Universidad Autónoma Metropolitana – Azcapotzalco

División de Ciencias Básicas e Ingeniería

Licenciatura en Ingeniería en Computación

Administración e Implementación de seguridad en una red corporativa

Modalidad: Estancia Profesional

Trimestre 2017-Primavera

Fabián Chávez Cruz
209203102

Asesor:

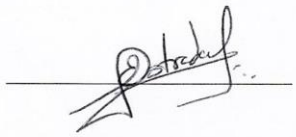
M. en C. José Alfredo Estrada Soto
Profesor Titular

Jefe directo:

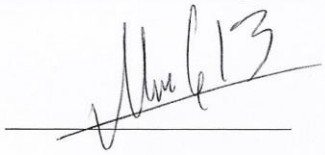
Ing. Mario Ernesto Gómez Romero

21 de julio de 2017

Yo, José Alfredo Estrada Soto, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.



Yo, Mario Ernesto Gómez Romero, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.



Yo, Fabián Chávez Cruz, doy mi autorización a la Coordinación de Servicios de la Universidad Autónoma Metropolitana, Unidad Azcapotzalco, para publicar el presente documento en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

Resumen.

El presente trabajo muestra el desarrollo del proyecto Administración e Implementación de seguridad en una red corporativa, lo cual resulta verdaderamente necesario hoy en día para que las empresas puedan efectuar de manera segura todas sus actividades, teniendo especial cuidado en mantener libre de riesgos los datos tanto del personal de la empresa, así como los de sus clientes.

A través del uso de firewalls de la marca Fortinet y la implementación de sus respectivas políticas, apoyado de otras herramientas de la misma marca y un sistema de monitorización se logró mantener la información segura.

Contenido

Introducción 1
Antecedentes 2
Justificación 4
Marco Teórico 5
Desarrollo del proyecto. 7
Resultados 38
Análisis y discusión de resultados 41
Conclusiones 43
Referencias Bibliográficas 44

Contenido figuras y tablas

Figura 1: IP Fortigate 7
Figura 2: Acceso Fortigate 8
Figura 3: Interfaces Fortigate 8
Figura 4: Interfaces de administración 9
Figura 5: Interfaces LAN 9
Figura 6: Web Rating Overrides 10
Figura 7: Edición Web Rating Overrides 10
Figura 8: Características Web Rating Overrides 10
Figura 9: Traffic Shaper 11
Figura 10: Características Traffic Shaper 12
Figura 11: Categorías web visitadas 13
Figura 12: Categorías por aplicación 14
Figura 13: Tráfico por aplicación 15
Figura 14: Tráfico fuente 15
Figura 15: Tráfico destino 16
Figura 16: Amenazas por sitio web 17
Figura 17: Amenazas por aplicación 18
Figura 18: Incidente IPS 18
Figura 19: Incidente IPS por fuente 18
Figura 20: Incidente IPS por destino 19
Figura 21: VPN's 19
Figura 22: Zabbix Dashboard 20
Figura 23: Gráfica Bestel 21
Figura 24: Gráfica MAXCOM 21
Figura 25: Gráfica SERVNET 22
Figura 26: LAN Azteca 22
Figura 27: LAN Jenner 23
Figura 28: LAN Olab 23
Figura 29: Túnel VPN FUJI 24
Figura 30: Gráfica PACS 24
Figura 31: Configuración hosts 25
Figura 32: Items 25
Figura 33: Filtro VPN 25
Figura 34: Información item 26
Figura 35: Continuación información item 27
Figura 36: Creación trigger 28
Figura 37: Túnel VPN sitio a sitio 29
Figura 38: Opciones VPN 30
Figura 39: Parámetros VPN 31
Figura 40: Autenticación 32
Figura 41: Fase 1 VPN 32
Figura 42: Autenticación extendida 33

Figura 43: Direccionamiento fase 2 33
Figura 44: Parámetros de cifrado 34
Figura 45: IPsec monitor 35
Figura 46: Estado túnel vpn 36
Figura 47: Ruta estática 36
Figura 48: Política VPN 37
Figura 49: Primer día de monitoreo 41
Figura 50: Cuarto día de monitoreo 41
Figura 51: Séptimo día de monitoreo 42

Tabla 1: Valores sugeridos VPN 31
Tabla 2: Valores sugeridos autenticación 32
Tabla 3: Parámetros fase 1 33
Tabla 4: Parámetros fase 2 35
Tabla 5: Sitios web de alto riesgo 38
Tabla 6: Ataques y vulnerabilidades 39
Tabla 7: Aplicaciones basadas en cloud 40

Introducción

Para los seres humanos la seguridad es una necesidad básica la cual se refiere a la certeza que tienen los mismos de estar libres de todo daño, amenaza, peligro o riesgo; tomando en cuenta lo anterior hoy en día la seguridad resulta de vital importancia en diversos ámbitos como, por ejemplo: las tecnologías de la información, pero particularmente en la seguridad de las redes de computadoras en las redes corporativas como tema central de esta propuesta.

La seguridad en las redes de computadoras es el conjunto de protocolos, dispositivos, herramientas y diversas técnicas que mantienen los datos protegidos e intenta minimizar el número de amenazas tanto como sea posible. Lo cual surge por la necesidad de evitar que personas no autorizadas y con fines malintencionados tengan acceso a la información.

Una red corporativa es aquella que nos permite conectar todos los departamentos de una empresa de forma privada, por lo que debe ser rápida y segura; a la vez comprende dos tipos de seguridad que son:

- Seguridad física: comprende lo referente a establecer barreras físicas y de control del personal que tiene acceso a los dispositivos que conforman la red, así como establecer medidas contra desastres naturales como incendios, descargas eléctricas, inundaciones, etc.
- Seguridad lógica: consiste en la aplicación de barreras y procedimientos, de tal forma que solo el personal autorizado pueda acceder a la información.

Las redes corporativas sufren cambios constantes debido a los avances tecnológicos, lo que implica también un cambio en el enfoque de las tecnologías de la información, por lo cual las soluciones a las diferentes problemáticas deberían estar diseñadas en función del paradigma empresarial y de los recursos tecnológicos que tengan a su disposición.

Por la tanto el presente documento muestra cómo se implementaron las políticas de seguridad y su sistema de monitoreo en una red corporativa.

Antecedentes

Proyectos de integración o terminales

Implementación de una NIDS en un sistema embebido para el análisis de tráfico en una red [1].

Este proyecto tiene una fuerte relación con la propuesta ya que hace uso del software de análisis de tráfico en una red. El software utilizado para este proyecto fue Zabbix, es un sistema de monitorización de redes de código abierto, el cual se adapta a las necesidades de la empresa.

Diseño e implementación de un sistema honeypot como elemento para la seguridad de una red privada [2].

El proyecto tiene una fuerte relación ya que al ser un dispositivo para la seguridad en redes, cuya función es atraer y analizar ataques, con el fin de conocer las pautas de ataque de los hackers, bots o alguna otra amenaza. El uso del honeypot no fue necesario ya que el firewall de la marca Fortinet al incorporar un IPS resulta suficiente para proporcionar protección en tiempo real de ataques maliciosos.

Artículos

Wireless Network Security and Interworking [3].

En redes WLAN la integridad de la información sigue teniendo una alta prioridad, al igual que en redes LAN se utilizan herramientas similares para la seguridad, pero al ser el medio físico de transmisión diferente se deberán tener consideraciones específicas dictadas por estándar IEEE 802.11. En este proyecto se interactuó con los dispositivos de red inalámbricos, en este caso Access Points, de fabricantes distintos, los cuales no tuvieron ningún problema para interactuar con el Firewall.

Using policies for effective network management [4].

En este artículo se presenta una clasificación de las políticas que nos ayudará a reducir la compleja administración de la red. En este proyecto las políticas fueron adecuadas en función de los servicios solicitados por el usuario.

Tesis

Algoritmos Genéticos Paralelos y su Aplicación al Diseño de Redes de Comunicación Confiables [5].

La tesis aborda el diseño de redes y los problemas que puedan surgir, planteando el diseño de una topología de un modo en que se puedan verificar características de confiabilidad mediante el uso de métodos heurísticos. En este proyecto las características fueron verificadas directamente sobre la topología de la red, usando la documentación correspondiente proporcionada por la empresa.

Vulnerabilidades de las Redes TCP/IP y Principales Mecanismos de Seguridad [6].

En esta tesis se aborda el tema de la seguridad de manera general en el modelo TCP/IP, describiendo las vulnerabilidades en cada una de las capas que lo conforman. En este proyecto se analizaron vulnerabilidades a nivel de las capas de Internet y Transporte.

Justificación

Hoy en día la inseguridad se encuentra presente de diversas formas en nuestro ámbito social, y las redes de computadoras no son la excepción. Particularmente en las empresas los usuarios de la red deben poder realizar el intercambio de información libre de cualquier riesgo, y así proteger los recursos y servicios informáticos de amenazas tanto internas como externas, por lo que deben contar con una red sólida y escalable.

Al contar con los mecanismos de seguridad adecuados y empleando las tecnologías disponibles, se logró un esquema más eficiente en la transferencia de archivos, en este caso imágenes de alta resolución.

Objetivo general

Administrar e implementar políticas de seguridad en una red corporativa con el fin de garantizar la integridad de la información.

Objetivos específicos

- Identificar los elementos que conforman la red corporativa, con el fin de tener la descripción física de la misma, mediante la elaboración de un diagrama red.
- Identificar las vulnerabilidades de la red, con el fin de encontrar las debilidades en las plataformas de software o hardware para solucionar las fallas antes de tener un impacto negativo en la información, utilizando un software de monitorización de red.
- Diseñar políticas de seguridad, para establecer medidas de seguridad, mediante la elaboración de la documentación donde se establecerán dichos procedimientos.

Marco Teórico

Seguridad en redes.

La seguridad de redes consiste en las políticas adoptadas para prevenir y monitorear el acceso no autorizado, el mal uso, la modificación o la denegación de una red de computadoras y recursos de acceso de red. La seguridad de redes cubre una variedad de redes, ya sean públicas o privadas, que se usan en los trabajos de todos los días; llevando a cabo transacciones y comunicación entre negocios, organismos gubernamentales e individuos [12].

Red Corporativa.

Una red corporativa es una red privada que maneja datos confidenciales y propietarios. Cada organización en cada ubicación geográfica puede poseer una red privada. Las redes privadas pueden tener direccionamientos y protocolos exclusivos y no tienen que ser compatibles con internet. Se podrían utilizar sistemas de traducción y diversos protocolos de tunelización para que interoperen redes privadas y públicas incompatibles [13].

QoS.

Calidad de servicio (QoS) es un conjunto de tecnologías que permite que las aplicaciones soliciten y reciban niveles de servicio predecibles en términos de la capacidad de rendimiento de datos (ancho de banda), variaciones de latencia (fluctuación) y retraso. En particular, las funciones de QoS ofrecen un servicio de red mejor y más previsible. A su vez refiere a la capacidad de una red de proporcionar un mejor servicio al tráfico de la red seleccionada sobre las diversas tecnologías subyacentes incluyendo el Frame Relay, Asynchronous Transfer Mode (ATM), los Ethernetes y 802.1 redes, SONET, y las redes ruteadas por IP [14].

Ancho de Banda.

En conexiones a Internet el ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bits por segundo (Bps), kilobits por segundo (Kbps), o megabits por segundo (Mbps) [15].

Firewall.

Es un dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad [16].

Traffic Shaping.

Es la manipulación y priorización del tráfico de red, cuyo objetivo es evitar la sobrecarga de red con altas ráfagas de tráfico inyectado, garantizando QoS. Esto se consigue retrasando el flujo de ciertos paquetes y priorizando el flujo de otras corrientes preferidas por conjuntos predeterminados de restricciones [17].

VPN.

Una VPN es una red privada que se crea mediante el uso de túneles sobre una red pública, usualmente internet. En lugar de utilizar conexiones físicas dedicadas, una VPN utiliza conexiones virtuales enrutadas a través de internet desde la organización hasta el sitio remoto [18].

VPN Sitio a Sitio.

Es aquella que se crea cuando los dispositivos de conexión en ambos extremos de la conexión VPN conocen la configuración VPN de antemano. La VPN permanece estática y los hosts internos no tienen conocimiento de la existencia de la VPN [18].

Desarrollo del proyecto.

En el proyecto se realizaron las siguientes actividades:

Administración de los firewalls.

Los firewalls utilizados en este proyecto son de la marca Fortinet entre los cuales tenemos los modelos 600D, 90D, 60D y 50C.

Para acceder a la interfaz gráfica de los dispositivos necesitamos lo siguiente:

- Dirección IP pública del Fortigate para acceder desde Internet.
- Puerto de acceso al Fortigate vía web (9447).
- Usuario y contraseña Super-Admin del dispositivo.

Acceso WEB.

Por default un Fortigate de fábrica siempre es accesado mediante el protocolo HTTPS a través del puerto 443, sin embargo, siguiendo las directrices de la empresa el acceso se efectúa a través del puerto 9447.

I. Mediante el uso de un navegador y de acuerdo a lo siguiente https://DIRECCIONIPPUBLICAFORTIGATE:9447

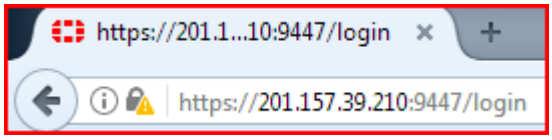


Figura 1: IP Fortigate

La figura anterior nos muestra el acceso a un Fortigate mediante su IP, a través de un navegador web, en este caso se hace uso de Mozilla FireFox.

II. Nos llevará a esta pantalla en la cual ingresaremos el usuario y contraseña con el nivel de privilegios necesarios.

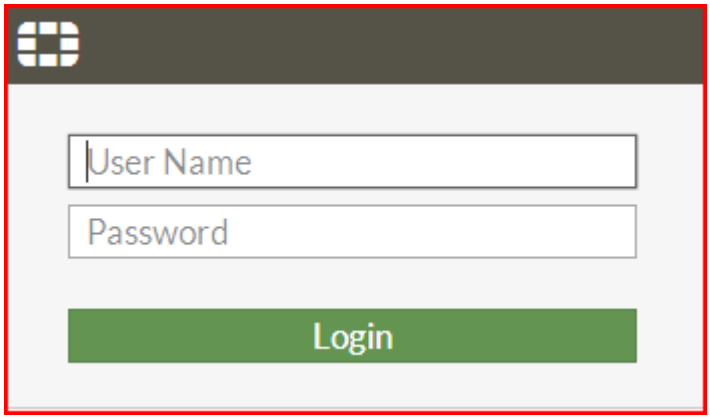


Figura 2: Acceso Fortigate

En la figura anterior nos muestra la interfaz en donde se escriben el usuario y contraseña, con los privilegios de SuperAdmin proporcionados por la empresa.

El Fortigate nos muestra de forma gráfica el estado de sus conexiones físicas, además de indicar los segmentos de red con su respectiva mascara que tiene conectados, en el caso de **Ref**, nos indica en cuantas políticas está presente.

Figura 3: Interfaces Fortigate

La figura anterior nos indica en color verde los puertos que se encuentra activos en el Fortigate.

Status	Name	Members	IP/Netmask	Type	Access	Ref.
sical (19)						
	mgmt1 (MAXCOM)		201.157.39.210 255.255.255.240	Physical Interface	PING HTTPS SSH SNMP	39
	mgmt2 (BESTEL)		201.148.87.138 255.255.255.248	Physical Interface	PING HTTPS SSH SNMP	39

Figura 4: Interfaces de administración

En la figura anterior nos muestra dos de las interfaces utilizadas para la administración del equipo, correspondiente a un ISP distinto cada una, a su vez nos indica la IP pública de cada interfaz con su respectiva mascara de red, el tipo de interfaz que es y los protocolos por los cuales el equipo puede ser accesado.

	port9 (LAN_Olab_CC)		172.17.2.254 255.255.255.0	Physical Interface	PING HTTPS SSH	42
	port10 (WIFI_OLABCC)		10.1.1.1 255.255.255.0	Physical Interface	PING HTTPS SSH	37
	port11 (PACS)		192.192.192.254 255.255.255.0	Physical Interface	PING HTTPS SSH	14
	port12 (LAN_Azteca_CC)		192.168.50.254 255.255.255.0	Physical Interface	PING HTTPS SSH	14
	port13 (SERVNET)		201.150.43.214 255.255.255.252	Physical Interface	PING HTTPS SSH	16
	port14 (LAN_Jenner_CC)		172.16.72.254 255.255.255.0	Physical Interface	PING HTTPS SSH	10

Figura 5: Interfaces LAN

La figura anterior muestra las redes que tiene conectadas el equipo tanto cableadas, así como las inalámbricas, tipo de interfaz y protocolos por los cuales pueden ser accesados.

Alta de URL´s.

El procedimiento a realizar es el siguiente:

i. Ingresar al Fortigate, ir al apartado de **Security Profiles -> Web Rating Overrides**, hacer click en el botón **Create New.**

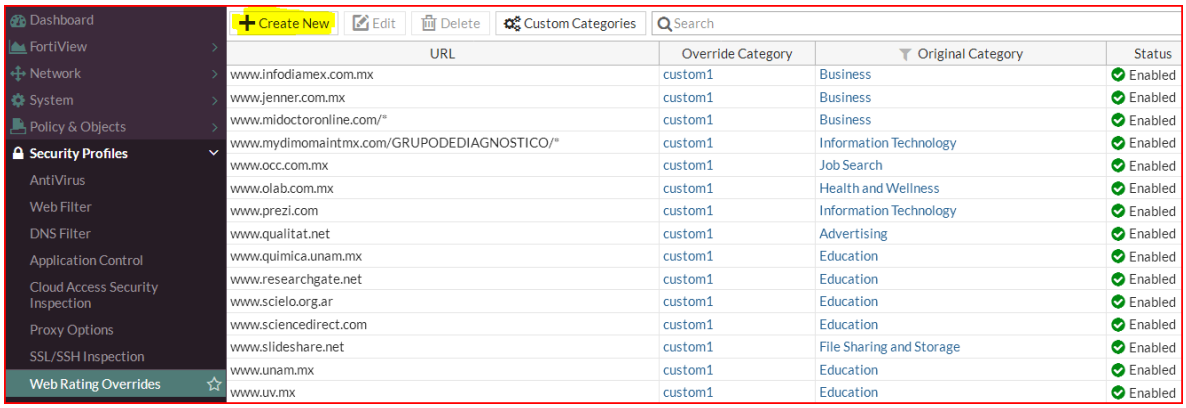


Figura 6: Web Rating Overrides

La figura anterior nos muestra el apartado de Web Rating Overrides, en donde podemos apreciar que ya hay otras URL's dada de alta.

ii. Ingresamos la URL en el campo URL, en la opción **Category** seleccionamos **Custom Categories** y en la opción **Sub-Category** seleccionamos **custom1**.

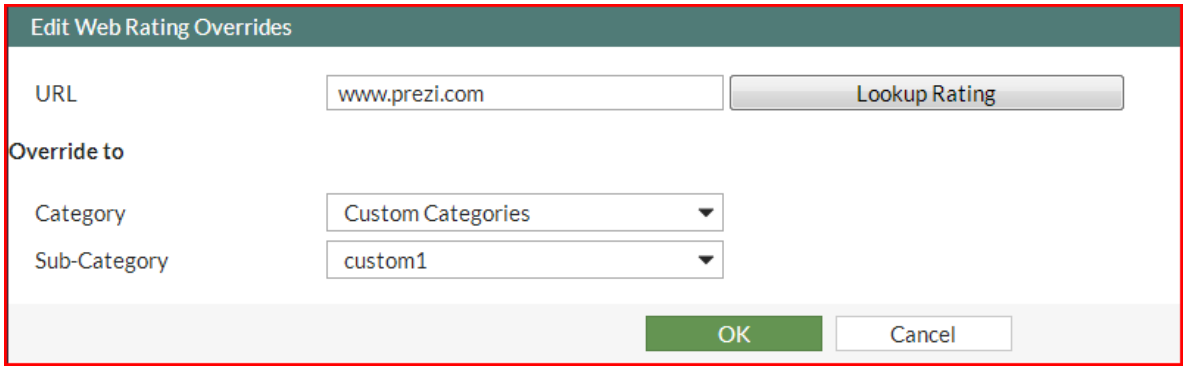


Figura 7: Edición Web Rating Overrides

La figura anterior muestra la ventana en donde se editan las URL's, en donde Custom Categories es lo que nos permitirá que pueda ser accesada la URL escrita con anterioridad sin ninguna restricción.

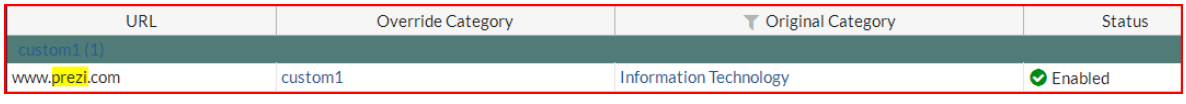


Figura 8: Características Web Rating Overrides

En la figura anterior podemos observar que la URL fue dada de alta de manera exitosa mostrándonos su estado y otras características.

Creación de Traffic Shapers.

i. Nos dirigimos al apartado de **Policy & Objects -> Traffic Shapers.**
ii. Damos click en **Create New**.
iii. Elegir un nombre para el objeto.
iv. Establecer la prioridad del traffic shaper.
v. Asignar el ancho de banda garantizado y máximo.
vi. Dar click en OK.

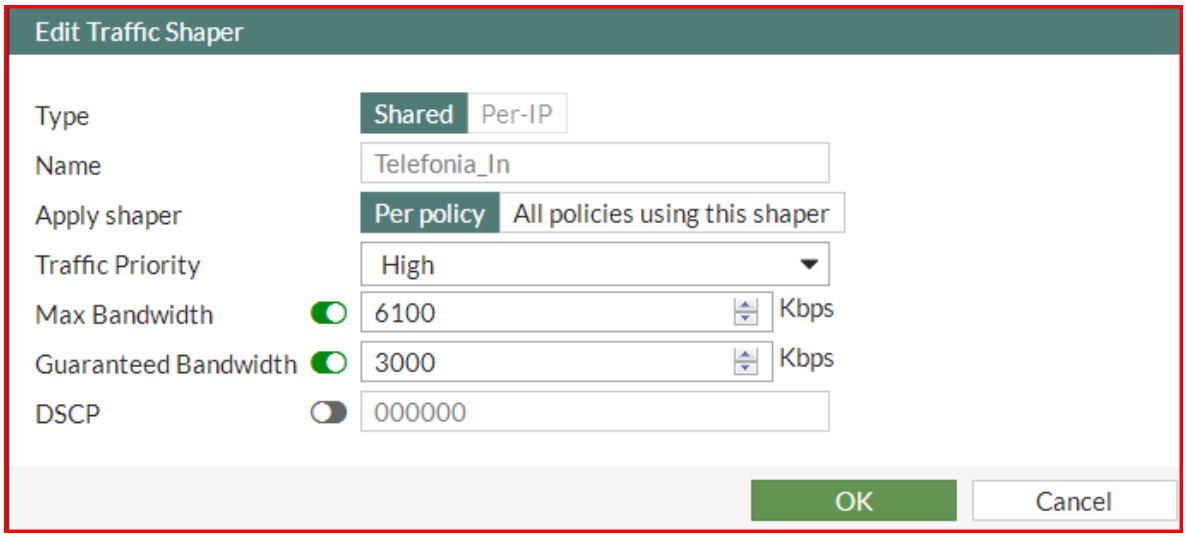


Figura 9: Traffic Shaper

En la figura anterior tenemos la ventana donde se edita el traffic shaper para su creación, se usa un nombre descriptivo ya que será empelado para telefonía, será utilizado por política, además se establece una prioridad alta ya que es bien sabido que la voz tiene siempre prioridad sobre los datos, y por último se estable su ancho de banda máximo y garantizado.

Name	Type	Guaranteed Bandwidth	Max Bandwidth	Bandwidth Utilization	Dropped Bytes	Priority	Ref.
Telefonia_In	Shared	3000 Kbps	6100 Kbps	40.24 kbps	0 B	High	4

Figura 10: Características Traffic Shaper

La figura anterior nos muestra el estado del traffic shaper y otras características, además de esto se debe tener en consideración que el ancho de banda asignado al traffic shaper está basada el ancho de banda total disponible para la sucursal.

Elaboración de reportes y monitorización de red.

Para la elaboración de los reportes se utilizó la herramienta FortiCloud en conjunto con el sistema de monitoreo Zabbix para conocer el estado de le red.

Con FortiCloud obtuvimos los siguientes datos:

i. Categorías de sitios web visitados.

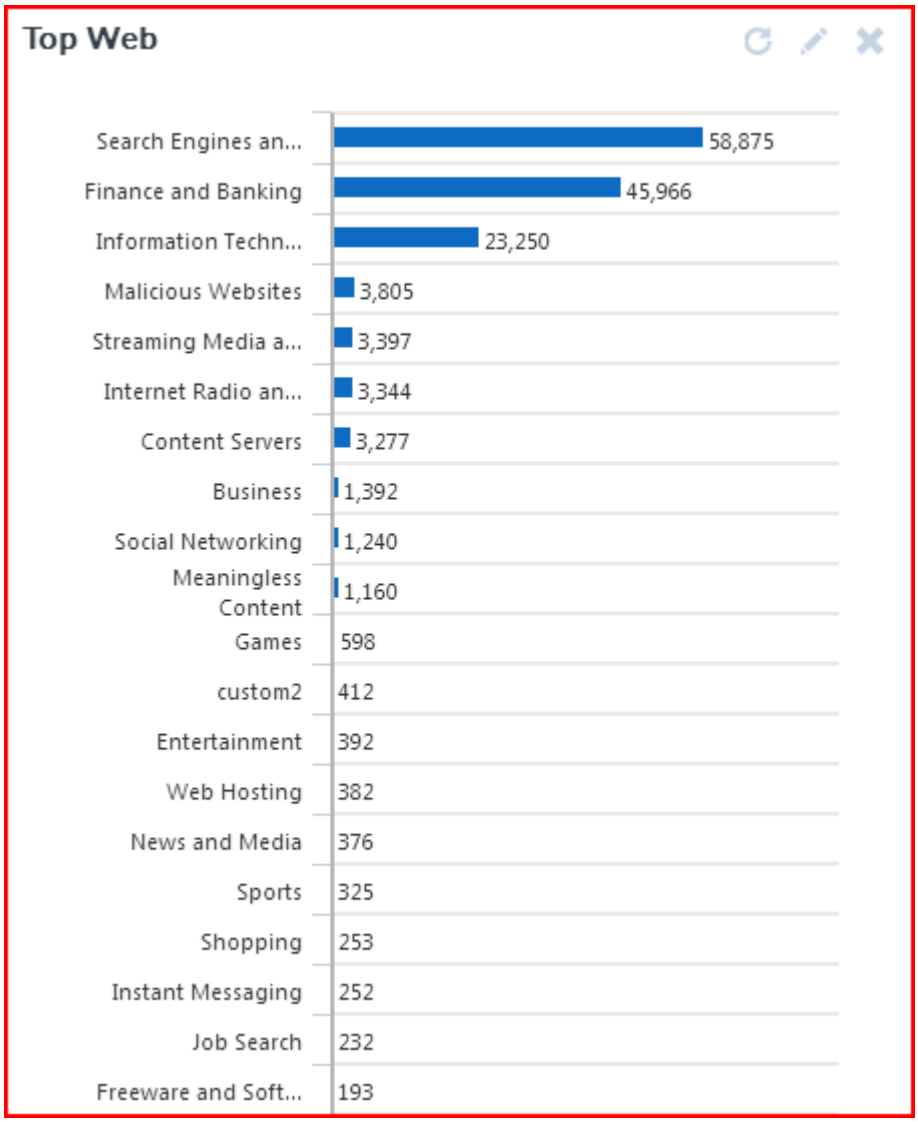


Figura 11: Categorías web visitadas

En la figura anterior observamos las categorías de los sitios web visitados, las tres primeras categorías de sitios web son indispensables para que se desarrollen las actividades diarias de la sucursal, sin embargo, en la categoría de sitios maliciosos se debe tener especial cuidado, por lo cual se revisó las direcciones IP con mayor consumo de ancho de banda, en las cuales algunas de los sitios correspondían a sitios maliciosos, por lo que se procedió al bloqueo de los mismo.

ii. Categorías por aplicación.

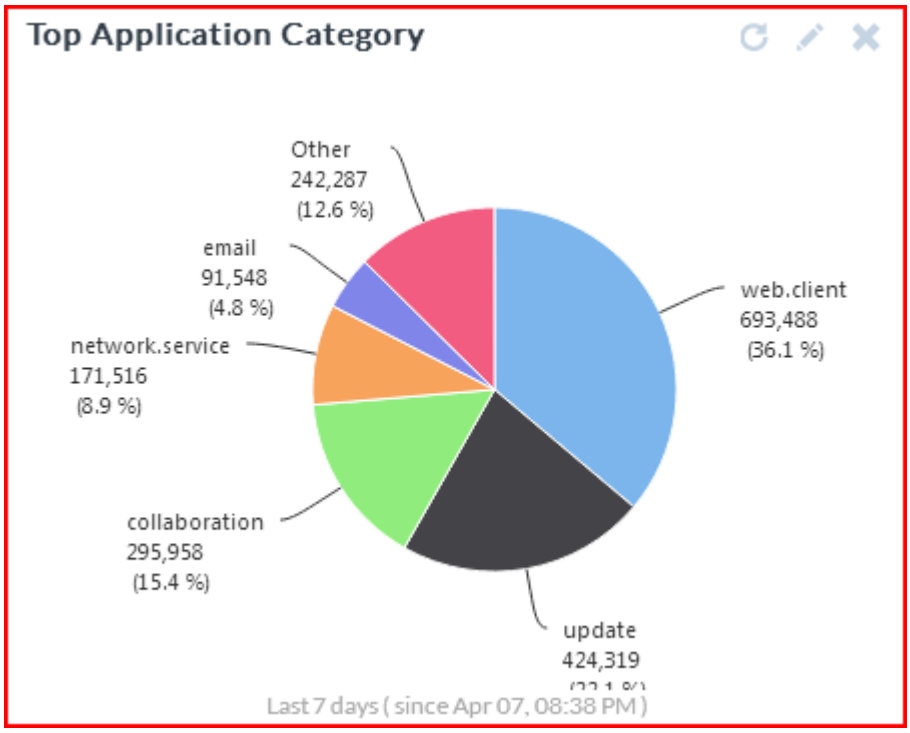
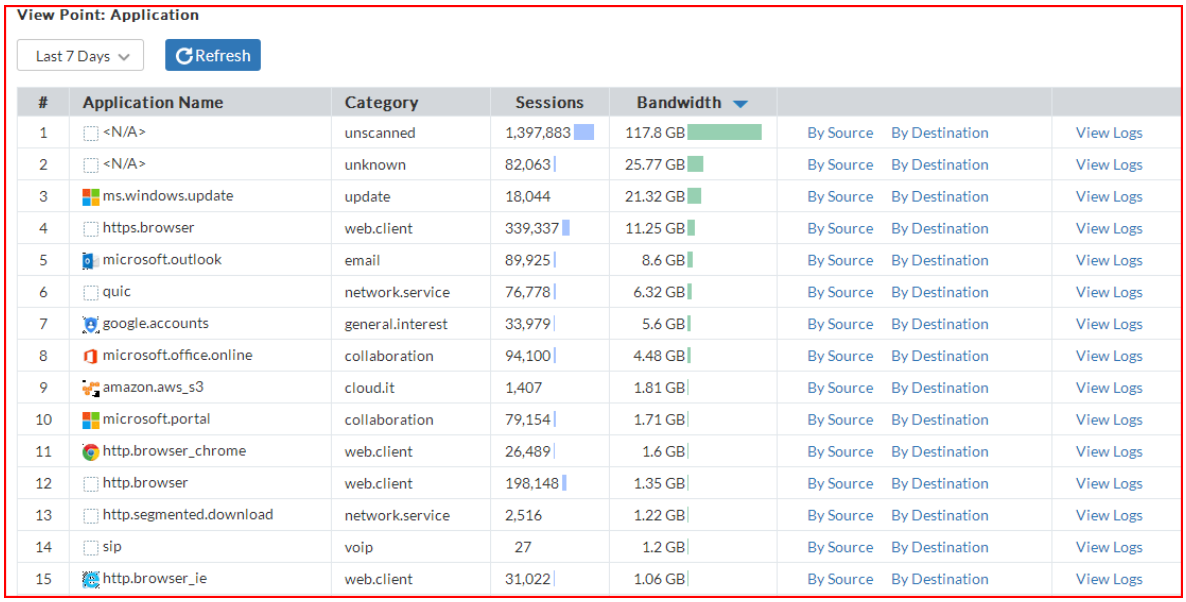


Figura 12: Categorías por aplicación

En la figura anterior observamos que la categoría con el mayor porcentaje es web client, este porcentaje está dentro del rango esperado con la empresa, ya que se realizan peticiones a su servidor central de forma constante, para él envió de archivo, en este caso de imágenes como los rayos X por ejemplo.

iii. Análisis de tráfico por aplicación.



View Point: Application

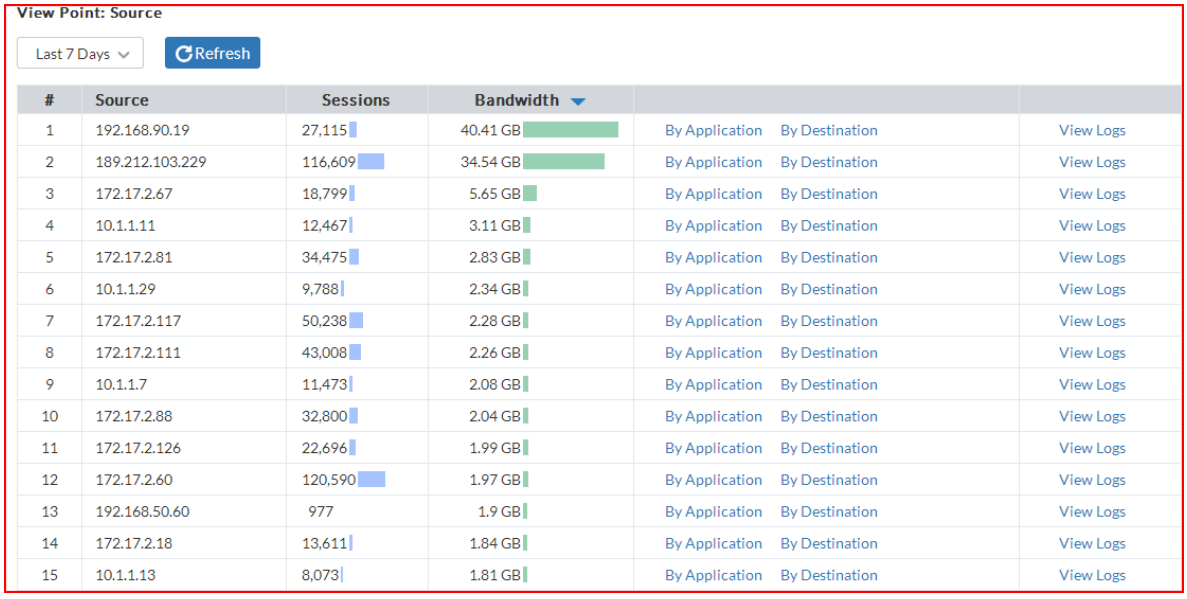
Last 7 Days | Refresh

#	Application Name	Category	Sessions	Bandwidth			
1	<N/A>	unscanned	1,397,883	117.8 GB	By Source	By Destination	View Logs
2	<N/A>	unknown	82,063	25.77 GB	By Source	By Destination	View Logs
3	ms.windows.update	update	18,044	21.32 GB	By Source	By Destination	View Logs
4	https.browser	web.client	339,337	11.25 GB	By Source	By Destination	View Logs
5	microsoft.outlook	email	89,925	8.6 GB	By Source	By Destination	View Logs
6	quic	network.service	76,778	6.32 GB	By Source	By Destination	View Logs
7	google.accounts	general.interest	33,979	5.6 GB	By Source	By Destination	View Logs
8	microsoft.office.online	collaboration	94,100	4.48 GB	By Source	By Destination	View Logs
9	amazon.aws_s3	cloud.it	1,407	1.81 GB	By Source	By Destination	View Logs
10	microsoft.portal	collaboration	79,154	1.71 GB	By Source	By Destination	View Logs
11	http.browser_chrome	web.client	26,489	1.6 GB	By Source	By Destination	View Logs
12	http.browser	web.client	198,148	1.35 GB	By Source	By Destination	View Logs
13	http.segmented.download	network.service	2,516	1.22 GB	By Source	By Destination	View Logs
14	sip	voip	27	1.2 GB	By Source	By Destination	View Logs
15	http.browser_ie	web.client	31,022	1.06 GB	By Source	By Destination	View Logs

Figura 13: Tráfico por aplicación

En la figura anterior se puede observar de manera más específica algunas de las aplicaciones que corresponden a correo electrónico, actualizaciones de sistema operativo, etc., y su número de sesiones y ancho de banda utilizado.

iv. Análisis de tráfico por dirección IP fuente.



View Point: Source

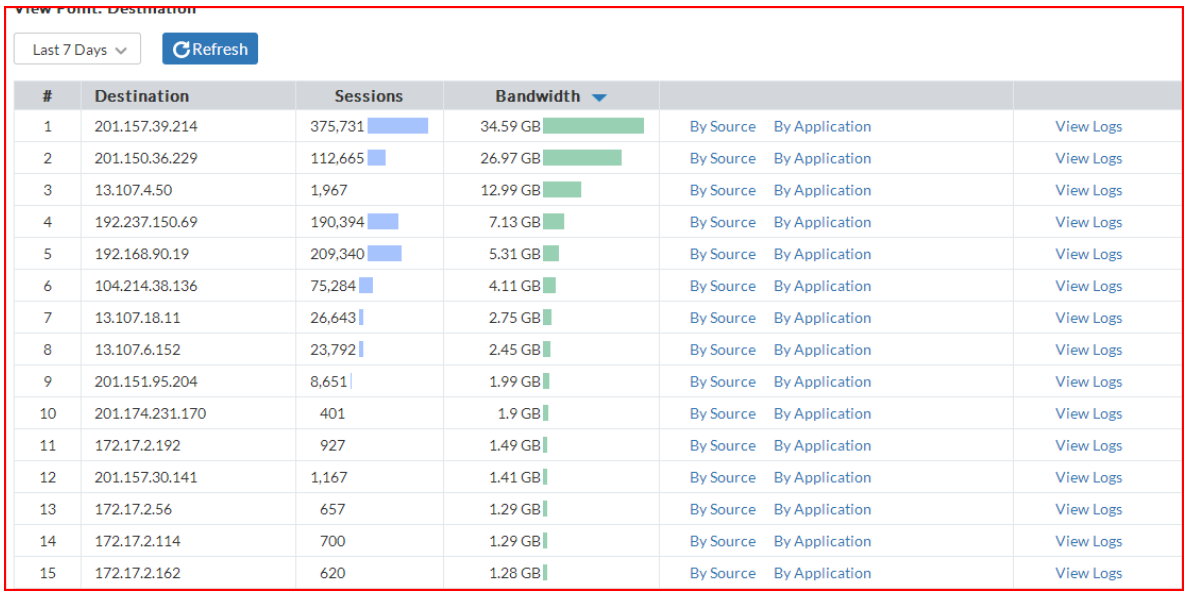
Last 7 Days | Refresh

#	Source	Sessions	Bandwidth			
1	192.168.90.19	27,115	40.41 GB	By Application	By Destination	View Logs
2	189.212.103.229	116,609	34.54 GB	By Application	By Destination	View Logs
3	172.17.2.67	18,799	5.65 GB	By Application	By Destination	View Logs
4	10.1.1.11	12,467	3.11 GB	By Application	By Destination	View Logs
5	172.17.2.81	34,475	2.83 GB	By Application	By Destination	View Logs
6	10.1.1.29	9,788	2.34 GB	By Application	By Destination	View Logs
7	172.17.2.117	50,238	2.28 GB	By Application	By Destination	View Logs
8	172.17.2.111	43,008	2.26 GB	By Application	By Destination	View Logs
9	10.1.1.7	11,473	2.08 GB	By Application	By Destination	View Logs
10	172.17.2.88	32,800	2.04 GB	By Application	By Destination	View Logs
11	172.17.2.126	22,696	1.99 GB	By Application	By Destination	View Logs
12	172.17.2.60	120,590	1.97 GB	By Application	By Destination	View Logs
13	192.168.50.60	977	1.9 GB	By Application	By Destination	View Logs
14	172.17.2.18	13,611	1.84 GB	By Application	By Destination	View Logs
15	10.1.1.13	8,073	1.81 GB	By Application	By Destination	View Logs

Figura 14: Tráfico fuente

En la figura anterior se puede observar el tráfico por dirección IP fuente, su número de sesiones y el ancho de banda utilizado. Si una IP muestra un gran consumo de ancho de banda, puede ser debido a que esa dirección fue asignada a una máquina, empleada para realizar estudios médicos como la de rayos X y esta a su vez genera varias imágenes de alta resolución, debido a que toma diferentes vistas de una extremidad.

v. Análisis de tráfico por dirección IP destino.

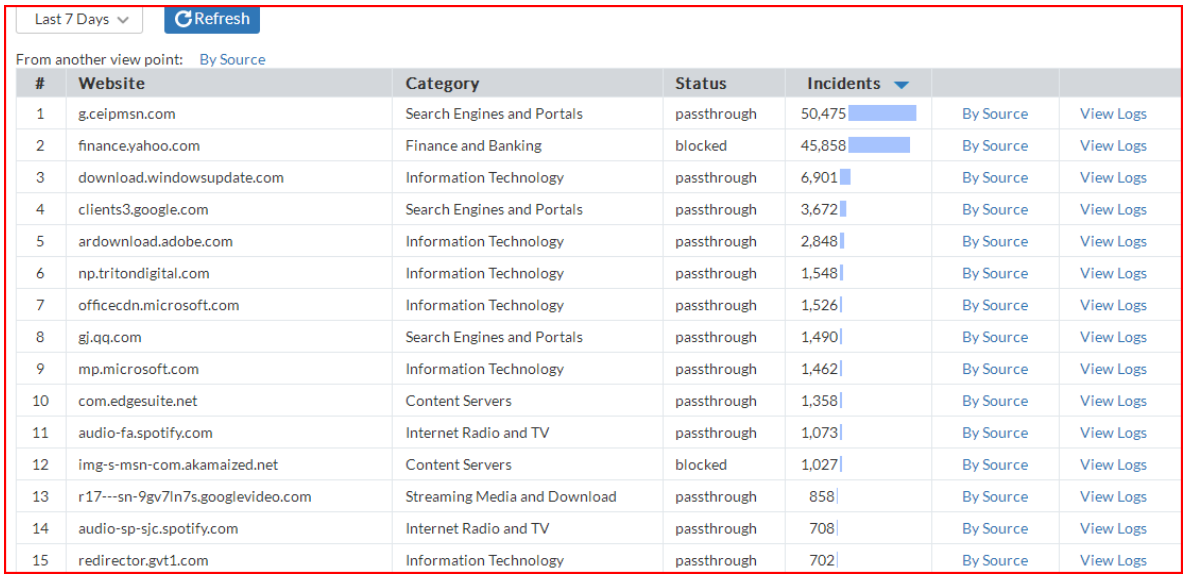


#	Destination	Sessions	Bandwidth		
1	201.157.39.214	375,731	34.59 GB	By Source By Application	View Logs
2	201.150.36.229	112,665	26.97 GB	By Source By Application	View Logs
3	13.107.4.50	1,967	12.99 GB	By Source By Application	View Logs
4	192.237.150.69	190,394	7.13 GB	By Source By Application	View Logs
5	192.168.90.19	209,340	5.31 GB	By Source By Application	View Logs
6	104.214.38.136	75,284	4.11 GB	By Source By Application	View Logs
7	13.107.18.11	26,643	2.75 GB	By Source By Application	View Logs
8	13.107.6.152	23,792	2.45 GB	By Source By Application	View Logs
9	201.151.95.204	8,651	1.99 GB	By Source By Application	View Logs
10	201.174.231.170	401	1.9 GB	By Source By Application	View Logs
11	172.17.2.192	927	1.49 GB	By Source By Application	View Logs
12	201.157.30.141	1,167	1.41 GB	By Source By Application	View Logs
13	172.17.2.56	657	1.29 GB	By Source By Application	View Logs
14	172.17.2.114	700	1.29 GB	By Source By Application	View Logs
15	172.17.2.162	620	1.28 GB	By Source By Application	View Logs

Figura 15: Tráfico destino

En la figura anterior es el mismo caso que el anterior, con excepción que la IP corresponda al servidor central o a algún otro servidor o dispositivo de otra sucursal.

vi. Gestión de sitios web y amenazas.



Last 7 Days | Refresh

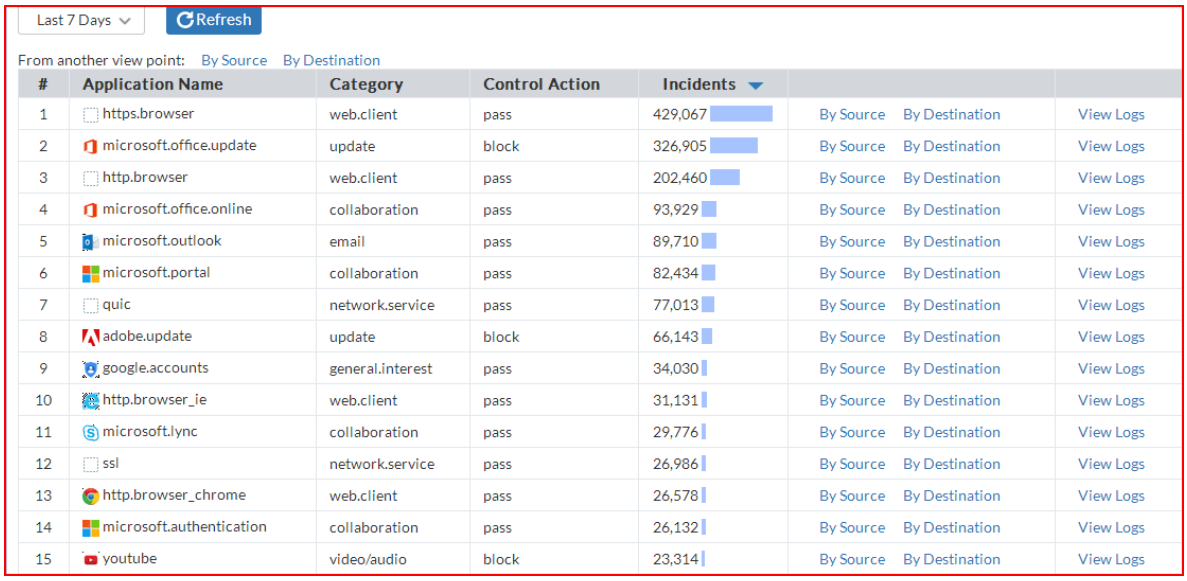
From another view point: By Source

#	Website	Category	Status	Incidents		
1	g.ceipmsn.com	Search Engines and Portals	passthrough	50,475	By Source	View Logs
2	finance.yahoo.com	Finance and Banking	blocked	45,858	By Source	View Logs
3	download.windowsupdate.com	Information Technology	passthrough	6,901	By Source	View Logs
4	clients3.google.com	Search Engines and Portals	passthrough	3,672	By Source	View Logs
5	ardownload.adobe.com	Information Technology	passthrough	2,848	By Source	View Logs
6	np.tritondigital.com	Information Technology	passthrough	1,548	By Source	View Logs
7	officecdn.microsoft.com	Information Technology	passthrough	1,526	By Source	View Logs
8	gj.qq.com	Search Engines and Portals	passthrough	1,490	By Source	View Logs
9	mp.microsoft.com	Information Technology	passthrough	1,462	By Source	View Logs
10	com.edgesuite.net	Content Servers	passthrough	1,358	By Source	View Logs
11	audio-fa.spotify.com	Internet Radio and TV	passthrough	1,073	By Source	View Logs
12	img-s-msn-com.akamaized.net	Content Servers	blocked	1,027	By Source	View Logs
13	r17---sn-9gv7ln7s.googlevideo.com	Streaming Media and Download	passthrough	858	By Source	View Logs
14	audio-sp-sjc.spotify.com	Internet Radio and TV	passthrough	708	By Source	View Logs
15	redirector.gvt1.com	Information Technology	passthrough	702	By Source	View Logs

Figura 16: Amenazas por sitio web

En la figura anterior observamos de forma más específica las amenazas por sitios web, pero en si algunos sitios no representan una amenaza verdadera, se catalogan así por su alto consumo de ancho de banda como Windows Update por ejemplo.

vii. Gestión de aplicaciones y amenazas.



Last 7 Days | Refresh

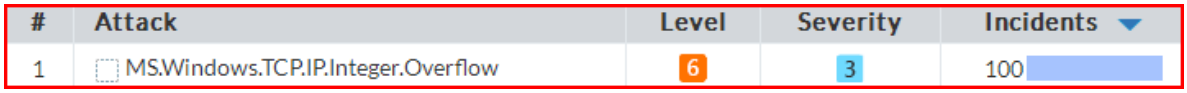
From another view point: By Source By Destination

#	Application Name	Category	Control Action	Incidents			
1	https.browser	web.client	pass	429,067	By Source	By Destination	View Logs
2	microsoft.office.update	update	block	326,905	By Source	By Destination	View Logs
3	http.browser	web.client	pass	202,460	By Source	By Destination	View Logs
4	microsoft.office.online	collaboration	pass	93,929	By Source	By Destination	View Logs
5	microsoft.outlook	email	pass	89,710	By Source	By Destination	View Logs
6	microsoft.portal	collaboration	pass	82,434	By Source	By Destination	View Logs
7	quic	network.service	pass	77,013	By Source	By Destination	View Logs
8	adobe.update	update	block	66,143	By Source	By Destination	View Logs
9	google.accounts	general.interest	pass	34,030	By Source	By Destination	View Logs
10	http.browser_ie	web.client	pass	31,131	By Source	By Destination	View Logs
11	microsoft.lync	collaboration	pass	29,776	By Source	By Destination	View Logs
12	ssl	network.service	pass	26,986	By Source	By Destination	View Logs
13	http.browser_chrome	web.client	pass	26,578	By Source	By Destination	View Logs
14	microsoft.authentication	collaboration	pass	26,132	By Source	By Destination	View Logs
15	youtube	video/audio	block	23,314	By Source	By Destination	View Logs

Figura 17: Amenazas por aplicación

En esta figura se observa un caso similar al anterior, en su mayoría todo corresponde al alto consumo de ancho de banda de las diferentes aplicaciones utilizadas.

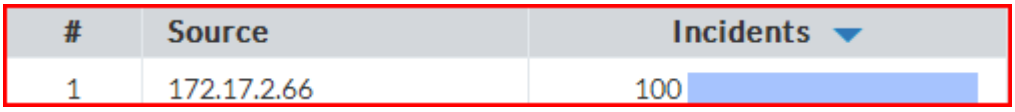
viii. Nos indica además las estadísticas del IPS, por nombre, por fuente y por destino.



#	Attack	Level	Severity	Incidents
1	MS.Windows.TCP.IP.Integer.Overflow	6	3	100

Figura 18: Incidente IPS

En esta figura se observa el tipo de ataque detectado por nombre en el Fortigate, así como su severidad y número de incidentes.



#	Source	Incidents
1	172.17.2.66	100

Figura 19: Incidente IPS por fuente

En la figura anterior hace referencia al mismo incidente, solo que ahora se indica por dirección IP fuente.

#	Destination	Incidents
1	23.76.194.83	36
2	104.92.20.84	21
3	172.230.197.192	16
4	104.72.39.91	9
5	104.208.31.113	5

Figura 20: Incidente IPS por destino

El total de incidentes correspondientes a la IP de la figura 19 se produjeron por visitar los destinos en de la figura anterior, en este caso solo se muestran los primeros 5.

ix. Estado VPN's.

#	VPN Tunnel	Tunnel-Down Incidents	Bandwidth
1	VPN_Elastix	2	92.83 GB
2	FUJI_Tlalp-Roma	0	24.56 GB
3	VPN_Elastix_Azt	0	0 B

Figura 21: VPN's

La figura anterior muestra los túneles VPN empleados para servicio de telefonía y transferencia de archivos, así como su número de incidentes y ancho de banda utilizado.

El sistema de monitoreo Zabbix nos muestra el siguiente entorno donde se encuentran los diferentes dispositivos monitoreados, además de indicarnos su estado, clasificación y

número de incidentes. En la siguiente captura podemos ver que todo se encuentra en orden con excepción de dos grupos de dispositivos los cuales se encuentran resaltados en color rojo y que nos indican un desastre.

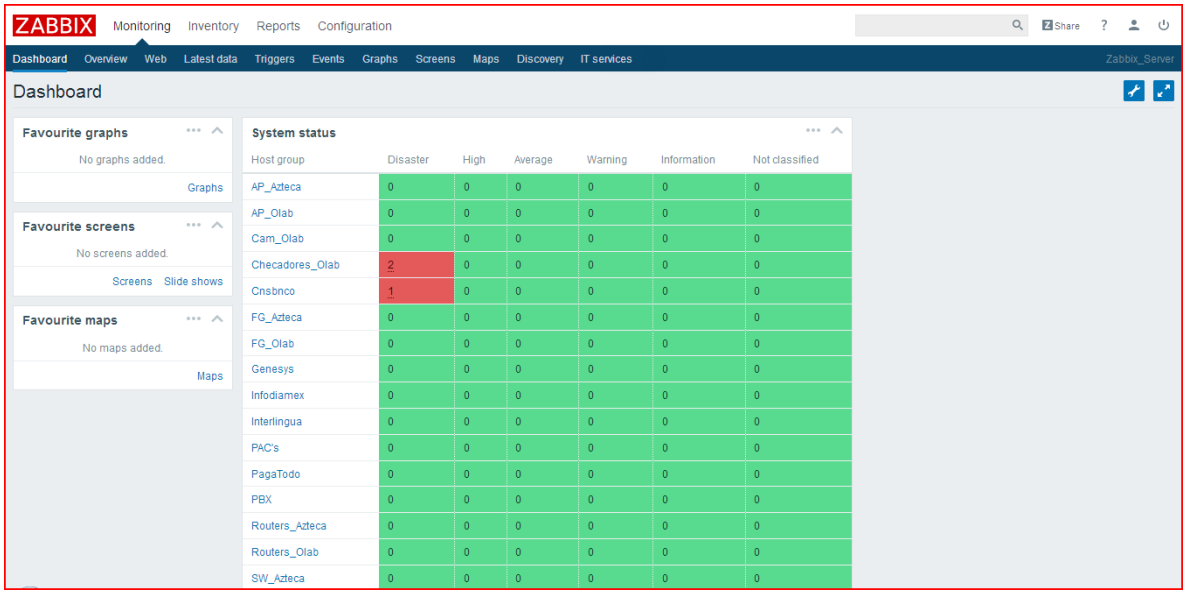


Figura 22: Zabbix Dashboard

La figura anterior nos muestra el entorno en la interfaz inicial de Zabbix, donde se pueden apreciar los grupos de dispositivos que son monitoreados y su estado.

En el apartado de Graphs nos permitió obtener las gráficas correspondientes al tráfico de cada interfaz del Fortigate como se muestra a continuación:

Las tres gráficas siguientes corresponden a las interfaces de los ISP de la sucursal.

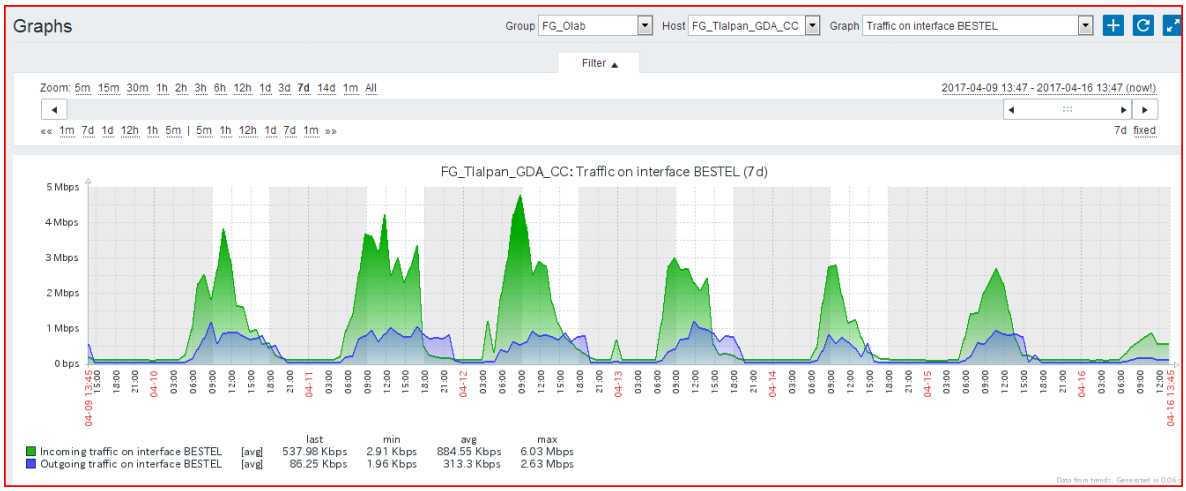


Figura 23: Gráfica Bestel

La gráfica anterior muestra el tráfico entrante (color verde) y saliente (color azul) correspondiente a la interfaz del ISP Bestel en un periodo de 7 días, indicándonos el tráfico máximo, mínimo y promedio en megabits por segundo (Mbps).

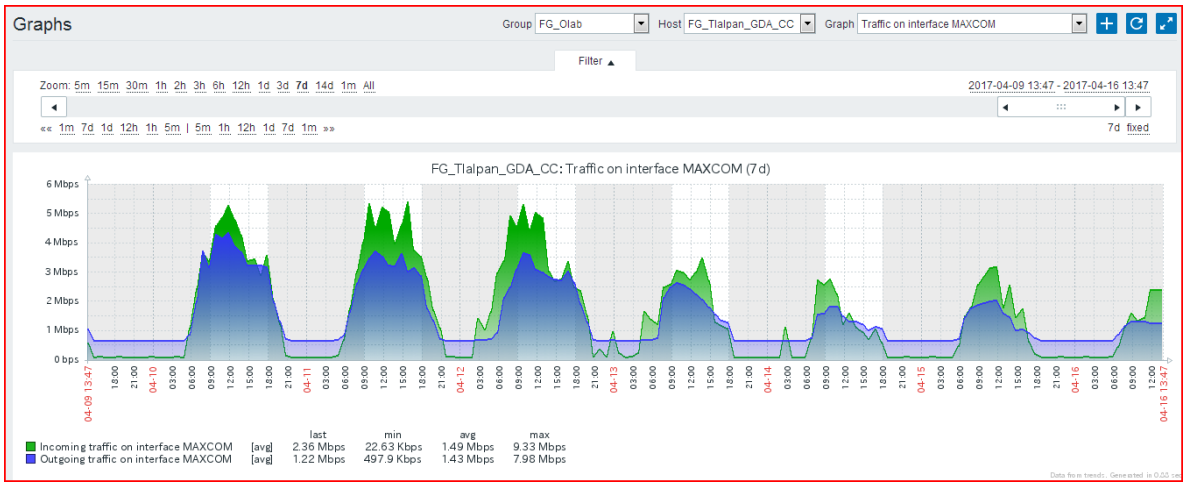


Figura 24: Gráfica MAXCOM

La gráfica anterior muestra el tráfico entrante (color verde) y saliente (color azul) correspondiente a la interfaz del ISP MAXCOM en un periodo de 7 días, indicándonos el tráfico máximo, mínimo y promedio en megabits por segundo (Mbps).

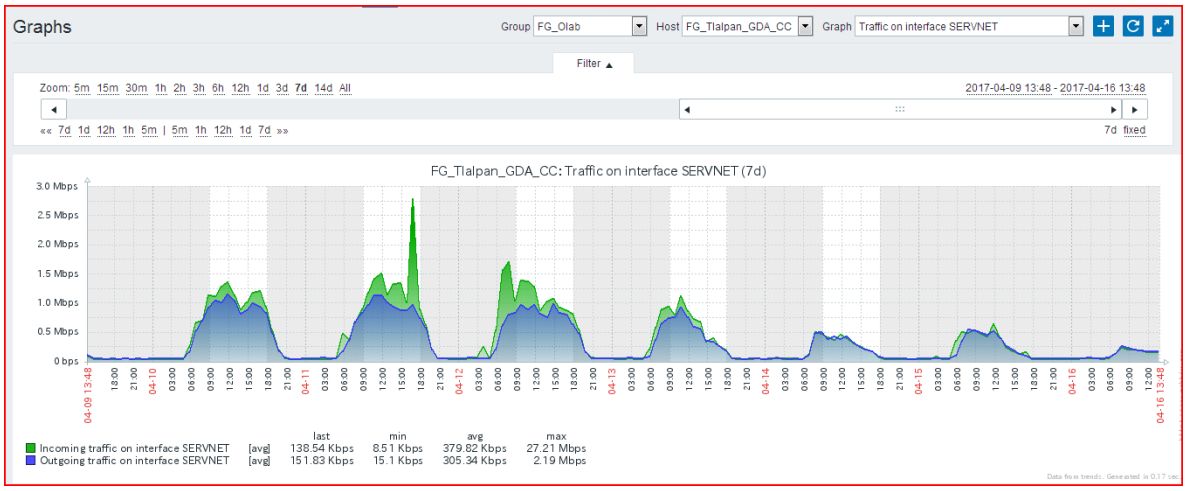


Figura 25: Gráfica SERVNET

La gráfica anterior muestra el tráfico entrante (color verde) y saliente (color azul) correspondiente a la interfaz del ISP SERVNET en un periodo de 7 días, indicándonos el tráfico máximo, mínimo y promedio en megabits por segundo (Mbps).

Las siguiente tres gráficas corresponden a las interfaces de las redes LAN de la sucursal.

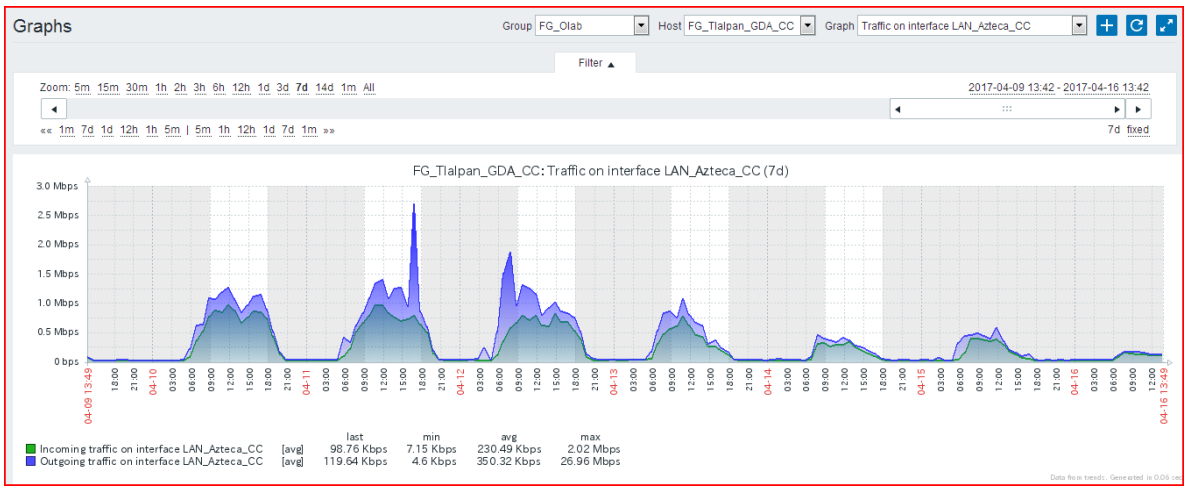


Figura 26: LAN Azteca

La gráfica anterior muestra el tráfico entrante (color verde) y saliente (color azul) correspondiente a la interfaz de la LAN Azteca, en un periodo de 7 días, indicándonos el tráfico máximo, mínimo y promedio en megabits por segundo (Mbps).

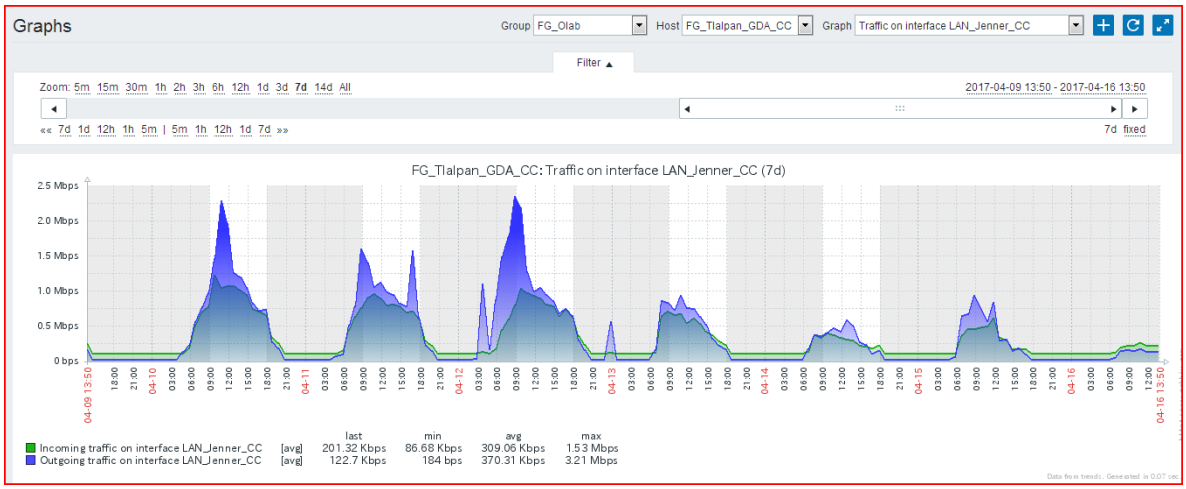


Figura 27: LAN Jenner

La gráfica anterior muestra el tráfico entrante (color verde) y saliente (color azul) correspondiente a la interfaz de la LAN Jenner, en un periodo de 7 días, indicándonos el tráfico máximo, mínimo y promedio en megabits por segundo (Mbps).

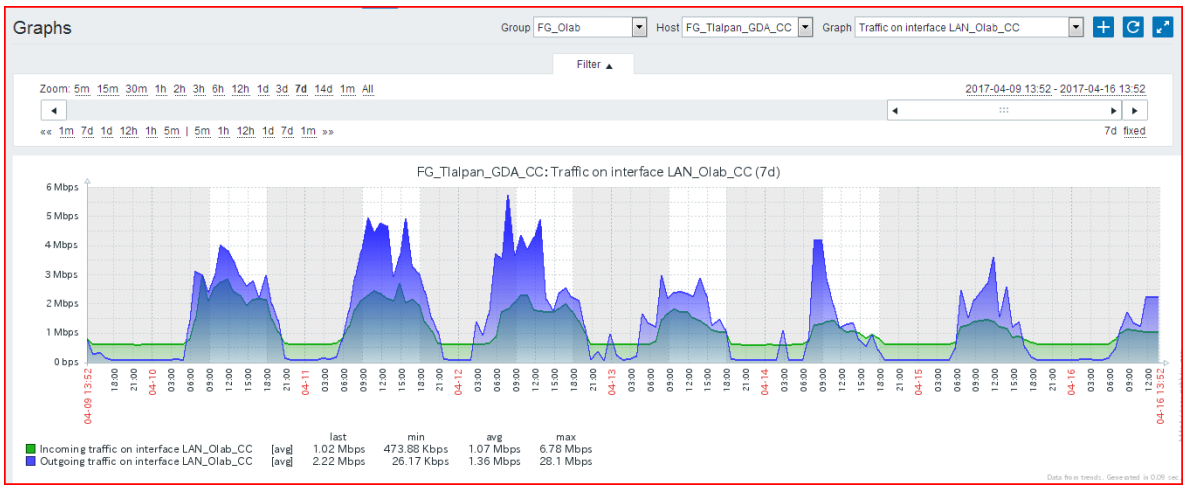


Figura 28: LAN Olab

La gráfica anterior muestra el tráfico entrante (color verde) y saliente (color azul) correspondiente a la interfaz de la LAN Olab, en un periodo de 7 días, indicándonos el tráfico máximo, mínimo y promedio en megabits por segundo (Mbps).

Las dos gráficas siguientes corresponden a la transferencia de archivos de la sucursal con su servidor central.

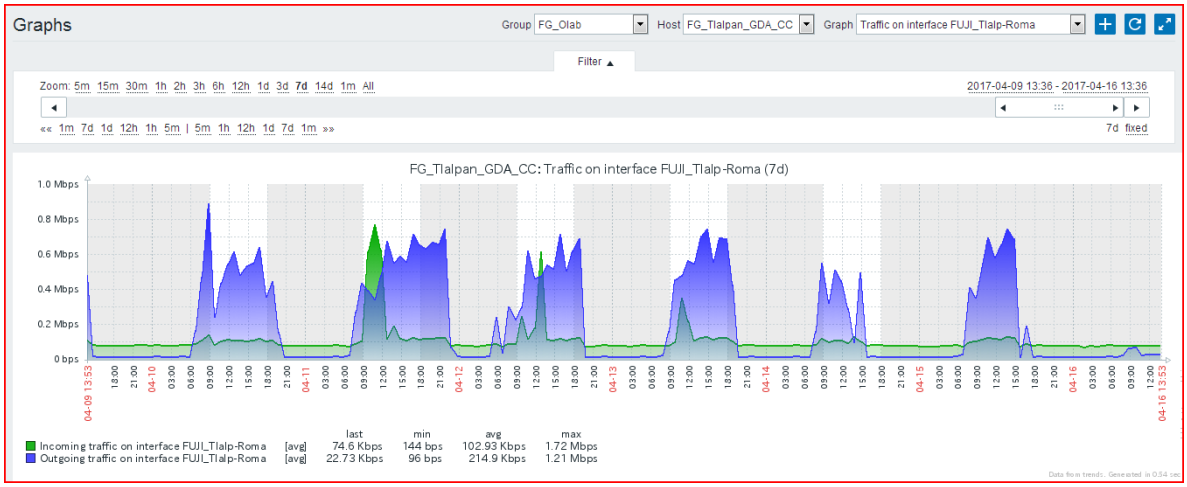


Figura 29: Túnel VPN FUJI

La gráfica anterior corresponde a la transferencia de archivos, en este caso imágenes de alta resolución por medio de un túnel VPN.

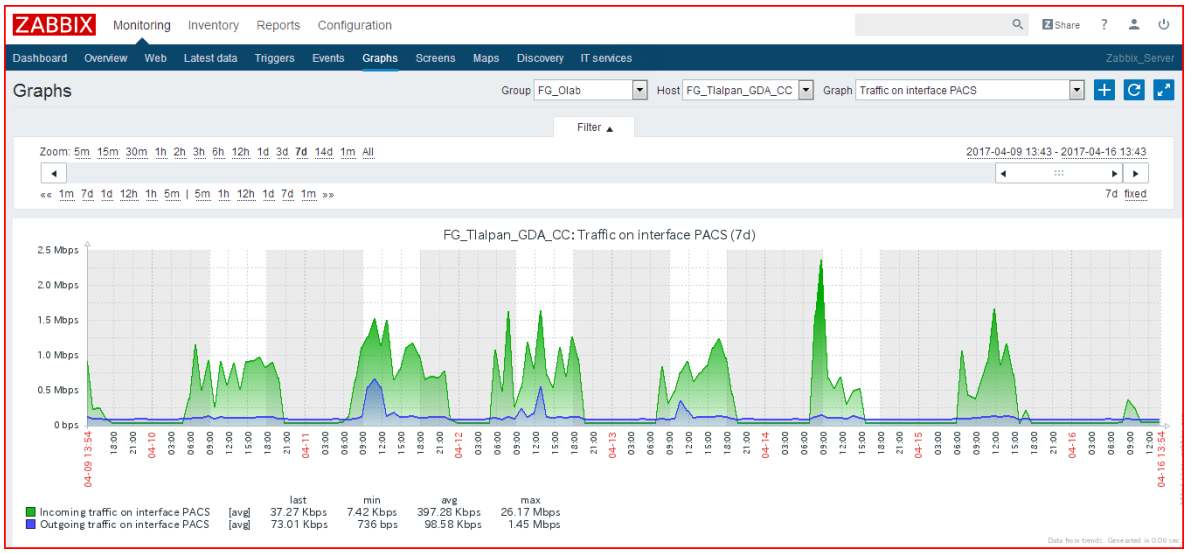


Figura 30: Gráfica PACS

La gráfica anterior corresponde a la transferencia de archivos, en este caso imágenes de alta resolución por medio del protocolo FTP.

Creación de ítem y triggers para monitoreo de túneles VPN.

La creación de los ítems y triggers corresponde a un grupo específico de hosts, para realizar estas tareas se realizó el siguiente procedimiento:

i. En el Dashboard de Zabbix dar click en el apartado de **Configuration** y seleccionamos **Hosts**.

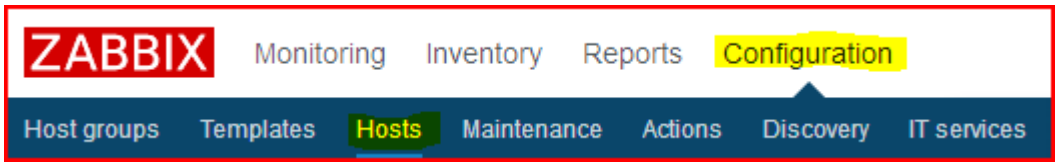


Figura 31: Configuración hosts

ii. Seleccionamos el apartado de **ítems** y en **Host** escribimos el grupo de dispositivos al que pertenecerán.

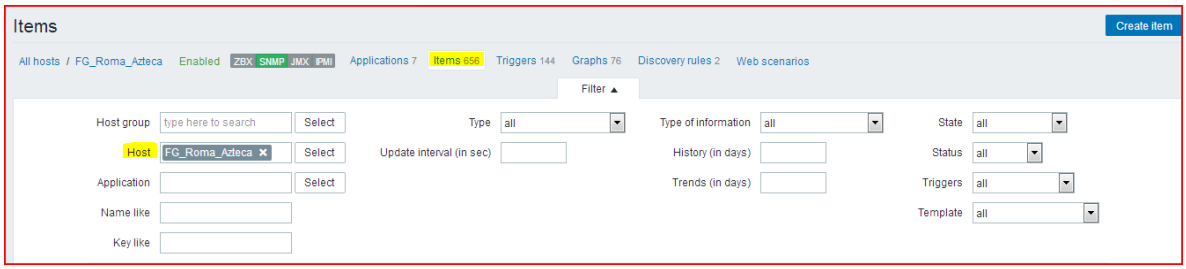


Figura 32: Items

iii. Seleccionamos el filtro **VPN** y después **Create ítem**.

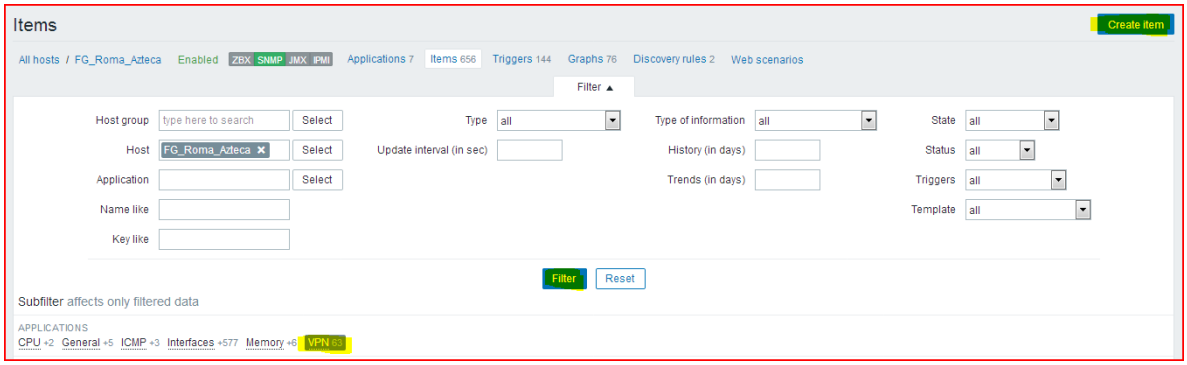


Figura 33: Filtro VPN

iv. A continuación, se llenan los siguientes campos tal y como se muestra en la siguiente figura los cuales tienen las siguientes características:

a. Nombre descriptivo de la sucursal.
b. Tipo de protocolo SNMPV2 para la administración de dispositivos.
c. En el caso de Key y SNMP OID es el mismo valor en cual los primeros seis números.
d. En Host interface corresponde a la dirección IP del Fortigate.
e. EN SNMP community se escriben los caracteres indicados en el campo.
f. Los siguientes campos se quedan como vienen por defecto con excepción de Update interval el cual se coloca a 60 seg.
g. Los campos siguientes se dejan tal y como se indica, y por último damos click en crear.

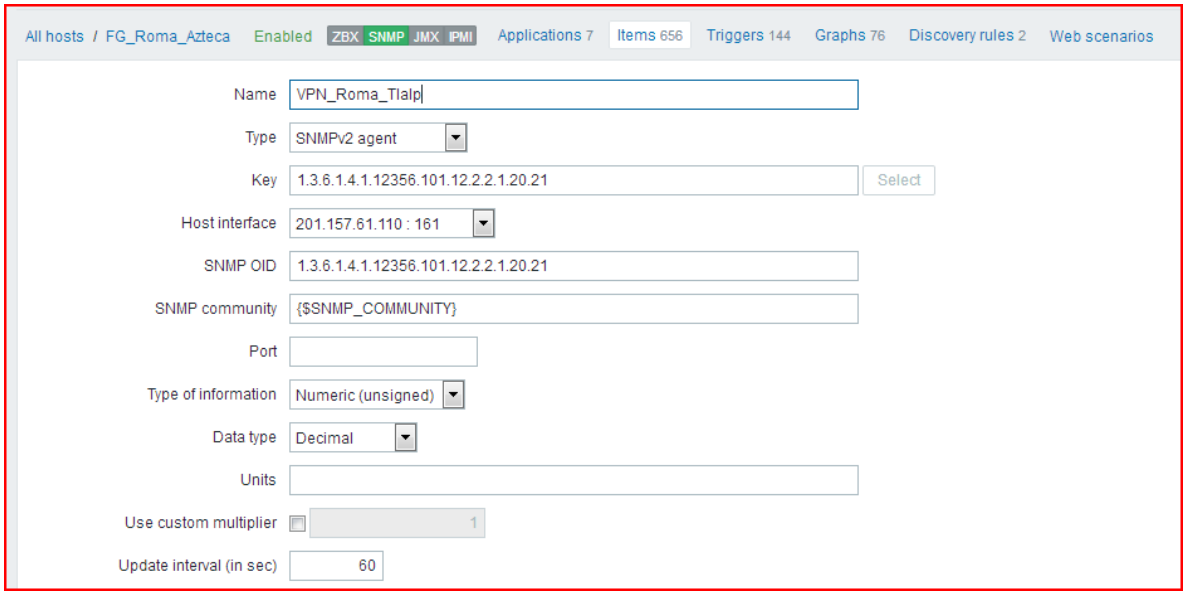


Figura 34: Información item

La figura anterior muestra los parámetros de la configuración del ítem VPN, incluyendo un nombre descriptivo, el protocolo empleado para la administración, la dirección IP pública del equipo. Por otra parte, tenemos que el campo Key y SNMP OID es el mismo valor en cual los primeros seis números, los cuales corresponden a un número otorgado por la IANA a las empresas, para la creación del ítem este número fue proporcionado por la empresa.

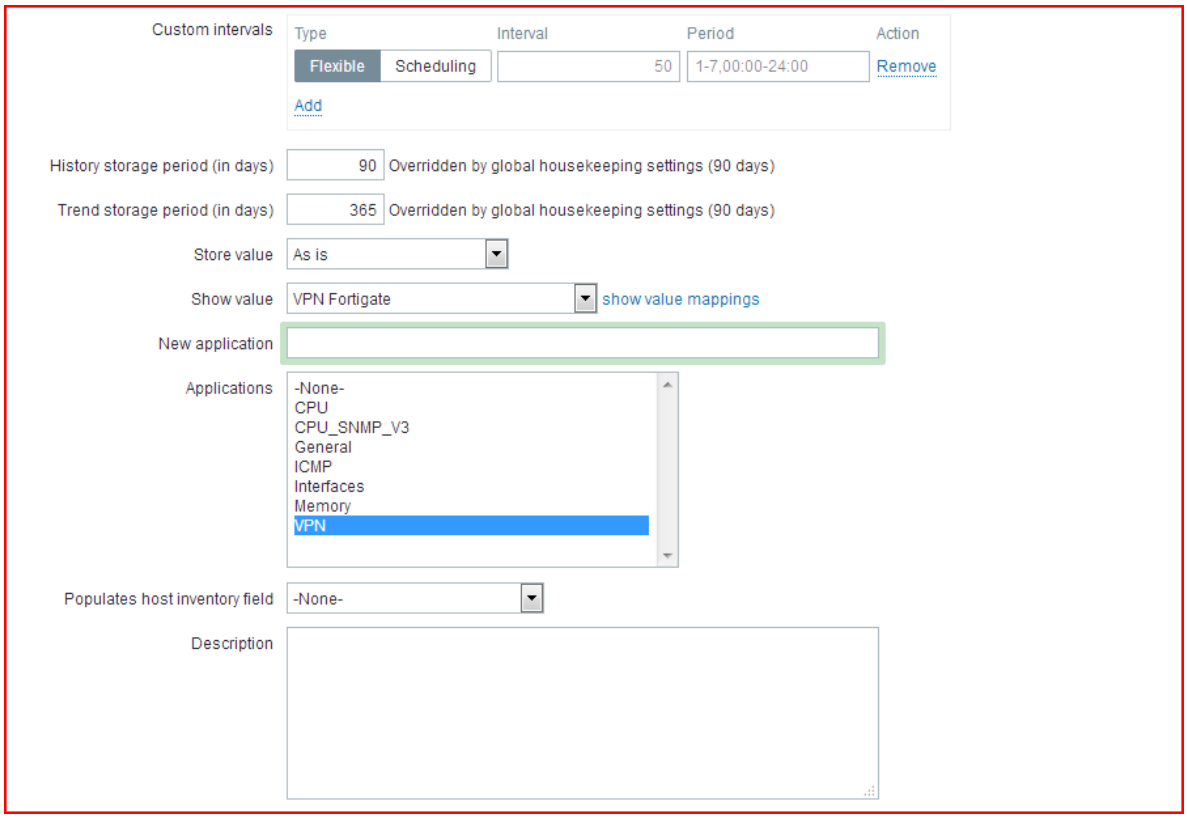


Figura 35: Continuación información item

En la figura anterior continuamos con los parámetros del ítem VPN, la mayoría se dejan como vienen por defecto con excepción de Show value el cual se cambia por VPN Fortigate, y en Applications seleccionamos VPN.

El siguiente paso es crear el trigger correspondiente del ítem creado con anterioridad. Lo siguiente es dirigirnos al apartado de triggers, escribir un nombre descriptivo, colocar los caracteres que aparecen en la siguiente figura, después en Severity seleccionamos Disaster el cual se marcara en color rojo y por último seleccionamos crear.

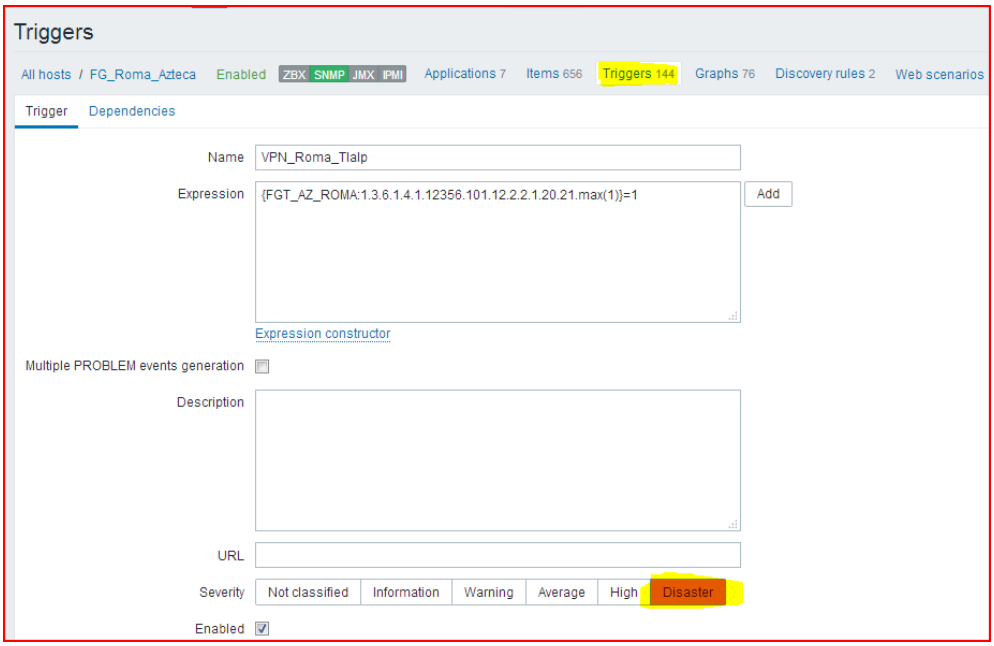


Figura 36: Creación trigger

En la figura anterior se establecen los parámetros para la creación del trigger el cual contiene una cadena de caracteres, donde se incluye el valor del OID y estableciendo el nivel máximo que puede alcanzar el trigger antes de considerarse un desastre, en este caso dicho valor es max (1) =1.

Implementación de túnel VPN.

Se realizó la implementación de un túnel VPN para la transferencia de archivos con el servidor central, con dicha implementación se reemplazó el esquema anterior para la transferencia de archivos la cual se realizaba mediante FTP.

El túnel fue implementado en una VPN sitio a sitio.

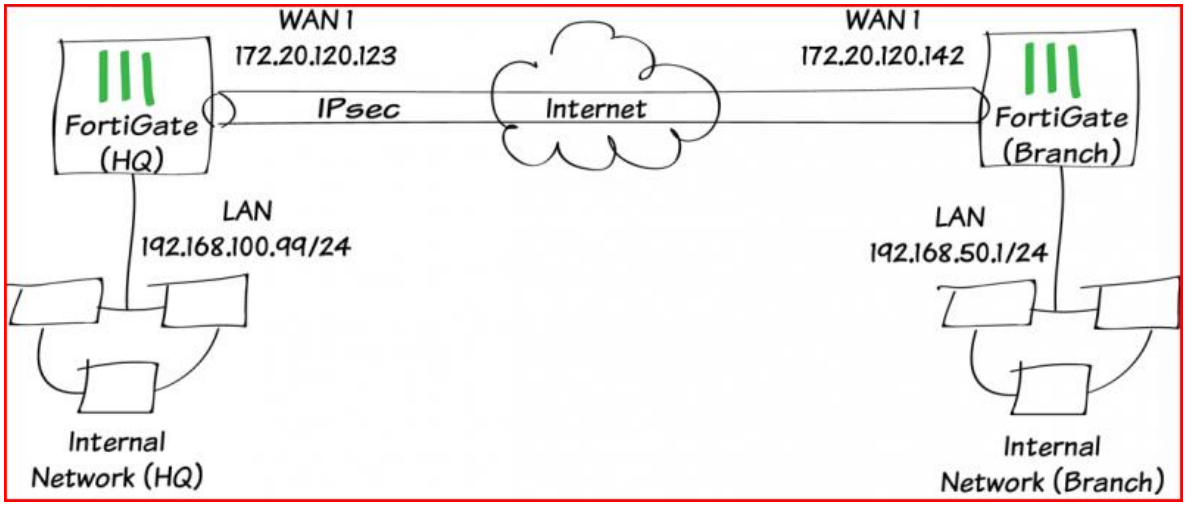


Figura 37: Túnel VPN sitio a sitio.

La figura anterior nos muestra a manera de ejemplo un diagrama de un túnel VPN sitio a sitio, en nuestro caso se realizó con diferentes redes e interfaces.

Para implementar el túnel VPN ingresamos en la sección VPN -> IPsec Tunnels y damos click en Create New como se muestra a continuación.

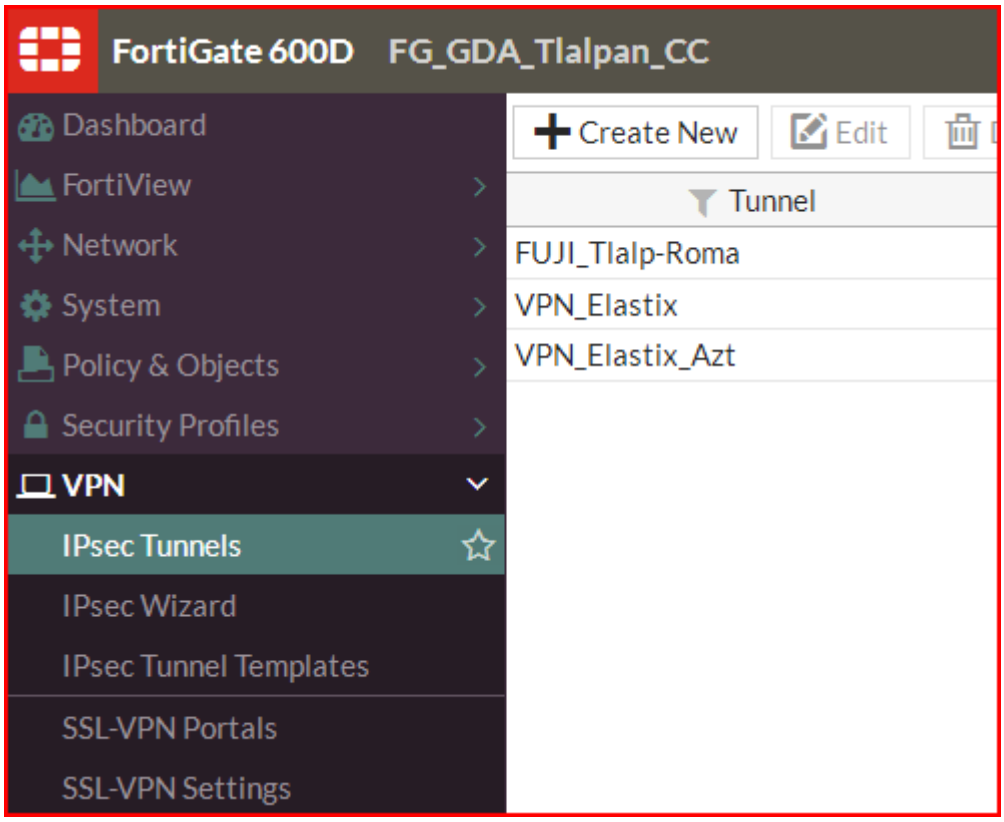


Figura 38: Opciones VPN

A continuación, se proporcionan los siguientes parámetros en la siguiente figura.

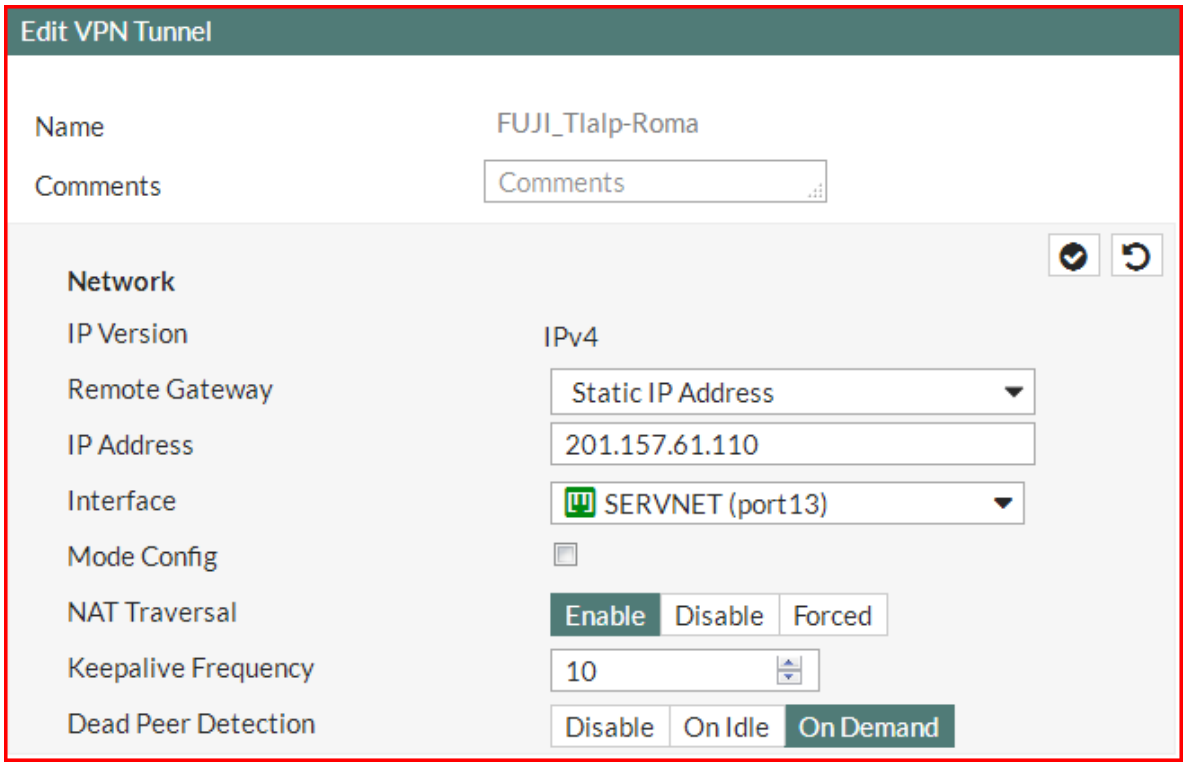


Figura 39: Parámetros VPN

Los parámetros proporcionados en la figura anterior corresponden a lo siguiente:

Parámetro	Valor	Descripción
IP Versión	IPv4	Valor por defecto
Remote Gateway	Static IP Address	Valor por defecto
IP Address	IP pública	IP pública del equipo remoto
Interface	SERVNET(port13)	Enlace a Internet del equipo local
Mode Config	Desmarcado	
Nat Traversal	Habilitado	
Keepalive Frequency	10	Comprueba que el enlace está funcionando o previene que se rompa
Dead Peer Detection	Marcado (On Demand)	

Tabla 1: Valores sugeridos VPN

Ahora configuramos clave y tipo de autenticación.

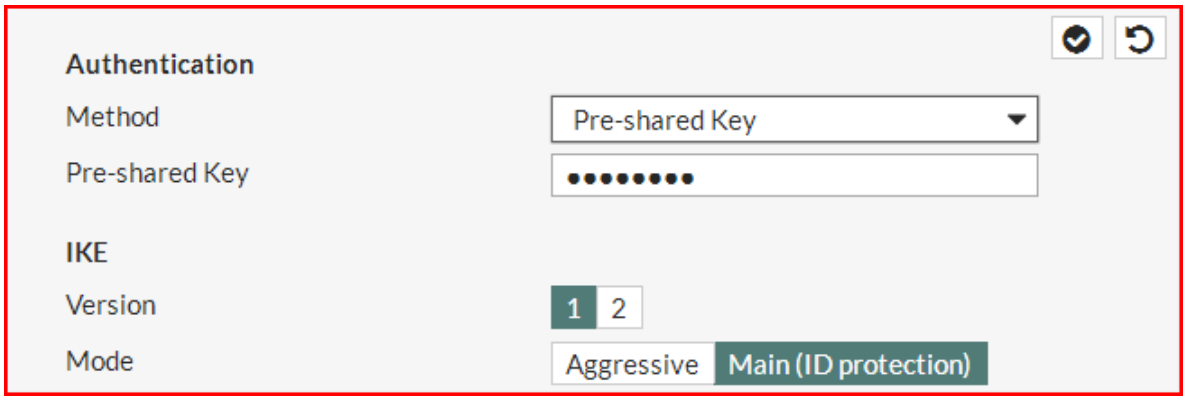


Figura 40: Autenticación

En la siguiente tabla se describe brevemente cada uno de los parámetros:

Parámetro	Valor	Descripción
Method	Pre-Shared Key	Valor por defecto
Pre-Shared Key	123456789	Contraseña acordada
Versión	1	Valor por defecto
Mode	Main (ID Protection)	Valor por defecto

Tabla 2: Valores sugeridos autenticación

Ahora continuamos con la configuración de la fase 1.

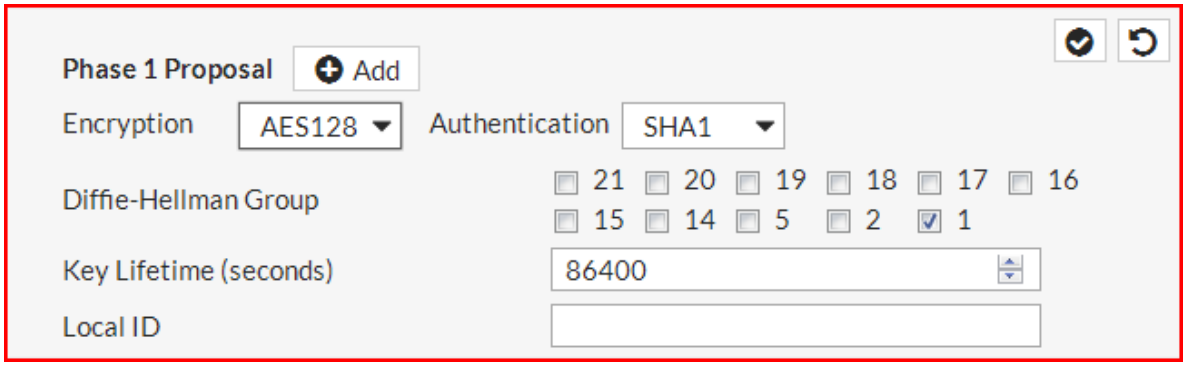


Figura 41: Fase 1 VPN

Descripción breve de los parámetros de la fase 1:

Parámetro	Valor	Descripción
Encryption	AES128 / SHA1	Mejores prácticas
Diffie Hellman Groups	1	Valor sugerido
Key Lifetime (Seconds)	86400	Disposición de cifrado-descifrado establecido por la empresa
Local ID	Ninguno	Valor por defecto

Tabla 3: Parámetros fase 1

Figura 42: Autenticación extendida

El parámetro de la figura anterior requiere un servidor dedicado de autenticación por lo que no se usa.

Lo siguientes es configurar la fase 2 del túnel VPN.

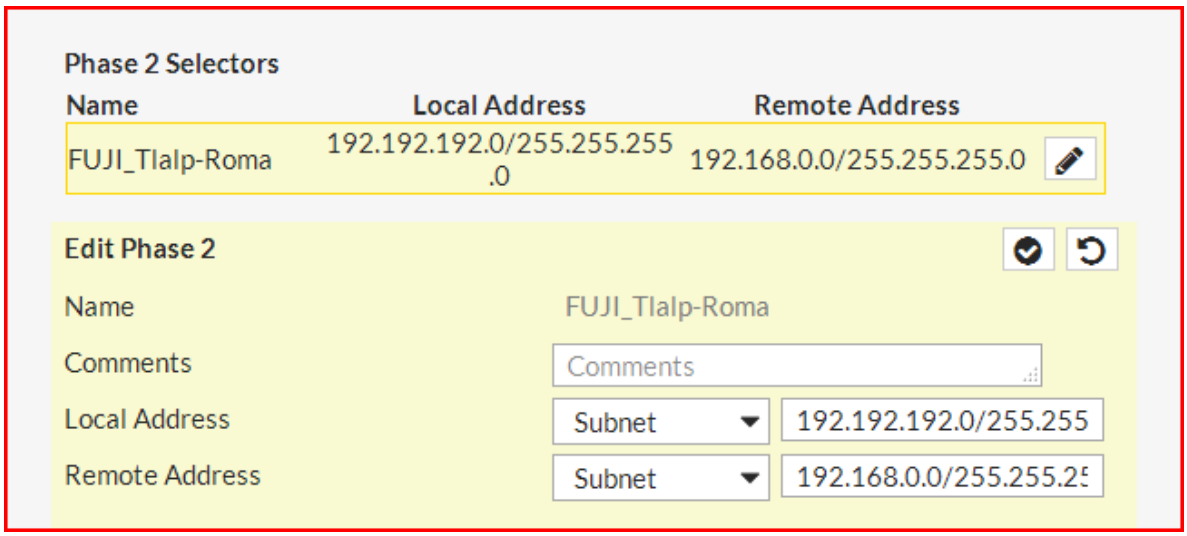


Figura 43: Direccionamiento fase 2

En la figura anterior nos muestra los parámetros como el nombre del túnel, dirección de red local y dirección de red remota.

Lo siguiente es configurar los parámetros de cifrado de la fase 2.

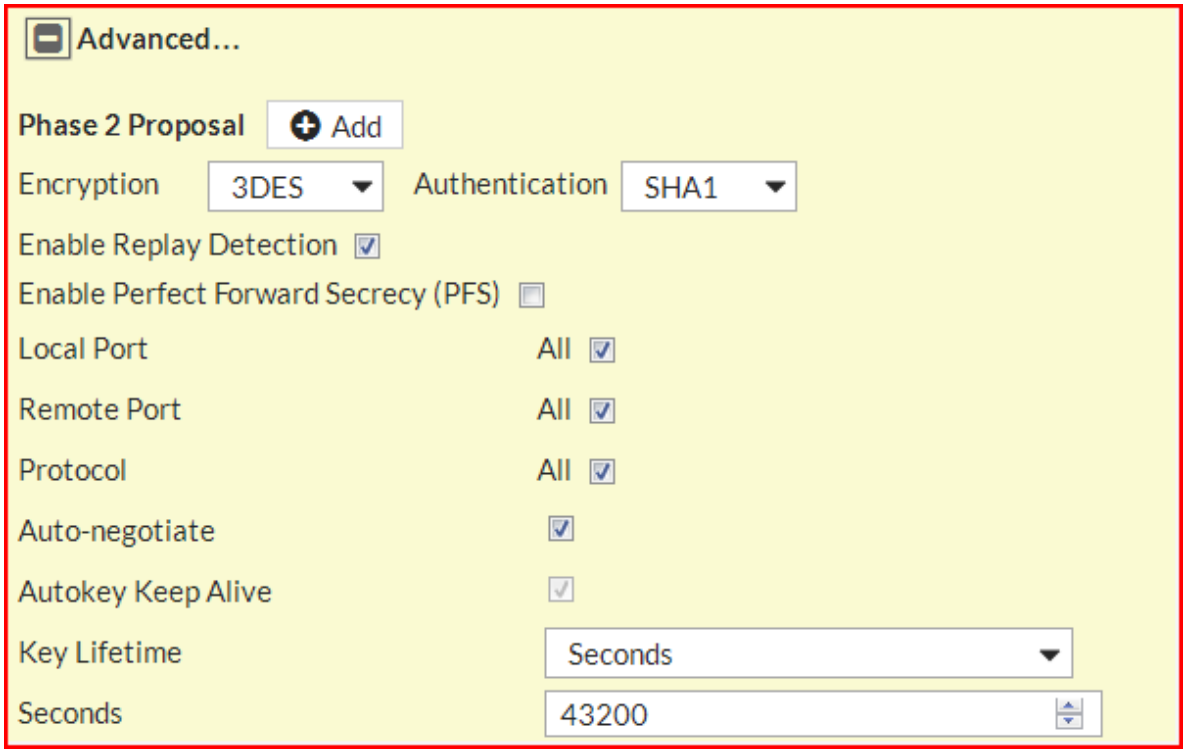


Figura 44: Parámetros de cifrado

En la siguiente tabla se muestra una breve descripción de los parámetros.

Parámetro	Valor	Descripción
Encryption	3DES/SHA1	Mejores prácticas
Enable Replay Detection	Marcada	Valor por defecto
Enable Perfect Forward Secrecy (PFS)	Marcada	Mejores prácticas
Diffie-Hellman Group	2	Valor sugerido
Local Port	Marcada	Valor por defecto
Remote Port	Marcada	Mejores prácticas
Protocol	Marcada	Mejores prácticas
Autokey Keep Alive	Desmarcada	Valor recomendado
Auto-negotiate	Marcada	
Key Lifetime	Seconds	Valor por defecto
Seconds	43200	Valor recomendado

Tabla 4: Parámetros fase 2

Ya que se configuraron los parámetros de ambas fases en el apartado monitor seleccionamos IPsec Monitor.

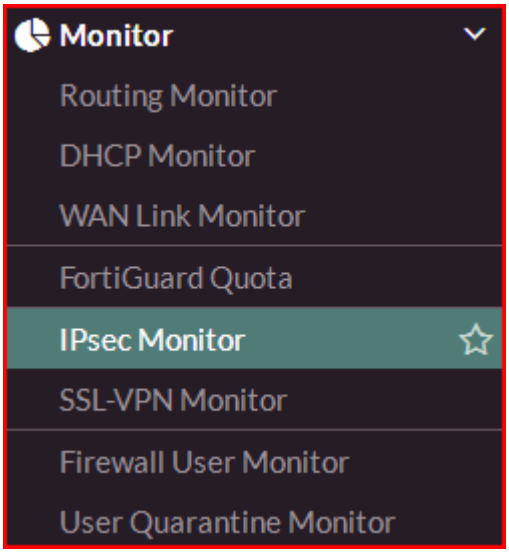


Figura 45: IPsec monitor

En donde se obtiene la siguiente información.

Name	Type	Remote Gateway	Status	Incoming Data	Outgoing Data	Phase 2 Selectors	Uptime
FUJI_Tlalp-Roma	Custom	201.157.61.110	Up	1.65 GB	3.81 GB	FUJI_Tlalp-Roma	23 Hours 22 seconds

Figura 46: Estado túnel vpn

En la figura anterior nos muestra el estado del túnel, así como el tráfico entrante y saliente desde que se habilito, además de indicarnos el tiempo que lleva activo.

Para que ambos extremos del túnel tengan comunicación se procede a la creación de una ruta estática para esto en el apartado Network seleccionamos Static Routes como se muestra a continuación.

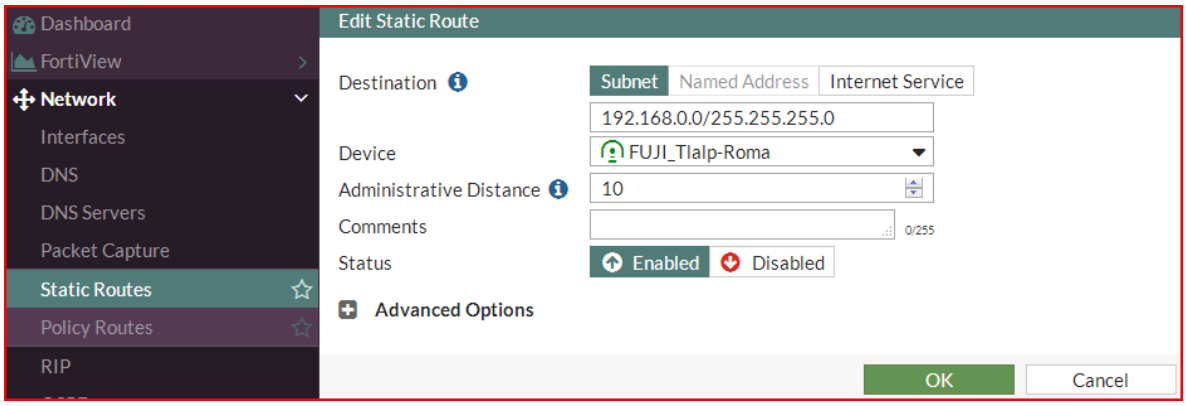


Figura 47: Ruta estática

La figura anterior contiene los campos correspondientes con la dirección IP destino y su respectiva máscara, en el caso de Device nos muestra la interfaz que se va a utilizar en este caso el túnel VPN creado FUJI_Tlalp-Roma, el resto de los campos contiene los valores por defecto, por último, damos click en OK y terminamos con la creación del túnel.

Por último, es necesario crear una política de comunicación que permita el flujo del tráfico en ambos extremos de las redes (local y remota), por lo que ahora nos ubicamos en el apartado Policy & Objects -> IPv4 Policy para proceder a llenar los campos correspondientes como se muestra en la siguiente figura.

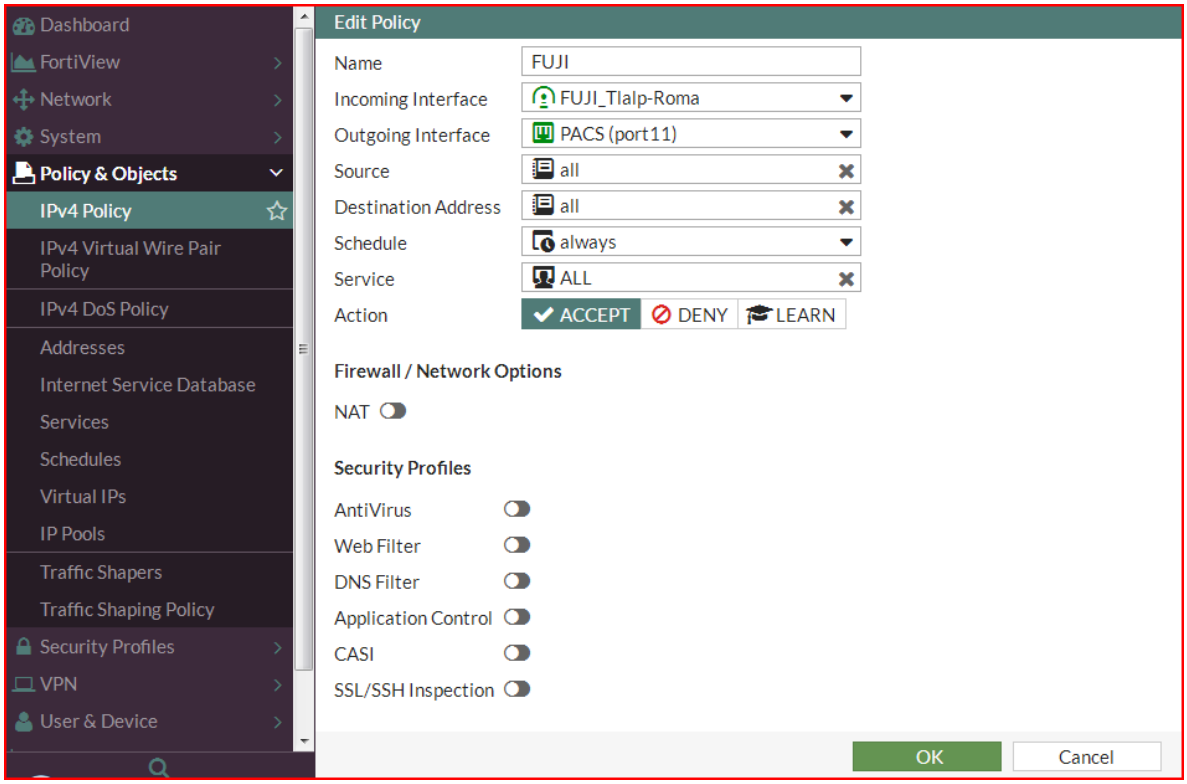


Figura 48: Política VPN

Resultados

Se cumplió el objetivo principal del proyecto manteniendo la información libre de riesgo, al tratarse de una empresa dedicada a los análisis y diagnósticos médicos en donde mantener la privacidad de los pacientes es prioritaria, además de que la transferencia, almacenamiento y disponibilidad de los estudios, por ejemplo: radiografías y electrocardiogramas fueron accesados por los especialistas correspondientes sin inconvenientes la mayoría de las veces. En las ocasiones que no se pudo acceder a esta información se debió a factores externos ajenos a la empresa, los cuales fueron cortes de la energía eléctrica y falla con el proveedor de servicios de internet. Por lo que el esquema de transferencia de archivos entre las sucursales y su servidor central resulta adecuado en base a las necesidades de la empresa.

En el caso del primer objetivo específico, el cual se cumplió obteniendo un diagrama de la red. Se trabajó con varios modelos de dispositivos, siendo el modelo 600D de los más recurrentes, al tratarse de una sucursal grande, el cual nos permitió implementar y gestionar las VPN's de manera satisfactoria para la transferencia de archivos y acceso a los recursos de red de forma remota, además de poder modelar y priorizar el tráfico de la red.

Para el segundo objetivo específico, el cual corresponde a identificar las vulnerabilidades de red, el cual se cumplió de igual forma se obtuvieron las siguientes tablas:

Principales sitios web de alto riesgo (top 10 por categoría)

Categoría del Sitio	Sitio	Usuarios	Hits
Spyware / Malicious Sites	ap.lijit.com	172.16.72.126 ip-172-17-254-114.···	3
Suspicious Content	pix04.revsci.net	172.16.72.105	1
Spam	vast.vms.cignalio.com/crossdomain.xml	ip-172-17-254-114.us-west-1.compute.internal (172.17.254.114)	1
Total: 3 Categories	**3 Sitios**	**3 Usuarios**	**5**

Tabla 5: Sitios web de alto riesgo

En la tabla anterior se puede observar el nombre y categoría de los sitios web de alto riesgo, así como las IP's correspondientes.

Principales ataques y vulnerabilidades software explotadas (top 20)

Ataque / Exploit	Source	Destination	Industria referencia	Eventos
Novell eDirectory HTTP Headers Denial of Service	ip-172-16-72-120.us-west-1.compute.internal (172.16.72.120)	198.72.116.185	CVE-2008-0927	2
		104.42.99.109	CVE-2008-0927	2
		ip-192-169-154-51.ip.secureserver.net (192.169.154.51)	CVE-2008-0927	2
		ns8710.websitewelcome.com (192.185.123.225)	CVE-2008-0927	2
		a2ss21.a2hosting.com (75.98.175.110)	CVE-2008-0927	2
		Total: 7 Destinations	1 Reference	14
	ip-172-16-72-108.us-west-1.compute.internal (172.16.72.108)	stephenking.com (67.192.185.138)	CVE-2008-0927	2
		Total: 1 Destination	1 Reference	2
	Total: 2 Sources	8 Destinations	1 Reference	16
Malformed Key Exchange Init Message	ip-192-168-50-7.us-west-1.compute.internal (192.168.50.7)	ip-192-168-50-250.us-west-1.compute.internal (192.168.50.250)	CAN-2006-2407 CAN-2006-2421	11
		Total: 1 Destination	2 References	11
	Total: 1 Source	1 Destination	2 References	11
Microsoft SMB Infinite Loop Denial of Service (MS09-050)	ip-172-16-72-109.us-west-1.compute.internal (172.16.72.109)	ip-172-16-72-80.us-west-1.compute.internal (172.16.72.80)	CVE-2009-2526	1
		Total: 1 Destination	1 Reference	1
Microsoft SMB Infinite Loop Denial of Service (MS09-050)	ip-172-16-72-120.us-west-1.compute.internal (172.16.72.120)	ip-172-16-72-80.us-west-1.compute.internal (172.16.72.80)	CVE-2009-2526	1
		Total: 1 Destination	1 Reference	1
	ip-172-16-72-111.us-west-1.compute.internal (172.16.72.111)	ip-172-16-72-80.us-west-1.compute.internal (172.16.72.80)	CVE-2009-2526	1
		Total: 1 Destination	1 Reference	1
	Total: 3 Sources	1 Destination	1 Reference	3
Total: 3 Ataques / Exploits	**5 Sources**	**10 Destinations**	**4 References**	**30**

Tabla 6: Ataques y vulnerabilidades

En la tabla anterior se observan los nombres de los ataques que fueron detectados, así como sus direcciones IP tanto fuente como destino, particularmente el ataque **Microsoft SMB Infinite Loop** fue el causante de una situación en la que un equipo no paraba de mandar solicitudes a una IP, lo cual provoco una saturación, debido a la gran cantidad de peticiones que se generaban hacia un servidor, lo cual comprometió el funcionamiento de los servicios de la sucursal.

En la siguiente tabla se muestra las aplicaciones web basadas en cloud, en las cuales se tuvo fuga de datos.

Aplicaciones web basadas en Cloud (top 20)

Nombre de Aplicación	Tráfico total en Bytes	Application Category	Usuarios
Dropbox	124.5MB	File Storage and Sharing	1 Usuario
Skype for Business (Lync)	109.2MB	Business / Economy	33 Usuarios
Office365	62.7MB	Business Applications	14 Usuarios
Office365-Outlook-web	30.0MB	Email	3 Usuarios
Google Analytics	5.6MB	Business Applications	22 Usuarios
Zendesk	2.6MB	Business Applications	4 Usuarios
Google Cloud Storage-download	1.7MB	File Storage and Sharing	8 Usuarios
Google Drive-web	1.0MB	File Storage and Sharing	1 Usuario
Adobe Connect	160.0KB	Web Conferencing	2 Usuarios
Google Cloud Storage	48.0KB	File Storage and Sharing	1 Usuario
Google App Engine	32.0KB	Web Services Provider	1 Usuario
Total: 11 Applications	**337.6MB**	**6 Categories**	**33 Usuarios**

Tabla 7: Aplicaciones basadas en cloud

Para el tercer objetivo específico el cual corresponde a diseñar políticas de seguridad, el cual también se cumplió, en este objetivo resulto ser una tarea más sencilla de lo esperado, ya que no se conocía la forma de operar del firewall. Para el caso de la implementación de la VPN crear la política es una tarea necesaria, ya que sin ella la comunicación entre ambos extremos de la comunicación no podría efectuarse. Anteriormente se mencionó el ataque

Análisis y discusión de resultados

Como se mencionó anteriormente se implementó una vpn para la transferencia de los archivos, con su política correspondiente, a continuación, se muestran tres gráficas en las cuales se observa en comportamiento de las vpn's durante una semana, solo se muestra su comportamiento al primero, cuarto y séptimo día.

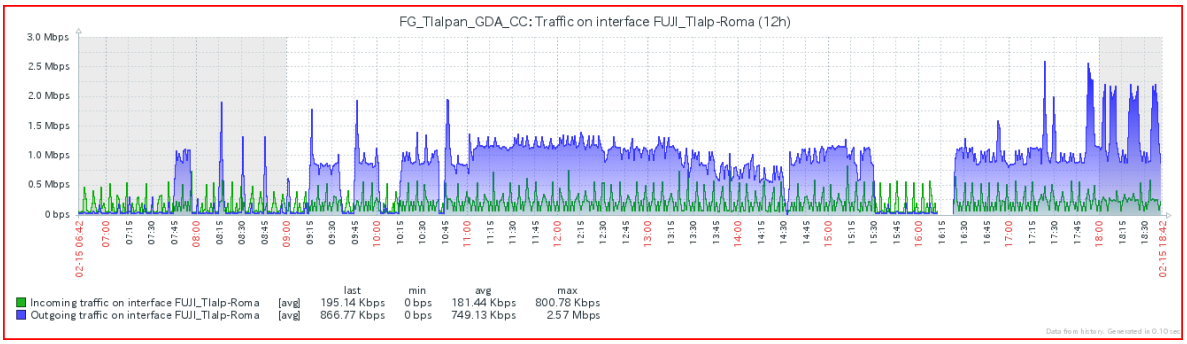


Figura 49: Primer día de monitoreo

Para la transferencia de archivos se había propuesto un traffic shaper de 1.5 Mbps, el cual claramente fue rebasado como se puede apreciar en la gráfica en más de una ocasión, alcanzo un valor ligeramente superior a los 2.5 Mbps, lo cual es demasiado y provocó una saturación. La propuesta del traffic shaper se realizó en base a un monitoreo semanal previo basado en el esquema de transferencia anterior mediante ftp. Adicionalmente observamos poca actividad desde las 15:30 pm, hasta encontrarnos con un corte de energía a las 16:15 pm.

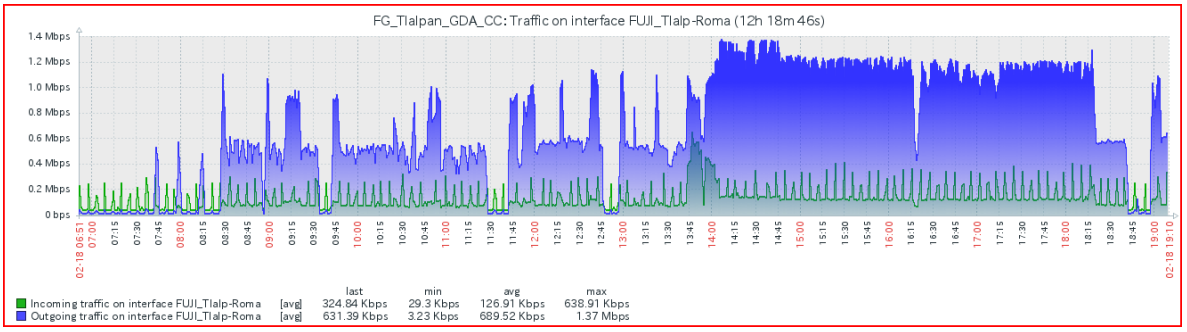


Figura 50: Cuarto día de monitoreo

En la gráfica del cuarto día se observa que el traffic shaper de 1.5 Mbps no es rebasado en ningún, su valor máximo alcanzado fue de casi de 1.4 Mbps, además se puede observar también un periodo de gran actividad desde las 13:00 pm hasta las 18:45 pm.

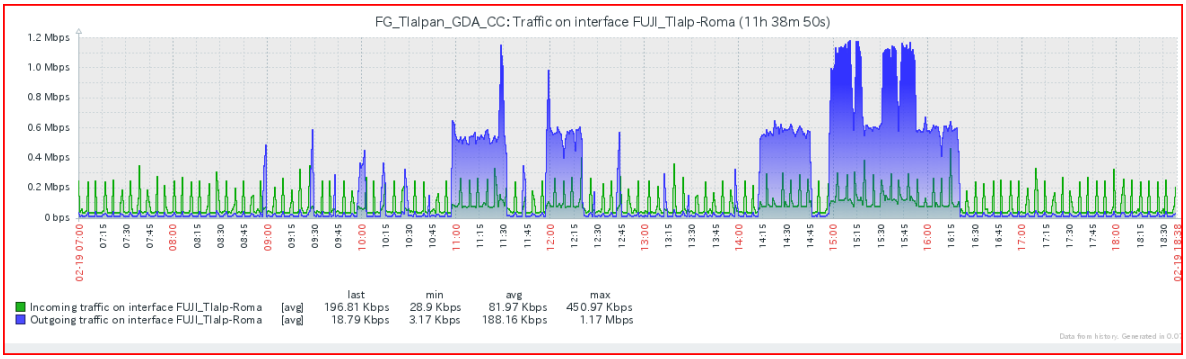


Figura 51: Séptimo día de monitoreo

Para la gráfica del séptimo día es claramente visible que la actividad es mucho menor comparada con los otros días, ya que corresponde al monitoreo de un domingo, aun así, su traffic shaper no fue rebasado, su valor máximo alcanzado fue de 1.17 Mbps.

Finalmente, después de una semana de monitoreo se concluyó que la implementación de la vpn fue satisfactoria, aunque al principio se encontraron algunos inconvenientes como la saturación en el primer día de monitoreo, por lo que se procedió a la reimplementación de la vpn y su traffic shaper. El comportamiento de la vpn puede variar considerando factores como: el día de la semana en que se efectúan los envíos, en donde claramente los fines de semanas es donde la actividad es menor, el tipo de estudio realizado, ya que hay estudios que requieren diferentes vistas de una misma extremidad y por último factores externos como cortes de energía y falla de proveedor de servicios de internet.

También se detectaron amenazas y vulnerabilidades en la red, en el caso del malware se debe a la explotación de las vulnerabilidades en los archivos descargados, como los archivos con la extensión .exe, los cuales en ocasiones son descargados por el personal desde sitios web no verificados y los archivos adjuntos de correo electrónico. Anteriormente se mencionó el ataque **Microsoft SMB Infinite Loop**, el cual corresponde a un ataque de denegación del servicio, si bien no dejo la red inhabilitada, si afecto la comunicación por voz y la transferencia de archivos tardaba más tiempo del normal en efectuarse. En cuanto a la fuga de datos en aplicaciones basadas en la nube, los cuales no resultaron ser tan significativos, pero es algo a tener en cuenta ya que de ser información valiosa la que se filtra pondría en una situación comprometedora a la empresa, esto ocurre en ocasiones por el desconocimiento del personal que de cómo funciona el sistema de transferencia de archivos y elijen la opción que consideran más fácil, así la solución inmediata más fácil es capacitar al personal y la otra es implementar un servicio en la nube propio de la empresa, pero eso dependerá de las necesidades y recursos de la empresa.

Conclusiones

En el desarrollo de este proyecto se puede apreciar que el tema de la seguridad en las redes de computadoras no siempre puede resultar ser una tarea tan sencilla como parece, ya que dicha tarea no solo se reduce a instalar antivirus y actualizar programas, en ocasiones el problema de la seguridad puede comprender desde un error en el diseño de la red, hasta el simple hecho de no contar con las herramientas adecuadas para dicho propósito, y así como hay avances en sistemas computacionales y otras tecnologías, nuevas amenazas surgen día a día para vulnerarlas.

Actualmente el uso del internet se ha vuelto imprescindible en los negocios y debido a la constante evolución del mismo hace que sea difícil de proteger y hacer cumplir su uso adecuado en un entorno corporativo. Ya que actualmente no solo podemos encontrar el clásico tráfico de las url's, sino que además se ha sumado a ellas el tráfico generado por aplicaciones basadas en la nube y el correspondiente a aplicaciones embebidas.

Por último, la experiencia de trabajar con dispositivos fortigate resultó satisfactoria, ya que permite una fácil implementación y gestión de las políticas, VPN's, filtros web y otras aplicaciones por medio su interfaz web. Un aspecto no tan favorable de esta marca es que las actualizaciones de su sistema operativo contienen bugs, lo cual soluciona problemas de versiones anteriores, pero puede comprometer la funcionalidad de otros componentes que funcionaban adecuadamente antes de dicha actualización, por lo que siempre es necesario revisar las notas de publicación para verificar que el funcionamiento de los componentes necesarios para mantener la seguridad en la red sea siempre el adecuado.

En base al calendario planteado en el documento de la propuesta del proyecto de integración, no se realizó ningún documento correspondiente a dichas actividades, ya que las actividades realizadas corresponden a las especificadas con anterioridad en el presente documento, y por lo tanto no fue necesario realizar documentos tan elaborados, por lo que los únicos entregables corresponden a los diagramas de red.

Referencias Bibliográficas

[1]G. Montero Quintero, "Implementación de una NIDS en un sistema embebido para el análisis de tráfico de una red", proyecto terminal, División de CBI, Universidad Autónoma Metropolitana Azcapotzalco, México, 2014.

[2]M. Villegas García, " Diseño e implementación de un sistema honeypot como elemento para la seguridad de una red privada ", proyecto terminal, División de CBI, Universidad Autónoma Metropolitana Azcapotzalco, México, 2015.

[3]M. Shin, J. Ma, A. Mishra and W. Arbaugh, "Wireless Network Security and Interworking", *Proceedings of the IEEE*, vol. 94, no. 2, pp. 455-466, 2006.

[4]M. Wright, "Using policies for effective network management", *International Journal of Network Management*, vol. 9, no. 2, pp. 118-125, 1999.

[5]S. Nesmachnow, "Algoritmos Genéticos Paralelos y su Aplicación al Diseño de Redes de Comunicación confiable", Universidad de la República de Montevideo, Uruguay, 2004.

[6]M. Riffo Gutiérrez, "Vulnerabilidades de las Redes TCP/IP y principales Mecanismos de Seguridad", Universidad Austral de Chile, Chile, 2009.

[7]*Protocolo TCP/IP,* IETF. RFC 801, 1981.

[8]*IEEE 802.3 Ethernet*, IEEE Std. 802.3, 1983.

[9]*Carrier Sense Multiple Access with Collision Detection*, IEEE Std. 802.3, 1983.

[10]*IEEE 802.11 Wireless LANs,* IEEE Std. 802.11, 1991.

[11]*Carrier Sense Multiple Access with Collision Avoidance*, IEEE Std. 802.11, 1991.

[12]"Seguridad de redes", *Es.wikipedia.org*, 2017. [Online]. Available: https://es.wikipedia.org/wiki/Seguridad_de_redes. [Accessed: 25- May- 2017].

[13]E. Cole, R. Krutz, J. Conley and Cole, *Network Security*, 1st ed. Hoboken: Wiley [Imprint], 2009, p. 419.

[14]S. TECNOLOGÍAS, Q. (QoS), Q. Policing, I. Tecnología and P. Tecnología, "Preguntas frecuentes sobre Calidad de servicio (QoS)", *Cisco*, 2017. [Online]. Available: http://www.cisco.com/c/es_mx/support/docs/quality-of-service-qos/qos-policing/22833-qos-faq.html. [Accessed: 18- Apr- 2017].

[15]"¿Qué es el ancho de banda? - Definición de ancho de banda", *Masadelante.com*, 2017. [Online]. Available: http://www.masadelante.com/faqs/ancho-de-banda. [Accessed: 13- Jul- 2017].

[16]P. servicios, "¿Qué es un firewall?", *Cisco*, 2017. [Online]. Available: http://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html. [Accessed: 18- Apr- 2017].

[17]"Traffic Shaping | A10 Networks", *A10 Networks*, 2017. [Online]. Available: https://www.a10networks.com/resources/glossary/traffic-shaping. [Accessed: 18- Apr- 2017].

[18]E. Ariganello, *Guía de estudio para la certificación CCNA security*, 1st ed. Madrid España: Alfaomega, 2013, p. 305.

[19]*enredajo*, "Mas de Redes: Que es una VPN y tipos de VPN", 2-Mar-2009. Available: http://enredajo.blogspot.mx/2009/03/que-es-una-vpn-y-tipos-de-vpn.html. [Accessed: 18- Apr- 2017].