UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

IMPLEMENTACIÓN DE SOLUCIÓN DE DATOS Y SEGURIDAD CON TECNOLOGÍA CISCO Y FORTINET

TRABAJO MONOGRÁFICO
PARA OBTENER EL GRADO DE
INGENIERO EN REDES

CARRERA

PRESENTA
GUILLERMO DE ANDA GONZÁLEZ

SUPERVISORES
DR. HOMERO TORAL CRUZ
DR. FREDDY IGNACIO CHAN PUC
ME. LUIS ANTONIO LÓPEZ MONROY

CHETUMAL QUINTANA ROO, MÉXICO, NOVIEMBRE DE 2018

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

TRABAJO MONOGRÁFICO TITULADO
"IMPLEMENTACIÓN DE SOLUCIÓN DE DATOS Y SEGURIDAD CON TECNOLOGÍA CISCO Y FORTINET"

ELABORADO POR
GUILLERMO DE ANDA GONZÁLEZ

BAJO SUPERVISIÓN DEL COMITÉ DEL PROGRAMA DE LICENCIATURA Y APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE:

INGENIERO EN REDES

COMITÉ SUPERVISOR

SUPERVISOR: _____
DR. HOMERO TORAL CRUZ

SUPERVISOR: _____
DR. FREDDY IGNACIO CHAN PUC

SUPERVISOR: _____
ME. LUIS ANTONIO LÓPEZ MONROY

CHETUMAL QUINTANA ROO, MÉXICO, NOVIEMBRE DE 2018

Agradecimientos

Primero que nada, le agradezco a Dios por todo, el haberme acompañado y guiado a lo largo de mi carrera, por ser la fortaleza en los momentos de debilidad y brindarme grandes personas que estuvieron conmigo a lo largo de la carrera.

A mis padres, que me apopyaron en cada momento, por los valores que me han inculcado y creer en mi y mis expectativas, gracias por el apoyo incondicional que me han otorgado, y el apoyo de darme lo necesario para poder resistir cada larga y agotadora noche de estudio.

A mi familia, por sus consejos y largar platicas para poder seguir adelante y continuar en este proceso de carrera universitaria, por el gran apoyo y sus grandes enseñanzas.

A mis compañeros y amigos, que fueron de gran influencia para concluir mi carreta, con las cuales he aprendido y disfrutado mis horas de estudio, gracias por el apoyo cuando en ocasiones me sentía perdido y por esa amistad sincera.

A mi supervisor, por el tiempo, dedicación y paciencia en la elaboración de este documento, agradezco sus consejos, sus lecciones y experiencias en formarme como una persona de bien y preparada para los retos que pone la vida.

A mi universida, por formarme con los mas altos estándares de calidad, las oportunidades que me brindó, la madurez que me fue dando y las grandes amistades que me permitio formar.

Dedicatoria

Antes que nada, le dedico a Dios este logro, que sin Él no podría haber concluido mi etapa universitaria.

Y con gran cariño hasta el cielo le dedico este logro a mi Abuelo, por sus grandes enseñanzas, sus historias y su amor indondicionable.

Resumen

A medida que una empresa u organismo gubernamental crece, también aumentan sus requisitos de red. Las organizaciones dependen de la infraestructura de red para proporcionar servicios esenciales, por tanto, las redes deben ser diseñadas e implementadas para que sean escalables y de alta disponibilidad.

Actualmente estamos trabajando para una empresa 100% mexicana, la cual está dedicada a la integración de soluciones basadas en equípo de cómputo y telecomunicaciones de alto rendimiento, con el propósito de lograr el crecimiento organizado de la infraestructura de los clientes, adaptándola a sus requerimientos actuales y futuros.

Nuestro principal objetivo es colaborar con nuestros clientes, ayudándolos a lograr sus objetivos, integrando soluciones confiables de tecnologías de información, para organizaciones medianas y grandes, a través de la especialización y disponibilidad del personal; de igual forma, nos enfocamos en ser el consultor de confianza de nuestros consumidores, para lograr la evolución de su infraestructura de TI en un escenario competitivo.

El presente documento, presenta la descripción ordenada de las actividades realizadas para una empresa; en el cual, por motivos de seguridad y confidencialidad se omite el nombre; de igual forma algunos datos como contraseñas e información sensible serán omitidos.

Dicha empresa se encuentra en continuo crecimiento, por tanto, para asegurar la entrega de servicios más eficientes, requiere de una infraestructura en su datacenter que ofrezca velocidades de conexión más altas, con mayores capacidades de procesamiento y almacenamiento, y actualización en la infraestructura de datos y seguridad.

De igual forma, la empresa continúa incorporando nuevos servicios, tal como telefonía IP; sin embargo, con la estructura actual, no podra aprovechar al máximo esta nueva tecnología de voz.

Por otro lado, el crecimiento de los departamentos requiere otorgar mayor velocidad y confiabilidad de conexión hacia el centro de datos; de igual forma, los servicios públicos que se ofrecen a la ciudadanía deben de estar siempre disponibles y estar protegidos ante cualquier intento de violación de la seguridad informática.

Contenido

Agradecimientos 3
Dedicatoria 4
Introducción....18
Planteamiento del Problema 20
Objetivos 22
Desarrollo....23
Capítulo 1 : Switching con Respecto a la Tecnología Cisco 23
1.1.- Protocolo de Internet (IP)....24
1.1.1.- Funcionamiento del protocolo IP 24
1.1.2.- Protocolos de transporte.... 24
1.1.3.- TCP y UDP.... 25
1.2.- Conmutación 26
1.2.1.- Funcionalidad de switching 27
1.2.2.- Conmutación de capa 2 27
1.3.- Switch Capa 3 28
1.3.1.- Funcionalidad multicapa 29
1.3.2- VLAN.... 29
1.3.3.- Enrutamiento entre VLAN.... 30
1.4.- Tipos de Puertos en un Switch 31
1.4.1.- Ethernet 31
1.4.2.- Fast Ethernet 32
1.4.3- Gigabit Ethernet.... 32
1.4.4.- 10-Gigabit Ethernet.... 32
1.5.- EtherChannel....33
1.5.1.- Distribución de tráfico 33
1.5.2.- Protocolos de negociación EtherChannel 34
1.6.- Spanning Tree Protocol 34
1.6.1.- Solución a los bucles de capa 2 35
1.6.2.- Funcionamiento de STP 36
1.6.3.- Elección del switch raíz.... 37
1.6.4.- Elección del puerto raíz.... 37
1.6.5.- Elección del puerto designado.... 39

1.6.6.- Estados STP 39
1.6.7.- Temporizadores de STP 40
Capítulo 2 : Routing con Respecto a la Tecnología Cisco 42
2.1.- Introducción 43
2.1.1.- Conexión por medio de routers 43
2.1.2.- Funciones del router 44
2.1.3.- Conexión de los dispositivos 45
2.2.- Acceso a la Consola 47
2.3.- Decisiones de Ruteo 49
2.3.1.- La mejor ruta 50
2.4.- Rutas Estáticas 51
2.4.1.- Enrutamiento estático 52
2.4.2.- Ruta estática por defecto 53
2.4.3.- Direccionamiento de red con clase 54
2.4.4.- Mascara de subred con clase 55
2.4.5.- Desperdicio de direccionamiento con clase 56
2.4.6.- Enrutamiento entre dominios sin clase 58
2.4.7.- Sumarización de rutas 58
2.5.- Rutas Dinámicas 62
2.5.1.- Historia 62
2.5.2.- Propósito del enrutamiento dinámico 63
2.5.3.- Detección de redes 65
2.5.4.- Tipos de protocolos de enrutamiento 67
2.5.5.- Protocolos de enrutamiento vector distancia 70
2.5.6.- Protocolos de enrutamiento estado de enlace 71
2.6.- Protocolo de Enrutamiento OSPF 73
2.6.1.- Funcionamiento de OSPF 74
2.6.2.- Mensajes OSPF 80
2.6.3.- Router designado (DR) y router designado de reserva (BDR) 82
2.6.4.- Costo 85
2.6.5.- Verificación de OSPF en una sola área 87
Capítulo 3 : Fortinet como Equipo de Seguridad Perimetral 94
3.1.- Introducción 95
3.2.- Unified Threat Management 96

3.2.1.- Redes y seguridad todo en uno 96
3.3.- Productos de Entrada de Fortinet 97
3.3.1.- Firewall empresarial 97
3.4.- FortiClient 100
3.4.1.- Seguridad al acceso remoto y movilidad 102
3.5.- FortiGate 600D 102
3.5.1.- Hardware del FortiGate 600D 104
3.5.2.- Modo de operación 105
3.6.- Logging y Monitoreo 106
3.6.1.- Entendiendo los logs 107
3.6.2.- FortiView 109
3.6.3.- Monitoreo 110
3.7.- Políticas de Firewall y su Autenticación 111
3.7.1.- Identificación del dispositivo 112
3.7.2.- Perfiles de seguridad 113
3.8.- VPN 115
3.8.1.- VPN IPSec 116
3.8.2.- ¿Cómo trabaja el protocolo IPsec? 118
3.9.- Antivirus 124
3.9.1.- ¿Qué es y cómo trabaja? 124
3.9.2.- Modos de inspección del FortiGate 126
3.9.3.- Filtrado web 129
3.9.4.- Filtrado de categoría respecto a FortiGuard 132
3.10.- Control de Aplicaciones 135
3.10.1.- Arquitectura Peer-to-Peer 136
3.11.- Enrutamiento 144
3.11.1.- Rutas estáticas y dinámicas 144
3.11.2.- Protocolo ECMP y balanceo de carga 147
3.11.3.- Políticas basadas en enrutamiento 152
3.12.- Alta Disponibilidad 155
3.12.2.- Enlace heartbeat 161
3.12.3.- Actualización de firmware en HA y estados 164
3.13.- IPS 168
3.13.1.- Sistema de prevención de intrusión 169

Capítulo 4 : Implementación de la Solución de Datos y Seguridad 174
4.1.- Levantamiento y Planeación 175
4.1.1.- Levantamiento de arquitectura 176
4.1.2.- Levantamiento y planeación por parte del área de ingeniería 179
4.1.3.- Reseñas de los productos 197
4.1.4.- Implementación en sitio con la tecnología Cisco 202
4.1.5.- Implementación en sitio con la tecnología Fortinet 229
Capítulo 5 : Resultados de la Implementación 240
5.1.- Resultados de la implementación 241
Conclusiones 243
Bibliografía 244

Índice de figuras

Figura 1-1. Protocolo TCP y UDP en la capa de transporte.....25

Figura 1-2. Ejemplo de conmutación de capa 2.....28

Figura 1-3. VLAN agrupadas lógicamente.....30

Figura 1-4. Agrupar varias VLAN en un mismo switch capa 2, router o switch capa 3.31

Figura 2-1. Envió de paquete entre routers 45

Figura 2-2. Ejemplo del envió de un paquete por capa dos y capa tres.....46

Figura 2-3. Ejemplo de configuración de ruta estática 47

Figura 2-4. Ejemplo de configuración de ruta dinámica 47

Figura 2-5. Requisitos para la conexión de consola 48

Figura 2-6. Puertos y cables para la conexión por consola.....49

Figura 2-7. Ejemplo de las capas del modelo OSI por dispositivo 50

Figura 2-8. Ejemplo de enrutamiento estatico 51

Figura 2-9. Ejemplo de enrutamiento dinámico 52

Figura 2-10. Red de clase A.....55

Figura 2-11. Red de clase B.....56

Figura 2-12. Red de clase C.....56

Figura 2-13. Grafico circular de las clases de red.....57

Figura 2-14. Ejemplo de sumarización de rutas.....59

Figura 2-15. Grafico circular de la división de subredes tradicional 60

Figura 2-16. Grafico circular de una división de subredes por VLSM 61

Figura 2-17. Ejemplo de una red grande 65

Figura 2-18. Inicio en frio de un router.....65

Figura 2-19. Actualización de una tabla de enrutamiento de un router en frio 66

Figura 2-20. Tabla de enrutamiento actualizada por cada router.....66

Figura 2-21. Protocolo RIP y OSPF....70
Figura 2-22. Protocolo vector distancia....70
Figura 2-23. Paquetes de intercambio de OSPF....75
Figura 2-24. Paquetes de saludo OSPF....76
Figura 2-25. Paquetes LSA de OSPF....77
Figura 2-26. Ejecución del algoritmo SPF....78
Figura 2-27. Tabla de enrutamiento OSPF del R1....79
Figura 2-28. Adyacencias de router....83
Figura 2-29. Diagrama de flujo para determinar el ID del router....84
Figura 2-30. Resultado del comando OSPF....88
Figura 2-31. Comandos show para OSPF....90
Figura 2-32. Comando show ip protocols....91
Figura 2-33. Comando show ip ospf database....93
Figura 2-34. Comando show ip ospf interface....93
Figura 3-1. Organizaciones de seguridad [10]....96
Figura 3-2. FortiAP y FortiSwitch....97
Figura 3-3. Modelos y rangos de FortiGate [10]....99
Figura 3-4. Conexión VPN FortiClient....102
Figura 3-5. FortiGate 600D [10]....105
Figura 3-6. Modo de operación del FortiGate....106
Figura 3-7. Menú FortiView....109
Figura 3-8. Ajustes de log....111
Figura 3-9. Secuencia de las políticas de firewall....112
Figura 3-10. Perfiles de seguridad en la política de firewall....114
Figura 3-11. Ejemplo de Traffic Shaper....115

Figura 3-12. Ejemplo de VPN 118
Figura 3-13. Encapsulación 120
Figura 3-14. Configuración de VPN fase 1 122
Figura 3-15. Configuración de VPN fase 2 123
Figura 3-16. Conexión TCP en un tipo de escaneo proxy-based 126
Figura 3-17. Escaneo proxy-based 127
Figura 3-18. Conexión TCP en un tipo de escaneo flow-based 128
Figura 3-19. Escaneo flow-based 129
Figura 3-20. Protocolos en el modo de inspección proxy-based 130
Figura 3-21. Filtro DNS y filtro web 131
Figura 3-22. Modos de inspección 132
Figura 3-23. FortiGate y FortiGuard en conjunto 133
Figura 3-24. Ejemplo de solicitud para clasificación de sitio 133
Figura 3-25. Botnet habilitado 134
Figura 3-26. Habilitar perfiles de seguridad en la política 135
Figura 3-27. Arquitectura de cliente-servidor 136
Figura 3-28. Arquitectura P2P 137
Figura 3-29. Firmas de control de aplicaciones 138
Figura 3-30. Habilitar sensor en la política 139
Figura 3-31. Orden de operaciones 140
Figura 3-32. Sección View Signatures 141
Figura 3-33. Bloqueo de página 142
Figura 3-34. Política de aplicación 143
Figura 3-35. Ruta estática 144
Figura 3-36. Tabla de enrutamiento de FortiGate [11]. 145

Figura 3-37. Ejemplo de configuración ECMP por CLI 148
Figura 3-38. Ejemplo de WAN Link Load Balancing 149
Figura 3-39. Configuración de WLLB 150
Figura 3-40. Interfaz WLLB 150
Figura 3-41. Comprobación de WAN.....151
Figura 3-42. Monitor de la verificación del enlace WAN 151
Figura 3-43. Enrutamiento de tráfico especifico.....152
Figura 3-44. Política de enrutamiento.....153
Figura 3-45. Acción de una PBR 154
Figura 3-46. Tabla de enrutamiento con redes activas 154
Figura 3-47. Base completa de la tabla de enrutamiento.....155
Figura 3-48. Alta disponibilidad de un FortiGate.....156
Figura 3-49. Sincronización de FortiGate primario y secundario.....157
Figura 3-50. Heartbeat del FortiGate.....158
Figura 3-51. Elección de un FortiGate primario 159
Figura 3-52. Alteración para la elección de un FortiGate primario 160
Figura 3-53. Sincronización de clúster HA.....162
Figura 3-54. MAC virtual.....164
Figura 3-55. Monitor del clúster H.A.....165
Figura 3-56. Comando de diagnóstico del HA 166
Figura 3-57. Comandos para la administración del HA.....166
Figura 3-58. Comando para la verificación checksum del clúster 167
Figura 3-59. Firmas.....170
Figura 3-60.Enciclopedia FortiGuard.....171
Figura 3-61. Firmas individuales.....172

Figura 3-62. Filtro de búsquedas de firmas 172
Figura 3-63. Habilitar sensor IPS en la política de firewall 173
Figura 4-1. Equipo HPE 3PAR 175
Figura 4-2. Diagrama físico del area de arquitectura 179
Figura 4-3. IDF (1)....180
Figura 4-4. IDF (2)....180
Figura 4-5. IDF (3)....181
Figura 4-6. IDF (4)....181
Figura 4-7. IDF (5)....182
Figura 4-8. Diagrama final de la propuesta....185
Figura 4-9. Diagrama físico de la propuesta 187
Figura 4-10. Interconexión final de la propuesta 189
Figura 4-11. Cisco Catalyst 4500E [6] 199
Figura 4-12. Cisco Catalyst 2960X [6] 200
Figura 4-13. FortiGate 600D [10]....202
Figura 4-14. Rack de gabinete cerrado 202
Figura 4-15. Montaje de Cisco Core en rack 203
Figura 4-16. Switch Cisco Core 4500R+E 207
Figura 4-17. Diagrama físico final de la implementación 224
Figura 4-18. Diagrama lógico final de la implementación 225
Figura 4-19. Interconexión del diagrama lógico final de la implementación 226
Figura 4-20. Clúster FortiGate....229
Figura 4-21. Clúster FortiGate y switch Cisco Core en rack 229
Figura 4-22. Diagrama lógico final....230
Figura 4-23. Diagrama físico final de la interconexión completa....231

Figura 4-24. Configuración de alta disponibilidad 232
Figura 4-25. Monitor de la alta disponibilidad 232
Figura 4-26. Dashboard del clúster 233
Figura 4-27. Interfaces del Clúster FortiGate.....234
Figura 4-28. Configuración de VPN IPsec por CLI del FortiGate local 235
Figura 4-29. Configuración de políticas de firewall por CLI del FortiGate local 236
Figura 4-30. Configuración de ruta estática por CLI del FortiGate local.....237
Figura 4-31. Configuración de VPN IPsec por CLI del FortiGate remoto 237
Figura 4-32. Configuración de la política del firewall por CLI del FortiGate remoto....238
Figura 4-33. Configuración de ruta estática por CLI del FortiGate remoto 238
Figura 4-34. Monitor de IPsec 239

Índice de tablas

Tabla 1. Capas del modelo OSI, su correspondiente PDU y dispositivo asociado 27
Tabla 2. Distribución del frame en dos enlaces EtherChannel 33
Tabla 3. Cantidad de bytes por BPDU 36
Tabla 4. Valor de costos por ancho de banda 38
Tabla 5. Sintaxis del comando para una ruta estática 54
Tabla 6. Clases de red tipo A, B, C, D y E 54
Tabla 7. Protocolos de gateway interior y exterior 63
Tabla 8. Ventajas y desventajas del enrutamiento estático 64
Tabla 9. Protocolos de enrutamiento 68
Tabla 10. Distancias administrativas de algunas rutas 73
Tabla 11. Tablas del OSPF 74
Tabla 12. Tipo de LSA y su descripción 81
Tabla 13. Contenido del paquete OSPF 81
Tabla 14. Calculo del costo por interfaz 86
Tabla 15. Descripción de algunos comandos 88
Tabla 16. Descripción de algunos comandos útiles 90
Tabla 17. Descripción de algunos comandos útiles para OSPF 91
Tabla 18. Características de algunos equipos Fortinet 98
Tabla 19. FortiClient 101
Tabla 20. Tipos de logs FortiGate 107
Tabla 21. Niveles de Syslog 108
Tabla 22. Puertos del protocolo IKE y ESP 119
Tabla 23. Distancias por defecto de algunos protocolos de enrutamiento 146
Tabla 24. Carga de trabajo entre los clústeres 164

Tabla 25. Exploit y anomalía 168
Tabla 26. Alcances de los equipos de datos 176
Tabla 27. Alcances de los equipos de seguridad....177
Tabla 28. Consideraciones comerciales....178
Tabla 29. Propuesta de direccionamiento 184
Tabla 30. Propuesta de redes para la interconexión....184
Tabla 31. Propuesta del enrutamiento de redes del switch Core....184
Tabla 32. Propuesta de VLAN's para los IDF's....186
Tabla 33. Propuesta de los segmentos del FortiGate....187
Tabla 34. Milestone del plan de trabajo de la solución de datos....190
Tabla 35. Riesgos en la implementación....192
Tabla 36. Cronograma de la solución de datos 192
Tabla 37. Milestone por porcentaje de la solución de seguridad....194
Tabla 38. Cronograma de actividades de la solución de seguridad....196
Tabla 39. Direccionamiento de administración 223
Tabla 40. Direccionamiento VLAN del MDF y los IDF’s....226
Tabla 41. Tabla comparativa del Cisco Core antiguo y el nuevo 241
Tabla 42. Tabla comparativa del switch de acceso antiguo y nuevo....242

Introducción

En la actualidad las organizaciones necesitan usar infraestructuras de red robustas para proporcionar servicios de comunicaciones. A medida que dichas organizaciones crecen y evolucionan, contratan más empleados, abren sucursales y se expanden a los mercados globales. Estos cambios afectan directamente los requisitos de la red. Una red debe permitir el intercambio de diversos tipos de tráfico, entre ellos archivos de datos, correo electrónico, telefonía IP y aplicaciones de videoconferencia, por tal motivo es necesario la integración de equipos que cuenten con innovación, robustez y seguridad. Un ejemplo de infraestructura en crecimiento, es una organización privada que acudió con nosotros para que realicemos su diseño, actualización e instalación de su red, la cual opto por elegir switches Cisco capa 2 y capa 3 como infraestructura de conmutación, y un dispositivo FortiGate para la cuestión de seguridad.

Cisco es actualmente reconocida a nivel mundial por sus equipos de gran capacidad y velocidad para la comunicación, conmutación, seguridad, su inteligencia y simplicidad, al igual que sus protocolos propietarios para el enrutamiento y comunicaciones.

Por otro lado, FortiGate es un equipo de seguridad perimetral perteneciente de la tecnología Fortinet, la cual se concentra en integrar soluciones de seguridad, busca acelerar tareas de procesamiento para mantener segura sus redes corporativas y, por otra parte, necesitan el respaldo de un esquema riguroso de investigación y soporte que les permita cumplir sus objetivos ante un ambiente global de amenazas. Bajo esta perspectiva, Fortinet se apuntala como la principal solución innovadora de alto desempeño para la seguridad de redes orientada a resolver problemas fundamentales que surgen en los entornos de redes de uso intensivo de ancho de banda donde las amenazas informáticas son cada vez más sofisticadas.

Al trabajar en un entorno relativamente grande, es necesario utilizar un marco de distribución, debido a que en este punto existe una terminación pasiva del cable. Estos se encuentran normalmente en la parte posterior del centro de datos o en una pared muy grande, ya que necesita una gran cantidad de conexiones para poder perforar las diferentes conexiones de cable y de distintos lugares. A menudo se utiliza esto con el nombre de una habitación o una ubicación. Esta es una parte muy importante de la red, ya que tiene todos los datos para todos sus sistemas que pasan a través de este marco de distribución.

El otro marco de distribución que normalmente hay, es el marco de distribución intermedio o el IDF. Esta es una extensión del MDF. Se puede pensar en él como un auxiliar del MDF, y es un lugar donde se puede traer a los usuarios y conectarlos en la red principal. Existen enlaces ascendentes desde aquí hasta el MDF.

El presente trabajo monográfico está compuesto por cinco capítulos:

El primer capítulo está conformado por los conceptos básicos de switching con respecto a la tecnología Cisco, así también como las configuraciones necesarias para establecer el objetivo de un switch con relación al proyecto documentado.

El segundo capítulo contiene los conceptos referentes al routing con respecto a la tecnología Cisco, de igual forma se muestran algunas de las configuraciones necesarias durante la implementación del proyecto realizado en la institución.

El tercer capítulo muestra ciertos conceptos para la comprensión de la tecnología Fortinet y su funcionamiento, el equipo FortiGate cuenta con diferentes funcionalidades, pero en el presente documento se añaden solamente las utilizadas en la implementación de dicha organización.

El cuarto capítulo contiene la metología usada en la implementación del proyecto para la solución de datos y seguridad.

El quinto capítulo proporciona los resultados de la implementación.

Planteamiento del Problema

La tecnología hoy en día es una vital función en varios aspectos de la vida, desde los hogares hasta los centros de trabajo. Por otro lado, el crecimiento de la tecnología es muy rápido, y las empresas privadas o gubernamentales tienen que adaptarse a ese crecimiento. Además, el crecimiento gradual de las empresas debe ser proporcional al crecimiento y actualización de su red de infraestructura.

Un ejemplo de infraestructura en constante crecimiento es una organización privada que acudió con nosotros para una solución, la cual ha optado por trasladar 4 oficinas a un nuevo edificio, para realizar esto fue necesario contar con una propuesta tecnológica que hiciera frente a las necesidades de servicios de datos y seguridad de las 4 oficinas en conjunto. El mismo crecimiento de los departamentos requiere otorgar mayor velocidad y confiabilidad de conexión hacia el centro de datos, de la misma los servicios públicos que se ofrecen a la ciudadanía deben de estar siempre disponibles y estar protegidos ante cualquier intento de violación de la seguridad informática.

Dicha empresa provee servicios de comunicación e internet a diferentes oficinas y departamentos. Para efecto del control de la seguridad y políticas de navegación se contaba con un firewall instalado en un servidor, sin embargo, para hacer frente a los crecientes requerimientos de crecimiento de la red y los servicios ofrecidos, la empresa optó por realizar una mejora en la infraestructura de firewall perimetral, así mismo se contempló el uso de un sistema de reporte de la actividad de firewall para la realización de auditorías y/o reportes de uso.

Como equipos de datos, la organización optó por utilizar la tecnología Cisco, tales como switches de capa 2 para el acceso de los usuarios y switches de capa 3 para el enrutamiento y comunicación.

Las actividades dieron inicio realizando el rediseño de la solución propuesta, proponiendo los direccionamientos y obteniendo información sobre las necesidades y requerimientos del proyecto.

La empresa cuenta con varios sitios remotos (MPLS), y en cada sitio tienen un router cisco, configurados por otro proveedor, en los cuales usan el protocolo de ruteo EIGRP externo, esto significa que tiene una distancia administrativa de 170, sin embargo, cuenta con velocidades demasiado lentas, enlaces dedicados desde 256 kbps hasta un máximo de 2 mbps, estos enlaces son intermitentes ya que se caen con frecuencia y abruman el trabajo de la organización. Una solución son las VPN’s IPsec Site-to-Site basado en enrutamiento; en cada sitio donde habrá un router Cisco y un pequeño FortiGate, que tendrán la capacidad para comunicarse por medio de VPNs con el FortiGate central del sitio principal. Estos enlaces VPN estarán interconectados, y el FortiGate central se comunicará con el switch Cisco principal por medio del protocolo OSPF, ya que, al ser equipos con diferentes tecnologías, este protocolo viene siendo el más adecuado para este trabajo, además tendrá una distancia administrativa de 100, el cual otorgará preferencia por los enlaces VPN, teniendo el enlace MPLS como rutas

de respaldo. Para el ruteo entre los equipos Cisco se optó por usar EIGRP, para que el switch Cisco principal conozca las redes de cada IDF.

Por la parte de seguridad de capa dos a nivel de puerto, se habilitó PortSecurity que, sin ser una protección perfecta, impide que un intruso pueda conectarse físicamente a la red, tener acceso Internet, entre otras actividades maliciosas. En cuanto se detectan tramas provenientes de una dirección MAC no autorizada, el puerto físico se bloquea y marca un error. Esta funcionalidad se activó en todos los puertos de los switch de acceso, para limitar la cantidad de direcciones MAC que se pueden conectar a través de un puerto, además evita la generación de bucles que puedan afectar el desempeño de la red. A continuación, se listan los requerimientos específicos:

- Permitir máximo dos dispositivos por puerto.
- Habilitar PortFast.
- Activar BPDUGuard para evitar la conexión de switches no contemplados en la topología.

Con base a los puntos mencionados anteriormente, en el presente trabajo monográfico se presenta la implementación de una solución de datos y seguridad, mediante las tecnologías Cisco y Fortinet; y se realiza la documentación de dicha implementación.

Objetivos

Implementar la infraestructura correspondiente para servicios de datos y seguridad con tecnologías Cisco y Fortinet, en una organización privada, para contar con una red que brinde confiabilidad en la información, y disponibilidad de los recursos; y realizar la documentación de dicha implementación.

Desarrollo

Capítulo 1 : Switching con Respecto a la Tecnología Cisco

1.1.- Protocolo de Internet (IP)

Una dirección IP (Internet Protocol, por sus siglas en ingles), es un código que funciona para la identificación de la interfaz. Actualmente, existen dos versiones de direcciones IP, IPv4 e IPv6 [1].

IPv4 está formado por un numero binario de 32 bits, que normalmente se representa como 4 número de base decimal del 0 al 255, separados por puntos, por ejemplo, la dirección de un localhost sería 127.0.0.1. [1].

1.1.1.- Funcionamiento del protocolo IP

Para identificar un equipo de manera única, se definen tres clases de direcciones. Clase A, el primer byte se ubica entre 1 y 126. Se utilizan 7 bits para el número de red y 24 bits para identificar el equipo. Una red de clase A puede soportar hasta 16 millones de equipos (224-2 posibilidades). En una clase B, el primer byte varía entre 128 y 191. Con 14 bits se hace el cifrado del número de red y con 16 bits el número de equipo. Se puede definir hasta 65.534 equipos en una misma red (216-2). La máscara por defecto es 255.255.0.0. La clase C está definida por un primer byte variable de 192 a 223. Se utilizan 21 bits para la red y 8 para el equipo. Podemos tener hasta 254 equipos por red en clase C [2].

El protocolo IP es un protocolo sin conexión que reside en la capa 3 del modelo OSI, la capa de red. Se puede usar en una casa o en un negocio, a través de cualquier medio que sea necesario, ya sea una red inalámbrica, banda ancha, etc.

Hay un cierto número de direcciones IP que se reservan para utilizarlas en la red interna. Estas direcciones definidas en RFC 1918 permiten asegurar a un servidor Proxy (que administra la conexión a Internet de una empresa) una diferenciación satisfactoria entre la red pública (Internet) y la red privada (intranet). Así, cada empresa conectada a Internet puede utilizar las mismas direcciones IP privadas internamente y diferenciar los accesos a Internet por medio de una única dirección IP pública externa [2].

Estas direcciones privadas son:

- 10.0.0.0 a 10.255.255.255
- 172.16.0.0 a 172.31.255.255
- 192.168.0.0 a 192.168.255.255

1.1.2.- Protocolos de transporte

En el modelo OSI, esta es la cuarta capa. Constituye la tercera dentro del protocolo TCP/IP, y con los mismos usos. Los niveles 3 y 4 a veces se agrupan bajo el nombre de capas medias. Las aplicaciones de tipo cliente/servidor que utilizan TCP/IP pueden emplear dos modos de transporte: orientado a la conexión gracias a TCP (Transmission Control Protocol) y orientado a la no conexión, mediante UDP (User Datagram Protocol) [2].

La capa de transporte es responsable de establecer una sesión de comunicación temporal entre dos aplicaciones y de transmitir datos entre ellas. TCP es considerado un protocolo seguro orientado a la conexión, ya que garantiza que los datos lleguen al destino, diferente al protocolo UDP, ya que es un protocolo orientado a la no conexión y no proporciona confiabilidad, pero los dos protocolos se encuentran en la capa de transporte como se muestra en la Figura 1-1) [2].

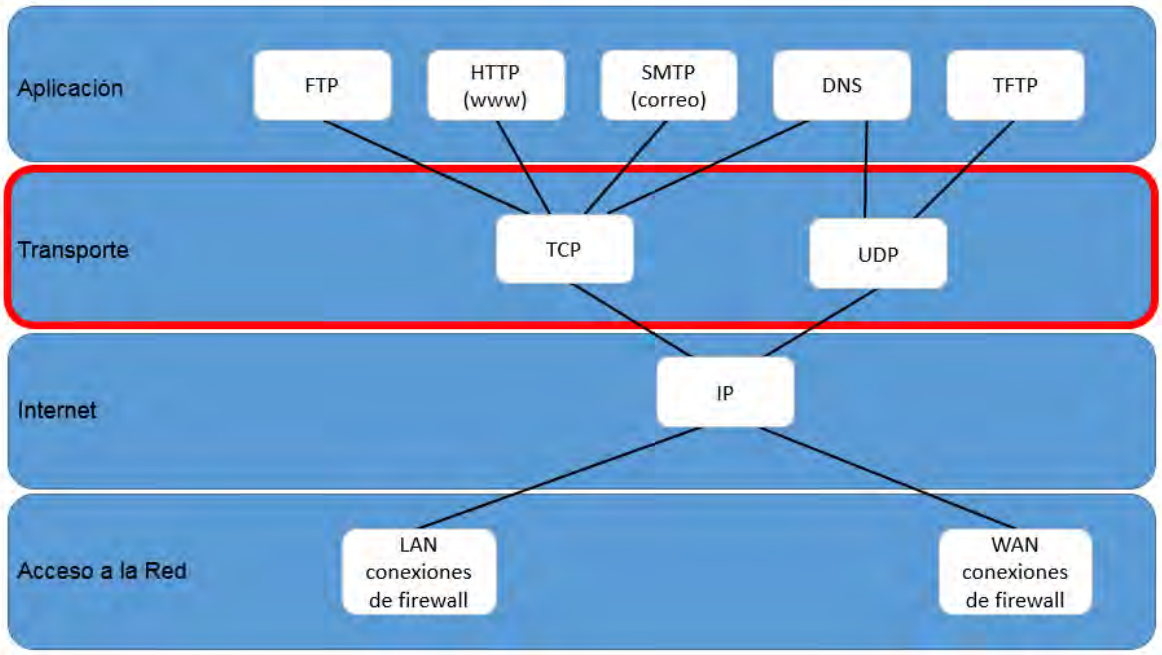


Figura 1-1. Protocolo TCP y UDP en la capa de transporte

1.1.3.- TCP y UDP

TCP se considera un protocolo de transporte confiable, lo que significa que incluye procesos para garantizar la entrega confiable entre aplicaciones mediante el uso de entrega con acuse de recibo. La función del protocolo de transporte TCP es similar al envío de paquetes de los que se hace un seguimiento de origen a destino [3].

Con TCP, las tres operaciones básicas de confiabilidad son las siguientes:

- Seguimiento de segmentos de datos transmitidos.
- Acuse de recibo de datos.
- Retransmisión de cualquier dato sin acuse de recibo.

TCP divide el mensaje en partes pequeñas, conocidas como segmentos. Los segmentos se numeran en secuencia y se pasan al proceso IP para armarse en paquetes. TCP realiza un seguimiento del número de segmentos que se enviaron a un host específico desde una aplicación específica. Si el emisor no recibe un acuse de recibo antes del transcurso de un período determinado, supone que los segmentos se perdieron y los vuelve a transmitir. Sólo se vuelve a enviar la parte del mensaje que se perdió, no todo el mensaje. En el host receptor, TCP se

encarga de rearmar los segmentos del mensaje y de pasarlos a la aplicación. El protocolo de transferencia de archivos (FTP) y el protocolo de transferencia de hipertexto (HTTP) son ejemplos de las aplicaciones que utilizan TCP para garantizar la entrega de datos [3].

Los procesos de confiabilidad generan una sobrecarga adicional en los recursos de la red debido a los procesos de acuse de recibo, rastreo y retransmisión. Para admitir estos procesos de confiabilidad, se intercambian más datos de control entre los hosts emisores y receptores. Esta información de control está incluida en un encabezado TCP [3].

Si bien las funciones de confiabilidad de TCP proporcionan una comunicación más sólida entre aplicaciones, también representan una sobrecarga adicional y pueden provocar demoras en la transmisión. Existe un compromiso entre el valor de la confiabilidad y la carga que implica para los recursos de la red. La imposición de sobrecarga para garantizar la confiabilidad para algunas aplicaciones podría reducir la utilidad a la aplicación e incluso ser perjudicial para esta. En estos casos, UDP es un protocolo de transporte más adecuado [3].

UDP proporciona solo las funciones básicas para entregar segmentos de datos entre las aplicaciones, con muy poca sobrecarga y revisión de datos. El protocolo UDP se conoce como protocolo de entrega de mejor esfuerzo. En el contexto de redes, la entrega de mejor esfuerzo se denomina “poco confiable”, porque no hay acuse de recibo que indique que los datos se recibieron en el destino. Con UDP, no existen procesos de capa de transporte que informen al emisor si la entrega se produjo correctamente [3].

El proceso de UDP es similar al envío por correo de una carta simple sin registrar. El emisor de la carta no sabe si el receptor está disponible para recibir la carta ni la oficina de correos es responsable de hacer un seguimiento de la carta o de informar al emisor si esta no llega a destino [3].

1.2.- Conmutación

Cuando se dispone de varios dispositivos, se tiene el problema de encontrar la forma de conectarlos para que la comunicación uno a uno sea posible. Una solución es instalar una conexión punto a punto entre cada par de dispositivos (una topología en malla) o entre un dispositivo central y cada dispositivo (una topología en estrella). Sin embargo, estos métodos, son impracticos cuando se aplican a redes muy grandes [4].

Una solución mejor es la conmutación. Una red conmutada consta de una serie de nodos interconectados, denominados conmutadores o switches. Los conmutadores son dispositivos hardware y/o softwares capaces de crear conexiones temporales entre dos o más dispositivos conectados al conmutador. En una red conmutada, algunos de estos nodos se conectan a dispositivos de comunicación. El resto se utiliza sólo para realizar el encaminamiento [4].

1.2.1.- Funcionalidad de switching

El proceso de encapsulamiento de los datos sigue la siguiente secuencia:

1. Datos
2. Segmentos
3. Paquetes
4. Tramas
5. Bits

La Tabla 1 describe las diferentes capas del modelo OSI, su correspondiente PDU (Protocol Data Unit) y el dispositivo asociado a estas:

Tabla 1. Capas del modelo OSI, su correspondiente PDU y dispositivo asociado

Capa	PDU	Dispositivo
7 Aplicación	Datos	Aplicaciones
6 Presentación		
5 Sesión		
4 Transporte	Segmentos	Puertos TCP
3 Red	Paquetes	Router
2 Enlace de datos	Tramas	Switch
1 Física	Bits	Medios

1.2.2.- Conmutación de capa 2

La función de conmutación de capa 2 es proporcionada por aquellos dispositivos que son capaces de transportar tramas entre dos interfaces ofreciendo las siguientes capacidades:

- Aprender direcciones MAC a partir de una trama entrante.
- Mantener actualizada una tabla en la que se asocie dirección MAC y puerto por el que se aprendió.
- Reenviar por todos los puertos excepto por el que se recibió tramas de broadcast y multicast.
- Evitar bucles de red entre los diferentes equipos involucrados utilizando el protocolo STP o cualquier otra tecnología usada a este fin.

Es muy importante tener clara la diferencia entre un bridge (puente) y un switch y su desempeño en esta capa, ya que son dispositivos involucrados fundamentalmente en este nivel. Los bridges son dispositivos capaces de conmutar tramas realizando las funciones arriba detalladas, mientras que los switches, además son capaces de conmutar las tramas y desarrollar esas funcionalidades utilizando ASIC (Application Specific Integrated Circuits) especifico, es decir, los switches son capaces de realizar esas funciones por hardware, de forma mucho más eficiente y rápida [5].

Por ejemplo, considere la Figura 1-3, que detalla un switch de cuatro puertos con las estaciones A en el puerto 1, B en el puerto 2, C en el puerto 3 y D en el puerto 4. Supongamos que A desea comunicarse con B y C desea comunicarse con D.

En un único puente de CPU, este reenvío se realizaría típicamente en software, donde la CPU captaría tramas de los cuadros de cada uno de los puertos y los reenviaría a los puertos de salida apropiados. Este proceso es altamente ineficiente en un escenario como el indicado, donde el tráfico entre A y B no tiene relación con el tráfico entre C y D.

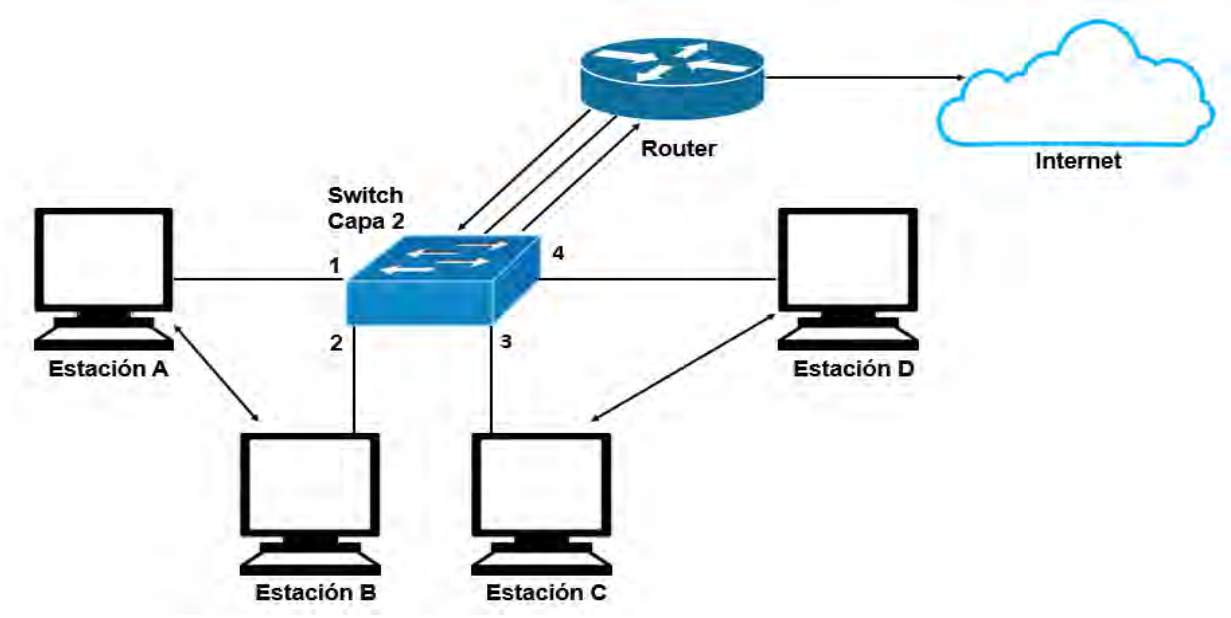


Figura 1-2. Ejemplo de conmutación de capa 2

Entrando en la conmutación de capa 2 basada en hardware. Los switches de capa 2 con su soporte de hardware son capaces de reenviar estas tramas en paralelo para que A y B y C y D puedan tener conversaciones simultáneas. El paralelismo tiene muchas ventajas. Suponga que A y B son estaciones NetBIOS, mientras que C y D son estaciones de Protocolo de Internet (IP). No puede haber razón para la comunicación entre A y C y A y D. La conmutación de la capa 2 permite esta coexistencia sin sacrificar la eficiencia.

1.3.- Switch Capa 3

Para el propósito de este tema, los switches de capa 3 son ruteadores súper rápidos que realizan el reenvío de capa 3 en hardware [5].

Es muy importante tener en cuenta la diferencia de la conmutación en capa 3 y el enrutamiento en capa 3 [5].

Los dispositivos involucrados en el enrutamiento de capa 3 realizan las siguientes funciones:

- Los paquetes se reenvían entre redes basándose en direcciones de capa 3.

- El camino óptimo entre dos puntos se calcula teniendo en cuentas diferentes métricas como pueden ser saltos, retardos, ancho de banda, combinación de las anteriores, etc.
- Para reenviar un paquete, el router busca en la tabla de enrutamiento cual es la dirección IP del siguiente salto para el destino concreto y la interfaz saliente del router.
- El camino óptimo para un destino puede ser elegido entre varias posibilidades, incluso puede ocurrir que existan varios caminos óptimos.
- Los equipos se comunican entre sí utilizando protocolos de enrutamiento o routing.
- Los paquetes de broadcast no se reenviarán (excepto en casos muy concretos).
- Los paquetes de multicast se reenviarán dependiendo de la configuración que tengan los routers.

Los dispositivos que son capaces de conmutar en capa 3 realizan las mismas funciones que los dispositivos capaces de enrutar en capa 3, pero teniendo en cuenta que las decisiones de reenvío se realizan mediante ASIC y no mediante ciclos de CPU, como lo hacen los routers, lo cual redunda en una conmutación a velocidad del medio, eliminando así los posibles cuellos de botella del enrutamiento de capa 3 [5].

1.3.1.- Funcionalidad multicapa

Los switches Catalyst de las series 3750, 4500, 6500, etc. Poseen la capacidad de trabajar a nivel de capa 2 y además de enrutar tráfico, esta función se conoce como switching multicapa MLS (Multilayer Switching) [5].

La conmutación multicapa permite que los dispositivos sean capaces de conmutar información combinando las ventajas de la conmutación en las capas 2,3 y 4, ejecutando la conmutación a velocidad de línea y gracias a CEF (Cisco Express Forwarding) la tabla de enrutamiento se mantiene actualizada entro los ASIC permitiendo así un alto rendimiento minimizando los retardos de operación. La conmutación multicapa cumple con las ventajas de la conmutación de capa 2, 3 y 4 pero con un rendimiento y una velocidad mucho mayor [5].

1.3.2- VLAN

Las redes conmutadas permiten eliminar las limitaciones impuestas por las redes planas dividiendo dicha red en varias redes virtuales (VLAN) [5].

Las VLAN proveen seguridad, segmentación, flexibilidad, permiten agrupar usuarios de un mismo dominio de broadcast con independencia de su ubicación física en la red. Usando tecnología VLAN se pueden agrupar lógicamente puertos del switch y los usuarios conectados a ellos en grupos de trabajo con interés común. Las VLAN pueden existir en un solo switch o bien abarcar varios de ellos como se muestra en la figura 1-4 [5].

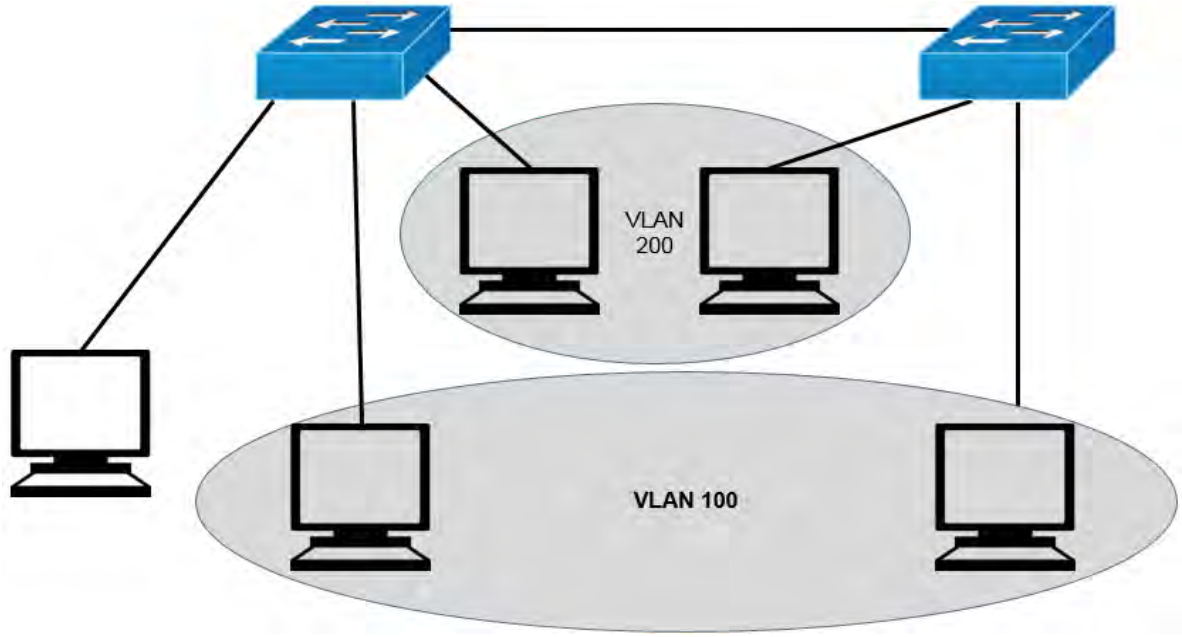


Figura 1-3. VLAN agrupadas lógicamente

Las VLAN estáticas son aquellas en la que los puertos deben agregarse de forma manual. En este tipo de VLAN no es necesario ningún tipo de negociación por parte del switch y toda la configuración se realiza manualmente por el administrador quien es, además, el encargado de asignar cada puerto a cada VLAN de forma manual [5].

1.3.3.- Enrutamiento entre VLAN

Para el envío y recepción de paquetes entre las VLAN es posible utilizar cualquiera de estos mecanismos:

- Un router con conexiones físicas hacia cada una de las VLAN.
- Un router con conexiones lógicas hacia cada una de las VLAN.
- Un switch multicapa.

Los switch multicapa pueden realizar conmutación de capa 2 con interfaces de capa 2 y enrutamiento entre VLAN con interfaces de capa 3. Estas interfaces de capa 3 podrían ser puertos del switch o interfaces SVI (Switch Virtual Interface), que es una interfaz de capa 3 virtual asignada a una VLAN [5].

La figura1-5 muestra cómo se puede utilizar los diferentes tipos de interfaz:

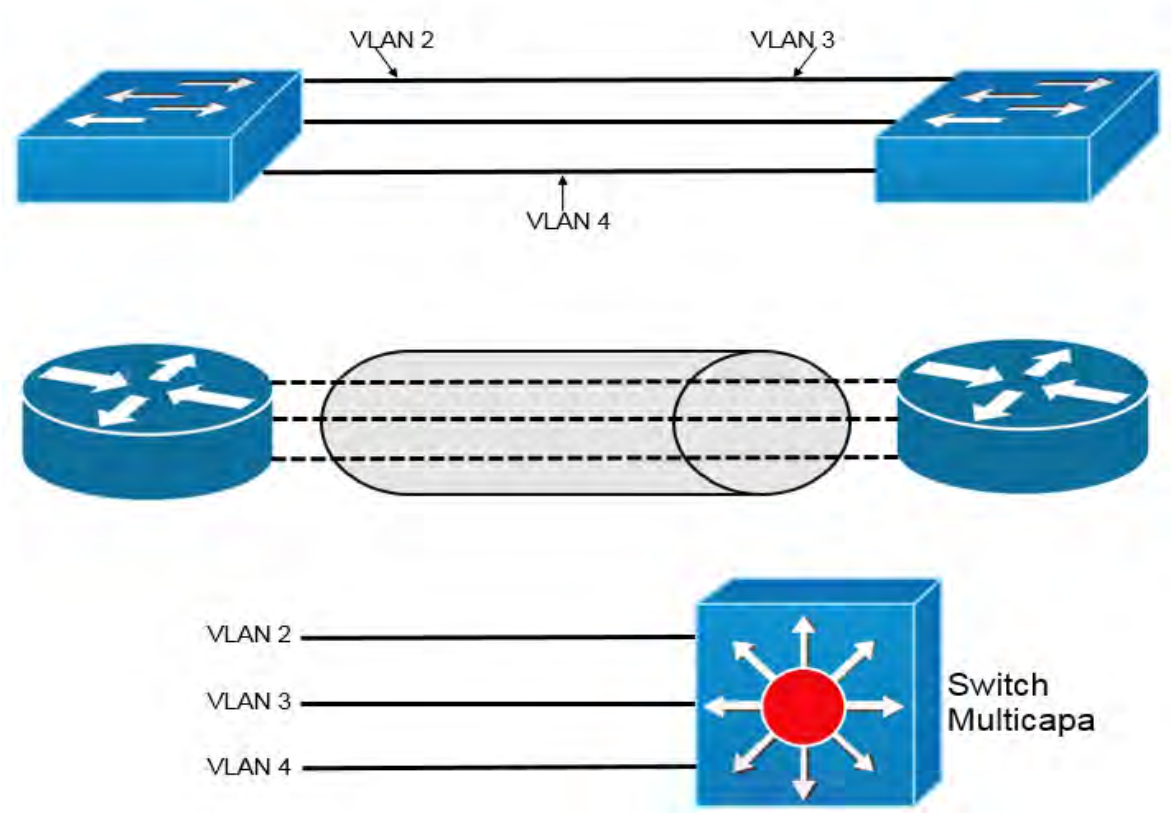


Figura 1-4. Agrupar varias VLAN en un mismo switch capa 2, router o switch capa 3

1.4.- Tipos de Puertos en un Switch

El principio de un conmutador Ethernet es posibilitar un segmento a 100 Mbps (incluso 1 Gbps) por puerto y que cada uno esté conectado a un ordenador. Cuando se transporta una trama a partir de un puerto, el conmutador establece un circuito virtual (CV) que corresponde a la dirección MAC origen y a la dirección MAC destino para los puertos especificados [5].

1.4.1.- Ethernet

Cuando comúnmente se habla de Ethernet se hace referencia a Ethernet basada en la norma de la IEEE 802.3, la cual describe Ethernet como un medio compartido que además es dominio de colisión y de difusión. En Ethernet dos estaciones no pueden transmitir simultáneamente y cuantas más estaciones existan en el segmento más probabilidad existe de colisión, esto solo ocurre en modo half-duplex, en el que una estación no es capaz de transmitir y recibir a la vez [5].

En el caso de full-duplex una estación podría enviar y recibir tramas de forma simultánea, lo cual hará que el rendimiento del medio se duplique, por ejemplo, de 10 Mbps ascienda hasta 20 Mbps, 10 para la transmisión y otros 10 para la recepción [5].

1.4.2.- Fast Ethernet

Fast Ethernet está definido en el estándar IEEE 802.3u, el cual define un nuevo estándar que compartiendo la subcapa de acceso al medio (MAC) con IEEE 802.3 puede transmitir a 100 Mbps [5].

Fast Ethernet proporciona la capacidad de full-duplex al igual que Ethernet, mejorando su rendimiento hasta 200 Mbps, y proporcionando la auto negociación [5].

1.4.3- Gigabit Ethernet

El estándar Gigabit Ethernet (IEEE 802.3z) es una mejora del Fast Ethernet que permite proporcionar velocidades de 1 Gbps, para conseguir este resultado fue necesario el estándar ANSI X3T11 – Fiberchannel junto con el estándar IEEE 802.3. De esta forma surgió un nuevo estándar con el mismo modo de operación que Ethernet, pero a 1 Gbps. Gigabit Ethernet permite la compatibilidad con sus predecesores, existen puertos de 10/100/1000 y es posible la auto negociación, que se realiza igual que en el caso de Fast Ethernet, pero añadiendo como más prioritario 1000BASE-T (full duplex) y posteriormente 1000BASE-T (half duplex) [5].

1.4.4.- 10-Gigabit Ethernet

En el caso de 10-Gigabit Ethernet (IEEE 802.3ae) funciona sobre una nueva capa física totalmente diferente a las anteriores, pero manteniendo la subcapa MAC exactamente igual que las versiones antecesoras. 10-Gigabit Ethernet solo funcionara a 10 Gbps full duplex, en este caso no existe compatibilidad con versiones anteriores de Ethernet ya que la capa física no es compatible [5].

En cuanto a la capa física se dispone de dos tipos de interfaces dependientes del medio PMD (Physical Media Dependent):

- **LAN PHY:** interconecta switches dentro de la misma red de campus.
- **WAN PHY:** interfaces para entornos WAN que utilicen tecnologías de transmisión síncrona.

1.5.- EtherChannel

Los dispositivos Cisco permiten realizar agregación de enlaces con la finalidad de aumentar el ancho de banda disponible a través de la tecnología EtherChannel. La agregación de puertos en Cisco se puede realizar con interfaces Fast Ethernet, Gigabit Ethernet o 10 Gigabit Ethernet [5].

Es posible añadir hasta 8 enlaces de tal forma que se comporten como si solo fuera uno, eliminando la posibilidad de formar bucles de capa 2 debido a que el comportamiento de estos enlaces es el de un único enlace [5].

La tecnología EtherChannel permite una distribución que no llega a ser un balanceo de carga perfecto por los métodos que utiliza, pero permite la correcta distribución del tráfico, además si uno de los enlaces que componen la agregación fallara, el tráfico se distribuiría entre los restantes sin perder la conectividad. Sin embargo no es posible agragar enlaces así sin más, es necesario que todos los enlaces que componen el EtherChannel tengan la misma configuración en cuanto a velocidad, duplex, VLAN que transportan y VLAN nativa [5].

1.5.1.- Distribución de tráfico

El tráfico es distribuido a través de los enlaces del EtherChannel de manera determinística. Sin embargo, la carga no va a ser distribuida equitativamente por ellos, esto depender del algoritmo de encriptación empleado. El algoritmo puede usar la dirección IP de origen, de destino, etc. [5].

Si solamente una IP o número de puerto son computados en el hash (combinación de valores de encriptación), el switch reenvía cada trama utilizando uno o más bits de bajo orden del valor del hash como índice dentro de los enlaces que forman el EtherChannel. Si dos direcciones IP o números de puerto son automatizados en el hash, el switch lleva a cabo una operación XOR (Or exclusiva) en uno o más de los bits de bajo orden de la dirección IP o puerto TCP/UDP como índice dentro de los enlaces que forman el EtherChannel (ver tabla 2) [5].

Tabla 2. Distribución del frame en dos enlaces EtherChannel

Último bit del cuarto octeto de la dirección IP	Operación XOR entre dos miembros EtherChannel
Dirección 1: xxxxxxx0 Dirección 2: xxxxxxx0	xxxxxxx0: Utilizará: 0
Dirección 1: xxxxxxx0 Dirección 2: xxxxxxx1	xxxxxxx1: Utilizará: 1
Dirección 1: xxxxxxx1 Dirección 2: xxxxxxx0	xxxxxxx1: Utilizará: 1
Dirección 1: xxxxxxx1 Dirección 2: xxxxxxx1	xxxxxxx0: Utilizará: 0

1.5.2.- Protocolos de negociación EtherChannel

Actualmente existen dos opciones para utilizar como protocolos de negociación en EtherChannel:

- **PAgP,** propietario de Cisco.
- **LACP,** como solución abierta.

PAgP (Port Aggregation Protocol) es un protocolo propietario de Cisco. Los paquetes PAgP son intercambiados entre switch a través de los enlaces configurados para ello. Los vecinos son identificados y sus capacidades comparadas con las capacidades locales [5].

Para que se forme el EtherChannel los dos puertos han de estar configurados de manera idéntica. Siempre es mejor realizar cualquier cambio sobre la interfaz EtherChannel, de esta manera el cambio afectara a todos los miembros asegurándose así que no haya conflictos de configuración [5].

Existen dos modos de configuración PAgP. Modo activo, desirable, en el cual el switch intentará formar un EtherChannel de manera activa y modo pasivo; auto, en el que el switch responderá a peticiones para formar el EtherChannel [5].

LACP (Link Aggregation Control Protocol) es la opción abierta y viene definida en el estándar 802.3ad, también conocida como IEEE 802.3 Clausula 43 “Link Aggregation”. El funcionamiento es bastante parecido al de PAgP, pero en el caso de LACP se asignan roles a cada uno de los extremos basándose en la prioridad del sistema, que se conforma con 2 bytes de prioridad más 6 de MAC [5].

Los puertos son seleccionados y activados acorde al valor “port priority” (2 bytes de prioridad seguido de 2 bytes de numero de puerto), el valor más bajo indica mayor prioridad. Se puede definir hasta 16 enlaces por cada EtherChannel [5].

Existen dos modos de configuración LACP: modo activo (active), en el cual el switch intentará formar un EtherChannel de manera activa, y modo pasivo (passive), en el que el switch responderá a peticiones de formar el EtherChannel [5].

1.6.- Spanning Tree Protocol

STP (Spanning Tree Protocol) proporciona soporte a nivel capa 2 de forma que los errores o fallas se pueden solventar de manera automática; está definido en el estándar IEEE 802.1D [5].

Un switch capa 2 imita las funciones de un bridge transparente, tiene que ofrecer segmentación entre dos redes mientras permanece de manera transparente para los dispositivos finales que están conectados a él [5].

Los bridges y los switches operan de la siguiente manera:

- Inicialmente un switch no posee ningún conocimiento de la red, por lo que debe “escuchar” las tramas que le llegan a cada uno de sus puertos para averiguar en qué red reside cada dispositivo. El bridge asume que cada dispositivo de origen está localizado detrás del puerto del cual ha recibido dicha trama mirando su MAC. A medida que el proceso de escucha continúa el bridge construye una tabla que relaciona direcciones MAC de origen con números de puertos. El bridge puede actualizar la tabla para reemplazar las direcciones MAC o detectar el cambio de localización de un puerto a otro. De esta manera podrá enviar las tramas mirando la MAC de destino buscando dicha dirección en la tabla y enviarla posteriormente a través del puerto donde el dispositivo final está localizado [5].
- Si una trama llega con una dirección de destino broadcast el bridge debe enviar la trama a través de todos los puertos disponibles salvo por el puerto donde se ha recibido. A este proceso se le llama flood. Si una trama llega con una dirección de destino que no es localizada en la tabla del bridge, este no podrá determinar por cual de sus puertos debe enviar la trama de destino. En estos casos el bridge trata esta trama como si fuera un broadcast siguiendo el mismo proceso que haría con una trama de difusión. A estas tramas se las llaman *unknow unicast.* Una vez que el destino responde a dicha trama, el bridge localiza el puerto para usos futuros [5].

La redundancia aumenta la disponibilidad de la topología de red al proteger la red de un único punto de falla, como un cable de red o switch que fallan. Cuando se introduce la redundancia física en un diseño, se producen bucles y se duplican las tramas. Esto trae consecuencias graves para las redes conmutadas. El protocolo de árbol de expansión (STP) fue desarrollado para enfrentar estos inconvenientes [6].

1.6.1.- Solución a los bucles de capa 2

Los switch de capa 2 cuando funcionan en paralelo, no se da cuenta de la existencia del otro. STP proporciona el mecanismo necesario para que los switches reconozcan la existencia del otro y puedan negociar un camino libre de bucles. Estos bucles son descubiertos antes de que puedan formarse y los enlaces conflictivos son desconectados automáticamente. Cada switch ejecuta el algoritmo STP basándose en la información recibida por los switch vecinos. Este algoritmo elige un punto de referencia en la red y calcula todos los caminos redundantes. Cuando localiza caminos redundantes STP elige alguno de esos caminos para enviar tramas y bloquea el resto de los posibles caminos. STP calcula una estructura de árbol que abarca todos los switches de un segmento determinado. Los caminos redundantes son colocados en un estado de bloqueo evitando que se envíen tramas. Obteniendo como resultado una red libre de bucles. En el caso que el puerto que este enviando tramas falle, STP vuelve a recalcular su algoritmo para que los enlaces bloqueados apropiados sean reactivados [5].

1.6.2.- Funcionamiento de STP

STP funciona de manera que los switches puedan operar entre ellos intercambiando mensajes de datos a través de las BPDU (Bridge Protocol Data Units). En la terminología de STP es común hablar de bridge en lugar de switch debido a que originalmente STP fue diseñado para los puentes o bridges. Cada switch envía las BPDU a través de un puerto usando la dirección MAC de ese switch por lo que las BPDU son enviadas con la dirección de destino multicast 01-80-C2-00-00-00 [5].

Existen dos tipos de BPDU:

- Configuration BPDU: utilizadas para el cálculo STP.
- Topology Change Notification (TCN) BPDU: utilizada para anunciar los cambios en la topología de la red.

Las configuraciones BPDU contienen campos mostrados en la Tabla 3:

Tabla 3. Cantidad de bytes por BPDU

Campo	Cantidad de Bytes
Protocol ID	2
Version	1
Message Type	1
Flags	1
Root Bridge ID	8
Root Path Cost	4
Sender Bridge ID	8
Port ID	2
Message Age	2
Maximum Age	2
Hello Time	2
Forward Delay	2

El intercambio de los mensajes BPDU tiene la función de elegir puntos de referencia para conseguir una topología STP estable. Los bucles pueden ser identificados y eliminados poniendo puertos redundantes específicos en los estados de bloqueando o standby. Varios de los campos de la BPDU son relativos a la identificación del switch, el coste de los caminos y a los valores de los temporizadores, todos ellos trabajan al unísono para que la red pueda converger en una topología de STP común eligiendo los mismos puntos de referencia dentro de la red [5].

Por defecto las BPDU son enviadas a través de todos los puertos de cada 2 segundos de tal manera que la información de la topología actual se intercambia para identificar los bucles rápidamente [5].

1.6.3.- Elección del switch raíz

Todos los switches de la red deben estar de acuerdo en elegir un marco común como referencia para crear una topología de capa 2 libre de bucles. Este punto de referencia se llama switch raíz o root bridge [5].

Para determinar el root bridge se lleva a cabo un proceso de elección, cada switch posee un bridge ID, que es un identificador único que lo diferencia de todos los demás switches. El bridge ID es un valor de 8 bytes que consiste en los campos que se detallan:

- **Bridge Priority:** son 2 bytes, es la prioridad de un switch en relación a todos los demás, este campo puede tener un valor entre 0 y 65535, cuyo valor por defecto es de 32768 [5].
- **Dirección MAC** son 6 bytes, esta dirección puede tener origen en un módulo supervisor o en el *backplane*, dentro de un rango de 1024 direcciones que son asignadas a cada uno dependiendo del modelo de switch. De cualquiera de las maneras es única e inamovible [5].

Cuando un switch se enciende no tiene una visión clara a su alrededor, por lo que se considera a sí mismo como root bridge. El proceso de elección inicia cuando todos los switches envían BPDU con el ID del root bridge puerto como su propio ID y su S*ender Bridge* ID, que es su propio ID. Este último indica a los demás switches quien es el verdadero emisor del mensaje BPDU. A partir de la elección del root bridge las BPDU de configuración solo son enviadas por el root bridge. Todos los demás switches deben confiar en estas BPDU añadiendo el *Sender Bridge* ID a ese mensaje. Los mensajes BPDU recibidos son analizados prioridad, que debe ser de un valor menor que las demás. Para el caso de que dicho valor de prioridad sea igual al actual, la MAC más baja se aplicara para la determinación de la prioridad [5].

Cuando un switch escucha acerca de un root bridge, es decir, un switch con una prioridad menos a la de sí mismo, reemplaza el root bridge ID anunciando en sus BPDU. El switch anunciara entonces dicho ID como root y su propio *Sender bridge* ID. Los switches convergen y se ponen de acuerdo sobre quien será el root bridge [5].

1.6.4.- Elección del puerto raíz

El puente raíz sirve como punto de referencia para todos los cálculos de árbol de expansión para determinar las rutas redundantes que deben bloquearse. Un proceso de elección determina el switch que se transforma en el puente raíz [6].

Una vez determinado el root bridge, cada uno de los demás switches que no son root deben identificar su posición en la red en relación con el root bridge. Esta acción se realiza seleccionando solamente un puerto raíz, en cada uno de los

switches. El puerto raíz siempre apunta hacia el actual root bridge. STP utiliza el concepto de coste para determinar y seleccionar un puerto raíz, lo que significa evaluar el coste de la ruta llamado *Root Path Cost.* Este valor es el coste acumulativo de todos los enlaces hacia el root bridge. Un simple enlace de un switch también conlleva un coste asociado a él [5].

A medida que los *Root Path Cost* atraviesan la red, otros switch pueden modificar su valor de manera acumulativa. El *Root Path Cost* no está dentro de la BPDU, solamente concierne al puerto del switch local donde éste reside. Cuanto mayor sea el ancho de banda del enlace menor será el coste de enlace. IEEE 802.1D define un *Root Path Cost* de 1000 Mbps dividido por el ancho de banda del enlace en Mbps. Las redes modernas superan este valor por lo que fue necesario cambiar los valores del coste [5].

La Tabla 4 muestra los valores de costos por ancho de banda:

Tabla 4. Valor de costos por ancho de banda

Ancho de banda	Coste antiguo de STP	Coste actual de STP
4 Mbps	250	250
10 Mbps	100	100
16 Mbps	63	62
45 Mbps	22	39
100 Mbps	10	19
155 Mbps	6	14
622 Mbps	2	6
1 Gbps	1	4
10 Gbps	0	2

El valor del coste se determina de la siguiente manera:

- El root bridge envía una BPDU con un valor de root path cost de 0 ya que su puerto está asociado directamente al switch.
- Cuando el siguiente switch recibe la BPDU añade a su propio coste donde fue recibida la BPDU.
- El vecino envía esa BPDU con el valor acumulativo modificando así el root path cost.
- El incremento es directamente proporcional al coste de los puertos de entrada a medida que la BPDU se recibe en cada uno de los switches de la topología.
- El root path cost se va incrementando a medida que las BPDU entran en los puertos.

Después de este incremento el switch guarda ese valor en la memoria, el valor más bajo de los almacenados será el nuevo path cost [5].

1.6.5.- Elección del puerto designado

Para eliminar la posibilidad de bucles de capa 2 en la red, STP realiza un cálculo para determinar los puertos designados en cada segmento de red. Cuando una trama aparece en un segmento todos los switches intentan enviarla hacia el otro segmento. Este comportamiento debe ser controlado de tal manera que solo un puerto envié tráfico desde y hacia ese segmento. El puerto que realiza esta tarea se llama puerto designado [5].

Los switches eligen solo un puerto designado para cada segmento basándose en el menor root path cost acumulativo hacia el root bridge. Cuando un switch recibe un root path cost mayor al que tiene asume el rol de puerto designado para ese segmento por el que recibe la root path costo mayor que la que posee [5].

Los puertos siguen en actividad por lo que aun así pueden producirse bucles. STP tiene una serie de estados progresivos por los cuales cada puerto debe pasar [5] .

En cada proceso de determinación cuando dos o más enlaces tengan el mismo root path cost, se determina la diferencia en el siguiente orden:

1. El menor de los root bridge ID.
2. El menor root path cost hacia el root bridge.
3. El menor sender bridge ID.
4. El menor sender port ID.

1.6.6.- Estados STP

El árbol de expansión queda determinado inmediatamente después de que el switch finaliza el proceso de arranque. Si un puerto de switch pasa directamente del estado de bloqueo al de reenvío sin información acerca de la topología completa durante la transición, el puerto puede crear un bucle de datos temporal. Por este motivo, STP introduce los cinco estados de puerto [6].

Los estados de STP son los siguientes:

- **Desconectado**, son los puertos que han sido apagados administrativamente por el administrador de la red o por fallos en el sistema, es un estado que no participa de la progresión normal de STP para un puerto [5].
- **Bloqueando**, es el estado de un puerto cuando se inicia de tal forma que no puede generar bucles de red. En este estado un puerto no puede recibir ni transmitir datos, solo puede recibir BPDU desde los vecinos sin poder añadir direcciones MAC en su tabla; además, los puertos que están en modo standby para evitar bucles entran con el estado bloqueando [5].
- **Escuchando,** un puerto pasa a este estado si el switch interpreta que el puerto puede ser seleccionado como puerto raíz o puerto designado como

previo al envió de tramas. En este estado no se pueden enviar ni recibir tramas, pero si pueden recibir y enviar BPDU de tal manera que el switch participa activamente en el proceso de STP. Si no hay mayores cambios el puerto vuelve al estado anterior, si por el contrario los cambios ocurren se pasa al siguiente estado [5].

- **Aprendiendo,** luego del periodo transcurrido llamado *forward delay* el puerto pasa a este estado donde puede enviar y recibir BPDU registrando, ahora sí, las MAC a las tablas correspondientes. El puerto participa de esta manera de forma silenciosa en el proceso mientras puede tener una visión de las tablas de direcciones MAC [5].
- **Enviando,** después de otro periodo transcurrido el puerto pasa a este estado donde puede enviar y recibir tramas, aprender direcciones MAC y guardarlas en las tablas, enviar y recibir BPDU. El puerto es ahora completamente funcional en la topología STP [5].

1.6.7.- Temporizadores de STP

STP opera de tal manera que los switches intercambian las BPDU entre sí.

Las BPDU toman una cantidad finita de tiempo para viajar en la red de un switch hacia otro, además los cambios o fallos en la topología pueden influir en la propagación de las BPDU. Es importante que los switches no converjan hasta que todos estos reciban exactamente la misma información [5].

Por defecto las BPDU son enviadas a través de todos los puertos cada 2 segundos de tal manera que la información de la topología actual se intercambia para identificar los bucles rápidamente [5].

- **Hello,** es el intervalo de tiempo en el cual las *configuration* BPDU se envían desde el root switch. La configuración se realiza únicamente en el root switch y determina el temporizador hello de todos los demás switch debido a que estos solo confían en las BPDU de configuración recibidas desde el root. Aun así, todos los demás switches tienen un temporizador local incorporado utilizado para temporizar las BPDU cuando hay cambios de topologías. El valor estándar por defecto es de 2 segundos [5].
- **Forward delay,** es el intervalo de tiempo en el que un switch está entre los estados escuchando y aprendiendo, el valor por defecto es de 15 segundos para cada uno de los estados [5].
- **Max (máximum) Age,** es el intervalo de tiempo que un switch guarda una BPDU antes de descartarla. Mientras se está ejecutando STP cada puerto del switch mantiene un registro de la mejor BPDU que ha escuchado. En caso de que el puerto del switch pierda contacto con el origen de esa BPDU el switch asume que ha ocurrido algún cambio en la topología, cuando el periodo Max Age termine la BPDU es eliminada. Por defecto el valor de este temporizador es de 20 segundos [5].

Los temporizadores de STP pueden ser ajustados y configurados en el switch, no obstante, cualquier cambio debe ser debidamente planificado y es recomendable hacerlo solo en el root. Todos estos temporizadores son

apropiados para una red de hasta 7 switches, desde el root hasta el más lejano [5].

Capítulo 2 : Routing con Respecto a la Tecnología Cisco

2.1.- Introducción

Las redes hoy en día son importantes como necesarias, hacen que las personas se comuniquen entre sí, que puedan colaborar e interactuar en el trabajo, así como en el hogar. Las redes se pueden utilizar para acceder a páginas web, acceso a internet, tener telefonía de VoIP, videoconferencias, estar en juegos online, realizar compras por internet, realizar trabajos, cursos o escuelas en línea y mucho más.

Los switches Ethernet funcionan en la capa de enlace de datos, la capa 2, y se utilizan para reenviar tramas de Ethernet entre dispositivos dentro de una misma red.

Sin embargo, cuando las direcciones IP de origen y destino están en distintas redes, la trama de Ethernet se debe enviar a un router.

Los routers o switches capa 3 conectan una red a otra red. El router o switch capa 3 es responsable de la entrega de paquetes a través de distintas redes. El destino de un paquete IP puede ser un servidor web en otro país o un servidor de correo electrónico en la red de área local.

El router o switch de capa 3 usa su tabla de enrutamiento para encontrar la mejor ruta para reenviar un paquete. Es responsabilidad de los routers o switches entregar esos paquetes a su debido tiempo. La efectividad de las comunicaciones de internetwork depende, en gran medida, de la capacidad de los routers o switches de reenviar paquetes de la manera más eficiente posible.

Cuando un host envía un paquete a un dispositivo en una red IP diferente, el paquete se reenvía al gateway predeterminado, ya que los dispositivos host no pueden comunicarse directamente con los dispositivos que están fuera de la red local. El gateway predeterminado es el destino que enruta el tráfico desde la red local hacia los dispositivos en las redes remotas. Con frecuencia, se utiliza para conectar una red local a Internet.

Debido a que los routers pueden enrutar paquetes entre redes, los dispositivos que están en redes distintas se pueden comunicar. En pocas palabras un router o switch de capa 3 conecta una red con otra red.

La comunicación entre redes no sería posible sin un router que determine la mejor ruta hacia el destino y que reenvíe el tráfico al router siguiente en esa ruta. El router o switch de capa 3 es responsable del enrutamiento del tráfico entre redes.

2.1.1.- Conexión por medio de routers

La mayoría de los usuarios desconocen la presencia de varios routers en su propia red o en Internet. Los usuarios esperan poder acceder a páginas web, enviar correo electrónico y descargar música, sin importar si el servidor al que acceden está en su propia red o en otra. Los profesionales de redes saben que es el router el que se encarga del reenvío de paquetes de una red a otra, desde el origen inicial hasta el destino final [6].

Un router conecta varias redes, lo que significa que posee varias interfaces, cada una de las cuales pertenece una red IP diferente. Cuando un router recibe un paquete IP en una interfaz, determina qué interfaz debe usar para reenviar el paquete hacia el destino. La interfaz que usa el router para reenviar el paquete puede ser el destino final o una red conectada a otro router que se usa para llegar a la red de destino [6].

Generalmente, cada red a la que se conecta un router requiere una interfaz separada. Estas interfaces se usan para conectar una combinación de redes de área local (LAN) y redes de área extensa (WAN). Por lo general, las LAN son redes Ethernet que contienen dispositivos como computadoras, impresoras y servidores. Las WAN se usan para conectar redes a través de un área geográfica extensa. Por ejemplo, las conexiones WAN suelen utilizarse para conectar una LAN a la red del proveedor de servicios de Internet (ISP) [6].

2.1.2.- Funciones del router

Las funciones principales de un router son las siguientes:

- Determinar la mejor ruta para enviar paquetes.
- Reenviar paquetes a su destino.

El router usa su tabla de enrutamiento para encontrar la mejor ruta para reenviar un paquete. Cuando el router recibe un paquete, analiza la dirección de destino del paquete y usa la tabla de enrutamiento para buscar la mejor ruta hacia esa red. La tabla de enrutamiento también incluye la interfaz que se debe usar para reenviar los paquetes a cada red conocida. Cuando se encuentra una coincidencia, el router encapsula el paquete en la trama de enlace de datos de la interfaz de salida, y el paquete se reenvía hacia el destino [7].

Un router puede recibir un paquete encapsulado en un tipo de trama de enlace de datos y reenviarlo por una interfaz que usa otro tipo de trama de enlace de datos. Por ejemplo, un router puede recibir un paquete en una interfaz Ethernet, pero debe reenviarlo por una interfaz configurada con el protocolo punto a punto (PPP). La encapsulación de enlace de datos depende del tipo de interfaz en el router y del tipo de medio al que se conecta. Las distintas tecnologías de enlace de datos a las que se puede conectar un router incluyen Ethernet, PPP, Frame Relay, DSL, tecnología de cable y tecnología inalámbrica (802.11, Bluetooth) [7].

En la Figura 2-1, se sigue un paquete desde la computadora de origen hasta la computadora de destino. Debe observarse que el router es responsable de encontrar la red de destino en su tabla de enrutamiento y reenviar el paquete hacia su destino. En este ejemplo, el router R1 recibe el paquete encapsulado en una trama de Ethernet, después de des-encapsular el paquete, el R1 usa la dirección IP de destino del paquete para buscar una dirección de red que coincida en su tabla de enrutamiento. Luego de encontrar una dirección de red de destino en la tabla de enrutamiento, R1 encapsula el paquete dentro de una trama PPP y reenvía el paquete a R2. El R2 realiza un proceso similar [7].

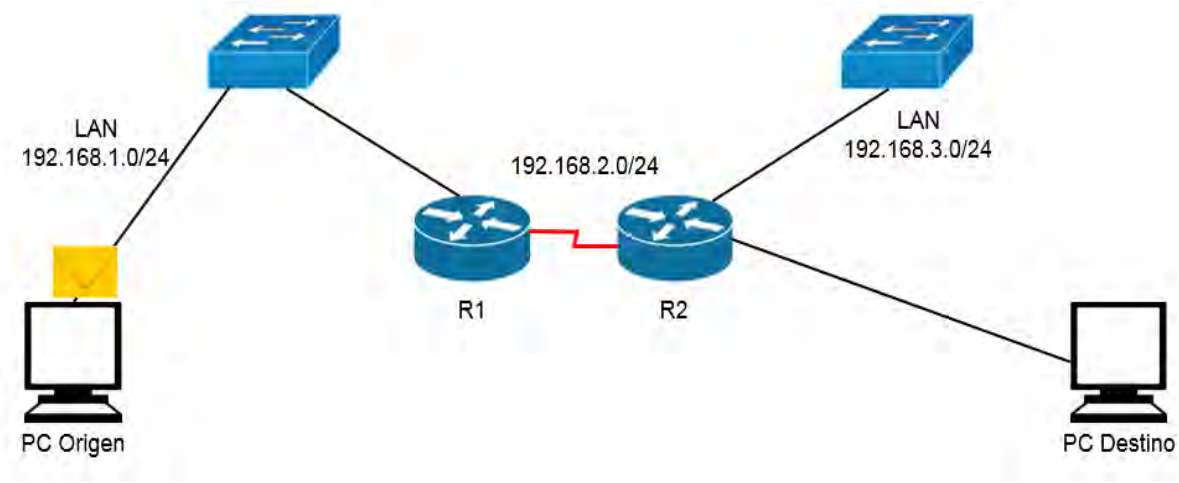


Figura 2-1. Envió de paquete entre routers

Los routers usan rutas estáticas y protocolos de enrutamiento dinámico para descubrir redes remotas y crear sus tablas de enrutamiento [7].

2.1.3.- Conexión de los dispositivos

Para habilitar el acceso a la red, se deben configurar los dispositivos con la información de dirección IP para identificar los elementos correspondientes, entre ellos:

- Dirección IP: identifica un host único en una red local.
- Máscara de subred: identifica con qué subred de la red se puede comunicar el host.
- Gateway predeterminado: identifica el router al que se debe enviar un paquete cuando el destino no está en la misma subred de la red local.

Cuando un host envía un paquete a un dispositivo que está en la misma red IP, el paquete tan solo se reenvía por la interfaz del host al dispositivo de destino [7].

Cuando un host envía un paquete a un dispositivo en una red IP diferente, el paquete se reenvía al gateway predeterminado, ya que los dispositivos host no pueden comunicarse directamente con los dispositivos que están fuera de la red local. El gateway predeterminado es el destino que enruta el tráfico desde la red local hacia los dispositivos en las redes remotas. Con frecuencia, se utiliza para conectar una red local a Internet [7].

Por lo general, el gateway predeterminado es la dirección de la interfaz en el router que se conecta a la red local. El router mantiene entradas de la tabla de enrutamiento de todas las redes conectadas, así como entradas de redes remotas, y determina la mejor ruta para llegar a esos destinos [7].

En este ejemplo, si la PC1 envía un paquete al Web Server (Servidor web) ubicado en 176.16.1.99, descubrirá que este no está en la red local y, por lo tanto, debe enviar el paquete a la dirección de control de acceso a los medios

(MAC) de su gateway predeterminado. La unidad de datos del protocolo (PDU) del paquete que se muestra en la Figura 2-2, identifica las direcciones MAC e IP de origen y destino.

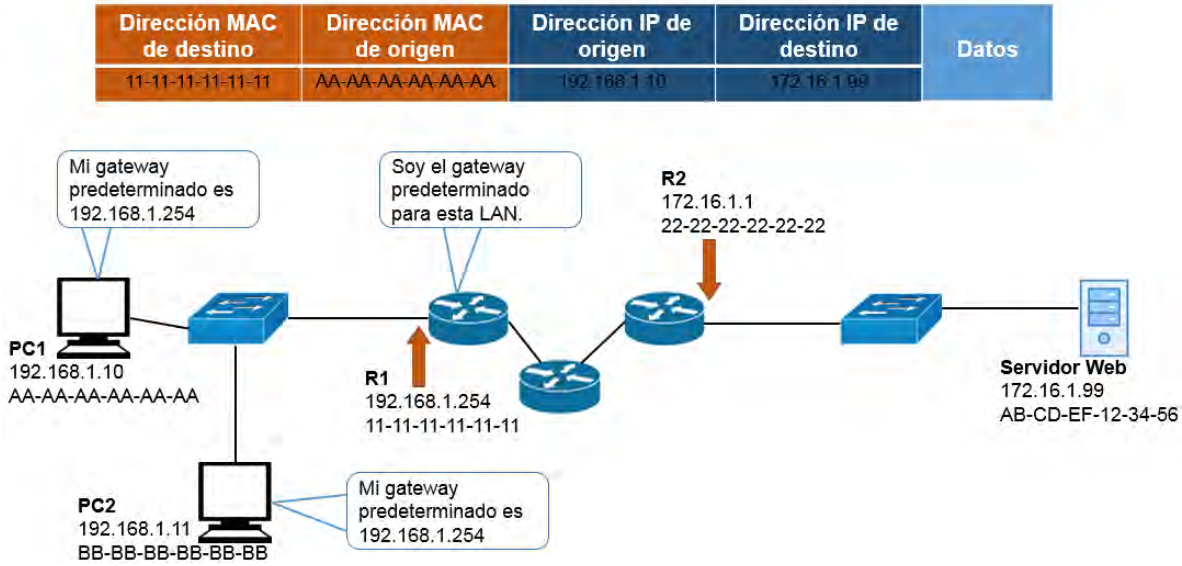


Figura 2-2. Ejemplo del envió de un paquete por capa dos y capa tres

Los routers también se suelen configurar con su propio gateway predeterminado. En ocasiones, este se conoce como “gateway de último recurso” [7].

2.1.4.- Habilitación de IP en un host.

Se puede asignar información de dirección IP a un host de dos formas:

- Estática: se asigna la dirección IP, la máscara de subred y el gateway predeterminado correctos al host de forma manual. También se puede configurar la dirección IP del servidor DNS.
- Dinámica: un servidor proporciona la información de dirección IP mediante el protocolo de configuración dinámica de host (DHCP). El servidor de DHCP proporciona una dirección IP, una máscara de subred y un gateway predeterminado válidos para las terminales. El servidor también puede proporcionar otra información.

En la Figura 2-3 y la Figura 2-4, se proporcionan ejemplos de configuración estática y dinámica de direcciones IPv4.

Por lo general, las direcciones asignadas estáticamente se usan para identificar recursos de red específicos, como servidores e impresoras de red. También se pueden usar en redes más pequeñas con pocos hosts. Sin embargo, la mayoría de los dispositivos host adquieren su información de dirección IPv4 accediendo a un servidor de DHCP. En las empresas grandes, se implementan servidores de DHCP dedicados que proporcionan servicios a muchas redes LAN. En un entorno más pequeño de sucursal u oficina pequeña, un switch Cisco Catalyst o un ISR Cisco pueden proporcionar los servicios de DHCP [7].

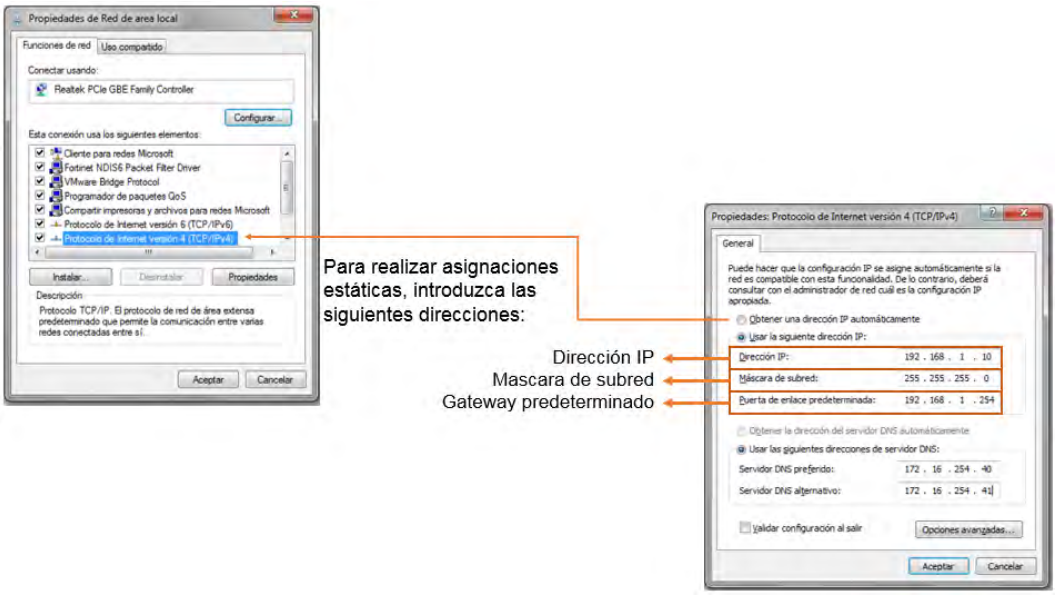


Figura 2-3. Ejemplo de configuración de ruta estática

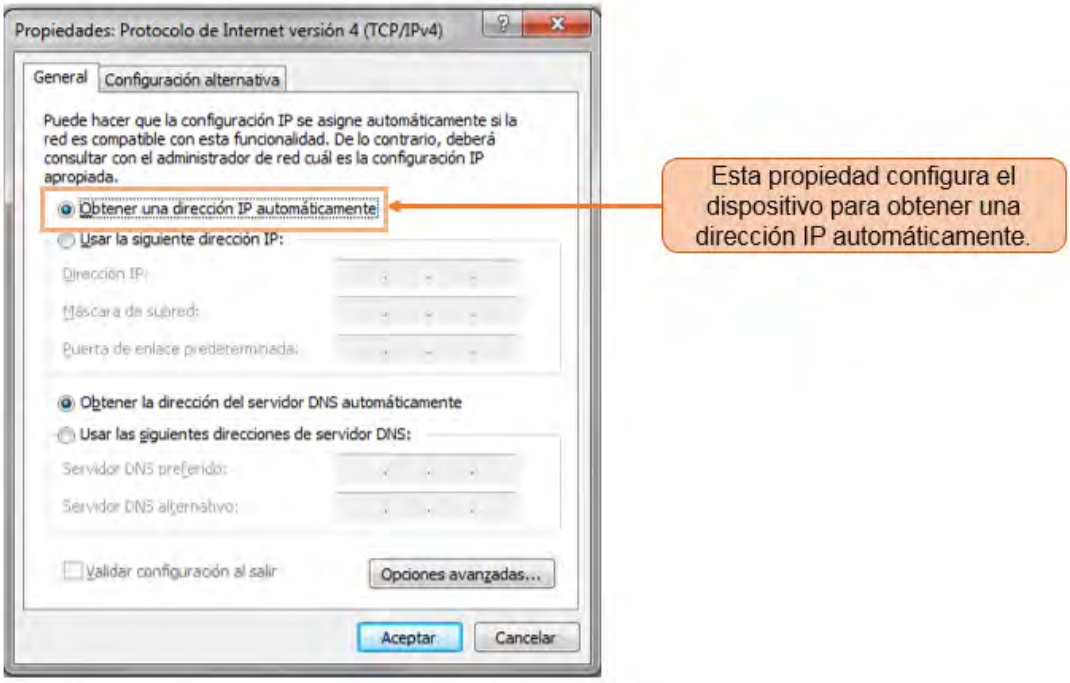


Figura 2-4. Ejemplo de configuración de ruta dinámica

2.2.- Acceso a la Consola

En un entorno de producción, generalmente se accede a los dispositivos de infraestructura de manera remota mediante shell seguro (SSH) o el protocolo de transferencia de hipertexto seguro (HTTPS). El acceso a la consola solo es realmente necesario para realizar la configuración inicial de un dispositivo o si el acceso remoto falla [7].

El acceso a la consola requiere lo siguiente:

- Cable de consola: un cable de consola RJ-45 a DB-9
- Software de emulación de terminal: Tera Term, PuTTY, HyperTerminal

El cable se conecta entre el puerto serie del host y el puerto de consola en el dispositivo. La mayoría de las computadoras portátiles y de escritorio ya no cuentan con puertos serie incorporados. Si el host no tiene ningún puerto serie, se puede utilizar el puerto USB para establecer una conexión de consola. Cuando se usa el puerto USB, se requiere un adaptador especial de puerto serie compatible USB a RS-232 [7].

En la siguiente Figura 2-5, se resumen los requisitos para las conexiones de consola. En la Figura 2-6, se muestran los distintos puertos y cables que se requieren [7].

<table>
<tr><th>Puerto en la computadora</th><th>Cable requerido</th><th>Puerto en el ISR</th><th>Emulación de terminal</th></tr>
<tr><td>Puerto serie</td><td>Cable de consola RJ-45 a DB-9</td><td rowspan="2">Puerto de consola RJ-45</td><td rowspan="3"> 
Tera Term

 
PuTTY</td></tr>
<tr><td rowspan="2">USB puerto tipo A</td><td>• Adaptador de puerto serie compatible con USB a RS-232
• El adaptador puede requerir un controlador de software
• Cable de consola RJ-45 a DB-9</td></tr>
<tr><td>• USB tipo A a USB tipo B (USB mini-B
• Se requiere un controlador de dispositivo</td><td>USB tipo B (USB mini-B)</td></tr>
</table>

Figura 2-5. Requisitos para la conexión de consola

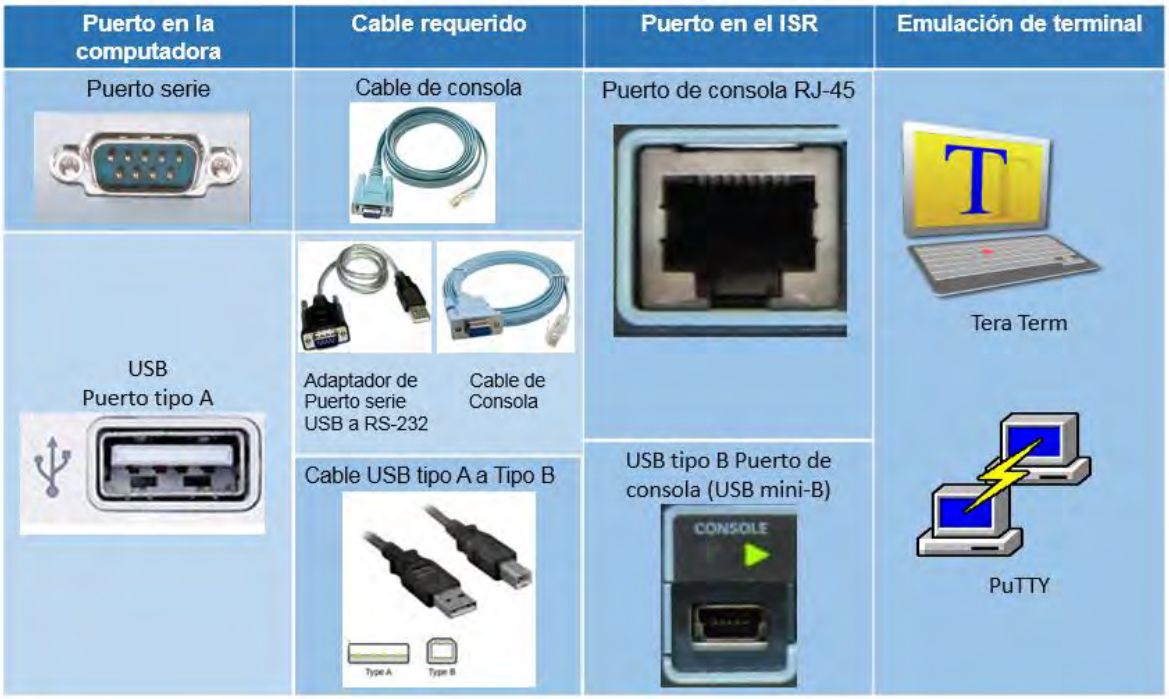


Figura 2-6. Puertos y cables para la conexión por consola

2.3.- Decisiones de Ruteo

Una de las principales funciones del router es el reenvió de paquetes hacia su destino. Se logra mediante una función de switching (que significa literalmente mover paquetes de origen a destino y no se debe confundir con la función de un switch de capa 2), que es el paso que utiliza un router para aceptar un paquete en una interfaz y reenviarlo por otra interfaz. Una responsabilidad clave de la función de conmutación es la de encapsular los paquetes en el tipo de trama de enlace de datos correcto para el enlace de datos de salida [7].

Una vez que el router determinó la interfaz de salida mediante la función de determinación de rutas, el router debe encapsular el paquete en la trama de enlace de datos de la interfaz de salida [7].

El router ejecuta los siguientes tres pasos principales:

1. Des-encapsula el paquete de capa 3 eliminando el encabezado y el tráiler de la trama de capa 2.
2. Examina la dirección IP de destino del paquete IP para encontrar el mejor camino en la tabla de enrutamiento.
3. Si el router encuentra una ruta hacia el destino, encapsula el paquete de capa 3 en una nueva trama de capa 2 y reenvía la trama por la interfaz de salida.

Como se muestra en la Figura 2-7, los dispositivos tienen direcciones IPv4 de capa 3, y las interfaces Ethernet tienen direcciones de enlace de datos de capa 2. Por ejemplo, la PC1 se configuró con la dirección IPv4 192.168.1.10 y una dirección MAC de ejemplo 0A-10. A medida que un paquete se desplaza desde

el dispositivo de origen hacia el dispositivo de destino final, las direcciones IP de capa 3 no se modifican. Sin embargo, las direcciones de enlace de datos de capa 2 cambian en cada salto cuando cada router des-encapsula y vuelve a encapsular el paquete en una nueva trama. Es muy probable que el paquete se encapsule en un tipo de trama de capa 2 diferente de la trama en la que se recibió. Por ejemplo, el router puede recibir una trama de Ethernet encapsulada en una interfaz FastEthernet y, a continuación, procesarla para reenviarla por una interfaz serial como trama encapsulada de protocolo punto a punto (PPP) [7].

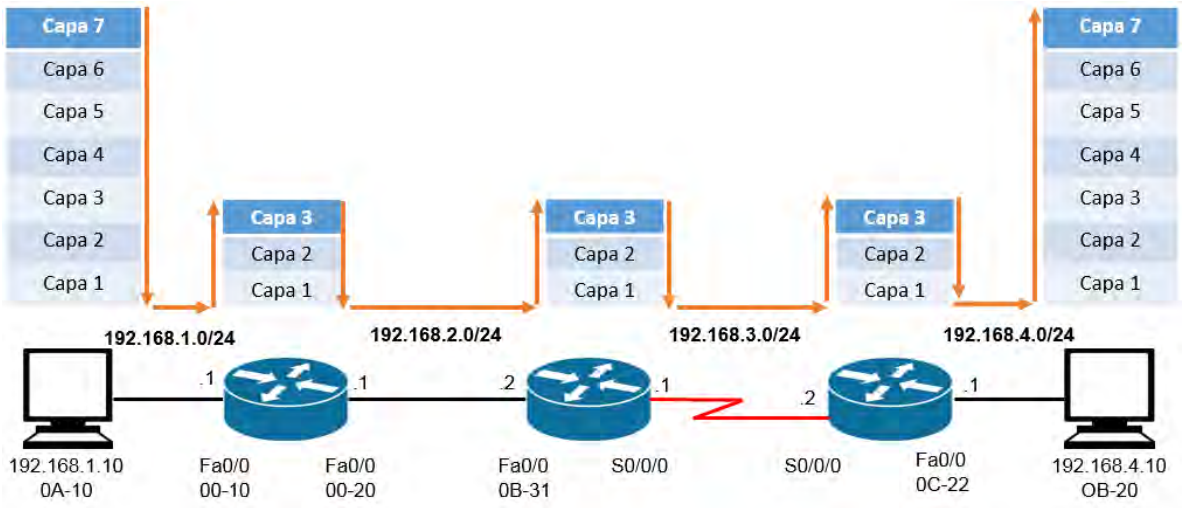


Figura 2-7. Ejemplo de las capas del modelo OSI por dispositivo

2.3.1.- La mejor ruta

La determinación de la mejor ruta implica la evaluación de varias rutas hacia la misma red de destino y la selección de la ruta óptima o la más corta para llegar a esa red. Cuando existen varias rutas hacia la misma red, cada ruta utiliza una interfaz de salida diferente en el router para llegar a esa red [7].

El mejor camino es elegido por un protocolo de enrutamiento en función del valor o la métrica que usa para determinar la distancia para llegar a esa red. Una métrica es un valor cuantitativo que se utiliza para medir la distancia que existe hasta una red determinada. El mejor camino a una red es la ruta con la métrica más baja [7].

Los protocolos de enrutamiento dinámico generalmente usan sus propias reglas y métricas para construir y actualizar las tablas de enrutamiento. El algoritmo de enrutamiento genera un valor, o una métrica, para cada ruta a través de la red. Las métricas se pueden calcular sobre la base de una sola característica o de varias características de una ruta. Algunos protocolos de enrutamiento pueden basar la elección de la ruta en varias métricas, combinándolas en un único valor métrico [7].

A continuación, se indican algunos protocolos dinámicos y las métricas que utilizan:

- Protocolo de información de routing (RIP): conteo de saltos.
- Protocolo OSPF (Open Shortest Path First): el costo de Cisco según el ancho de banda acumulativo de origen a destino.
- Protocolo de routing de gateway interior mejorado (EIGRP): ancho de banda, retardo, carga, confiabilidad.

2.4.- Rutas Estáticas

Hoy en día, el enrutamiento es fundamental para cualquier red de datos ya que transfiere información a través de una internetwork de origen a destino. Los routers son dispositivos que se encargan de transferir paquetes de una red a la siguiente. En muchos casos, los routers utilizan una combinación de protocolos de enrutamiento dinámico y rutas estáticas. Las rutas estáticas son muy comunes y no requieren la misma cantidad de procesamiento y sobrecarga que los protocolos de enrutamiento dinámico [7].

Un router puede descubrir redes remotas de dos maneras:

- Manualmente: las redes remotas se introducen de forma manual en la tabla de rutas por medio de rutas estáticas.
- Dinámicamente: las rutas remotas se descubren de forma automática mediante un protocolo de enrutamiento dinámico.

En la Figura 2-8, se proporciona una situación de ejemplo de enrutamiento estático. En la Figura 2-9, se proporciona una situación de ejemplo de enrutamiento dinámico con EIGRP.

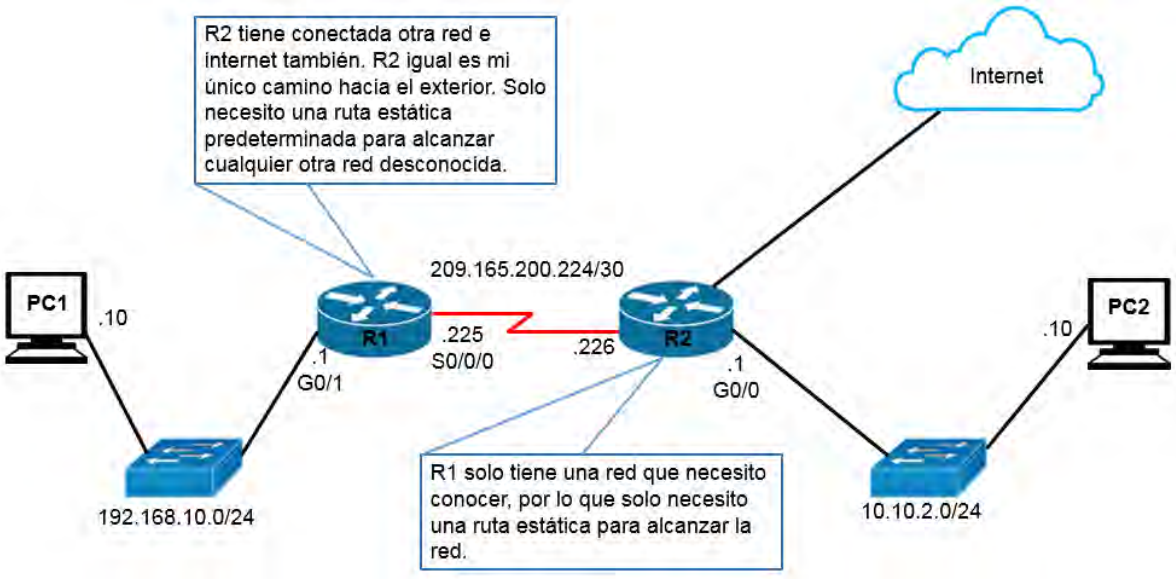


Figura 2-8. Ejemplo de enrutamiento estatico

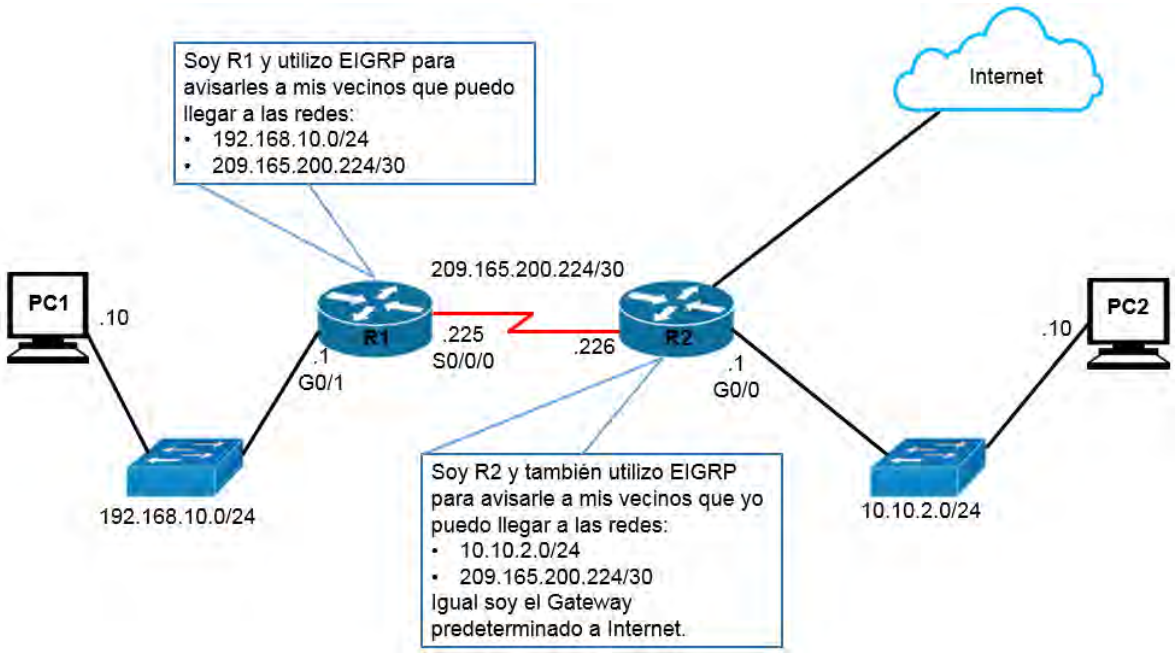


Figura 2-9. Ejemplo de enrutamiento dinámico

Un administrador de red puede configurar una ruta estática de forma manual para alcanzar una red específica. A diferencia de un protocolo de enrutamiento dinámico, las rutas estáticas no se actualizan automáticamente, y se deben volver a configurar de forma manual cada vez que cambia la topología de la red. Una ruta estática no cambia hasta que el administrador la vuelve a configurar en forma manual [7].

2.4.1.- Enrutamiento estático

Las ventajas del enrutamiento estático son:

- Las rutas estáticas no se anuncian a través de la red, lo cual aumenta la seguridad.
- Las rutas estáticas consumen menos ancho de banda que los protocolos de enrutamiento dinámico. No se utiliza ningún ciclo de CPU para calcular y comunicar las rutas.
- La ruta que usa una ruta estática para enviar datos es conocida.

Y sus desventajas serian:

- La configuración inicial y el mantenimiento son prolongados.
- La configuración es propensa a errores, especialmente en redes extensas.
- Se requiere la intervención del administrador para mantener la información cambiante de la ruta.
- No se adapta bien a las redes en crecimiento; el mantenimiento se torna cada vez más complicado.
- Requiere un conocimiento completo de toda la red para una correcta implementación.

Las rutas estáticas son útiles para redes más pequeñas con solo una ruta hacia una red externa. También proporcionan seguridad en una red más grande para ciertos tipos de tráfico o enlaces a otras redes que necesitan más control. Es importante comprender que el enrutamiento estático y el enrutamiento dinámico no son mutuamente excluyentes. En cambio, la mayoría de las redes utilizan una combinación de protocolos de enrutamiento dinámico y rutas estáticas. Esto puede ocasionar que el router tenga varias rutas a una red de destino a través de rutas estáticas y rutas descubiertas dinámicamente. Sin embargo, la distancia administrativa (AD) a una ruta estática es 1. Por lo tanto, una ruta estática tendrá prioridad sobre todas las rutas descubiertas dinámicamente [7].

2.4.2.- Ruta estática por defecto

Una ruta predeterminada es una ruta estática que coincide con todos los paquetes. En lugar de almacenar todas las rutas para todas las redes en la tabla de enrutamiento, un router puede almacenar una única ruta predeterminada que represente cualquier red que no esté en la tabla de enrutamiento [7].

Los routers suelen utilizar rutas predeterminadas configuradas de forma local, o bien, descubiertas por otro router, mediante un protocolo de enrutamiento dinámico. Una ruta predeterminada se utiliza cuando ninguna otra ruta de la tabla de enrutamiento coincide con la dirección IP de destino del paquete. Es decir, si no existe una coincidencia más específica, entonces se utiliza la ruta predeterminada como el gateway de último recurso [7].

En general, las rutas estáticas predeterminadas se utilizan al conectar:

- Un router perimetral a la red de un proveedor de servicios.
- Un router de rutas internas (aquel con solo un router vecino ascendente).

La mayoría del software de enrutamiento IP permite que las rutas por host se especifiquen como un caso especial. Tener rutas por host le da al administrador de red local más control sobre el uso de la red, permite las pruebas y también puede usarse para controlar el acceso por razones de seguridad. Al depurar conexiones de red o tablas de enrutamiento, la capacidad de especificar una ruta especial para una máquina individual resulta especialmente útil [8].

El enrutamiento por defecto es especialmente útil cuando un sitio tiene un pequeño conjunto de direcciones locales y solo una conexión con el resto de Internet. Por ejemplo, las rutas predeterminadas funcionan bien en equipos host que se conectan a una única red física y llegan a un solo enrutador que conduce al resto de Internet. La decisión de enrutamiento consta de dos pruebas: una para la red local y otra predeterminada que apunta al único enrutador. Incluso si el sitio contiene algunas redes locales, el enrutamiento es simple porque consiste en unas pocas pruebas para las redes locales más un valor predeterminado para todos los demás destinos [8].

Como se muestra en la Tabla 5, la sintaxis del comando para una ruta estática predeterminada es similar a la sintaxis del comando de cualquier otra ruta

estática, con la excepción de que la dirección de red es 0.0.0.0 y la máscara de subred es 0.0.0.0 [7].

Tabla 5. Sintaxis del comando para una ruta estática

Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-address | exit-intf}	
Parámetro	
0.0.0.0	
0.0.0.0	
direccion-ip	• Se le denomina comúnmente como dirección IP del router del siguiente salto. • Suele utilizarse para la conexión a un medio de difunsión (Ethernet). • Por lo general, crea una búsqueda recursiva.
	• Use la interfaz de salida para reenviar paquetes a la red de destino. • También se le denomina "ruta estatica conectada directamente". • Suele utilizarse para conectarse en una configuración punto a punto.

Una ruta estática predeterminada IPv4 suele llamarse "ruta de cuádruple cero". [7]

2.4.3.- Direccionamiento de red con clase

Lanzadas en 1981, RFC 790 y RFC 791 describen cómo se asignaron inicialmente las direcciones de red IPv4 según un sistema de clasificación. En la especificación original de IPv4, los autores establecieron las clases para proporcionar tres tamaños distintos de redes para organizaciones grandes, medianas y pequeñas. Por consiguiente, se definieron las direcciones de clase A, B y C con un formato específico para los bits de orden superior. Los bits de orden superior son los bits del extremo izquierdo en una dirección de 32 bits [7].

Como se muestra en la Tabla 6:

Tabla 6. Clases de red tipo A, B, C, D y E

Clase	Bits de orden superior	Inicio	Fin
Clase A	0xxxxxxx	0.0.0.0	127.255.255.255
Clase B	10xxxxxx	128.0.0.0	191.255.255.255
Clase C	110xxxxx	192.0.0.0	223.255.255.255
Clase D (Multidifusión)	1110xxxx	224.0.0.0	239.255.255.255
Clase E (reservada)	1111xxxx	240.0.0.0	255.255.255.255

- Direcciones de clase A que comienzan con 0: diseñadas para organizaciones grandes. Esta clase incluye todas las direcciones de 0.0.0.0 (00000000) a 127.255.255.255 (01111111). La dirección 0.0.0.0 se reserva para el enrutamiento predeterminado y la dirección 127.0.0.0, para la prueba de loopback.
- Direcciones de clase B que comienzan con 10: diseñadas para organizaciones medianas a grandes. Esta clase incluye todas las direcciones de 128.0.0.0 (10000000) a 191.255.255.255 (10111111).
- Direcciones de clase C que comienzan con 110: diseñadas para organizaciones pequeñas a medianas. Esta clase incluye todas las direcciones de 192.0.0.0 (11000000) a 223.255.255.255 (11011111).

Las direcciones restantes se reservaron para multicasting y futuros usos.

- Direcciones de multidifusión de clase D que comienzan con 1110: las direcciones de multidifusión se utilizan para identificar un grupo de hosts que forman parte de un grupo de multidifusión. Esto ayuda a reducir la cantidad de procesamientos de paquetes que realizan los hosts, en especial en los medios de difusión (es decir, las LAN Ethernet). Los protocolos de enrutamiento, como RIPv2, EIGRP y OSPF, utilizan direcciones de multidifusión designadas (RIP = 224.0.0.9, EIGRP = 224.0.0.10, OSPF 224.0.0.5 y 224.0.0.6).
- Direcciones IP de clase E reservadas que comienzan con 1111: estas direcciones se reservaron para uso experimental y futuro.

2.4.4.- Mascara de subred con clase

Cada clase de red tiene asociada una máscara de subred predeterminada.

Como se muestra en la Figura 2-10, las redes de clase A utilizan el primer octeto para identificar la porción de red de la dirección. Esto se traduce a una máscara de subred con clase 255.0.0.0. Debido a que solo se dejaron 7 bits en el primer octeto (recuerde que el primer bit es siempre 0), se elevó el 2 a la 7 a potencia, o se generaron 128 redes. El número real es de 126 redes, porque hay dos direcciones reservadas de clase A (es decir, 0.0.0.0/8 y 127.0.0.0/8). Con 24 bits en la porción de host, cada dirección de clase A tenía capacidad para más de 16 millones de direcciones host individuales [7].

	1er. Octeto	2° Octeto	3er. Octeto	4° Octeto
Siempre comienza con binario 0:	0xxxxxxx			
Equivalente decimal:	0-127			

	Red	Host	Host	Host
Mascara de subred	255	.0	.0	.0

Figura 2-10. Red de clase A

Como se muestra en la Figura 2-11, las redes de clase B utilizan los dos primeros octetos para identificar la porción de red de la dirección de red. Con los primeros dos bits ya establecidos en 1 y 0, quedaban 14 bits en los primeros dos octetos para asignar redes, lo que produjo 16 384 direcciones de red de clase B. Debido a que cada dirección de red de clase B contenía 16 bits en la porción de host, controlaba 65 534 direcciones. (Recuerde que dos direcciones se reservaron para las direcciones de red y de difusión) [7].

	1er. Octeto	2° Octeto	3er. Octeto	4° Octeto
Siempre comienza con binario 0:	10xxxxxx	xxxxxxxx		
Equivalente decimal:	128-191	0-255		

	Red	Host	Host	Host
Mascara de subred	255	.255	.0	.0

Figura 2-11. Red de clase B

Como se muestra en la Figura 2-12, las redes de clase C utilizan los dos primeros octetos para identificar la porción de red de la dirección de red. Con los primeros tres bits establecidos en 1 y 1, y 0, quedaban 21 bits para asignar redes para más de 2 millones de redes de clase C. Pero cada red de clase C sólo tenía 8 bits en la porción de host o 254 direcciones host posibles [7].

	1er. Octeto	2° Octeto	3er. Octeto	4° Octeto
Siempre comienza con binario 0:	110xxxxx	xxxxxxxx	xxxxxxxx	
Equivalente decimal:	192-223	0-255	0-255	

	Red	Host	Host	Host
Mascara de subred	255	.255	.255	.0

Figura 2-12. Red de clase C

Una ventaja de asignar máscaras de subred predeterminadas específicas a cada clase es que reduce los mensajes de actualización de enrutamiento. Los protocolos de enrutamiento con clase no incluyen la información de la máscara de subred en las actualizaciones. El router receptor aplica la máscara predeterminada según el valor del primer octeto que identifica la clase [7].

2.4.5.- Desperdicio de direccionamiento con clase

El direccionamiento con clase especificado en los RFC 790 y 791 generaba un enorme desperdicio de espacio de direcciones. En los albores de Internet, se asignó a las organizaciones una dirección de red con clase completa de clase A, B o C [7]. Como se muestra en la Figura 2-13.

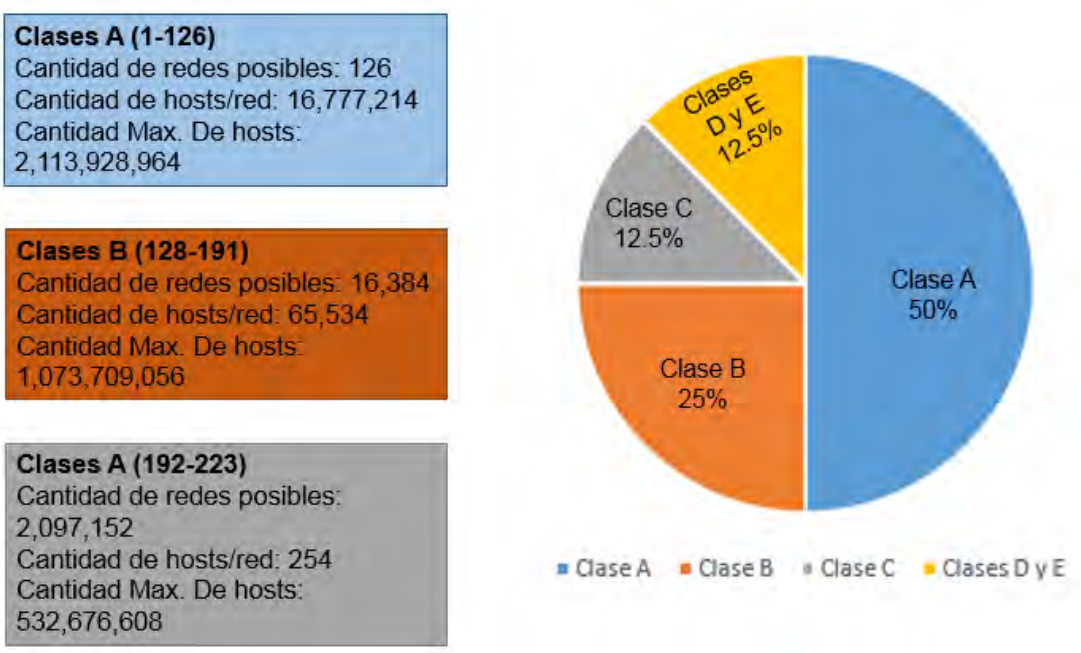


Figura 2-13. Grafico circular de las clases de red

La clase A tenía el 50% del espacio de direcciones total. Sin embargo, solo podía asignarse una dirección de red de clase “A” a 126 organizaciones. Lo ridículo era que cada una de estas organizaciones podía proporcionar direcciones para un máximo de 16 millones de hosts. A las organizaciones muy grandes se les asignaban bloques de direcciones enteros de clase A. Algunas empresas y organizaciones gubernamentales aún tienen direcciones de clase A. Por ejemplo, General Electric posee 3.0.0.0/8, Apple Computer, 17.0.0.0/8, y el servicio postal de los Estados Unidos, 56.0.0.0/8 [7].

La clase B tenía el 25% del espacio de direcciones total. Hasta 16 384 organizaciones podían tener asignada una dirección de red de clase B, y cada una de estas redes podía admitir hasta 65 534 hosts. Sólo las organizaciones más grandes y los gobiernos podían llegar a usar alguna vez las 65 000 direcciones. Al igual que las redes de clase A, muchas direcciones IP en el espacio de direcciones de clase B se perdían [7].

La clase C tenía el 12,5% del espacio de direcciones total. Muchas más organizaciones podían obtener las redes de clase C, pero estaban limitadas en el número total de hosts que podían conectar. De hecho, en muchos casos, las direcciones de clase C eran a menudo demasiado pequeñas para la mayoría de las organizaciones medianas [7].

Las clases D y E se utilizan para direcciones de multidifusión y reservadas. [7]

El resultado general fue que el direccionamiento con clase era un esquema de direccionamiento que generaba mucho desperdicio. Debía desarrollarse una mejor solución para el direccionamiento de red. Por este motivo, en 1993, se introdujo el enrutamiento entre dominios sin clase (CIDR) [7].

2.4.6.- Enrutamiento entre dominios sin clase

El CIDR reemplazó las asignaciones de red con clase y las clases de direcciones (A, B, C) se volvieron obsoletas. Con el CIDR, el valor del primer octeto ya no determina la dirección de red. En cambio, la porción de red de la dirección la determina la máscara de subred, también conocida como “prefijo de red” o “longitud de prefijo” (es decir, /8, /19, etc.) [7].

Los ISP ya no están limitados a una máscara de subred de /8, /16 o /24. Ahora pueden asignar espacio de direcciones de manera más eficaz mediante el uso de cualquier longitud de prefijo que comience con /8 y valores superiores (es decir, /8, /9, /10, etc.) [7].

El CIDR también reduce el tamaño de las tablas de enrutamiento y administra el espacio de direcciones IPv4 con mayor eficacia mediante:

- Sumarización de ruta: también conocida como “agregación de prefijos”. Las rutas se resumen en una única ruta para ayudar a reducir el tamaño de las tablas de enrutamiento. Por ejemplo, una ruta estática resumida puede reemplazar varias instrucciones de rutas estáticas específicas.
- Creación de superredes: ocurre cuando la máscara de sumarización de ruta es un valor menor que la máscara con clase predeterminada tradicional.

Una superred siempre es un resumen de rutas, pero un resumen de rutas no siempre es una superred [7].

2.4.7.- Sumarización de rutas

En la Figura 2-14, se nota que el ISP1 tiene cuatro clientes y que cada uno tiene una cantidad variable de espacio de direcciones IP. El espacio de direcciones de los cuatro clientes puede resumirse en un anuncio para el ISP2. La ruta 192.168.0.0/20 resumida o agregada incluye todas las redes que pertenecen a los clientes A, B, C y D. Este tipo de ruta se conoce como “ruta de superred”. Una superred resume varias direcciones de red con una máscara menor que la máscara con clase [7].

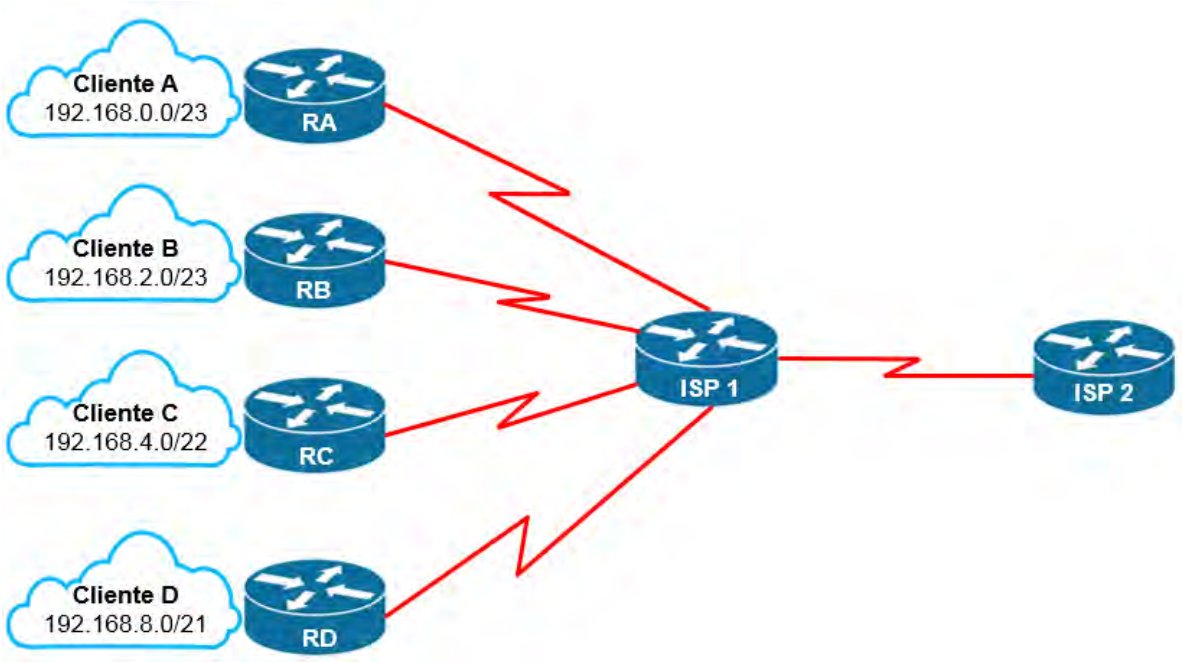


Figura 2-14. Ejemplo de sumarización de rutas

La determinación de la ruta resumida y la máscara de subred para un grupo de redes se pueden realizar en tres pasos:

1. Enumere las redes en formato binario.
2. Cuente el número de bits coincidentes del extremo izquierdo. Esta es la longitud de prefijo o máscara de subred de la ruta resumida.
3. Copie los bits coincidentes y luego agregue los bits 0 al resto de la dirección para determinar la dirección de red resumida.

La dirección de red sumarizada y la máscara de subred ahora pueden usarse como ruta sumarizada para este grupo de redes [7].

Las rutas resumidas pueden configurarse por medio de rutas estáticas y protocolos de enrutamiento sin clase [7].

2.4.8.- Mascara de subred de longitud variable

En la división en subredes tradicional se aplica la misma máscara de subred a todas las subredes. Esto significa que cada subred tiene la misma cantidad de direcciones de host disponibles [7].

Como se ilustra en la Figura 2-15, mediante la división en subredes tradicional se crean subredes de igual tamaño. Cada subred en un esquema tradicional utiliza la misma máscara de subred [7].

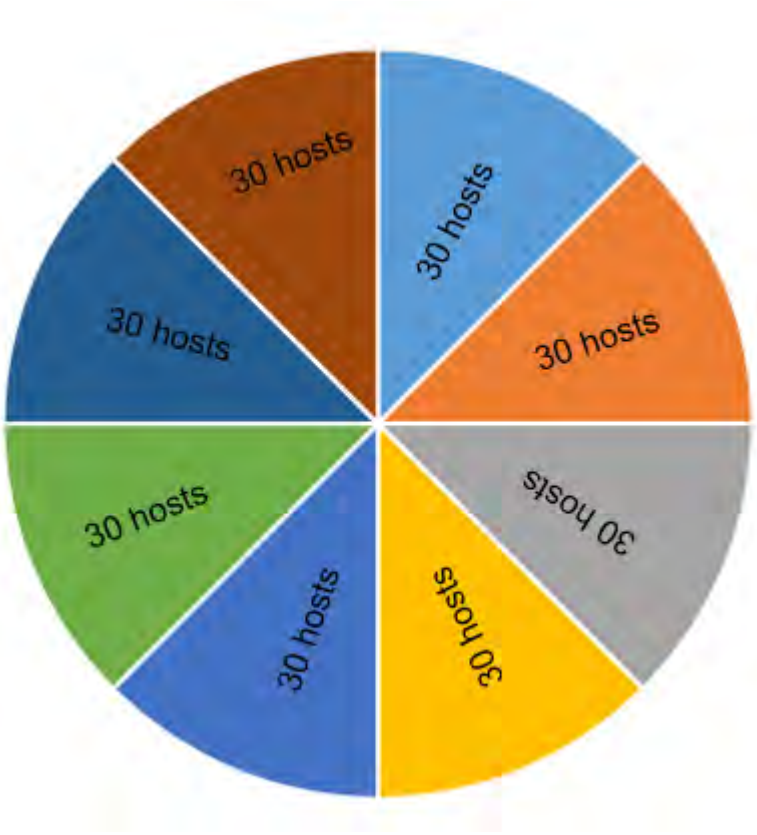


Figura 2-15. Grafico circular de la división de subredes tradicional

Con VLSM, la longitud de la máscara de subred varía según la cantidad de bits que se toman prestados para una subred específica, de lo cual deriva la parte "variable" de la máscara de subred de longitud variable. Como se muestra en la Figura 2-16, VLSM permite dividir un espacio de red en partes desiguales [7].

Figura 2-16. Grafico circular de una división de subredes por VLSM

La división en subredes de VLSM es similar a la división en subredes tradicional en cuanto a que se toman prestados bits para crear subredes. Las fórmulas para calcular la cantidad de hosts por subred y la cantidad de subredes que se crean también son válidas para VLSM. La diferencia es que la división en subredes no es una actividad que conste de un único paso. Con VLSM, la red primero se divide en subredes y, a continuación, las subredes se vuelven a dividir en subredes. Este proceso se puede repetir varias veces crear subredes de diversos tamaños [7].

VLSM permite el uso de diferentes máscaras para cada subred. Después de que una dirección de red se divide en subredes, esas subredes también se pueden dividir en subredes. VLSM simplemente subdivide una subred. Se puede considerar a VLSM como una división en sub-subredes. Las direcciones host individuales se asignan a partir de las direcciones de "sub-subredes" [7].

2.5.- Rutas Dinámicas

Las redes que usamos en nuestra vida cotidiana, sin saberlo, interactuamos desde redes locales pequeñas hasta grandes internetworks globales. En un hogar el usuario común puede tener un router y dos o más computadoras, en cambio en el trabajo, la organización puede que tenga varios switches y/o routers para atender las necesidades de cientos o hasta miles de computadoras [7].

Los routers se encargan de reenviar paquetes mediante la información que tienen en la tabla de enrutamiento. Estos routers pueden encontrar las rutas hacia las redes remotas de dos maneras, ya sea de forma estática o forma dinámica [7].

En redes grandes que cuentan con más subredes, las rutas estáticas como lo vimos en el punto anterior, cuentan con una gran configuración y el mantenimiento para las grandes redes conllevan una sobrecarga administrativa y operativa. Estas sobrecargas son pesadas especialmente cuando hay cambios en la red, como si un enlace estuviera fuera de servicio o la implementación de una nueva subred. Implementar el protocolo de enrutamiento dinámico puede apaciguar la carga de las tareas de configuración y de mantenimiento, además de que proporciona escalabilidad a la red [7].

2.5.1.- Historia

Uno de los primeros protocolos de enrutamiento fue el protocolo de información de routing (por sus siglas en ingles RIP). El protocolo RIP de versión 1 (RIPv1) se lanzó en 1988, y ya en 1969 se utilizaban algunos de los algoritmos básicos en dicho protocolo en la Advanced Research Projects Agency Network (ARPANET) [7].

A medida que las redes crecieron y se volvieron más complejas, surgieron nuevos protocolos de enrutamiento. El protocolo de enrutamiento RIP se actualizó a la versión 2 (RIPv2) a fin de admitir el crecimiento del entorno de red. No obstante, la versión más nueva de RIP aún no es escalable a las implementaciones de red más extensas de la actualidad. Con el objetivo de satisfacer las necesidades de las redes más grandes, se desarrollaron dos protocolos de enrutamiento: el protocolo OSPF (Open Shortest Path First) e Intermediate System-to-Intermediate System (IS-IS). Cisco desarrolló el protocolo de enrutamiento de gateway interior (IGRP) e IGRP mejorado (EIGRP), que también tiene buena escalabilidad en implementaciones de redes más grandes [7].

De esta forma, surgió la necesidad de conectar distintas internetworks y proporcionar enrutamiento entre ellas. En la actualidad, se utiliza el protocolo de gateway fronterizo (BGP) entre proveedores de servicios de Internet (ISP). El protocolo BGP también se utiliza entre los ISP y sus clientes privados más grandes para intercambiar información de enrutamiento [7]. En la siguiente Tabla 7, se clasifican los protocolos.

Tabla 7. Protocolos de gateway interior y exterior

	Protocolos de gateway interior				Protocolos de gateway exterior
	Vector distancia		Estado de enlace		Vector ruta
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP para IPv6	OSPFv3	IS-IS para IPv6	BGP-MP

Con la llegada de numerosos dispositivos que usan IP para los consumidores, el espacio de direccionamiento IPv4 quedó prácticamente agotado, por lo que surgió IPv6. A fin de admitir la comunicación basada en IPv6, se desarrollaron versiones más nuevas de los protocolos de enrutamiento IP. Donde, RIP es el más simple de los protocolos de enrutamiento dinámico [7].

2.5.2.- Propósito del enrutamiento dinámico

Los protocolos de enrutamiento se usan para facilitar el intercambio de información de enrutamiento entre los routers. Un protocolo de enrutamiento es un conjunto de procesos, algoritmos y mensajes que se usan para intercambiar información de enrutamiento y completar la tabla de enrutamiento con la elección de los mejores caminos que realiza el protocolo. El propósito de los protocolos de enrutamiento dinámico incluye lo siguiente:

- Descubrir redes remotas.
- Mantener la información de enrutamiento actualizada.
- Escoger el mejor camino hacia las redes de destino.
- Poder encontrar un mejor camino nuevo si la ruta actual deja de estar disponible.

Los componentes principales de los protocolos de enrutamiento dinámico incluyen los siguientes:

- Estructuras de datos: por lo general, los protocolos de enrutamiento utilizan tablas o bases de datos para sus operaciones. Esta información se guarda en la RAM.
- Mensajes del protocolo de enrutamiento: los protocolos de enrutamiento usan varios tipos de mensajes para descubrir routers vecinos, intercambiar información de enrutamiento y realizar otras tareas para descubrir la red y conservar información precisa acerca de ella.
- Algoritmo: un algoritmo es una lista finita de pasos que se usan para llevar a cabo una tarea. Los protocolos de enrutamiento usan algoritmos para facilitar información de enrutamiento y para determinar el mejor camino.

Los protocolos de enrutamiento permiten a los routers compartir información en forma dinámica sobre redes remotas y agregar esa información automáticamente a sus propias tablas de enrutamiento. Los protocolos de enrutamiento determinan la mejor ruta hacia cada red y, a continuación, esa ruta

se agrega a la tabla de enrutamiento. Uno de los beneficios principales de los protocolos de enrutamiento dinámico es que los routers intercambian información de enrutamiento cuando se produce un cambio en la topología. Este intercambio permite a los routers obtener automáticamente información sobre nuevas redes y también encontrar rutas alternativas cuando se produce una falla de enlace en la red actual. En comparación con el enrutamiento estático, los protocolos de enrutamiento dinámico requieren menos sobrecarga administrativa. Sin embargo, usar protocolos de enrutamiento dinámico implica el costo de dedicar parte de los recursos de un router a la operación del protocolo, incluidos tiempo de CPU y ancho de banda del enlace de red [7]. En la tabla 8, se destacan algunas de las ventajas y desventajas del enrutamiento estático.

Tabla 8. Ventajas y desventajas del enrutamiento estático

Ventajas	Desventajas
Adecuando en todas las topologías donde se requieren varios routers.	La implementación puede ser más compleja.
Por lo general, es independiente del tamaño de la red.	Menos seguro. Se requiere opciones de configuración adicionales para proporcionarle protección.
Si es posible, adapta automáticamente la topología para volver a enrutar el tráfico.	La ruta depende de la topología actual.
	Se requiere CPU, RAM y ancho de banda de enlaces adicionales.

Los protocolos de enrutamiento dinámico ayudan al administrador de red a administrar el proceso riguroso y lento de configuración y mantenimiento de rutas estáticas. El enrutamiento dinámico es la mejor opción para redes grandes como la que se muestra en la siguiente Figura 2-17 [7].

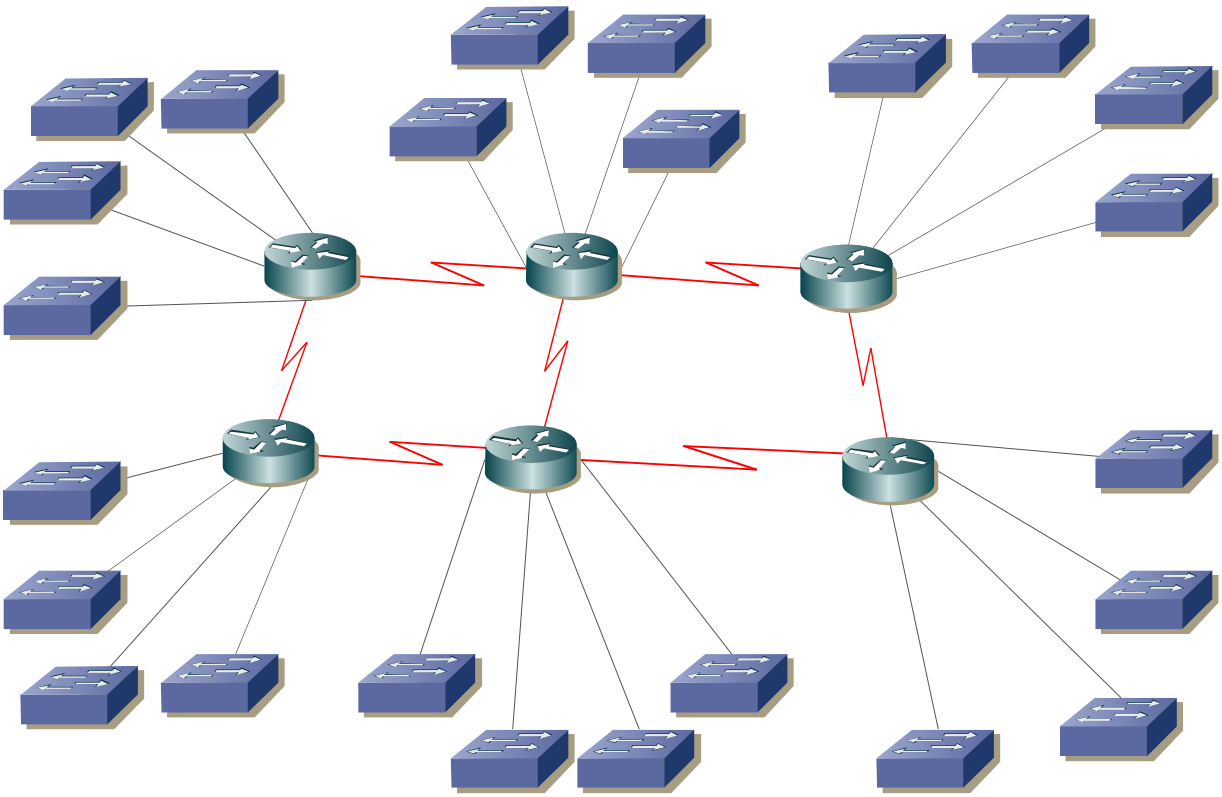
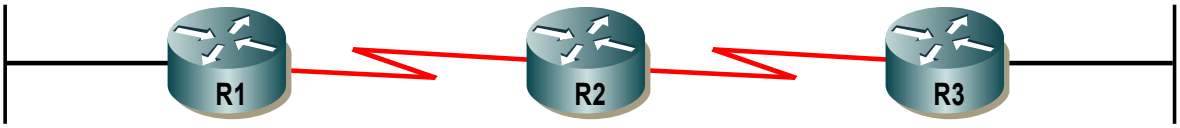


Figura 2-17. Ejemplo de una red grande

2.5.3.- Detección de redes

Todos los protocolos de enrutamiento siguen los mismos patrones de funcionamiento. Cuando un router se enciende, no tiene ninguna información sobre la topología de la red. Ni siquiera tiene conocimiento de que existen dispositivos en el otro extremo de sus enlaces. Una vez que un router arranca correctamente, aplica la configuración guardada. Si el direccionamiento IP está configurado de forma correcta, en primer lugar, el router detecta sus propias redes conectadas directamente [7]. En la Figura 2-18, se muestra un ejemplo de cómo inicia en frio un router y su tabla de enrutamiento.



Red	Interfaz	Salto
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0

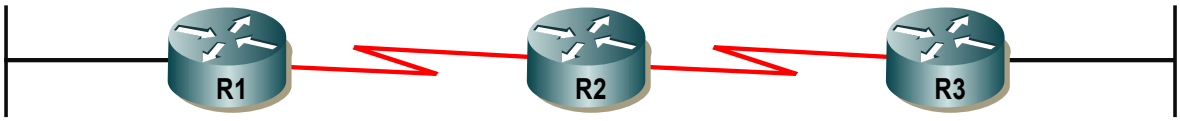
Red	Interfaz	Salto
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0

Red	Interfaz	Salto
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0

Figura 2-18. Inicio en frio de un router

Después del arranque inicial y del descubrimiento, la tabla de enrutamiento se actualiza con todas las redes conectadas directamente y las interfaces en las que residen dichas redes [7].

Si se configura un protocolo de enrutamiento, el siguiente paso es que el router comience a intercambiar actualizaciones de enrutamiento para obtener información sobre rutas remotas. El router envía un paquete de actualización por todas las interfaces habilitadas en el router. La actualización contiene la información de la tabla de enrutamiento, que en este momento consta de todas las redes conectadas directamente. Al mismo tiempo, el router también recibe y procesa actualizaciones similares de otros routers conectados. Una vez recibida la actualización, el router revisa si contiene información de red nueva, y se agrega a la tabla de enrutamiento toda red que no esté incluida en ella aún [7]. En la Figura 2-19, se muestra una actualización de la tabla de enrutamiento referente a la Figura 2-20.



Red	Interfaz	Salto
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1

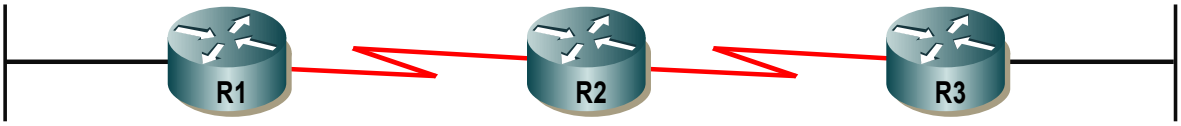
Red	Interfaz	Salto
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Red	Interfaz	Salto
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1

Figura 2-19. Actualización de una tabla de enrutamiento de un router en frio

En este punto, los routers tienen información sobre sus propias redes conectadas directamente y las de sus vecinos más cercanos. Siguiendo el camino hacia la convergencia, los routers intercambian la siguiente ronda de actualizaciones periódicas. Cada router verifica las actualizaciones nuevamente para comprobar si hay información nueva [7].

En la Figura 2-20 se muestra una tabla de enrutamiento actualizada, cada router siguió su proceso de convergencia mediante él envió y la recepción de actualizaciones.



Red	Interfaz	Salto
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Red	Interfaz	Salto
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Red	Interfaz	Salto
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Figura 2-20. Tabla de enrutamiento actualizada por cada router

Por lo general, los protocolos de enrutamiento vector distancia implementan una técnica para evitar los bucles de enrutamiento conocida como “horizonte dividido”. El horizonte dividido evita que la información se envíe desde la misma interfaz en la que se recibió dicha información. Por ejemplo, el R2 no envía una actualización que contenga la red 10.1.0.0 por la interfaz Serial 0/0/0, debido a

que obtuvo información acerca de la red 10.1.0.0 a través de la interfaz Serial 0/0/0 [7].

Una vez que los routers dentro de una red realizan la convergencia, el router puede utilizar la información que se encuentra en la tabla de rutas para determinar la mejor ruta para llegar a un destino. Los distintos protocolos de enrutamiento tienen diferentes maneras de calcular la mejor ruta [7].

La convergencia de la red se produce cuando todos los routers tienen información completa y precisa acerca de toda la red, como se muestra en la Figura 2-21. El tiempo de convergencia es el tiempo que los routers tardan en compartir información, calcular las mejores rutas y actualizar sus tablas de enrutamiento. Una red no es completamente operativa hasta que la red haya convergido; por lo tanto, la mayoría de las redes requieren tiempos de convergencia breves [7].

La convergencia es cooperativa e independiente al mismo tiempo. Los routers comparten información entre sí, pero deben calcular en forma independiente los impactos del cambio de topología en sus propias rutas. Dado que establecen un acuerdo con la nueva topología en forma independiente, se dice que convergen sobre este consenso. Las propiedades de convergencia incluyen la velocidad de propagación de la información de enrutamiento y el cálculo de los caminos óptimos. La velocidad de propagación se refiere al tiempo que tardan los routers dentro de la red en reenviar la información de enrutamiento [7].

2.5.4.- Tipos de protocolos de enrutamiento

Los protocolos de enrutamiento se pueden clasificar en diferentes grupos según sus características. Específicamente, los protocolos de enrutamiento se pueden clasificar según lo siguiente:

- Propósito: protocolo de gateway interior (IGP) o protocolo de gateway exterior (EGP).
- Operación: vector distancia, protocolo de estado de enlace, protocolo vector ruta.
- Comportamiento: protocolo con clase (antiguo) o protocolo sin clase.

Los protocolos de enrutamiento IPv4 se clasifican de la siguiente manera:

- RIPv1 (antiguo): IGP, vector distancia, protocolo con clase.
- IGRP (antiguo): IGP, vector distancia, protocolo con clase desarrollado por Cisco (cayó en desuso a partir del IOS 12.2).
- RIPv2: IGP, vector distancia, protocolo sin clase.
- EIGRP: IGP, vector distancia, protocolo sin clase desarrollado por Cisco.
- OSPF: IGP, estado de enlace, protocolo sin clase.
- IS-IS: IGP, estado de enlace, protocolo sin clase.
- BGP: EGP, vector ruta, protocolo sin clase.

Los protocolos de enrutamiento con clase, RIPv1 e IGRP, son protocolos antiguos y se utilizan solamente en redes antiguas. Estos protocolos de

enrutamiento se convirtieron en los protocolos de enrutamiento sin clase RIPv2 y EIGRP, respectivamente. Los protocolos de enrutamiento de estado de enlace son protocolos sin clase naturalmente [7].

Los protocolos de enrutamiento se pueden comparar según las siguientes características:

- Velocidad de convergencia: define cuán rápido comparten información de enrutamiento y alcanzan un estado de conocimiento coherente los routers de la topología de la red. Cuanto más rápida sea la convergencia, más preferible será el protocolo. Los loops de enrutamiento pueden ser el resultado de tablas de enrutamiento incongruentes que no se han actualizado debido a la lenta convergencia de una red sujeta a cambios [7].
- Escalabilidad: define cuán grande puede ser una red, según el protocolo de enrutamiento implementado. Cuanto más grande sea la red, más escalable debe ser el protocolo de enrutamiento [7].
- Con clase o sin clase (uso de VLSM): los protocolos de enrutamiento con clase no incluyen la máscara de subred y no admiten VLSM. Los protocolos de enrutamiento sin clase incluyen la máscara de subred en las actualizaciones. Los protocolos de enrutamiento sin clase admiten VLSM y una mejor sumarización de ruta [7].
- Uso de recursos: incluye los requisitos de un protocolo de enrutamiento, como el espacio de memoria (RAM), la utilización de la CPU y el uso del ancho de banda del enlace. Una mayor cantidad de requisitos de recursos exige hardware más potente para admitir la operación del protocolo de enrutamiento además de los procesos de reenvío de paquetes [7].
- Implementación y mantenimiento: describen el nivel de conocimiento necesario para que un administrador de red ponga en funcionamiento y mantenga la red según el protocolo de enrutamiento implementado [7]. En la Tabla 9, se resumen las características de cada protocolo de enrutamiento.

Tabla 9. Protocolos de enrutamiento

	Vector distancia				Estado de enlace	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Velocidad de convergencia	Lento	Lento	Lento	Rápido	Rápido	Rápido
Escalabilidad: tamaño de la red	Pequeño	Pequeño	Pequeño	Grande	Grande	Grande
Uso de VLSM	No	Si	No	Si	Si	Si

Uso de recursos	Bajo	Bajo	Bajo	Medio	Alto	Alto
Implementación y mantenimiento	Simple	Simple	Simple	Complejo	Complejo	Complejo

En algunos casos, un protocolo de enrutamiento obtiene información sobre más de una ruta hacia el mismo destino. Para seleccionar el mejor camino, el protocolo de enrutamiento debe poder evaluar y diferenciar entre las rutas disponibles. Esto se logra mediante el uso de métricas de enrutamiento. Una métrica es un valor mensurable que el protocolo de enrutamiento asigna a distintas rutas según la utilidad que tengan. En situaciones donde hay varias rutas hacia la misma red remota, las métricas de enrutamiento se utilizan para determinar el "costo" total de una ruta de origen a destino. Los protocolos de enrutamiento determinan la mejor ruta sobre la base del costo más bajo [7].

Los diferentes protocolos de enrutamiento pueden usar diferentes métricas. La métrica utilizada por un protocolo de enrutamiento no es comparable con la métrica utilizada por otro protocolo de enrutamiento. Dos protocolos de enrutamiento distintos pueden elegir diferentes rutas hacia el mismo destino [7].

En la Figura 2-21, se muestra que el protocolo RIP elegiría la ruta con la menor cantidad de saltos, es decir, partiendo de R1 terminando en R2, pero teniendo un ancho de banda de 56kbps, mientras que el protocolo OSPF elegiría la ruta con el mayor ancho de banda, partiendo de R1, redirigiéndose a R3 y terminando con R1.

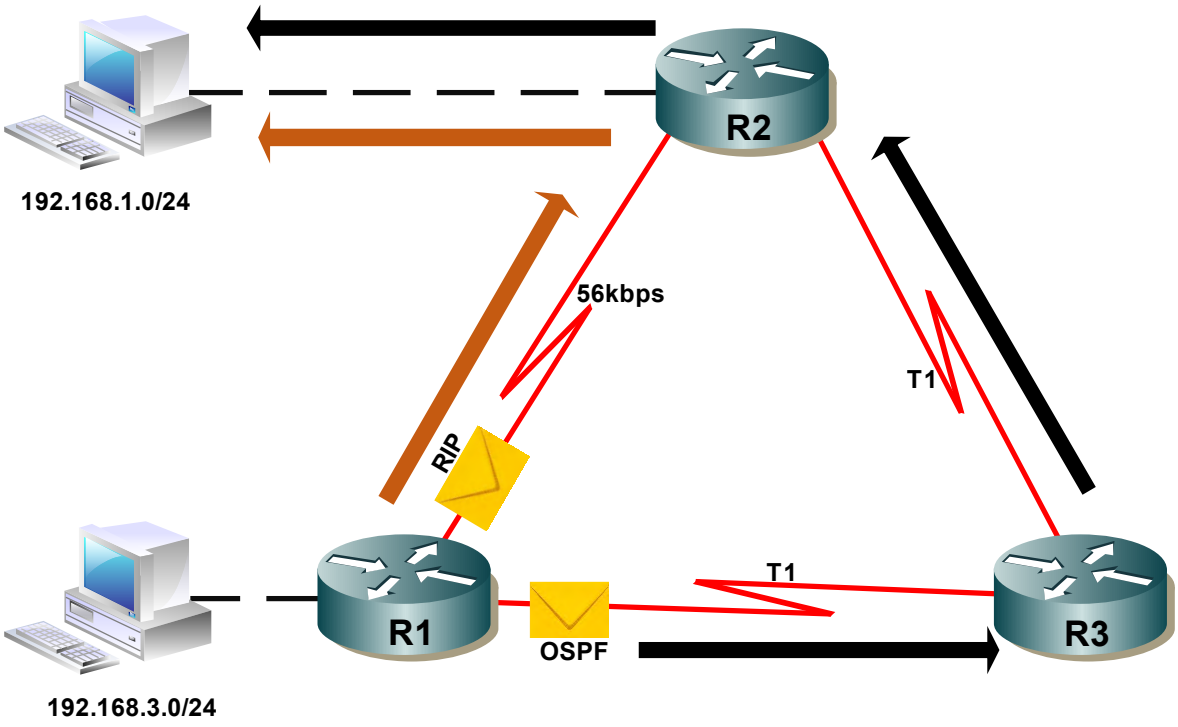


Figura 2-21. Protocolo RIP y OSPF

2.5.5.- Protocolos de enrutamiento vector distancia

"Vector distancia" significa que las rutas se anuncian proporcionando dos características:

- Distancia: identifica la distancia hasta la red de destino. Se basa en una métrica como el conteo de saltos, el costo, el ancho de banda y el retardo, entre otros [7].
- Vector: especifica el sentido en que se encuentra el router de siguiente salto o la interfaz de salida para llegar al destino [7].

Por ejemplo, en la Figura 2-22, el R1 tiene información que la distancia para llegar a la red 192.168.1.0/24 es de un salto y de que el sentido es a través de la interfaz S0/0/0 hacia el R2.

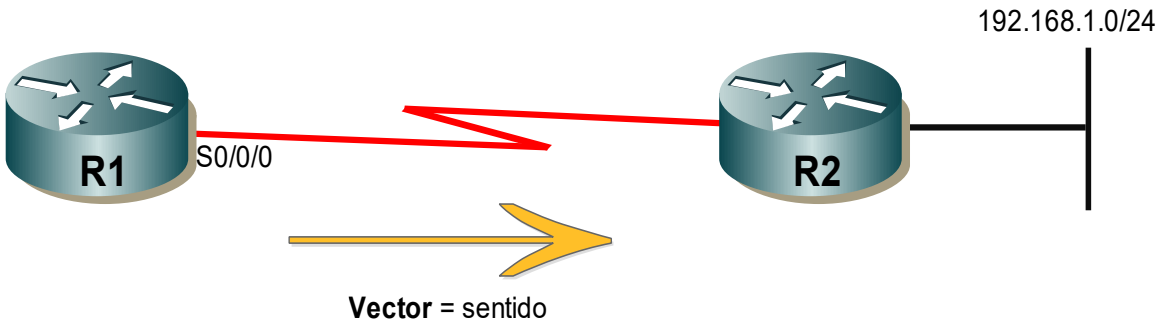


Figura 2-22. Protocolo vector distancia

Para el R1, 192.168.1.0/24 está a un salto (distancia), y puede alcanzarse a través del R2 (vector).

Un router que utiliza un protocolo de enrutamiento vector distancia no tiene la información de la ruta completa hasta la red de destino. Los protocolos vector distancia utilizan routers como letreros a lo largo de la ruta hacia el destino final. La única información que conoce el router sobre una red remota es la distancia o métrica para llegar a esa red y qué ruta o interfaz usar para alcanzarla. Los protocolos de enrutamiento vector distancia no tienen un mapa en sí de la topología de la red [7].

El término vector de distancia describe lo que sabe un router sobre cada ruta. Cuando un router aprende acerca de una ruta a una subred, los routers aprenden tres hechos importantes relacionados con cada ruta: la subred de destino, la distancia (es decir, la métrica del protocolo de enrutamiento) y el vector (es decir, el enlace y siguiente) [9].

Los algoritmos de enrutamiento vector distancia requieren que cada router envíe toda su tabla de enrutamiento en cada actualización, pero solo a sus vecinos. Los algoritmos de enrutamiento de vector distancia pueden ser propensos a los bucles de enrutamiento, pero son computacionalmente más simples que los algoritmos de enrutamiento de estado de enlace [9].

Hay cuatro IGP vector distancia IPv4:

- RIPv1: protocolo antiguo de primera generación.
- RIPv2: protocolo de enrutamiento vector distancia simple.
- IGRP: protocolo exclusivo de Cisco de primera generación (obsoleto y reemplazado por EIGRP).
- EIGRP: versión avanzada del enrutamiento vector distancia.

2.5.6.- Protocolos de enrutamiento estado de enlace

A diferencia de la operación del protocolo de enrutamiento vector distancia, un router configurado con un protocolo de enrutamiento de estado de enlace (link-state) puede crear una “vista completa” o una topología de la red al reunir información proveniente de todos los demás routers [7].

El uso de un protocolo de enrutamiento de link-state es como tener un mapa completo de la topología de la red. Los letreros, como se mencionaba en el enrutamiento vector distancia, a lo largo de la ruta de origen a destino no son necesarios, debido a que todos los routers de estado de enlace usan un mapa de la red idéntico. Un router de estado de enlace usa la información de estado de enlace para crear un mapa de la topología y seleccionar la mejor ruta hacia todas las redes de destino en la topología.

Los routers con RIP habilitado envían actualizaciones periódicas de su información de enrutamiento a sus vecinos. Los protocolos de enrutamiento de link-state no usan actualizaciones periódicas. Una vez que se produjo la

convergencia de la red, la actualización del estado de enlace solo se envía cuando se produce un cambio en la topología [7].

Los protocolos de link-state funcionan mejor en situaciones donde:

- El diseño de red es jerárquico, lo cual suele suceder en redes extensas.
- La rápida convergencia de la red es crucial.
- Los administradores tienen un conocimiento cabal del protocolo de enrutamiento de estado de enlace implementado.

Hay dos IGP de estado de enlace IPv4:

- OSPF: protocolo de enrutamiento muy popular basado en estándares.
- IS-IS: popular en redes de proveedores.

La principal alternativa a los algoritmos de vector de distancia es el estado de enlace, o el SPF por sus siglas en inglés (Shortest Path Fast). El algoritmo SPF requiere que cada enrutador participante tenga información de topología completa. La forma más fácil de pensar en la información de topología es imaginar que cada router tiene un mapa que muestra todos los demás routers y las redes a las que se conectan. En términos abstractos, los routers corresponden a los nodos en un gráfico y las redes que conectan los routers corresponden a los bordes. Hay un borde (enlace) entre dos nodos si y solo si los enrutadores correspondientes pueden comunicarse directamente [9].

En lugar de enviar mensajes que contienen listas de destinos, un router que participa en un algoritmo SPF realiza dos tareas. En primer lugar, prueba activamente el estado de todos los routers vecinos. En términos del gráfico, dos routers son vecinos si comparten un enlace; en términos de red, dos vecinos se conectan a una red común. En segundo lugar, propaga periódicamente la información de estado del enlace a todos los demás routers. Para comprobar el estado de un vecino directamente conectado, un router intercambia periódicamente mensajes cortos que pregunta si el vecino está vivo y accesible. Si el vecino responde, se dice que el enlace entre ellos está activo. De lo contrario, se dice que el enlace está inactivo. Para informar a todos los demás routers, cada router difunde periódicamente un mensaje que enumera el estado de cada uno de sus enlaces. Simplemente informa si la comunicación es posible entre los routers. El software de protocolo en los routers se encarga de entregar una copia de cada mensaje del estado del enlace a todos los routers participantes (si las redes subyacentes no admiten difusión, la entrega se realiza reenviando copias individuales del mensaje punto a punto) [9].

Cada vez que llega un mensaje de estado de enlace, un router utiliza la información para actualizar su mapa, marcando enlaces arriba o abajo. Cada vez que cambia el estado del enlace, el router vuelve a calcular las rutas aplicando el conocido algoritmo de ruta más corta de Dijkstra. El algoritmo de Dijkstra calcula las rutas más cortas a todos los destinos desde un único origen [9].

Una de las principales ventajas de los algoritmos SPF es que cada router calcula las rutas de forma independiente utilizando los mismos datos de estado

originales; no dependen del cálculo de máquinas intermedias. Debido a que los mensajes de estado del enlace se propagan sin cambios, es fácil solucionar problemas. Debido a que los routers realizan el cálculo de ruta localmente, se garantiza que converge. Finalmente, dado que los mensajes de estado del enlace solo transmiten información sobre las conexiones directas desde un solo router, el tamaño no depende de la cantidad de redes. Por lo tanto, los algoritmos SPF escalan mejor que los algoritmos de vector a distancia [9].

2.6.- Protocolo de Enrutamiento OSPF

OSPF (Open Shortest Path First) es un protocolo de enrutamiento estándar definido en la RFC 2328. Utiliza el algoritmo SPF (Shortest Path First) para encontrar las mejores rutas hacia los diferentes destinos y es capaz de converger muy rápidamente. Esto último conlleva un alto uso de CPU del router por lo que hay que tener precauciones a la hora de diseñar la red. Es flexible en el diseño de red y al ser un estándar soporta dispositivos de todos los fabricantes [5].

Un protocolo de estado de enlace es un protocolo sofisticado que utiliza el algoritmo de Dijkstra para determinar el camino más corto hacia el destino libre de bucles. Estos protocolos utilizan localmente mayores recursos que los protocolos vector distancia ya que deben calcular más datos con el objetivo de reducir tráfico de red. Los protocolos de estado de enlace llevan un registro de todas las posibles rutas para de esta manera no utilizar las técnicas de los vectores distancia para evitar bucles [5].

Algunas ventajas de OSPF sobre otros protocolos de estado de enlace son los siguientes:

- Es un protocolo sin clase, permitiendo sumarización.
- Converge muy rápidamente.
- Es estándar, lo que permite configurarlo en un escenario con diferentes fabricantes.
- Aprovecha el ancho de banda disponible.
- Utiliza multicast en lugar de broadcast.
- Envía actualizaciones incrementales.
- Utiliza el costo como única métrica.
- Es escalable, funciona bien en tamaños de redes grandes y pequeños.

En la Tabla 10, se muestra la distancia administrativa de algunas distancias incluyendo la de OSPF.

Tabla 10. Distancias administrativas de algunas rutas

Origen de la ruta	Distancia Administrativa
Conectada	0
Estática	1
Ruta sumarizada EIGRP	5

BGP externo	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170
BGP interno	200

La distancia administrativa (AD) es la confiabilidad o preferencia del origen de la ruta. OSPF tiene una distancia predeterminada de 110 como se muestra en la tabla, OSPF se prefiere sobre IS-IS y RIP.

2.6.1.- Funcionamiento de OSPF

Todos los protocolos de enrutamiento comparten componentes similares. Todos usan mensajes de protocolo de enrutamiento para intercambiar información de la ruta. Los mensajes contribuyen a armar estructuras de datos, que luego se procesan con un algoritmo de enrutamiento [7].

Los tres componentes principales del protocolo en enrutamiento OSPF incluyen lo siguiente:

OSPF crea y mantiene tres bases de datos como se ve en la Tabla 11:

Tabla 11. Tablas del OSPF

Base de datos	Tabla	Descripción
Base de datos de adyacencia	Tabla de vecinos	• Lista de todos los routers vecinos con los que un router estableció comunicación bidireccional. • Esta tabla es la única para cada router. • Se puede ver con el comando *show ip ospf neighbor.*
Base de datos de estado de enlace (LSDB)	Tabla de topología	• Muestra información sobre todos los otros routers en la red. • Esta base de datos representa la topología de la red. • Todos los routers dentro de un área tienen LSDB idénticas.

		• Se puede ver con el comando *show ip ospf database*.
Base de datos de reenvío	Tabla de enrutamiento	• Listas de rutas generada cuando se ejecuta un algoritmo en la base de datos de estado de enlace. • La tabla de enrutamiento de cada router es única y contiene información sobre cómo y dónde enviar paquetes para otros routers. • Se puede ver con el comando *show ip route.*

- La base de datos de adyacencia: crea la tabla de vecinos.
- La base de datos de estado enlace (LSDB): crea la tabla de topología
- La base de datos de reenvió: crea la tabla de enrutamiento o routing.

Estas tablas contienen una lista de routers vecinos para intercambiar información de routing, y se guardan y mantienen en la RAM [7].

OSPF intercambia mensajes para transmitir información de enrutamiento mediante cinco tipos de paquetes. Estos paquetes, se muestran en la Figura 2-23.

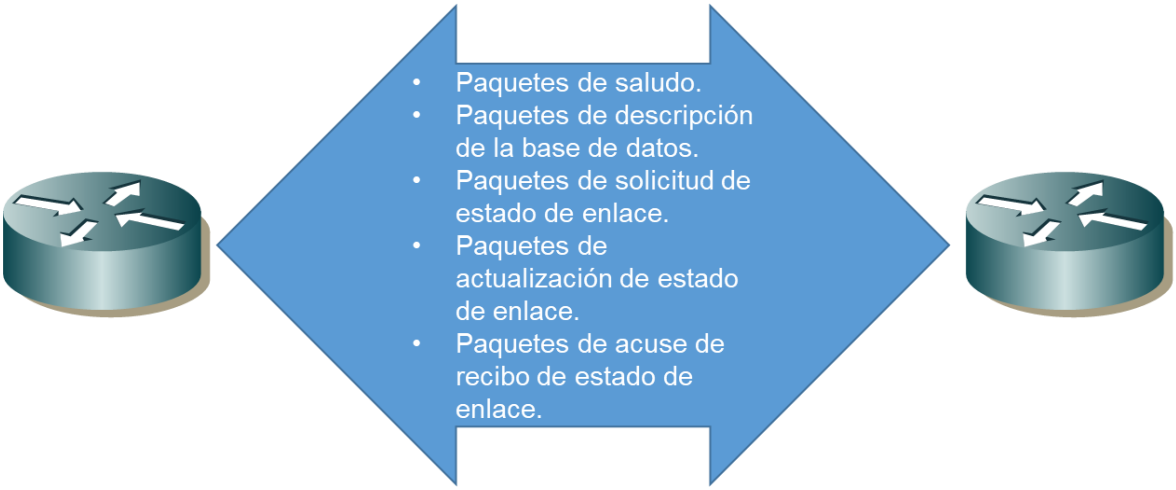


Figura 2-23. Paquetes de intercambio de OSPF

Estos paquetes se usan para describir routers vecinos y también para intercambiar información de enrutamiento a fin de mantener información precisa acerca de la red [7].

Los protocolos vector distancia anuncian rutas hacia los vecinos, pero los protocolos estado de enlace anuncian una lista de todas sus conexiones. Cuando un enlace se cae se envían LSA (Link-Statc Advertisement), que son compartidas por los vecinos como así también una base topológica LSDB (Link-State Database). Cuando los routers convergen tienen la misma LDSB, a partir

de ese momento SPF es capaz de determinar la mejor ruta hacia el destino. La tabla de topología es la visión que tiene el router de la red dentro del área en que se encuentra incluyendo además todos los routers [5].

A fin de mantener la información de routing, los routers OSPF realizan el siguiente proceso genérico de routing de estado de enlace para alcanzar un estado de convergencia:

1. Establecimiento de las adyacencias de vecinos como se ve en la Figura 2-24: los routers con OSPF habilitado deben reconocerse entre sí en la red antes de poder compartir información. Los routers con OSPF habilitado envían paquetes de saludo por todas las interfaces con OSPF habilitado para determinar si hay vecinos presentes en esos enlaces. Si se detecta un vecino, el router con OSPF habilitado intenta establecer una adyacencia de vecino con ese vecino.

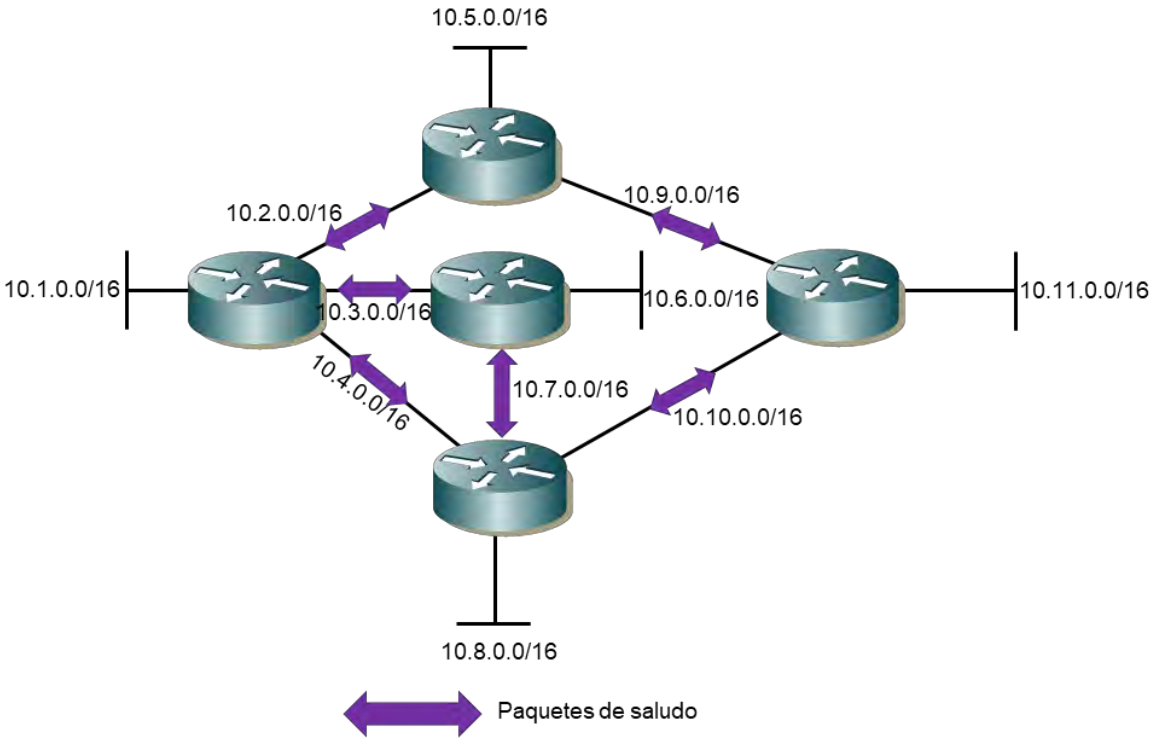


Figura 2-24. Paquetes de saludo OSPF

2. Intercambio de notificaciones de estado de enlace como se ve en la Figura 2-25: una vez que se establecen las adyacencias, los routers intercambian notificaciones de estado de enlace (LSA). Las LSA contienen el estado y el costo de cada enlace conectado directamente. Los routers saturan a los vecinos adyacentes con sus LSA. Los vecinos adyacentes que reciben las LSA saturan de inmediato a otros vecinos conectados directamente, hasta que todos los routers en el área tengan todas las LSA.

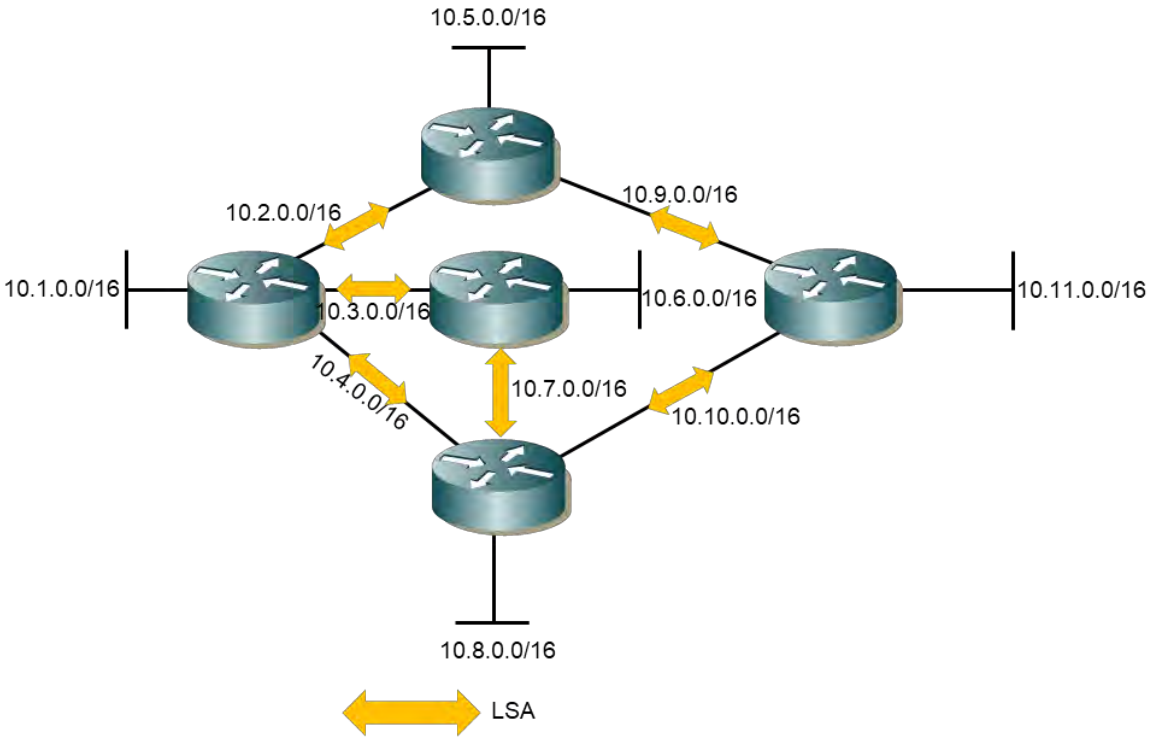


Figura 2-25. Paquetes LSA de OSPF

3. Creación de la tabla de topología, donde R1 crea su base de datos topológica: una vez que se reciben las LSA, los routers con OSPF habilitado crean la tabla de topología (LSDB) sobre la base de las LSA recibidas. Finalmente, esta base de datos contiene toda la información sobre la topología de la red.
4. Ejecución del algoritmo SPF como se observa en la Figura 2-26, donde R1 ejecuta el algoritmo SPF y crea el árbol SPF: a continuación, los routers ejecutan el algoritmo SPF. Los engranajes que se muestran en la ilustración se utilizan para indicar la ejecución del algoritmo SPF. El algoritmo SPF crea el árbol SPF.

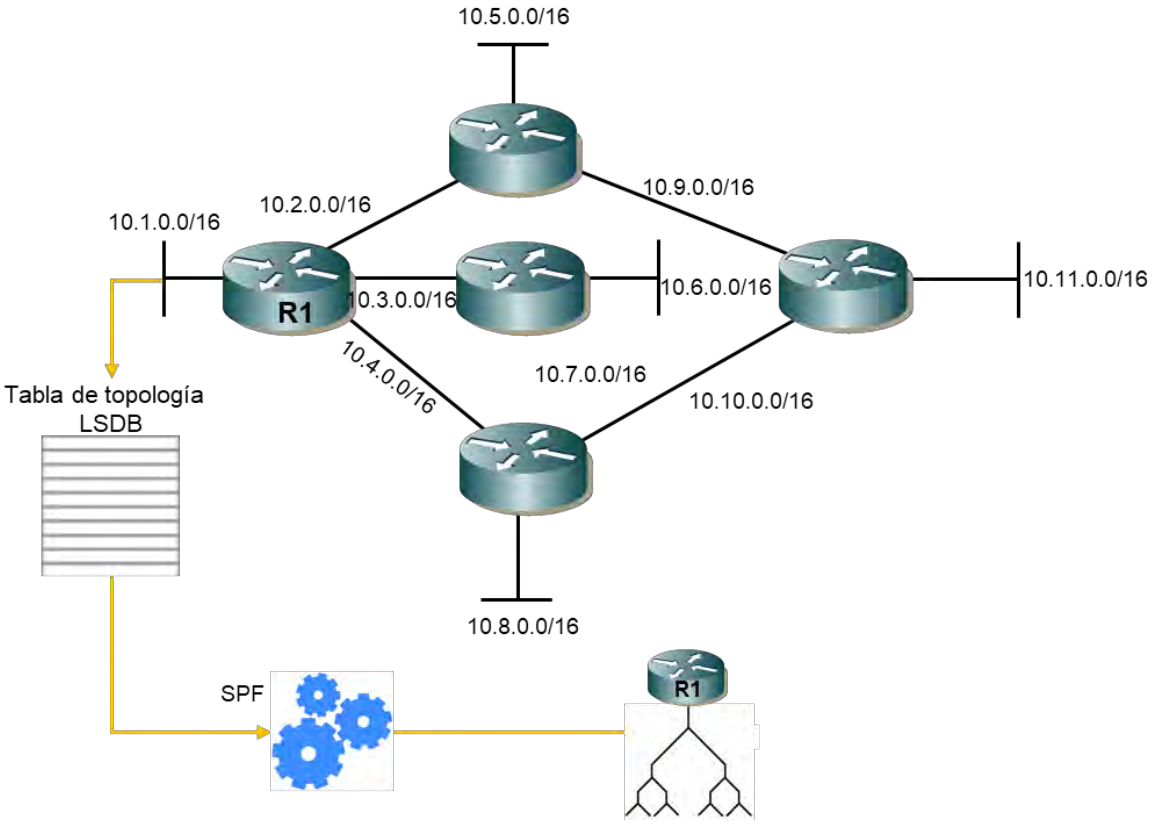
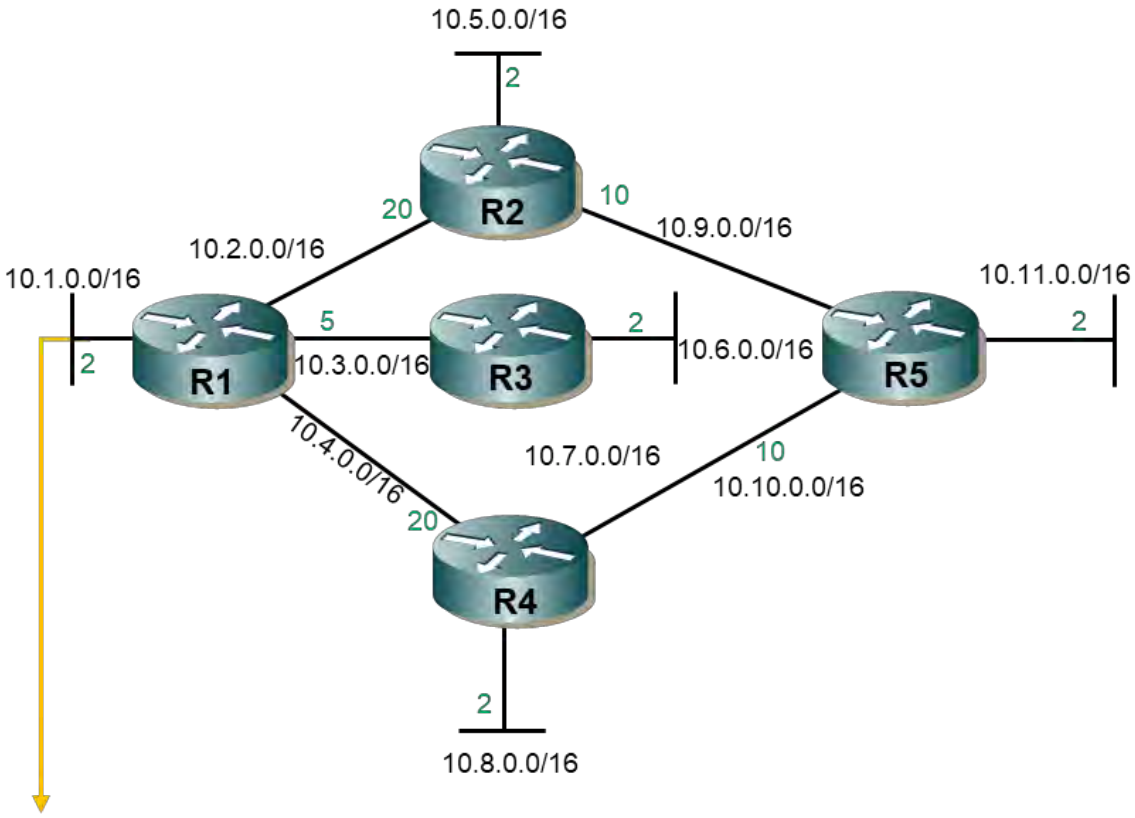


Figura 2-26. Ejecución del algoritmo SPF

En la Figura 2-27, se muestra el contenido del árbol SPF del R1.



Destino	Ruta mas corta	Costo
10.5.0.0/16	R1 → R2	22
10.6.0.0/16	R1 → R3	7
10.7.0.0/16	R1 → R3	15
10.8.0.0/16	R1 → R3 → R4	17
10.9.0.0/16	R1 → R2	30
10.10.0.0/16	R1 → R3 → R4	25
10.11.0.0/16	R1 → R3 → R4 → R5	27

Figura 2-27. Tabla de enrutamiento OSPF del R1

La tabla de topologías se actualiza por cada una de las LSA que envían cada uno de los routers dentro de la misma área y que todos estos routers comparten la misma base de datos. Si existen inconsistencias en esta base de datos podrían generarse bucles; es el propio router el encargado de avisar que ha habido algún cambio e informar del mismo [5]. Algunos problemas de las inconsistencias podrían ser:

- Perdida de conexión física o enlace en algunas de sus interfaces.

- No se reciben los hello en el tiempo establecido por sus vecinos.
- Se recibe un LSA con información de cambios en la topología.

En cualquier de los tres casos anteriores el router generará una LSA enviando a sus vecinos la siguiente información:

- Si la LSA es más reciente se añade a la base de datos. Se reenvían a todos los vecinos para que actualicen sus tablas y SPF comienza a funcionar.
- Si el número de secuencia es el mismo que el router ya tiene registrado en la base de datos, ignorará esta actualización.
- Si el número de secuencia es anterior al que está registrado, el router enviará la versión nueva al router que envió la anterior. De esta forma se asegura que todos los routers conservan la última versión.

Un área en OSPF es una agrupación de routers que están ejecutando el mismo proceso y que tienen una base de datos idéntica. También se puede decir que un área es una subdivisión del dominio de enrutamiento de OSPF. Cada área ejecuta su propio SPF y las sumarizaciones de redes son pasadas entre las respectivas áreas. [5]

OSPF se puede implementar de dos maneras:

- OSPF de área única: en la Figura 2-26, todos los routers se encuentran en un área llamada “área backbone” (área 0).
- OSPF multiárea: en la Figura 2-27, OSPF se implementa mediante varias áreas, de manera jerárquica. Todas las áreas deben conectarse al área backbone (área 0). Los routers que interconectan las áreas se denominan “routers fronterizos de área” (ABR).

Con OSPF multiárea, OSPF puede dividir un sistema autónomo (AS) grande en áreas más pequeñas, a fin de admitir el routing jerárquico. Con el enrutamiento jerárquico, se sigue produciendo el enrutamiento entre áreas, y muchas de las operaciones de enrutamiento que implican una gran exigencia para el procesador, como volver a calcular la base de datos, se guardan en un área [7].

Si hubiera demasiados routers en un área, la LSDB sería muy grande y se incrementaría la carga en la CPU. Por lo tanto, la disposición de los routers en distintas áreas divide de manera eficaz una base de datos potencialmente grande en bases de datos más pequeñas y más fáciles de administrar [7].

2.6.2.- Mensajes OSPF

Todo el tráfico en OSPF se encapsula en paquetes TP siendo reconocido con el puerto 89. OSPF utiliza cinco tipos de paquetes diferentes:

- Hello, establecen la comunicación con vecinos conectados directamente.
- Database Descriptor (DBD), envían una lista de los ID de los routers, las LSA y el número de secuencia. Esta información se utiliza para probar la red.

- Link State Request (LSR), siguen a los paquetes DBD preguntando por cualquier paquete LSA que se haya perdido.
- Link State Update (LSU), son las respuestas a las LSR con los datos que se han pedido.
- Link State Acknowledgements (LSAck), confirma la recepción del paquete.

Los DBD son la parte primaria de las LSA que tiene el router, los LSR solicitan las LSA completas y los LSU son las respuestas conteniendo las LSA completas que se habían solicitado [5].

El paquete LSU se utiliza para responder a un paquete LSR. Los paquetes LSU también se usan para reenviar actualizaciones de enrutamiento OSPF, como cambios de enlace. Específicamente, un paquete LSU puede contener 11 tipos de LSA OSPFv2, como se muestra en la Tabla 12.

Tabla 12. Tipo de LSA y su descripción

Tipo de LSA	Descripción
1	LSA de router
2	LSA de red
3 o 4	LSA de resumen
5	LSA externos del sistema autónomo
6	LSA de OSPF multicast
7	Definido para áreas no tan llenas
8	LSA de atributos externos para el protocolo gateway fronterizo (BGP)
9, 10, 11	LSA opacas

En ocasiones, la diferencia entre los términos LSU y LSA puede resultar confusa, ya que estos términos a menudo se usan de manera indistinta. Sin embargo, una LSU contiene una o más LSA. Los paquetes OSPF tienen un formato común que se representa en la siguiente Tabla 13:

Tabla 13. Contenido del paquete OSPF

Campo	Descripción
Version	Puede ser versión 2 o 3, según sea IPv4 o IPv6.
Type	Hay 5 tipos de paquetes numerados del 1 al 5.
Packet Lenght	Longitud medida en bytes.
Router ID	Identificador del router de 32 bits.
Area ID	Identificador del área de 32 bits.
Checksum	Control estándar de 16 bits.
Authentication Type	OSFPv2 soporta tres tipos de autenticación: • No autenticación. • Texto plano. • Encriptado MD5.

Authentication Data	Son 64 bits de datos que pueden estar vacíos, contener texto plano o encriptación MD5.
Data	Son los datos que se están enviando.

Cuando un router OSPF se conecta inicialmente a una red, intenta hacer lo siguiente:

- Crear adyacencias con los vecinos.
- Intercambiar información de routing.
- Calcular las mejores rutas.
- Lograr la convergencia.

Al intentar lograr la convergencia, OSPF atraviesa varios estados:

- Down: es el primer estado de OSPF y significa que no se ha escuchado ningún hello de este vecino.
- Attempt: este estado es únicamente para redes NBMA, durante este estado el router envía paquetes hello de tipo unicast hacia el vecino, aunque no se hayan recibido hello de ese vecino.
- Init: se ha recibido un paquete hello de un vecino, pero el ID del router no está listado en ese paquete hello.
- 2-Way: se ha establecido una comunicación bidireccional entre dos routers.
- Exstart: una vez elegidos el DR y el BDR el verdadero proceso de intercambiar información del estado del enlace se hace entre los routers y sus DR y BDR.
- Exchange: en este estado los routers intercambian la información de la base de datos DBD.
- Loading: es en este estado cuando se produce el verdadero intercambio de la información de estado de enlace.
- Full: finalmente los routers son totalmente adyacentes, se intercambian las LSA y las bases de datos de los routers están sincronizadas.

Los mensajes hello se siguen enviando periódicamente para mantener las adyacencias, en el caso de que no se reciban se dará por perdida dicha adyacencia. Tan pronto como OSPF detecta un problema modifica las LSA correspondientes y envía actualizaciones a todos los vecinos. Este proceso mejora el tiempo de convergencia y reduce al mínimo la cantidad de información que se envía a la red [5].

2.6.3.- Router designado (DR) y router designado de reserva (BDR)

Cuando varios routers están conectados a un segmento de red del tipo broadcast, uno de estos routers del segmento tomará el control y mantendrá las adyacencias entre todos los routers de ese segmento. Ese router toma el nombre de DR (Desígnate Router) y será elegido a través de la información que

contienen los mensajes hello que se intercambian los routers. Para una eficaz redundancia también se elige un router designado de reserva o BDR**.** Los DR son creados en enlaces multi-acceso debido a que el número de adyacencias incrementaría de manera significativa el tráfico en la red, de esta forma el DR y el BDR establecen adyacencias reduciendo la cantidad de adyacencias necesarias [5].

Para comprender el problema de las adyacencias múltiples, se debe estudiar una fórmula:

Para cualquier cantidad de routers (designada como n) en una red de accesos múltiples, hay n (n – 1) / 2 adyacencias. [7]

Según esta fórmula, respecto a la Figura 2-28, cuatro routers establecen 6 adyacencias: 4(4-1)/2=6. [5]

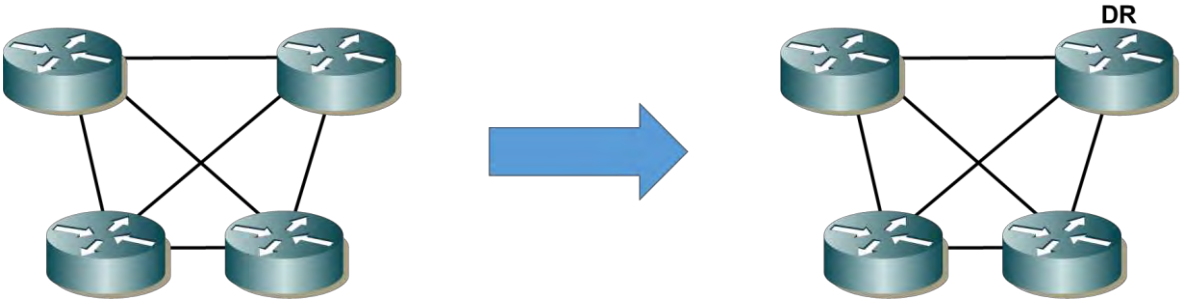


Figura 2-28. Adyacencias de router

Esta forma de añadir adyacencias consumiría gran cantidad de ancho de banda, recursos de memoria y CPU de los routers. El propósito final del DR es reducir al máximo este consumo de recursos haciendo que todos los demás routers establezcan adyacencias con él, quedando establecida en la formula n-1 [5].

El DR recibe actualizaciones y las distribuye a todos los demás routers del segmento asegurándose con acuses de recibo de que estos han recibido correctamente dichas actualizaciones y que poseen una copia sincronizada de la LSDB. Los routers notifican los cambios a través de la dirección multicast 224.0.0.6 a su vez el DR envía las LSA a los routers por la dirección multicast 224.0.0.5. El BDR escucha pasivamente y mantiene una tabla de relación con todos los demás routers, en el caso de que el DR deje de enviar hello el BDR tomará el papel del DR. Este concepto de DR y BDR en enlaces punto a punto no tendría sentido puesto que solo se establece una única adyacencia, por lo tanto, no hay necesidad de esta elección. Sin embargo, en enlaces punto a punto del tipo ethernet existe elección de DR y BDR, para evitar esto se recomienda un diseño del tipo punto a punto y así evitar la elección de estos [5].

L a elección de DR y BDR dependerá de la interfaz de loopback más alta que esté configurada en el router o también en el caso de que esté configurado el comando ip ospf prioritv. Por defecto la prioridad es 1, en un rango 0 a 255, a mayor prioridad mayores posibilidades de que sea elegido como DR. La

configuración de una prioridad 0 hace que el router no participe en la elección [5].

En caso de empate en la designación porque no este configurado el siguiente comando: *Router (config-if)# ip ospf priority number*, o los valores son iguales, entonces se remite a la interfaz loopback más alta; pero si aun así hay igualdades o no hay interfaz de loopback, será finalmente una interfaz física más alta la que participe en la elección del DR. La siguiente prioridad más baja determinará quién será el BDR. Una vez concluido el proceso de elección si se agregara a la red un router con mejor prioridad no tomaría el rol de DR o BDR, esto ocurriría si se caen las adyacencias o se reiniciara el router. Esta regla es importante a tener en cuenta en el momento de iniciar los routers en una red puesto que una vez hecha la elección no habrá cambios, aunque se añadan más routers. El administrador debe tener en cuenta este proceso considerando como muy importante el orden de inicio de la red. En muchos diseños se aconseja cambiar las prioridades a cero para que la elección sea la correcta [5]. En la Figura 2-29, se muestra un diagrama de flujo de como el router determina el ID de router.

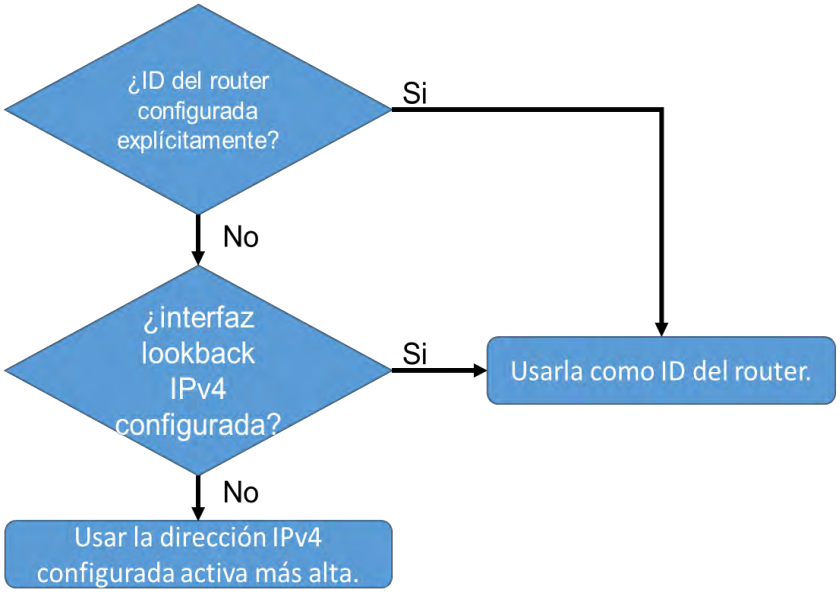


Figura 2-29. Diagrama de flujo para determinar el ID del router

Si el router usa la dirección IPv4 más alta para la ID del router, la interfaz no necesita tener OSPF habilitado. Esto significa que no se necesita incluir la dirección de interfaz en uno de los comandos *network* de OSPF para que el router use esa dirección IP como ID del router. El único requisito es que la interfaz esté activa y en estado up (activo) [7].

El comando *network* determina qué interfaces participan en el proceso de routing para un área OSPF. Cualquier interfaz de un router que coincida con la dirección de red en el comando *network* está habilitada para enviar y recibir paquetes OSPF. Como consecuencia, se incluye la dirección de red (o de subred) para la interfaz en las actualizaciones de routing OSPF [7].

La sintaxis básica del comando es: *network dirección-red máscara-wildcard area id-área*.

La sintaxis area *id-área* se refiere al área OSPF. Al configurar OSPF de área única, se debe configurar el comando network con el mismo valor *id-área* en todos los routers. Si bien se puede usar cualquier ID de área, es aconsejable utilizar una ID de área 0 con OSPF de área única. Esta convención facilita la tarea si posteriormente se modifica la red para admitir OSPF multiárea [7].

De manera predeterminada, los mensajes OSPF se reenvían por todas las interfaces con OSPF habilitado. Sin embargo, estos mensajes solo necesitan enviarse por las interfaces que se conectan a otros routers con OSPF habilitado [7].

Los mensajes OSPF se reenvían por las interfaces de los routers, aunque no exista ningún vecino OSPF en esa LAN. El envío de mensajes innecesarios en una LAN afecta la red de tres maneras:

- Uso ineficaz del ancho de banda: se consume el ancho de banda disponible con el transporte de mensajes innecesarios. Los mensajes se transmiten por multidifusión; por lo tanto, los switches también reenvían los mensajes por todos los puertos [7].
- Uso ineficaz de los recursos: todos los dispositivos en la LAN deben procesar el mensaje y, finalmente, descartarlo [7].
- Mayor riesgo de seguridad: anunciar actualizaciones en una red de difusión constituye un riesgo de seguridad. Los mensajes OSPF se pueden interceptar con software de detección de paquetes. Las actualizaciones de enrutamiento se pueden modificar y enviar de regreso al router, y dañar la tabla de enrutamiento con métricas falsas que desorientan el tráfico [7].

Para evitar estas afectaciones es necesario activar las rutas pasivas en los equipos. Una interfaz pasiva no participa en el proceso de enrutamiento. En RIP el proceso escucha, pero no envía actualizaciones de enrutamiento en una interfaz que es pasiva. En OSPF y EIGRP no se envían hello, por lo tanto, nunca se podrán formar relaciones de vecindad a través de la interfaz pasiva [5].

Las interfaces que participan en el proceso de enrutamiento son controladas por la configuración de la interfaz, dicha configuración instruye al proceso de enrutamiento para que sepa qué interfaces utilizar por medio del comando *network*. El comando: *passive interface,* es útil para deshabilitar el proceso de enrutamiento en interfaces específicas y ayuda a prevenir bucles.

2.6.4.- Costo

Un protocolo de enrutamiento utiliza una métrica para determinar la mejor ruta de un paquete a través de una red. Una métrica indica la sobrecarga que se requiere para enviar paquetes a través de una interfaz determinada. OSPF utiliza

el costo como métrica. Cuando el costo es menor, la ruta es mejor que una con un costo mayor [7].

OSPF utiliza el coste como cálculo de la métrica. Este valor se obtiene en base a la siguiente fórmula [5]:

$$\frac{10^8 bps}{VelocidadEnlace}$$

El ancho de banda de referencia predeterminado es 10^8 (100 000 000). En la Tabla 14 se muestra un desglose del cálculo del costo:

Tabla 14. Calculo del costo por interfaz

Tipo de interfaz	Ancho de banda de referencia en bps		Ancho de banda predeterminado en bps	Costo
10 Gigabit Ethernet - 10 Gbps	100,000,000	÷	10,000,000,000	1
Gigabit Ethernet - 1 Gbps	100,000,000	÷	1,000,000,000	1
Fast Ethernet - 100 Mbps	100,000,000	÷	100,000,000	1
Ethernet - 10 Mbps	100,000,000	÷	10,000,000	10
Serial - 1544 Mbps	100,000,000	÷	1,544,000	64
Serial - 128 kbps	100,000,000	÷	128,000	781
Serial - 64 kbps	100,000,000	÷	64,000	1562

Los tres primeros valores tienen el mismo costo debido al ancho de banda de referencia.

OSPF utiliza un ancho de banda de referencia de 100 Mb/s para todos los enlaces que sean iguales o más rápidos que una conexión Fast Ethernet. Por lo tanto, el costo asignado a una interfaz Fast Ethernet con un ancho de banda de interfaz de 100 Mb/s sería igual a 1, quedando la fórmula de la siguiente manera:

$$Costo = \frac{10^8 bps}{100\ 000\ 000} = 1.$$

Si bien este cálculo funciona para las interfaces Fast Ethernet, es problemático para los enlaces que son más rápidos que 100 Mb/s, debido a que la métrica de OSPF solo utiliza números enteros como costo final de un enlace. Si se calcula un valor menor que un número entero, OSPF redondea al número entero más cercano. Por este motivo, desde la perspectiva de OSPF, una interfaz con un ancho de banda de interfaz de 100 Mb/s (un costo de 1) tiene el mismo costo que una interfaz con un ancho de banda de 100 Gb/s (un costo de 1). Para ayudar a OSPF a determinar la ruta correcta, se debe cambiar el ancho de banda

de referencia a un valor superior, a fin de admitir redes con enlaces más rápidos que 100 Mb/s [7].

Dependiendo del diseño de red es conveniente efectuar cambios en el cálculo del coste para tener un mayor control sobre cómo OSPF calcula la métrica hacia los destinos. Cuanto menor sea el valor del coste mejor será el cálculo de la métrica. El valor del coste es de 16 bits, el administrador puede configurarlo en un rango de 0 a 6553 según la siguiente sintaxis: ip ospf cost *(costo)* [5].

Otra forma de que el router calcule el coste es modificando el numerador con que OSPF calcula de manera automática la métrica. El valor por defecto es 100, pero oscila en rango de 1 a 4294967 [5].

El comando es: ospf auto-cost reference-bandwidth (ancho de banda).

Es aconsejable aplicar este comando a todas las interfaces que participan en el proceso OSPF. También es importante saber que el comando, ip ospf cost, sobrescribe cualquier cálculo que el router haya hecho de manera automática [5].

2.6.5.- Verificación de OSPF en una sola área

A continuación, se describen los comandos más importantes para la verificación y control de OSPF en un área simple: show ip ospf *[id de proceso].*

Este comando muestra la configuración de OSPF en u n router en particular, es especialmente útil para saber el número de veces que se ha ejecutado el algoritmo SPF, que es un indicativo de la estabilidad de la red [5].

La siguiente Figura 2-30, muestra un ejemplo del comando: show ip ospf 220.

```
Router# show ip ospf 220
Routing Procesa "ospf 220" with ID 192.168.0.10
Supports only single TOS(TOSO) routes
It ia an i n t e m a l router
SPF achedule delay 5 seca, Hold time between tv/o SPFs 10 seca
Mínimum LSA interval 5 sec a . Minimum LSA arrival 1 seca
Number of external LSA 0. Checksum Sum 0x0
Number of DCbitless external LSA 0
Number of DoNotAge external LS A 0
Number of areas in thia router ia 1. 1 normal 0 atub 0 nasa
Area 3
Number of interfaces in thia area ia 3
Area has no authentication
SPF algorithm executed 10 times
Area ranges are
Link State üpdate Interval is 00:30:00 and due in 00:18:54
Link State Age Interval ia 00:20:00 and due in 00:08:53
Number of DCbitless LS A 2
Number of indication LSA 0
Number of DoNotAge LSA 0
```

Figura 2-30. Resultado del comando OSPF

La tabla 15 muestra la descripción de los parámetros del resultado del comando ejecutado:

Tabla 15. Descripción de algunos comandos

Campo	Descripción
Routing process "ospf 220" with ID 192.168.0.10	Muestra el ID del proceso local del OSPF y el router ID de OSPF.
It is an internal router	Tipo de router.
SPF schedule delay	Tiempo de espera SPF para ejecutarse después de recibir un LSA. Previene ejecutar SPF de manera frecuente.
Hold time between two SPFs	Tiempo mínimo entre cálculos de SPF.
Number of DCbitless external LSA	Se usa en circuitos de OSPF “on demand”.
Number of DoNotAge external LSA	Se usa en circuitos de OSPF “on demand”, por ejemplo ISDN.

Area 3 Number of interfaces in this area is 3 Area has no authentication SPF algorithm executed 10 times Area ranges are	Área que pertenece al router, como este router es interna solo pertenece a una. Cuantas interfaces hay en cada área. Autenticación ci la hay. Cuantas veces se ha ejecutado el algoritmo SPF. Si hay sumarizaciones.
Link State update Interval is 00:30:00 and due in 00:18:54	El tiempo por defecto de actualización de las LSA es 30 minutos y es usado para garantizar la integridad de la base de datos topológica.
Link State Age Interval is 00:20:00 and due in 00:08:53	Intervalo de borrado de max-aged y cuando serán eliminadas las rutas desactualizadas.

El siguiente comando: *show ip ospf neighbor [type number] [neighbor-id] [detail],* muestra los vecinos OSPF. Puede utilizarse listando todos los vecinos, por interfaces o con detalles más precisos de los vecinos, la Figura 2-31, es un ejemplo de los comandos ejecutados [5].

```
Router# show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
140.100.17.132 1 FULL/DROTHER 00:00:36 140.100.17.132 FastEth em e tl / 0
140.100.17.131 1 FULL/DROTHER 00:00:37 140.100.17.131 FastEthe m et l /0
140.100.23.1 1 FCJLL/BDR 00:00:38 140.100.17.130 FastEth e me t l/ 0
140.100.32.12 1 FULL/DROTHER 00:00:35 140.100.32.12 FddÍ2/0
140.100.32.11 1 FULL/DR 00:00:32 140.100.32.11 FddÍ2/0
140.100.17.194 1 FULL/DR 00:00:31 140.100.17.194 FaatEthernet3/0

Router# show ip ospf neighbor aerial0/0
Neighbor ID Pri State Dead Time Address Interface
140.100.32.12 1 FULL/DROTHER 00:00:36 140.100.32.12 serÍal2/0
140.100.32.11 1 FULL/DR 00:00:32 140.100.32.11 serÍal2/0

Router# show ip ospf neighbor detall
Neighbor 140.100.17.132, interface address 172.100.17.132
In the area 3 via interface F a s t E t he m et l /0
Neighbor priority is l, State is FULL, 6 State changes
DR is 172.100.17.129 BDR is 172.100.17.130
Options 2
Dead timer due in 00:00:35
Neighbor 140.100.17.131, interface address 140.100.17.131
In the area 3 via interface F a s t E t he m et l /0
Neighbor priority is l, State is FULL, 6 State changes
DR is 140.100.17.129 BDR is 140.100.17.130
Options 2
Dead timer due in 00:00:34
Neighbor 140.100.23.1, interface address 140.100.17.130
In the area 3 via interface F a s t E t he m et l /O
Neighbor priority is l, State is FULL, 6 State changes
DR is 140.100.17.129 BDR is 140.100.17.130
Options 2
Dead timer due in 00:00:36
Neighbor 140.100.32.12, interface address 140.100.32.12
In the area 3 via interface Fddi2/0
Neighbor priority is l, State is FULL, 6 State changes
DR is 140.100.32.11 BDR is 140.100.32.10
Options 2
Dead timer due in 00:00:32
Neighbor 140.100.32.11, interface address 140.100.32.11
In the area 3 via interface Fddi2/0
Neighbor priority is l, State is FULL, 6 State changes
DR is 140.100.32.11 BDR is 140.100.32.10
Options 2
Dead timer due in 00:00:38
Neighbor 140.100.17.194, interface address 140.100.17.194
In the area 3 via interface F a s t E t he m et 3 /0
Neighbor priority is l, State is FULL, 9 State changes
DR is 140.100.17.194 BDR is 140.100.17.1
```

Figura 2-31. Comandos show para OSPF

La Tabla 14, muestra la descripción de los parámetros del resultado del comando ejecutado:

Tabla 16. Descripción de algunos comandos útiles

Campo	Descripción
Neighbor	Router ID.
Neighbor priority	Prioridad enviada en el mensaje hello.

State	Muestra el estado en que se encuentra el vecino • Down • Attempt • Init • 2-way • Exstart • Exchange • Loading • Full
Dead Time	Periodo de tiempo que el router esperara sin escuchar hello para declarar al vecino como muerto.
Address	Dirección IP del vecino. Hay que tener en cuenta que no tiene por qué ser la misma que la del Router ID.
Interface	Interfaz por la cual se ha conocido el vecino.
Options	Identifica una stub área.

Con el comando *show ip protocols,* se puede ver la configuración de los protocolos de enrutamiento que estén habilitados en el router y cómo interactúan entre ellos. De igual forma se puede ver cuándo se producirá la siguiente actualización. [5]

La Figura 2-32, despliega el comando anterior.

```
Router# show ip protocols
Routing Protocol is "ospf 220"
Sending updates every 0 seconds
Invalid after 0 seconds, hold down 0, flushed after 0
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: ospf 220
Routing for Networks:
172.202.0.0
Routing Information Sources:
Gateway Distanee Last Update
172.202.17.131 110 00:50:23
172.202.17.132 110 00:50:23
172.202.17.194 110 00:07:39
172.202.23.1 110 00:50:23
Distance: (default is 110)
```

Figura 2-32. Comando show ip protocols

La tabla 17 muestra la descripción de los parámetros del resultado del comando ejecutado:

Tabla 17. Descripción de algunos comandos útiles para OSPF

Campo	Descripción

Routing protocol is “ospf 220”	Protocolo de enrutamiento configurado.
Sending updates every 0 seconds	Frecuencia de las actualizaciones.
Invalid after 0 seconds	Para protocolos vector-distancia indica el tiempo que una ruta es considerada válida.
Hold down 0	Hold down es un tiempo usado en protocolos vector-distancia.
Flushed after 0	Tiempo en el que un protocolo vector-distancia eliminará una ruta de la tabla de enrutamiento.
Outgoing update filter list for all interfaces is not set	Indica si hay algún filtro de salida.
Incoming update filter list for all interfaces is not set	Indica si hay algún filtro de entrada.
Redistributing: ospf 220	Muestra información de redistribuciones.
Routing for networks: 172.202.0.0	Configuración del comando network.
Routing information sources	Direcciones de origen de los router que envían actualizaciones a este router.
Gateway	Dirección del router que proporciona actualizaciones.
Distance	Distancia administrativa.
Last update	Tiempo desde que el router recibió la última actualización.
Distance: (default is 110)	La distancia administrativa se puede cambiar para todo el protocolo o por origen.

El comando: *show ip ospf database,* muestra los contenidos de la base de datos topológica, como se ve en el siguiente ejemplo de la Figura 2-33.

```
Router# show ip ospf database
OSPF Router with ID (172.100.32.10) (Process ID 220>
Router Link States (Area 2)
Link ID AD V Router Age Seq# Checksum Link count
172.100.17.131 172.100.17.131 471 0x80000008 0xA469 1
172.100.17.132 172.100.17.132 215 0x80000007 0xA467 1
172.100.17.194 172.100.17.194 1489 Ox8000000B 0XFF16 1
172.100.23.1 172.100.23.1 505 0x80000006 0x56B3 1
172.100.32.10 172.100.32.10 512 Ox8000000C 0x46BA 3
172.100.32.11 172.100.32.11 150 0x80000006 0x6A73 1
172.100.32.12 172.100.32.12 1135 0x80000002 0x8E30 1
Net Link States (Area 2)
Link ID A DV Router Age Seq# Checksum
172.100.17.130 172.100.23.1 220 0x80000007 0x3B42
172.100.17.194 172.100.17.194 1490 0x80000002 0xl5C9
172.100.32.11 172.100.32.11 150 0x80000004 0x379E
```

Figura 2-33. Comando show ip ospf database

El comando *show ip ospf interfaces [tipo de numero],* brinda información sobre como OSPF está configurado en cada una de las interfaces, como se ve en la Figura 2-34.

```
Router#show ip ospf interface fastethernet0/0
Fastethernet0/0 is up, line protocol is up
Internet Address 172.100.17.129/28, Are a 2
Process ID 100, Router ID 172.100.32.10, NetWork Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 100
Designated Router (ID) 172.100.32.10, Interface address 172.100.17.129
Backup Designated router (ID) 172.100.23.1, Interface address 172.100.17.130
Timer intervals configurad, Helio 10, Dead 40, Wait 40, Retransmit 5
Helio due in 00:00:06
Neighbor Count is 3, Adjacent neighbor count is 2
Adjacent with neighbor 172.100.17.132
Adjacent with neighbor 172.100.23.1 (Backup Designated Router)
Suppress helio for 0 neighbor(s)
```

Figura 2-34. Comando show ip ospf interface

Capítulo 3 : Fortinet como Equipo de Seguridad Perimetral

3.1.- Introducción

La fábrica de seguridad de Fortinet o también llamado el tejido de seguridad de Fortinet (Fortinet Security Fabric) es una empresa que tiene una visión para el cumplimiento de seguridad sin compromiso: es inteligente, poderoso y sin fisuras. Es diseñado para adaptar el envolvimiento dinámico de la infraestructura de TI, y dar una rápida respuesta a los cambios de ataque de la parte exterior de una red [10].

Fortinet integra la seguridad para los usuarios finales (endpoint), seguridad para la capa de acceso inalámbrica, seguridad a la red, seguridad de las aplicaciones utilizadas dentro de la red, seguridad para el data center y la nube dentro de una solución cooperativa que puede ser administrada, analizada y dirigida a través de una interfaz administradamente [10].

Fortinet está construido alrededor de tres críticas e independientes atributos:

- Consiente: La inteligencia de la seguridad debe ser consiente, los componentes con el entorno deben estar visible dentro de toda la infraestructura, incluyendo los usuarios finales, los elementos de la red, los data center, la nube y los datos propios. Hay que tener conciencia de que los datos y los elementos antes mencionados, fluyen para, desde y a través de ellos, de esta forma los administradores pueden segmentar el ambiente por niveles de confianza. La segmentación de las redes no solo separa lógicamente los datos y los recursos, sino que también permite una visibilidad avanzada de datos y las amenazas y de cómo se mueven desde una zona de red a otra. Desde una perspectiva de amenaza, la segmentación de la red divide zonas de seguridad para ayudar en el cumplimiento, monitorear internamente el tráfico y los dispositivos, prevenir accesos no autorizados para restringir los datos y los recursos, y el control de la propagación de intrusos y malware. Las soluciones de seguridad deben automáticamente trabajar juntos como un sistema para mapear, monitorear y asegurar la distribución de la empresa, combinado con el control de políticas y coordinar las respuestas entre diferentes dispositivos de seguridad como una controladora principal desarrollado por Fortinet. Este enlaza los datos, aplicaciones, dispositivos y flujos de trabajo, de tal forma que proveen un nivel de conciencia y sensibilidad [10].
- Escalable: La seguridad de Fortinet de igual forma debe ser poderoso y no puede comprometer el rendimiento total o parcial de la red. El mismo rendimiento de seguridad que tiene Fortinet, debe darla a los endpoint como computadoras o teléfonos móviles, que están en la capa de acceso de la red, ya sea cableado o de forma inalámbrica. Fortinet es capaz de escalar su seguridad desde pequeñas oficinas hasta un crecimiento de redes grandes, con datos más complejos y con ambiente de data center. Fortinet también puede proteger redes privadas virtuales, hibridas y nubes públicas [10].

- Accionable: actualmente la seguridad estratégicamente la llaman, seguridad sin fisuras. Fortinet entrega alertas de seguridad, recomendaciones e informes de auditoría sin fisuras cruzando todos los elementos de seguridad. Mediante el intercambio en tiempo real de la inteligencia de las amenazas locales y globales (a través de una interfaz de análisis y gestión unificada), Fortinet habilita una respuesta dinámica para las capacidades criminales mientras implementan nuevas estrategias para las amenazas y ataques al zero-day [10].

3.2.- Unified Threat Management

Una Unified Threat Management (UTM), es una plataforma convergida que provee características de los productos de seguridad de puntos tradicionalmente separados. En empresas grandes estos productos son proporcionados por aparatos individuales dedicados, por ejemplo, para la seguridad de la red (firewall, VPN, IPS y el control de aplicación), para la seguridad de la web (incluyen el filtrado web y antimalware) y los mensajes de seguridad (anti spam, antipishing, y otros) [10]

Fortinet ofrece seguridad todo en uno de alto rendimiento, es un sistema altamente efectivo y fácil de administrar para pequeñas y medianas empresas. La seguridad que ofrece Fortinet de todo en uno se refiere no solo a las redes tradicionales, web y mensajes de seguridad, sino que también a los nuevos servicios de seguridad como los firewalls de aplicaciones web, administración de seguridad a los endpoint y más. Agregando, los modelos Fortinet cuentan con un controlador inalámbrico y de Access point (AP) [10].

3.2.1.- Redes y seguridad todo en uno

Hay diferentes modelos de equipos de Fortinet con UTM que cuentan con distintos rendimientos y características de hardware, todos los modelos incluyen un controlador inalámbrico y tienen integrado el Power over Ethernet (PoE), que son puertos para una fácil expansión. Ambos servicios de seguridad y características de redes son administrados todos desde una única interfaz [11].

Los ya antes mencionados servicios de seguridad demuestran alta efectividad durante pruebas conducidas por organizaciones como Virus Bulletin, AV comparatives, NSS Labs, ICSA, entre otros, como se muestra en la Figura 3-1 [11].

Figura 3-1. Organizaciones de seguridad [10]

Cada Fortinet conectado al UTM es fácil para usar y cuenta con rápidas guías de instalación, su administración igual es muy sencilla de manejar con una ventana para observar y controlar toda la seguridad y características de la red. Haciendo esto, Fortinet ofrece una manera fácil de mantener una consistente política cruzando todos los servicios de seguridad [11].

Se debe tomar en cuenta, que para obtener los servicios de UTM es necesario una compra y registro de licenciamiento, ya que sin esto queda deshabilitado la seguridad de su equipo de Fortinet.

Mencionando rápidamente, el FortiAP 221C y el FortiSwitch 224D son los más comunes aliados para el FortiGate UTM, Fortinet recomienda considerar incluir un AP o switch con una orden UTM, unos ejemplos de los equipos son como los que se muestra en la Figura 3-2 [11].

Objetivo	Interior	SSIDs Simultáneos	8 (7 para clientes 1 para monitoreo)
Numero de antenas	221B: 4 internos 223B: 4 externos	Max. Poder de transmisión	17 dBm (50mW)
Numero de radio	2	Soporte de PoE	802.3af
Tx / RX Stream (802.11n)	2x2 MIMO con Dual espacial streams, 600 Mbps total		

Capacidad de Switch	48 Gbps	Soporta VLAN	4096
Almacenamiento MAC	16,000	Total de puertos en grupo Link Aggregation	Hasta 8 puertos
Administración	FOS, CLI & Web	PoE Power	180 W
Objetivo	Convergente LAN Edge	Administración FortiGate	Yes

Figura 3-2. FortiAP y FortiSwitch

3.3.- Productos de Entrada de Fortinet

Fortinet busca una solución que pueda proveer consolidación de seguridad y funciones de red, y así mismo decrecer la complejidad inherente en la administración de la red de miles de distintos tipos de empresas con una política unificada, para así usar un único “pane of glass” o también conocido como único panel de administración [11].

Fortinet busca reducir los costos WAN y al mismo tiempo asegurar el acceso público a las aplicaciones de la nube [11].

3.3.1.- Firewall empresarial

La solución de firewall empresarial de Fortinet es líder de la industria de seguridad en la red y efectivo en un único sistema operativo [10].

Provee la más rápida “fábrica de seguridad cooperativa” (Cooperative Security Fabric) para las más avanzadas amenazas, el objetivo de estos equipos firewall,

que normalmente se encuentran en el borde de la red, es detectar las amenazas vistas durante el día [10].

El equipo de firewall empresarial de Fortinet cuenta con un sistema operativo de red consolidado que incorpora todo el sistema y las capacidades de funciones de la red en un único sistema operativo. El único panel de administración lo usa para mantener, configurar y controlar varias políticas de seguridad, que también incluye el inicio de sesión, monitoreo y reportes [10].

La unidad central de los equipos, el compartir la inteligencia de amenazas entre los firewalls y la seguridad de la tecnología, es una característica de estos equipos de Fortinet, esto ayuda a una rápida detección y remedios de nuevas amenazas [10] .

Su alta velocidad de procesamiento para la seguridad es otra de las características de estos equipos de Fortinet, es lo suficientemente rápido para establecer los puntos de ingreso y egreso de la red interna y la red externa de la infraestructura de la empresa [10].

Los múltiples factores que Fortinet ofrece, se puede abordar con la variedad de los distintos modelos de FortiGate [10].

La tecnología de inteligencia de amenazas para una efectiva seguridad es regularizada por el FortiGuard [10].

La consolidación de los sistemas operativos de la red, requiere de un nivel de unificación en sistema y la funcionalidad de la red, que esto es otorgado por el FortiOS [10].

El FortiManager permite centralizar un control de todos los diversos posibles equipos de FortiGate, el FortiManager provee un único panel de administración para la facilidad del control [10].

La fábrica de seguridad cooperativa de Fortinet es una alta dependencia en intercomunicaciones que ayuda a que diversas aplicaciones puedan comunicarse entre ellas como por ejemplo entre el FortiOS y el FortiManager [10].

Y finalmente, todas estas operaciones, son interacciones que deben ocurrir rápidamente y que tenga una muy poca, o ninguna degradación del rendimiento, para eso Fortinet cuenta con el procesador FortiASIC que da potencia a los productos FortiGate [10].

En la siguiente Tabla 18, se muestra las características y puntos clave de los ya mencionados productos [10].

Tabla 18. Características de algunos equipos Fortinet

Factores	Tecnología	Productos
Factores de formas múltiples	Firewall	FortiGate

Seguridad efectiva	Inteligencia de amenazas	FortiGuard
Consolidación de los sistemas operativos de la red	Sistema Operativo	FortiOS
Único panel de administración	Administración	FortiManager
Tela cooperativa de seguridad	API	FortiOS & FortiManager
Procesamiento de seguridad de alta velocidad	Procesamiento de la red y la seguridad	FortiGate (FortiASIC)

En la Figura 3-3, se muestra los modelos y rangos de FortiGate y el uso más común que se les da [10].

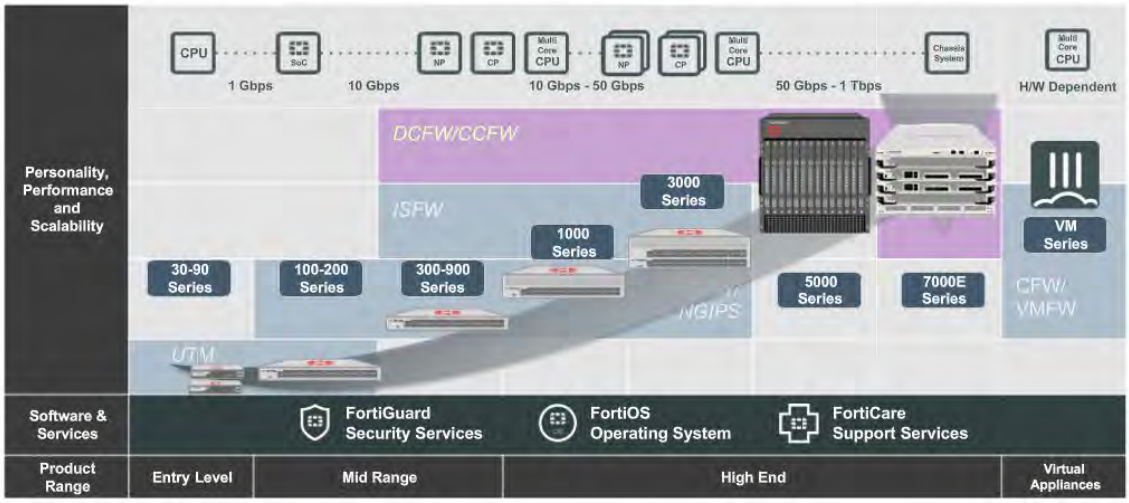


Figura 3-3. Modelos y rangos de FortiGate [10]

El FortiGate de modelos 30 y 90, representan el primer rango de nivel de entrada, son los más comúnmente usados en los UTM y para las sucursales de empresas o empresas en desarrollo [11].

El FortiGate de series 100-200 es del nivel de rango medio, los usuarios usualmente utilizan estos modelos por su seguridad de UTM, son firewalls next generation de menor rendimiento [11].

Los FortiGate de series 300-900 son la línea de medio rendimiento, son los más comunes para el uso de firewall de next generation para pequeñas a medianas empresas [11] .

El FortiGate series 1000 es una línea de firewall de next generation de fuerte poder, este FortiGate tiene grandes capacidades de procesamiento y son ocupadas dentro de las más grandes redes empresariales [11].

El FortiGate series 3000 son hecho para ambientes de altos rendimientos, debido a las cantidades de interfaces que pueden ser usadas para una muy alta respuesta de procesamiento dentro de la red, normalmente son utilizadas en la capa de núcleo [11].

El FortiGate series 5000, es el más poderoso, y que está construido en base al sistema de chasis, por lo que puede ser configurado y ranurado en varias maneras ya que son modulares. Muchas empresas prefieren estos sistemas que son tendientes a crecer para futuras necesidades, es bueno comentar que varias empresas de telecomunicaciones y proveedores de servicios usan esta serie de FortiGate [11].

El nuevo FortiGate de series 7000E, aprovecha la última innovación de procesamiento de FortiASIC CP9 que da grande rendimiento a los firewalls de next generation y una gran aceleración al trafico SSL. Estos modelos vienen pre-configurados en seis diferentes opciones para establecer a las necesidades de los requerimientos de la empresa y tener un fácil desarrollo para la infraestructura de la red [11].

Finalmente, las series de virtualización representan un sistema que puede ser desarrollado a base de los requerimientos específicos que necesite la empresa para su red.

3.4.- FortiClient

Los usuarios finales autónomos, son en la actualidad una solución de gran optimización y bajo costo para las empresas, en resumen, el cliente puede conectarse a los servicios de la empresa desde cualquier parte del mundo con solo tener conexión de internet. Pero cuando hablamos de las cyber amenazas es necesario entrar a una estrategia cohesiva en detectar y responder a las amenazas avanzadas hoy en día [11].

La “Enterprise Adoption of Next-generation” es una solución de Fortinet para dar seguridad a los endpoint que se encuentran fuera de la sucursal.

Para los usuarios finales que se encuentran fuera de las instalaciones de la empresa, una solución es utilizar un software para la conexión VPN y así tomar recursos de la red. Pero una conexión única de VPN sin tener autenticación o la famosa autenticación two-factor es riesgosa para los actuales ataques en la red, otra posible solución a ese problema, es instalar otro software para tener esa autenticación y hacer un poco más segura la conexión VPN, el inconveniente es que el usuario final tiende a tener más incómodo la conexión al utilizar múltiples softwares [11].

La solución es el FortiClient, que es una unificada protección para el endpoint que integra diversas plataformas en lo general a la arquitectura de seguridad, automáticamente protege contra las amenazas y otorga seguridad remota por accesos a la VPN. FortiClient es soportado para diversas plataformas como Windows, Mac, Linux, iOS y Android [11].

El FortiClient está integrado con la fábrica de seguridad de Fortinet, protege al usuario contra a las amenazas avanzadas conocidas y no conocidas basando su seguridad e integración con el FortiSandbox, la seguridad en tiempo real hace del FortiClient más confiable y estable para el usuario final. La seguridad del acceso remoto otorga movilidad, de esta forma la autorización y la seguridad del acceso externo a la corporación viene siendo por medio de una VPN con autenticación two-factor acoplado con una autenticación single sign on (SSO) [11].

Como se muestra en la Tabla 19, FortiClient tiene incorporado un antivirus, aplicación de firewall, filtro web y administración de vulnerabilidades, todos trabajando en conjunto para reducir los ataques que provienen del exterior.

Tabla 19. FortiClient

Antivirus	Aplicación Firewall	Filtro Web	Escaneo de Vulnerabilidad
Protección al host en tiempo real	Detección de actividad en la red	Clasificacioón de URL basada en la nube	Aplicaciones actualizadas
Actualizaciones cada hora	Categorías de aplicaciones	Opción de búsqueda segura	Parches automáticos
Horario de escaneo	Especificación de aplicaciones individuales	Lista de exclusión	Horarios programados de escaneo
Prevención de Malware	Reducir ataques del exterior	Evitar unidades de descarga	Prevención de Exploit

Hay actualizaciones cada hora, donde el FortiClient previene malware por medio de los laboratorios de Fortinet, hacen su mitigación de ataques a través de los motores del antivirus. El escaneo del antivirus puede ser por horario o hecho manualmente por el usuario o también por el operador de seguridad. El FortiClient mitiga el ataque del exterior por medio de la aplicación firewall, usando las políticas de este firewall establecidas desde la fábrica de seguridad de Fortinet, aunque el usuario puede ser capaz de habilitar o deshabilitar esta opción. Si la aplicación firewall cree que el usuario está siendo infectado y da riesgos para la red de la sucursal, el firewall pone en cuarentena al usuario y desconecta de inmediatamente de la red al usuario [11].

El FortiClient ayuda a prevenir grandes unidades de descargas basándose en la reputación de sitios web y de esta forma da a la red un rendimiento óptimo. La protección dinámica del FortiClient proviene de la nube inteligente de FortiGuard [11].

De igual forma el FortiClient previene los exploits, escaneando el host periódicamente o si la situación lo demanda para buscar vulnerabilidades en las aplicaciones instaladas o en el sistema operativo. Sí el FortiClient busca dichas vulnerabilidades, sin necesidad de una intervención por el usuario, pone parches

automáticamente para esas vulnerabilidades, aunque el usuario de igual forma puede escoger si instalar o no esos parches [11].

3.4.1.- Seguridad al acceso remoto y movilidad

Como una unificada protección del producto del usuario final, el FortiClient incluye una conexión VPN SSL e IPSec que trabaja en conjunto con el FortiGate para permitir el acceso a la red interna del corporativo. Las capacidades de autenticación de la VPN son mejoradas con el FortiAutenticador, permitiendo a la VPN del FortiClient trabajar con el FortiToken para una autenticación two-factor. Esta autenticación consiste en tener una llave (FortiToken) que se conecta a Fortinet y te da aleatoriamente un número y además teniendo otra contraseña propia, puedes autenticarte de forma segura para ingresar a la red, de esta forma le das seguridad extra a tu red. El Single sign-on (SSO) funciona por medio de políticas de identidad para el usuario y para dar un acceso especifico. Por ejemplo, en la siguiente Figura 3-4, vemos que podría ser posible garantizar solamente el acceso al administrador financiero para entrar a la base de datos de finanzas [11].

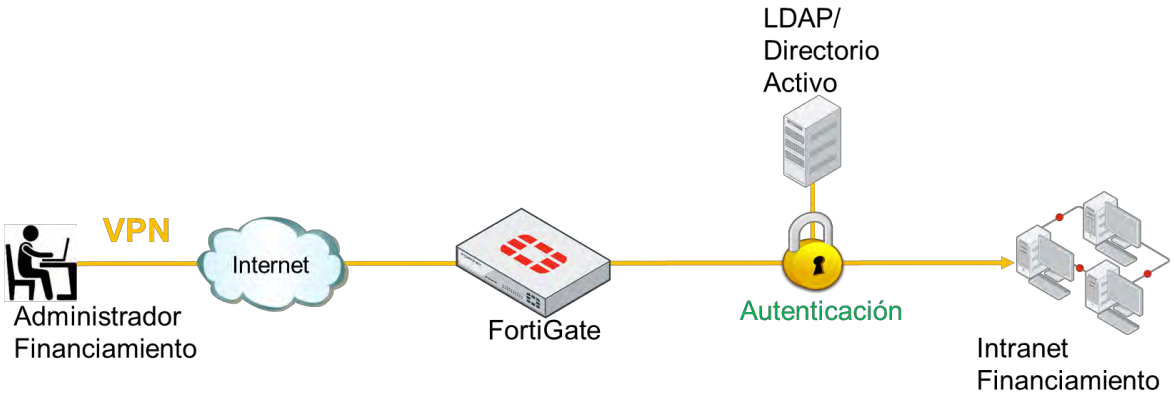


Figura 3-4. Conexión VPN FortiClient

El FortiClient además de ser un software para la conexión VPN, es un antivirus que cuenta con actualizaciones directa del UTM de Fortinet, el cual no solo protege la conexión de sitio a sitio, sino que también protege al usuario final.

3.5.- FortiGate 600D

El FortiGate 600D, que será utilizado en este proyecto como seguridad perimetral, es un “firewall next generation” para medianas a grandes empresas, con una gran flexibilidad para desarrollo en el campus o una sucursal de alguna empresa. Protege su red contra las amenazas con un alto rendimiento de la mejor tecnología de procesadores, es seguro, eficaz y de profunda visibilidad. Algunas de sus principales características se mencionan a continuación:

Seguridad.

- Protege la red contra los conocidos exploits, malware y sitios web maliciosos usando continuamente la inteligencia de amenazas que provee los laboratorios del FortiGuard [11].
- Tiene la capacidad para identificar miles de aplicaciones, incluidas las aplicaciones en la nube y de igual forma hace una inspección profunda en el tráfico de la red [11].
- No solo protege a la red contra los ataques conocidos, de igual forma detecta los ataques desconocidos utilizando análisis dinámicos y proporciona mitigación automatizada para detener ataques dirigidos [11].

Rendimiento.

- Otorga el mejor rendimiento de protección contra las amenazas de las industrias, su retardo es muy bajo ya que usa la tecnología de procesador de seguridad (SPU) [11].
- FortiGate es líder en la industria proporcionando un gran rendimiento y protección contra el tráfico cifrado SSL [11].

Certificación.

- Ha sido probado y validado al entregar la mejor efectividad en la seguridad y el rendimiento [10].
- Recibió certificaciones de terceros sin precedentes provenientes de NSS Labs, ICSA, Virus Bulletin y AV Comparatives [10].

Networking.

- Ofrece un extensivo enrutamiento, switching, controlador inalámbrico y capacidades de alto rendimiento para VPN IPsec, consolidando la funcionalidad completa de la red y su seguridad [11].
- Es una implementación bastante flexible como firewall de próxima generación y de seguridad WAN [11].

Administración.

- La facilidad de usar el panel único de administración (Single Pane of Glass) con el centro de operaciones de red (NOC), hacen al FortiGate bastante atractivo por su flexibilidad y velocidad para identificar problemas de forma intuitiva [11].

Tejido de seguridad.

- A todos los partners de Fortinet y sus productos, permite la integración y seguridad de extremo a extremo en toda la superficie de ataque [11].
- Construye automáticamente visualizaciones de topología de red que hace descubrimientos de los dispositivos IoT (internet of things) y proporciona una visibilidad completa de los productos de Fortinet [11].

El FortiGate 600D combina las capacidades de seguridad de prevención de amenazas en un único dispositivo de alto rendimiento, además reduce la complejidad proporcionando gran visibilidad de dispositivos, usuarios e

información de amenazas, de esta forma crea vista topológica de campus. Este FortiGate detecta de forma proactiva las amenazas desconocidas maliciosas, utilizando el servicio de sandbox integrado basado en la nube [11].

El FortiGate 600D es eficaz al utilizarlo como una red de área amplia basada en internet (SD-WAN). La SD-WAN, llamada por sus siglas en inglés como Software Defined Wide Area Network, es el sustituto correcto para una MPLS que tiene un alto costo, la SD-WAN utiliza conexiones a internet y junto con la inteligencia del equipo de FortiGate 600D, permite usar todas las conexiones a la vez y dirigir a través de las rutas más apropiadas para la empresa, este FortiGate como SD-WAN cuenta con innovaciones como son la controladora central, análisis del tráfico, aprovisionamiento de dispositivos en forma remota y monitoreo de la red de dispositivos, reduciendo de esta forma dramáticamente los costos de una MPLS. El FortiGate 600D asegura el acceso directo a internet para aplicaciones en la nube, de esta forma reduce el retardo y costos de WAN, tiene capacidades eficaces, rentables y de alta prevención de amenazas. Este FortiGate cuenta con un procesador de seguridad que mejora el rendimiento de una VPN IPsec y SSL.

3.5.1.- Hardware del FortiGate 600D

El desarrollo de SPU del FortiGate, proporcionan la potencia necesaria para detectar contenido malicioso a gran velocidad, de esta forma puede reaccionar y bloquear las amenazas emergentes, el FortiGate 600D cumple con las rigurosas certificaciones de terceros para dar solución de seguridad de red y no se conviertan en cuello de botella [11].

Este FortiGate 600D cuenta con el nuevo procesador de red SPU NP6 desarrollado por Fortinet para las ocupaciones del FortiOS y cuenta con las siguientes funciones:

- Ventaja de firewall superior para el tráfico de IPv4/IPv6, SCTP y trafico multicast con un bajo retardo de hasta 2 microsegundos [11].
- Cuenta con la aceleración de IP, túnel VPN y CAPWAP [11].
- Prevención de intrusos basados en anomalías, comprobación de errores checksum y desfragmentación de paquetes [11].
- Tráfico compartido y prioridad [11].

El procesador funciona fuera del flujo directo del tráfico, de esta forma otorga servicios de inspección de contenido y criptografías de alta velocidad, incluye aceleración de trafico de inspección basado en firmas, cuenta con encriptación y descarga de des-encriptación.

En la Figura 3-5, podemos encontrar una vista física del FortiGate 600D.

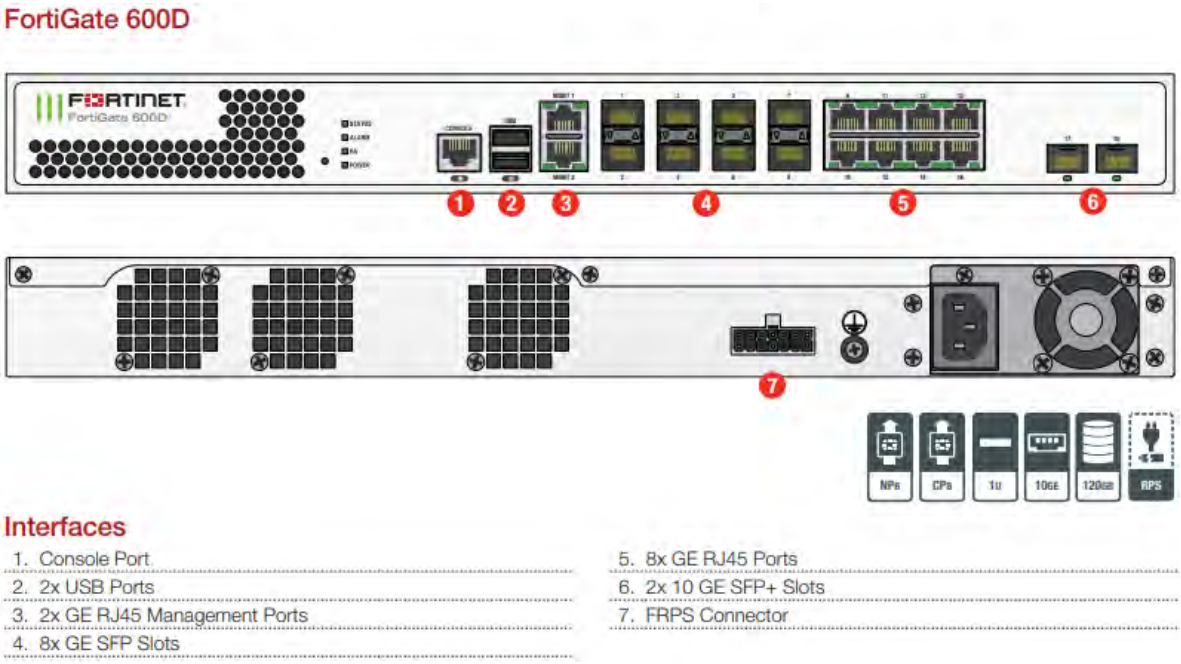


Figura 3-5. FortiGate 600D [10]

1. Como podemos observar, el FortiGate cuenta con interfaces de puerto consola RJ45 para poder entrar a la línea de comandos (CLI) del FortiGate.
2. Tiene dos puertos USB que nos sirve para el backup de configuración del FortiGate o para cargar el firmware si se llega a corromper el sistema.
3. De igual forma cuenta con dos puertos RJ45 de Gigabit Ethernet para la administración del FortiGate y así poder acceder al GUI.
4. Este FortiGate tiene cuatro puertos Gigabit Ethernet para conexiones de switching o routing.
5. Cuenta con cuatro slots SFP que está diseñado para soportar Sonet (red óptica sincronizada), canal de fibra, Gigabit Ethernet y otros estándares de comunicación.
6. El conector FRPS que tiene este FortiGate es para tener una redundancia de alimentación que es esencial en el funcionamiento de las redes de misión crítica. Nos sirve para tener una fuente de alimentación redundante externa, diseñada para aumentar la disponibilidad y el tiempo de actividad de la red.

3.5.2.- Modo de operación

Acerca de la arquitectura del software, el FortiGate puede operar de dos modos, en modo NAT y en modo Transparente [11].

En el modo NAT, el FortiGate reenvía los paquetes basados en la capa 3, como un router. Cada una de sus interfaces de red lógica tiene una dirección IP [11].

En el modo transparente, el FortiGate reenvía paquetes basados en la capa 2, como un switch, de esta forma para la administración de la interfaz, no cuentan con IP las interfaces [11].

En la Figura 3-6, nos muestra las capas del modelo OSI, y como interactúa el tráfico con respecto al FortiGate.

	Capa	Aplicación	Dispositivo/protocolos
NAT	Aplicación (7)	Capa del usuario final	Aplicaciones de usuario
NAT	Presentación (6)	Capa de sintaxis	JPEG/ASCII/GIF/PICT
	Sesión (5)	Sincronización y envió a puertos	Puertos lógicos
	Transporte (4)	TCP	TCP/SPX/UDP
	Red (3)	Paquetes	Routers, IP/IPX/ICMP
Transparente	Enlace (2)	Tramas	Switches, PPP/SLIP
	Física (1)	Estructura física	Hubs, cables, etc.

Figura 3-6. Modo de operación del FortiGate

El modo NAT es el común utilizado, la dirección del destino viene siendo la dirección del FortiGate. Típicamente, FortiGate reescribirá la dirección de destino, el número de puerto y el origen de la dirección IP de la capa de red, en la dirección de red privada del servidor antes de reenviar el paquete, en otras palabras, se aplicará el NAT y el port forwarding [11].

En modo transparente, la dirección del destino es la dirección del servidor, no la interfaz del FortiGate. Como consecuencia, no es necesario reescribir las capas de encapsulación. Solamente la dirección MAC en la trama es reescrito [11].

El NAT es el modo de operación por defecto, y de igual forma por defecto hay otros ajustes de forma general, por ejemplo, el port 1 del FortiGate tiene una dirección 192.168.1.99/24, también tiene habilitado los protocolos para administración de PING, HTTP, HTTPS y SSH. El servidor DHCP para modelos bajos se encuentra activado. Para hacer el login a la administración del FortiGate de manera por defecto tiene como credenciales, en usuario admin, y como de contraseña queda en blanco. Fortinet como recomendación nos dice que pongamos contraseña para el ingreso al GUI, ya que el login por defecto es de conocimiento público [11] .

3.6.- Logging y Monitoreo

Cuando el trafico pasa a través del FortiGate a la red, el FortiGate escanea el tráfico y toma acciones basadas en las políticas de su firewall. Las actividades sucedidas dentro de la red, son grabadas y almacenadas como mensajes de log, pueden ser dentro del disco duro del FortiGate o en un dispositivo externo [11].

El propósito de los logs, es ayudar para monitorear el tráfico de la red, localizar problemas y otras operaciones más. Los logs permiten visualizar problemas que pongan en riesgo tu red y de esta forma puedes hacer ajustes necesarios a la seguridad [11].

3.6.1.- Entendiendo los logs

En el FortiGate hay tres diferentes tipos de logs: Logs de tráfico, logs de eventos y logs de seguridad, cada tipo de log es dividido en subtipos. En la Tabla 20, se muestran los tipos y subtipos de los logs.

Tabla 20. Tipos de logs FortiGate

Trafico	Evento	Seguridad
Forward	Control de Endpoint	Control de aplicación
Local	Alta disponibilidad	Antivirus
Sniffer	Sistema	DLP
	Usuario	Anti Spam
	Router	Filtro Web
	VPN	IPS
	WAD	Anomalías
	Inalámbrico	WAF

Los logs de “Tráfico”, está dividido en tres subtipos: forward, local y sniffer.

- Subtipo Forward: contiene información acerca del tráfico que el FortiGate podría aceptar o rechazar, todo dependiendo de las políticas que influyen en él.
- Subtipo Local: este subtipo contiene información que va para y desde la dirección IP de la administración del FortiGate, también incluyen información de consultas para el GUI y el FortiGuard.
- Subtipo Sniffer: contiene información relacionado a la captura de paquetes.

Los logs del tipo “Evento”, guardan información como es el de agregar o modificar configuraciones y actividades de los daemons. También cuenta con subtipos llamados, control de endpoint, alta disponibilidad, sistema, usuario, router, VPN y el inalámbrico [11].

- Subtipo control de endpoint: contiene información acerca del uso de la red de los usuarios finales.

- Subtipo alta disponibilidad: los logs de este subtipo aparecen cuando la alta disponibilidad es activada, tiene información de los cambios o configuraciones que sufre la alta disponibilidad.
- Subtipo sistema: contiene información relacionado a las operaciones, como las actualizaciones automáticas del FortiGuard e inicios de sesión del GUI.
- Subtipo usuario: cuenta con eventos de inicio y cierre de sesión para las políticas de firewall con autenticación de usuario.
- Subtipo router, VPN, WAN e inalámbrico: incluyen logs para estas características.

Y finalmente, los logs del tipo "Seguridad", guardan información para los eventos de seguridad, como los ataques de virus e intentos de intrusión. Su información del tipo de seguridad es de perfil type (log type = utm), incluyen el control de aplicación, antivirus, DLP, anti spam, filtro web, IPS, anomalías y el WAF. Estos logs de seguridad, y sus subtipos, son solo visibles en el menú del GUI, solamente si hay entradas de logs creadas, si no hay eventos de seguridad existentes, no aparecerán en el menú del GUI [11]. Hay distintos tipos de niveles de gravedad, las cuales se muestran en la Tabla 21.

Tabla 21. Niveles de Syslog

Niveles	Descripción
0 – Emergencia	Sistema inestable
1 – Alerta	Acción inmediata requerida
2 – Critico	Funcionalidad afectada
3 – Error	Error existente que pueda afectar la funcionalidad
4 – Advertencia	La funcionalidad puede ser afectada
5 – Notificación	Información acerca de eventos anormales
6 – Información	Información general del sistema

Cada entrada de log incluye un nivel de log o nivel de prioridad por rango en orden de importancia desde emergencia a información.

También hay un nivel de debug, que viene siendo el nivel más bajo y nos sirve esencialmente para información de diagnóstico. El nivel de debug es raramente usado, solo si se activa para alguna investigación del soporte técnico de Fortinet.

El FortiGate tiene la ventaja de seleccionar diferentes almacenamientos para los logs, puede ser localmente, ya que el FortiGate cuenta con su propia memoria en un disco duro. O de igual forma se puede almacenar remotamente, ya sea en servidores syslog, en SNMP o en los propios productos externos que Fortinet ofrece, los cuales son el FortiCloud, FortiAnalyzer y FortiManager [11].

La limitante de almacenar logs dentro del propio FortiGate, es que tiene un disco duro limitado, por lo que los logs más antiguos de 7 días, por defecto serán eliminados del disco duro. FortiGate da la opción de hacer backup de los logs, hasta en los USB (Para los FortiGate que cuentan con entrada USB) [11].

3.6.2.- FortiView

FortiView es un sistema comprensivo de monitoreo para la red que integra datos históricos en tiempo real en una única vista dentro del FortiGate. Con este sistema, el usuario puede ver logs y monitoreo de las amenazas en la red, filtrar datos en múltiples niveles, dar seguimiento de actividades administrativas, entre otras [11].

Atreves de varias páginas sobre el menú de FortiView, se puede investigar actividades del tráfico en la red, y desarrollar múltiples filtros más precisos para ver sobre un tiempo específico, para la vista de FortiView y los logs, al menos son requeridos 24 horas de almacenamiento [11]. Algunas de las áreas que se pueden monitorear en el Menú FortiView se muestran en la Figura 3-7.

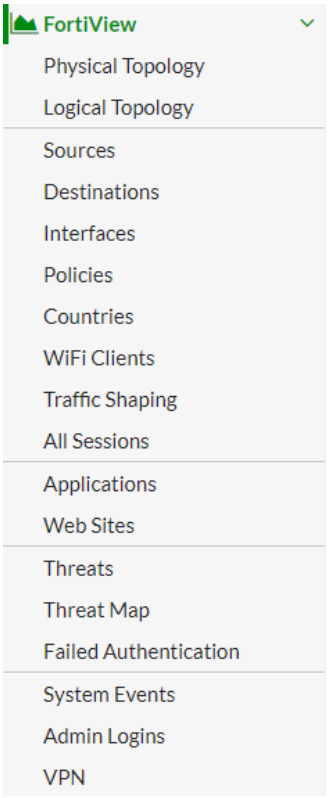


Figura 3-7. Menú FortiView

- Sources y destinations: permite ver información del tráfico de origen y destino dentro del FortiGate.
- Interfaces: permite realizar un monitoreo actual e histórico por interfaz, con la posibilidad de monitorear el ancho de banda.
- Countries: permite filtrar el tráfico de acuerdo al origen y destino de países que también incluye la opción de poder ver la visualización del mapa del país.
- Traffic Shaping: permite ver la información acerca del tráfico, incluye las sesiones, ancho de banda, bytes desechados y más.

- All sessions: permite ver información acerca de todo el tráfico del FortiGate. Esta consola tiene grandes números de opciones de filtro de columna.
- Applications: permite ver la información de las aplicaciones que están siendo usadas en la red.
- Cloud Applications: permite ver la información acerca de las aplicaciones basadas en la nube que están siendo usadas en la red.
- Web sites: permite ver la información acerca de las páginas más visitadas permitidas y bloqueadas por la categoría del FortiGuard o por dominio.
- Threats: permite ver información de los usuarios involucrados en incidentes con las mayores amenazas en la red.
- Threat Map: permite ver los riesgos que vienen desde varias localizaciones internacionales hacia la localización propia, es mostrado a través de un mapa.
- System Events: permite ver eventos de seguridad detectados por FortiGate e incluye niveles severos y números de instancias que fueron detectados.

3.6.3.- Monitoreo

Desde el menú Monitor, se puede monitorear varias funciones, como enrutamiento, DHCP, WAN link, Cuota de FortiGuard, IPsec, SSL VPN, usuarios de firewall, usuarios en cuarentena, FortiClient, Wifi y puntos de acceso [11].

Debido a que no es posible estar siempre dentro del dispositivo FortiGate, FortiGate da la opción de ajustar mensajes de alerta vía correo electrónico. Las alertas de correo electrónico proporcionan un efectivo método directo de notificación y eventos de administración. Antes de cualquier ajuste por correo electrónico, se debe tener un servidor SMTP establecido en el FortiGate, una vez configurado aparecerá un nuevo menú de alertas de email [11].

La base de datos del FortiGate que es usado para almacenar logs, es también usada para extraer información para los reportes. La base de datos de los logs usa Structure Query Language (SQL). Los reportes son construidos desde datasets, que son estados SQL que le dicen al FortiGate que información extraer desde la base de datos. El FortiGate incluye dos reportes por defecto: Learning report y Local report [11].

Los reportes del FortiOS son configurados desde el almacenamiento de logs en el disco duro del FortiGate. Para dicho reporte, es requerido activar el logging en la página Log Settings. También se debe habilitar los reportes locales en orden para ver y editar reportes como se muestra en la Figura 3-8.

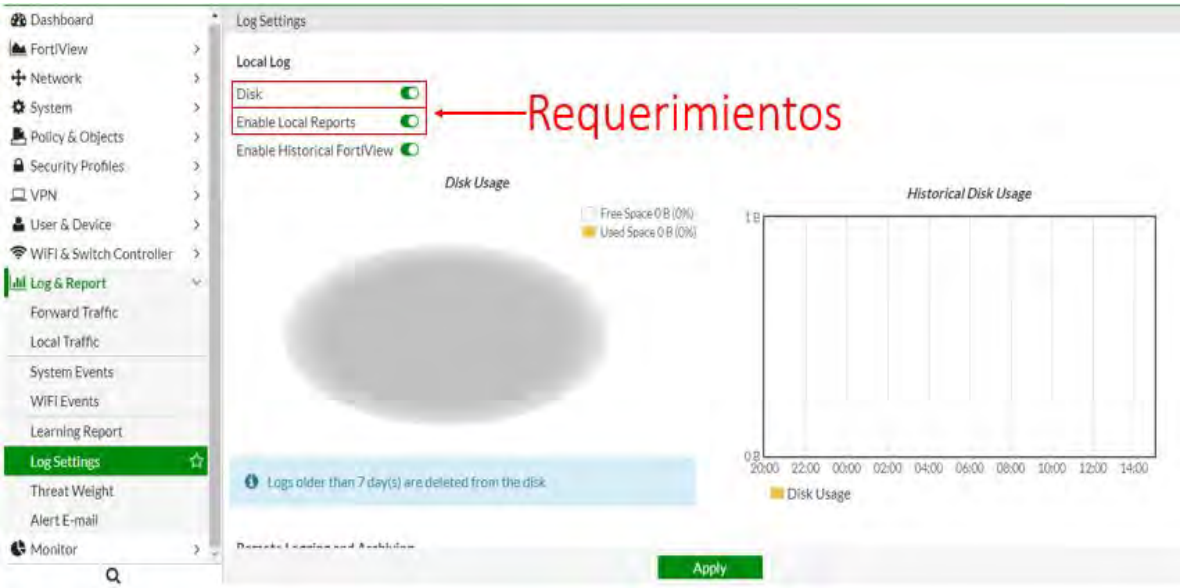


Figura 3-8. Ajustes de log

3.7.- Políticas de Firewall y su Autenticación

La seguridad de red es un tema bastante amplio, y una de las grandes habilidades que deben tener los equipos de seguridad y los administradores de red son las configuraciones de las políticas de firewall o listas de control de acceso (ACL). Una ACL es una lista secuencial de instrucciones “permit” (permitir) o “deny” (denegar) que se aplican a los protocolos de capa superior o a las direcciones. Las ACL son una herramienta potente para controlar el tráfico hacia y desde la red. Se pueden configurar ACL para todos los protocolos de red enrutada [7].

Ahora bien, hablando específicamente de equipos FortiGate, las políticas de Firewall definen cual tráfico hará coincidencia y lo que el FortiGate hará si no hay. Ahora bien, ¿el trafico debe ser permitido?, esto es la primera decisión basada en criterio simple como el origen, entonces, si la política misma no bloquea el tráfico, FortiGate comienza más inspección de perfil de seguridad computacionalmente costosa. Las políticas también pueden determinar si el NAT es aplicado o si la autenticación para la navegación es requerida, una vez que toda la configuración es terminada, el FortiGate reenvía los paquetes hacia su destino [11].

El FortiGate busca una coincidencia de las políticas de firewall desde el “top to bottom”, quiere decir que desde la parte de arriba desplazándose hacia abajo y, si la coincidencia es encontrada, el tráfico es basado en la política de firewall. Si no hay coincidencia de tráfico, finalmente el tráfico es desechado por que al final se encuentra una política implícita que deniega todo, como se muestra en la Figura 3-9.

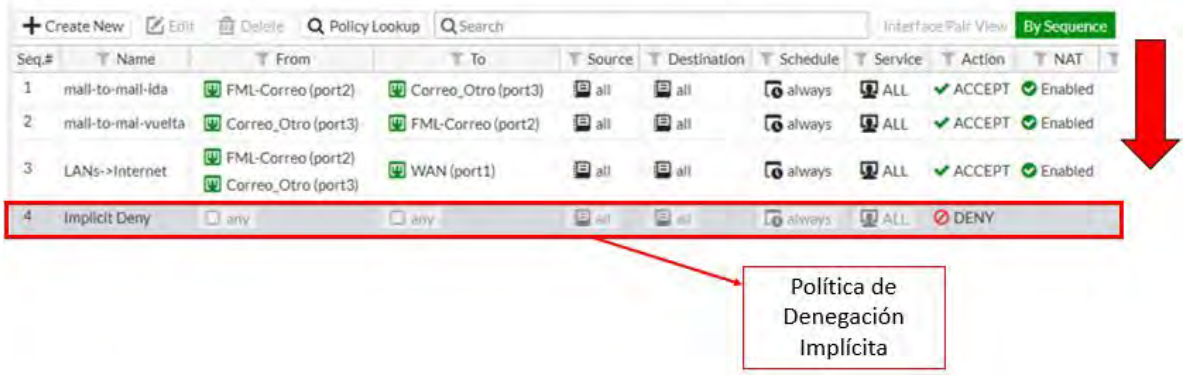


Figura 3-9. Secuencia de las políticas de firewall

Las políticas se determinan por criterio de coincidencia, que se definen usando los siguientes objetos:

- Ingreso o Egreso.
- Origen y destino: dirección IP, ID de dispositivo o usuario.
- Servicios de red: protocolo de IP y número de puerto.
- Horario: aplica durante los tiempos de configuración.
- Acción: aceptar o denegar.

Una vez que el FortiGate busca una coincidencia de política, se aplica los ajustes de la configuración por el paquete del procesamiento.

3.7.1.- Identificación del dispositivo

Hay dos técnicas de identificación de dispositivo: con un agente y sin uno.

El uso del tráfico del dispositivo sin agentes, los dispositivos son indexados por su dirección MAC lo cual FortiGate tiene varias maneras para identificar los dispositivos:

- HTTP “user-agent”: cabecera.
- Huella dactilar de TCP.
- Dirección MAC de identificador único de organización (OUI).
- DHCP.
- Microsoft Windows browser service (MWBS).
- Agente de usuario SIP.
- Link Layer Discovery Protocol (LLDP).
- Simple Service Discovery Protocol (SSDP).

El FortiGate usa el famoso “first come, first served” (primero en entrar, primero en salir), para determinar la identidad del dispositivo. Por ejemplo, si un dispositivo es detectado por un usuario de agente HTTP, FortiGate actualiza su tabla de dispositivos con la dirección de MAC detectada y el escaneo es detenido tan pronto como el tipo haya sido determinado por la dirección de MAC [11].

Basado en agente, es utilizado por el FortiClient. El FortiClient envía información al FortiGate, y el dispositivo es rastreado por una única User ID del FortiClient [11].

Los firewalls tradicionales, garantizan acceso a la red por autenticación de dirección de IP y dispositivo. Esto es inadecuado y puede poseer riesgos de seguridad, ya que el firewall no pueda determinar quién está usando el dispositivo al que otorga acceso. FortiGate incluye autenticación por usuario o grupo de usuarios y da como resultado, que pueda seguir al usuario en varios dispositivos. El acceso es controlado por usuario o grupo de usuarios, los usuarios, para ingresar deben autenticarse validando credenciales como un nombre de usuario y contraseña. Una vez que el FortiGate valida el usuario, FortiGate aplica políticas de firewall y perfiles para permitir o denegar el acceso a la red especifica [11].

El FortiGate incluye tres tipos de autenticación de Firewall:

- Autenticación por contraseña local: este método es el más simple y es almacenado localmente.
- Autenticación por contraseña basada en servidor, también llamado autenticación por contraseña remota: las cuentas son almacenadas en un servidor remoto, aunque el administrador puede crear un usuario localmente y especificar el servidor para la verificación de la contraseña.
- Autenticación por dos factores. Este método es habilitado cuando algún método de los antes ya mencionados fue activado, acompañado de un token o un certificado.

3.7.2.- Perfiles de seguridad

Una de las más importantes características que una política de firewall puede aplicar son los perfiles de seguridad, como un IPS y antivirus. Un perfil de seguridad inspecciona cada paquete que fluya en el tráfico, donde las sesiones hayan sido condicionalmente aceptadas por la política de firewall. En la política de firewall se deben habilitar dichos perfiles de seguridad, como se muestra en la Figura 3-10.

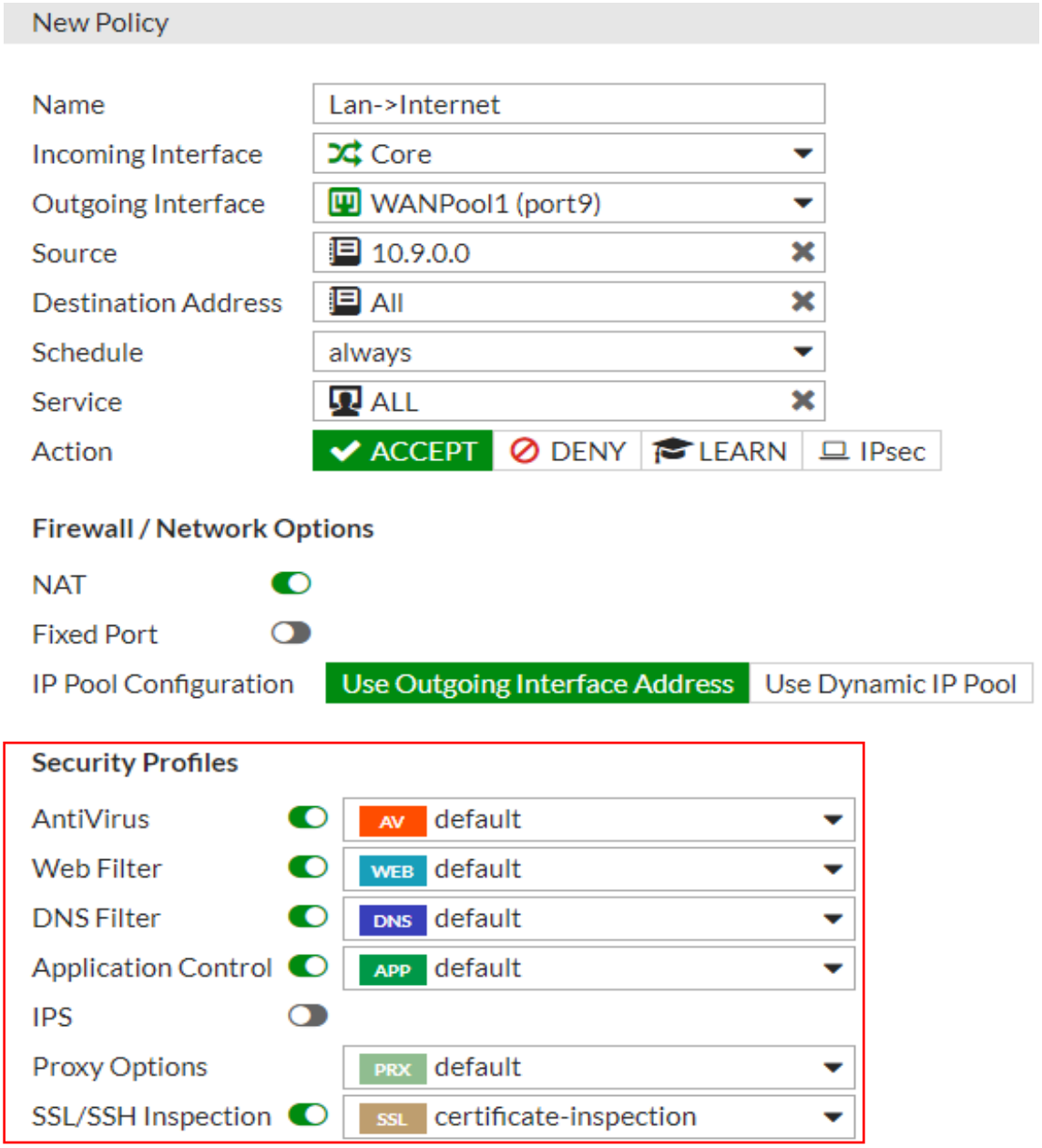


Figura 3-10. Perfiles de seguridad en la política de firewall

Cuando el tráfico es inspeccionado, FortiGate puede usar uno de dos métodos: flow-based o proxy-based. Las diferentes características de seguridad son compatibles con cada tipo.

También es posible habilitar el modo aprendizaje en la política de firewall. Cuando se establece la acción aprender (LEARN), la política de firewall automáticamente aplica perfiles estáticos por defecto y para el tráfico para a los perfiles de seguridad para monitoreo. También habilita los logs con capacidades completas, las cuales son etiquetadas como logs en aprendizaje [11].

Dentro de las políticas de firewall, se encuentra una sección llamada Traffic Shapers, el cual sirve para administrar el ancho de banda, útil para un control más granular del ancho de banda.

Hay dos tipos de traffic shaper que pueden ser configurados: compartido (shared) y por IP (per-IP).

Un shaper compartido aplica al total de ancho de banda para que todos compartan el tráfico configurado. El alcance puede ser por política o por todas las políticas que se encuentren referenciados al shaper. FortiGate puede contar el límite de los paquetes de ingreso y egreso al tráfico de la política [11].

El shaper por IP, como su nombre lo dice, otorga un ancho de banda por IP, la función del shaper puede ser configurado para la administración del ancho de banda por política de seguridad, por páginas web o por aplicaciones, como Youtube o Facebook.

En la Figura 3-11, se muestra un ejemplo de la función de cada uno.

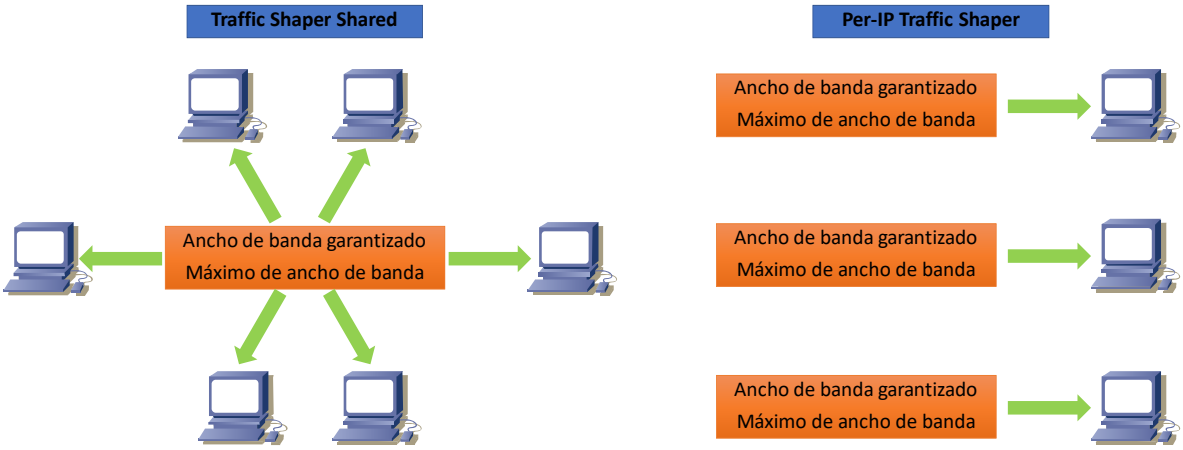


Figura 3-11. Ejemplo de Traffic Shaper

Cuando las políticas del traffic shaper son creadas, se debe asegurar que el criterio de coincidencia es el mismo que las políticas de firewall donde se quiere aplicar este shaper. Este shaper se puede aplicar de igual forma a los protocolos TCP y UDP [11].

3.8.- VPN

Las tecnologías de red privada virtual (VPN) proporcionan un medio para realizar estas eficiencias empresariales junto con gastos operacionales de TI muy reducidos. Se discutirá cómo las tecnologías VPN actuales permiten que las fuerzas laborales compartan datos de manera transparente y segura a través de infraestructuras de red comunes pero mantenidas por separado.

En el entorno informático distribuido de hoy, la red privada virtual (VPN) ofrece una solución atractiva para los administradores de red. En esencia, una VPN consiste en un conjunto de computadoras que interconectan por medio de una red relativamente insegura y que utilizan cifrado y protocolos especiales para

brindar seguridad. En cada sitio corporativo, las estaciones de trabajo, los servidores y las bases de datos están conectados por una o más redes de área local (LAN). Las LAN están bajo el control del administrador de red y pueden configurarse y ajustarse para un rendimiento rentable. Internet o alguna otra red pública puede usarse para interconectar sitios, proporcionando un ahorro de costos sobre el uso de una red privada y descargando la tarea de administración de red de área amplia al proveedor de red pública. Esa misma red pública proporciona una ruta de acceso para que los teletrabajadores y otros empleados móviles inicien sesión en sistemas corporativos desde sitios remotos [12].

Pero el administrador de red enfrenta un requisito fundamental: seguridad. El uso de una red pública expone el tráfico corporativo a escuchas ilegales y proporciona un punto de entrada para usuarios no autorizados. Para contrarrestar este problema, el administrador puede elegir entre una variedad de paquetes y productos de cifrado y autenticación. Las soluciones propietarias plantean una serie de problemas. Primero, ¿qué tan segura es la solución? Si se usan esquemas de encriptación o autenticación patentados, puede haber poca seguridad en la literatura técnica en cuanto al nivel de seguridad proporcionado. El segundo es la cuestión de la compatibilidad. Ningún gerente quiere estar limitado en la elección de estaciones de trabajo, servidores, enrutadores, cortafuegos, etc. por la necesidad de compatibilidad con la instalación de seguridad. Esta es la motivación para el conjunto de estándares de Internet de seguridad IP también llamado IPSec [12].

3.8.1.- VPN IPSec

En 1994, el Internet Architecture Board (IAB) publicó un informe titulado "Seguridad en la arquitectura de Internet" (RFC 1636). El informe establecía el consenso general de que Internet necesita más y mejor seguridad e identificó áreas clave para los mecanismos de seguridad. Entre ellos se encontraba la necesidad de asegurar la infraestructura de red contra el monitoreo y control no autorizado del tráfico de la red y la necesidad de asegurar el tráfico del usuario final utilizando mecanismos de autenticación y cifrado [12].

Para proporcionar seguridad, el IAB incluyó la autenticación y el cifrado como características de seguridad necesarias en la IP de próxima generación, que se ha emitido como IPv6. Afortunadamente, estas capacidades de seguridad fueron diseñadas para ser utilizables tanto con el IPv4 actual como con el IPv6 futuro. Esto significa que los proveedores pueden comenzar a ofrecer estas características ahora, y muchos proveedores tienen alguna capacidad IPSec en sus productos hoy en día. La especificación IPSec existe como un conjunto de estándares de Internet [12].

El protocolo de seguridad IP, más comúnmente conocido como IPsec, proporciona seguridad en la capa de red. IPsec protege datagramas IP entre dos entidades de capa de red, incluidos hosts y routers. Muchas instituciones (corporaciones, sucursales gubernamentales, organizaciones sin fines de lucro, etc.) usan IPsec para crear redes privadas virtuales (VPN) que se ejecutan en Internet público [13].

Con la confidencialidad de la capa de red entre un par de entidades de red (por ejemplo, entre dos routers, entre dos hosts, o entre un router y un host), la entidad emisora encripta las cargas útiles (payload) de todos los datagramas que envía a la entidad receptora. La carga útil encriptada podría ser un segmento TCP, un segmento UDP, un mensaje ICMP, etc. Si dicho servicio de capa de red estuviera en su lugar, todos los datos enviados de una entidad a la otra, incluido el correo electrónico, páginas web, mensajes de protocolo de enlace TCP y mensajes de gestión (como ICMP y SNMP), quedarían ocultos de cualquier tercero, parte que podría estar analizando la red. Por esta razón, se dice que la seguridad de la capa de red proporciona "cobertura global" [13].

Además de la confidencialidad, un protocolo de seguridad de capa de red podría proporcionar otros servicios de seguridad. Por ejemplo, podría proporcionar autenticación de origen, de modo que la entidad receptora pueda verificar la fuente del datagrama protegido. Un protocolo de seguridad de capa de red podría proporcionar integridad de datos, de modo que la entidad receptora pueda verificar cualquier alteración del datagrama que pueda haberse producido mientras el datagrama estaba en tránsito. Un servicio de seguridad de capa de red también podría proporcionar prevención de ataques de repetición, lo que significa que cualquiera podría detectar cualquier datagrama duplicado que un atacante pueda insertar. IPsec proporciona mecanismos para todos estos servicios de seguridad, es decir, para la confidencialidad, la autenticación de origen, la integridad de los datos y la prevención de ataques repetitivos [13].

En teoría, IPSec no soporta encriptación nula, quiere decir, que se puede hacer que las VPN’s no encripten el tráfico. IPSec también soporta integridad de datos nulo. Pero, ¿eso proporciona ventajas sobre el tráfico plano? No. Nadie puede confiar en el tráfico que pudo haber tenido un ataque inyectado por un atacante. Raramente la gente quiere enviar datos a una persona desconocida. La mayoría de la gente quiere una red de datos privada para proporcionar datos personales, como una transacción de tarjeta de crédito, registros médicos o permanecer su situación privadamente [11]. En la Figura 3-12, se muestra un ejemplo de los beneficios de una VPN IPSec.

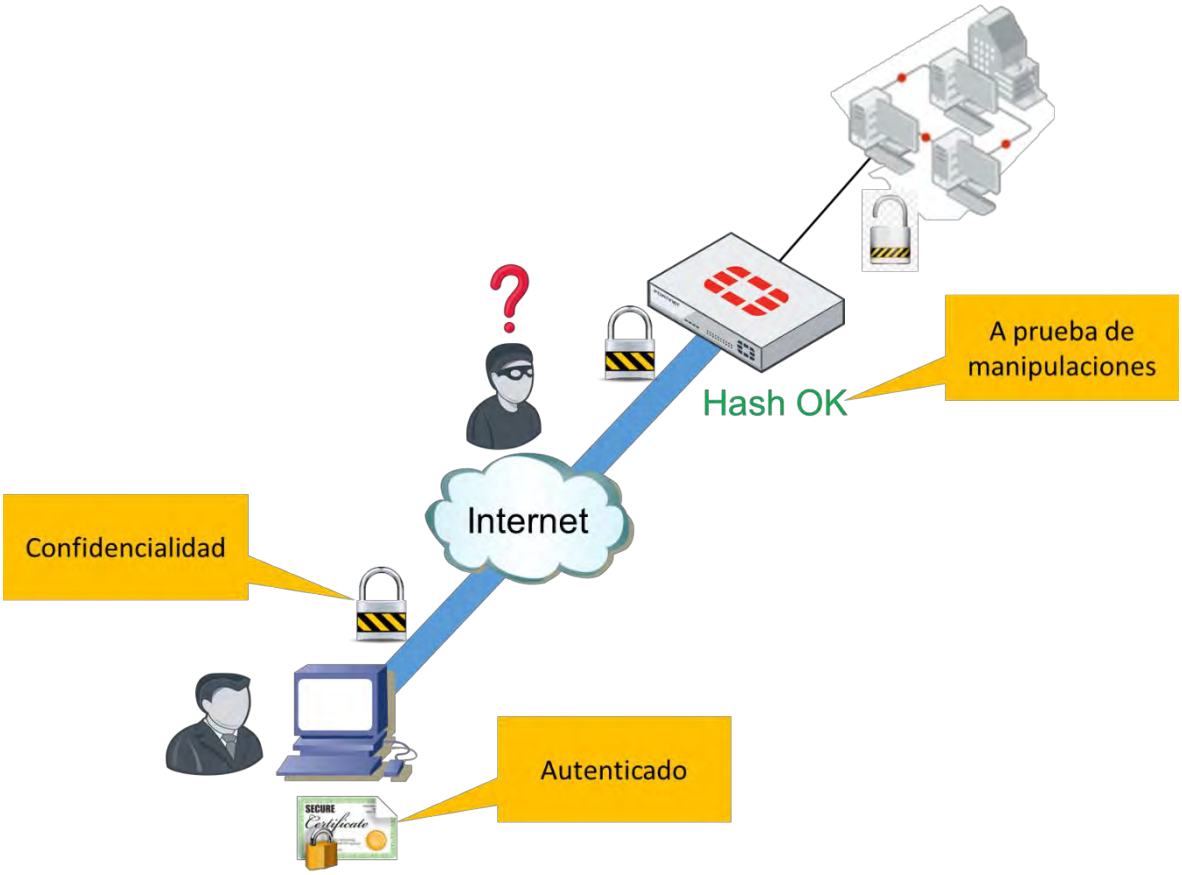


Figura 3-12. Ejemplo de VPN

Así que, en realidad, independientemente del fabricante, las VPN's IPSec casi siempre tienen configuraciones con tres beneficios importantes:

- Autenticación, para verificar la identidad de ambos usuarios finales.
- Integridad de datos, o HMAC, que provee la encapsulación de datos que no ha sido alterado el cual atraviesa una red potencialmente hostil.
- Confidencialidad, o encriptación, el cual asegura que solamente la información pueda ser leído por el destinatario.

3.8.2.- ¿Cómo trabaja el protocolo IPsec?

Si se tiene establecido la VPN entre firewalls, se debe tener en cuenta que protocolos permitir. El protocolo de IPSec otorga servicios a la capa de red. Durante el túnel de establecimiento, ambos dispositivos finales negocian la encriptación y el algoritmo de autenticación a usar. Después que el túnel haya sido negociado y este arriba, la encriptación de datos y la encapsulación ingresan dentro de paquetes ESP [11].

Actualmente, múltiples protocolos trabajan juntos, para hacer posible el IPsec, por ejemplo, el AH (Authentication Header) otorga integridad, pero no encriptación, así que, aunque esté definido en el RFC, FortiGate no lo utiliza.

Cuando una entidad fuente IPsec (generalmente un host o un router) envía datagramas seguros a una entidad de destino (también un host o un router), lo hace con el protocolo AH o el protocolo ESP. El protocolo AH proporciona autenticación de fuente e integridad de datos, pero no brinda confidencialidad. El protocolo ESP proporciona autenticación de fuente, integridad de datos y confidencialidad. Debido a que la confidencialidad es a menudo crítica para las VPN y otras aplicaciones IPsec, el protocolo ESP es mucho más utilizado que el protocolo AH [13].

Ralamente el protocolo IPsec es una serie de protocolos separados, la cual incluye:

- Internet Key Exchange (IKE): IKE es usado para autenticar, intercambiar llaves y negociar la encriptación y verificación de datos que serán usadas, esencialmente, es el control del canal.
- Authentication Header (AH): AH contiene la cabecera de autenticación, viene siendo la suma de verificación (Checksum) que comprueba la integridad de datos.
- Encapsulation Security Payload (ESP): ESP es la encapsulación segura de la carga útil, el payload encriptado, esencialmente, viene siendo el canal de datos.

En la Tabla 22, se muestra los números de puertos, encapsulación y las variables dependiendo si hay o no hay NAT:

Tabla 22. Puertos del protocolo IKE y ESP

Protocolo	NAT	No NAT
IKE RFC 2409 (IKEv1) RFC 4306 (IKEv2)	Protocolo IP 17: Puerto UDP 500 (UDP 4500 para la llave y el quick mode)	Protocolo IP 17: Puerto UDP 500
ESP RFC 4303	Protocolo IP 17: Puerto UDP 4500	Protocolo IP 50

Así que, si es necesario pasar tráfico a través de firewalls, permitir solamente el protocolo o número de puerto, usualmente con eso es suficiente.

Como se mencionaba anteriormente, el RFC indica que el IPsec utiliza AH, sin embargo, AH no ofrece encriptación, un beneficio importante, por lo que no es utilizado por FortiGate, como resultado, no es necesario permitir el protocolo IP 51.

IPsec puede operar en dos modos: modo de transporte o modo túnel.

El encabezado IP original no está protegido y no se agrega un encabezado IP adicional [11].

El modo túnel es un túnel confiable. El conjunto de paquetes IP es encapsulado y una nueva cabecera IP es agregada en el inicio. Una vez que los paquetes de

IPsec alcanzan la red LAN remota, y es desenvuelto, el paquete original puede continuar en su camino [11]. En la Figura 3-13, se muestra la encapsulación de los túneles antes mencionados.

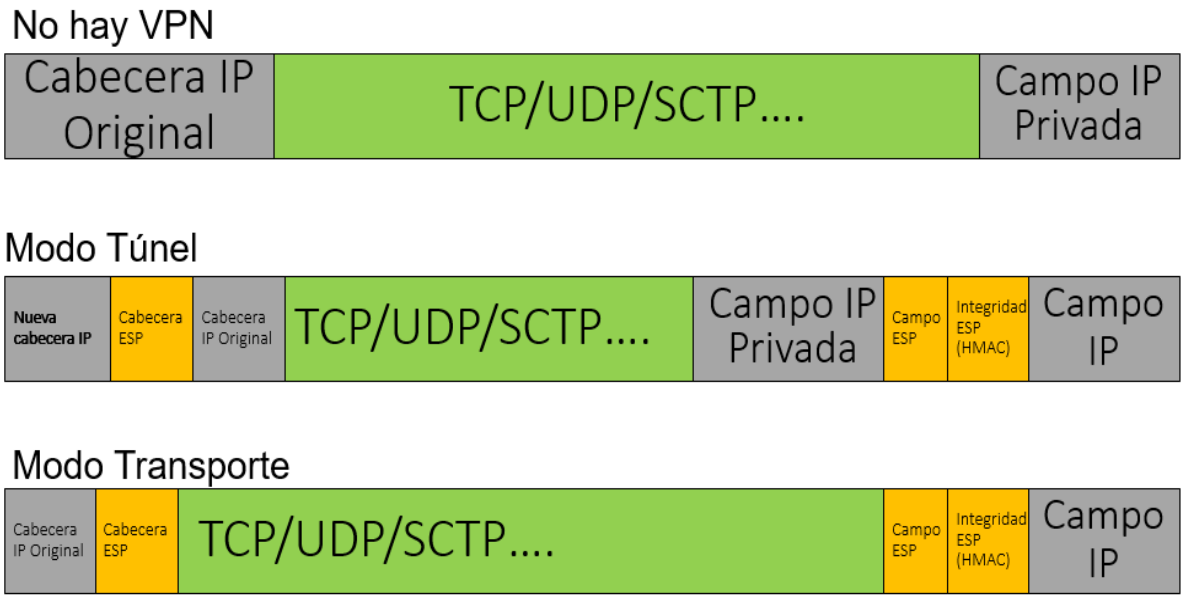


Figura 3-13. Encapsulación

Para crear un túnel IPsec en orden, ambos dispositivos deben establecer sus asociaciones de seguridad (SAs) y llaves secretas, las cuales son otorgadas por el protocolo IKE. El protocolo IKE permite a las partes involucradas en una transacción para establecer sus asociaciones de seguridad (SAs) [11].

Un SA es un simple paquete de algoritmos y parámetros siendo usados para encriptar y autentificar los datos que viajan a través del túnel. En el tráfico bidireccional, este intercambio es asegurado por el par de SAs. Una para cada dirección de tráfico. Esencialmente, ambos sitios de túnel deben ser acordados en las reglas de seguridad. Si ambos sitios no pueden ser acordados en las reglas para enviar datos y la verificar la identidad de cada uno, entonces el túnel no será establecido [11].

IKE usa dos fases distintas: Fase 1 y fase 2. La fase 1 es cuando cada dispositivo final del túnel no es seguro aún. Un atacante en el medio puede interceptar las llaves sin encriptar. Ningún dispositivo de un lado, tiene la garantía de la identidad del otro, por lo tanto, ellos no podrán intercambiar las llaves privadas, para resolver este problema, primero, ambos dispositivos finales tienen que crear un canal temporal seguro. Ellos usaran este canal para protegerse con una autenticación fuerte y una negociación de llaves para un túnel posterior [11].

La fase 1 es donde los dispositivos se saludan y crean un SA que define un canal seguro temporal. El SA es llamado el IKE SA y es bidireccional. Los ajustes de cada dispositivo final deben ser acordados, de otra manera, la fase 1 fallará, en este momento, cada sitio no puede ser posible el encriptar o autenticar el tráfico

desde el otro. Al final de la fase 1, la negociación IKE SA es usada para negociar las llaves del Diffie-Hellman que serán usadas en la fase 2 [11].

Diffie y Hellman [Diffie 1976] demostraron un algoritmo (conocido ahora como Diffie-Hellman Key Exchange) para hacer justamente eso: un enfoque radicalmente diferente y maravillosamente elegante hacia la comunicación segura que ha llevado al desarrollo de los sistemas criptográficos de clave pública de hoy en día. Los sistemas de criptografía de clave pública también tienen varias propiedades maravillosas que los hacen útiles no solo para el cifrado, sino también para la autenticación y las firmas digitales. Curiosamente, recientemente ha salido a la luz que ideas similares a las de [Diffie 1976] y [RSA 1978] se desarrollaron independientemente a principios de la década de 1970 en una serie de informes secretos de investigadores del Communications-Electronics Security Group en el Reino Unido. [Ellis 1987]. Como suele ser el caso, las grandes ideas pueden surgir independientemente en muchos lugares; Afortunadamente, los avances de clave pública tuvieron lugar no solo en privado, sino también en la vista pública [13].

Diffie-Hellman usa la llave publica que ambos dispositivos finales conocen más un factor matemático llamado nonce (marcas aleatorias) para generar una clave privada común. Un nonce es un número que un protocolo usará solo una vez en la vida. Es decir, una vez que un protocolo usa un nonce, nunca volverá a usar ese número [13].

Esto es crucial, con Diffie-Hellman, incluso si un atacante puede escuchar los mensajes que contienen la llave publica, ellos no pueden determinar la llave secreta. La nueva llave secreta es usada para calcular llaves adicionales para encriptación simétrica y autenticación [11].

Cada FortiGate usa una llave secreta compartida más una marca aleatoria para calcular las llaves para:

- Encriptación de algoritmos simétricos (como 3DES, AES)
- Autenticación simétrica (HMACs)

El protocolo ESP usualmente tiene problemas al cruzar con dispositivos que están haciendo NAT. Una de las razones es que el protocolo ESP no tiene número de puestos, como TCP y UDP hechos, para diferenciar el tráfico desde un túnel a otro. Para resolver este problema, nos encontramos con el NAT Transversal (NAT-T) que fue agregado para especificaciones de IPsec. Cuando el NAT-T está habilitado en ambos dispositivos finales, los pares pueden detectar cualquier dispositivo NAT a lo largo del camino. Si es NAT es encontrado, entonces ambas fases 2 y el resto de los paquetes de la fase 1 cambiarán al puerto UDP 4500, además, ambos dispositivos finales se encapsularán ESP dentro del puerto UDP 4500 [11].

Esto es recomendado cuando se tienen dos FortiGate que se encuentran detrás del NAT, por ejemplo, un modem de un proveedor de servicio que tiene NAT, probablemente será necesario habilitar este ajuste, cuando el NAT-T es

establecido para forzarlo, el puerto 4500 siempre será usado, incluso cuando no hay un dispositivo NAT a lo largo de la trayectoria. En la Figura 3-14, se muestra un ejemplo de la configuración de la fase 1 en FortiGate.

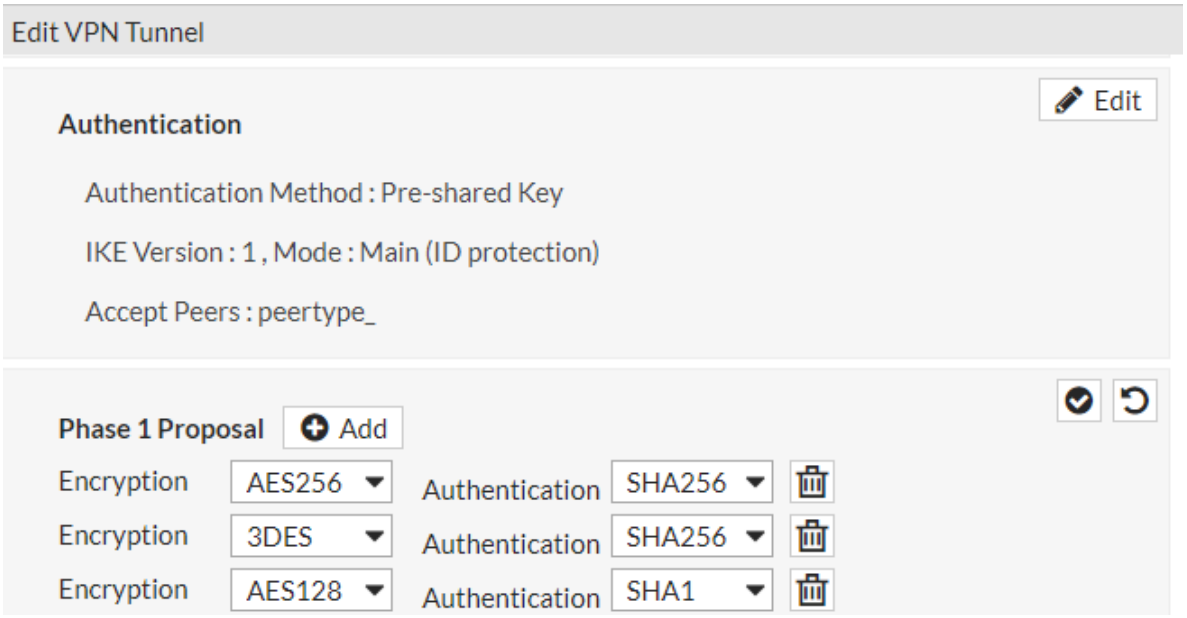


Figura 3-14. Configuración de VPN fase 1

Una vez que la fase 1 este establecida en un canal seguro con las llaves privadas, la fase 2 inicia.

La fase 2 negocia los parámetros seguros para dos IPsec SAs (No hay que confundirse con la IKE SA). Los SAs son la fase 2 el cual el protocolo ESP usa para transmitir datos entre las LANs. El protocolo IKE de la fase 2 no termina una vez que inicia el protocolo ESP. La fase 2 periódicamente vuelve a negociar la criptografía, esto mantiene la seguridad. FortiGate usará Diffie-Hellman para volver a recalcular la nueva llave secreta, la cual no estará derivado de viejas llaves, haciendo esto mucho más difícil para un atacante a corromper el túnel [11].

Durante la fase 2, se debe configurar un par de ajustes llamados quick mode selectors, las cuales identifican el tráfico directo apropiado en la fase 2, en otras palabras, permite un ajuste más granular del SAs. Los selectores se comportan similar a una política de firewall. El trafico VPN debe tener coincidencia con los selectores en la fase 2 del SA, si no se encuentra una coincidencia, el tráfico es desechado [11]. En la Figura 3-15, muestra un ejemplo de la configuración de la fase 2 en FortiGate.

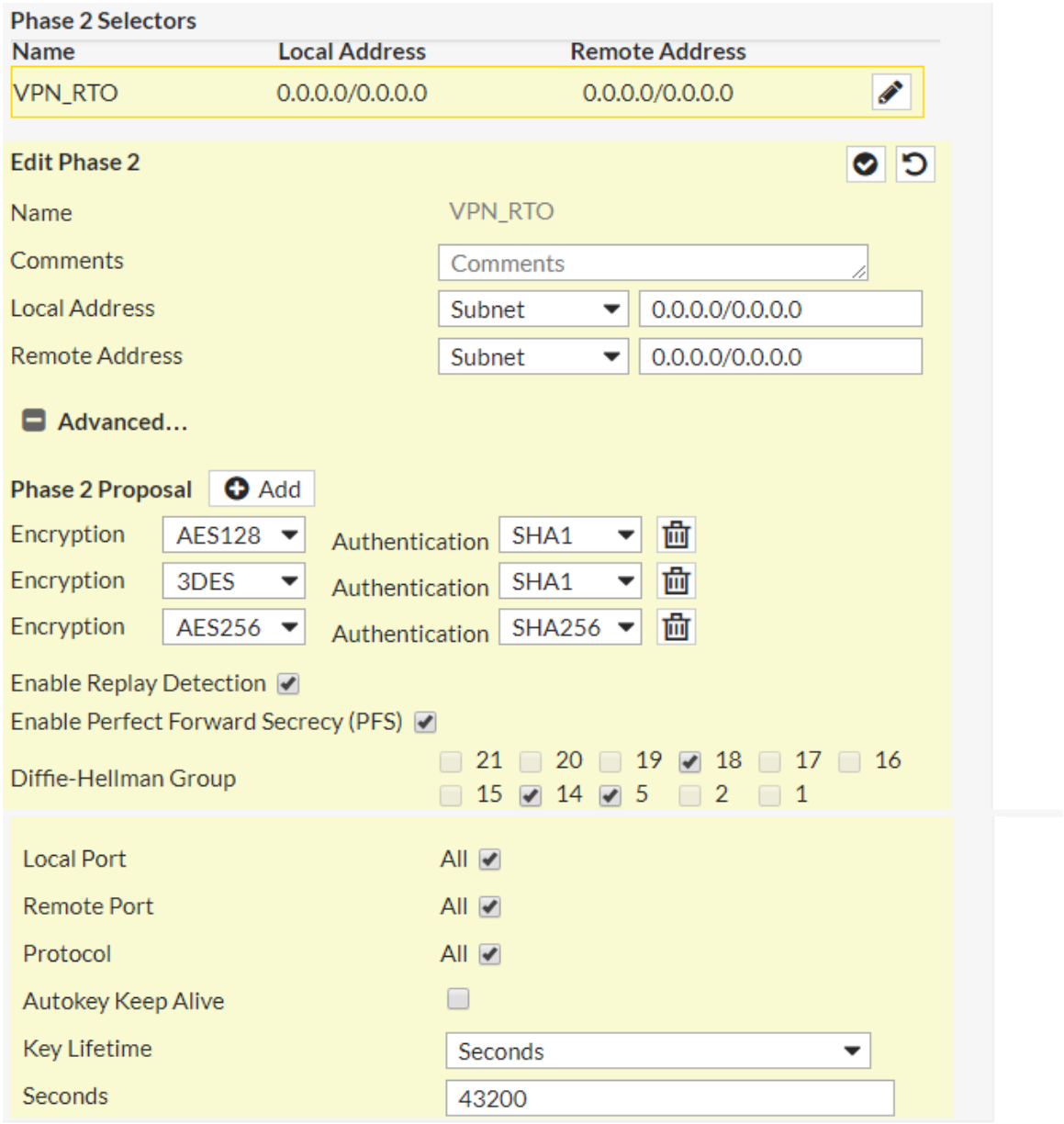


Figura 3-15. Configuración de VPN fase 2

Una vez que la fase 1 está completa, la fase 2 inicia, la cual establece un túnel ESP que será usada para la transferencia de datos actual. Para cada subred en cada dispositivo final de la VPN, se puede especificar niveles diferentes de seguridad ESP. Por ejemplo, las conexiones de una oficina remota que maneje transacciones, podría necesitar grandes tamaños de llaves y una muy fuerte autenticación, para hacer esto, es necesario configurar múltiples entradas de fase 2. Para simplificarlo, en la Figura 3-15, se muestra solamente una fase 2, la dirección local de la LAN (Local Address), y la dirección remota de la LAN (Remote Address).

3.9.- Antivirus

El software malicioso ha y sigue evolucionando día tras día, aunque no todo software no deseado se comporta como un virus. El malware esta categorizado como un software que tiene efectos perjudícales, como el de acceder a un sistema, reunir información sensible, corromper el sistema o destruir datos.

Los virus, tienen código instalado para auto replicarse e instalarse en otros programas, incluso el de adjuntarse a un archivo ejecutable (.exe). No requiere el consentimiento de un usuario o simplemente engañan a los usuarios para que otorguen su permiso. Los virus infectan y se propagan por sí mismo.

Los grayware son aplicaciones no deseadas que no son clasificadas como virus pero que pueden ser molestos y podrían causar riesgos de seguridad. Pueden requerir algún tipo de interacción con el usuario. Convence al usuario que el beneficio de la instalación supera el costo, como una barra en el navegador que también encamina al usuario para instalar ads en páginas web.

3.9.1.- ¿Qué es y cómo trabaja?

Un antivirus, es una base de datos de las firmas de virus que identifican las infecciones de dichos virus. Durante un escaneo de un antivirus, para ser detectado como virus, el virus debe coincidir con un patrón definido llamado signature. Diferentes vendedores o proveedores tienen diferentes nombres para el mismo virus, algunos vendedores usan patrones que detectan un virus para cada patrón, mientras otros usan patrones que son más flexibles y pueden atrapar múltiples virus con un único patrón. El patrón que es usado depende del motor del proveedor [11].

¿Cuál estándar es la designación del vector del ataque?, se encuentra en el principio del nombre, por ejemplo, si el vector es W32, esto representar el Windows de 32-bit, el W64 representa el Windows de 64-bit, y el JS representa el JavaScript. En el nivel de host, un host basado en el software de antivirus como un FortiClient puede ayudar, pero el host basado en antivirus, no puede ser instalado en routers, otro claro ejemplo seria la red de invitados o el ISP de los clientes, también podrían no tener software de antivirus instalado, así que, ¿Cómo se pueden proteger de esto en la red donde hay un riesgo grande de amenazas de virus? [11].

Los virus tienen muchas maneras de evitar la detección, FortiGate tiene muchas técnicas que puede usar para detectarlas, las cuales incluyen:

- Escaneo de Antivirus: el primero, el más rápido, la manera más simple para detectar malware es si el motor de FortiGate encuentra alguna coincidencia para una firma en la base de datos del antivirus.
- Grayware: aunque no es técnicamente un virus, a menudo es un paquete con un software inocuo (que no hace daño físico ni moralmente), pero tiene efectos secundarios no deseados, así que se podría catalogar como malware. Casi siempre, el grayware puede ser detectado como virus.

- Heurística: son basados en probabilidad, así que son subidos a la posibilidad de marcar falsos positivos, pero ellos también pueden ser marcados como virus del día cero, virus que son nuevos y desconocidos, por lo tanto, no hay firmas existentes aún. Si la red es frecuentemente un blanco, habilitar la parte de heurísticas, puede valer la pena el costo de rendimiento porque puede ayudar a detectar virus antes de iniciar una epidemia dentro de la red. Por defecto, cuando el motor de escaneo del antivirus detecta un virus con características heurísticas, se mostrará un log del archivo sospechoso, pero no lo bloqueará. Se puede escoger si bloquearlo o no.

El FortiGate tiene la capacidad de actualizar su base de datos de antivirus ya sea por horarios o en el momento que uno quiera. La actualización por horarios te permite configurar por intervalos, como un horario, un día o por semana. Es posible también habilitar las actualizaciones push, el cual te permite agregar nuevas definiciones tan pronto como sean liberados por el FortiGuard. Esto es útil para ambientes de alta seguridad, el FortiGate recibirá urgentemente actualizaciones de seguridad tan pronto como también sean liberadas [11].

Múltiples bases de datos de antivirus del FortiGuard existen y pueden ser configuradas en los ajustes del antivirus del FortiGate. Todos los equipos FortiGate tienen la base de datos normal, el cual solo contiene firmas para la detección de virus en meses recientes detectadas por el equipo de seguridad global de FortiGuard, esto es una base de datos pequeña y, sin embargo, resulta bastante rápido el escaneo, pero no detecta la base de datos de todos los virus conocidos [11].

Algunos modelos soportan la base de datos extendida, el cual detecta virus que no han sido activadas hace bastante tiempo. Las plataformas vulnerables son todavía comunes, y/o estos virus pueden ser un problema después. Incluyen la base de datos normal más los virus recientes no activos [11].

La base de datos extremo es destinada para ambientes de alta seguridad el cual detecta todos los virus conocidos, incluyendo para sistemas operativos heredados que ya no se usan ampliamente. Incluyen la base de datos extendida más los antiguos virus inactivos [11].

Si es necesario el acertar más un programa heurístico, ser más sofisticado, más acertado para detectar malware o buscar virus más a fondo de ataques de día cero, es posible la integración de FortiSandbox con el antivirus.

FortiSandbox ejecuta un archivo con un ambiente protegido, y luego examina los efectos del software para ver si es dañino, por ejemplo, digamos que tenemos dos archivos, ambos alteran el registro del sistema y, por lo tanto, son sospechosos, uno es un driver de instalación (tiene un comportamiento normal), pero el segundo instala un virus que conecta a un comando de botnet y un servidor de control. El Sandbox podría revelar la diferencia, y puede ser configurado para recibir firmas suplementarias de la base de datos de Sandbox [11].

3.9.2.- Modos de inspección del FortiGate

El FortiGate incluye dos modos de inspección: Flow-based y proxy-based. El modo de inspección se determina como FortiGate va a escanear el tráfico para las diferentes características de los perfiles de seguridad.

El escaneo de proxy-based típicamente se refiere al proxy transparente, es llamado transparente porque la capa de red, FortiGate no es la dirección destino, aun así, FortiGate intercepta el tráfico de cualquier modo. En las conexiones TCP, el proxy de FortiGate genera el SYN-ACK para el cliente y completa el saludo de tres vías con el cliente antes de crear una segunda nueva conexión para el servidor, en la Figura 3-16, vemos un ejemplo de como el FortiGate interactúa con las conexiones TCP aplicando un escaneo proxy-based [11].

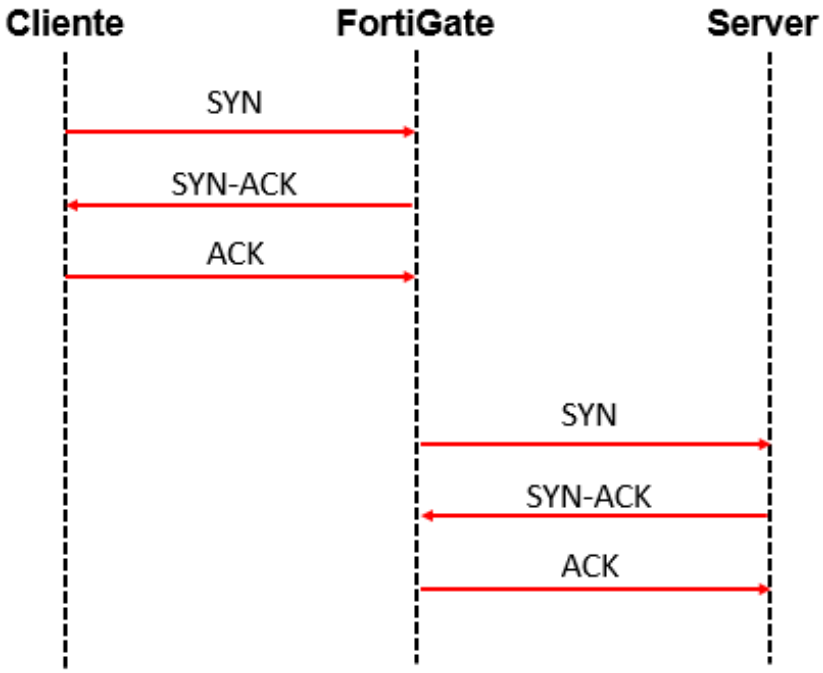


Figura 3-16. Conexión TCP en un tipo de escaneo proxy-based

El escaneo proxy-based hace una inspección más completa, pero agrega retardo, asimismo utiliza dos conexiones TCP, desde el cliente al FortiGate actuando como servidor proxy y desde el FortiGate al servidor, como se muestra en la Figura 3-16, además que la comunicación termina en la capa de transporte (capa 4).

Cada protocolo proxy recoge una conexión y almacena en buffer el archivo entero (o espera hasta el límite del tamaño alcanzado) antes de escanear. El cliente debe esperar a que el escaneo este completo, si el virus es detectado, una página de bloqueo será remplazado y mostrado inmediatamente. Como FortiGate tiene que almacenar todo el archivo para después hacer el escaneo, esto toma bastante tiempo. También desde el punto de vista del cliente, tiene que esperar para que el escaneo termine y poder terminar la conexión debido falta de datos. Es posible configurar el FortiGate para que pueda trasmitir desde

el proxy lentamente algunos datos hasta que pueda completar el buffer y terminar el escaneo, esto previene una conexión o sesión de tiempo muerto (timeout). En caso de que un virus sea detectado, no aparecerá un mensaje de bloqueo en el primer intento, hasta que el FortiGate termine de transmitir todos los paquetes al cliente final [11].

En la Figura 3-17, vemos cómo funciona el escaneo proxy-based cuando un cliente envía una solicitud al FortiGate.

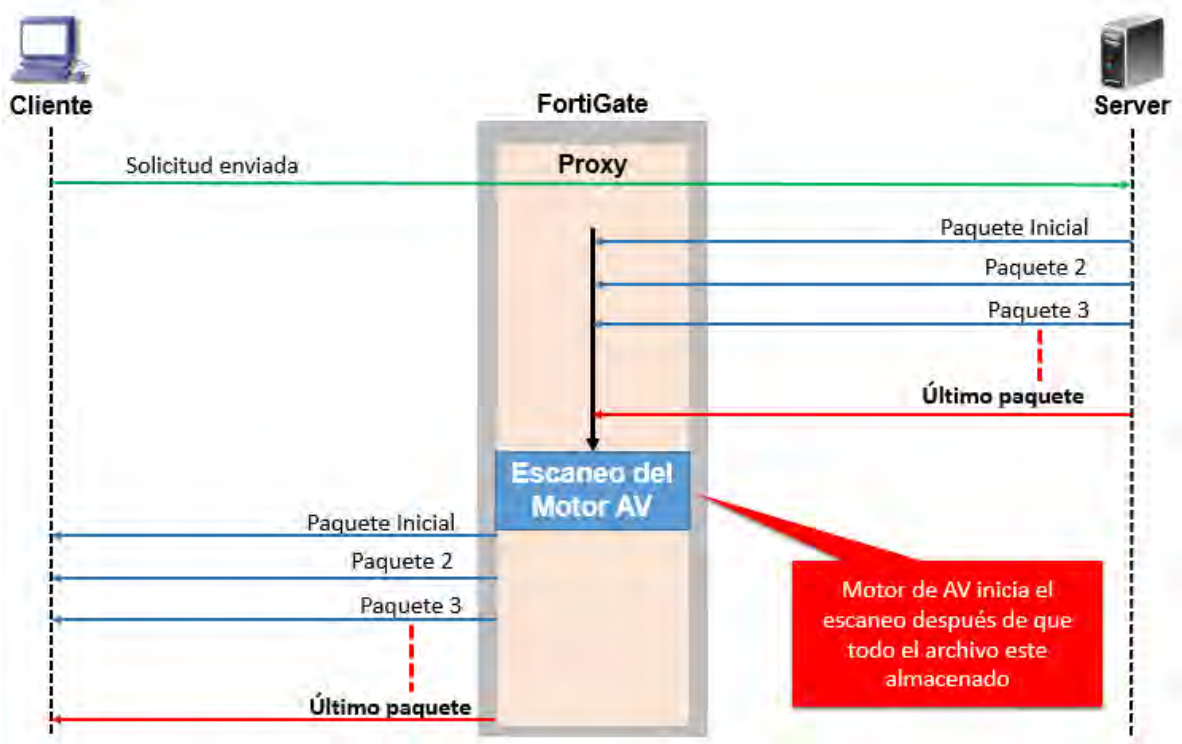


Figura 3-17. Escaneo proxy-based

Con el escaneo de proxy-based, el cliente envía una solicitud y el FortiGate inicia el almacenamiento después de que el archivo se almacena, entonces lo envía al motor de AV para el escaneo. Si el archivo está limpio de virus, FortiGate inicia a transmitir el archivo para el cliente final, en cambio, si el virus es encontrado, los paquetes no serán entregados para el cliente final y el proxy enviara un mensaje remplazando al archivo para el cliente final.

El escaneo flow-based no es un proxy, la función de FortiGate en este tipo de escaneo es de analizar los paraqués y reenviarlos como son recibidos. Originalmente el tráfico no es alterado, por lo tanto, las características avanzadas que modifican el contenido, como la aplicación de búsqueda segura, no es soportado [11]. En la Figura 3-18, se ve cómo trabaja las conexiones TCP en un tipo de escaneo flow-based.

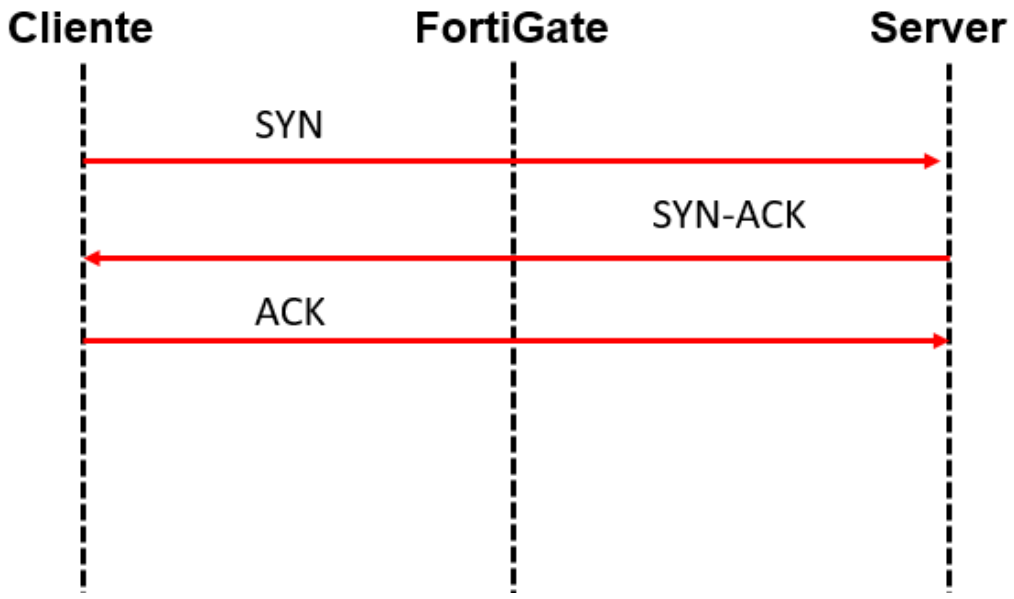


Figura 3-18. Conexión TCP en un tipo de escaneo flow-based

El escaneo flow-based es un escaneo muy rápido, comparado con el proxy-based, el archivo se escanea en una base de flujo TCP a medida que pasa a través de FortiGate.

El modo de análisis antivirus completo flow-based usa la base de datos de antivirus completo y el motor IPS examina el tráfico de la red. Como el archivo es transmitido simultáneamente, el escaneo de flow-based consume más ciclos de CPU, pero, dependiendo el modelo, algunas operaciones de flow-based pueden ser realizados por un chip especializado como el FortiASIC, el cual mejora aún más el rendimiento. El escaneo flow-based almacena una copia de paquetes localmente en el FortiGate y también reenvía el paquete al cliente final al mismo tiempo. Una vez que el paquete es recibido, FortiGate también lo almacena, pero pone el paquete en espera, de esta forma tiene todo el archivo para escanear. El motor IPS checa alguna coincidencia de reglas, entonces envía al motor AV para el escaneo [11].

Hay dos posibles escenarios cuando un virus es detectado:

- Si el escaneo detecta un virus, en la sesión TCP cuando puede tener ya paquetes reenviados al cliente, la conexión se resetea, pero no inserta una página de bloqueo al cliente, así el cliente puede pensar que fue un error de la red e intentar de nuevo, el motor de IPS almacena el URL y, durante el segundo intento para descargar el mismo archivo, la página de bloqueo remplazará el archivo. Incluso si el cliente tiene recibido más de un archivo en el primer intento, el archivo será cortado y el cliente no podrá abrir el archivo cortado.
- Si el virus es detectado en el inicio del stream, el escaneo de flow-base puede insertar un mensaje de bloqueo en lugar de recibir el archivo, inmediatamente en el primer intento.

En la Figura 3-19, observamos el funcionamiento del escaneo proxy-based cuando un cliente envía una solicitud al FortiGate.

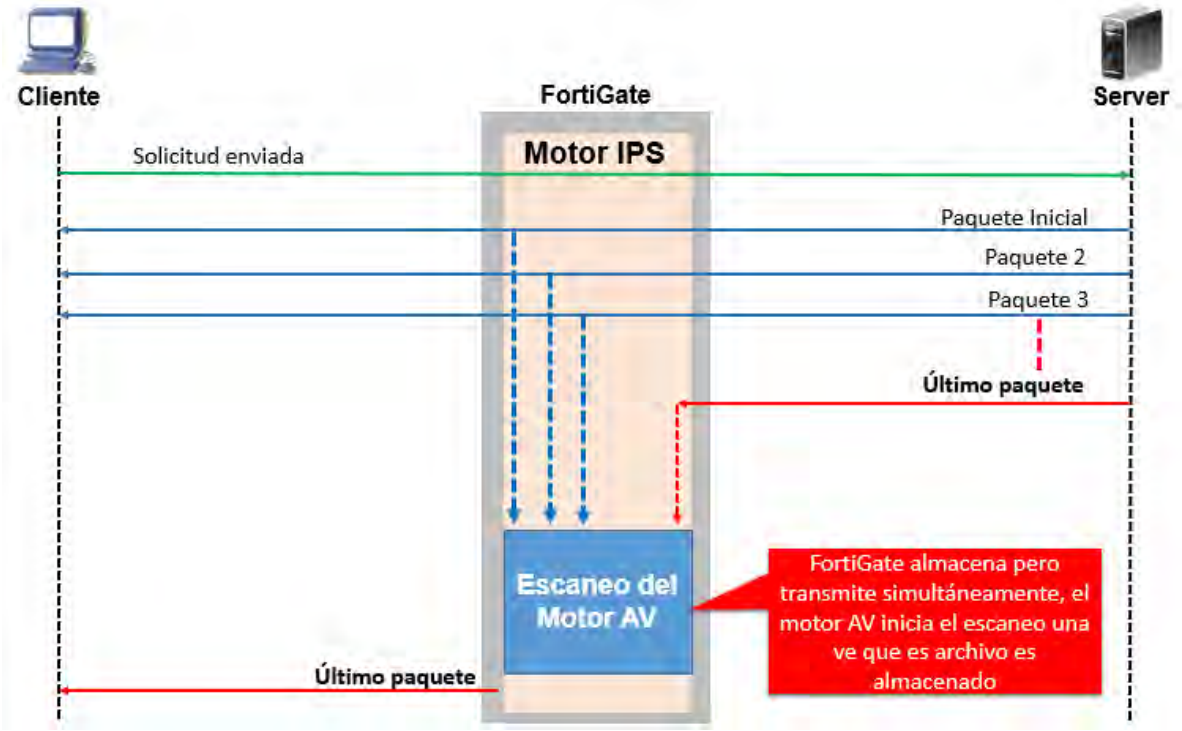


Figura 3-19. Escaneo flow-based

Como se puede observar, el cliente envía una solicitud e inicia el paquete recibiendo inmediatamente, pero FortiGate también almacena esos paquetes simultáneamente. Cuando el último paquete es recibido, FortiGate lo almacena y lo pone en espera, entonces envía el archivo almacenado al motor del IPS donde busca coincidencia de reglas para luego pasar al motor del AV para después ser escaneado. Si el AV no detecta ningún virus y el resultado es correcto, el último paquete almacenado es regenerado y reenviado al cliente, sin embargo, si un virus es encontrado, el último paquete es eliminado, incluso si el cliente no recibe el resto del archivo, el archivo será truncado y el cliente no podrá abrir ese archivo truncado.

Independientemente de qué modo se use, las técnicas de escaneo darán tazas de detecciones similares, la diferencia de estos dos modos de escaneo, va a depender mucho del rendimiento del dispositivo FortiGate, eso será la prioridad, recomendando que, para un equipo con bajos recursos, el método flow-based es más apropiado, si la seguridad es la prioridad, el método proxy-based será el apropiado.

3.9.3.- Filtrado web

El filtrado de sitios web es comúnmente usado por los administradores de red. El filtrado web ayuda a controlar, o encaminar, los sitios web que la gente visita, como: preservar productividad del empleado, prevenir congestión de la red

donde el valor del ancho de banda es usado para propósitos fuera del negocio, previene pérdidas o exposición de amenazas basadas en web, limita la responsabilidad legal cuando los empleados acceden o descargan material inapropiado u ofensivo, también prevenir el infringir los derechos de autor causados por descargas por empleados o la distribución de materiales de derechos de autor, de igual forma, previene a los menores de edad el ver material inapropiado.

El filtrado web que maneja FortiGate también son perfiles de seguridad, el cual son personalizables de acuerdo al modo de inspección seleccionado. Por lo tanto, el primer paso antes de ajustar cualquier filtro web es el de configurar el modo de inspección [11].

Cuando el dispositivo FortiGate es establecido como modo de inspección proxy, un perfil de opciones proxy deben ser también definidas. Este perfil determina el protocolo que se establece en los perfiles de seguridad que se usaran, por ejemplo, para inspeccionar el tráfico web o DNS [11].

Hay protocolos predefinidos que son utilizados para la inspección, aunque se pueden personalizar, en la Figura 3-20, se muestra un ejemplo.

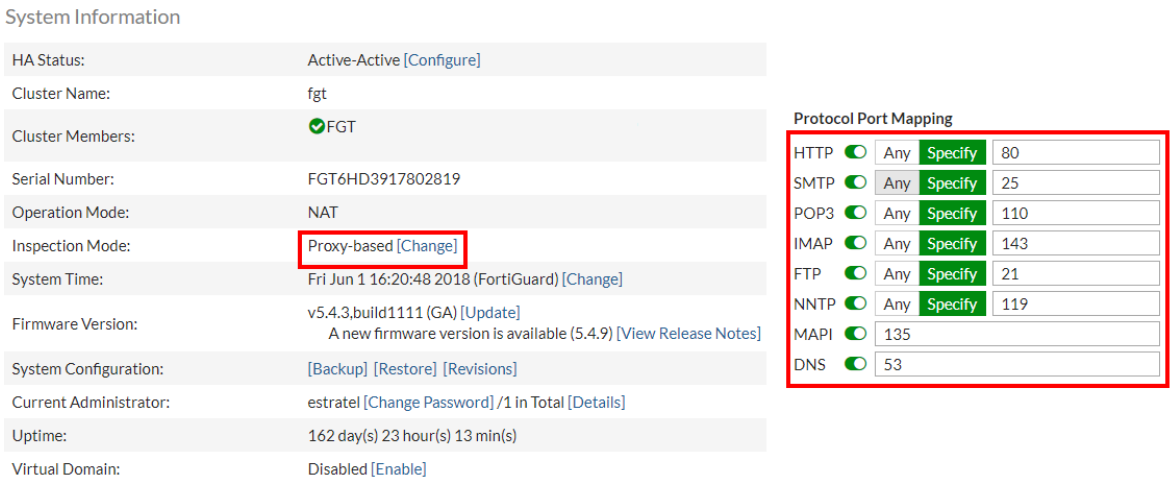


Figura 3-20. Protocolos en el modo de inspección proxy-based

Los modos de inspección del FortiGate tienen diferentes consideraciones para filtrar los sitios web:

- El modo flow-based de filtro web, es logrado al analizar el flujo TCP del tráfico entre el cliente y el servidor, esto otorga menos flexibilidad, y tiene menos opciones de configuración para la inspección del trafico web, el modo flow-based intercepta la capa de red y trabaja con la capa de transporte.
- El modo proxy-based de filtro web, es logrado al usar un proxy transparente que intercepta el tráfico entre el cliente y el servidor. El modo proxy-based otorga más flexibilidad al inspeccionar el trafico web ya que intercepta el tráfico en la capa de aplicación. También tiene más opciones de configuración, sin embargo, esta opción usa más recursos.

Como se mencionó, se puede inspeccionar el trafico DNS, pero esta opción es limitada solamente en el modo proxy-based, y es presentado como un nuevo perfil de seguridad. Este perfil busca el protocolo HTTP, esta opción filtra las solicitudes DNS que ocurren antes para obtener una solicitud GET de HTTP. Esto tiene la ventaja de iniciar bastante ligero, pero con un costo, porque carece de precisión de filtro HTTP [11].

Cada protocolo genera una solicitud DNS para resolver un nombre de host, por lo tanto, este tipo de filtrado impactara todos de los protocolos de nivel que dependen en DNS, no solo el trafico web, por ejemplo, puede aplicar a categorías FortiGuard para solicitudes DNS para servidores FTP, muy pocas características de filtro web son posibles más allá del filtrado de nombre del host, debido al moto de datos disponibles en el punto de inspección.

En la Figura 3-21, muestra la diferencia entre un filtro tradicional de HTTP y el proceso de un filtro de búsqueda DNS.

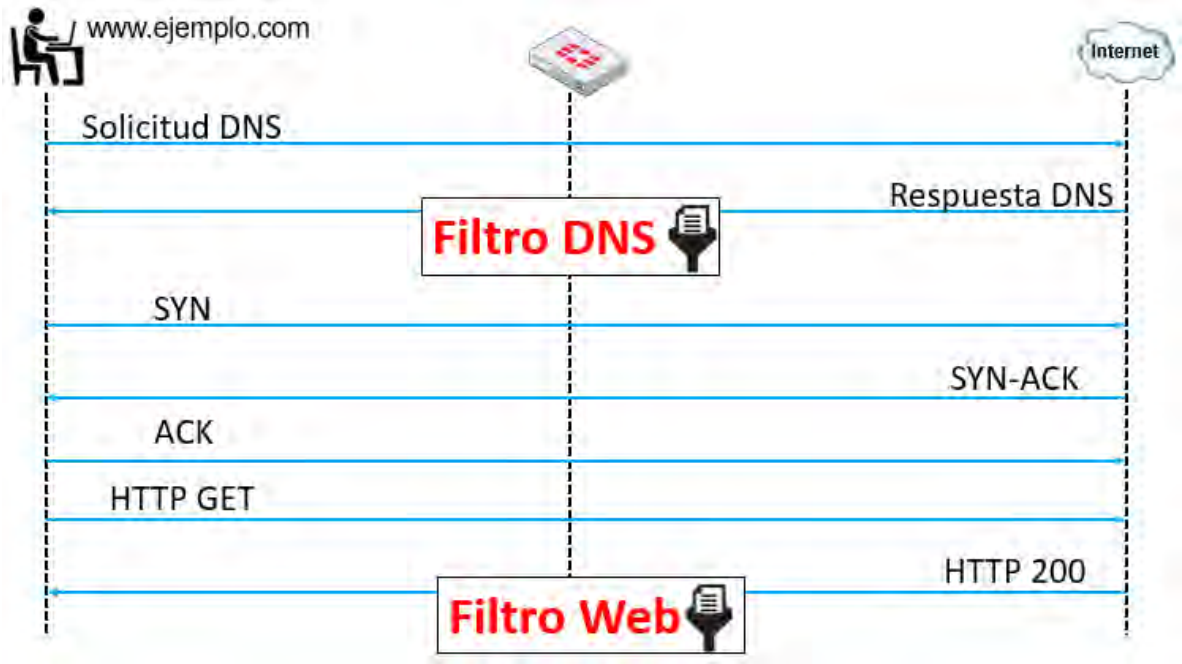


Figura 3-21. Filtro DNS y filtro web

El filtro DNS busca una respuesta del nameserver, el cual típicamente ocurre cuando se conecta al sitio web, el filtro web busca una respuesta de HTTP 200, retornando cuando se accede correctamente al sitio web. Por lo tanto, así como se muestra en la Figura 3-21, en el nombre de dominio de HTTP y el URL son piezas separadas, el nombre de dominio podría buscar en la cabecera: www.ejemplo.com, y el URL podría buscar en la cabecera: /index.php?login=true. El host (header), es lo que se obtiene de la búsqueda DNS antes de la solicitud HTTP. Obviamente el URL no es una solicitud DNS [11].

Si el filtro por dominio, a veces se bloquea mucho, por ejemplo, el blog en tumblr.com son considerados con contenido diferente, debido a todos los diferentes autores, en este caso, se puede ser más específico, y bloquear la parte de URL, tumblr.com/hacking, por ejemplo [11]. En la Figura 3-22, se resumen los siguientes modos de inspección web.

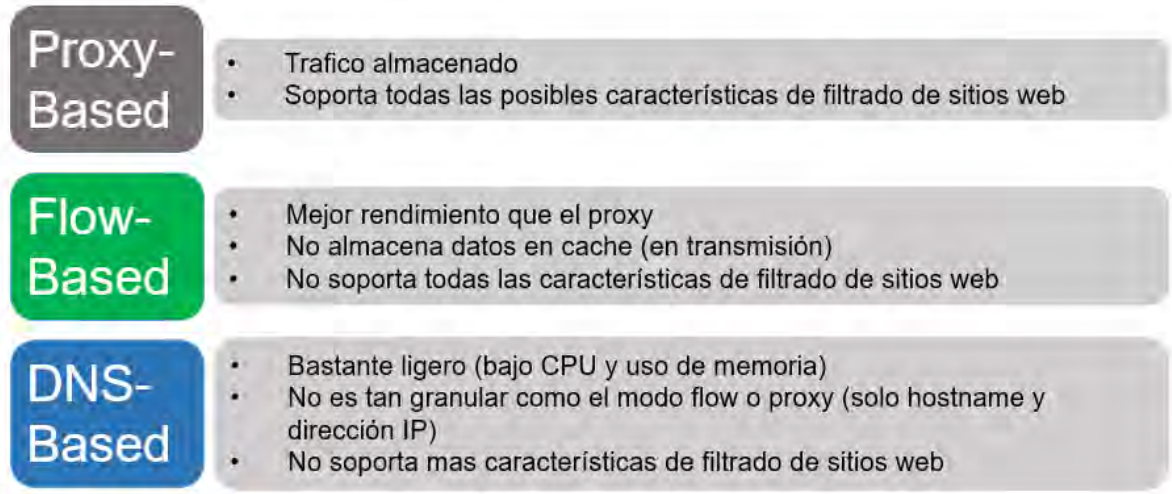


Figura 3-22. Modos de inspección

El modo proxy-based almacena el tráfico en cache, por lo tanto, esto podría causar retrasos notables dependiendo el tamaño, el límite de peso y la velocidad de conexión, sin embargo, soporta gran número de características de filtrado web.

El modo flow-based tiene gran taza de rendimiento, comparado a proxy-based, pero no almacena datos en cache, así que no hay retraso en la transmisión.

El modo DNS-based es bastante ligero ya que manipula solamente las consultas del servidor de dominio o nameserver, pero sufre de problemas de precisión porque no ve la URL completa.

3.9.4.- Filtrado de categoría respecto a FortiGuard

En lugar de bloquear o permitir sitios web individualmente, el filtro de categoría FortiGuard analiza la categoría con la que se calificó un sitio web, la acción es tomada basada en la categoría, y no basada en el URL de sí mismo [11].

La categoría de filtrado del FortiGuard cuenta con un servicio en vivo que requiere conexiones a la red de FortiGuard, se debe tomar en cuenta que un contrato para este servicio es requerido.

Las categorías son determinadas automáticamente y por métodos humanos, el equipo de FortiGuard automáticamente rastrea los sitios web buscando varios aspectos del sitio (análisis de textos, explotación de la estructura web) y así subirlos en una clasificación, de igual forma hay personas del equipo de FortiGuard (evaluador humano) examinando los sitios y buscando dentro de la clasificación para determinar categorías. Para revisar completamente la lista de

las categorías y subcategorías o también solicitar cambiar sitios web de categorías, es necesario ingresar en el siguiente sitio web: www.fortiguard.com/webfilter [11]. En la figura 3-23, se muestra un ejemplo de cómo trabaja FortiGate y FortiGuard para el filtrado de categorías.

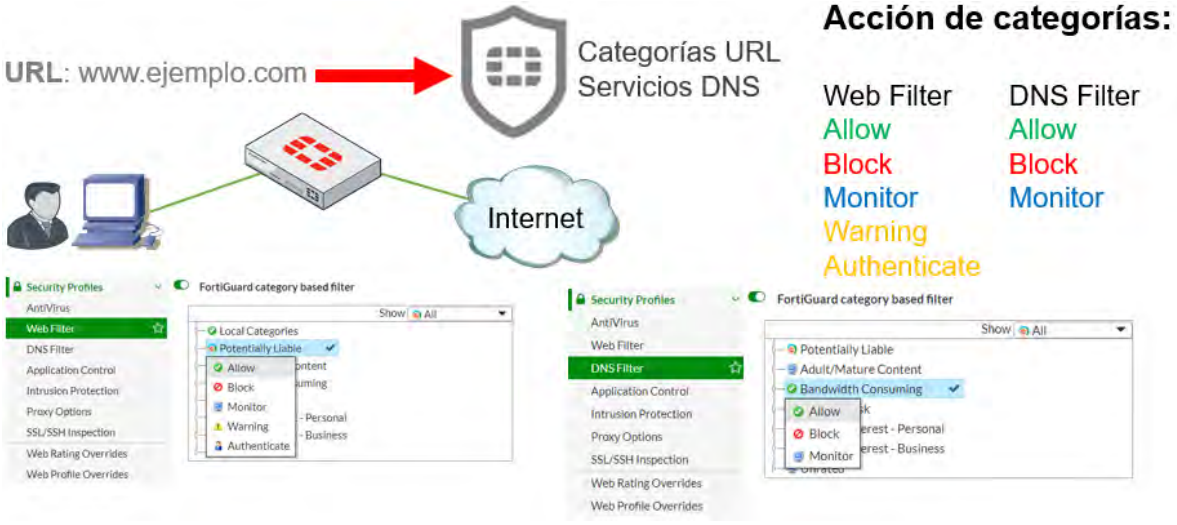


Figura 3-23. FortiGate y FortiGuard en conjunto

Como se observa en el ejemplo de la Figura 3-23, FortiGate hace peticiones al FortiGuard Distribution Network (FDN) para determinar la categoría de la página web solicitada, por lo tanto, cuando los usuarios visiten los sitios web, FortiGate usara el servicio de FortiGuard live para descubrir la categoría para el URL y tomar una acción configurada para esa categoría, como permitir o bloquear el acceso, hay diversas acciones como son el de permitir, bloquear, monitorear, advertencia y el de autenticación. Con esa característica se pueden realizar el aumento del filtro web sin necesidad de definir individualmente cada sitio web.

Siempre hay la posibilidad para errores de clasificación, o un escenario donde simplemente no se esté de acuerdo con la clasificación dada, así que, existe la posibilidad de usar el portal web para contactarse con el equipo de FortiGuard para enviar una solicitud de una nueva clasificación, o el de obtenerlo clasificado de no estarlo en la base de datos. Las solicitudes para una nueva clasificación de sitios web son en la página www.fortiguard.com/webfilter [11]. En la Figura 3-24, se muestra un ejemplo para solicitar una clasificación de sitios web ingresando desde el FortiGate.

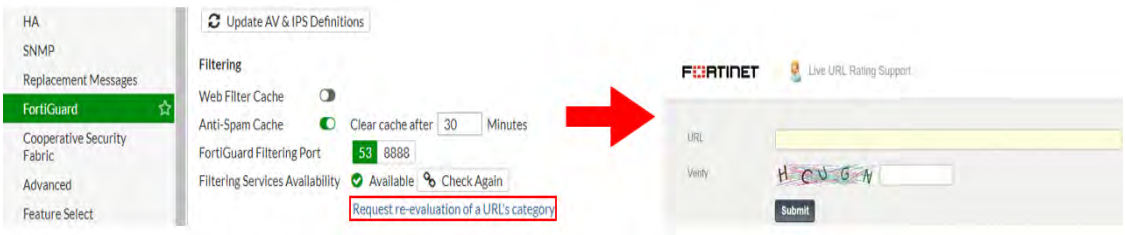


Figura 3-24. Ejemplo de solicitud para clasificación de sitio

Para usar el filtro DNS de FortiGate, se debe usar el servicio DNS de FortiGuard para hacer búsquedas DNS, las solicitudes de búsquedas DNS se envían al servicio DNS FortiGuard y regresa con una dirección IP y una clasificación de dominio que incluye la categoría FortiGuard de la página web [11].

FortiGate puede mantener una lista de sitios web por clasificación que han sido visitados recientemente almacenados en la memoria, así que, si la URL ya es conocida, FortiGate no enviara una solicitud a FortiGuard. Dos puertos deben estar disponibles para la solicitud a los servidores de FortiGuard, el puerto 53 y el puerto 8888. El puerto 53 se encuentra por defecto, por lo tanto, es también utilizado como el puerto para ser usado por el DNS el cual debe estar casi siempre abierto. Sin embargo, cualquier tipo de inspección revelará que este tráfico no es DNS e impide que el servicio funcione, en ese caso, es posible intercambiar o alternar al puerto 8888, pero este puerto no es recomendado para ser abierto en todas las redes, así que se necesitará verificar de antemano [11].

Cuando es habilitado las peticiones del Block DNS para conocer que páginas contienen botnet C&C (comando y control) desde el perfil del filtro DNS, el DNS hace búsquedas para hacer comprobaciones con la base de datos y el control de botnet. Esta base de datos es dinámicamente actualizada desde el FortiGuard y almacenada en el FortiGate. Todo lo que tenga coincidencia con búsquedas DNS serán bloqueadas, para estos servicios es necesario una licencia activa de filtro web [11].

La Figura 3-25, se muestra un ejemplo de que el botnet C&C está habilitado en el perfil por defecto, el cual contiene una base de datos bastante grandes de páginas donde el riesgo de botnet es crítico.

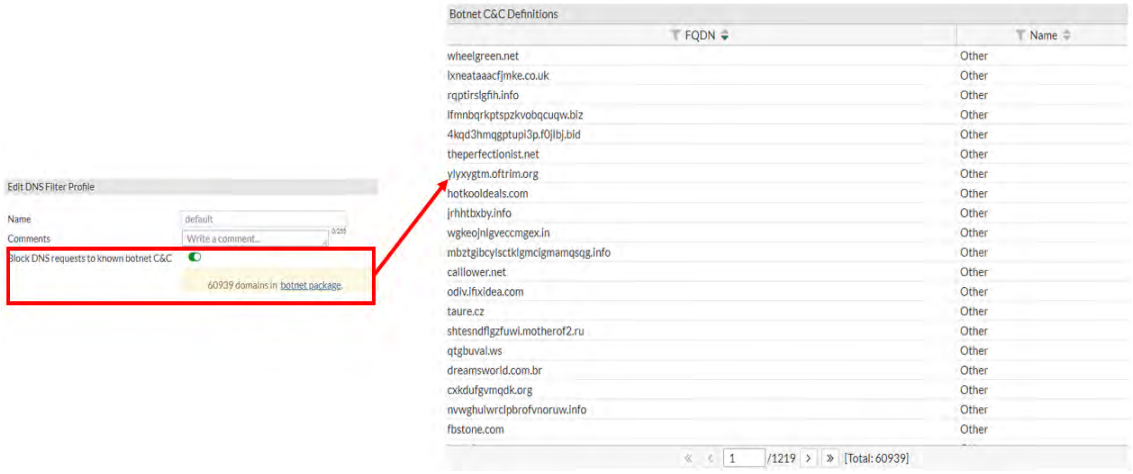


Figura 3-25. Botnet habilitado

Estos perfiles de seguridad son necesarios activarlos en la política para que hagan coincidencia con el tráfico y realicen la función deseada, en la Figura 3-26, se ve un ejemplo de una política de firewall con un perfil habilitado.

Figura 3-26. Habilitar perfiles de seguridad en la política

Si un perfil de filtrado web o de filtrado DNS no funcionará correctamente este podría ser una de las causas, que dichos perfiles no se encuentren habilitados ya que, de esta forma, FortiGate no encontraría coincidencia de tráfico y no haría la función de bloquear y/o permitir sitios web.

3.10.- Control de Aplicaciones

El control de aplicaciones (Application control) tiene la capacidad de detectar aplicaciones (incluso unos que consumen más ancho de banda) y permitir que tomen apropiadamente acciones relacionado al tráfico de aplicaciones, como monitorear, bloquear o aplicar conformado de tráfico (traffic shaping), el cual permite tener un control del ancho de banda.

Una aplicación puede ser solamente identificada si tiene una transmisión con patrones de algún modo únicas, sin embargo, no todas las aplicaciones tienen comportamientos únicos, muchas de ellas re-usan las aplicaciones que ya existen, de igual forma están los protocolos estándares y los métodos de comunicación, por ejemplo, muchos video juegos como World of Warcraft ahora usa el protocolo de BitTorrent para distribuir parches para sus juegos [11].

El control de aplicaciones puede ser configurado en los modos proxy-based y flow-based, pero la inspección siempre es flow-based ya que utiliza el motor IPS el cual es una inspección flow-based. En comparación, cuando se aplica el filtrado web y el antivirus a través de un proxy HTTP, el proxy primero analiza el HTTP y remueve el protocolo, y entonces escanea el payload que lleva dentro [11].

Detecta y actúa con el tráfico de las aplicaciones en la red, como Facebook, Skype, Gmail, LogMeIn, etc. De igual forma soporta muchas aplicaciones y categorías, incluyendo P2P y proxy, incluso puede escanear protocolos seguros.

A diferencia de otros perfiles de seguridad, como el filtrado web o el antivirus, el control de aplicaciones no es aplicado por un proxy, este usa un motor IPS para analizar el tráfico de la red y detectar el tráfico de la aplicación, incluso si la aplicación está usando protocolos y puertos estándar no que no sean estándar [11].

3.10.1.- Arquitectura Peer-to-Peer

Cuando HTTP y otros protocolos fueron diseñados, ellos fueron diseñados para ser más fácil el rastrearlos, de esta manera, un administrador podría fácilmente dar accedo a ciertos servidores que se encuentran detrás de un NAT, como routers y, más tarde, firewalls. Pero cuando las aplicaciones P2P fueron diseñadas, ellas tenían que poder trabajar sin ayuda (o cooperando) desde la red de administradores, con el fin de lograr esto, los diseñadores hicieron aplicaciones P2P para poder evitar firewalls y ser difícilmente de detectarlos. Puertos aleatorios, pinholes (puertos no protegidos por firewall), y el cambiar los patrones de encriptación, son algunas de las técnicas que el protocolo P2P usa. Estas técnicas hacen que las aplicaciones P2P sean más difícil de bloquear usando una política de firewall, y también hacen difíciles de detectar para la inspección del modo proxy-based. La inspección del modo flow-based usa el motor IPS el cual puede analizar los paquetes para la búsqueda de ciertos patrones y entonces buscar los patrones para detectar las aplicaciones P2P [11].

¿Por qué el trafico peer-to-peer es difícil de detectar?, los protocolos tradicionales (HTTP, FTP) tienen una arquitectura de cliente-servidor, el cual es un único servidor con un gran ancho de banda para muchos clientes, de igual forma requiere de números de puertos predecibles, políticas de firewall, NAT/PAT, etc. En cambio, los protocolos (Skype, BitTorrent) peer-to-peer tienen una arquitectura distribuida, cada peer es un servidor con un pequeño ancho de banda para compartir, es difícil de administrar hacia múltiples políticas de firewall para bloquear dichas aplicaciones, también no dependen de un solo puerto de reenvió y además usan técnicas evasivas para estas limitaciones. En la Figura 3-27, se ve claramente la arquitectura de un cliente-servidor.

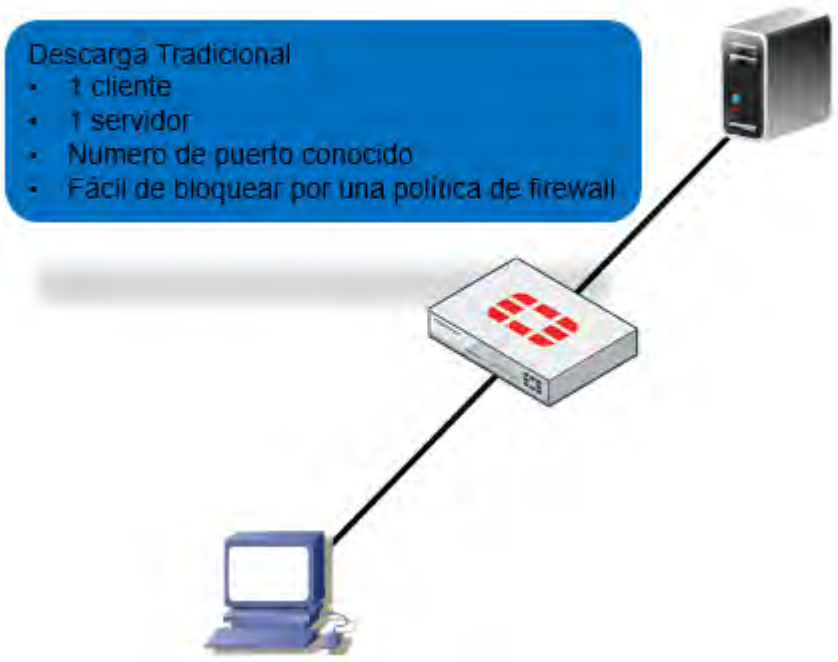


Figura 3-27. Arquitectura de cliente-servidor

Las descargas tradicionales usan un puerto definido por encima de un numero de puerto estándar, ya sea desde sitio web o un sitio FTP, la descarga es desde una única dirección IP, hacia otra única dirección IP, por lo tanto, el bloquear este tipo de tráfico resulta muy fácil, con una política de firewall.

Pero, ¿Por qué resulta más difícil bloquear aplicaciones peer-to-peer?, en la Figura 3-28, observamos un ejemplo de la arquitectura de un P2P.

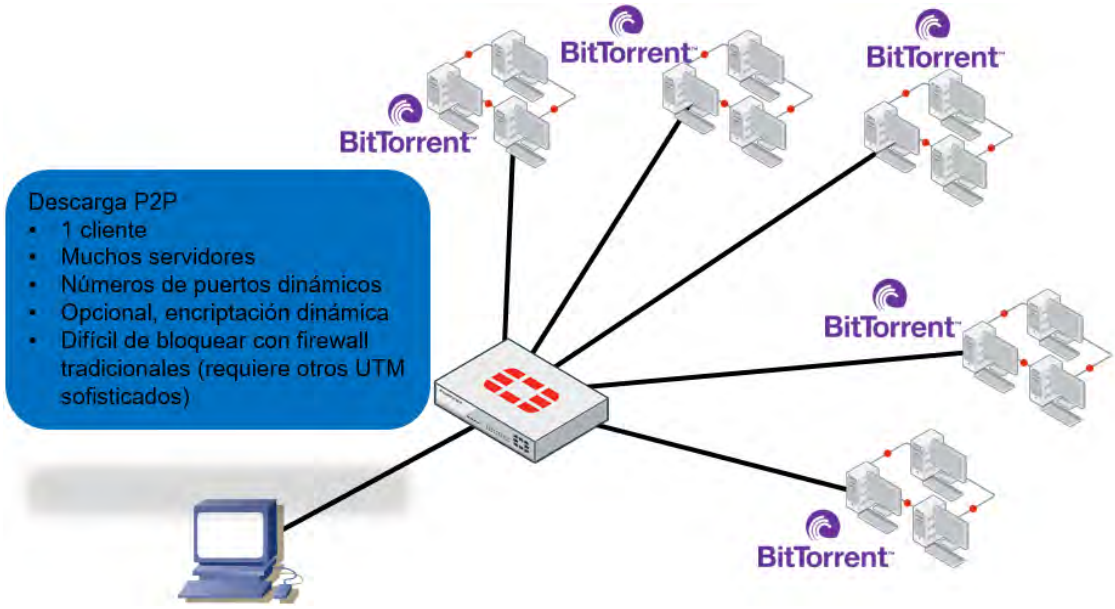


Figura 3-28. Arquitectura P2P

Las descargas P2P dividen cada archivo entre múltiples clientes (teóricamente ilimitada). Cada cliente entrega parte del archivo, mientras se tengan muchos clientes es una desventaja en las arquitecturas cliente-servidor, esto para las arquitecturas P2P son una ventaja, como el numero clientes incrementa a n, el archivo es entregado rápidamente en n veces. Eso hace que la popularidad incremente la velocidad de la entrega (a diferencia de la arquitectura cliente-servidor), donde la popularidad podría efectivamente causar un ataque de denegación de servicios al servidor, algunos software, como el BitTorrent, algunas distribuciones de Linux, y los juegos que emplean distribuciones de nuevos parches, aprovechan esta ventaja, incluso si cada cliente tiene un bajo ancho de banda, juntos, ellos pueden ofrecer más ancho de banda que muchos otros poderosos servidores [11].

El control de aplicación del FortiGate usa un motor IPS para detectar estas aplicaciones y los cambios que radican en ellos, las actualizaciones del FortiGuard son cruciales. Es posible ver la base de datos y su versión en el sitio web www.fortiguard.com, o entrando en la sección de Application Signatures, en el perfil del control de aplicación. La base de datos del control de aplicación otorga detalles acerca del control de aplicación de las firmas basadas en categorías, tecnologías y riesgos por nombrar algunos [11].

Cuando se construye una firma del control de aplicación, la seguridad del FortiGuard investiga y evalúa la aplicación para después asignarle un nivel de riesgo, la asignación del nivel de riesgo es basada en un tipo de riesgo de seguridad [11].

Si hay aplicaciones que son necesarias controlar que no se encuentran categorizados, y la última versión incluye definiciones para dichas aplicaciones, es posible ir al sitio web de FortiGuard y enviar una solicitud para tener nuevas aplicaciones agregadas, muy similar al perfil del filtro web, que se vio anteriormente.

El perfil de control de aplicación consiste en tres diferentes tipos de filtros:

- Categories: consiste en la aplicación y son basadas en agrupación similar, por ejemplo, todas las aplicaciones que son capaces de otorgar acceso remoto son agrupadas en la categoría Remote Access. Es posible ver las firmas de todas las aplicaciones en una categoría o aplicar una acción a dicha categoría.
- Application Overrides: la anulación de la aplicación otorga flexibilidad al control específico de firmas y aplicaciones.
- Filter Overrides: las anulaciones de filtro pueden ser útil cuando una categoría predeterminada no conoce los requerimientos del administrador de red, y necesita bloquear todas las aplicaciones basadas en criterios que no está disponible en las categorías. Se puede configurar la categorización de aplicaciones basadas en comportamiento, popularidad, protocolo, riesgo, marca, y/o la tecnología usada por la aplicación, y tomar acciones basadas en eso.

El perfil de control de aplicación se puede configurar desde la página Application Control, es posible configurar acciones basadas en categorías, anulación de aplicación y anulación de filtro como se mencionó anteriormente, de igual forma también se puede ver la lista de las firmas del control de aplicaciones como se muestra en la Figura 3-29.

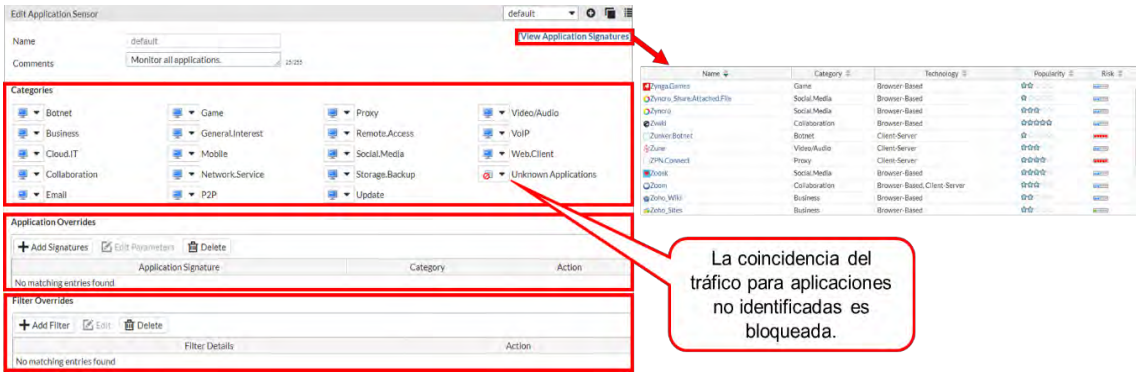


Figura 3-29. Firmas de control de aplicaciones

Las aplicaciones que no hagan coincidencia en el tráfico con ninguna otra firma de las aplicaciones que ya están categorizadas, se catalogan como desconocidas.

Identificar el tráfico como desconocido podría causar muchas entradas de logs, y frecuentemente muchas entradas de logs bajan el rendimiento del equipo. Es recomendable que en la política se deshabilite la opción de logs, esta opción se puede utilizar cuando se necesite analizar el tráfico en la red o cuando se aprecie que hay aplicaciones que puedan dañar el rendimiento de dicha red.

Una vez que se tenga listo las configuraciones de categorías del control de aplicación, es de gran importancia habilitar el sensor en la política donde se requiere que haga la función deseada como se muestra en la Figura 3-30.

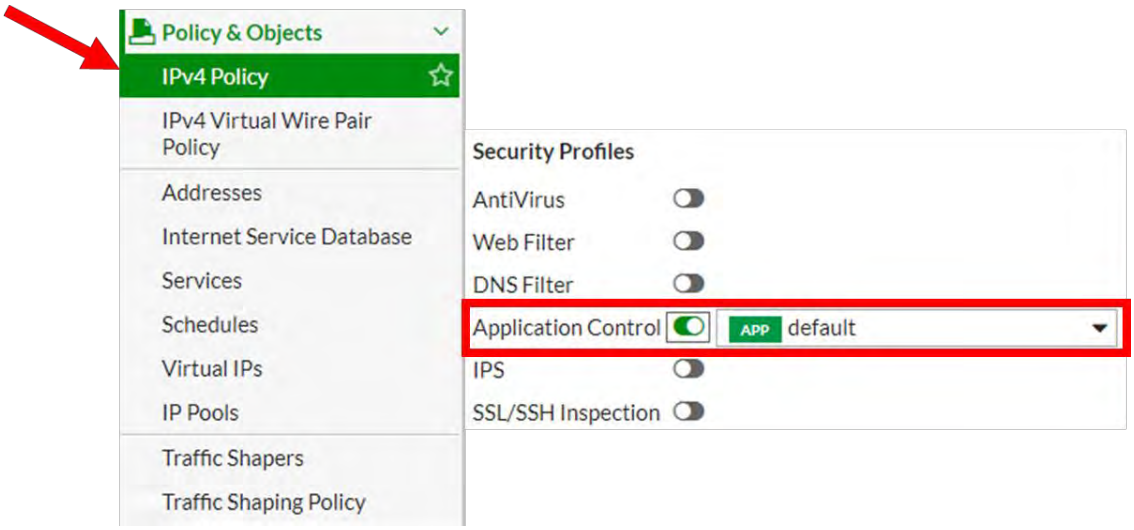


Figura 3-30. Habilitar sensor en la política

Como en cualquier otro perfil de seguridad, estos ajustes no son globales. FortiGate solamente las aplicara en el tráfico donde gobierne en la política de firewall, donde se habilita el perfil del control de aplicación. Esto permite un control granular.

El motor IPS examina el flujo del tráfico en busca de coincidencias de firmas, entonces, FortiGate escanea los paquetes que coincidan en un orden especifico, para el perfil del control de aplicación:

1. Application Overrides: si se tiene configurado cualquier anulación de aplicación, el perfil del control de aplicación considera esto primero, busca una coincidencia iniciando en la anulación de la parte superior de la lista, igual que el comportamiento de las políticas de firewall.
2. Filter Overrides: si no hay coincidencia existente en la operación de aplication override, entonces el perfil del control de aplicación emplea la acción basada en la operación configurada de Filter Overrides.
3. Categories: Finalmente, el perfil del control de aplicación usa la acción que se tenga configurada en la aplicación Categories.

También vale la pena mencionar que múltiples overrides para la misma firma no puede ser creada.

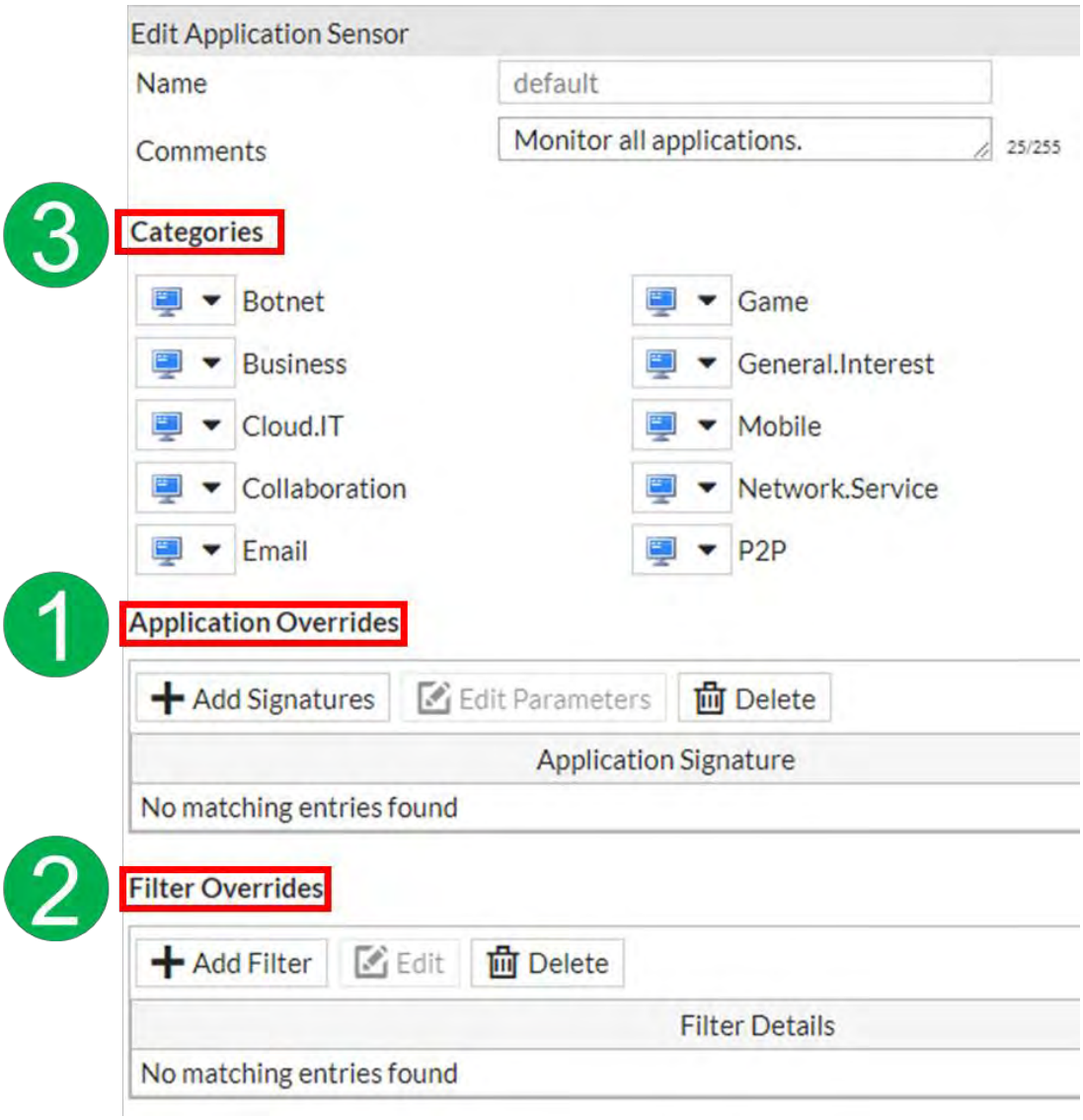


Figura 3-31. Orden de operaciones

En la Figura 3-31, se ve el orden de las operaciones como se mencionó anteriormente, el motor IPS es el encargado de la identificación de la aplicación.

Para cada filtro en el perfil del control de aplicación, se debe indicar la acción que el FortiGate hará cuando se encuentre una coincidencia de tráfico, las cuales son las siguientes:

- Allow – simplemente pasa el tráfico y no genera log.
- Monitor – pasa el tráfico, pero también genera mensajes de log.
- Block – deja caer el tráfico y genera mensajes de log.
- Quarantine – Bloquea el tráfico desde una IP atacante hasta que expira el tiempo que haya sido alcanzado, esto también genera mensajes de log.

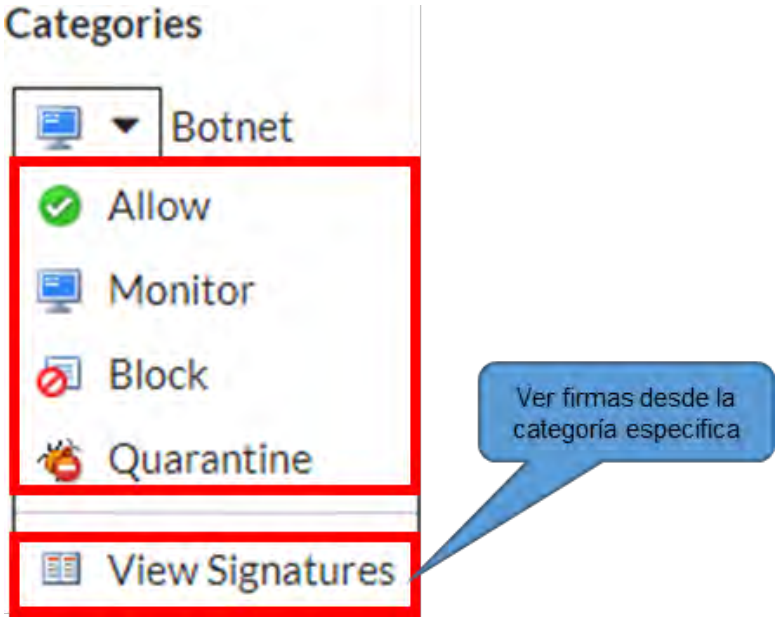


Figura 3-32. Sección View Signatures

La acción View Signatures como se muestra en la Figura 3-32, solamente permite ver las firmas desde una categoría en particular y no es una acción configurable.

Si no se está seguro de que acción escoger, la acción de Monitor puede ser útil inicialmente, mientras se estudia la red. Una vez que se tenga el estudio del tráfico de la red, se puede afinar la selección de filtros para escoger la acción más apropiada, de otra manera, la más efectiva acción para el recurso del FortiGate sería el de bloquear.

Es muy importante mencionar, que el control de aplicaciones pasa primero a ser escaneado antes del filtrado web, así que, si se tiene bloqueado una categoría en el filtrado web pero el tráfico está permitido en el control de aplicaciones, por consiguiente, el tráfico será permitido.

Para aplicaciones basadas en HTTP, el control de aplicaciones puede otorgar una realimentación para el usuario acerca del porque su aplicación fue bloqueada, esto es llamada la página de bloqueo, como se muestra en la Figura 3-33, y es similar a la que se configuran para el bloqueo de URLs que se bloquean en el filtro web del FortiGuard [11].

Figura 3-33. Bloqueo de página

El bloqueo de la página puede contener la siguiente información:

- La firma que detecto la aplicación (en este caso, BitTorrent).
- La categoría de la firma (P2P).
- La URL que fue específicamente bloqueada (en este caso, la página principal de bittorrent.com), ya que una página web puede ser ensamblada desde múltiples URLs.
- La IP origen del cliente (10.0.1.10).
- La IP destino del servidor (20.x.x.x).
- El nombre de usuario (si la autenticación se encuentra habilitada).
- El UUID de la política donde gobierna el tráfico.
- El nombre del host del FortiGate.

Las últimas dos piezas de información en la lista pueden ser de ayuda para determinar cuál FortiGate bloquea la página, incluso si se tiene una gran red con muchos FortiGates asegurando diferentes segmentos [11].

De igual forma es posible limitar el ancho de banda de una categoría de aplicación o especificar la aplicación para configurar una política, a esto se le llama traffic shaping [11].

Se debe asegurar que los criterios de coincidencia se alinean con la política de firewall o políticas a la que se quiera aplicar el shaping, eso hace que no se tenga que coincidir directamente, por ejemplo, si el origen en la política de firewall es establecido para todo (0.0.0.0/0.0.0.0), el origen en la política del traffic shaping puede ser establecido para cualquier origen que es incluida en todo, por ejemplo, ESTUDIANTES_INTERNA (10.0.1.0/24), así como se muestra en la Figura 3-34.

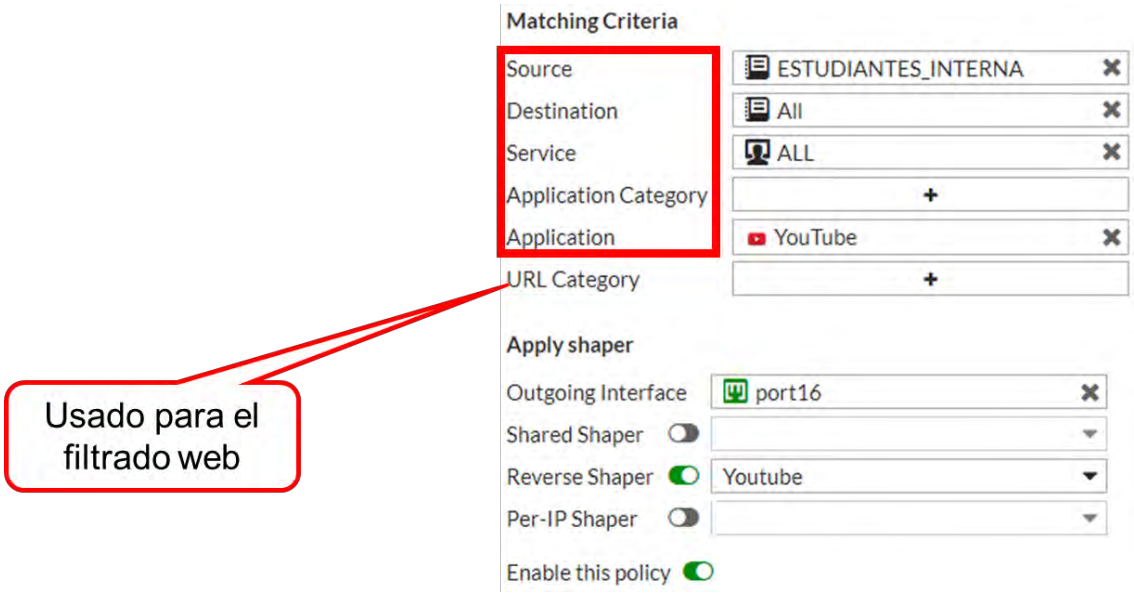


Figura 3-34. Política de aplicación

La salida de interfaz es usualmente la salida de egreso o de internet (WAN). La opción de Shared Shaper es aplicado para el tráfico que ingresa hacia el egreso, el cual es útil para restringir el ancho de banda de subida. La opción de Reverse Shaper es también un shaper compartido, pero se aplica al tráfico en dirección de reversa (tráfico de egreso al ingreso). Es útil para restringir el ancho de banda para descargas o streaming, ya que limita el ancho de banda desde la interfaz externa a la interfaz interna [11].

Hay dos tipos de shapers que pueden ser configurados desde la página de Traffic Shaping Policy, y pueden ser aplicados en la política del traffic shaping. Esos dos tipos son:

- Shared Shaper: un Shared Shaper aplica al total ancho de banda para todo el tráfico usando ese shaper. El alcance puede ser por política o por todas las políticas que tengan referenciado ese shaper.
- Per-IP Shaper: un per-IP shaper te permite aplicar el traffic shaping para todas las direcciones IP en la política de seguridad, el ancho de banda es igualmente dividido entre el grupo.

Las estadísticas del traffic shaping se pueden observar desde el FortiView, esta vista otorga detalles acerca de la información compartida, sesiones, ancho de banda, bytes descartados, entre otras [11].

Sobre el menú FortiView, la página de Applications otorga detalles para cada aplicación, como un nombre de aplicación, categorías, y ancho de banda, es posible profundizar para ver detalles más granulares el cual puede otorgar una vista acerca de orígenes, destinos, políticas o sesiones para la aplicación seleccionada [11].

3.11.- Enrutamiento

Se observará cómo se maneja el enrutamiento dinámico, estático y las políticas basadas en enrutamiento (PBR) desde la perspectiva del FortiGate. Un FortiGate en modo NAT, es, entre otras cosas, un router de capa 3.

El enrutamiento decide, donde el FortiGate, el cual debe estar funcionando en modo NAT, enviará los paquetes que reciban y lo que enviará. Todos los dispositivos que hagan enrutamiento, tienen una tabla de ruteo. La tabla de ruteo contiene una serie de reglas, una o más reglas por cada destino de red, cada regla especifica como el paquete deberá ser alcanzado por el destino, por ejemplo, el FortiGate checa el campo de destino de la cabecera IP, si las reglas de enrutamiento tienen coincidencia a ese destino, FortiGate podrá transmitir el paquete desde el puerto 1 al puerto 2.

Si un paquete llega hacia un FortiGate, lo siguiente que hará este dispositivo es buscar en su tabla de enrutamiento, dentro de sus rutas activas, alguna coincidencia que pueda usar ese paquete. FortiGate puede entregar el paquete directamente al destino final, o retransmitir al siguiente router a lo largo del camino, hacia el destino final. Usualmente, el enrutamiento IP está basado en las direcciones IP destino, sin embargo, se pueden usar paquetes usando más que una dirección IP destino.

Una apropiada configuración de enrutamiento es importante, si las direcciones de enrutamiento son mal configuradas, los paquetes no alcanzarán su destino y serán perdidas.

3.11.1.- Rutas estáticas y dinámicas

Un tipo de configuración manual de rutas es llamado una ruta estática. En la tabla de enrutamiento, este tipo de columna es establecido como Static [11].

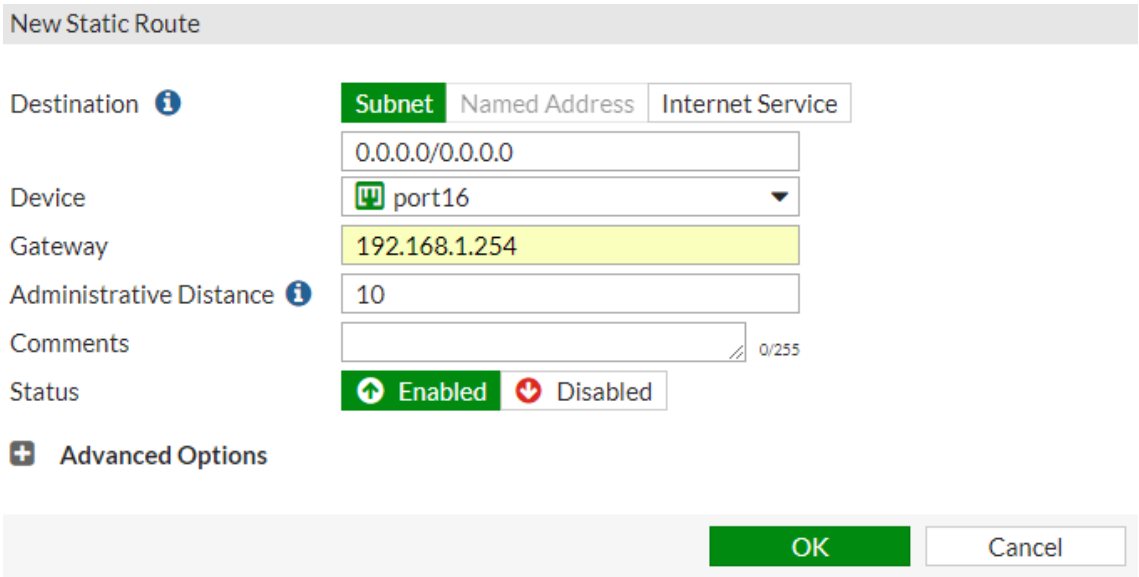


Figura 3-35. Ruta estática

Cuando se configura una ruta estática, como se observa en la Figura 3-36, el dispositivo FortiGate verá un paquete cuyo destino que este dentro de ese rango de direcciones de destino, se enviará a través de esa interfaz hacia ese router (Gateway), cuando se configura la distancia y la prioridad, el FortiGate conocerá cuando es la mejor ruta. Por ejemplo, en una simple red de hogar, automáticamente el DHCP entrega y configura una ruta estática, el modem entonces enviará toda la salida del tráfico hacia el internet del router el ISP, el cual tendrá la función de retransmitir los paquetes hacia su destino [11].

Una ruta estática no es requerida cuando el destino está directamente cableado a una de las interfaces de la red del FortiGate, sin una ruta entre ellas, el FortiGate será consiente del destino, en la tabla de enrutamiento, este tipo se llama Connected [11].

Para redes grandes, configurar manualmente cientos de rutas estáticas puede no ser práctico. Para eso están las rutas dinámicas, FortiGate soporta varios protocolos de enrutamiento dinámico como: RIP, OSPF, IS-IS y BGP [11].

En el enrutamiento dinámico, FortiGate comunica con los routers cercanos para descubrir sus caminos, y para anunciar sus propias rutas directamente conectadas. Al descubrir los caminos, estos son directamente agregados a la tabla de enrutamiento del FortiGate. Grandes redes también podrían necesitar el balanceo de enrutamiento a lo largo de múltiples caminos válidos, detectar y validar si las rutas se encuentran caídas [11]. El monitoreo de la tabla de enrutamiento del FortiGate visible en el GUI, solo publican las rutas activas.

Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	10.200.1.254	port1	
Static		0.0.0.0/0	10.200.2.254	port2	
Connected		10.0.1.0/24	0.0.0.0	port3	
BGP		10.0.2.0/24	10.200.3.1		0 00:00:05
Connected		10.200.1.0/24	0.0.0.0	port1	
Connected		10.200.2.0/24	0.0.0.0	port2	
BGP		10.200.3.0/24	10.200.3.1		0 00:00:05
BGP		10.200.4.0/24	10.200.3.1		0 00:00:05
Connected		192.168.1.0/24	0.0.0.0	port8	

Figura 3-36. Tabla de enrutamiento de FortiGate [11].

Como se observa en la Figura 3-37, hay rutas estáticas, dinámicas y directamente conectadas.

Para las subredes directamente conectadas, cuando una subred es asignada a la interfaz del router, una ruta a la subred es automáticamente agregada a la tabla de enrutamiento, el FortiGate sabrá como enrutar esos paquetes. Para las rutas dinámicas, en redes amplias, el FortiGate podrá recibir rutas desde otros routers, a través de protocolos como BGP. Esto es más rápido y es escalable que configurar manualmente muchas rutas [11].

En la Figura 3-35, no se exhiben dos tipos de rutas que soporta FortiGate, las cuales son las rutas inactivas y las rutas basado en políticas:

- Rutas inactivas – en el monitoreo del GUI del FortiGate solamente se muestran las rutas activas (el cual son usualmente el mejor camino).
- Policy routes – estas igual son omitidas por diseño, ya que las políticas de enrutamiento sobrescriben la tabla de enrutamiento.

Cada ruta en la tabla de enrutamiento incluye varios ajustes con valores asociados, estos valores son usados para retransmitir o entregar cada coincidencia de paquete. Cada router en la tabla de enrutamiento tiene:

- Dirección IP de destino y mascara para la coincidencia de paquetes.
- Dirección IP de Gateway.
- Distancia.
- Métrica.
- Prioridad.
- Dispositivo (salida de interfaz).

La dirección IP de destino y la dirección IP del Gateway están bien definidos, pero ¿qué pasa con la distancia, métrica y prioridad?

La distancia o distancia administrativa, es un número que estima la confiabilidad o calidad de cada protocolo de enrutamiento y ruta estática, si hay dos rutas hacia el mismo destino, la que tenga el valor más bajo es la que se encontrará activada y será usada para el enrutamiento porque es considerada para ser de mayor confianza. Las rutas con mayor distancia no son activadas y no son usadas para el enrutamiento [11].

Los valores por defecto de algunas distancias ya se habían mostrado en el capítulo anterior, para recordarlo se muestran las distancias de algunos protocolos en la Tabla 23:

Tabla 23. Distancias por defecto de algunos protocolos de enrutamiento

Directamente conectadas	0
DHCP Gateway	5
Rutas estáticas	10
Rutas EBGP	20
Rutas OSPF	110
Rutas RIP	120
Rutas IBGP	200

Por defecto, las rutas aprendidas a través del protocolo RIP tienen un valor más grande que las rutas aprendidas por el protocolo OSPF. OSPF es considerado más preciso que RIP.

En el caso de las rutas aprendidas a través de un protocolo dinámico, la métrica es otro valor que es usado para determinar la mejor ruta para el destino, si dos

rutas tienen la misma distancia, la métrica es usada para romper ese empate, la ruta con la menor métrica es activa y usada para el enrutamiento. En pocas palabras, la métrica es usada por protocolos de enrutamiento dinámico para determinar la mejor ruta para el destino, el cálculo se mide de maneras diferentes según el protocolo de enrutamiento, por ejemplo, RIP usa conteo de saltos, que es el número de rutas para alcanzar el destino y OSPF usa el costo del ancho de banda, que se determina por la cantidad de ancho de banda que tiene un enlace [11].

Cuando múltiples rutas estáticas tienen el mismo valor de distancia, el valor de prioridad es usado para determinar la mejor ruta, es decir, FortiGate usa la ruta con los ajustes de menor prioridad. La prioridad es usada por rutas estáticas para determinar la mejor ruta a un destino. A diferencia de las rutas que tienen los mismos ajustes de distancia y métrica, todas las rutas con la misma distancia son activadas, sin embargo, solo la ruta con el ajuste que tenga la menor prioridad es usada para enrutar el tráfico [11].

La distancia, métrica y prioridad son ajustes usadas para determinar la mejor ruta para un destino, pero, ¿qué pasa cuando dos o más rutas al mismo destino compartes los mismos valores para todos estos ajustes?, sin importar que sean múltiples rutas estáticas, OSPF o rutas BGP.

3.11.2.- Protocolo ECMP y balanceo de carga

Todas las rutas son activadas y FortiGate va a distribuir o balancear el tráfico entre ellos, esto es llamado Equal Cost Multi-Path (ECMP) [11].

Las sesiones pueden ser balanceadas entre rutas iguales dependiendo del origen de la dirección IP, direcciones IP origen y destino o peso de la interfaz. Hay un método adicional llamado usage-based o spillover, las cuales se describen a continuación:

- Source IP (defecto): las sesiones desde la misma dirección IP origen usan la misma ruta.
- Source-destination IP: las sesiones con el mismo par de IP de origen y destino utilizan la misma ruta, los flujos de tráfico destinados a diferentes pares tienden a tomar caminos diferentes.
- Weighted: las sesiones son distribuidas basadas en el peso de la interfaz.
- Usage (Spillover): una ruta es usada hasta que el límite del volumen es alcanzado, entonces la siguiente ruta es usada.

Hay otro mecanismo que FortiGate utiliza, el llamado Link Health Monitor, su función es la de detectar cuando un router a lo largo del camino se ha caído, es incluso usado donde hay rutas redundantes, por ejemplo, si hay dos enlaces de internet. Cuando es habilitado, FortiGate periódicamente envía señales a través de uno de los gateway a un servidor que actúa como un faro. El servidor puede ser cualquier host que debe normalmente ser alcanzable a través del camino, usualmente, es mejor escoger un servidor estable con infraestructura robusta, y escoger el protocolo con el cual el servidor normalmente respondería [11].

Si el FortiGate para de recibir una respuesta desde el servidor, todas las rutas usandas por ese gateway serán removidas desde la tabla de enrutamiento, alternativamente, se puede configurar el dispositivo para administrativamente cambiar a apagado una interfaz, así todas las rutas usando esa interfaz será removidas, mientras un servidor no tenga respuesta, FortiGate continuará enviando señales de monitoreo al enlace, tan pronto como FortiGate recibe una respuesta, las rutas se van a reintegrar [11].

En la Figura 3-37, se muestra un ejemplo de la configuración del protocolo ECMP en el FortiGate desde el CLI solamente.

```
1  config system link-monitor
2      edit <nombre>
3          set srcintf <interfaz>
4          set server <ip_servidor>
5          set gateway-ip <ip_gateway>
6          set protocol [ping | tcp-echo | udp-echo| twamp | http]
7      set update-static-route enable
8      next
9  end
```

Figura 3-37. Ejemplo de configuración ECMP por CLI

Como se observa en Figura 3-37, así es como se configura el link health monitor desde el CLI, en la línea 2, se debe establecer el nombre de la configuración del link health monitor, en la línea 3 se pone la interfaz a monitorear, en la línea 4 se implanta la dirección IP con la que FortiGate mantendrá comunicación, en la línea 5 se ingresa la dirección IP del gateway del router, en la línea 6 se establece el protocolo por el cual se comunicará FortiGate y el servidor por medio del gateway que se situó anteriormente, en la línea 7 se habilita la actualización de la ruta estática, sirve esencialmente para agregar o eliminar la ruta en la tabla de enrutamiento del FortiGate, y finalmente la línea 8 y 9 son para terminar la configuración del link health monitor.

Esta configuración es útil, por ejemplo, cuando se tienen dos enlaces de internet y quieres mantener tu red en redundancia.

Existe otro método que FortiGate soporta, se llama WAN link load balancing (WLLB), la cual consiste en conectar múltiples grupos de interfaces que usualmente están conectadas a enlaces ISPs, FortiGate ve todas estas interfaces de internet como una sola interfaz lógica llamada como una interfaz de WLLB. Esto simplifica la configuración ya que el administrador podría configurar una única ruta y las políticas de firewall serán aplicadas a todos estos enlaces de internet [11]. La Figura 3-38, es un ejemplo del WLLB.

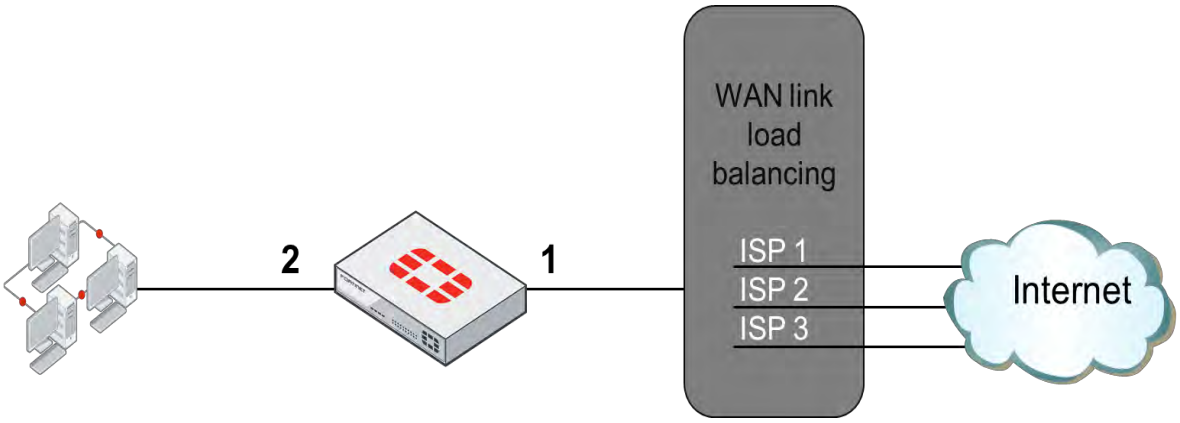


Figura 3-38. Ejemplo de WAN Link Load Balancing

El enlace 1 es un enlace virtual que contiene múltiples interfaces (miembros), conectadas a múltiples enlaces ISP. Con este WLLB, la configuración se simplifica bastante.

El WAN link load balancing, usa métodos de distribución de tráfico similares a ECMP, sin embargo, WAN link load balancing incluye un método más de balanceo: volume [11].

El WLLB usa los siguientes métodos:

- Source IP: el tráfico desde la misma dirección IP usa el mismo enlace.
- Source-destination IP: el tráfico desde el mismo par de dirección IP origen y destino usa el mismo enlace.
- Spillover: similar al método spillover de ECMP, un enlace en ruta todo el tráfico hasta que el límite del volumen es alcanzado, después de eso, otro enlace es utilizado.
- Sessions: el peso de la interfaz define la proporción de la sesión que cada enlace debe tener, la sesiones son distribuidas entre los enlaces basados en el peso de la interfaz.
- Volume: el peso de la interfaz define la proporción del volumen del tráfico que cada enlace debe tener, las sesiones son balanceadas para que el volumen del tráfico se distribuya según en el peso de la interfaz.

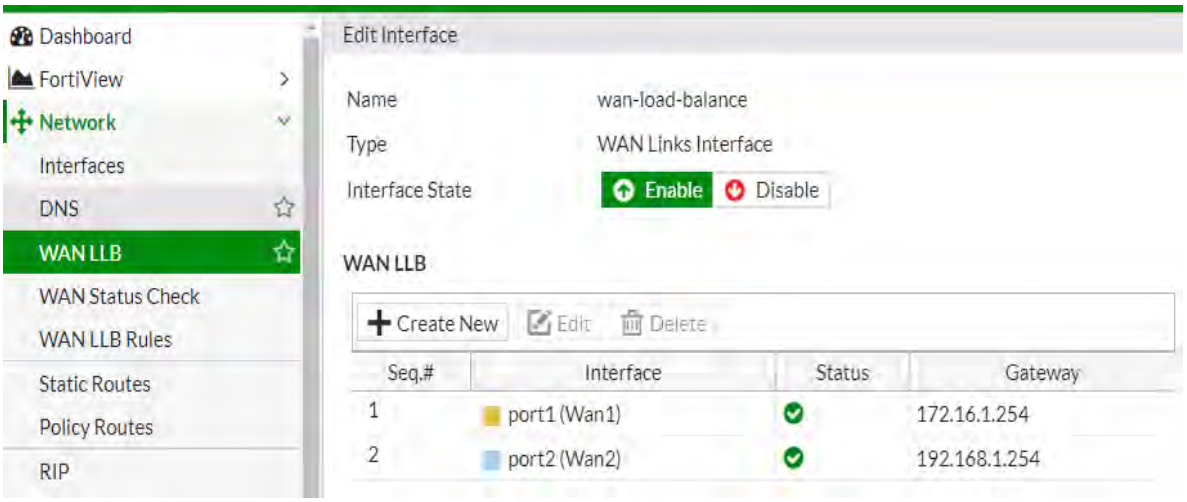


Figura 3-39. Configuración de WLLB

La Figura 3-39, se muestra la configuración del WAN link load balancing, en el cual se deben especificar que interfaces serán miembros, en otras palabras, que interfaces son las que están conectadas a internet, en este caso, las interfaces o los puertos 1 y 2.

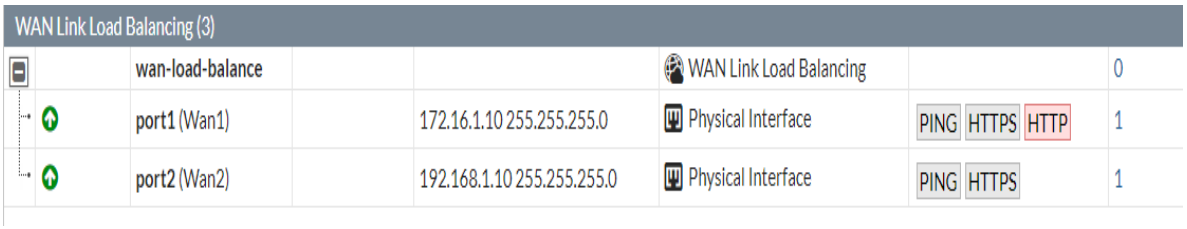


Figura 3-40. Interfaz WLLB

Como se observa en la Figura 3-40, después de que se configura el WLLB, una interfaz lógica es creada con el nombre de wan-load-balance la cual es automáticamente agregada a la configuración, las rutas y las políticas se van a configurar usando esta interfaz lógica.

FortiGate puede verificar el estatus (health) de cada miembro de la interfaz de un grupo del WAN link load balancing, después de configurar un protocolo, una dirección IP de servidor, y un límite en caso de falla, como se muestra en la Figura 3-41, FortiGate periódicamente enviara paquetes IP hacia el servidor a través de cada enlace, si el número de paquetes consecutivos no son respondidos en un enlace, y rebasan el límite máximo, entonces el enlace del grupo del WLLB será removido [11].

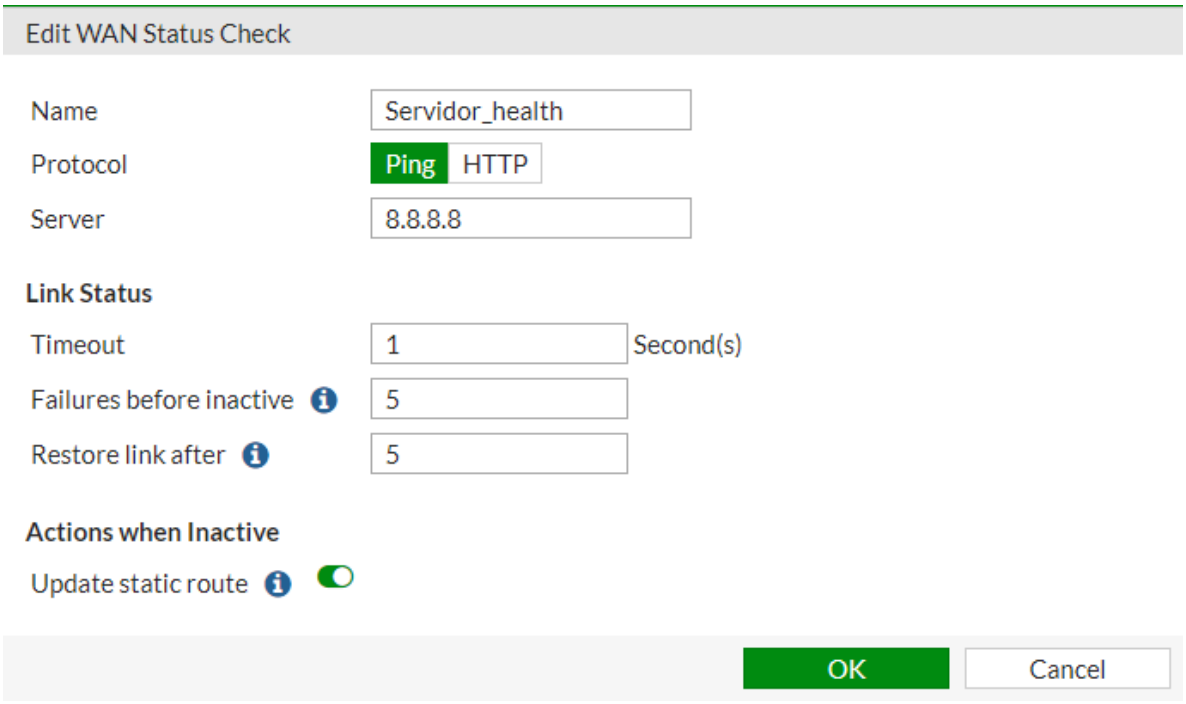


Figura 3-41. Comprobación de WAN

La conectividad es verificada entre cada interfaz y un servidor. También mide la calidad del enlace de cada miembro basado en tres diferentes criterios: latencia (retardo), jitter y porcentaje de paquetes perdidos. Así como se observa en la Figura 3-42.

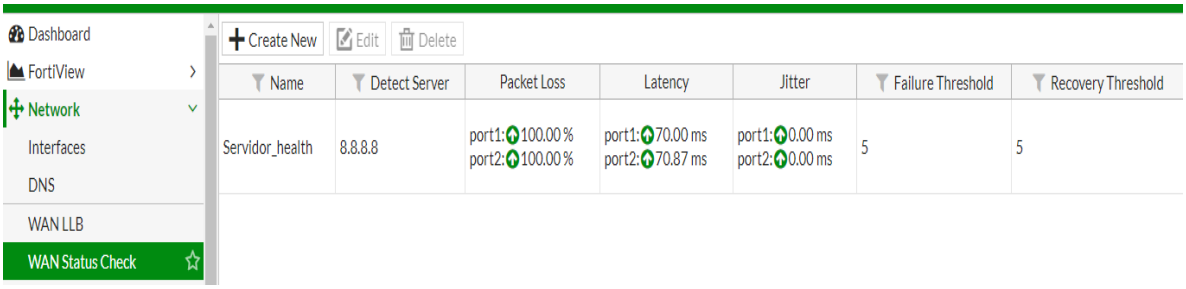


Figura 3-42. Monitor de la verificación del enlace WAN

Las reglas de prioridad se pueden usar para enrutar el tráfico según la calidad del enlace de cada miembro.

Las reglas de prioridad te permiten especificar que tráfico se quiere enrutar a través de alguna interfaz, se puede usar prioridad en las reglas para enrutar el tráfico a través de interfaces específicas, o a través de interfaces con la mayor calidad del enlace. Las reglas de enrutamiento pueden ser basadas en cualquiera de los tres criterios: latencia, jitter o porcentaje de paquetes perdido. La prioridad de las reglas es evaluada de la misma manera que las políticas de firewall, desde la parte superior, usando la primera coincidencia, los siguientes parámetros pueden ser usados para la coincidencia de tráfico:

- Dirección IP de origen.
- Dirección IP de destino.
- Número de puerto destino.
- Servicio de internet.
- Usuarios y/o grupo de usuarios.
- Tipo de servicio (ToS).

Esto ofrece gran flexibilidad para poder enrutar el tráfico, por ejemplo, se puede enrutar el tráfico de Netflix desde usuarios específicos a través de un enlace ISP, mientras se mantiene los otros tráficos de internet a través de otros enlaces ISP.

La Figura 3-43, muestra un ejemplo de como FortiGate enruta el trafico LAN de la red de origen 10.1.0.0/24 al destino netflix por un enlace especifico de ISP, mientras que el demás tráfico sigue siendo balanceada.

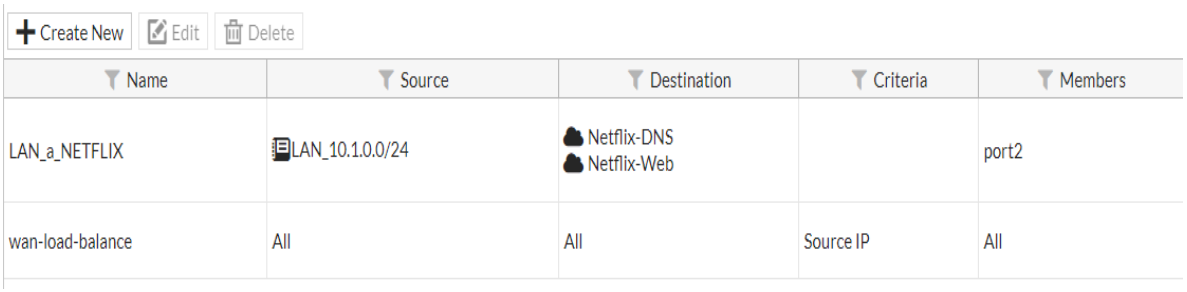


Figura 3-43. Enrutamiento de tráfico especifico

Las reglas de prioridad son agregadas como políticas de enrutamiento (PBR).

3.11.3.- Políticas basadas en enrutamiento

Las rutas estáticas son simples y son con frecuencia útil para redes pequeñas, las políticas basadas en enrutamiento, sin embargo, son más flexibles, ellos pueden coincidir con mas que solo una dirección IP destino, por ejemplo, si se tiene dos enlaces, una rápida y otra lenta, se puede enrutar paquetes con baja prioridad al enlace lento.

Las políticas de enrutamiento con la acción Forward Traffic, así como se ve el ejemplo de la Figura 3-44, tienen precedencia sobre rutas estáticas y dinámicas, así que, si un paquete coincide con una política de enrutamiento, FortiGate evitará la búsqueda en la tabla de enrutamiento [11].

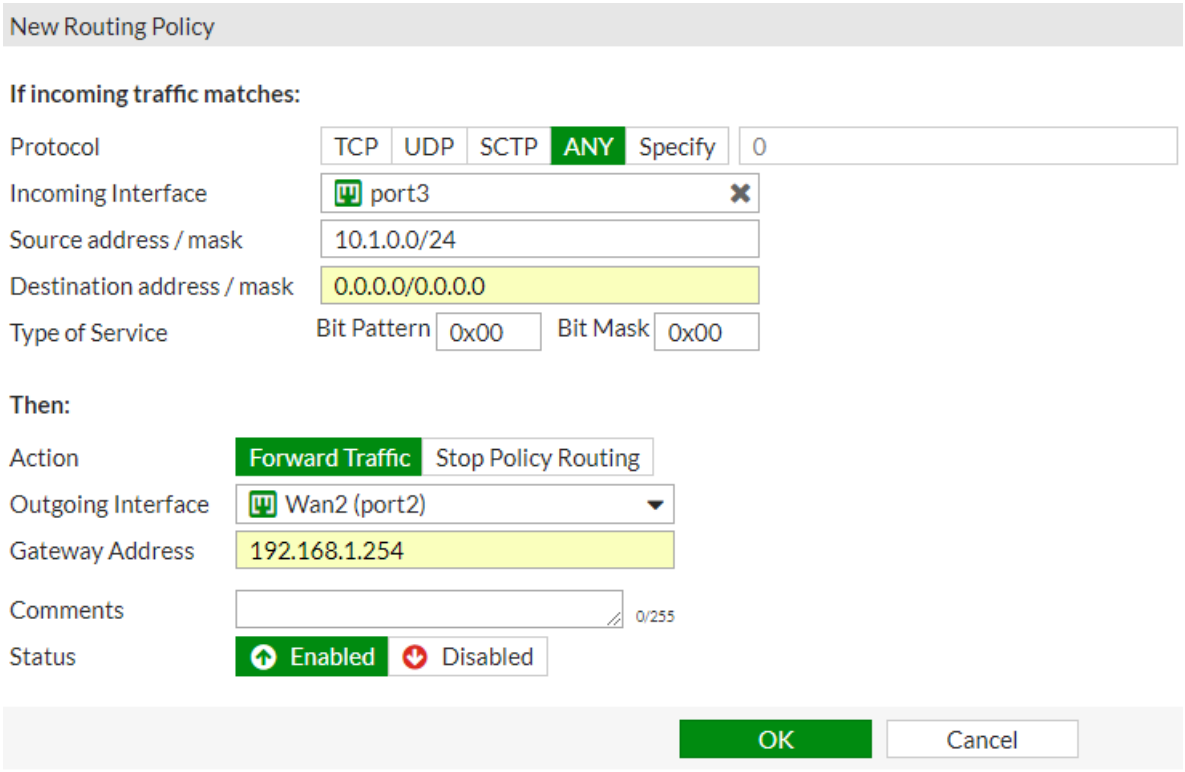


Figura 3-44. Política de enrutamiento

Las PBR son más sofisticadas para la coincidencia que las rutas estáticas. Como las rutas estáticas, en las PBR deben ser válidos: un destino y un gateway que son requerido, una desconexión (o caída) de la interfaz no puede ser utilizada, como las rutas estáticas, los paquetes deben también coincidir todas con las subredes específicas y el tipo de servicio y el número de puerto, así que, si no se quiere algún tipo de ajuste para ser incluido en un criterio de coincidencia, dejarlo en blanco [11].

Cuando un paquete encuentra una coincidencia con una PBR, FortiGate tomara una de dos acciones, ya sea enrutar los paquetes a la interfaz configurada y pasar por alto la tabla de enrutamiento, o parar la revisión de la PBR, y así los paquetes serán enrutados basado en la tabla de enrutamiento [11].

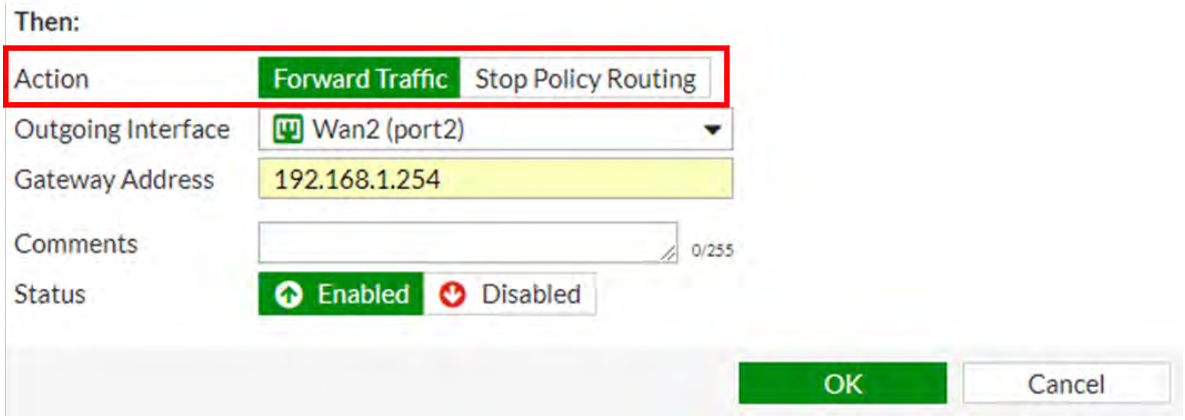


Figura 3-45. Acción de una PBR

Como se muestra en la Figura 3-45, cuando el tráfico coincida con una PBR, FortiGate tomará una de dos acciones:

- Forward Traffic: Reenviar el tráfico para especificar la interfaz de salida y la puerta de enlace.
- Stop Policy Routing: Detener la política de enrutamiento para usar la tabla de enrutamiento en su lugar.

Se mostrarán algunos comandos útiles para el FortiGate relacionado al enrutamiento,

Como se mencionó anteriormente, en el GUI del FortiGate solo se pueden ver la tabla de enrutamiento y las rutas activas, para poder hacer lo mismo en el CLI de FortiGate, es necesario correr un comando como se muestra en la Figura 3-46.

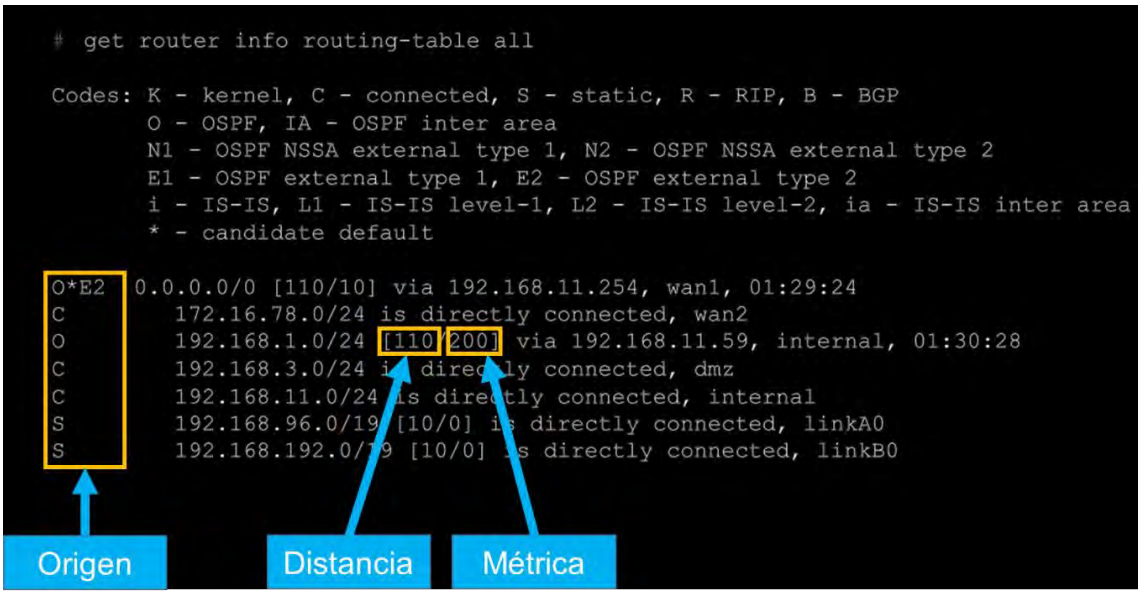


Figura 3-46. Tabla de enrutamiento con redes activas

El comando *get router info routing-table all*, exhibe en pantalla todas las rutas activas en la tabla de enrutamiento, la columna de la izquierda indica el origen para la ruta, el primer número dentro de los corchetes es la distancia y el segundo número es la métrica. Este comando no muestra las rutas inactivas, por ejemplo, cuando dos rutas estáticas tienen la misma subred destino tienen diferentes distancias, la que tenga el menor coste es la distancia que está activa, la otra con mayor distancia es inactiva, por lo tanto, este comando muestra solamente la que tenga la menor distancia (la única activa) [11].

Ahora bien, si se quiere mostrar en pantalla ambas rutas, las activas e inactivas, se utiliza el siguiente comando en CLI: *get router info routing-table database*.

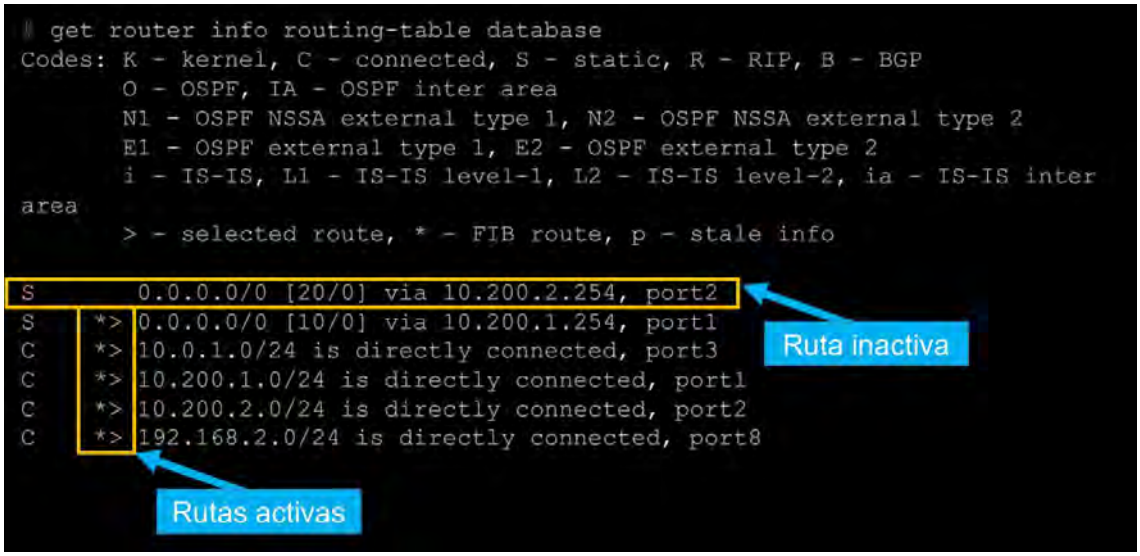


Figura 3-47. Base completa de la tabla de enrutamiento

El ejemplo de la Figura 3-47, se puede observar que el comando mostro una ruta inactiva, la ruta esta inactiva porque tiene una distancia mayor que una de abajo.

3.12.- Alta Disponibilidad

La idea de la alta disponibilidad (High Availability) es simple, él HA (por sus siglas en inglés) enlaza dos o más dispositivos.

En FortiGate HA, un equipo FortiGate actúa como el dispositivo primario (también llamado el FortiGate activo), este equipo sincroniza su configuración a los otros dispositivos, los otros FortiGate son llamados secundarios o dispositivos standby como se muestra en la Figura 3-48.

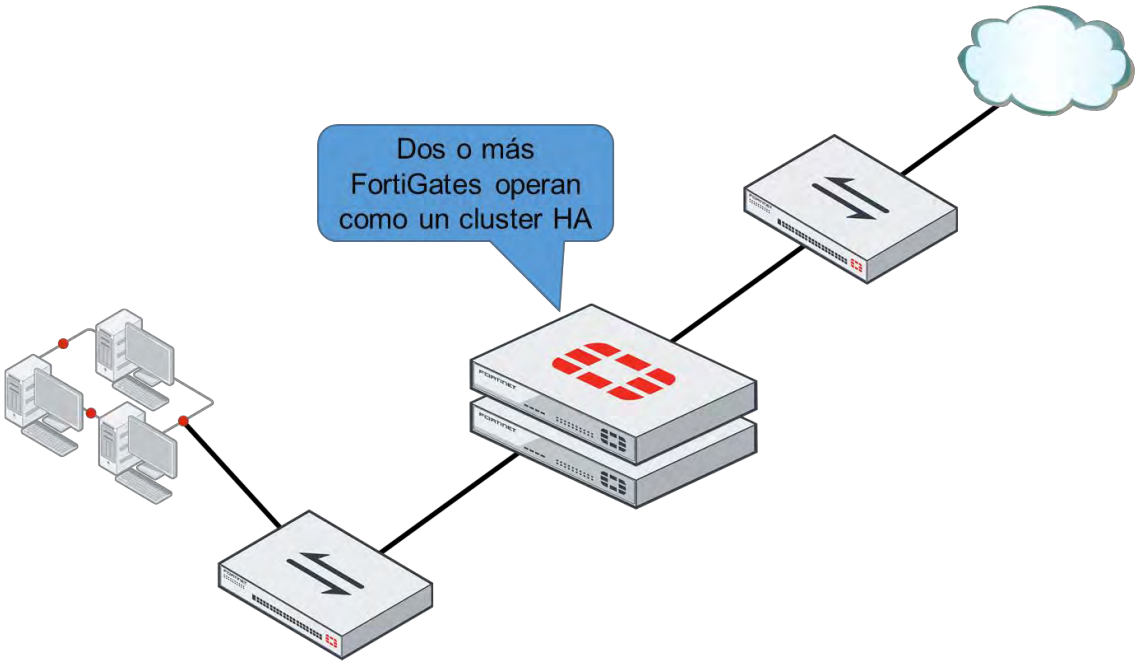


Figura 3-48. Alta disponibilidad de un FortiGate

Un enlace heartbeat entre todos los equipos es usado para detectar dispositivos que no respondan.

Actualmente hay dos modos de HA disponibles: activo-activo y activo-pasivo. Los dos serán examinados.

3.10.1.- HA activo-activo y activo-pasivo.

En cualquier de los dos modos de operaciones del HA, la configuración del FortiGate secundario es sincronizado con la configuración del dispositivo primario como se muestra en la Figura 3-49 [11].

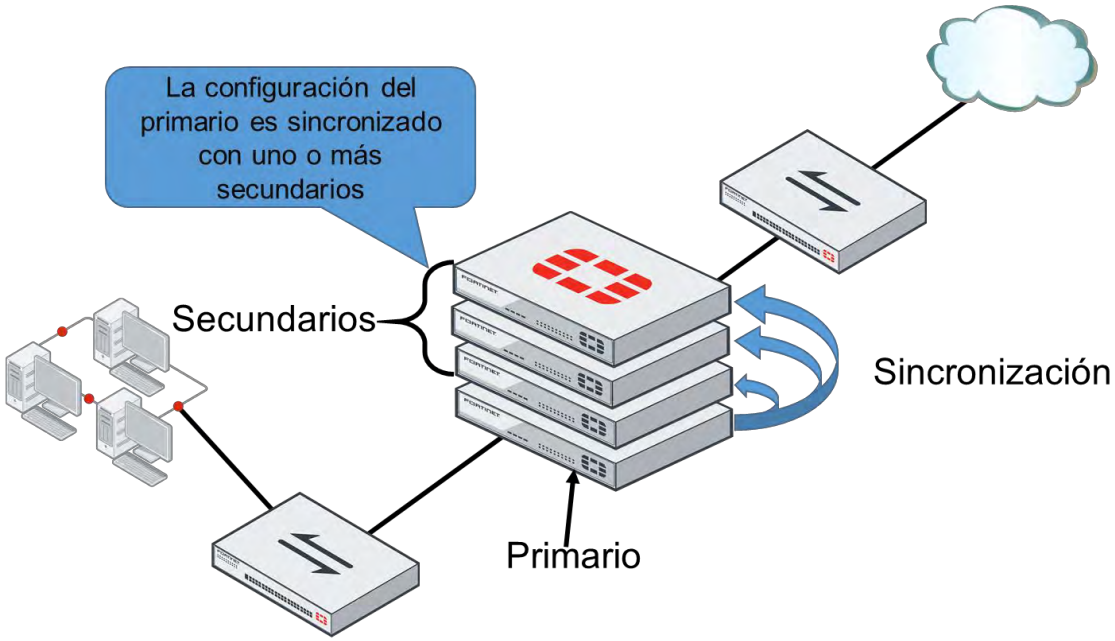


Figura 3-49. Sincronización de FortiGate primario y secundario

En el modo activo-pasivo, el FortiGate primario es el único dispositivo FortiGate que activa el proceso del tráfico, el FortiGate secundario permanece en el modo pasivo, monitoreando el estado del dispositivo primario. Si un problema es detectado en el FortiGate primario, uno de los dispositivos primarios tomará el rol de primario, este evento es llamado HA failover [11].

El otro modo HA es llamado activo-activo, como en el modo activo-pasivo, en el modo activo-activo, todos los FortiGates configurados son sincronizados, además, si un problema es detectado en el dispositivo primario, uno de los secundarios tomara el rol de primario, para procesar el tráfico. Sin embargo, una de las principales diferencias con el modo activo-pasivo es que, en el modo activo-activo, todos los otros FortiGates están procesando el tráfico, una de las tareas del FortiGate primario en el modo activo-activo es el de balancear algo del tráfico entre los dispositivos secundarios [11].

Para la comunicación entre los dispositivos FortiGate en clúster, usan un protocolo llamado FortiGate Clustering Protocol (FGCP). FGCP viaja entre los dispositivos FortiGate del clúster sobre los enlaces que se tienen designados como hearbeats. Un enlace heartbeat entre dos dispositivos FortiGate debe ser enlazado usando un cable regular RJ45 o un cable cruzado (crossover). Si se tiene algún otro dispositivo entre los FortiGate, como un switch, se tiene que asegurar que es dedicado y aislado del resto de la red, de este modo, el tráfico critico FGCP no necesita competir con otro tráfico para el ancho de banda [11].

El clúster en modo NAT y el clúster en modo transparente usan diferentes tipos de valores Ethernet para descubrir y verificar el estado de otro FortiGate en una operación clúster. Los FortiGates en un clúster también usan sesiones telnet sobre el puerto TCP 23 con un tipo Ethernet 0x8893 sobre los enlaces heartbeat

para sincronizar la configuración del clúster y para conectarse al CLI desde otro FortiGate en el clúster [11].

La disposición del FortiGate en HA requiere los siguientes dispositivos y configuraciones, primero, al menos uno de dos, pero hasta máximo cuatro, dispositivos FortiGate con el mismo:

- Firmware.
- Modelo de hardware y licencia VM.
- Capacidad de disco duro y particiones.
- Modo de operación (transparente o NAT).

Segundo, al menos un enlace entre los dispositivos FortiGate para la comunicación en HA, el cual es llamado trafico heartbeat, para la redundancia, un máximo de ocho interfaces puede ser utilizadas, si un enlace falla, él HA usara el siguiente equipo, como es indicado por prioridad y posición en la lista de la interfaz del heartbeat [11].

Tercero, las mismas interfaces en cada dispositivo FortiGate tienen que ser conectados al mismo switch o segmento de LAN, en el ejemplo de la Figura 3-50, los dispositivos FortiGate son redundantes para mitigar las fallas, pero, los switches y sus enlaces aún son un único punto de falla [11].

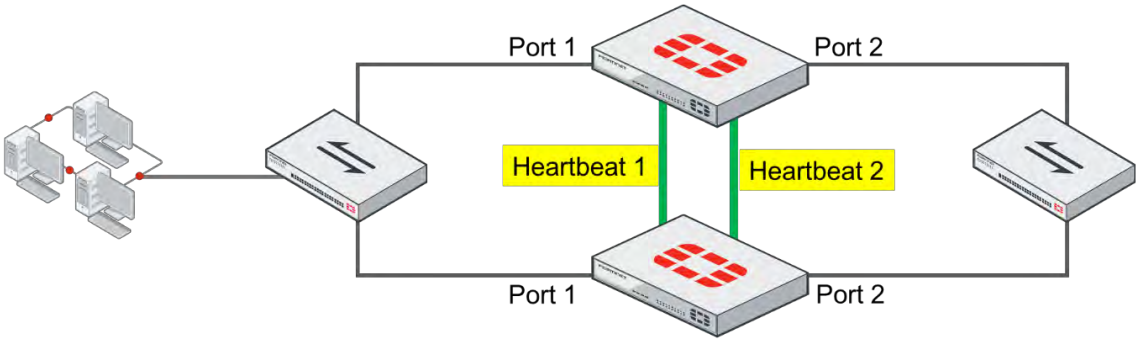


Figura 3-50. Heartbeat del FortiGate

Los clústeres en HA pueden incluir interfaces cuyas direcciones son asignadas dinámicamente, mediante DHCP o PPPoE. La mejor práctica, y una recomendación de Fortinet, es configurar las interfaces con dirección de rutas estáticas cuando se esté formando el clúster en HA, una vez que un HA es formado, se puede configurar el direccionamiento DHCP o PPPoE para una interfaz, si una interfaz es configurada para DHCP o PPPoE habilitando él HA podría resultar en la interfaz el recibir una dirección incorrecta o que no sea posible conectarse al servidor DHCP o PPPoE [11].

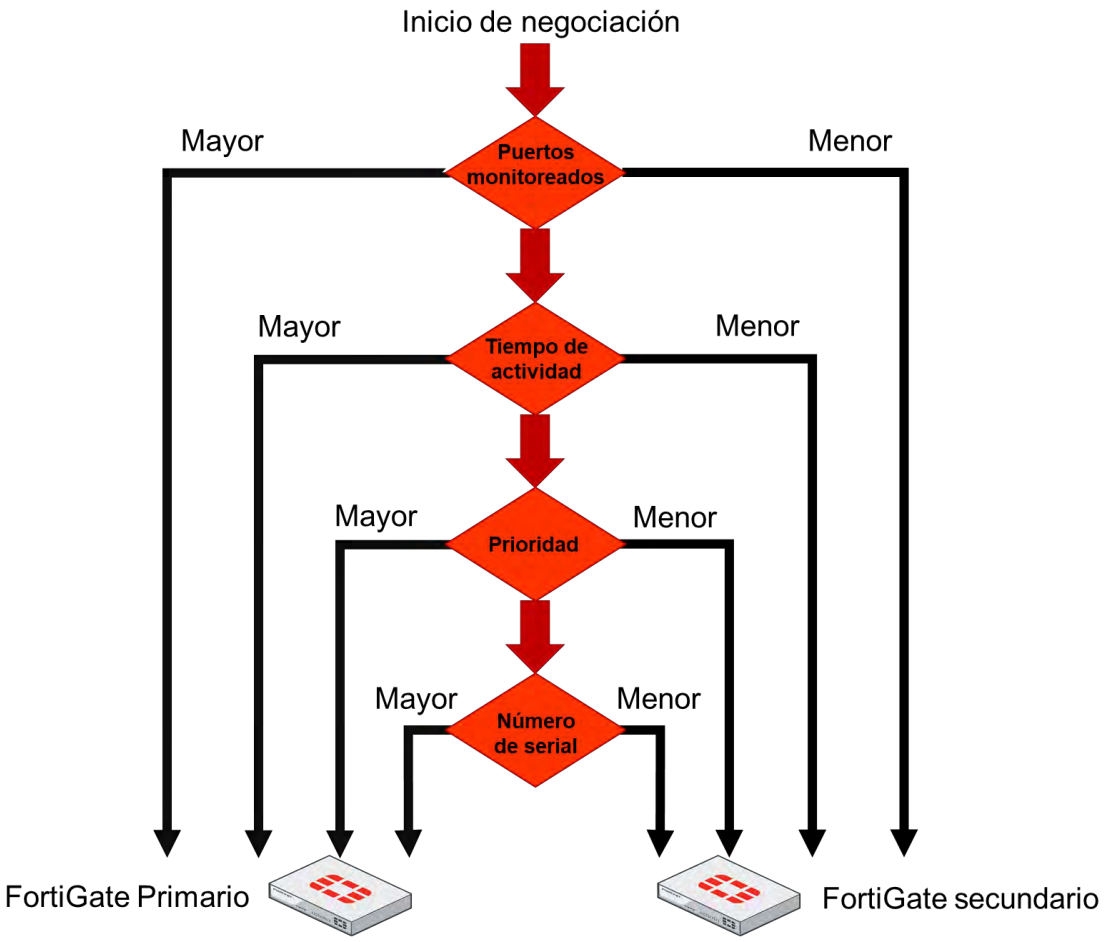


Figura 3-51. Elección de un FortiGate primario

El proceso para elegir el FortiGate primario depende de una configuración de alta disponibilidad llamada anulación de alta disponibilidad (HA override), en la Figura 3-51, se muestra el proceso y selección de criterio que un clúster usa para elegir el FortiGate cuando el ajuste de anulación del HA es deshabilitado, el cual es el comportamiento por defecto. La selección del proceso se detiene en la primera coincidencia del criterio que fue exitoso al seleccionar un FortiGate primario dentro de un clúster [11].

El proceso que un clúster compara se describe a continuación:

- El clúster primero compara el número de interfaces monitoreadas cuyos estatus están arriba. Los dispositivos FortiGate con la mayoría de las interfaces supervisadas disponibles se convierten en las principales.
- Lo siguiente es comparar los tiempos de actividad en el clúster, si el tiempo de actividad del sistema de un dispositivo es cinco minutos más que el tiempo de actividad de otro FortiGate, se convierte en el primario.
- Luego, el FortiGate va a comparar la configuración con la mayor prioridad, ese FortiGate se convertirá en el primario.

- Si el clúster no encuentra coincidencia en ningún punto anteriormente mencionado, al final los equipos FortiGate escogerán el primario comparando los números de serial.

Cuando él HA override es deshabilitado, el tiempo de actividad tiene preferencia sobre los ajustes de prioridad, si por alguna razón, es necesario cambiar el dispositivo actualmente primario, se puede manualmente forzar un evento failover. Cuando el ajuste de anulación es deshabilitado, la manera más fácil de hacer esto es ejecutando el siguiente comando CLI en el FortiGate primario: *diagnose sys ha reset-uptime* [11].

El comando para resetear el tiempo de actividad, va a reiniciar la edad interna del HA y no afectará el tiempo de actividad mostrado en el tablero principal del FortiGate. Además, si una interfaz de monitoreo falla, o un FortiGate en un clúster se reinicia, el tiempo de actividad para el FortiGate se resetea a 0 [11].

Es posible alterar el orden de la selección del criterio que los clústeres consideran cuando se selecciona el FortiGate primario, como se muestra en la Figura 3-52, si el ajuste de anulación del HA es habilitado, la prioridad es considerado antes que el tiempo de actividad [11].

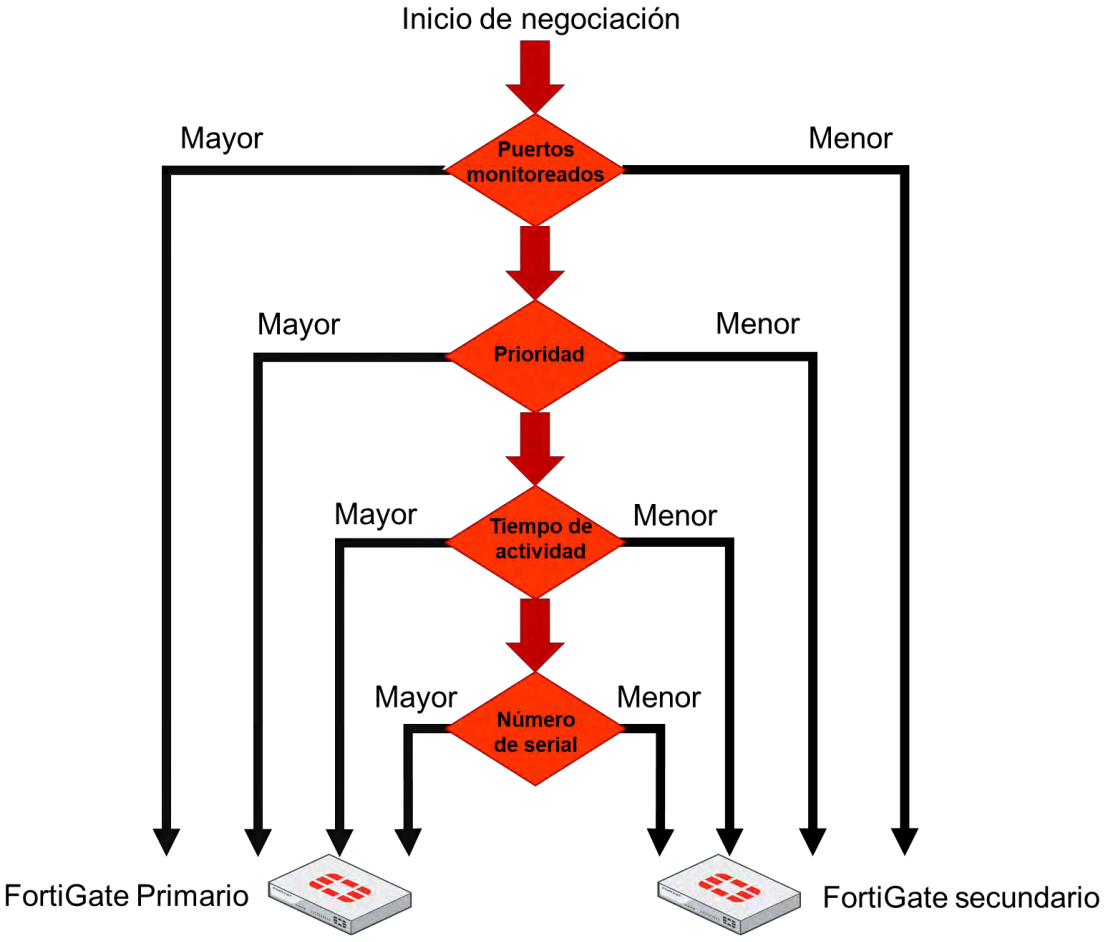


Figura 3-52. Alteración para la elección de un FortiGate primario

La ventaja de este método es que se puede especificar que dispositivo es preferido para ser el primario cada vez (mientras esté en funcionamiento) que se configura con el valor de prioridad de HA más alto. La desventaja es que el evento failover es disparado no solamente cuando falla el dispositivo primario, también cuando el equipo primario es disponible de nuevo. Cuando un dispositivo primario se convierte en disponible de nuevo, toma su lugar como el rol primario desde el FortiGate secundario que temporalmente lo remplazo [11].

El comando para habilitar el override en el CLI es el siguiente: *#config system ha > set override enable > end*.

Cuando el override es habilitado, la manera más fácil de disparar el failover es cambiando la prioridad del HA, por ejemplo, es posible ya sea, incrementar la prioridad en uno de los equipos secundarios, o disminuir la prioridad en el primario. El ajuste override y el valor del dispositivo primario no son sincronizados para todos los miembros del clúster, es necesario habilitar el override y manualmente ajustar la prioridad, este ajuste es por cada miembro del clúster [11].

Las tareas del FortiGate primario es monitorear el clúster, enviando señales de hello y escuchando las respuestas, para determinar si otro FortiGate está vivo y disponible, de igual forma sincroniza la tabla de enrutamiento y parte de esta configuración a otros dispositivos. Opcionalmente se puede configurar el FortiGate primario para sincronizar alguna información de las sesiones de tráfico para todos los dispositivos secundarios, esto permite una rápida conmutación sin errores para algunas sesiones. Algunos usuarios no necesitarán restablecer sus sesiones después de un fallo del FortiGate primario. Solamente en el modo activo-activo del FortiGate, un equipo primario también distribuye el tráfico entre todos los dispositivos disponibles en el clúster [11].

Las tareas de los FortiGates secundarios en el modo activo-pasivo, simplemente esperan, reciben sincronizaciones de datos, pero no procesan ningún tráfico. Si el FortiGate primario falla, el secundario será elegido como el nuevo primario. En el modo activo-activo, el secundario no espera pasivamente, ellos procesan todo el tráfico asignado a ellos por el dispositivo primario [11].

3.12.2.- Enlace heartbeat

No son necesario configurarlas, el protocolo FGCP automáticamente van a negociar la dirección IP del heartbeat basado en cada número serial del dispositivo. La dirección IP 169.254.0.1 es asignado para el dispositivo con el mayor número de serial. La dirección IP 169.254.0.2 es asignado para el dispositivo con el segundo mayor número de serial, y así sucesivamente. La asignación de la dirección IP no cambia cuando un failover pasa, independientemente del papel del dispositivo, en cualquier momento (primario o secundario), su dirección IP virtual del heartbeat permanece igual [11].

Un cambio en la dirección IP del heartbeat puede suceder, cuando un dispositivo FortiGate se une o deja el clúster, en estos casos, el clúster renegocia la dirección IP asignada del heartbeat, esta vez teniendo en cuenta el número de

serial de cada dispositivo nuevo, o remover el número de serial de cualquier dispositivo que deja el clúster [11].

Hay algunos detalles que se necesita ser considerado cuando se conecta interfaces heartbeat y se configuran interfaces de monitoreo.

Los puertos heartbeat contienen información sensible acerca de la configuración del clúster y requieren una buena cantidad de ancho de banda para asegurar que la configuración está en estado de sincronización en todo momento. Es necesario tener al menos un puerto de tráfico heartbeat, preferiblemente dos. La comunicación del heartbeat puede ser habilitado por interfaces físicas, pero no para subinterfaces VLAN, interfaces VPN IPsec, interfaces redundantes, interfaces de agregación 802.3ad, o puertos de switch FortiGate. No se debe configurar puertos de monitoreo para puertos heartbeat dedicados [11].

Para prepararse para un failover, un clúster HA mantiene su configuración en sincronización. El FortiGate en HA usa una combinación de incremento y completa las sincronizaciones, cuando un nuevo FortiGate es agregado al clúster, el FortiGate primario compara su checksum con la configuración checksum del nuevo FortiGate secundario, si el checksum no coincide, el FortiGate sube su configuración completa hacia el FortiGate secundario, así como se muestra en la Figura 3-53.

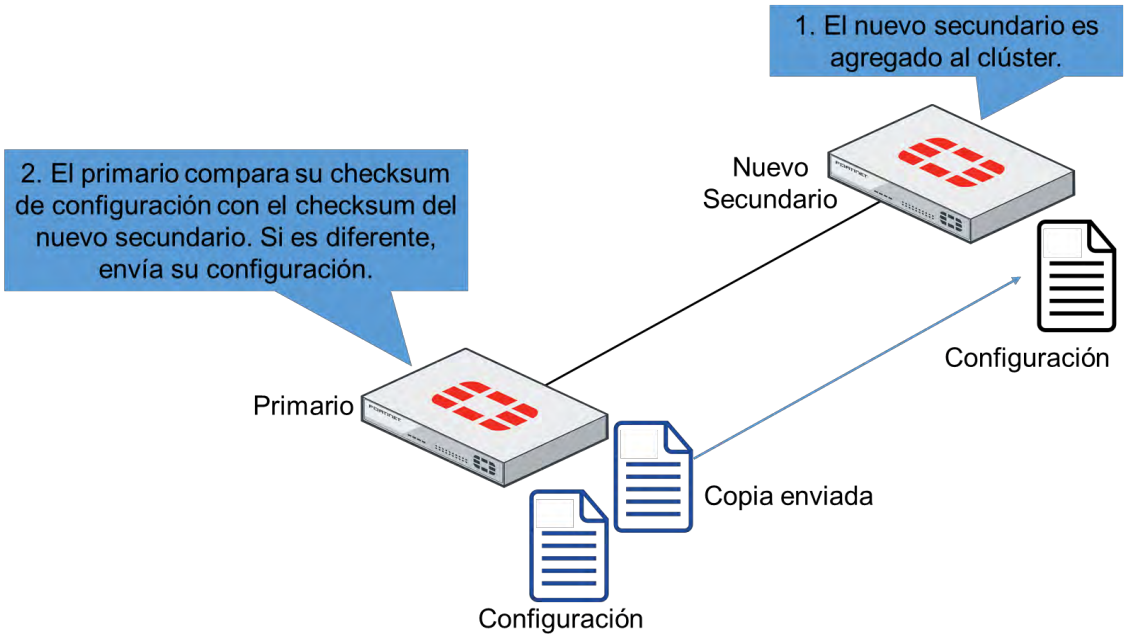


Figura 3-53. Sincronización de clúster HA

Después de que la sincronización inicial es completada, el FortiGate primario enviara cualquier cambio de configuración en un futuro a todos los otros equipos secundarios, por ejemplo, si se crea una dirección de objeto de firewall, el equipo primario no reenvía su configuración completa, solo envía el nuevo objeto creado [11].

Periódicamente, él HA es comprobado para la sincronización, por defecto, los clústeres checan la configuración cada 60 segundos para asegurar que todos los dispositivos están sincronizados, si algún equipo secundario se encuentra fuera de sincronización, el checksum del dispositivo secundario es entonces comprobado cada 15 segundos. Si los checksum no coinciden por cinco comprobaciones consecutivas, una re-sincronización completa es hecha [11].

No todo el ajuste de configuración es sincronizado, hay algunas que no lo son, como:

- Los ajustes de administración de las interfaces HA.
- La ruta por defecto del HA para la interfaz administrativa reservada.
- El override del HA.
- La prioridad del dispositivo del HA.
- La prioridad del clúster virtual del HA.
- El nombre de host del FortiGate.
- Los ajustes de prioridad del HA para la configuración del ping al servidor (o la detección del gateway caído).

El FortiGate primario sincroniza todos los otros ajustes de configuración, incluyendo otras configuraciones relacionadas a los ajustes HA [11].

La sincronización de sesiones permite la conmutación por error sin problemas para cierto tráfico. La información de algunas sesiones es sincronizada, de este modo cuando el primario falle, el nuevo primario puede tomar esas sesiones donde ellos se quedaron y mantenerlos abiertos. El tráfico puede ser interrumpido por algunos segundos, pero las aplicaciones de la red no necesitan reconectar las sesiones de nuevo [11].

Por defecto, algunas sesiones de sincronización son habilitadas, los dispositivos sincronizan el TCP y las sesiones VPN IPsec que cumplen con un requerimiento: ellos no pueden manipular un proxy UTM, como un antivirus o filtro web [11].

Para reenviar el trafico correctamente, una solución de FortiGate en HA usa dirección de MAC virtual. Cuando un dispositivo primario se une a un clúster HA, cada interfaz es dado a una dirección MAC virtual. Mediante los heartbeats, el primario informa a todos los secundarios acerca de la asignación de la dirección virtual de la MAC. Sobre el failover, un secundario adopta la misma dirección MAC virtual para la equivalencia de interfaces como se muestra en la Figura 3-54 [11].

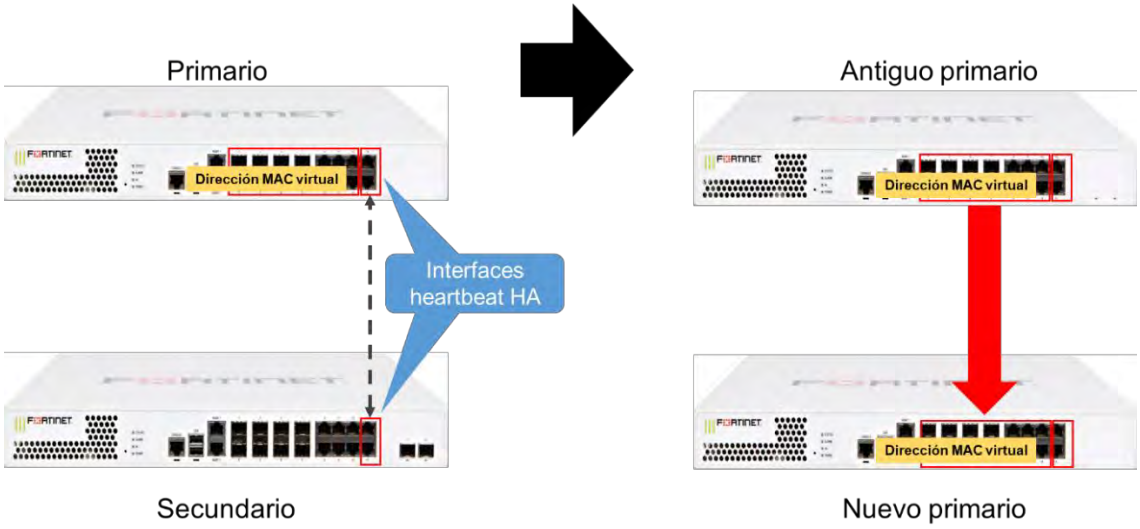


Figura 3-54. MAC virtual

Después de un failover, los paquetes ARP informan a la red por medio de broadcasts, que la dirección virtual MAC es ahora alcanzable a través de un diferente FortiGate [11].

Existen diferentes tipos de failover, los más comunes es cuando un dispositivo falla o el enlace que los interconecta falla. Un dispositivo con fallo es básicamente alarmado cuando el FortiGate primario para de enviar tráfico por el heartbeat, cuando esto pasa, el secundario inicia la renegociación como nuevo primario. Un enlace con fallo ocurre cuando el estado del enlace de una interfaz monitoreada en el FortiGate principal se cae. Es posible configurar un clúster HA para monitorear el estado del enlace de algunas interfaces, si una interfaz monitoreada en el FortiGate es desconectada, o el estado del link se cae, un nuevo FortiGate es elegido [11].

En la Tabla 24, se muestra como la carga de trabajo es distribuida entre los roles de cada equipo, dependiendo el modo del HA.

Tabla 24. Carga de trabajo entre los clústeres

Activo-pasivo	Activo-activo
El primario recibe y procesa todo el tráfico.	El primario recibe todo el tráfico.
El secundario espera pasivamente.	Redirige algo de tráfico a los secundarios.

La carga del tráfico no es distribuida en el modo activo-pasivo, pero si en el modo activo-activo.

3.12.3.- Actualización de firmware en HA y estados

Como un dispositivo único (standalone), cuando se actualiza un clúster HA, para cada actualización de dispositivo es necesario el reinicio. Como la actualización

interrumpible esta activada de manera predeterminada, el clúster actualiza el FortiGate secundario primero, una vez que todos los FortiGate secundarios están corriendo el nuevo firmware, un nuevo equipo primario es elegido y el firmware en el dispositivo primario es actualizado [11].

Para actualizar un clúster en HA, solo es necesario subir el nuevo firmware en el primario:

1. Si el clúster está operando en el modo activo-activo, el balanceo de cargas del tráfico es apagado.
2. El clúster sube el firmware en todos los dispositivos secundarios primero.
3. Un nuevo primario es elegido.
4. El clúster actualiza el firmware en el anterior primario.
5. Si el clúster está operando en el modo activo-activo, el tráfico de balanceo de cargas es iniciado.

Si un clúster HA se formó adecuadamente, el GUI muestra todos los FortiGates en el clúster, ambos con sus propios hostname, números de serial, rol o papel, y prioridades, como se muestra en la Figura 3-55 [11].

Figura 3-55. Monitor del clúster H.A

De igual forma es posible observar estadísticas, las cual permite ver el tiempo activo, sesiones activas y la utilización de la red. También se puede desconectar un miembro del clúster y editar configuraciones del HA.

Es posible obtener más información acerca de los estados del HA desde el CLI, por ejemplo, el comando *diagnose sys ha status*, muestra estadísticas del trafico heartbeat, así como se muestra en la Figura 4-56, tanto como el número de serial, y la prioridad HA de cada FortiGate. Este comando también muestra la dirección IP de la interfaz heartbeat que se es asignado automáticamente al FortiGate con el número de serial más alto [11].

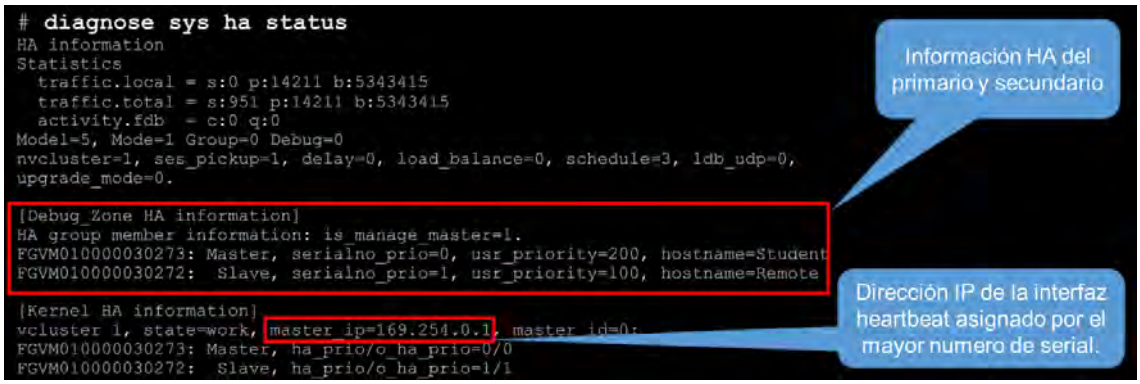


Figura 3-56. Comando de diagnóstico del HA

Hay que tener en cuenta, que la dirección IP del heartbeat asignado, cambia solamente cuando un FortiGate deja o se une a un clúster.

Cuando se tiene un problema en un clúster HA, es útil saber que se puede conectar al CLI de cada FortiGate secundario desde el CLI del FortiGate primario, se tiene que usar el comando: *execute ha manage*, con el índex del HA para ese propósito, como se muestra en la Figura 3-57.

- Usando el CLI del FortiGate primario, se puede conectar a cualquier CLI secundario con el comando:

```
# execute ha manage <HA_device_index>
```

- Para enlistar el numero de index por cada FortiGate, se usa el símbolo de interrogación:

```
# execute ha manage ?
<id>      please input peer box index.
<1>       Subsidary unit FGVM0100000xx
```

Figura 3-57. Comandos para la administración del HA

Otra indicación para ver el estado de la configuración de la sincronización de un clúster en HA, es con el comando: diagnose sys ha checksum, el cual proporciona tres opciones para verificar o recalcular el checksum del HA, el principal es el checksum, así como se muestra en la Figura 3-58 [11].

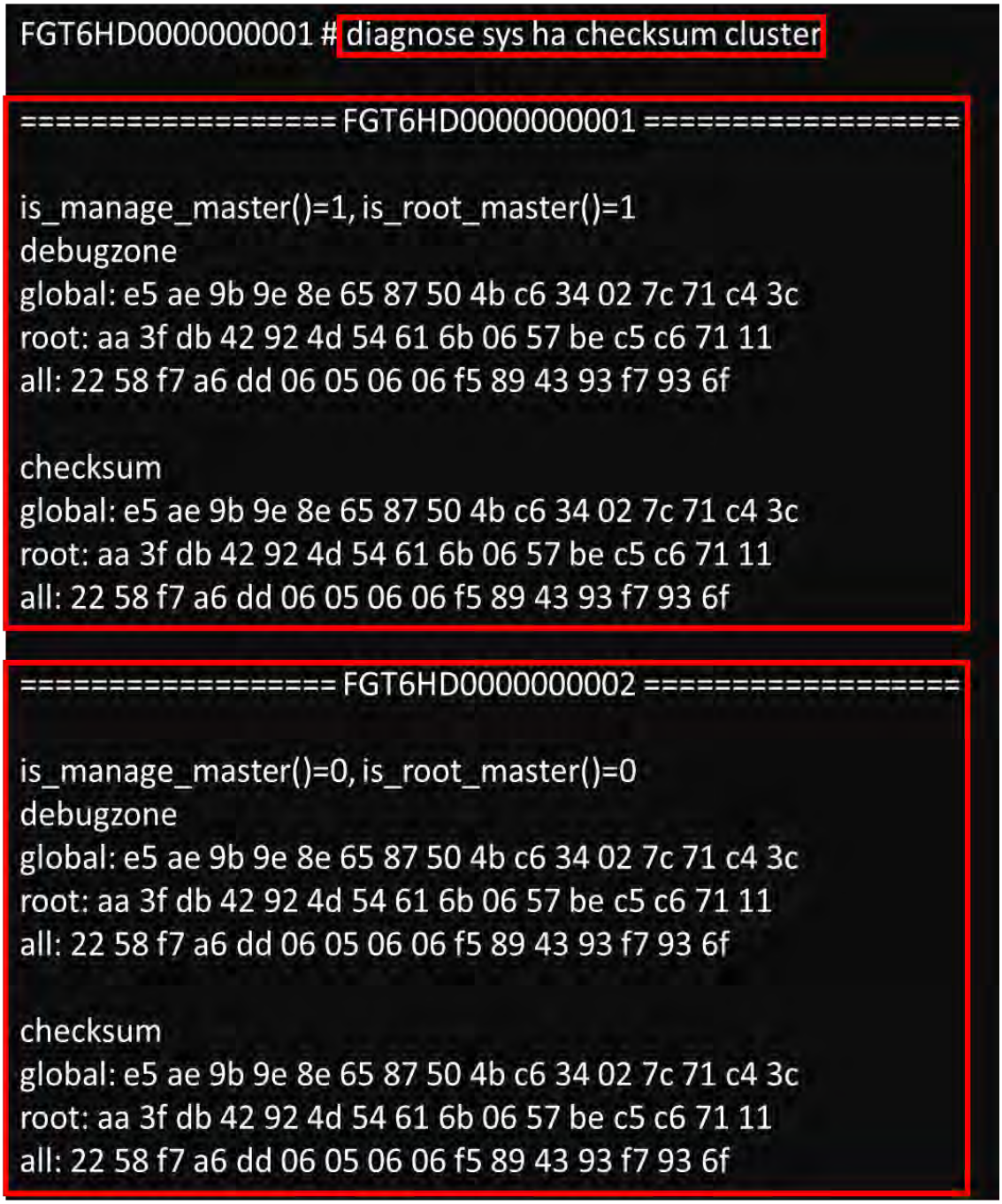


Figura 3-58. Comando para la verificación checksum del clúster

- El comando: *diagnose sys ha checksum*, verifica el checksum de todos los miembros del clúster.
- El comando: *diagnose sys ha show*, comprueba el checksum del FortiGate individual desde cualquier comando ejecutado.
- El comando: *diagnose sys ha recalculate*, recalcula el checksum del HA y puede ser ejecutado desde cualquier miembro del clúster.

Si un FortiGate secundario, enseña exactamente la misma secuencia de los números que el primario, la configuración está bien sincronizada con el FortiGate primario del clúster, como se ve en el ejemplo de la Figura 3-58. El Global, representa el checksum de la configuración global, como los administradores, los perfiles del administrador, los ajustes globales del logging, y los ajustes del FortiGuard, por nombrar algunos [11].

3.13.- IPS

Antes de empezar, es importante entender la diferencia entre una anomalía y un exploit, también es importante conocer que características de FortiGate ofrecen protección contra cada una de esos dos tipos de amenazas, así como se muestra en la Tabla 25.

Tabla 25. Exploit y anomalía

Exploit	Anomalía
Es conocido, ataque confirmado	Puede ser un ataque zero-day o denegación de servicios (DoS).
Detectado cuando un archivo o trafico coincide con un patrón de firma: • **Firmas IPS** • **Firmas de firewall de aplicaciones web** • **Firmas de antivirus**	Detectado por análisis de comportamiento: • **Basado en tasas de firmas de IPS** • **Políticas DoS** • **Inspección de restricciones de protocolo**
Ejemplo: Explotación de vulnerabilidades de aplicaciones conocidas.	Ejemplo: tasas de trafico normalmente altas (DoS/flood).

Los exploits son ataques conocidos, con patrones conocidos, que pueden ser coincidir por un IPS, aplicación de firewall web, o firmas de antivirus.

Las anomalías son usualmente encontradas en la red, como un alto uso de CPU o gran tráfico de red. Las anomalías deben ser detectadas y monitoreadas ya que ellos pueden ser el síntoma de algo nuevo, un ataque nunca antes visto. Las anomalías son usualmente mejor detectadas por un análisis de comportamiento, como una firma de IPS basado en tasas, políticas DoS, y por medio de la inspección de restricciones de protocolos.

Los exploits de vulnerabilidades desconocidas, llamados ataques de día cero (zero-day, son vendidas por mucho dinero en el mercado negro, desde que los exploits no son conocidos por el fabricante, o la seguridad experta, no hay parches disponibles o detección de firmas, eso hace que sean extremadamente peligroso.

Algunas compañías y organizaciones como Facebook y Google, ofrecen recompensas por la revelación de esos exploits, pero hay mucha rentabilidad en el mercado negro para los hackers de sombrero negro.

Un ataque de zero-day se refiere a cuánto tiempo los "chicos buenos" han conocido sobre un problema de seguridad en el software. Hay dos tipos de días cero. Una vulnerabilidad de día cero es un agujero en la seguridad del software y puede estar presente en un navegador o una aplicación. Un exploit de día cero, por otro lado, es un ataque digital que aprovecha las vulnerabilidades de día cero para instalar software malicioso en un dispositivo [14].

Pero, ¿Cómo puedes protegerte contra ataques de zero-day?

- Estudiar tu red desde la base de un comportamiento normal.
- Monitorear volúmenes de tráfico inusual y sus patrones.
- Bloquear el tráfico no necesario, las políticas de firewall deben permitir solamente las conexiones requeridas por aplicaciones.
- Aplicar restricciones de protocolos, como prevenir desbordamientos de buffer, cross-site scripting (CSRF), etcétera.
- Honeypots.

3.13.1.- Sistema de prevención de intrusión

El sistema de prevención de intrusión (IPS por sus siglas en ingles), usa firmas de base de datos para detectar ataques conocidos, las firmas del IPS pueden también ser usadas para detectar errores en la red y anomalías. Como la firma de la base de datos del AV, las firmas de la base de datos de un IPS son también actualizadas a través del FortiGuard [11].

El motor de un IPS es responsable de las características mostradas a continuación: protección de intrusos, decodificadores de protocolos y más. También es responsable para el control de aplicaciones, la protección del antivirus en el modo flow-based, filtrado web y filtro email [11].

Los protocolos decodificadores analizan cada paquete de acuerdo a las especificaciones del protocolo, algunos protocolos decodificadores requieren un número de puerto específico, pero usualmente (configurado en el CLI), el protocolo es automáticamente detectado. Si el tráfico no se ajusta a la especificación, por ejemplo, si se envía un comando malformado o inválido al servidor, entonces el protocolo decodificador detecta el error [11].

Por defecto, inicialmente son establecidas las firmas IPS en cada firmware de FortiGate liberado, el servicio de FortiGuard actualiza las firmas IPS, a veces diario con nuevas firmas, de esa manera, el IPS permanece efectivo contra nuevos exploits. A no ser que un protocolo específico de cambios en el RFC (el cual no es muy a menudo), el protocolo decodificador es raramente actualizado. El motor IPS cambia el mismo con más frecuencia, pero no a menudo [11].

Las firmas del IPS son a menudo actualizadas, las nuevas firmas son identificadas y construidas por los equipos de investigación del FortiGuard, como las firmas de los antivirus. Así que, si el contrato del servicio con el FortiGuard expira, aún es posible usar el IPS, sin embargo, solo como un escaneo de antivirus, el escaneo del IPS cada vez más se convierte en inefectivos si se deja

de actualizar, las viejas firmas no pueden defenderse contra nuevos ataques [11].

Cuando el FortiGate descarga paquetes IPS de FortiGuard, las nuevas firmas aparecen en una lista de firmas, cuando se está configurando el FortiGate, se puede cambiar el ajuste de acción para cada sensor que usa una firma, un ejemplo es como se muestra en la Figura 3-59.

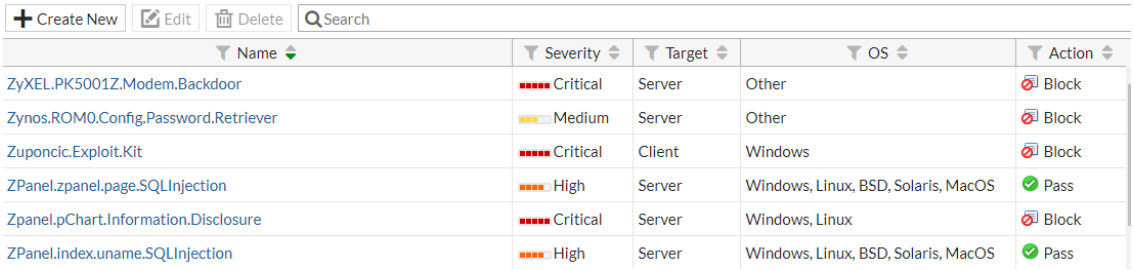


Figura 3-59. Firmas

El ajuste de la acción es a menudo correcto, excepto en estos casos:

- Algún software de un fabricante libero un parche de seguridad, el seguir escaneando exploits desperdiciará recursos del FortiGate.
- La red tiene una aplicación personalizada con tráfico que reacciona a los motores del IPS. Así que se puede deshabilitar el ajuste hasta que se notifique a Fortinet y el FortiGuard pueda modificar la firma para evitar falsos positivos.

Los niveles severos de cada firma son también enlistados en la lista de las firmas IPS [11].

Si no se está seguro si se debe habilitar una firma de IPS en el FortiGate, se puede buscar en la enciclopedia del sitio web del FortiGuard como se muestra en la Figura 3-60 [11].

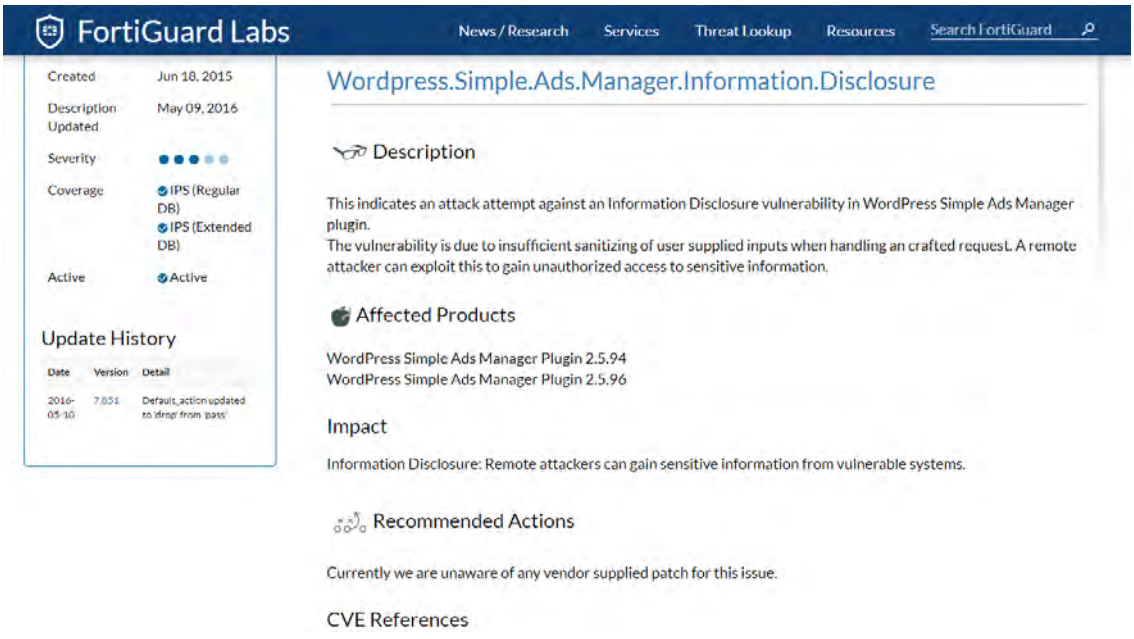


Figura 3-60.Enciclopedia FortiGuard

La enciclopedia contiene información útil, como sistemas afectados y recomendaciones de acciones correctivos. Así que, si no usas el protocolo o no tienes una vulnerabilidad del sistema, se puede deshabilitar sin peligro la firma correspondiente. Pero si tienes una vulnerabilidad, la enciclopedia puede darte información acerca de cómo protegerte tú mismo. La enciclopedia de FortiGuard solo contiene vulnerabilidades públicas reveladas, no contiene vulnerabilidades que no puedan ser de responsabilidad pública, independientemente de la razón [11].

Hay maneras de agregar firmas predefinidas para un sensor IPS. Una manera es el de seleccionar las firmas individuales como se muestra en la Figura 3-61 [11].

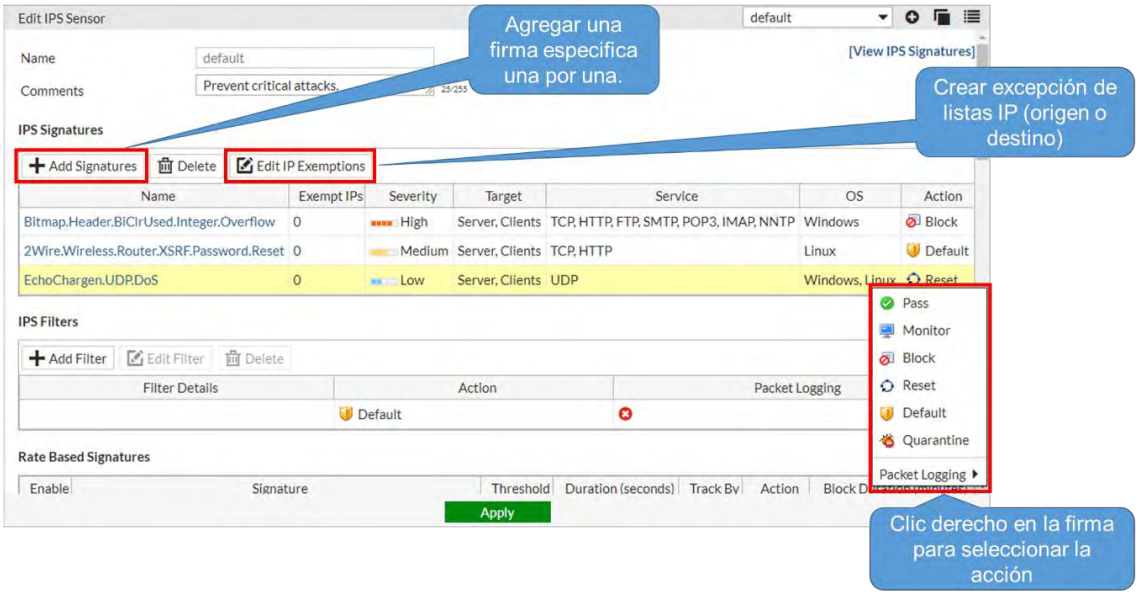


Figura 3-61. Firmas individuales

Cuando se usa este método, se puede crear una excepción de listas basadas en la dirección IP de origen o destino. Una vez que la firma fue seleccionada desde la lista, es agregada al sensor con la acción que lleva por defecto. Después de eso, se puede hacer clic derecho en la firma y cambiar la acción.

La segunda manera es agregar firmas a un sensor que esté usando filtros. FortiGate agregara las firmas que coincidan con los filtros. En la Figura 3-62, hay un ejemplo donde se crea un filtro para incluir todas las firmas que protegen al servidor Apache corriendo sobre un sistema operativo Linux. La acción es establecida para bloquear todo el tráfico que coincida con esas firmas.

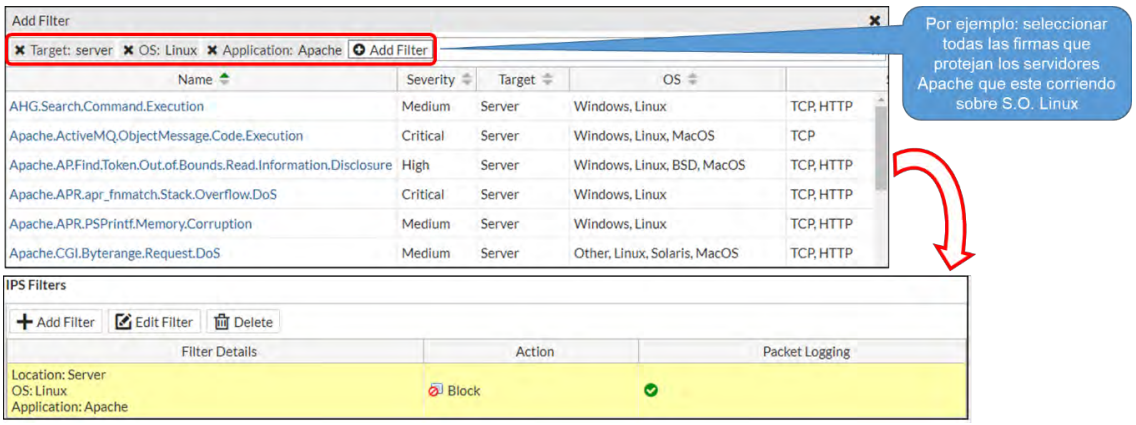


Figura 3-62. Filtro de búsquedas de firmas

Cada firma individual puede incluir múltiples etiquetas, como HTTP, Microsoft, ISS, y TCP. Para ser más específicos, se puede crear filtros, para disminuir recursos que serán usados para escanear el tráfico. Esto es porque las partes de las firmas raramente coincidirán con el tráfico, de este modo, el motor IPS puede rápidamente continuar con la siguiente comparación o escaneo [11].

Para aplicar un sensor IPS, es necesario habilitar el IPS y seleccionar el sensor en la política de firewall donde quiere que se aplique el tráfico.

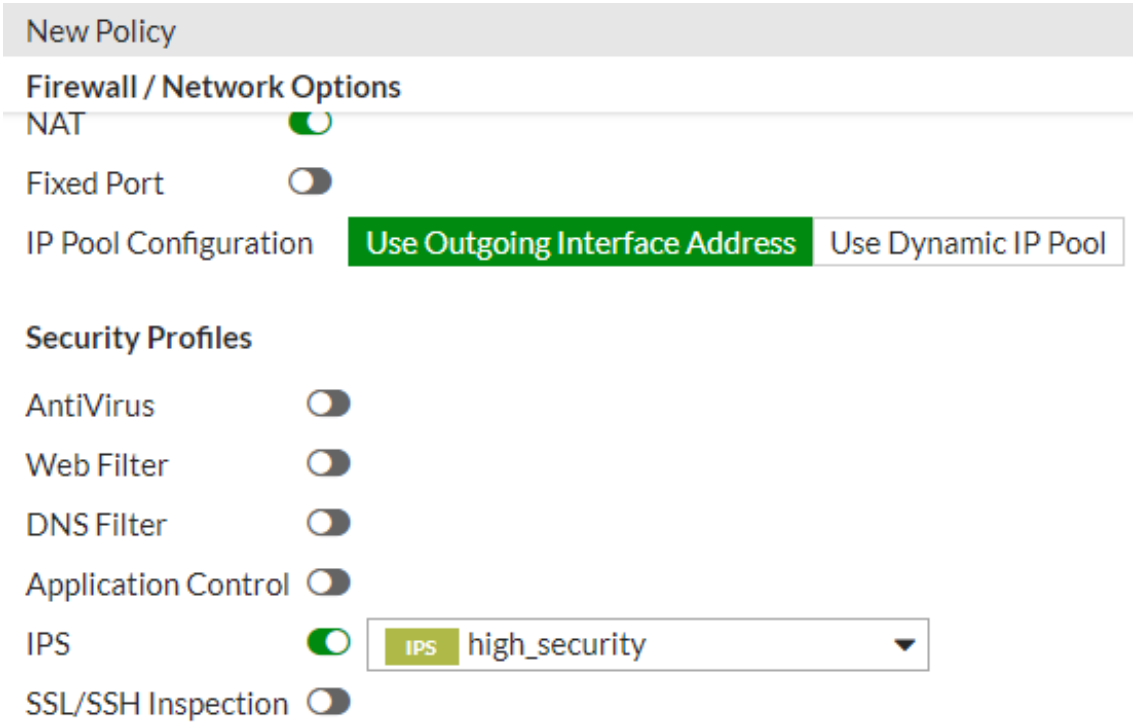


Figura 3-63. Habilitar sensor IPS en la política de firewall

La Figura 3-63, es un ejemplo de cómo se habilita el sensor en la política.

Capítulo 4 : Implementación de la Solución de Datos y Seguridad

4.1.- Levantamiento y Planeación

Un proyecto de gran magnitud, tiene diversas fases para su implementación, primero, el equipo comercial se acerca con el cliente de la institución, se hace un levantamiento con el equipo de arquitectura y se da una posible solución para sus problemas de red.

La empresa cliente, ha adquirido un gran equipo modular, como se aprecia en la Figura 4-1, el cual, es un equipo HPE 3PAR entre otros dispositivos; donde el cliente aloja sus diversos servidores de forma virtualizada. Sin embargo, la comunicación entre el router principal y el equipo 3PAR, son por medio de un cable ethernet 100/1000 Mbps, por tal motivo, no están explotando las capacidades del gran equipo con el que cuentan.

Figura 4-1. Equipo HPE 3PAR

Una vez que se ha concretado la compra del equipo antes mencionado, el equipo eléctrico verifica la correcta instalación. En este proyecto, fueron necesarios varias modificaciones electricas, en el cual se adquirieron equipos de respaldo de la energía eléctrica. Cuando el equipo eléctrico da el visto bueno de las instalaciones, se empieza las adecuaciones para que el equipo de datos y seguridad (donde actualmente nos encuentramos laborando), pueda empezar con la estrategia para la instalación y configuración de los equipos.

4.1.1.- Levantamiento de arquitectura

El equipo de arquitectura nos proporciona el primer levantamiento y la adquisición de los equipos, el cual se muestra a continuación. La sección de ingeniería en el área de datos, se describe en la Tabla 26:

Tabla 26. Alcances de los equipos de datos

Equipo	Descripción de la instalación
Switch Cisco Core 4500E	**Alcances:** 1. Montaje y configuración del equipo incluyendo: Armado de equipo, instalación en rack, armado de stack. 2. Configuración de una I.P. en el Switch. 3. Configuración de hasta 5 Vlan en el Switch. 4. Configuración del equipo incluyendo: Configuración del sistema conforme a la topología y direccionamiento proporcionado. 5. Conexión hacia dispositivos de red y servicios en panel de parcheo. 6. Pruebas de operación. 7. Entrega de memoria técnica. 8. Incluye transferencia de conocimientos. **Pre requisitos del Servicio:** 1. El cliente deberá definir la topología y direccionamiento que se va a configurar. **No incluye:** 1. Instalación y/o configuración de cualquier otro componente de la red (PC, servidor, impresora, teléfono, AP´s, etc.) 2. Cableado eléctrico, tierra física o de datos. 3. Conexión de servicios del lado del usuario. 4. No incluye configuración avanzada del software de monitoreo Cisco Prime Infraestructura.

16 equipos Switch Cisco 2960X	1. Montaje y configuración del equipo incluyendo: Armado de equipo, instalación en rack, armado de stack 2. Configuración del equipo incluyendo: Configuración del sistema conforme a la topología y direccionamiento proporcionado. 3. Conexión hacia dispositivos de red y servicios en panel de parcheo. 4. Pruebas de operación. 5. Entrega de memoria técnica. 6. Incluye transferencia de conocimientos. **Pre requisitos del Servicio:** 1. El cliente deberá definir la topología y direccionamiento que se va a configurar. **No incluye:** 1. Instalación y/o configuración de cualquier otro componente de la red (PC, servidor, impresora, teléfono, AP´s, etc.). 2. Cableado eléctrico, tierra física o de datos. 3. Conexión de servicios del lado del usuario.

La sección de ingeniería en el área de seguridad, se describe en la Tabla 27:

Tabla 27. Alcances de los equipos de seguridad

Equipo	Descripción de la instalación
FortiGate 600D	**Alcances:** 1. Incluye instalación física de 2 equipos FG-600D en H.A. (protección de site central de la organización). 2. Instalación de los siguientes servicios para el FG-600D en H.A: FW, VPN, AV, APCL, IPS, Web Filtering, AS. 3. Incluye transferencia de conocimientos a 3 administradores. 4. Registro de los Appliance en el portal Web del fabricante. 5. Actualización de firmware a la última versión estable. 6. Pruebas de funcionalidad sobre servicios habilitados. 7. Entrega de memoria técnica. 8. Acta de entrega de culminación de trabajos. 9. Incluye planeación y diseño.

Las consideraciones comerciales se describen en la Tabla 28:

Tabla 28. Consideraciones comerciales

No.	Consideración
1	Se incluyen en las horas de servicio los materiales mixtos necesarios para el servicio.
2	No se incluyen revisiones a sistemas operativos, kernel, configuraciones u otros servicios diferentes a los especificados en el alcance.
3	Se recomienda que el cliente o usuario final cuente con garantía de soporte técnico por parte del fabricante.
4	No se incluye revisiones al sitio de comunicaciones ni a otros subsistemas.
5	No se incluye la configuración de extensiones o la instalación de equipos o sistemas adicionales.
6	Debe confirmarse el servicio con al menos 2 semanas de anticipación
7	No se incluye servicios de arquitectura o de validación de compatibilidad de HW.

De igual forma, se entregó por parte del área de arquitectura, un diagrama físico de la propuesta que se le dio a conocer al cliente, como se ve en la Figura 4-2.

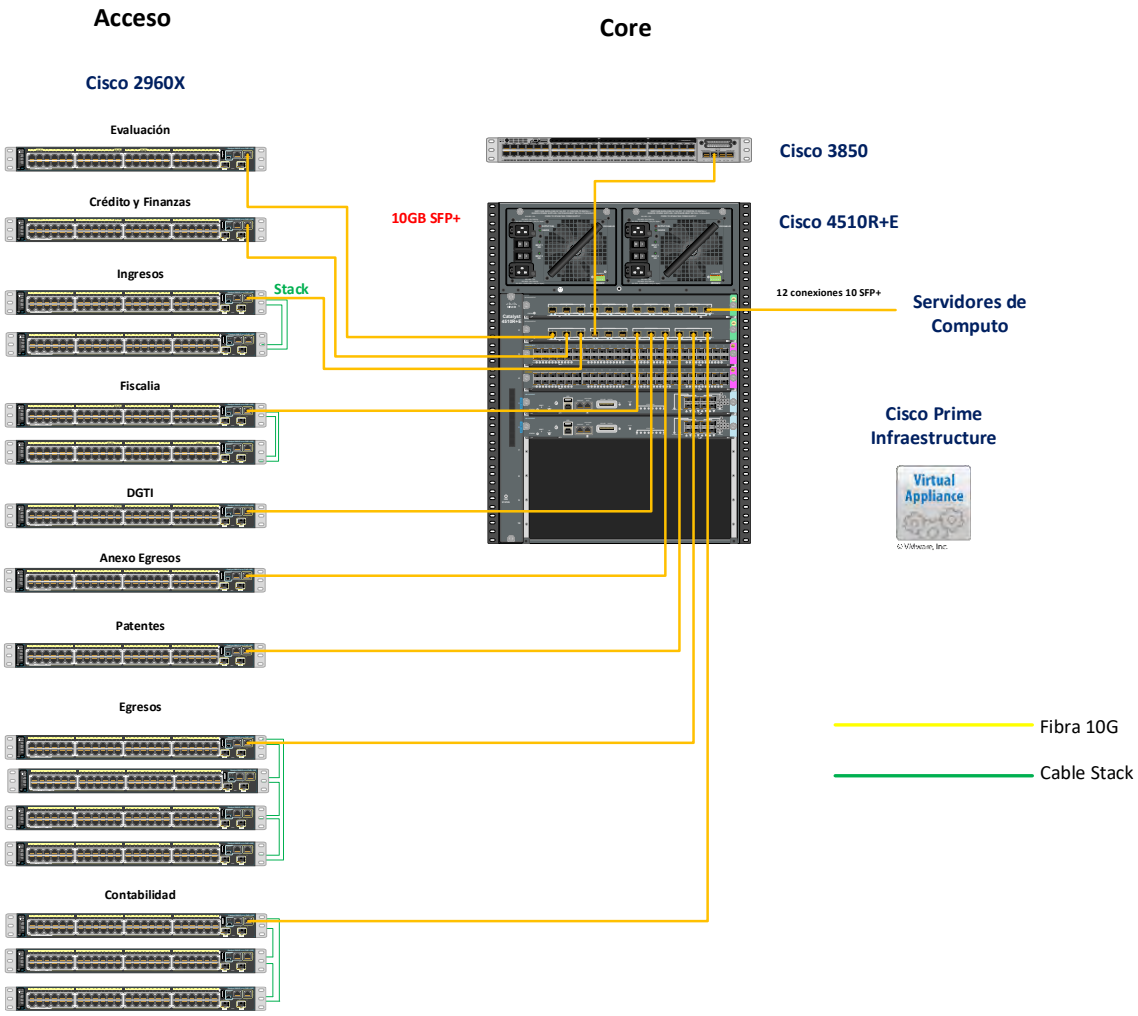


Figura 4-2. Diagrama físico del area de arquitectura

De esta forma, el área comercial y el área de arquitectura concluyen con su parte en el proyecto.

4.1.2.- Levantamiento y planeación por parte del área de ingeniería

Ahora es nuestro turno, lo primero fue tener un acercamiento con los gerentes y el personal de la parte técnica para el levantamiento de la red actual.

Se realizó un levantamiento en toda la organización observando todos los IDF's y el MDF; en las Figuras 4-3, 4-4, 4-5, 4-6 y 4-7, se muestra el recorrido en algunas partes de los IDF's de la institución.

Figura 4-3. IDF (1)

Figura 4-4. IDF (2)

Figura 4-5. IDF (3)

Figura 4-6. IDF (4)

Figura 4-7. IDF (5)

Durante esta actividad se pudo observar que los switches de los IDF's son de diferentes marcas y de diferentes modelos, algunos de ellos no son posibles administrar, por consiguiente, solo otorgan funcionalidades mínimas, pero es necesario algunos requerimientos como hacer un tag en los puertos para la telefonía sobre la red de datos.

Cabe mencionar que la organización tenía poco tiempo de haber adquirido un nuevo conmutador y varios teléfonos IP, de los cuales solo funcionaban en switches donde eran administrables.

En el MDF se identifican dos equipos switch Cisco capa 3 que cumplen la función de Core, los cuales se encuentran en alta disponibilidad mediante un protocolo que solo permite esquema activo-pasivo, sin embargo, en caso de falla es

necesario hacer cambios físicos en los puertos ya que las conexiones a otros equipos solo se encuentran en uno de los switches, esto debido a que juntos suman solo 36 puertos Ethernet.

Para la parte de seguridad se cuenta con un FortiGate 500A que tiene una versión de firmware muy antigua, lo que lo hace vulnerable a ataques muy sofisticados que se encuentran en la actualidad, además que el equipo físico también es bastante antiguo y obsoleto, de esta forma no cuenta con soporte del fabricante. Este firewall también tiene la función de interconectar módulos u oficinas remotas a través de VPN, la VPN implementada está configurada con versiones de autenticación y cifrado bastante antiguas, debido al que el firmware también es antiguo.

Una vez que se tiene el levantamiento, se hace una planeación para acometer el proyecto, entre ellas se describe los alcances y la propuesta para la implementación de los nuevos equipos.

A continuación, se describe el alcance para este proyecto que contempla la instalación y sustitución de equipos primordiales que durante la ejecución podrán afectar la operatividad normal de la institución.

El proyecto de la implementación de datos y seguridad comprende la instalación y puesta a punto de los siguientes equipos:

1. FortiGate 600D en H.A
    a. Proveer mediante el Clúster H.A alta disponibilidad a fallas.
    b. Publicar servidores web.
    c. Proveer acceso a internet de manera segura a los usuarios locales y remotos.
    d. Concentración de VPN de los sitios remotos.

2. Switch Core Cisco 4500
    a. Ruteo entre las redes locales.
    b. Interconexión a switches de IDF.
    c. Interconexión a Blade VMWare.

3. 16 Switches de acceso 2960X
    a. Proveer nodos de acceso a usuarios finales a servicios de red y telefonía

Una vez que el levantamiento y los alcances están listos, continuamos con la propuesta.

Esta propuesta se divide en tres partes, la parte del switch Cisco Core, los switches de acceso y el firewall perimetral.

Para la parte del switch Core de datos se describe lo siguiente:

El Core de la red está conformado por un switch Cisco 4500 con 24 puertos de fibra SFP+ de 10G y 96 puertos RJ45. Se cuenta con dos supervisoras que ofrecen alta disponibilidad para asegurar la continuidad del servicio.

Este equipo cumplirá las siguientes funciones principales:

- Interconexión en capa dos hacia los IDF's del edificio.
- Interconexión de la infraestructura VMWare mediante 12 fibras de 10G.
- Ruteo entre las redes de los IDF's.
- Otorgar mediante ruteo los servicios del Firewall.

En la Tabla 29, se presentan las redes que serán creadas como interfaces VLAN:

Tabla 29. Propuesta de direccionamiento

Vlan ID	IP/Mask	Nombre	Dirmto.
2	10.9.2.254/24	Datos 1	Estático
3	10.9.3.254/24	Datos 2	Estático
4	10.9.4.254/24	Datos 3	Estático
5	10.9.5.254/24	Datos 4	Estático
6	10.9.6.254/24	Datos 5	Estático
250	172.16.250.254/24	ADM Switches	Estático

En la Tabla 30, se describen las redes que se usaran para interconectar a otros servicios mediante el ruteo, estos segmentos se asignan a la interfaz indicada en modo capa 3:

Tabla 30. Propuesta de redes para la interconexión

Interfaz	IP/Mask	Nombre
Gi 0/0	10.9.1.254/24	Enlace MPLS
Gi 0/1	10.9.251.254/24	Enlace a Firewall

La Tabla 31, describe el ruteo de redes que el switch Core deberá proveer:

Tabla 31. Propuesta del enrutamiento de redes del switch Core

IP/Mask	Destino	Tipo	Distancia Adm.	Descripción
0.0.0.0/0	10.9.251.1	Estático	1	Ruta por defecto
10.0.0.0/8	10.9.1.252	EIGRP	170	Sitios remotos por MPLS
10.0.0.0/8	10.9.251.1	OSPF	100	Sitios remotos por VPN

El acceso a las redes de los sitios remotos será otorgado por dos medios; el enlace MPLS que se encuentra en cada sitio y una VPN sobre un enlace de internet local, la manera principal de llegar al sitio deberá ser por la VPN ya que esta cuenta con mayor velocidad, la VPN será accesible a través del firewall, el cual estará publicando los sitios con VPN activa mediante OSPF hacia el switch Core.

El switch Core debe usar una distancia administrativa para OSPF menor que EIGRP para que prefiera usar las rutas otorgadas por el firewall en vez del enlace MPLS.

El siguiente diagrama lógico de conexión representa la interconexión de entre el switch Core y los equipos que le permiten enrutar hacia servicios externos.

La empresa cuenta con varios sitios remotos (MPLS), y en cada sitio tienen un router Cisco, configurados por otro proveedor, que usan el protocolo de ruteo EIGRP externo, esto significa que tiene una distancia administrativa de 170, sin embargo, cuenta con velocidades demasiado lentas, enlaces dedicados desde 256 kbps hasta un máximo de 2 Mbps, estos enlaces son intermitentes ya que se caen con frecuencia y abruman el trabajo de la organización. Una solución son las VPN's IPsec Site-to-Site basado en enrutamiento. En cada sitio donde hay un router cisco, también hay un FortiGate de gama baja, que tiene la capacidad para comunicarse por medio de VPN's con el FortiGate central del sitio principal. Estos enlaces VPN estarán interconectados, y el FortiGate central se comunicará con el Switch cisco principal por medio del protocolo OSPF, ya que, al ser de equipos con diferentes tecnologías, este protocolo viene siendo el más óptimo para este trabajo, además tendrá una distancia administrativa de 100, el cual otorgará preferencia por los enlaces VPN, teniendo el enlace MPLS como unas rutas de respaldo, el diagrama final quedaría como se ve en la Figura 4-8.

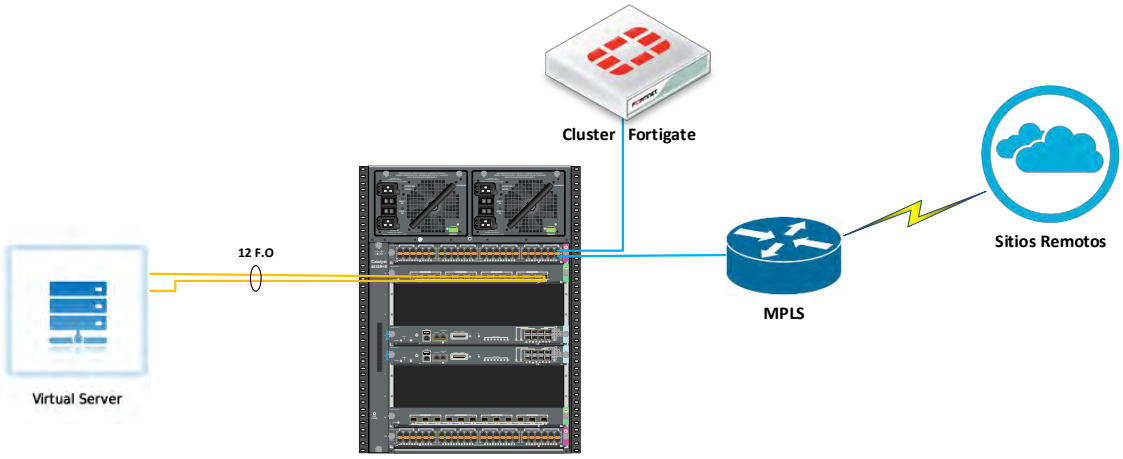


Figura 4-8. Diagrama final de la propuesta

Ahora bien, vamos con la parte de los switches de acceso. Para la conexión de los usuarios a la red se cuentan con 16 switches Cisco de acceso de última

generación que ofrecen conectividad a velocidad de GigabitEthernet, los cuales son completamente administrables y ofrecen protocolos de capa 2 que facilitan la gestión y otorgan seguridad a nivel de puertos físico.

Este equipo cumplirá las siguientes funciones principales:

- Interconexión hacia capa de Core.
- Provee acceso a la red de datos.
- Provee acceso a servicios de telefonía IP.

Los switches darán acceso a la red de datos correspondiente al IDF en el que se encuentre, esta distribución de la red ya está establecida por el cliente y debido a que se usa direccionamiento estático se debe respetar.

La tabla 32 indica la configuración de VLAN's para los IDF:

Tabla 32. Propuesta de VLAN's para los IDF's

VLAN	Nombre	Modo	IP
1 a 6	DatosIDF[X]	Untag	N/A
400	Voz	Tagged	N/A
250	AdminSW	Tagged	172.16.250.[X]

Donde la X representa el número del IDF en cuestión, por la naturaleza de la división de redes realizada por el cliente, algunos IDF pueden compartir la misma VLAN de datos.

Para evitar la generación de bucles que puedan afectar el desempeño de la red se contempla la habilitación de PortSecurity en todos los puertos de los switches de acceso. A continuación de listan los requerimientos específicos:

- Permitir máximo dos dispositivos por puerto.
- Habilitar PortFast.
- Activar BPDUGuard para evitar la conexión de switches no contemplados en la topología.

El la Figura 4-9, se propone el diagrama topológico, el cual describe la distribución de los switches dentro de los IDF, así como la asignación de la VLAN de datos.

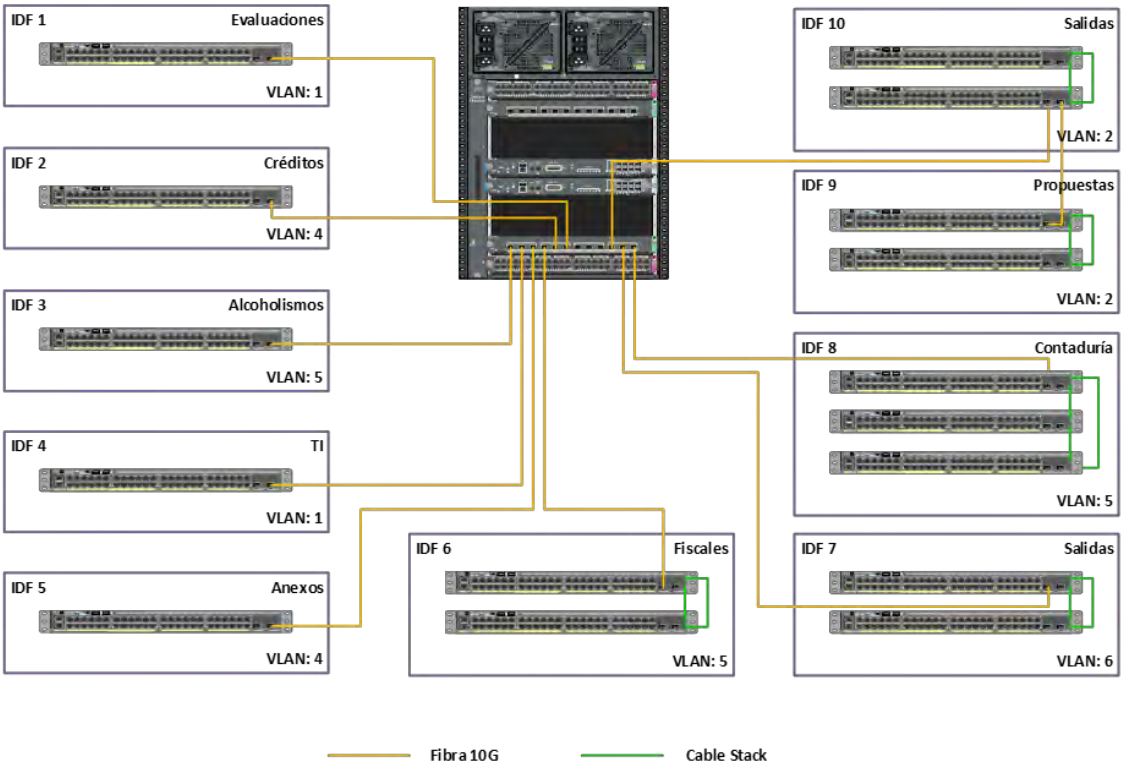


Figura 4-9. Diagrama físico de la propuesta

Para terminar esta fase, pasamos con la parte del firewall perimetral. En la periferia hacia Internet se contempla un firewall FortiGate 600D en alta disponibilidad que tendrá tres funciones principales; publicar servicios hacia internet, dar acceso seguro a los usuarios y concentrar las VPN's de los sitios remotos donde ya se cuenta con un equipo configurado.

La navegación de usuarios estará sujeta a los filtros web y de aplicaciones para evitar mal uso del servicio, también se aplicará inspección de antivirus, con esto se pretende reducir la posibilidad de alguna infección o ataque proveniente de las estaciones de trabajo de los usuarios.

La publicación de servidores será inspeccionada por el IPS y el antivirus.

El firewall provee acceso a los sitios remotos a través de una VPN, aunque existe otra manera de llegar a los sitios remotos que controla el switch Core, la VPN será en enlace principal por el que se alcancen, la cual será de tipo Site-to-Site en modo interfaz ya que ofrece estabilidad y trasparencia en el ruteo.

En la Tabla 33, se indica la asignación de segmentos del FortiGate:

Tabla 33. Propuesta de los segmentos del FortiGate

Interfaz	Nombre	IP/Mask
Port1	WAN1	IP Publica estática

Port2	WAN2	IP Publica estática
Port3	WAN3	DHCP
Port4	Enlace policía	10.33.7.4/24
Port5	Enlace Gb.	10.1.11.253/24
Port6	Enlace SW Core	10.9.251.1/24

Para proveer el filtrado de contenido a los usuarios se tienen las siguientes consideraciones actuales que se mantendrán después de la implementación:

- El direccionamiento IP de las redes de datos es estático.
- El Firewall 500A en producción ya tiene dado de alta a todos los usuarios los cuales están agrupados por departamentos

El equipo actualmente ya tiene definidos perfiles de aplicaciones y filtrado web, sin embargo, debido al cambio de versión las clasificaciones han cambiado, por lo que se crearan nuevos perfiles equivalentes que mantengan las restricciones actuales.

Se tienen dos funciones principales que cumplen las VPN's en el esquema actual; conectar a dos bancos y ser un enlace principal hacia las oficinas/departamentos remotos, todo mediante VPN's Site-to-Site en modo interfaz.

Las VPN hacia los bancos se mantendrán de la misma manera, para que el cambio sea trasparente. Las que conectan a los sitios remotos serán reconfiguradas en modo interfaz de manera que se pueda correr OSPF dentro de la VPN, de esta manera el FortiGate mantendrá el ruteo solo a los sitios que sean alcanzables por este medio.

Se cuenta con tres enlaces de internet, dos son para publicación de servicios y uno para la navegación de usuarios, el comportamiento del ruteo hacia internet cumplirá los siguientes puntos:

- Se definirán las tres rutas por defecto haciendo ECMP.
- Los servidores publicados deben salir a internet por el mismo enlace y con la misma IP.
- Los usuarios solo deben salir a internet por el enlace de infinitum.

El ruteo entre el Firewall y el Core será implementado por medio de OSPF, el firewall deberá publicar la ruta por defecto al Core, siendo que las interfaces de estos equipos pertenecerán al área 0.

La VPN hacia los sitios remotos también correrá OSPF, mediante el área backbone, esto permitirá que los sitios remotos conozcan las redes locales y se puedan sumarizar.

En cuanto a las redes que se alcanzan por MPLS, será el Core el encargado de realizar la redistribución de las rutas por EIGRP hacia OSPF.

En la Figura 4-10, se propone el diagrama de conexión que describe la interconexión del Clúster FortiGate hacia la red local y los servicios externos.

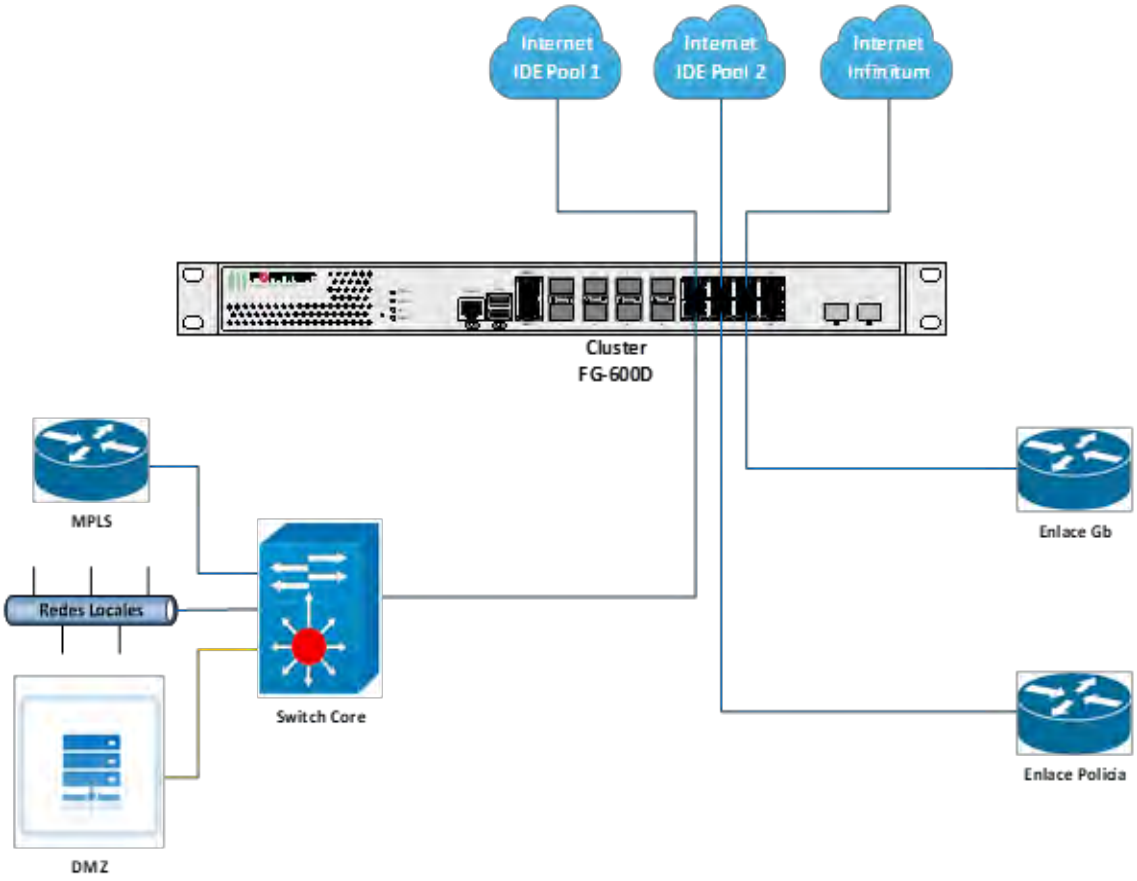


Figura 4-10. Interconexión final de la propuesta

De esta manera, completamos las tres partes de la propuesta, el switch Core, los switches de acceso para los usuarios y el firewall perimetral.

Una vez que está listo la propuesta, lo siguiente es elaborar un plan de trabajo que se le presentará al cliente.

Para este proyecto, se crearon dos planes de trabajo, uno para los equipos de Cisco que viene siendo el área de datos, y otro plan de trabajo para el área de seguridad que en este caso es para el equipo de Fortinet el FortiGate 600D.

Primero empezaremos con el plan de trabajo que se presentará al cliente para el switch Cisco Core.

En el siguiente plan de trabajo, se va a presentar las actividades a realizar para la implementación del proyecto data center en las instalaciones de la organización, que incluye la configuración de 16 Switches Cisco de acceso, un switch Core 4500 y un Switch capa tres 3850, para la distribución y enrutamiento de la red de la organización. Esto puede resumirse en los siguientes servicios:

- Montaje de equipos Cisco Core 4500 y Cisco 3850 en rack del MDF.
- Montaje de 16 equipos Cisco 2960 distribuidos en los racks de cada IDF.
- Configuración de IP administrativa y métodos de acceso a los switches.
- Creación de VLANs, redes y direccionamiento.
- Implementación de enrutamiento dinámico por EIGRP y OSPF en el Switch Core.

En la Tabla 34, se despliegan los milestones del plan de trabajo.

Tabla 34. Milestone del plan de trabajo de la solución de datos

Milestone	Responsable	Porcentaje
Validación de requerimientos de hardware y software • Verificación de Site • Verificación de arranque de equipo	Estratel	5%
Instalación de equipos Switch Cisco Core 4500 y Cisco 3850 en MDF • Instalación de los módulos y fuentes de poder en todos los equipos. • Montaje físico de equipo Switch Cisco Core y Cisco 3850 en rack APC.	Estratel	15%
Configuración de equipos en MDF • Configuración de parámetros básicos • Configuración de ruteo y segmentación según el diseño.	Estratel	20%
Instalación de 16 equipos Cisco 2960 en IDF's • Instalación de los módulos y fuentes de poder en los equipos que lo requieran. • Montaje físico de los 16 switches de acceso, los cuales se distribuirán entre todos los IDF según el diseño.	Estratel	20%

Configuración de equipos en IDF • Configuración de IP administrativa. • Configuración de métodos y claves de acceso. • Configuración de VLANs en todos los equipos según lo solicitado. • Configuración de Gateway.	Estratel	25%
Pruebas de Funcionalidad General • Aplicar pruebas de operación de paquetes de acuerdo a las rutas establecidas.	Estratel/Cliente	10%
Transferencia • Realizar una transferencia de conocimiento al personal responsable del equipo.	Estratel/Cliente	3%
Respaldo • Respaldo final para la entrega al cliente	Estratel/Cliente	2%

Como se puede observar en la tabla 34, en la primera columna del milestone, hace referencia a las actividades. En la columna siguiente, se nombran los responsables de cada milestone. Y en la columna final, se enumera en porcentaje el avance del proyecto.

En seguida, se enlista los pre-requisitos que el cliente deberá contemplar para el inicio de las actividades:

- El cliente deberá proporcionar información acerca del estado actual de la red, así como consideraciones adicionales a tomarse en cuenta durante la implementación.
- En caso de que la transferencia de conocimiento sea para más de una persona, es necesario contar con un salón o área adecuada en las instalaciones del cliente con un proyector y pantalla.
- Se debe considerar los permisos de acceso al sitio un día antes de cada instalación en caso de que haya alguna guardia en el sitio. En caso de que el sitio este cerrado, se debe contar con las llaves para acceder al interior. Igualmente se debe considerar las llaves para abrir el gabinete o rack donde se instala el equipo.

Para dar inicio a las actividades del proyecto, se requiere cubrir en su totalidad con los requisitos mencionados anteriormente. En caso de no contar con tierra física, debe firmarse un documento en el que el cliente da el visto bueno al

arranque de instalación, con el conocimiento de que no aplicará garantía en caso de problemas eléctricos no atribuidos a un mal uso o manejo de equipo.

Los riegos más importantes identificados que pueden demorar y afectar las actividades durante la implementación de las actividades se despliegan en la Tabla 35:

Tabla 35. Riesgos en la implementación

Riesgo	Causas	Impacto	Ponderación	Acción
No hay acceso al sitio por falta de personal o llaves de acceso	No se notificó un día antes de la visita al sitio	Puede generar retrasos y tiempos muertos que afecten la planeación del proyecto e incluso prolongarlo más de lo debido	Media	Notificar un día antes al personal responsable del sitio remoto
Que no encienda el equipo	Equipo dañado	Retraso en la instalación	Alta	Solicitar reemplazo de equipo
Que el sitio no cuente con las condiciones adecuadas para instalar los equipos (Luz, espacio, instalaciones eléctricas adecuadas)	No se revisó los requerimientos del sitio un día antes de la visita al sitio.	Que no se instale el equipo en la fecha correspondiente. Si el cliente decide instalarlo pese a que no cumple las indicaciones correctas, puede verse afectado la garantía del producto.	Alta	Revisar las condiciones del sitio y verificar que cuente con las adecuadas antes de la instalación.

Para terminar, en la Tabla 36, se muestra un cronograma de las actividades, para que el cliente se dé una idea del tiempo que se llevará la solución de datos.

Tabla 36. Cronograma de la solución de datos

Milestone	Responsable	Días							
		1	2	3	4	5	6	7	8
Validación de requerimientos de hardware y software									
Verificación de site	Estratel								

Verificación de equipos	Estratel								
Instalación de equipos Cisco Core y Cisco 3850 en MDF									
Configuración física	Estratel								
Montaje físico	Estratel								
Configuración de equipos Cisco Core y Cisco 3850 en MDF									
Configuración de red	Estratel								
Instalación de 16 equipos Cisco Switch 2960 en IDF									
Configuración física	Estratel								
Montaje físico	Estratel								
Configuración de 16 equipos Cisco Switch 2960 en IDF									
Configuración de red	Estratel								
Pruebas de Funcionalidad									
Pruebas de conexión y pruebas de red	Estratel								
Transferencia de conocimiento									

Transferencia de conocimiento	Estratel/Cliente								
Respaldos									
Respaldo final previa entrega al cliente	Estratel								

Ahora bien, lo siguiente es presentar al cliente el otro plan de trabajo, que viene siendo el de seguridad perimetral de Fortinet.

En el siguiente plan de trabajo para la solución de seguridad, se presentará las actividades que se estarán realizando para la implementación del proyecto solución de datos y seguridad en las instalaciones del site principal de la organización, que incluye la sustitución de un Firewall Fortinet FortiGate 500A a un Firewall Fortinet FortiGate 600D en alta disponibilidad (HA). Esto puede resumirse en los siguientes servicios:

- Instalación y configuración de 2 equipos FortiGate 600D (FG-600D) en HA.
- Registro de los appliance en el portal Web del fabricante.
- Actualización de los equipos a la última versión del firmware estable.
- Migración de objetos, políticas y servicios de FortiGate 500A al equipo FortiGate 600D.
- Creación de perfiles de seguridad para las políticas de publicación (IPS y Antivirus).
- Creación de perfiles de seguridad para navegación a Internet (Application Control, Web Filtering e IPS).
- Creación de VPN Site to Site.
- Pruebas de operación.

En la Tabla 37, se despliegan los milestones del plan de trabajo de la solución de seguridad.

Tabla 37. Milestone por porcentaje de la solución de seguridad

Milestone	Responsable	Porcentaje
Validación de requerimientos de hardware y software • Verificar espacio en rack.	Cliente	10%

• Verificar alimentación eléctrica.		
Actualización, Montaje físico y registro de equipos • Se realiza el montaje físico de 2 equipos FG-600D en HA. • Se actualizarán los equipos a la última versión de firmware estable. • Registro de equipos en el portal Web del fabricante.	Estratel	10%
Preparación y configuración de equipo FG-600D • Configuración básica de equipos (direccionamiento IP, Hostname, ruta por defecto, usuario y contraseña). • Configuración de ruta estática por defecto del FG-600D. • Migración de objetos de firewall del 500A al 600D. • Creación de perfiles de seguridad para políticas de publicación, IPS y Antivirus. • Configuración de objetos NAT y políticas de publicación de servicios. • Creación de grupos y usuarios para navegación a Internet. • Creación de perfiles de seguridad de Application control, Web Filtering y políticas de navegación a Internet. • Creación de VPN para acceder remotamente a redes locales. • Sustitución del equipo 500A por FortiGate 600D.	Estratel	45%
Pruebas de Funcionalidad General • Validación de servicios publicados. • Validación de políticas de Firewall y Navegación. • Validación de servicio VPN.	Estratel/cliente	10%
Transferencia • Transferencia de conocimiento.	Estratel/cliente	3%
Respaldo • Respaldo de configuración del FG-600D.	Estratel/cliente	2%

Como se puede observar en la Tabla 37, y al igual que el primer plan de trabajo, en la primera columna del milestone, hace referencia a las actividades. En la

siguiente columna, se nombran los responsables de cada milestone. Y en la columna final, se enumera en porcentaje el avance del proyecto.

En seguida, se enlista los pre-requisitos que el cliente deberá contemplar para el inicio de las actividades:

- Proporcionar acceso al equipo 500A que será sustituido por el equipo FG-600D en HA, para poder extraer la configuración.
- Disponibilidad de tiempo de personal para supervisión y validación de cambios.
- Acordar fecha y hora para instalación y configuración.
- Se debe contar con acceso al sitio y personal responsable del sitio el día de la instalación.
- Contar con 1 unidad de rack para montaje de equipo para cada FG-600D.
- Se debe contemplar una ventana de tiempo de 1 hora para el intercambio del FortiGate 500A al 600D.
- En caso de que la transferencia de conocimiento sea para más de una persona, es necesario contar un proyector o pantalla mediana en las instalaciones del cliente.

Para finalizar el plan de trabajo con respecto a la solución de seguridad perimetral, en la Tabla 38, se muestra un cronograma de las actividades de la solución de seguridad, para que el cliente se dé una idea del tiempo que se llevará la solución de datos.

Es importante mencionar que ambos cronogramas mostrados en el plan de trabajo de la solución de datos y seguridad, serán trabajados al mismo tiempo.

Tabla 38. Cronograma de actividades de la solución de seguridad

Milestone	**Responsable**	**Días**					
		1	**2**	**3**	**4**	**5**	**6**
Configuración de equipo FG-600D							
Validación de requerimientos	Estratel						

Actualización, Montaje físico y registro de equipos.	Estratel						
Preparación y configuración de equipo FG-600D en HA	Estratel						
Pruebas de funcionalidad y transferencia							
Validación de los servicios publicados	Estratel						
Transferencia de conocimientos	Estratel						
Respaldo final	Estratel						

4.1.3.- Reseñas de los productos

Cisco Catalyst series 4500E. Características y beneficios. Los switches Catalyst 4500 Series de Cisco brindan experiencias de usuario seguras, móviles y de alto rendimiento a través de inversiones en switching de Capa 2-4. Permiten la seguridad, la movilidad, el rendimiento de las aplicaciones, el video y el ahorro de energía en una infraestructura que admite resiliencia, virtualización y automatización. Los switches Cisco Catalyst 4500 Series brindan un rendimiento sin fronteras, escalabilidad y servicios con un costo total de propiedad (TCO) reducido y una protección de inversión superior.

El Cisco Catalyst 4500 tiene una arquitectura de reenvío centralizada que permite la colaboración, la virtualización y la capacidad de administración operativa a través de operaciones simplificadas. Con compatibilidad hacia adelante y hacia atrás que abarca múltiples generaciones, la nueva serie Cisco Catalyst 4500E ofrece protección de inversión excepcional y flexibilidad de implementación para satisfacer las necesidades cambiantes de organizaciones

de todos los tamaños. La plataforma Cisco Catalyst 4500E Series tiene enlaces ascendentes de 10 Gigabit Ethernet (GE) y admite Power over Ethernet Plus (PoE+) y Universal PoE (UPOE), lo que permite a los clientes probar su red en el futuro.

Los chasis de la serie E vienen en cuatro diferentes formas: 3 ranuras (4503-E), 6 ranuras (4506-E), 7 ranuras (4507R+E) y 10 ranuras (4500R+E). Los chasis 4503-E, 4506-E, 4507R+E y 4510R+E son extremadamente flexibles y admiten 24 o 48 Gbps por ranura de tarjeta de línea. La resistencia integrada en la Serie Catalyst 4500E de Cisco incluye redundancia de motor de supervisor 1 + 1 (solo chasis de 10 ranuras y 7 ranuras), ventiladores redundantes, tolerancia a fallas basada en software y redundancia de suministro de energía 1 + 1. La resistencia integrada tanto en hardware como en software minimiza el tiempo de inactividad de la red, ayudando a garantizar la productividad de la fuerza laboral, la rentabilidad y el éxito del cliente.

Cisco Catalyst 4500E Series ofrece cuatro opciones de chasis y cuatro opciones de motor de supervisor. Proporciona una arquitectura común que puede escalar hasta 388 puertos. El chasis redundante R+E de Cisco Catalyst ofrece alta disponibilidad al admitir motores de supervisor redundantes 1 + 1 con un segundo tiempo de conmutación por error y actualizaciones de software en servicio (ISSU) a pantalla completa. El reenvío continuo con conmutación con estado (NSF/SSO) e ISSU ayudan a garantizar el reenvío continuo de paquetes durante el cambio de motor del supervisor para ayudar a garantizar una alta disponibilidad para aplicaciones de colaboración y voz sobre IP (VoIP). Utilizando las mismas tarjetas de línea que los switches Cisco Catalyst 4000 Series y los clásicos switches Cisco Catalyst 4500 Series, la serie Catalyst 4500E de Cisco aumenta el compromiso de Cisco con la escalabilidad de la empresa y la sucursal.

Figura 4-11. Cisco Catalyst 4500E [6]

Cisco Catalyst 2960-X. Características y beneficios. Los switches Catalyst 2960-X de la serie Cisco son switches Gigabit Ethernet de configuración fija y stackable que brindan acceso de clase empresarial para aplicaciones de campus y sucursales. Operan en el software Cisco IOS y admiten la gestión simple de dispositivos y la gestión de red. Las series Cisco Catalyst 2960-X proporcionan una incorporación, configuración, supervisión y resolución de problemas fáciles de los dispositivos. Estos switches totalmente administrados pueden proporcionar funciones avanzadas de Layer 2 y Layer 3, así como potencia opcional Power over Ethernet Plus (PoE+). Diseñados para la simplicidad operativa para reducir el costo total de propiedad, permiten operaciones comerciales escalables, seguras y energéticamente eficientes con servicios inteligentes. Los switch Cisco ofrecen visibilidad de aplicaciones mejorada, confiabilidad y resistencia de red.

Característica de los switches Cisco Catalyst 2960-X:

- Puertos Gigabit Ethernet de 24 o 48 con rendimiento de reenvío de velocidad de línea.
- 4 enlaces ascendentes de 1 Gigabit Ethernet de factor de forma pequeño conectable (SFP) o 2 enlaces ascendentes SFP+ de 10 Gigabit Ethernet fijos.
- Soporte PoE+ con un presupuesto de potencia de hasta 740W y PoE perpetuo.
- Cisco IOS LAN Base o LAN Lite y Cisco IOS IP Lite.

- Administración de dispositivos con interfaz de usuario web, acceso over-the-air a través de Bluetooth, interfaz de línea de comandos (CLI), protocolo simple de administración de redes (SNMP) y acceso a la consola RJ-45 o USB.
- Gestión de red con Cisco Prime, Cisco Network Plug and Play y Cisco DNA Center.
- Apilamiento (stacking) con FlexStack-Plus y FlexStack-Extended
- Funciones de capa 3 con acceso enrutado (Open Shortest Path First [OSPF]), enrutamiento estático y Routing Information Protocol (RIP).
- Visibilidad con el Sistema de nombres de dominio como fuente autorizada (DNS-AS) y NetFlow completo (flexible).
- Seguridad con 802.1X, analizador de puerto serie (SPAN) y unidad de datos de protocolo de puente Guard (BPDU).
- Confiabilidad con mayor tiempo medio entre fallas (MTBF) y garantía de por vida limitada mejorada (E-LLW).
- Resistencia con fuentes de alimentación opcionales reemplazables en el campo.

Figura 4-12. Cisco Catalyst 2960X [6]

Fortinet FortiGate 600D. Características y beneficios. El FortiGate 600D ofrece funcionalidades de firewall de próxima generación para medianas y grandes empresas, con la flexibilidad de implementarse en el campus o en el borde del centro de datos y en los segmentos internos. Protege contra las amenazas cibernéticas con un alto rendimiento de rendimiento de seguridad, eficacia de seguridad y gran visibilidad.

Desarrollado por FortiASICs – Los procesadores de encargo FortiASIC ofrecen la potencia que necesidad de detectar contenido malicioso a velocidades de varios gigabits.

Otras tecnologías de seguridad no pueden proteger contra amplia gama de hoy del contenido y conexión basada en amenazas porque se basan en las CPU de propósito general, causando una brecha en el desempeño peligroso.

Procesadores FortiASIC proporcionan el rendimiento necesario para bloquear las amenazas emergentes, conocer rigurosa de terceros certificaciones, y garantizar que la seguridad de su red solución no se convierta en un cuello de botella de la red.

- Procesador de Red – Procesador de red avance NP6 FortiASIC nueva de Fortinet trabaja en línea con funciones FortiOS que proporcionen:
    - rendimiento de firewall Superior para IPv4/IPv6, SCTP y multicast el tráfico con latencia ultra baja hasta 2 microsegundos.
    - VPN, CAPWAP IP y la aceleración del túnel prevención de intrusiones basadas en Anomalía, y la descarga de checksum desfragmentación de paquetes.
    - Asignación de tráfico y la prioridad de colas.

Procesador contenido – El procesador de contenidos FortiASIC CP8 trabaja fuera del flujo directo del tráfico, proporcionando la criptografía de alta velocidad y el contenido servicios de inspección, incluyendo:

- basada en firmas aceleración de inspección de contenido
- cifrado y descifrado de descarga

10 GE Conectividad de red Segmentación – conectividad de alta velocidad es esencial para la seguridad de la red la segmentación en el núcleo de las redes de datos. El FortiGate 600D proporciona la más alta densidad de puertos 10 GE en el mercado, lo que simplifica diseños de red sin depender de dispositivos adicionales para cerrar conectividad deseado.

Figura 4-13. FortiGate 600D [10]

4.1.4.- Implementación en sitio con la tecnología Cisco

La instalación se comenzó según lo planeado, se empezó por trabajar en un día inhábil para el cliente, de esta forma afectando lo mínimo posible de los servicios de la institución. Se inició por armar el rack donde estarían los equipos de seguridad y el switch Core Cisco 4500, en la Figura 4-14, se ve el tipo de gabinete cerrado.

Figura 4-14. Rack de gabinete cerrado

Después optamos por el ensamblado del switch Cisco Core 4500, y la instalación en el gabinete, de igual forma se instaló el switch Cisco 3510 como se ve en la Figura 4-15. Cabe mencionar que dicho switch Cisco 3510, no se configuró, la institución lo designó para futuras instalaciones.

Figura 4-15. Montaje de Cisco Core en rack

Es importante mencionar que la propuesta que se había presentado, hubo modificaciones por el cliente, las cuales se irán presentando a continuación, cabe señalar que casos como este, se presentan casi siempre en las implementaciones, las cuales se deben limitar si son posibles o no por el tiempo calculado y que no influyan en la entrega de lo planeado.

Inmediatamente, se encendió y se iniciaron las configuraciones básicas siguientes:

- Nombre de equipo.
- Configuración de contraseña enable secret.
- Configuración de contraseña de consola.
- Configuración de usuario y contraseña de acceso por vty.
- Configuración de aviso banner.
- Configuración para desactivar la búsqueda de dominio DNS.

La configuración CLI se resume de la siguiente manera:

```
hostname Core
!
enable secret 5 $1$p7Ov$SqlhJffKuEUoXHmxJarOB0
!
enable password 7 0822455D0A49
!
username admin password 2 93657A9B099C
!
line vty 0 4
 session-timeout 1800
 password 7 23149B3D447C
 login local
!
service password encryption
!
banner motd ‘Solo personal autorizado’
!
no ip domain-lookup
```

Una vez que la configuración básica se encuentra realizada, seguidamente se hacen las creaciones de las VLANs y su direccionamiento:

- Se crearon 10 VLANs distintas, con direccionamiento IP y mascara de subred.

Resumiendo, la configuración CLI queda de la siguiente manera:

```
interface Vlan1
 ip address 10.9.1.254 255.255.255.0
!
interface Vlan2
 ip address 10.9.2.254 255.255.255.0
!
interface Vlan3
 ip address 10.9.3.254 255.255.255.0
!
interface Vlan4
 ip address 10.9.4.254 255.255.255.0
!
interface Vlan5
 ip address 10.9.5.254 255.255.255.0
!
interface Vlan6
 ip address 10.9.6.254 255.255.255.0
!
interface Vlan250
 description "Red de administracion de switches"
 ip address 172.16.250.254 255.255.255.0
!
interface Vlan252
 description "Red de Manager"
 ip address 10.9.252.254 255.255.255.0
!
interface Vlan400
description "Red de VoIP"
 ip address 192.168.10.254 255.255.254.0
```

Después seguimos con la configuración de las interfaces de las fibras. Según la posición de las navajas insertadas, como se muestra en la Figura 4-16, es como se señalan las configuraciones en el CLI. Por ejemplo, para la configuración en CLI de la interfaz uno por fibra, sería: *interface TenGigabitEthernet3/1,* donde el 3 pertenece a la navaja y el 1 al número de interfaz de dicha navaja.

Cisco 4500R+E

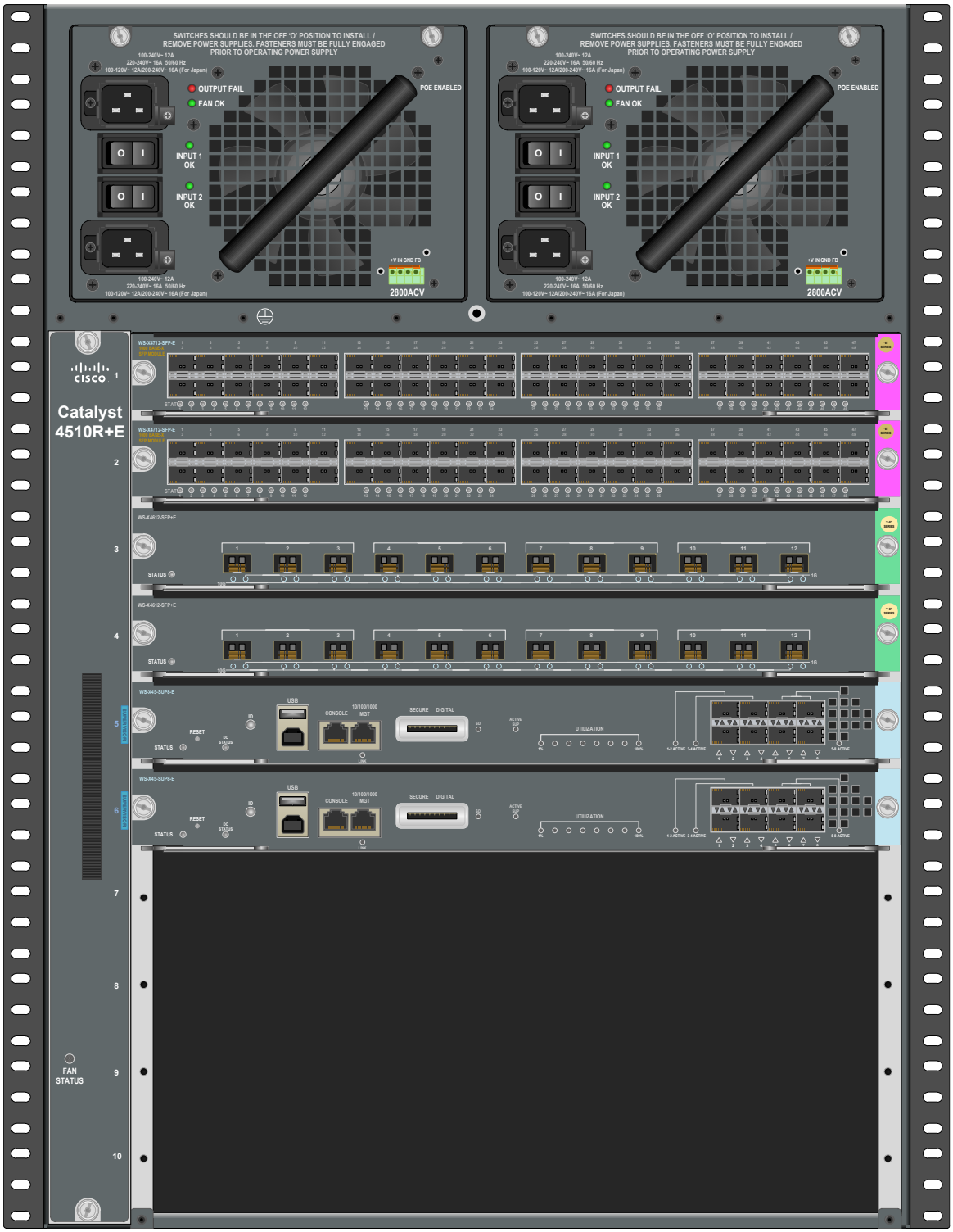


Figura 4-16. Switch Cisco Core 4500R+E

Las primeras seis interfaces de cada navaja 3 y 4, están reservadas para la comunicación con el equipo HPE 3PAR. Esas interfaces se dejaron configuradas como modo acceso a la VLAN de sus servidores, que viene siendo la VLAN 3.

La configuración en CLI se resume de la siguiente manera:

```
interface TenGigabitEthernet3/1
 switchport access vlan 3
 switchport mode access
!
interface TenGigabitEthernet3/2
 switchport access vlan 3
 switchport mode access
!
interface TenGigabitEthernet3/3
 switchport access vlan 3
 switchport mode access
!
interface TenGigabitEthernet3/4
 switchport access vlan 3
 switchport mode access
!
interface TenGigabitEthernet3/5
 switchport access vlan 3
 switchport mode access
!
interface TenGigabitEthernet3/6
 switchport access vlan 3
 switchport mode access
!
interface TenGigabitEthernet4/1
 switchport access vlan 3
```

```
 switchport mode access
!
interface TenGigabitEthernet4/2
 switchport access vlan 3
 switchport mode access
!
interface TenGigabitEthernet4/3
 switchport access vlan 3
 switchport mode access
!
interface TenGigabitEthernet4/4
 switchport access vlan 3
 switchport mode access
!
interface TenGigabitEthernet4/5
 switchport access vlan 3
 switchport mode access
!
interface TenGigabitEthernet4/6
 switchport access vlan 3
 switchport mode access
```

Las interfaces 9,10, 11 y 12, de cada navaja, van conectadas a los IDFs de los switch de acceso, dichas interfaces se encuentran configuradas por los consecuentes puntos:

- Interfaz modo trunk.
- VLAN trunk navita 99.
- Configuración de VLANs permitidas, ALL.

Dichas configuraciones en CLI se expresan de la siguiente manera:

```
interface TenGigabitEthernet3/9
 description "Enlace a Anexos"
switchport trunk native vlan 99
```

```
 switchport mode trunk
!
interface TenGigabitEthernet3/10
 description "Enlace a Creditos"
switchport trunk native vlan 99
 switchport mode trunk
!
interface TenGigabitEthernet3/11
 description "Enlace a Salidas"
switchport trunk native vlan 99
 switchport mode trunk
!
interface TenGigabitEthernet3/12
 description "Enlace Contaduria"
switchport trunk native vlan 99
 switchport mode trunk
!
interface TenGigabitEthernet4/9
 description "Enlace a TI"
switchport trunk native vlan 99
 switchport mode trunk
!
interface TenGigabitEthernet4/10
 description "Enlace a Administracion"
switchport trunk native vlan 99
 switchport mode trunk
!
interface TenGigabitEthernet4/11
 description "Enlace Entradas"
 switchport trunk native vlan 99
```

```
 switchport mode trunk
!
interface TenGigabitEthernet4/12
 description "Enlace a Alcoholismo"
switchport trunk native vlan 99
switchport mode trunk
```

A continuación, se agrega la configuración de las diferentes interconexiones del switch Cisco Core:

```
!
interface GigabitEthernet1/41
 description "Recepcion del Pool IP publica.209"
 switchport access vlan 148
 switchport mode access
!
interface GigabitEthernet1/42
 description "Recepcion del Pool IP publica.209"
 switchport access vlan 148
 switchport mode access
!
interface GigabitEthernet1/43
 description "Recepcion del Pool IP publica.218"
 switchport access vlan 148
 switchport mode access
!
interface GigabitEthernet1/44
 description "Recepcion del Pool IP publica.218"
 switchport access vlan 148
 switchport mode access
!
interface GigabitEthernet1/45
```

```
 description "Conexion Core-FGT"
 switchport trunk allowed vlan 251,252,500,501
 switchport trunk native vlan 251
 switchport mode access
!
interface GigabitEthernet1/46
 description "Conexion Core-FGT"
 switchport trunk allowed vlan 251,252,500,501
 switchport trunk native vlan 251
 switchport mode access
!
interface GigabitEthernet1/47
 description "Conexion Maganer"
 switchport access vlan 252
!
```

Explicando la configuración de interconexión anterior:

- La interfaz 41 y 42 es para la recepción de la IP publicas fijas, como ya se mencionó, la organización tiene un par de pools de IP públicas y, al contar el cliente con dos equipos FortiGate en H.A. en modo activo-activo, al equipo FortiGate no se le puede poner una dirección IP fija a un solo equipo, como el clúster trabaja con MAC virtuales, debe ocuparse con switches conviviendo en la misma red o VLAN, de esta forma el clúster FortiGate designará quien tendrá la IP pública.
- La interfaz 43 y 44 es para la misma función, pero para el otro pool de IP públicas fijas.
- La interfaz 45 y 46 es para la comunicación entre el equipo FortiGate y el switch Cisco Core.
- La interfaz 47 es para sus equipos de administración que tienen en la red.

Las demás interfaces quedaron configuradas en la VLAN 10, y dependiendo de los requerimientos de la organización, se irán configurando respecto a sus necesidades.

Para el enrutamiento estático, se configuró lo siguiente:

- Ruta estática por defecto.

Y para el enrutamiento dinámico, se configuró lo siguiente:

- Enrutamiento EIGRP entre switch Cisco Core y router MPLS.
- Enrutamiento OSPF entre switch Cisco Core y FortiGate.

Dichas disposiciones de enrutamientos, se resume en la configuración CLI a continuación:

- Para el enrutamiento estático por defecto, se utilizara una ruta que enviará cualquier petición de red que el switch Core desconozca al FortiGate:

```
!
ip route 0.0.0.0 0.0.0.0 10.9.1.250
!
```

- Para el enrutamiento dinámico EIGRP, en el router Core antiguo, ya estaba configurado, de tal manera, que se pasó dicha configuración al switch Core nuevo:

```
!
router eigrp 1
 network 10.0.0.0
 redistribute static
!
```

- Se configuró el protocolo de enrutamiento OSPF para la comunicación entre las VPN's del FortiGate y la red interna del nuevo switch Core.
  La configuración por CLI del switch Core queda de la siguiente manera:

```
!
router ospf 1
 network 10.9.0.0 0.0.255.255 area 0.0.0.0
 network 192.168.10.0 0.0.1.255 area 0.0.0.0
!
```

  Para la configuración OSPF del equipo FortiGate queda de la siguiente manera:

```
config router ospf
    set router-id 2
    config area
        edit 0.0.0.0
        next
    end
    config ospf-interface
        edit "Core"
            set interface "Core"
            set dead-interval 40
            set hello-interval 10
        next
    end
    config network
```

```
        edit 1
            set prefix 10.9.1.0 255.255.255.0
        next
    end
    config redistribute "connected"
    end
    config redistribute "static"
        set status enable
end
```

Explicando la configuración anterior del OSPF:

- El ID del switch Core es 1, mientras que el ID del FortiGate es 2.
- El área es el 0.0.0.0 para la comunicación entre los equipos.
- Las redes redistribuidas por el switch Cisco Core es la red 10.9.0.0/16 que viene siendo la red interna de la organización. Mientras que la red 192.168.10.0/23, viene siendo la red de VoIP que tienen en dicha organización.
- Las redes redistribuidas por el FortiGate es la red 10.9.1.0/24, además está habilitada la redistribución de las redes estáticas en el FortiGate, en este caso, las VPN's conectadas a los sitios remotos.

Con esta configuración, el equipo FortiGate y el switch Cisco Core ya tienen adyacencia.

Para los equipos de acceso, los Cisco 2960X se configuró lo siguiente:

- Asignación de IP administrativa.
- Asignación a todos los puertos con su VLAN de acceso correspondiente respecto al diagrama antes mencionado.
- Las interfaces de fibra óptica son configuradas en modo trunk.

Dicha configuración en CLI se puede expresar de la siguiente manera:

Se colocará la configuración de un switch de acceso como ejemplo:

```
!
service password-encryption
!
hostname Creditos
!
!
interface GigabitEthernet1/0/1
 switchport access vlan 4
 switchport mode access
```

```
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/2
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/3
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/4
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/5
```

```
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/6
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/7
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/8
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
```

```
!
interface GigabitEthernet1/0/9
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/10
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/11
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/12
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
```

```
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/13
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/14
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/15
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/16
 switchport access vlan 4
 switchport mode access
```

```
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/17
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/18
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/19
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/20
```

```
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/21
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/22
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/23
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
```

```
!
interface GigabitEthernet1/0/24
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 400
 switchport port-security maximum 2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan250
 ip address 172.16.250.2 255.255.255.0
!
line con 0
 password 7 529783114A2F
 login
line vty 0 4
 password 7 529783114A2F
 login
line vty 5 15
 password 7 529783114A2F
 login
!
```

Explicación de la configuración anterior:

- El acceso de la VLAN para este switch es la VLAN 4.
- Para el tag de voz es la VLAN 400.
- Se encuentra habilitado el portfast y el BPDGuard.

- El port-security igual se encuentra habilitado y tiene un máximo número de seguridad de 2 para la dirección MAC.
- Tiene una IP de administración del switch con dirección 172.16.250.2

Todos los equipos switch de acceso tienen la misma configuración, a diferencia que la VLAN de acceso para algunos es diferente y la VLAN de administración es diferente para cada switch, que más adelante se resumirá.

Para ingresar al equipo es necesario ingresar por las IP's administrativas indicadas en la Tabla 39.

Tabla 39. Direccionamiento de administración

Switch	IP Admin	Hostname
Core	172.16.250.254	CORE
IDF1	172.16.250.1	TI
IDF2	172.16.250.2	Creditos
IDF3	172.16.250.3	Alcoholismos
IDF4	172.16.250.4	Anexos
IDF5	172.16.250.5	Fiscales
IDF6	172.16.250.6	Entradas
IDF7	172.16.250.7	Contaduria
IDF8	172.16.250.8	Salidas
IDF9	172.16.250.9	Administracion
IDF10	172.16.250.10	Evaluaciones
IDF11	172.16.250.11	Sub_Secretaria
IDF12	172.16.250.12	Propuestas

Este acceso puede ser por los siguientes servicios:

- Telnet, TCP 23
- SSH, TCP 22

La contraseña para ingresar en modo EXEC privilegiado y configuración global, por razones de seguridad, no son conveniente mencionarlos, además fueron entregados al cliente en un sobre y con firma de recibido.

La sesión de la conexión vence después de 15 minutos de inactividad.

A continuación, en la Figura 4-17, se muestra el diagrama físico final de la interconexión entre el MDF y los IDF's.

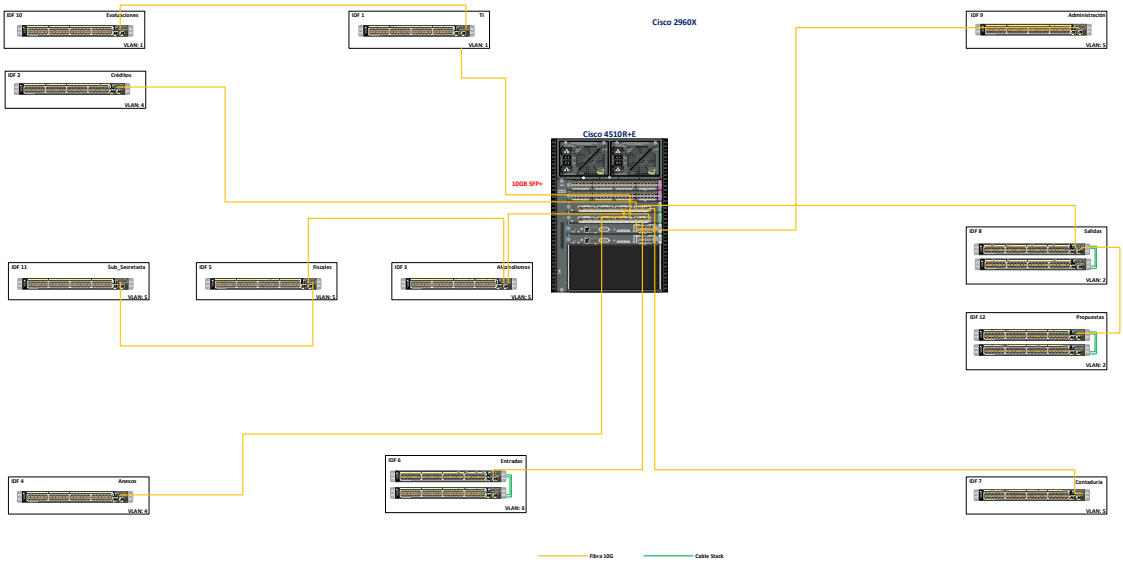


Figura 4-17. Diagrama físico final de la implementación

De igual forma, en la Figura 4-18, se muestra el diagrama lógico final de la interconexión entre el clúster FortiGate y el Switch Cisco Core.

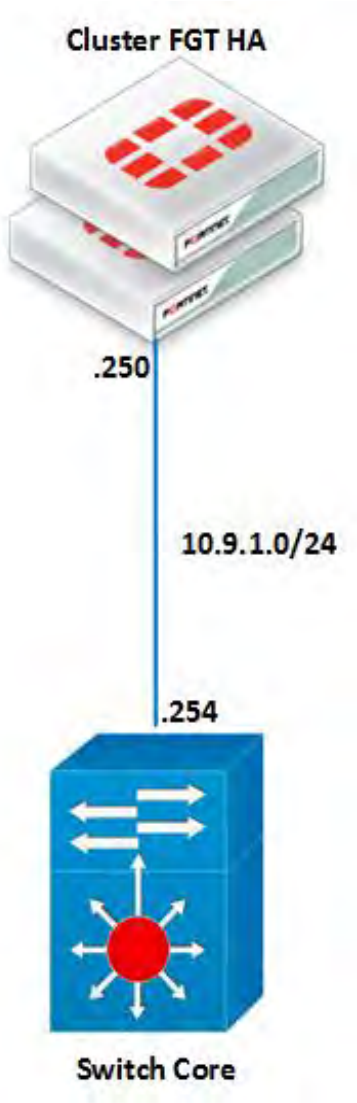


Figura 4-18. Diagrama lógico final de la implementación

A continuación, en la Figura 4-18, se muestra la interconexión del diagrama lógico entre el Switch Core y la MPLS por medio del protocolo de enrutamiento EIGRP, sumarizando la red 10.0.0.0 para la interconexión con los sitios remotos.

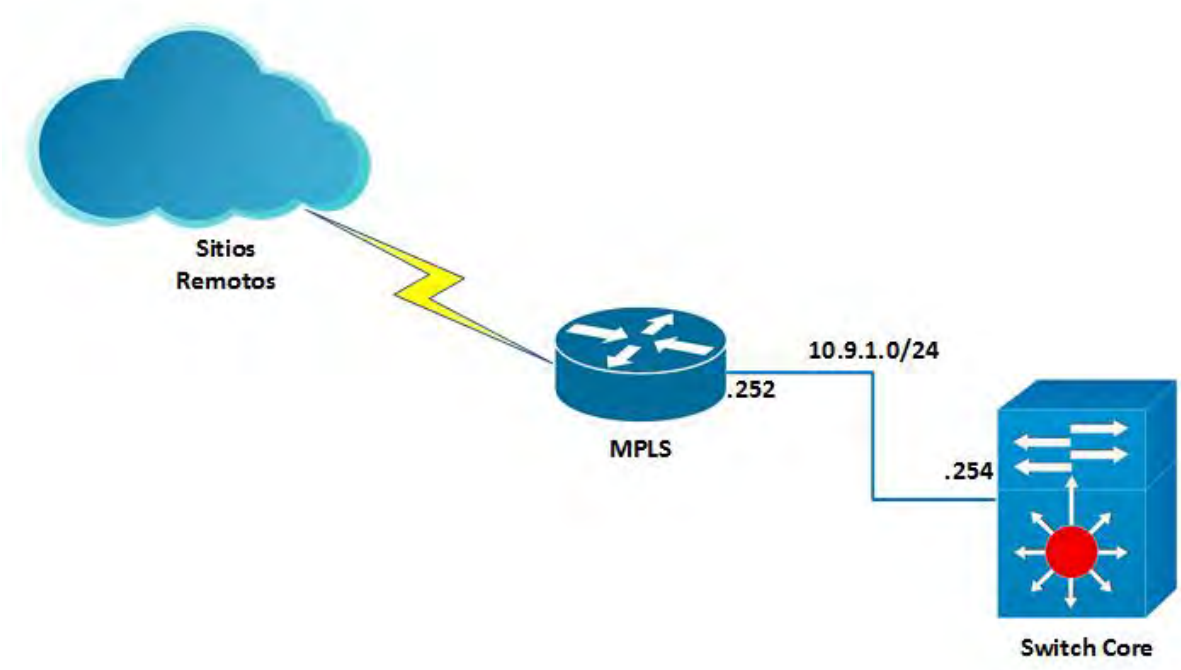


Figura 4-19. Interconexión del diagrama lógico final de la implementación

En la Tabla 40, se presentan las VLANs y sus interfaces IP creadas en el MDF y cada IDF como se había mencionado anteriormente en la configuración:

Tabla 40. Direccionamiento VLAN del MDF y los IDF's

Site	Vlan ID	Vlan Name	IP/Mask
MDF			
	1	Datos10_9_1_254	10.9.1.254/24
	2	Datos10_9_2_254	10.9.2.254/24
	3	Datos10_9_3_254	10.9.3.254/24
	4	Datos10_9_4_254	10.9.4.254/24
	5	Datos10_9_5_254	10.9.5.254/24
	6	Datos10_9_6_254	10.9.6.254/24
	250	ADM Switches	172.16.250.254/24
	400	Telefonía	192.168.10.254/23
IDF 1 – TI			
	1	Datos1	

	400	Telefonía	
	250	ADM Switches	172.16.250.1/24
IDF 2 – Créditos			
	4	Datos1	
	400	Telefonía	
	250	ADM Switches	172.16.250.2/24
IDF 3 – Alcoholismos			
	5	Datos1	
	400	Telefonía	
	250	ADM Switches	172.16.250.3/24
IDF 4 – Anexos			
	4	Datos1	
	400	Telefonía	
	250	ADM Switches	172.16.250.4/24
IDF 5 – Fiscales			
	5	Datos1	
	400	Telefonía	
	250	ADM Switches	172.16.250.5/24
IDF 6 – Entradas			
	6	Datos1	
	400	Telefonía	
	250	ADM Switches	172.16.250.6/24
IDF 7 – Contaduria			
	5	Datos1	
	400	Telefonía	
	250	ADM Switches	172.16.250.7/24
IDF 8 – Salidas			
	2	Datos1	
	400	Telefonía	

	250	ADM Switches	172.16.250.8/24
IDF 9 – Administración			
	5	Datos1	
	400	Telefonía	
	250	ADM Switches	172.16.250.9/24
IDF 10 – Evaluaciones			
	1	Datos1	
	400	Telefonía	
	250	ADM Switches	172.16.250.10/24
IDF 11 – Sub_Secretaría			
	5	Datos1	
	400	Telefonía	
	250	ADM Switches	172.16.250.11/24
IDF 12 – Propuestas			
	2	Datos1	
	400	Telefonía	
	250	ADM Switches	172.16.250.12/24

4.1.5.- Implementación en sitio con la tecnología Fortinet

Por propósitos de seguridad, se omite información que pueda ser sensible para la organización como direccionamiento IP publico fijo, credenciales o configuración de contraseñas de VPN's y demás.

La instalación física del clúster FortiGate 600D se realizó en el mismo rack que en el switch Cisco Core como se muestra en la Figura 4-20 y en la Figura 4-21.

Figura 4-20. Clúster FortiGate

Figura 4-21. Clúster FortiGate y switch Cisco Core en rack

Una vez instalado e iniciado físicamente, se empieza a migrar la configuración del antiguo FortiGate 500A al nuevo clúster FortiGate 600D, básicamente la migración es copiar y traducir la configuración por medio de CLI de un equipo al otro.

Por motivos de seguridad, los métodos de acceso para ingresar al equipo fueron entregados al cliente en un sobre, y firmados de recibidos.

Se configuró para que pudieran acceder desde internet por los siguientes servicios:

- HTTPS, TCP 40443
- SSH, TCP 22

La sesión de la conexión vence después de 15 minutos para https y ssh.

En la Figura 4-22, se muestra el diagrama lógico final de la interconexión del clúster FortiGate 600D.

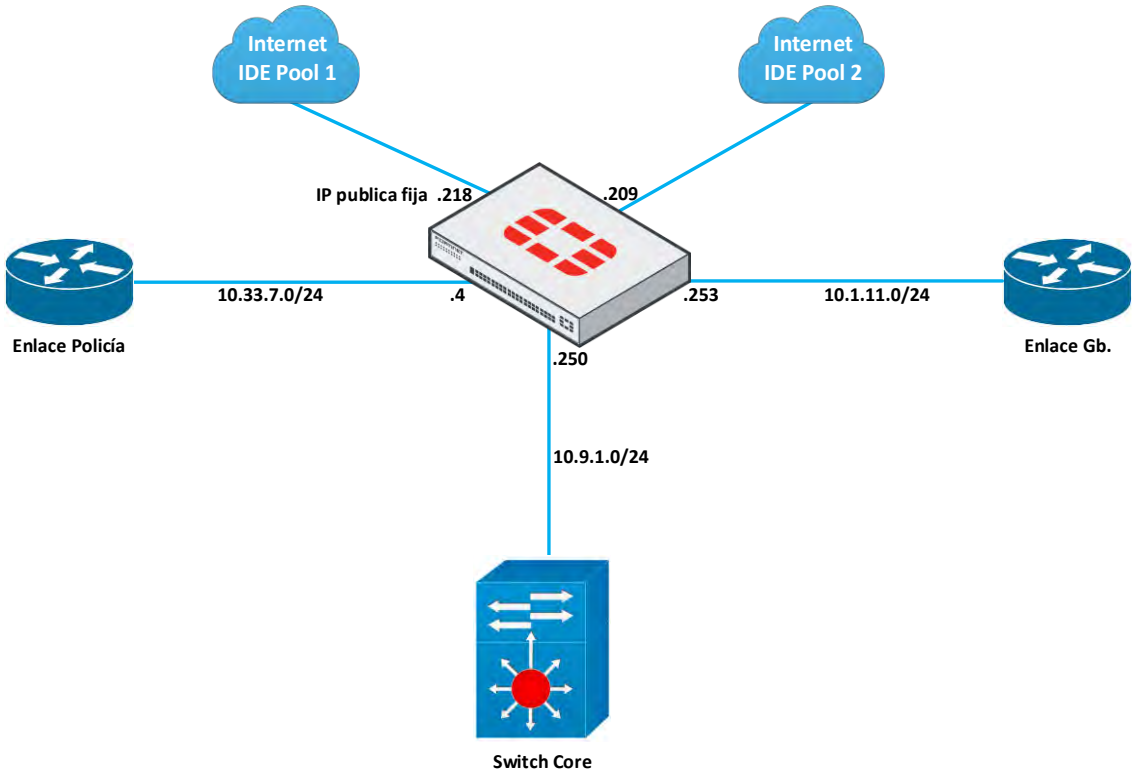


Figura 4-22. Diagrama lógico final

A continuación, en la Figura 4-23 se muestra el diagrama físico final de la interconexión del FortiGate.

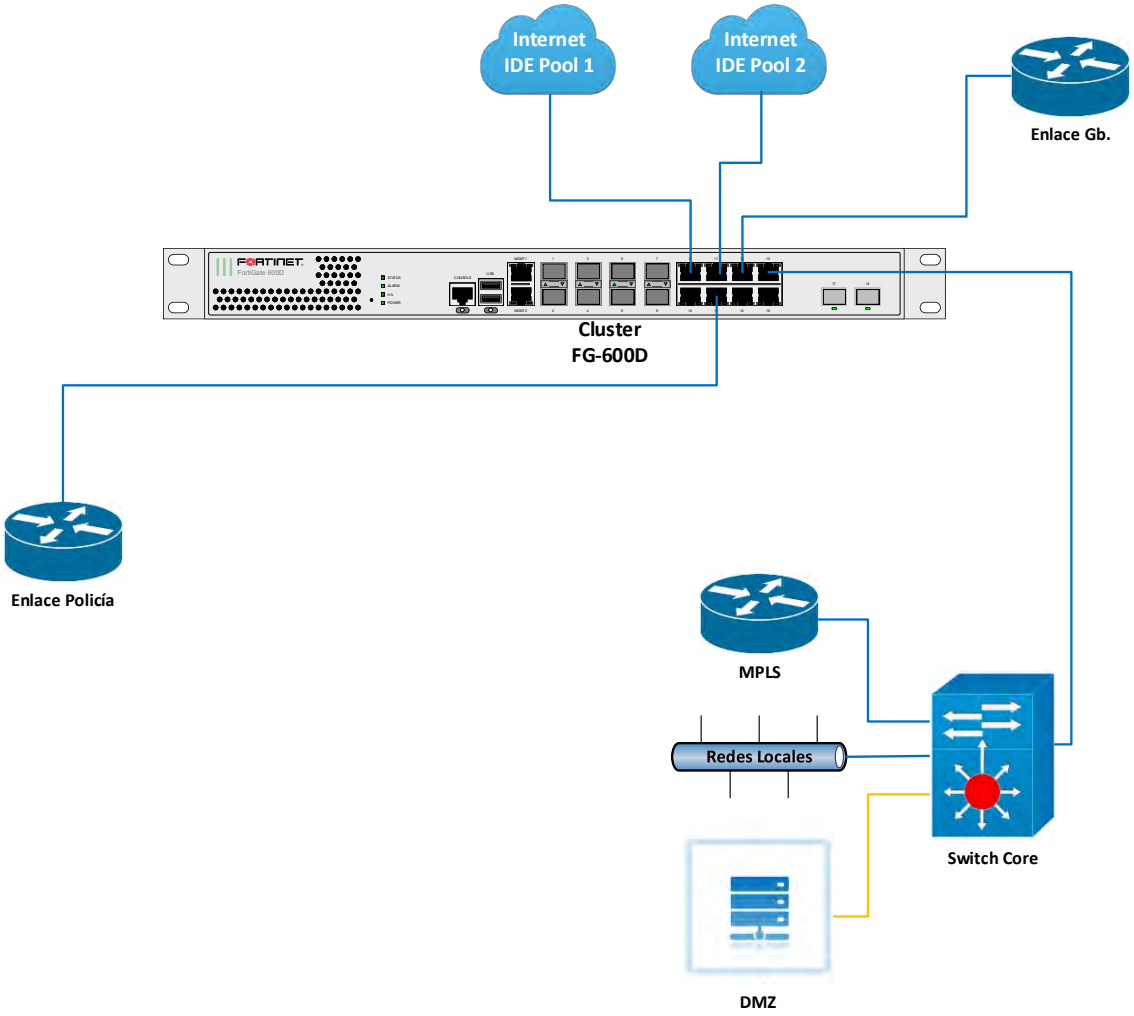


Figura 4-23. Diagrama físico final de la interconexión completa

La instalación consistió en configurar el FortiGate 600D en High Availability (HA) como gateway de navegación para ofrecer el control de perfiles de navegación y la aplicación del antivirus perimetral, de igual forma protegiendo y permitiendo solo el trafico necesario hacia los servidores que se encuentran en el datacenter.

Ahora se realizará el Clúster H.A. en modo Activo-Activo. Para eso, tendremos que desplazarnos al menú System, submenú H.A., como se muestra en la imagen 4-24.

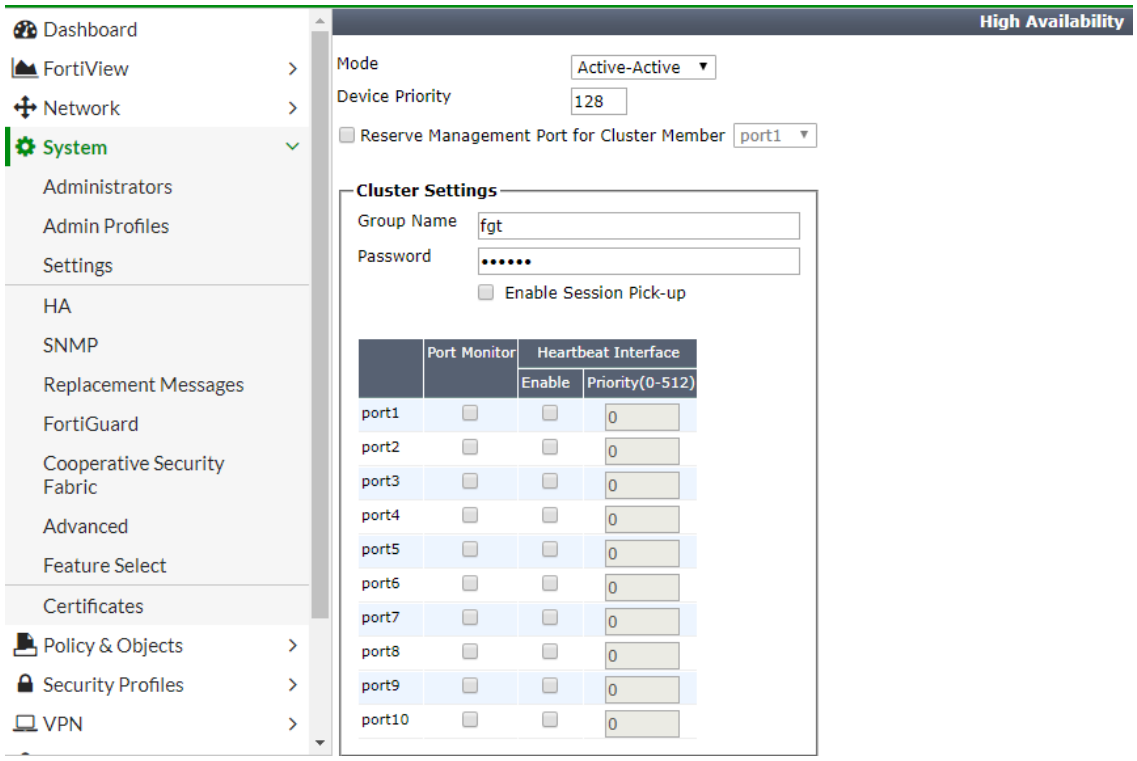


Figura 4-24. Configuración de alta disponibilidad

En el modo, se pone Active-Active, la prioridad del dispositivo en un FortiGate será de 128 y en el otro será de 64, esto para elegir quien tendrá el rol principal.

En el Group Name, se elegirá el nombre del clúster y una contraseña, esto es principalmente para evitar problemas con otros clústeres que se encuentren en la red.

Una vez terminada la configuración, se formará el clúster como se muestra en la Figura 4-25.

Figura 4-25. Monitor de la alta disponibilidad

La Figura 4-26, muestra la información del sistema del clúster FortiGate 600D.

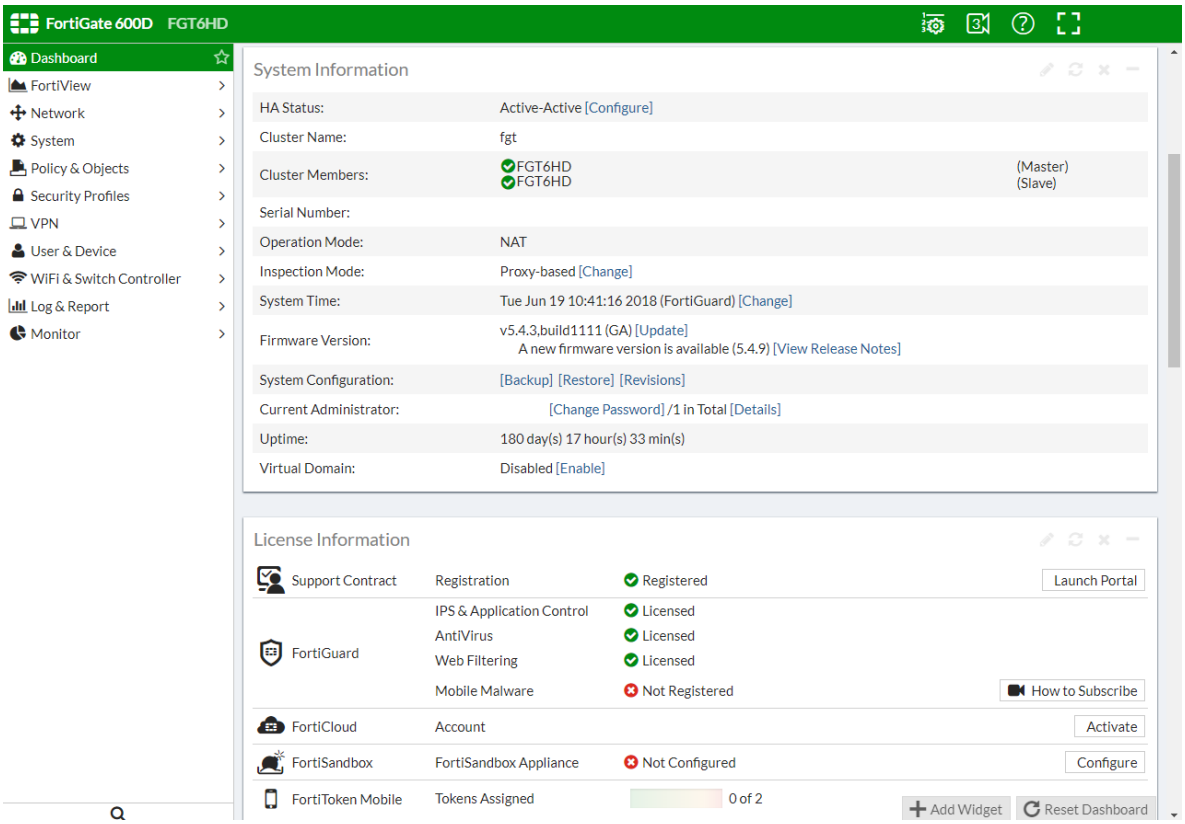


Figura 4-26. Dashboard del clúster

En esta ventana del dashboard que tiene el FortiGate, es para ver la información general del equipo, ahí podemos encontrar el estatus del HA, los nombres de los equipos y su rol, el modo de operación, fechas, información de licencias, entre otras cosas más.

Las interfaces del clúster se pueden encontrar en el menú Network, en la sección interfaces, como se muestra en la Figura 4-27.

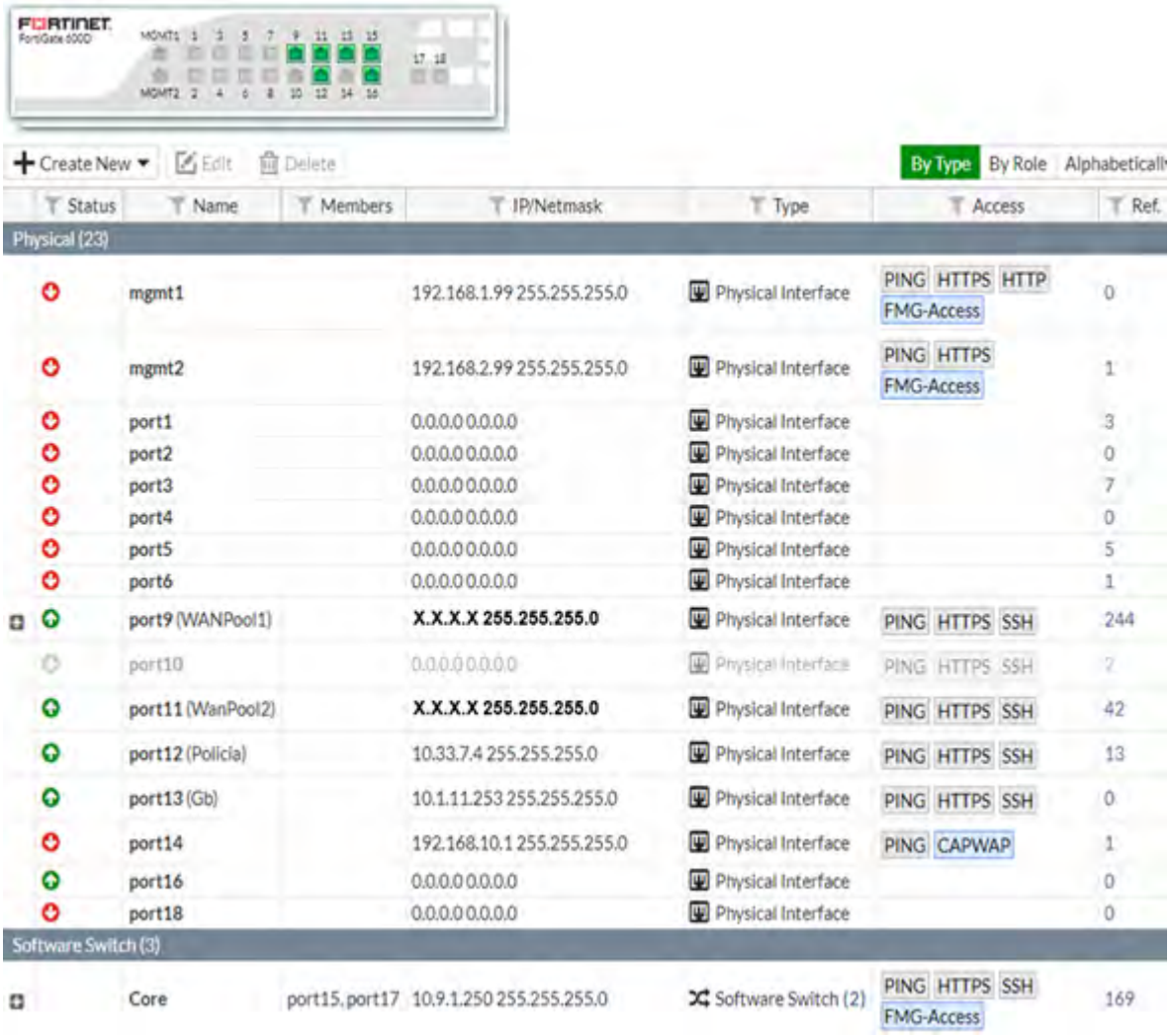


Figura 4-27. Interfaces del Clúster FortiGate

Por seguridad, se omitió la dirección IP pública fija. La interfaz 9 es el la WAN IDE Pool1, la interfaz 11 viene siendo la WAN IDE Pool2, y sirven principalmente para la publicación de sus servidores, además para otorgarles internet a sus usuarios dentro de la red LAN. La interfaz 12 es el enlace a la policía que ya tenían anteriormente configurado, la interfaz 13 es el enlace a Gb que también ya tenían configurado.

La interfaz 15 y 17 se configuró como modo switch y es el enlace al Switch Core para la red interna de la organización, la interfaz 17 es un puerto de fibra, que en ese momento no tenían un gigabit de fibra, pero se configuró para un futuro próximo.

Finalmente, la interfaz 16 se configuró como interfaz Hearbeat, que es el que mantiene las unidades de clúster comunicadas entre sí.

Para la configuración de las VPN a un sitio remoto, se realizó en una, y las demás el cliente se encargó de realizarlas, a continuación, se muestra un ejemplo de

los detalles más relevantes para la configuración de la VPN site-to-site en modo ruteo.

Para lograr la conexión VPN, se tiene que hacer tres pasos.

Primero, la configuración de la VPN, como se ve en la Figura 4-28.

```
config vpn ipsec phase1-interface
    edit "VPN_Forti"
        set interface "port1"
        set peertype any
        set proposal des-md5 des-sha512
        set remote-gw 172.16.1.20
        set psksecret ENC sXn1JVZCGORH6GCuIJyi2V7nBwhZa9XYzeKaQ97wk6OmiN4jQTcYgd
m3LiicL0nYLbaffBd/v8UHGb0RLX9P1Q9MHKVp4bVPXAWevVvYx1YgXnPdLy+nKLCB5jzmiLAFkw5IP
rI15a1icAPyEGkr1lMGvcZRRf89Ie0FgfUQWMwv/1Pq+Jd8FAdQEz1uwJEIrYNnA==
    next
end
```

Figura 4-28. Configuración de VPN IPsec por CLI del FortiGate local

Explicando la configuración CLI anterior:

- El nombre de la VPN es VPN_Forti.
- La comunicación que se establece entre un FortiGate y el otro FortiGate es por el puerto 1.
- La puerta de enlace del FortiGate remoto es la IP 172.16.1.20
- La contraseña viene cifrada.
- Para la fase 2, los quick mode selectors, se dejará por default, ya que en las políticas se hará la granularidad de las redes a comunicar.

Segundo, se crean dos políticas como se muestra en la Figura 4-29, uno va de la LAN que queremos comunicar a la VPN, y otra de la VPN a la LAN.

```
config firewall policy
    edit 1
        set name "Lan->VPN"
        set uuid bc866cb0-73bf-51e8-1d2d-7766e40c2986
        set srcintf "port4"
        set dstintf "VPN_Forti"
        set srcaddr "LAN_10.9.0.0"
        set dstaddr "LAN_192.168.50.0"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "VPN->Lan"
        set uuid ce57c948-73bf-51e8-3d09-c1dfc7ef62de
        set srcintf "VPN_Forti"
        set dstintf "port4"
        set srcaddr "LAN_192.168.50.0"
        set dstaddr "LAN_10.9.0.0"
        set action accept
        set schedule "always"
        set service "ALL"
    next
```

Figura 4-29. Configuración de políticas de firewall por CLI del FortiGate local

Explicando la configuración CLI anterior:

- En la política 1, el nombre es Lan->VPN.
- El puerto de origen es el puerto 4, donde se encuentra la LAN.
- La dirección origen es la LAN 10.9.0.0/16.
- El puerto destino es la VPN_Forti, que se creó anteriormente.
- La acción es aceptar, con un horario de siempre y aceptando todos los servicios.
  Para la política 2, el nombre es VPN->Lan.
- El puerto de origen es el puerto VPN_Forti, que es la LAN remota.
- La LAN de remota es la 192.168.50.0/24.
- La acción es aceptar, con un horario de siempre y aceptando todos los servicios.

Tercero, se debe crear una ruta estática con gateway de destino, como se muestra en la Figura 4-30.

```
config router static
    edit 1
        set dst 192.168.50.0 255.255.255.0
        set device "VPN_Forti"
    next
end
```

Figura 4-30. Configuración de ruta estática por CLI del FortiGate local

Explicando la configuración CLI anterior:

- Se crea una ruta estática con red de destino 192.168.50.0/24 que es la red remota.
- La red indicada se encontrará por la interfaz llamada VPN_Forti.

Con esto terminamos la configuración del FortiGate Local, para el FortiGate remoto son los mismos pasos, pero las direcciones serán al revés. A continuación, se muestra las configuraciones realizadas en el equipo remoto.

Primero la configuración de la VPN. Para la fase 1, la configuración es como se muestra en la Figura 4-31, se debe establecer la misma contraseña y la misma autenticación que la del FortiGate local, de lo contrario la VPN no se levantará.

```
config vpn ipsec phase1-interface
    edit "VPN_FGT"
        set interface "port1"
        set peertype any
        set proposal des-md5 des-sha512
        set remote-gw 172.16.1.10
        set psksecret ENC 3jLnI56NowzdQ30K+AVamyIgD86CoRJR20hMsznbbb2ubSzSJsov3g
LhuYTuz4GQYUqoNMJLezPNBIfp/LThlCxws8N/oK1UWBbqKYCqxQgFieaRaks5qbWiRVrOvge5yeOJzK
5G1kg86r/OoqYPcus3R8aI98VUwbjz26G20El1UpFZ252ncMV8qkJYVi1swMl1NA==
    next
end
```

Figura 4-31. Configuración de VPN IPsec por CLI del FortiGate remoto

Segundo, las políticas de firewall como se muestra en la Figura 4-32.

```
config firewall policy
    edit 1
        set name "lan->vpn"
        set uuid 852aa514-73c0-51e8-827d-6aa93ce3f803
        set srcintf "port4"
        set dstintf "VPN_FGT"
        set srcaddr "lan_192.168.50.0"
        set dstaddr "lan_10.9.0.0"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "vpn->lan"
        set uuid 936ec72c-73c0-51e8-168c-40def0e8783b
        set srcintf "VPN_FGT"
        set dstintf "port4"
        set srcaddr "lan_10.9.0.0"
        set dstaddr "lan_192.168.50.0"
        set action accept
        set schedule "always"
        set service "ALL"
    next
```

Figura 4-32. Configuración de la política del firewall por CLI del FortiGate remoto

Y tercero, la ruta estática.

```
config router static
    edit 1
        set dst 10.9.0.0 255.255.0.0
        set device "VPN_FGT"
    next
end
```

Figura 4-33. Configuración de ruta estática por CLI del FortiGate remoto

Con esto, la VPN debe estar arriba, para visualizarlo, se puede ver de manera simple en el GUI, en el menú Monitor, en la sección IPsec monitor, en la Figura 4-33, se ve un ejemplo de cómo debe verse.

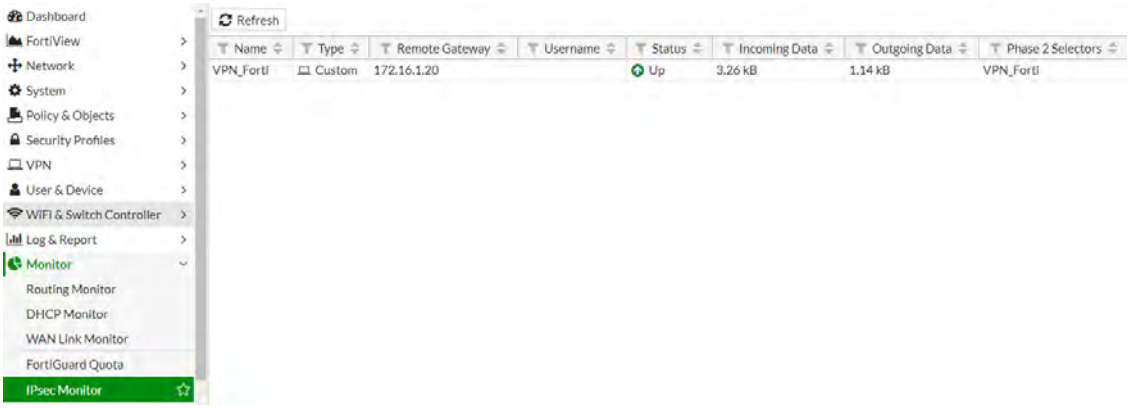


Figura 4-34. Monitor de IPsec

En la Figura 4-34 se ve un panorama del FortiGate local, donde su gateway remoto es la ip 172.16.1.20, el estatus es “Up”, hay comunicación entre las LAN al ver que hay datos entrando y saliendo, y al final se ve la fase 2 de los selectores.

Capítulo 5 : Resultados de la Implementación

5.1.- Resultados de la implementación

La implementación fue un éxito, la organización actualizó toda su infraestructura de datos y seguridad, incluyendo su cableado, que era necesario para que los equipos nuevos funcionaran a su máxima capacidad. La interconexión entre los equipos que se encuentran en el MDF y los IDF's eran por medio de cableado UTP, la cual fue sustituida por fibra óptica, sumándole a esto los conectores 10 Gigabit Ethernet (10GbE) entre cada conexión de switch, dándole un mejor desempeño a la red y multiplicando hasta por 10 veces su velocidad.

Dicha organización tenía como switch principal y con el que hacían el ruteo, dos equipos switches Cisco 3550G capa 3 que cumplían la función de Core, el cual estaba en alta disponibilidad mediante un protocolo que solo permitía un esquema activo-pasivo, sin embargo, en caso de falla era necesario hacer cambios físicos en los puertos ya que las conexiones a otros equipos solo se encontraban en uno de los switches, esto debido a que juntos sumaban 36 puertos Ethernet.

Se instalo un nuevo equipo switch Cisco Core 4500, el cual está conformado con 24 puertos fibra óptica a 10 gbps, que es por donde se logra la comunicación entre el MDF y los IDF's y que, de ser necesario, pueden adquirir otra navaja para aumentar la cantidad de puertos fibra. Además, actualmente cuentan con 96 puertos RJ45, y también, de ser necesario, pueden adquirir otra navaja aumentan la cantidad de puertos que requiera la empresa, este equipo Cisco es de 10 navajas, las cuales solo están ocupadas por 6. De igual forma cuentan con una alta disponibilidad, ya que este switch Cisco Core tiene dos fuentes de alimentación eléctrica y tienen dos supervisoras que ofrecen esta alta disponibilidad para asegurar la continuidad del servicio. Este equipo

En la tabla 41, se ve una comparación de algunas características entre el switch antiguo y el switch nuevo.

Tabla 41. Tabla comparativa del Cisco Core antiguo y el nuevo

Descripción	Cisco 3560G	Cisco 4510E
Cantidad de puertos RJ45.	36 puertos fijos.	96 puertos expandibles.
Velocidad por puerto RJ45.	34 puertos 10/100 2 puertos 10/100/1000	Todos los puertos a 10/100/1000
Soporte PoE puertos RJ45.	N/A	Los 96 puertos.
Cantidad de puertos fibra.	N/A	24 puertos expandibles.
Velocidad de puerto fibra.	N/A	10 Gbps.

Dicha organización contaba con equipos Cisco 2950 muy antiguos de 24 puertos, estos eran utilizados como switch de acceso para el usuario final, además tenían switches de otras marcas que no eran administrables, teniendo un gran problema en ese punto, ya que contaban con un nuevo equipo de VoIP y su telefonía

funcionaban solamente en las áreas donde habían switches administrables, de la misma manera, su velocidad máxima que alcanzaban era de 100 Mbps por puerto del switch.

Los nuevos equipos Cisco 2960X, cuentan con 48 puertos ethernet que, además de ser de una velocidad 10/100/1000, está disponible la energía PoE que cuenta con hasta 30W, muy útil para los nuevos equipos de telefonía que la empresa estaba adquiriendo, también cuenta con dos interfaces SFP+, para la interconexión de fibra a 10 Gbps. De igual forma, estos equipos tienen la posibilidad de estar en modo stack que cuenta con hasta 80 GB de ancho de banda de stack y hasta 8 miembros en un stack, que también te permite una mejor administración de los equipos.

Cabe mencionar que los nuevos switches Cisco, son de bajo consumo y soporta la tecnología EnergyWise, la cual ayuda a las empresas a gestionar el consumo de energía de la infraestructura de red y los dispositivos conectados en los switches, reduciendo así sus costos de energía y su huella de carbono. Estos equipos switch Cisco son mucho más ahorrativos que sus predecesores, ayudan a maximizar la productividad y proporcionen protección de la inversión al permitir una red unificada para datos, voz y video.

A continuación, en la Tabla 42 comparativa entre el switch antiguo y el nuevo.

Tabla 42. Tabla comparativa del switch de acceso antiguo y nuevo

Descripción	Cisco 2950 y otros.	Cisco 2960X
Cantidad de puertos RJ45.	24 puertos	48 puertos
Velocidad por puerto RJ45.	10/100	10/100/1000
Soporte PoE puertos RJ45.	N/A	Los 48 puertos
Cantidad de puertos fibra.	N/A	2 puertos SFP+
Velocidad de puerto fibra.	N/A	10 Gbps.

Conclusiones

En este trabajo monográfico se trata de mostrar al lector como se lleva a cabo el trabajo de campo de un ingeniero en tecnologías de la información, desde que el equipo comercial tiene el primer contacto con el cliente, el equipo de arquitectura da una posible solución a su problemática, el equipo de consultoría e ingeniería diseñan la solución, hasta donde el equipo de ingeniería nuevamente, entra en su rol para la implementación del proyecto.

Como resultado del presente trabajo se resumen las conclusiones de la siguiente manera:

En cuanto a la tecnología Cisco:

Para el switching y el routing, la tecnología Cisco fue seleccionada por el cliente de entre las múltiples opciones de proveedores que se le dio a conocer. Esta tecnología es muy popular a nivel internacional ya que Cisco cuenta con mucho material de estudio y laboratorios para su práctica e implementación, además que tienen una academia para un mejor entendimiento, esto al cliente le interesó bastante ya que su idea es tener ellos mismos una administración de los equipos.

Generalmente, se les resta importancia a factores tales como la escalabilidad, el crecimiento, y la fiabilidad; esto produce a menudo costos ocultos tales como caídas de red y pérdida de productividad y la pérdida de oportunidades.

En cuanto a la tecnología Fortinet.

Para la seguridad perimetral, la tecnología Fortinet FortiGate fue elegida y definitiva por el cliente, la organización anteriormente ya había manejado diferentes equipos de seguridad, pero el equipo FortiGate es el que más ha gustado.

La línea de productos Fortinet está pensada para satisfacer las necesidades de una gran cantidad de clientes, desde pequeñas empresas hasta grandes corporaciones. La gran ventaja que tiene sobre todas sus competencias, es la administración en una sola consola como se menciona durante esta monografía. Lo que un administrador busca es tener una flexibilidad a la hora de administrar sus equipos, FortiGate la otorga, en lugar de utilizar muchos equipos diferentes para distintas funciones, el equipo de FortiGate las tiene implementadas en un mismo dispositivo, por ejemplo, el control de aplicaciones, el antivirus, el filtro web, el anti Spam, la aceleración WAN, optimización de tráfico, VPN, IPS, controlados inalámbrico, entre otras.

Bibliografía

[1] J. Niño, Sistemas operativos monopuesto, Editorial Editex, 2011.

[2] J. Dordoigne, Redes Informaticas, nociones fundamentales, Paris: ENI, 2009.

[3] Cisco, «Introduction to Networks,» 1997. [En línea]. Available: www.netacad.com. [Último acceso: 20 09 2017].

[4] B. A. Forouzan, Transmisión de datos y redes de comunicaciones, Madrid: McGRAW-HILL, 2002.

[5] E. Ariganello y E. Barrientos Sevilla, Redes Cisco. Guía de estudio para la certificación CCNP., Madrid, España: RA-MA, S.A., 2014.

[6] Cisco, «CCNA R&S: Scaling Networks,» Cisco, 1997. [En línea]. Available: www.netacad.com. [Último acceso: 10 09 2017].

[7] Cisco, «CCNA Routing and Switching: Routing and Switching Essentials,» Cisco, 1997. [En línea]. Available: www.netacad.com. [Último acceso: 07 02 2018].

[8] D. E. Comer, Internetworking with TCP/IP principles, protocolos, and architectures, New Jersey: PRENTICE-HALL INTERNATIONAL, 2007.

[9] Cisco Systems, Inc., CCNA Routing and Switching 200-125, Indianapolis: Cisco Press, 2016.

[10] Fortinet, Inc., «partnerportal,» Febrero 2018. [En línea]. Available: partnerportal.fortinet.com. [Último acceso: 30 Marzo 2018].

[11] Fortinet, Inc., «training fortinet,» 2016. [En línea]. Available: training.fortinet.com. [Último acceso: Abril 2018].

[12] W. Stallings, Data and Computer Communications, New Jersey: Pearson Prentice Hall, 2007.

[13] J. K. &. K. Ross, Computer Networking, Massachusetts: Pearson, 2017.

[14] AVAST, «avast,» Avast Software s.r.o., 2016. [En línea]. Available: www.avast.com. [Último acceso: 10 Junio 2018].