Licenciatura en Ingeniería en Computación

Estancia Profesional

# Seguridad Perimetral en red usando Firewall UTM (VPN, IDS e IPS)

Eduardo Mendoza Valdez

209204310

M. en C. José Alfredo Estrada Soto

Ing. Mario Ernesto Gómez Romero

Trimestre 2017-Invierno

25 de Abril 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, Eduardo Mendoza Valdez, doy mi autorización a la Coordinación de Servicios de Información 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**

La Seguridad Perimetral es de principal interés para empresas y personas que necesitan proteger información de posibles fugas o sencillamente asegurar la integridad de ésta, la protección se realiza en dos sentidos, supervisando las actividades dentro del perímetro de seguridad establecido y vigilando las conexiones que se realizan con el exterior del perímetro (entrantes y salientes).

Para poder llevar a cabo esta tarea, se hizo uso de un conjunto de herramientas que nos proporcionan diferentes niveles de seguridad de acuerdo a la necesidad de los usuarios de la red.

Se utilizaron en todo el proceso mecanismos de bloqueo para las conexiones entrantes y salientes, sistemas de detección de comportamiento/actividades poco usuales, identificación de software/protocolos ya conocidos para la toma de decisiones, sistemas de verificación de estado de las herramientas usadas.

Como resultado de la aplicación de las herramientas mencionadas se aumentó la seguridad en la red en términos de conectividad y confiabilidad de las conexiones, integridad y disponibilidad de la información.

**Tabla de contenidos**

**Índice de figuras**

**Índice de imágenes**

## 1. Introducción

En al área de las Tecnologías de la Información y la Comunicación, y en especial la rama de las Redes Computacionales y de Comunicaciones, existen problemáticas enfocadas al buen uso y resguardo de la información que se transmite y maneja, de aquí que surja una preocupación para poder subsanar las carencias de las redes de uso diario que hoy tenemos.

Una forma de proteger los datos (información) que viajan a través de las Redes de Computadoras es por medio de Seguridad Perimetral. Como bien lo indica su nombre, la Seguridad Perimetral provee a las redes de computadoras mecanismos con los cuales puedan implementar seguridad en varios aspectos y niveles de confianza, principalmente en sus canales de comunicación con el exterior a la red que se está protegiendo.

Para este proyecto, se implementaron diferentes tecnologías, tales como VPN[1], IDS[2] e IPS[3], para generar una política robusta de Seguridad Perimetral que permita diferentes niveles de confiabilidad para la transmisión de datos.

## 2. Justificación

Las redes computacionales convencionales, carecen de recursos y/o mecanismos con los cuales puedan dar niveles de confianza a los usuarios de la red. La mayoría de estas se limitan a configuraciones para poder establecer comunicación entre los dispositivos, lo que no basta para proporcionar a los usuarios de la red un mecanismo seguro con el cual puedan comunicarse y enviar información tanto a nivel local como general.

La implementación de mecanismos para la Seguridad Perimetral, infiere directamente en la necesidad de los usuarios en salvaguardar la información que viaja a través de sus ordenadores, así como determinar que los destinatarios a los que se les envíe información la reciban con integridad y confiabilidad.

La aplicación de dichos mecanismos, debe ser de forma sencilla y transparente hacia el usuario, para poder otorgar la misma o en su caso una mejor usabilidad de los servicios en la red a los que se ésta accediendo.

---

[1] Es una tecnología de red de computadoras que permite una extensión segura de la red de área local(LAN) sobre una red pública o no controlada como Internet.

[2] Un sistema de detección de intrusiones (o IDS de sus siglas en inglés Intrusion Detection System) es un programa de detección de accesos no autorizados a un computador o a una red.

[3] Un sistema de prevención de intrusos (o por sus siglas en inglés IPS) es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

## 3. Objetivos

**Objetivo general:**

- Desarrollar un protocolo de Seguridad Perimetral para mejorar los niveles de confianza a los usuarios de una red corporativa.

**Objetivos específicos:**

- Categorizar el listado de equipos y tipo de conexión.
- Determinar la topología de red implementada.
- Generar una lista de los servicios y/o aplicativos para obtener los utilizados en la red, en función de las responsabilidades de cada usuario.
- Implementar el Firewall UTM[4] para crear el primer pilar de gestión de seguridad.
- Identificar las situaciones que generen alertas, que ayuden a establecer la actuación del IDS, comunicando al Firewall de cualquier inconsistencia.
- Generar políticas de funcionamiento para el IPS que verifiquen el tráfico entrante y saliente de la red con los niveles de confianza asignados.
- Implementar una VPN para transmisión de información segura entre nodos lejanos.
- Validar el funcionamiento del protocolo de seguridad perimetral en todos sus niveles.

## 4. Antecedentes

### Proyectos

**Sistema de filtrado para una red de computadoras mediante herramientas gráficas en Linux [1]**

- Al igual que en este proyecto se buscó hacer un filtrado de paquetes (datos) para mantener un nivel de seguridad mayor al usado por defecto. Para su realización, dicho trabajo utiliza Iptables, un firewall que incorpora NAT[5], en comparativa con lo que se realizó es que el filtrado a través de reglas y uso de NAT en modo gráfico ya se encuentran integrados en el Firewall UTM del que se hizo uso, así como otras herramientas y módulos para la seguridad de la red.

**Diseño e implantación de una LAN virtual con switches de red [2]**

- El proyecto describe el proceso de simulación para formular una red LAN(Local Area Network) utilizando el software Packet Tracer[6], de forma similar a lo realizado,

[4] UTM (en inglés: Unified Threat Management) o Gestión Unificada de Amenazas. El término fue utilizado por primera vez por Charles Kolodgy, de International Data Corporation (IDC), en 2004.

[5] La traducción de direcciones de red o NAT (del inglés Network Address Translation) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

[6] Cisco Packet Tracer de Cisco es un programa de simulación de redes que permite a los estudiantes experimentar con el comportamiento de la red y resolver preguntas del tipo «¿qué pasaría si...?».

abunda en la conectividad y la utilización de políticas de ruteo, que ayudan a mejorar a la dispersión de los segmentos de red, apoyando de cierta manera la integridad de los datos en calidad de servicio y las rutas permitidas en los segmentos ahí utilizados, ello, a diferencia de que lo realizado, se enfocó de forma profunda en brindar mecanismos de seguridad en los segmentos de red más allá de una LAN virtual o física, para mejorar la integridad y seguridad básica con que cuenta la red.

**El problema de agotamiento de las direcciones lógicas y un método para su resolución en IPv.4 [3]**

- En el proyecto se hace uso de NAT e IPv.6(Internet Protocol versión 6) para solucionar la escasez de direcciones en IPv.4, en el caso de lo realizado también es usado NAT pero no para subsanar el agotamiento de direcciones sino que es usado para el redireccionamiento de IP Públicas(externas) a Privadas(Internas) con la finalidad de proporcionar los servicios solicitados.

**Artículos**

**Seguridad y privacidad en los sistemas informáticos [4]**

- El artículo muestra la seguridad de los sistemas informáticos en términos generales, teniendo una buena referencia sobre la seguridad perimetral, también de la manera en que actúan los distintos componentes que conforman las políticas de seguridad informática, en lo realizado se hace uso de tecnologías precisas y la aplicación de las mismas, así como determinadas tareas específicas necesarias para su aplicación.

**Software**

**Adaptive Security Appliance (ASA) Software [5]**

- Este software ofrece un sistema Unificado de protección muy similar al que se utilizó, con la principal diferencia de que su enfoque mantiene la administración vía consola, esto implica una mayor complejidad en cuanto al uso de sus herramientas para poder ejercer las políticas de seguridad.

**Endpoint Security [6]**

- Se centra en un sistema de soluciones distribuidas más que unificadas, razón por la cual hace falta implementar los mecanismos que nos ofrece en sus diversas categorías, en lo realizado se utiliza un Sistema Unificado para dar solución integral a las problemáticas que se nos presentan.

## 5. Marco Teórico

Se ha explicado en la introducción sobre la importancia de la Seguridad Perimetral, debemos conocer las clasificaciones respecto los sistemas de seguridad perimetral, y cuál es el enfoque que llevan.

Entre los principales sistemas encontramos: Sistemas perimetrales abiertos, Sistemas perimetrales cerrados.

Los sistemas abiertos y cerrados, a su vez son clasificados por su actuación física, clasificados por sistemas de soporte, clasificados por la geometría de su cobertura.

### Sistemas perimetrales abiertos

Estos sistemas son dependientes de las condiciones ambientales, previenen y detectan problemas climáticos, desastres naturales, alteraciones en el entorno físico, situaciones de emergencia o que representen alguna amenaza hacia el perímetro asegurado.

Los elementos más comunes a encontrar en los sistemas abiertos son:

- Sistemas de videocámaras
- Sensores de temperatura, vibración y movimiento
- Alarmas de microondas

El uso de los sistemas perimetrales abiertos está destinado principalmente a estaciones médicas, fronteras, aeropuertos, bases militares, bancarias, establecimientos gubernamentales, y su aplicación tiene un alcance generalizado a todo el personal que se encuentra de la zona perimetral a asegurada.

### Sistemas perimetrales cerrados

Los sistemas perimetrales abiertos no dependen de las condiciones ambientales, al igual que los sistemas cerrados previenen y detectan problemas, alteraciones o desastres que puedan presentarse en el perímetro asegurado, la diferencia reside en que lo hacen en los sistemas de cableado, fibra óptica, sensores y aparatos de comunicaciones.

Sus elementos más comunes son:

- Analizadores biométricos
- Tarjetas inteligentes
- Cerraduras eléctricas
- Sensores de continuidad eléctrica

Estos elementos pueden desempeñar sus funciones de manera individual o en conjunto dentro de equipos de comunicación o transporte de información, muchos de los últimos con un enfoque informático o de redes computacionales.

**Clasificados por actuación física, por sistemas de soporte, por la geometría de su cobertura**

La clasificación en éste sentido es muy laxa, ya que existe una infinidad de ambientes de aplicación en los que la combinación entre las clasificaciones esta dada.

En el caso de actuación físico el tipo de fibra o cableado en caso alámbrico, frecuencias y canales en caso inalámbrico.

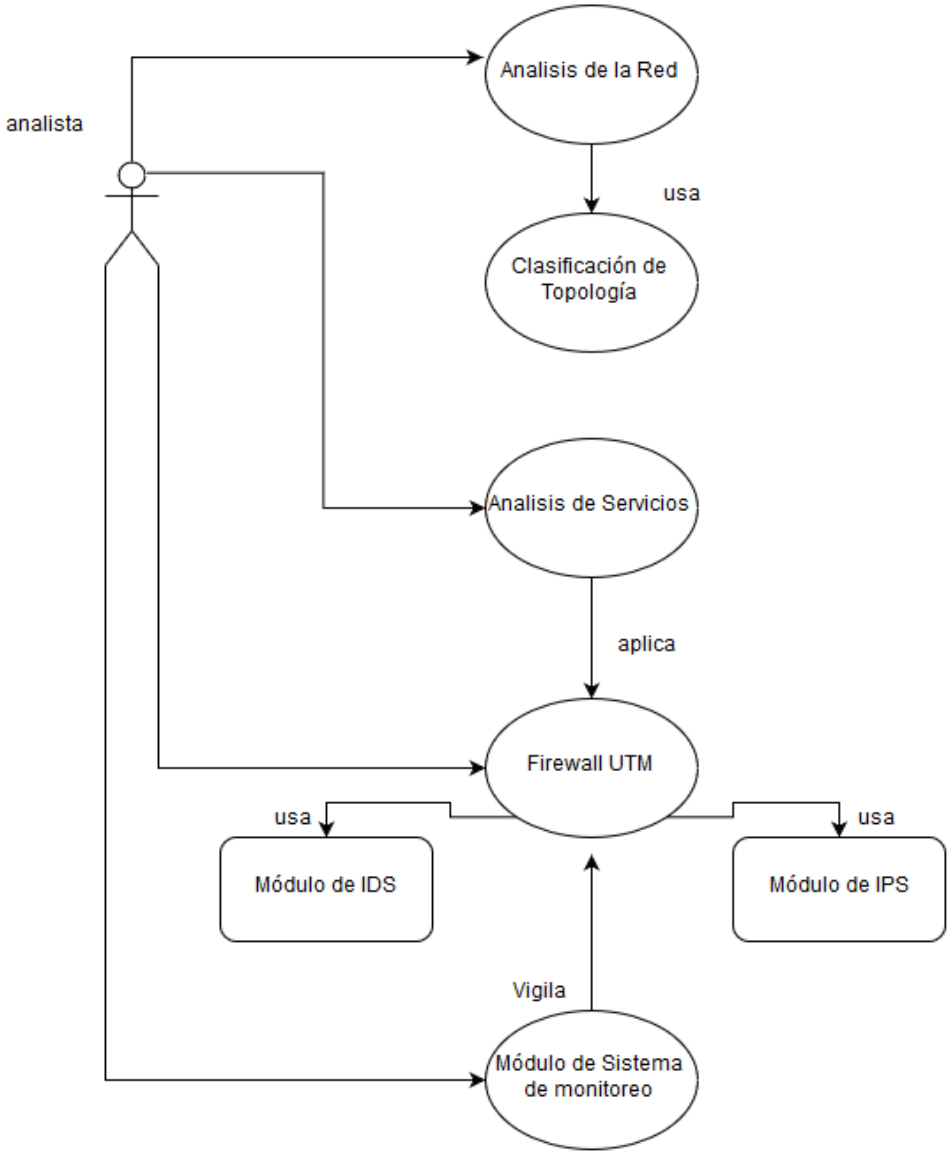
Para los clasificados por sistema de soporte derivan en si nativamente son auto-soportados por la plataforma, si son soportados de alguna forma, se encuentran enterrados, pueden ser detectados visualmente.

Finalmente, los clasificados por la geométrica de su cobertura, de estos se dicen si son volumétricos, superficiales o lineales en cuanto su aplicación en el sistema.

## 6. Desarrollo del proyecto

### 6.1 Descripción técnica

En la Figura 1 se describe la interacción entre los módulos de la política de seguridad llevada a cabo en términos generales, usando la metodología de casos de uso.




***"Figura 1. Proceso general para la implementación de una política de Seguridad Perimetral."***

**Descripción de los Módulos que componen la Seguridad Perimetral**

Análisis de Topología

La función de esta fase es registrar todos los elementos que componen la red y como están interconectados entre sí, entregando un listado de los dispositivos encontrados.


***"Figura 2. Fase de Análisis de Topología."***

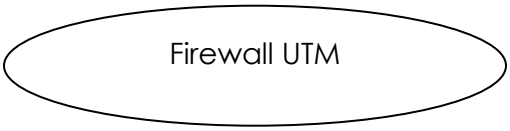
Análisis de Servicios

Su objetivo es establecer que Servicios son requeridos por los usuarios en términos de aplicativos, puertos o protocolos, entregando un listado de los servicios y protocolos usados.


***"Figura 3. Fase de Análisis de Servicios."***

Firewall UTM

Su función es poner a disposición de la red componentes que sirven para su gestión y funcionamiento planificado.




***"Figura 4. Implementación de Firewall UTM."***

Módulo de IDS

Se encarga de generar las alertas de un comportamiento fuera de lo esperado para su posterior bloqueo por el Firewall.


***"Figura 5. Integración del Módulo IDS."***

Módulo IPS

La tarea que desempeña es corroborar que las políticas de seguridad que norman el tráfico de la información sean cumplidas, permitiendo o denegando el servicio según se indica, abonando la generación de la política de seguridad general.


***"Figura 6. Integración del Módulo IPS."***

Sistema Monitoreo

La función de este sistema consiste en supervisar que los equipos tengan disponibilidad en tiempo real, así como verificar el estado de los servicios que ofrece este dentro de lo establecido.


***"Figura 7. Integración del Sistema de Monitoreo."***

### 6.2 Especificación técnica

Se desarrolló el proyecto utilizando primeramente los 8 tipos de Topologías reconocidas en el ámbito de las Redes Computacionales para categorizar cuál o cuáles son el tipo de red que contamos; lo antes mencionado se llevó a cabo tomando en cuenta los tipos de conexiones y dispositivos enlazados, después de la verificación física de equipos y conexiones, y en los casos en que se tuvo que aclarar algún segmento privado o del cual no se tuvo suficiente información, utilizamos el Software de escaneo Network Mapper[7](NMAP) para apoyarnos en la tarea de realizar el mapa de la red de los diferentes hosts y dispositivos en el segmento.

Se escanearon los servicios usados con NMAP, se clasificaron cuáles eran necesarios y por tanto debían ser permitidos y monitorizados, también se complementó la tabla de protocolos y servicios usados por los Hosts en los que usamos el control de aplicaciones.

El resultado del uso de aplicaciones, tareas y cargos a realizar por parte de los usuarios dio como resultado diversos niveles de confianza, estos van desde Básico, General, Intermedio o Avanzado también llamado VIP(Very Important Person); éstos niveles de confianza o perfiles van disminuyendo las restricciones hablando de acceso a diferentes sitios o aplicaciones, ancho de banda, o tipo de asignación de IP. Todas estas reglas están directamente aplicadas en las políticas de tráfico.

[7] Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon (más conocido por su alias Fyodor Vaskovich y cuyo desarrollo se encuentra hoy a cargo de una comunidad.

Teniendo en cuenta lo anterior, implementamos el Firewall UTM haciendo uso de equipo de la línea Fortigate tecnología perteneciente a la empresa Fortinet para poder configurar los bloqueos, trabajando en conjunto con las alertas que definimos en el Módulo IDS sobre el estado de la Red y el mismo Firewall.

Creamos políticas de tráfico para la entrada y salida de datos con las que evalúa el Módulo IPS los bloqueos de paquetes y conexiones que se realizan en el momento que es recibida una solicitud a determinados destinos.

Se especificó la conexión de un canal VPN con RSA[8] o SHA[9] e IKE[10] para la codificación y encriptación del túnel entre nodos distantes, para hacer conexiones seguras que permitirán el intercambio de información, esto gracias al túnel encapsulado que ya puede viajar sobre redes no cifradas.

Monitoreamos el estado de los equipos con el Software Zabbix por medio del protocolo SNMP, el cual nos proporciona la información de saturación, conexión, uso de memoria interna y la cantidad de procesamiento ocupado por nuestro Firewall y equipos asociados.

Al concluir el proyecto de integración se entregará un disco compacto al Coordinador de Estudios de Ingeniería en Computación que incluirá el reporte final del proyecto en un archivo PDF (sin restricciones) y el código fuente de la aplicación en un archivo comprimido (sin restricciones)[11] . El reporte final contendrá al menos: portada, resumen, tabla de contenido, introducción, antecedentes, justificación, objetivos, marco teórico, desarrollo del proyecto, resultados, conclusiones, bibliografía, apéndices y otros entregables (en caso de ser necesario). Los apéndices contendrán al menos un listado del código fuente desarrollado.

8 En criptografía, RSA (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.
9 El SHA (Secure Hash Algorithm, Algoritmo de Hash Seguro) es una familia de funciones hash de cifrado publicadas por el Instituto Nacional de Estándares y Tecnología (NIST).
10 Internet key exchange (IKE) es un protocolo usado para establecer una Asociación de Seguridad (SA) en el protocolo IPsec.
11 Se debe poder descomprimir sin restricciones tecnológicas.

### 6.3 Recursos Empleados

#### Hardware

- FortiGate 100D
- FortiAP-320C
- Cisco 3500 Series 48 Port Switch
- PC Corei7 6G 6700K, 32 Gb 3200Mhz, 1 SSD 120GB, 2 HDD 1TB, 4 Adaptadores Red 1Gb, Cosair 80H.

#### Software

- FortiOS 5.4
- Nmap 7.30
- Zabbix 3.0.2

## 7 Resultados

Una vez aplicados los procedimientos para acoplar el sistema de seguridad perimetral a la red computacional y cumpliendo los objetivos propuestos, podemos observar:

- Alta disponibilidad de los recursos y servicios de red proporcionados.
- Mejor distribución en el ancho de banda asignado a los diferentes segmentos de red.
- Avisos oportunos al intentar acceder a segmentos o sitios no autorizados.
- Calidad de servicio en los enlaces de comunicación.
- Aumento de la confiabilidad en los canales de transferencia de información.
- Mayor nivel de seguridad a nivel de red y aplicación dentro de la red asegurada con la aplicación de permisos de usuario.

## 8 Análisis y discusión de resultados

Es crucial observar que para poder llevar acabo los diferentes procedimientos es necesario hacer un estudio a detalle de las necesidades de la red, los recursos físicos con que se cuentan y el enfoque que se quiere dar a la red y en general al sistema de seguridad perimetral.

Para lo cual debemos observar el comportamiento de los equipos de la red, así como de las personas, es fácil notar que a mayor nivel de detalle se tenga en la observación para cada segmento de red, que para el caso de una empresa son áreas, departamentos, puestos y usuarios, mejor serán los perfiles de seguridad y una mejor experiencia se podrá dar en cuanto a la personalización de niveles de confianza, conectividad, accesibilidad a los servicios y recursos de red, etc.

## 9 Conclusiones

La aplicación de Sistemas de Seguridad Perimetral es un paso importante para la protección de la información dentro de las redes informáticas y los sistemas computacionales en general.

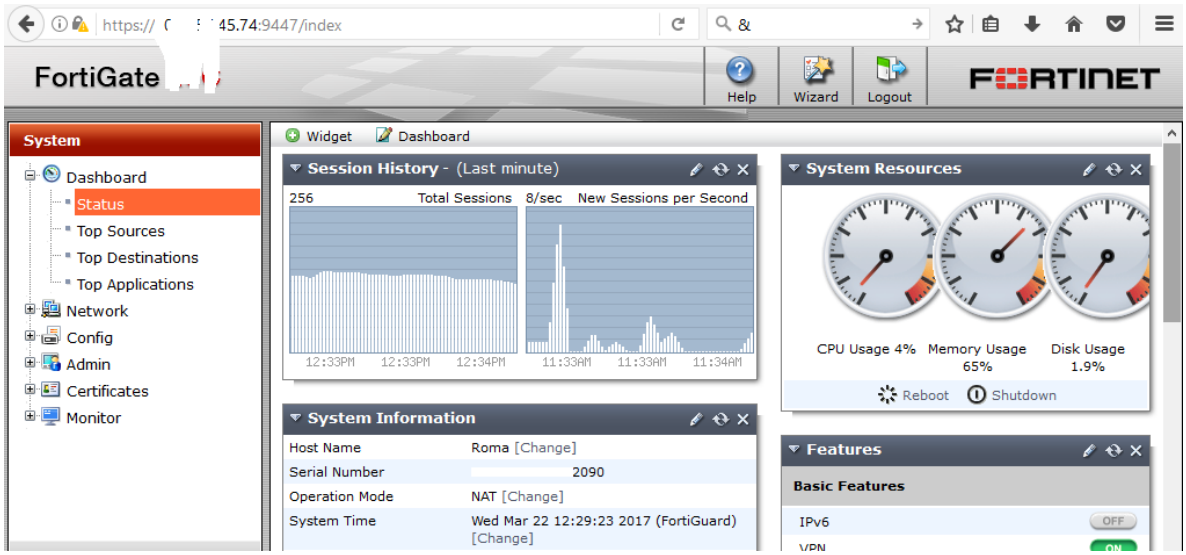
Esto es debido a que nos ayuda a tener un nivel se certeza en el intercambio de datos de un lugar a otro, además de proporcionarnos mejor disponibilidad a los servicios con que cuenta la red.

También es importante recalcar que implementa niveles de jerarquía a los usuarios de acuerdo a la naturaleza de sus necesidades, proporcionando desde un mayor ancho de

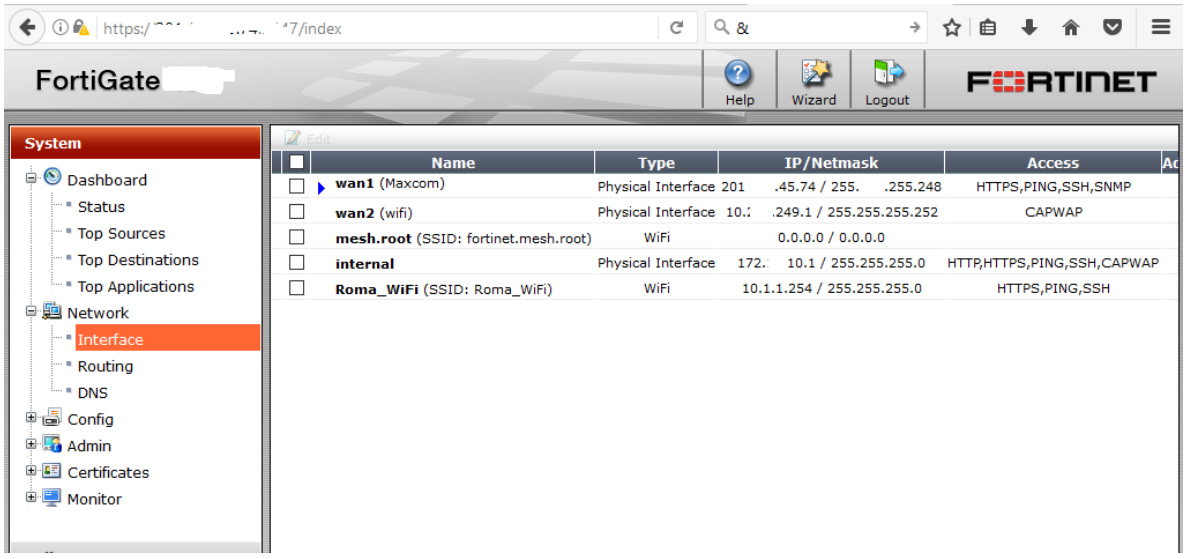
banda, hasta acceso a diferentes servicios, mejorando en términos generales el funcionamiento total de la red, así como el de sus usuarios.

## 10 Entregables

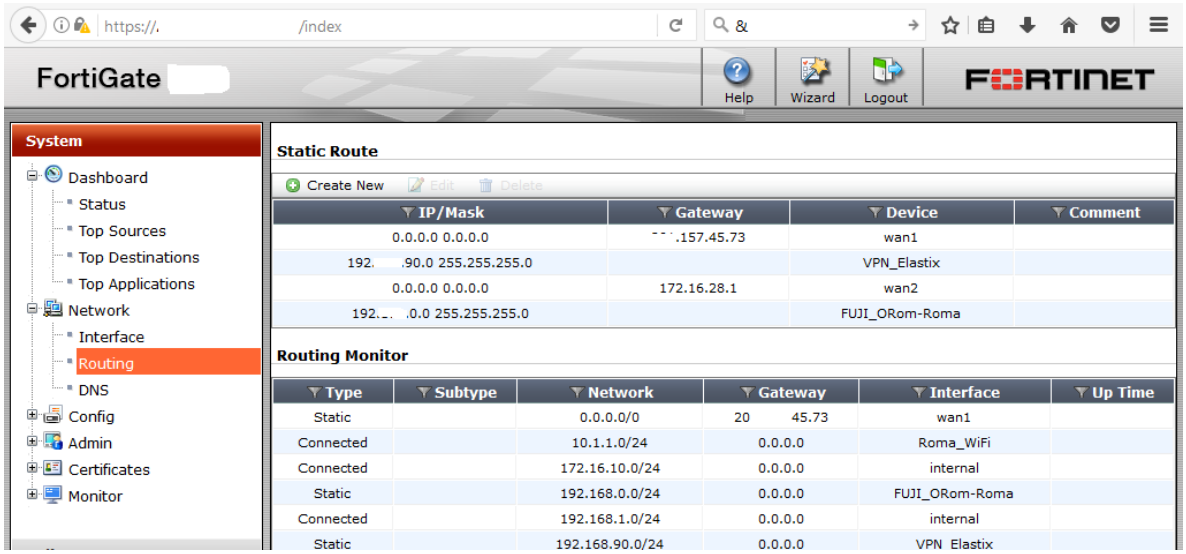
Vistas de funcionamiento general.



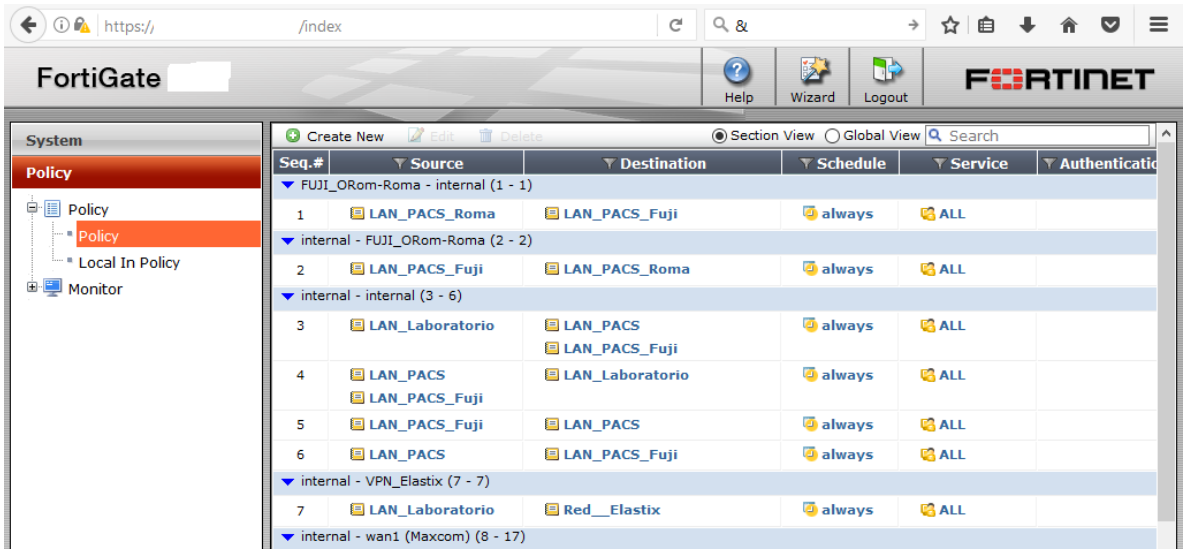

*"Imagen 1. Estado general del Equipo."*



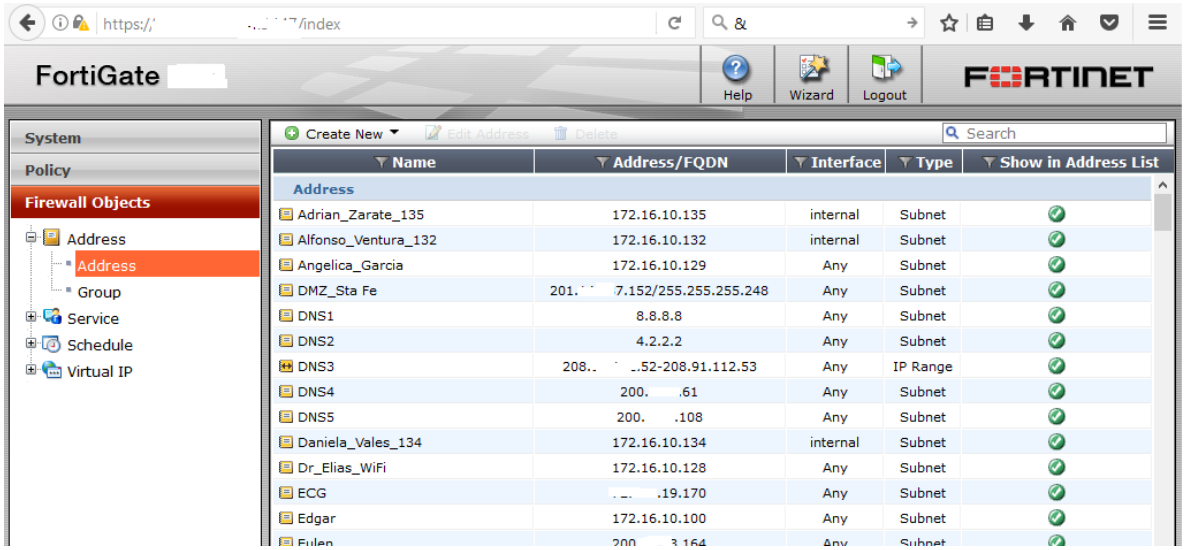

*"Imagen 2. Interfaces físicas del Firewall."*



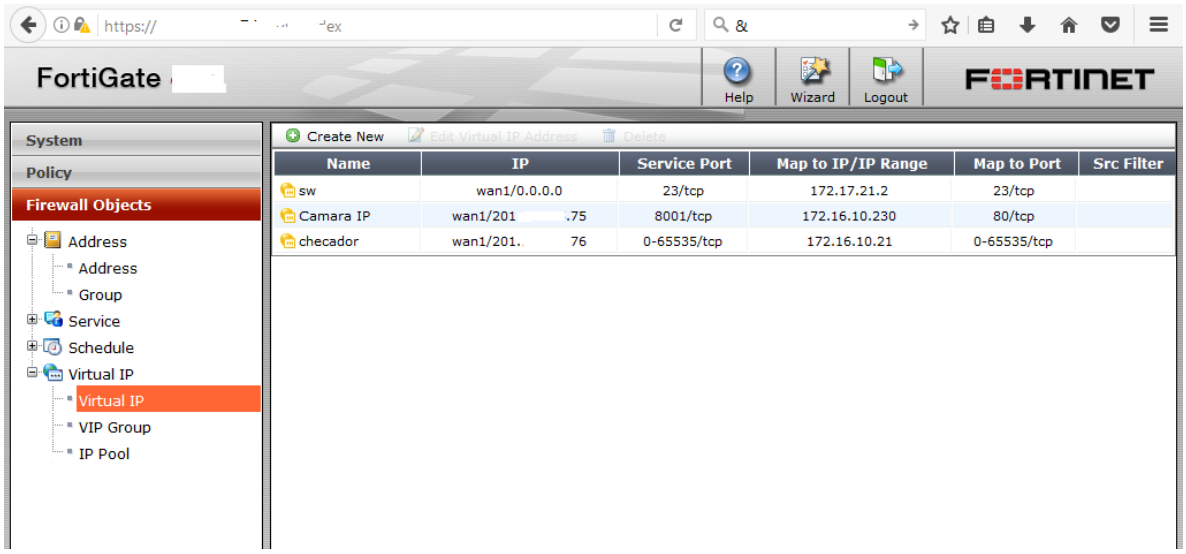

*"Imagen 3. Direcciones de ruteo estático."*



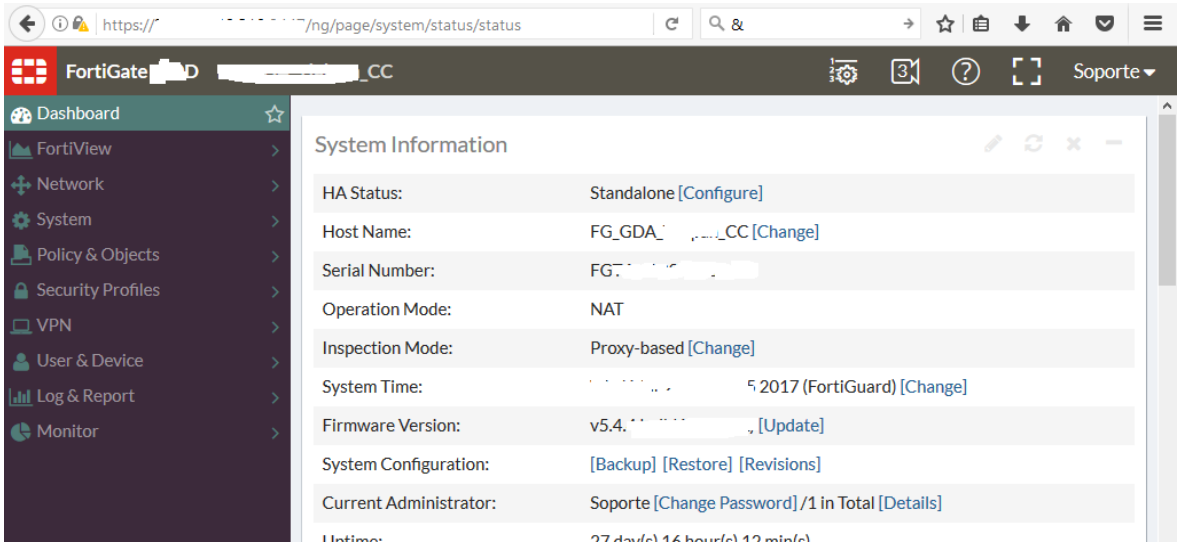

*"Imagen 4. Políticas de tráfico interno y externo."*



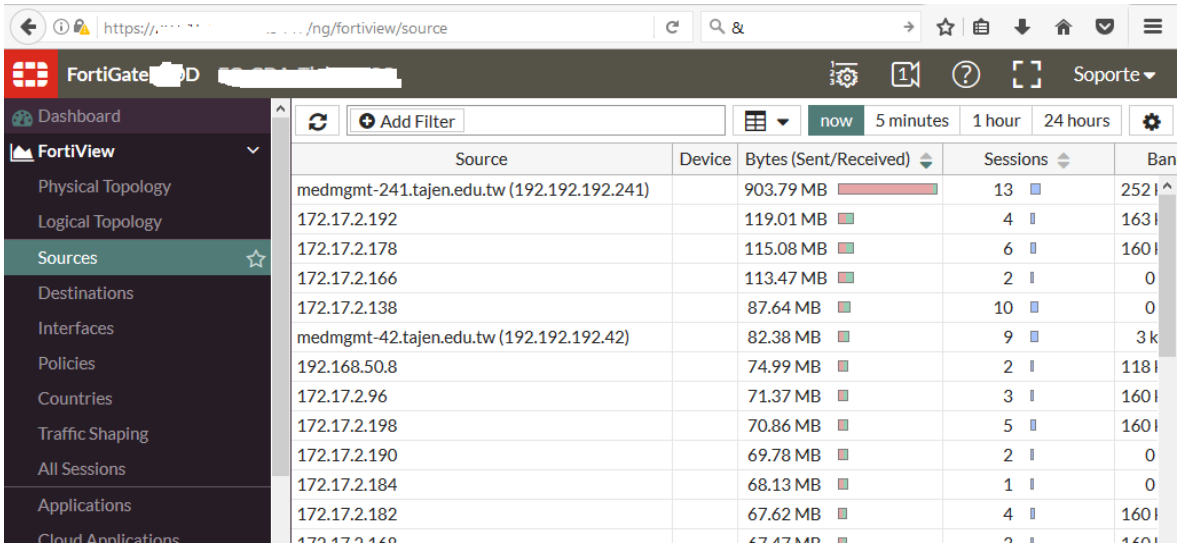

*"Imagen 5. Objetos de los usuarios usados en las políticas y restricciones."*



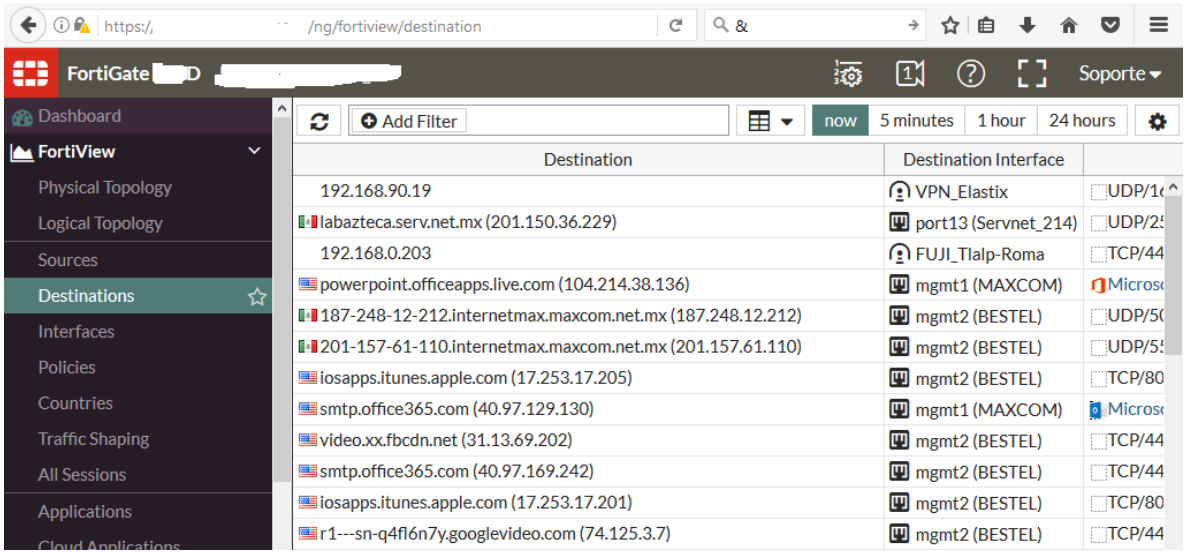

*"Imagen 6. Objetos de recursos externos usados en las políticas y restricciones."*



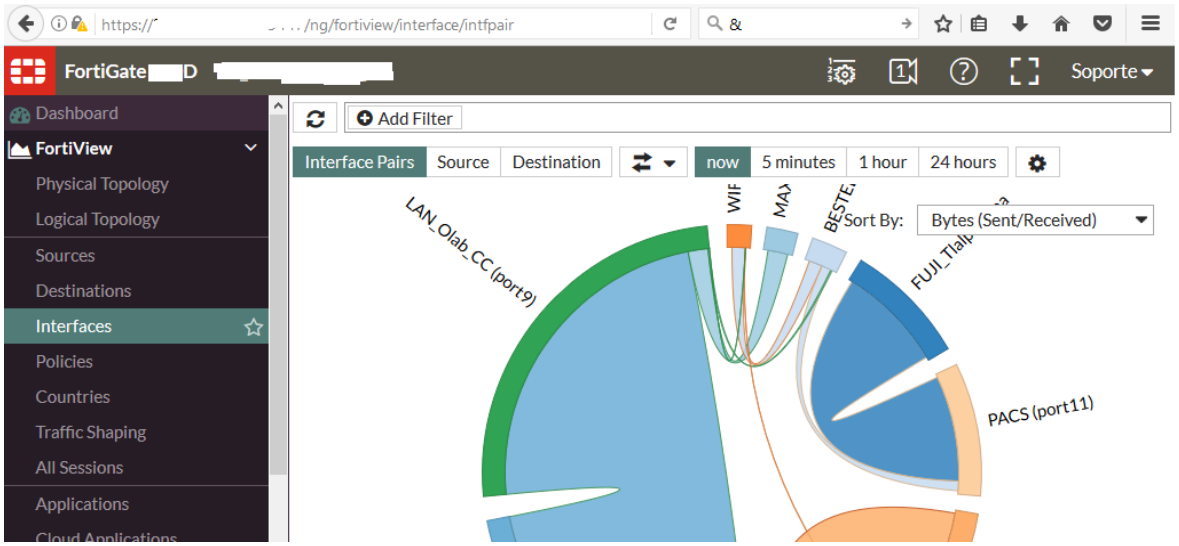

*"Imagen 7. Información administrativa y modo de operación del Equipo."*



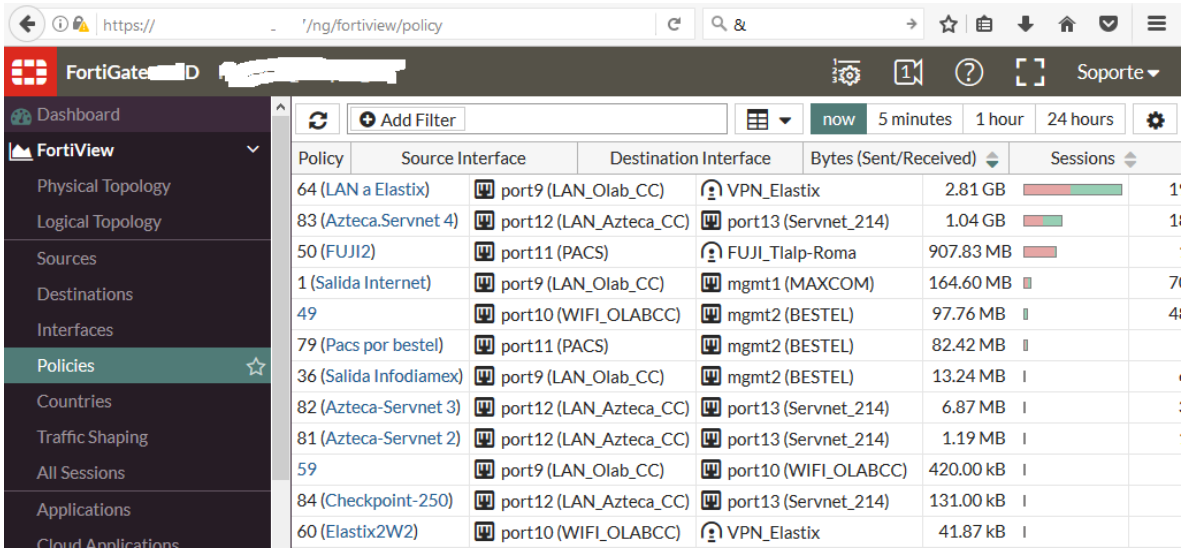

*"Imagen 8. Fuentes de consumo de tráfico."*



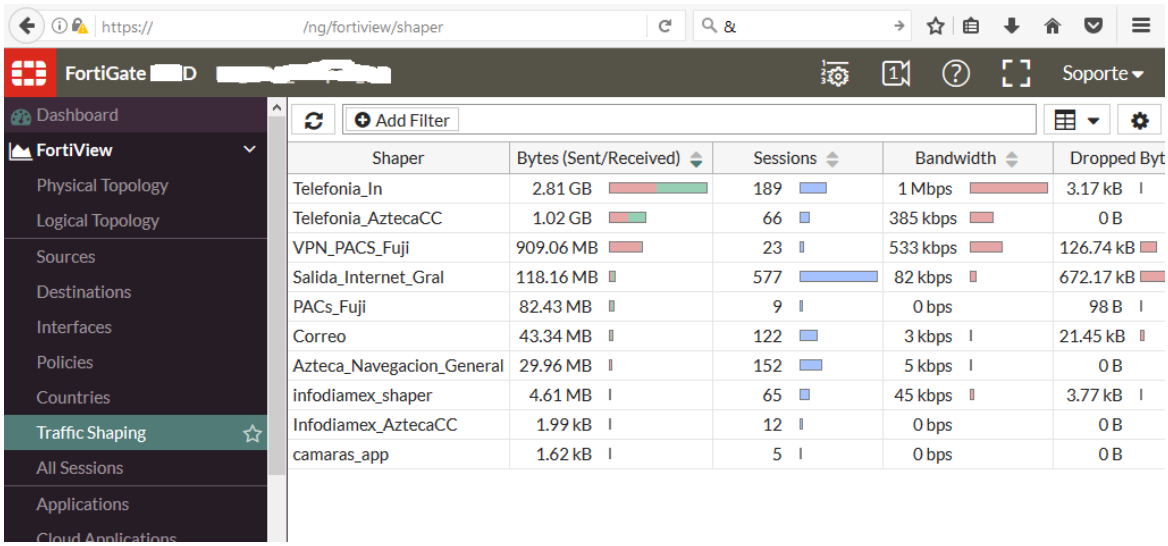

*"Imagen 9. Destinos del tráfico consumido."*



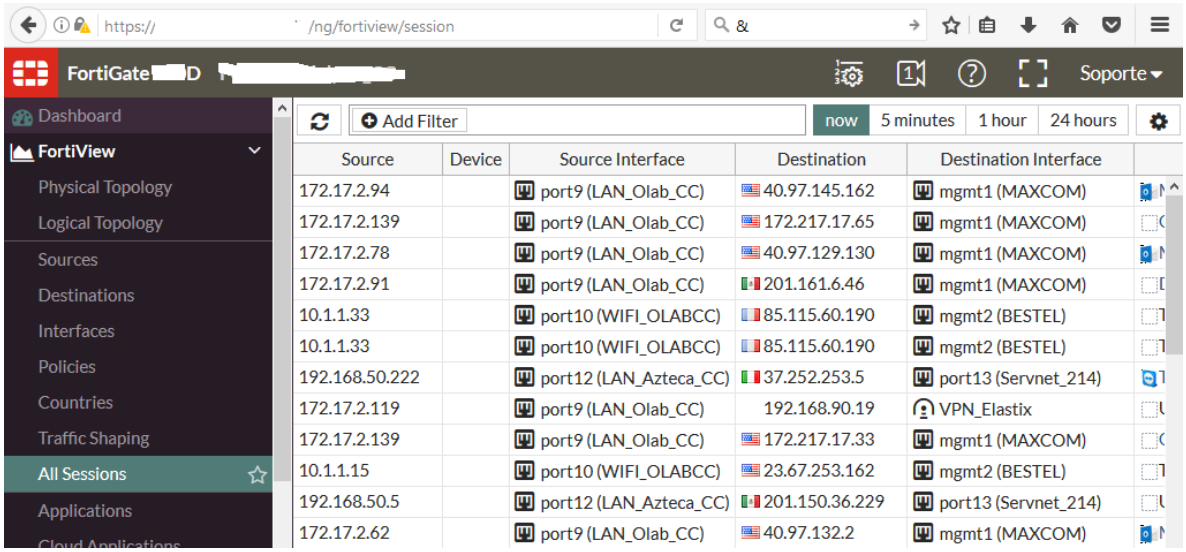

*"Imagen 10. Interfaces con tráfico permitido entre ellas."*



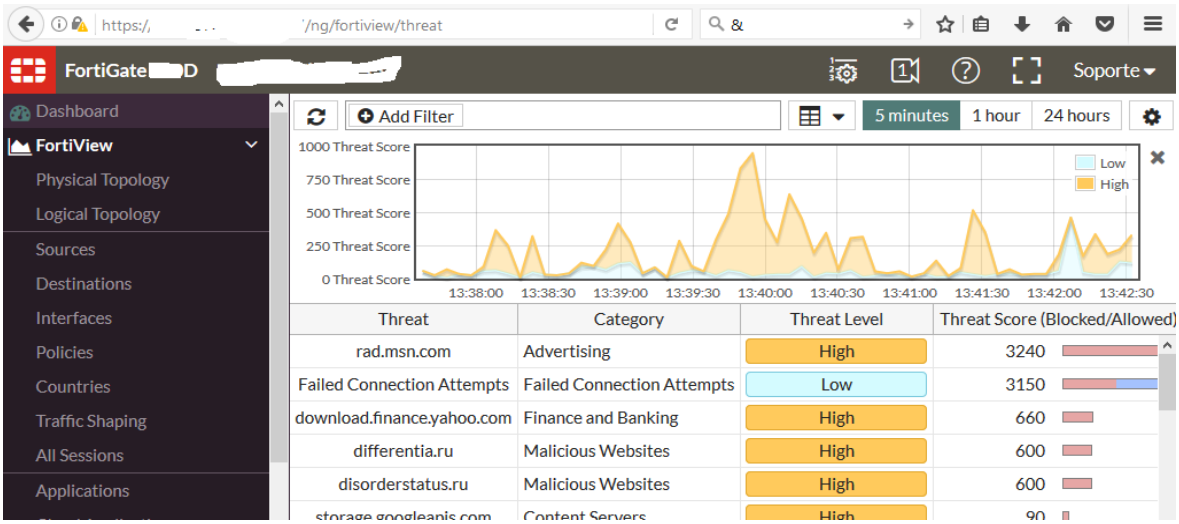

***"Imagen 11. Políticas de tráfico aplicadas a los objetos."***



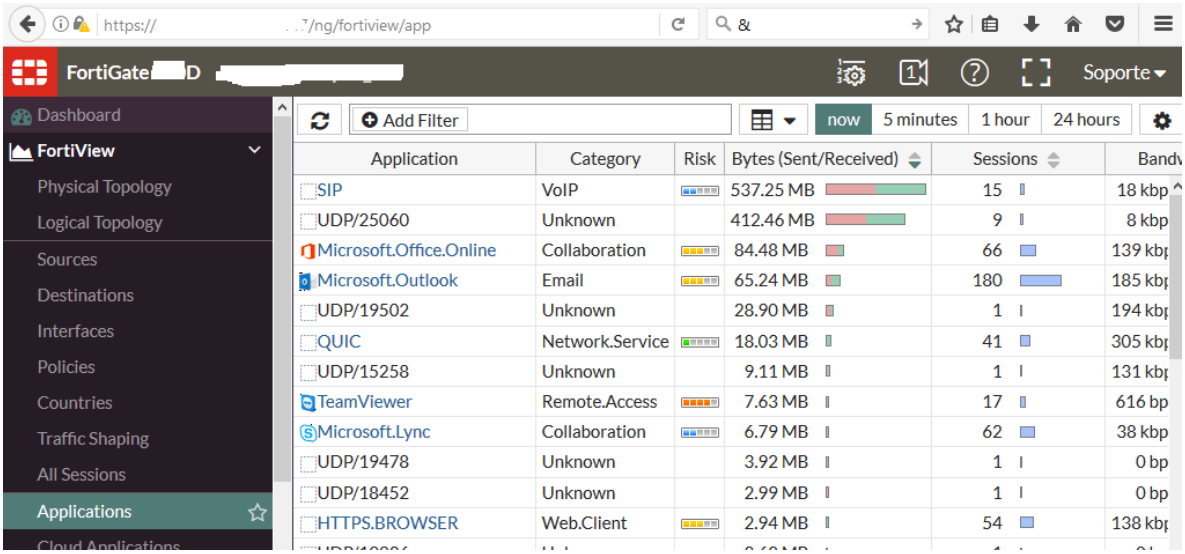

***"Imagen 12. Límites de tráfico para su uso en políticas."***



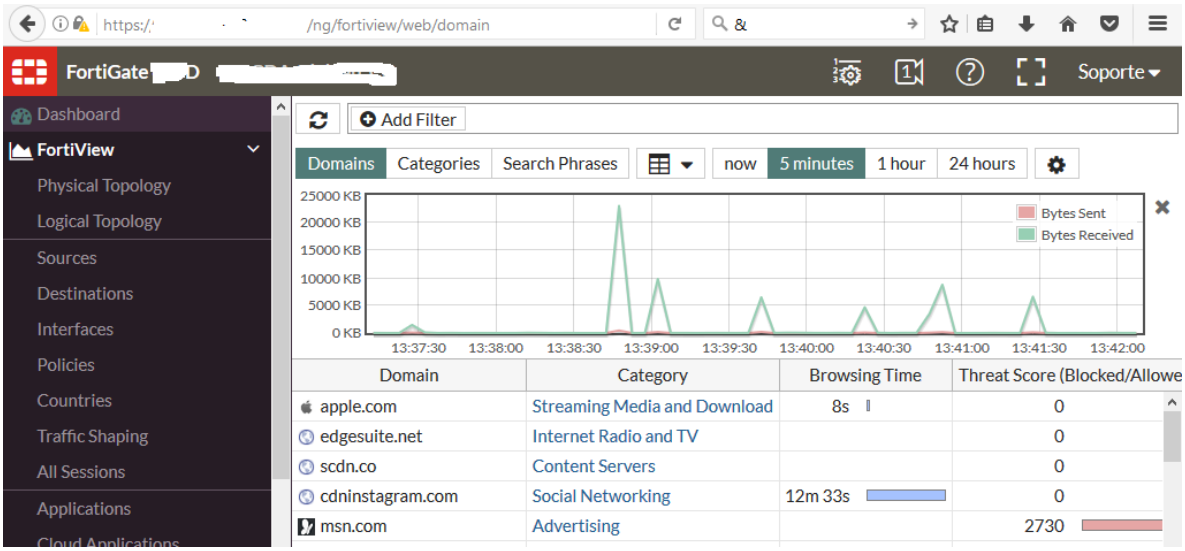

***"Imagen 13. Registro de conexiones internas y externas de los equipos de la red."***



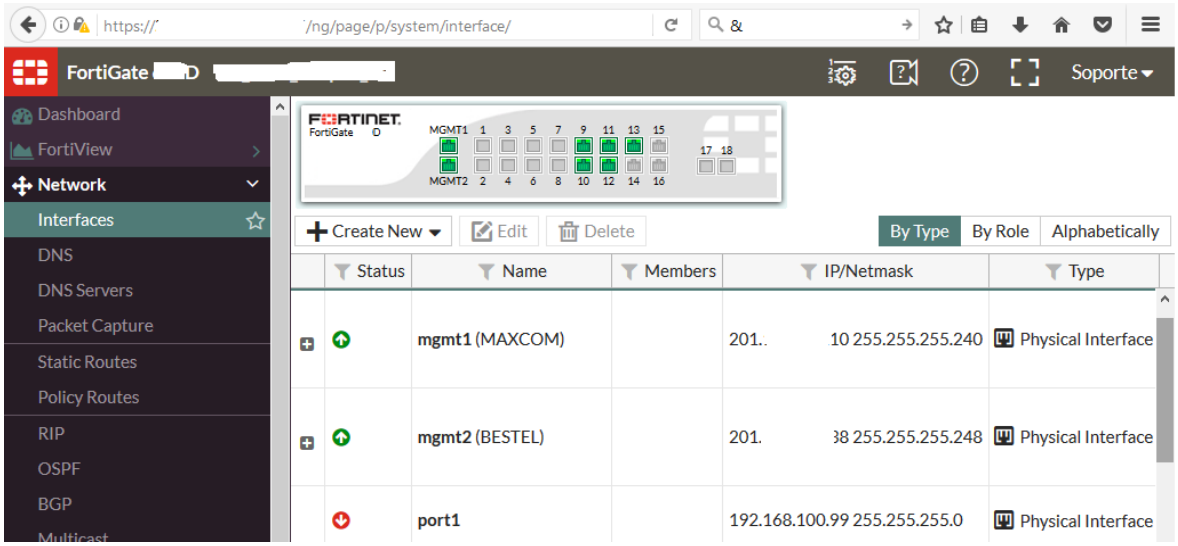

***"Imagen 14. Amenazas detectadas categorizadas."***



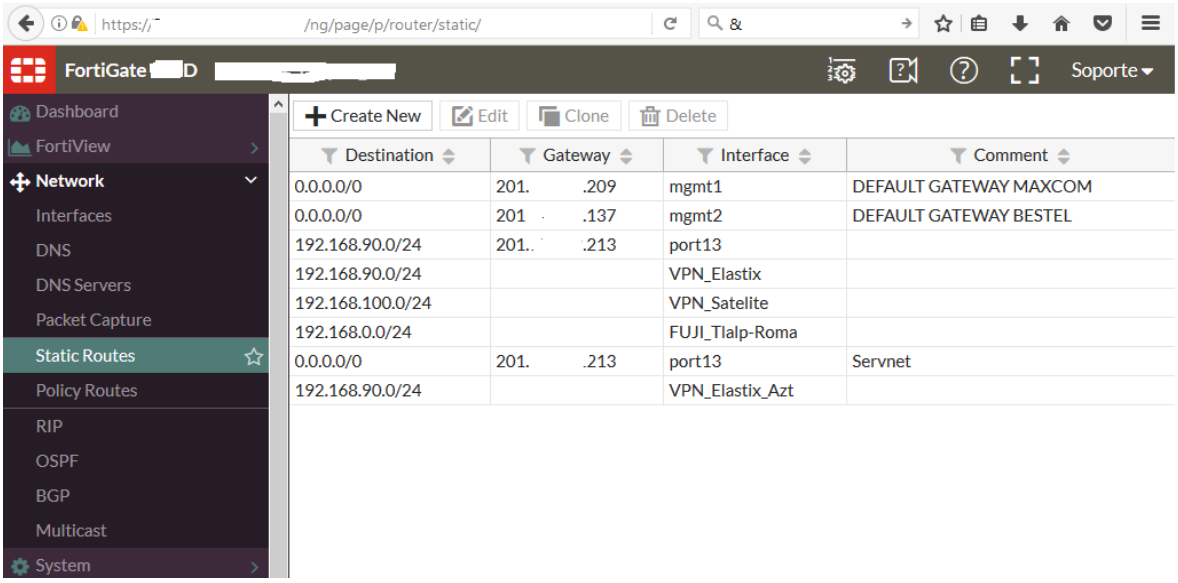

*"Imagen 15. Control de aplicaciones para perfiles de seguridad."*



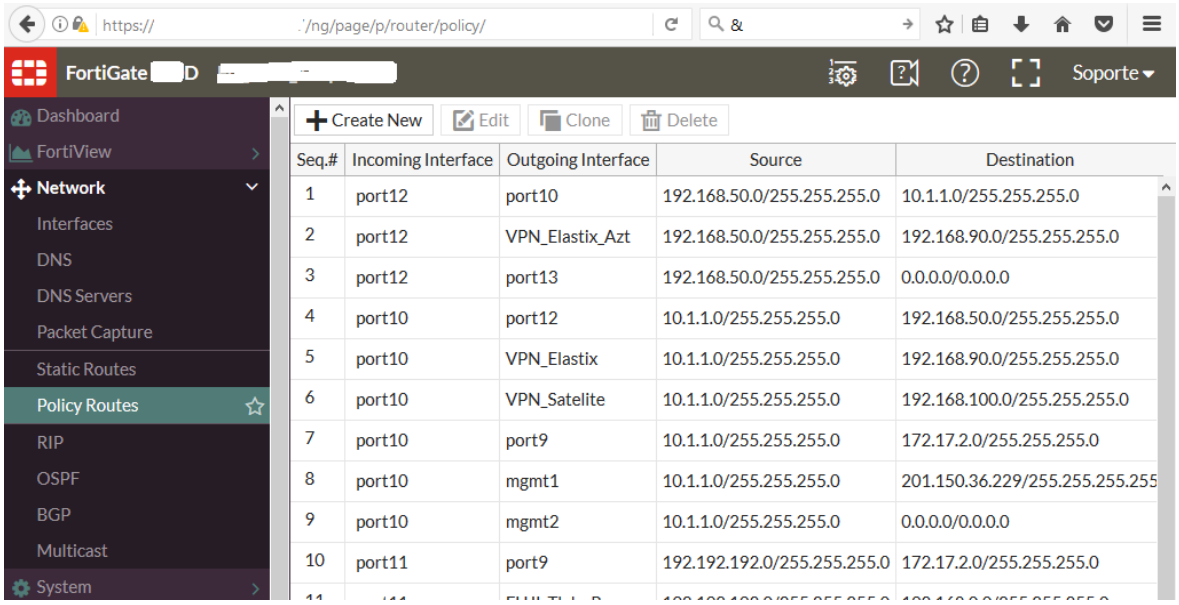

*"Imagen 16. Registro de conexiones web externas."*



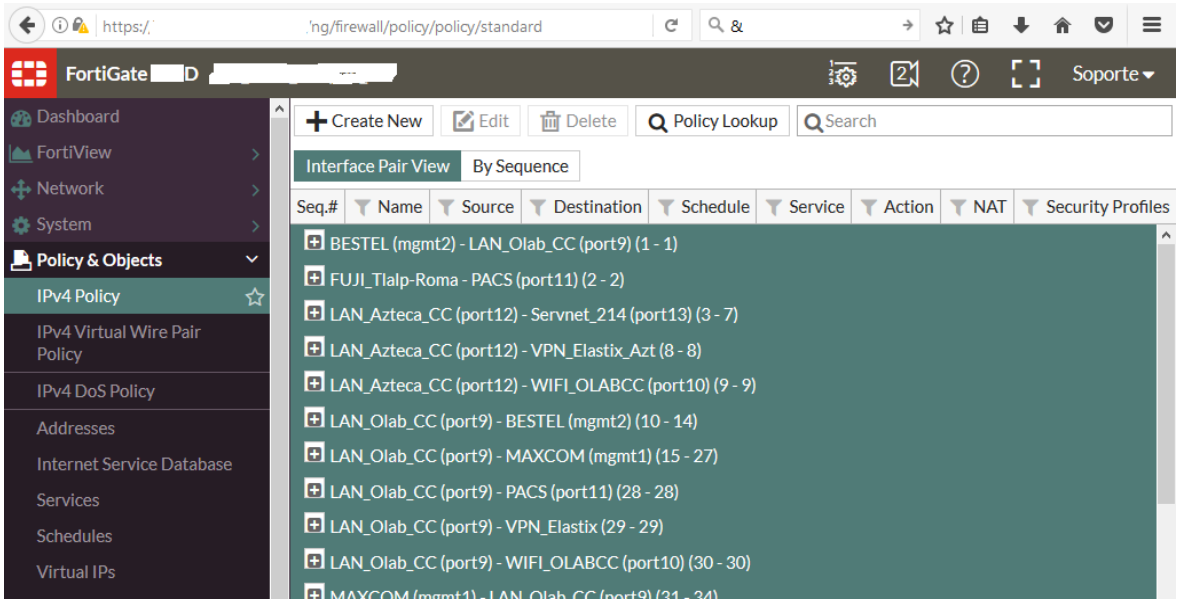

*"Imagen 17. Configuración de las interfaces físicas."*



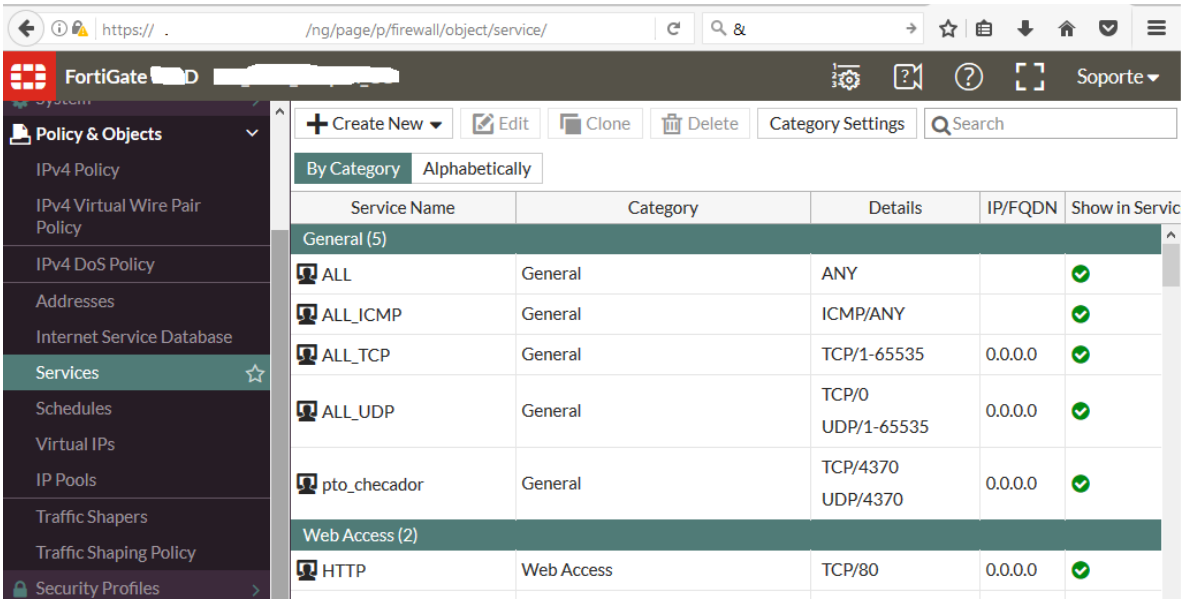

*"Imagen 18. Ruteo de la VPN."*



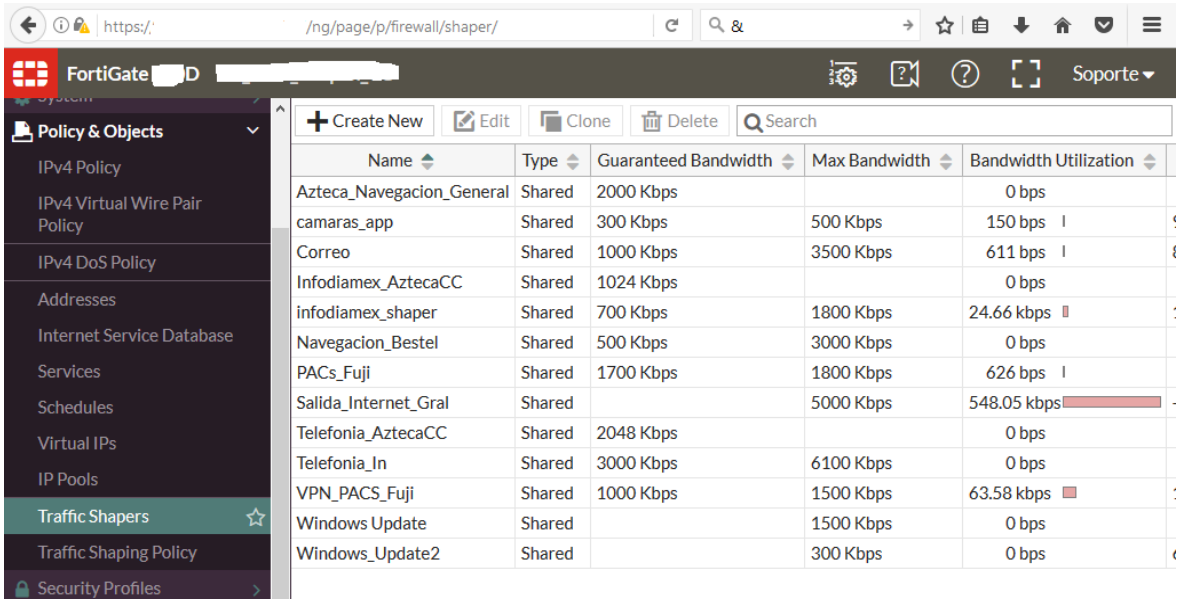

***"Imagen 19. Creación de políticas de ruteo."***



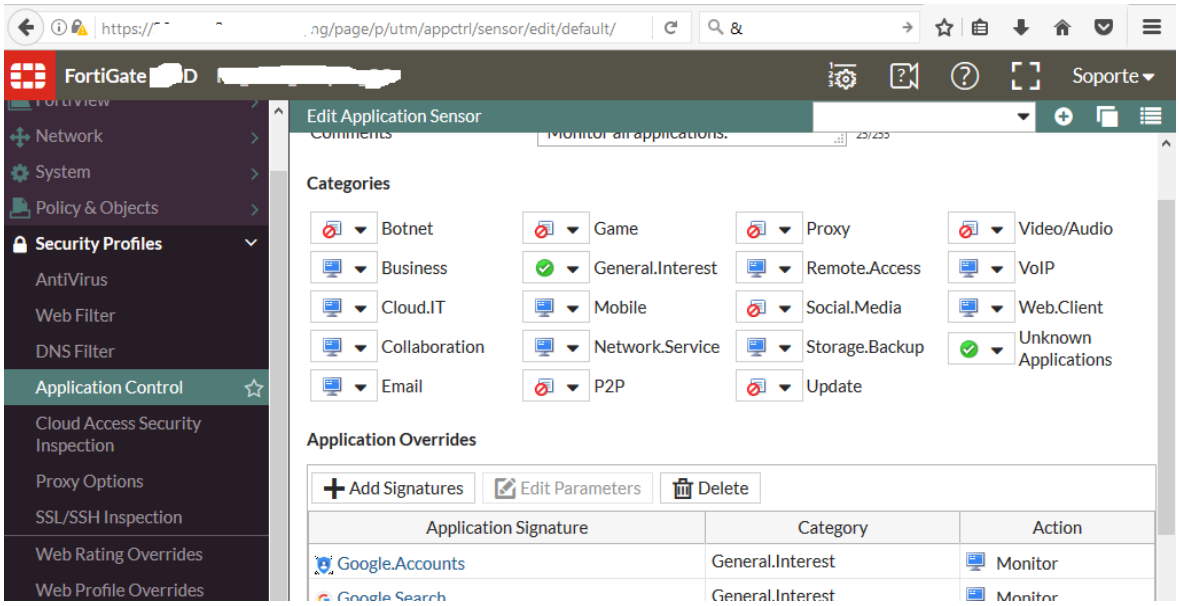

***"Imagen 20. Políticas de ruteo por segmento de red."***



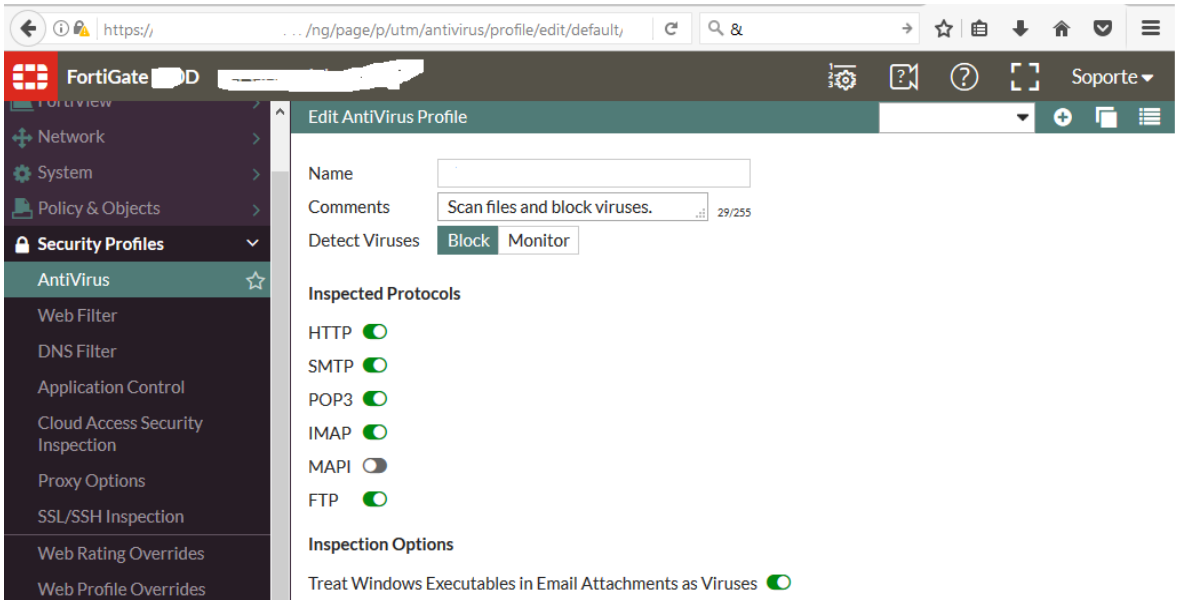

*"Imagen 21. Servicios y protocolos permitidos."*



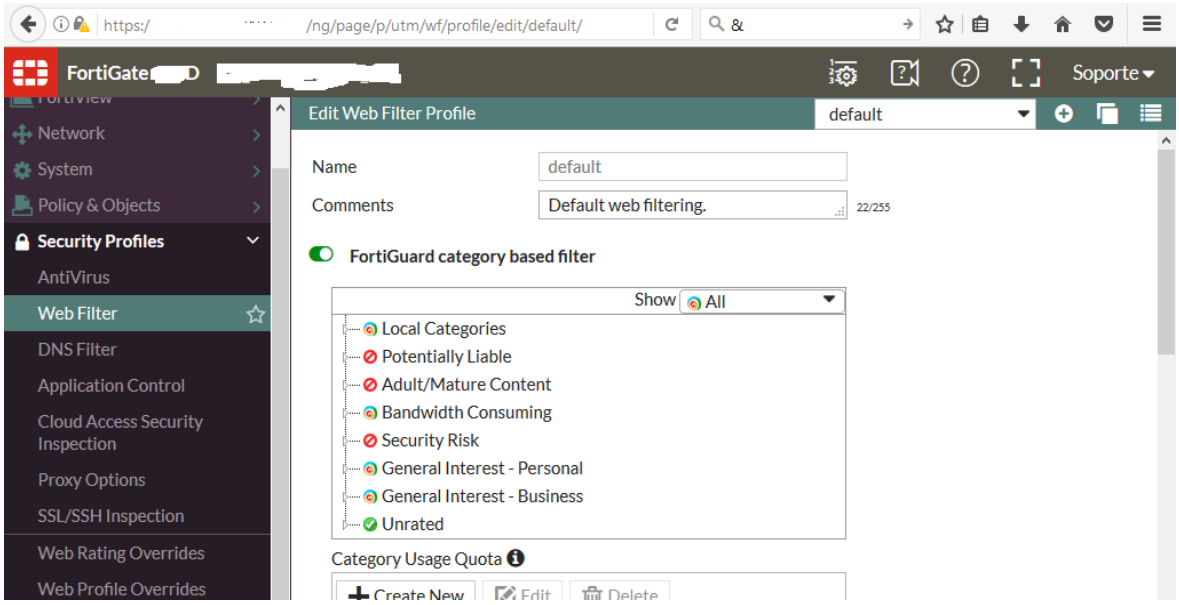

*"Imagen 22. Creación de límites de tráfico."*



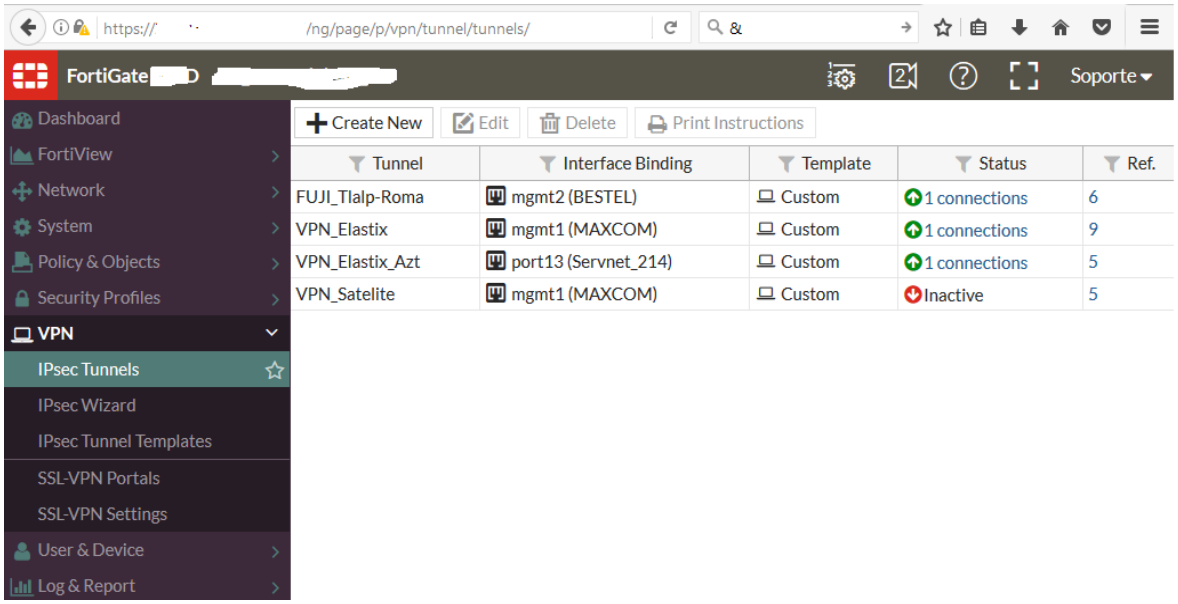

*"Imagen 23. Creación de perfiles para el control de aplicaciones."*



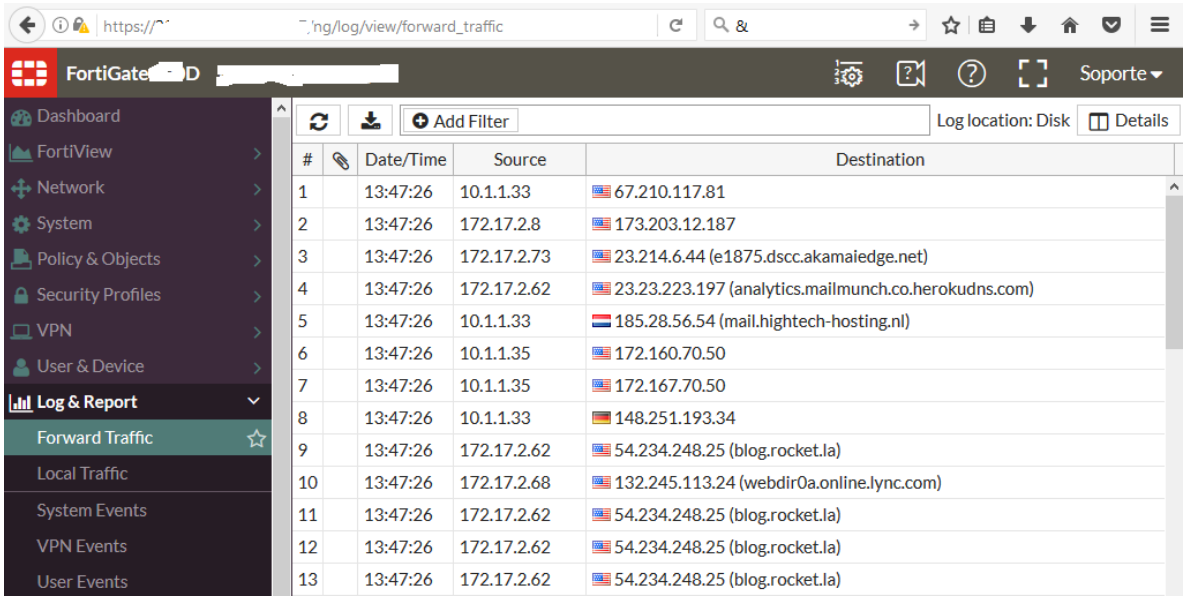

*"Imagen 24. Creación de perfiles de Antivirus."*



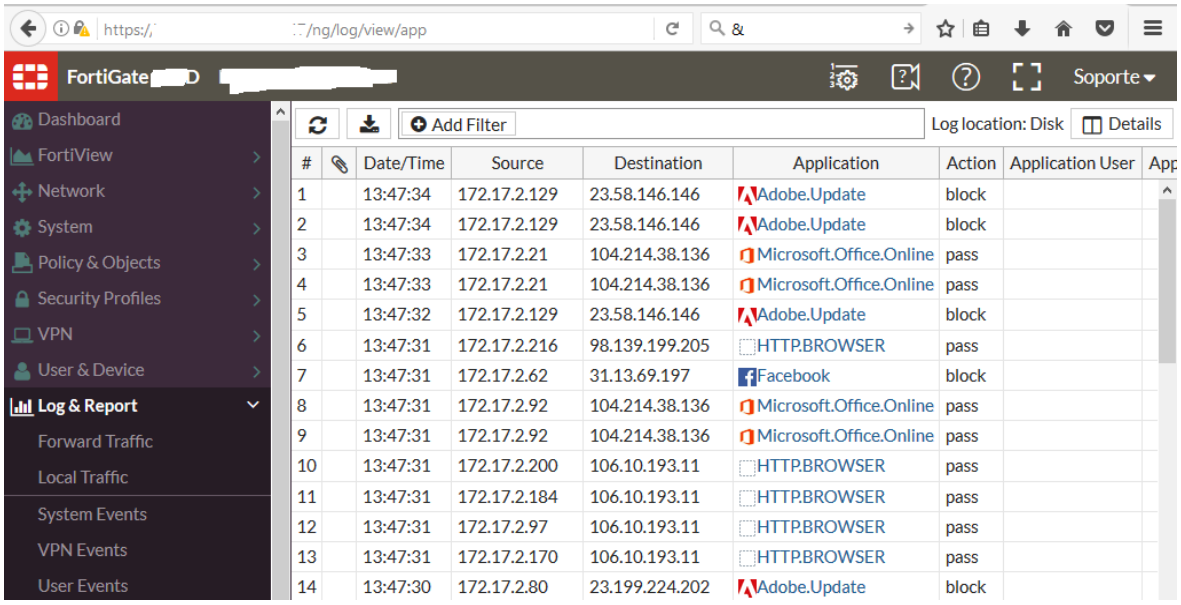

*"Imagen 25. Creación de perfiles del Filtrado Web."*



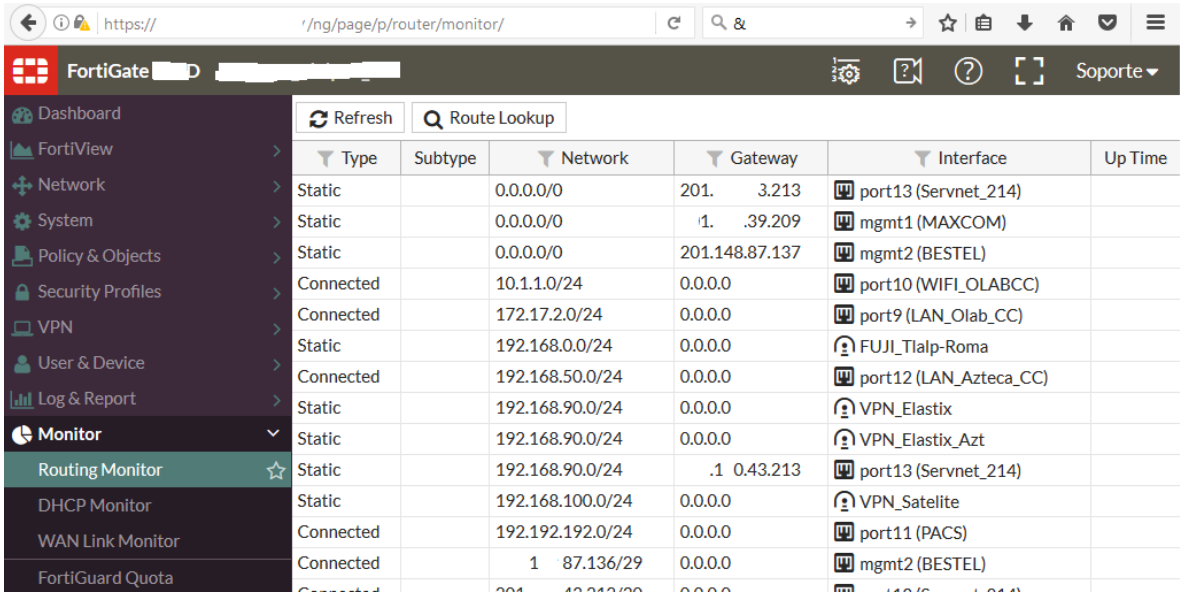

*"Imagen 26. Configuración de túneles para conexión de la VPN."*



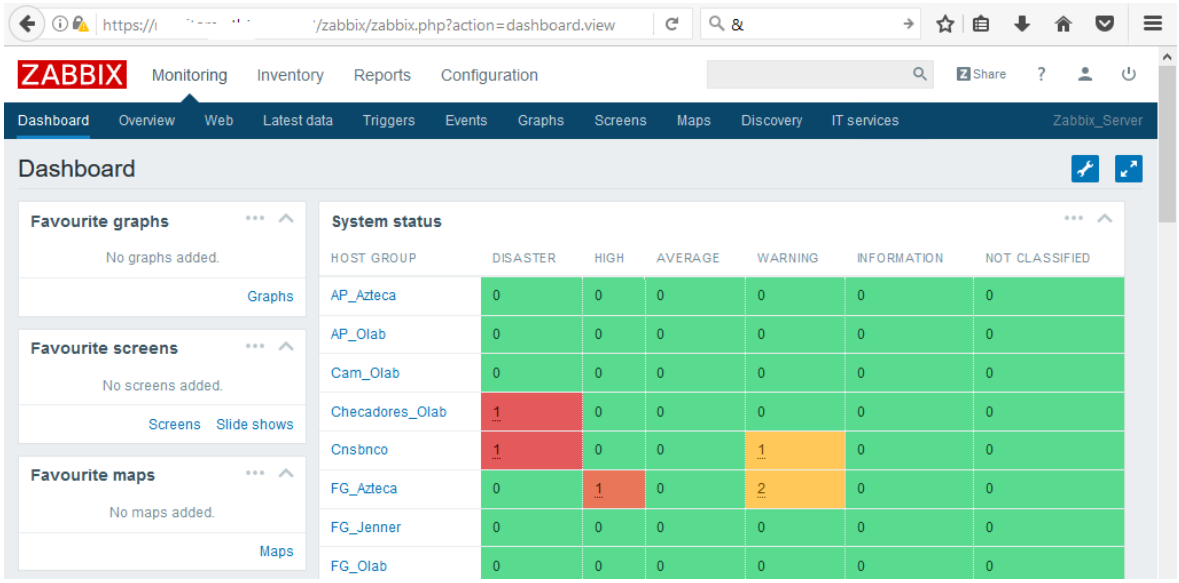

*"Imagen 27. Registro del tráfico externo."*



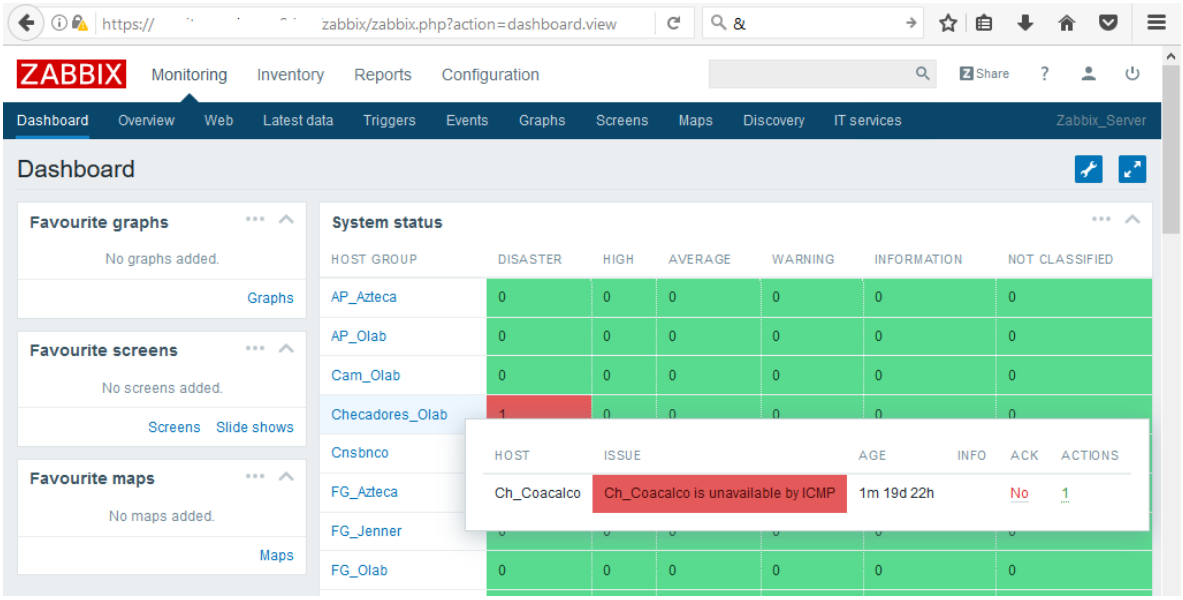

*"Imagen 28. Registro de aplicaciones en uso."*



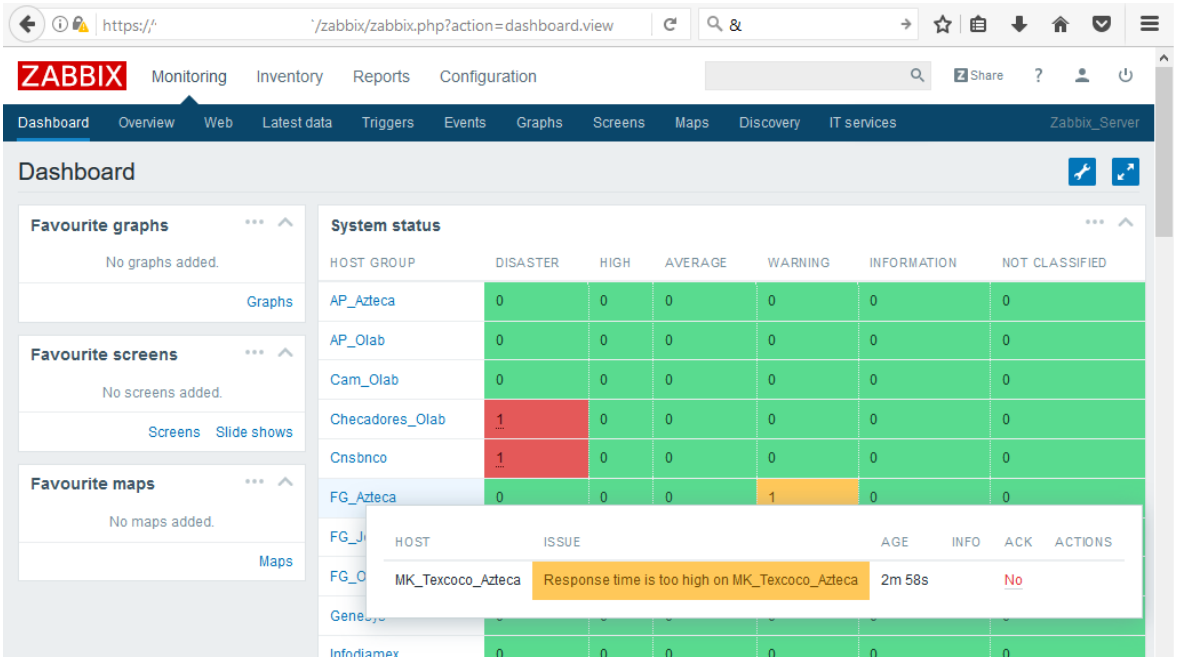

*"Imagen 29. Monitoreo general de conexiones."*



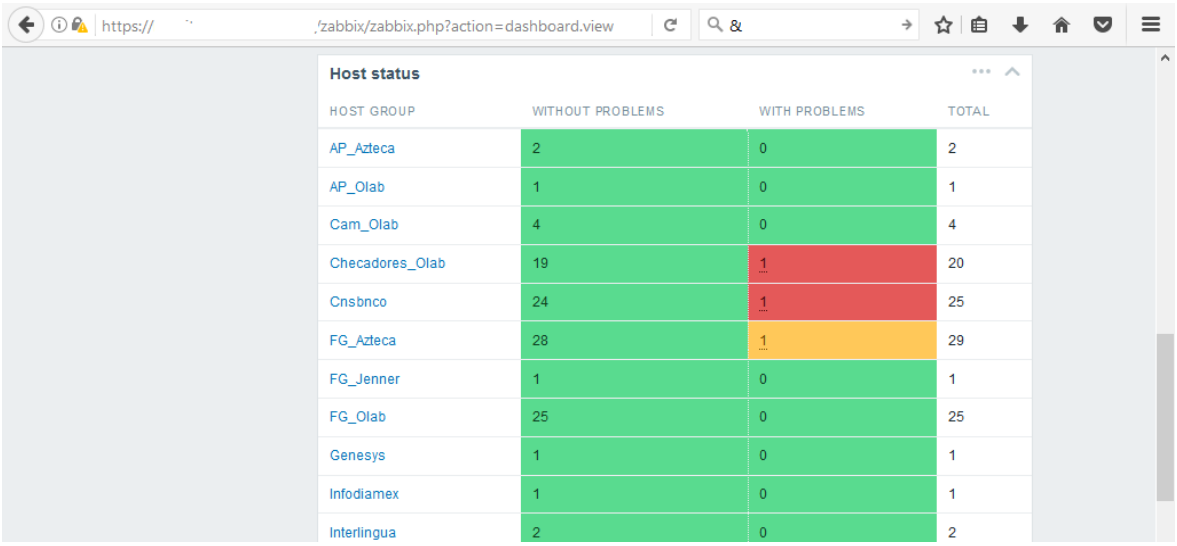

*"Imagen 30. Estado de los equipos desde el monitor de comportamiento."*



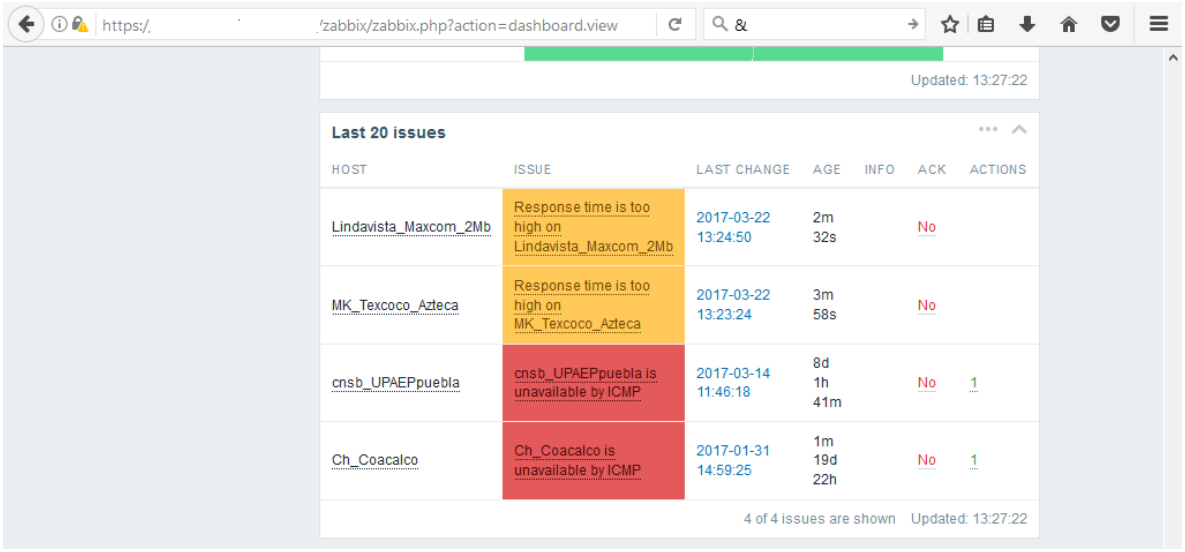

*"Imagen 31. Alerta de seguridad alta."*



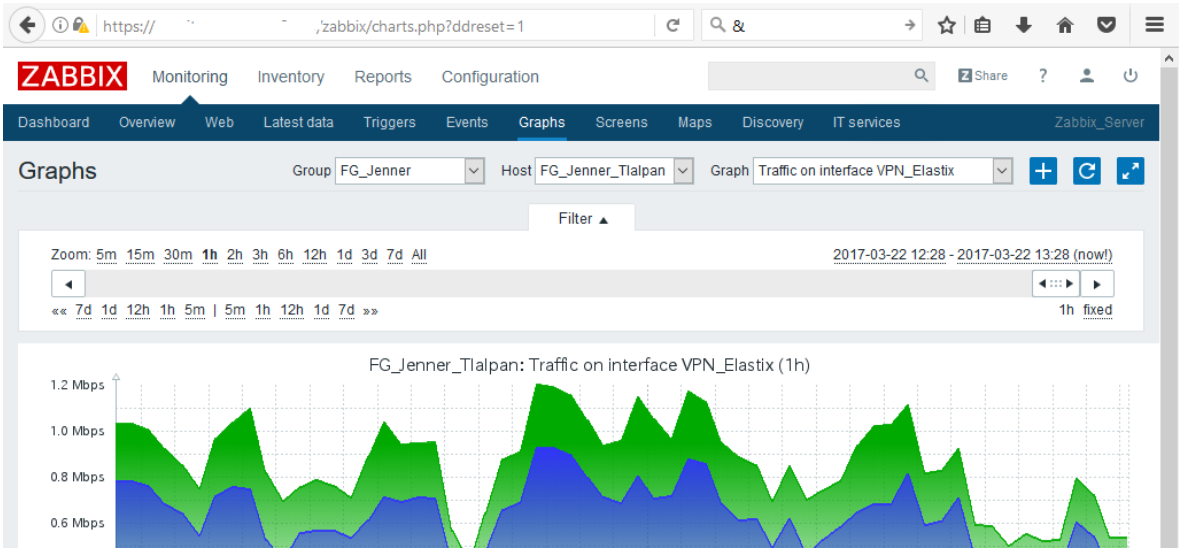

*"Imagen 32. Alerta de seguridad media."*



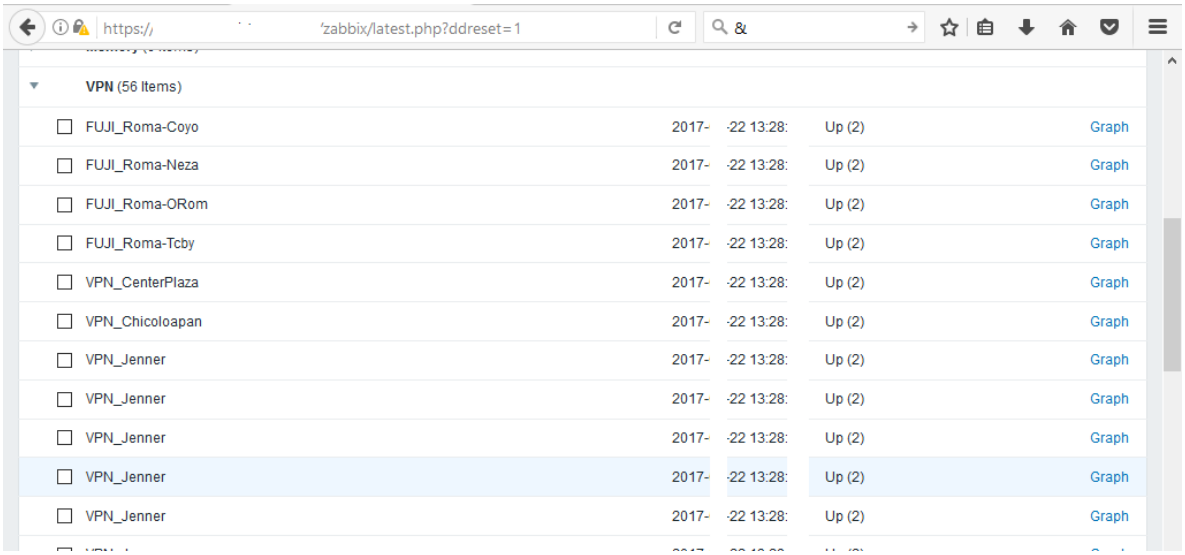

*"Imagen 33. Concentrado de alertas en equipos."*




*"Imagen 34. Detalle de las alertas en equipos."*




***"Imagen 35. Comportamiento del tráfico por hora."***




***"Imagen 36. Registro del comportamiento de las conexiones en equipos."***

**Enlaces de CookBook y HandBook de equipo Fortinet**

http://docs.fortinet.com/d/fortigate-fortios-handbook-online-version-the-complete-guide-to-fortios-5.4

http://docs.fortinet.com/d/fortigate-the-fortigate-cookbook-5.4

**Documentación del software libre utilizado.**

https://www.zabbix.com/documentation

https://nmap.org/docs.html

## 11 Referencias bibliográficas


[1] M. Azamar Ramos, “Sistema de Filtrado para redes de computadoras con herramientas Gráficas en Linux,” proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Azcapotzalco, México, 2010.

[2] J. A. Castillo Cabrera, “Diseño e implantación de una LAN virtual con switches de red,” proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Azcapotzalco, México, 2010.

[3] A. Browder Serrano, “El problema de agotamiento de las direcciones lógicas y un método para su resolución en IPv.4,” proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Azcapotzalco, México, 2012.

[4] E. Hernández Orallo, “Seguridad y privacidad en los sistemas informáticos”, 2004

[5] Adaptive Security Appliance (ASA) Software, Cisco Systems.

[6] Endpoint Security, Check Point Software Technologies Ltd.