Escuela Politécnica Superior de Jaén

Grado en Ingeniería Informática

UNIVERSIDAD DE JAÉN
Escuela Politécnica Superior de Jaén

Trabajo Fin de Grado

DISEÑO E IMPLEMENTACIÓN DE LA RED E INFRAESTRUCTURA DE COMUNICACIONES DE UNA EMPRESA

Alumno: Pablo José Nieto Solana

Tutor: Prof. D. Joaquín Cañada Bago

Dpto: Ingeniería de Telecomunicación

Universidad de Jaén
Escuela Politécnica Superior de Jaén
Departamento de Informática

Don Joaquín Cañada Bago , tutor del Proyecto Fin de Carrera titulado: *Diseño e implementación de la red e infraestructura de comunicaciones de una empresa*, que presenta Pablo José Nieto Solana, autoriza su presentación para defensa y evaluación en la Escuela Politécnica Superior de Jaén.

Jaén, Abril de 2024

El alumno:

Firmado por NIETO SOLANA PABLO JOSE - ***3262** el día 12/04/2024 con un certificado emitido por AC FNMT Usuarios. Número de serie: 89343798710116928305467689317229918393

Los tutores:

CAÑADA BAGO JOAQUIN - 25969508R

Firmado digitalmente por CAÑADA BAGO JOAQUIN - 25969508R
Fecha: 2024.04.12 11:13:10 +02'00'

Pablo José Nieto Solana

Joaquín Cañada Bago

Agradecimientos

Antes de comenzar con esta memoria, no puedo evitar agradecer a aquellas personas que me acompañaron y apoyaron desde el primer día.

Empezando por mis padres y mi hermano, que me levantaron el ánimo siempre y, sobre todo, en aquel primer año de carrera que tan duro fue. Tampoco puedo olvidar a mis abuelos, que también han estado siempre ahí.

Agradecer también a mis compañeros de piso durante estos años, Francisco, Alberto y Adrián, por esos momentos de conversación que, aunque solo fueran diez minutos en la cocina mientras se terminaba de hacer la comida, te daban ánimo para seguir en otra larga tarde de estudio.

Finalmente, quiero agradecer también a mis compañeros de trabajo, de los cuales aprendo cosas nuevas cada día.

Índice de contenido

1. Introducción 7
2. Objetivos 7
2.1. Diseñar la red jerárquica de la sede central y la red de las sedes distribuidas. 8
2.2. Incorporar tecnologías que incrementen la seguridad 8
2.3. Diseñar el acceso a Internet y la conexión Segura con otras sedes y con teletrabajadores 8
2.4. Diseñar la zona DMZ, de servidores públicos y privados 8
2.5. Instalación de un IDS en la sede central 8
2.6. Implementación de una parte de la red, utilizando los equipos disponibles en el laboratorio de la Universidad 9
2.7. Verificar las prestaciones de la red 9
3. Glosario de siglas 9
4. Estado el Arte 11
4.1. El modelo TCP/IP 11
4.2. Ethernet (IEEE 802.3) 14
4.2.1. Especificaciones de Fast Ethernet (IEEE 802.3 a 100 Mbps) 16
4.2.2. Especificaciones de Gigabit Ethernet (IEEE 802.3 a 1 Gbps) 17
4.3. Protocolo IP 18
4.3.1. IPv4 e IPv6 18
4.3.2. Datagrama IPv4 20
4.3.3. Datagrama IPv6 22
4.4. Tecnologías de seguridad en la red 24
4.4.1. Cortafuegos 24
4.4.2. VLAN 26
4.4.3. DMZ: Zona Desmilitarizada 26
4.4.4. ACL: Lista de control de acceso 26
4.5. VPN e IPSec 27
4.5.1. Beneficios del uso de IPSec 28
4.5.2. Asociaciones de seguridad 29
4.5.3. AH: Cabecera de Autentificación 31
4.5.4. ESP: Encapsulamiento de la carga útil de seguridad 32
4.5.5. La ventana contra repeticiones 34

4.5.6. Usos de IPSec 35
4.5.7. Alternativas a IPSec 36
4.5.8. L2TP 37
4.6. Redes jerárquicas 38
4.6.1. Niveles en una red jerárquica 39
4.6.2. Diseño de núcleo colapsado 42
4.6.3. Diseño modular de la red 43
4.6.4. Modelo de arquitectura empresarial propuesto por Cisco 45
4.6.5. La sede central o campus empresarial 46
4.6.6. La frontera empresarial 47
4.6.7. La frontera del proveedor de servicios 47
4.6.8. El área funcional remota 50
4.7. Sistemas de detección de intrusiones (IDS) 50
4.7.1. Técnicas de burla a un IDS 52
4.8. Snort 53
4.8.1. Componentes de Snort 54
4.8.2. Reglas de Snort 54
4.8.3. Niveles de amenaza 59
4.8.4. Falsos positivos 59
4.8.5. Reglas preinstaladas 60
4.9. Protocolo SNMP 61
5. Diseño de la red de la organización 65
5.1. Diseño de la sede central 66
5.1.1. Requisitos de seguridad 66
5.2. Diseño de las sedes remotas 70
5.3. Diseño de las redes privadas virtuales (VPN) 72
6. Montaje de una parte de la red 75
6.1. Definición de las VLAN 75
6.2. Configuración del servidor DHCP 77
6.3. Configuración del port mirroring hacia el IDS 81
6.4. Creación y prueba de reglas en el IDS 82
6.5. Solución al problema con el puerto espejo y configuración de SNMP 85
6.6. Configuración de Snort y Swatch para que el IDS pueda tomar acciones en el switch 89

6.6.1. Snort 89
6.6.2. Swatch 91
6.7. Ejecución y comprobación del funcionamiento 92
6.8. Esquema de la red montada 93
6.9. Observaciones finales 94
7. Cronograma de trabajo 95
8. Presupuesto 96
9. Bibliografía 98

1. Introducción

Hace años que no se concibe una organización sin infraestructura de comunicaciones, ni siquiera a pequeña escala. Las comunicaciones son, sencillamente, vitales para la productividad, hasta el punto de que, incluso pequeños negocios con uno o dos empleados, están digitalizando su actividad. Se atribuye a Bill Gates la cita *si tu negocio no está en internet, tu negocio no existe*.

En el caso de una organización con un cierto tamaño, aparece la necesidad de organizar adecuadamente la red, de forma que los equipos conectados a la misma queden segmentados y que se puedan controlar, con relativa facilidad, los problemas que puedan surgir durante el uso de la infraestructura (fallos en equipos, aumentos en la demanda que requieren, a su vez, aumentos en la capacidad de la red, problemas de seguridad, y un largo etcétera).

Partiendo de los conocimientos adquiridos en las diferentes asignaturas del Grado en las que se trabaja con redes, así como de bastante lectura e investigación, se presenta este trabajo. En la parte de diseño, se construirá una red relativamente grande y, en la parte práctica, la realizada con equipos de laboratorio, la atención se centrará en la seguridad. El objetivo, en ese momento, será convertir un sistema de detección de intrusiones en un elemento activo, capaz de proteger la red sin necesidad de intervención humana.

2. Objetivos

Se diseñará la red de una organización compuesta por una sede central, dos sedes remotas y teletrabajadores. La sede central seguirá un diseño jerárquico y se apoyará en tecnologías como las VLAN o la zona desmilitarizada (DMZ) para mejorar la seguridad, complementados con un sistema de detección de intrusiones (IDS).

Los objetivos del presente Trabajo de Fin de Grado se presentan a continuación.

2.1. Diseñar la red jerárquica de la sede central y la red de las sedes distribuidas.

Para el diseño jerárquico de la red de la sede central se seguirán las indicaciones de Cisco.

2.2. Incorporar tecnologías que incrementen la seguridad

Se emplearán redes privadas virtuales (VPN), listas de control de acceso (ACL), cortafuegos y cualquier otra tecnología relacionada con la seguridad de la red que se considere oportuna durante el diseño de la misma. Adicionalmente, se utilizará un sistema de detección de intrusiones.

2.3. Diseñar el acceso a Internet y la conexión Segura con otras sedes y con teletrabajadores

En relación con el punto anterior, tendrán protagonismo las VPN.

2.4. Diseñar la zona DMZ, de servidores públicos y privados

Al igual que ocurre con el diseño de las conexiones entre sedes y teletrabajadores, este punto está relacionado con el 2.2, pues se tendrán que tomar las medidas de seguridad oportunas para controlar el tráfico de los servidores.

2.5. Instalación de un IDS en la sede central

Como se mencionó en el objetivo 2.2, en la sede central de la organización se colocará un equipo, en la ubicación óptima para esta finalidad, que se encargará de filtrar el tráfico de red y generar las alertas necesarias.

2.6. Implementación de una parte de la red, utilizando los equipos disponibles en el laboratorio de la Universidad

Aunque no será posible completar el montaje de toda la red de la organización, se realizará una pequeña parte de la misma con los equipos Cisco disponibles en los laboratorios, poniendo el foco en la parte de seguridad basada en el IDS.

2.7. Verificar las prestaciones de la red

Se comprobará el correcto funcionamiento de la parte de la red montada.

3. Glosario de siglas

Se presentan, en este apartado, las siglas que aparecerán a lo largo del Trabajo de Fin de Grado, junto con su significado.

Siglas	Significado
DMZ	Zona Desmilitarizada (*Demilitarized Zone*, en inglés).
IDS	Sistema de detección de intrusiones (*Intrusion Detection System*, en inglés)
IPS	Sistema de prevención de intrusiones (*Intrusion Prevention System*, en inglés)
VPN	Red Privada Virtual (*Virtual Private Network*, en inglés)
ACL	Lista de control de acceso (*Access Control List*, en inglés)
PDU	Unidad de datos del protocolo (*Protocol Data Unit*, en inglés)
QoS	Calidad de servicio (*Quality of Service*, en inglés)
SFD	Delimitador de comienzo de trama, en una trama MAC (*Start Frame Delimiter*, en inglés)

ISP	Proveedor de servicios de Internet (*Internet Services Provider*, en inglés)
SA	Asociación de seguridad (*Security Association*, en inglés)
AH	Cabeceta de autentificación (*Authentication Header*, en inglés)
ESP	Encapsulamiento de la carga útil de seguridad (*Encapsulating Security Payload*, en inglés)
VLAN	Red de área local virtual (*Virtual Local Area Network*, en inglés)
L2TP	Protocolo de túnel de capa 2 (*Layer 2 Tunneling Protocol*, en inglés)
SNMP	Protocolo simple de administración de red (*Simple Network Management Protocol*, en inglés)
OID	Identificador de objeto en SNMP (*Object ID*, en inglés)
MIB	Base de información gestionada (*Management Information Base*, en inglés)
GVRP	Protocolo genérico de registro de VLAN (*Generic VLAN Registration Protocol*, en Inglés).

4. Estado el Arte

Se inicia este trabajo con un análisis de la situación actual de las comunicaciones y sus bases, que pondrá al lector en contexto para poder afrontar los siguientes capítulos sin dificultad.

4.1. El modelo TCP/IP

Dado que se va a llevar a cabo el diseño de una red, es fundamental introducir la pila de protocolos TCPI/IP en los que se sustentará, con base en (Stallings, Comunicaciones y Redes de Computadores, 2004).

TCP/IP separa el proceso de comunicación en cinco capas independientes, de forma que los cambios que se puedan realizar en una capa no deben afectar al resto de capas. En cada una de ellas, se ofrecen una serie de servicios a las capas de nivel superior, a la vez que se libera a estas de llevar a cabo las funciones más básicas necesarias para realizar su trabajo.

Las capas en las que se divide la pila de protocolos TCP/IP son:

- **Capa física (nivel 1):** Es la interfaz entre el dispositivo que transmite la información y el propio medio físico por el que esta se propaga. En esta capa se definen, entre otras, las características de las señales eléctricas o la velocidad a la que se deben transmitir los datos.
- **Capa de acceso a red (nivel 2):** Permite el intercambio de datos entre el sistema de origen de los mismos y la red, de forma que el software situado sobre esta capa funciona de forma independiente a las características de la misma. En el caso de una red local, el encaminamiento se realiza mediante las direcciones MAC de esta capa. Un ejemplo de dispositivo de nivel 2 son los switches. La unidad de datos del protocolo (PDU) en esta capa se denomina *trama*.
- **Capa Internet (nivel 3):** Si la capa anterior permitía la comunicación entre dispositivos conectados a una misma red, en esta capa se realiza la conexión

de dispositivos en distintas redes, utilizando, para ello, el protocolo IP (*Internet Protocol*). Los routers son dispositivos que funcionan en este nivel, encaminando los paquetes según su dirección IP de destino (entre otros condicionantes, como el estado de las rutas o la configuración de calidad de servicio -QoS, por sus siglas en Inglés-). En este caso, a una unidad de datos se le denomina *paquete* o *datagrama*.

- **Capa de transporte (nivel 4):** En esta capa se ejecutan protocolos, como TCP, que proporciona mecanismos de fiabilidad, para garantizar (en mayor o menor medida, según el protocolo usado) que los datos lleguen correctamente a la aplicación de destino. En este nivel, el direccionamiento se realiza mediante número de puerto, que identifica a una aplicación concreta de la capa superior. La unidad de datos se denomina *segmento*.

  Vale la pena detenerse brevemente para comentar los dos protocolos principales que se ejecutan en esta capa: TCP y UDP.

  - TCP es un protocolo orientado a conexión (esto es, para iniciar una transmisión de datos, primero se debe haber establecido una conexión entre las capas de transporte de los sistemas involucrados en la misma) que proporciona mecanismos para que los sistemas de origen y destino puedan seguir la pista a los segmentos, de forma que se puedan recuperar (esto es, volver a transmitir) aquellos que nunca lleguen a su destino, o que se garantice que los paquetes se reciben en el mismo orden en el que se transmiten y solo una vez.
  - UDP, por el contrario, no garantiza que los segmentos lleguen, ni tampoco que lo hagan en orden y sin duplicados. Ni siquiera es un protocolo orientado a conexión. Su uso tiene sentido en aquellas aplicaciones en las que no generan problemas las pérdidas moderadas de datos e, incluso, son preferibles a tener que esperar una retransmisión de los mismos. Un ejemplo son las aplicaciones multimedia, como llamadas por VoIP, en las que una pérdida de paquetes baja no supone un mayor problema y la recuperación de

segmentos perdidos generaría un retardo que haría difícil la comunicación entre los participantes.

- **Capa de aplicación (nivel 5):** En esta capa se ejecutan las aplicaciones de usuario propiamente dichas, como puede ser un reproductor multimedia, un servidor FTP o un navegador web.

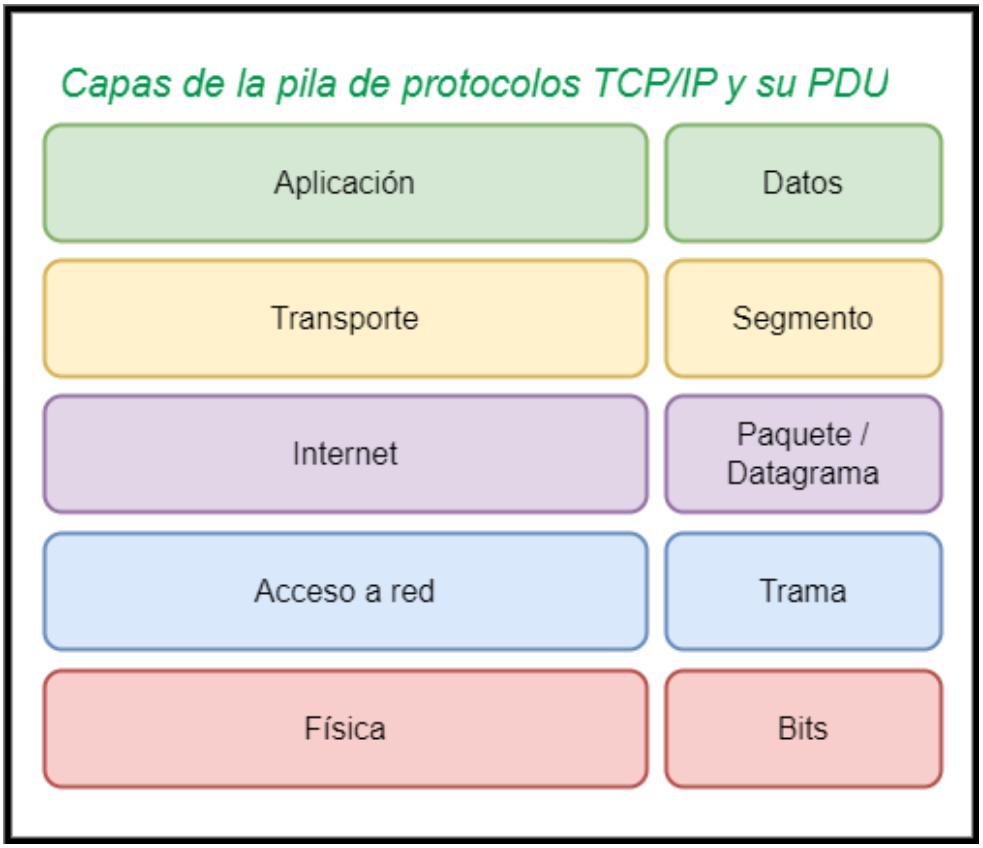


Figura 1: Capas TCP/IP y su PDU. Fuente: Elaboración propia.

Para el funcionamiento de TCP/IP, la unidad de datos del protocolo (PDU) de cada una de las capas se empaqueta como carga útil dentro de la unidad de datos de la capa inferior, añadiendo las cabeceras propias en cada uno de los niveles. En el dispositivo de destino, el proceso es el contrario: en cada capa se van eliminando las cabeceras propias y pasando los datos a la capa superior, hasta llegar a la capa de aplicación.

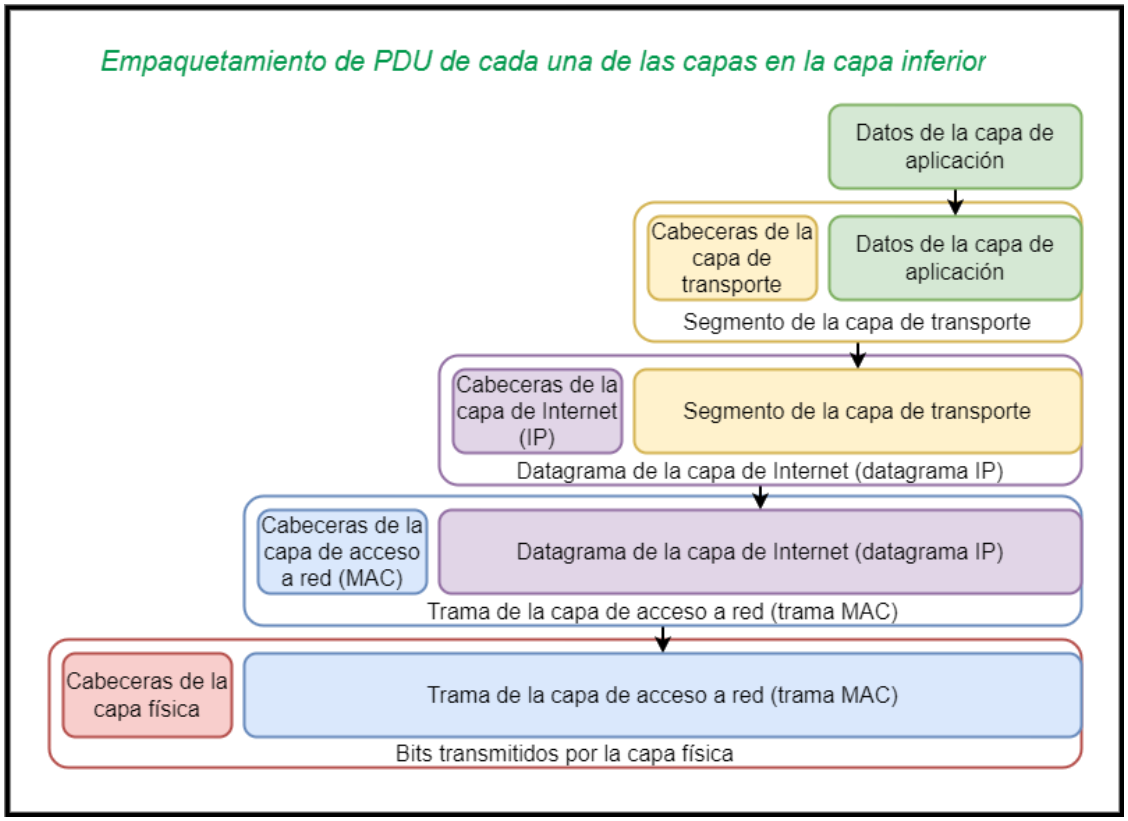


Figura 2: Empaquetamiento de las unidades de datos en las diferentes capas TCP/IP. Fuente: Elaboración propia.

4.2. Ethernet (IEEE 802.3)

Para la comunicación entre los dispositivos y los equipos de red, se va a utilizar tecnología ethernet, la cual se explica a continuación, usando como referencia bibliográfica (Stallings, Comunicaciones y Redes de Computadores, 2004). Dado que actualmente los *hub* o concentradores son completamente obsoletos, se omite la explicación referente al control de acceso al medio y la detección de colisiones, pues con el uso de conmutadores (switches) no es posible que estas se produzcan.

Antes de proseguir, conviene detenerse un poco más en las razones para no utilizar concentradores. Un *hub* o concentrador es físicamente muy similar a un switch: consta de una serie de puertos ethernet a los que se conectan los dispositivos. La principal diferencia es qué ocurre cuando un dispositivo envía datos a través de uno de esos puertos.

En un *hub*, que es un dispositivo de capa 1, estos datos son repetidos por todos los demás puertos, es decir, no tiene conocimiento de cuál es el destino de los datos.

Dado que Ethernet es un medio compartido, solo un equipo puede transmitir en un momento determinado, lo cual deriva en la existencia de colisiones, generadas cuando dos o más dispositivos intentan transmitir datos a la vez. Debido a esto, si se utilizan concentradores, los equipos conectados a la red tienen que utilizar algún sistema de control de acceso al medio (normalmente, CSMA/CD) para evitar estas colisiones, lo cual implica pérdida de aprovechamiento del ancho de banda, pues los dispositivos tienen que esperar a que el canal esté libre para poder transmitir datos.

Por otra parte, el funcionamiento de un *hub* es *half-dúplex*, esto es, los datos solo se pueden transmitir en una dirección a la vez (o *hablas*, o *escuchas*, pero no ambos).

Finalmente, el hecho de que los datos se transmitan por todos los puertos es propenso a la aparición de problemas de seguridad y privacidad en la red, pues todos los equipos los reciben, aunque no se dirijan a ellos.

El sucesor natural del *hub* es el switch. Este dispositivo trabaja en la capa 2 y retransmite los datos recibidos por un puerto únicamente por el puerto en el que está conectado el dispositivo de destino, basándose en la dirección MAC de destino de la trama. Las ventajas son fáciles de deducir:

- Mejor seguridad y privacidad, al dirigirse los datos solo a su destino.
- Se evitan las colisiones. Aunque dos dispositivos transmitan datos a la vez, estos no interferirán entre sí.
- Se puede trabajar en modo full-dúplex, esto es, se pueden transmitir y recibir datos al mismo tiempo.

En consecuencia, en la red que se diseñará más adelante en este TFG, siempre se emplearán switches.

4.2.1. Especificaciones de Fast Ethernet (IEEE 802.3 a 100 Mbps)

Dado que, en la actualidad, no es en absoluto común encontrarse con las versiones anteriores de Ethernet (como Ethernet a 10 Mbps), estas se omiten.

Para esta especificación de Ethernet, se puede utilizar tanto cable de pares trenzados (100 BASE-T) como fibra óptica (100 BASE-F), si bien es mucho más común la primera opción.

100BASE-TX (IEEE 802.3u)

Se emplean dos pares trenzados, uno para transmisión y otro para recepción, siendo la opción más recomendable el cable UTP de categoría 6. La longitud máxima de un cable de red es de 100 metros, sin que se produzcan pérdidas significativas que afecten a la comunicación.

El límite teórico de 100 Mbps se da por la forma de transmisión de los bits, en grupos de cuatro por cada tiempo de un reloj a 25 Mhz. La velocidad real alcanzada es menor, por la cabecera y la secuencia de comprobación de trama.

La alternativa en Fibra Óptica es 100BASE-FX, pero no se describe, al estar descartada para este proyecto.

Modo *Full-Dúplex*

Ethernet a 100 Mbps puede funcionar en modo *semi-dúplex* -un equipo conectado a la red puede enviar o recibir datos, pero no ambos a la vez- o *full-dúplex*, caso en el que se pueden enviar y recibir datos a la vez a la máxima velocidad en ambos sentidos (100 Mbps en sentido ascendente y 100 Mbps en sentido descendente). Las tarjetas de red deben soportarlo y es requisito imprescindible el uso de switches, para que nunca se puedan producir colisiones. Casi todos los switches soportan el modo *full-dúplex*, pero es necesario asegurarse de ello.

Otras consideraciones sobre Ethernet a 100 Mbps

Existe una versión, denominada 100 BASE-T4, que permite obtener una velocidad de 100 Mbps sobre cables obsoletos de categoría tres, pero solo permite el trabajo en modo *half-dúplex*, puesto que, de los cuatro pares que conforman un cable, se utilizan tres simultáneamente.

Los dispositivos Ethernet a 100 Mbps se pueden combinar con otros que solo dispongan de Ethernet a 10 Mbps, siempre que los switches soporten ambas especificaciones.

4.2.2. Especificaciones de Gigabit Ethernet (IEEE 802.3 a 1 Gbps)

En la actualidad, es la versión Ethernet más empleada, incluso en redes domésticas, debido a que el equipamiento instalado por los operadores (ISP) comunes suele incluir, desde hace años, esta tecnología, así como los ordenadores personales. Además, es retrocompatible con Ethernet a 100 Mbps y a 10 Mbps, de forma que un dispositivo más antiguo se puede conectar sin problemas a un puerto Ethernet a 1 Gbps.

1000BASE-T (IEEE 802.3ab)

Es la versión de Gigabit Ethernet pensada para funcionar sobre cables de pares trenzados, permitiéndose longitudes de hasta 100 metros. Para trabajar con garantías a 1 Gbps se requiere que los cables sean, como mínimo, de categoría 5e y, preferiblemente, de categoría 6.

Las opciones sobre fibra óptica son 1000BASE-SX y 1000BASE-LX, pero no se describen al estar descartadas para este TFG, dado que aumentan los costes y no son compatibles con los equipos presentes en los laboratorios.

Aunque no se empleará en este Trabajo de Fin de Grado, conviene mencionar que existe también Ethernet a 10 Gbps, con estándares como 10GBASE-S,

10GBASE-L, 10GBASE-E o 10GBASE-LX4, que emplean la fibra óptica como medio de transmisión.

4.3. Protocolo IP

El protocolo IP o protocolo de Internet, (Stallings, Comunicaciones y Redes de Computadores, 2004), (Wikipedia, Protocolo de internet, 2023), permite la transmisión de datos entre dispositivos conectados a diferentes redes, usando para el enrutamiento las direcciones IP. Es un protocolo no orientado a conexión, es decir, que no establece un canal de comunicación previo entre el emisor y el receptor, sino que, por el contrario, un equipo puede enviar datos a otro sin que haya existido una negociación previa.

El hecho de que sea un protocolo no orientado a conexión implica que tampoco es fiable, en el sentido de que no existen mecanismos para garantizar la entrega de los datagramas y las sumas de comprobación solo se aplican a las cabeceras, no a la carga útil del paquete. Para la entrega de los paquetes, IP sigue un modelo *best effort* o mejor esfuerzo, esto es, tratando de enrutar los paquetes para que lleguen al destino en el menor tiempo posible, pero sin garantías.

4.3.1. IPv4 e IPv6

Son las dos versiones del protocolo IP en uso. Aunque la idea es que, en algún momento, IPv6 reemplace a IPv4, la realidad es que, a 19 de diciembre de 2023, la adopción de IPv6 en Internet según datos de (Google, 2023) es del 41.18%.

Como se detalla más adelante, las direcciones en IPv4 tienen una longitud de 32 bits, frente a los 128 bits de una dirección IPv6. Esa limitación del espacio de direcciones que permite IPv4 fue la principal motivación para el desarrollo de su sucesor, pues supone algunos problemas:

- En IPv4, las direcciones se dividen, mediante la máscara de red, en dos partes: identificador de red y dispositivo. Esto implica que, una vez se ha definido el identificador de red, todas las direcciones de la misma quedan

reservadas y, si en esa red no existen tantos equipos, las direcciones sobrantes no se pueden aprovechar.

- Dado que el número de dispositivos conectados a Internet es cada vez mayor, es imposible identificar a cada uno con una dirección única, de ahí que se hayan tenido que idear sistemas como NAT, para que varios dispositivos puedan navegar por la red con una sola dirección IP pública.

Algunas de las mejoras que introduce IPv6 frente a IPv4 son las siguientes:

- **Mayor espacio de direcciones:** Aumentar de 32 a 128 bits el tamaño de la dirección ofrece un total de direcciones posibles (no todas son usables) de 2^{128}, frente a las 2^{32} de IPv4. Consecuentemente, se puede asignar una dirección única a cada dispositivo conectado a Internet en el mundo y, aun así, sobrarán direcciones.
- **Cabeceras opcionales:** En IPv6, además de la propia cabecera del protocolo, se pueden incluir otras con diferentes opciones que, normalmente, solo son procesadas por el equipo de destino, reduciendo la carga de los dispositivos de encaminamiento.
- **Configuración automática de direcciones:** Gracias a esta capacidad, los equipos pueden conectarse a una red y ser capaces de transmitir datos sin necesidad de que un servidor DHCP les asigne una dirección IP. Mediante configuración automática de direcciones, los dispositivos pueden:
    - Generar una dirección local de enlace única en la red, mediante un protocolo de descubrimiento de vecinos.
    - Usando esa dirección local, puede comunicarse con el router que gestiona esa red y, de esta forma, obtener un prefijo con el que determinar su dirección global en Internet.
- **Monodifusión (*anycast*):** Las direcciones monodifusión se pueden asignar a la vez a varias tarjetas de red. Un paquete que tenga como destino una de estas direcciones solo lo recibirá el dispositivo con esta dirección asignada más próximo al origen. Además de las direcciones monodifusión, existen:

  - Direcciones unidifusión (*unicast*): direcciones únicas para una tarjeta de red.
  - Direcciones multidifusión (*multicast*): identifican múltiples interfaces de red y, cuando un paquete se envía a una dirección de este tipo, todos los nodos lo reciben.
- **Funcionalidad para calidad de servicio:** Como se verá a continuación, con la definición de los campos de la cabecera de los datagramas, en IPv4 existía un campo tipo de tráfico cuyo significado se acabó alterando para usarlo en el marcado de paquetes en clases de tráfico. IPv6 ya incluye un campo específico para ese fin.

4.3.2. Datagrama IPv4

Los campos que constituyen la cabecera de un datagrama IPv4, (Postel, 1981), son los siguientes:

- **Versión:** 4 bits que indican si se está utilizando IPv4 o IPv6.
- **Longitud de cabecera de Internet:** También con 4 bits, este campo indica el tamaño total de la cabecera en palabras de 32 bits. Dado que una cabecera IP tiene una longitud mínima de 160 bits, el valor mínimo que se puede encontrar en este campo es 5.
- **Tipo de servicio:** Con una longitud de 8 bits, en su origen tenía otra finalidad, si bien actualmente se emplean los seis primeros bits como marca para servicios diferenciados (que es el sistema de calidad de servicio más empleado), mientras que los dos bits restantes se pueden utilizar para notificar congestión (notificación explícita de congestión o ECN) de la siguiente forma:
  - 00 → Indica que no se está utilizando ECN.
  - 01 y 10 → Ambos estados indican que ECN es compatible con los equipos involucrados en la comunicación y, por tanto, se puede utilizar.
  - 11 → Indica que existe congestión.

Inicialmente, este campo se dividía en cinco bits para indicar características del servicio (los cinco bits menos significativos) y tres bits para indicar la prioridad de los mensajes.

- **Longitud total:** 16 bits que indican, en octetos, el tamaño del datagrama completo.
- **Identificador:** 16 bits que identifican de forma inequívoca un datagrama, en base a las direcciones de origen y destino y al protocolo que se está utilizando. Permite reconstruir un datagrama en caso de que exista fragmentación (es decir, que esté dividido en varias partes porque, por su tamaño, no haya sido posible su transmisión).
- **Indicadores (*flags*):** Tres bits utilizados de la siguiente forma:
  - Bit 0: Siempre debe ser un 0.
  - Bit 1: En caso de estar a 1, impide la fragmentación del datagrama. Esto significa que, si no puede enviarse sin fragmentar, simplemente no se enviará.
  - Bit 2: Se pone a 1 cuando hay más fragmentos del mismo datagrama y a 0 cuando se trata del último fragmento. Como se puede intuir, el valor de este bit siempre será 0 en un datagrama no fragmentado.
- **Desplazamiento del fragmento:** 13 bits para indicar la posición de un fragmento en el datagrama completo. La longitud de este campo impone un límite de 8192 fragmentos para un mismo datagrama.
- **Tiempo de vida (TTL):** Aunque la unidad definida para este campo son los segundos, en la práctica indica el número máximo de saltos (esto es, de routers) por los que puede pasar un datagrama hasta llegar a su destino final, pues este número se decrementa -típicamente y como mínimo- en una unidad por cada salto.

Si en un router el TTL llega a 0, el paquete es descartado y se notifica al origen mediante un mensaje ICMP (de hecho, *traceroute* se basa en este principio para conocer el camino seguido por un paquete hasta su destino).

Mediante el uso del TTL se evita que los datagramas puedan quedar indefinidamente saltando entre routers en caso de que el destino sea inalcanzable.

- **Protocolo:** 8 bits que indican el protocolo de la capa superior cuya cabecera va incluida en la carga útil del datagrama.
- **Suma de comprobación:** Tiene una longitud de 16 bits y se calcula únicamente con la cabecera. Cuando un router recibe un datagrama, comprueba este campo para verificar que la información de la cabecera no ha sido alterada y, además, lo vuelve a calcular antes de enviarlo al siguiente salto, debido a que algunos campos de la cabecera (como el TTL), habrán cambiado su valor.
- **Dirección de origen:** No necesita mayor explicación, son 32 bits que identifican la dirección IP del equipo origen del datagrama.
- **Dirección de destino**
- **Opciones:** Campo de longitud variable, sólo limitado por la longitud máxima de la cabecera. Algunos ejemplos de opciones son *Time Stamp* (indica a cada salto que grabe en el datagrama la fecha y la hora de paso) o *Record Route* (hace que cada router guarde su propia IP en el paquete para que el destino pueda conocer la ruta que ha seguido el mismo).

4.3.3. Datagrama IPv6

En caso de emplear IPv6, (Deering & Hinden, 2017), se cuenta con una cabecera obligatoria (de 320 bits, frente a los 160 de la cabecera IPv4) pero, además, se pueden incluir otras cabeceras. Estas son:

- Cabecera de opciones salto a salto: Incluye opciones que deberán ser examinadas por todos los routers por los que pase el paquete.
- Cabecera de encaminamiento: Determina la ruta que deberá seguir el paquete, con un listado de routers por los que debería pasar. En caso de que algún router sea inalcanzable, el paquete será descartado (a excepción de

que esté ya en el último router, caso en el cual el campo segmentos restantes valdrá cero) y se notificará al origen mediante ICMP.

- Cabecera de fragmentación: Contiene la información necesaria para que el destino pueda reensamblar los paquetes fragmentados.
- Cabecera de autenticación: Utilizada por AH, como se explica más adelante en el apartado dedicado a IPSec.
- Cabecera de encapsulamiento de la carga de seguridad: Utilizada por ESP, se explica en el apartado de IPSec.
- Cabecera de opciones para el destino: Incluye información que solo es útil para el equipo que recibirá el paquete, por lo que no es examinada por los dispositivos de encaminamiento.

Se desarrolla solo el contenido de la cabecera IPv6, compuesta por los siguientes campos:

- **Versión:** Al igual que en IPv4, los primeros cuatro bits indican si se utiliza IPv4 o IPv6.
- **Clase de tráfico:** Campo de 8 bits equivalente al uso actual que recibe el campo *tipo de servicio* en IPv4.
- **Etiqueta de flujo:** En IPv6 existen los flujos, que son secuencias de paquetes con un origen y destino concretos, identificadas por sus direcciones de origen y destino y por esta etiqueta de flujo.

  El equipo de origen, mediante una cabecera de extensión, puede indicar a los routers que den un tratamiento especial a los paquetes de un determinado flujo (por ejemplo, para que ignoren su etiqueta de clase de tráfico y le den cierta prioridad).

- **Longitud de la carga útil:** 16 bits que indican, en octetos, el tamaño de las cabeceras de extensión más el de la PDU del protocolo de la capa de nivel superior.

- **Límite de saltos:** Número máximo de saltos entre routers que puede dar un paquete. En este caso, directamente se establece en número de saltos y no en segundos pues, en la práctica y como se ha comentado anteriormente, no se trataba como segundos tampoco en IPv4.
- **Dirección de origen:** A diferencia de IPv4, en IPv6 las direcciones son de 128 bits.
- **Dirección de destino**

4.4. Tecnologías de seguridad en la red

4.4.1. Cortafuegos

La finalidad de un cortafuegos es el bloqueo del tráfico de red no autorizado, en base a una serie de reglas que se definan en el mismo. Pueden ser software, que corre sobre un sistema operativo, o hardware, que son dispositivos similares a un router.

A la hora de ubicar un cortafuegos en la red de la organización, se debe tener en cuenta que todo el tráfico que provenga o se dirija al exterior debe pasar por el mismo, permitiéndose solo aquel que esté autorizado.

Por otra parte, existen cuatro técnicas diferentes que un cortafuegos puede emplear:

- **Control del servicio:** Determina a qué servicios de Internet se puede acceder, usualmente basándose en direcciones IP y números de puerto.
- **Control de dirección:** Se filtra según el sentido del tráfico (entrante o saliente).
- **Control de usuario:** Se permite o no el acceso a un servicio según el usuario que lo intente realizar. En una red local, es posible que el propio cortafuegos conozca a los usuarios mientras que, para tráfico entrante desde Internet, los usuarios tendrán que identificarse.
- **Control de comportamiento:** Controla el uso de los servicios, bloqueando, por ejemplo, el acceso a páginas webs concretas o el correo no deseado.

Por supuesto, los cortafuegos no son una tecnología de seguridad infalible, sino que presentan algunas limitaciones, como la imposibilidad de evitar infecciones de malware en los dispositivos de la red, o de evitar un ataque interno (voluntario o no).

Atendiendo a los tipos de cortafuegos que se pueden encontrar, se puede diferenciar entre cortafuegos de filtrado de paquetes, de nivel de circuito (que trabajan en la capa de transporte) o de nivel de aplicación, filtrando tráfico específico de aplicaciones (como FTP, SMTP…).

Para el caso de este trabajo, interesan los cortafuegos de filtrado de paquetes, que se basan en la siguiente información de los mismos para permitir o impedir el tráfico:

- IP de origen.
- IP de destino.
- Números de puerto de la capa de transporte.
- Protocolo de la capa de transporte.
- Interfaz, en el caso de un router con tres o más interfaces de red.

A la hora de establecer la política del cortafuegos, se puede optar por *descartar por defecto*, es decir, que todo está bloqueado salvo lo que esté explícitamente autorizado (lista blanca); o *permitir por defecto*, es decir, todo está permitido excepto lo que está explícitamente bloqueado (lista negra). Para los usuarios es más cómoda la segunda opción -el cortafuegos pasará prácticamente desapercibido para ellos- pero, a nivel de seguridad, es mucho mejor la primera, pues se acerca más a una política de confianza cero (*zero trust*).

Para la documentación de este punto se ha consultado (Stallings, Fundamentos de seguridad en redes. Aplicaciones y Estándares. Segunda Edición., 2004).

4.4.2. VLAN

Una red de área local virtual permite dividir una red física en diferentes redes lógicas independientes, limitando los dominios de difusión y evitando el intercambio de datos en red local entre dispositivos que no deben hacerlo.

Para el etiquetado de los paquetes se utiliza el estándar IEEE 802.1Q, que introduce una cabecera adicional a la trama MAC de Ethernet, de forma que se pueden configurar varias VLAN en un mismo puerto. Esto resulta imprescindible para enlaces troncales.

En el caso de los dispositivos finales, es posible que las VLAN deban ir sin etiquetar, pero, como resulta evidente, solo se puede tener una única VLAN sin etiquetar, dado que el dispositivo no tiene forma de diferenciarlas.

4.4.3. DMZ: Zona Desmilitarizada

Es una red local ubicada entre Internet y la red interna de una organización, en la cual se suelen ubicar servidores accesibles por el público, de forma que no se pueda saltar desde esta zona de la red a la red interna.

Mediante la configuración de una zona desmilitarizada se evita la exposición al exterior de servidores ubicados en la red interna, evitando posibles accesos no autorizados a la misma.

Una forma de implementar una DMZ es ubicándola entre dos cortafuegos. El primero, expuesto a Internet, permite el tráfico del exterior hacia la DMZ y el segundo impide el tráfico desde la DMZ hacia el interior de la red, a la vez que lo permite en el sentido contrario. Lo habitual es que, adicionalmente, la DMZ se encuentre en una VLAN específica.

4.4.4. ACL: Lista de control de acceso

Las listas de control de acceso son similares a los cortafuegos, en tanto que permiten filtrar el tráfico de red en base a una serie de reglas, siendo un gran complemento a ellos.

Pongamos como ejemplo la siguiente red:

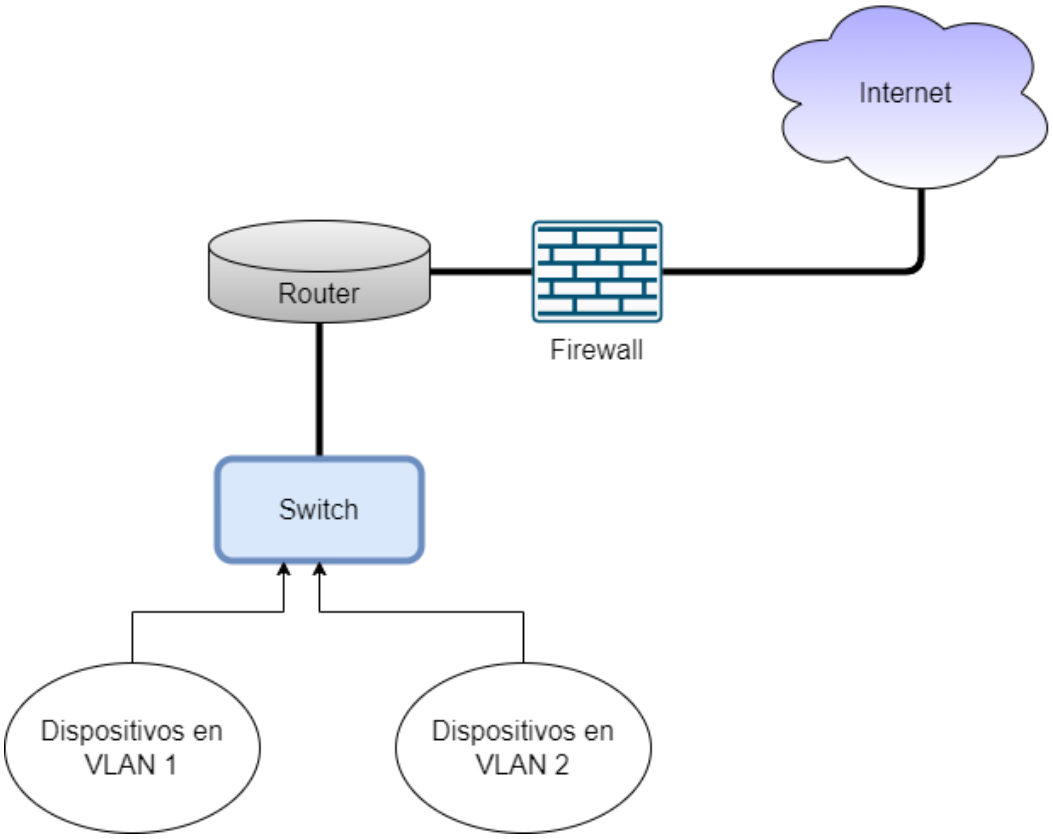


Figura 3: Ejemplo de red en la que puede ser necesaria una ACL

A nivel 2, los dispositivos de la VLAN 1 no pueden comunicar con los dispositivos de la VLAN 2, y viceversa. Sin embargo, sí es posible que lo puedan hacer a nivel 3, pues el tráfico llegará al router y este, según su configuración, lo dirigirá a los dispositivos de destino.

Configurando una lista de control de acceso en el router, es posible filtrar este tráfico sin hacer necesario dirigirlo hasta el firewall, para hacer allí el filtrado.

4.5. VPN e IPSec

Una red privada virtual, o VPN (de *Virtual Private Network*, en inglés), permite extender una red de área local (LAN) a través de una red WAN insegura, como Internet, extendiendo también todas las políticas de dicha red privada.

Una VPN segura debe proporcionar autentificación, confidencialidad mediante el cifrado de datos, garantía de integridad de los mensajes recibidos, no repudio, control de acceso (para evitar que agentes no deseados se conecten a la red privada), capacidad de recuperación ante errores y un buen rendimiento (se busca que no sea perceptible la pérdida de velocidad con respecto a estar realmente conectado a una red LAN).

Se diferencian tres tipos de VPN, según cada extremo de la misma:

- **VPN *Client to Site*:** Un dispositivo remoto obtiene acceso a la red local de una organización.
- **VPN *Site to Site*:** En este caso, se conectan dos redes locales, normalmente dos VLAN, de forma que se comportan como si fuesen una única red local.
- **VPN *Client to Client*:** Se conectan dos equipos, uno con otro, como si estuviesen solos en una red local. Para ello, primero se necesita tener una VPN *Site to Site* que conecte las redes locales en las que están los dispositivos.

4.5.1. Beneficios del uso de IPSec

Cuando se utiliza IPSec [(Stallings, Comunicaciones y Redes de Computadores, 2004), (Stallings, Fundamentos de seguridad en redes. Aplicaciones y Estándares. Segunda Edición., 2004)] para obtener seguridad a nivel de red, se obtienen una serie de ventajas, como son:

- Se puede implementar en los routers o cortafuegos hardware, de forma que todo el tráfico que los atraviese quede protegido. Así, se libra a los equipos de los usuarios de realizar este trabajo, a la vez que se garantiza que todo el tráfico, independientemente de su origen, queda bajo IPSec.
- Extendiendo el punto anterior, si un router o cortafuegos con IPSec es el único punto de entrada desde Internet a la red, se garantiza que todo el tráfico de entrada debe venir protegido con IPSec.
- Dado que IPSec trabaja en la capa de Internet, por debajo de la capa de transporte, no requiere ningún cambio en las aplicaciones para funcionar y es

capaz de proteger todo el tráfico, independientemente del protocolo de la capa de transporte empleado o de la aplicación a la que corresponda el tráfico.

- Es invisible para los usuarios finales, que no tendrán que ocuparse de gestionar ellos mismos las claves ni necesitarán formación para el uso de IPSec.
- En el caso de, por ejemplo, trabajadores remotos que necesiten acceso a la red local de la organización, IPSec también cubre sus necesidades, pues puede asegurar también las comunicaciones de un solo dispositivo.
- A nivel de seguridad en los protocolos de enrutamiento, IPSec también proporciona mecanismos útiles, como:
    - Garantía de que un anuncio de un router proviene de un router de confianza.
    - Si un router vecino quiere comunicarse con un router en otra red, este deberá ser autorizado.
    - Cuando se recibe una respuesta a un mensaje, se tiene garantía de que proviene del mismo router al que se envió en mensaje original.
    - No se puede falsificar una actualización de las tablas de rutas.

4.5.2. Asociaciones de seguridad

Tal como se define en (Stallings, Fundamentos de seguridad en redes. Aplicaciones y Estándares. Segunda Edición., 2004):

> *Una asociación de seguridad es una relación unidireccional entre un emisor y un receptor que ofrece servicios de seguridad al tráfico que transporta.*

Las asociaciones de seguridad (SA, *Security Association*) son unidireccionales, por lo que, para conseguir una comunicación bidireccional segura, se requieren dos asociaciones.

Para que los extremos de una comunicación puedan identificar una SA de forma unívoca, se utilizan tres campos:

- **Índice de parámetros de seguridad o SPI**: Se transporta en las cabeceras AH y ESP de IPSec (se explicarán más adelante) y está relacionado únicamente con una asociación de seguridad.
- **IP de destino**: Dirección del sistema final de la asociación de seguridad.
- **Identificador del protocolo de seguridad**: Identifica si se utiliza ESP o AH.

El resto de parámetros que definen una SA son:

- **Contador de número de secuencia**: 32 bits a partir de los cuales se genera el campo *número de secuencia*, presente en las cabeceras AH y ESP.
- **Desbordamiento del contador de secuencia**: Indica que el contador de número de secuencia se ha desbordado y, por tanto, esta asociación de seguridad no se puede seguir utilizando.
- **Ventana contra repeticiones**: Permite identificar si un paquete es una repetición.
- **Información AH o ESP**: Algoritmo de cifrado, tiempo de vida, claves y demás parámetros propios de las implementaciones AH o ESP.
- **Tiempo de vida de la SA**: Número máximo de bytes que se pueden transmitir por una SA, o segundos de duración de la misma.
- **Modo de protocolo IPSec**: Si se usa modo túnel o modo transporte.
- **MTU del camino**: Indica el tamaño máximo de un paquete para que este no tenga que ser fragmentado.

Los dispositivos finales y de encaminamiento deben ser capaces de asociar un paquete (entendiendo *paquete* como un *datagrama* IPv4 o *paquete* IPv6) a una determinada asociación de seguridad. Para ello, poseen una Base de Datos de Políticas de Seguridad que relaciona el tráfico IP con una SA, atendiendo a propiedades de los paquetes como las direcciones de origen y destino, el identificador de usuario, el protocolo IPSec, el protocolo de la capa de transporte, los números de puerto empleados o las clases de tráfico.

4.5.3. AH: Cabecera de Autentificación

IPSec tiene dos modos de funcionamiento: AH y ESP. En este punto, y en el siguiente, se describe cada uno de ellos.

AH permite la autentificación del origen de los datos y garantiza su integridad, haciendo imposible que estos sean alterados en el camino. Esto permite el filtrado del tráfico y evitar ataques de repetición o de suplantación de dirección.

La cabecera AH consta de los siguientes campos:

- **Cabecera siguiente**: 8 bits que indican qué cabecera hay después de esta.
- **Longitud de carga útil**: También de 8 bits, indica la longitud de la cabecera AH en palabras de 32 bits menos 2 (esto es, si la cabecera tiene una longitud de seis palabras, en este campo se colocará un 4).
- **Espacio reservado para usos posteriores** (16 bits)
- **Índice de parámetros de seguridad**: 32 bits que identifican la asociación de seguridad a la que pertenece el paquete, tal y como se indicó en el anterior punto sobre las asociaciones de seguridad.
- **Número de secuencia**: Número de 32 bits que se incrementa con cada paquete enviado y que se utiliza, como se explicará más adelante, para la protección contra ataques de repetición.
- **Datos de autentificación**: Contiene el valor de verificación de integridad del paquete, que suele ser el resultado de aplicación de una función HMAC calculada sobre:
    - Los campos de la cabecera IP que no se modifican en el camino o cuyo valor de llegada es predecible. Los campos variables o de valor impredecible se fijan a cero para el cálculo.
    - La propia cabecera AH, excluyendo este campo.
    - Todos los datos del protocolo de nivel superior encapsulados como carga útil del paquete IP.

Si se usa modo transporte, la cabecera AH se incluye entre la cabecera IP y la carga útil en el caso de IPv4, y después de la cabecera IP y de las cabeceras salto a salto, enrutamiento y fragmentación en el caso de IPv6. Si se tiene una cabecera de opciones para el destino (solo IPv6), esta puede ir delante o detrás de la cabecera AH.

En modo túnel, la cabecera AH se coloca entre la cabecera IP original y la cabecera IP del nuevo paquete (cuyas direcciones de origen y destino, recuerde, no tienen por qué coincidir con las del paquete original).

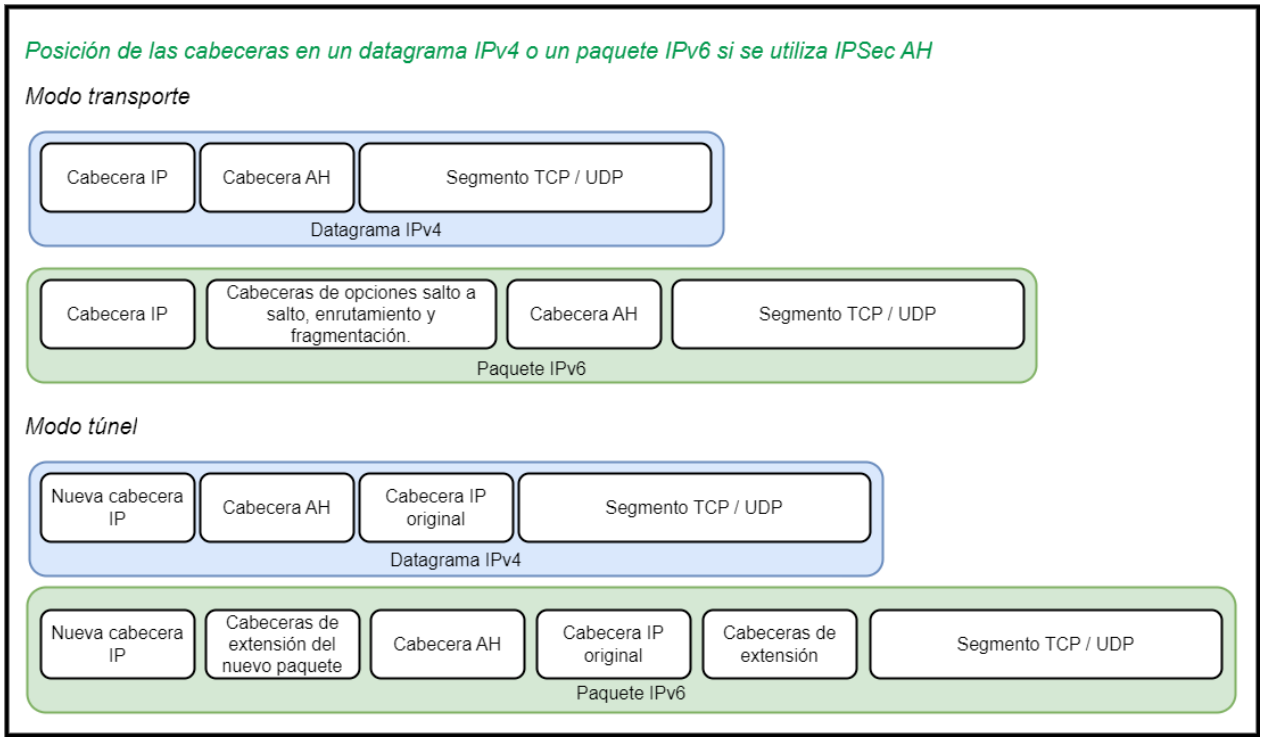


Figura 4: Ubicación de la cabecera AH en modo transporte y modo túnel, para IPv4 e IPv6. Fuente: Elaboración propia.

4.5.4. ESP: Encapsulamiento de la carga útil de seguridad

ESP proporciona confidencialidad a los mensajes y al tráfico y, opcionalmente, puede ofrecer también la autentificación proporcionada por AH.

Los campos que forman un paquete ESP son:

- **Índice de parámetros de seguridad:** Mismo significado que en AH, 32 bits que identifican la asociación de seguridad en uso.

- **Número de secuencia:** 32 bits con un número que se incrementa de forma secuencial, usado para la protección contra ataques de repetición.
- **Datos de carga útil:** En modo transporte, es un segmento de la capa de transporte. En modo túnel, es el datagrama IP protegido.
- **Relleno:** Puede tener una longitud de hasta 255 bytes y existe por tres razones:
    - En primer lugar, ESP requiere que los campos *longitud de relleno* y *cabecera siguiente* estén alineados en una palabra de 32 bits. El relleno se emplea para conseguir este alineamiento.
    - Permite aumentar la longitud del texto claro a cifrar, si así lo requiere el algoritmo de cifrado empleado.
    - Puede ofuscar la longitud real de la carga útil, ofreciendo confidencialidad parcial al tráfico.
- **Longitud de relleno:** 8 bits que indican el número de bytes que ocupa el relleno.
- **Cabecera siguiente:** 8 bits que indican cuál es la primera cabecera en la carga útil.
- **Datos de autentificación:** La longitud de este campo es variable, formado por palabras de 32 bits. Contiene el valor de comprobación de integridad (al igual que en AH, suele ser una función HMAC) aplicado a todo el paquete ESP menos este campo. Solo está presente si, además del cifrado, se utiliza autentificación (esto es, ESP+AH).

Estos campos se dividen en dos grupos: la cabecera ESP, formada por los campos *índice de parámetros de seguridad* y *número de secuencia*, que es insertada antes de la cabecera de la capa de transporte; y la terminación ESP, formada por los campos *relleno*, *longitud de relleno* y *cabecera siguiente*, que es insertada después del segmento de la capa de transporte.

Modo transporte

En modo transporte, que se suele emplear para comunicación directa entre dos hosts, ESP opera de la siguiente forma:

1.- En primer lugar, en el dispositivo de origen, cifra la carga útil del mismo y la terminación ESP. Si, además, se está utilizando autentificación, se añade el campo correspondiente.

2.- El paquete se encamina al destino, sin que los equipos intermedios puedan examinar los campos cifrados.

3.- En el dispositivo de destino, se puede descifrar el paquete recibido a partir del índice de parámetros de seguridad presente en la cabecera ESP.

Modo túnel

En este caso, se cifra el datagrama IP completo, sustituyendo su cabecera IP original por una nueva. Se siguen los siguientes pasos:

1.- En origen, la cabecera ESP se coloca delante de la cabecera IP original. A continuación, se cifra el paquete y la terminación ESP, añadiendo, si se utiliza, la información de autentificación. Por último, se antepone una nueva cabecera IP, cuya dirección de destino será el router o cortafuegos donde se implementa IPSec en el otro lado del túnel.

2.- El paquete se encamina al router o cortafuegos de destino, sin que los routers intermedios tengan posibilidad de examinar la parte cifrada del mismo.

3.- El router o cortafuegos IPSec del destino se basa en el SPI de la cabecera ESP para descifrar el paquete y obtener el original, que se transmite mediante la red interna al equipo de destino.

4.5.5. La ventana contra repeticiones

Un ataque de repetición es aquel mediante el cual se transmiten paquetes legítimos hacia su destino, que han sido capturados previamente, intentando provocar saturación en el mismo u obtener acceso a un sistema de forma fraudulenta (por ejemplo, si se repiten paquetes con claves de identificación consideradas válidas por el destino).

Para evitarlos, se emplea el número de secuencia ligado a una asociación de seguridad. En el origen de los paquetes, se inicia el contador a 0 y se incrementa en 1 cada vez que se va a enviar un paquete para, a continuación, colocar este valor en el correspondiente campo de la cabecera AH o ESP -dado que se incrementa antes de escribirlo en la cabecera, el primer paquete no lleva un 0, sino un 1-. Puesto que el número de secuencia es un campo de 32 bits, el número máximo de paquetes que se pueden transmitir por una asociación de seguridad es de $2^{32} - 1$, siendo necesario crear una nueva SA cuando se alcance dicho número.

En el equipo receptor, se crea una ventana de un determinado tamaño (*W*) que, inicialmente, será 64. El extremo derecho de la ventana siempre será el mayor número de secuencia recibido hasta el momento en un paquete válido.

Al recibir un paquete, se sigue el siguiente procedimiento:

- En primer lugar, se comprueba si el paquete cae dentro de la ventana. De ser así, y siempre que los datos de autentificación sean válidos y este paquete no se haya recibido anteriormente (esto es, que la ranura no esté ya marcada), se marca dicha ranura.
- En caso de que el paquete caiga a la derecha de la ventana, esta avanza hasta que su extremo derecho coincida con el número de secuencia del paquete recibido, por supuesto, siempre que el paquete supere la verificación de autentificación.
- Si el paquete cae a la izquierda de la ventana o no supera la comprobación de autentificación, es descartado.

4.5.6. Usos de IPSec

De forma general y para cerrar este punto sobre IPSec, se presentan algunos usos comunes de esta tecnología, basándose en (Stallings, Comunicaciones y Redes de Computadores, 2004).

- **Conectividad segura entre sucursales de una empresa:** Una organización compuesta por varias sedes puede conectarlas de forma segura a través de

Internet, sin necesidad de crear una costosa (o, incluso, imposible de construir) red WAN propia.

- **Acceso remoto seguro:** Un trabajador de una empresa puede conectarse a la red interna de la misma a través de Internet y trabajar como si lo hiciese en la propia oficina, todo ello de forma segura. A raíz de la pandemia del SARS-CoV-2 (COVID) el teletrabajo ha aumentado exponencialmente y, con él, el uso de IPSec y otras tecnologías (como *WireGuard*) para la creación de redes privadas virtuales seguras.
- **Aumento de la seguridad en el comercio electrónico:** A pesar de que la seguridad que se puede implementar en capas superiores (por ejemplo, en la capa de transporte, con el uso de TLS), añadir una capa de seguridad a nivel de red siempre aumenta la fiabilidad de operaciones importantes. Es por este motivo por el que, cuando se conectan dispositivos a una red considerada "poco segura", conviene utilizar una VPN hacia un servidor de confianza y navegar a través de ella. Para esta finalidad, una muy buena idea puede ser montar un servidor VPN en casa y conectarse a él cuando se requiera esa seguridad extra.

4.5.7. Alternativas a IPSec

Aunque, en este proyecto, se utilizará IPSec para las VPN, existen algunas alternativas al mismo que vale la pena tener en cuenta y que se presentan brevemente a continuación.

En primer lugar, *OpenVPN*, una solución de código abierto basada en SSL o TLS. Algunas características:

- Permite, por ejemplo, crear túneles IP utilizando UDP o TCP (solo necesita un puerto).
- Soporta cifrado y autentificación las comunicaciones a través de la red privada.
- Soporta IPv6.
- Permite utilizar cifrado simétrico o asimétrico.

Otra gran alternativa puede ser *WireGuard*, normalmente más rápido que *IPSec* y que *OpenVPN*. Uno de sus bastiones es la simplicidad de cara a los usuarios, que no necesitan tener grandes conocimientos para poder crear un túnel VNP, dado que se ocupa de forma automática de aspectos como el intercambio de claves o la gestión de conexiones. Utiliza protocolos considerados seguros, como *Curve25519* para el intercambio de claves de Diffie-Hellmann, o *ChaCha20*, entre otros. En el caso de Linux, *WireGuard* está integrado con el propio *Kernel*, lo que ofrece un funcionamiento extremadamente rápido.

Como última alternativa, y sin extender demasiado el apartado, se pueden mencionar las VPN basadas directamente en SSL o, preferiblemente, el más seguro TLS. Poseen la ventaja de poder implementarse sin que los usuarios tengan que instalar software adicional, pues basta con un navegador web para conectarse a una VPN de este tipo y acceder a los recursos de la organización.

Antes finalizar, conviene comentar *IKEv2*. Es un protocolo que trabaja conjuntamente con *IPSec* -así que, realmente, no es una alternativa al mismo- y se ocupa de gestionar las asociaciones de seguridad. Una de las razones por las que se utiliza es la movilidad, con dispositivos que cambian de red y de dirección IP con frecuencia y necesitan reestablecer la asociación de seguridad de la forma más rápida posible.

Como referencias para este punto, se pueden mencionar (Donenfeld, 2020), (OpenVPN, 2022), (Kaufman, Hoffman, Nir, Eronen, & Kivinen, 2014) o (Rosencrance, 2021).

4.5.8. L2TP

L2TP, siglas en inglés de *Protocolo de Túnel de Capa 2*, (Valencia, y otros, 1999) permite la creación de un túnel VPN entre dos puntos, encapsulando los datos dentro de un paquete UDP que, a su vez, se introduce como carga útil de un paquete IP cuyas direcciones de origen y destino son las de los extremos del túnel.

L2TP se suele usar en combinación con IPSec ya que, por sí solo, no proporciona cifrado a los datos que viajan por el túnel y la autentificación no se realiza tampoco con cada uno de los paquetes que por él viajan. Sin embargo, dado que lo que se tiene es un paquete IP, a este se le pueden aplicar las cabeceras ESP y/o AH, obteniendo cifrado y/o autentificación para los datos.

Aunque al utilizar L2TP junto a IPSec los datos deben ser encapsulados y desencapsulados dos veces, esto no supone una gran ralentización de la conexión, debido a que L2TP se ejecuta de forma nativa en el espacio del *kernel* de la mayoría de sistemas operativos relativamente modernos, resultando en una operativa muy rápida.

4.6. Redes jerárquicas

En el presente Trabajo de Fin de Grado, como se extrae de los objetivos presentados al inicio, se diseñará una red empresarial, jerárquica en la sede central y también modular, pues hay que definir una zona desmilitarizada donde se ubicarán los servidores que presten servicios al exterior y, además, existirán sedes remotas y teletrabajadores, que deberán conectarse de forma segura a la sede central de la organización.

El análisis del “estado del arte” respecto a las redes jerárquicas se basa en (Cisco, 2014).

Para entender por qué es adecuado el diseño jerárquico de la red, hay que ponerse en contexto: Cuando en las organizaciones se comenzó con la instalación de las primeras redes, estas se hacían con topología plana, sin distinguir distintos niveles en las mismas. El resultado fueron redes de difícil escalabilidad y con dificultades para controlar los problemas y el tráfico indeseado. A modo ilustrativo, en una red plana, cuando la cantidad de tráfico aumenta de forma considerable, es probable que se produzcan problemas en el servicio por la incapacidad de los equipos de red de hacer frente a ese aumento en la demanda de tráfico. La solución pasa por la actualización de estos dispositivos a unos con mayor capacidad.

En una red jerárquica, por el contrario, la red se divide en diferentes capas, cada una con unas funciones bien definidas y en las cuales el tráfico no pasa a una capa superior si no se dirige a otra red. En caso de un aumento en la demanda de tráfico, solo será necesario actualizar los equipos de red de la capa en la que se esté produciendo la saturación.

Una red jerárquica se basa en los cuatro principios de la ingeniería estructurada. El primero de ellos es la **jerarquía**, esto es, la división de la red en capas independientes. Dado que se está tratando el diseño de una red *jerárquica*, resulta trivial el respeto a este principio.

El segundo principio es la **modularidad**, consistente en dividir la red en módulos independientes, lo cual facilita el diseño y el control de posibles fallos en la misma.

Como tercer principio, la **resiliencia**. La red diseñada debería mantener su disponibilidad no solo en condiciones de tráfico normal, sino también en condiciones anormales, con cantidades de tráfico inusuales (por ejemplo, por un ataque de denegación de servicio) o fallos en algún equipo.

Por último, la **flexibilidad**, esto es, las posibilidades que ofrece la red para aumentar su capacidad o el número total de dispositivos conectados, sin que ello implique el reemplazo de los principales equipos de la misma.

4.6.1. Niveles en una red jerárquica

Siguiendo siempre el modelo propuesto por (Cisco, 2014), se diferencian tres capas. La primera es la **capa de acceso**, donde se conectan los usuarios a la red. En ella se pueden encontrar, por ejemplo, los ordenadores de los empleados de una organización.

La capa intermedia o **capa de distribución** limita el flujo de tráfico entre la capa de acceso y la capa central (*core*), basándose, normalmente, en políticas de seguridad.

Por último, la **capa central**, se compone de equipos destinados a la conmutación de paquetes entre diferentes módulos de la red, como puede ser la frontera de Internet o un centro de datos.

Se presentan a continuación, con mayor detenimiento, cada uno de estos niveles de la red.

Capa de acceso

Como se ha indicado anteriormente, es aquí donde se proporciona conexión a los dispositivos de los miembros de una organización. Otras funciones de la capa de acceso son la seguridad a nivel de puerto (entre otros, la desconexión del puerto en el que un equipo está llevando a cabo actividad potencialmente maliciosa), el manejo de redes privadas virtuales (VLAN), la clasificación y etiquetado para Calidad de Servicio (QoS) o la inspección ARP dinámica (que ayuda a evitar suplantaciones ARP).

Las conexiones remotas realizadas a través de Internet o de redes WAN a la red de la organización también se hacen en esta capa (es el caso, por ejemplo, de teletrabajadores que acceden mediante un escritorio remoto a sus equipos en la sede).

Los dispositivos que, comúnmente, se emplean en esta capa, son los *switches* y también puntos de acceso para los diferentes terminales.

Capa de distribución

En esta capa, se agregan los datos recibidos desde la capa de acceso, antes de enviarlos a la capa central para que sean enrutados a su destino.

La agregación, como su propio nombre indica, consiste en agrupar los flujos de datos de varios enlaces en uno solo, que se dirigirá a la capa central. Hay que tener en cuenta que a un switch o router -pueden emplearse tanto switches multicapa

como routers- de esta capa de distribución se pueden conectar numerosos switches del nivel de acceso.

Algunos servicios proporcionados en este nivel, además de la ya mencionada agregación de enlaces, son:

- Seguridad mediante listas de control de acceso (ACL, por sus siglas en inglés).
- Enrutamiento de paquetes entre diferentes VLAN.
- Balanceo de carga.
- Redundancia, que ayuda a mantener la red en funcionamiento cuando algún equipo falla.

Por otra parte, se debe tener en cuenta que los switches o routers de esta capa no reenvían paquetes de difusión, de forma que actúan como fronteras entre los dominios de difusión que puedan existir en la red.

Capa central (*Core*)

Se compone de dispositivos cuya finalidad es la conmutación de paquetes lo más rápido posible, para establecer comunicaciones entre diferentes módulos (como servidores internos, centros de datos o la propia WAN).

En el *core* de la red se espera una alta disponibilidad, lograda mediante redundancia de equipos, pues no es permisible que se pierda la conexión entre módulos o el acceso a Internet por el fallo de un solo equipo.

Para el escalado, normalmente, no se añaden nuevos dispositivos, sino que se sustituyen los ya existentes por otros más rápidos.

Finalmente, conviene resaltar que en la capa central no se llevan a cabo tareas que consuman gran cantidad de tiempo de CPU, como puede ser el etiquetado QoS o el filtrado por razones de seguridad, que quedan relegadas a las capas inferiores.

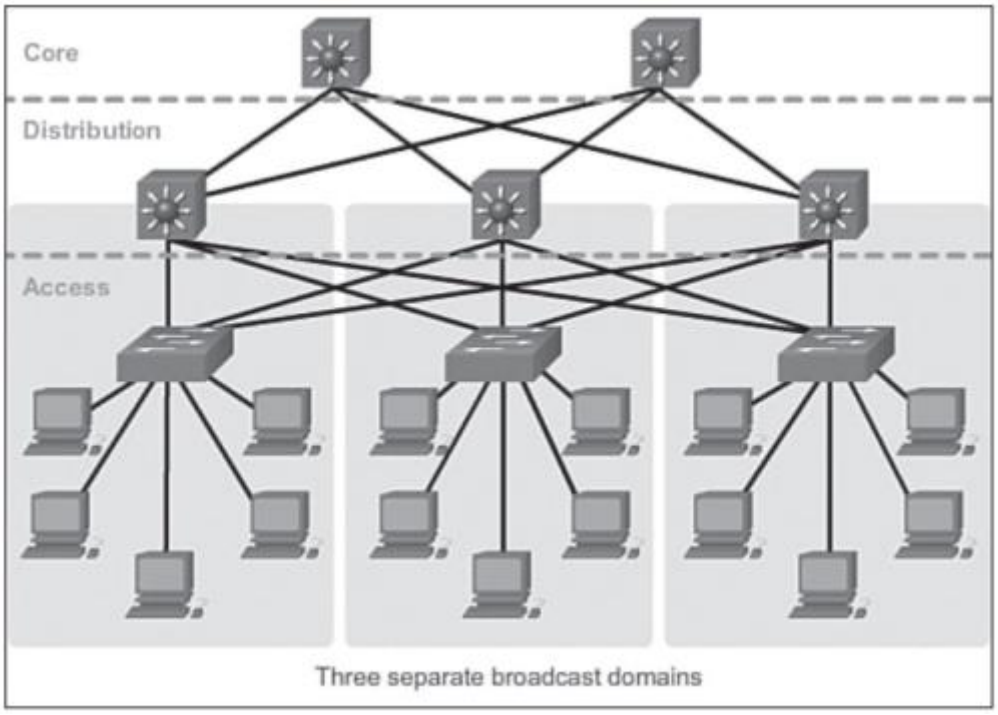


Figura 5: Estructura jerárquica en tres niveles de una red empresarial. Fuente: (Cisco, 2014)

4.6.2. Diseño de núcleo colapsado

En ocasiones, el tamaño de una organización no justifica la división de la red en tres capas, dado que el número de equipos conectados a la misma no es demasiado elevado y tampoco se prevé que crezca demasiado con el tiempo.

En estos casos, se pueden juntar las capas de distribución y central en una sola, llamada “capa de núcleo colapsado”. De esta forma, se siguen manteniendo muchas de las ventajas de una red jerárquica, como la modularidad o la flexibilidad de la red, pero logrando un importante ahorro de costes en equipamiento.

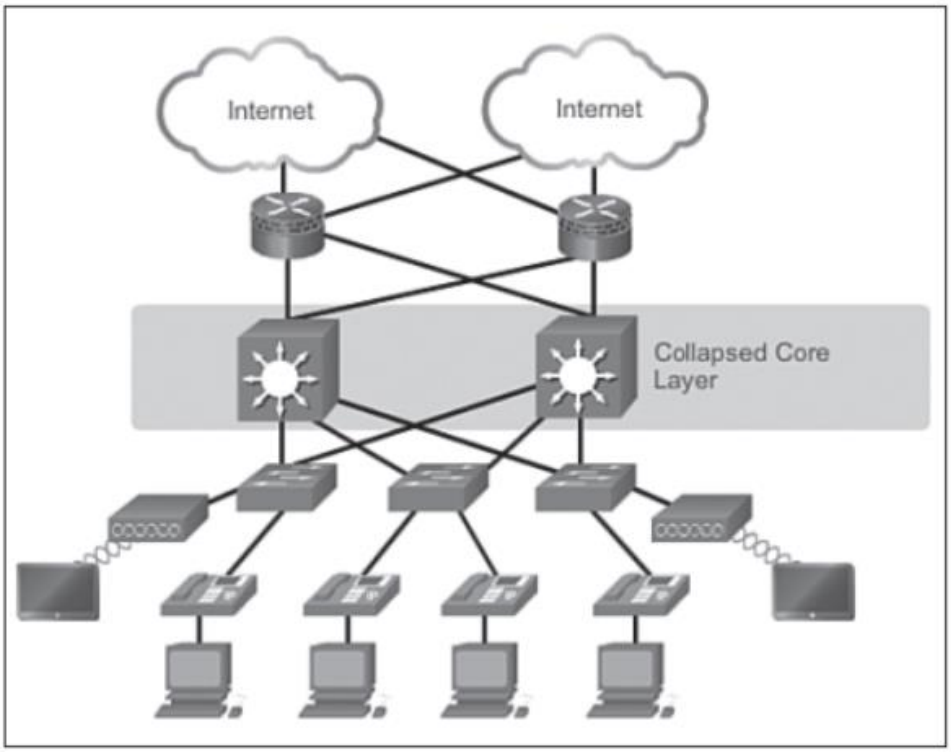


Figura 6: Estructura de núcleo colapsado en una red jerárquica. Fuente: (Cisco, 2014)

4.6.3. Diseño modular de la red

Actualmente, el diseño jerárquico de la red no cubre todas las necesidades de una organización, pues no tiene en cuenta nuevos requisitos, como la conexión de teletrabajadores o la existencia de varias sedes que deberán estar conectadas. El diseño modular de la red aporta soluciones al respecto.

En el apartado anterior, sobre la estructura de una red jerárquica, ya se han mencionado los módulos de la red, pero, ¿qué son exactamente?

Son divisiones de la red en diversas zonas o áreas (módulos), cada una de las cuales tiene una función específica e independiente, lo cual proporciona algunas ventajas:

- En primer lugar, si se produce un fallo en algún módulo, este se puede identificar y aislar de forma más sencilla, facilitando el proceso de recuperación.

- Por otra parte, las mejoras en la red o la introducción de nuevas capacidades se pueden hacer por etapas, centrándose en un módulo cada vez. Consecuentemente, si un módulo ya no tiene capacidad para cumplir su función, puede sustituirse por otro sin afectar al resto de módulos que conforman la red de la organización.
- La seguridad puede ser modular, lo cual no solo permite un control más granular, sino que también facilita el aislamiento y la mitigación de un posible ataque.

Se estudiará el diseño modular propuesto por (Cisco, 2014). Pero, antes, se presentan de forma introductoria cuáles son los principales módulos que se deben diferenciar en la red de una organización.

Módulos diferenciados en la red

- **Módulo de acceso y distribución**: Como su nombre indica, abarca las capas de acceso y distribución de la red jerárquica.
- **Módulo de servicios**: Aquí se incluyen puntos de acceso inalámbricos o dispositivos de comunicación (como teléfonos IP).
- **Centro de datos**: Formado por los servidores que permiten llevar a cabo operaciones comerciales, intercambio de archivos o comunicaciones entre los trabajadores, entre otros.
- **Perímetro empresarial**: Aquí se encuentran la frontera de Internet, a través de la cual se accede al mismo, y la frontera WAN, mediante la que se accede a alguna red WAN (que no tiene por qué ser Internet). Es normal ubicar en este módulo un cortafuegos que filtre el tráfico saliente y, sobre todo, entrante.

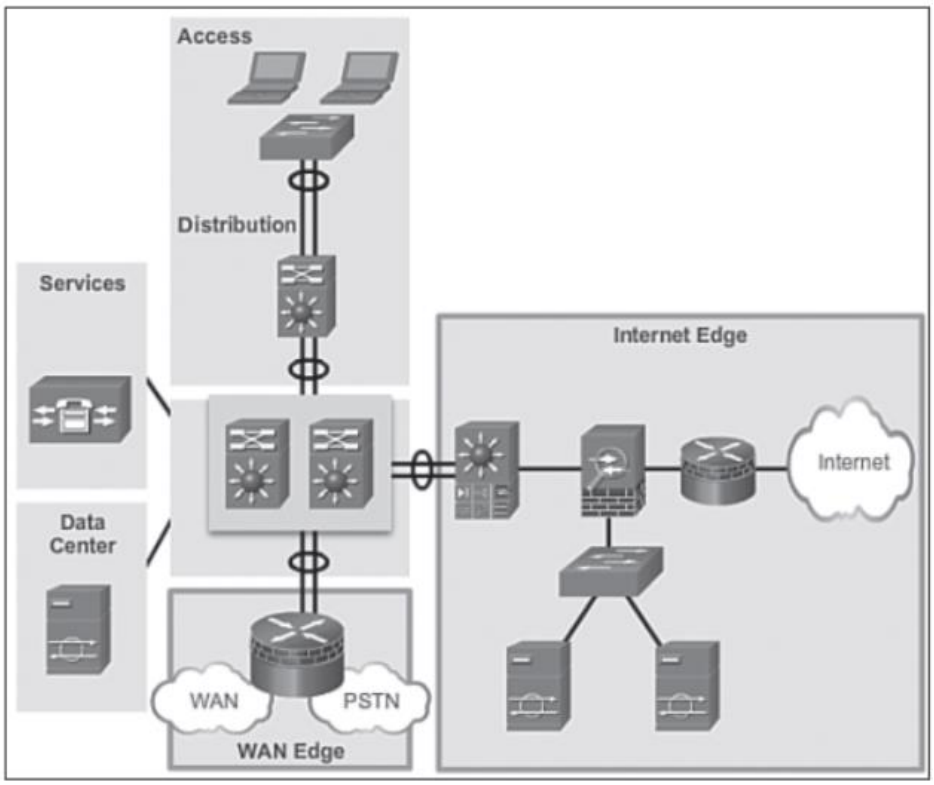


Figura 7: Módulos de la red. Fuente: (Cisco, 2014)

4.6.4. Modelo de arquitectura empresarial propuesto por Cisco

(Cisco, 2014) propone la división de la red en cuatro módulos principales:

- La sede empresarial, o campus empresarial.
- La frontera empresarial.
- La frontera del proveedor de servicios (ISP).
- Los elementos remotos (como otras sedes o teletrabajadores) que se conectan a la frontera del proveedor de servicios.

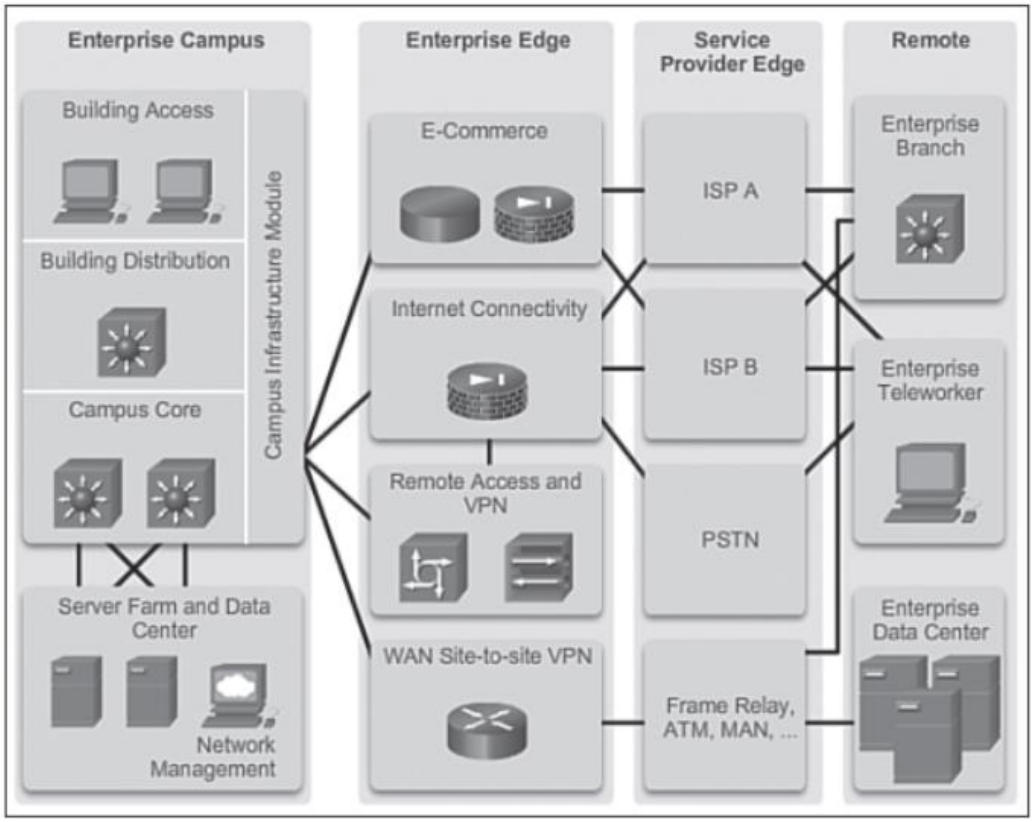


Figura 8: Modelo de arquitectura empresarial de Cisco. Fuente: (Cisco, 2014)

En la imagen sobre estas líneas se puede observar como la red en la sede central de la empresa tiene una estructura jerárquica.

4.6.5. La sede central o campus empresarial

Compuesta por la propia red jerárquica y el centro de datos:

- Proporciona alta disponibilidad, algo que deriva directamente del diseño jerárquico y del uso de equipos redundantes.
- Integra comunicaciones IP y políticas de seguridad avanzada, como VLAN, o listas de control de acceso (ACL). Gracias a estas políticas de seguridad, es posible mitigar el efecto de un ataque incluso a nivel de puerto de Switch.
- Puede emplear QoS (calidad de servicio) para optimizar el tráfico y priorizar determinados tipos.

4.6.6. La frontera empresarial

Contiene los submódulos que proporcionan acceso a servicios externos a la empresa, como Internet, comunicaciones o conexión a redes privadas virtuales (VPN). Se pueden destacar:

- **Servidores públicos:** Son accesibles desde el exterior, para la web de la empresa o el comercio electrónico, por ejemplo. Dentro de este módulo se suelen ubicar también cortafuegos (software o hardware) y sistemas de prevención de intrusiones (IPS, por sus siglas en Inglés).
- **Conexión a Internet:** Ofrece conexión a Internet para los usuarios internos de la organización. Se puede lograr redundancia mediante la conexión a varios proveedores de servicios de Internet (ISP, por sus siglas en Inglés). Al igual que ocurre en el submódulo de servidores públicos, es normal encontrar cortafuegos supervisando el tráfico.
- **Acceso remoto y VPN:** Permite la conexión de trabajadores remotos, para que tengan acceso a la red de la sede. Se utilizan IPS y cortafuegos.
- **WAN:** Este último submódulo utiliza tecnologías WAN como Metro Ethernet, redes ópticas (GPON, XGS-PON…) o *frame relay* para la conexión a redes de área amplia.

4.6.7. La frontera del proveedor de servicios

Permite la conexión entre la sede central y las sedes remotas o Internet, extendiéndose a grandes áreas geográficas y empaquetando los diferentes servicios (voz, datos, video…) en una misma conexión IP.

Con los ISP se pueden alcanzar acuerdos de nivel de servicio (SLA) que permitan utilizar QoS para priorizar determinados tipos de tráfico.

En este módulo debe tener presencia la redundancia en las conexiones a los proveedores de servicios, que se puede lograr de diversas formas.

En el caso de que solo se vaya a conectar a un ISP, se tienen dos opciones:

- ***Single homed*:** Solo hay una conexión a un ISP, con lo que no se dispone de redundancia y la conectividad se perderá en caso de fallo.
- ***Dual homed*:** Se tienen varias conexiones a un solo ISP. Puede hacerse con un solo router y varias conexiones (en este caso, solo se tiene redundancia en caso de fallo de las conexiones, pero no en caso de fallo del router) o con varios routers.

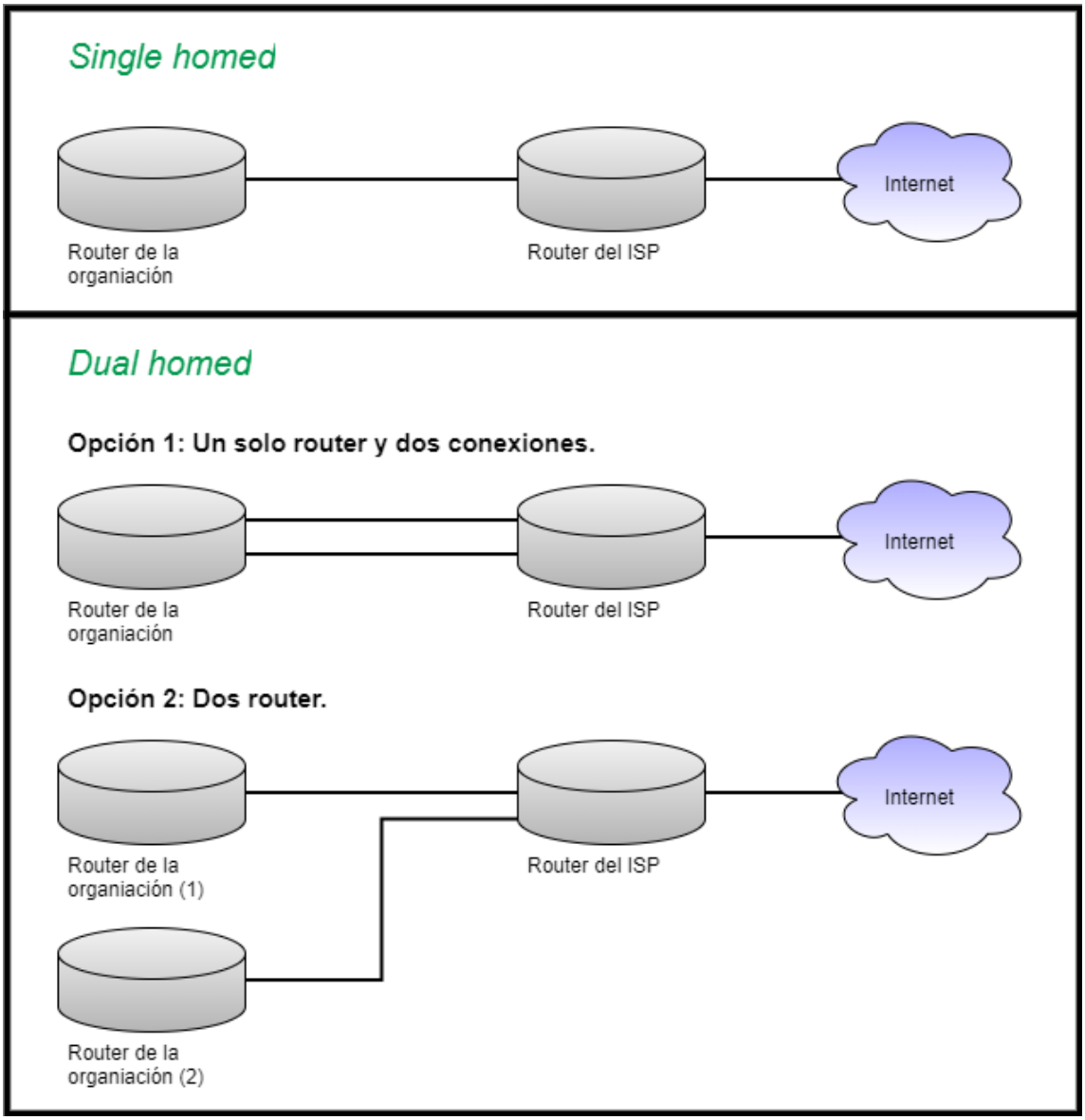


Figura 9: Opciones de conexión a un solo ISP. Fuente: Elaboración propia.

Si se va a establecer conexión con varios ISP, también se dispone de dos opciones, derivadas de las anteriores:

- ***Multimhomed***: Se establecen conexiones con más de un proveedor, pero solo una por proveedor. Esto significa que la redundancia se consigue solo por la variedad de ISP.
- ***Dual - multihomed***: Al igual que en el caso anterior, se establecen conexiones con varios ISP, con la diferencia de que, ahora, sí existe redundancia a nivel de conexión con cada proveedor.

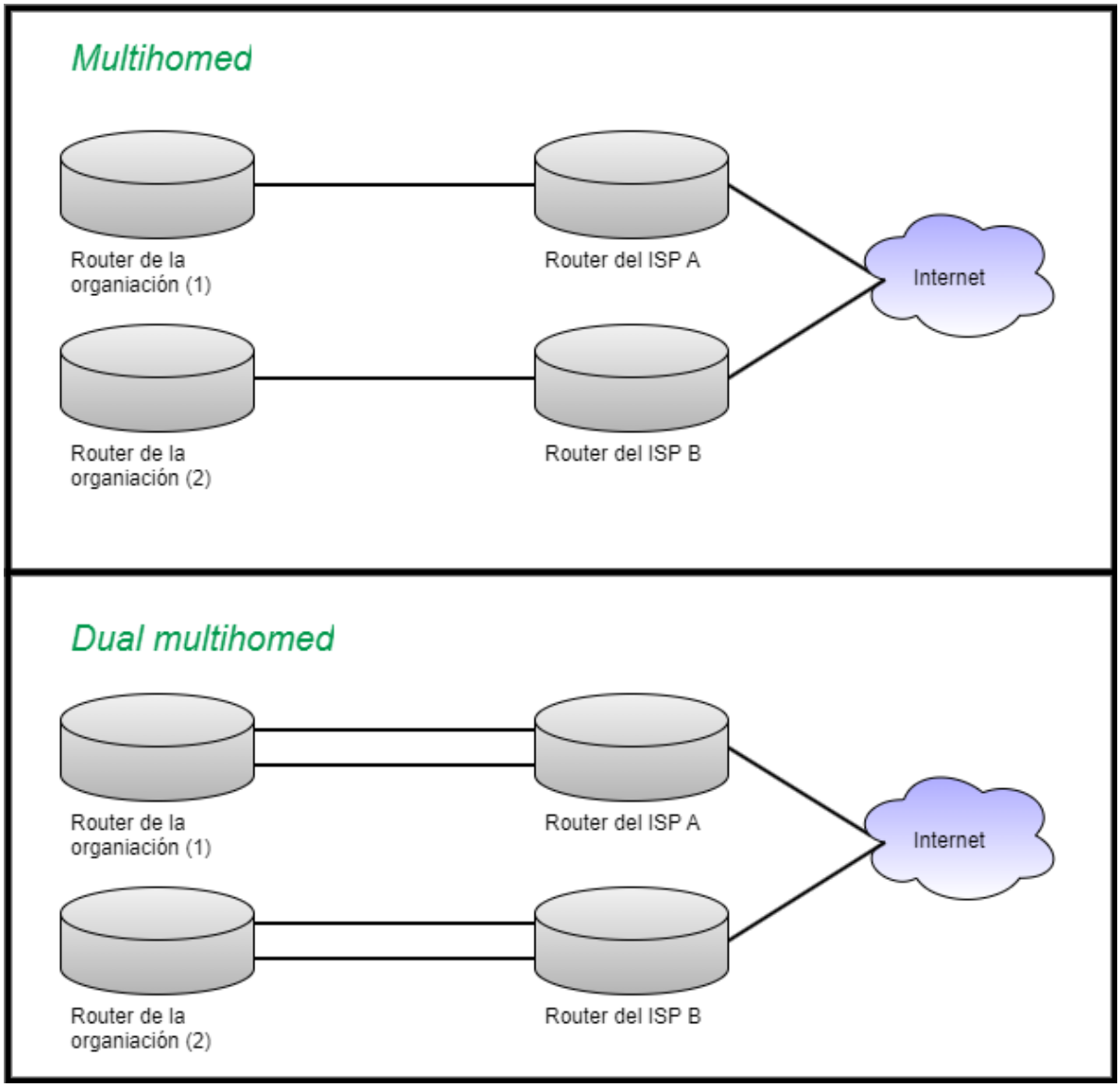


Figura 10: Conexiones a varios ISP. Fuente: Elaboración propia.

4.6.8. El área funcional remota

En esta zona se encuentran todos aquellos elementos ajenos a la propia sede central de la organización.

Como ejemplo, una sucursal de la empresa, que necesita conectarse a la sede central. Puede hacerlo mediante un enlace WAN propio o mediante Internet, utilizando, en este último caso, redes VPN para lograr la necesaria seguridad y privacidad de la conexión. Otro caso habitual es la existencia de teletrabajadores, que acceden a la red de la sede central a través de una VPN, utilizando su conexión a Internet.

Por último, se puede mencionar la posible existencia de un centro de datos remoto, fuera de la sede de la organización (lo cual es ventajoso para utilizarlo en recuperación ante desastres). Normalmente, el enlace se realiza a través de una red WAN.

4.7. Sistemas de detección de intrusiones (IDS)

Una intrusión se define como un intento de violación de las políticas de seguridad de un sistema, pudiendo afectar a la integridad de los datos contenidos en el mismo, a su confidencialidad (si agentes no deseados tienen acceso a los mismos) o a su disponibilidad (si los datos son destruidos o el acceso a ellos impedido).

Para el caso de una red empresarial, una intrusión sería el acceso desde una zona de la red a otra no autorizada, como un salto desde la zona desmilitarizada de servidores públicos a la red interna de la organización. También podría darse dentro de la propia red, por ejemplo, si un empleado accede con su equipo a una VLAN a la que no debería tener acceso (como puede ser la VLAN de gestión).

IDS

Un IDS, siglas en inglés de Sistema de Detección de Intrusiones, (Wikipedia, Sistema de detección de intrusos, 2023), consiste en un software especializado en la detección de accesos no autorizados a un sistema, normalmente basándose en una serie de reglas que pueden venir incluidas en el mismo o bien ser creadas por el propio administrador ocupado de su configuración.

Para detectar los ataques, el IDS suele tener un *sniffer* de paquetes que captura y analiza todo el tráfico de la red, buscando, principalmente, dos elementos:

- Comportamientos sospechosos que se puedan corresponder con un ataque, como pueden ser escaneos de puertos abiertos o paquetes repetidos, con violaciones del protocolo o muy fragmentados. Un IDS con este funcionamiento sería un **IDS basado en anomalías**.
- Contenido en los paquetes recibidos que satisfaga las normas de detección cargadas en el IDS, como pueden ser paquetes con una determinada dirección de origen o destino, o que se dirijan a un rango de puertos concreto. Los IDS con este comportamiento son los **basados en firmas**.

Lo normal es que un IDS no esté solo como mecanismo de seguridad, sino que se apoye en un cortafuegos que, directamente, descarte paquetes no deseados por su origen o sus características. Conviene resaltar, también, que un sistema de detección de intrusos puede utilizar, a la vez, detección basada en firmas y en anomalías.

Según el ámbito protegido, se pueden diferenciar dos tipos de IDS, (CheckPoint, 2023):

- **IDS basados en host**: Protegen a un solo equipo, buscando en el mismo signos que puedan corresponder con una intrusión y generando las alertas correspondientes. Lugares en los que el IDS puede buscar estos rastros de intrusión pueden ser la bitácora del sistema, la lista de procesos en ejecución o el historial del sistema de archivos.

- **IDS basados en red**: Protege toda una red mediante una interfaz configurada en modo promiscuo, de forma que puede analizar todos los paquetes en circulación.

Otra distinción que se puede realizar es entre sistemas pasivos, que solo avisan de posibles intrusiones, pero no las evitan; y sistemas reactivos, que sí son capaces de detener de forma automática un ataque y responden al nombre de Sistemas de **Prevención** de Intrusiones (IPS).

4.7.1. Técnicas de burla a un IDS

En el contexto actual de ciberseguridad, nunca se está lo suficientemente actualizado. A continuación, se exponen algunos métodos de burla de IDS conocidos, pero la lista no incluye, ni mucho menos, todos los que una organización puede tener que afrontar si está bajo ataque. De igual forma, algunos de estos métodos de evasión fueron efectivos en el pasado, pero no lo son con los sistemas actuales.

- **Ataque de ofuscación:** Consiste en enviar los paquetes de forma que el IDS no los pueda analizar, por ejemplo, cifrando la carga útil de los mismos.
- **Saturación del IDS:** Es una especie de ataque de denegación de servicio, en el cual se genera una enorme cantidad de paquetes maliciosos que el IDS deberá detectar, intentando producir en este una situación de bloqueo.
- **Fragmentación:** Si se fragmentan los paquetes, es posible que el IDS no los reconstruya y, por tanto, no los pueda analizar.
- **Ataque de TTL:** Si se genera un paquete con un tiempo de vida que solo le permita llegar hasta el IDS, este lo analizará, pero el paquete será descartado y no llegará al destino. Es posible que el IDS no analice dos paquetes si son iguales, con lo cual, si se vuelve a enviar el mismo paquete con el TTL correcto, puede que ahora sí llegue al destino sin que el IDS lo haya examinado.
- **Paquetes con *checksum* errónea:** Algunos IDS no comprobaban la integridad de los paquetes que analizaban. Así, por ejemplo, un atacante

podría enviar un paquete RST con suma de control errónea para cerrar una conexión, de forma que el IDS daría por finalizada la transmisión y no analizaría más paquetes, pero el destino mantendría la conexión abierta, pues el paquete no válido sería descartado.

Estas técnicas se han extraído del temario de la asignatura *Técnicas Avanzadas de Seguridad*, en concreto, de (Lucena López, 2022).

4.8. Snort

Snort, (Atico34, 2023), (Snort Team, 2020), es un sistema de detección de intrusos gratuito y de código abierto, actualmente mantenido por Cisco. Utiliza la biblioteca *libpcap* para capturar los paquetes que transitan por la red y proceder a su análisis, según las reglas definidas.

Snort es capaz de identificar ataques de denegación de servicio, desbordamiento de buffer o escaneos de puertos, entre otros. Dispone de tres modos de operación:

- **Modo *Sniffer*:** Sirve para ver todos los paquetes que circulan por la red, pudiendo guardar un registro.
- **Modo *Packet Logger*:** Se comporta igual que el modo *sniffer*, con la salvedad de que se guarda un registro de actividad, pudiéndose filtrar qué se guarda y qué no mediante reglas.
- **Modo NIDS:** Este modo de Sistema de Detección de Intrusiones basado en Red también se basa en la escucha de paquetes, pero, en este caso, se aplicarán las reglas de detección de instrucciones predefinidas y se lanzarán los avisos oportunos, según la configuración que se haya aplicado a Snort.

4.8.1. Componentes de Snort

- **Decodificador:** Forma los paquetes que serán analizados por el resto de componentes, teniendo en cuenta los protocolos utilizados y el tamaño de los datos, así como su ubicación dentro del paquete. El decodificador puede producir alertas en el caso de encontrar encabezados que no correspondan con las especificaciones del protocolo.
- **Preprocesadores:** Snort cuenta con varios de estos, normalmente uno por protocolo. Se ocupan de transformar los paquetes (por ejemplo, desfragmentándolos) para evitar que se pueda burlar el motor de detección. También se ocupan de detectar escaneos de puertos o ataques por suplantación ARP.
- **Motor de detección:** Aplica las reglas definidas para determinar si un paquete corresponde con una intrusión. En caso afirmativo, se toman acciones, también definidas en las reglas (como puede ser descartar los paquetes) y se registra la incidencia (si se disparan varias reglas, se registra la de mayor nivel de alerta).
- **Módulos de salida:** Controlan qué salidas ofrece Snort, como el registro de las incidencias en una base de datos o en el *syslog*, o la generación de informes.

4.8.2. Reglas de Snort

Snort ofrece una serie de reglas de forma gratuita que abarcan un amplio abanico de ataques, llamadas *Community Rules*. Entre ellas, se pueden encontrar reglas para evitar ataques basados en desbordamiento de buffer, ataques a servidores de correo, web o FTP, o actividad de malware conocido.

Sin embargo, el administrador del sistema puede crear las reglas que considere oportunas para adaptar SNORT a sus necesidades. Una regla se compone de dos partes:

- **Encabezado**: Define la acción a tomar cuando se dispare la regla, el protocolo del paquete, las direcciones IP de origen y destino y los números de

puerto, además de la dirección del tráfico. Los diferentes valores que puede tomar cada uno de los campos del encabezado se exponen a continuación:

- Para la **acción**, se puede optar por las siguientes alternativas:
  - ***alert***: Se genera un aviso y se registra el evento en la bitácora.
  - ***log***: Simplemente se registra el suceso en la bitácora.
  - ***pass***: Se ignora el disparo de la regla y se permite el paso del paquete.
  - ***drop***: Se impide que el paquete alcance su destino y se registra el incidente.
  - ***reject***: Adicionalmente a las acciones llevadas a cabo por la acción *drop*, ahora también se envía un *reset* si el protocolo es TCP o un paquete ICMP de destino inalcanzable si es UDP.
  - ***sdrop***: El paquete es bloqueado, pero no se registra el disparo de la regla en el log del sistema.
- En el caso del **protocolo**, están soportados UDP, TCP, IP e ICMP.
- Las **direcciones IP** se deben indicar en notación CIDR (salvo *any*, que indica *cualquier dirección* y no requiere nada más). Se pueden cubrir todas las direcciones de un rango simplemente colocando el identificador de red (por ejemplo, para cubrir las direcciones desde la 192.168.10.1 hasta la 192.168.10.255, se indica `192.168.10.0/24`).

  La última opción es incluir una lista de direcciones IP separadas por comas y sin espacios entre ellas. Por ejemplo: `[192.168.10.5/24,192.168.10.40/24]`.

  Adicionalmente, se puede hacer una negación con el operador *!*, de forma que la regla aplique a todas las direcciones IP a excepción de la indicada. Como muestra, `!192.168.10.10/24` filtrará todo lo que provenga de cualquier dirección, salvo esa. Ídem para las direcciones IP de destino. Esto también es extensible a rangos y listas de direcciones.

- Los **números de puerto**, además de con *any* para indicar cualquier puerto, se pueden expresar de diversas formas:
  - Como un único puerto, simplemente indicando el número.
  - Como un rango de puertos, colocando dos puntos (:) delante del número de puerto, como sigue:
    - Si se colocan de forma `aaa:bbb`, indica todos los puertos entre *aaa* y *bbb*, ambos incluidos.
    - Si se colocan a la izquierda de un puerto (`:aaa`), indica todos los puertos de número menor o igual que dicho puerto.
    - Extendiendo el punto anterior, colocándolos a la derecha de un número (`aaa:`), se indican todos los puertos mayores o iguales que el mismo.
  - Como una negación, de la misma forma que con las direcciones IP.
- El **indicador (u operador) de dirección del tráfico**, que simplemente permite diferenciar si el tráfico que puede hacer saltar la regla es unidireccional (->) o bidireccional (<>).

Un ejemplo de encabezado de regla es el siguiente:

```
alert tcp 192.168.1.10/24 23500 -> 192.168.1.54/24 25000
```

- La acción sería *alert*.
- El protocolo de la capa de transporte es TCP.
- La dirección IP de origen es 192.168.1.10, con máscara de red 255.255.255.0.
- El número de puerto de origen es 23500.
- La dirección IP de destino es 192.168.1.54, con la misma máscara que la de origen.
- El puerto de destino es el 25000.
- El tráfico solo es analizado desde el origen al destino y no al contrario (para ello, el operador de dirección debería ser <>).

- **Opciones de regla**: Se colocan entre paréntesis. Una misma regla puede tener varias opciones, que se separan con un punto y coma y pueden ser de cuatro tipos:

    - Opciones generales: Ofrecen información sobre la regla, sin interferir en la detección.

      Como ejemplos de opciones generales, se pueden mencionar ***msg*** (determina el mensaje con el que se debe registrar la alerta), ***reference*** (permite incluir referencias a otros sistemas de detección de ataques), ***sid*** (identifica de forma única una regla de Snort) o ***classtype*** (asocia una clase a la regla, lo cual es útil para organizar las reglas según su finalidad).

    - Opciones de carga útil: Definen el contenido que Snort debe buscar en la carga útil de los paquetes analizados para que se dispare la regla.

      La opción de carga útil más importante es ***content***, que indica el contenido del paquete que hará saltar la regla, pudiendo ser cadenas de texto o binarios (expresados en hexadecimal). A su vez, esta opción tiene muchos modificadores -que también son, realmente, opciones de carga útil-, como ***rawbytes***, que hace que Snort busque en el contenido en bruto del paquete, ignorando las posibles transformaciones que los preprocesadores hayan hecho al mismo; o ***distance***, que indica a partir de qué punto empezar a buscar el contenido indicado.

    - Opciones fuera de la carga útil: Snort también puede buscar indicios de intrusión fuera de la carga útil de los paquetes, si se definen estas opciones.

      En este caso también se dispone de un gran abanico de posibilidades, como ***fragoffset*** (compara el desplazamiento indicado en un paquete IP con un valor indicado), ***ttl*** (comprueba el tiempo de vida del paquete

recibido) o ***ipopts*** (indica a Snort que busque alguna opción IP en específico, como el registro de ruta o la marca de tiempo).

- Opciones de post detección: Especifican qué acciones debe llevar a cabo Snort cuando se dispare la regla. Como ejemplos, ***logto*** (determina en qué archivo de registro almacenar los disparos de la regla), ***session*** (extrae los datos de los segmentos TCP) o ***react*** (genera una respuesta activa al disparo de la regla, como puede ser el cierre de la conexión, notificando al otro participante).

Extendiendo el ejemplo del encabezado de regla propuesto anteriormente, se puede obtener la siguiente regla completa:

```
alert tcp 192.168.1.10/24 23500 -> 192.168.1.54/24 25000 (content: "inseguro";sid:1001;)
```

Se ha utilizado la opción de carga útil *content*, para que la regla se dispare cuando el contenido de los paquetes contenga la palabra "inseguro".

Un aspecto a tener en cuenta es que, en la actualidad, es muy común (y recomendable) utilizar comunicaciones cifradas. Así, por ejemplo, la enorme mayoría de webs utilizan el protocolo HTTPS, cifrando los datos que se intercambian entre el navegador y el servidor; también es común encontrar SSH en lugar de Telnet, o SFTP en lugar de FTP. El problema, para Snort, es que esto dificulta enormemente su labor, pues no puede analizar la carga útil de los paquetes, debiendo decantarse por otras opciones, como el tamaño de los mismos, el protocolo o las direcciones de origen y destino, lo cual puede originar más falsos positivos (y también falsos negativos, es decir, paquetes maliciosos que no disparan ninguna regla) de los deseables.

Es importante destacar que este capítulo no pretende ser un manual de Snort, con lo que solo se han mencionado algunas opciones del mismo a modo de referencia, debiéndose acudir a la documentación oficial referenciada en la

bibliografía si se desea obtener más información. También se ha empleado (Ramiro, 2020).

4.8.3. Niveles de amenaza

A la hora de determinar la gravedad de las posibles intrusiones detectadas por Snort, se puede hablar de tres niveles de amenaza, (Ramiro, 2020):

- **Equipos comprometidos:** En la red existen host con malware instalado o en manos de usuarios maliciosos, con lo que se debe actuar a la mayor brevedad posible.
- **Políticas de seguridad infringidas:** Es posible que los usuarios utilicen aplicaciones no permitidas, o que intenten conectarse a servidores prohibidos. Al detectar estas amenazas, se deberán tomar las medidas oportunas con dichos usuarios de la red porque, si bien es posible que el riesgo para la seguridad de la misma no sea inminente, sí es potencial.
- **Análisis de puertos o ataques:** Es posible que detectemos a un atacante intentando encontrar puertos abiertos en el cortafuegos de la red, o tratando de llevar a cabo un ataque de denegación de servicio. Según el contexto, puede ser conveniente tomar acciones (como bloquear todas las peticiones hacia un servidor provenientes de determinadas direcciones IP).

4.8.4. Falsos positivos

Un falso positivo sucede cuando se dispara indebidamente una regla, generando una alerta sobre una posible intrusión que, en realidad, no existe. Son un problema habitual en el software de seguridad, sea este un IDS, un antivirus, un cortafuegos…

Hay que intentar reducir la tasa de falsos positivos, pues, por una parte, se puede llegar a saturar el IDS y a hacer que los archivos de bitácora ocupen más espacio del esperable. Por otra parte, tener demasiadas falsas alarmas puede generar desconfianza en el IDS, haciendo que los administradores de la red comiencen a ignorarlas y llevando a una situación en la que, probablemente, no se

reaccione a tiempo ante una intrusión real por la falta de confianza que se tiene en el sistema.

Algunos ajustes que se pueden hacer para tratar de reducir al mínimo la tasa de falsos positivos son:

- Eliminar aquellas reglas que, por las características de la red, no sean relevantes.
- Las reglas que se mantengan, deberán refinarse y restringirse todo lo posible. Por ejemplo, cambiando un rango de direcciones IP por una lista de direcciones concretas más pequeña.
- Colocar un cortafuegos delante del equipo que ejecuta Snort, de forma que muchos paquetes malintencionados sean descartados sin que ni siquiera tengan que ser analizados por el IDS.
- Aprovechar los preprocesadores para normalizar los paquetes (por ejemplo, eliminando de los mismos secuencias de escape que, eventualmente, pudieran disparar alguna regla).

4.8.5. Reglas preinstaladas

Estas reglas se ofrecen de forma gratuita, por lo que son un buen punto de partida. Algunos tipos de reglas que includas se mencionan a continuación.

- **Reglas P2P**: En principio, están destinadas a la detección de diferentes tipos de tráfico generados por las aplicaciones de intercambio de archivos, como pueden ser BitTorrent o Emule (siendo más efectivas las reglas para el primero que para el segundo, pues, en este último, se basan en cadenas muy cortas que generan gran cantidad de falsos positivos).

  Un problema que sufren estas reglas ya se ha comentado anteriormente, y es que el tráfico suele ir cifrado, con lo que su efectividad se ve claramente disminuida.

- **Equipos comprometidos y software indeseado**: Algunas reglas preinstaladas son capaces de detectar signos de equipos infectados con malware, pero también de detectar software que, si bien no encaja estrictamente en la definición de malware, sí es indeseado por lo molesto que puede llegar a resultar (por ejemplo, *adware*).
- **Detección de ataques**: Son reglas genéricas que pueden indicar que la organización se encuentra ante un ataque, si bien algunas son demasiado simples (por ejemplo, el acceso a determinadas Webs o la recepción de enlaces por aplicaciones de mensajería) como para ser significativas.
- También las hay para detectar ataques web, analizando cadenas de contenido, pero, por un lado, TLS impide su operación y, por otro lado, son bastante susceptibles a falsos positivos.

Instalando Snort, se pueden ver todas las reglas que trae preinstaladas listando el directorio correspondiente (en GNU/Linux, **/etc/snort/rules**):

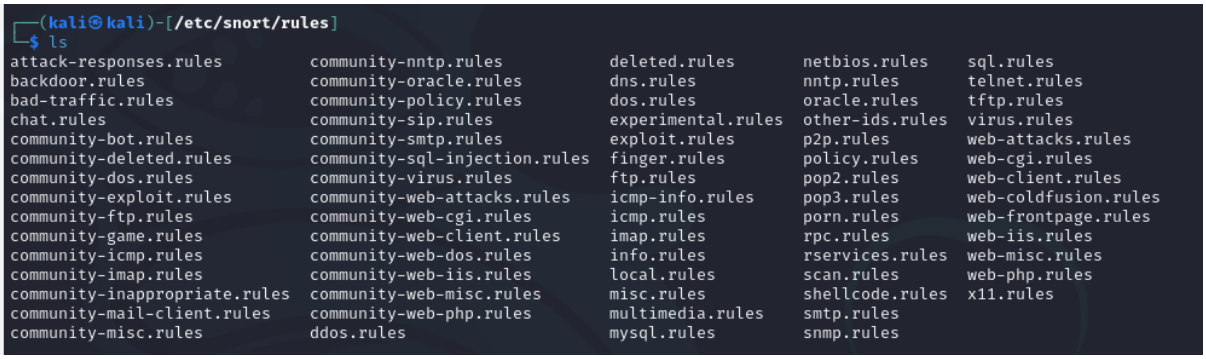


Figura 11: Contenido del directorio */etc/snort/rules* tras la instalación del programa en una máquina virtual de Kali Linux

4.9. Protocolo SNMP

En el presente trabajo, se complementará el IDS con la capacidad de lanzar mensajes SNMP cuando se detecte una intrusión, por ejemplo, para desconectar un puerto del switch.

SNMP, siglas en inglés de Protocolo Simple de Administración de Red [(Stallings, Comunicaciones y Redes de Computadores, 2004), (Paessler AG, 2023), (Manage Engine, 2023)], permite monitorizar y controlar todos los

componentes de una red de forma centralizada. Suele estar soportado por dispositivos como routers, switches o impresoras.

Para su funcionamiento, se basa en un escenario agente-gestor. El gestor es el que supervisa y controla el resto de dispositivos de la red, mientras que el agente (que es un proceso que se ejecuta en cada uno de los dispositivos supervisados) se ocupa de recopilar los datos del dispositivo y enviarlos al gestor. De esta forma, se pueden diferenciar tres componentes en una red administrada mediante SNMP:

- **Sistema administrador de red:** Es el gestor, ocupado de la administración del resto de dispositivos. Lo más común es que haya uno solo, pero podría haber varios.
- **Dispositivos administrados:** Contienen la información de la red y la ponen a disposición del gestor.
- **Agente:** Software en ejecución en cada uno de los dispositivos administrados, encargado de organizar la información y enviarla en el formato definido por SNMP.

Se diferencian tres versiones de SNMP. La primera, SNMPv1, posee una cadena de comunidad (que es el ID que permite el acceso a los datos de los dispositivos y se envía junto a los mensajes) como única medida de seguridad, poco efectiva, pues se transmite en texto claro.

La segunda versión (SNMPv2) introdujo la cadena de comunidad cifrada, comandos SET mejorados y los tipos de mensajes GETBULK e INFORM, que se definen a continuación.

Por último, la tercera versión, SNMPv3, se centra en la seguridad, utilizando identificación mediante usuario y contraseña en lugar de una cadena de comunidad. También permite cifrar los mensajes completos, de forma que se tienen tres alternativas de niveles de seguridad:

- **noAuthNoPriv:** Los mensajes ni se autentifican ni se cifran, empleándose solo un nombre de usuario para la identificación.

- **authNoPriv:** Los mensajes se autentifican, usándose identificación por usuario y contraseña, pero no se cifran.
- **authPriv:** Los mensajes se cifran y autentifican.

Mediante SNMP se pueden intercambiar site tipos diferentes de mensajes:

- **Solicitud GET:** Recuperan un dato de un dispositivo de red.
- **Solicitud GETNEXT:** Se utiliza para recuperar un registro a continuación de otro. Es útil para la lectura de tablas.
- **Solicitud GETBULK:** Soportada a partir de la versión 2 del protocolo SNMP, permite obtener con una sola solicitud un número determinado de datos, sin tener que hacer varias solicitudes GETNEXT.
- **Solicitud SET:** Permite establecer un parámetro en uno de los dispositivos, como puede ser una dirección IP.
- **Respuesta GET:** Mensaje dado por un dispositivo supervisado como respuesta a una solicitud.
- **Trampa SNMP:** Mensajes enviados por los dispositivos supervisados hacia el sistema administrador sin que este lo solicite. Se emplean para dar avisos sobre situaciones no previstas.
- **Solicitud INFORM:** Tienen el mismo objetivo que las trampas, pero el administrador debe confirmar su recepción.

Para el intercambio de mensajes se emplea el protocolo UDP de la capa de transporte, usando el puerto 161 (162 en el caso de las trampas).

Los dispositivos administrados se localizan por su OID (identificador de objetos), que se introduce en una base de datos llamada MIB (base de información gestionada). En dicha base de datos, se diferencian dos tipos de objetos:

- Tabulares, en los que un mismo OID puede devolver varios resultados, pues el OID define varias instancias relacionadas de un objeto. Puede ocurrir, por ejemplo, si se está supervisando una CPU de varios núcleos.

- Escalares, en los que un OID identifica de forma unívoca una instancia de un objeto, como un switch.

En la siguiente imagen se presenta la estructura de una base MIB:

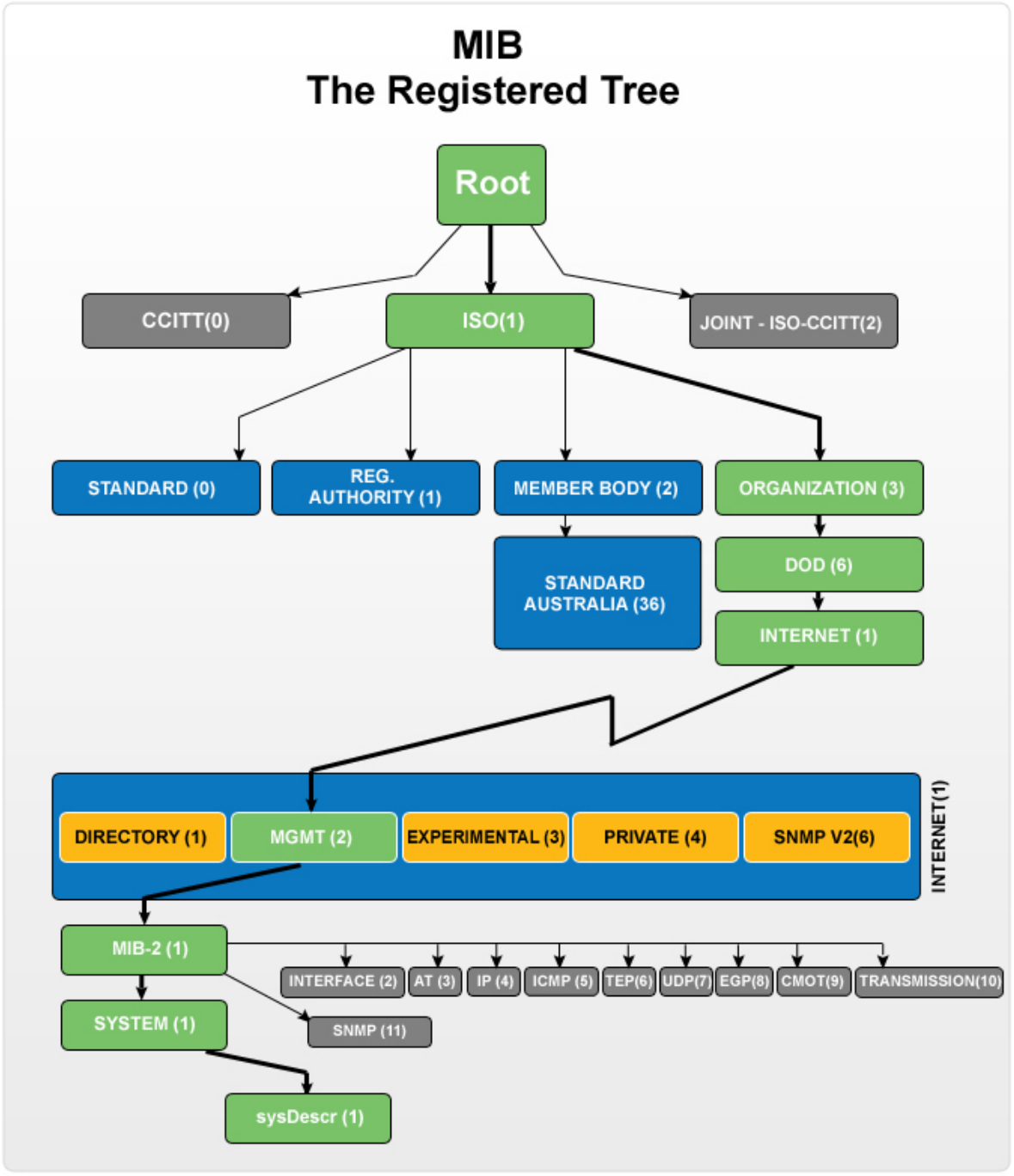


Figura 12: Árbol MIB. Fuente: (Manage Engine, 2023)

Un OID se describe mediante enteros separados por un punto. Por ejemplo, para llegar al nodo SNMP en la base MIB anterior, se usaría el OID **.1.3.6.1.2.1.11**.

5. Diseño de la red de la organización

La red propuesta para el presente proyecto consta de una sede central de la organización, dos sedes remotas más pequeñas y teletrabajadores que deben conectarse de forma segura a la sede central.

A modo introductorio, se puede representar la red a diseñar como sigue:

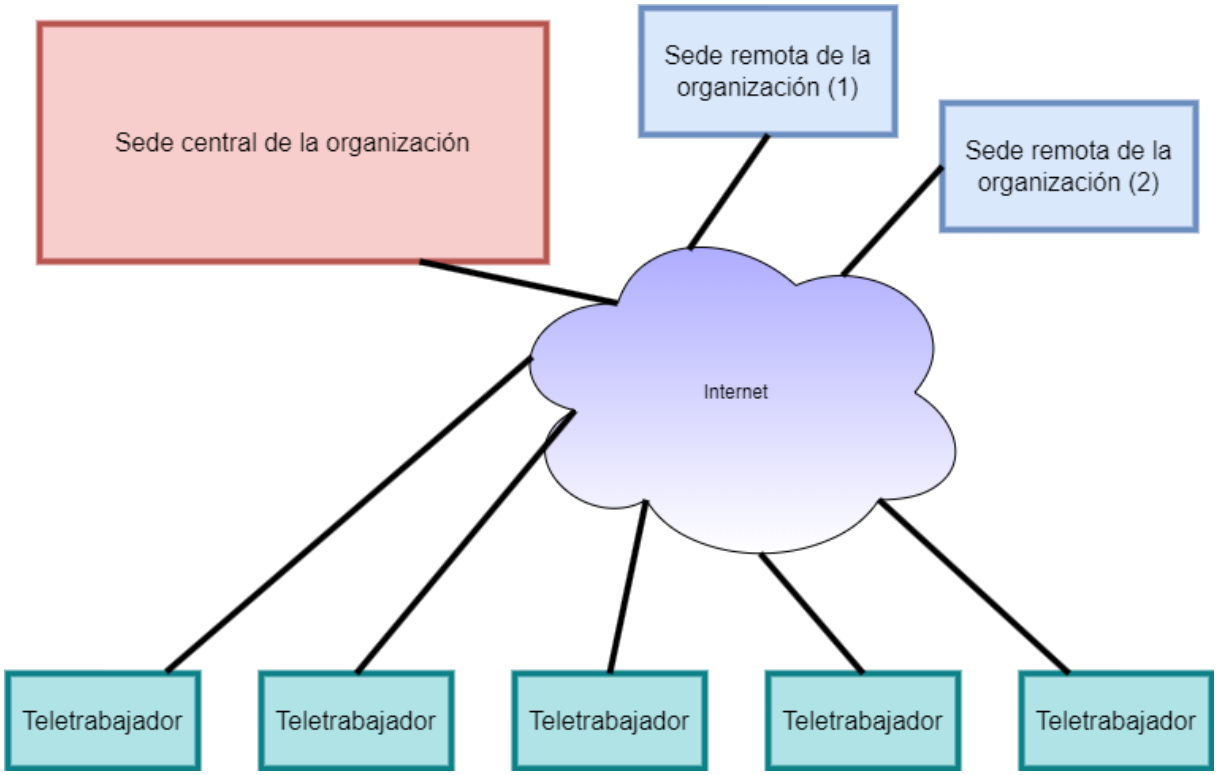


Figura 13: Diseño introductorio de la red

Como se muestra, las conexiones entre las sedes remotas y la sede central y entre los teletrabajadores y la sede central se realizan a través de Internet, lo cual exige el uso de redes privadas virtuales que proporcionen la necesaria seguridad a las comunicaciones.

En los siguientes apartados se presenta el diseño detallado de cada una de las partes de la red empresarial.

5.1. Diseño de la sede central

La sede principal de la organización dispondrá de tres tipos de equipos conectados:

- Empleados, divididos a su vez en:
  - Programación
  - Comerciales
- Equipos del departamento de sistemas.
- Clientes e invitados.

Además de estos equipos finales, existirán:

- Una zona desmilitarizada (DMZ), con un servidor web accesible desde Internet.
- Un centro de datos, solo accesible para los miembros de la organización (es decir, programadores, comerciales y sistemas).

Como se comentó en el Estado del Arte, el diseño elegido será una red jerárquica de núcleo colapsado, dado que el número de usuarios de la misma no justifica una red jerárquica de tres niveles.

En cuanto a la conexión a Internet de la sede, se empleará un modelo *single-homed*, con una única conexión a un proveedor de servicios de Internet.

5.1.1. Requisitos de seguridad

Como en toda red, la seguridad y el control de las comunicaciones es imprescindible. Por ello, se exponen los requisitos de seguridad de esta sede central:

- Los empleados solo pueden comunicarse con otros empleados de su mismo tipo, así como con los servidores ubicados en el centro de datos. Es decir, los programadores podrán comunicarse directamente con los equipos de otros programadores, pero no con los equipos de los comerciales; y viceversa.

En este punto, se debe tener en cuenta que en la sede remota también habrá empleados que deberán poder comunicarse con los de esta sede -con las mismas restricciones ya impuestas-, así como con el centro de datos.

- Los equipos pertenecientes al departamento de sistemas serán los únicos con acceso a la configuración de los dispositivos de red y solo podrán comunicarse con otros equipos del mismo departamento y con los ubicados en el centro de datos.
- Los dispositivos de los invitados y clientes no tendrán acceso a otros dispositivos de la red (ni siquiera a los de otros invitados, por razones de seguridad, al ser equipos cuya seguridad no es comprobable por la organización).
- Desde los servidores ubicados en la DMZ tampoco se podrá acceder a ningún otro equipo en la red.
- Desde los servidores ubicados en el centro de datos tampoco debe ser posible acceder al resto de equipos de la organización.

Estos requisitos de seguridad se traducen en la configuración de redes VLAN para cada división en la red, además de un cortafuegos o una lista de control de acceso (ACL) para que los dispositivos del personal ajeno a la organización (invitados y clientes) estén aislados entre sí. Por supuesto, será necesaria la configuración de VPN, aunque estas se comentarán más adelante.

Además de todo lo ya expuesto, en esta sede central se colocará un sistema de detección de intrusiones (IDS), que se ubicará directamente conectado al switch Core, pues es la mejor ubicación para poder filtrar el tráfico entrante y saliente de la red. Si se colocase en uno de los switch de acceso, habría una gran cantidad de tráfico que no podría analizar y, si se colocase directamente conectado al router de la organización, el tráfico local pasaría desapercibido para el sistema.

El diseño de esta sede central se muestra en la siguiente imagen:

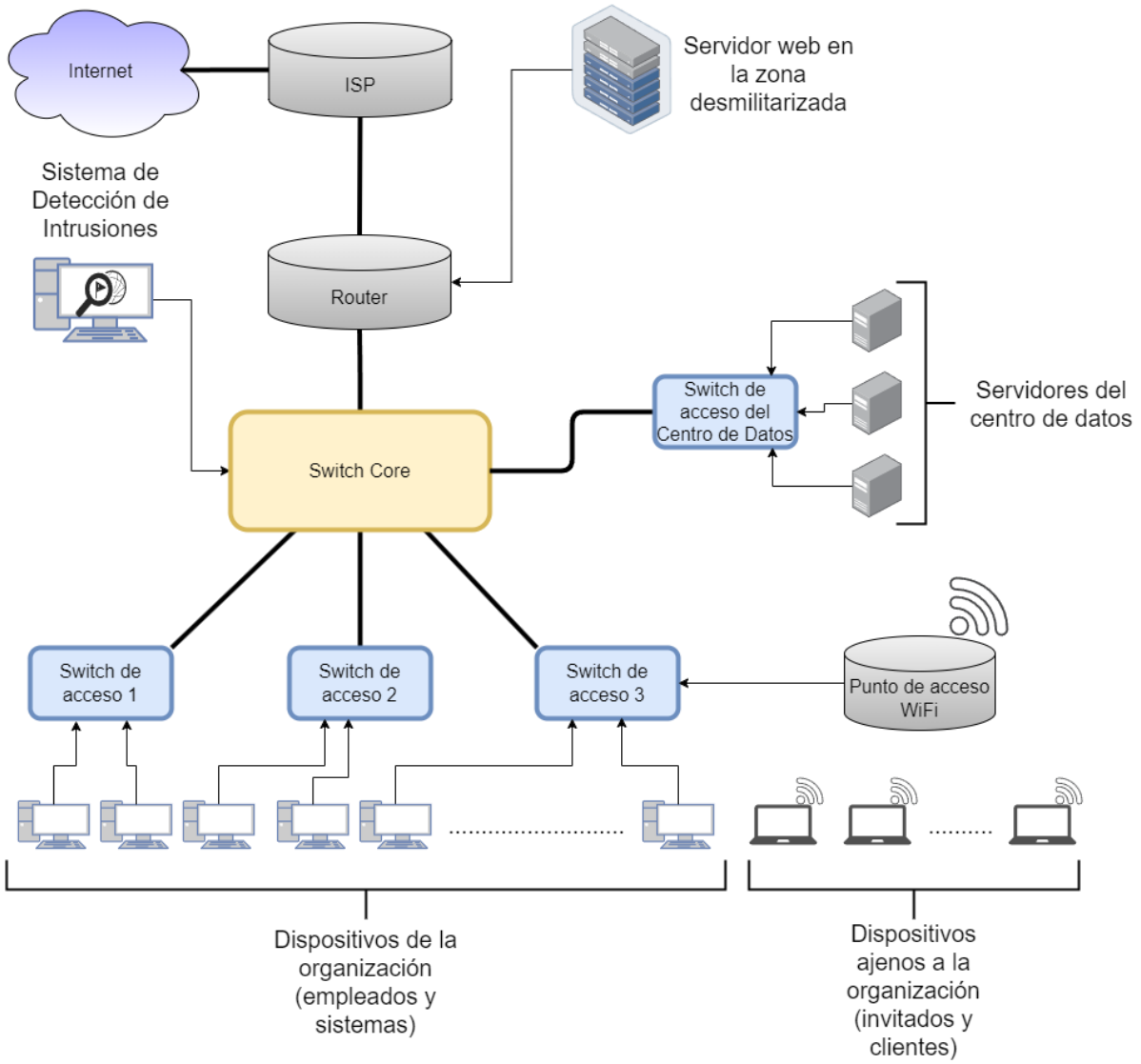


Figura 14: Diseño de la sede central de la organización

Para la separación de las diferentes zonas de la red es necesario configurar las siguientes VLAN:

- VLAN de gestión, en la que se ubicarán los equipos del departamento de sistemas y la única que tiene acceso a la configuración de los equipos de comunicaciones (VLAN 1).
- VLAN para programadores (VLAN 2).

- VLAN para comerciales (VLAN 3).
- VLAN para el centro de datos (VLAN 4).
- VLAN para la zona desmilitarizada (VLAN 5).
- VLAN para el IDS (VLAN 6).
- VLAN para dispositivos ajenos a la organización (VLAN 7).

Estas VLAN deben configurarse en los switches de acceso, en el switch Core y en el router que da acceso a Internet.

No todas estas VLAN deben estar aisladas, sino que habrá que activar la interconexión (VLAN *Internetworking* en equipos de Cisco) en el caso del centro de datos, programación, comerciales y sistemas, para que los equipos en dichas VLAN tengan acceso al primero. De esta forma, el aislamiento entre las VLAN de los distintos tipos de empleados deberá realizarse mediante ACL.

Por otra parte, para que el IDS sea capaz de analizar todo el tráfico de la red, será necesario interconectar su VLAN con todas las demás.

Si se piensa que el número de dispositivos en algunas VLAN puede ser muy grande, una buena opción es decantarse por una red con 16 bits para el identificador de red y 16 bits para el dispositivo (esto es, máscara de red 255.255.0.0). En consecuencia, se puede considerar la red **192.168.0.0/16**, donde el reparto de direcciones IP entre las VLAN quedaría como sigue:

- 192.168.0.0/19 para la VLAN 1.
- 192.168.32.0/19 para la VLAN 2.
- 192.168.64.0/19 para la VLAN 3.
- 192.168.96.0/19 para la VLAN 4.
- 192.168.128.0/19 para la VLAN 5.
- 192.168.160.0/19 para la VLAN 6.
- 192.168.192.0/19 para la VLAN 7.

Si el número de dispositivos en cada VLAN no se espera demasiado grande, se puede hacer con una red con máscara 255.255.255.0, por ejemplo, con la red 192.168.1.0/24, tal como sigue:

- 192.168.1.0/27 para la VLAN 1.
- 192.168.1.32/27 para la VLAN 2.
- 192.168.1.64/27 para la VLAN 3.
- 192.168.1.96/27 para la VLAN 4.
- 192.168.1.128/27 para la VLAN 5.
- 192.168.1.160/27 para la VLAN 6.
- 192.168.1.192/27 para la VLAN 7.

Con la primera opción, quedan 2^{13} - 2 direcciones disponibles para dispositivos, pudiendo conectar hasta 8190 dispositivos por VLAN. Con la segunda, por el contrario, solo se pueden direccionar 2^5 - 2 dispositivos por VLAN, esto es, 30 dispositivos.

En la red que se está diseñando, y dado que no se está considerando una gran organización, **será más que suficiente con la segunda opción**.

Por último, los servidores web en la zona desmilitarizada deberán ubicarse entre dos cortafuegos. Uno de ellos filtrará indeseado desde el exterior hacia los servidores y, el otro, evitará que un posible atacante consiga saltar desde la DMZ al resto de la red.

5.2. Diseño de las sedes remotas

En las sedes remotas solo hay tres tipos de dispositivos: sistemas, programadores y comerciales. En estos casos, el diseño de la red es más sencillo, no necesitando hacer diferenciación entre las capas de acceso y central, como se muestra en la siguiente ilustración:

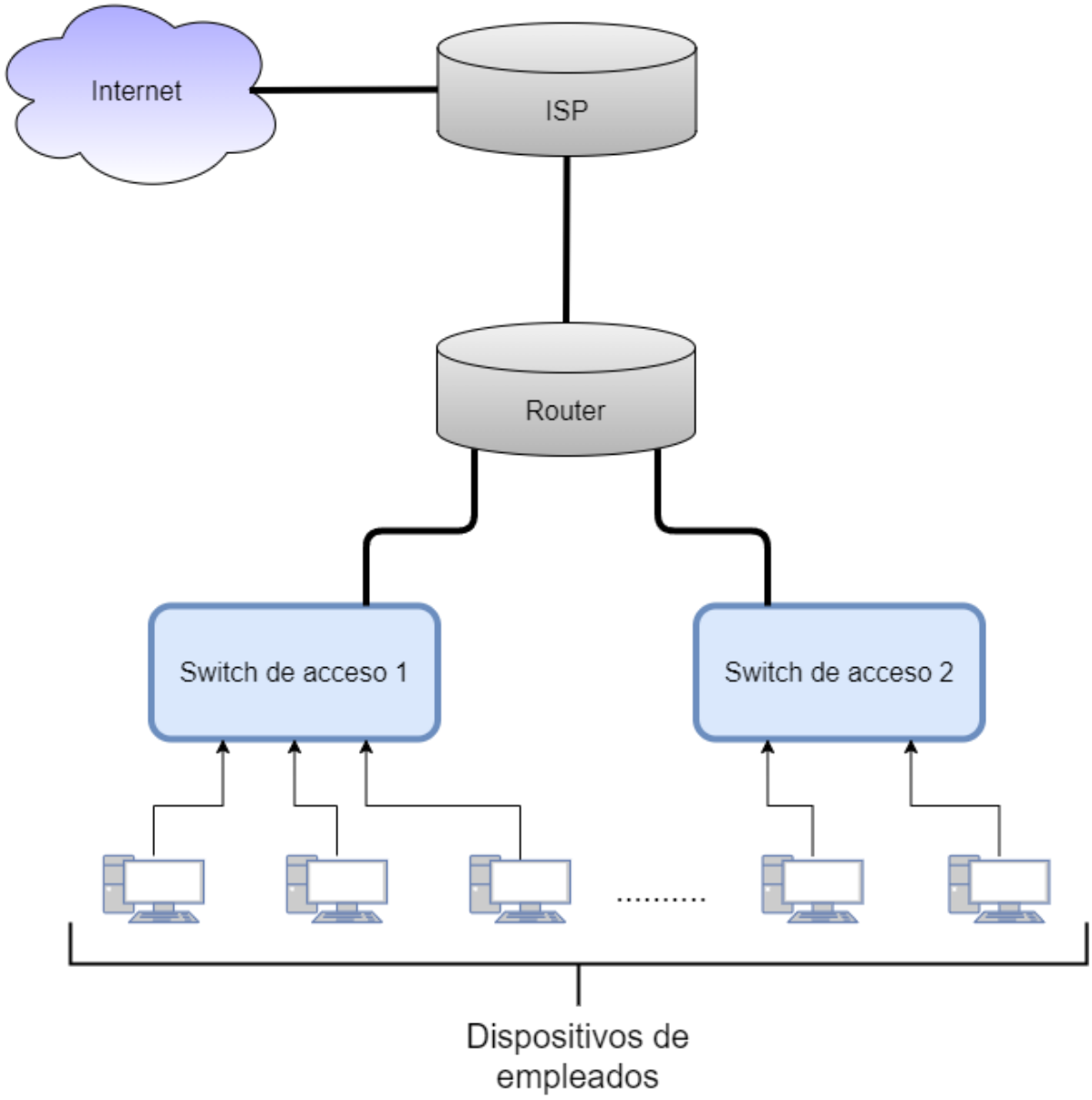


Figura 15. Diseño de las sedes remotas de la organización

El requisito de seguridad es que los tres tipos de dispositivos estén aislados entre sí y que solo desde los equipos del departamento de sistemas se pueda acceder a la configuración de los sistemas de comunicaciones.

En estas sedes tendremos que configurar tres VLAN, en los switches y en el router:

- VLAN de gestión, donde estarán los equipos de sistemas y desde la que se podrá acceder a la configuración de los sistemas de red (VLAN 1).

- VLAN de programadores (VLAN 2).
- VLAN de comerciales (VLAN 3).

Así pues, basta con 2 bits para identificar cada VLAN.

Dado que el número de dispositivos en estas dos sedes no va a ser especialmente grande, la red se basará en una máscara 255.255.255.0. Por ejemplo, se puede emplear la red **192.168.10.0/24 para la sede remota 1** y la red **192.168.20.0/24 para la sede remota 2**. Así, el reparto de direcciones IP en cada VLAN quedaría de la siguiente forma:

SEDE REMOTA 1

- 192.168.10.0/26 para la VLAN 1.
- 192.168.10.64/26 para la VLAN 2.
- 192.168.10.128/26 para la VLAN 3.

SEDE REMOTA 2

- 192.168.20.0/26 para la VLAN 1.
- 192.168.20.64/26 para la VLAN 2.
- 192.168.20.128/26 para la VLAN 3.

Con esta división, se tienen 2^6 - 2 direcciones válidas por VLAN, es decir, hasta 62 dispositivos, más que suficiente.

5.3. Diseño de las redes privadas virtuales (VPN)

Para conectar las diferentes sedes de la empresa y los teletrabajadores a la sede central, se requiere de conexiones de red privada virtual que proporcionen seguridad y autentificación a dichas conexiones. Con estos requisitos, las VPN serán de tipo IPSec ESP + AH, combinando las cabeceras de autentificación y cifrado.

Analizando la red antes diseñada, junto con sus requisitos, se observa que son necesarias las siguientes VPN:

- Dos *Site to Site* para conectar la VLAN de gestión de la sede central con la VLAN de gestión de cada sede remota. Serán las VPN 1 y 2.
- Dos *Site to Site* para conectar la VLAN de programadores de la sede central con la VLAN de programadores de las sedes remotas. Serán las VPN 3 y 4.
- Dos *Site to Site* que conecten la VLAN de comerciales de la sede central con las VLAN de comerciales en las sedes remotas. Serán las VPN 5 y 6.
- Cada teletrabajador tendrá una VPN *Client to Site* que le permitirá acceder a la VLAN de la sede central que le corresponda (comercial o programador). Serán las VPN 7 en adelante.

Así pues, se definen las VPN requeridas en la siguiente tabla:

VPN	**Equipos donde se configura**	**Modo**	**Protocolo**	**Objetivos**
1	Router de la sede central y router de la sede remota 1.	Túnel	IPSec ESP + AH	Conectar dos VLAN, en concreto, la VLAN de gestión de la sede central con la VLAN de gestión de la sede remota 1.
2	Router de la sede central y router de la sede remota 2.	Túnel	IPSec ESP + AH	Conectar dos VLAN, en concreto, la VLAN de gestión de la sede central con la VLAN de gestión de la sede remota 2.

3	Router de la sede central y router de la sede remota 1.	Túnel	IPSec ESP + AH	Conectar dos VLAN, en concreto, la VLAN de programadores de la sede central con la VLAN de programadores de la sede remota 1.
4	Router de la sede central y router de la sede remota 2.	Túnel	IPSec ESP + AH	Conectar dos VLAN, en concreto, la VLAN de programadores de la sede central con la VLAN de programadores de la sede remota 2.
5	Router de la sede central y router de la sede remota 1.	Túnel	IPSec ESP + AH	Conectar dos VLAN, en concreto, la VLAN de comerciales de la sede central con la VLAN de comerciales de la sede remota 1.
6	Router de la sede central y router de la sede remota 2.	Túnel	IPSec ESP + AH	Conectar dos VLAN, en concreto, la VLAN de comerciales de la sede central con la VLAN de comerciales de la sede remota 2.

7	Dispositivo del teletrabajador y router de la sede central.	Transporte	IPSec ESP + AH, combinado con L2TP.	Conectar un dispositivo (del teletrabajador) con una VLAN (la de programadores o la de comerciales)

Tabla 1. Características de las VPN necesarias

6. Montaje de una parte de la red

Teniendo prestados del laboratorio un router Cisco RV320 y un switch Cisco SG-300, se procede a montar una pequeña parte de la red, poniendo el foco, principalmente, en la parte de seguridad, combinando Snort con SNMP.

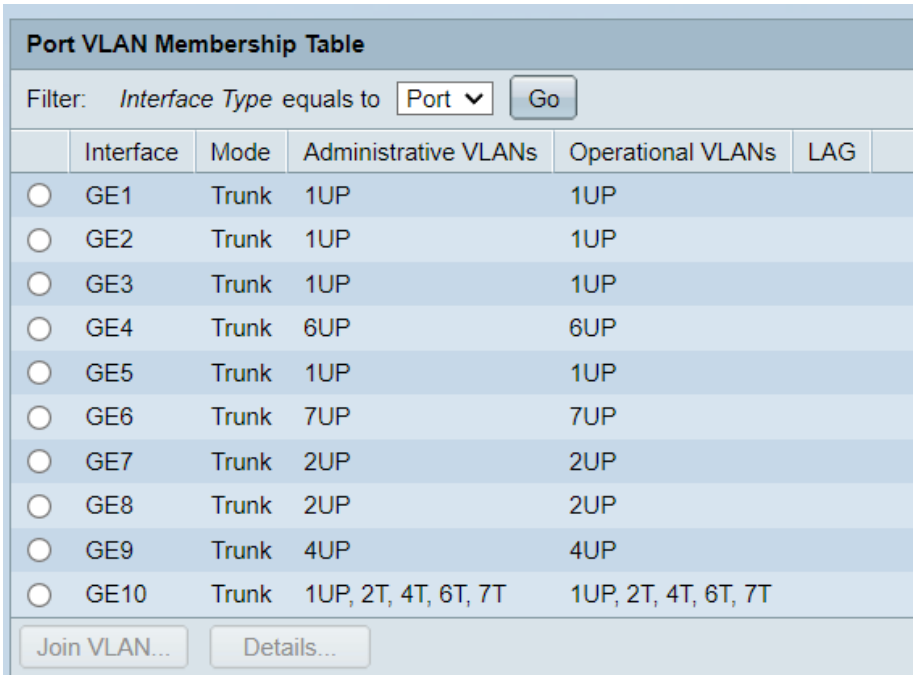
6.1. Definición de las VLAN

En el switch, se han definido las siguientes VLAN (intentando respetar, en lo posible, la numeración propuesta en el diseño de la sede central):

- VLAN 1: VLAN por defecto y desde la que se puede acceder a la configuración de los dispositivos de red.
- VLAN 2: Asociada a los puertos 7 y 8, sin etiquetar, corresponderá a los equipos de Programación, es decir, propios de la organización.
- VLAN 4: Asociada al puerto 9 y sin etiquetar, será usada por el equipo que representa el centro de datos interno de la organización.
- VLAN 6: La asociamos al puerto 4, también sin etiquetar. A ella se conectará el IDS.
- VLAN 7: Asociada al puerto 6, no etiquetada, corresponde a los dispositivos ajenos a la organización.

En el puerto 10 del switch, que es con el que se hace la conexión al puerto LAN 1 del router, se realiza la agregación de todas las VLAN, de forma que solo la VLAN

1 va sin etiquetar. A continuación, se muestra una captura de pantalla de la configuración de las VLAN en el switch:



Port VLAN Membership Table

Filter: *Interface Type* equals to Port Go

	Interface	Mode	Administrative VLANs	Operational VLANs	LAG
○	GE1	Trunk	1UP	1UP	
○	GE2	Trunk	1UP	1UP	
○	GE3	Trunk	1UP	1UP	
○	GE4	Trunk	6UP	6UP	
○	GE5	Trunk	1UP	1UP	
○	GE6	Trunk	7UP	7UP	
○	GE7	Trunk	2UP	2UP	
○	GE8	Trunk	2UP	2UP	
○	GE9	Trunk	4UP	4UP	
○	GE10	Trunk	1UP, 2T, 4T, 6T, 7T	1UP, 2T, 4T, 6T, 7T	

Join VLAN... Details...

Figura 16: Configuración de las VLAN en el Switch Cisco SG-300

De la misma forma, esta configuración se ha extendido a las VLAN configuradas en el router Cisco RV320, como se puede ver en la siguiente captura de pantalla:

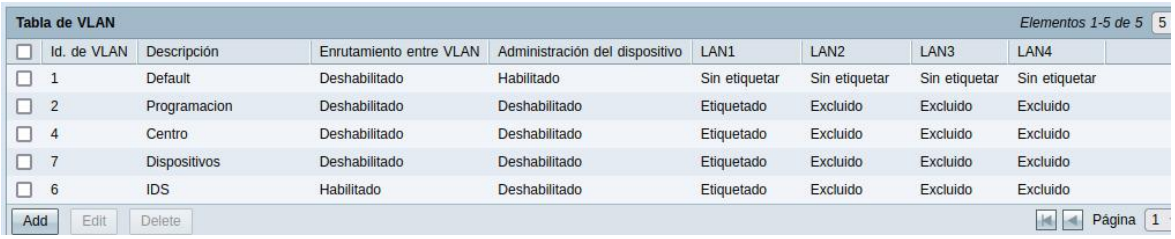


Tabla de VLAN *Elementos 1-5 de 5* 5

	Id. de VLAN	Descripción	Enrutamiento entre VLAN	Administración del dispositivo	LAN1	LAN2	LAN3	LAN4
☐	1	Default	Deshabilitado	Habilitado	Sin etiquetar	Sin etiquetar	Sin etiquetar	Sin etiquetar
☐	2	Programacion	Deshabilitado	Deshabilitado	Etiquetado	Excluido	Excluido	Excluido
☐	4	Centro	Deshabilitado	Deshabilitado	Etiquetado	Excluido	Excluido	Excluido
☐	7	Dispositivos	Deshabilitado	Deshabilitado	Etiquetado	Excluido	Excluido	Excluido
☐	6	IDS	Habilitado	Deshabilitado	Etiquetado	Excluido	Excluido	Excluido

Add Edit Delete Página 1

Figura 17: Configuración de las VLAN en el Router Cisco RV320

Es importante el detalle de que, para la VLAN donde se ubica el IDS, se ha activado el enrutamiento entre VLAN (*VLAN Internetworking*). No obstante, como se verá más adelante, finalmente esta VLAN no se empleará.

6.2. Configuración del servidor DHCP

Una vez definidas las VLAN, es necesario configurar el servidor DHCP del router para que sirva direcciones IP adecuadas a cada dispositivo.

Dado que la red doméstica en la que se ha hecho el montaje, dependiente de un HGU de Movistar, trabaja en la red 192.168.1.0/24 (por tanto, dado que el puerto WAN del router lo he conectado a un puerto LAN del HGU, la IP WAN del router será una de dicho rango), para este montaje se empleará la red 192.168.10.0/24.

Teniendo en cuenta hay definidas cinco VLAN, se requieren tres bits para identificar a cada una de ellas, de forma que podemos dividir la red como sigue:

- 192.168.10.0/27 para la VLAN 1.
- 192.168.10.32/27 para la VLAN 2.
- 192.168.10.64/27 para la VLAN 4.
- 192.168.10.96/27 para la VLAN 6.
- 192.168.10.128/27 para la VLAN 7.

Para una red /27, la máscara de red es 255.255.255.224.

Por tanto, el servidor DHCP queda configurado como se muestra en las siguientes figuras:

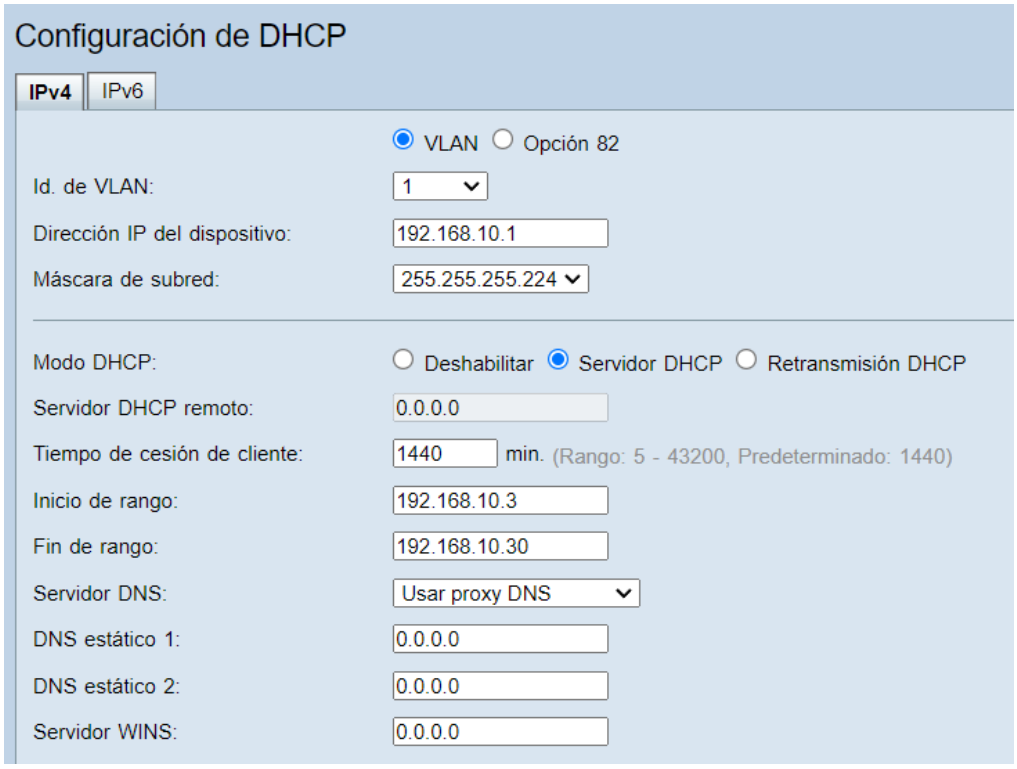


Figura 18: Configuración del servidor DHCP del router para la VLAN 1

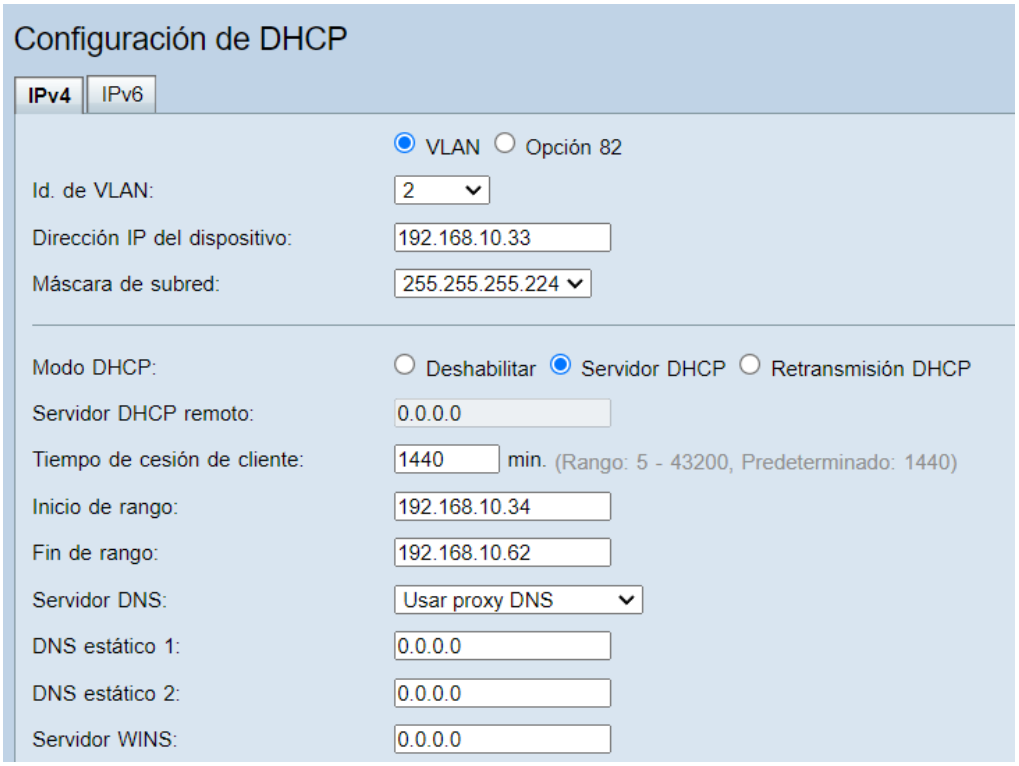


Figura 19: Configuración del servidor DHCP del router para la VLAN 2

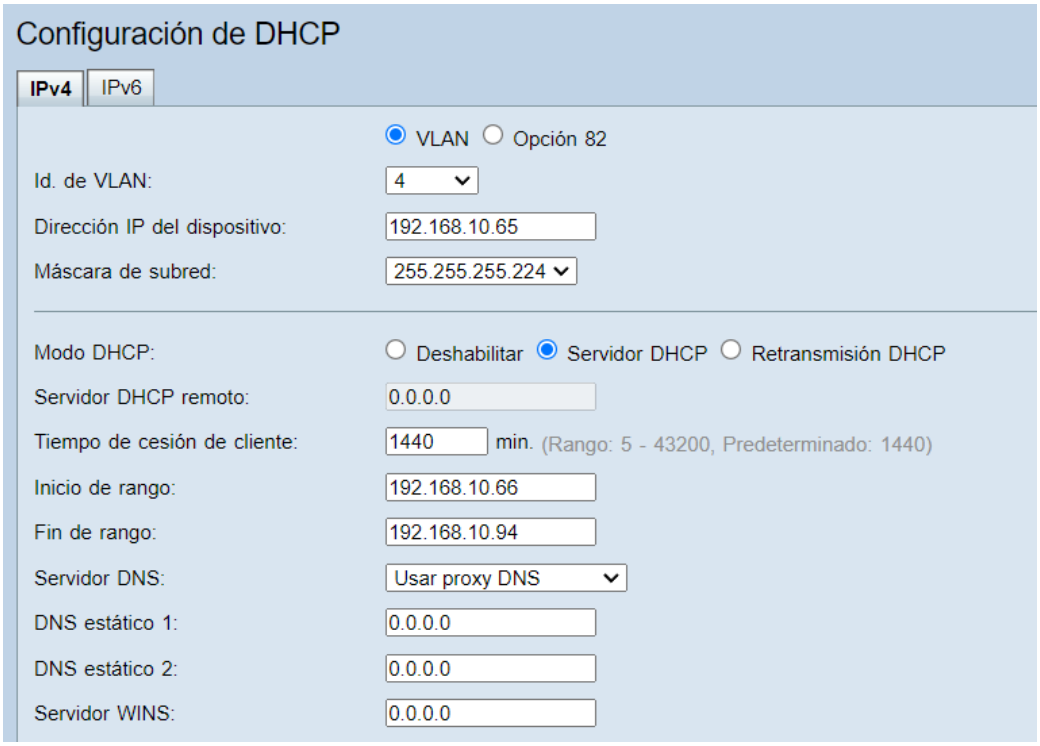


Figura 20: Configuración del servidor DHCP del router para la VLAN 4

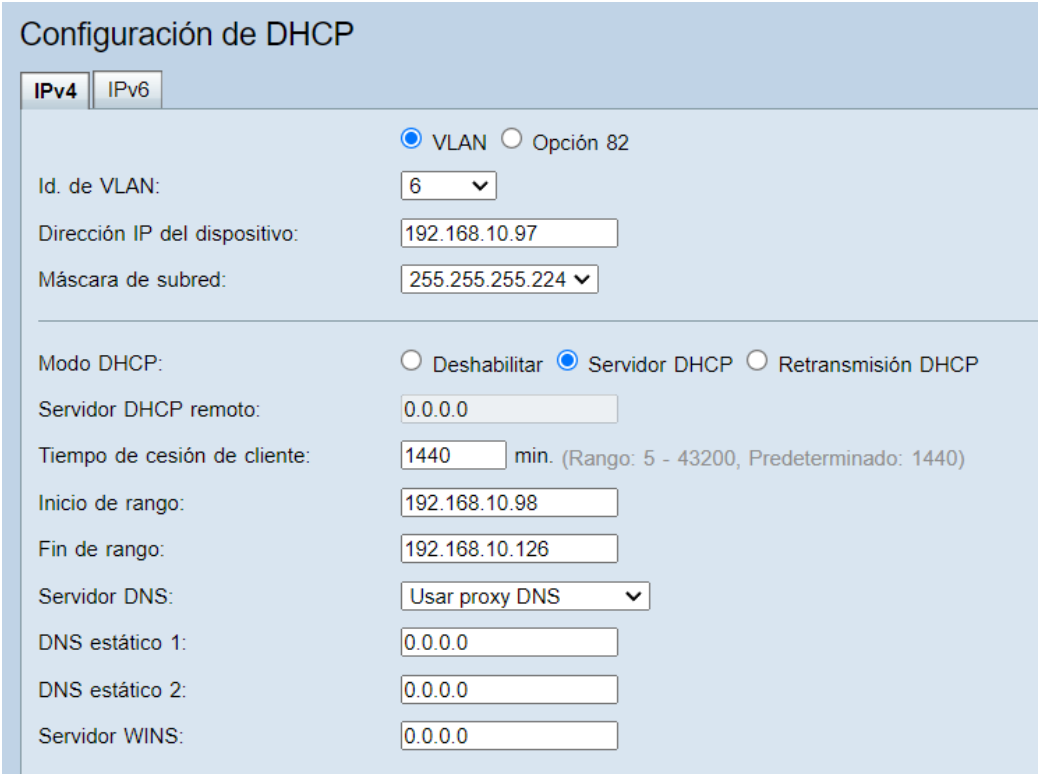


Figura 21: Configuración del servidor DHCP del router para la VLAN 6

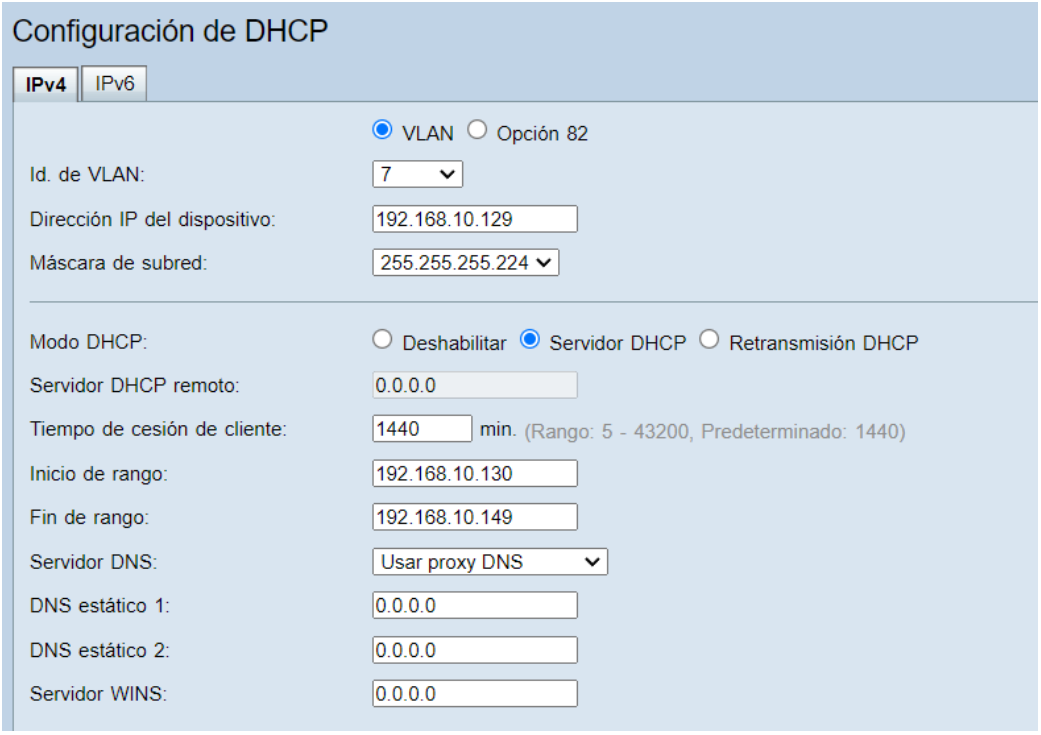


Figura 22: Configuración del servidor DHCP del router para la VLAN 7

Como se puede observar, el rango de direcciones asignables de la VLAN 7 termina en la 149, y no en la 158, como sería esperable. La razón es que el router, por defecto, reserva el rango 192.168.10.150 a 192.168.10.159 para PPTP y no permite cambiarlo ni desactivarlo (parece un bug del sistema).

Por otra parte, en la VLAN 1, se ha excluido la dirección 192.160.10.2 del rango del DHCP. Esto se debe a que se va a configurar de forma estática en el switch, como se ve en la siguiente imagen:

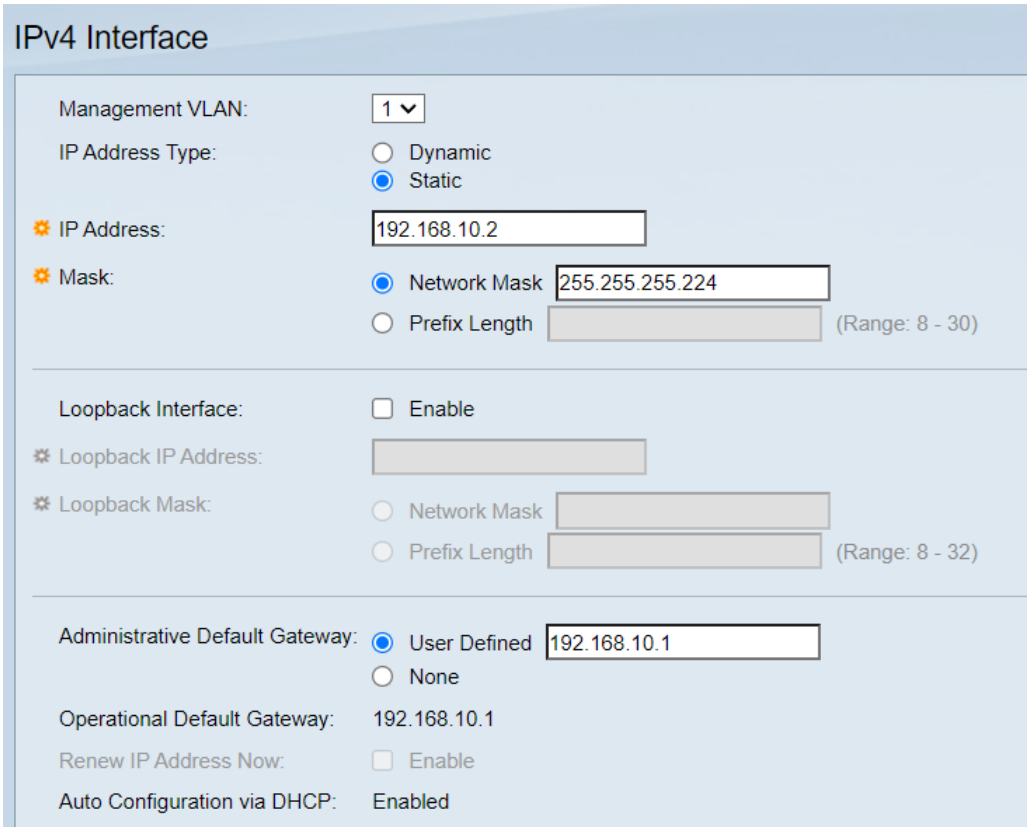


Figura 23: Configuración de IP estática en el Switch, para poder acceder a la configuración del mismo.

6.3. Configuración del port mirroring hacia el IDS

Ahora, es necesario configurar el *port mirroring* (Puerto Espejo) en el puerto donde está conectado el IDS. Por limitaciones del switch, no puede haber una VLAN conectada en dicho puerto, así que se reubica el IDS en el puerto 2 (que no se había empleado en la configuración de VLAN) y se redirige a él todo el tráfico de la VLAN 4, que es donde se conecta el centro de datos a proteger:

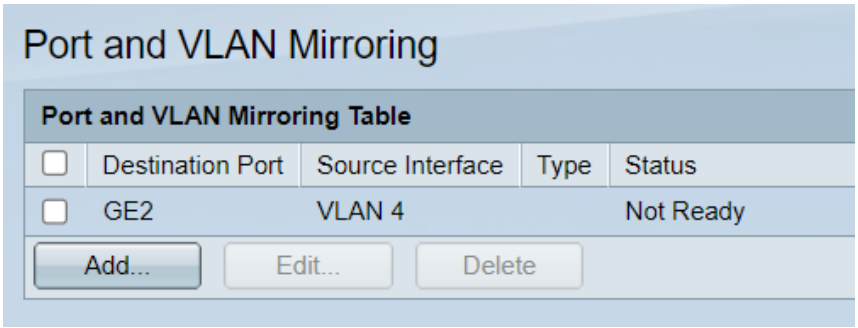


Figura 24: Configuración del Port Mirroring en el Switch

Hecho eso, los equipos quedan conectados de la siguiente forma:

- El IDS, como se ha indicado anteriormente, al puerto 2 del switch.
- El equipo con el que se ha estado realizando la configuración, pasa a estar conectado al puerto 6, de forma que se convierte en un "Dispositivo ajeno a la organización", perteneciente a la VLAN 7.
- Un tercer equipo se conecta al puerto 9 del switch, representando al centro de datos.

Lo que se pretende impedir, mediante el IDS y SNMP, es que los dispositivos ajenos a la organización accedan al centro de datos interno.

Para poder probar esto, se ha activado, de forma "forzada", el enrutamiento entre VLAN para el centro de datos y los dispositivos ajenos a la organización:

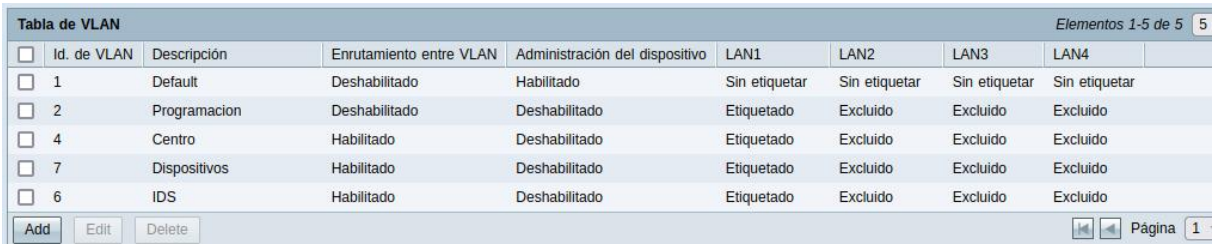


Tabla de VLAN — Elementos 1-5 de 5

Id. de VLAN	Descripción	Enrutamiento entre VLAN	Administración del dispositivo	LAN1	LAN2	LAN3	LAN4
1	Default	Deshabilitado	Habilitado	Sin etiquetar	Sin etiquetar	Sin etiquetar	Sin etiquetar
2	Programacion	Deshabilitado	Deshabilitado	Etiquetado	Excluido	Excluido	Excluido
4	Centro	Habilitado	Deshabilitado	Etiquetado	Excluido	Excluido	Excluido
7	Dispositivos	Habilitado	Deshabilitado	Etiquetado	Excluido	Excluido	Excluido
6	IDS	Habilitado	Deshabilitado	Etiquetado	Excluido	Excluido	Excluido

Add Edit Delete Página 1

Figura 25: VLAN Internetworking activado para el centro de datos y los dispositivos ajenos a la organización

Al conectar el equipo donde se ubica el IDS al puerto 2, se observa que no obtiene la configuración por DHCP, al estar activo el *port morroring*. Esta limitación se analizará más en detalle en el siguiente punto.

6.4. Creación y prueba de reglas en el IDS

Ahora, en el IDS, se crea una regla que avisa cuando exista tráfico TCP desde cualquier IP de la VLAN 7 (dispositivos ajenos) hacia cualquier IP de la VLAN 4 (centro de datos). Esta queda como sigue:

```
alert tcp 192.168.10.128/27 any -> 192.168.10.64/27 any (msg:"Intento de acceso TCP al centro de datos";sid:10003;)
```

Se ejecuta Snort con el comando:

```
sudo snort -d -l /etc/snort/log -b -c /etc/snort/snort.conf
```

Una vez que Snort está corriendo, basta con acceder, usando un navegador, desde el equipo ajeno a la organización a la dirección IP del centro de datos. Snort detecta esos intentos de conexión y avisa de ello:

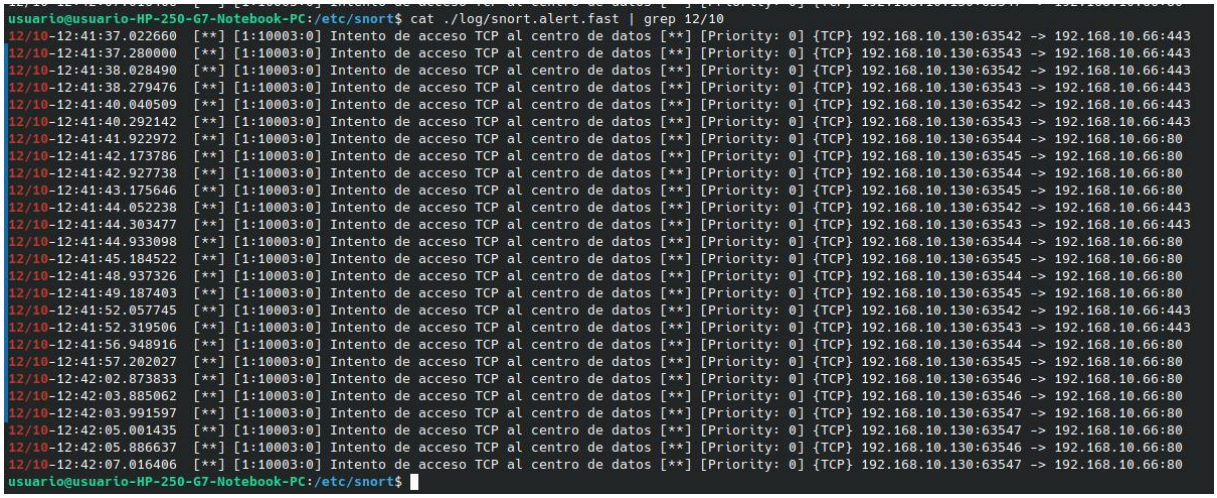


Figura 26: Alertas generadas por Snort al intentar acceder al centro de datos desde un dispositivo ajeno a la organización.

En este punto, se presenta un problema. No es posible establecer ninguna comunicación saliente desde el equipo conectado al puerto configurado como espejo. De hecho, aun configurando manualmente una IP en la interfaz de red (por DHCP no puede obtenerla), es imposible ni siquiera hacer un ping al router (192.168.10.1) o al switch (192.168.10.2), como se puede comprobar en la siguiente imagen:

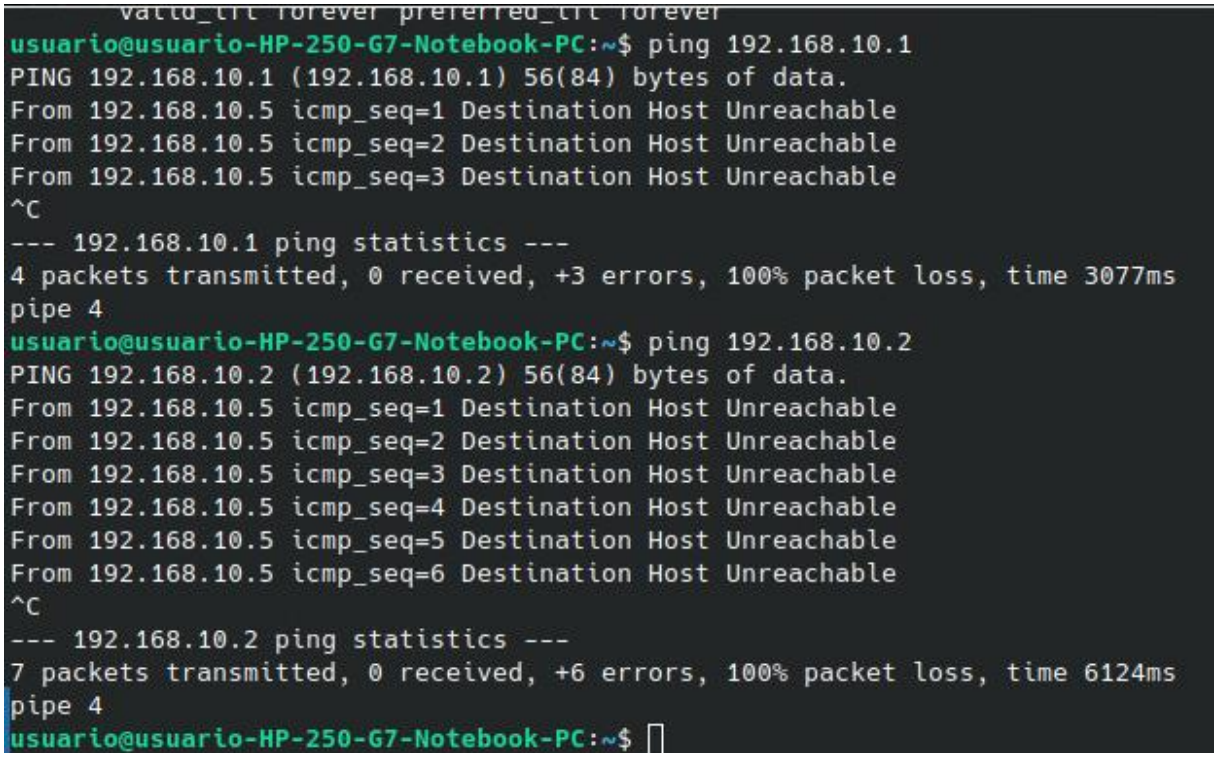


Figura 27: Intento fallido de realizar Ping al router y al switch, desde el equipo conectado al puerto espejo

En el manual técnico, (Cisco Systems, Inc., 2014), de los Switch Cisco SG-300, en la página 740, aparecen las limitaciones de un puerto espejo:

- El puerto del switch no es miembro de un canal de puertos.
- No hay interfaz IP configurada en el puerto.
- GVRP (*Generic VLAN Registration Protocol*) no está activado en el puerto.
- El puerto no es miembro de ninguna VLAN, excepto la VLAN por defecto.
- Protocolos L2, como: LLDP, CDP, LBD, STP, LACP, no están activos en el puerto de destino.

En resumen, no va a ser posible establecer comunicación por dicho puerto, al no estar ni siquiera configurada una interfaz IP en él. En el siguiente punto se solventa este inconveniente.

6.5. Solución al problema con el puerto espejo y configuración de SNMP

Para resolver el problema anteriormente planteado, hay que instalar dos interfaces de red en el IDS. Una de ellas estará conectada al puerto espejo y solo servirá para que Snort escuche en ella. La otra, se conectará a otro puerto de switch y sí que permitirá al IDS acceder a la red y enviar mensajes SNMP.

Con la configuración de VLAN establecida, sería necesario activar el enrutamiento entre VLAN para la del IDS, a fin de que este pudiera comunicarse con la IP del switch, además de permitir la configuración del mismo desde una VLAN distinta a la de gestión. Dado que no conviene hacer esto, se conecta la interfaz de red del IDS que no está en el puerto espejo directamente a esa VLAN 1, mediante el puerto 1, eliminando la VLAN 6 de la configuración. El resultado, por tanto, es el siguiente:

Port VLAN Membership Table

Filter: *Interface Type* equals to Port Go

	Interface	Mode	Administrative VLANs	Operational VLANs	LAG
○	GE1	Trunk	1UP	1UP	
○	GE2	Trunk	1P	1P	
○	GE3	Trunk	1UP	1UP	
○	GE4	Trunk	1UP	1UP	
○	GE5	Trunk	1UP	1UP	
○	GE6	Trunk	7UP	7UP	
○	GE7	Trunk	2UP	2UP	
○	GE8	Trunk	2UP	2UP	
○	GE9	Trunk	4UP	4UP	
○	GE10	Trunk	1UP, 2T, 4T, 7T	1UP, 2T, 4T, 7T	

Figura 28: Estado de las VLAN en el Switch tras eliminar la VLAN 6, destinada inicialmente al IDS

Eliminar la VLAN en el router no es posible, por la configuración de PPTP:

Figura 29: Error en el router al eliminar la VLAN 6

Si se intenta mover el rango PPTP, obliga a ubicarlo en alguna subred, pero, al hacerlo, obliga a excluir esas direcciones IP del servidor DHCP, lo cual tampoco es deseable. Lo esperable sería que, desactivando PPTP, su pudieran dejar las direcciones IP en blanco, pero el router no lo admite:

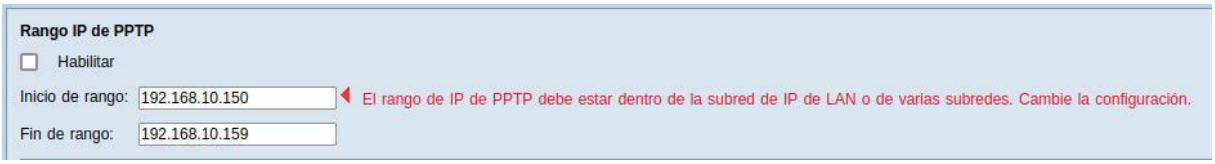


Figura 29: No es posible desactivar PPTP en el router, y siempre genera un error.

Esto no supone un problema, pues del switch sí se ha podido eliminar esta VLAN y, simplemente, no se utiliza.

Una vez hechos estos cambios, las conexiones quedan como sigue:

- Puerto 1 → Interfaz por la cual el IDS lanzará mensajes SNMP al switch (VLAN 1).
- Puerto 2 → Puerto espejo, al que se conecta la segunda interfaz de red del IDS para poner Snort en escucha.
- Puerto 6 → Equipo perteneciente a la VLAN 7, de dispositivos ajenos a la organización.
- Puerto 9 → Equipo perteneciente a la VLAN 4, que representa al centro de datos de la organización.
- Puerto 10 → Enlace con el router.

Ahora, es necesario activar SNMP en el switch. Para ello, en primer lugar, hay que poner en funcionamiento el servicio en *Seguridad* → *Servicios TCP/UDP*:

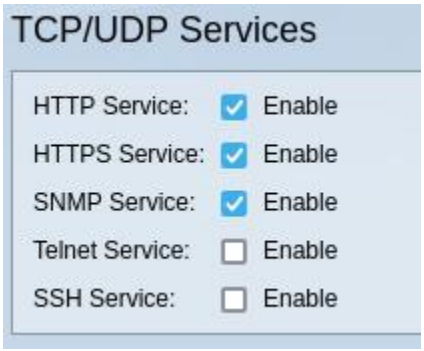


Figura 30: Servicio SNMP activado en el Switch

Por otra parte, se establecen dos comunidades:

- *Public* → Solo permite la lectura de parámetros.
- *Private* → Permite lectura y escritura de parámetros. Es la que se empleará en el IDS.

En la siguiente imagen es visible esta configuración:

Figura 31: Comunidades SNMP creadas en el switch

En este punto, se busca apoyo en la herramienta MIB Browser, de iReasoning. En concreto, para obtener el OID de las interfaces, prestando atención a los nodos *ifDescr* (indican el nombre de cada interfaz) e *ifAdminStatus* (valor de lectura y escritura que determina el estado del puerto):

Name/OID	Value	Type	IP:Port
ifDescr.49	gigabitethernet1	OctetString	192.168.10.2:161
ifDescr.50	gigabitethernet2	OctetString	192.168.10.2:161
ifDescr.51	gigabitethernet3	OctetString	192.168.10.2:161
ifDescr.52	gigabitethernet4	OctetString	192.168.10.2:161
ifDescr.53	gigabitethernet5	OctetString	192.168.10.2:161
ifDescr.54	gigabitethernet6	OctetString	192.168.10.2:161
ifDescr.55	gigabitethernet7	OctetString	192.168.10.2:161
ifDescr.56	gigabitethernet8	OctetString	192.168.10.2:161
ifDescr.57	gigabitethernet9	OctetString	192.168.10.2:161
ifDescr.58	gigabitethernet10	OctetString	192.168.10.2:161
ifAdminStatus.49	up (1)	Integer	192.168.10.2:161
ifAdminStatus.50	up (1)	Integer	192.168.10.2:161
ifAdminStatus.51	up (1)	Integer	192.168.10.2:161
ifAdminStatus.52	up (1)	Integer	192.168.10.2:161
ifAdminStatus.53	up (1)	Integer	192.168.10.2:161
ifAdminStatus.54	up (1)	Integer	192.168.10.2:161
ifAdminStatus.55	up (1)	Integer	192.168.10.2:161
ifAdminStatus.56	up (1)	Integer	192.168.10.2:161
ifAdminStatus.57	up (1)	Integer	192.168.10.2:161
ifAdminStatus.58	up (1)	Integer	192.168.10.2:161

Figura 32: Herramienta MIB Browser mostrando el nombre de las interfaces de red y su estado

Dado que el puerto de los dispositivos ajenos a la organización es el 6, el OID que permite modificar su comportamiento es **.1.3.6.1.2.1.2.2.1.7.54**, como se puede ver en la siguiente imagen:

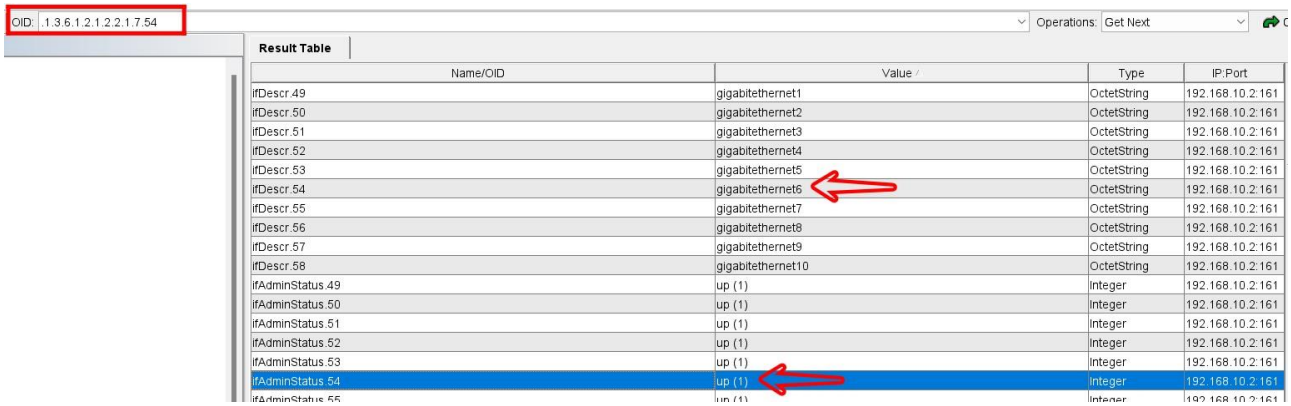


Figura 33: Localizando del OID correspondiente al puerto 6 del Switch

Los posibles valores para un *ifAdminStatus* son:

- 1 → Puerto activo.
- 2 → Puerto inactivo.
- 3 → Test.

Consecuentemente, para desactivar el puerto, hay que poner el estado de su *ifAdminStatus* a 2.

6.6. Configuración de Snort y Swatch para que el IDS pueda tomar acciones en el switch

Para conseguir que las alertas generadas por Snort se conviertan en mensajes SNMP, es necesario hacer algunos cambios en la configuración del mismo, así como un script *bash* que se ejecutará cuando se dispare una alerta.

6.6.1. Snort

En primer lugar, se configura Snort para que registre las alertas también en la bitácora del sistema, editando, para ello, el archivo **/etc/snort/snort.conf** y añadiendo la siguiente línea en el apartado 6 (módulos de salida):

```
output alert_syslog: LOG_DAEMON LOG_ALERT LOG_PID
```

De esta forma, las alertas de Snort aparecerán también en **/var/log/syslog**.

Ahora, se crean las reglas oportunas de Snort, para detectar conexiones UDP y TCP desde la VLAN de dispositivos ajenos a la organización a la VLAN del centro de datos. Son las siguientes:

```
alert tcp 192.168.10.128/27 any -> 192.168.10.64/27 any (msg:"Intento de acceso TCP al centro de datos";sid:10003;)
```

```
alert udp 192.168.10.128/27 any -> 192.168.10.64/27 any (msg:"Intento de acceso UDP al centro de datos";sid:10004;)
```

Estas reglas quedan ubicadas en **/etc/snort/rules/local.rules**.

Con esto, Snort está configurado y listo para trabajar. Para lanzarlo, hay que indicar cuál de las dos interfaces de red es en la que debe escuchar. Es fácil identificarla con la herramienta IP incluida en el sistema, mediante el comando `ip a`, que muestra todas las interfaces de red del sistema:

```
usuario@usuario-HP-250-G7-Notebook-PC:/etc/snort$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eno1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether b0:0c:d1:f0:4d:e3 brd ff:ff:ff:ff:ff:ff
    altname enp1s0
4: enx54af975c121b: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 54:af:97:5c:12:1b brd ff:ff:ff:ff:ff:ff
5: wlo1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 48:5f:99:75:68:7b brd ff:ff:ff:ff:ff:ff
    altname wlp2s0
7: enx40ed00028d34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 40:ed:00:02:8d:34 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.3/27 brd 192.168.10.31 scope global dynamic noprefixroute enx40ed00028d34
       valid_lft 74652sec preferred_lft 74652sec
    inet6 fe80::4f69:3c16:8e7e:eb9e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
usuario@usuario-HP-250-G7-Notebook-PC:/etc/snort$
```

Figura 34: Salida de la herramienta IP al consultar las interfaces de red.

La interfaz de red en la que no hay IP configurada es **enx54af975c121b**, por lo que será en ella en la que Snort escuchará. De esta forma, el comando con el que se lanzará Snort es el siguiente:

```
sudo snort -d -l /etc/snort/log/ -b -c /etc/snort/snort.conf -i enx54af975c121b
```

El equipo que representa al centro de datos tiene la dirección IP **192.168.10.66**. Accediendo desde el navegador a dicha IP se puede ver que, en efecto, las alertas saltan como se espera y se registran tanto en el log de Snort como en el del sistema:

```
usuario@usuario-HP-250-G7-Notebook-PC:/etc/snort$ cat ./log/snort.alert.fast | grep 12/17
12/17-14:36:18.714031  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55632 -> 192.168.10.66:80
12/17-14:36:18.978273  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55633 -> 192.168.10.66:80
12/17-14:36:19.217553  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55632 -> 192.168.10.66:80
12/17-14:36:19.494138  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55633 -> 192.168.10.66:80
12/17-14:36:19.728280  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55632 -> 192.168.10.66:80
12/17-14:36:19.998648  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55633 -> 192.168.10.66:80
12/17-14:36:20.230985  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55632 -> 192.168.10.66:80
12/17-14:36:20.515483  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55633 -> 192.168.10.66:80
12/17-14:36:20.745441  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55632 -> 192.168.10.66:80
12/17-14:36:20.758806  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55634 -> 192.168.10.66:443
12/17-14:36:21.010166  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55635 -> 192.168.10.66:443
12/17-14:36:21.024112  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55633 -> 192.168.10.66:80
12/17-14:36:21.265269  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55634 -> 192.168.10.66:443
12/17-14:36:21.532027  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55635 -> 192.168.10.66:443
12/17-14:36:21.778392  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55634 -> 192.168.10.66:443
12/17-14:36:22.040367  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55635 -> 192.168.10.66:443
12/17-14:36:22.298616  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55634 -> 192.168.10.66:443
12/17-14:36:22.543687  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55635 -> 192.168.10.66:443
12/17-14:36:22.806609  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55634 -> 192.168.10.66:443
12/17-14:36:23.053880  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55635 -> 192.168.10.66:443
12/17-14:36:28.474052  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55636 -> 192.168.10.66:443
12/17-14:36:28.732934  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55637 -> 192.168.10.66:443
12/17-14:36:28.983839  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55636 -> 192.168.10.66:443
12/17-14:36:29.237220  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55637 -> 192.168.10.66:443
12/17-14:36:29.489315  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55636 -> 192.168.10.66:443
12/17-14:36:29.741832  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55637 -> 192.168.10.66:443
12/17-14:36:30.004922  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55636 -> 192.168.10.66:443
12/17-14:36:30.257458  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55637 -> 192.168.10.66:443
12/17-14:36:30.507719  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55636 -> 192.168.10.66:443
12/17-14:36:30.769178  [**] [1:10003:0] Intento de acceso TCP al centro de datos [**] [Priority: 0] {TCP} 192.168.10.130:55637 -> 192.168.10.66:443
usuario@usuario-HP-250-G7-Notebook-PC:/etc/snort$
```

Figura 35: Alertas de Snort en el log del programa

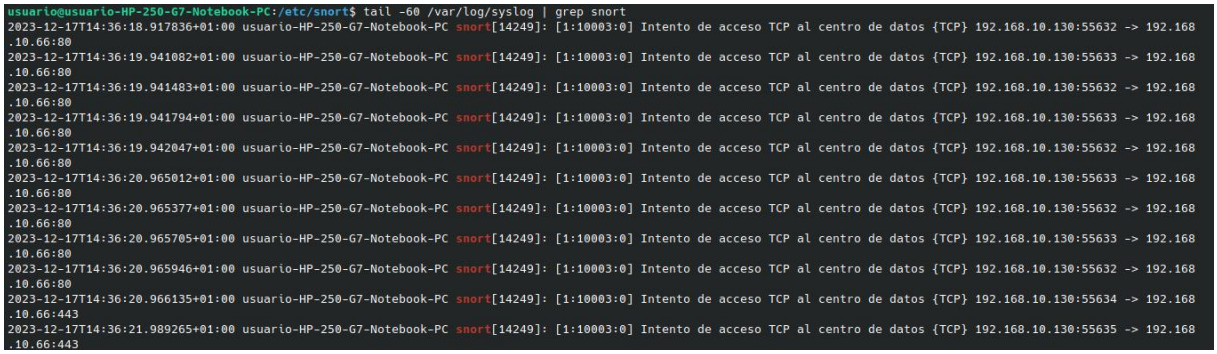


Figura 36: Alertas de Snort en el log del sistema

6.6.2. Swatch

Ahora, se pretende convertir esas alertas en acciones sobre el switch. En primer lugar, se crea el siguiente script *bash*, ubicado en **/home/usuario/swatch**:

```
#!/bin/bash

echo "$(date) - SNMPSET enviado, puerto de dispositivos ajenos a
la organizacion desconectado" >> logScriptSwatch.txt

snmpset -v2c -c private 192.168.10.2 .1.3.6.1.2.1.2.2.1.7.54 i 2
```

El script realiza dos acciones:

- En primer lugar, registra en una bitácora propia la acción tomada.
- En segundo lugar, ejecuta un SNMPSET sobre el OID del *ifAdminStatus* del puerto 6 del switch, desconectándolo (esto es, poniendo el valor a 2 -la *i* indica que se trata de un valor entero-).

También se crea, en el mismo directorio, el siguiente archivo de configuración, **swatch.conf**:

```
watchfor /.*snort.*:10003:.*/

    exec /home/usuario/swatch/script.sh

watchfor /.*snort.*:10004:.*/

    exec /home/usuario/swatch/script.sh
```

Con esta configuración, *Swatch* supervisará la bitácora del sistema en busca de patrones que coincidan con las expresiones regulares (se buscan líneas que incluyan la palabra *snort* y el ID de las reglas) junto a ***watchfor*** y, cuando las encuentre, ejecutará el script que antes se programó.

Para ejecutar *Swatch* en modo demonio (esto es, en segundo plano) con esta configuración, se emplea el siguiente comando:

```
swatchdog --daemon -c swatch.conf -t /var/log/syslog
```

6.7. Ejecución y comprobación del funcionamiento

Para probar el funcionamiento, se lanzan *Snort* y *Swatch* y se intenta acceder, desde el navegador del equipo que representa a los dispositivos ajenos, a la dirección IP del equipo que representa el centro de datos.

El resultado es satisfactorio. En la siguiente imagen se muestra cómo el puerto estaba activo (1) y cambió a inactivo (2) en pocos segundos, cuando se hizo el acceso indebido al centro de datos:

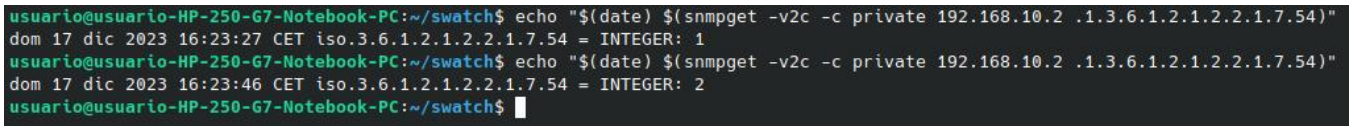


Figura 37: Resultado de la ejecución de la prueba con Snort y Swatch

De igual forma, las acciones tomadas se han registrado en el log del script:

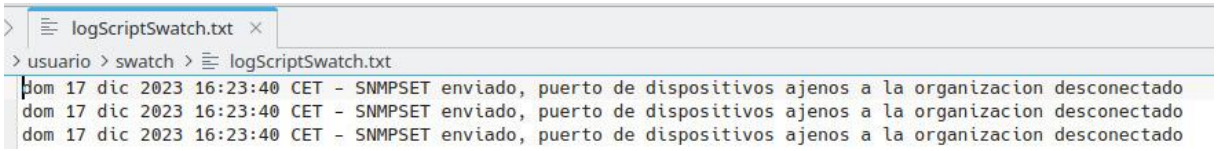


Figura 38: Acciones tomadas por el script tras la prueba realizada

Finalmente, se prueba también la regla creada para UDP, usando Packet Sender, como se observa en la siguiente imagen:

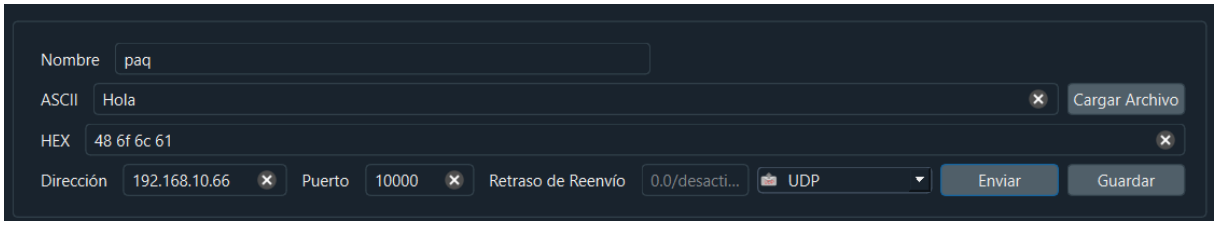


Figura 39: Configuración de Packet Sender para probar la regla UDP

El resultado, al igual que con TCP, es satisfactorio:

```
usuario@usuario-HP-250-G7-Notebook-PC:~/swatch$ echo "$(date) $(snmpget -v2c -c private 192.168.10.2 .1.3.6.1.2.1.2.2.1.7.54)"
dom 17 dic 2023 17:04:57 CET iso.3.6.1.2.1.2.2.1.7.54 = INTEGER: 1
usuario@usuario-HP-250-G7-Notebook-PC:~/swatch$ echo "$(date) $(snmpget -v2c -c private 192.168.10.2 .1.3.6.1.2.1.2.2.1.7.54)"
dom 17 dic 2023 17:05:56 CET iso.3.6.1.2.1.2.2.1.7.54 = INTEGER: 2
```

Figura 40: Resultado de enviar un paquete UDP. Al igual que con TCP, el puerto se desactiva

6.8. Esquema de la red montada

A modo de referencia, se muestra a continuación un esquema visual de la red montada en este apartado.

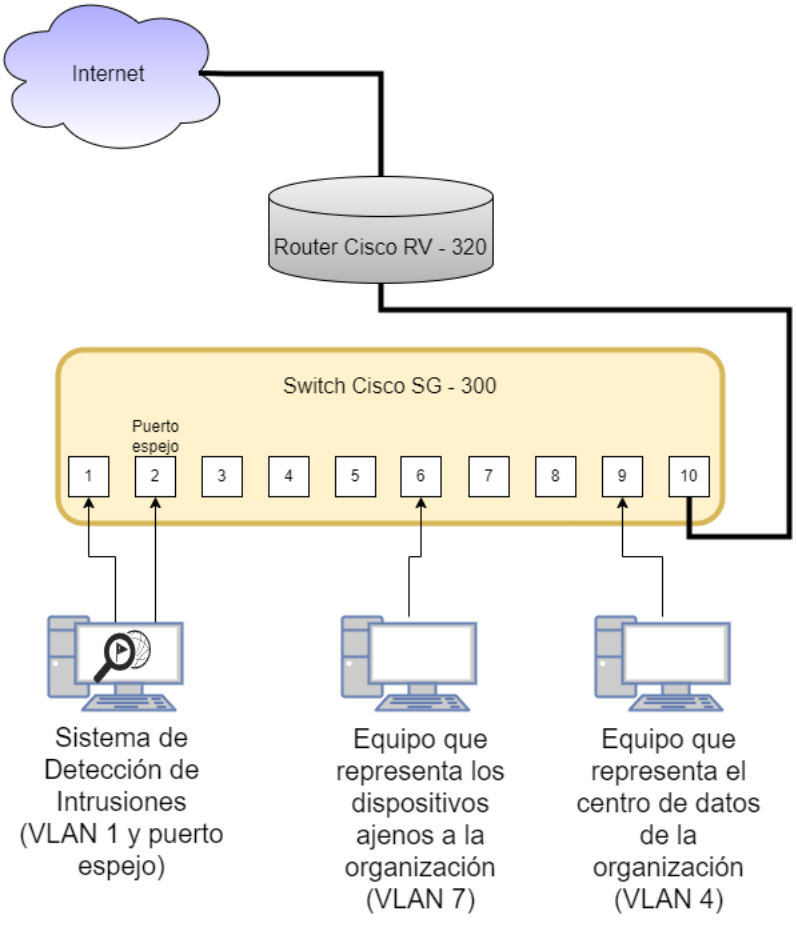


Figura 41: Esquema de la red montada

6.9. Observaciones finales

La forma en que se han convertido las alertas de Snort en configuraciones directamente en el switch, utilizando para ello SNMP, puede ser de aplicación en un entorno corporativo real, más grande.

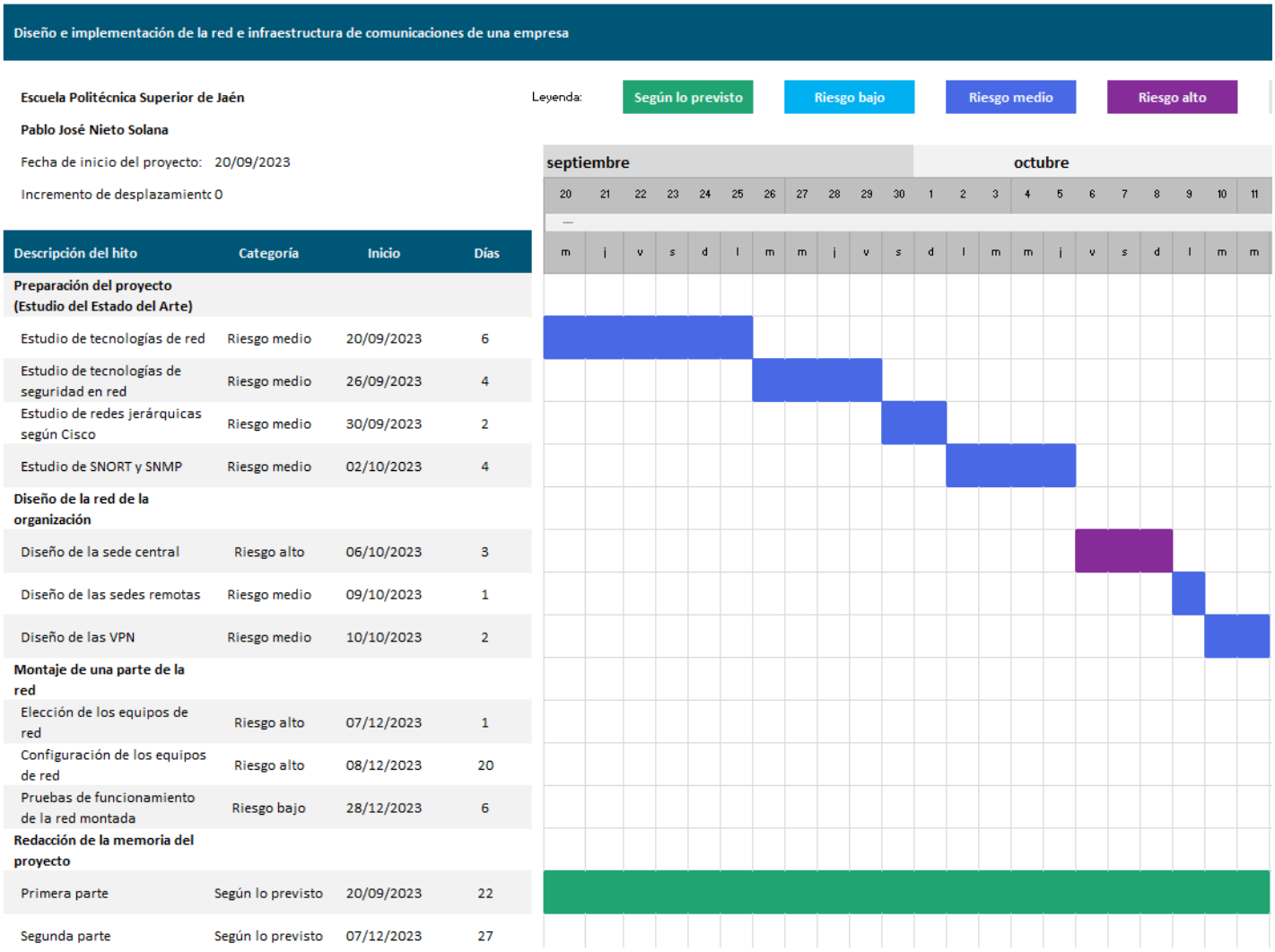
En este caso, no se han implementado las medidas de seguridad en el switch, como una lista de control de acceso, de forma intencionada, para derivar la gestión en el equipo con el IDS. En un entorno real, el IDS quedaría como última barrera, preparado para actuar en caso de que algún agente malicioso consiguiera saltarse la seguridad configurada en los equipos de red. Otra ventaja del uso de un IDS es la posibilidad de desconectar a un equipo con comportamiento indebido de la red local, cortando la conexión en el propio switch de acceso.

El contexto actual de seguridad es complicado, cabe la posibilidad de que se encuentren vulnerabilidades en el software de los equipos de red, permitiendo sortear la seguridad implementada en los mismos, por lo que resulta de gran utilidad tener una capa de seguridad adicional. Es lo que se ha pretendido mostrar en la parte práctica del presente trabajo, cómo es posible proteger una red sin depender, de forma exclusiva, de la seguridad configurada en los equipos que la conforman.

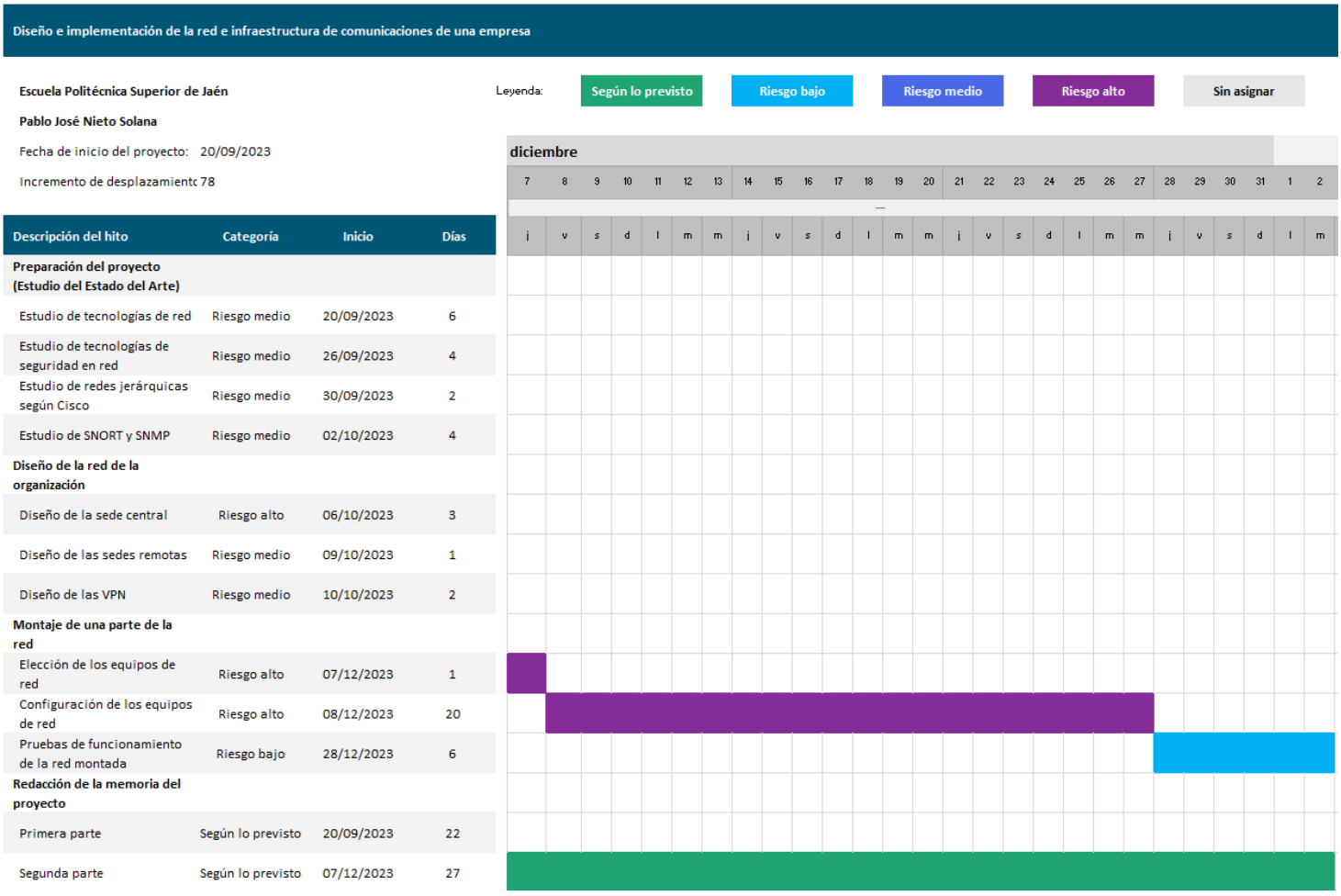
Adicionalmente, cabe destacar que todo esto se ha podido realizar utilizando, exclusivamente, software libre disponible de forma gratuita. Así, el equipo en el que se ha instalado el IDS utiliza Ubuntu 22.04 (concretamente, Kubuntu, con el escritorio KDE Plasma) y tanto el IDS empleado (*Snort*) como *Swatch* son, también, software libre.

7. Cronograma de trabajo

Las tareas que se han desarrollado durante la realización del Trabajo de Fin de Grado, así como su duración y distribución temporal, se muestran en el siguiente diagrama de Gantt:



Descripción del hito	Categoría	Inicio	Días
Preparación del proyecto (Estudio del Estado del Arte)			
Estudio de tecnologías de red	Riesgo medio	20/09/2023	6
Estudio de tecnologías de seguridad en red	Riesgo medio	26/09/2023	4
Estudio de redes jerárquicas según Cisco	Riesgo medio	30/09/2023	2
Estudio de SNORT y SNMP	Riesgo medio	02/10/2023	4
Diseño de la red de la organización			
Diseño de la sede central	Riesgo alto	06/10/2023	3
Diseño de las sedes remotas	Riesgo medio	09/10/2023	1
Diseño de las VPN	Riesgo medio	10/10/2023	2
Montaje de una parte de la red			
Elección de los equipos de red	Riesgo alto	07/12/2023	1
Configuración de los equipos de red	Riesgo alto	08/12/2023	20
Pruebas de funcionamiento de la red montada	Riesgo bajo	28/12/2023	6
Redacción de la memoria del proyecto			
Primera parte	Según lo previsto	20/09/2023	22
Segunda parte	Según lo previsto	07/12/2023	27



8. Presupuesto

Para las redes diseñadas en el TFG, se requieren:

- 3 router, uno para cada sede.
- 1 switch Core, para la sede central.
- 8 switches de acceso, 4 para la sede central y 2 para cada sede remota.
- 1 punto de acceso WiFi, para los dispositivos ajenos a la organización en la sede central.
- 48 horas de trabajo de diseño (6 días de 8 horas).
- 240 horas de trabajo de instalación (30 días de 8 horas).

El desglose queda presentado en la siguiente tabla:

CONCEPTO	PRODUCTO	CANTIDAD	IMPORTE POR UNIDAD	IMPORTE TOTAL
Router	Cisco C1111-8P	3	2.033,00 €	6.099,00 €
Switch Core	Cisco C9400-LC-48T	1	7.780,00 €	7.780,00 €
Switch de acceso	Cisco C1000-8T-2G-L	8	763,00 €	6.104,00 €
Puntos de acceso WiFi	Ubiquity Unifi U6+	1	114,00 €	114,00 €
Horas de trabajo (diseño)	Diseño de la red	48	15,00 €	720,00 €
Horas de trabajo (instalación)	Instalación de la red	240	15,00 €	3.600,00 €
IMPORTE TOTAL				24.417,00 €

9. Bibliografía

Atico34, G. (2023). *Así es Snort, el sistema de detección de intrusos más popular*. Obtenido de Atico34: https://protecciondatos-lopd.com/empresas/snort-deteccion-intrusos/

CheckPoint. (2023). *Clasificación de los sistemas de detección de intrusiones*. Obtenido de CheckPoint: https://www.checkpoint.com/es/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/#Definici%C3%B3ndeIDS

Cisco Systems, Inc. (2014). *Cisco 300 Series Stackable Managed Switches Command Line Interface Reference Guide, Release 1.4.*

Cisco, A. (2014). *Connecting Networks Companion Guide.* Cisco Press.

Deering, S., & Hinden, R. (julio de 2017). *Internet Protocol, Version 6 (IPv6) Specification.* doi:10.17487/RFC8200

Donenfeld, J. (1 de junio de 2020). *WireGuard: Next Generation Kernel Network Tunnel*. Obtenido de WireGuard: https://www.wireguard.com/papers/wireguard.pdf

Google. (19 de diciembre de 2023). *Estadísticas sobre la adopción de IPv6 en Internet*. Obtenido de Google: https://www.google.com/intl/es/ipv6/statistics.html

Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., & Kivinen, T. (octubre de 2014). *Internet Key Exchange Protocol Version 2 (IKEv2).* doi:10.17487/RFC7296

Lucena López, M. (30 de enero de 2022). *Tema 6: Sistemas de Detección de Intrusiones, Cortafuegos y Sistemas Trampa - Técnicas Avanzadas de Seguridad.*

Manage Engine. (2023). *Tutorial de SNMP*. Obtenido de Manage Engine: https://www.manageengine.com/es/network-monitoring/what-is-snmp.html

OpenVPN, C. (3 de octubre de 2022). *Overview of OpenVPN*. Obtenido de OpenVPN Community: https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn

Paessler AG. (2023). *IT Explained: SNMP*. Obtenido de Paessler: https://www.paessler.com/es/it-explained/snmp

Postel, J. (septiembre de 1981). *Internet Protocol.* doi:10.17487/RFC0791

Ramiro, R. (22 de noviembre de 2020). *Reglas SNORT , detección de intrusos y uso no autorizado*. Obtenido de Ciberseguridad Blog: https://ciberseguridad.blog/reglas-snort-deteccion-de-intrusos-y-uso-no-autorizado/

Rosencrance, L. (agosto de 2021). *VPN SSL o red privada virtual Secure Sockets Layer*. Obtenido de ComputerWeekly: https://www.computerweekly.com/es/definicion/VPN-SSL-o-red-privada-virtual-Secure-Sockets-Layer

Snort Team. (2020). *SNORT Users Manual*. Obtenido de http://manual-snort-org.s3-website-us-east-1.amazonaws.com/

Stallings, W. (2004). *Comunicaciones y Redes de Computadores* (Séptima ed.). Madrid: PEARSON EDUCACIÓN, S.A.

Stallings, W. (2004). *Fundamentos de seguridad en redes. Aplicaciones y Estándares. Segunda Edición.* Madrid, España: Pearson Educación.

Valencia, A., Zorn, G., Palter, W., Pall, G.-S., Townsley, M., & Rubens, A. (agosto de 1999). *Layer Two Tunneling Protocol "L2TP".* Obtenido de RFC Editor: https://www.rfc-editor.org/info/rfc2661

Wikipedia, c. d. (29 de noviembre de 2023). *Protocolo de internet*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Protocolo_de_internet

Wikipedia, c. d. (7 de julio de 2023). *Sistema de detección de intrusos*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos