

UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA ELECTRÓNICA TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

"INGENIERO ELECTRÓNICO"

TITULO DEL PROYECTO TÉCNICO:

"DISEÑO E IMPLEMENTACIÓN DE UN BANCO DE PRUEBAS VIRTUALIZADO CON TECNOLOGÍA DE REDES DEFINIDAS POR SOFTWARE PARA REDES DE AREA AMPLIA (SD-WAN) EN EL LABORATORIO DE TELECOMUNICACIONES PARA LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL"

AUTORES

VERA VÉLEZ ERICK ÁLVARO LLAMBO VERA OSCAR OMAR

DIRECTOR

PhD. BREMNEN VÉLIZ NOBOA

GUAYAQUIL – ECUADOR

2021

CERTIFICADOS DE RESPONSABILIDAD Y AUTORÍA

Nosotros, Vera Vélez Erick Álvaro y Llambo Vera Oscar Omar permitimos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de titulación y su respectiva trascripción sin fines de lucro. También, exponemos que los conceptos, análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de los autores.

Vera Velez Erick Álvaro Cl: 0930497151

Llambo Vera Oscar Omar Cl: 0923652903

CERTIFICADO DE CESIÓN DE DEREECHOS DE AUTOR

Nosotros, Erick Álvaro Vera Vélez con documento de identificación N° 0930497151 y Oscar Omar Llambo Vera con documento de identificación N° 0923652903, declaramos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación titulado "DISEÑO E IMPLEMENTACIÓN DE UN BANCO DE PRUEBAS VIRTUALIZADO CON TECNOLOGÍA DE REDES DEFINIDAS POR SOFTWARE PARA REDES DE AREA AMPLIA (SD-WAN) ΕN EL LABORATORIO DE TELECOMUNICACIONES PARA LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL ", mismo que ha sido desarrollado para optar por el título de "INGENIERO ELECTRÓNICO", en el laboratorio de telecomunicaciones de la Universidad Politécnica Salesiana sede Guayaguil, quedando la Universidad autorizada para ejercer plenamente los derechos aprobados anteriormente.

Vera Velez Erick Álvaro CI: 0930497151

Llambo Vera Oscar Omar Cl: 0923652903

CERTIFICADO DE DIRECCIÓN DE TRABAJO DE TITULACIÓN

Yo PhD. Bremnen Véliz, expresó que bajo mi dirección y asesoría fue proyecto técnico de desarrollado el titulación "DISEÑO Е IMPLEMENTACIÓN DE UN BANCO DE PRUEBAS VIRTUALIZADO CON TECNOLOGÍA DE REDES DEFINIDAS POR SOFTWARE PARA REDES DE AREA AMPLIA (SD-WAN) EN EL LABORATORIO DE TELECOMUNICACIONES PARA LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL", realizado por los estudiantes VERA VÉLEZ ERICK ÁLVARO con cédula ciudadanía 0930497151 y LLAMBO VERA OSCAR OMAR con cedula de ciudadanía 0923652903 obteniendo un producto que cumple con los objetivos del diseño de aprobación, informe final y además los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerado como trabajo final de titulación.

Onerun M

Tutor del Trabajo de titulación Docente Ing. Bremnen Véliz Noboa, PhD. Cl: 0703865139

DECLARATORIA DE RESPONSABILIDAD

Nosotros, Erick Álvaro Vera Vélez portador de la cédula de identidad N° 0930497151 y Oscar Omar Llambo Vera portador de la cedula de identidad N° 0923652903, estudiantes de la Universidad Politécnica Salesiana con sede Guayaquil, expresamos que la responsabilidad del contenido de este proyecto de titulación pertenece meramente y es propiedad intelectual de la Universidad Politécnica Salesiana sede Guayaquil.

Vera Velez Erick Álvaro CI: 0930497151

Llambo Vera Oscar Omar CI: 0923652903

DEDICATORIA

Este proyecto de titulación va dedicado inicialmente a Dios y a mis padres, quienes me han conducido y apoyado durante todo este tiempo en mis estudios para culminarlos y ser un profesional.

Agradezco a mi padre el Ab. Rolando Vera por su ayuda constante y esfuerzo para lograr este objetivo también a mi madre la Sra. Digna Vélez por sus consejos que me dio durante toda la vida desde que. fui un niño a hasta ahora a ellos le dedico cada logro personal y profesional que he alcanzado.

Erick Álvaro Vera Vélez

DEDICATORIA

La presente tesis esta dedicada a mis padres ya que sin ellos no sabia posible lograr concluir mis proyectos profesionales. También quiero dedicar este proyecto a mis hermanos que creyeron en mi y me apoyaron para que persista en mis objetivos y por ultimo a mis compañeros que estuvieron desde el principio y a lo que se unieron en el camino y fueron de gran compañía en todos estos años.

Oscar Omar Llambo Vera

.

AGRADECIMIENTO

Agradezco a Dios primeramente por haberme dado la vida, salud y sabiduría para llegar a esta etapa de mi vida que es mi titulación como profesional logrando superar cada uno de los obstáculos que se presentan, gracias a mi familia y a mi hija Emma Vera que fueron el motor principal para obtener hoy esta alegría y por apoyarme en cada decisión de este proyecto también me gustaría agradecer a los docentes de la carrera por sus enseñanzas en el aula y sus experiencias que nos compartían durante toda mi carrera universitaria porque todos han aportado con un granito de arena a mi formación como profesional.

Erick Álvaro Vera Vélez

AGRADECIMIENTO

En primera instancia quiero agredecer a Dios, a mis padres ya que me supieron inculcar el trabajo e integridad, a mis compañero tesista ya que sin ellos no había sido posible este proyecto. Deseo expresar mis mas sinceros agradecimiento hacia la Universidad Polictécnica Salesiana sede Guayaquil, a sus directivos y docentes por haberme formado como profesionales a lo largo de estos años

Oscar Omar Llambo Vera

RESUMEN DEL PROYECTO

La presente tesis: "DISEÑO E IMPLEMENTACIÓN DE UN BANCO DE PRUEBAS VIRTUALIZADO CON REDES DEFINIDAS POR SOFTWARE (SD-WAN) EN EL LABORATORIO DE TELECOMUNICACIONES PARA LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL", se basa en la necesidad de contar con un banco de prueba virtualizado para REDES POR SOFTWARE, MPLS, FRAME DEFINIDAS RELAY, BGP, ENRUTAMIENTO ESTÁTICO, SWTICHES ADMINISTRABLES y para diferentes tipos de tecnologías de routers, firewall, switches que se encuentran en las empresas donde los estudiantes y los docentes podrán configurar estos dispositivos, observar el comportamiento y la fiabilidad de la red viendo que dispositivo es más seguro en el momento de implementación para la proteger la información de los usuarios finales y aprender de ellos.

El estudio de esta nueva tecnología se fundamenta en controlar la demanda de servicios, ancho de banda, menor ping para mejorar la optimización de la capacidad de la red donde la redes definidas por software escogen el enlace WAN con menor fluctuación. Para la simulación de esta tecnología se virtualizo un servidor DELL R210 II que se encuentra en el laboratorio de telecomunicaciones el cual se optimizó en memorias ram y disco duros SSD para mejor rendimiento en el momento de la simulación.

El objetivo de este proyecto es constuir un banco de pruebas virtualizado para ayudar a los estudiante y docentes de la universidad para simular ROUTERS, SWITCH, FIREWALL de diferentes marcas comerciales, los estudiantes no cuentan con un infraestructura donde se pueda simular estas nuevas tecnologías de redes para realizar las configuraciones de estos dispotivos, el laboratorio de telecomunicaciones cuenta con el programa CISCO PACKET TRACER que solo permite simular los dispositivos que vienen en su software permitiendo una configuración restringida en el momento de diseñar una topología de una red por ejemplo al configurar una red MPLS las versiones actuales no permiten la configuración de esta tecnología.

ABSTRACT

This thesis: "DESIGN AND IMPLEMENTATION OF A VIRTUALIZED TEST BANK SOFTWARE WITH **NETWORKS** DEFINED ΒY (SD-WAN) IN THE TELECOMMUNICATIONS LAB FOR THE UNIVERSIDAD POLITÉCNICA SEDE GUAYAQUIL", is based on the test of having a virtualized NETWORK DEFINED BY SOFTWARE, MPLS, FRAME RELAY, BGP, STATIC ROUTING, ADMINISTRABLE SWTICHES and for different types of technologies of routers, firewall, switches found in companies where students and teachers can configure these devices, observe the behavior and the network reliability seeing that the device is more secure at the time of deployment to protect the information of the end users and learn from them.

The study of this new technology is based on controlling the demand for services, bandwidth, lower ping to improve the optimization of network capacity where softwaredefined networks choose the WAN link with the least fluctuation. For the simulation of this technology, it was virtualized on a DELL R210 II server that is in the telecommunications laboratory, which was optimized in ram memories and SSD hard drives for better performance at the time of simulation.

The objective of this project is to build a virtualized test bed to help university students and teachers to simulate ROUTERS, SWITCH, FIREWALL of different commercial brands, the students do not have an infrastructure where these new network technologies can be simulated To configure these devices, the telecommunications laboratory has the CISCO PACKET TRACER program that only allows simulating the devices that come in its software allowing a restricted configuration when designing a network topology, for example when configuring a network MPLS current versions do not allow the configuration of this technology.

Tabla de contenido

CERTIFICADOS DE RESPONSABILIDAD Y AUTORÍA	
CERTIFICADO DE CESIÓN DE DEREECHOS DE AUTOR	
CERTIFICADO DE DIRECCIÓN DE TRABAJO DE TITULACIÓN	
DECLARATORIA DE RESPONSABILIDAD	5
DEDICATORIA	6
DEDICATORIA	7
AGRADECIMIENTO	
AGRADECIMIENTO	9
RESUMEN DEL PROYECTO	
ABSTRACT	
INTRODUCCIÓN	29
CAPÍTULO I	
1.1. DESCRIPCIÓN DEL PROBLEMA	
1.2. ANTECEDENTES	
1.3. IMPORTANCIA Y ALCANCES	
1.4. DELIMITACIÓN	
1.4.1. ESPACIAL	
1.4.2. ACADÉMICA	
1.4.3. TEMPORAL	
1.5. OBJETIVOS	
1.5.1 OBJETIVO GENERAL	
1.5.2 OBJETIVOS ESPECIFICOS	
1.5.2 DESCRIPCIÓN DE LA PROPUESTA	¡Error! Marcador no definido.
1.5.2 METODOLOGÍA	
1.5.2 BENEFICIARIOS DE LA PROPUESTA E INTERVENCIÓN	
CAPÍTULO II	
MARCO TEÓRICO	
2.1. VIRTUALIZACIÓN	
2.2.1. TIPOS DE VIRTUALIZACIÓN	
2.2.2. VIRTUALIZACIÓN POR SERVIDORES	
2.2.3. VIRTUALIZACIÓN POR MEMORIAS	
2.2.4. VIRTUALIZACIÓN DE ALMACENAMIENTO (STORAGE	

2.2	2.5.	VIRTUALIZACIÓN DE ESCRITORIO (DESKTOP)	36
2.2	2.6.	VIRTUALIZACIÓN DE REDES (NETWORK)	36
2.3.	TIPO	DS DE REDES	37
2.3	8.1.	SEGÚN SU EXTENSIÓN	37
2.3	3.2.	SEGÚN SU TOPOLOGÍA	39
2.3	8.3.	SEGÚN EL TIPO DE ACCESO A LA RED	42
2.3	8.4.	SEGÚN EL MEDIO DE TRANSMISIÓN	43
2.4.	DISI	POSITIVOS DE INTERCONEXIÓN DE REDES	44
2.5.	CAE	BLEADO ESTRUCTURADO	48
2.5	5.1.	CONJUNTO DE CABLEADO ESTRUCTURADO	48
2.6.	TIPO	OS DE SOFTWARE PARA EMULAR REDES INFORMÁTICAS	54
2.7.	SER	VIDORES	55
2.7	7.1.	TIPOS DE DISEÑOS DE SERVIDORES	56
2.7	7.2.	SISTEMAS RAID SERVIDORES	56
2.7	7.3.	SOFTWARE DEL SERVIDOR	58
2.7	7.4.	ESTRUCTURA CLIENTE/SERVIDOR	59
CAPÍ	TULO I	III	60
DISEŔ	ŇΟ Ε ΙΙ	MPLEMENTACION DEL BANCO DE PRUEBAS	60
3.1.	PRC	POSITO DEL DISEÑO	60
3.2.	CON	NSTRUCCIÓN DEL BANCO DE PRUEBA	61
3.3.	CON	NFIGURACIÓN DE DISCO DUROS DEL SERVIDOR DELL R210 II	64
3.4.	INS	TALACIÓN DEL SISTEMA OPERATIVO EXSI 6.5 U3 EN EL SERVIDOR DELL R210 II	67
3.5.	CON	NFIGURACIÓN DE GNS3-SERVER EN EL SERVIDOR	75
3.6.	INS	TALACIÓN DE LOS IOS EN EL SERVIDOR GNS3	84
3.7.	DES	CRIPCIÓN TÉCNICA DE LOS DISPOSITIVOS DEL BANCO	88
3.8.	Dell	PowerEdge R210 II	89
3.9.	KIN	GSTON A400 SSD SATA de 2,5"	89
CAPÍ	TULO I	IV	90
MAN	UAL D	E PRÁCTICAS DEL LABORATORIO	90
4.1.	GUI	A DE PRÁCTICAS PARA PRUEBAS DE REDES DEFINIDAS POR SOFTWARE PARA REE	DES
DE AI	rea ai	MPLIA (SD-WAN)	90
4.1	.1.	PRÁCTICA 1	91
4.1	2.	PRÁCTICA 2	96

4.1.3.	PRÁCTICA 3	117
4.1.4.	PRÁCTICA 4	134
4.1.5.	PRÁCTICA 5	155
4.1.6.	PRÁCTICA 6	169
4.1.7.	PRÁCTICA 7	182
4.1.8.	PRÁCTICA 8	197
4.1.9.	PRÁCTICA 9	215
4.1.10.	PRÁCTICA 10	228
CAPÍTULO	۷	
ANÁLISI	S DE RESULTADOS	243
5.1.	Análisis del proyecto	243
5.2.	Comunicación de las computadoras clientes al servidor	
5.3.	Elaboración del banco de prueba y prácticas	243
5.4.	Pruebas realizadas	243
CAPÍTULO	VI	246
CONCLU	JSIONES	246
CAPÍTULO	VII	248
RECOMI	ENDACIONES	248
CAPÍTULO	VIII	249
REFERE	NCIAS BIBLIOGRAFÍA	249
CAPÍTULO	IX	250
ANEXOS		250
ANEXO	A. CRONOGRAMA DE DURACIÓN DEL PROYECTO	250
ANEXOS	B. Sistemas Operativos de virtualización	250
ANEXO	C. DELL R210 II	251
ANEXO	D. Disco Solido SSD	253
ANEXO	E. LISTADO DE MATERIALES	253

Tabla de ilustraciones

Figura 1 Vista de una virtualización
Figura 2 Virtualización de un servidor
Figura 3. Virtualizacon de memoria
Figura 4. Virtualizacon de Almacenamiento
Figura 5. Virtualizacion de Escritorio
Figura 6
Figura 7. Red Pan
Figura 8. Red Lan
Figura 9. Red Metropolitana
Figura 10. Red Wan
Figura 11. Topologia en Bus
Figura 12.Topologia en Anillo
Figura 13. Topología en Estrella40
Figura 14. Topología Jerárquica41
Figura 15. Topología de Malla41
Figura 16. Topologia de red lógica42
Figura 17. Red pública
Figura 18. Red privada
Figura 19. Red cableda
Figura 20. Red inalambrica 44
Figura 21. HUB
Figura 22. Conmutadores o switches 45
Figura 23. Enrutadores o routers
Figura 24. Enrutadores o routers
Figura 25. Módem
Figura 26. Cable módem

Figura 27. Cableado Campus	48
Figura 28. Sala de Equipamiento	49
Figura 29. Cableado Troncal	49
Figura 30. Sala de Equipamiento	50
Figura 31. Cableado Horizontal	50
Figura 32. Área de trabajo	51
Figura 33. Par tranzado no apantallado	52
Figura 34. Par tranzado apantallado	53
Figura 35. Cable multipar	53
Figura 36 Cisco Packet Tracer	54
Figura 37. GNS3	55
Figura 38. NETSIM	55
Figura 39. Parte interna de un servidor	56
Figura 40. RAID 0	57
Figura 41. RAID 1	57
Figura 42. RAID 5	58
Figura 43. Software de Virtualización	58
Figura 44. Modelo Cliente-Servidor	59
Figura 45. Diseño del banco de prueba	60
Figura 46. Desmontar Dell R210 II	61
Figura 47 Mantenimiento Correctivo Dell R210 II	61
Figura 48. Desmontaje del disipador y aplicación de pasta térmica Dell R210 II	62
Figura 49. Instalación SSD Dell R210 II y memorias ram	63
Figura 50. Configuración de los discos duros Dell R210 II	64
Figura 51. SAS controller PERC H200A Dell R210 II	64
Figura 52. Raid propiedades Dell R210 II	65
Figura 53. Selección del RAID 1 Dell R210 II	65

Figura 54. Selección de disco duros Dell R210 II	66
Figura 55. Selección del RAID 1 Dell R210 II	66
Figura 56. Boot Manager Dell R210 II	68
Figura 57. Boot CD-ROM 1 Dell R210 II	68
Figura 58. Boot Menu Dell R210 II	68
Figura 59. Loading Exsi 6.5.0	69
Figura 60. Welcome Exsi 6.5	69
Figura 61. Términos y Condiciones Exsi 6.5	70
Figura 62 Instalación Exsi 6.5	70
Figura 63.Configuración del idioma del teclado Exsi 6.5	71
Figura 64 Contraseña del Exsi 6.5	71
Figura 65.Contraseña del Exsi 6.5	72
Figura 66. SO EXSI 6.5	72
Figura 67.Autenticación del Exsi 6.5	73
Figura 68.Configure Network Exsi 6.5	73
Figura 69.Configurar ipv4	74
Figura 70. Configurar IP estática	74
Figura 71. Confirmación de cambios en la tarjeta de red	75
Figura 72.Descarga VMware ESXi 2.2.16	75
Figura 73. Descomprimir archivo zip Exsi 2.2.16	76
Figura 74.Login Exsi 6.5 Browser	76
Figura 75.Máquina Virtual Exsi 6.5	77
Figura 76.Creación de la máquina virtual	77
Figura 77.Instalación de la máquina Virutal	78
Figura 78.Selección de almacenamiento	78
Figura 79.Aprovisionamiento fino máquina virtual	79
Figura 80.Instalación OVF GNS3	79

Figura 81.Performance de la máquina virtual	80
Figura 82. Encendido de la máquina virtual	80
Figura 83.GNS3-SERVER encendida	81
Figura 84. Ventana de configuración GNS3 2.2.16	81
Figura 85.Network GNS3 2.2.16	82
Figura 86. Configuración IP estática GNS3 2.2.16	83
Figura 87. GNS3 2.2.16	84
Figura 88.Import appliance GNS3 2.2.16	85
Figura 89.Ubicación del archivo Gns3	85
Figura 90.Selección de instalación	86
Figura 91.Selección de instalación	86
Figura 92.Selección del archivo vmware disk	87
Figura 93. Selección del archivo vmware disk	87
Figura 94. Finalización del archivo	88
Figura 95. Dell R210 II	89
Figura 96.SSD Kingston A400	89
Figura 97. Descargar Gns3	92
Figura 98. Conexión al servidor	93
Figura 99. Datos de conexión al servidor	94
Figura100. Conexión establecida a gns3 server	94
Figura101. Proyecto en Gns3	95
Figura102. Nuevo proyecto	97
Figura103. Diseño de la red práctica №2	97
Figura104. Encendido de sucursales fortigate 6.2.0	98
Figura105. Ingresar CLI Sucursal 2	98
Figura106. Visualización del CLI	99
Figura 107. Dirección IP sucursal 2 del Fortigate 6.2.0	99

Figura108. Interfaz Web Fortigate	100
Figura109. Selección del port2 sucursal 2	100
Figura110. Configuración del port2	101
Figura111. Interface Virtual	101
Figura112. Configuración de interfaz VLAN-IP	102
Figura113. Configuración de DHCP interfaz VLAN 10	102
Figura114. Interfaces Configuradas Fortigate Oficina Central	103
Figura115. Módulo de static routes	103
Figura116. Configuración static routes	104
Figura117. Ping a Google	104
Figura 118. Ipv4 Policy Sucursal 2	105
Figura119.Configuración de los servicios Sucursal 2	105
Figura120. Políticas Vlan 10	105
Figura121.Configuración de las políticas para Sucursal 1	106
Figura122. Iniciando Switch	107
Figura123. Creación VLAN-10 Datos	107
Figura124. Puerto Trunk VLAN	108
Figura125. Puerto Access VLAN 10	108
Figura 126. Comprobación de internet PC3 Sucursal 2	109
Figura 127. Comprobación de internet PC3 Sucursal 2	109
Figura128. Browser Fortigate Sucursal 2	110
Figura 129. Port2 Fortigate Sucursal 2	110
Figura130.Configuración del port2 sucursal 1	111
Figura131.Interfaz Vlan Sucursal 1	111
Figura132. DHCP VLAN Sucursal 1	112
Figura133.SD-WAN Sucursal 1	112
Figura 134. Configuracion Static Routes Sucursal 1	113

Figura135.Interfaz IPv4 Policy Sucursal 1	113
Figura136.Configuracíon IPv4 Policy Sucursal 1	114
Figura137.Ping Google Fortigate Sucursal 1	114
Figura 138. Configuración VLAN 20	115
Figura139. Puerto Trunk switch Sucursal 1	115
Figura 140. Puerto Access VLAN 20	116
Figura 141. Verificacion de red local y navegación Sucursal 1	116
Figura 142. Diseño de la red práctica Nº3	118
Figura 143.Configuracion IP fortigate principal port2	119
Figura 144.Configuracion IP fortigate principal port3	119
Figura 145.Configuracion IP fortigate principal port4	120
Figura 146.Configuracion IP fortigate principal port5	120
Figura 147. Crear zonas de interfaces	121
Figura 148. Interface members fortigate principal	121
Figura 149. Interface members fortigate principal	122
Figura 150. Static routes fortigate principal	122
Figura 151. Regla de internet para el fortigate sucursal 1	123
Figura 152. Regla de internet para fortigate sucursal 2	123
Figura 153. Dirección IP port2 fortigate sucursal 1	124
Figura 154. Dirección IP port3 fortigate sucursal 1	124
Figura 155. Configuración red local del fortigate	125
Figura 156. SD-WAN zone fortigate sucursal 1	125
Figura 157. SD-WAN enlace wan 1	126
Figura 158. SD-WAN enlace WAN 1	126
Figura 159. Static routes para SD-WAN fortigate sucursal 1	127
Figura 160. Static routes para SD-WAN fortigate sucursal 1	127
Figura 161. Configuración de static routes SD-WAN del fortigate	128

Figura 162. Configuración de static routes SD-WAN del fortigate	128
Figura 163. Diagrama de calidad de sevicio de sucrusal 1	129
Figura 164. Configuracion IP fortigate WAN sucrsal 2	129
Figura 165. Configuracion IP fortigate WAN sucursal 2	130
Figura 166. Configuración red local del fortigate	130
Figura 167.SD-WAN zone fortigate sucursal 2	131
Figura 168. SD-WAN sucursal 2 para puerto 2	131
Figura 169. SD-WAN sucursal 2 para puerto 3	132
Figura 170. Static routes para SD-WAN fortigate sucursal 2	132
Figura 171. Static routes para sd-wan fortigate sucursal 2	133
Figura.172 Gráficas la sucursal 2	133
Figura 173. Diseño de la red práctica №4	136
Figura 174.Configuracion IP fortigate principal port2	136
Figura 175.Configuracion IP fortigate principal port3	136
Figura 176.Configuracion IP fortigate principal port4	137
Figura 177.Configuracion IP fortigate principal port5	137
Figura 178. Crear zonas de interfaces	138
Figura 179. Interface members fortigate principal	138
Figura 180. Interface members fortigate principal	139
Figura 181. Static routes fortigate principal	139
Figura 182. Regla de internet para el fortigate sucursal 1	140
Figura 183. Regla de internet para fortigate sucursal 2	140
Figura 184. Dirección IP port2 fortigate sucursal 1	141
Figura 185. Dirección IP port3 fortigate sucursal 1	141
Figura 186. Configuración red local del fortigate	142
Figura 187. Sd-wan zone fortigate sucursal 1	142
Figura 188. Sd-wan enlace wan 1	143

Figura 189. Sd-wan enlace wan 1	143
Figura 190. Static routes para sd-wan fortigate sucursal 1	144
Figura 191. Static routes para sd-wan fortigate sucursal 1	144
Figura 192. SD-WAN Rules para Faceboox- fortigate sucursal 1	145
Figura 193. SD-WAN Rules para TeamViewer- fortigate sucursal 1	145
Figura 194. SD-WAN Rules para Adobe- fortigate sucursal 1	146
Figura 195. SD-WAN Rules para fortigate sucursal 1	146
Figura 196. SD-WAN Rules para Amazon- fortigate sucursal 2	147
Figura 197. SD-WAN Rules para Likendin- fortigate sucursal 1	148
Figura. 198 SD-WAN Rules - fortigate sucursal 2	149
Figura 199. Configuración de static routes SD-WAN del fortigate	149
Figura 200. Diagrama de calidad de sevicio de sucrusal 1	150
Figura 201. Configuracion IP fortigate wan sucrsal 2	150
Figura 202. Configuracion IP fortigate wan sucursal 2	151
Figura 203. Configuración red local del fortigate	151
Figura 204. Sd-wan zone fortigate sucursal 2	152
Figura 205 Sd-wan sucursal 2 para puerto 2	152
Figura 206. Sd-wan sucursal 2 para puerto 3	153
Figura 207. Static routes para sd-wan fortigate sucursal 2	153
Figura 208. Static routes para sd-wan fortigate sucursal 2	154
Figura 209. Configuración de static routes sd-wan del fortigate	154
Figura 210. Diseño de la red práctica Nº5	156
Figura 211. Interfaz port2 FG-principal	157
Figura 212. Interfaz port2 FG-principal	157
Figura 213. Firewall Policy port2	158
Figura 214. Servidor sd-wan port2	158
Figura 215. Servidor sd-wan port3	159

Figura 216. Servidor sd-wan port4	159
Figura 217. Servidor sd-wan port5	160
Figura 218. Interfaz sd-wan port3 servidor	160
Figura 219. Interfaz sd-wan port4 servidor	161
Figura 220. Interfaz sd-wan port5 servidor	161
Figura 221. Interfaz sd-wan port2 servidor	162
Figura 222. Static routes servidor-sd wan	162
Figura 223. Static routes servidor-sd wan	163
Figura 224. Gráfica de bandwith servidor-sd wan	163
Figura 225. Sd-wan ISP	164
Figura 226. Descarga de winbox	164
Figura 227.Neighbors Winbox	165
Figura 228.Seleccionar mikrotik a configurar	166
Figura 229.Cambiar nombre al mikrotik	166
Figura 230.Ip addresses mikrotik-daule	167
Figura 231.DNS mikrotik-daule	167
Figura 232. Static routes mikrotik-daule	168
Figura 233. Ping a udemy mikrotik-daule	168
Figura 234. Diseño de la red práctica nº6	170
Figura 235. Configuración del port2 oficina	171
Figura 236. Configuración del port2 central	172
Figura 237. Configuración static routes Oficina	172
Figura 238. Configuración static routes Central	173
Figura 239. Regla de internet para el fortigate Central	173
Figura 240. Regla de internet para el fortigate Oficina	174
Figura 241. VPN Setup en el fortigate Oficina	174
Figura 242. Remote IP address en el fortigate Oficina	175

Figura 243.Policy & Routing para el fortigate Oficina	175
Figura 244 Review Settings para el fortigate Oficina	176
Figura 245. Review Settings para el fortigate Oficina	176
Figura 246. Review Settings para el fortigate Oficina	177
Figura 247. Review Settings para el fortigate Oficina	177
Figura248.VPN Setup en el fortigate Central	178
Figura 249. Remote IP address en el fortigate Central	178
Figura 250. IPSEC para el fortigate Central	179
Figura 251. Review Settings para el fortigate Central	179
Figura 252 Revisar configuraciones para el fortigate Central	180
Figura 253. Bring up en el fortigate Oficina	180
Figura 254. Bring up en el fortigate Central	181
Figura 255. Ping en el fortigate Oficina y Central	181
Figura 256. Diseño de la red práctica Nº7	183
Figura 257.Configuracion IP fortigate campus1 port2	183
Figura 258.Configuracion IP fortigate campus1 port3	184
Figura 259. Configuración red local del fortigate	184
Figura 260. Interfaz SD-WAN port 1 campus 1	185
Figura 261. Configuracion VPN WAN 1 campus 1	185
Figura 262. Configuracion VPN WAN 2 campus 1	186
Figura 263. Interfaz VPN SDWAN1 campus 1	186
Figura 264 SD-WAN Zones Campus 1	187
Figura 265Bring up VPN `S	187
Figura 266. Stattc routes para SD-WAN fortigate campus 1	188
Figura 267. Firewall Policy SD-WAN fortigate campus 1	188
Figura 268. Firewall Policy Intternet red local fortigate campus 1	189
Figura 269.Configuracion interfaz port2 fortigate fg-principal	189

Figura 270.Configuracion IP fortigate principal port3	190
Figura 271.Configuracion IP fortigate principal port4	190
Figura 272. Configuracion VPN WAN 1 principal	191
Figura 273. Configuracion VPN WAN 2 principal	191
Figura 274. Interfaz VPN SDWAN1 princpal	192
Figura 275. SD-WAN Zones Principal	192
Figura 276 Bring up VPN `S principal	193
Figura 277 VPN `S principal activadas	193
Figura 278. Stattc routes para SD-WAN fortigate fg-principal	193
Figura 279. Firewall Policy SD-WAN fortigate fg-principal 1	194
Figura 280. Firewall Policy Intternet red local fortigate fg-principal	194
Figura 281. Firewall Policy Intternet SD-WAN fortigate fg-principal	195
Figura 282. Configuracion static routes SD-WAN campus1	195
Figura 283 Ping en el fortigate campus y fg-primcipal	196
Figura 284. Diseño de la red práctica №8	198
Figura 285.Configuracion IP fortigate FG-WAN port2	199
Figura 286. Configuración static routes FG-WAN port 1	199
Figura 287. Configuracion Policy FG-WAN port1	199
Figura 288. Elección del Routerboard para failover	200
Figura 289.Añadir IP para ISP1-ethe1	200
Figura 290.Añadir IP para ISP1-ethe2	201
Figura 291. Añadir DNS a router Mikrotic	201
Figura 292.Configuracion de Firewall ethe 1 (a)	202
Figura 293.Configuracion de Firewall ethe 1 (b)	202
Figura 294.Configuracion de Firewall ethe 2 (a)	203
Figura 295.Configuracion de Firewall ethe 2 (b)	203
Figura 296. Configuracion NAT para WAN 1 (a)	204

Figura 297. Configuracion NAT para WAN 1 (b)	204
Figura 298.Configuracion NAT para WAN 2 (a)	205
Figura 299.Configuracion NAT para WAN 2 (b)	205
Figura 300.Configuracion WAN IPS 1 para distancia	206
Figura 301.Configuracion WAN IPS 2 para distancia	206
Figura 302. Test Failover	207
Figura 303.Configuracion eth3 para la WAN1 FG-SUCURSAL	207
Figura 304.Configuracion eth4 para la WAN2 FG-SUCURSAL	208
Figura 305. Configuracion port 2 FG-SUCURSAL para la WAN 1	208
Figura 306.Configuracion port 3 FG-SUCURSAL para la WAN 2	209
Figura 307.Configuracion port 4 red local FG-SUCURSAL	209
Figura 308.Configuracion interface WAN 1 FG-SUCURSAL	210
Figura 309.Configuracion interface WAN 2 FG-SUCURSAL	210
Figura 310.Configuracion static routes SD-WAN FG-SUCURSAL	211
Figura 311.Configuracion DNS FG-SUCURSAL	211
Figura 312. Configuracion firewall policy para la red local FG-SUCURSAL	212
Figura 313.Configuracion perfomance SLA FG-SUCURSAL	212
Figura 314.Observacion Perfomance SLA	213
Figura 315.Activacion interfaz WAN 'S	213
Figura 316. Ping failover conectando FG-SUCURSAL	214
Figura 317. Ping failover desconectando FG-SUCURSAL	214
Figura 318. Diseño de la red práctica Nº9	216
Figura 319. Diseño de la red práctica Nº9	216
Figura 320. Configuracion DNS Mikrotik ISP	217
Figura 321. Configuracion NAT mikrotik ISP (a)	217
Figura 322. Configuracion NAT masquerade mikrotik ISP (b)	218
Figura 323. Configuracion IP port 2 FG-SUCURSAL	218

Figura 324. Configuracion red local port 4 FG-SUCURSAL	219
Figura 325. Configuración DNS FG-SUCURSAL	219
Figura 326. Configuración SD-WAN Zones FG-SUCURSAL	220
Figura 327. Configuración Static routes FG-SUCURSAL	220
Figura 328. Configuración firewall policy FG-SUCURSAL	221
Figura 329. Configuración marcado de conexiones a la redpuerto 80 y 443 (a)	221
Figura 330. Configuración marcado de conexiones puerto 80 y 443 (b)	222
Figura 331. Configuración marcado de paquetes puerto 80 y 443 (a)	222
Figura 332. Configuracion marcado de paquetes puerto 80 y 443 (b)	223
Figura 333. Visualizacion marcado de paquetes SD-WAN FG – SUCURSAL	223
Figura 334. Configuracion marcado de paquetes DNS (a)	224
Figura 335. Configuracion marcado de paquetes DNS (b)	224
Figura 336. Agregando address-list para marcado	225
Figura 337. Configuracion marcado de paquetes SD-WAN (a)	225
Figura 338. Configuracion marcado de paquetes SD-WAN (b)	226
Figura 339. Configuracion marcado de paquetes SD-WAN (c)	226
Figura 340. Visualizacion marcado de paquetes SD-WAN	227
Figura 341. Diseño de la red práctica Nº 10	229
Figura 342. Configuración eth2 mikrotik	229
Figura 343. Configuracion DNS mikrotik	230
Figura 344. Configuración del NAT mikrotik (a)	230
Figura345. Configuración del NAT masquerade (b)	231
Figura 346. Configuracion IP port 2 FG-SUCURSAL	231
Figura 347. Configuracion red local port 4 FG-SUCURSAL	232
Figura 348. Configuracion DNS FG-SUCURSAL	232
Figura 349. Configuracion SD-WAN Zones FG-SUCURSAL	233
Figura 350. Configuracion Static routes FG-SUCURSAL	233

Figura 351. Configuracion layer 7 redes sociales	234
Figura 352. Configuracion layer 7 youtube.	234
Figura 353. Marcado de conexión enlace sd-wan.(a)	235
Figura 354. Marcado de conexión enlace sd-wan. (b)	235
Figura 355. Marcado de redes sociales. (a)	236
Figura 356. Layer 7 redes sociales. (b)	236
Figura357. Configuración del packet mark redes sociales. (c)	237
Figura 358. Marcado de paquetes youtube. (a)	237
Figura 359. Layer 7 youtube. (b)	238
Figura 360. Configuración del packet mark youtube. (c)	238
Figura 361. Visualización marcado de paquetes layer 7	239
Figura 362. QOS enlace SD-WAN	239
Figura 363. QOS youtube	240
Figura 364. QOS marcado de paquetes youtube	240
Figura 365. QOS redes sociales	241
Figura 366. QOS marcado de paquetes redes sociales	241
Figura 367. Verificación de conexión al servidor	244
Figura 368. Verificación de conexión al servidor	244
Figura 369. Firewall bloqueando conexión	245

INTRODUCCIÓN

La presente investigación se refiere al tema de diseño e implementación de un banco de pruebas virtualizado con tecnología de redes definidas por software para redes de área amplia (SD-WAN).

Una red SD-WAN se define como una sustitución del hardware de redes WAN tradicional como los enrutadores configurados mediante de línea de comandos (CLI) con administración centralizada al aplicar redes definidas por software (SDN) a conexiones de red de área amplia (WAN) para ofrecer de manera más eficaz aplicaciones a usuarios en largas distancias.

La característica principal de este tipo de red es que no depende de amplia cantidad de equipos físicos, lo que brinda una flexibilidad y eficacia en la administración, enrutando dinámicamente el tráfico a través de enlaces privados y públicos, tales como enlaces MPLS arrendados y banda ancha, Long Term Evolution (LTE) y/o inalámbricos.

La realización de este proyecto se basa que al no contar con un laboratorio donde se pueda implementar las nuevas tecnologías de manera virtualizada con emuladores Gns3 en el cual se pueda realizar simulaciones, modificaciones, configuraciones de redes físicas y virtuales, sea capaz de satisfacer las necesidades de los estudiantes y se puedan preparar para la incorporación de nuevas tecnologías y formas de uso.

Asimismo percibiremos en los siguientes capítulos como virtualizar un servidor, repotenciar su hadware a través de las especificaciones del equipo y la elección del software para virtualizar y crear el ambiente virtual para el desarrollo de las diez prácticas que se diseño de redes definidas por software para redes de área amplias.

El actual documento se ejecuta en el diseño e implementación de un banco de pruebas virtualizado para redes definidas por software para redes de área amplia (SD-WAN) empleada en la Universidad Politécnica Salesiana sede Guayaquil la cual cumple con la formación académica de los estudiantes.

CAPÍTULO I

EL PROBLEMA

1.1. DESCRIPCIÓN DEL PROBLEMA

La tecnología para la comunicación global va evolucionando con el transcurso del tiempo, surgiendo nuevas formas para comunicarse que demanda más dispositivos en la red. Llegará un punto en el cual no podremos seguir conectados restringiendo el acceso a la conexión de dispositivos a nuestra red local o empresarial generando cuellos de botellas, banda ancha limitada, ataques de información causando retrasos al momento de transferir información. Actualmente encontramos en el mercado hardware que va a permitir solucionar este tipo de inconvenientes dentro la red o para enlaces WAN, pero suelen ser costosa.

En la nube encontramos software que nos permiten de una manera virtual emular dispositivos como routers, switches, firewall y sistemas operativos, usando recursos físicos de nuestros equipos informáticos en disco duro, CPU y memoria RAM, los estudiantes de las carreas de Ingeniería Electrónica e Ingeniería en Telecomunicaciones podrán realizar estas simulaciones.

El laboratorio de telecomunicaciones de la Universidad Politécnica Salesiana sede Guayaquil no cuenta con el hardware necesario para efectuar simulaciones de redes definidas por software para redes de áreas amplias de forma virtualizada donde los estudiantes obtendrán las prácticas para la conexión de estas redes, para cifrar y segmentar el tráfico de la red, permitir identificar problemas para una solución rápida, lograr un mayor rendimiento de las aplicaciones, para conseguir una experiencia optima y garantizar la disminución de latencia en la red.

1.2. ANTECEDENTES

El laboratorio de telecomunicaciones de la Universidad Politécnica Salesiana sede Guayaquil actualmente no consta con una plataforma para virtualizar o emular redes de datos por lo cual se ha considerado desarrollar este proyecto, al ser una tecnología nueva que no se encuentra implementada en la Universidad Politécnica Salesiana. Las practicas propuestas permitirán de manera virtualizada hacer la conexión de redes WAN, cifrar y segmentar el tráfico de la red, identificar problemas de red, lograr un mayor rendimiento de las aplicaciones, conseguir una experiencia optima y garantizar la disminución de latencia en la red.

El desarrollo de este proyecto será de gran beneficio, principalmente a los estudiantes y los docentes que imparten las materias de redes de computadores y redes de comunicaciones permitiendo el desarrollo e investigación de nuevas tecnologías donde se podrá cambiar el

comportamiento de una red dinámica, mejorar el rendimiento de las redes actuales, los cuales aportaran al entendimiento de este nuevo tipo de arquitectura.

1.3. IMPORTANCIA Y ALCANCES

Este proyecto tiene como propósito ser de impacto e innovación como resultado la preparación y conocimiento para enfrentarse a los cambios que se presentarán a futuro en diferentes empresas de telecomunicaciones que deseen implementar las nuevas soluciones de conectividad abaratando costos de implementación lo cual reduce la intervención de técnicos y la probabilidad de errores.

1.4. DELIMITACIÓN

1.4.1. ESPACIAL

El proyecto técnico para la obtención del título de "Ingeniero Electrónico mención Telecomunicaciones", fue implementado en la Universidad Politécnica Salesiana sede Guayaquil.

1.4.2. ACADÉMICA

Orientado a las materias de Redes de Computadoras 1, Redes de Computadoras II y Redes de Comunicación.

1.4.3. TEMPORAL

El presente proyecto técnico se realizó durante en el período 2020-2021.

1.5. OBJETIVOS

1.5.1 OBJETIVO GENERAL

Diseñar e implementar un banco de pruebas virtualizado con tecnología de redes definidas por software para redes de área amplia (SD-WAN) para el laboratorio de telecomunicaciones de la Universidad Politécnica salesiana sede Guayaquil.

1.5.2 OBJETIVOS ESPECIFICOS

- Comparar los diferentes tipos de tecnologías de virtualización.
- Generar un escenario virtual para el acceso remoto a los estudianes al servidor.
- Analizar el funcionamiento de los protocolos TCP/IP con la tecnología SD-WAN.
- Diseñar e implementar diez prácticas con diversos protocolos de red para pruebas de conectividad.

1.5.2 METODOLOGÍA

Se usa la metodología experimental porque es el instrumento principal debido a que los estudiantes podrán manipular, configurar, diseñar y comparar redes definidas por software de manera virtual obtenido resultados positivos y acertados estas pruebas fueron desarrolladas con el fin de demostrar el enlace de comunicación consiguiendo sacar terminaciones sobre los resultados de las prácticas llevando a cabo los conocimientos técnicos y teóricos aprendidos a lo largo de nuestra vida universitaria.

1.5.2 BENEFICIARIOS DE LA PROPUESTA E INTERVENCIÓN

Los alumnos de las carreras de Ingeniería Electrónica e Ingeniería en Telecomunicaciones son los principales beneficiarios en la elaboración de este proyecto.

CAPÍTULO II

MARCO TEÓRICO

2.1. VIRTUALIZACIÓN

La virtualización es la forma que se complementa el hardware y software de los sistemas operativos que se van a utilizar. Nos permite ejecutar varios sistemas operativos de manera concurrente en un solo servidor físico, donde podemos provisionar alcamenamiento de discos duro, memoria RAM y CPU para las diferentes maquinas virtuales dependiendo la necesidad de los beneficiarios o empresa.(Fernández & García, 2011).



Fuente: Seguridad para la nube y la virtualización FOR DUMMIES [DANIEL Reis, 2013]

2.2.1.TIPOS DE VIRTUALIZACIÓN

En la actualidad encontramos diversos ejemplos de virtualización:

- Virtualización por servidores.
- Virtualización de memorias.
- Virtualización de Almacenamiento (Storage).
- Virtualización de Escritorio (Desktop).
- Virtualización de redes (network)

2.2.2. VIRTUALIZACIÓN POR SERVIDORES

Esta manera de virtualizar a través de servidores es un entorno que está constituido en hardware mediante un software propietario que representa un

ambiente computacional. El software invitado, que habitualmente es un SO completo comienza a iniciar como si fuera un hardware independiente.

Las diversas máquinas virtuales son simuladas por un servidor físico para que esto funcione se asigna los recursos tales como memoria RAM, CPU y almacenamiento del servidordor y estos recursos ser determinados primeramente por un árbitro (hypervisor). (Fernández & García, 2011).



Figura 2 Virtualización de un servidor Fuente. Virtualización de servidores por Alex Marquez.Universidad Politécnica de Catalunya (UPC)[Alex Márquez, 2011]

2.2.3. VIRTUALIZACIÓN POR MEMORIAS

Este tipo de virtualización por memorias sirve de un modo diferente tienendo como recurso a las diversas restricciones que imputa la memoria física, siendo el motivo de los cuellos de botella para el funcionamiento de las aplicaciones o servicios.

Debemos tener en cuenta los siguientes objetivos en el instante de virtualizar por memoria:

- Asignar los recursos suficentes de memoria RAM a diferentes aplicaciones y sistemas operativos teniendo en cuenta la demanda.
- Aumentar la eficacia y disminuir en el tiempo de ejecución de aplicaciones de los servidores que usan un intenso consumo de memoria. (Fernández & García, 2011).



Figura 3. Virtualizacon de memoria Fuente. Virtualización..Yenisleidy Fernández Romero1, Karen García Pombo2 [Fernandez & Garcia, 2011]

2.2.4. VIRTUALIZACIÓN DE ALMACENAMIENTO (STORAGE)

La representación de virtualización por almacenamiento se describe como el método de utilizar el almacenamiento físico en almacenamiento lógico. Su principal objetivo es el ahorro de recursos de almacenamiento en los servidores su función es en dirigir, administar y gestionar los espacios de almacenamiento físico..(Fernández & García, 2011).



Figura 4. Virtualizacon de Almacenamiento Fuente. <u>https://sites.google.com/site/wwwvirtualizacioneducom/</u>

2.2.5. VIRTUALIZACIÓN DE ESCRITORIO (DESKTOP)

Este método refiere a elaborar un entorno de cliente-servidor este se guarda en un servidor principal o central, con sus funciones, servicios y aplicaciones para acceder mediante uan conexión remota desde el escritorio virtual. (Fernández & García, 2011).



Figura 5. Virtualizacion de Escritorio Fuente. <u>http://www.vsolutionsvs.com/site/index.php/soluciones/virtualizacion-de-escritorios</u>

2.2.6. VIRTUALIZACIÓN DE REDES (NETWORK)

Este método se refiere a fusionar los recursos entre el software y hardware y funcionalidades de red de datos en una sola identidad establecida en software, siendo nombrada como una red virtual. Al realizar la implementación facilita y provee el asunto de gestión, ofreciendo a los administradores de red en conservar un control preciso sobre los recursos de la red que gestiona.

Las VLANs permiten a los encargados de gestionar la red acoplar elementos de redes a comodidad, proporcionando la eventualidad de inspeccionar todo lo que ocurre en la red. (Fernández & García, 2011).


Figura 6

Fuente.Virtualizacion de redes y servidores emulando infrestructura tecnológica [Casierra Cavada, J., Quiñonez Ku, X., Herrera Izquierdo, L., Egas Acosta, C, (2018]

2.3. TIPOS DE REDES

Las redes de computadoras consiguen atender a variadas clasificaciones en ocupación de los elementos que se hayan tenido en mente, las redes de datos se especifican de esta manera:

2.3.1. SEGÚN SU EXTENSIÓN

En función del recorrido físico en la que se encuentra conectados los diferentes nodos se puede decir la siguiente clasificación:

 Red de área personal (PAN): son redes de computadoras que son utilizadas para la comunicacion entre dispositivos por ejemplo impresoras, laptop y scanner su alcance consigue llegar a 10 metros son generalmente por cable USB.



Figura 7. Red Pan Fuente. Redes de computadoras Tanenbum/Wetherall [Tanenbaun & Wetherall, 2012]

 Red de área local (LAN):Esta red es de uso doméstico como una oficina o lugar de un centro comercial sirve para compartir recursos, imágenes o NAS y es un red de clase C.



Fuente. Introduccrion a las Redes de Computadores [Alvarez & Monsalve, 2008]

 Red de área metropolitana (MAN): Tiene como objetivo en ofrecer una cobertura de internet geográfica a través de fibra óptica este ejemplo de red logra ser privada o pública igualmente cuenta una banda ancha extensa y su alcance es máximo de 50 km.



Figura 9. Red Metropolitana Fuente. Redes de computadoras Tanenbum/Wetherall [Tanenbaun & Wetherall, 2012]

 Red de área extensa (WAN): Enlaza ciudades y países alredor del planeta entre sí. Regularmente son implantadas por las empresas de servicios de Internet (ISP). (Castaño & López, 2013).



Figura 10. Red Wan Fuente. Redes de computadoras Tanenbum/Wetherall [Tanenbaun & Wetherall, 2012]

2.3.2. SEGÚN SU TOPOLOGÍA

Constan dos diferentes ejemplos de topología:

- Topología física: Representa la red de datos en los medios de transmisión.
- Topología lógica: Se específica cómo se conecta las computadoras a la red de datos.

• Topología física de la red

Las topologías físicas de redes de datos más manejadas son:

• Topología de bus: Esta topología tiene como fin usar un único segmento de cable permitiendo que todos los equipos se acoplen de manera inmediata.



Figura 11. Topologia en Bus Fuente. Teccnologia de la información [Daniel Kohen, Enrique Asin]

 Topología de anillo: Domina una sola conexión de entrada y salida una de sus desventajas es que posee una trasmisión más lenta que las otras topologías.



Figura 12.Topologia en Anillo Fuente. Teccnologia de la información [Daniel Kohen, Enrique Asin]

• Topología de estrella: Cada computadora va conectada a cada puerto del dispositivo central de concentración por lo habitual puede ser un hub o un switch.



Figura 13. Topología en Estrella

Fuente. Tecnología de la información [Daniel Kohen, Enrique Asin]

 Topología jerárquica: Una red jerárquica agrupa las características de una red estrella extendida.



Figura 14. Topología Jerárquica Fuente. Tecnología de la información [Daniel Kohen, Enrique Asin]

• Topología de malla: Esta topología surge en encaminar los datos y voz no requiere de un servidor central o nodo. (Castaño & López, 2013).



Figura 15. Topología de Malla Fuente. https://sites.google.com/site/topologiasdered708/home/topologia-de-red-demaya

Topología lógica de la red

La topología de la red lógica se detalla en la manera que las computadoras y dispositivos se participan internamente en la red de datos. (Castaño & López, 2013).



Figura 16. Topologia de red lógica Fuente. Cisco CCNA v5

2.3.3. SEGÚN EL TIPO DE ACCESO A LA RED

Los dispositivos, servidores y computadoras de una red de datos se enlazan con otras redes usando una dirección IP. Se especifican de la siguiente forma:

 Red pública: Enlazan una red de datos usando una dirección IP única que les ortoga su distribuidor de servicio para internet (ISP).(Castaño & López, 2013).





 Red privada: Es una red que usa direcciones IP privadas de clase C y debe ser nateada y enmascarada con la red pública para lograr tener acceso a internet. A network serving a home, building or campus is considered a Local Area Network (LAN).



Figura 18. Red privada Fuente. Cisco CCNA v5

2.3.4. SEGÚN EL MEDIO DE TRANSMISIÓN

El canal maneja una red de datos o de voz para transmitir y recibir información, y se pueda formar la sucesiva clasificación:

• Red cableada: Las computadoras o servidores se enlazan a la red a través de un cable de red o patchcord. Este cable de red puede ser de diferentes tipos según la velocidad de la NIC.



Figura 19. Red cableda Fuente.Universidad de Cadiz, Facultad de ciencia sociales y de la comunicacion, Redes de datos [M Fernandez]

• Red inalámbrica: comunica y toma información a través de transmisiones electromagnéticas. Las ondas son enviadas y recibidas a través de las antenas que tienen los ordenadores y como los celulares o laptop que se conectan a la red WIFI. (Castaño & López, 2013).



<u>Conexiones posibles actualmente usando</u> tecnologia de infrarrojos.

Figura 20. Red inalambrica Fuente.Universidad de Cadiz, Facultad de ciencia sociales y de la comunicacion, Redes de datos

2.4. DISPOSITIVOS DE INTERCONEXIÓN DE REDES

Sirven para comunicar los equipos terminales y la conexión que va a Internet conoceremos diferentes dispositivo mencionados en la vida cotidiana que son los siguientes:

 Concentradores o hubs: sirven para restablecer el pulso eléctrico de transmisión cada cierto tiempo, por que la señal va sufriendo perdidas en una determinada distancia.



Figura 21. HUB Fuente.Redes Locales. Alfredo Abad Domingo

 Conmutadores o switches: es un dispositivo que logra fraccionar la red en múltiples segmentos dependiéndo la cantidad de puertos que posea el switch alcanzando que nunca se produzca una colisión en el envío de paquetes.



Figura 22. Conmutadores o switches Fuente.Redes Locales. Alfredo Abad Domingo

 Enrutadores o routers: son utilizados para enviar y recibir el tráfico de la red. Se aprovecha cuando queremos acoplar diferentes LAN a través de enrutamiento estáticos o dinámicos.



Figura 23. Enrutadores o routers Fuente.Redes Locales. Alfredo Abad Domingo

• Cortafuegos o firewall: es un dispositivo que tiene como función gestionar y administar la seguridad de la red a través de reglas que son declaras en el equipo.



Figura 24. Enrutadores o routers Fuente.Redes Locales. Alfredo Abad Domingo

 Módem: es un aparato usado para transmitir señales de datos por medio de cables de teléfono.



Figura 25. Módem Fuente.Redes Locales. Alfredo Abad Domingo

 Cable módem: es similar al módem, pero remite datos por medio de patchcord de coaxial. También logra trasladar señales de televisión. (Castaño & López, 2013).



Figura 26. Cable módem Fuente.Redes Locales. Alfredo Abad Domingo

2.5. CABLEADO ESTRUCTURADO

El estándar de cableado estructurado nos describe cómo podemos realizar un montaje del cableado de comunicaciones en instituciones públicas, instituciones privadas u edificios. El estándar explica de forma breve los diferentes tipos de cables utp que se vayan a manejar, terminales, distancias máximas, distribución de elementos de interconexión, se debe seleccionar el tipo de cable dependiendo la instalación que se vaya a realizar. (Bellido ,2013).

2.5.1.CONJUNTO DE CABLEADO ESTRUCTURADO

La agrupación del cableado estructurado debe estar constituido en distintas partes, cada uno contiene un subsistema. Son los siguientes:

 Cableado de campus: Interconecta los distintos edificios de una organización o institución. Se sugiere utilizar fibra óptica para no tener pérdida de paquetes.



Figura 27. Cableado Campus Fuente.Cisco CNNA v5

• Sala de equipamiento: Lugar en el que coinciden todas las conexiones y enlaces del edificio.



Figura 28. Sala de Equipamiento Fuente.Redes Locales. Alfredo Abad Domingo

• Cableado troncal: Este se encarga de llevar a cabo todas las conexiones través del cableado vertical. (Molina, 2014).



Figura 29. Cableado Troncal Fuente. https://sites.google.com/site/stigestionydesarrollo/recuperacion/desarrollo-1/tema10/3

 Sala de Telecomunicaciones: Es una espacio centralizado adentro de una institución, colegio o edificio que alberga los dispositivos del sistema de cableado de telecomunicaciones.



Figura 30. Sala de Equipamiento Fuente.Redes Locales. Alfredo Abad Domingo

• Cableado horizontal: Proviene desde las conexiones de pared llamadas rosetas o faceplate por los caneles telecomunicacionesde hasta los rack de comunicaciones.



Figura 31. Cableado Horizontal Fuente.Redes Locales. Alfredo Abad Domingo

• Área de trabajo: Se llama área de trabajo al lugar donde se encuentra una sala de telecomunicaciones que proporciona o ofrece un determinado servicio. (Bellido ,2013).



Figura 32. Área de trabajo Fuente. https://es.slideshare.net/lismark93/cableado-estructurado-36423999

2.5.2 ESTÁNDARES DE CABLE UTP/STP

El siguiente estándar ANSI/EIA/TIA-568 queda separado en diferentes procesos técnicos que constituyen los elementos de transmisión. Estos son:

- TSB36: Detalla el uso del cableado de par trenzado.
- TSB40: Define la querencia del conector RJ-45 y los procesos que se ejecutan en los empalmes de cableado.
- TSB53: Describe el manejo de cableado de par trenzado apantallado.

Los estándares de cableado estructurado ANSI/EIA/TIA 568 e ISO/IEC 11808:2002 aceptan diferentes tipos de cableado: UTP/FTP para las instalaciones de cobre y cable multimodo (50/125 μ m o 62.5/125 μ m) y monomodo para las instalaciones de fibra óptica. En el caso del cable trenzado de cobre, las diferentes calidades existentes, es decir, la categoría (según ANSI/EIA/TIA-568) o clase (según ISO/IEC 11801), determinarán la rapidez máxima de entrega y el trayecto máximo entre las conexiones. La categoría del cable depende de la cantidad de trenzado por metro (cuanto mayor es este valor, mayor es su inmunidad al ruido) y la existencia o no de una pantalla protectora. (Molina, 2014).

2.5.3 TIPOS DE CABLES

El par trenzado es un cable muy manejado en pequeñas y grandes instalaciones. Su uso es debido a su facilidad de instalación, su reducido coste y su buen rendimiento, además de que se trata de una tecnología muy desarrollada actualmente. El cableado de par trenzado está disponible en varias versiones.

 Par trenzado no apantallado (UTP): este cableado dispone de una mayor flexibilidad, por lo que suele instalarse como latiguillos en los paneles de parcheo y las conexiones del área de trabajo entre los enchufes de pared y los equipos, donde además su longitud suele ser bastante reducida. Tiene una impedancia característica de 100 Ω y está formado por cuatro pares: blanco-azul y azul, blanco-naranja y naranja, blanco-verde y verde, y blanco-marrón y marrón.



Figura 33. Par tranzado no apantallado Fuente. <u>http://carloseduca.byethost11.com/FPB/ELECTRICIDAD/ut2_Cableadoyconexiones/rec</u> ursos/tiposcablesRed.pdf?i=1

 Par trenzado apantallado (STP, S/STP, FTP, S/FTP o S/UTP): este tipo de cable está formado por cuatro pares apantallados par a par o globalmente por una malla conductora. Debido a su pantalla, se trata de un cable más rígido y de mayor coste, pero permite una mayor protección frente a interferencias. Tiene una impedancia característica de 150 Ω y su espesor no es significativamente superior que el cable no apantallado.



Figura 34. Par tranzado apantallado Fuente. <u>http://carloseduca.byethost11.com/FPB/ELECTRICIDAD/ut2_Cableadoyconexiones/rec</u> <u>ursos/tiposcablesRed.pdf?i=1</u>

• Cable multipar: Se trata de un cable de par trenzado que puede ir apantallado o no y que incluye una gran cantidad de pares. En los estándares de cableado estructurado aparece normalmente definido por 25 pares. Hay que tener en cuenta que en este tipo de cable no deben circular señales incompatibles que puedan producir diafonía.



Figura 35. Cable multipar Fuente. http://carloseduca.byethost11.com/FPB/ELECTRICIDAD/ut2_Cableadoyconexiones/rec ursos/tiposcablesRed.pdf?i=1 Los cables de par trenzado, al igual que otros cables de cobre, están caracterizados por el diámetro del núcleo conductor. Cuanto mayor es este diámetro, mayor grosor tendrá el cable y menor resistencia tendrá al paso de la corriente eléctrica. Esto quiere decir que un cable de cobre de mayor grosor tendrá unas características de atenuación mejores con respecto a cables de menor grosor, por lo que serán capaces de cubrir distancias más largas. La mayoría de los fabricantes utilizan la medida del AWG (American Wire Gauge o Calibre del Cable Americano) para indicar el grosor del cable. El valor más común para el par trenzado es 24 AWG, que se corresponde con un diámetro del cobre de 1/24 de pulgada. El valor del AWG puede variar en los cables trenzados actuales de 9 a 26 AWG.

2.6. TIPOS DE SOFTWARE PARA EMULAR REDES INFORMÁTICAS

Existen diferentes software para emular redes informáticas se nombran las mas usadas por los usuarios son las siguientes:

- Cisco Packet Tracer
- GNS3
- NetSim
- CISCO PACKET TRACER.- Es una herramienta desarrollada por Cisco sirve para emular redes informáticas, donde ellos ofrecen en su software routers, switches de la marca y es fácil de utilizar una de sus desventajas solo se puede emular equipos CISCO.



Figura 36.. Cisco Packet Tracer Fuente. <u>http://net4dd.com/guia-de-implementacion-de-cisco-packet-tracer-en-</u> windows/

 GNS3 .- Es un simulador grafico para redes informáticas de código abierto sirve para realizar una simlacion de redes informáticas complejas como se trabajaría, se comportaría la red en tiempo real una de sus ventajas se puede cargar Qemu y KVM de dififerentes fabricantes como CISCO,HP.FORTINET,SOPHOS y siendo una herramienta usada por todos los ingenieros y personas que se van a certificar en dichos equipos.



Figura 37. GNS3

Fuente. https://www.gns3.com/

• NETSIM.- Este simulador es usado especialmente en investigación y también en desarrollos de redes y aplicaciones de defensas.



Figura 38. NETSIM Fuente. <u>https://www.comsnets.org/archive/2015/demos_exhibits.html</u>

2.7. SERVIDORES

Los servidores son computadoras potentes que tienen un profundo rendimiento usadas en empresas y organizaciones ,los servidores también ofrecen servicios a varios beneficiarios clientes y servicios.

El hadware del servidor se perfecciona y logra un tiempo de contestación optimo para diversas peticiones dentro de la red de datos. Los servidores poseen distintas unidades de procesamiento central (CPU) y hilos , bastante capacidad de memorias (RAM) y diferentes unidades de almacenamiento como discos HDD y SSD de alta capacidad que admiten hallar información de forma tremendamente rápida. (Bellido ,2013).



Figura 39. Parte interna de un servidor Fuente. Administrador de Servidores []Marchionni, Enzo Augusto 2011

2.7.1. TIPOS DE DISEÑOS DE SERVIDORES

Constan diversos diseños de servidores como una torre independiente, estos pueden ser acoplados en bastidores, o bien, pueden poseer un diseño en blade. Estos servidores pueden tomar la función de NAS ,Streaming, servidor de datos y dispositivos para usuarios finales.(Bellido ,2013).

- Servidor Blade :Entregan la máxima concentración de potencia de computo y escalabilidad.
- Servidor acoplado en bastidor: Son excelentes para poseer mas espacios libres.
- Servidores independientes: Se usan en pequeñas empresas y proveen felixibilidad para escoger componentes internos. (Bellido ,2013).

2.7.2. SISTEMAS RAID SERVIDORES

Un array de RAID (Redundant Array of Independent Disk) esta formado por varios conjunto de discos que funcionan de manera colectiva como un único sistema de almacenamiento los sistemas RAID son los siguientes: RAID 0. Son discos con bandas sin tolerancia al error. El nivel 0 de RAID no es redundante, así que no se incumbe puntualmente al acrónimo es fragmentada logrando un unidad de mayor volumen. (Gómez, 2014).



Figura 40. RAID 0 Fuente. Administrador de Servidores []Marchionni, Enzo Augusto 2011

 RAID 1 o disco espejo. El RAID 1 provee redundancia al plagiar todos los datos de disco a otr. El beneficio de un array 1 es un poco superior que cuando se posee una sola unidad para cumplir esta función se necesita 2 discos siempre deben ser pares.



Figura 41. RAID 1 Fuente. Administrador de Servidores []Marchionni, Enzo Augusto 2011

 RAID 5. Para utilizar array 5 se neceita minimo 3 unidades de discos duros estos trabajan diferentes con bloques de paridad distribuidos. El RAID 5 en vez de reproducir totalmente los datos del disco duro se utilizan los bits de paridad para que en estos asunto se rompa un disco duro poder reformar la información del mismo. (Gómez, 2014).



Figura 42. RAID 5 Fuente. Administrador de Servidores []Marchionni, Enzo Augusto 2011

2.7.3. SOFTWARE DEL SERVIDOR

Primariamente constan dos grandiosos alternativas al momento de preferir un SO: los asentados en UNIX (o su homólogo Linux) o Windows. Linux es un sistema de código abierto, Windows es un producto comercial propiedad de Microsoft la selección de estas dos alternativas no está libre de controversia. (Gómez, 2014).

Ambos sistemas operativos consiguen actuar como cliente o servidor (Gómez, 2014).

EMPRESA	SOLUCIÓN	WEB
VMware	Vsphere	www.vmware.com/products/vsphere
Microsoft	Hyper-V	www.microsoft.com/hyper-v-server
Citrix	XenServer	www.citrix.com/xenserver
Oracle	Oracle VM	www.oracle.com/us/technologies/virtualization
Oracle Solaris	Oracle Solaris Containers	www.oracle.com/us/products/servers-storage/solaris/virtua
Red Hat	Enterprise Virtualization	www.latam.redhat.com/rhel/virtualization
Parallels	Parallels Server	www.parallels.com/virtualization/server
Novell	Suse Linux Enterprise Server	www.novell.com/es-es/products/server/virtualization.html

Figura 43. Software de Virtualización Fuente. Administrador de Servidores [Marchionni, Enzo Augusto 2011]

2.7.4. ESTRUCTURA CLIENTE/SERVIDOR

La estructura cliente/servidor está compuesta por servicios alojados en servidores y clientes que son los que realizan peticiones de servicios al servidor; para que esto sea viable, cliente y servidor tienen de estar en redes semejantes. (Carvajal,2017).

El cliente es el que establece haciendo la petición al servidor y el servidor es quien soluciona la petición una vez admitida. El servidor toma una multitud de peticiones de los clientes y éste inmediatamente las procesa. Dependiendo del número de clientes simultáneos que se vaya a atender, tendremos que seleccionar un servidor con unas características, tanto de software como de hardware. (Carvajal,2017).



Figura 44. Modelo Cliente-Servidor Fuente.El modelo Cliente / Servidor [E Marini 2012]

CAPÍTULO III

DISEÑO E IMPLEMENTACION DEL BANCO DE PRUEBAS

3.1. PROPOSITO DEL DISEÑO

El propósito de este diseño e implementación del banco de pruebas virtualizado se lo plasma con la finalidad de dar conocer las redes definidas por software para redes de áreas amplias para la administración de tráfico, control centralizado de la red a través de diversos enlaces, permitiendo a los estudiantes programar este de tipo de redes de comunicación sujetando tiempos de abastecimiento y restando o separando la necesidad de configurar manualmente routers o firewall habituales, optimizando la conectividad del servicio de la oficina central y la nube.

Para este diseño e implementacion del banco de prueba se utilizo la topología estrella para la comunicación de las computadoras hacia el servidor que esta conectado a un punto de red en el laboratorio de telecomunicaciones y para la simulacion de redes definidas por software se virtualizo el servidor Dell R210II con el software EXSI 6.5 UPDATE 3, se instalo GNS3 – SERVER dentro del servidor y se añadio todos los QEMU y KVM para la realización de las prácticas.

El banco de prueba o entorno virtual se diseñó para abastecer las computadoras que se encuentran en el laboratorio de telecomunicaciones de la Universidad Politécnica Salesiana sede Guayaquil.

En la siguente figura se describe la topoligía de red y la conexión de comunicación del banco de prueba:





3.2. CONSTRUCCIÓN DEL BANCO DE PRUEBA

Para la parte inicial del proceso de elaboración del banco de pruebas se realizó en los siguientes pasos:

1. Proceder a desarmar el servidor Dell R210 II para mantenimiento correctivo.



Figura 46. Desmontar Dell R210 II Fuente: Los autores

2. Limpieza del Servidor Dell R210 II.



Figura 47 Mantenimiento Correctivo Dell R210 II Fuente: Los autores

3. Desarmar disipador y aplicar pasta térmica para la CPU del servidor Dell R210 II



Figura 48. Desmontaje del disipador y aplicación de pasta térmica Dell R210 II Fuente: Los autores

4. Instalación de discos duros y memorias RAM.



Figura 49. Instalación SSD Dell R210 II y memorias ram Fuente: Los autores

3.3. CONFIGURACIÓN DE DISCO DUROS DEL SERVIDOR DELL R210 II

Para la instalación de sistemas operativos de virtualización se procedió primero a configurar los discos duro en RAID 1 y se lo detalla en los siguientes pasos.

1. Realizar la configuración de disco duros dentro del servidor Dell R210 II

tecleamos la combinación Ctrl+C.



Figura 50. Configuración de los discos duros Dell R210 II Fuente: Los autores

2. Seleccionar SAS Controller a configurar



3. Vamos a la opción RAID PROPERTIES.

LSI Corp Config Utility For Dell SAS Ct Adapter Properties SAS2008	lr ∨7.11.10.00 (2011.06.02)
Adapter PCI Address(Bus/Dev) MPT Firmware Revision Package Version SAS Address NVDATA Version Status Boot Order Boot Support RAID Properties	PERC H200A 01:00 7.15.08.00-IR 7.03.05.00 5848F690:EB37CB00 07.00.00.19 Enabled 0
SAS Topology	
Advanced Adapter Properties	
Esc = Exit Menu F1/Shift+1 = Help Enter = Select Item -/+/Enter = Change	Item

Figura 52. Raid propiedades Dell R210 II Fuente: Los autores

4. Seleccionar RAID 1



Figura 53. Selección del RAID 1 Dell R210 II Fuente: Los autores

5. Seleccionar disco primario y disco secundario o espejo, tecleamos

C para crear el volumen del RAID.



Figura 54. Selección de disco duros Dell R210 II Fuente: Los autores

6. Creación del Volumen RAID 1



Figura 55. Selección del RAID 1 Dell R210 II Fuente: Los autores

3.1.3. COMPARACIÓN DE LOS DIFERENTES TIPOS DE SOFTWARE PARA VIRTUALIZAR SERVIDOR

Para la virtualización de servidores tenemos varios sistemas operativos que son usados en diferentes empresas detallaremos sus características de cada uno de ellos.

Estos son los principales proveedores en el espacio de virtualización del servidor mas usados. Ver Anexo A

- VMware vSphere
- Red Hat Virtualization
- Proxmox VE
- Microsoft Hyper-V

Para la virtualización del proyecto técnico se escogio el sistema de WMware ESXi 6.5 es un sistema que permite instalar, administar y configurar maquinas virtuales que se encuentan en el servidor de forma rápida y flexible ayudando asi la incorporación de la virtualización.

3.4. INSTALACIÓN DEL SISTEMA OPERATIVO EXSI 6.5 U3 EN EL SERVIDOR DELL R210 II

La instalación del sistema operativo del servidor Dell R210 II se consideró el sistema de EXSI 6.5 U3 porque nos permite una rápida instalación y administración de las maquinas virtuales en el servidor también es un software que la mayoría de las empresas lo utilizan para gestionar sus servicios por su alta disponibilidad en producción ,se tenia previsto instalar PROXMOX un sistema operativo de código abierto para la virtualización del equipo pero presentaba el problema en cargar los archivos ova y con EXSI 6.7 U3 problemas con el CPU que no soportaba el sistema. 1. Botear el servidor con la tecla F11 Boot Manager



Figura 56. Boot Manager Dell R210 II Fuente: Los autores

2. Seleccionar el medio de instalación del sistema CD-ROM.



Figura 57. Boot CD-ROM 1 Dell R210 II Fuente: Los autores

3. Seleccionar en el Boot Menu Dell EXSI 6.5.



Figura 58. Boot Menu Dell R210 II Fuente: Los autores

4. Carga del sistema operativo EXSI 6.5 U3.

		Loading ESXi	installer		
Loading /v	vmw_ahci.v00				
Loading />	xhci_xhc.v00				
Loading /e	emulex_e.v00				
Loading /t	btldr.t00				
Loading /ı	weaselin.t00				
Loading /e	esx_dvfi.v00				
Loading /e	esx_ui.v00				
Loading /	Isu_hp_h.v00				
Loading /!	Isu_Isivuu				
Loading /!	150_151001				
Loading /!	ISU_ISIVUZ				
Loading /!	150_151003				
Loading /					
Loading /r	native_0.000 rste u00				
Loading //	umuare e u00				
Loading /	vnaar <u>2_</u> 0.000 usan uAA				
Loading /	vsanheal.vAA				
Loading /	vsannant.v00				
Loading /1	tools.t00				

Figura 59. Loading Exsi 6.5.0 Fuente: Los autores

5. Bienvenida a la instalación de EXSI 6.5 U3 en el servidor Dell R210 II.



Figura 60. Welcome Exsi 6.5 Fuente: Los autores 6. Aceptación de términos y licencia EXSI 6.5 U3.

End User License Agreement (EULA)		
VMWARE END USER LICENSE AGREEMENT		
PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.		
IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT		
Use the arrow keys to scroll the EULA text		
(ESC) Do not Accept (F11) Accept and Continue		

Figura 61. Términos y Condiciones Exsi 6.5 Fuente: Los autores

7. Instalación de EXSI 6.5 U3 en los discos duros del servidor Dell R210 II.



Figura 62 Instalación Exsi 6.5 Fuente: Los autores

8. Configuración de idioma del teclado.

Please select a keyboard layout
Swiss French Swiss German Turkish US Default US Dvorak Ukrainian United Kingdom
Use the arrow keys to scroll.
(Esc) Cancel (F9) Back (Enter) Continue

Figura 63.Configuración del idioma del teclado Exsi 6.5 Fuente: Los autores

9. Configuración de contraseña del EXSI 6.5 U3.

Enter a root password				
Root password: Confirm password:	********** ***************************	ch.		
(Esc) Cancel	(F9) Back	(Enter) Continue		

Figura 64 Contraseña del Exsi 6.5

Fuente: Los autores



10. Sistema operativo EXSI 6.5 U3 instalandose en el servidor Dell R210 II.

Figura 65.Contraseña del Exsi 6.5 Fuente: Los autores

11. Sistema operativo EXSI 6.5 U3 instalado.



Figura 66. SO EXSI 6.5 Fuente: Los autores
12. Para acceder al modo de configuración presionamos F2 y se nos aparece el siguiente cuadro donde colocaremos las credenciales que se configuro en el proceso de instalación.

Login name:root Password:Up\$Gye2o2o

Authentication A	Required
Enter an author localhost	ized login name and password for
Configured Keybo Login Name: Password:	oard (US Default) [root] [*******]]
	<pre> Kenter> OK Kesc> Cancel </pre>

Figura 67.Autenticación del Exsi 6.5 Fuente: Los autores

13. Configuración de IP estática para el servidor Dell R210 II.



Figura 68.Configure Network Exsi 6.5 Fuente: Los autores

13.1. Seleccionar IPv4 Configuración.



Figura 69.Configurar ipv4 Fuente: Los autores

13.1.2 Asignar la siguiente IP de manera estática al servidor 172.18.142.5/24, no se añade ninguna IP al Gateway porque no se requiere salida a internet el servidor



Figura 70. Configurar IP estática Fuente: Los autores

13.1.3 Aceptar cambios de configuración.



Figura 71. Confirmación de cambios en la tarjeta de red Fuente: Los autores

3.5. CONFIGURACIÓN DE GNS3-SERVER EN EL SERVIDOR

 Para la instalación de GNS3 SERVER se procede la descarga en la siguiente dirección <u>https://www.gns3.com/software/download-vm</u> y se seleccionamos GNS3 EXSI.



Figura 72.Descarga VMware ESXi 2.2.16 Fuente: Los autores

2. Descomprimir el archivo GNS3.VM.VMware.ESXI.2.2.16

GNS3.VM.VMware.ESXI.2.2.16	5/11/2020 15:25	zip Archive	631.018 KB
GNS3.VM.VMware.ESXI.2.2.16	5/11/2020 15:25	Carpeta de archivos	

Figura 73. Descomprimir archivo zip Exsi 2.2.16 Fuente: Los autores

3. Entrar al browser y ingresamos al servidor exsi con la dirección ip 172.18.142.5, las credenciales administrativas son:

Nombre del usuario: root Password: Up\$Gye2o2o

🥜 Iniciar sesión - VMware ESXi 🛛 🗙	+
$\overleftarrow{\bullet}$ \rightarrow $\overleftarrow{\bullet}$	0 🐔 🕾 https://172.18.142.5/ui/#/login
vmwar	e.
Nombre de usuario root	
Contraseña	
	laisist sasián

Figura 74.Login Exsi 6.5 Browser Fuente: Los autores 4. Ingresamos al sistema de administración para escoger la opción de máquinas virtuales.

vmware [,] esxi ⁻								root@172.18.142.5 🗸	Ayuda 🗸 (Q Buscar
Navegador		🗊 localhost.localdomain - Máquinas vir	tuales							
✓ ☐ Host Administrar		指 Crear/Registrar máquina virtual	💕 Consola 📗	Encender	🛢 Apagar 📲 Susp	ender	C Actualizar 💧	Acciones	Q BU	iscar
Supervisar		Máquina virtual	~	Condicv	Espacio utilizado	Sis	tema operativo invit 🗸	Nombre del host	~ CPU de host	✓ Memoria de ✓
🔮 Máquinas virtuales	0				No hay mác	luinas	virtuales			
Almacenamiento	1	Filtros rápidos	~						No hay elem	entos para mostrar _"
-										

Figura 75.Máquina Virtual Exsi 6.5 Fuente: Los autores

5. Damos clic en crear/registrar máquina virtual y se nos muestra la siguiente ventana, se selecciona implementar una maquinar virtual a partir de un archivo existente OVF u OVA.



Figura 76.Creación de la máquina virtual Fuente: Los autores

6. Introducir el nombre de la máquina virtual y seleccionamos el archivo OVF descargado.

🔁 Nueva máquina virtual - GNS3-SERV	ER		
 1 Seleccionar tipo de creación 2 Seleccione los archivos OVF y 	Seleccione los archivos OVF y VMDK	♦ Carga de archivos ♦ → ▲ ▲ SS3 > GNS3.VM.VMware.ESXI	Buscar en GNS3.VM.VMware
VMDK 3 Seleccionar almacenamiento 4 Contratos de licencia	Introduzca un nombre para la máquina virtual.	Organizar Vueva carpeta	
Configuración adicional Configuración adicional Los nombres de máquinas virtuales pueden tener hasta 80 cara	Escritorio Mombre Descargas M GNS3 VM	Fecha de modificación Iipo 7/10/2020 0:34 Open Virtualizat	
7 Listo para completar	Haga clic para seleccionar ar	 Imágenes * Música Initelecom Proteus8 Vídeos OneDrive Este equipo 	
vm ware [.]		PS3 PIRATA (F:) v < Nombre: GNS3 VM	Todos los archivos Abrir Cancelar
		Atras Siguiente Finalizar Cancelar 20 10:00:67	Se completó correctamente. 05/11/202



7. Seleccionar el almacenamiento donde se va alojar la máquina en nuestro servidor.

🖆 Nueva máquina virtual - GNS3-SERV	ER						
 1 Seleccionar tipo de creación 2 Seleccione los archivos OVF y VMDK 3 Seleccionar almacenamiento 4 Contratos de licencia 5 Opciones de implementación 6 Configuración adicional 7 Listo para completar 	Seleccionar almacenamiento Seleccionar tipo de almacenamiento y almacenamiento Estándar Memoria persistente Seleccione un almacén de datos para los a virtuales.	ién de datos	figuración de la	máquina virtua	l y todos sus d	scos	
	Nombre ~	Capacid 🗸	Libre ~	Tipo ~	Aprovisi 🗸	Acceso	~
	datastore1	215,5 GB	214,55 GB	VMFS5	Compatible	Individual	
						l elementos	3
vm ware [®]							v
			Atrás	Siguien	te Finaliza	ar Can	celar



8. Seleccionar la opción aprovisionamiento fino.

 1 Seleccionar tipo de creación 2 Seleccionar tipo de creación 	Opciones de implementad	lón
VMDK	Seleccionar opciones de implementació	in
 3 seleccionar aimacenamiento 4 Opciones de implementación 5 Listo para completar 	Asignaciones de red	hostonly GNS3 ~
	Aprovisionamiento de disco	€ Fino ○ Grueso
	Encendido automático	
vm ware		
		Atrás Siguiente Finalizar Cancelar

Figura 79.Aprovisionamiento fino máquina virtual Fuente: Los autores

9. Esperar que se cargue la implementación de la máquina virtual.

Navegador 🗆	😰 localhost.localdomain - Máquinas virtuales						
✓ Host Administrar	🖆 Crear/Registrar máquina virtual 📔 💕 Conso	ola 🕨 Encender	📕 Apagar 📲 Susper	nder 🤁 Actualizar 🖏	Acciones	Q Buscar	
Supervisar	Máquina virtual	✓ Condic✓	Espacio utilizado 🛛 🗸	Sistema operativo invit ~	Nombre del host 🗸 🗸	CPU de host 🗸 Mem	oria de 🗸
🗿 Máquinas virtuales 🛛 🚺	🔲 👸 GNS3-SERVER	📀 Nor	0 B	Ubuntu Linux (64 bits)	Desconocido	0 MHz 0 MB	
Almacenamiento Almacena	Filtros rápidos v					1 e	lementos "
	😨 Tareas recientes						c.
	Tarea v D)estino	✓ Iniciador	~ En cola ~	Iniciado v R	esultado 🔺 🗸 🗸	Completade
	Cargar disco - GNS3_VM-disk2.vmdk (2 of 2)	D GNS3-SERVER	root	05/11/2020 15:31:12	05/11/2020 15:31:12	Se completó correctamente.	05/11/2020 1
	Cargar disco - GNS3_VM-disk1.vmdk (1 of 2)	GNS3-SERVER	root	05/11/2020 15:31:12	05/11/2020 15:31:12	O	En ejecución
	Cargar disco - GNS3_VM-disk1.vmdk (1 of 2)	🖞 GNS3 - SERVER	root	05/11/2020 15:05:54	05/11/2020 15:05:54	Se completó correctamente.	05/11/2020 1
	Cargar disco - GNS3_VM-disk2.vmdk (2 of 2)	🖞 GNS3 - SERVER	root	05/11/2020 15:05:54	05/11/2020 15:05:54	Se completó correctamente.	05/11/2020 1
	Destroy	GNS3 - SERVER	root	05/11/2020 10:18:27	05/11/2020 10:18:27	Se completó correctamente.	05/11/2020 1

Figura 80.Instalación OVF GNS3 Fuente: Los autores

10. Performance de la máquina virtual GNS3-SERVER.

🖆 Editar configuración - GNS3-SERVER	Máquina virtual con ESXi 6.0.)		
Hardware virtual Opciones de máq	ui		
🔜 Agregar disco duro 🛛 🎫 Agregar a	daptador de red 🛛 😑 Agregar otro dispositivo		
► 🖬 CPU	3 v		
🕨 🏧 Memoria	21000 MB ~		
Disco duro 1	150 GB ~		8
Disco duro 2	488,28125 GB ~		0
Controladora SCSI 0	LSI Logic Parallel	~	0
Adaptador de red 1	GNS3	V Conectar	\otimes
▶ 🗐 Unidad de CD/DVD 1	Dispositivo host	✓ Conectar	\otimes
Tarjeta de vídeo	Especificar configuración personalizada	~	
			Guardar Cancelar

Figura 81.Performance de la máquina virtual Fuente: Los autores

11. Encender nuestra máquina virutal GNS3-SERVER.

Navegador	🔒 localhost.localdomain - Máquinas vir	tuales						
▼ 🛱 Host Administrar Supervisar	Crear/Registrar máquina virtual	🔮 Consola	Encender	Apagar Suspe	ender C Actualizar 🤹	Acciones	Q Busc	ar Memoria de v
📑 Máquinas virtuales 🛛 🚺	GNS3-SERVER		🕑 Nor	92,26 GB	Ubuntu Linux (64 bits)	gns3vm	27 MHz	1,36 GB
Almacenamiento 1 Q Redes 2	Filtros rápidos	~						1 elementos #
		GNS3-SERVER Sistema operativo inv Compatibilidad	it Ubuntu Li	nux (64 bits)				сри 🔲 27 MHz
		VMware Tools CPU	Sí 3					MEMORIA 1,36 GB
		Memoria Nombre del host	21,48 GB gns3vm				ALM	92,26 GB

Figura 82.Encendido de la máquina virtual Fuente: Los autores 12. Ventana de nuestra máquina virtual encendida.



Figura 83.GNS3-SERVER encendida Fuente: Los autores

12.1 Entrar en las configuraciones de GNS3 2.2.16 para dejar definida la ip estática de la máquina virtual, damos enter en OK.



Figura 84. Ventana de configuración GNS3 2.2.16 Fuente: Los autores

12.2 Para acceder a las configuraciones de red, vamos a la opción Network.

GNS3 2.2.16 Information Channel Upgrade Shell Log Test Qemu Security Keyboard Console Configure Proxy Migrate Restore Shrink Reboot Shutdown	Display VM information Select the release channel Upgrade the GNS3 VM Open a shell Show the GNS3 server log Check Internet connection Switch Qenu version Configure server authentication Change keyboard layout Change console settings (font size etc.) Edit server configuration (advanced users ONLY) Configure proxy settings Configure network settings Migrate data to another GNS3 VM Restore the VM (if an upgrade has failed) Shrink the VM disk Reboot the VM
	< <u>OK</u> → <cancel></cancel>

Figura 85.Network GNS3 2.2.16 Fuente: Los autores 12.2 Configuración de la IP estática para GNS3 2.2.16, una vez asignada la dirección IP tecleamos Crtl+O para guardar los cambios.



Figura 86. Configuración IP estática GNS3 2.2.16 Fuente: Los autores 13. Ventana de GNS3 2.2.16 con la nueva dirección IP.



Figura 87. GNS3 2.2.16 Fuente: Los autores

3.6. INSTALACIÓN DE LOS IOS EN EL SERVIDOR GNS3.

Para elaboración de las prácticas de redes definidas por software se instaló routers, switches, firewall y sistemas operativos de Windows que se detallan a continuación:

ROUTERS

SERIE C1700, SERIE C2600, SERIE C3620, SERIE C3660, SERIE C2691,SERIE C3725 SERIE C7200, ROUTERBOARD MIKROTIK Y HPE VSR1001.

SO WINDOWS

WINDOWS7, WINDOWS 10.

FIREWALL

FORTIGATE, SOPHOS XG, CHECKPOINT FIREWALL, PALO ALTO Y JUNIPER FIREWALL Y PFSENSE.

SWITCHES

CISCO Lv2.

Se detalla los pasos a seguir para la instalación de los IOS en el servidor GNS3-SERVER.

1. Buscar el archivo gns3a para la instalación de la aplicación de Windows



Figura 88.Import appliance GNS3 2.2.16 Fuente: Los autores

2. Abrir archivo Gns3a donde se encuentra ubicado.



Figura 89.Ubicación del archivo Gns3 Fuente: Los autores 3. Seleccionar donde se va a guardar la aplicación de Windows 7.

👌 Install Windo	ows appliance						
erver Please choose	a server type to instal	the appliance. The gr	ayed out server ty	pes are not suppo	orted or configure	d.	
Server type							
O Install t	he appliance on a remo	te server					
🔿 Install t	he appliance on the GN						
• Install t	he appliance on the ma	in server					
							Analasa : C
							Appliance info

Figura 90.Selección de instalación Fuente: Los autores

4. Elegir la versión de Windows en este caso es Windows 7.





5. Cargar los archivos VMware disk del sistema seleccionado que va a ser almacenado en el servidor.

Required Please	I files select one version of Windows and import t	he required files. Files are s	Abrir ← → ▼ ↑	v ♂ . P Buscar en IE11-Win7-VMWare
Appli:	ance version and files /indows version 10 w/ Edge MSEdge-Win10-V/Mware-disk1.vmdk /indows version 10 w/ Edge (Preview) MSEdgeWin10_preview.vmdk /indows version 8.1 w/ IE11 IE11Win8.1-disk1.vmdk /indows version 7 w/ IE10 IE10Win7-disk1.vmdk /indows version 7 w/ IE9 IE9Win7-disk1.vmdk /indows version 7 w/ IE8	Size Status 6.8 GB Missing files 6.8 GB Missing files 10.2 GB Missing files 5.3 GB Missing files 5.3 GB Missing files 3.8 GB Missing files	Organizar ▼ Nueva carpeta Escritorio Descargas Documentos Inágenes gns3 firewall Música Proteus8	Fecha de modificación Tipo 7/3/2018 3:54 Archivo MF 7/3/2018 3:54 Open Virtualizat 7/3/2018 3:54 Virtual Machine
Ĩu	Iport Download	3.9 UB Wissing	OneDrive Este equipo PS3 PIRATA (F:) Allow custom files Greate a new version	All Files Abrir Cancelar

Figura 92.Selección del archivo vmware disk Fuente: Los autores

6. Esperar que el archivo se transfiera al servidor, depende del tamaño del archivo esto demorar en cargar.

Appliance version and files	Size	Status
 Windows version 10 w/ Edge MSEdge-Win10-VMwsredisk1/wmdk Windows version 10 w/ Edge (Preview) MSEdge-Win10_preview.vmdk Windows version 8.1 w/ IE11 IE11Win8.1-disk1/wmdk Windows version 7 w/ IE10 IE10_Win7-disk1/wmdk Windows version 7 w/ IE10 IE10_Win7-disk1/wmdk Windows version 7 w/ IE8 Windows version 7 w/ IE8 	6.8 GB 6.8 GB 10.2 GB 10.2 GB 5.3 GB 5.3 GB 3.8 GB 3.8 GB 3.8 GB 3.8 GB 3.8 GB 3.8 GB 3.8 GB 3.8 GB 3.8 GB	Missing files Missing Missing files Missing files Missing files Missing files Missing tiles Missing ↓ Uploading IE11
IE8Win7-disk1.vmdk	3.9 GB	Missir 92%

Figura 93. Selección del archivo vmware disk Fuente: Los autores 7. Una vez finalizada la transferencia del archivo le aparece el siguiente mensaje.

ne template will be available in the guest	category.				
nese virtual machines expire after 90 da	ys; i.e. you have to re-create them	in your project after this tim	e but you don't have to re-impo	ort the appliance.	
efault credentials: IEUser / Passw0rd!					
			Appliance infe	-k Einich	

Figura 94. Finalización del archivo Fuente: Los autores

Nota:

Para la instalación de los archivos restante como es firewall,routers y switch seguir los pasos anteriores.

3.7. DESCRIPCIÓN TÉCNICA DE LOS DISPOSITIVOS DEL BANCO

Los dispositvos del banco de pruebas de redes definidas por software para redes de área amplia (SD-WAN), fueron seleccionados para sastifacer la necesidad de recursos faltante en el momento de simular este tipo de tecnología orientado para los estudiantes y docentes que imparten las materias de redes de computadoras y redes de comunicación que van hacer uso de este banco de pruebas siendo asi que la mayoría de estos dispositivos informáticos se encuentra en nuestro mercado local y son fácil de adquision en caso llegaran a averiarse.

A continuación detallamos los elementos incluidos en el banco de prueba.

3.8. Dell PowerEdge R210 II

El R210 II se puede implementar en prácticamente cualquier entorno, tiene la potencia que se necesita para que su empresa funcione y brinda la escalabilidad para ayudarla a crecer.Comparta, administre y proteja sus datos, todo con un solo sistema. (DELL,2012).

Dentro de sus características técnicas:

- Valor empresarial: rendimiento y funciones para facilitar la colaboración, el uso compartido y la protección de datos y la fácil escalabilidad.
- Fácil de administrar: controladora del ciclo de vida de Dell™ y conjunto completo OpenManage™ para una administración remota simplificada.
- Tecnología flexible y segura: discos duros redundantes integrados, cifrado, opciones de seguridad y protección de datos. Ver Anexo C



Figura 95. Dell R210 II Fuente: https://www.dell.com/ec/empresas/p/poweredge-r210-2/pd

3.9. KINGSTON A400 SSD SATA de 2,5"

La unidad A400 de estado sólido de Kingston brinda formidables mejoras en la velocidad de respuesta, sin actualizaciones agregadas del hardware. Ofrece tiempos de arranque, carga y de transmisión de archivos extraordinariamente más transitorios en comparación con las unidades de disco duro mecánico. Ver Anexo D



Figura 96.SSD Kingston A400 Fuente: https://www.kingston.com/es/ssd/a400-solid-state-drive

CAPÍTULO IV

MANUAL DE PRÁCTICAS DEL LABORATORIO

Se realiza el desglose de practicas a implementar en el banco de pruebas virtualizado para redes definidas por software para redes de área amplia (SD-WAN) para la ejecución de estas practicas los estudiantes deben tener conocimiento de las materias de redes de computadoras I y redes de computadoras II teniendo en cuenta los dispositivos que van para configurar para fortalecer sus destrezas técnicas en el momento de realizar las simulaciones.

4.1. GUIA DE PRÁCTICAS PARA PRUEBAS DE REDES DEFINIDAS POR SOFTWARE PARA REDES DE AREA AMPLIA (SD-WAN)

PRÁCTICA 1: Conexión remota al servidor virtual con el software GNS3.

PRÁCTICA 2: Configuración de una red SD-WAN con Fortigate 6.2.0.

PRÁCTICA 3: Configuración de una red SD-WAN con perfomance SLA en

fortigate 6.4.2.

PRÁCTICA 4: Configuración de una red SD-WAN con prioridad de servicios

con sd-wan rules.

PRÁCTICA 5: Configuración de una red SD-WAN con fortigate y enlazados

con dispositivos mikrotik.

PRÁCTICA 6: Configuración de una red VPN IPSEC fortigate a fortigate.

PRÁCTICA 7: Configuración de una red VPN IPSEC con balanceo sd-wan.

PRÁCTICA 8: Configuración de un failover con mikrotik para un enlace SD-WAN

PRÁCTICA 9: Configuración de un mangle con mikrotik para el enlace SD-WAN.

PRÁCTICA 10: Configuración de un layer 7 con calidad de servicios QOS para el enlace SD-WAN utilizando mikrotik.

4.1.1. PRÁCTICA 1

Conexión remota al servidor virtual con el software de GNS3.

DATOS INFORMATIVOS

- > MATERIA: Redes de comunicación
- > PRÁCTICA Nº 1
- > NUMERO DE COMPUTADORAS: 10
- > **TIEMPO QUERIDO:** 2 Horas

DATOS DE LA PRÁTICA

TEMA: Conexión de acceso remota al servidor virtual con el software de

GNS3.

OBJETIVOS

General

Establecer conexión de manera remota para seguir la realización de las prácticas de laboratorio para redes definidas por software para redes de área amplia (SD-WAN).

Específicos

- > Descargar, instalar en la computadora GNS3.
- > Conectar remotamente la computadora al servidor virtual.

GLOSARIO

GNS3 .- GNS3 es un software manejado por ingenieros de redes para emular, configurar, experimentar y solucionar dificultades de redes virtuales y reales.

SD-WAN.- Las redes de área amplia definidas por software o SD-WAN (software-defined networking area network), tienen como enfoque el diseño empresarial , instituicional y corporativo para mejorar el uso de recursos en las redes internas de empresas en la red, para optimizar el desempeño y concretar el tráfico de nuestra red, sea de Internet o interconexión de sedes.

CONEXIÓN REMOTA. - Tiene como hecho de conectarse a servicios, aplicaciones o datos de TI desde un sitio diferente a la sede central o una establecimiento más cercana al centro de datos. Esta conexión consiente a los usuarios acceder a una red o una computadora de forma remota por medio de una conexión a Internet.

IP.- La internet protocol address se fundamenta en el protocolo de Internet, que es, también, la base del funcionamiento de Internet. Se trata de la dirección inequívoca de un dispositivo (por ejemplo, una computadora,un servidor de streaming o de una impresora) dentro de una red interna o externa.

MARCO PROCEDIMENTAL

1. Descargar e instalar el software GNS3 para conexión remota al servidor virtualizado, desde el siguiente link.

Download GNS3 Select the installer for your favourite OS Image: Constant of the installer for your favourite OS </t

https://www.gns3.com/software/download

Figura 97. Descargar Gns3 Fuente: Los autores

2. Conectar de manera remota nuestra computadora a través de TCP/IP al servidor virtualizado.

😵 Setup Wizard		?	\times
Server Please choose how would like to run your GNS3 network simulation is strongly recommended on Windows and Mac OS X.	ons. The GNS3 \	/M optio	n
O Run appliances in a virtual machine			
Requires to download and install the GNS3 VM (available for free)			
Run appliances on my local computer			
A limited number of appliances like the Cisco IOS routers <= C720	0 can be run		
Run appliances on a remote server (advanced usage)			
The server will be on a remote computer and can be shared with r	nultiple users		
Don't show this again			
N	ext >	Cancel	

Figura 98. Conexión al servidor Fuente: Los autores. 3. Escribir la dirección IP que se encuentra en la imagen y colocamos en usuario y contraseñas la palabra gns3.

🔮 Setup Wi	zard	?	\times
Remote s Everyt	erver hing will run on a remote server. No data will be saved on this computer.		
Host:	172.18.142.8		
Port:	80 TCP		\$
✓ Enable	authentication		
User:	gns3		
Password:	••••		
	< <u>B</u> ack <u>N</u> ext >	Cano	el



4. Conexión existosa al servidor

😤 Setup Wizard				?	\times
Summary The server typ	e has been configure	d, please see the su	mmary of the setting	s below	
Server type: Host: Port: User:	Remote 172.18.142.8 80 gns3				
		< <u>B</u> ack	Einish	Cance	1

Figura 100. Conexión establecida a gns3 server Fuente: Los autores

5. Seleccionar el proyecto o crear nuevo proyecto.

GNS3	: View Control Node Annotate Tools Help				- 0 X
			<u>^</u>	Topolog Node	yy Summary 🛛 🕅 🕅 Console
		Project Project Project Project New project New project Den project Eccent project 1. REDES DEFINIDAS POR SOFTWARE PARA REDES DE AREA AMPLIA (SD-WAN)	?	×	mmary @ @ sin server CPU 0.0%, RAM 17.2%
5	Console GNSS management console. Running GNS3 version 2.2.13 on Windows (64-bit) with Coxynight (c) 2006-2020 GNS3 Technologes. Use Help -> GNS3 Doctor to detect common issues. =>	Settings OK	c	ancel	02

Figura101. Proyecto en Gns3 Fuente: Los autores

RECURSOS UTILIZADOS

- > COMPUTADORA
- > CABLE DE RED (PATCHCORD)

CRONOGRAMA/CALENDARIO

De acuerdo con la planificación de cada docente

4.1.2. **PRÁCTICA 2**

DATOS INFORMATIVOS

- > MATERIA: Redes de comunicación
- > PRÁCTICA Nº 2
- > NUMERO DE COMPUTADORAS: 16
- > TIEMPO CONSIDERADO: 2 Horas

DATOS DE LA PRÁTICA

TEMA: Configuración de una red SD-WAN con Fortigate 6.2.0

OBJETIVOS

<u>General</u>

Configurar punto a punto con redes definidas con software para redes de

área amplia SD-WAN para acceso a internet.

Específicos

- > Realizar uso más efectivo de conexiones de internet.
- > Configurar Vlans para administración de la red.
- > Programar interfaces SD-WAN para los enlaces a internet.

GLOSARIO

SD-WAN.- Las redes de área amplia definidas por software o SD-WAN (software-defined networking area network), tienen como enfoque el diseño empresarial , instituicional y corporativo para mejorar el uso de recursos en las redes internas de empresas en la red, para optimizar el desempeño y concretar el tráfico de nuestra red, sea de Internet o interconexión de sedes.

VLANS.- Una Virtual Local Area Network (VLAN) o red de área local virtual es un conjunto flexible de dispositivos que se hallan en diferente sitio de una red de área local pero se notifican como si existieran en el mismo segmento físico.

SWITCH O CONMUTADOR.- Es un dispositivo de interconexión utilizado para enlazar equipos en una redde datos estableciendo lo que se conoce como una red de área local (LAN). MARCO PROCEDIMENTAL

1. Crear nuevo proyecto para realizar la práctica 2.

😵 Project	?	\times
New project Projects library		
New project		
Name: PRACTICA 2)
Open project		
Recent projects		
Settings OK	Cance	ł

Figura102. Nuevo proyecto Fuente: Los autores

2. Diseñar la topología de la práctica 2 donde las sucursales son los dispositivos de firewall fortigate.



Figura103. Diseño de la red práctica №2 Fuente: Los autores

3. Encender sucursal 1 y sucursal 2.



Figura104. Encendido de sucursales fortigate 6.2.0 Fuente: Los autores

4. Iniciar por modo console en sucursal 2



Fuente: Los autores

5. Escribir en el login la palabra admin y la contraseña en blanco en esta versión de fortigate 6.2.0, te permite ingresar a la configuración sin realizar el cambio de contraseña a la administración del equipo comenzaremos a configurar sucursal 2.



Figura106. Visualización del CLI Fuente: Los autores

6. Para mostrar la IP del fortigate de sucursal1 debemos ingresar el siguiente comando: get system interface – donde en port1 nos muestra la dirección IP que obtuvo de muestro router.

FortiGate-VM64-KVM # get system interface
name: port1 mode: dhcp ip: 172.18.142.84 255.255.255.0 status: up netbios-forward: disable type: physical net
flow-sampler: disable sflow-sampler: disable src-check: enable explicit-web-proxy: disable explicit-ftp-proxy: d
isable proxy-captive-portal: disable mtu-override: disable wccp: disable drop-overlapped-fragment: disable dr
op-fragment: disable
= [port2]
name: port2 mode: static ip: 0.0.0.0.0.0.0.0 status: up netbios-forward: disable type: physical netflow-sampl
er: disable sflow-sampler: disable src-check: enable explicit-web-proxy: disable explicit-ftp-proxy: disable
proxy-captive-portal: disable mtu-override: disable wccp: disable drop-overlapped-fragment: disable drop-fragmen
t: disable
== [port3]
name: port3 mode: static ip: 0.0.0.0 0.0.0.0 status: up netbios-forward: disable type: physical netflow-sampl
er: disable sflow-sampler: disable src-check: enable explicit-web-proxy: disable explicit-ftp-proxy: disable

Figura107. Dirección IP sucursal 2 del Fortigate 6.2.0 Fuente: Los autores 7. Ingresar al fortigate por navegador con la dirección la dirección IP que obtuvo de nuestro router.

172.18.142.84/login	×		
)→ ሮ	0 🔏 172.18.142.84/	igin	🖂 🕁
		4**	
		Username	
		Password	
		Login	
			_

Figura 108. Interfaz Web Fortigate Fuente: Los autores

8. Configurar la dirección ip para la red SD-WAN, damos en click en la interface port2.

FortiGate VM64-	KVM For	tiGate-VM64-KV	/M					≻ [] @+ 4 0	🕗 admin •
Dashboard	> ^								
🔆 Security Fabric	>	E FortiGat	e VM64-KVM	135					
E FortiView	>		11						
+ Network	~			246	8 10 12 14 16 18				
Interfaces	☆	+ Create Ne	w • Inter	face	🔳 port2]		By Type By Role Al	phabetically
DNS		T Status	Link		10000 Mbps / Full Duplex	sk	T Type	T Access	T Ref.
Packet Capture		Physical (6)	Туре		Physical Interface				
SD-WAN		0	port: Fort	Telemetry	8 172.18.142.83 255.25	5.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access	0
SD-WAN Rules		O	port2		0.0.0.0 0.0.0.0	-	Physical Interface		0
Performance SLA		0	port3		0.0.0.0 0.0.0.0		Physical Interface		0
Chattle Davidas		0	port4		0.0.0.0 0.0.0.0		Physical Interface		0
Static Routes		0	port5		0.0.0.0 0.0.0.0		Physical Interface		0
Policy Routes		0	port6		0.0.0.0 0.0.0.0		Physical Interface		0



^ Edit Interface Dashboard > 🔆 Security Fabric > Interface Name port2 (0C:96:EC:36:6F:01) E FortiView > Alias INTERNET- SUCURSAL 1 Network ~ Link Status Up 🕥 Interfaces Physical Interface Туре DNS kbps Downstream Estimated Bandwidth 0 kbps Upstream 0 Packet Capture SD-WAN Tags SD-WAN Rules Role 1 WAN • Performance SLA Add Tag Category Static Routes Policy Routes Address RIP Manual DHCP Addressing mode OSPF IP/Network Mask 10.10.10.2/255.255.255.252 BGP Administrative Access Multicast ✓ HTTPS PING FMG-Access CAPWAP System > IPv4 SSH SNMP 🗆 FTM Policy & Objects > RADIUS Accounting FortiTelemetry Security Profiles > Receive LLDP 1 Use VDOM Setting Enable Disable

9. Ingresar nombre de la interfaz y su respectiva dirección de red.

Figura110. Configuración del port2 Fuente: Los autores

Ingresar a create new para la configuración de la interface VLAN
 10

Dashboard Security Fabric	> ^ >	E FortiG	iate VM64-k	(VM 1357944	43 45 47				
E FortiView	>		III						
+ Network	~			2 4 6 8 10 12	14 16 18				
Interfaces	☆	+ Create	New 🕶 🥒	Edit 📋 Delete				By Type By Role Alphab	etically
DNS		Interface		T Name	T Members	T IP/Netmask	▼ Туре	T Access	T Ref.
Packet Capture		Zone							
SD-WAN		Virtual Wir	e Pair 1			172.18.142.83 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access	0
SD-WAN Rules		0	port2 (IN	ITERNET SUCURSAL 1)		10.10.10.2 255.255.255.252	Physical Interface	PING	0
Performance SLA		o	port3			0.0.0.0 0.0.0.0	Physical Interface		0
Chattle Davitas		0	port4			0.0.0.0 0.0.0.0	Physical Interface		0
Static Routes		ο	port5			0.0.0.0 0.0.0.0	Physical Interface		0
Policy Routes		0	port6			0.0.0.0 0.0.0.0	Physical Interface		0

Figura111. Interface Virtual Fuente: Los autores

11. Configurar la interfaz VLAN 10 para la red local.

Dashboard >	New	
☆ Security Fabric >		
► FortiView >	Interface Name VLAN 10	
+ Network	Alias DATOS	
	Type VLAN 💌	
IIIterraces H	Interface port3	
DNS	VLANID 10	
Packet Capture		
SD-WAN	Tags	
SD-WAN Rules	Role 🚺 I AN 👻	
Performance SLA	Add Tag Category	
Static Routes	- 0 0 /	
Policy Routes	Address	
RIP	Addressing mode Manual DHCP	
OSPF	IP/Network Mask 192.168.0.1/24	
BGP	Create address object matching subnet 🔘	
Multicast	Name IVLAN 10 address	
T TOTE TO OUT		

Figura112. Configuración de interfaz VLAN-IP Fuente: Los autores

12. Configurar DHCP server para la red local de la interfaz vlan 10

FortiGate VM64-KV	M For	tiGate-VM64-KVM							>_	0	?∙	4	👤 admir
2 Dashboard	> ^	Edit Interface											
🔆 Security Fabric	>												
🛎 FortiView	>	Administrative Acce	ISS										
+ Network	~	IPv4 HTTPS	PIN	G	FMG-Access	CAPWA	р						
Interfaces	☆	RADIUS A	LI SNN Accounting	чР	FIM FortiTelemetry								
DNS													
Packet Capture		O DHCP Server											
SD-WAN		Address Range											
SD-WAN Rules		+ Create New	🖋 Edit	🗊 Delete	е								
Performance SLA		Starting IP	Er	nd IP									
Static Routes		192.168.0.2	192.168.0	.254									
Policy Routes		Netmask	255.255.255	5.0									
RIP		Default Gateway	Same as Inte	erface IP	Specify								
OSPF		DNS Server	Same as Syst	tem DNS	Same as Interface	P Specify							
BGP		Advanced											
Multicast													

Figura 113. Configuración de DHCP interfaz VLAN 10 Fuente: Los autores

13. Visualización de todas las interfaces de red configuradas.

Dashboard	> ^			40 45 47				
🔆 Security Fabric	>	E. FortiGa	te vmo4-kvm					
🖿 FortiView	>							
+ Network	~		2 4 6 8 10 14	14 16 18				
Interfaces	☆	+ Create N	ew 🕶 🎤 Edit 📋 Delete				By Type By Role Alphab	oetically
DNS		▼ Status	T Name	T Members	T IP/Netmask	▼ Туре	T Access	T Ref.
Packet Capture	- 11	Physical (7)						
SD-WAN		0	port1		172.18.142.83 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access	0
SD-WAN Rules		0	port2 (INTERNET SUCURSAL 1)		10.10.10.2 255.255.255.252	Physical Interface	PING	0
Performance SLA		• •	port3		0.0.0.0 0.0.0.0	Physical Interface		1
Static Pouton			VLAN 10 (DATOS)		192.168.0.1 255.255.255.0	🚳 VLAN	PING HTTPS	2
Static Routes		0	port4		0.0.0.0 0.0.0.0	Physical Interface		0
Policy Routes		0	port5		0.0.0.0 0.0.0.0	Physical Interface		0
RIP		0	port6		0.0.0.0 0.0.0.0	Physical Interface		0

Figura114. Interfaces Configuradas Fortigate Oficina Central Fuente: Los autores

14. Seleccionar static route para salida a internet.

Dashboard	> ^	+ Create New 🖋 Edit	Clone 🗎 Delete Search		Q	
☆ Security Fabric Image: A security Fabric	>	Destination 🗢	Gateway IP 🌲	Interface 🌩	Status ≑	Comments ≑
+ Network	~					
Interfaces						
DNS						
Packet Capture						
SD-WAN						
SD-WAN Rules						
Performance SLA						
Static Routes	☆					
D-8 Dt				No cosulto		

Figura115. Módulo de static routes Fuente: Los autores 15. Configurar la por cual interfaz tendremos salida internet en este caso es por el port1 donde se asignará automáticamente la IP del Gateway de nuestro router, también se le puede asignar de manera manual.

New Static Route		
Destination 6	Subpet Internet Service	
Destination		
	0.0.0.0/0.0.0.0	
Interface	m port1 👻	
Gateway Address 🕄	Dynamic Specify 172.18.142.100	
Administrative Distance 🕄	10	
Comments	Write a comment:: 0/255	
Status	• Enabled • Disabled	

Figura116. Configuración static routes Fuente: Los autores

16. Realizaremos un ping a la siguiente dirección 8.8.8.8 para verificar la salida de internet del dentro del fortigate de sucursal 2.

🍘 Dashboard	•	System Inform	nation	-	Licenses	CLI Console 🛛 🗎 📩 🖪	×
Status	☆				LICENSES		l
Top Usage LAN/DMZ			FortiGate-VM64-KVM		FortiCare Support	Connected	l
Security			FGVMEVSGCGCQNFCC		Firmware & Gen	FortiGate-VM64-KVM # execute ping 8.8.8.8 PING 8.8.8.8 (8.8.8.8): 56 data bytes	
🔆 Security Fabric	>		v6.2.0 build0866 (GA)		O IPS	64 bytes from 8.8.8.8: icmp_seq=0 ttl=110 time=63.1 ms 64 bytes from 8.8.8.8: icmp_seq=1 ttl=110 time=66.2 ms	l
🛎 FortiView	>		NAT		AntiVirus	64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=68.7 ms 64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=65.6 ms	
Network	>		2020/09/13 12:18:56		Mah Filtoring	64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=64.3 ms	l
System	>		00:00:11:24		CostiTakan	8.8.8.8 ping statistics	
📕 Policy & Objects	>		Unknown		FOLLIOKEN	round-trip min/avg/max = 63.1/65.5/68.7 ms	l
Security Profiles	>				070	FortiGate-VM64-KVM #	
□ VPN	>		Eia	ura	117 Pina	a Google	l

Figura117. Ping a Google Fuente: Los autores

17. Configurar la política para tener todos los servicios de navegación para nuestra red de la sucursal 1 y la red local de la VLAN 10, solo se puede crear máximo 5 políticas en este entorno virtual.

FortiGate VM64-KV	M For	tiGate-	VM64-KVM									⑦ • ↓2
Dashboard	> ^	+ (Create New 🖌	Edit 🗊	Delete Q Pol	licy Lookup	Search				Q Interfac	ce Pair View By Sequence
🔆 Security Fabric	>	ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bvtes
FortiView	>		aplicit 1							,	Ŭ	,
Network	>	0	Implicit Denv	:≣ all							Disabled	0.B
System	>	<u>v</u>	Implicit Deliy	all	all	LO always	ALL	U LINI			Disabica	00
Policy & Objects	~											
IPv4 Policy	ជ											
Authentication Rules												
IPv4 DoS Policy												

Figura 118. Ipv4 Policy Sucursal 2 Fuente: Los autores

FortiGate VM64-KV	/M Fo	rtiGate-VM64-KVM						≻_ []_ @•	Д🛛 🕗 admin т
Bashboard	> ^	New Policy			Service	🖪 ALL			
🔆 Security Fabric	>				Category	General	Coloct Entrico		
🖿 FortiView	>	Name 🜖	DATOS VLAN		Protocols	any	O Seereb	+ Creata	
Network	>	Incoming Interface	d DATOS (VLAN 10)	•	References	0		T Create	
System	>	Outgoing Interface	i port1	•	View		General (5)		
Policy & Objects	~	Source	🖃 all	×			* ALL	Ø	
IPv4 Policy	☆		+				ALL_ICMP		
Authentication Rules		Destination	😑 all	×			ALL_ICMP6		
Authentication Rules			+				ALL_TCP		
IPv4 DoS Policy		Schedule	o always	-			ALL_UDP		
Addresses		Service	ALL	×			Web Access (2)		
Wildcard FQDN			+				HTTP		
Addresses		Action	✓ ACCEPT Ø DENY				HTTPS		
Internet Service Databas	se						File Access (8)		
Services		Inspection Mode	Flow-based Proxy-based				AFS3		
Cabadulaa							FTP FTP		
Schedules		Firewall / Network O	Intions				FTP_GET		
Virtual IPs		Thewait/ Network C	prions				FTP_PUT		
IP Pools		NAT	•				NFS		
D		IP Pool Configuration	n Use Outgoing Interface Add	Iress Use	Dvnamic IP Pool		SAMRA	¥	
		Figura	119.Configura	ción	de los s	servi	cios Sucur	sal 2	
		0	Fuer	nte I	os auto	res			

18. Realizar la configuración de la política para navegación sin restricción para la red local.

19. Políticas creadas para la VLAN 10 de red local

FortiGate VM64-KV	A For	tiGate-\	/M64-KVM							>_	[] @•	🗘 🛛 👤 admin 🕶 🗸
Dashboard	> ^	+ (reate New 🧳	Edit 📋	Delete Q Pol	icy Lookup	Search			Q	Interface Pair	View By Sequence
🔆 Security Fabric	>											
E FortiView	>	U	Name	Source	Destination	Schedule	Service	Action	NAI	Security Profiles	Log	Bytes
Network	>		DATOS (VLAN :	L0) → 🔜 por	t1 1							
System	>	1	DATOS VLAN	🔳 all	🖃 all	o always	🛛 ALL	✓ ACCEPT	Enabled		UTM	
Policy & Objects	~	🗖 In	nplicit 1									
IPv4 Policy	☆	0	Implicit Deny	🗐 all	🔳 all	o always	ALL ALL	O DENY			8 Disabled	0 B

Figura 120. Políticas Vlan 10 Fuente: Los autores

20. Realizar la configuración de la política de navegación para la red de la

🚯 Dashboard	> ^	Edit Policy		
🔆 Security Fabric	>			
FortiView	>	Name 🚯	INTERNET-SUCURSAL 1	
Network	>	Incoming Interface	INTERNET- SUCURSAL 1 (port2) 🔻
System	>	Outgoing Interface	MAN - INTERNET (port1)	•
🖹 Policy & Objects	~	Source	🗐 all	×
IPv4 Policy	☆		+	
Authentication Rules		Destination	🗉 all	×
IPv4 DoS Policy		Schodulo	T always	
Addresses		Sonvico		•
Wildcard FQDN Addresses Internet Service Databa	ase	Action		
Services		Inspection Mode	Flow-based Proxy-based	
Virtual IPs		Firewall / Network O	ptions	
IP Pools		NAT		
Protocol Options		IP Pool Configuration	Use Outgoing Interface Addre	ss Use Dynamic IP Pool
Traffic Shapers		Preserve Source Port		
Traffic Chaning Dollar		Protocol Options	PRX default	→
			sucursal	

Figura 121. Configuración de las políticas para Sucursal 1 Fuente: Los autores 21. Iniciar Switch 2 para la configuración de la VLAN 10.

:	SWITCH2	× 🕀						_ □	×
Nov 1 Nov 1	6 21:06:00.736: 6 21:06:00.736: 6 21:06:00.739: 6 21:06:00.741: 6 21:06:00.741: 6 21:06:00.741: 6 21:06:00.745: 6 21:06:00.745: 6 21:06:00.746: 6 21:06:00.746: 6 21:06:00.751: 6 21:06:00.015: 6 21:06:02.0075: 6 21:06:02.0075: 6 21:06:02.0015: 6 21:06:02.011: 6 21:06:02.015: 6 21:06:23.015: 6 21:06:33.05: 7 20:05:33.05: 7 20:05:35.05: 7 20:05	%LINK-3-UPDOWN: Inte %LINK-3-UPDOWN: Inte %LINEPROTO-5-UPDOWN: %LINEPROTO-5-UPDOWN: %LINEPROTO-5-UPDOWN: %LINEPROTO-5-UPDOWN: %LINEPROTO-5-UPDOWN: %LINEPROTO-5-UPDOWN: %LINEPROTO-5-UPDOWN: %LINEPROTO-5-UPDOWN: %LINEPROTO-5-UPDOWN: %LINEPROTO-5-UPDOWN: %LINEPROTO-5-UPDOWN: %LINEPROTO-5-UPDOWN: %LINEPROTO-5-UPDOWN: %LINEPROTO-5-UPDOWN: %SYS5-RESTART: Syst %LINEPROTO-5-UPDOWN: %SYS5-RESTART: Syst %LINEPROTO-5-UPDOWN: %PLATFORM-5-SIGNATUR %PLATFORM-5-SIGNATUR	face GigabitEthern face GigabitE	tet3/0, changed tet2/3, changed tet2/2, changed tet2/2, changed tet1/3, changed tet1/2, changed tet1/2, changed tet1/2, changed tet1/2, changed tet0/3, changed tet0/3, changed tet0/1, changed tet0/2, change	state to down state to up itEthernet3/2, itEthernet2/3, itEthernet2/4, itEthernet2/8, itEthernet2/8, itEthernet1/2, s.2(4.0.55)E,	changed sta changed sta	te to dow te to dow ste to dow te to dow te to dow	n in in in in in in i j_WEEKLY B	∧ VILD, ifica
tion ******	*****								
* IOSv * educa * Techa * of tl * purpa * Cisca ****** Switch	is strictly lim ation. IOSv is p nical Advisory O he IOSv Software oses is express o in writing.	ited to use for eval rovided as-is and is enter. Any use or di or Documentation to y prohibited except	Nation, demonstrati not supported by C closure, in whole any third party fo s otherwise author	ion and IOS * Sisco's * or in part, * or any * vized by *					v

Figura 122. Iniciando Switch Fuente: Los autores

22. Configurar la VLAN 10 en el switch.



Figura 123. Creación VLAN-10 Datos Fuente: Los autores

23. Configurar puerto troncal switch 2.



Figura 124. Puerto Trunk VLAN Fuente: Los autores

24. Asignar VLAN la 10 a los puertos que vamos usar.



Figura 125. Puerto Access VLAN 10 Fuente: Los autores
25. Iniciar las VPCS ,teclear DHCP para obtener dirección IP y realizamos un ping a la siguiente dirección para verificar la salida a internet.



Figura 126. Comprobación de internet PC3 Sucursal 2 Fuente: Los autores

26. Entrar por console al fortigate sucursal 1 para obtener la dirección IP que obtuvo de nuestro router local escribimos el siguiente comando get system interface.

.

ortiGate-VM64-KVM # get system interface
- [port] me: port] mode: dhcp ip: 172.18.142.93 255.255.255.0 status: up netbios-forward: disable type: physical net low-sampler: disable sflow-sampler: disable src-check: enable explicit-web-proxy: disable explicit-ftp-proxy: d sable proxy-captive-portal: disable mtu-override: disable wccp: disable drop-overlapped-fragment: disable dr p-fragment: disable = [port2]
ame: port2 mode: static ip: 10.10.10.2 255.255.252 status: up netbios-forward: disable type: physical ne flow-sampler: disable sflow-sampler: disable src-check: enable explicit-web-proxy: disable explicit-ftp-proxy: isable proxy-captive-portal: disable mtu-override: disable wccp: disable drop-overlapped-fragment: disable d pp-fragment: disable = [port3]
ame: port3 mode: static ip: 0.0.0.0.0.0.0.0.0 status: up netbios-forward: disable type: physical netflow-sampl r: disable sflow-sampler: disable src-check: enable explicit-web-proxy: disable explicit-ftp-proxy: disable roxy-captive-portal: disable mtu-override: disable wccp: disable drop-overlapped-fragment: disable drop-fragmen : disable = [port4]
ame: port4 mode: static ip: 0.0.0.0 0.0.0 status: up netbios-forward: disable type: physical netflow-sampl : disable sflow-sampler: disable src-check: enable explicit-web-proxy: disable explicit-ftp-proxy: disable roxy-captive-portal: disable mtu-override: disable wccp: disable drop-overlapped-fragment: disable drop-fragmen : disable -More
solarwinds 🕫 Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

Figura 127. Comprobación de internet PC3 Sucursal 2 Fuente: Los autores

27. Entrar via browser con la IP asignada.

172.18.142.93/login	× +					
(←) → C ²	0 🔏 172	.18.142.93/login				
<u> </u>						
			272			
			l	Jsername		
			F	Password		
					Login	

Figura 128. Browser Fortigate Sucursal 2 Fuente: Los autores

28. Configurar la interface port2 fortigate sucursal 1.

Dashboard	> ^	The second	- 104/4 10.04	4 2 5 7 0	44 40 45 47		
🔆 Security Fabric	>	FortiGat	е имо4-ким				
FortiView	>		11				
+ Network	~			2 4 6 8 40	12 14 16 18		
Interfaces	☆	+ Create Ne	w 🕶 🖋 Edit	🗊 Delete			By Type By Rr
DNS		T Status	Name	T Members	T IP/Netmask	▼ Туре	T Access
Packet Capture		Physical (7)					
SD-WAN		0	port1		172.18.142.93 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Acco
SD-WAN Rules		O	port2		0.0.0.0 0.0.0.0	Physical Interface	PING
Performance SLA	6	3 O	port3		0.0.0.0 0.0.0.0	Physical Interface	
Ctatia Davitas		0	port4		0.0.0.0 0.0.0.0	Physical Interface	
Static Routes		0	port5		0.0.0.0 0.0.0.0	Physical Interface	
Policy Routes		0	port6		0.0.0.0 0.0.0.0	Physical Interface	
PID							

Figura 129. Port2 Fortigate Sucursal 2 Fuente: Los autores

FortiGate VM64-KVM	Fort	iGate-VM64-KVM					>_	11	?∙	∆ 1	👤 admin •
Dashboard >	> ^	Edit Interface									
 ☆ Security Fabric ➢ FortiView ➢ FortiView ➢ Network ✓ Interfaces △ DNS Packet Capture SD-WAN SD-WAN Rules 	> > 	Interface Name Alias Link Status Type Estimated Bandwidth 3 Tags Role 3 WAN	port2 (0C:DB:C3:CA:O SD-WAN Up Physical Interface 0	CB:01)	0	kbps Downstream					Â
Performance SLA		Ac	ld Tag Category								- 1
Static Routes Policy Routes		Address									_
RIP OSPF BGP		Addressing mode Manu IP/Network Mask 10.10	al DHCP .10.1/255.255.255.252	2							
Multicast		Administrative Access									
System > Policy & Objects >	> >	IPv4	TPS ☑ PING I □ SNMP DIUS Accounting	FMG-A FTM FTM FortiTele	ccess CAPWAP						
Security Profiles	> 、 ~	Receive LLDP 1 Use V	DOM Setting Enable	Disable	ОК С	ancel					v

29. Configuracion del port2 para la red SD-WAN del fortigate sucursal 1.

Figura130.Configuración del port2 sucursal 1 Fuente: Los autores

30. Configurar interface VLAN 20 en el fortigate sucursal 1.

Dashboard	> ^	New	
🔆 Security Fabric	>		
📥 FortiView	>	Interface Name VLAN 20	
+ Network	~	Alias DATOS	
Interfaces	☆	Type VLAN 👻	
DNS		Interface port3	
Packet Capture		VLAN ID 20	
SD-WAN		Tags	
SD-WAN Rules		Role 1 IAN	
Performance SLA		Add Tag Category	
Static Routes			
Policy Routes		Address	
RIP		Addressing mode Manual DHCP	
OSPF		IP/Network Mask 192.168.1.1/24	
BGP		Create address object matching subnet 🜑	
Multicast		Name 🔲 VLAN 2 address	
System	>	Definition 192.168.1.0/24	
📕 Policy & Objects	>		
-		Administrative Access	Activar

Figura131.Interfaz Vlan Sucursal 1 Fuente: Los autores 31. Activar DHCP Server para la interfaz VLAN 20.

• • • • • • • • • •	Edit Interface
Interfaces ☆	Name 🔤 VLAN DATOS address
DNS	Definition 192.168.1.0/24
Packet Capture	
SD-WAN	Administrative Access
SD-WAN Rules	IPv4 🗹 HTTPS 🗹 PING 🗌 FMG-Access 🗌 CAPWAP
Performance SLA	SSH SNMP FTM
Static Routes	
Policy Routes	C DHCP Server
RIP	Address Range
OSPF	A Curte New A Cutte Charles
BGP	
Multicast	Starting IP End IP
A System	192.168.1.2 192.168.1.254
System /	Netmask 255.255.255.0
Policy & Objects >	Default Gateway Same as Interface IP Specify
▲ Security Profiles >	DNS Server Same as System DNS Same as Interface IP Specify
□ VPN >	Advanced
Loser & Device >	

Figura132. DHCP VLAN Sucursal 1 Fuente: Los autores

32. Configuracion de la SD-WAN, le damos enable para activar la interfaz.

FortiGate VM64-KVM	For	tiGate-VM64-KVM	>_	53	 ∆ 0	🕗 admin -
Dashboard	> ^	SD-WAN				
🔆 Security Fabric	>	North SD-WAN				^
🖿 FortiView	>					
+ Network	~					
Interfaces						
DNS		SD-WAN Interface Members				
Packet Capture	_	Interface 🛛 🖬 SD-WAN (port2) 🗸 🗶				
SD-WAN	☆	Gateway 10.10.10.2				
SD-WAN Rules		Cost 0				
Performance SLA		Status O Enable O Disable				
Static Routes		0				
Policy Routes						
RIP		SD-WAN Usage				
OSPF		Bandwidth Volume Sessions				
BGP		Unstream Downstream				
Multicast						
System	>	port2 🔮				
Policy & Objects	>					
Security Profiles	>					~
Q	、 *	Appiy				

Figura133.SD-WAN Sucursal 1 Fuente: Los autores 33. Configurar static routes para salida a internet del enlace SD-WAN.

FortiGate VM64-KVM	Fort	iGate-VM64-KVM				>_	0	 ∆ 1	👤 admin 🕶
Dashboard	> ^	Edit Static Route							
🔆 Security Fabric	>								
🖿 FortiView	>	Destination 🕖	Subnet Internet Service						
+ Network	~		0.0.0/0.0.0.0						
Interfaces		Interface	SD-WAN	•					
DNS		Administrative Distance 🛈	1	Interface	SD-WAN				
Packet Canture		Comments	Write a comment:: 0	Link	0				
CD WALL		Status	Enabled Obsabled	Туре	SD-WAN Interface				
SD-WAN				Role	WAN				
SD-WAN Rules				Members	SD-WAN (port2)				
Performance SLA				Load Balancing Algorithm	Source IP				
Static Routes	☆								
Policy Routes									

Figura 134. Configuracion Static Routes Sucursal 1 Fuente: Los autores

34. Configurar IPv4 policy donde direccionaremos la salida a internet por el enlace SD-WAN a nuestra red local.

FortiGate VM64-KV	M <u>Fo</u>	rtiGate-VM	164-KVM							≻ [] @)• Д0	👤 admin 🕶
Dashboard	> '	+ Cre	ate New 🥖	'Edit 📋 De	elete Q Policy Lo	okup Search				Q Interface	Pair View	By Sequence
🔆 Security Fabric	>	ID	Namo	Source	Destination	Schodulo	Sorvico	Action	NAT	Security Profiles	Log	Putton
E FortiView	>		INdiffe	Jource	Destination	Schedule	Jervice	Action	INAI	Security Profiles	LUg	Dytes
🕂 Network	>	🕒 Impl	licit 1									
System	>											
📕 Policy & Objects	~											
IPv4 Policy	☆											
Authentication Rules												
IPv4 DoS Policy												
Addresses												
Wildcard FQDN Addresses												

Figura135.Interfaz IPv4 Policy Sucursal 1 Fuente: Los autores 35. Configuración de la regla para internet.

FortiGate VM64-KVN	Fort	iGate-VM64-KVM				
Dashboard	> ^	Edit Policy				
🔆 Security Fabric	>					
EortiView	>	Name 🚯	INTERNET			
Network	>	Incoming Interface	o DATOS (VLAN 2	20) -	•	
System	>	Outgoing Interface	🚳 SD-WAN	•	·	
Policy & Objects	~	Source	🔳 all	3	:	
IPv4 Policy	☆			+		
Authentication Rules		Destination	≣ all	* *		
IPv4 DoS Policy		Schedule	always		•	
Addresses		Service	ALL	×		
Wildcard FQDN Addresses		Action		+ DENY		
Internet Service Database Services		Inspection Mode	Flow-based Proxy-l	based		
Schedules		Firewall (Network C	Intions			
Virtual IPs		Firewait/ Network O	ptions			
IP Pools		NAT	•			
Protocol Options		IP Pool Configuration	Use Outgoing	Interface Address	Use Dynamic IP Pool	
Traffic Shapers		Preserve Source Por				
Traffic Shaping Policy	~	Protocol Options	PRX default		▼ Ø ²	
Q					OK	Cancel

Figura136.Configuracíon IPv4 Policy Sucursal 1 Fuente: Los autores

36. Realizar un ping a la siguiente dirección 8.8.8.8 para verificar la salida de internet del fortigate Sucursal 1.



Figura137.Ping Google Fortigate Sucursal 1 Fuente: Los autores 37. Configurar switch con la VLAN 20 para nuestra red local.



Figura 138. Configuración VLAN 20 Fuente: Los autores

38. Configurar el puerto troncal del switch.



Figura139. Puerto Trunk switch Sucursal 1 Fuente: Los autores 39. Asignar la VLAN 20 a los puertos que vamos usar.



Figura 140. Puerto Access VLAN 20 Fuente: Los autores

40. Para asignación de IP de manera automática tecleamos en el CLI la palabra dhcp, show para que nos muestre que IP nos entrega y realizamos un ping a google.

:	• PC1	×				-	×
PC1> 0 DORA 1	dhcp IP 192.168.1.2/24 GW	192.168.1.1					^
PC1> :	show						
NAME PC1	IP/MASK 192.168.1.2/24 fe80::250:79ff:fe60	GATEWAY 192.168.1.1 5:6800/64	MAC 00:50:79:66:68:00	LPORT 20102	RHOST:PORT 127.0.0.1:20103		
PC1> 84 by ⁻ 84 by ⁻ 84 by ⁻ 84 by ⁻ 84 by ⁻	ping 8.8.8.8 tes from 8.8.8.8 icmp tes from 8.8.8.8 icmp tes from 8.8.8.8 icmp tes from 8.8.8.8 icmp tes from 8.8.8.8 icmp	<pre>b_seq=1 ttl=114 tin b_seq=2 ttl=114 tin b_seq=3 ttl=114 tin b_seq=4 ttl=114 tin b_seq=5 ttl=114 tin b_seq=5 ttl=114 tin</pre>	ne=63.294 ms ne=69.327 ms ne=66.905 ms ne=68.054 ms ne=64.920 ms				
PC1>	•						

Figura 141. Verificacion de red local y navegación Sucursal 1 Fuente: Los autores

RECURSOS UTILIZADOS

- > COMPUTADORA
- CABLE DE RED (PATCHCORD)
- ➢ GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente

4.1.3. PRÁCTICA 3

Configuración de una red SD-WAN con perfomance SLA en fortigate 6.4.2.

DATOS INFORMATIVOS

- > MATERIA: Redes de comunicación
- > PRÁCTICA Nº 3
- > NUMERO DE COMPUTADORAS: 10
- > TIEMPO CONSIDERADO: 2 Horas

DATOS DE LA PRÁTICA

TEMA: Configuración de una red SD-WAN para el equilibrio de carga

con SLA.

OBJETIVOS

General

Configurar equilibrio de carga con SLA.

Específicos

- ➢ Configruar la red SD-WAN.
- Configurar preformance SLA.
- > Seleccionar la conexiones que tenga menos ping o jitter.

GLOSARIO

PING.- Ping es un instrucción o una herramienta de diagnóstico que consiente realizar una verificación del estado de una determinada conexión o host local.

JITTER.- Jitter es la diferencia de velocidad entre los paquetes más lentos y más rápidos. Esencialmente, es una variación en el retraso. En aplicaciones que son sensibles a los paquetes retrasados, como la transmisión, VoIP o juegos, esto podría afectar negativamente la experiencia del usuario si es demasiado alta.

LACTENCIA.- Es cuando en una red se presenta retardo dentro del tiempo estimado de trasmisión.

PACKET LOSS.- Es cuando en una red se en envían o reciben paquetes de datos y este no llegan a su destino.

SLA.- Se define como un conjunto de condicionamiento que se utiliza para especificar el nivel de servicio que un cliente podría esperar de su proveedor de servicio.

HTTPS.- Es un protocolo que se lo utiliza para la transferecia de datos entre el host y un sevidor utilizando un cifrado ssl para una conexión segura.

DNS.- (acrónimo de Domain Name System) Es un protocolo el cual relaciona el nombre de dominio de una pagina web con su dirección ip publica.

MARCO PROCEDIMENTAL



1. Diseñar la topología de la red para la práctica 3.

Figura 142. Diseño de la red práctica Nº3 Fuente: Los autores

2. Configurar la dirección IP en puerto 2 en el fortigate principal para el enlace WAN para el fortigate sucursal 1.

FortiGate VM64-KVN	PRIN	ICIPAL					Q• >_ [] @•	۵۵
Dashboard	> ^	Edit Interface						
Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules	→	Name Alias Type VRF ID 1 Role 1 Estimated bandwidth 1	WAN-SUCURSAL WAN-SUCURSAL Physical Interfac 0 WAN 0 -	AL 1 (port2) 1 ce	kbps Upstream		FortiGate FRINCIPAL Status Up MAC address Oc:d3:9a:d0:eb:01	
Performance SLA Static Routes Policy Routes RIP		Address Addressing mode IP/Netmask	0 Manual DHCP 10.10.10.1/255.22	Auto-managed by For 55.255.252	kbps Downstream	n	Speed Test Execute speed test C Documentation C Documentation	
OSPF BGP Multicast		Secondary IP address	•				Video Tutorials	
 System Policy & Objects Security Profiles VPN User & Authentication 	> > > >	IPv4 F	HTTPS SSH RADIUS Accounting e VDOM Setting En	PING SNMP Security Fabric Connection Disable	CK	Cancel		

Figura 143.Configuracion IP fortigate principal port2 Fuente: Los autores

3. Configurar la dirección IP en puerto 3 en el fortigate principal para el enlace wan para el fortigate sucursal 1.

FortiGate VM64-KVN	1 PRI	NCIPAL				Q • >_ [] @• 41
Dashboard	> ^	Edit Interface				
Security Fabric Network Interfaces DNS	> ~ ☆	Name Alias Type	WAN-SUCURSAL 1	1-1 (port3) -1		FortiGate
Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA		Role 1 Estimated bandwidth 1	0 WAN 0 0	•	kbps Upstream kbps Downstream	MAC address Oc:d3:9a:d0:eb:02 Speed Test
Static Routes Policy Routes RIP		Address Addressing mode	Manual DHCP /	Auto-managed by For	tiIPAM	Execute speed test Documentation
OSPF BGP Multicast		Secondary IP address				 Online Help C[*] Video Tutorials C[*]
 System Policy & Objects Security Profiles VPN 	> > > >	IPv4 H SS Receive LLDP 1 Use	TTPS 5H ADIUS Accounting VDOM Setting	 PING SNMP Security Fabric Connection 1 Disable 	FMG-Access FTM	
User & Authentication	> _				OK Cancel	

Figura 144.Configuracion IP fortigate principal port3 Fuente: Los autores 4. Configurar la dirección ip en el puerto 4 en el fortigate principal para el enlace wan para el fortigate sucursal 2.

FortiGate VM64-KVN	A PRI	NCIPAL				٩٠ ≻ [] @• 4
🚯 Dashboard	> ^	Edit Interface				
Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA	> ☆	Name Alias Type VRF ID 1 Role 1 Estimated bandwidth 1	port4 WAN-SUCURSAL 1 Physical Interface 0 WAN 0 0 0 0	2	kbps Upstream kbps Downstream	FortiGate PRINCIPAL Status Up MAC address Octd3:9ard0:eb:03 Speed Test
Static Routes Policy Routes RIP		Address Addressing mode IP/Netmask	Manual DHCP / 40.40.40.1/30	Auto-managed by Fo	tiipam	Execute speed test
OSPF BGP Multicast		Secondary IP address	•			Video Tutorials
 System Policy & Objects Security Profiles VPN 	> > >	IPv4 H S Receive LLDP () Use	HTTPS ISH RADIUS Accounting e VDOM Setting	PING SNMP Scurity Fabric Connection	FMG-Access FTM	
User & Authentication	>				OK Cancel	

Figura 145.Configuracion IP fortigate principal port4 Fuente: Los autores

5. Configurar la dirección IP en el puerto 5 en el fortigate principal para el enlace WAN para el fortigate sucursal 2.

FortiGate VM64-KV	PRIN	ICIPAL				Q • >_ [] @• 4 0
Dashboard	> ^	Edit Interface				
 Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Destrumence SI A 	> 	Name Alias Type VRF ID 9 Role 9 Estimated bandwidth 9	WAN-SUCURSAL Physical Interfac WAN O O O	AL1.3 (port5) 1.3 .e kb kb kb	ps Upstream ps Downstream	FortiGate PRINCIPAL Status Up MAC address Oc:d3:9a:d0:eb:04 Speed Test
Static Routes Policy Routes RIP		Address Addressing mode IP/Netmask	Manual DHCP 30.30.30.1/255.25	Auto-managed by FortilF 55.255.252	АМ	Execute speed test O Documentation
OSPF BGP Multicast		Secondary IP address	•			Video Tutorials
 System Policy & Objects Security Profiles VPN 	> > >	IPv4	HTTPS SSH RADIUS Accounting se VDOM Setting En	 PING SNMP Security Fabric Connection (1) able 	FMG-Access FTM	
User & Authentication	> _			C	Cancel	

Figura 146.Configuracion IP fortigate principal port5 Fuente: Los autores

6. Crear una zona de interfaces para añadir una sola regla en el policy IPv4 en el fortigate principal.

FortiGate VM64-	KVM <u>PR</u>	INCIPAL					Q•≻_[] @•	r 🗘 🚺 🕗 admin 🕶
 Dashboard Security Fabric 	> ^ >	E FortiGate VN	164-KVM 1 3	5 7 9 11 13 15 17 19 2	1 23			
Network Interfaces	~ ☆		m m [2 4	6 8 10 12 14 16 18 20 2	2 24			
DNS		+ Create New •	🖋 Edit 🗎 🖻 D	Delete Search			Q	📓 Group By Type 🔻
Packet Capture SD-WAN Zones		Interface Zone	ie 🗢	Туре 🗢	Members 🗢	IP/Netmask 🗘	Administrative Access 🗢	DHCP Clients 🗢
SD-WAN Rules		Virtual Wire Pair	egate 1					
Performance SLA	_	FortiExtender		802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection	

Figura 147. Crear zonas de interfaces Fuente: Los autores

7. Damos nombre a la zone y arrastar las interfaces a que van unir en la interface para el fortigate surcusal 1.

FortiGate VM64-K	/M PR	INCIPAL				Q • >	- 13	?• ₽0
Dashboard	> '	Edit Zone						
Security Fabric Vetwork Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA	> ☆	Name Block intra-zone traffic C Interface members Comments	ZONAS WAN WAN-SUCURSAL 1 (port2) WAN-SUCURSAL 1-1 (port3) + 0/12]	For	rtiGate PRINCIPAL Documentation Online Help C Video Tutorials C		
Static Routes Policy Routes RIP OSPF BGP Multicast								
System	>			ОК	Cancel			

Figura 148. Interface members fortigate principal Fuente: Los autores 8. Damos nombre a la zone y arrastar las interfaces a que van unir en una la interface para el fortigate sucursal 2.

FortiGate VM64-KVM	M PR	INCIPAL			Q.+	× (1	?∙	41	👤 admin •
Dashboard	> ^	Edit Zone							
 Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA Static Routes Policy Routes RIP OSPF BGP Her to be 	>	Name Block intra-zone traffic C Interface members Comments	ZONA WAN 2 WAN-SUCURSAL 1.2 (port4) * WAN-SUCURSAL 1.3 (port5) * + 0/127	FortiGate PRINCIPAL Documentatio Online Help Video Tutoria	n C ^a als C ^a				
System	>		OK Canc	el					



9. Configurar static routes para el fortigate principal, le damos click en la opción dynamic y obtendrá el Gateway del router principal.

FortiGate VM64-KVM	PRI	NCIPAL		Q	>	11	?∙	40	👤 admin 🕶
Dashboard	> ^	New Static Route							
Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Pacfarements CLA	> *	Dynamic Gateway ① ① Destination ① Gateway Address ① Interface Administrative Distance ① Comments	Subnet Internet Service 0.0.0/0.0.00 Dynamic Dynamic Specify 172:18:142:100 Im Im 10 Im Write a comment Im Im Im						
Static Routes	☆	Status	C Enabled O Disabled						
Policy Routes		Advanced Options							
RIP OSPF			OK Cancel						

Figura 150. Static routes fortigate principal Fuente: Los autores 10. Configurar la regla que nos permitirá la salida a internet al enlace SD-WAN del fortigate sucursal 1.

FortiGate VM64-KVM	PRIN	NCIPAL						Q	>	11	? •	40
Dashboard	> ^	Edit Policy										
🔆 Security Fabric	>					ID						
Network	>	Name 🚯	INTERNET SD-WAN SUCUR	RSAL 1		1						
System	>	Incoming Interface	ZONAS WAN	•		Last u	sed					
📕 Policy & Objects	~	Outgoing Interface	im port1	•		N/A						
Firewall Policy	☆	Source	🔳 all	×		Firstu	ised					
IPv4 DoS Policy			+			IN/A						
Addresses		Destination	ill +	×		Hit co	unt					
Internet Service		Schedule	lo always	-		A atta						
Database		Service	ALL .	×		0	sessions					
Services			+									
Schedules		Action	✓ ACCEPT Ø DENY			0 second(s) ago	n	ow.			
Virtual IPs						Total	ovtes					
IP Pools		Inspection Mode	Flow-based Proxy-based			OB						
Protocol Options						Curre	nt bandwidth					
Traffic Shapers		Firewall / Network O	ptions			0 B/s						
Traffic Shaping Policy		NAT										
Traffic Shaping Profile		IP Pool Configuration	Use Outgoing Interface	Address Us	e Dynamic IP Pool							
Security Profiles	>	Preserve Source Port				(? D	ocumentation					
	,	Protocol Options	PROT default		▼ #			×				
Liser & Authentication	, v				ОК	Cancel						
	F	-ioura 151	Reala de inte	rnet na	ara el fort	inate su	rursal	1				

Figura 151. Regla de internet para el fortigate sucursal 1 Fuente: Los autores

11. Configurar la regla que nos permitirá la salida a internet al enlace SD-WAN del fortigate sucursal 2.

FortiGate VM64-KVM	PRIN	ICIPAL				Q• >_ [] @• A	1
Dashboard	> ^	Edit Policy					
🔆 Security Fabric	>				ID		
+ Network	>	Name 🚯	INTERNET SD-WAN SUCURSAL 2		2		
System	>	Incoming Interface	C ZONA WAN 2	•	Last used		
Policy & Objects	~	Outgoing Interface	m port1	-	N/A		
Firewall Policy	☆	Source	🔳 all	×	First used		
IPv4 DoS Policy			+		IN/A		
Addresses		Destination	;⊒ all +	*	Hit count O		
Internet Service Database		Schedule	G always	•	Active sessions		
Services		Service	ALL +	×	0		
Schedules		Action	✓ ACCEPT Ø DENY		0 second(s) ago	now	
Virtual IPs					Total bytes		
IP Pools		Inspection Mode	Flow-based Proxy-based		OB		
Protocol Options					Current bandwidth		
Traffic Shapers		Firewall / Network O	ptions		0 B/s		
Traffic Shaping Policy		NAT	•	_			
Traffic Shaping Profile		IP Pool Configuration	Use Outgoing Interface Address	Use Dynamic IP Pool			
Security Profiles	>	Preserve Source Port			⑦ Documentation		
	>	Protocol Options	PROT default	✓ d ²	R Astronom C	R.	
LISER & Authentication	> v			OK	Cancel		



12. Configurar la dirección IP al port2 del fortigate de la sucursal 1.

FortiGate VM64-KVN	I SUC	URSAL-1				Q•>_ [] @• 4(
Dashboard	> ^	Edit Interface				
 Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules 	> ~ ☆	Name Alias Type VRF ID 1 Role 1 Estimated bandwidth	 ENLACE WAN 1 ENLACE WAN 1 Physical Interface 0 WAN 0 0 	(port2)	ps Upstream ps Downstream	FortiGate Status Up MAC address Oc:d3:9a:95:d9:01 Second Lett
Performance SLA Static Routes Policy Routes		Address Addressing mode	Manual DHCP	Auto-managed by FortilF	AM	Execute speed test
OSPF BGP		Secondary IP address	s 🕥	5.233.232		 Online Help C Video Tutorials C
Multicast		Administrative Acces	SS			
 System Policy & Objects Security Profiles VPN 	> > >	IPv4 Receive LLDP	HTTPS SSH RADIUS Accounting Use VDOM Setting Ena	 PING SNMP Security Fabric Connection 1 Disable 	☐ FMG-Access ☐ FTM	
User & Authentication	> 、			C	Cancel	



13. Configurar la dirección IP al port3 del fortigate de la sucursal 1.

FortiGate VM64-KV	M <u>s</u> i	JCURSAL-1				Q - >_ [] Ø:
Dashboard	>	Edit Interface				
Security Fabric	>	Name	ENLACE WAN	2 (port3)		FortiGate
Interfaces	☆	Alias	ENLACE WAN 2	re		SUCURSAL-1
DNS		VRFID 1	0			Status O Up
Packet Capture		Role 1	WAN	•		MAG adda
SD-WAN Zones		Estimated bandwid	lth 🚯 🛛 0		kbps Upstream	Oc:d3:9a:95:d9:02
SD-WAN Rules			0	÷	kbps Downstream	Spood Test
Performance SLA						Speed lest
Static Routes		Address				Execute speed test
Policy Routes		Addressing mode	Manual DHCP	Auto-managed by For	tiIPAM	
RIP		IP/Netmask	20.20.20.2/255.2	55.255.252		Documentation
OSPF		Secondary IP addre	ess 🔘			Video Tutorials
BGP						
Multicast		Administrative Acc	ess			
System	>	IPv4		PING	FMG-Access	
Policy & Objects	>		□ SSH	SNMP	L) FTM	
Security Profiles	>		RADIUS Accounting	Connection ()		
□ VPN	>	Receive LLDP ()	Use VDOM Setting En	able Disable		
User & Authentication	>	~			OK Cancel	
		Eiguro 15	1 Diroopión	ID nort2 fo	rtigata avauraal	1

Figura 154. Dirección IP port3 fortigate sucursal 1 Fuente: Los autores

14. Configurar la interface port4 para la red local con su DHCP del fortigate sucursal.

FortiGate VM64-KVM	SUC						
🚯 Dashboard	>	Edit Interface					
🔆 Security Fabric	>		port4			FortiGate	
+ Network	~	Name 💻	port4			SUCURSAL-1	
Interfaces	☆	Alias L	AN-SUCURSAL 1				
DNS		Type 📖	Physical Interface			Status	
Packet Capture			,			O Up	
SD-WAN Zones		Role 😈	LAN	•		MAC address	
SD-WAN Rules		Address				0c:d3:9a:95:d9:03	
Performance SLA		Addressing mod	le	Manual DHCP Auto	managed by EastilBAM One-Arm Sniffer	 Documentation 	
Static Routes		ID/Netmock	ic .	192 168 0 1/24	Che-Alli Shine		
Policy Routes		Create address (object matching subnet	172.100.0.1724		Video Tutorials 🕼	
PIP		Secondary IP ad	dress				
OSPE		Secondary in da					
BGP		Administrative A	Access				
Multicast		IPv4	HTTPS	PING	FMG-Access		
System	>		SSH	SNMP	□ FTM		
Policy & Objects	>		RADIUS Accountin	Connection			
Security Profiles	>	Receive LLDP	Use VDOM Setting	Enable Disable			
I VPN	>	Transmit LLDP	Use VDOM Setting	Enable Disable			
User & Authentication	>	DUCD C	-				
Log & Report	>	DHCP Serve	er				
		Address range	192.168.0.2-192.168.	0.254			
			0				
		Netmask	255.255.255.0				
					OK Ca	ancel	



15. Crear SD-WAN Member en la sucursal 1.

FortiGate VM64-KV	/M <u>SU(</u>	CURSAL-1			Q • >_ []	() • 🗘 🛛 🕗 admin •
Security Fabric	> ^	Bandwidth Volume Sessions				
+ Network	~	Dow	nload port2		Upload	port2
DNS						
Packet Capture	_					
SD-WAN Zones SD-WAN Rules	☆					
Performance SLA						
Static Routes		+ Create New - Sedit 📋 Delet	te			
Policy Routes		SD-WAN Member	Gateway ≜	Cost ≜	Download ≜	Lipload ≜
RIP		SD-WAN Zone	Gateway 🗸	COSt	Downidad	opioid •

Figura 156. SD-WAN zone fortigate sucursal 1 Fuente: Los autores 16. Crear SD-WAN para la interface enlace WAN 1.

🔆 Security Fabric	> ^	Edit SD-WAN Me	mber			
 Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA Static Routes Policy Routes RIP OSPF BGP Multicast 	\$	Interface SD-WAN Zone Gateway Cost Status	 ENLACE WAN 1 (port2) virtual-wan-link 10.10.10.1 0 Enabled Disabled 			(
System	>					
 System Policy & Objects 	>	Figura 157 Fue	. SD-WAN enlace wan 1 ente: Los autores	ОК	Cancel	

17. Crear SD-WAN para la interface enlace WAN 2.

FortiGate VM64-K	VM <u>SUC</u>	URSAL-1			
	> ^	New SD-WAN Me	ember		
Network Interfaces DNS Packet Capture	~	Interface SD-WAN Zone Gateway	ENLACE WAN 2 (port3)		¢
SD-WAN Zones SD-WAN Rules Performance SLA Static Routes	☆	Status	Enabled Disabled		¢
RIP OSPF BGP Multicast					
SystemPolicy & Objects	>			ОК	Cancel



18. Configurar static routes para la SD-WAN.

FortiGate VM64-	KVM <u>SU</u>	CURSAL-1						Q -		 40	👤 admin 🕶
Dashboard	> ^	New Static Route									
🔆 Security Fabric	>										
Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Performance SI A	~	Destination	Subnet Internet Service 0.0.0/0.0.0.0 SD-WAN Write a comment O Enabled O Disabled	: 0/2	Interface Type •	e 🗟 SD-WAI SD-WAN Ini	N terface				
Static Routes	☆				OK	(Cancel				
Policy Routes											

Figura 159. Static routes para SD-WAN fortigate sucursal 1 Fuente: Los autores

19. Configurar la regla de salida a internet que permite a la SD-WAN dar acceso a internet a la red local del fortigate sucursal 1.

FortiGate VM64-KVI	M <u>s</u> l	JCURSAL-1				Q•≻ [] @• 4 8
Dashboard	>	New Policy				
🔆 Security Fabric	>				⑦ Documer	itation
Network	>	Name 🚯	INTERNET		Online	Help 🗷
System	>	Incoming Interface	LAN-SUCURSAL 1 (port4)	•	Video T	utorials 🗹
Policy & Objects	~	Outgoing Interface	🝘 virtual-wan-link	•		
Firewall Policy	☆	Source	🗐 all	×		
IPv4 DoS Policy			+			
Addresses		Destination	i⊒ all +	×		
Internet Service Database		Schedule	Co always	~		
Services		Service	ALL +	×		
Schedules		Action	✓ ACCEPT Ø DENY			
Virtual IPs						
IP Pools		Inspection Mode	Flow-based Proxy-based			
Protocol Options						
Traffic Shapers		Firewall / Network C	Options			
Traffic Shaping Policy		NAT	•			
Traffic Shaping Profile		IP Pool Configuratio	N Use Outgoing Interface Add	ress Use Dynamic IP Pool		
Security Profiles	>	Preserve Source Por	t 🛈			
I VPN	>	Protocol Options	PROT default	- <i>i</i>		
Liser & Authentication	, ·			OK	Cancel	

Figura 160. Static routes para SD-WAN fortigate sucursal 1 Fuente: Los autores

20. Configurar perfomance SLA SD-WAN para balancear la conexión que tenga menos ping o latencia donde fortigate eligira cual será el mejor vinculo que tenga mejor calidad de servicio dames click en créate new.

FortiGate VM64-KV	M <u>S</u> Ų	CURSAL-1					Q • >_	0		∆ 0	👤 admi
Dashboard	> ^	Packet Loss Latency	litter								
🔆 Security Fabric	>										
+ Network	~										
Interfaces											
DNS					No data						
Packet Capture											
SD-WAN Zones											
SD-WAN Rules											
Performance SLA	☆										
Static Routes		+ Create New	dit 🗇 Delete Search				Q				
Policy Routes		Name ≑	Detect Server ≑	Packet Loss	Latency	Jitter	Failure Threshold ≑		Recov	ery Thr	eshold 🌲
RIP		Default_AWS	http://aws.amazon.com/				5	1	.0		
OSPF		Default_DNS	208.91.112.53				5	1	.0		
BGP			208.91.112.52								
Multicast			(System DNS)								
System	>	Default_FortiGuard	http://fortiguard.com/				5	1	.0		
Policy & Objects	>	Default_Gmail	gmail.com				5	1	.0		
Security Profiles	>	Default_Google Search	http://www.google.com/				5	1	.0		
I VPN	>	Default_Office_365	http://www.office.com/				5	1	.0		
User & Authentication	>										

Figura 161. Configuración de static routes SD-WAN del fortigate Fuente: Los autores

21. Realizar un SLA a travez de ping a google salga a travez de la SD-WAN.

FortiGate VM64-K	VM SUC	URSAL-1	Q • >_	- [] ⑦	- 40
Dashboard	> ^	Edit Performance SLA			
🔆 Security Fabric	>		SLA Details		
+ Network	~	Name GOOGLE		Packet Loss	Latency
Interfaces		Protocol Ping HTTP DNS	ENLACE WAN 1 (port2)	0.00%	63.36ms
DNS		Servers 8.8.8		0.00%	(0.40
Packet Capture		8.8.4.4	ENLACE WAN 2 (port3)	0.00%	02.43ms
SD-WAN Zones		Participants All SD-WAN Members Specify			
SD-WAN Rules		Enable probe packets			
Performance SLA	☆	SI & Target	Performance SLA Setup Gu	ides	
Static Routes		Service Servic	🗐 Link Monitoring 🖸		
Policy Routes		Link Status	SLA Targets I		
RIP		Check interval 500 ms	⑦ Documentation		
OSPE		Failures before inactive 1 5	Online Help II		
BGP		Restore link after (1) 4 check(s)	Video Tutorials		
Multicast					
System	>	Actions when Inactive			
Policy & Objects	>	Update static route 🚯 🜑			
Security Profiles	>				
U VPN	,	ОК	Cancel		

Figura 162. Configuración de static routes SD-WAN del fortigate Fuente: Los autores

22. Veremos que tenemos menos ping y jiptter en una de las interfaces configuradas donde sd-wan eligue en enlace con mejor calidad de servicios.



Figura 163. Diagrama de calidad de sevicio de sucrusal 1 Fuente: Los autores

23. Configurar la dirección IP en puerto 2 en el fortigate principal para el enlace WAN para el fortigate sucursal 2.

FortiGate VM64-KVM	SUCURSAL2				۹۰۰ 🌅 💽 عرف العام العام (عام العام العام العام العام العام العام العام العام (عام العام العام العام العام الع
Dashboard >	Edit Interface				
Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Derformance SLA	Name Alias Type VRF ID 3 Role 3 Estimated bandwidth	WAN SUC WAN SUC Physical 0 WAN 0 0	ICURSAL 2 (port2) URSAL 2 Interface	 kbps Upstream kbps Downstream 	FortiGate FortiGate-VM64-KVM Status Up MAC address Oc:d3:9a:31:99:01 Speed Test
Static Routes Policy Routes RIP OSPF BGP	Address Addressing mode IP/Netmask Secondary IP address	Manual (40.40.40.2	DHCP Auto-managed by /255.255.255.252	FortiIPAM	Execute speed test ⑦ Documentation ④ Online Help C ➡ Video Tutorials C
Multicast System Policy & Objects Security Profiles VPN VPN	Administrative Acces	IS HTTPS SSH RADIUS Accou Use VDOM Settin	PING SNMP Security Fabric Connection	FMG-Access	
User & Authentication >	-			OK Ca	ncel

Figura 164. Configuracion IP fortigate WAN sucrsal 2 Fuente: Los autores

24. Configurar la dirección IP en puerto 3 en el frotigate principal para el enlace wan para el fortigate sucursal 2.

FortiGate VM64-KV	M SUC	CURSAL2						Q •	>_ []	 ۵۵	🕗 admin 🖥
Dashboard	> ^	Edit Interface									
Security Fabric Avenue of the second secon	> ☆	Name Alias Type VRF ID 0 Role 0 Estimated bandwidth 0	WAN SUCURS Physical Inter O WAN O	RSAL 2 (port3) AL 2 rface	▼ kbps Upstream		FortiGate Status O Up MAC address 0::d3:9a:31:99:02				
SD-WAN Rules Performance SLA Static Routes Policy Routes		Address Addressing mode	0 Manual DHC	P Auto-managed by F	kbps Downstrea	am	Speed Test Execute speed test Documentation				
RIP OSPF BGP Multicast		IP/Netmask Secondary IP address C Administrative Access	30.30.30.2/25	5.255.255.252			 Online Help Q Video Tutorials 	3 5 C			
System System Policy & Objects Security Profiles VPN	> > >	IPv4	HTTPS SSH RADIUS Accountin se VDOM Setting	PING SNMP Security Fabric Connection 1 Enable Disable	FMG-Access FTM						
User & Authentication	> •				ОК	Cancel					

Figura 165. Configuracion IP fortigate WAN sucursal 2 Fuente: Los autores

25. Configurar la interface port4 para la red local con su DHCP del fortigate sucursal 2.

FortiGate VM64-KVM	sucu	IRSAL2					Q+≻ []	@- 4 0	👤 admin
🖚 Dashboard	>	Edit Interface							
🔆 Security Fabric	>	Name 🗮 po	ort4			FortiGate			
+ Network	~	Alias RED	D LOCAL SUCURSAL 2			G SUCURSAL2			
Interfaces	☆	Type 📓 Ph	hysical Interface						
DNS		VRFID 0				Status			
Packet Capture		Role 🜖 LAN	4	•		O Up			
SD-WAN Zones		Address				MAC address			
SD-WAN Rules		Addressing mode	Ma	anual DHCR Auto-manag	red by FortilBAM One-Arm Sniffer	0c:d3:9a:31:99:03			
Performance SLA		IP/Netmask	10	2 168 0 1/24	Chevan Shire	⑦ Documentation			
Static Routes		Create address obje	ect matching subnet	2.100.0.1/24		🖉 Online Help 📝			
Policy Routes		Secondary IP addre	ess O			Video Tutorials 🗹			
RIP									
OSPF		Administrative Acce	iess						
BGP		IPv4		PING	FMG-Access				
Multicast			SSH SSH	SNMP	□ FTM				
System	>		RADIUS Accounting	Connection ()					
Policy & Objects	>	Receive LLDP 🚯	Use VDOM Setting Enabl	le Disable					
Security Profiles	>	Transmit LLDP 🚯	Use VDOM Setting Enab	Disable					
I VPN	>								
User & Authentication	>	DHCP Server							
📶 Log & Report	>	Address range	192.168.0.2-192.168.0.254						
		Netmask	255.255.255.0						
		Default gateway	Same as Interface IP Speci	ify					

Figura	166.	Configuración	red local	del fortigate
		Fuente: Los	autores	

26. Crear SD-WAN Member en la sucursal 2.

FortiGate VM64	-KVM SUCURSAL	2			Q • >	[] 🛛 🔹 🗘 🛛 admin 🕶
Dashboard	> Band	width Volume Sessions				
🔆 Security Fabric	>	Dow	vnload		Upload	
+ Network	~		port2			port2
Interfaces						
DNS						
Packet Capture						
SD-WAN Zones	☆					
SD-WAN Rules						
Performance SLA						
Static Routes	+ c	reate New 🔻 🖋 Edit 🗊 Dele	ete			
Policy Routes		Interfaces ≑	Gateway 🌲	Cost 🌩	Download 🗢	Upload 🗢
RIP	8	virtual-wan-link				
OSPF						

Figura 167.SD-WAN zone fortigate sucursal 2 Fuente: Los autores

27. Crear SD-WAN para la interface sucursal 2.

Network	~ ^	Edit SD-WAN Me	mber		
Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA Static Routes Policy Routes	\$	Interface SD-WAN Zone Gateway Cost Status	 WAN SUCURSAL 2 (port2) virtual-wan-link 40.40.40.1 0 Enabled O Disabled 	*	
RIP OSPF BGP Multicast					
System	>				
Policy & Objects	>			ОК	Cancel

Figura 168. SD-WAN sucursal 2 para puerto 2 Fuente: Los autores

28. Crear SD-WAN para la interface sucursal 2.

FortiGate VM64-	KVM SUC	CURSAL2				
+ Network	× ^	Edit SD-WAN Me	mber			
Interfaces DNS Packet Capture		Interface SD-WAN Zone	WAN SUCURSAL 2 (port3)	~		(
SD-WAN Zones SD-WAN Rules	☆	Cost	0			
Performance SLA Static Routes		Status	Enabled V Disabled			
Policy Routes						
OSPF BGP						
Multicast	>					
Policy & Objects	>				OK	Cancel

Figura 169. SD-WAN sucursal 2 para puerto 3 Fuente: Los autores

29. Configurar static routes para la SD-WAN sucursal 2.

FortiGate VM64-K	CVM <u>SU</u>	CURSAL2					Q - >.	. D	 ۵4	🕗 admin 🕶
Dashboard	> ^	New Static Route								
🔆 Security Fabric	>									
Network Interfaces DNS Packet Capture	~	Dynamic Gateway Destination Commente	ubnet Internet Service 0.0.0/0.0.0.0 SD-WAN							
SD-WAN Zones SD-WAN Rules Performance SLA		Status	Enabled O Disabled	/0/255						
Static Routes Policy Routes RIP	☆				ОК	Cancel				

Figura 170. Static routes para SD-WAN fortigate sucursal 2 Fuente: Los autores

30. Configurar la regla de salida a internet que permite a la SD-WAN dar acceso a internet a la red local del fortigate sucursal 2.

FortiGate VM64-KVM	1 <u>su</u>	ICURSAL2					Q • >_	0	⑦- ↓0	👤 admin
Dashboard	> '	New Policy								
🔆 Security Fabric	>				00	Documentation				
🕂 Network	>	Name 🚯	RED LOCAL SUCURSAL 2			Online Help 🖸				
System	>	Incoming Interface	RED LOCAL SUCURSAL 2 (port4)	•		Video Tutorials	C			
🖹 Policy & Objects	~	Outgoing Interface	virtual-wan-link	•						
Firewall Policy	☆	Source	🗉 all	×						
IPv4 DoS Policy			+							
Addresses		Destination	≣ all +	×						
Internet Service Database		Schedule	Co always	•						
Services		Service	ALL +	×						
Schedules		Action	✓ ACCEPT Ø DENY							
Virtual IPs										
IP Pools		Inspection Mode	Flow-based Proxy-based							
Protocol Options										
Traffic Shapers		Firewall / Network O	ptions							
Traffic Shaping Policy		NAT	•	_						
Traffic Shaping Profile		IP Pool Configuration	Use Outgoing Interface Address	Use Dynamic IP Pool						
Security Profiles	>	Preserve Source Port	t 🛈							
므 VPN	>	Protocol Options	PROT default	✓ di ¹						
▲ Liser & Authentication	, ,			OK	Cancel					



31. Configurar perfomance SLA SD-WAN para balancear la conexión que tenga menos ping o latencia donde fortigate eligira cual será el mejor vinculo que tenga mejor calidad de servicio dames click en créate new para sucursal 2.



Figura. 172 Gráficas la sucursal 2

Fuente: Los autores

RECURSOS UTILIZADOS

> COMPUTADORA

- CABLE DE RED (PATCHCORD)
- > GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente

4.1.4. PRÁCTICA 4

Configuración de una red SD-WAN con prioridad de servicios con sd-wan

rules.

DATOS INFORMATIVOS

- > **MATERIA:** Redes de comunicación
- > PRÁCTICA Nº 4
- > NUMERO DE COMPUTADORAS: 10
- > **TIEMPO ESTIMADO:** 2 Horas

DATOS DE LA PRÁTICA

TEMA: Configuración de una red SD-WAN con prioridad de servicios con sd-

wan rules.

OBJETIVOS

<u>General</u>

Configurar el balanceo de carga con SD-WAN rules

Específicos

- Configurar uan red SD-WAN.
- Establecer configuraciones de SD-WAN rules.
- > Calidad de servicios al enlace SD-WAN.

GLOSARIO

SD-WAN RULES.- Son reglas que se utilizan para examinar como se divide las sesiones a los miembros de SD-WAN

PING.- Ping es un comando o una herramienta de diagnóstico que permite hacer una verificación del estado de una determinada conexión o host local.

JITTER.- Jitter es la diferencia de velocidad entre los paquetes más lentos y más rápidos. Esencialmente, es una variación en el retraso. En

aplicaciones que son sensibles a los paquetes retrasados, como la transmisión, VoIP o juegos, esto podría afectar negativamente la experiencia del usuario si es demasiado alta.

LACTENCIA.- Es cuando en una red se presenta retardo dentro del tiempo estimado de trasmisión.

PACKET LOSS.- Es cuando en una red se en envían o reciben paquetes de datos y este no llegan a su destino.

MAXIMIZE BANDWIDTH (SLA).- El tráfico se distribuye entre todos los enlaces disponibles según el algoritmo de equilibrio de carga seleccionado.

LOWEST COST (SLA).- A las interfaces se les asigna una prioridad en función de la configuración de SLA seleccionada.

BEST QUALITY.- A la interfaz se le asigna una prioridad basada en el factor de costo de enlace de la interfaz

MARCO PRODECIMENTAL

1. Diseñar la topología de la red para la prática 4.



Figura 173. Diseño de la red práctica Nº4 Fuente: Los autores

2. Configurar la dirección IP en puerto 2 en el fortigate principal para el enlace WAN para el fortigate sucursal 1.

FortiGate VM64-KVM	PRIN	CIPAL					, ,	Q • →_ []	?• ↓1
Dashboard	> ^	Edit Interface							
🔆 Security Fabric	>	Name	WAN-SUCURS	AL 1 (port2)			Fort	Gate	
+ Network	~	Alles		4			G.	PRINCIPAL	
Interfaces	습	Allas	Physical Interfac	1					
DNS		Nor ID					State	us Jn	
Packet Capture		VRFID U	0					- F	
SD-WAN Zones		Role U	WAN	•			MAC	address	
SD-WAN Rules		Estimated bandwidth	0		kbps Upstrea	m	Oc:d	3:9a:d0:eb:01	
Performance SLA			0		kbps Downst	ream	Spee	d Test	
Static Routes		Address					Exe	ecute speed test	
Policy Routes		Addressing mode	Manual DHCP	Auto-managed by Fort	IPAM				
RIP		IP/Netmask	10.10.10.1/255.25	5.255.252			() [Documentation	
OSPF		Secondary IP address)					Online Help 🖸 Video Tutorials 📝	
BGP									
Multicast		Administrative Access							
System	>	IPv4	HTTPS	PING		FMG-Access			
Policy & Objects	>		SSH	SNMP		FTM			
Security Profiles	>		RADIUS Accounting	Connection ()					
L VPN	>	Receive LLDP ()	se VDOM Setting Ena	able Disable					
User & Authentication	> ्				OK	Cancel			

Figura 174.Configuracion IP fortigate principal port2 Fuente: Los autores

3. Configurar la dirección IP en puerto 3 en el fortigate principal para el enlace WAN para el fortigate sucursal 1.

FortiGate vivio4-KV		ICIFAL				Q: /_ [] (): (
2 Dashboard	> ^	Edit Interface				
🔆 Security Fabric	>	Name	WAN-SUCURSA	L 1-1 (port3)		FortiGate
Network	~	Alias		1 1		RINCIPAL
Interfaces	☆	Tuno	Physical Interfac	P		
DNS		VREID 6				Status O Up
Packet Capture		Pala C		_		
SD-WAN Zones		Fotierstad bandwidth	WAN	• 	- ! !	MAC address
SD-WAN Rules		Estimated bandwidth	0	KDp	s Opstream	01.03.78.00.65.02
Performance SLA			0	кор	s Downstream	Speed Test
Static Routes		Address				Execute speed test
Policy Routes		Addressing mode	Manual DHCP	Auto-managed by FortilPA	M	
RIP		IP/Netmask	20.20.20.1/255.25	5.255.252		O Documentation
OSPF		Secondary IP address)			Video Tutorials
BGP						
Multicast		Administrative Access				
System	>	IPv4	HTTPS	PING	FMG-Access	
Policy & Objects	>		SSH	SNMP	FTM	
Security Profiles	>		RADIUS Accounting	Connection ()		
I VPN	>	Receive LLDP () U	se VDOM Setting Ena	ble Disable		
User & Authentication	>			Ok	Cancel	

Figura 175.Configuracion IP fortigate principal port3 Fuente: Los autores

4. Configurar la dirección IP en el puerto 4 en el fortigate principal para el enlace WAN para el fortigate sucursal 2.

FortiGate VM64-KV		ICIPAL				Q• ≻ [] @• 4
Dashboard	> ^	Edit Interface				
Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Pulse	> ↓ ☆	Name Alias Type VRF ID 1 Role 1 Estimated bandwidd	port4 WAN-SUCURSA Physical Interf 0 WAN th O	L 1.2 ace	kbps Upstream	FortlGate Status Up MAC address Oc:d3:9a:d0:eb:03
SD-WAN Rules Performance SLA Static Routes Policy Routes RIP OSPF		Address Addressing mode IP/Netmask Secondary IP addre	0 Manual DHCP 40.40.40.1/30	Auto-managed by Forti	kbps Downstream	Speed Test Execute speed test ⑦ Documentation ● Online Help C³ ● Video Tutorials C³
BGP Multicast System Policy & Objects Security Profiles VPN	> > >	Administrative Acco	ess HTTPS SSH RADIUS Accounting Use VDOM Setting	PING SNMP Security Fabric Connection () nable Disable	FMG-Access	
User & Authentication	> 、				OK Cancel	

Figura 176.Configuracion IP fortigate principal port4 Fuente: Los autores

5. Configurar la dirección IP en el puerto 5 en el fortigate principal para el enlace WAN para el fortigate sucursal 2.

FortiGate VM64-KVM	PRIN	ICIPAL				Q•>_ [] @• 40
Dashboard	> ^	Edit Interface				
 Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules 	>☆	Name Alias Type VRF ID 1 Role 1 Estimated bandwidth	WAN-SUCURSAL WAN-SUCURSAL Physical Interfac 0 WAN 0 0	kl.1.3 (port5) 1.3 e k kl kl kl	ops Upstream bps Downstream	FortiGate PRINCIPAL Status Up MAC address Oc:d3:9a:d0:eb:04 Sneed Tect
Performance SLA Static Routes Policy Routes RIP OSPF		Address Addressing mode IP/Netmask Secondary IP address	Manual DHCP 30.30.30.1/255.25	Auto-managed by Fortill 5.255.252	РАМ	Execute speed test Execute speed test Documentation Online Help Video Tutorials
BGP Multicast System Policy & Objects Security Profiles VPN	> > >	Administrative Access IPv4 Receive LLDP) HTTPS) SSH) RADIUS Accounting Jse VDOM Setting Eng	 PING SNMP Security Fabric Connection ⁽¹⁾ bible Disable 	FMG-Access FTM	
User & Authentication	> _			(OK Cancel	

Figura 177.Configuracion IP fortigate principal port5 Fuente: Los autores

6. Crear una zona de interfaces para añadir una sola regla en el policy IPv4 en el fortigate principal.

FortiGate VM64-	KVM <u>Pri</u>	NCIPAL						Q• >_ [] @•	🗘 🚺 👤 admin •
 ⚠ Dashboard ※ Security Fabric ♣ Network 	> ^ > ~	E FortiGate VN	164-KVM 1 3 5	7 9 11 13 15 17 19	21 23				
Interfaces	☆		Z 4 0	0 10 12 14 10 10 20	22 24				
DNS		+ Create New ▼	🖋 Edit 📋 De	elete Search			Q		📓 Group By Type 🔻
Packet Capture		Interface	ie 🕈	Туре ≑	Members ≑	IP/Netmask ≑		Administrative Access 🖨	DHCP Clients ≑
SD-WAN Zones		Zone Virtual Wire Pair	regate 1						
Performance SLA		FortiExtender		802.3ad Aggregat	е	Dedicated to FortiSwitch	1	PING Security Fabric Connection	

Figura 178. Crear zonas de interfaces Fuente: Los autores

7. Damos nombre a la zone y arrastar las interfaces a que van unir en la interface para el fortigate surcusal 1.

FortiGate VM64-KVM	PRIN	NCIPAL				Q • >_ []	?• ₽1
Dashboard	> ^	Edit Zone					
Security Fabric Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA Static Routes Policy Routes RIP OSSE	> → ☆	Name Block intra-zone traffic C Interface members Comments	ZONAS WAN WAN-SUCURSAL 1 (port2) 3 WAN-SUCURSAL 1-1 (port3) 3 + 	27	Fo	rtiGate PRINCIPAL Occumentation Online Help C Video Tutorials C	
OSPF BGP Multicast							
System	> 、			ОК	Cancel		

Figura 179. Interface members fortigate principal Fuente: Los autores 8. Damos nombre a la zone y arrastar las interfaces a que van unir en una la interface para el fortigate sucursal 2.

FortiGate VM64-KVM	PRINCIPAL	Q • >	- 0	 40 (👤 admin 🕶
Dashboard	> ^ Edit Zone				
 Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA 	Name ZONA WAN 2 FortiGate Block Intra-zone traffic Interface members WAN-SUCURSAL 1.2 (port4) * Interface members WAN-SUCURSAL 1.3 (port5) * WAN-SUCURSAL 1.3 (port5) * Video Tutorial Comments 0/127	2 Is 2			
Static Routes Policy Routes RIP OSPF BGP Multicast System	> OK Cancel				

Figura 180. Interface members fortigate principal Fuente: Los autores

9. Configurar static routes para el fortigate principal, le damos click en la opción dynamic y obtendrá el dns del router principal.

FortiGate VM64-KVM	PRI	NCIPAL						Q -	× []	?∙	۵۵	🕗 admin 🕶
Dashboard	> ^	New Static Route										
🔆 Security Fabric	>											
+ Network	*	Dynamic Gateway () Destination ()	Subnet Internet Se	rvice								
DNS		Gateway Address 🚯	0.0.0.0/0.0.0	172 18 142 100								
Packet Capture		Interface	port1	▼								
SD-WAN Zones		Administrative Distance ()	10									
SD-WAN Rules Performance SLA		Comments	Write a comment									
Static Routes	☆	Status	Unabled Unis	ableu								
Policy Routes		Advanced Options										
RIP					ОК	Cance	el					
OSPF						Sanoa						

Figura 181. Static routes fortigate principal Fuente: Los autores 10. Configurar la regla que nos permitirá la salida a internet al enlace SD-WAN del fortigate sucursal 1.

FortiGate VM64-KVM	PRI	ICIPAL						Q + >_	11	?∙	40
Dashboard	> ^	Edit Policy									
🔆 Security Fabric	>						ID				
🕂 Network	>	Name ()	INTERNET SD-WAN SUCU	RSAL 1			1				
System	>	Incoming Interface	ZONAS WAN	•			Last used				
Policy & Objects	~	Outgoing Interface	🗎 port1	•			N/A				
Firewall Policy	☆	Source	🖃 all	×			First used				
IPv4 DoS Policy			+				IN/A				
Addresses		Destination	≣ all +	×			Hit count 0				
Internet Service		Schedule	always	•							
Database		Service	😨 ALL	×			0				
Services			+								
Schedules		Action	✓ ACCEPT Ø DENY				O second(s) ago	now			
Virtual IPs							Total bytes				
IP Pools		Inspection Mode	Flow-based Proxy-based			1	0 B				
Protocol Options		E					Current bandwidth				
Traffic Shapers		Firewall / Network O	ptions			1	0 B/s				
Traffic Shaping Policy		NAT	•								
Traffic Shaping Profile		IP Pool Configuration	Use Outgoing Interfac	e Address Use D	ynamic IP Pool						
Security Profiles	>	Preserve Source Port					⑦ Documentation				
므 VPN	>	Protocol Options	PROT default	•	ø		A ALE. (1997)				
Liser & Δuthentication	、 ~				OK	Cancel					
	F	igura 182.	Regla de inte	ernet pa	ra el for	tigate	e sucursa	11			
		0	Fuent	e. Los al	utores	0					

11. Configurar la regla que nos permitirá la salida a internet al enlace SD-WAN del fortigate sucursal 2.

	DDIN	ICIDAL					0 -			<u> </u>	0.0
FortiGate VM64-KVM	PKI	ICIPAL					Q.1	<i>^</i>	6.0	<u>ه</u> ٠	40
🔁 Dashboard	> ^	Edit Policy									
🔆 Security Fabric	>					ID					
Network	>	Name 🚯	INTERNET SD-WAN SUCURSAL 2			2					
System	>	Incoming Interface	ZONA WAN 2	-		Last used					
Policy & Objects	~	Outgoing Interface	🖮 port1	-		N/A					
Firewall Policy	☆	Source	🗐 all	×		First used					
IPv4 DoS Policy			+			N/A					
Addresses		Destination	🖃 all	×		Hit count					
Internet Service		Schedule	G always	-		0					
Database		Service		×		Active sessions					
Services		0011100	+			-					
Schedules		Action	✓ ACCEPT Ø DENY			O second(s) ago		now			
Virtual IPs						Total bytes					
IP Pools		Inspection Mode	Flow-based Proxy-based			OB					
Protocol Options						Current bandwidth					
Traffic Shapers		Firewall / Network C	Options			O B/s					
Traffic Shaping Policy		NAT	•								
Traffic Shaping Profile		IP Pool Configuration	Use Outgoing Interface Addre	ess U	se Dynamic IP Pool						
Security Profiles	>	Preserve Source Por	t 🗇			⑦ Documentation	1				
	>	Protocol Options	PROT default		- <i>s</i>	R 0.0000000	~*				
Liser & Authentication	× ×				OK Cano	el					

Figura 183. Regla de internet para fortigate sucursal 2 Fuente: Los autores

FortiGate VM64-KV	M SUCURSAL-1				٩٠ ≻ [] @• 4
Dashboard Security Fabric Hetwork Interfaces DNS	> Celt Interface > Name Alias Type	Edit Interface Name ENLACE WAN 1 (port2) Alias ENLACE WAN 1 Type Physical Interface			FortiGate Status
Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA	VRF ID 0 Role 0 Estimated band	0 WAN 0 0	▼ kb	ops Upstream ops Downstream	♥ Up MAC address Oc:d3:9a:95:d9:01 Speed Test
Static Routes Policy Routes RIP OSPF BGP	Address Addressing mod IP/Netmask Secondary IP ad	le <u>Manual</u> DHCP 10.10.10.2/255.25 dress ①	Auto-managed by FortilF 55.255.252	AM	Execute speed test ⑦ Documentation ⑦ Online Help ⑦ ♥ Video Tutorials ⑦
Multicast System Policy & Objects Security Profiles VPN	Administrative / > IPv4 > > Receive LLDP	Access HTTPS SSH RADIUS Accounting Use VDOM Setting	PING SNMP Security Fabric Connection Disable Disable	FMG-Access	
User & Authentication	` Figur	a 184. Direcci Fuel	ón IP port2 : nte: Los auto	fortigate sucur	rsal 1

12. Configurar la dirección IP al port2 del fortigate de la sucursal 1.

13. Configurar la dirección IP al port3 del fortigate de la sucursal 1.

FortiGate VM64-KVN	A <u>SU</u>	CURSAL-1				Q•≻[] @•
Dashboard	> ^	Edit Interface				
 Security Fabric Network Interfaces DNS 	> ~ ☆	Name Alias Type VRF ID	 ENLACE WAN 2 ENLACE WAN 2 Physical Interface 0 	(port3)]	FortiGate SUCURSAL-1 Status Up
Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA		Role 1 Estimated bandwidth	WAN 0 0 0	•	kbps Upstream kbps Downstream	MAC address Oc:d3:9a:95:d9:02 Speed Test
Static Routes Policy Routes		Address Addressing mode	Manual DHCP	Auto-managed by For	tiIPAM	Execute speed test
RIP OSPF BGP		IP/Netmask Secondary IP address	20.20.2/255.25	5.255.252		 ② Documentation ② Online Help C ■ Video Tutorials C
Multicast		Administrative Access				
 System Policy & Objects Security Profiles VPN 	> > > >	IPv4] HTTPS] SSH] RADIUS Accounting Use VDOM Setting Ena	PING SNMP Security Fabric Connection Disable	FMG-Access FTM	
User & Authentication	> 、				OK Cancel	

Figura 185. Dirección IP port3 fortigate sucursal 1 Fuente: Los autores 14. Configurar la interface port4 para la red local con su dhcp del fortigate sucursal.

FortiGate VM64-KVM	CURSAL-1	٩٠ ≻ [] @٠
🚯 Dashboard >	Edit Interface	
Security Fabric Network Network Network Network DIS Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA Static Routes RIP OCRE	Name Rott4 Alias LAN-SUCURSAL1 Type Physical Interface VRF ID 0 Role LAN Address 0cd3/9a/95 Address object matching subnet 9 Docume IP/Netmask 192.168.0.1/24 Create address object matching subnet 9	ISAL-1 X9903 Intation Help C Tutorials C
BGP	Administrative Access	
Multicast	IPv4 HTTPS PING FMG-Access	
System Policy & Objects Security Profiles VPN User & Authentication	Control Contr	
lılıl Log & Report →	DHCPServer Address range 192.168.0.2-192.168.0.254 Image: Comparison of the state	
	OK Cancel	

Figura 186. Configuración red local del fortigate Fuente: Los autores

15. Crear SD-WAN Member en la sucursal 1.

FortiGate VM64-H	KVM SUCL	JRSAL-1			Q + >_ [] 🕐 🗘 🛛 🥥 admin 🔹
Security Fabric	> ^	Bandwidth Volume Sessions				
Network Interfaces	~	Do	wnload		Upload	port2
DNS						
Packet Capture SD-WAN Zones	☆					
SD-WAN Rules			7			
Static Routes		+ Create New ▼	lete			
Policy Routes		SD-WAN Member	Gateway 🗢	Cost 🗘	Download 🗢	Upload ≑
OSDE		Virtual-wan-link				

Figura 187. Sd-wan zone fortigate sucursal 1 Fuente: Los autores

	^				
🔆 Security Fabric	>	Edit SD-WAN Mei	nber		
Network Interfaces	~	Interface	ENLACE WAN 1 (port2)		
DNS		SD-WAN Zone Gateway	Virtual-wan-link • 10.10.10.1		
Packet Capture		Cost	0		
SD-WAN Zones	☆	Status	• Enabled • Disabled		
SD-WAN Rules					
Performance SLA					
Static Routes					
Policy Routes					
RIP					
OSPF					
BGP					
Multicast					
System	>				
Policy & Objects	>			ОК	Cancel
		Figura	188. Sd-wan enlace wan	1	
			Fuente: Los autores		

16. Crear SD-WAN para la interface enlace wan 1.

17. Crear SD-WAN para la interface enlace wan 2.

FortiGate VM64-	KVM SUC	URSAL-1			
Security Fabric	> ^	New SD-WAN Me	ember		
 Network Interfaces DNS Packet Capture 	×	Interface SD-WAN Zone Gateway Cost	 ENLACE WAN 2 (port3) virtual-wan-link 20.20.20.2 0]]]	¢
SD-WAN Zones SD-WAN Rules Performance SLA Static Routes Policy Routes	☆	Status	Enabled O Disabled		୯
RIP OSPF BGP Multicast					
SystemPolicy & Objects	>			ОК С	ancel

Figura 189. Sd-wan enlace wan 1 Fuente: Los autores 18. Configurar static routes para la SD-WAN.

FortiGate VM64-	KVM <u>SU</u>	CURSAL-1			Q • ≻_ []
Dashboard	> ^	New Static Route			
🔆 Security Fabric	>				
+ Network	~	Dynamic Gateway	Subset Internet Convice	Interface @ SD-WAN	
Interfaces		Destination	Subhet Internet Service		
DNC			0.0.0/0.0.0	Type SD-WAN Interface	
DINS		Interface	SD-WAN	-	
Packet Capture		Comments	Write a comment	- 0/055	
SD-WAN Zones		Status	• Enabled • Disabled	0/255	
SD-WAN Rules					
Performance SLA					
Static Routes	☆			OK Cancel	
Policy Routes					

Figura 190. Static routes para sd-wan fortigate sucursal 1 Fuente: Los autores

19. Configurar la regla de salida a internet que permite a la SD-WAN dar acceso a internet a la red local del fortigate sucursal 1.

FortiGate VM64-KV	N SUC	URSAL-1				Q·≻ [] @· A 1
Dashboard	> ^	New Policy				
🔆 Security Fabric	>				⑦ Documenta	ation
Network	>	Name 🚯	INTERNET		Online He	elp 🗗
System	>	Incoming Interface	LAN-SUCURSAL 1 (port4)	•	Video Tut	orials 🕜
Policy & Objects	~	Outgoing Interface	🔞 virtual-wan-link	-		
Firewall Policy	☆	Source	🖃 all	×		
IPv4 DoS Policy			+			
Addresses		Destination	🗐 all 🕂	×		
Internet Service Database		Schedule	C always	~		
Services		Service	ALL +	×		
Schedules		Action	✓ ACCEPT Ø DENY			
Virtual IPs						
IP Pools		Inspection Mode	Flow-based Proxy-based			
Protocol Options						
Traffic Shapers		Firewall / Network C	options			
Traffic Shaping Policy		NAT	•			
Traffic Shaping Profile		IP Pool Configuration	Use Outgoing Interface Add	ress Use Dynamic IP Pool		
Security Profiles	>	Preserve Source Por	t 🛈			
C VPN	>	Protocol Options	PROT default	✓ Ø	Canad	
Liser & Authentication	× ×			OK	Cancel	

Figura 191. Static routes para sd-wan fortigate sucursal 1 Fuente: Los autores
20. Configurar SD-WAN Rules en sucurasal 1 para controlar como se distribuye las sesiones a los miembros de SD WAN dames click en créate new y nombramos nuestra primera regla que se llamara Faceboox.

FortiGate VM64-KVM	SUCURSAL1						
20 Dashboard	> Priority Rule						
🔆 Security Fabric							
+ Network	PACEDOCK						
Interfaces	Source						
DNS	Source address I all X						
Packet Capture	+						
SD-WAN Zones	User group +						
SD-WAN Rules							
Performance SLA	Destination						
Static Routes	Address 🚯 +						
Policy Routes	Internet Service Facebook-Web X						
RIP	+						
OSPF	Application +						
BGP	Outputer later facer						
Multicast	ougoing menaces						
System	Select a strategy for how outgoing interfaces will be chosen.						
Policy & Objects	> O Manual						
Security Profiles	Manually assign outgoing interfaces.						
III VPN	 Best Quality The interface with the best measured performance is selected. 						
User & Authentication	> O Lowest Cost (SLA)						
Log & Report	The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.						
	Maximize Bandwidth (SLA) Traffic is load balanced among interfaces that meet SLA targets.						
	Interface preference Interface preference M ENLACE WAN 1 (port2) M ENLACE WAN 2 (port3) M						
	Measured SLA GOOGLE -						
	Quality criteria Jitter						
	Status O Enable O Disable						

Figura 192. SD-WAN Rules para Faceboox- fortigate sucursal 1 Fuente: Los autores

21. Creamos una nueva regla llamada TeamViewer y llenamos los campos mostrados.

Security Fabric Network Interfaces DNS	Name TeamWiber					
Network Interfaces DNS	Name TeamWiber					
Interfaces DNS						
DNS	Source					
	Source address III all X					
Packet Capture	+					
SD-WAN Zones	User group +					
SD-WAN Rules						
Performance SLA	Destination					
Static Routes	Address 🚯 +					
Policy Routes	Internet Service TeamViewer-Web X					
RIP	+					
OSPF	Application +					
BGP	Outpoint Interfaces					
Multicast	Cougoing manazes					
System	Select a strategy for how outgoing interfaces will be chosen.					
Policy & Objects	O Manual					
Security Profiles	Manually assign outgoing Interfaces.					
I VPN	 Best Quality The interface with the best measured performance is selected. 					
Subser & Authentication	O Lowest Cost (SLA)					
🖬 Log & Report	The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.					
	O Maximize Bandwidth (SLA)					
	Traffic is load balanced among interfaces that meet SLA targets.					
	Interface preference ENLACE WAN 1 (port2)					
	ENLACE WAN 2 (port3) X					
	+					
	Measured SLA GOOGLE					
	Quality criteria Packet Loss					

Figura 193. SD-WAN Rules para TeamViewer- fortigate sucursal 1 Fuente: Los autores

22. Por ultimo nuestra ultima regla se llamara Adobe y llenamos los campos mostardos.

Dashboard	> Priority Rule						
Security Fabric	>						
* Network	Vame Adobe						
Interfaces	Source						
DNS	Source address	1 all	×				
Packet Capture	Source address	+					
SD-WAN Zones	User group	+					
SD-WAN Rules	☆						
Performance SLA	Destination						
Static Routes	Address ()	+					
Policy Routes	Internet Service	Adobe-Web	×				
RIP		+					
OSPF	Application	+					
BGP							
Multicast	Outgoing Interfaces						
System	> Select a strategy for I	Select a strategy for how outgoing interfaces will be chosen.					
Policy & Objects	> O Manual						
Security Profiles	> Manually assign	outgoing interfaces.					
L VPN	Best Quality						
User & Authentication	> Contract Contract	th the best measured performance is	s selected.				
Log & Report	> Lowest Cost (SL The interface th	A) at meets SLA targets is selected. Wh	en there is a tie, the interface with the lowest assigned cost is selected.				
	O Maximize Band	width (SLA)					
	Traffic is load ba	lanced among interfaces that meet S	SLA targets.				
	Interface preference	ENLACE WAN 1 (port2)	×				
		+					
	Measured SLA	GOOGLE	•				
	Quality criteria	Latency	v				
	Status	Enable O Disable					

Figura 194. SD-WAN Rules para Adobe- fortigate sucursal 1 Fuente: Los autores

23. Mostramos todas las SD-WAN Rules el cual indica porque enlace va a navegar nuestra regla y cual criterio tomara en cuenta para poder hacerlo.

FortiGate VM64-K	VM <u>SU</u>	CURSAL-1					Q • >_ []	() • 🗘 🚺 🕗 admin •
🚯 Dashboard	> ^	+ Crea	te New 📝 Edit	Delete	Search		Q	
X Security Fabric	>		Name	Courses	Destination	Critteria	Mandara	Litt Court
🕂 Network	~		Name	Source	Destination	Criteria	Members	HILCOUNL
Interfaces		IPv4	3					
DNS		1	Facebook	😐 all	Facebook-Web	Jitter	 ENLACE WAN 1 (port2) ENLACE WAN 2 (port3) 	
Packet Capture		2	TeamWiber	🔳 all	TeamViewer-Web	Packet Loss	🔳 ENLACE WAN 1 (port2) 🛇	0
SD-WAN Zones							ENLACE WAN 2 (port3)	
SD-WAN Rules	ជ	3	Adobe	🖃 all	Adobe-Web	Latency	🔳 ENLACE WAN 1 (port2) 🛇	<u>0</u>
Performance SLA							ENLACE WAN 2 (port3)	
Static Routes		🗖 Impli	cit 1					
Policy Routes			sd-wan	🔳 all	🗐 all	Source-Destination IP	🗆 any	
RIP								
OSPF								
BGP								
Multicast								
System	>							
Policy & Objects	>							
		F	igura19	5. SD-V	NAN Rules	para fortiga	ate sucursal 1	



24. Configurar SD-WAN Rules en sucurasal 2 para controlar como se distribuye las sesiones a los miembros de SD-WAN dames click en créate new y nombramos nuestra primera regla que se llamara Amazon.

FortiGate VM64-KVM	SUCURSAL2
🚯 Dashboard	> Priority Rule
🔆 Security Fabric	
+ Network	v Name Amazon
Interfaces	Source
DNS	Source address
Packet Capture	+ · · · · · · · · · · · · · · · · · · ·
SD-WAN Zones	User group +
SD-WAN Rules	☆
Performance SLA	Destination
Static Routes	Address 🛈 +
Policy Routes	Internet Service Amazon-Web X
RIP	+
OSPF	Application +
BGP	Outraing Interfaces
Multicast	Outgoing interfaces
System	Select a strategy for how outgoing interfaces will be chosen.
📕 Policy & Objects	> O Manual
Security Profiles	Manually assign outgoing interfaces.
L VPN	Best Quality The interface with the best measured performance is selected.
User & Authentication	> O Lowest Cost (SLA)
네 Log & Report	The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.
	O Maximize Bandwidth (SLA)
	Traffic is load balanced among interfaces that meet SLA targets.
	Interface preference WAN SUCURSAL 2 (port2) * WAN SUCURSAL 2 (port3) * +
	Measured SLA Google 💌
	Quality criteria Packet Loss 💌
	Status C Enable C Disable

Figura 196. SD-WAN Rules para Amazon- fortigate sucursal 2 Fuente: Los autores 25. Del mismo modo creamos otra nueva SD-Rules la cual nombraremos Likendin y llenamos los campos mostrados.



Figura 197. SD-WAN Rules para Likendin- fortigate sucursal 1 Fuente: Los autores

26. Mostramos todas las SD-WAN Rules el cual indica porque enlace va a navegar nuestra regla y cual criterio tomara en cuenta para poder hacerlo.

FortiGate VM64-K	VM <u>su</u>	ICURSAL2					Q+ >_	[]
Dashboard	> 1	+ Create	e New 🔗 Edit	Delete	Search		Q	
🔆 Security Fabric	>		Namo	Sourco	Destination	Critoria	Momhore	Hit Count
🕂 Network	~		Indille	Jource	Destination	Criteria	Members	Hit Coulit
Interfaces		E IPv4 2						
DNS		1	Amazon	🗐 all	Amazon-Web	Packet Loss	 WAN SUCURSAL 2 (port2) WAN SUCURSAL 2 (port3) 	<u>0</u>
SD-WAN Zones		2	Likendin	🗐 all	LinkedIn-Web	Downstream	 WAN SUCURSAL 2 (port2) WAN SUCURSAL 2 (port3) 	0
SD-WAN Rules	☆	🗖 Implicit	1					
Performance SLA	☆		sd-wan	🗉 all	🗉 all	Source IP	🛛 any	
Static Routes								
Policy Routes								
RIP								
OSPF	_							
BGP	_							
Multicast								
System	>					,		

Figura.198 SD-WAN Rules - fortigate sucursal 2 Fuente: Los autores

27. Realizar un SLA a travez de PING a google salga a travez de la SD-WAN.

FortiGate VM64-K	VM SUCI	URSAL-1				۵. >	_ [] ()	- QO (l
Dashboard	> ^	Edit Performance SLA							
🔆 Security Fabric	>					SLA Details			
Network	~	Name Protocol	GOOGLE Ping HTTP DNS				Packet Loss	Latency	
Interfaces DNS		Servers	8.8.8.8 8.8.4.4	× ×		ENLACE WAN 1 (port2)ENLACE WAN 2 (port3)	0.00%	63.36ms 62.43ms	
SD-WAN Zones SD-WAN Rules		Participants Enable probe packets	All SD-WAN Members Sp	becify					
Performance SLA Static Routes	☆	SLA Target 🕥 Link Status				 Performance SLA Setup G Link Monitoring SLA Targets 	uides		
RIP OSPF BGP		Check interval Failures before inactive Restore link after ()	500 5 4	ms check(s)		 ⑦ Documentation ⑧ Online Help ⑦ ● Video Tutorials ⑦ 			
Multicast System	>	Actions when Inactive							
 Policy & Objects Security Profiles 	>	opuate static foure	-	<u> </u>					
LL VPN	>			OK	Cancel				

Figura 199. Configuración de static routes SD-WAN del fortigate Fuente: Los autores

28. Veremos que tenemos menos PING y JIPTTER en una de las interfaces configuradas donde SD-WAN eligue en enlace con mejor calidad de servicios.

FortiGate VM64-KVM	JCURSAL-1				Q • ≻_ [] @•	🔎 🕗 admin 🕶
Dashboard >	Packet Loss	Latency Jitter				
☆ Security Fabric >	120ms					port2
Network ×	100ms					nort3
Interfaces	80ms					
DNS	60ms					
Packet Capture	40ms					
SD-WAN Zones	20ms					
SD-WAN Rules	Oms					
Performance SLA 🏠	15:10:3	30 15:11:00 15:11	1:30 15:12:00 15:12:30 15:1	13:00 15:13:30 15:14:00 15:14:	30 15:15:00 15:15:30 15:16:	00 15:16:30
Static Routes	+ Create	New 🖋 Edit 📋	Delete Search	(2	
Policy Routes	Name ≑	Detect Server ≑	Packet Loss	Latency	Jitter	Failure Threshold ≑
RIP	GOOGLE	8.8.8.8	ENLACE WAN 1 (port2): 0.00%	ENLACE WAN 1 (port2): 63.31ms	ENLACE WAN 1 (port2): 01.13ms	5
OSPF		8.8.4.4	ENLACE WAN 2 (port3): 0.00%	ENLACE WAN 2 (port3): 62.33ms	ENLACE WAN 2 (port3): 0.52ms	

Figura 200. Diagrama de calidad de sevicio de sucrusal 1

Fuente: Los autores

29. Configurar la dirección IP en puerto 2 en el fortigate principal para el enlace WAN para el fortigate sucursal 2.

FortiGate VM64-K	VM <u>su</u>	CURSAL2					Q + >_	13	? •	۵4	🕗 admir
Dashboard	> ⁴	Edit Interface									
Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules	`	Name Alias Type VRF ID 3 Role 3 Estimated bandwidth	WAN SU WAN SUC Physical WAN 0 0	ICURSAL 2 (port2) URSAL 2 Interface	 kbps Upstream kbps Downstream 	FortiGate FortiGate-VM6 Status Up MAC address 0::d3:9a:31:99:01 Courd Turb	4-KVM				
Performance SLA Static Routes Policy Routes RIP OSPF BGP		Address Addressing mode IP/Netmask Secondary IP address Administrative Access	Manual 40.40.40.2	DHCP Auto-managed by /255.255.255.252	FortiIPAM	Execute speed test Execute speed test Documentation Online Help C Video Tutorials	ď				
System Solution Solu	> > > >	IPv4) HTTPS) SSH) RADIUS Accou Jse VDOM Setti	PING SNMP Security Fabric Connection	FMG-Access FTM	rcel					
		Figura	201 C	onfiguracion	IP fortigate	wan sucreal	2				

Figura 201. Configuracion IP fortigate wan sucrsal 2 Fuente: Los autores

30. Configurar la dirección IP en puerto 3 en el frotigate principal para el enlace WAN para el fortigate sucursal 2.

FortiGate VM64-KVM	I SUC	URSAL2						Q + >_	. D		۵۵	🕗 admin •
🍪 Dashboard	> ^	Edit Interface										
 Security Fabric Network Interfaces DNS 	> ~ ☆	Name Alias Type VRFID	WAN SUCURSAL 2 (port3) WAN SUCURSAL 2 Physical Interface 0				FortiGate SUCURSAL2 Status OUp					
Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA		Role 1 Estimated bandwidth 1	WAN 0 0	•	kbps Upstream kbps Downstrea	am	MAC address 0c:d3:9a:31:99:02 Speed Test					
Static Routes		Address	Manual DUK	CD Auto menored by Cr	HIDANA		Execute speed test					
RIP OSPF BGP		IP/Netmask Secondary IP address	30.30.30.2/25	5.255.255.252			 ⑦ Documentation ⑧ Online Help G ● Video Tutorials 	3 5 C				
Multicast		Administrative Access										
 System Policy & Objects Security Profiles VPN 	> > >	IPv4	HTTPS SSH RADIUS Accountin Se VDOM Setting	PING SNMP Security Fabric Connection (1) Enable Disable	FMG-Access FTM							
User & Authentication	> .				ОК	Cancel						

Figura 202. Configuracion IP fortigate wan sucursal 2 Fuente: Los autores

31. Configurar la interface port4 para la red local con su DHCP del fortigate sucursal. 2.

FortiGate VM64-KVN	suc	URSAL2			Q.+ >_ [] @+ A 👰 🕗 admin
2 Dashboard	>	Edit Interface			
🔆 Security Fabric	>	Name 🕅 P	114		FortiGate
+ Network	÷	Alias	LOCAL SUCURSAL 2		SUCURSAL2
Interfaces	4	Туре 🗎 Р	isical Interface		
DNS		VRFID 0			Status
Packet Capture		Role 1	•		O Up
SD-WAN Zones SD-WAN Rules Performance SLA		Address Addressing mode	Manual DHCP Auto-m	anaged by FortilPAM One-Arm Sniffer	MAC address Oc:d3:9x:31:99:03 ② Documentation
Static Routes Policy Routes		Create address ob Secondary IP addr	ct matching subnet ①		 Ø Online Help IS IN Video Tutorials IS
RIP					
OSPF		Administrative Acc	55		
BGP		IPv4	HTTPS PING	FMG-Access	
Multicast			SSH SNMP	C FTM	
System	>		RADIUS Accounting Connection 0		
🕭 Policy & Objects	>	Receive LLDP 🚯	Use VDOM Setting Enable Disable		
Security Profiles	×.	Transmit LLDP ()	Use VDOM Setting Enable Disable		
Q VPN	>	DHCD Senses			
User & Authentication	>	U DHCP Server			
Leg & Report	>	Address range	0		
		Netmask	255.255.255.0		
		Default gateway	Same as Interface IP Specify		



32. Crear SD-WAN Member en la sucursal 2.

FortiGate VM64-	KVM SUCURSAL	2			Q + >_ [] _ ⑦ + _ Д 10 _ admin +
🚯 Dashboard	> 🔶 Band	width Volume Sessions				
Security Fabric	>	Dow	Upload			
+ Network	~		port2			port2
Interfaces						
DNS						
Packet Capture						
SD-WAN Zones	☆					
SD-WAN Rules						
Performance SLA						
Static Routes	+ 0	reate New▼ 🖋 Edit 📋 Dele	te			
Policy Routes		Interfaces ≑	Gateway 🌲	Cost ≑	Download ≑	Upload 🗢
RIP	•	virtual-wan-link				
OSPF						

Figura 204. Sd-wan zone fortigate sucursal 2 Fuente: Los autores

33. Crear SD-WAN para la interface sucursal 2.

FortiGate VM64-K	VM SUC	CURSAL2			
🕂 Network	~ ^	Edit SD-WAN Me	mber		
Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA	☆	Interface SD-WAN Zone Gateway Cost Status	WAN SUCURSAL 2 (port2) Image: Wan Sucursal 2 (port2)		() () ()
Static Routes Policy Routes					
RIP OSPF BGP Multicast					
 System Policy & Objects Security Profiles 	>			ОК	Cancel

Figura 205 Sd-wan sucursal 2 para puerto 2 Fuente: Los autores 34. Crear SD-WAN para la interface sucursal 2.

Network	~ ^	Edit SD-WAN Me	mber		
Interfaces DNS Packet Capture SD-WAN Zones	쇼	Interface SD-WAN Zone Gateway Cost	 WAN SUCURSAL 2 (port3) virtual-wan-link 30.30.30.1 	▼ ▼	
Performance SLA Static Routes Policy Routes		Status	• Enabled • Disabled		
RIP OSPF BGP Multicast					
System	>				
Policy & Objects	>			ОК	Cancel

Figura 206. Sd-wan sucursal 2 para puerto 3 Fuente: Los autores

35. Configurar static routes para la SD-WAN sucursal 2

FortiGate VM64-H	KVM <u>SUC</u>	CURSAL2				Q • >_ []	@• ⊉1	👤 admin 🕶
Dashboard	> ^	New Static Route						
🔆 Security Fabric	>		-					
Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Pulse	~	Dynamic Gateway Destination Interface Comments Status	Subnet Internet Service 0.0.0/0.0.0 SD-WAN Write a comment Enabled Disabled	• 0/255				
Performance SLA Static Routes Policy Routes RIP OCODE	☆			ОК	Cancel			

Figura 207. Static routes para sd-wan fortigate sucursal 2 Fuente: Los autores 36. Configurar la regla de salida a internet que permite a la SD-WAN dar acceso a internet a la red local del fortigate sucursal 2.

FortiGate VM64-KVI	M <u>SU</u>	CURSAL2						Q -	<u>>_ [</u>] ⑦	۵۵	🕗 admin
Dashboard	> ^	New Policy										
🔆 Security Fabric	>						 Documentation 					
🕂 Network	>	Name 🕚	RED LOCAL SUCURSAL 2				🕘 Online Help 🖸	8				
System	>	Incoming Interface	RED LOCAL SUCURSAL 2	? (port4) 🔻			Video Tutorials	s 🕐				
Policy & Objects	~	Outgoing Interface	virtual-wan-link	•								
Firewall Policy	☆	Source	🗐 all	×								
IPv4 DoS Policy			+									
Addresses		Destination	≣ all +	×								
Internet Service		Schedule	G always	•								
Services		Service	ALL +	×								
Schedules		Action	✓ ACCEPT Ø DENY									
Virtual IPs												
IP Pools		Inspection Mode	Flow-based Proxy-based									
Protocol Options												
Traffic Shapers		Firewall / Network O	ptions									
Traffic Shaping Policy		NAT	•									
Traffic Shaping Profile		IP Pool Configuration	Use Outgoing Interface	Address U	se Dynamic IP Pool							
Security Profiles	>	Preserve Source Port	. 🔿									
I VPN	>	Protocol Options	PROT default	_	▼ Ø							
Liser & Δuthentication	· ·				ОК	Cancel						

Figura 208. Static routes para sd-wan fortigate sucursal 2 Fuente: Los autores

37. Configurar perfomance SLA SD-WAN para balancear la conexión que tenga menos PING o latencia donde fortigate eligira cual será el mejor vinculo que tenga mejor calidad de servicio dames click en créate new para sucursal 2.



RECURSOS UTILIZADOS

- > COMPUTADORA
- CABLE DE RED (PATCHCORD)
- ➢ GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente

4.1.5. **PRÁCTICA 5**

Configuración de una red SD-WAN con fortigate y enlazados con

dispositivos mikrotik.

DATOS INFORMATIVOS

- > MATERIA: Redes de comunicación
- > PRÁCTICA № 5
- > NUMERO DE COMPUTADORAS: 10
- > **TIEMPO ESTIMADO:** 2 Horas

DATOS DE LA PRÁTICA

TEMA: Configuración de una red SD-WAN con fortigate y enlazarlos con

dispositivos mikrotik.

OBJETIVOS

General

Configurar la red sd-wan y enlazarlos con enrutamiento estático.

Específicos

- > Configurar enrutamiento estático en los mikrotik.
- > Configurar dispositivos mikrotik para salida a internet.
- > Comprobar compatibilidad de los enlaces finales.

GLOSARIO

MIKROTIK.- Mikrotik es un fabricante de hardware y software de routers su kernel esta basado en Linux 2.6.

DHCP.- Es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP determina dinámicamente una dirección IP a un dispotivo dentro de la red de datos por ejemplo celulares y computadoras.

DHCP-CLIENT.- El cliente aceptará una dirección, máscara de red, puerta de enlace predeterminada y dos direcciones de servidor DNS de su proveedor de internet ISP.

NAT.- Es manejado por los routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles, NAT es usada por las redes IPv4.

WINBOX.- Es una herramienta que permite la administración de equipos mikrotik manejando una GUI rápida y sencilla.

MARCO PROCIDEMENTAL.

1. Diseñar la topología de la red para la práctica 5



Figura 210. Diseño de la red práctica Nº5 Fuente: Los autores

2. Configurar la red del enlace WAN en el fortigate principal para el fortigate servidor sd-wan.

FortiGate VM64-KV	M FG-I	PRINCIPAL			
Dashboard	> ^	Edit Interface			
Security Fabric Network	> ~ ☆	Name Alias	WAN-SERVIDO	PR (port2)	
DNS Packet Capture		Type VRF ID 10 Role 10	Physical Interface 0 WAN	ce	
SD-WAN Zones SD-WAN Rules Performance SLA		Estimated bandwidth	100000 100000		kbps Upstream kbps Downstream
Static Routes Policy Routes		Address Addressing mode	Manual DHCP	Auto-managed by For	tiIPAM
RIP OSPF BGP		IP/Netmask Secondary IP address	10.10.1/255.2	55.255.252	
Multicast		Administrative Access			
 System Policy & Objects Security Profiles VPN 	>	IPv4	HTTPS SSH RADIUS Accounting se VDOM Setting En	 PING SNMP Security Fabric Connection 3 able Disable 	FMG-Access FTM
User & Authentication	>				OK Cancel

Figura 211. Interfaz port2 FG-principal Fuente: Los autores

3. Configurar ruta estática para el fortigate principal para la salida a internet, damos click en dynamic para obtener la configuración del ISP.

FortiGate VM64-	KVM FG-PRINCIPAL
Dashboard	> ^ New Static Route
 Security Fabric Network Interfaces DNS 	 Dynamic Gateway 1 Destination 1 Subnet Internet Service 0.0.0/0.0.0.0 Gateway Address 1 Dynamic Specify 172.18.142.100
Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA	Interface mort1 Administrative Distance 10 10 Comments Write a comment Status Image: Comment in the state in
Static Routes Policy Routes RIP OSRE	☆ ▲ Advanced Options OK

Figura 212. Interfaz port2 FG-principal Fuente: Los autores

4. Configurar la regla en el firewall que permitirá la salida a internet al servidor SD-WAN.

FortiGate VM64-KVM	FG	PRINCIPAL			Q • >_
Dashboard	> ^	New Policy			
🔆 Security Fabric	>				⑦ Documentation
Network	>	Name 🕚	INTERNET ENLACE WAN		Online Help I I
System	>	Incoming Interface	MAN-SERVIDOR (port2)	-	Video Tutorials 🖸
Policy & Objects	~	Outgoing Interface	m port1	•	
Firewall Policy	☆	Source	🗐 all	×	
IPv4 DoS Policy			+		
Addresses		Destination	i≣ all +	*	
Internet Service Database		Schedule	o always	•	
Services		Service	ALL +	×	
Schedules		Action	✓ ACCEPT Ø DENY		
Virtual IPs					
IP Pools		Inspection Mode	Flow-based Proxy-based		
Protocol Options					
Traffic Shapers		Firewall / Network O	ptions		
Traffic Shaping Policy		NAT	•		
Traffic Shaping Profile		IP Pool Configuration	Use Outgoing Interface Ad	dress Use Dynamic IP Pool	
Security Profiles	>	Preserve Source Port			
D VPN	>	Protocol Options	PROT default	▼ Ø	
Liser & Δuthentication	、 ~			ОК	Cancel

Figura 213. Firewall Policy port2 Fuente: Los autores

5. Configurar la red del enlace principal en el fortigate servidor SD-WAN.

FortiGate VM64-KVN	A SER	VIDOR-SD-WAN			
Dashboard	> ^	Edit Interface			
Security Fabric	>	Name	🔝 WAN - ENLACE (port2)	
Interfaces	☆	Alias	WAN - ENLACE		
DNS		Type VRFID (1)			
Packet Capture		Role 1	WAN	•	
SD-WAN Zones SD-WAN Rules Performance SLA		Estimated bandwidth 🚯	0		kbps Upstream kbps Downstream
Static Routes		Address			
Policy Routes		Addressing mode	Manual DHCP	Auto-managed by For	tiIPAM
RIP OSPF BGP		IP/Netmask Secondary IP address 🖸	10.10.10.2/255.255	5.255.252	
Multicast		Administrative Access			
 System Policy & Objects Security Profiles VPN 	> > > >	IPv4 IF	HTTPS SSH RADIUS Accounting e VDOM Setting Enal	PING SNMP Security Fabric Connection Disable	FMG-Access FTM
User & Authentication	> ن				OK Cancel

Figura 214. Servidor sd-wan port2 Fuente: Los autores

6. Configurar las interfaces port3 en el servidor SD-WAN que se comunicara con el mikrotik-daule.

Dashboard	> ^	Edit Interface			
Security Fabric	>	Mana		(ANI 1 (port 2)	
• Network	~	Name	ENLACE 3D-W		
Interfaces	☆	Alias	ENLACE SD-WA	N 1	
DNS		Туре	Physical Interna	ice	
Packet Capture		VRFID (1)	0		
SD-W/AN Zones		Role 🚯	WAN	•	
SD-WAN Dules		Estimated bandwidth	0 20000	kbps	Upstream
SD-WAIN Rules			20000	kbps	Downstream
Performance SLA					
Static Routes		Address			
Policy Routes		Addressing mode	Manual DHCP	Auto-managed by FortilPA	M
RIP		IP/Netmask	20.20.20.1/255.2	255.255.252	
OSPF		Secondary IP address			
BGP					
Multicast		Administrative Acces	s		
System	>	IPv4 (☐ HTTPS	PING	FMG-Access
Policy & Objects	>	(SSH	SNMP	FTM
Security Profiles	,	(RADIUS Accounting	Security Fabric Connection (1)	
		Receive LLDP ()	Use VDOM Setting E	nable Disable	
	· ·				

Figura 215. Servidor sd-wan port3 Fuente: Los autores

7. Configurar la interface port4 en el servidor SD-WAN que se comunicara con el mikrotik-salinas.

FortiGate VM64-KVI	M <u>SE</u>	RVIDOR-SD-WAN			
Dashboard	> ^	Edit Interface			
🔆 Security Fabric	>	Name	ENLACE SD-WA	N 2 (port4)	
+ Network	~	Alias	ENLACE SD-WAN	2	
Interfaces	☆	Type	Physical Interface	2	
DNS		VREID 6			
Packet Capture					
SD-WAN Zones			WAN 25000	•	likes Destaurs
SD-WAN Rules		Estimated bandwidth U	25000		kbps Opstream
Performance SLA			25000		kbps Downstream
Static Routes		Address			
Policy Routes		Addressing mode	Manual DHCP	Auto-managed by For	TIPAM
, RIP		IP/Netmask	30.30.30.1/255.25	5.255.252	
OSPE		Secondary IP address			
BGP					
Multicast		Administrative Access			
System	>	IPv4 🗌 H	TTPS	PING	FMG-Access
Policy & Objects	>	□ S!	SH		□ FTM
Security Profiles	>	🗆 R	ADIUS Accounting	Connection ()	
Q VPN	>	Receive LLDP () Use	VDOM Setting Ena	ble Disable	
User & Authentication	>				OK Cancel

Figura 216. Servidor sd-wan port4 Fuente: Los autores

8. Configurar port5 en el servidor SD-WAN que se comunicara con el mikrotik-salitre.

FortiGate VM64-KV	M <u>SER</u>	VIDOR-SD-WAN			
Dashboard	> ^	Edit Interface			
 Security Fabric Network Interfaces DNS Packet Capture 	> ~ ☆	Name Alias Type VRF ID 0	ENLACE SD-WA ENLACE SD-WAM Physical Interfat 0 MAN	AN3 (port5) 13 ce]
SD-WAN Zones SD-WAN Rules Performance SLA		Estimated bandwidth	25000 25000		kbps Upstream kbps Downstream
Policy Routes		Addressing mode	Manual DHCP	Auto-managed by For	tiIPAM
RIP OSPF BGP		IP/Netmask Secondary IP address (15.15.15.1/30		
Multicast		Administrative Access			
 System Policy & Objects Security Profiles VPN 	> > >	IPv4	HTTPS SSH RADIUS Accounting se VDOM Setting	PING SNMP Security Fabric Connection able Disable	FMG-Access
User & Authentication	>				OK Cancel

Figura 217. Servidor sd-wan port5 Fuente: Los autores

9. Configurar la interfaz port3 en SD-WAN MEMBER para el enlace con mikrotik-daule.

FortiGate VM64-KVM	SER	VIDOR-SD-WAN			
Dashboard	> ^	New SD-WAN Me	mber		
Dashboard Security Fabric Vetwork Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA Static Routes		New SD-WAN Mee Interface SD-WAN Zone Gateway Cost Status	mber Image: ENLACE SD-WAN 1 (port3) Image: Enclose in the second sec		(
Policy Routes RIP OSPF BGP Multicast • System	>			ОК	Cancel

Figura 218. Interfaz sd-wan port3 servidor Fuente: Los autores

10. Configurar la interfaz port4 en SD-WAN MEMBER para el enlace con mikrotik-salinas.

FortiGate VM64-K	VM SERV	VIDOR-SD-WAN			
Dashboard	> ^	New SD-WAN Me	mber		
🔆 Security Fabric	>				
Network Interfaces DNS	×	SD-WAN Zone Gateway	ENLACE SD-WAN 2 (port4) virtual-wan-link 30.30.30.1		
Packet Capture SD-WAN Zones	☆	Cost Status	0 C Enabled O Disabled		
SD-WAN Rules Performance SLA					
Static Routes Policy Routes					
RIP OSPF					
BGP Multicast					
System	>			OK Cance	el
Policy & Objects	>				

Figura 219. Interfaz sd-wan port4 servidor Fuente: Los autores

11. Configurar la interfaz port5 en SD-WAN member para el enlace con mikrotik-salitre.

FortiGate VM64-KV	M SER	VIDOR-SD-WAN		
🚯 Dashboard	> ^	New SD-WAN Me	ember	
🔆 Security Fabric	>	Interface		
Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA Static Routes Policy Routes RIP OSPF BGP	✓	Interface SD-WAN Zone Gateway Cost Status	 ENLACE SD-WAN3 (ports) virtual-wan-link 15.15.15.1 0 C Enabled C Disabled 	
Multicast				
System	>		OK Cancel	

Figura 220. Interfaz sd-wan port5 servidor Fuente: Los autores

12. Configurar la interfaz port2 en SD-WAN MEMBER que dara paso a la nube SD-WAN ISP a internet.

FortiGate VM64-I	KVM SER	vidor-sd-wan			
Dashboard	> ^	Edit SD-WAN Mer	nber		
🔆 Security Fabric	>				
 Network Interfaces DNS Packet Capture SD-WAN Zones 	× ☆	SD-WAN Zone Gateway Cost Status	WAN - ENLACE (port2) virtual-wan-link 10.10.10.1 0 Enabled Disabled		
SD-WAN Rules Performance SLA Static Routes					
Policy Routes RIP OSPF BGP Multicast					
 System Policy & Objects 	>			ОК	Cancel

Figura 221. Interfaz sd-wan port2 servidor Fuente: Los autores

13. Configurar la static routes para el servidor SD-WAN.

FortiGate VM64-K	VM SER	RVIDOR-SD-WAN			
Dashboard	> ^	Edit Static Route			
🔆 Security Fabric	>				
Network Interfaces DNS Packet Capture SD-WAN Zones	~	Dynamic Gateway Destination Interface Comments	Subnet Internet Service 0.0.0.0/0.0.0 Image: Comparison of the service SD-WAN Image: Comparison of the service Write a comment Image: Comparison of the service		
SD-WAN Rules Performance SLA Static Routes	☆	Status	• Enabled • Disabled	ОК	Cancel
Policy Routes					

Figura 222. Static routes servidor-sd wan Fuente: Los autores 14. Configurar regla para la salida a internet a las sucursales atrevez del enlace SD-WAN.

FortiGate VM64-KV	M <u>Ser</u>	VIDOR-SD-WAN			
Dashboard	> ^	Edit Policy			
🔆 Security Fabric	>				ID
Network	>	Name 🚯	INTERNET ENLACE -SD W	AN	1
System	>	Incoming Interface	🚳 virtual-wan-link	•	Las
Policy & Objects	~	Outgoing Interface	🚳 virtual-wan-link	•	N//
Firewall Policy	☆	Source	🗐 all	×	Firs
IPv4 DoS Policy			+		N/A
Addresses		Destination	I all +	×	Hit
Internet Service Database		Schedule	always	•	Act
Services		Service	ALL +	×	0
Schedules		Action	✓ ACCEPT Ø DENY		0 sec
Virtual IPs					Tot
IP Pools		Inspection Mode	How-based Proxy-based		OB
Protocol Options		Firewall / Network C	Intions		Cu
Traffic Shapers		FIREWall / INELWORK C	ptions		0.8
Traffic Shaping Policy		NAT	•		
Traffic Shaping Profile		IP Pool Configuration	Use Outgoing Interfac	e Address Use Dynamic IP Pool	
Security Profiles	>	Preserve Source Port	t 🛈		?
I VPN	>	Protocol Options	PROT default	- #	
User & Authentication	> ~			ОК	Cancel

Figura 223. Static routes servidor-sd wan Fuente: Los autores

15. Vemos que tenemos ya tráfico en la interfaz SD-WAN en el servidor.



Figura 224. Gráfica de bandwith servidor-sd wan

Fuente: Los autores

16. En la nube SD-WAN vemos que están configurada los puertos con sus respectiva VLAN'S para la comunicación con los dispositivos.

Name:	SD-WAN-ISP					
Console type:	none					-
ettings			Ports			
Port: VLAN: Type: QinQ EtherTyp	6 1 access e: 0x8100	*	Port	VLAN 2 2 4 4 6 6	Type access access access access access access access	EtherType
Ado			4			

Fuente: Los autores

- 17. Descargar Winbox para configurar los mikrotik para la red SD-WAN.
 - Link de descargar: https://mikrotik.com/download

(←) → C'	💿 🔒 https://mikrotik.com/download 🖂 🏠 🖞 🔝 🖉
	MikroTik Home About Buy Jobs Hardware Support Training Account
	Software Downloads Changelogs Download archive RouterOS The Dude Mobile app
	Upgrading RouterOS
	If you are already running RouterOS, upgrading to the latest version can be done by clicking on "Check For Updates" in QuickSet or System > Packages menu in WebFig or WinBox.
	See the documentation for more information about upgrading and release types.
	To manage your router, use the web interface, or download the maintenance utilities. Winbox to connect to your device, Dude to monitor your network and Netinstall for recovery and re-installation.
	WinBox v The Dude v Netinstall v Bandwidth Test
	WinBox 3.27 (64-bit)
	WinBox 3.27 (32-bit)

Figura 226. Descarga de winbox Fuente: Los autores

18. Abrir Winbox y nos aparecerá la mac address del mikrotik Daule).
--	----

SinBox (64bit) v3	.27 (Addresses)				_		\times
File Tools Connect To: Login: admin Password: Add/3	Set		Connect T	o RoMON Conne	V Keep P	assword) New Wir	ndow
Managed Neighbors					Find	all	₹
MAC Address	IP Address	Identity	Version	Board	Uptime		-
0C:BC:C2:2C:A8:01	fe80::ebc:c2ff.fe2c:a8	MikroTik	7.0beta8	CHR	00:02:16		
0C:BC:C2:2C:A8:01	0.0.0.0	MikroTik	7.0beta8	CHR	00:02:16		



19. Damos click en la MAC ADDRESS y en connect para ingresar a la interfaz del mikrotik-DAULE.

Connect To:	0C:BC:C2:2C:A8:0	1			✓ Keep P	assword	
Login: Password:	admin				Open Ir	n New W	indov
	Add/Set		Connect -	To RoMON	Connect		
Managed Nei	ghbors						
Refresh]				Find	all	
AC Address	/ IP Address	dentity	Version	Board	Uptime		
C:BC:C2:2C:A8	:01 fe80::ebc)	c2ff.fe2c:a8 MikroTik	7.0beta8	CHR	00:05:09		
2.00.02.20.MV	.01 0.0.0.0	PIRTO FIR	7.000180	. em	00.03.03		

Figura 228.Seleccionar mikrotik a configurar Fuente: Los autores

20. Cambiar el nombre del dispositivo system y seleccionamos identity.

Safe Mode	Session: 0C:BC:C2:2C:A8:01		
🚀 Quick Set			
CAPsMAN			
Interfaces			
Wireless			
😹 Bridge			
🛓 PPP			
° ⊺ å Mesh	Auto Upgrade		
IP 🗅	Certificates		
🛒 IPv6 🛛 🗅	Clock		
Routing N	Console		
System N	~ Disks		
Queues	Health	11-19-	
Files	History		
🗏 Log	Identity	Identity: MIKROTIK-DAULE	ОК
AP RADIUS	LEDs		Cancel
X Tools	License		
New Terminal	Logging		Apply
Make Supout rif	NTP Client		
- marce support in	NTD Conver		

Figura 229.Cambiar nombre al mikrotik Fuente: Los autores

21. Configurar la dirección IP a la interfaz del mikrotik-DAULE.

-					
Safe Mode	Session: 0C:BC:C2:2C:A8:0	1			
🏏 Quick Set					
CAPsMAN					
Interfaces					
Wireless					
👯 Bridge					
The second secon					
°∐° Mesh			Address List		
🐺 IP 🗈 🗅	ARP			Find	
🛒 IPv6 🛛 🗅	Addresses		Address 🖉 Network	Interface 🔻	
Routing N	Cloud		+ 20.20.20.2/30 20.20.20.0	ether1	
System N	DHCP Client				
Queues	DHCP Relay		Address <20.20.20.2/30>		
Files	DHCP Server		Addresse: 20.20.20.2/20		
Log	DNS		Address: 20.20.20.2/30	OK	
an RADIUS	Firewall		Network: 20.20.20.0	Cancel	
X Tools	Hotspot		Interface: ether1	Apply	
New Termina	ID				

Figura 230.1p addresses mikrotik-daule Fuente: Los autores

22. Configurar el DNS del mikrotik se ingresa el Gateway de la red SD-WAN.

Interfaces				
Wireless				
Bridge				
🛓 PPP				
°∐ <mark>°</mark> Mesh				
P N	ARP	DNS Settings		🗆 🛛
🖞 IPv6 🗈	Addresses	Servers	20.20.20.1	€ ОК
Routing 1	Cloud	Dynamic Servers		
🔯 System 🗅	DHCP Client		L	Cancel
🗣 Queues	DHCP Relay	Use DoH Server:		 Apply
Files	DHCP Server		Verify DoH Certificate	Chatta
🗒 Log	DNS			Stauc
RADIUS	Firewall		Allow Remote Requests	Cache
🔀 Tools 🛛 🗅	Hotspot	Max UDP Packet Size:	4096	
🕮 New Terminal	IPsec	Query Server Timeout	2 000	8
💫 Make Supout.rif	Kid Control	Query Tetal Treased	10.000	
🚨 Manual	Neighbors	Guery Total Timeout.	10.000	8
New WinBox	Packing	Max. Concurrent Queries:	100	
🛃 Exit	Pool	Max. Concurrent TCP Sessions:	20	
	Routes			
	SMB	Cache Size:	2048	KiB
	SNMP	Cache Max TTL:	7d 00:00:00	
	Services	Cache Used:	27 KiB	

Figura 231.DNS mikrotik-daule Fuente: Los autores

Mesh							
T P N	ARP	Route List		Route <0.0.0/0->20	0.20.20.1>		
🗐 IPv6 🛛 🗠	Addresses	Routes Nexthop	s Rules	General BGP R	IP OSPF MPLS		OK
Routing 1	Cloud			Det Address	0.0.0.0/0		Cancel
🔛 System 🗈	DHCP Client			Dat. Audreas.	0.0.000	_	
n Gueues	DHCP Relay	Dst. Addres	IS / Gateway	Gateway:	20.20.20.1		Apply
Files	DHCP Server	DAC > 20.20.2	0.0/30 ether1	Immediate Gateway:	20.20.20.1%ether1		Disable
Log	DNS			Check Gateway:		•	Commont
RADIUS	Firewall			Type	unicast	-	comment
🗙 Tools 🛛 🗋	Hotspot						Сору
Mew Terminal	IPsec			Distance:	1	▲	Remove
Make Supout.rif	Kid Control			Scope:	30	^	
Manual	Neighbors			Target Scope:	10	•	
New WinBox	Packing			VRF Interface:		•	
K Exit	Pool			Pref Source:		_	
	Routes						
	SMB			Create Time:			
	SNMP			Update Time:			
	Services	2 items out of 8		Densities of France			
	Settings			neceived From:			
	Socks			Belongs To:	Static route		
	IFIP			enabled		active	

23. Configurar la routes para la salida a internet por el enlace SD-WAN.

Figura 232. Static routes mikrotik-daule Fuente: Los autores

24. Hacer un ping a udemy para comprobar si tenemos internet dentro del router.

	admin@0C-BC-C2:	C·A8:01 (MikroTik) - WinBoy (64bit) v7 0beta8 on CHR	(~86.64)			_		×
	aurinie/0CibCiCCi	C.Adder (Wilkie Hk) - Wilbex (04bit) Wildbetab on CHK)	(x00_04)					~
Se	ssion Settings Da	shboard					 	
Ю	😋 🛛 Safe Mode	Session: 0C:BC:C2:2C:A8:01						
	🚀 Quick Set							
	CAPsMAN							
	Interfaces							
	Wireless	Terminal						
	👯 Bridge	invalid value for argument address:						+
	t = PPP	invalid value of mac-address, mac ad	ldress requir	ed				
	• Mesh	invalid value for argument ipv6-addr	ess					
	ES IP	Interrupted						
		SEQ HOST	SIZE	TTL	TIME	STATUS		
	Pouting N	0 104.16.65.85	56	52	65ms			
	Rodung P	1 104.16.65.85	56	52	566ms			
	System P	2 104.16.65.85	56	52	559ms			
	n Queues	3 104.16.65.85	50	52	SS9MS 90mg			
	📔 Files	5 104.16.65.85	56	52	63ms			
	🚊 Log	6 104.16.65.85	56	52	63ms			
X	RADIUS	7 104.16.65.85	56	52	526ms			
ğ	X Tools	8 104.16.65.85	56	52	517ms			
in	New Torminal	9 104.16.65.85	56	52	63ms			
		10 104.16.65.85	56	52	62ms			
S	Make Supout.nt	12 104.16.65.85	56	52	62ms			
Ó	Manual	13 104.16.65.85	56	52	61ms			
ā	🔘 New WinBox	14 104.16.65.85	56	52	61ms			
H	🛃 Exit	15 104.16.65.85	56	52	61ms			
2		16 104.16.65.85	56	52	62ms			_
-								•

Figura 233. Ping a udemy mikrotik-daule Fuente: Los autores **NOTA:** Para la configuración de los siguientes sucursales realizar los pasos anteriores.

RECURSOS UTILIZADOS

- > COMPUTADORA
- > CABLE DE RED (PATCHCORD)
- ➢ GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente

4.1.6. PRÁCTICA 6

Configuración de una red vpn ipsec fortigate a fortigate.

DATOS INFORMATIVOS

- > **MATERIA:** Redes de comunicación
- ➢ PRÁCTICA № 6
- > NUMERO DE COMPUTADORAS: 10
- > TIEMPO CONSIDERADO: 2 Horas

DATOS DE LA PRÁCTICA

TEMA: Configuración de una red vpn ipsec fortigate a fortigate.

OBJETIVOS

<u>General</u>

Configurar vpn's en fortigate

Específicos

- Configurar vpn ipsec
- > Configurar fortigates firewall.
- Realizar ping entre subredes.

GLOSARIO

VPN.- Red virtual privada es una tecnología que usa Internet para conectarse a un sitio determinado y de esta forma poder permitir conexión a ciertos servicios.

IPSEC.- Es un framework o colección de protocolos que operan en la capa de Red del modelo OSI y que juntos establecen una de las tecnologías más seguras y soportadas, utilizada regularmente para instaurar túneles a través de redes IP, las llamadas Redes Privadas Virtuales (VPN).

NAT.- Es manejado por los routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles, NAT es usada por las redes IPv4.

MARCO PROCIDEMENTAL



1. Diseño de la topología de la red para la práctica 6

Figura 234. Diseño de la red práctica n°6 Fuente: Los autores

FortiGate VM64-KVM	OFIC					
🚯 Dashboard	>	Edit Interface				
X Security Fabric	>	Name 🛅	port2			
🕂 Network	~	Alias	RED LOCAL			
Interfaces	☆	Туре 🔳	Physical Interface			
DNS		VRFID 0	0			
Packet Capture		Role 🚯	LAN	-		
SD-WAN Zones						
SD-WAN Rules		Address				
Performance SLA		Addressing mod	le	Manual DHCP	Auto-managed by Forti	IPAM One-Arm Sniffer
Static Routes		IP/Netmask		192.168.1.1/24		
Policy Routes		Create address	object matching subnet			
RIP		Secondary IP ad	idress 🕕			
OSPF		Administrative	Access			
BGP		IPv4				IG-Access
Multicast			□ SSH			M
System	>		RADIUS Accounting	Security Connection	Fabric ion 🚯	
Policy & Objects	>	Receive LLDP	Use VDOM Setting	nable Disable		
Security Profiles	>	Transmit LLDP	Use VDOM Setting	Enable Disable		
U VPN	>					
User & Authentication	>	O DHCP Server	er			
네 Log & Report	>	Address range	192.168.1.2-192.168.1	254		
			0			
		Netmask	255.255.255.0			
		Default gatowo	Como os latorfoco ID	inneifer		OK Cancel

2. Configurar la red local del fortigate oficina en el port2 por DHCP.

Figura 235. Configuración del port2 oficina Fuente: Los autores

3. Configurar la red local del fortigate central en port2 por DHCP.

FortiGate VM64-KVM	1 CENTRAL
🙆 Dashboard	> Edit Interface
Security Fabric Network	Name port2 Alias RED LOCAL CENTRAL
DNS Packet Capture SD-WAN Zones	Type Physical Interface VRF ID 0 Role LAN
SD-WAN Rules Performance SLA	Address Addressing mode Manual DHCP Auto-managed by FortilPAM One-Arm Sniffer
Static Routes Policy Routes RIP	IP/Netmask 192.168.10.1/24 Create address object matching subnet Secondary IP address
OSPF BGP	Administrative Access
Multicast System Policy & Objects Security Profiles VPN	IPv4 HTTPS PING FMG-Access SSH SNMP FTM RADIUS Accounting Security Fabric Connection I FMG-Access Receive LLDP I Use VDOM Setting Enable Disable Transmit LLDP I Use VDOM Setting Enable Disable
Log & Report	DHCP Server Address range 192.168.10.2-192.168.10.254
	Netmask 255.255.255.0 OK Cancel

Figura 236. Configuración del port2 central

Fuente: Los autores

4. Configurar static routes para el fortigate-oficina.

FortiGate VM64-KVM	OF	CINA	
🚯 Dashboard	>	New Static Route	
X Security Fabric	>	Dynamic Gateway 🚯 🕥	
Network Interfaces	ř	Destination 0	Subnet Internet Service
DNS Basket Capture		Gateway Address 🟮	Dynamic Specify 172.18.142.100
SD-WAN Zones		Interface Administrative Distance ()	m port1
SD-WAN Rules		Comments	Write a comment
Static Routes	☆	Status	C Enabled C Disabled
Policy Routes		Advanced Options	
RIP			OK Cancel
OSPF			
BGP			
Multicast			



5. Configuración static routes fortigate central.

FortiGate VM64-KVM	CEN	ITRAL	
🚯 Dashboard	>	Edit Static Route	
🔆 Security Fabric	>		
+ Network	*	Dynamic Gateway 😈 🔍	Subnet Named Address Internet Service
Interfaces			0.0.0/0.0.0
DNS		Interface	port1 V
Packet Capture		Gateway Address 🚯	Dynamic Specify 172.18.142.100
SD-WAN Zones		Administrative Distance 🜖	10
SD-WAN Rules		Comments	Write a comment di 0/255
Performance SLA		Status	Enabled Oisabled
Static Routes	삽		
Policy Routes		Advanced Options	
RIP			OK Carel
OSPF			UN Calicer
BGP			
Multicast			

Figura 238. Configuración static routes Central Fuente: Los autores

6. Configuracion de salida a internet a la red local.

FortiGate VM64-KVM	CEN	TRAL					
🙆 Dashboard	>	New Policy					
🔆 Security Fabric	>						
🕂 Network	>	Name 🚯	WAN CENTRAL				
System	>	Incoming Interface	RED LOCAL CENTRAL (port2)	•			
🕭 Policy & Objects	~	Outgoing Interface	🛅 port1	-			
Firewall Policy	☆	Source	😑 all	×			
IPv4 DoS Policy			+				
Addresses		Destination	i⊒ all +	×			
Internet Service Database		Schedule	G always	•			
Services		Service	ALL	×			
Schedules			+				
Virtual IPs		Action	✓ ACCEPT Ø DENY				
IP Pools		Inspection Mode	Flow based Drown based				
Protocol Options		Inspection Mode	Proxy-based Proxy-based				
Traffic Shapers		Firewall / Network O	ptions				
Traffic Shaping Policy		NAT	C				
Traffic Shaping Profile		IP Pool Configuration	Use Outgoing Interface Addre	ss Use Dynamic IP I	Pool		
Security Profiles	>	Preserve Source Port					
D VPN	>	Protocol Options	PROT default	▼ Ø			
User & Authentication	>						
Log & Report	>	Security Profiles					
		AntiVirus	0				
		Web Filter (0				
		DNS Filter			_		
						ОК	Cancel

Figura 239. Regla de internet para el fortigate Central Fuente: Los autores

7. Configurar la regla para salida a internet atravez de nuestra red local.

FortiGate VM64-KVM	OFI	CINA	
🚯 Dashboard	>	New Policy	
🔆 Security Fabric	>		
🕂 Network	>	Name 🚯	WAN
System	>	Incoming Interface	📓 RED LOCAL (port2) 🔻
Policy & Objects	~	Outgoing Interface	🖷 port1 💌
Firewall Policy	☆	Source	all ×
IPv4 DoS Policy			+
Addresses		Destination	≌all × +
Internet Service Database		Schedule	To always
Services		Service	I ALL X
Schedules			+
Virtual IPs		Action	✓ ACCEPT Ø DENY
IP Pools		Inspection Mode	Flow based
Protocol Options		Inspection Mode	How-based Proxy-based
Traffic Shapers		Firewall / Network O	Dptions
Traffic Shaping Policy		NAT	0
Traffic Shaping Profile		IP Pool Configuration	n Use Outgoing Interface Address Use Dynamic IP Pool
Security Profiles	>	Preserve Source Port	t 🕽
D VPN	>	Protocol Options	PROT default 🔻 🖋
User & Authentication	>		
네네 Log & Report	>	Security Profiles	
		AntiVirus	0
		Web Filter	0
		DNS Filter	•
			OK Cancel

Figura 240. Regla de internet para el fortigate Oficina Fuente: Los autores

8. Configurar la VPN que nos permitirá la conexión virtual al fortigate central.



Figura 241. VPN Setup en el fortigate Oficina Fuente: Los autores

9. Agregar la IP del fortigate central en remote IP address en el fortigate oficina y agregamos un cifrado siguiente ups2020.

FortiGate VM64-KVM	OF	CINA						Q+ >_ []	②• ↓ 0
🚯 Dashboard	>	VPN Creation Wizard							
🔆 Security Fabric	>	VPN Setup	uthentication > ③ Policy & Ro	uting 🔪 4 I	Review Settings				
Network	>	Remote device	IP Address Dynamic DNS			Site to Site - FortiGate			
System	>	Remote IP address	172.18.142.36						
Policy & Objects	>	Outgoing Interface	📓 port1	•				\frown	
Security Profiles	>	Authentication method	Pre-shared Key Signature				Internet	-(11)	
므 VPN	*	Pre-shared key	ups2020	Ø		1		11	
Overlay Controller VPN						This FortiGate		Remote FortiGate	
IPsec Tunnels									
IPsec Wizard	습				< Back Next	> Cancel			
IPsec Tunnel Template									
SSL-VPN Portals									
SSL-VPN Settings									
VPN Location Map									
User & Authentication	>								
Log & Report	>								

Figura 242. Remote IP address en el fortigate Oficina Fuente: Los autores

10. Agregar la IP de red local del fortigate oficina que permitirá la comunicación y en remote subnets el Gateway de la red local del fortigate central.

FortiGate VM64-KVM	OF	ICINA					Q+ >_	C ()• A 1	👤 admin+
🚯 Dashboard	>	VPN Creation Wizard								
X Security Fabric	>	VPN Setup	Authentication 3 Policy & Rou	uting	A Review Settings					
🕂 Network	>	Local interface	RED LOCAL (port2)	¥	Citata Cita EastiCat					
System	>	Local Incertace	+	î	Site to Site - Foll toda					
Policy & Objects	>	Local subnets	192.168.1.0/24				\frown			
Security Profiles	>		0			Internet	_(11))		
므 VPN	*	Remote Subnets	192.168.10.1/24		Mar.		11			
Overlay Controller VPN			0		This FortiGate		Remote FortiGat	te		
IPsec Tunnels		Internet Access	None Share Local Use Remote							
IPsec Wizard	☆									
IPsec Tunnel Template					< Back Next > Cancel					
SSL-VPN Portals										
SSL-VPN Settings										
VPN Location Map										
🌡 User & Authentication	>									
📶 Log & Report	>									

Figura 243.Policy & Routing para el fortigate Oficina Fuente: Los autores

11. Tunel ipsec fortigate oficina configurado.

FortiGate VM64-KVM	I OF	CINA								Q- >_	۵. ۲	۹۰ >_ [] @۰	٩- ٢ـ 🕄 📀 ٩- ٩-
🙆 Dashboard	>	VPN Creation Wizard											
🔆 Security Fabric	>	🕢 VPN Setup 🔪 🕢	Authentication 🖒 🕢 Policy & Routing 🔪 4 Review Se	ettings									
Network	>		<u> </u>										
System	>	The following se	ttings should be reviewed prior to creating the VPN.										
Policy & Objects	>												
Security Profiles	>	Object Summary											
모 VPN	×	Phase 1 interface	VPN-OFICINA										
Overlay Controller VPN		Local address group	VPN-OFICINA_local										
IPsec Tunnels		Remote address group	VPN-OFICINA_remote										
IPsec Wizard	☆	Phase 2 interface	VPN-OFICINA										
IPsec Tunnel Template		Static route	static										
SSL-VPN Portals		Blackhole route	static										
SSL-VPN Settings		Local to remote policies	vpn_VPN-OFICINA_local										
VPN Location Map		Remote to local policies	vpn_VPN-OFICINA_remote										
🌡 User & Authentication	>												
Log & Report	>			< Back	Create	Ca	ncel	ncel	ncel	ncel	ncel	ncel	ncel

Figura 244.. Review Settings para el fortigate Oficina Fuente: Los autores

12. Entrar en VPN tunels para ver si esta activo y nos mostrara en estado rojo.



Figura 245. Review Settings para el fortigate Oficina Fuente: Los autores

FortiGate VM64-KVM	FICINA				Q + >_ [] ③+ Д 🛛 🕗 admin+
B Dashboard >	+ Create New 🖉 Edit 🖷 Clone	Delete Search		Q	-
☆ Security Fabric >	Destination \$	Gateway IP ≑	Interface 🗘	Status 🗢	Comments ≑
+ Network ~	IPv4 3				
Interfaces	0000/0	172 18 142 100	port1	Enabled	
DNS	型 VPN-OFICINA remote		VPN-OFICINA	Enabled	VPN: VPN-OFICINA [Created by VPN wizard]
Packet Capture	VPN-OFICINA remote		Blackhole	Enabled	VPN: VPN-OFICINA [Created by VPN wizard]
SD-WAN Zones					
SD-WAN Rules					
Static Deutes					
Static Routes					
Policy Routes					
OSPE					
BGP					
Multicast					
System >					
Policy & Objects					
Security Profiles					
U VPN					
User & Authentication >					
Log & Report >					

13. En static routes se configurara automáticamente.

Figura 246. Review Settings para el fortigate Oficina Fuente: Los autores

14. Se crea las policy automáticamente en el fortigate oficina.

FortiGate VM64-KVM	OFI	CINA							Q٠	>_ []	② • Δ ● ● admin •
2 Dashboard	>	🕇 Create New 🖋 Edit 🗎 🗈	Delete Q Policy Lookup	Search			Q			Interfa	ce Pair View By Sequence
X Security Fabric	>	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Network	>	■ I RED LOCAL (port2) → por	t1 1								
System	>	WAN	all all	🗉 all	always	ALL	✓ ACCEPT	Enabled	ss. no-inspection	U UTM	08
Policy & Objects	× 	■ ED LOCAL (port2) → VP		_		-		-	·		
IPv4 DoS Policy	ч П	vpn_VPN-OFICINA_local_0	VPN-OFICINA_local	Proficina_remote	🐻 always	🖸 ALL	✓ ACCEPT	8 Disabled	59. no-inspection	🛡 ОТМ	0 B
Addresses	_	■ VPN-OFICINA → ■ RED LO	CAL (port2) 1								
Internet Service Database		vpn_VPN-OFICINA_remote_0	The VPN-OFICINA_remote	VPN-OFICINA_local	🐻 always	🛛 ALL	✓ ACCEPT	Oisabled	ss. no-inspection	🛡 UTM	0 B
Services		🗄 Implicit 1									
Schedules											
Virtual IPs											
IP Pools											
Protocol Options											
Traffic Shapers											
Traffic Shaping Policy											
Traffic Shaping Profile											
Security Profiles	>										
D VPN	>										
User & Authentication	>										
🕍 Log & Report	>										
Figura 247. Review Settings para el fortigate Oficina											

Fuente: Los autores

FortiGate VM64-KVN		NTRAL					Q+ ≻_ []	@• 4	🔹 🕗 admin •
🚯 Dashboard	>	VPN Creation Wizard							
🔆 Security Fabric	>	1 VPN Setup	Authentication 3 Bolicy & Routing 3 Breview	Settings					
Network	>	Name							
System	>	Template type	Site to Site Hub-and-Spoke Remote Access Custo	m	Site to Site - PortiGate				
Policy & Objects	>	NAT configuration	No NAT between sites				\sim		
Security Profiles	>		This site is behind NAT			Internet			
므 VPN	~		The remote site is behind NAT		11 ¹¹		II .		
Overlay Controller VPN		Remote device type	FortiGate		This FortiGate		Remote FortiGate		
IPsec Tunnels			tere Cisco						
IPsec Wizard	☆								
IPsec Tunnel Template				< Back Next >	Cancel				
SSL-VPN Portals									
SSL-VPN Settings									
VPN Location Map									
User & Authentication	>								
Log & Report	>								
Figura248.VPN Setup en el fortigate Central									

Fuente: Los autores

16. Configurar la red remota del fortigate central.



Figura 249. Remote IP address en el fortigate Central Fuente: Los autores

17. Agregar la IP de red local de l fortigate central que permitirá la comunicación y en remote subnets el Gateway de la red local del fortigate oficina.

FortiGate VM64-KVM	CE	NTRAL							Q - >_	:: @)• A 1	🕗 admin+
🚯 Dashboard	>	VPN Creation Wizard										
🔆 Security Fabric	>	VPN Setup	Authentication 3 Policy & Routing	A Review S	Settings							
Network	>	Local interface	REDLOCAL CENTRAL (port2)									
System	>	Local Internace	+				Site to Site - PortiGate					
Policy & Objects	>	Local subnets	192.168.10.0/24						\sim			
Security Profiles	>		0					Internet	_(11)	1		
III VPN	~	Remote Subnets	192.168.1.1/24				The second secon		No. 1	-		
Overlay Controller VPN			0				This FortiGate		Remote FortiGa	te		
IPsec Tunnels		Internet Access 🚯	None Share Local Use Remote									
IPsec Wizard												
IPsec Tunnel Template					< Back	Next >	Cancel					
SSL-VPN Portals												
SSL-VPN Settings												
VPN Location Map												
User & Authentication	>											
Log & Report	>											

Figura 250. IPSEC para el fortigate Central

Fuente: Los autores

18. Tunel IPSEC fortigate central configurado.

FortiGate VM64-KVM	CEI	ITRAL							🛛 🕗 admin
🍪 Dashboard	>	VPN Creation Wizard							
X Security Fabric	>	VPN Setup	Authentication 🕽 🔗 Policy & Routing 🔰 🗿 Review Se	ttings					
Network	>								
System	>	The following set	ttings should be reviewed prior to creating the VPN						
Policy & Objects	>	•							
Security Profiles	>	Object Summary							
III VPN	~	Phase 1 interface	VPN CENTRAL						
Overlay Controller VPN		Local address group	VPN CENTRAL_local						
IPsec Tunnels		Remote address group	VPN CENTRAL_remote						
IPsec Wizard	☆	Phase 2 interface	VPN CENTRAL						
IPsec Tunnel Template		Static route	static						
SSL-VPN Portals		Blackhole route	static						
SSL-VPN Settings		Local to remote policies	vpn_VPN CENTRAL_local						
VPN Location Map		Remote to local policies	vpn_VPN CENTRAL_remote						
🌡 User & Authentication	>								
Log & Report	>			< Back	Create	Cancel			

Figura 251. Review Settings para el fortigate Central Fuente: Los autores 19. Activar VPN el fortigate oficina.





20. Activar VPN en el fortigate oficina bring up.

FortiGate VM64-KVM	OFIC	CINA					Q.+ :	>_ [] @@ Δ@ 🕗 admin≁
🕸 Dashboard	*	+ Add Widget						
Status								^
Security		♦ IPsec						C C 1-
Network	1	Reset Statistics	ring Up 🔹 😌 Bring Down 🔹	Q Locate on VPN Map				
Users & Devices		Name 🗢	Remote Gateway 🗢	Peer ID ≑	Incoming Data ≑	Outgoing Data ≑	Phase 1 🗘	Phase 2 Selectors 🖨
FortiView Sources		📮 🌐 Site to Site - FortiGate	1					
FortiView Destinations		VPN-OFICINA	172.18.142.36		0 B	0.8	VPN-OFICINA	VPN-OFICINA
FortiView Applications								
FortiView Web Sites								
FortiView Policies								
FortiView Sessions								
+								
🔆 Security Fabric	>							
🕂 Network	>							
System	>							
Policy & Objects	>							
Security Profiles	>							
D VPN	>							
User & Authentication	>							
🕍 Log & Report	>							


21. En el fortigate central bring up.

FortiGate VM64-KVM	CEN	ITRAL					Q+ >.	_ [] 🛛 🗘 💶 🕘 admin
 Dashboard Security Fabric Network System 	> > >	+ Add Widget IPsec Reset Statistics	Sing Up * OBring Down *	Q Locate on VPN Map]			3 2 i-
Policy & Objects Security Profiles VPN	> > >	Name 🕈	Phase 2 Selector: VPN CENTRAL All Phase 2 Selectors TiGate 1	Peer ID 🗘	Incoming Data 븆	Outgoing Data 🗘	Phase 1 🗘	Phase 2 Selectors ≑
User & Authentication	> >	O VPN CENTRAL	. 172.18.142.35		OB	08	VPN CENTRAL	O VPN CENTRAL
				5.4				

Figura 254. Bring up en el fortigate Central Fuente: Los autores

22. Realizar ping a la red local del fortigate central.



Figura 255. Ping en el fortigate Oficina y Central Fuente: Los autores

RECURSOS UTILIZADOS

- > COMPUTADORA
- > CABLE DE RED (PATCHCORD)
- ➢ GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente

4.1.7. **PRÁCTICA** 7

Configuración de una red vpn ipsec con balanceo sd-wan.

DATOS INFORMATIVOS

- > MATERIA: Redes de comunicación
- ➢ PRÁCTICA № 7
- > NUMERO DE COMPUTADORAS: 10
- > **TIEMPO ESTIMADO:** 2 Horas

DATOS DE LA PRÁCTICA

TEMA: Configuración de una red vpn ipsec con balanceo sd-wan.

OBJETIVOS

General

Configurar balanceo SD-WAN atravez de VPN

Específicos

- Configurar vpn ipsec con fortigate.
- Realizar balanceo de la red SD-WAN con VPN.
- > Comprobar comunicación entre las subredes.

GLOSARIO

VPN.- Red virtual privada es una tecnología que usa Internet para conectarse a un sitio determinado y de esta forma poder permitir conexión a ciertos servicios.

IPSEC.- Es un framework o colección de protocolos que operan en la capa de Red del modelo OSI y que juntos establecen una de las tecnologías más seguras y soportadas.

SUBREDES.- Una subred es una categoría de direcciones lógicas. cuando una red se vuelve muy extensa, concierta dividirla en subredes.

MARCO PROCEDIMENTAL

1. Diseñar la topología de la red para la práctica 7.





2. Configurar la dirección IP en el port2 de la interfaz en el fortigate campus-1 que se usara para la SD-WAN y la VPN.

FortiGate VM64-KVN		IPUS-1			
🚯 Dashboard	> ^	Edit Interface			
Security Fabric Network Interfaces DNS Packet Capture SD.WAN Zenerc	> ~	Name port2 Alias WAN-1 Type Physic VRF ID 0 Role 0 Undefi	2 cal Interface ned		
SD-WAN Zolies SD-WAN Rules Performance SLA Static Routes Policy Routes		Address Addressing mode IP/Netmask Secondary IP address	Manual DHCP 10.10.10.2/30	Auto-managed by FortilPAM	One-Arm Sniffer
OSPF		Administrative Access			
BGP Multicast	>	IPv4] HTTPS] SSH] RADIUS Accounting	PING SNMP Security Fabric Connection	FMG-Access FTM
 Policy & Objects Security Profiles VPN 	> > >	Receive LLDP ()	Jse VDOM Setting Enables VDOM Setting Enables	able Disable able Disable	
User & Authentication	> _			ОК	Cancel

Figura 257.Configuracion IP fortigate campus1 port2 Fuente: Los autores

3. Configurar la dirección IP en el port3 de la interfaz en el fortigate campus-1 que se usara para la SD-WAN y la VPN.

FortiGate VM64-KV	M CAM	IPUS-1			
Dashboard	> ^	Edit Interface			
X Security Fabric	>	Nama	port3		
+ Network	~				
Interfaces	☆	Tuno 🕅	Physical Interface		
DNS			,		
Packet Capture		Role 6	AN	•	
SD-WAN Zones					
SD-WAN Rules		Address			
Performance SLA		Addressing mode	e	Manual DHCP Auto-manage	by FortilPAM One-Arm Sniffer
Static Routes		IP/Netmask	:	20.20.20.2/30	
Policy Routes		Create address of	object matching subnet 🕥		
RIP		Secondary IP add	dress 🗨		
OSPF					
BGP		Administrative A	CCess		
Multicast		IPv4			FMG-Access
System	>			Security Fabric	U FIM
Policy & Objects	>		RADIUS Accounting	Connection ()	
Security Profiles	>	Receive LLDP 🕄	Use VDOM Setting En	able Disable	
I VPN	>	Transmit LLDP	Use VDOM Setting En	able Disable	
User & Authentication	> _			ОК	Cancel
	Figu	ra 258.Co	nfiguracion IP f Fuente: Los a	ortigate campus1 autores	port3

4. Configurar la red local en el port4 del campus-1.

FortiGate VM64-KVM	CAMPUS-1		
😰 Dashboard	> Edit Interface	ce	
X Security Fabric	> Name	nort4	
+ Network	 Name 		
Interfaces	Allas	LAN-CAMPUS-1	
DNS	Type		
Packet Capture	Role 0		
SD-WAN Zones		onderned	
SD-WAN Rules	Address		
Performance SLA	Addressing	g mode Manual DHCP Auto-managed by FortilPAM One-Arm Sniffer	
Static Routes	IP/Netmask	ik 192.168.1.1/24	
Policy Routes	Secondary II	IP address 🕥	
RIP			
OSPF	Administrati	ative Access	
BGP	IPv4	HTTPS PING FMG-Access	
Multicast		SSH SNMP FTM	
System	>	Connection ()	
Policy & Objects	> Receive LLD	DP 1 Use VDOM Setting Enable Disable	
Security Profiles	> Transmit LLE	LDP () Use VDOM Setting Enable Disable	
- VPN		Com una	
User & Authentication	> DHCPS	Server	
Log & Report	> Address rang	inge 192.168.1.2-192.168.1.254	
		U	
	Netmask	255.255.255.0	
	Default gate	teway Same as Interface IP Specify	
		ОК	Cancel

Figura 259. Configuración red local del fortigate Fuente: Los autores

5. Configurar la VPN dentro del módulo SD-WAN.





6. Configurar la VPN para WAN-1.

FortiGate VM64-KV	м	CAN	4PUS-1						Q •	>_	13	 ۵4	🕗 admin •
Dashboard	>	^	Edit SD-WAN M	Create IPsec VPN for SD-V	WAN members								2
X Security Fabric	>		Interface	1 Authentication	2 Review Settings								
+ Network	~		Interrace	Namo	VDN SDWANI		-						
Interfaces			SD-WAN Zone	Remote device	IP Address Dynamic DN	IS							
DNS			Gateway	Remote ID address	10.10.10.1	15							
Packet Capture			Cost	Outgoing Interface	10.10.10.1		•						
SD-WAN Zones	슙			Outgoing internace	+		•						
SD-WAN Rules				Authentication method	Pre-shared Key Signatu	re							
Performance SLA				Pre-shared key	ups2020	4	Б						
Static Routes													
Policy Routes				Site to Site - FortiGate (S	D-WAN)								
RIP					Data Center								
OSPF													
BGP													
Multicast													
System	>			VPN T	unnel	、 、							
📕 Policy & Objects	>					\backslash							
Security Profiles	>				/	\backslash							
□ VPN	>			\mathcal{C}	\sim	\geq							
User & Authentication	>	~)	<u> </u>					

Figura 261. Configuracion VPN WAN 1 campus 1 Fuente: Los autores

7. Configurar la VPN para la WAN 2.



Figura 262. Configuracion VPN WAN 2 campus 1 Fuente: Los autores

8. Seleccionar las interfaces VPN configuradas en la SD-WAN.

FortiGate VM64-KV	M CAN	4PUS-1		
 Bashboard ☆ Security Fabric ◆ Network Interfaces 	>	New SD-WAN Me Interface SD-WAN Zone	WPN-SDWAN1 CQSearch VPN	
DNS Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA Static Routes Dalige Reutes	☆	Gateway Cost Status	 port1 WAN-1 (port2) WAN-2 (port3) LAN-CAMPUS-1 (port4) port5 port6 VPN-SDWAN1 VPN-WAN2 None 	Interface VPN-SDWAN1 Link O Port Speed Auto-Negotiation Type Tunnel Interface
RIP OSPF BGP Multicast				
 System Policy & Objects Security Profiles VPN 	> > > >			
User & Authentication	> 🗸			OK Cancel

Figura 263. Interfaz VPN SDWAN1 campus 1 Fuente: Los autores

FortiGate VM64-KV	M CAMP	PUS-1				Q • >	≻_ [] ⑦• 众@ 👤 admin•
Dashboard	> ^	Bandw	idth Volume Sessions				
🔆 Security Fabric	>		Do	wnload		Uploa	ad
+ Network	~			VPN-SDW	AN1		VPN-SDWAN1
Interfaces					-		
DNS							
Packet Capture							
SD-WAN Zones	☆						
SD-WAN Rules							
Performance SLA	ł	1.0					
Static Routes	4	T Cre	eate New V Boit De	lete			
Policy Routes			Interfaces ≑	Gateway ≑	Cost ≑	Download ≑	Upload ≑
RIP	6		😤 virtual-wan-link				
OSPF		•	VPN-SDWAN1	0.0.0.0	0	0 bps	0 bps
BGP		•	VPN-WAN2	0.0.0.0	0	0 bps	0 bps
Multicast							
camp	ous-1	•					

9. Visualización de las interfaces VPN dentro de la sd-wan del fortigate

Figura 264 SD-WAN Zones Campus 1 Fuente: Los autores

10. Activar las vpn para comunicación con el fg-principal.

FortiGate VM64-KVM	CAN	1PUS-1					Q•≻ [] @O	🔎 🚺 admin •
2 Dashboard	>	IPsec						C [.
Security Fabric Hetwork	> >	Reset Statistics	Bring Up O Bring	g Down 👻 🔍 🔍	Locate on VPN Map			
System	>	Name 🗢	Phase 2 Selector: VPN-SD All Phase 2 Selectors	WAN1	Incoming Data ≑	Outgoing Data 🌩	Phase 1 🗘	Phase 2 Selectors
Policy & Objects	>	📮 🌐 Site to Site - For	iGate (SD-WAN) 2					
Security Profiles	>	VPN-SDWAN1	10.10.10.1		0 B	0 B	O VPN-SDWAN1	VPN-SDWAN1
므 VPN	*	VPN-WAN2	20.20.20.1		0 B	0 B	O VPN-WAN2	VPN-WAN2
Overlay Controller VPN IPsec Tunnels IPsec Wizard IPsec Tunnel Template SSL-VPN Portals SSL-VPN Settings VPN Location Map User & Authentication	>							
Log & Report	>							
			Figura 2 Fue	265Bri ente: Lo	ng up VPN os autores	`S		

11. Crear la static routes con la dirección de red local del fg-principal.

FortiGate VM64-H	(VM CAM	MPUS-1		Q •	>_ []	?∙	۵۵	👤 admin 🕶
Dashboard	> ^	New Static Route						
🔆 Security Fabric	>							
Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Desformance SI A	~	Dynamic Gateway 🗘 🗇 Destination () Interface Comments Status	Subnet Internet Service 192.168.10.0/24 SD-WAN Write a comment Write a comment O/255 O Enabled					
Static Routes	☆		OK Cancel					
Policy Routes								

Figura 266. Stattc routes para SD-WAN fortigate campus 1 Fuente: Los autores

12. Crear las políticas para la comunicación entre VPN'S en fortigate campus-1.

FortiGate VM64-KV	M CAM	1PUS-1						Q	> []		Д1	👤 admin 🕶
8 Dashboard	> ^	New Policy										
🔆 Security Fabric	>						⑦ Documentation					^
Network	>	Name 🕚	regla-vpns				Online Help G	7				
System	>	Incoming Interface	🚳 virtual-wan-link	•			Video Tutorials	· C				
Policy & Objects	~	Outgoing Interface	LAN-CAMPUS-1 (port4)	-								
Firewall Policy	☆	Source	🗐 all	×								
IPv4 DoS Policy			+									
Addresses		Destination	i≣ all +	×								
Internet Service Database		Schedule	o always	•								_
Services		Service	₽ ALL	×								
Schedules		Action	✓ ACCEPT Ø DENY									
Virtual IPs												
IP Pools		Inspection Mode	low-based Proxy-based									
Protocol Options												
Traffic Shapers		Firewall / Network O	ptions									
Traffic Shaping Policy		NAT 🕥										
Traffic Shaping Profile		Protocol Options	PROT default	•								
Security Profiles	>	Converte Des 61a										
므 VPN	>	Security Promies		_	01/	0						~
Llear & Authentication	、 v	F ' O				Cancel						
		⊢ıgura 26	57. Firewall Po	licy	SD-WA	IN to	rtigate ca	amp	ous	1		

Fuente: Los autores

13. Política para la salida a internet de la red local del campus-1.

FortiGate VM64-KV	M <u>Ca</u>	MPUS-1				
Dashboard	> ^	New Policy				
🔆 Security Fabric	>					
Network	>	Name 🚯	INTERNET RED LOCAL			
System	>	Incoming Interface	LAN-CAMPUS-1 (port4)	•		
Policy & Objects	~	Outgoing Interface	🎯 virtual-wan-link	-		
Firewall Policy	☆	Source	🚍 all	×		
IPv4 DoS Policy			+			
Addresses		Destination	il all	×		
Internet Service Database		Schedule	lo always	•		
Services		Service	ALL +	×		
Schedules		Action	✓ ACCEPT Ø DENY			
Virtual IPs						
IP Pools		Inspection Mode	Flow-based Proxy-based			
Protocol Options						
Traffic Shapers		Firewall / Network O	ptions			
Traffic Shaping Policy		NAT 🔿				
Traffic Shaping Profile		Protocol Options	PROT default	▼ Ø		
Security Profiles	>					
	>	Security Profiles				
Liser & Authentication	> v				OK	Cancel

Figura 268. Firewall Policy Intternet red local fortigate campus 1 Fuente: Los autores

14. Configurar la interfaz port2 en el fg-principal.

FortiGate VM64-KV	M FG-	PRINCIPAL			
Dashboard	> ^	Edit Interface			
🔆 Security Fabric	>	Mana	nort2		
Network	~	Name			
Interfaces	☆	Alias	WAN-1		
DNS		Type			
Packet Capture		VRF ID	0		
SD-WAN Zones		Role 1	WAN	•	
SD-WAN Rules		Estimated bandwidth ()	0	k	bps Upstream
Performance SLA			0	k	bps Downstream
Static Routes		Δddress			
Policy Poutes		Addressing made	Manual DUICD	Nuter an and her Contil	DANA
Poncy Routes		Addressing mode	Manual DHCP	Auto-managed by Forth	PAM
RIP OCDE		IP/Netmask	10.10.10.1/30		
OSPF		Secondary IP address			
BGP		Administrative Access			
Multicast		Administrative Access			
System	>	IPv4	HTTPS		FMG-Access
Policy & Objects	>			Security Fabric	
Security Profiles	>		CADIOS Accounting	Connection 🕄	
□ VPN	>	Receive LLDP () Us	e VDOM Setting Enab	Disable	
User & Authentication	> 、				OK Cancel

Figura 269.Configuracion interfaz port2 fortigate fg-principal Fuente: Los autores

15. Configurar port3 en el fg-principal para la WAN-2.

	> ^	Edit Interface			
Security Fabric	>				
Network	~	Name	im port3		
Interfaces	~	Alias	WAN-2		
DNG	м	Туре	Physical Interfac	e	
DNS		VRF ID 0	0		
Packet Capture		Role 🚯	WAN	•	
SD-WAN Zones		Estimated bandwidt	:h 🚯 🛛 0	kbp	s Upstream
SD-WAN Rules			0	kbp	s Downstream
Performance SLA					
Static Routes		Address			
Policy Routes		Addressing mode	Manual DHCP	Auto-managed by FortilPA	M
RIP		IP/Netmask	20.20.20.1/30		
OSPF		Secondary IP addres	ss 🕥		
BGP					
Multicast		Administrative Acce	ess		
System	>	IPv4	HTTPS	PING	FMG-Access
Policy & Objects	>		SSH SSH		FTM
Security Profiles	>		RADIUS Accounting	Connection (1)	
, VPN	>	Receive LLDP ()	Use VDOM Setting Ena	ble Disable	
User & Authentication	>	-			Canad

Fuente: Los autores

16. Configurar el port4 para la red local del fg-principal.

FortiGate VM64-KVM	FG-PRINCIPAL
🚯 Dashboard	> Edit Interface
 Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules 	Name Dort Alias LOCAL Type Physical Interface Type Physical Interface VRF ID 0 Role LAN
Performance SLA Static Routes	Addressing mode Manual DHCP Auto-managed by FortilPAM One-Arm Sniffer IP/Netmask 192.168.10.1/24
RIP	Secondary IP address
BGP	Administrative Access
Multicast	IPv4
 System Policy & Objects Security Profiles VPN 	> SSH SNMP FIM > RADIUS Accounting Security Fabric Connection • > Receive LLDP • Use VDOM Setting Enable > Transmit LLDP • Use VDOM Setting Enable
User & Authentication	> DHCP Server
Log & Report	Address range 192.168.10.2-192.168.10.254 • • Netmask 255.255.255.0
	OK Cancel

Figura 271.Configuracion IP fortigate principal port4 Fuente: Los autores



17. Configurar la VPN que pertnece a la WAN-1.

Figura 272. Configuracion VPN WAN 1 principal Fuente: Los autores

18. Configurar la VPN que pertenece a la WAN-2.

FortiGate VM64-KVM	FG-I	PRINCIPAL						Q -	>_	0	? -	۵۵	👤 admin+
🚯 Dashboard	>	Edit SD-WAN Men	nber	Create IPsec VPN for SD-V	VAN members								×
X Security Fabric	>	Interface		1 Authentication	2 Review Settings								^
+ Network	~	SD-WAN Zone	Q Search	Name	VPN-WAN2								
Interfaces			m port1	Remote device	IP Address Dynamic DNS	S							
DNS		Cost	. WAN-1 (port2)	Remote IP address	20.20.20.2								
Packet Capture			WAN-2 (port3)	Outgoing Interface	MAN-2 (port3)	×							
SD-WAN Zones	☆		LOCAL-FG (port port5		+								
SD-WAN Rules			m port6	Authentication method	Pre-shared Key Signatur	e							
Performance SLA			VPN-WAN1	Pre-shared key	ups2020	Þ							
Static Routes			None										
Policy Routes				Site to Site - FortiGate (S	D-WAN)								
RIP					Data Center								
OSPF													
BGP													
Multicast													
System	>			VPN T	unnel 🔶 🔪	、 、							
Policy & Objects	>					\backslash							
Security Profiles	>					\backslash							
L VPN	>			\Box			`						
User & Authentication	>)						
Log & Report	>				9		/						
				This Fo	rtiGate	Devices							

Figura 273. Configuracion VPN WAN 2 principal Fuente: Los autores

19. Asignar las VPN a la SD-WAN

Dashboard	>	Edit SD-WAN Mer	nber				
Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA Static Routes	> ~ ☆	Interface SD-WAN Zone Gateway Cost Status	VPN-WAN1 Search VPN-WAN1 WAN-1 (port2) WAN-2 (port3) LOCAL-FG (port4) port5 port6 VPN-WAN1 VPN-WAN1	• • VPN	Interface Link Port Speed Type	VPN-WAN1 Auto-Negotiation Tunnel Interface	
Policy Routes			None				
RIP OSPF BGP Multicast							
System	>						
Policy & Objects Security Profiles	>					ОК	Cano

Figura 274. Interfaz VPN SDWAN1 princpal Fuente: Los autores

20. Visualizar las VPN configuradas en la sd-wan del fg-principal.

FortiGate VM64-KV	VM FG-	PRINCIP	AL			c	λ• ≻ [] @• Δ္0 🕗 admin•
🚯 Dashboard	>	Bandy	vidth Volume Sessions				
X Security Fabric	>		Dow	rnload		Upload	
+ Network	~			VPN-WAN1			VPN-WAN1
Interfaces				VENTANZ			VEN-WANZ
DNS							
Packet Capture							
SD-WAN Zones	☆						
SD-WAN Rules							
Performance SLA		_					
Static Routes		+ Ci	reate New • / / Edit 📋 Delete				
Policy Routes			Interfaces ≑	Gateway 🖨	Cost ≑	Download 🌩	Upload 🗘
RIP			🎕 virtual-wan-link				
OSPF		• • • •	VPN-WAN1	0.0.0.0	0	0 bps	0 bps
BGP			VPN-WAN2	0.0.0.0	0	0 bps	0 bps
Multicast							

Figura 275. SD-WAN Zones Principal Fuente: Los autores 21. Activar las VPN'S para comunicación entre las interfaces.

FortiGate VM64-KVM	FG-F	PRINCIPAL					٩. >_	[] 💿 🗘 🚺 👤 admin•
🍘 Dashboard	>	IDeee						
🔆 Security Fabric	>	IPSec						
Network	>	Reset Statistics	O Bring Up • O Bring Dov	wn * Q Locate	on VPN Map			
System	>	Name 🗢	Phase 2 Selector: VPN-WAN1	Peer ID ≑	Incoming Data ≑	Outgoing Data 🌲	Phase 1 🖨	Phase 2 Selectors ≑
📕 Policy & Objects	>	🕒 🌐 Site to Site - Fo	rtiGate (SD-WAN) (2)					
Security Profiles	>	O VPN-WAN1	10.10.10.2		0 B	0 B	O VPN-WAN1	O VPN-WAN1
L VPN	~	O VPN-WAN2	20.20.20.2		0 B	0 B	VPN-WAN2	O VPN-WAN2
Overlay Controller VPN								
IPsec Tunnels								



22. Gráfico de VPN'S activadas.

FortiGate VM64-KVM	FG	PRINCIPAL		Q.	≻_ [] @+ 🎝 🖲 🧶 admin+
🚯 Dashboard	>	+ Create New • & Edit 🗎 Delete Sr	earch	Q	
X Security Fabric	>	Tunnel	Interface Binding	Ctatus A	Dof A
Network	>	Tunner 🗸	Internace binding +	Status 👳	Rei. 👳
System	>	Site to Site - FortiGate (SD-WAN) 2			
Policy & Objects	>	O VPN-WAN1	WAN-1 (port2)	O Up	2
Security Profiles	>	O VPN-WAN2	WAN-2 (port3)	O Up	2
😐 VPN	•				
Overlay Controller VPN					
IPsec Tunnels	☆				
IPsec Wizard					
		Figura 2	277 VPN `S princip	al activadas	

Fuente: Los autores

23. Crear static routes para la comuniacion de la red local del fg-principal con el campus-1.

FortiGate VM64-KVM		PRINCIPAL		53	40	🕗 admin -
🚯 Dashboard	>	New Static Route				
X Security Fabric	>					
Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules	~	Destination ● Submet Internet Service 192.168.1.0/24 Interface ● SD-WAN ● Comments Write a comment				
Static Routes	☆	OK				
Policy Routes RIP						

Figura 278. Stattc routes para SD-WAN fortigate fg-principal Fuente: Los autores

FortiGate VM64-KVM	FG	PRINCIPAL						٩.	>_	: @-	40	👤 admin+
🚯 Dashboard	>	New Policy										
🔆 Security Fabric	>						⑦ Documentation					^
Network	>	Name	regla vpn's				Online Help C					
System	>	Incoming Interface	virtual-wan-link	•			Video Tutorials 🗹					
Policy & Objects	~	Outgoing Interface	LOCAL-FG (port4)	•								
Firewall Policy	☆	Source	🗉 all	×								
IPv4 DoS Policy			+									
Addresses		Destination	all +	×								
Internet Service Database		Schedule	lo always	•								
Services		Service	ALL	×								
Schedules			+									
Virtual IPs		Action	✓ ACCEPT Ø DENY									
IP Pools			Flue based - Deve based									
Protocol Options		Inspection Mode	Flow-based Proxy-based									
Traffic Shapers		Firewall / Network O	Intions									
Traffic Shaping Policy		NAT										
Traffic Shaping Profile		Protocol Ontions	PROT default									
Security Profiles	>		deradic .	6								
III VPN	>	Security Profiles										
User & Authentication	>	AntiVirus	•									
Lull Log & Report	>	Web Filter	•									
					ОК	Cancel						Ŷ

Figura 279. Firewall Policy SD-WAN fortigate fg-principal 1 Fuente: Los autores

FortiGate VM64-KVM	FG-	PRINCIPAL				Q + >_	[] @·	40	🕗 admin+
🚯 Dashboard	>	New Policy							
🔆 Security Fabric	>				⑦ Documentation				^
🕂 Network	>	Name 🕚	internet red local		🗐 Online Help 🕜				
System	>	Incoming Interface	LOCAL-FG (port4)		Video Tutorials 🗹				
Policy & Objects	~	Outgoing Interface	🚳 virtual-wan-link 🔹]					
Firewall Policy	☆	Source	🗉 all 🛛 🗙						
IPv4 DoS Policy			+						
Addresses		Destination	≌ali X						
Internet Service Database		Schedule	🔽 always 🗸						
Services		Service	ALL ×						
Schedules			+						
Virtual IPs		Action	✓ ACCEPT Ø DENY						
IP Pools			Flow based Draws based						
Protocol Options		Inspection Mode	Flow-based Proxy-based						
Traffic Shapers		Firewall / Network O	ptions						
Traffic Shaping Policy		NAT							
Traffic Shaping Profile		Protocol Ontions	PROT default	1					
Security Profiles	>	Trouses Options	delaur	•					
D VPN	>	Security Profiles							
User & Authentication	>	AntiVirus	0						
Log & Report	>	Web Filter							
			-	OK Cancel					v

25. Politica para salida a internet red local.

Figura 280. Firewall Policy Internet red local fortigate fg-principal Fuente: Los autores

26. Politica para navegación de internet para la SD-WAN.

Dashboard	> ^	Edit Policy			
Security Fabric	>				
• Network	>	Name 🚯	internet-sdwan		
System	>	Incoming Interface	🗟 virtual-wan-link	•	
Policy & Objects	~	Outgoing Interface	m port1	•	
Firewall Policy	☆	Source	🖃 all	×	
IPv4 DoS Policy			+		
Addresses		Destination	⊒ all +	×	
Internet Service		Schedule	always	•	
Services		Service	ALL +	×	
Schedules		Action	✓ ACCEPT Ø DENY		
Virtual IPs					
IP Pools		Inspection Mode	Flow-based Proxy-based		
Protocol Options					
Traffic Shapers		Firewall / Network C	Options		
Traffic Shaping Policy		NAT			
Traffic Shaping Profile		IP Pool Configuration	Use Outgoing Interface	Address Use Dynamic	IP Pool
Security Profiles	>	Preserve Source Por	t 🗇		
		Protocol Options	PROT default	▼ 🖋	

Figura 281. Firewall Policy Internet SD-WAN fortigate fg-principal Fuente: Los autores

27. Configurar static routes de la SD-WAN en el fortigate campus-1.

FortiGate VM64-H	CVM can	npus-1				C	- ×_	0	 ۵۵	🕗 admin 🕶
Dashboard	> ^	Edit Static Route								
Security Fabric		Dynamic Gateway 🕄 🔾								
Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules		Destination 0 Interface Comments Status	Subnet Internet Service 0.0.0.0/0.0.0 Image: Comparison of the service SD-WAN Write a comment O Enabled O Disabled	▼ 						
Performance SLA Static Routes	☆			ОК	Cancel					
Policy Routes										

Figura 282. Configuracion static routes SD-WAN campus1 Fuente: Los autores

28. Ping entre red locales de cada fortigate y google.



Figura 283 Ping en el fortigate campus y fg-primcipal Fuente: Los autores

RECURSOS UTILIZADOS

- > COMPUTADORA
- CABLE DE RED (PATCHCORD)
- > GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente

4.1.8. PRÁCTICA 8

DATOS INFORMATIVOS

- > MATERIA: Redes de comunicación
- PRÁCTICA Nº 8
- > NUMERO DE COMPUTADORAS: 10
- > **TIEMPO CONSIDERADO:** 2 Horas

DATOS DE LA PRÁCTICA

TEMA: Configuración de un failover con mikrotik para un enlace SD-

WAN.

OBJETIVOS

General

Configurar un failover con mikrotik para un enlace SD-WAN.

Específicos

- > Configurar Failover con mikrotik.
- Establecer un fortigate WAN.
- > Comprobar la comunicación del Failover.

GLOSARIO

FAILOVER.- También llamada conmutacion por error el cual funciona como un respaldo, cuando se presenta un fallo en unas de nuestras redes WAN este entra a funcionar de manera automática, asi no se vera afectado nuestros dispositivos finales.

WAN.- Se la conoce también como red de área amplia, se compone de varias redes LANS ubicadas alrededor del globo terráqueo.

ISP.- Son siglas usadas en telecomunicaciones y su definición es Internet Service provider el cual prorpociona de una compañía servicio de internet como por ejemplo Claro, Telconet, Telefonica.

MARCO PROCEDIMENTAL

1. Diseñar la topología de la red para la práctica 8.



Figura 284. Diseño de la red práctica Nº8 Fuente: Los autores

2. Configurar el port2 del fortigate WAN para el enlace FAILOVER al

mikrotik.

FortiGate VM64-K	VM FG	WAN		2 👤 admin
Dashboard	> ^	Edit Interface		
 ☆ Security Fabric ▲ FortiView ◆ Network Interfaces DNS 	> > ☆	Interface Name Alias Link Status Type Estimated Bandwidth ()	port2 (0C:C8:A2:F3:83:01) WAN-MIKROTIK Up Physical Interface 0 kbps Upstream 0 kbps Downstream	
Packet Capture SD-WAN SD-WAN Rules		Tags Role 1 WAN	· · · · ·	
Static Routes		O A	dd Tag Category	
RIP OSPF BGP		Addressing mode Man IP/Network Mask 40.4	ual DHCP 0.40.1/255.255.255.252	
Multicast	- 1	Administrative Access		
 System Policy & Objects Security Profiles 	> > >	IPv4 Ø HT Ø SS □ RA Receive LL DP 1 Use	TPS	
	、 v	Notelive LEDF 😈 USE	OK Cancel	

Figura 285.Configuracion IP fortigate FG-WAN port2 Fuente: Los autores.

- FortiGate VM64-KVM FG-WAN > ^ Edit Static Route Dashboard 🔆 Security Fabric > Subnet Internet Service Destination 🜖 📥 FortiView > 0.0.0/0.0.0.0 + Network Interface 🔳 port1 -Interfaces Gateway Address 🜖 Dynamic Specify 172.18.142.100 DNS Administrative Distance 🚯 10 Packet Capture Write a comment... Comments .:: 0/255 SD-WAN • Enabled • Disabled Status SD-WAN Rules Performance SLA Advanced Options Static Routes Cancel Policy Routes RIP OSPF
- 3. Configurar la static routes al FG-WAN.

Figura 286.	Configuración static routes FG-WAN po	ort 1
	Fuente: Los autores	

4. Configurar la regla en el firewall para salida de internet a la WAN para mikrotik.

FortiGate VM64-KV	/M <u>FG</u>	-WAN						0 - Δ0	👤 admin
Dashboard	> '	Edit Policy							
🔆 Security Fabric	>					ID			
E FortiView	>	Name 🚯	WAN-MIKROTIK			1			
Network	>	Incoming Interface	WAN-MIKROTIK (port2)	•		Active sessions			
System	>	Outgoing Interface	🔚 port1	•		0			
Policy & Objects	~	Source	🗉 all	×		O second(s) ago	now		
IPv4 Policy	☆		+			Total bytes			
Authentication Rules		Destination	i≣ all +	×		OB			
IPv4 DoS Policy		Schedule	lo always	•		Current bandwidth			
Addresses		Service	ALL	×		0 B/s			
Wildcard FQDN Addresses		Action	+ ACCEPT Ø DENY						
Internet Service Databas	se								
Services		Inspection Mode	Flow-based Proxy-based						
Schedules	- 1					Video Tutorials	5		
Virtual IPs		Firewall / Network O	ptions						
IP Pools		NAT							
Protocol Options		IP Pool Configuration	Use Outgoing Interface	Address Use Dynamic	IP Pool				
Traffic Shapers		Preserve Source Port							
Traffic Shaping Policy		Protocol Options	PRX default	- /	_				
Q				OK	Cancel				
		Figura	287. Configu	iracion Po	olicy FG·	-WAN port	1		
		C C	Fuen	te: Los au	tores				

5. Abrir winbox y seleccionar el routerboards que vamos a configurar el faiolver.

Sine VinBox v3.27 (Addresses) File Tools				_		×
Connect To: 0C:C8:A2:E3:6B:00				✓ Keep F	assword	
Login: admin				Open l	n New Wir	ndow
Password						
Add/Set		Connect T	o RoMON Conne	ect		
Managed Neighbors						
T Refresh				Find	all	₹
MAC Address / IP Address	Identity	Version	Board	Uptime		-
0C:C8:A2:E3:6B:00 fe80::ec8:a2ff.fee3:6b	. MikroTik	7.0beta8	CHR	00:01:46		
0C:C8:A2:E3:6B:00 0.0.0.0	Mikro Tik	7.0beta8	CHR	00:01:46		
2 items (1 selected)						

Figura 288. Elección del Routerboard para failover Fuente: Los autores

6. Damos click en IP- ADDRESS y en la cruz azul agregamos la IP del ISP-1 a la eth1.

Bridge		Addre	ess List		
🛓 PPP					Find
°∏° Mesh		-			FIND
📴 IP 🛛 🗅	ARP		Address / Network	Interfac	e 🔻
🛒 IPv6 🛛 🗅	Addresses		1/2.10.142.30 1/2.10.142.0	eutert	
Routing D	Cloud				
🔯 System 🗅	DHCP Client				
🙅 Queues	DHCP Relay		Address <1/2.18.142.50/24>		
Files	DHCP Server		Address: 172.18.142.50/24		OK
🗒 Log	DNS		Network: 172.18.142.0]▲ [Cancel
RADIUS	Firewall		Interface: ether1	TT -	
🔀 Tools 🛛 🗅	Hotspot				Apply
🔤 New Terminal	IPsec				Disable
Nake Supout.rif	Kid Control				Comment
🖳 Manual	Neighbors				Comment
New WinBox	Packing				Сору
Exit	Pool	1 item			Remove
	Routes		enabled		
	SMR		enabled		

Figura 289.Añadir IP para ISP1-ethe1 Fuente: Los autores 7. Agregar la IP a la eth2 del fortigate WAN que nos simulara de ISP.



Figura 290.Añadir IP para ISP1-ethe2 Fuente: Los autores

8. Agregar los DNS al router mikrotik se puede usar los de google o del router local.

				_	
🚀 Quick Set					
CAPsMAN					
Interfaces					
Wireless					
Bridge					
🏣 PPP					
°∏ <mark>°</mark> Mesh		DNS Settings			
👪 IP 🗈	ARP	Sonrom:	172 19 142 100		
🛫 IPv6 🛛 🗅	Addresses	Jerveis.	1/2.10.142.100	Ţ	UK
Routing	Cloud		8.8.8.8	Ŧ	Cancel
🔯 System	DHCP Client		8.8.4.4	ŧ	Apply
🗣 Queues	DHCP Relay	Dynamic Servers:			
Files	DHCP Server	Lies Doll Server		-	Static
🗐 Log	DNS	Use Don Jerver.		•	Cache
RADIUS	Firewall		Venty DoH Certificate		
🗙 Tools 🛛 🗅	Hotspot		Allow Remote Requests		
🔤 New Terminal	IPsec	Max UDP Packet Size:	4096		
Make Supout.rif	Kid Control			-	
Manual	Neighbors	Query Server Timeout:	2.000	S	
New WinBox	Packing	Query Total Timeout:	10.000	s	
🛃 Exit	Pool	Mar Carried Ourier	100	_	
	Routes	Max. Concurrent Queries:	100	=	
	SMB	Max. Concurrent TCP Sessions:	20		
	SNMP	Cache Size:	2048	КiВ	
	Services	Cache May TTL:	74.00:00:00	_	
	Settings		70.00.00	-	
	Socks	Cache Used:	27 NB		

Figura 291. Añadir DNS a router Mikrotic Fuente: Los autores

9. Configurar en FIREWALL opción NAT para la salida de internet del eth1.

Ses	ion Settings Das	npoard		
Ŋ	C Safe Mode	Session: 0C:C8:A2:E3:6B:00		
	🖌 Quick Set		NAT Rule <172.18.142.0/24>	Shadow Mo
	CAPsMAN		General Advanced Extra Action Statistics	ОК
	Interfaces		Chain: Internet	Cancel
	Wireless	Address L		Cancer
	Bridge	+ -	Src. Address: 172.18.142.0/24	Apply
	PPP	Addre	Dst. Address:	Disable
	Mesh	÷ 10	Protocol:	Comment
	E IPv6	4	Src. Port:	Carry
	Routing N	• 1	Dst. Port:	Сору
	System		Any, Port:	Remove
	Queues		h. Interface:	Reset Counters
	Files		Out Interface: ether1	Reset All Counters
	Log			
	RADIUS		In. Interface List:	
	🔀 Tools 🛛 🗅		Out. Interface List:	
	Mew Terminal		Packet Mark:	
	Make Supout.rif		Connection Made	
	Manual			
	New WinBox	4 items (1	Routing Mark:	
	🛃 Exit		Routing Table:	
			Connection Type:	

Figura 292.Configuracion de Firewall ethe 1 (a) Fuente: Los autores

Session Settings Dashboard		
Safe Mode Session: 0C:C8:A2:E3:6B:00		
🔀 Quick Set	NAT Rule <172.18.142.0/24>	Sha
CAPsMAN	General Advanced Extra Action Statistics	OK
Interfaces		
♀ Wireless	Address Action: masquerade	Cancel
💢 Bridge		Apply
🛓 PPP	Add Lon Device	2.11
°[, Mesh		Disable
🐺 IP 🗅 Firewall	To Ports:	Comment
💯 IPv6 🗅 Ditor Pulso NA	T Mar	Сору
Routing N Nite Tules 1.0		Demons
💭 System 🗅 🕂 🛨 🗸		nemove
🗣 Queues # Action	Chain	Reset Counters
Files 0 t mas.	sronal	Reset All Counters
Log	SICTId	
and RADIUS		

Figura 293.Configuracion de Firewall ethe 1 (b) Fuente: Los autores 10. Configurar en FIREWALL opción NAT para la salida de internet del eth2.

🚀 Quick Set	Frewal		
CAPsMAN	Filter Bules NAT Mannle		
🛤 Interfaces	NAT Rule <40.40.40.0/30>		
Wireless	+ - Katistics General Advanced Extra Action Statistics		ОК
Bridge	# Action Chain Chain Chain Chain	Ē	Capped
🏣 PPP			Cancer
°T <mark>°</mark> Mesh	2 t mas sonat Src. Address: 40.40.40.0/30	•	Apply
🐺 IP 🛛 🗅	3 1 mas srcnat Dst. Address:	•	Disable
🐺 IPv6 🛛 🗅	Protocol:	-	
Routing D		_	Comment
🔯 System 🗈	Sic. roit.	Ť	Сору
🙅 Queues	Ust. Port:	•	Remove
📔 Files	Any. Port:	•	
🗒 Log	In. Interface:	•	Reset Counters
ar RADIUS	Out. Interface: ether2		Reset All Counters
🗙 Tools 🛛 🗅			
🔤 New Terminal	In. Interface List:	•	
📐 Make Supout.rif	Out. Interface List:	•	
🖻 Manual	e rems (i selected) Packet Mark	-	

Figura 294.Configuracion de Firewall ethe 2 (a) Fuente: Los autores





11. Configurar la NAT para la WAN-1 para los enlaces SD-WAN.

Session Settings Dashboard		
Safe Mode Session: 0C:C8:A2:E	E3:6B:00	
V Quick Set Firewall	NAT Rule <10.10.10.0/30>	
CAPsMAN Filter Rules NAT	Mangle General Advanced Extra Action Statistics	ОК
m Interfaces		Cancel
Wireless 4	Chain Srn Addrese: 10.10.0/20	
+ ppp 0 1 mas	srcnat	Арріу
• Mach	srcnat	Disable
2 mas	srchat Protocol:	Comment
	Src. Port:	Conv
Routing N	Dst. Port:	Сору
🔯 System 🗅	Any. Port:	Remove
🙊 Queues	In. Interface:	Reset Counters
Files	Out. Interface:	Reset All Counters
🗒 Log		-
ap RADIUS	In. Interface List:	
🔀 Tools 🗈	Out. Interface List:	
Mew Terminal	Packet Mark:	
Make Supout.rif 4 items (1 selected)		
Manual	De des Medu	
Vew WinBox		
Exit	Routing Table:	
	Connection Type:	



Session Settings Dashboard								
Safe Mode	Session: 0C:C8:A2:E3:6B:00							
🏏 Quick Set	Firewall	NAT Rule <10.10.10.0/30>						
CAPsMAN	Filter Rules NAT Mangle	General Advanced Extra Action Statistics	ОК					
Interfaces								
Wireless	+ - / X 🗅	Action: masquerade	Cancel					
💥 Bridge	# Action Chain		Apply					
🏣 PPP	0 1 mas srcnat							
1 Mesh	2 mas srcnat		Disable					
IP N	3 amas srcnat	To Ports:	Comment					
IPv6			Сору					
Routing 1								
🔯 System 🗅			Hemove					
🙅 Queues			Reset Counters					
Files			Reset All Counters					
🗏 Log								
ar RADIUS								

Figura 297. Configuracion NAT para WAN 1 (b) Fuente: Los autores

2 Safe Mode Session: (DC.CB.42/E3.68:00) CArbsMAN Filter Rules NAT Made <20.00 // 00/00	Session Settings Das	shboard			
Quick Set Feendl NAT Rule <20 20 20 0/30> CAPsMAN Filter Rules NAT Manpe Interfaces Imassront General Advanced Exta Action Statistics Wretess Imassront	Safe Mode	Session: 0C:C8:A2:E3:6B:00			
CAPsMAN Fiter Rules NAT Margie Wrieless Image: Second in the faces PPP 0 1 Image: Second in the faces 2 Umage: Second in the faces 3 Umage: Second in the faces 4 Convection Mark: 2 New WinBox 2 Exit Connection Type: Connection Type: Conne	🚀 Quick Set	Firewall	NAT Rule <20.20.0/30>		
Interfaces Wreekes Wreekes Wreekes PPP 0 Imassroat 1 1 Imassroat 2 1 Mesh 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	CAPsMAN	Filter Rules NAT Mangle	General Advanced Extra Action Statistics		OK
Wreless Image <	Interfaces			-	Canad
# Action Chain Src. Address: [20.20.0/30] Apply # PPP 1 Imassrcnat Protocol: Imassrcnat Imassrcnat # IPv6 N 2 Imassrcnat Protocol: Imassrcnat Imassrcsrcnat Imassrcsrcsrcsrcsrcsrcsrcsr	Wireless			•	Cancer
PPP U U masstroat Mesh 2 U masstroat Wesh 2 U masstroat PP 0 U masstroat P 1 U masstroat P P 1 <th1< th=""> <th1< th=""> <th1< th=""></th1<></th1<></th1<>	Bridge	# Action Chain	Src. Address: 20.20.20.0/30	•	Apply
Mesh 2 1 mas sronat IP P 3 Imas sronat IP P 1 System Image: System Image: System Image: System	The PPP	1 mas srcnat	Dst. Address:	•	Disable
Igs IP N 3 Imas stonat Incoded Comment Igs IP 6 N Src. Poit. Image: Src.	"[" Mesh	2 🕴 mas srcnat	Protocol	•	Diddio
IPv6 N Roting N System N Outures N Iteration V RADIUS V Nake Suport if V Make Suport if V Make Suport if Feet All Counters Packet Mark: V Connection Mark: V Routing Table: V Connection Type: V	🍄 IP 🗈 🗅	3 🕴 mas srcnat			Comment
Roting P Queues Any. Pot: Queues In. Inteface: Is Queues Is In. Inteface: Out. Inteface: In. Inteface: Out. Inteface: In. Inteface: Out. Inteface: In. Inteface: In. Inteface: In. Inteface: Out. Inteface: In. Inteface: In. Inteface: In. Inteface: In. Inteface: In. Inteface: In. Inteface: In. Inteface: Out. Inteface: In. Inteface: In. Inteface: In. Inteface: In. Inteface: Inteface:	🖞 IPv6 🗈		Src. Port:	•	Сору
System New Yet Queues In. Interface: In. Interface: In. Interface: Out. Interface: Interface: Out. Interface: Interface: In. Interface: Interface:	Routing N		Dst. Port:	•	Remove
Queues In. Inteface: In: Preset Counters Preset Counters Is page In: Inteface: In: Inteface: Preset Counters Preset Counter	j⊇ System ト		Any, Port:	•	
Files Out. Inteface: I Log I Manual I Soting Mark: Routing Table: <	🙅 Queues		In. Interface:	•	Reset Counters
I Dg ▲P RADIUS ▲ RADIUS ▲ Tools ► Make Supoutri ▲ Manual ▲ Manual ▲ Atems (1 selected) Connection Mark: ■ Routing Table: ■ Connection Type:	Files		Out. Interface:	•	Reset All Counters
A PADIUS In. Interface List: ✓ X Tools Make Suport if Make Suport if ✓ Make Suport if 4 #ems (1 selected) Connection Mark: ✓ Markal Fouting Mark: Markal Fouting Table: Connection Type: Connection Type:	Log			_	
Y Tools P New Terminal Packet Mark: Markal 4 tems (1 selected) Markal Connection Mark: New WinBox Routing Mark: E bit Routing Table: Connection Type: V	RADIUS		In. Interface List:	•	
Image: Support of Make Support	🗙 Tools 🛛 🗅		Out. Interface List:	•	
Make Supout if Manual 4 items (1 selected) Connection Mark:	🔤 New Terminal			-	
Manual 4 tems (1 selected) Connection Mark: <	Nake Supout.rif		Packet Mark:	•	
New WinBox Routing Mark: Exit Routing Table: Connection Type:	Manual	4 items (1 selected)	Connection Mark:	•	
Exit Routing Table:	🔘 New WinBox		Routing Mark:	•	
Connection Type:	🛃 Exit		Routing Table:	•	
			Connection Type:	•	

12. Configurar la NAT para la WAN-2 para los enlaces SD-WAN.



Session Settings Da	shboard							
Safe Mode	Image: Safe Mode Session: (0C.C8:A2:E3:6B:00)							
🏏 Quick Set	Firewall	NAT Rule <20.20.20.0/30>						
CAPsMAN	Filter Rules NAT Mangle	General Advanced Extra Action Statistics	ОК					
Interfaces			Canad					
Wireless		Action: Imasquerade	Cancel					
💥 Bridge	# Action Chain		Apply					
🛓 PPP	1 mas srcnat							
°∐ <mark>°</mark> Mesh	2 mas srcnat	Log Pleix.	Disable					
🐺 IP 🗈 🗅	3 🎽 mas srcnat	To Ports:	Comment					
🐺 IPv6 🛛 🗅			Сору					
Routing 1	-		Remove					
🔯 System 🗅								
🙅 Queues			Reset Counters					
Files			Reset All Counters					
🗒 Log								
2 RADIUS								
	F	igura 200 Configuracion NAT para M/AN 2 (b)						

Figura 299.Configuracion NAT para WAN 2 (b) Fuente: Los autores 13. Configurar la routes para la WAN ISP-1 donde se agregra la menor distancia a la WAN que tenga mejor banda ancha en casos reales.

1	ARP		
1	Addresses	Route <0.0.0.0/0->172.18.142.100>	
) 1	Cloud	General BGP RIP OSPF MPLS	
ystem ∖`	DHCP Client	Det Address: 0.0.0.0/0	(
Jueues	DHCP Relay	Catavaru 173 10 143 100	—
files	DHCP Server	Gateway: 172.18.142.100	
Log	DNS	Immediate Gateway: 17/2.18.142.100%ether1	D
RADIUS	Firewall	Check Gateway:	6
Tools ト	Hotspot	Type: unicast	
New Terminal	IPsec		(
Make Supout.rif	Kid Control	Distance: 1	Re
Manual	Neighbors	Scope: 30	
New WinBox	Packing	Target Scope: 10	
Exit	Pool	VRF Interface:	
	Routes	Prof. Source:	
	SMB		
	SNMP	Create Time:	
	Services	Update Time:	
	Settings		
	Socks	Received From:	
	TFTP	Belongs To: Static route	
	Traffic Flow	enabled active static	
	UPnP		



14. Configurar la routes para la ISP-2.

	Route						Γ	
Wireless	Paul							
Bindge	Rou	ites Nexthops Rule:	s					
	+	- 🖌 🗙 🗂	$\overline{\mathbf{v}}$				Find	
		Dst. Address	Gateway			Distance	Pref. Source	•
₩ P	AS	▶ 0.0.0.0/0	172.18.142.100				1	
	DAC	▶ 40.40.40.0/30	40.40.40.1 ether2				2	
Routing P	DAC	▶ 172.18.142.0/	ether1				5	
Oueuee		Route <0.0.0.0/0->40	.40.40.1>			×		
Files		General BGP R	IP OSPF MPLS		ОК			
🗐 Log		Dst. Address:	0.0.0/0		Cancel			
RADIUS		Gateway:	40.40.40.1	-1	Apply	-1		
🔀 Tools 🛛 🗅		Immediate Gateway:	40.40.40.1% ether?	-1	Apply			
🔤 New Terminal			TO TO TO TO TO STORE		Disable			
Make Supout.rif		Check Gateway:		•	Comment			
Manual		Type:	unicast	₹	Conv	-1		
New WinBox		Distance:	2		Сору	-		
🔣 Exit	4 iten	Distance.	20		Remove			
		Scope:	30					
		Target Scope:	10	^				
		VRF Interface:		•				
		Pref. Source:		^				
		Create Time:						
5		Update Time:						
5		Received From:						
		Belongs To:	Static route					
Ď.		enabled	active	stat	ic	-		

Figura 301.Configuracion WAN IPS 2 para distancia Fuente: Los autores

15. Realizar la prueba de FailOver se desconectara la eth1 y automáticamente el ping se debe restablecer por la eth2 tal como se observa en la imagen.



Figura 302. Test Failover

Fuente: Los autores

16. Configurar la ETH3 para la WAN-1 del fg-sucursal.

Session Settings Das	hboard	
Safe Mode	Session: 0C:C8:A2:E3:6B:00	
Quick Set CAPsMAN CAPsMAN Interfaces Wireless Bridge PPP Mesh Exp PP	ARP	Address List Image: Constraint of the second
PV6 F Routing Routing F Routing Routing Make Support of Manual N New Terminal N New Terminal N N New WinBox	Addresses Cloud DHCP Clent DHCP Relay DHCP Server DNS Firewall Hotspot IPsec Kid Control Neighbors Packing	Address 10.10.10.1/30 Address 10.10.10.1/30 Network: 10.10.00 Interface: ether3 OK Cancel Interface: ether3 Opply Disable Convent Copy Remove Remove
	Pool Routes SMB SNMP Services	enabled

Figura 303.Configuracion eth3 para la WAN1 FG-SUCURSAL Fuente: Los autores

17. Configurar la eth4 para la WAN-2 del fg-sucursal.

Session Se	ettings Das	shboard	
6	Safe Mode	Session: 0C:C8:A2:E3:6B:00	
Quicl Q CAPs Im Interf Wirel St Bridg To PPP C Mesh	k Set sMAN faces less ge h		Address List Image: Constraint of the second
또한 IP 또 IPv6 Routing	1 1 1 1	ARP Addresses Cloud	
💭 Syste 🜪 Queu 🖿 Files	em ♪ ues	DHCP Client DHCP Relay DHCP Server	Address: 20.20.20.1/30 OK Network: 20.20.20.0 Cancel
🗐 Log 🎒 RAD	DIUS	DNS Firewall	Interface: ether4
New Make	s l` Terminal e Supout.rif	Hotspot IPsec Kid Control	Comment
S New	WinBox	Packing Pool	Remove
×		Routes SMB SNMP Services	enabled
0			

Figura 304.Configuracion eth4 para la WAN2 FG-SUCURSAL Fuente: Los autores

18. Configurar el port2 en fg-sucursal para la WAN-1.

FortiGate VM64-KV	M <u>FG-</u>	SUCURSAL			
Dashboard	> ^	Edit Interface			
X Security Fabric	>	Namo	WAN-1 (port2)		
+ Network	~	Alias			
Interfaces	☆	Tune	Physical Interface	à	
DNS			0	·	
Packet Capture		Role 0	WAN	•	
SD-WAN Zones		Estimated bandwidth	0		kbns Unstream
SD-WAN Rules			0		kbps Downstream
Performance SLA			_		
Static Routes		Address			
Policy Routes		Addressing mode	Manual DHCP	Auto-managed by For	tiIPAM
RIP		IP/Netmask	10.10.10.2/255.255	5.255.252	
OSPF		Secondary IP address			
BGP					
Multicast		Administrative Access			
System	>	IPv4 🗹 F	ITTPS	PING	FMG-Access
📕 Policy & Objects	>		SH	SNMP	LIFIM
Security Profiles	>		ADIUS Accounting	Connection ()	
□ VPN	>	Receive LLDP () Use	e VDOM Setting Enal	ble Disable	
User & Authentication	> 、	_			OK Cancel
Figura	305.	Configuracion	port 2 FG-S	UCURSAL	para la WAN 1

Fuente: Los autores

19. Configurar el port3 para WAN-2 del fg-sucursal.

FortiGate VM64-KV	M FG-	SUCURSAL				
Dashboard	> ^	Edit Interface				
🔆 Security Fabric	>	Mana	M(AN -2 (port2)			
+ Network	~	Name			7	
Interfaces	☆	Allas	VVAIN -2]	
DNS		Type		,	7	
Packet Capture		VRFID 0	0		1	
SD-WAN Zones		Role 🚺	WAN	•		
SD-WAN Rules		Estimated bandwidth	0		kbps Upstream	
Performance SLA			0		kbps Downstream	
Static Routes		Address				
Deller Poutes		Address	D 1100			
Policy Routes		Addressing mode	Manual DHCP	Auto-managed by For	TIPAM	
RIP		IP/Netmask	20.20.20.2/30			
OSPF		Secondary IP address				
BGP						
Multicast		Administrative Access				
System	>	IPv4	A HTTPS		FMG-Access	
Policy & Objects	>		_ 55H	SNMP Security Fabric	LIFIM	
Security Profiles	>		□ RADIUS Accounting	Connection (1)		
므 VPN	>	Receive LLDP 🚯	Use VDOM Setting Enal	ble Disable		
User & Authentication	>				OK Cancel	
Eigura	206	Configuracio	n nort 2 EC-S		para la M/AN/2	

Figura 306.Configuracion port 3 FG-SUCURSAL para la WAN 2 Fuente: Los autores

20. Configurar el port4 para la red local del fg-sucursal.

FortiGate VM64-KVI	M FG-S	SUCURSAL			
Dashboard	> ^	Edit Interface			
🔆 Security Fabric	>	Nama	LAN (port4)		
+ Network	~				
Interfaces	☆	Allas L	AN Dhysical Interface		
DNS			r nysical interface		
Packet Capture			AN	-	
SD-WAN Zones			AN	·	
SD-WAN Rules		Address			
Performance SLA		Addressing mod	e N	Anual DHCP Auto-man	aged by FortiIPAM
Static Routes		IP/Netmask	1	92.168.1.50/255.255.255.0	
Policy Routes		Create address of	object matching subnet 🕥		
RIP		Secondary IP add	dress 🔾 🔾		
OSPF					
BGP		Administrative A	ccess		
Multicast		IPv4	HTTPS	PING	FMG-Access
System	>		SSH SSH	SNMP	□ FTM
📕 Policy & Objects	>		RADIUS Accounting	Connection ()	
Security Profiles	>	Receive LLDP (Use VDOM Setting Ena	able Disable	
I VPN	>	Transmit LLDP	Use VDOM Setting Ena	ble Disable	
User & Authentication	> 、			ОК	Cancel

Figura 307.Configuracion port 4 red local FG-SUCURSAL Fuente: Los autores

21. Configurar las interface WAN-1 para la SD-WAN.

FortiGate VM64-KVN	FG-	SUCURSAL		
Dashboard	> ^	Edit SD-WAN Mer	mber	
🔆 Security Fabric	>	Interface	WAN-1 (port2)	•
+ Network	~	SD-WAN Zone	wirtual-wan-link	• •
Interfaces		Gateway		
DNS		Cost	0	
Packet Capture		Status	• Enabled O Disabled	
SD-WAN Zones	☆	Status		
SD-WAN Rules				
Performance SLA				
Static Routes				
Policy Routes				
RIP				
OSPF				
BGP				
Multicast				
System	>			OK Cancel
Policy & Objects	>			
Figura	308	.Configurac	ion interface WAN 1	FG-SUCURSAL

Fuente: Los autores

22. Configurar la interface WAN-2 para la SD-WAN.

FortiGate VM64-KV	M FG-	SUCURSAL	
Dashboard	> ^	Edit SD-WAN Me	mber
🔆 Security Fabric	>		
+ Network	~	Interface	WAN-2 (port3)
Interfaces		Gateway	20.20.20.1
DNS Decket Conture		Cost	0
SD-WAN Zones	☆	Status	Enabled Disabled
SD-WAN Rules			
Performance SLA			
Static Routes			
Policy Routes			
RIP			
OSPF			
BGP			
Multicast			
System	>		OK Cancel
📕 Policy & Objects	>		

Figura 309.Configuracion interface WAN 2 FG-SUCURSAL Fuente: Los autores

23. Configurar la static routes para el enlace SD-WAN.

FortiGate VM64-K	M FG	SUCURSAL		
Dashboard	> ^	Edit Static Route		
Security Fabric Network Interfaces DNS Packet Capture	~	Dynamic Gateway 🖲 🕥 Destination 🕄 Interface	Subnet Internet Service 0.0.0.0/0.0.0.0 SD-WAN	
SD-WAN Zones SD-WAN Rules Performance SLA Static Routes	☆	Comments Status	Write a comment all 0/255 C Enabled Disabled OK Cancel	
Policy Routes				

Figura 310.Configuracion static routes SD-WAN FG-SUCURSAL Fuente: Los autores

FortiGate VM64-KV	M FG-S	UCURSAL		
Dashboard	> ^	DNS Settings		
 Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones 	> ~ ☆	DNS Servers Primary DNS Server Secondary DNS Server Local Domain Name	Use FortiGuard Servers Specify 172.18.253.10 0.0.0	
SD-WAN Rules Performance SLA		Dynamically Obtained D		
Static Routes Policy Routes RIP		Interface DNS Serv port1 172.18.253	er 3.10	
OSPF BGP Multicast				
 System Policy & Objects 	> >			Apply

24. Configurar los DNS en el fg-sucursal.

Figura 311.Configuracion DNS FG-SUCURSAL Fuente: Los autores

25. Configurar la política para salidad de internet para la red local.

FortiGate VM64-KVM	FG-	5UCURSAL				
🚯 Dashboard	> ^	Edit Policy				
🔆 Security Fabric	>					
Network	>	Name 🚯	SD-WAN]	
System	>	Incoming Interface	🔳 LAN (port4)	•]	
Policy & Objects	~	Outgoing Interface	🚳 virtual-wan-link	•]	
Firewall Policy	☆	Source	🔳 all	×		
IPv4 DoS Policy			+]	
Addresses		Destination	:⊒ ali +	~		
Internet Service Database		Schedule	G always	•		
Services		Service	ALL +	×		
Schedules		Action	✓ ACCEPT Ø DENY	·]	
Virtual IPs						
IP Pools		Inspection Mode	low-based Proxy-based			
Protocol Options						
Traffic Shapers		Firewall / Network O	ptions			
Traffic Shaping Policy		NAT	•			
Traffic Shaping Profile		IP Pool Configuration	Use Outgoing Interf	ace Address	Use Dynamic IP Pool	
Security Profiles	>	Preserve Source Port				
므 VPN	>	Protocol Options	PROT default			
User & Authentication	> ~				OK	Cancel

Figura 312.Configuracion firewall policy para la red local FG-SUCURSAL Fuente: Los autores

26. Configurar la perfomance SLA para ver los jitter de las WAN'S.

FortiGate VM64-K	VM FG-SUCURSAL
Dashboard	Cdit Performance SLA
Security Fabric	Name PING
Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules	Protocol Ping HTTP DNS Servers 8.8.8.8 X 8.8.4.4 X Participants All SD-WAN Members Specify Enable probe packets Image: Color of the second se
Performance SLA Static Routes Policy Routes	SLA Target Link Status
RIP OSPF BGP	Check interval 500 ms Failures before inactive 5 Restore link after 5 check(s)
System Policy & Objects	Actions when Inactive Update static route 1 •
Security Profiles VPN	> OK Cance

Figura 313.Configuracion perfomance SLA FG-SUCURSAL Fuente: Los autores

27. Se desactivara todas las WAN'S ISP que van al fg-sucursal y obversamos en perfomance SLA caído .



Figura 314.Observacion Perfomance SLA Fuente: Los autores

28. Activar una interfaz de la WAN'S que van al fg-sucursal y veremos como se activan las 2 activan automáticamente las interfaces.



Figura 315.Activacion interfaz WAN 'S Fuente: Los autores

29. FailOver actuando en la red local del fg-sucursal.



Figura 316.Ping failover conectando FG-SUCURSAL Fuente: Los autores

30. FailOver actuando desconectando unos de los WAN que van al fgsucursal.



Figura 317.Ping failover desconectando FG-SUCURSAL Fuente: Los autores

RECURSOS UTILIZADOS

- > COMPUTADORA
- CABLE DE RED (PATCHCORD)
- ➢ GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente.

4.1.9. **PRÁCTICA 9**

Configuración de un mangle con mikrotik para el enlace sd-wan.

DATOS INFORMATIVOS

- > MATERIA: Redes de comunicación
- ➢ PRÁCTICA № 9
- > NUMERO DE COMPUTADORAS: 10
- **TIEMPO ESTIMADO:** 2 Horas.

DATOS DE LA PRÁCTICA

TEMA: Configuración de un mangle con mikrotik para el enlace SD-

WAN.

OBJETIVOS

<u>General</u>

Configurar un mangle con mikrotik para el enlace sd-wan.

Específicos

- > Configurar mangle para el enlace SD-WAN.
- Realizar una red SD-WAN
- > Marcar paquetes del enlace SD-WAN.

GLOSARIO

MANGLE.- Es una especie de marcador que marca los paquetes para el procesamiento futuro con marcas especiales estas marcas se las puedes realizar en el NAT, QUEUE TREES y en el enrutamiento.

ROUTEROS.- Es el sistema operativo del hardware RouterBOARD tiene todas las características necesarias para un ISP.

MARCO PROCEDIMENTAL

1. Diseñar la topología de red para la práctica 9.



Figura 318. Diseño de la red práctica Nº9 Fuente: Los autores

2. Configurar la eth2 en el mikrotik para la WAN-1 del fg-sucursal.

ø	0	Safe Mode	Session: 0C:7B:78:A8:02:0	00	Shadow Mor
		Quick Set CAPsMAN Arherfaces Bridge PPP Wesh P Pv6 diting System Jueues Files Log RADIUS Tools Vew Terminal Make Supout ri Manual Vew WinBox Exit		Address List Find Address / Network Interface / Network Interface / Network Address / Network Interface: / Network Disable Comment Copy Remove enabled // Zerns (1 selected)	Shadow Moc


3. Configurar DNS para el mikrotik-ISP.

		-		
🖉 Quick Set				
CAPsMAN				
Interfaces				
Wireless				
👫 Bridge				
🛓 PPP		DNS Settings		
°T <mark>°</mark> Mesh		Server		<u></u>
🐺 IP 🛛 🗅	ARP	Servers.		▼ 0K
🖞 IPv6 🛛 🗅	Addresses	Dynamic Servers:	172.18.253.10	Cancel
Routing N	Cloud	Use DoH Server:		 Apply
🔯 System 🗈	DHCP Client		Verify DoH Certificate	
🙅 Queues	DHCP Relay		tony borroonalouto	Static
Files	DHCP Server		 Allow Remote Requests 	Cache
📃 Log	DNS	Max UDP Packet Size:	4096	
RADIUS	Firewall		0.000	
🔀 Tools 🛛 🗋	Hotspot	Query Server Timeout:	2.000 s	
New Terminal	IPsec	Query Total Timeout:	10.000 s	
📐 Make Supout.rif	Kid Control	Max, Concurrent Queries:	100	
🖳 Manual	Neighbors	Max Consument TCD Sessions	20	_
🔘 New WinBox	Packing	Max. Concurrent TCF Sessions.	20	
🛃 Exit	Pool	Cache Size:	2048	ΰB
	Routes	Cache Max TTL:	7d 00:00:00	
	SMB	Cache Used:	26 KiB	
	SNMP		20100	
	Services			

Figura 320. Configuracion DNS Mikrotik ISP Fuente: Los autores

4. Configurar la NAT para la red de la WAN-1.

Session Settings Das	hboard				
🖒 🍳 🛛 Safe Mode	Session: 0C:7B:78:A8:02:0	D		Shadow Mode	
🚀 Quick Set			NAT Rule <10.10.10.0/30>		
CAPsMAN			General Advanced Extra Action	. ОК	
Interfaces			Chain: srcnat	T Cancel	
Wireless			Sro. Address: 10.10.10.0/30		
*_ ppp			Dat Address:	Арріу	
•T• Mesh			Usi. Address.	Disable	
	ARP		Protocol:	 Comment 	
🕎 IPv6 🛛 🗅	Addresses	Firewall	Src. Port:	- Copy	
Routing D	Cloud	Filter Rules NAT Mande Raw Service Ports Cou	Dst. Port:	▼	
🔛 System 🗈 🗈	DHCP Client		Any. Port:	Tremove	
👰 Queues	DHCP Relay	🕈 🗕 🗸 🖬 γ το Reset Counters τ	In. Interface:	Reset Counters	<i>⊢ino</i> al •
Files	DHCP Server	# Action Chain Src. Address	Out. Interface: dether1	Reset All Counters	Inter Out. Int Src. Ad Dst. Ad Bytes Pat
Log	DNS		In Interface Unit		10.010
APRADIUS	Firewall				
New Tempinel	Hotspot		Out. Interface List:		
Make Supert of	IPsec		Packet Mark:	•	
Manual	Na Control		Connection Mark:	•	
New WinBox	Packing		Routing Mark:	•	
Exit	Pool		Routing Table:	•	
_	Routes				
	SMB		Connection Type:	-	
	SNMP				
1.1					1

Figura 321. Configuracion NAT mikrotik ISP (a) Fuente: Los autores



Figura 322. Configuracion NAT masquerade mikrotik ISP (b)

Fuente: Los autores

5. Configurar la IP para el port2 del fg-sucursal.

FortiGate VM64-KV	M FG-S	UCURSAL			
Dashboard	> ^	Edit Interface			
X Security Fabric	>	Name	🔳 WAN-1 (port2)		
Network Interfaces	~ ☆	Alias	WAN-1		
DNS		Type VRFID 1	Physical Interface		
Packet Capture		Role (1)	WAN	•	
SD-WAN Zones		Estimated bandwidth	0		kbps Upstream
Performance SLA			0		kbps Downstream
Static Routes		Address			
Policy Routes		Addressing mode	Manual DHCP	Auto-managed by Fort	LIPAM
RIP		IP/Netmask	10.10.10.2/255.255	.255.252	
OSPF		Secondary IP address			
BGP					
Multicast		Administrative Access			
System	>	IPv4	HTTPS	PING	FMG-Access
Policy & Objects	>		J SSH	SNMP Security Fabric	LIFIM
Security Profiles	>		J RADIUS Accounting	Connection ()	
D VPN	>	Receive LLDP 🕄	Use VDOM Setting Enab	le Disable	
User & Authentication	>				OK Cancel

Figura 323. Configuracion IP port 2 FG-SUCURSAL Fuente: Los autores 6. Configurar el port4 para la red local del fg-sucursal.

FortiGate VM64-KVM	G-SUCURSAL							
🚯 Dashboard	> Edit Interface							
Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules	Name RED-LOCAL (port4) Alias RED-LOCAL Type Physical Interface VRF ID 0 Role LAN Address							
Performance SLA	Addressing mode Manual DHCP Auto-managed by FortilPAM							
Static Routes Policy Routes RIP	IP/Netmask 192.168.1.20/255.255.255.0 Create address object matching subnet Secondary IP address							
OSPF	Administrative Access							
BGP Multicast System	IPv4 IPv4 ITTPS IPNG FMG-Access SSH SNMP FTM RADIUS Accounting Security Fabric Connection 0							
Security Profiles VPN	Receive LLDP ① Use VDOM Setting Enable Disable Transmit LLDP ① Use VDOM Setting Enable Disable							
User & Authentication	DHCP Server							
וש נטק א אפאטור	Address range 192.168.1.1·192.168.1.19 X 192.168.1.21·192.168.1.254 X							
	OK Cancel							
Figura	a 324. Configuracion red local port 4 FG-SUCURSAL Fuente: Los autores							

7. Configurar DNS al fg-sucursal.

Dashboard	>	DNS Settings	
Security Fabric	>		
Network	~	DNS Servers	Use FortiGuard Servers Specify
Interfaces		Primary DNS Server	8.8.8.8
DNS	☆	Secondary DNS Server	8.8.4.4
Packet Capture		Local Domain Name	
SD-WAN Zones		DNC sure TLC	
SD-WAN Rules		DINS OVER TES U	Disable Enable Enforce
Performance SLA		Dynamically Obtained D	NS Servers
Static Routes		Interfere DNC Come	
Policy Routes		Interrace Divisions Serve	
RIP		port1 172.18.253	.10
OSPF			
BGP			
Multicast			
System	>		
Policy & Objects	>		
Security Profiles	>		
L VPN	>		Apply
•			Арргу

Fuente: Los autores

8. Configurar la interfaz que va a pertenecer a la SD-WAN.

FortiGate VM64-KVM	FG-	SUCURSAL					
🚯 Dashboard	>	Edit SD-WAN Memb	er				
 ☆ Security Fabric • Network Interfaces DNS Packet Capture 	> ~	Interface I SD-WAN Zone Gateway 1 Cost Gataus	WAN-1 (port2) Virtual-wan-link 0.10.10.1 Enabled O Disab				
SD-WAN Zones SD-WAN Rules Performance SLA Static Routes Policy Routes	\$						
RIP OSPF BGP Multicast							
 System Policy & Objects Security Profiles 	> > >					ОК	Cancel
Figura	a 32	26. Configu	ración SD-V	VAN Zo	nes FG-SL	ICURSA	<u> </u>

- Fuente: Los autores
- 9. Configurar la static routes para la SD-WAN.

FortiGate VM64-KVM	FG-	SUCURSAL				
🚯 Dashboard	>	Edit Static Route				
🔆 Security Fabric	>		_			
Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Pacformance SI A	~	Destination ① Interface Comments Status	Subnet Internet Service 0.0.0.0/0.0.0 Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Constraint of the service Image: Cons			
Static Routes	☆			ОК	Cancel	
Policy Routes						

Figura 327. Configuración Static routes FG-SUCURSAL

Fuente: Los autores

10. Configurar la regla para la salida a internet a la red loca del fgsucursal.

FortiGate VM64-KVM	FG-	SUCURSAL					
🚯 Dashboard	>	Edit Policy					
🔆 Security Fabric	>						
Network	>	Name 🚯	REGLA - RED LOCAL				
System	>	Incoming Interface	RED-LOCAL (por	t4) 🔻	•		
Policy & Objects	~	Outgoing Interface	🗟 virtual-wan-link	•	•		
Firewall Policy	☆	Source	🔳 all	2	6		
IPv4 DoS Policy			+				
Addresses		Destination	🖼 all 🔶	3	C		
Internet Service Database		Schedule	always		•		
Services		Service	ALL ALL		6		
Schedules			+				
Virtual IPs		Action	✓ ACCEPT Ø DI	ENY			
IP Pools							
Protocol Options		Inspection Mode	low-based Proxy-ba	sed			
Traffic Shapers		Firewall / Network O	ptions				
Traffic Shaping Policy		NAT					
Traffic Shaping Profile		IP Pool Configuration		terface Address	Lise Dynamic IP Pool		
Security Profiles	>	Preserve Source Port		terrace Address	OSE Dynamic II 1 Oor		
L VPN	>	Protocol Ontions	PROT default		▼ #		
User & Authentication	>	1 TOLOCOL OPTIONS	derault				
네 Log & Report	>	Security Profiles					
					C	0K	Cancel

Figura 328. Configuración firewall policy FG-SUCURSAL Fuente: Los autores

11. Configurar un marcado de conexiones para los puertos 80 y 443.

C Safe Mode	Session: 0C:7B:78:A8:02:00	Shad	ow Mo	de	
🖋 Quick Set	Firewall	Child	000 1010		
CAPsMAN	Filter Rules NAT Mang	le Raw Service Ports Connections Address Lists Laver7 Protocols			
Interfaces					
Wireless		1 Reset Counters Conterns			
Bridge	# Action Chain	Src. Address Dst. Address Proto Src. Port Dst. Port In. Inter Out. Int In. Inter Out. Int Src. Ad	Dst. Ad.	Bytes	Packets
E PPP	U Se mar preroutil	Mangle Rule <10.10.10.0/30>			
📲 Mesh		General Advanced Extra Action Statistics			ок
💯 IP 🗈 🗈	ARP	Charles and the			Connel
🛫 IPv6 🗈 🗈	Addresses	Chain: prerouting			Cancel
Routing 1	Cloud	Src. Address: 10.10.0/30	^		Apply
System 🗅	DHCP Client	Dst. Address:	-		Disable
🗣 Queues	DHCP Relay	Protocol:	.		-
Files	DHCP Server	Con Date	-11		Comment
🚊 Log	DNS	Src. Port:	_ * I		Сору
P RADIUS	Firewall	Dst. Port:	-		Remove
🔀 Tools 💦 🕅	Hotspot	Any. Port:	-		De la Caratan
New Terminal	IPsec	In. Interface:	-		Reset Counters
Make Supout.rlf	Kid Control	Out. Interface:	•	R	eset All Counters
🚈 Manual	Neighbors				
🕓 New WinBox	Packing	In. Interface List:	_		
Kit Exit	Pool	Out. Interface List:	-		
	Routes	Packet Mark:	•		
	SMB	Connection Made	-		
	SNMP				
	Services	Routing Mark:			
	Settings		•		
	Socks	enabled			
	TETO	La.			

Figura 329. Configuración marcado de conexiones a la redpuerto 80 y 443 (a) Fuente: Los autores

🛓 PPP		Mangle Rule <10.10.0/30>	
° ⊺ ° Mesh		General Advanced Extra Action Statistics	ОК
IP	1		Canad
₩ IPv6	1		Cancel
Routing	1		Apply
System		Log Prefix:	Dieable
🙅 Queues			
Files		New Connection Mark: enlace_sd-wan	Comment
🗎 Log		✓ Passthrough	Сору
AP RADIUS			Remove
X Tools	1		Deast Counterr
Mew Termin	al		Reset Counters
Make Supo	ut.rif		Reset All Counters
🖳 Manual			

Figura 330. Configuración marcado de conexiones puerto 80 y 443 (b)

Fuente: Los autores

12. Configurar un marcado de paquetes para los puertos 80 y 443

Endge		Downell									_
🏣 PPP		Mangle Rule	e <443,80>								
°T <mark>°</mark> Mesh		F General 4	Advanced	Extra Action	Statistics					OK	
255 IP		4	/ avancea	Exite / Iotion	otutionea					UN	Fin
🛒 IPv6	Þ		Chain:	prerouting				₹	•	Cancel	Det Ad By
Routing	\uparrow	Sr	irc. Address:					•		Apply	
🔯 System	\uparrow	D	st. Address:					•		Disable	
👰 Queues				_				_		Disable	
📔 Files			Protocol:	6 (tcp)			1	E_▲		Comment	
🗐 Log			Src. Port:					•		Сору	
RADIUS			Dst. Port:	443,80		 		•			
🔀 Tools	\uparrow		Any. Port:					•		Remove	
🔤 New Termina	al	Ir	n. Interface:					•		Reset Counters	
📡 Make Supou	t.rif	Out	t Interface:					•		Reset All Counters	
🔁 Manual											
🕓 New WinBox		In. Int	terface List:					•			
🔣 Exit		Out. Int	iterface List:					•			
		Pa	acket Mark			 		7.			
			asiter maint.	_							
		Conne	ection Mark:	enlace_sd	-wan		•				
											1

Figura 331. Configuración marcado de paquetes puerto 80 y 443 (a) Fuente: Los autores

💥 Bridge		Mangle Rule	e <443,80>					
🛓 PPP		General	Advanced	Extra A	ction	Statistics	Γ	OK
°∏ <mark>°</mark> Mesh			A					0.1
355 IP	Þ		Action:	mark paci	<et< th=""><td>,•</td><td></td><td>Cancel</td></et<>	,•		Cancel
🛒 IPv6	Þ			Log				Apply
Routing	Þ		Log Prefix:			▼		Disable
🔯 System	Þ		-					Diddbio
👰 Queues		New Pa	acket Mark:	marcado_	pk_en	lace-sdwan 🔻		Comment
📔 Files				Passth	rough			Сору
🗒 Log								Remove
RADIUS							+	
\chi Tools	Þ							Reset Counters
💹 New Termin	nal						R	Reset All Counters
Make Supe	a af							

Figura 332. Configuracion marcado de paquetes puerto 80 y 443 (b) Fuente: Los autores

13. Visulización de los marcados de nuestro enlace SD-WAN desde la red local fgsucursal.

👯 Bridge		Fire	ادس																X
指 PPP			maii								_								
° 🕻 Mesh		R	ter Ru	es NAT	Mangle	Raw Service	Ports Conn	ections	Address Li	sts Layer7	Protocols								
55 IP	ľ	÷	-	v X	; 🖪 🏹	7 (O Reset C	ounters (O	Reset A	Counters								Find	al	Ŧ
🖞 IPv6	<u></u> ↑	#		Action	Chain	Src. Address	Dst. Address	Proto	Src. Port	Dst. Port	In. Inter	Out. Int	In. Inter	Out. Int	Src. Ad	Dst. Ad	Bytes	Packets	v
Routing	N		0	🖉 mar	prerouting	10.10.10.0/											879.8 KiB	15 658	
System	N		1	🖉 mar	prerouting			6 (tcp)		443,80							188.7 KiB	3 806	
Queues																			

Figura 333. Visualizacion marcado de paquetes SD-WAN FG – SUCURSAL Fuente: Los autores

14. Configurar marcado de paquetes a DNS.

+_ ppp	e Rule <53>		
•1° Mesh Gene	eral Advanced Extra Action Statistics		ОК
IP N	Chain area the	.	Canoel
🐺 IPv6 🗈	Chain, <u>Interduting</u>		
Routing N	Sic. Address.	<u> </u>	Apply
🔯 System 🗈	USI. Address.		Disable
n Queues	Protocol: 17 (udp)	₹ ▲	Comment
Files	Src. Port:	•	Conv
	Dst. Port: 🗌 53		Demons
	Any. Port:	•	Remove
Mew Terminal	In. Interface:	•	Reset Counters
Make Supout rif	Out. Interface:	•	Reset All Counters
🖻 Manual	le leiséface liúi	_	
S New WinBox		<u> </u>	
Kit	Jur. Interface List.		
	Packet Mark:	•	
	Connection Mark: 🗌 enlace_sd-wan	₹ ▲	
	Routing Mark:	•	
<u> </u>	Routing Table:	•	
		+	
≥ 3 enable	xd		

Figura 334. Configuracion marcado de paquetes DNS (a) Fuente: Los Autores

🖉 Quick S	et												
🗘 CAPsM/	N												
🛤 Interface	s												
Wireless													
💥 Bridge			1					 	 	 	 		
🏣 PPP		Mangle Ru	ile <53>	_		1							X
°∏ <mark>°</mark> Mesh		General	Advanced	Extra A	Action	Statistics							OK
355 IP	Þ	•	Action:	mark pac	ket							Ŧ	Cancel
Pv6 Routing	1			Log									Apply
🔯 System	Þ		Log Prefix:									•	Disable
Queues		New	Packet Mark:	marcado_	_pk_er	nlace-sdwa	n					 Ŧ	Comment
Log				Passth	nrough								Сору
an RADIUS													Remove
🗙 Tools	1												Reset Counters

Figura 335. Configuracion marcado de paquetes DNS (b) Fuente: Los Autores

15. Agregar un address-list para el marcado de paquetes para youtube.

25 bruge	Frewal	
🏣 PPP		
°T <mark>°</mark> Mesh	Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer? Protocols	
₩ IP		Find al ∓
🛂 IPv6 🗈 🗎	Name / Address Timeout Creation Time	•
Routing N	youtube youtube.com Dec/19/2020 18:	
🔯 System 🗈	::: youtube.com	
👰 Queues		
📔 Files	Name: youtube • OK	
🗏 Log	Address: voutube.com Cancel	
RADIUS	Timeout:	
🗙 Tools 🛛 🗎	Creation Time: Dec/19/2020 18:31:47	
💵 New Terminal	Disable	
📔 Make Supout.rif	Comment	
Manual		
🔇 New WinBox		
🔣 Exit	Remove	
	anablad	

Figura 336. Agregando address-list para marcado Fuente: Los Autores

16. Configurar el marcado de paquetes para youtube para el enlace sdwan.

Image: PPP Procession Margle Rule Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol Image: Photocol							Financal		M bruge
Mesh Riter Rules Natige Raw Margle Raw							Theman		🏣 PPP
Image: Proof in the image: Proof in		Ľ			Mangle Hule <>	r Mangle Raw	Filter Rules NAT		° 🕻 Mesh
Image: Project Project Image: Project Project Project Project Project Image: Project ProjectProject Project Project Project Project Project Project Project P		OK		t Extra Action Statistics	General Advanced	K 🖸 🍸 🛛	+ - v x	Þ	🏥 IP
Routing IIII MARCADO DE CONEXION HT Src. Address: IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		Cancel	٠	in: prerouting	Chain:	Chain Src.	# Action	Þ	🖞 IPv6
System 0 mar preouting 10 Queues 1 mar preouting V Disable Imar preouting Protocol: V Disable Comment Imar preouting Str. Pot: V V Disable Comment Imar preouting Str. Pot: V V Convent Convent Imar preouting Disable V V Protocol: V V Imar preouting Str. Pot: V V Protocol: V V Imar preouting Dist. Pot: V V Protocol: V <td>5</td> <th>Apply</th> <th></th> <td>88'</td> <td>Src: Address:</td> <td>)E CONEXION HTT</td> <td>::: MARCADO DE</td> <td>Þ</td> <td>Routing</td>	5	Apply		88'	Src: Address:)E CONEXION HTT	::: MARCADO DE	Þ	Routing
Queues 1 Disable Queues 1 Disable Image: prevoting Protocol: Image: prevoting Image: prevoting Image: prevoting Protocol: Image: prevoting Image: prevoting Image: prevoting Protocol: Image: prevoting Image: prevoting Image: prevoting Ima		- Ahhia			D. All	prerouting 10.1	0 🖋 mar	Þ	🔯 System
Files 2 mail prevoding 2 mail prevoding 1 Marc. ADD PAQUETES DNS 3 mail 3 mail 4 mail Dat. Port: Copy		Disable		l\$	Ust. Address:	DE PAQUETE HTT	::: MAHCADO Di		👰 Queues
□ Log MARCADO PAQUETES DNS 3 / mar prerouting 4 / mar prerouting Dst. Pot: ▼ Copy Remove	=	Comment		ol:	Protocol:	prerouting	2 🖉 mar		Files
3 mar prerouting 3/c. rott. Copy A Parallelis A Parallelis Tools V		Comment			Core Darks	AQUETES DNS	::: MARCADO P/		🗏 Loa
Tools N		Сору			SIC. FOIL	prerouting	3 🖉 mar		10 RADIUS
X TOOIS I' Hemove	51			vi:	Dst. Port:	prerouting	4 🖋 mar	N	N/ Test
Any. Port:		Hemove		vt:	Any, Port;			1 ⁷	X 100IS
Sev Teminal Reset Courters	3	Reset Counter			h hufer				🔤 New Terminal
Make Support if	=	D			in. Interface:			trif	📔 Make Supout.
Manual Out. Interface:	.rs	Reset All Counte		xe:▼	Out. Interface:				Manual
♦ New WinBox				id ⁱ	In Interface List:				🔇 New WinBox
Et Et				ŭ.					🛃 Exit
Out. Interface List:				₫.:▼	Out. Interface List:				
Packet Mark:				k:	Packet Mark:				
Connection Mark: 🗌 enlace_sd-wan				rk: □ enlace_sd-wan 🐨 🔺	Connection Mark:				

Figura 337. Configuracion marcado de paquetes SD-WAN (a) Fuente: Los Autores

👯 Bindge	Firewal			
🏣 PPP		Und Dir o		
° 🕻 Mesh	Filter Rules NAT Mangle Raw	Mange Rule O		
🛱 🖻 🗈 🗎	+ - • × 🗅 🍸 «	General Advanced Extra Action Statistics		ОК
🖞 IPv6 🗈	# Action Chain Src.	Src. Address List.	•	Cancel
Routing	::: MARCADO DE CONEXION HTT	Dat. Address List: Voutube	Ŧ A	Apply
🔯 System 🗈	0 8 mar prerouting 10.1			Арру
🗣 Queues	::: MARCADO DE PAQUETE HTTT 1 9 mar prerouting	Layer7 Protocol:	•	Disable
📔 Files	2 🖉 mar prerouting	Content	7.	Comment
🗒 Log	::: MARCADO PAQUETES DNS			
8 RADIUS	3 mar prerouting	Connection Bytes:		Сору
🗙 Tools 🔹 N	4 gr mar prerodung	Connection Rate:	•	Remove
💵 New Teminal		Per Connection Classifier.	T	Reset Counters
🎦 Make Supout rif		Src. MAC Address:	•	
Manual				Reset All Counters

Figura 338. Configuracion marcado de paquetes SD-WAN (b) Fuente: Los Autores

👬 Bindge		Finual		
指 PPP				
", Mesh		FiterRules NAT Mangle Raw Mangle Hule ↔		
55 IP	Þ	+ - 🗸 🗶 🔽 🍸 🖞 General Advanced Extra Action Statistics		OK
IPv6	ŀ	# Action Chain Src Action: mark packet	Ŧ	Cancel
Routing	N	;;; MARCADO DE CONEXION HT		And
🔯 System	N	0 🖉 mar prerouting 10.1 🛛 🗌 Log		Арріу
		;;; MARCADO DE PAQUETE HTT		Deally
	_	1 new perceting		Lisable
Files	- 1	2 🖉 mar prerouting	-	Comment
🗏 Loo		;;; MARCADO PAQUETES DNS new rackel wark: [marcado_px_enade=dowan	•	
		3 ∮mar prerouting Passthrough		Сору
ADIUS		4 🖉 mar prerouting		
¥ Tools	N			Remove

Figura 339. Configuracion marcado de paquetes SD-WAN (c) Fuente: Los Autores

17. Visualizacion de los marcados de paquetes del enlace sd-wan.

Session Settings D	ashboard																	
Safe Mode	Session: 00	C:7B:78:A8:02:00									5	Shadov	w Mod	e				
🏏 Quick Set																		
CAPsMAN																		
Interfaces																		
Wireless																		
🚉 Bridge		Dennell																
🏣 PPP		Firewall		1			(1								
*[° Mesh		Filter Rules NA	T Mangle	Raw Service	Ports Co	nnections	Address Li	sts Layer7	Protocols									
🐺 IP		+ - 🖉 :	× 🗆 🍸	(© Reset C	ounters	o Reset A	Il Counters									Find	all	₹
🖞 IPv6 👘		# Action	Chain	Src. Address	Dst. Addre	ss Proto.	. Src. Port	Dst. Port	In. Inter	Out. Int	In. Inter	Out. Int	Src. Ad	. Dst. Ad	Bytes	Packets		-
Routing	>	::: MARCADO	DE CONEXION	HTTPS-HTTP	0													
System		0 Semar	prerouting	10.10.10.0/											5.0 MiE	60 211		
🙅 Queues		1 🖉 mar	. prerouting	5		6 (tcp)		443,80							4310.5 KiE	51 510		
Files		2 🖉 mar.	. prerouting											youtube	390.9 KiE	259		
🗐 Log		::: MARCADO	PAQUETES D	NS		17/		50							00.4165	1 000		
RADIUS		3 / mar	prerouting			6 (tcn)		25 587							80.4 NE	1233		
🔀 Tools 🕺	5		prerouting			o (top)		20,007								, v		
🛤 New Terminal																		
Nake Supout.rif																		
🖾 Manual																		
New WinBox																		
🛃 Exit																		
X																		
B																		
/i/																		
>		5 items																
00		p		1														

Figura 340. Visualizacion marcado de paquetes SD-WAN Fuente: Los Autores

RECURSOS UTILIZADOS

- > COMPUTADORA
- CABLE DE RED (PATCHCORD)
- ➢ GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente

4.1.10. PRÁCTICA 10

Configuración de un layer 7 con calidad de servicios QOS para el enlace

SD-WAN utilizando mikrotik.

DATOS INFORMATIVOS

- > MATERIA: Redes de comunicación
- ➢ PRÁCTICA № 10
- > NUMERO DE COMPUTADORAS: 10
- > **TIEMPO ESTIMADO:** 2 Horas

DATOS DE LA PRÁCTICA

TEMA: Configuración de un layer 7 con calidad de servicios QOS para el

enlace SD-WAN utilizando mikrotik.

OBJETIVOS

General

Configurar layer 7 con mikrotik para el enlace SD-WAN

Específicos

- Configurar layer 7 en mikrotik
- Realizar un marcado de paquetes y conexiones.
- > Elaborar un simple queues a los servicios y marcados de conexión.

GLOSARIO

MANGLE.- Es una especie de marcador que marca los paquetes para el procesamiento futuro con marcas especiales estas marcas se las puedes realizar en el NAT, QUEUE TREES y en el enrutamiento.

ROUTEROS.- Es el sistema operativo del hardware RouterBOARD tiene todas las características necesarias para un ISP.

LAYER 7.- Es un método de búsqueda de patrones en flujos ICMP / TCP / UDP.

QUEUE.- Las colas se utilizan para limitar y priorizar el tráfico.

MARCO PRODECIMENTAL

1. Diseñar la topología de red para la práctica 10.



Figura 341. Diseño de la red práctica Nº 10 Fuente: Los autores

2. Configurar la eth2 en el mikrotik para la WAN-1 del fg-sucursal.



Figura 342. Configuración eth2 mikrotik Fuente: Los autores

3. Configurar DNS para el mikrotik-ISP.

CAPsMAN				
Interfaces				
Wireless				
👫 Bridge				
The second secon		DNS Settinge		
"[<mark>" Mes</mark> h		Divis Settings		
🐺 IP 🗈 🗈	ARP	Servers:	≑	OK
🖞 IPv6 🛛 🗅	Addresses	Dynamic Servers:	172.18.253.10	Cancel
Routing 1	Cloud	Use DoH Server:		Apply
🔯 System 🗈	DHCP Client		Vorify Dold Cortification	
🙅 Queues	DHCP Relay		Venily Dorr Celtificate	Static
📄 Files	DHCP Server		 Allow Remote Requests 	Cache
🗐 Log	DNS	Max UDP Packet Size:	4096	
RADIUS	Firewall			
🔀 Tools 🛛 🔿	Hotspot	Query Server Timeout:	2.000 s	
New Terminal	IPsec	Query Total Timeout:	10.000 s	
Make Supout.rif	Kid Control	Max. Concurrent Queries:	100	
🖳 Manual	Neighbors	May Consumpt TCD Social	20	
🔘 New WinBox	Packing	Max. Concurrent TCP Sessions:	20	
🛃 Exit	Pool	Cache Size:	2048 KiB	
	Routes	Cache Max TTL:	7d 00:00:00	
	SMB	Cache Used:	26 KiB	
	SNMP	Cache Gada.		

Figura 343. Configuracion DNS mikrotik Fuente: Los autores

4. Configurar la NAT para la red de la WAN-1.

				NAT Rule <10.10.10.0/30>				
CAPsMAN				General Advanced Extra Action		ОК		
Interfaces								
Wireless				Chain: srcnat	₹	Cancel		
Bridge				Src. Address: 10.10.10.0/30	_ ▲	Apply		
🟣 PPP				Dst. Address:	•			
"T. Mesh						Disable		
₩ IP	Þ	ARP		Protocol:	•	Comment		
🛒 IPv6	Þ	Addresses	Firewall	Src. Port:		Сору		1
Routing	1	Cloud	TO DI NAT IL DI DI DI DI DI	Dst. Port:				
10% System	Þ	DUCP Clicat	Hiter Rules INAT Mangle Raw Service Ports Cor	Any Port		Remove		
Change Change		DHCF Client	🕂 🗕 🖌 🗶 🗂 🍸 🗯 Reset Counters 🕼	Phy. Force		Reset Counters	Find all F	
Tueues		DHCP Relay		In. Interface:	•			
Files		DHCP Server	# Action Chain Src. Address	Out. Interface: ether1	∓ ▲	Reset All Counters	Inter Out. Int Src. Ad Dst. Ad Bytes Pa	
🗏 Loa		DNS	0 (mas srcnat 10.10.10.0/30		-		40.9 KiB	

Figura 344. Configuración del NAT mikrotik (a) Fuente: Los autores

🖉 Quick Set		NAT Rule <10.10.10.0/30>		
🗘 CAP\$MAN		Advanced Extra Action Statistics	OK	
Interfaces				
🔉 Wireless		Action: masquerade	Cancel	
💥 Bridge		Log	Apply	
🏣 PPP		Log Prefix:	Disable	
° ° Mesh			Disable	
🐺 IP 🛛 🗎		To Ports:	Comment	
掉 IPv6 🛛 🗅	Frewal		Сору	
Routing 🗈 🕅	Filter Rules NAT Manole Raw Service Ports Co		Permote	
💭 System 🗈			Inciliove	
👰 Queues	🕂 💻 🖌 🗶 🔁 🦞 🙆 Reset Counters 🧃		Reset Counters	Find al 🐺
Files	# Action / Chain Src. Address		Reset All Counters	Inter Out. Int Src. Ad Dst. Ad Bytes Pa
🗏 Log	0 (mas srcnat 10.10.10.0/30			40.9 KiB

Figura 345. Configuración del NAT masquerade (b)

Fuente: Los autores

5. Configurar la IP para el port2 del fg-sucursal.

FortiGate VM64-KV	M FG-	SUCURSAL			
🚯 Dashboard	> ^	Edit Interface			
🔆 Security Fabric	>		MANI 1 (port2)		
Network	~	Name	WAN-1 (port2)		
Interfaces	☆	Allas	WAN-1		
DNS					
Packet Capture		VRFID U	0		
SD-WAN Zones		Fotimated handwidth (•	khua Linetroom
SD-WAN Rules		Estimated bandwidth	0		kbps Opsitiean
Performance SLA			0		KDps Downstream
Static Routes		Address			
Policy Routes		Addressing mode	Manual DHCP	Auto-managed by For	tiIPAM
RIP		IP/Netmask	10.10.10.2/255.255	5.255.252	
OSPF		Secondary IP address			
BGP					
Multicast		Administrative Access			
System	>	IPv4	HTTPS	PING	FMG-Access
Policy & Objects	>) SSH	SNMP	FTM
Security Profiles	>		RADIUS Accounting	Connection (
므 VPN	>	Receive LLDP 🕄	Jse VDOM Setting Enal	ble Disable	
User & Authentication	> _				OK Cancel

Figura 346. Configuracion IP port 2 FG-SUCURSAL Fuente: Los autores 6. Configurar el port4 para la red local del fg-sucursal.

FortiGate VM64-KVM	FG-SUCURSAL
🚯 Dashboard	> Edit Interface
Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules	Name RED-LOCAL (port4) Alias RED-LOCAL Type Physical Interface VRF ID O Role LAN
Performance SLA Static Routes Policy Routes RIP OSPE	Addressing mode Manual DHCP Auto-managed by FortilPAM IP/Netmask 192.168.1.20/255.255.255.0 Create address object matching subnet Secondary IP address
BGP	Administrative Access
Multicast System Policy & Objects Security Profiles VPN	IPv4 IPv4 IPv5 IPv6 FMG-Access SSH SNMP FTM RADIUS Accounting Security Fabric Connection 0 FMG-Access Receive LLDP 0 Use VDOM Setting Enable Transmit LLDP 0 Use VDOM Setting Enable
User & Authentication	> ODHCP Server
l네! Log & Report	Address range 192.168.1.1-192.168.1.19 X 192.168.1.21-192.168.1.254 X
	OK Cancel

Figura 347. Configuracion red local port 4 FG-SUCURSAL Fuente: Los autores

7. Configurar DNS al fg-sucursal.

FortiGate VM64-KVM	FG	SUCURSAL	
🚯 Dashboard	>	DNS Settings	
 Security Fabric Network Interfaces DNS Packet Capture 	> ~ ☆	DNS Servers Primary DNS Server Secondary DNS Server Local Domain Name	Use FortiGuard Servers Specify 8.8.8.8 8.8.4.4
SD-WAN Zones SD-WAN Rules Performance SLA		DNS over TLS ()	Disable Enable Enforce
Static Routes Policy Routes RIP OSPF		Interface DNS Server	r 10
BGP Multicast			
 System Policy & Objects Security Profiles 	>		
	>		Apply

Figura 348. Configuracion DNS FG-SUCURSAL Fuente: Los autores

8. Configurar la interfaz que va a pertenecer a la SD-WAN.

FortiGate VM64-KVM	FG-9	SUCURSAL	
🚯 Dashboard	>	Edit SD-WAN Mer	mber
Security Fabric Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules Performance SLA Static Routes Policy Routes RIP		Interface SD-WAN Zone Gateway Cost Status	WAN-1 (port2) Wan-link 10.10.10.1 0 0 Enabled Disabled
OSPF BGP Multicast			
System	>		
Policy & Objects	>		OK Cancel
Security Profiles	>		

Figura 349. Configuracion SD-WAN Zones FG-SUCURSAL Fuente: Los autores

9. Configurar la static routes para la SD-WAN.

FortiGate VM64-KVM	FG-	SUCURSAL					
Dashboard	>	Edit Static Route					
X Security Fabric	>	Duranta Catavara A	2				
Network Interfaces DNS Packet Capture SD-WAN Zones SD-WAN Rules	~	Destination 1 Interface Comments Status	Subnet Internet Service 0.0.0.0/0.0.0.0 Image: SD-WAN Write a comment Image: SD-Walk Image: SD-Walk <th>▼ :: 0/255</th> <th></th> <th></th> <th></th>	▼ :: 0/255			
Static Routes	☆				ОК	Cancel	
Policy Routes							

Figura 350. Configuracion Static routes FG-SUCURSAL Fuente: Los autores 10. Configurar los layer 7 en el mikrotik de redes sociales.

🔔 Wireless		Firewall
👫 Bridge		
🛓 PPP		Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer / Protocols
°T <mark>°</mark> Mesh		
E IP	ARP	Name T Regexp
😴 IPv6 🛛 🗅	Addresses	
Routing D	Cloud	New Firewall L7 Protocol
🔯 System 🗈	DHCP Client	Name: REDES SOCIALES
🗣 Queues	DHCP Relay	Regero:
Files	DHCP Server	Cancel
🗒 Log	DNS	+\$ Apply
RADIUS	Firewall	
🔀 Tools 🛛 🕅	Hotspot	Comment
💵 New Terminal	IPsec	Сору
Nake Supout.rif	Kid Control	Remove
🔁 Manual	Neighbors	
🔘 New WinBox	Packing	,

Figura 351. Configuracion layer 7 redes sociales. Fuente: Los autores

11. Configurar layer 7 para youtube.

vvireiess		Firewall
👯 Bridge		
🛓 PPP		Hiter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer/ Protocols
°T <mark>°</mark> Mesh		
🐺 IP 🗈 🗈	ARP	Name $ abla Regexp$
🖞 IPv6 🗈	Addresses	 YOUTUBE ^.+(youtube.com)youtu.belgooglevideo.com).+\$
Routing N	Cloud	REDES S ^.+(facebook/twitteringtocrom/whatepool) + f Firewall I.7 Protocol (YOUTURE)
🙀 System 🛛 🗅	DHCP Client	
🙅 Queues	DHCP Relay	Name: YOUTUBE OK
📔 Files	DHCP Server	Regexp: Cancel
🗒 Log	DNS	googlevideo.com).+\$ Apply
RADIUS	Firewall	
🔀 Tools 🛛 🗅	Hotspot	Comment
💵 New Terminal	IPsec	Сору
📡 Make Supout.rif	Kid Control	Remove
🖾 Manual	Neighbors	
🚫 New WinBox	Packing	

Figura 352. Configuracion layer 7 youtube. Fuente: Los autores

🏏 Quick Set						
CAPsMAN						
Interfaces						
Wireless		Manda Bula x10.10.10.0/20s				
💥 Bridge				Г		
🏣 PPP		General Advanced Extra Action Statistics			ОК	
1 Mesh		Chain: prerouting	i	1	Cancel	inc
₩ P	Þ	Src. Address: [] 10.10.0/30		Ιľ	Apply	ets
🛬 IPv6	Þ	Det Address	•		1444	
Routing	Þ				Disable	
💭 System	Þ	Protocol:	•	IΓ	Comment	
🗣 Queues		Src. Port:			Cany	
📄 Files		Det Port	•		copy	

12. Configurar un marcado de conexión para la red del enlace SD-WAN.



Mangle Rule <10.10.10.0/30>	
General Advanced Extra Action Statistics	OK
Action: mark connection	₹ Cancel
[] [] [] [] [] [] [] [] [] [] [] [] []	Арріу
Log Prefix:	▼ Disable
New Connection Mark: enlace_sd-wan	Ţ Comment
✓ Passthrough	Сору
Figura 354. Marcado de conexión enlace sd-	wan. (b)

gura 354. Marcado de conexion enlace sa-wan. Fuente: Los autores 13. Configurar un marcado de paquetes para redes sociales.

Mangle Rule <>																										
General Advanced	Extra	Action	Statistics	•																			_		ОК	
Chain:	prerou	ting				_	_	_	_		_	_								 	 ₹				Cancel	
Src. Address:																					•				Apply	
Dst. Address:																					•			[Enable	
Protocol:																					•				Comment	
Src. Port:																									Сору	
Dst. Port:																					•				Remove	
Any. Port:					 								 	 	 						•				Reset Coun	ters
In. Interface:					 	_	 _	_	_		_	_	 	 •				Peart All Cau	ntere							
Out. Interface:					 	_		_		_				 			 		 	 	 •			L	Nesel Al Cou	riters
In. Interface List:																					•					
Out. Interface List:																					•					
Packet Mark:																					•					
Connection Mark:	er	lace_sd-v	van			_															•	h				
Routing Mark:																					 •					
Routing Table:									_		_										•					
																							1			
disabled																										

Figura 355. Marcado de redes sociales. (a) Fuente: Los autores

Mangle Rule <>			
General Advanced Extra Action Statistics			ОК
Src. Address List:	•	•	Cancel
Dst. Address List:	•		Apply
Layer7 Protocol: REDES SOCIALES	•		Enable
Content:	•		Comment
Connection Bytes:	•		Сору
Connection Rate:	•		Remove
Per Connection Classifier:	•		Reset Counters
Src. MAC Address:	•		Reset All Counters
Out. Bridge Port:	•		
In. Bridge Port:	•		
In. Bridge Port List:	•		
Out. Bridge Port List:	-		
IPsec Policy	•		
TLS Host:	-		
		•	
disabled			

Figura 356. Layer 7 redes sociales. (b) Fuente: Los autores

Mangle Rule <>		
General Advanced	Extra Action Statistics	ОК
Action:	mark packet	Cancel
		Apply
Log Prefix:	<pre></pre>	Disable
New Packet Mark:	marcado_pk-REDES-SOCIALES_enlace-sdwan	Comment
	Passthrough	Сору
		Remove
		Reset Counters
		Reset All Counters
enabled	Tiguro 257 Configurosión del poetrot morte redeo escielos (-)

Figura 357. Configuración del packet mark redes sociales. (c) *Fuente: Los autores*

6. Configurar marcado de paquetes para youtube.

Mangle Rule <>							
General Advanced	Extra Action	Statistics					ОК
Chain:	prerouting				₹		Cancel
Src. Address:					•		Apply
Dst. Address:					•		Disable
Protocol:			 	 	•		Comment
Src. Port:					-		Сору
Dst. Port:					_ •		Remove
Any. Port:					_ *		Reset Counters
In. Interface:							Reset All Counters
Out. Interface:					_ •		
In. Interface List:					•		
Out. Interface List:					•		
Packet Mark:					•		
Connection Mark:	enlace_sd-w	van			₹ ▲		
Routing Mark:					•		
Routing Table:					•		
						•	

Figura 358. Marcado de paquetes youtube. (a) Fuente: Los autores

Mangle Rule 🔿				×
General Advanced Extra Action Statistics			ОК	
Src. Address List:	•	٠	Cancel	
Dst. Address List:	•		Apply	
Layer7 Protocol: 🔲 YOUTUBE	F 🔺		Disable	٦
Content:	•		Comment	Ī
Connection Bytes:	-		Сору	
Connection Rate:	•		Remove	Ī
Per Connection Classifier:	•		Reset Counters	Ī
Src. MAC Address:	•		Reset All Counters	Ī
Out. Bridge Port:	•	H		
In. Bridge Port:	•			
In. Bridge Port List:	•			
Out. Bridge Port List:	-			
IPsec Policy:	•			
TLS Host:	•			
		٠		
enabled				-

Figura 359. Layer 7 youtube. (b) Fuente: Los autores

Mangle Rule <>					
General Advanced	Extra Ad	tion Stat	tistics		ОК
Action	mark pack	et		Ŧ	Cancel
	Log			_	Apply
Log Prefix	:			•	Disable
New Packet Mark	marcado_p	ok-YOUTU	IBE_enlace-sdwan	Ŧ	Comment
	Passthro	ough			Сору
					Remove
					Reset Counters
					Reset All Counters
enabled					

Figura 360. Configuración del packet mark youtube. (c) Fuente: Los autores

7. Entrar a youtbe o alguna red social configurada en el layer 7 del mikrotik y vemos que genera paquetes.

Firewall															
Filter Rules NAT Mangle	Raw Ser	vice Ports (Connections	Address Lists	Layer	7 Protocols									
	7 (O Res	et Counters	C Reset A	I Counters									Find	all	Ŧ
# Action Chain	Src. Addre	ss [Proto	Src. Port	Dst Port	In Inter	Out Int	In Inter	Out Int	Src. Ad	Dst Ad	Bytes	Packets			•
::: MARCADO DE CONEXIO	N RED LOC	AL													
0 🔗 mar prerouting	10.10.10.)/									1829.2 KiB	17 508			
::: MARCADO PAQUETES 1	YOUTUBE														
1 🥜 mar prerouting											685 B	6			
::: MARCADO DE PAQUET	E REDES SC	CIALES									000 D				
2 Se mar prerouting											333 B	4			
3 items															



8. Crear una calidad de servicio para el enlace SD-WAN se le asignara upload 10MB y download 10MB.



Figura 362. QOS enlace SD-WAN. Fuente: Los autores

9. Configurar QOS para youtube 4MB/4MB.

Sadmin@0C:78:78:A8:02:00 (MikroTik) - WinBox v7.0beta8 on CHR (x86_64) Session Settings Dashboard ▶ ♥ Safe Mode Session: 0C:7B:78:A8:02:00 🚀 Quick Set CAPsMAN Simple Queues Interface Queues Queue Tree Queue Types 🛨 🗕 🖌 🗶 🖸 🍸 ro Reset Counters ro Reset All Counters Wireless Wireless Bridge PPP Nesh
 #
 Name

 0
 Image: QOS-SDWAN
 Upload Max Limit Download Max Limit Packet Marks 10M 10M Total Max Limit (bi... Target 10.10.10.0/30 YOUTUBE REDES SOCIALES ether2 1M 1M cado_pk-YOU.. eth e <YOUTUBE Pv6 General Advanced Statistics Traffic Total Total Statistics ок Routing Name: YOUTUBE Cance System Target: 10.10.10.0/30 ∓ ≑ Apply Queues
Files Dst.: - -Disable Log Target Upload Target Download Comment Max Limit: 4M ₹ 4M ▼ bits/s Сору X Tools - ▲· Burst Remove ∓ unlimited ∓ bits/s Burst Limit: unlimited Make Supout.rif Reset Counters Burst Threshold: unlimited ∓ unlimited ∓ bits/s 🖳 Manual Burst Time: 0 0 s Reset All Counters New WinBox Time Torch nabled Figura 363. QOS youtube

Fuente: Los autores

10. Configurar al marcado de paquetes de youtube 3MB/3MB

admin@0C:7B:78:A8:0	02:00 (MikroTik) - WinBox v7.0beta8 on CHR (x86_64)	
C ⁴ Safe Mode	Session: 0C:78:78:A8:02:00	
🖌 Quick Set	Queue List	
CAPsMAN	Simple Queues Interface Queues Queue Tree Queue Types	
Interfaces		
Wireless	T V X U V Heset Counters	
👯 Bridge	# Name Target Upload Max Limit Download Max Limit Packet Marks Total Max Limit (bi	
늘 PPP	1 = YOUTUBE 10.10.10./30 4M 4M marcado pk-YOU	
° 🕻 Mesh	2 REDES SOCIALES ether service woll TURES	
IP N	Simple Queue <toutube></toutube>	
🛫 IPv6 🛛 🗅	General Advanced Statistics Traffic Total Total Statistics OK	
Routing N	Packet Marks: marcado_pk-YOUTUBE_enlace-sdwan ▼ ◆ Cancel	
💭 System 🗅		
Queues	Target Upload Target Download 74000	
Files	Limit At: [3M = [3M = bits/s] Disable	,
Log	Priority: 8 8 Commer	*
RADIUS	Bucket Size: 0.100 0.100 ratio	<u> </u>
🔀 Tools 🛛 🗅	Queue Type: default-small Copy Copy	
💵 New Terminal	Remove	e
Make Supout.rif	Parent: none 🗧 Reset Cour	nters
🖳 Manual	Durb 41 Co	
New WinBox	Heset All Cou	Inters
🛃 Exit	Torch	
	enabled	

Figura 364. QOS marcado de paquetes youtube Fuente: Los autores

11. Configurar QOS para redes sociales.

🔘 ac Sessi	lmin@0C:7B:78: on Settings	A8:0 Dasł	2:00 (MikroTik) hboard	- WinBox v7.0b	eta8 or	n CHR (x86_64)							
6	CM Safe Mode	;	Session: 0C:7B:7	78:A8:02:00									
	 Quick Set CAPsMAN Interfaces 		Queue List Simple Queues	Interface Que	ues G	Queue Tree Que	eue Type	is	_				
0.00	Wireless		# Name 0 = QO 1 = YO	S-SDWAN UTUBE	Targ 10.1 10.1	et 0.10.0/30 0.10.0/30	Upload 10M 4M	Max Limit	Downloa 10M 4M	ad Max I	imit Packet Marks	Total Max Limit (b	i
	Mesh IP IPv6 Routing	1	2 💻 RE	DES SOCIALES	ethe	Simple Queue < General Adv	REDES anced	SOCIALES> Statistics	Traffic	Total	Total Statistics		
	System Queues Files	1				Targe Dst	t: ether	2 2	2			₹	Apply
	Log PRADIUS	1				Max Limi - ▲ · Burst	t: 4M		Target	Upload Ŧ	Targ 4M	et Download The bits/s	Comment
	New Terminal Make Supout.ri Manual	if				Burst Limi Burst Threshold	t: unlimi d: unlimi	ted ted		Ŧ	unlimited unlimited	➡ bits/s ➡ bits/s	Remove Reset Counters
	New WinBox					Burst Time	e: U				0	S	Reset All Counters
						enabled							

Figura 365. QOS redes sociales. Fuente: Los autores

12. Configurar QOS al marcado de paquetes para redes sociales.



Figura 366. QOS marcado de paquetes redes sociales. *Fuente: Los autores*

RECURSOS UTILIZADOS

- > COMPUTADORA
- CABLE DE RED (PATCHCORD)
- ≻ GNS3

CRONOGRAMA/CALENDARIO

De acuerdo a la planificación de cada docente

CAPÍTULO V

ANÁLISIS DE RESULTADOS

5.1. Análisis del proyecto

Se realizó la respectiva verificación que el proyecto cumpla los objetivos preliminarmente determinados y además se comprobó el funcionamento correcto del servidor DELL R210 II y el uso de aplicación cliente de GNS3 al instante de ejecutar la conexión al GNS3-SERVER donde utilizara los recursos de memoria RAM y CPU que le suministrara el servidor.

5.2. Comunicación de las computadoras clientes al servidor

Mediante conexión Ethernet, el servidor y las computadoras clientes deben estar conectadas a un mismo switch y pertenecer al mismo segmento de red, para la conexión al ambiente virtual para ejecutar las simulaciones de redes definidas por software se debe encender la máquina virtual que se halla instalada en el servidor accediendo a el a tráves de la dirección IP se que configuro, una vez iniciada la máquina virtual de GNS3-SERVER se instala la aplicación de GNS3 cliente y se enlaza mediante la dirección IP del GNS3-SERVER.

5.3. Elaboración del banco de prueba y prácticas.

Se realiza diez prácticas de redes definidas por software para redes de área amplias utilizando el ambiente virtual de GNS3 con sus respectivos dispositivos como routers, firewall y switch para la simulación además en este proyecto se manifiesta la instalación de virtualización con EXSI, GNS3 SERVER, memorias RAM, disco duros de estado sólidos SSD este banco de prueba sirve para simular diferentes protocolos de redes y nuevos equipos de seguridad, routers, switches y sistemas operativos que vayan surgiendo a tráves del tiempo.

5.4. Pruebas realizadas

Se ejecuta la verificación que las computadoras clientes del laboratorio de telecomunicaciones de la Universidad Politécnica Salesiana sede Guayaquil tengan conexión con el servidor a través de la aplicación de GNS3 cliente.



Figura 367. Verificación de conexión al servidor Fuente. Los autores

Una vez realizada la conexión al servidor ingresamos automáticamente al ambiente virtual donde se encuentran elaboradas las prácticas.



Figura 368. Verificación de conexión al servidor Fuente. Los autores

Adicional antes de instalar GNS3 o al conectarse a través de la aplicación desactivar el antivirus o firewall del sistema operativo que se utilizando le mostrara en letras amarillas que esta siendo bloqueada la conexión al servidor.



Figura 369. Firewall bloqueando conexión Fuente. Los autores

CAPÍTULO VI

CONCLUSIONES

El objetivo principal de este proyecto técnico de un banco de pruebas para redes definidas por software de una manera virtualizada es que el estudiante consiga trabajar, configurar y diseñar redes de última generación, diseños de redes complejos con CISCO, Mikrotik, Palo Alto solo añadiendo el KVM de cualquier dispositivo al servidor utilizando los recursos de CPU y memoria RAM donde solo con la aplicación de GNS3 cliente podrá conectarse al servidor, se lo puede realizar con cualquier equipo sea PC o laptop alta y baja gama.

Para la elaboración del banco de pruebas se mejoró los recursos del servidor instalando adicionalmente 16GB de memoria RAM, el servidor constaba con 8GB de memoria y asimismo se incrementó dos unidades de estado sólido de 240GB cada uno sustituyendo el HDD mecánico.

Cabe resaltar que en el laboratorio de telecomunicaciones de la Universidad Politécnica Salesiana sede Guayaquil constan computadoras de baja gama para la actualidad y frena desarrollar prácticas de simulaciones de redes informáticas en la actualidad se utiliza CISCO PACKET TRACER obteniendo una limitante en el momento de diseñar una red de datos complejas permitiendo solo simular sus dispositivos que aparecen incluidos en el software.

El resultado de este proyecto técnico es que los estudiantes ensayen como configurar equipos que en la actualidad son costosos en obtener, una de las ventajas de este proyecto que los estudiantes lograrán defenderse en el momento de efectuar sus pasantías pre-profesionales simulando equipos que constan instalado en las empresas asi obteniendo conocimiento para futuros proyectos.

Al instante de terminar la instalaciones de los discos SSD, memorias RAM, software de virtualización y la creación de la maquina virtual para el ambiente de desarrollo para las prácticas se realizó la conexión de todas las computadoras del laboratorio de telecomunicaciones de la Universidad Politécnica Salesiana sede Guayaquil al servidor, obteniendo un resultado satisfactorio.

Para el desarrollo de este proyecto se realizo diez prácticas **PRÁCTICA 1**: Conexión remota al servidor virtual con el software GNS3, **PRÁCTICA 2**: Configuración de una red SD-WAN con Fortigate 6.2.0,**PRÁCTICA 3**: Configuración de una red SD-WAN con perfomance SLA en fortigate 6.4.2, **PRÁCTICA 4**: Configuración de una red SD-WAN con prioridad de servicios con sd-wan rules, **PRÁCTICA 5:** Configuración de una red SD-WAN con fortigate y enlazados con dispositivos mikrotik, **PRÁCTICA 6:** Configuración de una red VPN IPSEC fortigate a fortigate, **PRÁCTICA 7:** Configuración de una red VPN IPSEC con balanceo sd-wan, **PRÁCTICA 8:** Configuración de un failover con mikrotik para un enlace SD-WAN,**PRÁCTICA 9:** Configuración de un mangle con mikrotik para el enlace SD-WAN, **PRÁCTICA 10:** Configuración de un layer 7 con calidad de servicios QOS para el enlace SD-WAN utilizando mikrotik, donde los estudiantes pondrán los recursos suficientes para las prácticas y nuevos KVM para simular diferentes equipos.

CAPÍTULO VII

RECOMENDACIONES

Verificar que todas las conexiones eléctricas que se conectan al servidor estén en perfecto estado.

Actualizar el ambiente virtual del GNS3-SERVER cada vez que surja una nueva versión a través de la configuración del software de la máquina virtual.

Antes de actualizar realizar un backup a la máquina virtual.

Cambiar el servidor por uno más actual para realizar multiples conexiones de usuarios finales y poder realizar simulaciones de alto rendimiento en CPU y memoria RAM.

Instalar software libre de virtualización se recomienda PROXMOX.

El servidor debe estar conectado en un punto de red del laboratorio de telecomunicaciones.

Para la administración del servidor y sus configuraciones se pide que tenga conocimiento en EXSI.

CAPÍTULO VIII

REFERENCIAS BIBLIOGRAFÍA

Yenisleidy Fernández, Karen García. (2011). *Virtualización*. Cuba: Revista Digital De Las Tecnologías De La Información Y Las Comunicaciones. Obtenido de http://revistatelematica.cujae.edu.cu/index.php/tele/issue/view/4

Andrew.S. Tanenbaum & David Wetherall. (2012). *Redes de computadoras.* México: Pearson Educación. Obtenido de <u>https://bibliotecavirtualapure.files.wordpress.com/2015/06/redes_de_comput</u> <u>adoras-freelibros-org.pdf</u>

Francisco Molina.(2014). *Redes Locales*.Madrid:RA-MA,S.A. Obtenido de <u>https://bibliotecas.ups.edu.ec:2708/lib/bibliotecaupssp/detail.action?docID=3</u> 228517

Rafael Castaño, Jesús López.(2013). *Redes Locales*.España: MacMillan Iberia,S.A.Obtenido de <u>https://bibliotecas.ups.edu.ec:2708/lib/bibliotecaupssp/detail.action?docID=3</u>217345&query=redes+locales

Enrique Bellido.(2013). *Implementanción de los elementos de la red local*. Madrid:Editorial CEP,S.L. Obtenido de <u>https://bibliotecas.ups.edu.ec:2708/lib/bibliotecaupssp/detail.action?docID=4</u> <u>499051&query=red+local</u>

Julio Gómez López.(2014). *ADMINISTRACIÓN DE SISTEMAS OPERATIVOS*.MADRID:RA-MA EDITORIAL. Obtenido de <u>https://bibliotecas.ups.edu.ec:2708/lib/bibliotecaupssp/detail.action?docID=5</u> <u>758899&query=administracion+de+sistemas</u>

Francisco Carvajal Palomares.(2017). Instalación y configuración del software del servidor Web.Madrid: Editorial CEP S.L. Obtenido de <u>https://bibliotecas.ups.edu.ec:2708/lib/bibliotecaupssp/detail.action?docID=5</u>214031&query=Instalaci%C3%B3n+y+configuraci%C3%B3n+del+software+<u>de+servidor+Web</u>

Alfredo Abad Domingo.(2012).*Redes Locales*. McGraw-Hill/Interamericana de España, S.L. Obtenido de <u>https://juanantonioleonlopez.files.wordpress.com/2017/11/redes-locales.pdf</u>

CAPÍTULO IX

ANEXOS

ANEXO A. CRONOGRAMA DE DURACIÓN DEL PROYECTO

CRONOGRAMA DEL PROYECTO						
		6 M	ESES			
MES 1	MES 2	MES 3	MES 4	MES 5	MES 6	
	DEL PRO	DEL PROYECTO MES 1 MES 2 	DEL PROYECTO 6 M MES 1 MES 2 MES 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	DEL PROYECTO 6 MESES MES 1 MES 2 MES 3 MES 4 MES 1 MES 2 MES 3 MES 4 1 MES 4 1 MES 2 MES 3 MES 4 1 MES 4	DEL PROYECTO 6 MESES MES 1 MES 2 MES 3 MES 4 MES 5 MES 1 MES 2 MES 3 MES 4 MES 5 MES 1 MES 2 MES 3 MES 4 MES 5 MES 1 MES 2 MES 3 MES 4 MES 5 MES 1 MES 2 MES 3 MES 4 MES 5 MES 1 MES 2 MES 3 MES 4 MES 5 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Image: MES 1 Ima	

Tabla 1. Cronograma del proyecto técnico

ANEXOS B. Sistemas Operativos de virtualización

SOFTWARE DE VIRTUALIZACIÓN	CARACTERISTICAS	VENTAJAS	DESVENTAJAS
VMware Sphere	Consolidar el hadware para mejorar la utilización de la capacidad. Aumentar el rendimiento para logar una ventaja competitiva. Reducir la inversión en capital y los gastos operativos,	Eficiencia gracias a la utilización y a la automatización. Reducción drástica de los costes de TI.	El precio de una solución paga de vSphere puede llegar entre \$4000y \$8000. No es compatible con una gran lista de hardware domestico.
Red Hat Virtualization	Basado en Linux. Colaboración open source.	Virtualizacion abierta permite ahorrar dinero. Rendimiento mejorado de las cargas de trabajo.	Acceder a un soporte completo y adecuado. Regimen de pago o suscripción.

		Configuración sencilla.	
Proxmox VE	Código abierto. Permite la migración. Plantillas SO.	Aprovechamiento de recursos. Flexibildiad para testing. Clustering. Alta disponibilidad (HA).	RAID (desventaja en relación a la necesidad de tener discos iguales. Requiere hardware costoso. Mayor probabilidad a fallas fatales.
Microsoft Hyper-V	Memoria dinámica. Migración en vivo. Migración de almacenamiento.	Ahorro en costes de hardware.Facilitación de creación de backup.Establece o amplia un entorno de nube privado.	Aplicaciones mas lentas. Requiere licencia de software. Es utilizado generalmente para Windows.

Tabla 2. Comparación de sistemas operativos de virtualización

ANEXO C. DELL R210 II

Procesadores	Familia de productos del procesador E3- 1200 de cuatro núcleos Intel® Xeon® Familia de productos del procesador i3- 2100 de dos núcleos Intel Core™ Series G600 y G800 de dos núcleos Intel Pentium® Series G400 y G500 de dos núcleos Intel Celeron®
Chipset	Intel C202
Memoria	Hasta 32 GB (4 ranuras DIMM): DDR3 de 1 GB/2 GB/4 GB/8 GB hasta de 1333 MHz
Opciones de virtualización	Citrix® XenServer®
	VMware® vSphere® ESX™ y ESXi™ Red Hat Enterprise Virtualization®
	Microsoft® Windows Server® 2012
Sistemas operativos	Microsoft Windows Server 2012 Essentials

	Microsoft Windows® Small Business Server 2011					
	Microsoft Windows Small Business Server 2008					
	Microsoft Windows Server 2008 R2 Foundation SP1					
	Microsoft Windows Server 2008 SP2, x86/x64 (x64 incluye Hyper-V®)					
	Microsoft Windows Server 2008 R2 SP1, x64 (incluye Hyper-V v2)					
	Microsoft Windows HPC Server 2008					
	Novell® SUSE® Linux Enterprise Server					
	Red Hat® Enterprise Linux®					
	Unidad de estado sólido de 2,5" SATA, SAS (10.000 RPM)					
Opciones de almacenamiento	SAS (15.000 RPM) de 3,5", SAS nearline (7.200 RPM), SATA (5.400 RPM, 7.200 RPM).					
Capacidad máxima de almacenamiento interno	Hasta 6 TB					
Controladora integrada de red	Una Broadcom BCM 5716 de dos puertos					
	PERC S100 (basada en software)					
Controladoras RAID	PERC S300 (basada en software)					
	PERC H200 (6 Gb/s)					

Tabla 3 .Especificaciones del Servidor Dell PowerEdge R210 II
ANEXO D. Disco Solido SSD

Factor de forma	2,5" y M.2 2280
Interfaz	SATA Rev. 3.0 (6 Gb/s), retrocompatible con SATA Rev. 2.0 (3 Gb/s)
Capacidades ²	120GB, 240GB, 480GB, 960GB, 1,92 TB
NAND	3D
Consumo eléctrico	0,195 W en reposo / 0,279 W promedio / 0,642 W (máx) lectura / 1,535 W (máx) escritura
Dimensiones	100,0 mm x 69,9 mm x 7,0 mm (2,5") 80 mm x 22 mm x 1,35 mm (M.2)
Peso	40g
Temperatura de servicio	0°C~70°C
Temperatura de almacenamiento	-40°C~85°C
Vibraciones en funcionamiento	2,17 G máxima (7-800 Hz)
Vibración en reposo	20 G máximo (10-2000 Hz)
Vida útil	1 millón de horas MTBF
Bytes escritos en total (TBW) ⁴	240GB: 80TB

Tabla 4: KINGSTON A400 SSD SATA de 2,5"

ANEXO E. LISTADO DE MATERIALES

EQUIPO	VALOAR
MEMORIAS RAM	125 \$
DISCO DUROS SSD	85 \$

Tabla 4: Materiales del proyecto técnico