La configuración IKE se desarrolla en el Anexo XV.

En este punto, ya estaría configurado DMVPN y para verificarlo sería necesario el comando show dmvpn para ver las entradas estáticas de los router de los extremos y las entradas dinámicas del router central.

El comando Show Crypto map muestra los crypto maps configurados

El comando Show crypto isakmp policy muestra las políticas IKE

[4] OSPF usa un algoritmo de tipo estado de enlace.
[5] IGRP utiliza la tecnología de ruteo del vector de distancia.

El comando Show crypto ipsec transform-set muestra la plantilla para IKE fase 2, transformaciones

El comando Show crypto ipsec sa muestra los túneles establecidos IPSEC.

4.3 ANÁLISIS DE MERCADO

Los servicios que presta el uso de un túnel VPN para transmitir información de la red interna superan las prestaciones de los equipos que actualmente se encuentran en los distintos niveles de la Compañía de Transmisiones del Batallón de Cuartel General de cualquier Brigada del ET.

La búsqueda de nuevos sistemas de comunicación se ha realizado en función del análisis de los actuales medios que están en uso en zona de operación como, por ejemplo, de la aplicación ATAK, *Android Team Awareness Kit* (Interfaz de la aplicación en la Figura 18 (American Security Today, 2018)

Dicha aplicación desarrollada por el Laboratorio Draper, en su versión militar, anunció que ayudaría a reducir las bajas civiles cuando salió la versión inicial en 2010. Hace uso del sistema operativo Android para introducir una solución informática móvil a través de dispositivos portátiles como pueden ser las *tablets* o los teléfonos móviles y que son capaces de conectarse a las radios militares.

Con los desarrolladores de esta aplicación en versión militar se permite agregar diversas funcionalidades dependiendo de la misión como pueden ser compartición de archivos o herramientas de medición del alcance o el rumbo (Android Team Awareness Kit, 2020). Otras posibles ventajas que presentan son la facilidad de su portabilidad y la simpleza de la configuración. Sin embargo, presenta una limitación fundamental para descartar dicho uso dentro del ámbito militar y es la dependencia a las antenas cuyos propietarios son empresas privadas (Orange, Moviestar, Vodafone) cuya localización del equipo principal emisor de redes que da acceso a Internet sería muy fácil y por tanto, pondría en riesgo el desarrollo de la misión.

Figura 18. Militar usando la aplicación ATK. Fuente: American Security Today

4.4 GESTIÓN DEL PROYECTO

A lo largo del desarrollo de este apartado se va a tratar de definir aquellos usuarios en la implementación de este proyecto para facilitar el mando y control dentro de las Unidades donde estén encuadrados, así como los riesgos a asumir por parte del MINISDEF y el tiempo necesario para el funcionamiento de un servidor VPN dentro del ET.

4.4.1 Stakeholders

La matriz interés-poder (Tabla 4) es de gran utilidad para el análisis estratégico del proyecto, ya que permite diseñar estrategias dirigidas a facilitar sus relaciones con los *stakeholders* o grupos de interés que irían desde el Ministerio de Defensa hasta la sociedad española pasando por los militares encargados tanto del mando y control de los ejercicios militares como de la configuración. De esta forma, se pueden diseñar estrategias que sean aceptadas por todos y cada uno de sus grupos de interés.

	INTERÉS BAJO	INTERÉS ALTO
PODER BAJO	Estrategia de esfuerzo mínimo	Estrategia de mantener informados
	Usuarios de equipo (tropa, suboficiales)	Usuarios de mando (oficiales)
PODER ALTO	Estrategia de mantener la satisfacción	Estrategia de actores clave
	Empresas privadas que ofrezcan este servicio	Ministerio de Defensa

Tabla 4. Matriz interés - poder. Fuente: elaboración propia.

El grupo de usuarios de interés para comenzar dicho proyecto es el encabezado por el Ministerio de Defensa, del cual depende la implementación de los servicios de VPN a las Unidades del ET asegurándose de que la información se transmite de manera íntegra entre todos los usuarios autentificados. Sin embargo, esta matriz ofrece una visión estática de la situación, que deberá complementarse con un análisis dinámico de los *stakeholders*, que permita analizar su evolución a lo largo del tiempo, dado que tanto su grado de interés como su poder de influencia pueden cambiar.

Otro posible actor clave en la orgánica de la Unidad, es la necesidad de una figura experta en este recurso de redes, por lo que sería necesario profesionalización y concienciación en la escala de mandos superiores. Lo que es evidente, es que los usuarios, es decir, los militares operarios de esta aplicación deben estar informados, aunque el interés para la implementación no dependa directamente de ellos.

4.4.2 Gestión de riesgos

Como cualquier otro proyecto, puede haber una serie de factores de riesgos que debemos identificar con antelación, para ello se ha consultado tanto a los miembros interesados de su implementación como a los usuarios finales, en este caso, las Unidades del Ejército de Tierra dentro del Ministerio de Defensa. El objetivo es anticiparse a la aparición del riesgo.

Los riesgos se pueden clasificar según su origen, tanto interno (falta de presupuesto, usuarios cometiendo infracciones, información clasificada expuesta al ámbito público) como externos (fallos en los protocolos de seguridad de la red, imposibilidad de desencriptar una información, cambio en la normativa reguladora, etc.)

También se pueden clasificar según el tipo, por ejemplo, técnico, calidad, financiero, contractual, de proceso o incluso de logística o mercado.

Para llevar un registro de riesgos se ha optado por hacer uso de una herramienta de análisis cualitativa. Dicha herramienta permitirá comprobar la viabilidad del proyecto. Este análisis consiste en el estudio de las causas de las posibles amenazas, así como probables sucesos no deseados y las consecuencias y daños que éstas puedan producir (Val, 2021). Los riesgos que se muestran en la Tabla 4 han sido identificados a través de la consulta de documentación y las entrevistas realizadas a expertos de la Unidad (Anexo II).

Cada riesgo tiene asignado un impacto (H: Alto, M: Medio, L: Bajo) así como una probabilidad de ocurrencia (1, 2, 3) que han sido evaluados a partir de la entrevista al personal interesado en la implementación del servidor VPN. La combinación del impacto que puede ocasionar el riesgo al objetivo del proyecto y la probabilidad de ocurrencia genera como resultado una clasificación cualitativa de los riesgos. El análisis realizado incluye, además, los efectos que tienen los riesgos en el proyecto, así como las medidas y/o soluciones alternativas que intentan disminuir o eliminar la gravedad de los riesgos detectados.

CAUSA	IMPACTO (H,M,L)	PROBABILI DAD (1,2,3)	CLASE	EFECTO	ALTERNATIVA
Creación de una incorrecta arquitectura de red	H	2	2H	Fallos del servidor	Cursos para obtener personal cualificado
Control de acceso y autenticación	M	1	1M	Dispositivos no protegidos contra amenazas externas	Detectar los malware
Ancho de banda de trabajo remoto	M	3	3M	Problemas de velocidad	Políticas restrictivas según prioridad
Rechazo del proyecto por desconocimiento	H	1	1H	No implementación del servidor	Iniciar fase de marketing
Falta de jurisdicción	L	2	2L	Destinatario erróneo en el intercambio de información encriptada o clasificada	Redactar documentos oficiales para poner en común nueva información

Tabla 5. Matriz probabilidad - impacto. Fuente: elaboración propia.

En caso de riesgo bajo no se prevé ningún inconveniente grave ya que se asumirían las consecuencias en caso de materializarse. Por ejemplo, este sería el caso del riesgo “rechazo del proyecto por desconocimiento”, que tendría una probabilidad de ocurrencia muy bajo debido a la sencillez de la implementación, la facilidad de uso y la mejora en la operatividad de la misión. Otro caso sería el riesgo “la falta de jurisdicción”, problema que se solucionaría con nuevas normativas y actualización de las políticas de información actuales.

En caso de riesgo moderado se plantean actividades de seguimiento y control de las áreas afectadas por el propio riesgo. Este es el caso de la existencia de políticas de prioridad según el nivel de usuarios, cuya solución a nivel de red pública ya no dependería del operador sino del uso que esté haciendo el resto. La matriz probabilidad-impacto obtenida del análisis anterior aparece en la Tabla 6.

CLASE DE RIESGO	NÚMERO
CRÍTICO	0
ALTO-MEDIO	2
MEDIO	2
BAJO	1
TOTAL	5

Tabla 6. Resultados de la matriz probabilidad - impacto. Fuente: elaboración propia.

Cabe destacar la ausencia de riesgos críticos que supondrían la inviabilidad de implementar el servidor VPN. Existen riesgos de nivel alto-medio que, sin embargo, podrían ser solventados con las acciones propuestas (por ejemplo, la creación de una incorrecta arquitectura de red que daría lugar a fallos en el servidor, puede solucionarse a través de cursos de formación específicos para obtener personal cualificado). De igual modo, los problemas que aparecen a niveles medio-bajos podrían subsanar por medio de actividades relativamente accesibles a todas las Unidades. Con todo ello, a partir de este análisis se puede concluir que, tomando las medidas adecuadas, el proyecto planteado es viable.

4.4.3 Gestión de tiempo

Este proyecto se ha podido implementar en el periodo de prácticas, es decir, durante 6 semanas siguiendo las etapas de tiempo seguidas en la Tabla 7 que se adjunta a continuación.

Primeramente, se realizó un estudio de la normativa, legislación y proyectos actuales que está siguiendo el Ministerio de Defensa en lo relativo a la transmisión de información por medio de Internet. A la semana siguiente, se procuró recopilar todas las opiniones de expertos, es decir, personal encuadrado dentro de la Compañía de Transmisiones de la BRILAT que indicó las limitaciones de los equipos actuales y la posibilidad de una nueva forma de teletrabajar independientemente de la distancia a la Base sin perjudicar la seguridad de la información.

Seguidamente, se trató de estudiar lo referente a los tipos, modos y arquitecturas de las que hacen uso los túneles VPN durante la fase intermedia. Así en la fase de creación, se pudo realizar una práctica de implementación de dicho servicio. Verificando en una fase final la viabilidad del proyecto.

Etapa	Proceso	Fecha Inicio	Duración	Fecha Fin
Fase Informática	Manuales Ministerio de Defensa	06/09/2021	5	11/09/2021
	Manuales de VPN	11/09/2021	2	13/09/2021
	Manuales seguridad de la información	13/09/2021	2	15/09/2021
Fase Consultiva	Consultas personal experto de la BRILAT	15/09/2021	5	20/09/2021
	Consultas personal destinado en misión	20/09/2021	2	22/09/2021
	Consultas personal del Ministerio de Defensa	22/09/2021	2	24/09/2021
Fase Intermedia	Estudiar y analizar los tipos de VPN	22/09/2021	7	29/09/2021
	Estudio ventajas y desventajas	11/09/2021	15	26/09/2021
	Estudio protección del servidor VPN	29/09/2021	2	01/10/2021
	Estudiar y analizar la viabilidad del proyecto	01/10/2021	4	05/10/2021
Fase Creación	Creación del la Arquitectura de red VPN	05/10/2021	7	12/10/2021
	Creación servidor VPN	08/10/2021	7	15/10/2021
	Protección y mejora del servidor VPN	12/10/2021	7	19/10/2021
Fase Control	Lanzamiento del servidor	20/10/2021		20/10/2021
	Verificación del servidor	20/10/2021	3	23/10/2021
	Validación del servidor	23/10/2021	2	25/10/2021

Tabla 7. Fases del proyecto. Fuente: elaboración propia.

Con el Diagrama de Gantt de la Tabla 8, se aprecia de una forma visual el recorrido seguido en la implementación de dicho proyecto dentro de la Brigada, para facilitar las labores de mando y control.

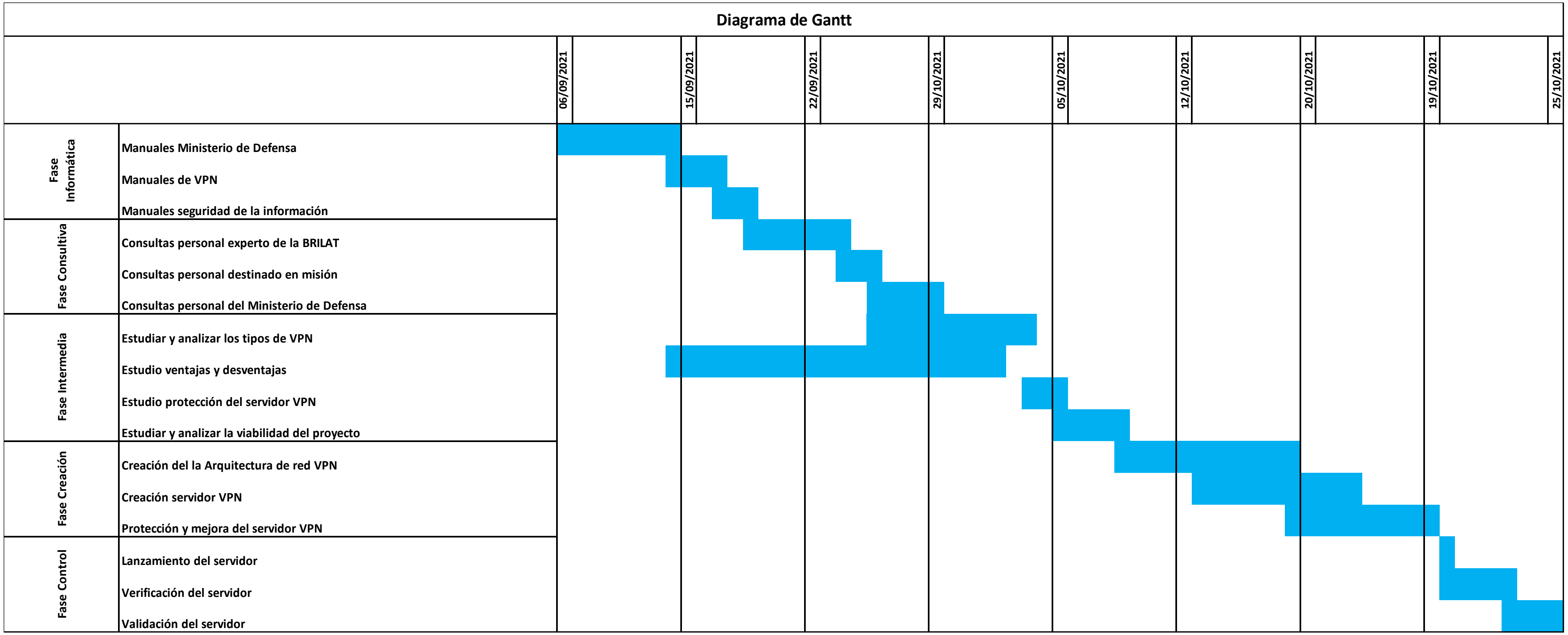

Tabla 8. Diagrama de Gantt. Fuente: elaboración propia.

5 VERIFICACIÓN Y VALIDACIÓN

Tras una búsqueda entre manuales y personal experto sobre la viabilidad del proyecto, se está comprobando los beneficios que provee la creación de VPN a las Unidades.

5.1 VERIFICACIÓN

Para la verificación del proyecto, se ha consultado la opinión de un experto por medio de una entrevista. En este caso a un Sargento 1º encuadrado en la Compañía de Transmisiones de la BRILAT con más de treinta años de experiencia. En este apartado se resumen los aspectos más importantes de la entrevista. La entrevista completa se encuentra en el Anexo II.

Desde el punto de vista de usuario cabe destacar la importancia de manejar una interfaz web que a nivel de aplicación sea sencilla y rápida ante cualquier tipo de adversidad en el que se requiera transmitir información de una manera segura y eficiente.

Se menciona también posicionarse en una situación ventajosa frente a posibles amenazas externas y nos permitiría un ancho de banda suficiente para trabajar a los usuarios. Así cómo la necesidad de crear una normativa común a todas las Unidades para la implementación de esta arquitectura de red para mayor operatividad del ET, necesitando para ello personal cualificado.

5.2 VALIDACIÓN

Para la validación del proyecto se ha consultado la opinión de un usuario por medio de una entrevista. En este caso a un Teniente destinado en la Compañía de Transmisiones de la Brigada Aragón I desde su primer destino y que actualmente se encuentra desplegado en una misión internaiconal. En este apartado se resumen los aspectos más relevantes de la entrevista. La entrevista se encuentra en el Anexo II.

De esta entrevista cabe destacar la importancia que remarca el usuario del uso de una VPN para una comunicación segura a través de una red pública como es internet, lo que aporta mayor rendimiento como por ejemplo un mayor ancho de banda acorde a las actuales del ET.

Es necesario el uso de este servicio de acceso remoto para el mando y control de las Unidades propias y del despliegue en el que se encuentre integrada la propia Brigada a través de un interfaz web de sencillo manejo para los usuarios. Ya que facilita el acceso a información relevante para cumplir el fin último de los objetivos de un militar como puede ser conocer las coordenadas geográficas de los compañeros, los vehículos de recuperación disponibles para salir de la Base o averiguar el HLZ más cercana dónde se encuentra el convoy si se produjesen posibles incidencias.

Al generar este tipo de red se ofrece también seguridad al traspaso de la información haciendo uso de algoritmos de cifra robustos capaces de defenderse de ataques en la red.

Se menciona en la entrevista el aprovechamiento de la estructura propia del territorio tanto nacional como fuera de las fronteras para no tener pérdidas de ninguna capacidad y así poder suplir las actuales en caso de fallo.

6 CONCLUSIONES

6.1 CONCLUSIONES

En los últimos tiempos la arquitectura de redes VPN se ha convertido en un factor crítico para cualquier organización. Cada vez se transmite más información de gran importancia a través de ellas. Es por este motivo por el cual deben cumplir unos atributos tales como el alcance geográfico o la fiabilidad sin olvidar en ningún momento la seguridad tanto de la información a transmitir como de todo lo que respecta a los usuarios de los propios equipos que exploten dicha arquitectura.

Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las organizaciones. Esto ha significado una gran ventaja para las mismas, sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia. Sin embargo, hay que destacar que estas redes remotas son objetivos para atacar los servidores y las redes para obtener información confidencial, conocido como los famosos *Firewalls* (Cortafuegos) y las RPV (Red Privada Virtual).

El objetivo principal de este trabajo ha sido analizar la viabilidad del empleo un servidor de acceso remoto VPN para el mando y control de una unidad operativa a nivel Brigada con el objetivo de facilitar la labor de las Unidades tanto desplegadas en zona de operaciones durante misiones internacionales como en territorio nacional para facilitar el acceso a información y servicios específicos.

Se ha comprobado que es posible la implementación de una VPN siguiendo la configuración desarrollada en el proyecto para todos los equipos que sean necesarios por medio de DMPVN. Dicho objetivo conseguido, demuestra ser un recurso que generaría un mayor rendimiento laboral ya que a nivel de mando llega a alcanzar los objetivos propuestos para la labor de seguimiento y control de las Unidades y a nivel usuario facilita la transmisión segura de información independientemente de la distancia a la que se encuentren.

Con el desarrollo del proyecto se ha verificado una arquitectura de red sencilla capaz de implementarse en los equipos del ET de una forma rápida y sencilla, lo que optimiza el rendimiento de la Unidad de forma íntegra a todos los niveles con la seguridad que proporciona la propia VPN. Por otra parte, se ha estudiado la necesidad de dotar a personal experto en la materia para configurar y mostrar el procedimiento al mayor número de Unidades posibles.

A modo de resumen se exponen los principales objetivos conseguidos en este trabajo:

Seguridad: Si el servidor de VPN lleva incorporado algoritmo de seguridad, la probabilidad de que existan vulnerabilidades que puedan ser explotadas por un atacante disminuye.

Escalabilidad: Se refiere a la capacidad de expandir la VPN para añadir más conexiones remotas, usuarios o equipos. La escalabilidad dependerá del equipo físico y sus características. No sería complicado aumentando los recursos de los equipos.

Rendimiento: La ejecución de las funciones VPN tiene un elevado consumo de recursos debido, principalmente, a las actividades de cifrado y descifrado de datos.

Capacidades de control: En el caso de utilizar dispositivos de la infraestructura, se pierden capacidades de control relacionadas con el equipo físico o el software de base.

Operación y mantenimiento: Se requieren actividades de mantenimiento. Hay que tener en cuenta los equipos que se añaden a la infraestructura hardware de la organización.

6.2 LÍNEAS FUTURAS

La proyección más evidente de este TFG está en el ámbito militar. En este apartado se presentan algunas líneas de investigación que pueden ser objeto de interés.

6.2.1 Propuesta primera: GESCOM cifrado a través de Internet

Investigar la posibilidad de un acceso seguro a GESCOM a través de Internet con una VPN.

Es el sistema de gestión seleccionado por el Ejército de Tierra Español para coordinar y administrar las Comunicaciones de Voz y Datos en entornos tácticos a nivel de Batallón, alcanzando también el nivel de Brigada.

GESCOMET es una solución táctica definida por Software y personalizada para Ejército de Tierra que incluye capacidades avanzadas para el encaminamiento de datos IP, telecontrol y gestión de la voz en las redes radio de combate. Ofrece integración de los medios en dotación de distintos fabricantes, herramientas avanzadas de priorización del tráfico, telecontrol de los principales equipos, servidor de Voz táctico e integración de Voz y Datos inteligente.

El sistema GESCOMET se integra con los principales servicios y aplicaciones desplegados por ET como por ejemplo BMS, TALOS o SIMACET, encaminando dinámicamente los flujos de datos y voz a través de los medios de radio y radioenlaces.

6.2.2 Propuesta segunda: Creación de burbujas LTE

El sistema LTE, (Long Term Evolution) es una tecnología de banda ancha inalámbrica que permite transmitir datos para el acceso a Internet desde los dispositivos móviles.

Dicho estándar de comunicaciones ofrece la posibilidad de crear una burbuja en las inmediaciones de los puestos de mando de la Brigada, que permite a los mandos el empleo eficaz de dispositivos móviles, ordenadores o tablets con el envío de información.

Con esta tecnología, se abre una nueva ventana en el mundo de los sistemas de información y telecomunicaciones de las Unidades del ET.

6.2.3 Propuesta tercera: Uso de VPN en los drones

Se plantea investigar sobre el uso de una VPN para ejecutar aplicaciones de vuelo de los drones asegurándose la protección de sus datos y el desbloqueo de restricciones geográficas.

7 REFERENCIAS BIBLIOGRÁFICAS

American Security Today, 2018. [En línea] Available at: https://americansecuritytoday.com/mapping-apps-are-endangering-special-operators-anger-us-troops/

Android Team Awareness Kit, 2020. [En línea] Available at: https://play.google.com/store/apps/details?id=com.atakmap.app.civ&hl=es&gl=US

CCN, 2021. [En línea] Available at: 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

Centro Criptológico Nacional, 2021. *Arquitecturas de Acceso Remoto Seguro.* [En línea] Available at: https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/boletines-pytec/335-pildorapytec-31ago2020-arquitecturas-de-acceso-remoto-seguro/file

Centro Criptológico Nacional, 2021. *Hash Code,* s.l.: s.n.

Cisco, 2017. *Cisco VPN S2S con Certificado,* s.l.: s.n.

Cisco, 2021. *Cisco.* [En línea] Available at: https://www.cisco.com/c/es_es/index.html?dtid=pseggl000183&oid=0&ccid=cc000870&_bk=cisco&_bt=512458719771&_bm=e&_bn=g&_bg=62533590844&gclid=Cj0KCQiA8vSOBhCkARIsAGdp6RSzs1bFNytlkza7SXb3bmXNdciA87Nc5U5taiYzEC_uvxStucX4Ub4aAkUqEALw_wcB&gclsrc=aw.ds

Janet Abbate, 2009. Internet: su evolución y sus desafíos. En: *Fronteras del conocimiento.* s.l.:s.n.

Jefatura del Estado, 2022. *Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.,* s.l.: s.n.

Militarpedia, 2016. *VPN Wikicis.* [En línea] Available at: http://wikicis/index.php?title=VPN_-_Red_Privada_Virtual

Ministerio de Defensa, 2004. *Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.,* s.l.: s.n.

Ministerio de Defensa, 2006. *Modelos de Arquitectura del Ministerio de Defensa,* s.l.: s.n.

Ministerio de Defensa, 2019. *Entrono Operativo 2035,* s.l.: s.n.

Ministerio de la Presidencia, 2010. *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.,* s.l.: s.n.

Ortín, J., 2020/2021. Tema 3: Nivel de enlace. En: *Redes y servicios de comunicaciones.* s.l.:s.n.

Val, J. S., 2021. Gestión de riesgos. En: *Oficina de Proyectos.* s.l.:s.n.

Varios, 2009. *Fronteras del conocimiento.* s.l.:s.n.

ANEXOS

Anexo I. Organigrama Unidad

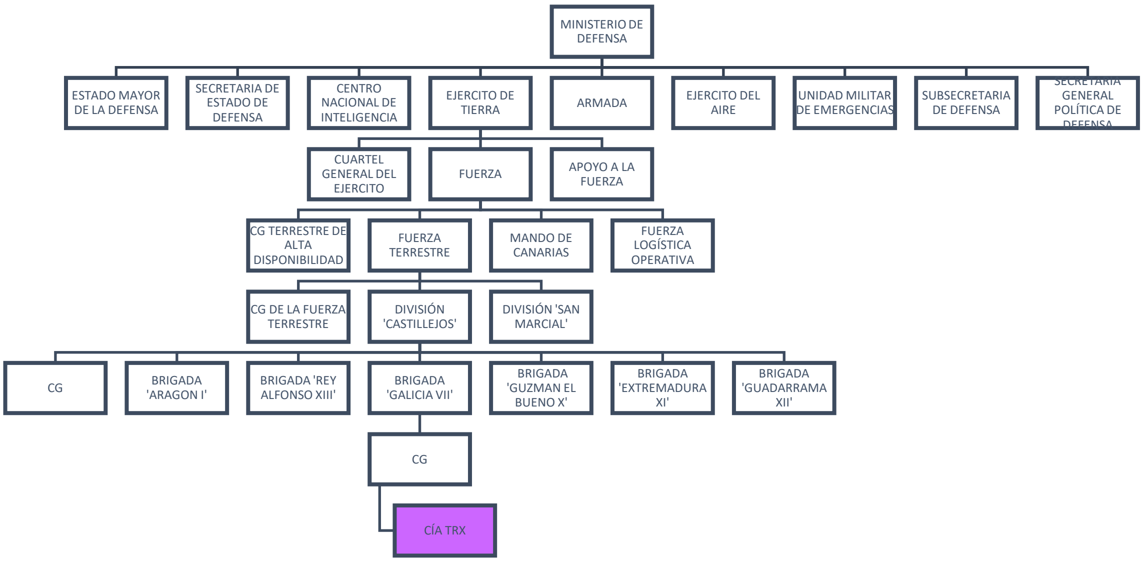

Figura 19. Organigrama BRILAT. Fuente: elaboración propia.

La Compañía de Transmisiones encuadrada dentro del cuartel General de la BRILTA (Figura 19), en la ejecución de su maniobra, facilita el mando y control al jefe de la gran unidad con los sistemas de telecomunicaciones e información. Es responsable de establecer y mantener los CIS para el mando y control de la brigada, ejecutando el planeamiento realizado por la sección G-6, y apoyando y reforzando el establecimiento y funcionamiento de los CIS de los escalones subordinados.

El sistema de telecomunicaciones se establece basándose en los medios tácticos propios de la compañía, pudiendo recibir apoyo en servicios de telecomunicaciones de otras redes, tanto civiles como militares.

Con el asesoramiento del G-6, se decide las redes a establecer de acuerdo con la maniobra, la situación táctica y el personal y medios disponibles.

Las telecomunicaciones en la brigada están basadas en la red radio de combate (RRC) y se complementan con radioenlaces y terminales satélite. Los medios principales son utilizados para soportar el flujo de información de mando y control de las operaciones (voz, SIMENFAS, BMS (Battlefield Management System. Sistema de gestión del campo de batalla para PU)/FFT (Friend Force Tracking. Sistema de seguimiento de fuerzas propias), TALOS (Sistema de mando y control de apoyos de fuego), TDL (Datalink Terminal. Terminal de enlace de datos) 11/11B/16/JRE, imágenes fijas y vídeo de calidad media, navegación web, etc.), mientras que los complementarios servirán de soporte a aquellos servicios que requieran mayor ancho de banda o se usen para el apoyo a las operaciones (SIMACET, SIM, vídeo de alta calidad, SIGLE, SIPERDEF, etc.). Se dispone también de estaciones satélite en movimiento para el apoyo al PCMOV o a las pequeñas unidades (PU) de combate o de apoyo al combate.

Los puestos de mando de brigada establecerán sus redes de área local mediante acceso inalámbrico (WIFI: *Wireless High Fidelity)* seguro (hasta RESERVADO NACIONAL), aunque también disponen de medios para desplegar una red alámbrica (preferiblemente fibra óptica) en situaciones estáticas.

Anexo II. Entrevista personal experto

En el presente anexo se transcriben las diferentes entrevistas que se han realizado al personal perteneciente al ET. Las preguntas se realizaron con preguntas abiertas que cada uno de los entrevistados respondió desde su experiencia propia, ya sea de misión o durante el desarrollo de las maniobras. La identidad de los entrevistados no se muestra, pero sí su empleo.

ENTREVISTA PRIMERA

Empleo: Teniente desplegado en misión

Unidad: Brigada Aragón I (Jefe de Sección del Arma de Transmisiones)

SOBRE LA IMPLEMENTACIÓN:

1. Desde su experiencia en misión. ¿Qué ventajas presenta implementar un servidor VPN para el sistema de mando y control?

Permite una comunicación segura a través de un medio no seguro. Lo que aporta un ancho de banda acorde a las necesidades que tenemos hoy en día. Cabe destacar también la capacidad de transmitir voz y datos en cualquier área de la zona de operaciones y en cualquier momento.

2. ¿Podría explicar los motivos por los que se escogió este tipo de conexión de red?

Para que el puesto de mando tuviese la opción de controlar las patrullas tanto propias como del resto de Unidades del despliegue, se nos ocurrió crear una red interna a través de internet. Dentro de esta red propia se creó un servidor dinámico a través del interfaz web para la conexión de múltiples usuarios.

SOBRE LOS SERVICIOS:

3. ¿Qué es lo más importante que aporta un servidor VPN?

La creación de una red interna que funciona a través de la red móvil local. Es decir, una conexión punto a punto a través de interfaces virtuales.

4. ¿Cuáles son los servicios a los que podría dar acceso remoto de forma segura (BMS, VTC, etc.)?

En el momento que se genera una red de VPN, con la presencia de un servidor de certificados de seguridad, se puede ofrecer toda la seguridad posible a las Unidades.

Todo el mundo habla con todo el mundo. En el momento que se conecta a la VPN consigue la interoperabilidad entre todos los usuarios pertenecientes a la misma red interna. Consiguen verse entre ellos, poder mandar fotos y dialogar.

5. ¿Cuál es el algoritmo que se está utilizando?

La interfaz web que estamos usando nosotros tiene un algoritmo de cifra AES-256, uno de los algoritmos de cifra más robustos que existen en el mundo. Un algoritmo que es usado incluso por los Gobiernos. Teniendo capacidad de añadir cualquier certificado SSL, TLS…

6. ¿Los usuarios siguen unos protocolos de seguridad determinados?, ¿cuáles?

Los protocolos de seguridad que tenemos establecidos, es que el propio usuario para poder registrarse tiene que estar en presencia del Jefe de Unidad. La aplicación provee un código que permite ser controlado por el usuario que crea la red para permitir o no su acceso a la misma.

Una vez que tengo la comprobación visual en mi interfaz de su código y coincide, el Jefe de Unidad le da la autentificación.

SOBRE LOS USUARIOS:

7. Aptitudes y conocimiento necesario para el uso de este servidor por parte de los usuarios.

Es un sistema muy sencillo, no requiere de especificación técnica a nivel aplicación. A nivel enlace sería necesario un experto en la materia que diseñe e implemente la arquitectura de red.

SOBRE LA FINALIDAD:

8. ¿Cómo valora usted la importancia de implementar el servidor para el éxito de la misión?

Este sistema responde a unas necesidades, lo que aporta capacidad de enlace de los medios actuales del ET como pueden ser *tablets* a través de un único punto de acceso a la red.

Ahora mismo, valoraría el servidor muy positivamente por permitir hacer uso de una aplicación con una capacidad de mando y control operativa además de permitir la obtención de las coordenadas geográficas de los usuarios, los vehículos de recuperación disponibles para salir de la Base, averiguar un HLZ cercana dónde está el convoy por posibles incidencias. A parte de mandar imágenes, mensajes de información para facilitar las 5 líneas entre que se corta y el entendimiento.

9. ¿Qué beneficios le aportó profesionalmente este sistema para escogerlo?

Hay que intentar aprovechar la estructura propia del país. Porque si no, en el momento que tengas un medio de comunicación inoperativo por escaso ancho de banda, provoca la pérdida de unas capacidades innecesarias.

ENTREVISTA SEGUNDA

Empleo: Sargento 1º

Unidad: BRILAT

1. Desde su experiencia como posible futuro usuario del servidor VPN ¿Cree usted necesaria su implementación?

Desde el punto de vista de usuario, tunelizar una red pública para asegurar un mayor rendimiento en el traspaso de nuestra información sin perder nuestra seguridad es positivo.

Por otra parte, nos posicionaría en una situación ventajosa frente a posibles amenazas externas y nos permitiría un ancho de banda suficiente para trabajar a los usuarios.

En definitiva, es una solución de ciberseguridad muy avanzada que aporta la máxima protección contra cualquier ataque a las Unidades del ET.

2. ¿Qué desventajas cree que presentaría la implementación del servidor?

Supongo que sería necesario hacer una normativa a nivel Ministerio de Defensa para normalizar la implementación de esta red. Otro aspecto a tener en cuenta sería la posibilidad de crear una red de forma errónea por medio de la cual sufrir ciberataques. Por ello, es necesario la especialización del personal y eso requiere tiempo.

3. ¿Haría uso de este servicio?

El servicio de VPN presenta una sencilla implementación que aporta fácil manejo a la hora de teletrabajar desde mi casa hasta en misión, sin depender de elementos externos que no sea capaz de controlar el ET, diseñándolo exclusivamente para dar sus propios servicios.

Anexo III. Arquitectura Internet

La arquitectura de Internet constaba de dos elementos principales. El primero era un conjunto de protocolos llamado TCP/IP (siglas de Transmision Control Protocol, Protocolo de control de transmisiones y de Internet Protocol, Protocolo para Internet, respectivamente) (Cerf y Kahn 1974).

El TCP tenía como función establecer y mantener la conexión entre dos ordenadores dentro de una red, garantizando una conexión fiable reduciendo los requerimientos de fiabilidad de la red. El uso del protocolo TCP abrió Internet a muchas más redes.

Por otro lado, el Internet Protocol permitía a los paquetes pasar de una máquina a otra conforme circulaban por la red. IP se convirtió en el lenguaje común de Internet.

El segundo elemento creativo fue el uso de ordenadores especiales llamados puertas de acceso o gateways a modo de interfaz entre redes diferentes (Cerf 1979). En la actualidad se conocen como router y, tal y como su nombre indica, su función es determinar la ruta que los paquetes deben seguir para pasar de una red a otra. Una red dirige paquetes no locales a una puerta de acceso cercana, la cual a su vez los envía a su red de destino. Al repartir la tarea de enrutamiento entre distintas redes y gateways, esta arquitectura hacía más fácil el crecimiento de Internet: las redes individuales ya no necesitaban conocer la topología de toda la red, tan sólo saber cómo llegar a la puerta de acceso más cercana; a su vez, las puertas de acceso no precisaban ser capaces de llegar a todas las redes dentro de Internet, únicamente a los anfitriones individuales dentro de una red.

Otro invento notable que contribuyó a hacer más manejable el crecimiento a escala global de Internet fue el Sistema de nombres por dominio o Domain Name System, creado en 1985 por Paul Mockapetris (Cerf 993; Leiner et al. 1997). Los ordenadores que forman parte de la red se identifican unos a otros mediante direcciones numéricas. En la ARPANET originaria, los nombres y direcciones de todos los ordenadores se guardaban en un gran archivo que tenía que ser constantemente actualizado y distribuido a todos los anfitriones. Claramente este mecanismo no estaba a la altura de una red de miles e incluso millones de ordenadores. El Sistema de nombres por dominio descentralizó la tarea de localizar direcciones creando grupos de nombres conocidos como dominios (tales como .com o .org) y ordenadores especiales llamados servidores de nombres, encargados de mantener bases de datos con las direcciones correspondientes a cada nombre de dominio. Para encontrar una dirección el anfitrión únicamente debía introducir sus términos de búsqueda en el servidor apropiado. El nuevo sistema también permitía descentralizar la autoridad para asignar nombres de manera que, por ejemplo, cada país pudiera controlar su propio dominio.

Anexo IV. Protocolo de red encapsulador

Una red es un conjunto de dispositivos conectados entre sí (ver Figura 20) y formada por equipos terminales (equipos de usuario o host), por dispositivos de conmutación (nodos intermedios) y por los enlaces de comunicación. El equipo terminal o host es el dispositivo de usuario conectado a la red, el dispositivo de conmutación es el encargado de reenviar los mensajes que le llegan por un enlace a otros dispositivos de conmutación. Por último, el enlace de comunicación une los dispositivos de usuarios con los de conmutación entre sí.

Las funciones necesarias para la comunicación de organizan en capas o niveles, cada nivel realiza un subconjunto de funciones y se definen los siguientes conceptos:

Servicio: capacidad que un nivel ofrece al nivel inmediatamente superior.

Protocolo: Conjunto de reglas que gobiernan el intercambio de datos entre dos entidades de un mismo nivel para ofrecer al nivel superior sus servicios.

Las reglas que fija un protocolo pueden referirse al formato de los mensajes intercambiados, a su orden como a las acciones a tomar ante la recepción de estos.

El PDU (Protocol Data Unit) es el protocolo a seguir entre bloques de información que se intercambian dentro del mismo nivel en máquinas distintas.

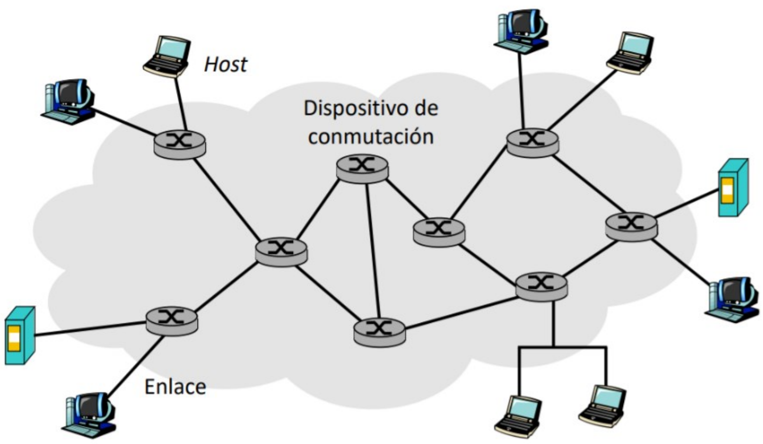

Figura 20. Protocolo de red encapsulador. Fuente: Ortín.

Anexo V. Requisitos nodo extranet

Se establecen los siguientes requerimientos para el funcionamiento del Nodo Extranet del Ministerio de Defensa:

Identificación y Autenticación.

Los procedimientos de acceso a los servicios del Nodo Extranet de todos los usuarios contarán con mecanismos de autenticación fuerte, basados en certificados emitidos por la PKI del Ministerio de Defensa (cuando esté disponible).

Cifrado de las Comunicaciones.

Las comunicaciones entre el Nodo Extranet y sus interlocutores externos deberán ir cifradas, con los mecanismos apropiados, para cumplir con la Política de Seguridad de las Tecnologías de la Información y las Normas de Protección de la Información Clasificada del Centro Criptológico Nacional del Centro Nacional de Inteligencia (CCN/CNI).

Auditoría y Trazabilidad.

Para permitir las necesarias labores de auditoría y trazabilidad, los mecanismos de cifrado se implementarán por defecto entre el punto de entrada exterior al Nodo Extranet y sus respectivos interlocutores, permitiendo el manejo de la información "en claro" dentro de dicho Nodo.

Prevención/Detección de Intrusiones.

Al estar directamente conectado a Internet, es importante disponer de un sistema de detección y/o prevención de intrusiones para evitar posibles ataques al sistema en el Nodo Extranet.

Disponibilidad.

Para garantizar la disponibilidad del servicio es necesario que los dispositivos de red y de servicios del Nodo Extranet tengan la característica de tolerancia a fallos, de forma que si ocurriera cualquier anomalía en algún dispositivo existiera otro que asumiera la prestación del servicio sin que el mismo se viera afectado.

Nodo de Respaldo.

Para garantizar la adecuada protección de la disponibilidad de las conexiones externas del Ministerio de Defensa se deberá contar con una infraestructura de respaldo. Dicha infraestructura de respaldo ha de estar estructurada y dimensionada adecuadamente para soportar la transferencia parcial o total de los servicios del Nodo Principal, e integrada en el Centro de Respaldo de los servicios generales del CCEA. Para minimizar los riesgos asociados, la ubicación física de este Centro de Respaldo será distinta de la del Nodo Principal a una distancia segura.

Líneas de Comunicaciones.

Este Nodo de Interconexión necesita una serie de líneas de comunicaciones que provea el acceso al mismo. Dichas líneas de comunicaciones facilitarán el acceso punto a punto con terceros, el acceso a Internet y el acceso PSTN (Public Switched Telephone Network).

Para la conexión a Internet tendrá garantizado un caudal de acceso suficiente para satisfacer los múltiples accesos a los servicios del Nodo Extranet.

En el nodo principal deberá existir una línea principal y otra de respaldo para poder garantizar dicha conexión.

Anexo VI. Procedimiento implementación

Una vez realizada la implantación del dispositivo VPN SSL los usuarios de acceso remoto podrán acceder desde un puesto conectado a Internet de la siguiente manera:

-El usuario establecerá, por sus medios, una sesión a Internet mediante un proveedor de Internet (ISP).

-El usuario abrirá el navegador Web y escribirá la dirección del “gateway” SSL VPN estableciendo una conexión segura, autenticando con certificado de cliente proporcionado por la PKI del Ministerio de Defensa, o en su defecto, el tipo de autenticación que establezcan los condicionantes de seguridad.

-Cabe destacar que, en caso de que el dispositivo de acceso no cumpla con los requisitos de seguridad (Sistema Operativo y versión, actualizaciones de seguridad, software de antivirus, etc.), éste será redireccionado a una “red en cuarentena” hasta que dicha situación sea remediada.

-Como esta solución permite establecer conexiones SSL VPN con la intranet sin la necesidad de tener que instalar en el puesto del usuario ningún cliente especial, el usuario remoto, en función de sus permisos y tipo de acceso, podrá:

- Conectar a servidores Web de la Intranet de la WAN PG a los que esté autorizado utilizando el portal de acceso Web del gateway VPN SSL.

- Conectar a servidores internos mediante aplicaciones pesadas (Ej: Lotus Notes) que utilizan un cliente Java desde la interfaz Web del gateway, permitiendo al usuario trabajar en remoto como si lo hiciera desde la propia WAN PG.

- Conectar a servidores internos (Ej.: máquinas UNIX, host, servidores Terminal Server o servidores de ficheros) sin necesidad de tener ningún cliente pesado instalado en su equipo.

Anexo VII. Algoritmos matemáticos

Clave simétrica.

Es cuando un algoritmo de cifrado, utiliza la misma clave tanto para cifrar como descifrar. La transferencia entre dos equipos exige, que ambos hayan acordado mediante un medio seguro, una clave simétrica común.

Usados por IOS: DES(56), 3DES(168), AES(128, 192 ó 256).

Mecanismo de un solo sentido (one-way hash).

Es un algoritmo público, que se utiliza para producir una “digestión”, que consiste en una “firma” no descifrable. No sirve, por tanto, para enviar información cifrada, sino como “checksum” de la información que acompaña.

- Propiedades: El hash resultante varía al modificar el texto de entrada, aunque sea sólo un byte (dispersión). Existen “colisiones”, textos completamente distintos que producen la misma firma.

- La longitud de la firma es una constante del método matemático, independiente de la longitud del texto al que se aplica el cálculo de hash.

- El equipo receptor compara este “hash” recibido con el que calcula él mismo (no necesita clave). Rechazará el paquete si no son iguales.

Usados por IOS: MD5(longitud de hash 128), SHA-1(longitud de hash 160).

Clave asimétrica.

Consiste en un algoritmo que a partir de una “semilla”, genera un auténtico número aleatorio. Con este número aleatorio, se genera a continuación una pareja de claves que tienen la propiedad de poder usarse para descifrar la información que haya sido cifrada con la otra. Pero, en cambio, no pueden usarse para descifrar la información que haya sido cifrada por ellas mismas.

- La segunda clave se transmite en texto claro a los equipos compañeros y se denomina “clave pública”.

- La primera clave no se transmite bajo ningún concepto, y se almacena en el equipo de modo que no pueda ser leída ni por el administrador. Se denomina “clave privada”.

- No se puede deducir una clave a partir de la otra.

- Para enviar información en modo seguro, utilizaremos la clave pública del equipo destinatario.

- Los otros equipos para mandarnos información en modo seguro, utilizarán para cifrar la clave pública.

- Excepción a estas reglas: Para demostrar a un destinatario que nosotros somos el generador de la clave pública que posee, le enviaremos un mensaje cifrado con la clave privada.

Usados por IOS: RSA con diferentes módulos de generación: 512, 768, 1024, ...

Firma digital.

Consiste en enviar información a un destinatario, de modo que este pueda comprobar dos cosas: que el propio usuario certifique ser el generador de la información y que ésta no ha sido modificada durante el tránsito.

También consiste en calcular el “hash” de la información a enviar, y cifrarlo con la clave privada. El resultado se añadirá a la información a enviar.

El receptor descifrará el hash con la clave pública y la comparará con el “hash” que calcule él mismo a partir de la información recibida. Rechazará el paquete si no son iguales.

La información se puede enviar cifrada o no, con una clave simétrica. Si se hiciera, el destinatario debe conocer esa clave simétrica para poder descifrarla y acceder a la información y calcular posteriormente su “hash”.

Acuerdo de Diffie-Helman.

Consiste en generar en dos equipos la misma clave simétrica a partir de intercambiar información en texto claro. En cambio, los equipos que “escuchen” estos mensajes no podrán hacerlo.

Se comienza intercambiando números primos grandes para factorizarlos. Cada uno genera una clave privada. Pero para generar la clave pública se utiliza un algoritmo en el que intervienen los números intercambiados previamente además de la clave privada local.

Las claves públicas se transmiten al otro equipo, pero no son independientes entre sí debido al modo en que han sido generadas. La propiedad que tienen es que cada equipo puede generar, por separado, la misma clave simétrica a partir de su privada y la pública del otro.

Anexo VIII. Boletín de concienciación

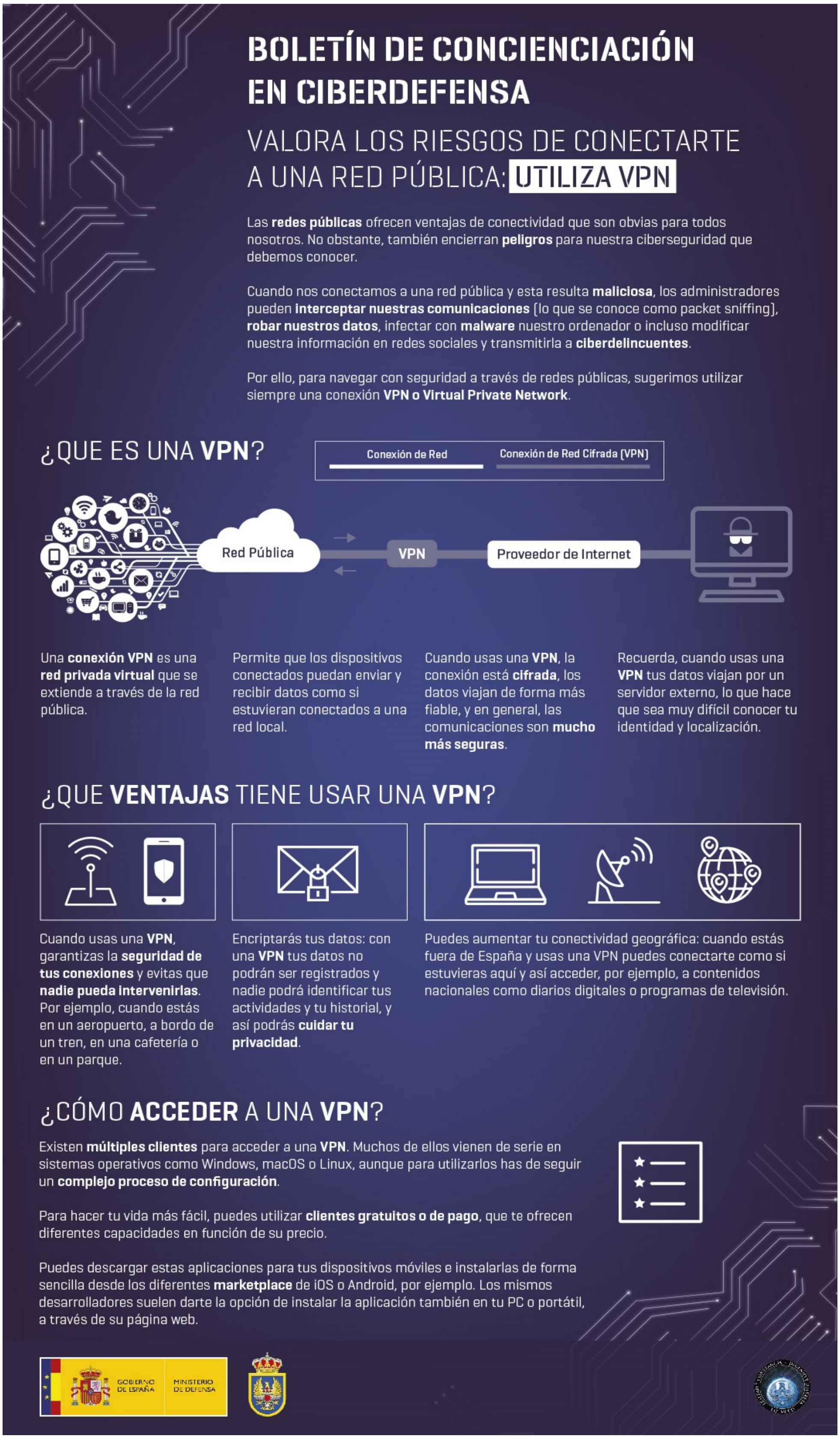

Figura 21. Boletín de concienciación en ciberdefensa. Fuente: Ministerio de Defensa.

Anexo IX. BMS

El Battlefield Management System surge como una evolución de los sistemas C2IS a los Sistemas de Información para Mando, Control y Comunicaciones (Command, Control & Communication Information System (C3IS)) dentro del Plan de Modernización de los Sistemas de Mando, Control y Comunicaciones del ET (MC3) (Ejército de Tierra, "Plan MC3 'Plan de modernización de los Sistemas de Mando, Control y Comunicaciones del Ejército de Tierra'" 2015). Un plan por el cual el Jefe del Estado Mayor de la Defensa (JEMAD) pretende alcanzar la superioridad en la adquisición, tratamiento, distribución y empleo de la información, reduciendo los plazos de tiempo en la toma de decisiones y permitiendo el flujo de la información en tiempo útil entre puestos de mando, unidades, sensores y sistemas de armas.

La configuración del BMS, se establece a partir de una serie de servidores, redes y nodos (nombre que recibe cada terminal de red). Los nodos permiten el acceso al sistema por parte de los usuarios, cada uno con un puesto definido dentro del despliegue de su unidad. Estos puestos vienen definidos en los conocidos como "Ficheros de misión" donde se digitaliza el espacio de batalla antes de cada operación. (Ejército de Tierra, Manual de Administración BMS-ET (MT-022). 2019)

Anexo X. Estructuras y encapsulamiento de paquetes IPSec

- Modo Túnel. Hay dos cabeceras IP: La exterior sin cifrar, cuyas direcciones IP son las de los extremos del túnel. Otra interior, (en la parte cifrada), con las direcciones IP de los equipos que transmiten a través del túnel.

- Modo Transporte. Sólo hay una cabecera IP, sin cifrar y con las direcciones IP de los equipos que transmiten a través del túnel. La parte cifrada contiene el paquete del usuario a partir de la capa de transporte.

- AH. Consiste en una cabecera adicional que se inserta tras la “cabecera IP exterior”, y el resto del paquete que no está cifrado. Aporta integridad y autentificación, pero no confidencialidad.

- ESP. Consiste en una estructura que se coloca detrás de la “cabecera exterior”, que incluye la información de usuario cifrada. Aporta integridad, autentificación y confidencialidad.

- AH + ESP. Si se quieren utilizar ambas, (aporta redundancia en autentificación y confidencialidad). Se ha de colocar la cabecera AH primero. La firma digital de AH cubre los campos fijos de la cabecera IP exterior. La firma digital de ESP cubre la información de usuario.

Anexo XI. Plantilla IKE

PLANTILLA IKE phase 1

- La plantilla consiste en una combinación concreta de algoritmos a utilizar.

. Método de encriptación. (DES, 3DES, AES-192, AES-256, ...)

. Módulo del acuerdo de Diffie-Helmann. (512, 768, 1024, ...)

. Uso o no, de la cabecera AH. (AH con md5 / AH con sha-1 / AH con sha-2) . Uso o no, de la estructura ESP. (ESP con md5 / ESP con sha-1 / ESP con sha-2) y además (ESP null / ESP des / ESP 3des / ESP aes-192 / ESP aes-256)

. Método de autentificación (pre-shared / certificados digitales de una misma entidad / Intercambio de claves públicas)

. Tiempo de vida del túnel. Se elige el valor en segundos menor propuesto por ambos extremos.

PLANTILLA IKE pase 2

. Método de encriptación. (DES, 3DES, AES-192, AES-256, ...)

. Módulo del acuerdo de Diffie-Helmann. (512, 768, 1024, ...) . Uso o no, de la cabecera AH. (AH con md5 / AH con sha-1 / AH con sha-2)

. Uso o no, de la estructura ESP. (ESP con md5 / ESP con sha-1 / ESP con sha-2) y además (ESP null / ESP des / ESP 3des / ESP aes-192 /ESP aes-256)

. Modo túnel o transporte.

. Tiempo de vida del túnel. Se elige el valor menor propuesto por ambos extremos, y puede ser segundos o datos transmitidos.

Anexo XII. Configuración inicial routers

Configuración del Router "Internet", switch de L3

Hostname SW-Central- Internet

Ip routing

Interface vlan 210

ip address 200.1.10.2 255.255.255.0

Interface vlan 211

ip address 200.1.1.2 255.255.255.0

Interface vlan 212

ip address 200.1.2.2 255.255.255.0

Interface vlan 213

ip address 200.1.3.2 255.255.255.0

Configuración del Router Central, "HUB-Router"

Hostname HUB-Central

interface Loopback0

ip address 172.16.10.1 255.255.255.0

!!interface GigabitEthernet0/0

ip address 200.1.10.1 255.255.255.0

no shutdown

!i

p route 200.1.1.0 255.255.255.0 200.1.10.2

ip route 200.1.2.0 255.255.255.0 200.1.10.2

ip route 200.1.3.0 255.255.255.0 200.1.10.2

Configuración del Router "Spoke-1"

Hostname Branch-1

interface Loopback0

ip address 172.16.1.1 255.255.255.0

!!interface GigabitEthernet0/1

ip address 200.1.1.1 255.255.255.0

no shutdown

!i

p route 200.1.10.0 255.255.255.0 200.1.1.2

ip route 200.1.2.0 255.255.255.0 200.1.1.2

ip route 200.1.3.0 255.255.255.0 200.1.1.2

Configuración del Router "Spoke-2"

Hostname Branch-2

interface Loopback0

ip address 172.16.2.1 255.255.255.0

!!interface GigabitEthernet0/1

ip address 200.1.2.1 255.255.255.0

no shutdown

!i

p route 200.1.10.0 255.255.255.0 200.1.2.2

ip route 200.1.1.0 255.255.255.0 200.1.2.2

ip route 200.1.3.0 255.255.255.0 200.1.2.2

Configuración del Router “Spoke-3”

Hostname Branch-3

interface Loopback0

ip address 172.16.3.1 255.255.255.0

!!interface GigabitEthernet0/1

ip address 200.1.3.1 255.255.255.0

no shutdown

!i

p route 200.1.10.0 255.255.255.0 200.1.3.2

ip route 200.1.1.0 255.255.255.0 200.1.3.2

ip route 200.1.2.0 255.255.255.0 200.1.3.2

Anexo XIII. Configuración túneles GRE

Configuración del Router Central, “HUB-Router”

interface Tunnel0

ip address 10.1.1.1 255.255.255.0

tunnel source 200.1.10.1

tunnel mode gre multipoint

Configuración del Router “Spoke-1”

interface Tunnel0

ip address 10.1.1.2 255.255.255.0

tunnel source 200.1.1.1

tunnel mode gre multipoint

Configuración del Router “Spoke-2”

interface Tunnel0

ip address 10.1.1.3 255.255.255.0

tunnel source 200.1.2.1

tunnel mode gre multipoint

Configuración del Router “Spoke-3”

interface Tunnel0

ip address 10.1.1.4 255.255.255.0

tunnel source 200.1.3.1

tunnel mode gre multipoint

Anexo XIV. Configuración de NHRP

Configuración del Router "Spoke-1"

interface Tunnel0

ip nhrp map 10.1.1.1 200.1.10.1

ip nhrp map multicast 200.1.10.1

ip nhrp network-id 1

ip nhrp nhs 10.1.1.1

ip mtu 1416

Configuración del Router "Spoke-2"

interface Tunnel0

ip nhrp map 10.1.1.1 200.1.10.1

ip nhrp map multicast 200.1.10.1

ip nhrp network-id 1

ip nhrp nhs 10.1.1.1

ip mtu 1416

Configuración del Router "Spoke-3"

interface Tunnel0

ip nhrp map 10.1.1.1 200.1.10.1

ip nhrp map multicast 200.1.10.1

ip nhrp network-id 1

ip nhrp nhs 10.1.1.1

ip mtu 1416

Configuración del Router Central, "HUB-Router"

interface Tunnel0

ip nhrp map multicast dynamic

ip nhrp network-id 1

ip mtu 1416

! ip nhrp holdtime 300

! ip nhrp redirect

Anexo XV. Configuración IKE

Configuración del Router Central, "HUB-Router"

!

crypto isakmp policy 1

encr aes

authentication pre-share

group 5

crypto isakmp key 6 CISCO address 0.0.0.0

!

crypto ipsec transform-set DMVPN_trans esp-aes 192

mode transport

!

crypto ipsec profile DMVPN_profile

set transform-set DMVPN_trans

!i

nterface Tunnel0

tunnel protection ipsec profile DMVPN_profile

Configuración del Router Branch-1, "Spoke-1"

!

crypto isakmp policy 1

encr aes

authentication pre-share

group 5

crypto isakmp key 6 CISCO address 0.0.0.0

!

crypto ipsec transform-set DMVPN_trans esp-aes 192

mode transport

!

crypto ipsec profile DMVPN_profile

set transform-set DMVPN_trans

!i

nterface Tunnel0

tunnel protection ipsec profile DMVPN_profile

Configuración del Router Branch-2, "Spoke-2"

!

crypto isakmp policy 1

encr aes

authentication pre-share

group 5

crypto isakmp key 6 CISCO address 0.0.0.0

!

crypto ipsec transform-set DMVPN_trans esp-aes 192

mode transport

!

crypto ipsec profile DMVPN_profile

set transform-set DMVPN_trans

!i

nterface Tunnel0

tunnel protection ipsec profile DMVPN_profile

<u>Configuración del Router Branch-3, “Spoke-3”</u>

!

crypto isakmp policy 1

encr aes

authentication pre-share

group 5

crypto isakmp key 6 CISCO address 0.0.0.0

!

crypto ipsec transform-set DMVPN_trans esp-aes 192

mode transport

!

crypto ipsec profile DMVPN_profile

set transform-set DMVPN_trans

!i

nterface Tunnel0

tunnel protection ipsec profile DMVPN_profile