Estudio de comunicaciones seguras en redes de área amplia (WAN) privadas y críticas evolucionadas con SD-WAN

Autor: Apellidos, Nombre

Directores: Carlos Zamorano Pinal y José María Núñez Ortuño.

Contacto: smarga1978@gmail.com

Resumen: Este estudio se centra en las infraestructuras de telecomunicaciones (ITs) privadas tradicionales con las características de ser críticas e implementar comunicaciones seguras.

Una posibilidad de mejora de estas infraestructuras es aplicar el concepto de Redes Definidas por Software (SDN), que tiene su aplicación en las redes de área amplia (WAN) tradicionales con la tecnología de redes WAN definidas por software (SDWAN).

Con la finalidad de sacar conclusiones concretas en el estudio, se aplica una solución de SDWAN a la infraestructura de telecomunicaciones descrita en la Arquitectura Global CIS/TIC del Ministerio de Defensa (AG CIS/TIC) [1], que se caracteriza por unificar dos WAN en una única, por implementar comunicaciones seguras, y por ser una infraestructura de telecomunicaciones privada y crítica.

Palabras clave: Infraestructura de telecomunicaciones, privada, crítica, seguridad, SD-WAN

---

1. Introducción

El estudio sigue la definición de comunicaciones seguras de la recomendación X.1205 de la UIT, que define que son aquellas tienen por finalidad “garantizar la confidencialidad, la integridad y la exactitud de las comunicaciones de red” [1]. Con ese objeto se han de emplear técnicas de encriptación para el tráfico de la organización mediante técnicas VPN en la WAN (en el alcance del trabajo se consideran IPSec y MACsec). Se considera además que en la relación de confianza entre la organización y los operadores de telecomunicaciones la VPN es implementada y operada por la organización.

Las soluciones SD-WAN desarrolladas por los fabricantes se basan en soluciones con tunelización IPSec. El carácter complementario de MACsec e IPsec requieren de un estudio particularizado para cada organización, que depende de la WAN y redes de transporte que compongan la infraestructura.

En este estudio se va a analizar la implantación de SDWAN en infraestructuras de telecomunicaciones:

- Privadas, que proporcionan conectividad entre las sedes de la organización y con el exterior de la organización. Se establece que la organización implementa VPNs en propiedad, no contratadas al operador de telecomunicaciones, entre todas las sedes de la organización.
- Críticas, con requerimientos de mantener confidencialidad, integridad y disponibilidad, según el nivel de clasificación del tráfico de la organización. Se incluye en el estudio la disponibilidad de la conectividad entre sedes y la garantía del tráfico.

Dado que el SDWAN requiere de un estudio particularizado en cada organización, se aplicará el estudio a la Infraestructura de Telecomunicaciones del Ministerio de Defensa, definida en la Arquitectura Global del Ministerio de Defensa [2], por contar con una red de área amplia, por ser un caso claro de organización que tiene una infraestructura privada y crítica, con necesidad de comunicaciones seguras, y a la que se podría aplicar el SDWAN.

La arquitectura de red de la AG CIS/TIC es comparable a la arquitectura genérica de WAN mostrada en la figura 1-1. El Ministerio de Defensa define a sus sedes o "branches" como Nodos Permanentes o Desplegables, en función de las características de transmisión debidas a las operaciones militares.

Además, se dispone de un CPD de Defensa, como sede central de la organización, y cuenta con la defensa perimetral que da conectividad al Ministerio con internet, aunque en el caso del Ministerio de Defensa se amplía la interconexión a redes de naciones u organizaciones aliadas, el Nodo de Interconexión Clase II, o con redes desplegables, el Nodo de Interconexión Clase I

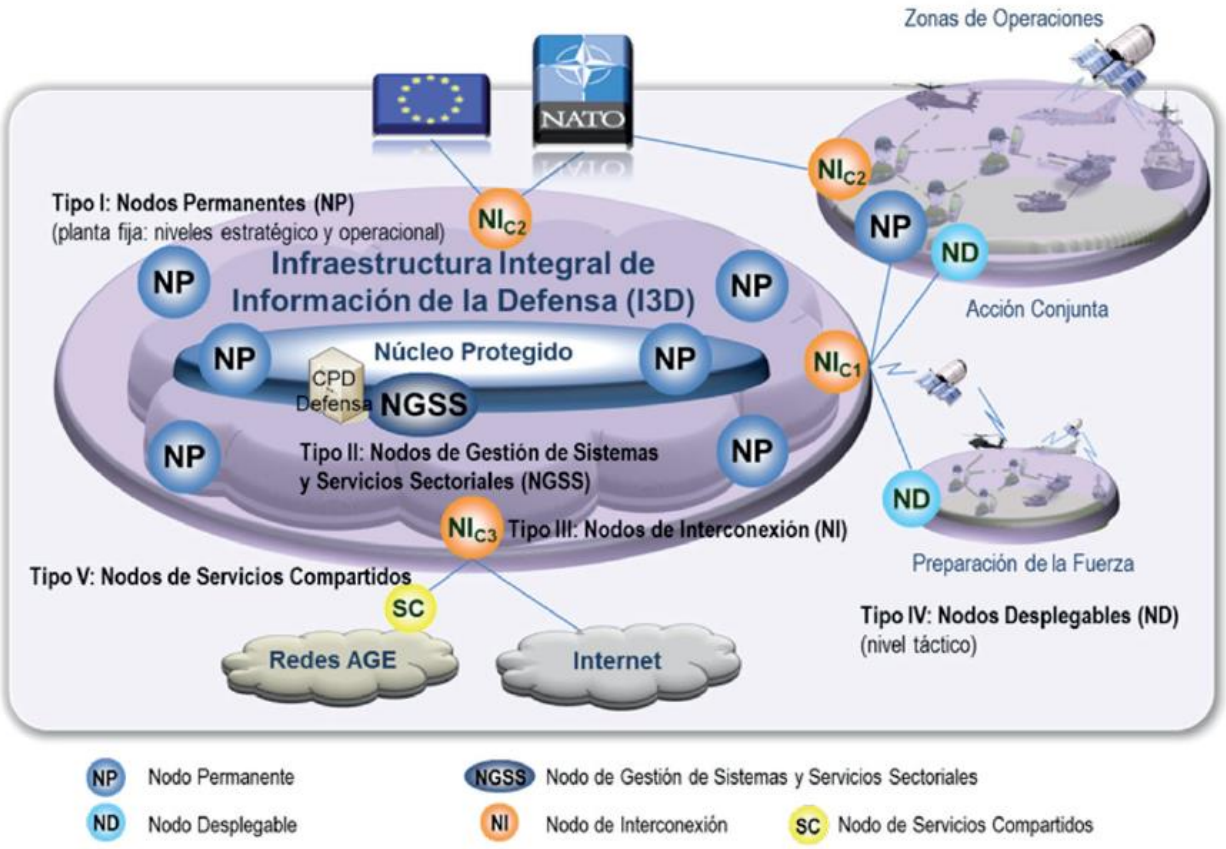

Figura 0-1 Arquitectura de red de área amplia del Ministerio de Defensa [2]

2. Desarrollo

En el año 2015 el Ministerio de Defensa inicia la evolución de las Redes de Área Amplia de Propósito General (WAN PG) y de Mando y Control (WAN C2), a una Red de Área Amplia única a la que denomina Infraestructura Integral de Información (I3D) de la Defensa. Los documentos públicos de alto nivel donde se define la I3D son:

- Orden DEF/2639/2015, de 3 de diciembre, que establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (en adelante Política CIS/TIC) y define la estructura de gobierno que permite su coordinación, control y seguimiento [3]. La Política CIS/TIC da una visión global de alto nivel estructura el gobierno de los CIS/TIC del Ministerio de Defensa, además de priorizar las capacidades CIS/TIC para las Fuerzas Armadas.

- Instrucción 58/2016, de 28 de octubre, del Secretario de Estado de Defensa, por la que se aprueba la Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa (AG CIS/TIC) [2]. En la AG CISTIC se describe a alto nivel las capacidades de la I3D, y se establecen las Arquitecturas necesarias para su implantación. Se define un modelo de Arquitecturas que desarrolla la AG CIS/ITC mediante Arquitecturas de Referencia (AR) y Objetivo (AO):

  • Las AR desarrollarán las Capacidades CIS/TIC identificadas en esta AG CIS/TIC, determinando los Sistemas CIS/TIC necesarios para su consecución. Así mismo, son la base para el desarrollo de las Arquitecturas Objetivo de los citados sistemas.

  • Las AO identifican en detalle los Componentes CIS/TIC de los Sistemas CIS/TIC determinados en las referidas AR's y establecerán las bases para su especificación técnica. Además, desarrollarán dichos Sistemas CIS/TIC detallando y especificando sus características, y la descomposición de los sistemas en subsistemas y equipos. Constituyen la base para el desarrollo de los proyectos y los Pliegos de Prescripciones Técnicas (PPT's) para la adquisición de CIS/TIC y la contratación de servicios.

- Instrucción 33 /2018, de 6 de junio, del Secretario de Estado de Defensa, por la que se aprueba el Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (PECIS) [4]. En cuanto a la implantación de la infraestructura de telecomunicaciones que sustituirá o evolucionará a la WAN PG y WAN C2, el documento clave para comprender las diferentes posibilidades es el PECIS. La I3D tiene varios componentes. El Eje estratégico 1.1 "Avanzar hacia una única Infraestructura integral de Información para la Defensa(I3D) gestionada por el CESTIC"] se especifica el diseño y despliegue de la Infraestructura de Telecomunicaciones de la I3D, que está compuesta por:

  - Infraestructura de Telecomunicaciones Terrestres (ITT).
  - Infraestructura de Telecomunicaciones Vía Satélite (ITS).
  - Infraestructura de Telecomunicaciones Inalámbricas (ITI).

El Objetivo Estratégico (OE) 1.1 del PECIS es Diseñar y Desplegar las Capacidades de Infraestructura de Telecomunicaciones de la I3D:

"La nueva I3D, deberá asegurar la provisión de Servicios CIS/TIC a los diferentes tipos de usuarios del Ministerio de Defensa en todos los emplazamientos, plataformas, puestos de trabajo y operativos en su caso. Así mismo, debe permitir el acceso a los usuarios desde emplazamientos y ubicaciones no pertenecientes al Ministerio de Defensa (redes y usuarios remotos) así como la interacción de usuarios del Departamento con otras organizaciones, nacionales e internacionales, a través de pasarelas y puntos de interconexión de Servicios CIS/TIC debidamente asegurados y normalizados. Todos los Servicios CIS/TIC de la I3D se ofrecerán de modo extremo a extremo, a través de una gestión centralizada y única, manteniendo los medios desplegables un cierto grado de autonomía en su gestión" [4, p. 30].

Además, establece que *"Se debe diseñar una ITT de la I3D provista de un segmento de cableado (basado en fibra óptica) y un segmento de radiocomunicaciones (basado en radioenlaces), en algunos casos redundando el anterior segmento, que unan los emplazamientos del Ministerio de Defensa en todo el territorio nacional*" [4, p. 31].

Por último, se incluye en la AG CIS/TIC un requisito propio de infraestructuras críticas, el Núcleo Protegido:

"*la infraestructura única dispondrá de un núcleo protegido que asegure la supervivencia de determinados Servicios CIS/TIC, con el alcance necesario que posibilite el funcionamiento del Sistema de Mando y Control Militar, incluso en situaciones adversas o ante cualquier tipo de incidente que afecte a la misma*" [2, p. 51].

A esta infraestructura de telecomunicaciones operada por el Ministerio de Defensa se pueden unir, como complemento para su disponibilidad y capilaridad, los servicios de telecomunicaciones contratados a un operador de telecomunicaciones.

De esta manera, contando con una infraestructura de telecomunicaciones operada por el Ministerio de Defensa complementada por la contratada a los operadores de telecomunicaciones, es posible realizar el estudio de una hipotética implantación de SDWAN con comunicaciones seguras en la infraestructura de telecomunicaciones de la I3D:

- Infraestructura privada que proporcionan conectividad entre las sedes de la organización, y con el exterior de la organización, con requerimientos de confidencialidad e integridad de la información que dependen del nivel de clasificación del tráfico. Se establece la premisa de que la I3D implementa VPNs "on premise" y operadas de forma centralizada por el Ministerio de Defensa

- Infraestructuras críticas con requerimiento de disponibilidad para posibilitar el Sistema de Mando y control Militar en situaciones críticas. Se incluye en el estudio la disponibilidad de la conectividad entre sedes y la garantía del tráfico.

3. Resultados y discusión

Los resultados obtenidos en la práctica permiten evaluar el valor añadido por:

- Disponer de conectividad WAN en capa 3 cifradas entre las sedes. Esto proporciona comunicaciones seguras en las que todo el tráfico está cifrado con los algoritmos públicos más seguros disponibles en la actualidad.
- Separar el plano de gestión de la red del plano de datos, mediante la creación de un overlay sobre las distintas redes y medios físicos disponibles que trabajan de forma coordinada. Esto genera múltiples ventajas:
  - Mayor disponibilidad, ya que a medida que se incluyen redes distintas orientadas a dar el mismo servicio se incrementa la fiabilidad de la red overlay.
  - Flexibilidad de la red al permitir cursar todos los servicios de la organización en todas las sedes independientemente de la cobertura de red que haya disponible.
  - Ahorro de costes al incluir redes con más ancho de banda y menos coste al configurar posteriormente la capa de seguridad con la propia solución.
  - Optimización de la red al ser el plano de control el encargado del envío de tráfico por el mejor enlace disponible en cada momento, permitiendo su cambio a otro enlace en tiempo real en caso de degradación del enlace.
- Posibilidad de comportamiento de los medios de transmisión en tiempo real.

4. Conclusiones

Se concluye que el SDWAN y las comunicaciones seguras son una opción aplicable a la AG CIS/TIC del Ministerio de Defensa, en particular a su infraestructura de telecomunicaciones del Ministerio de Defensa. La arquitectura de SDWAN estudiada es una opción viable para evaluar a gran escala:

- Supervisión centralizada y continua de la conectividad del Ministerio de Defensa.
- Uso complementario de redes propias del Ministerio de Defensa y contratadas a operador de telecomunicaciones.
- Empleo de circuitos hasta 100 Gbps en la infraestructura de telecomunicaciones. La complementariedad del uso de MACsec e IPsec permiten adaptar las comunicaciones seguras.
- Automatización del tunelizado IPsec.
- Optimización del uso del ancho de banda, permitiendo la selección de caminos a seguir por el tráfico de la organización mediante el SDWAN.

Agradecimientos

A mi familia, amigos, y compañeros, por hacer posible este trabajo.

Referencias

[1] UIT-T, «X.1205 Serie X: Redes de datos, comunicaciones de sistemas abiertos y seguridad,» 04 2008. [En línea]. Available: https://www.itu.int/rec/T-REC-X.1205-200804-I/es. [Último acceso: 12 10 2021].

[2] Ministerio de Defensa, «Arquitectura Global de sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa (AG CIS/TIC),» 03 2017. [En línea]. Available: https://publicaciones.defensa.gob.es/arquitectura-global-de-sistemas-y-tecnologias-de-informacion-y-comunicaciones-del-ministerio-de-defensa-ag-cis-tic.html. [Último acceso: 12 10 2021].

[3] Ministerio de Defensa, «Plan Director de sistemas de Información y Telecomunicaciones,» 14 02 2002. [En línea]. Available: https://boe.es/boe/dias/2002/02/20/pdfs/A06752-06756.pdf. [Último acceso: 31 10 2021].

[4] Ministerio de Defensa, Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa(PECIS), 2018.