**Universidad Autónoma Metropolitana**
**Unidad Azcapotzalco**
**División de Ciencias Básicas e Ingeniería**
**Licenciatura en Ingeniería en Computación**

# REPORTE FINAL

Modalidad: Estancia Profesional en T&B TALENT

Nombre del proyecto: Configuración e implementación de políticas de seguridad para la protección de una red corporativa

Nombre del alumno: Miguel Angel Ruiz Mompala

Matrícula: 209205007

Nombre de los asesores:
Asesor Interno: M. en C. José Alfredo Estrada Soto
Asesor Externo: Ing. Mario Ernesto Gómez Romero

Trimestre 2014 Otoño

28 de Noviembre de 2014

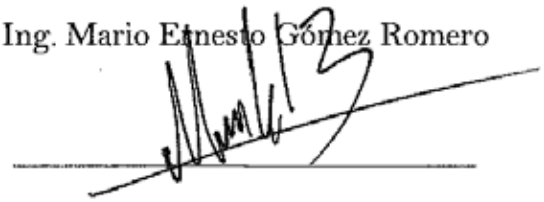
# Declaratoria

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.

M. en C. José Alfredo Estrada Soto

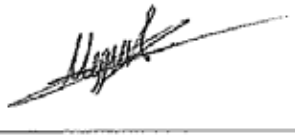
Yo, Mario Ernesto Gómez Romero, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

Ing. Mario Ernesto Gómez Romero



Yo, Miguel Angel Ruiz Mompala, 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.

Miguel Angel Ruiz Mompala



# Resumen

Se describe y elabora un **Reporte de Proyecto de Integración I** en **Ingeniería en Computación**, el cual contiene todo lo descrito en la propuesta antes entregada al comité de estudios correspondiente de la **Universidad Autónoma Metropolitana Unidad Azcapotzalco**, cuya modalidad de estancia profesional realizada en la empresa **T & B TALENT S.A. de C.V.**, se asignó el proyecto de configurar e implementar políticas de seguridad para la protección de la red corporativa de la empresa **ORIÓN INTEGRACIÓN, DESARROLLO Y TALENTO S.A. de C.V.**, empresa dedicada a la contratación de personal en la industria aeronáutica.

El proyecto de configurar e implementar políticas de seguridad en una red corporativa nace de la idea de tener bajo control la información, esa información es de vital importancia para la empresa, de tal forma que los datos no sean alterados, modificados o robados, y que la empresa pueda poner bajo resguardo tanto a los usuarios como sus datos.

Cabe mencionar que el control de la información se hace dentro de la organización con fines de resguardar toda la información que fluye por la red corporativa. Estas políticas de seguridad se implementan a partir de un estudio exhaustivo en las vulnerabilidades de la red corporativa, las vulnerabilidades pueden ser atacadas y amenazas por distintos tipos.

Las industrias necesitan soluciones de seguridad que brinden confiabilidad tanto en los datos como en la calidad del flujo de estos. Para ofrecer una red segura es necesaria una protección contra ataques y amenazas que garanticen condiciones de alta disponibilidad, tiempo de respuesta apropiado, fiabilidad, integridad y adaptación.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios.

La seguridad ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas. En este sentido, las políticas de seguridad surgen como una herramienta para concientizar a cada uno de los usuarios de la organización sobre la importancia y la sensibilidad de la información.

Las organizaciones modernas suelen estar dispersas geográficamente, y sus oficinas están situadas en dispersos puntos de un país e incluso en diferentes lugares del mundo. En este trabajo no solo se implementan y configuran políticas de seguridad para satisfacer la necesidad de proteger los recursos y la información de dicha empresa, también se intenta concientizar a las empresas y organizaciones para que realicen trabajos de protección y aseguramiento de la información.

# Tabla de contenido

# Índice de figuras

# Índice de diagramas



# Índice de tablas



# Índice de fotografías



# Introducción

En la actualidad el crecimiento de las redes y la cantidad de información disponible en estás ha llegado a ser casi ilimitada, los usuarios de las redes van ganando cada vez más experiencia, encontrando con mayor facilidad información. Esto da como resultado que las redes se vean vulnerables a ataques y robos de información y tengan una debilitación inminente volviéndose cada vez más inseguras**.** Se dice **insegura** a una red en la cual la privacidad de los datos se encuentra en riesgo de ser interceptados, alterados o robados, así como propensos a transmitir información que dañe la red misma, no brindando tranquilidad de un funcionamiento constante y óptimo.

Las industrias necesitan soluciones de seguridad que brinden confiabilidad tanto en los datos como en la calidad del flujo de estos. Para ofrecer una red segura es necesaria una protección contra ataques malintencionados o imprevistos, y garantizar condiciones de alta disponibilidad, tiempo de respuesta apropiado, fiabilidad, integridad y adaptación.

Esta **seguridad** no es más que tomar medidas preventivas e implementar políticas de seguridad que puedan evitar en su mayor totalidad la intromisión de terceros no autorizados.

La **red corporativa** tiene como objetivo la compartición de recursos, hacer que todos los programas, el equipo y, en particular, los datos estén disponibles para todos los **usuarios autorizados** de tal red.

Este trabajo que aquí se presenta está enfocado hacia la seguridad de redes corporativas, donde la empresa en donde se realizó esta seguridad, puede confiar que su información valiosa está protegida ante amenazas del exterior.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

## Antecedentes

En los últimos tres siglos la tecnología ha dominado: El siglo XVIII fue la era de los grandes sistemas mecánicos que acompañaron la Revolución Industrial. El siglo XIX fue la edad de las maquinas de vapor. Durante el siglo XX la tecnología clave es la obtención, el procesamiento y la distribución de la información [1].

Durante las primeras décadas de su existencia, las redes de computadoras fueron usadas principalmente por investigadores universitarios para el envió de correo electrónico, y por empleados corporativos para compartir impresoras. En estas condiciones, la seguridad no recibió mucha atención. Pero ahora, cuando millones de ciudadanos comunes usan redes para sus transacciones bancarias, compras y declaraciones de impuestos, la seguridad de las redes aparece en el horizonte como un problema potencial de grandes proporciones.

Con el paso de los años se han ido desarrollando nuevos ataques cada vez más sofisticados para explorar vulnerabilidades tanto para el diseño de redes TCP/IP como en la configuración y operación de los sistemas informáticos que conforman las redes conectadas a Internet. Estos nuevos métodos de ataque se han ido automatizando, por lo que en muchos casos sólo se necesita un conocimiento técnico muy básico para realizarlos. Cualquier usuario con una conexión a Internet tiene acceso hoy en día a numerosas aplicaciones para realizar estos ataques y las instrucciones necesarias para ejecutarlos.

En la mayor parte de la bibliografía relacionada con la seguridad en redes informáticas podemos encontrar clasificadas las tres generaciones de ataques siguientes:

**Primera generación: ataques físicos.** Encontramos aquí ataques que se centran en componentes electrónicos, como podrían ser los propios ordenadores, los cables o los dispositivos de red. Actualmente se conocen soluciones para estos ataques, utilizando protocolos distribuidos y de redundancia para conseguir una tolerancia a fallos aceptable.

**Segunda generación: ataques sintácticos.** Se trata de ataques contra la lógica operativa de los ordenadores y las redes, que quieren explotar vulnerabilidades existentes en el software, algoritmos de cifrado y en protocolos. Aunque no existen soluciones globales para contrarrestar de forma eficiente estos ataques, podemos encontrar soluciones cada vez más eficaces.

**Tercera generación: ataques semánticos.** Finalmente, podemos hablar de aquellos ataques que se aprovechan de la confianza de los usuarios en la información. Este tipo de ataques pueden ir desde la colocación de información falsa en boletines informativos y correos electrónicos hasta la modificación del contenido de los datos en servicios de confianza, como, por ejemplo, la manipulación de bases de datos con información pública, sistemas de información bursátil, sistemas de control de tráfico aéreo, etc.

Las amenazas contra la seguridad basadas en la red han provocado robos de identidad y fraude financiero generalizados. El correo no deseado, los virus[1] y el spyware[2] causan graves problemas a empresas y consumidores.

Una infracción de seguridad puede causar un daño irreparable a la reputación o la imagen de una compañía. Los ataques actuales contra la información son un negocio rentable y a menudo están controlados por los sindicatos del crimen organizado.

---

[1] Es un programa informático que se ejecuta en el ordenador sin previo aviso y que puede corromper el resto de los programas, ficheros de datos e, incluso el mismo sistema operativo. Afortunadamente, los virus no provocan daños en el hardware del ordenador. Sin embargo pueden borrar los datos del disco duro. Éste podrá volver a utilizarse, una vez eliminado el virus del ordenador.

[2] Son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos.

Un creciente número de sofisticados modelos comerciales de ciberdelincuencia, incluido el auge de empresas delictivas, se basa en la venta de herramientas y servicios para lanzar ataques contra la red, más que en la venta de la información obtenida con los ataques.

La tecnología de seguridad en Internet sigue progresando, y está pasando de tener un enfoque pasivo y puntual basado en productos, a tener planteamientos activos de punta a punta basados en reconocimiento, contención y cuarentena. Además, los proveedores de servicios de Internet (ISP) están compitiendo en seguridad y los ISP dirigidos al consumidor ofrecen seguridad de Internet dentro de su paquete de servicios.

Los legisladores de todo el mundo están centrados en el estado de la infraestructura de la información. Los legisladores quieren asegurarse de que los usuarios de las redes emplean la mejor tecnología y prácticas de procesos para hacer que sus redes sean lo más seguras posibles. Los gobiernos y las empresas actualizan de forma continua sus estrategias de prevención de ataques, y se han formado asociaciones entre órganos públicos y privados con el fin de desarrollar planteamientos de seguridad voluntarios basados en el mercado.

## Justificación

El efectuar este proyecto ayudará a mantener bajo protección los recursos y la información con que se cuenta en la red corporativa a través de procedimientos basados en políticas de seguridad, así como fomentar un mejor planteamiento de la red corporativa para resolver problemas que tengan que ver con la comunicación.

En la actualidad las redes de comunicación juegan un papel preponderante en casi todos los sistemas productivos de la sociedad, especialmente en aquellos que demandan una gran eficiencia en el almacenamiento, transmisión y sobre todo el acceso seguro de la información. Las empresas necesitan intercambiar información y datos, a menudo a diario. Es por eso que las redes corporativas proporcionan la posibilidad de que computadoras o algún otro dispositivo electrónico pueda intercambiar datos, hacer accesibles los programas y los datos a todo el personal autorizado de la empresa.

La complejidad derivará del desafío de resolver problemas en el sitio y en tiempo real al pretender administras un conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información. La seguridad ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización.

Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas, en este sentido, las políticas de seguridad surgen como una herramienta para concientizar a cada uno de los usuarios de la organización sobre la importancia y la sensibilidad de la información. Las organizaciones modernas suelen estar dispersas geográficamente, y sus oficinas están situadas en dispersos puntos de un país e incluso en diferentes lugares del mundo.

## Objetivos

*OBJETIVO GENERAL*

- Configurar e implementar políticas de seguridad para la protección de recursos e información de la red corporativa.

*OBJETIVOS PARTICULARES*

- Analizar e identificar vulnerabilidades que existan en la red corporativa.
- Diseñar a partir de políticas de seguridad un plan de protección para la red corporativa sus recursos e información.
- Implementar y configurar la red corporativa bajo el plan de protección.
- Realizar pruebas de conectividad y visualizar la seguridad en la red.
- Controlar el acceso a las personas y a los dispositivos autorizados.
- Verificar la identidad de las personas y los dispositivos autorizados.
- Crear un registro de las personas y los dispositivos autorizados.

## Marco teórico

Antes de comenzar a desarrollar y configurar políticas de seguridad es necesario conocer algunos conceptos que nos ayudan a comprender más las necesidades que tienen las empresas u organizaciones.

El término **«seguridad»** se utiliza en el sentido de minimizar las vulnerabilidades de los bienes y recursos. Un ***«bien»*** es todo elemento de valor. Una **«vulnerabilidad»** es toda debilidad que pudiera explotarse para violar un sistema o las informaciones que éste contiene. Una ***«amenaza»*** es una violación potencial de la seguridad. Conociendo estos conceptos podremos darnos cuenta de lo importante que es la seguridad y lo que implicará implementar políticas de seguridad para la empresa, nos da una idea más clara de lo que queremos hacer.

Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red corporativa, a través de procedimientos basados en políticas de seguridad, tales que permitan un control adecuado.

Existen recursos que son fundamentales para la empresa, pero los que se muestran a continuación son de vital importancia, ya que sin estos el funcionamiento de la empresa no sería el mismo. Es por eso que estos recursos tienen mayor importancia y son los que vamos a proteger.

**¿Qué elementos queremos proteger?**

Los tres principales elementos a proteger son los detallados a continuación en la tabla 1.1.

| Elemento | Descripción |
|---|---|
| Hardware | Conjunto formado por todos los elementos físicos de un sistema informático o de red. |
| Software | Conjunto de programas lógicos que hacen funcional al hardware, tanto sistemas operativos como aplicaciones. |
| Datos | Conjunto de información lógica que manejan el software y el hardware. |

**Tabla 1.1. Elementos a proteger.**

En este reporte se presenta la problemática de la seguridad en las redes de computadores y, más concretamente, en las redes TCP[3]/IP[4]. La estructuración sigue el siguiente modelo. La familia de protocolos TCP/IP se divide en las cuatro capas siguientes:

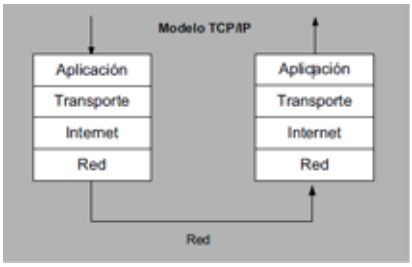



**Figura 1.1. Modelo TCP/IP.**

[3] En inglés, Transmission Control Protocol.
[4] En inglés, Internet Protocol.

**Capa de red.** Normalmente está formada por una red LAN[5] o WAN[6] (de conexión punto a punto) homogénea. Todos los equipos conectados a Internet implementan esta capa.

**Capa de Internet** (o capa de Internetworking). Da unidad a todos los miembros de la red y, por lo tanto, es la capa que permite que todos se puedan interconectar, independientemente de si se conectan mediante línea telefónica o mediante una red local Ethernet. La dirección y el encaminamiento son sus principales funciones. Todos los equipos conectados a Internet implementan esta capa.

**Capa de transporte.** Da fiabilidad a la red. El control de flujo y de errores se lleva a cabo principalmente dentro esta capa, que sólo es implementada por equipos usuarios de Internet o por terminales de Internet. Los dispositivos de encaminamiento[7] (encaminadores) no la necesitan.

**Capa de aplicación.** Engloba todo lo que hay por encima de la capa de transporte. Es la capa en la que encontramos las aplicaciones que utilizan Internet: clientes y servidores de Web, correo electrónico, FTP[8], etc. Sólo es implementada por los equipos usuarios de Internet o por terminales de Internet. Los dispositivos de encaminamiento no la utilizan.

En cada capa del modelo TCP/IP pueden existir distintas vulnerabilidades y un atacante puede explorar los protocolos asociados a cada una de ellas. Cada día se descubren nuevas deficiencias, la mayoría de las cuales se hacen públicas por organismos internacionales, tratando de documentar, si es posible, la forma de solucionar y contrarrestar los problemas.

A continuación presentamos algunas de las vulnerabilidades más comunes de las distintas capas:

**Vulnerabilidades de la capa de red.** Las vulnerabilidades de la capa de red están estrechamente ligadas al medio sobre el que se realiza la conexión. Esta capa presenta problemas de control de acceso y confidencialidad.

Son ejemplos de vulnerabilidades a este nivel los ataques a las líneas punto a punto: desvío de los cables de conexión hacia otros sistemas, interceptación intrusiva de las comunicaciones, escuchas no intrusivas en medios de transmisión sin cables, etc.

**Vulnerabilidades de la capa Internet.** En esta capa se puede realizar cualquier ataque que afecte un datagrama IP.

---

[5] En inglés, Local Area Network.
[6] En inglés, Wide Area Network.
[7] En inglés, routers.
[8] Nombre del protocolo estándar de transferencia de archivos (File Transfer Protocol).

Se incluyen como ataques contra esta capa las técnicas de sniffing[9], la suplantación de mensajes, la modificación de datos, los retrasos de mensajes y la denegación de mensajes. Cualquier atacante puede suplantar un paquete si indica que proviene de otro sistema. La suplantación de un mensaje se puede realizar, por ejemplo, dando una respuesta a otro mensaje antes de que lo haga el suplantado.

En esta capa, la autenticación de los paquetes se realiza a nivel de máquina (por dirección IP) y no a nivel de usuario. Si un sistema suministra una dirección de máquina errónea, el receptor no detectará la suplantación.
Para conseguir su objetivo, este tipo de ataques suele utilizar otras técnicas, como la predicción de números de secuencia TCP, el envenenamiento de tablas caché, etc. Por otro lado, los paquetes se pueden manipular si se modifican sus datos y se reconstruyen de forma adecuada los controles de las cabeceras. Si esto es posible, el receptor será incapaz de detectar el cambio.

**Vulnerabilidades de la capa de transporte.** La capa de transporte transmite información TCP o UDP[10] sobre datagramas IP. En esta capa podamos encontrar problemas de autenticación, de integridad y de confidencialidad. Algunos de los ataques más conocidos en esta capa son las denegaciones de servicio debidas a protocolos de transporte.

En cuanto a los mecanismos de seguridad incorporados en el diseño del protocolo de TCP (como las negociaciones involucradas en el establecimiento de una sesión TCP), existe una serie de ataques que aprovechan ciertas deficiencias en su diseño. Una de las vulnerabilidades más graves contra estos mecanismos de control puede comportar la posibilidad de interceptación de sesiones TCP establecidas, con el objetivo de secuestrarlas y dirigirlas a otros equipos con fines deshonestos.

Estos ataques de secuestro se aprovechan de la poca exigencia en el protocolo de intercambio de TCP respecto a la autenticación de los equipos involucrados en una sesión. Así, si un usuario hostil puede observar los intercambios de información utilizados durante el inicio de la sesión y es capaz de interceptar con éxito una conexión en marcha con todos los parámetros de autenticación configurados adecuadamente, podrá secuestrar la sesión.

**Vulnerabilidades de la capa de aplicación.** Como en el resto de niveles, la capa de aplicación presenta varias deficiencias de seguridad asociadas a sus protocolos. Debido al gran número de protocolos definidos en esta capa, la cantidad de deficiencias presentes también será superior al resto de capas.

[9] Técnica por la cual se puede "escuchar" todo lo que circula por una red.
[10] En inglés, User Datagram Protocol.

Algunos ejemplos de deficiencias de seguridad a este nivel podrían ser los siguientes:

- **Servicio de nombres de dominio.** Normalmente, cuando un sistema solicita conexión a un servicio, pide la dirección IP de un nombre de dominio y envía un paquete UDP a un servidor DNS[11]; entonces, éste responde con la dirección IP del dominio solicitado o una referencia que apunta a otro DNS que pueda suministrar la dirección IP solicitada.

  Un servidor DNS debe entregar la dirección IP correcta pero, además, también puede entregar un nombre de dominio dado una dirección IP u otro tipo de información. En el fondo, un servidor de DNS es una base de datos accesible desde Internet. Por lo tanto, un atacante puede modificar la información que suministra ésta base de datos o acceder a información sensible almacenada en la base de datos por error, pudiendo obtener información relativa a la topología de la red de una organización concreta (por ejemplo, la lista de los sistemas que tiene la organización).

- **Telnet.** Normalmente, el servicio Telnet autentica al usuario mediante la solicitud del identificador de usuario y su contraseña, que se transmiten en claro por la red.

  Así, al igual que el resto de servicios de Internet que no protegen los datos mediante mecanismos de protección, el protocolo de aplicación Telnet hace posible la captura de aplicación sensible mediante el uso de técnicas de sniffing. Actualmente existen otros protocolos a nivel de aplicación (como, por ejemplo, SSH[12]) para acceder a un servicio equivalente a Telnet pero de manera segura (mediante autenticación fuerte). Aun así, el hecho de cifrar el identificador del usuario y la contraseña no impide que un atacante que las conozca acceda al servicio.

- **File Transfer Protocol.** Al igual que Telnet, FTP es un protocolo que envía la información en claro (tanto por el canal de datos como por el canal de comandos). Así pues, al enviar el identificador de usuario y la contraseña en claro por una red potencialmente hostil, presenta las mismas deficiencias de seguridad que veíamos anteriormente con el protocolo Telnet.

[11] En inglés, Domain Name System.
12 En inglés, Secure SHell.

Aparte de pensar en mecanismos de protección de información para solucionar el problema, FTP permite la conexión anónima a una zona restringida en la cual sólo se permite la descarga de archivos.
De este modo, se restringen considerablemente los posibles problemas de seguridad relacionados con la captura de contraseñas, sin limitar una de las funcionalidades más interesantes del servicio.

- **Hypertext Transfer Protocol.** El protocolo HTTP es el responsable del servicio World Wide Web. Una de sus vulnerabilidades más conocidas procede de la posibilidad de entrega de información por parte de los usuarios del servicio. Esta entrega de información desde el cliente de HTTP es posible mediante la ejecución remota de código en la parte del servidor.

  La ejecución de este código por parte del servidor suele utilizarse para dar el formato adecuado tanto a la información entregada por el usuario como a los resultados devueltos (para que el navegador del cliente la pueda visualizar correctamente). Si este código que se ejecuta presenta deficiencias de programación, la seguridad del equipo en el que esté funcionando el servidor se podrá poner en peligro.

# Desarrollo del proyecto

La realización de estas políticas de seguridad se llevaron a cabo en la empresa **ORIÓN INTEGRACIÓN, DESARROLLO Y TALENTO S.A. de C.V.,** empresa dedicada al reclutamiento, selección y contratación de personal básicamente en la industria de la aviación.

El proyecto de realizar la configuración e implementación de políticas de seguridad para la protección de una red corporativa, fue asignado por la empresa **T & B TALENT S.A. de C.V.,** conocida comercialmente como **"TBT"**, que es una empresa 100% mexicana, con más de 10 años de experiencia que ofrece estos servicios de seguridad, donde se configurarán e implementarán dichas políticas de seguridad. Las políticas de seguridad que se describen posteriormente se basaron en el estándar X.805 de la Unión Internacional de Telecomunicaciones (ITU) que integra las condiciones de gestión, control y utilización de la infraestructura, los servicios y las aplicaciones de red.

**Conocer y diseñar el diagrama de la red corporativa**

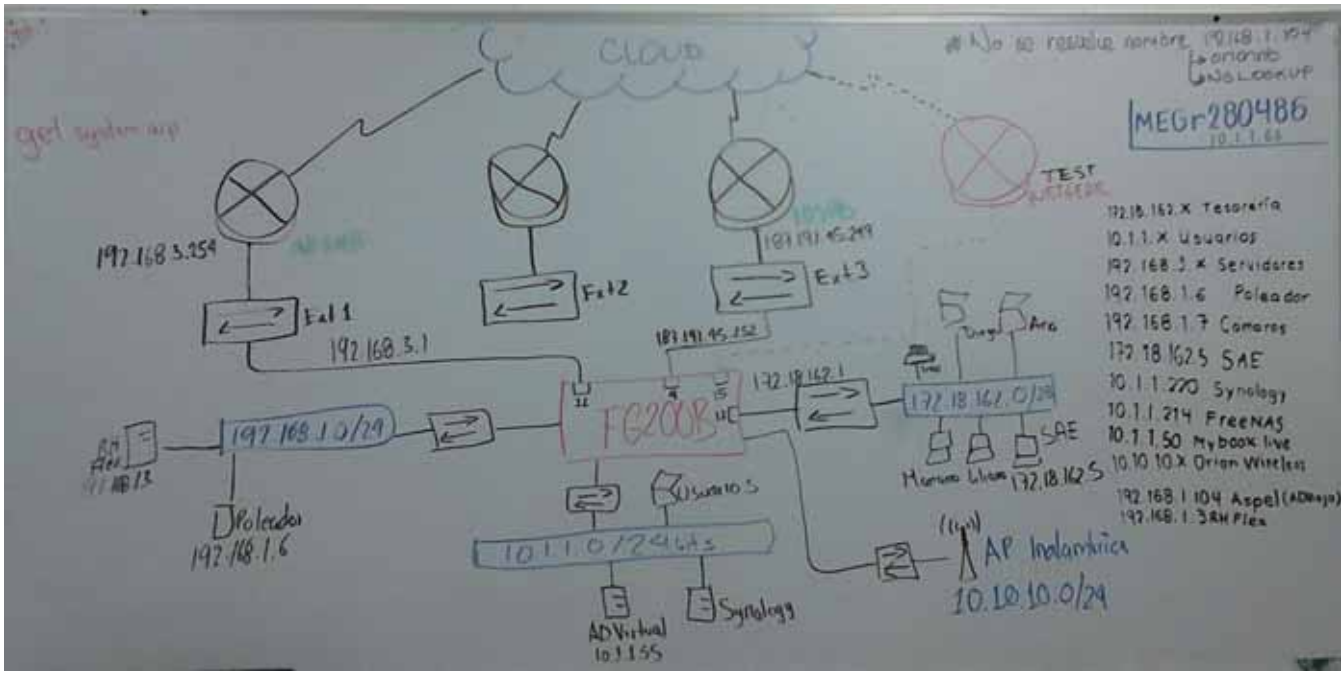
La empresa ***ORIÓN INTEGRACIÓN, DESARROLLO Y TALENTO, S.A de C.V.,*** está conformada por los departamentos de tesorería, reclutamiento, selección y contratación, estos departamentos tiene una gran influencia en la transmisión de los datos y tienen gran trascendencia dentro de la red corporativa.

De acuerdo con la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares**, el respetar la privacidad y la confidencialidad de los clientes de la empresa, candidatos y empleados es fundamental, ya que al realizar las políticas de seguridad debemos de proporcionar calidad, lealtad, responsabilidad y sobre todo seguridad de todos los datos que inundaran la red corporativa.

Los dispositivos que se enuncian a continuación pertenecen y crean la red corporativa de la empresa, la hacen funcional y hacen que la comunicación sea óptima y que la información llegue de un punto a otro:

- Switch Cisco de 24 puertos Catalyst 2960
- Servidor tipo rack Dell PowerEdge SC1435
- Router Cisco 7200 Series Rack Mount Options
- ReadyNAS RN104 de Netgear
- Sygnology DS212j 2-Bay NAS Server
- FortiGate 200B de FortineNet

Uno de los dispositivos clave, que interactúan en la red corporativa y es de gran importancia para este proyecto de configurar e implementar políticas de seguridad es FortiGate que constituye una nueva generación de equipos de seguridad de muy alto rendimiento que garantizan la protección completa de sistemas en tiempo real. FortiGate líder del mercado UTM (Unified Thereat Managment - Gestión Unificada de Amenazas).




**Fotografía 1.1. Análisis de la red corporativa.**

La red corporativa está integrada de la siguiente manera:

La red está conformada por el departamento de **tesorería** cuya dirección IP es **172.18.162.0**, en esta red se encuentran cuatro usuarios (Diego, Ana, Mariano y Liliana) y el sistema **SAE** (**172.18.162.5**) controla el ciclo de todas las operaciones de compra-venta de la empresa como: inventarios, clientes, facturación, cuentas por cobrar, vendedores, compras, proveedores y cuentas por pagar; automatizando eficientemente los procesos administrativos y asegurando el cumplimiento de las disposiciones fiscales.

SAE brinda reportes, estadísticas, gráficas y consultas de alto nivel que colaboran en la oportuna toma de decisiones y desarrollo de estrategias comerciales.

El segmento de red conformado por la IP **10.1.1.0** está conformado por **todos los demás usuarios** (reclutamiento, selección y contratación) de la red corporativa. También en esta parte de la red se encuentra el segmento de red **10.1.1.50** (**WD My Book Live**), es un dispositivo de almacenamiento personal la nube, esto es tener el contenido seguro y bajo control.

Siguiendo con la red, hay otros dos dispositivos que son parte importante para la red corporativa, el **FreeNAS**[13] (10.1.1.214) y **Synology**[14] (10.1.1.220).

Otro segmento de red tiene que ver con la **red inalámbrica** de la empresa y su segmento dentro de la red es **10.10.10.0.** Por último tenemos los segmentos de red **192.168.1.3** (**RH Flex**), **192.168.1.6** (**Poleador**), **192.168.1.7** (**Cámaras de seguridad**), **192.168.1.104** (**Active Directory**).

**RH Flex**, es un software orientado a la administración de recursos humanos, su uso permite la agilización y administración del recurso más importante en la empresa, el recurso humano, garantizando la disminución de tiempo en el proceso global que se invertiría de manera tradicional. Se encuentra organizado en módulos que permiten el control y administración de los diversos aspectos relacionados al recurso humano en la empresa, como son el manejo de nómina, fondo y caja de ahorro, IMSS, contratación de personal, asistencia y otros más.

---

[13] Es un sistema operativo basado en FreeBSD que proporciona servicios de almacenamiento en red. NAS son las siglas en inglés de Almacenamiento Conectado en Red (Network Attached Storage). Este sistema operativo gratuito, open-source y software libre (basado en licencia BSD) permite convertir una computadora personal en un soporte de almacenamiento accesible desde red, por ejemplo para almacenamientos masivos de información, música, backups, etc.

[14] Es una corporación taiwanesa especializada en dispositivos que tienen que ver con el almacenamiento conectado en red (NAS).

**Poleador**, es un sistema denominado así por la empresa, dedicado a mostrar la información sobre el estado de los vuelos, salidas y llegadas de vuelos de las aerolíneas; Iberia, Air France, Aeromexico, American Airlines, Banamex, British Airways, Capital Estratégico, Continental Airlines, Copa Airlines, Delta Airlines, KLM Lineas Aéreas Holandesas de Aviación, US Airways.

Las **cámaras de seguridad** proporcionan protección en tiempo real de manera tal que podemos ver a través de un monitor de computadora lo que sucede y así proteger de gente no autorizada tanto dentro como fuera de la empresa.

El directorio activo (**Active Directory**), este servicio de directorio es un servicio de red que almacena información acerca de los recursos de la red y permite el acceso de los usuarios y las aplicaciones a dichos recursos, de forma que se convierte en un medio de organizar, controlar y administrar centralizadamente el acceso a los recursos de la red.

El cableado en la red es la manera de conectar todos los departamentos que conforman la red corporativa, es muy útil para las empresas, hace más eficiente el trabajo de la red.

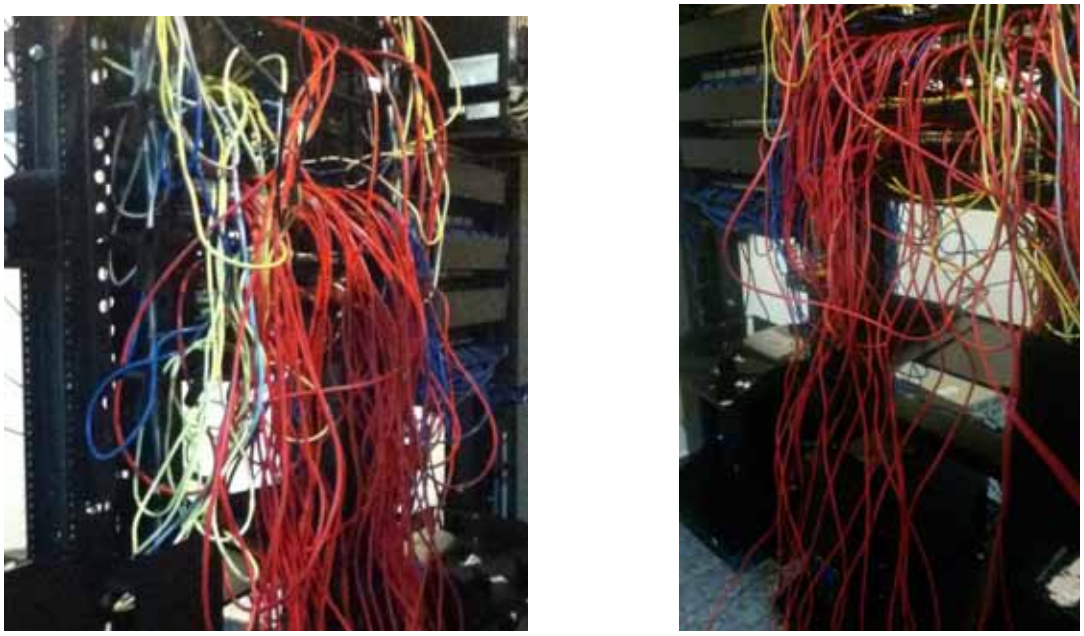
Conforme aumenta el número de usuarios que comparte dispositivos y periféricos en las redes, se efectúa un número mayor de tareas de misión crítica y crece la necesidad de acceso más rápido a la información; es decir, la comunicación se vuelve más compleja, y por lo tanto, se requiere una mejor infraestructura que sea capaz de soportar una amplia variedad de aplicaciones.

Un sistema de cableado estructurado permite integrar todas las necesidades de conectividad de una organización. Está diseñado para usarse en cualquier cosa, en cualquier lugar y en cualquier momento.

Además, se instala una sola vez y puede adaptarse a cualquier aplicación (telefonía, y redes locales) y migrar de manera transparente a nuevas topologías de red y tecnologías emergentes.

Otras ventajas de este tipo de cableado son la localización sencilla y rápida de fallas, la fácil administración de traslados, adiciones y cambios, y la eliminación de las reglas de un proveedor en particular, concernientes a tipos de cable, conectores, distancias o topologías.

El cableado se red se encuentra conformado por cables RJ45 categoría 6 de colores para identificarlos de tal forma que los cables grises son lo de tesorería, los cables azules son de los servidores, los cables rojos son los usuarios y los amarillos son enlaces dedicados.



**Fotografía 1.2. Cableado de la red (antes).**

**Fotografía 1.3. Cableado de la red (después).**

El diagrama 1.1 muestra como está conformada la red corporativa de **ORIÓN INTEGRACIÓN, DESARROLLO Y TALENTO, S.A. DE C.V.**

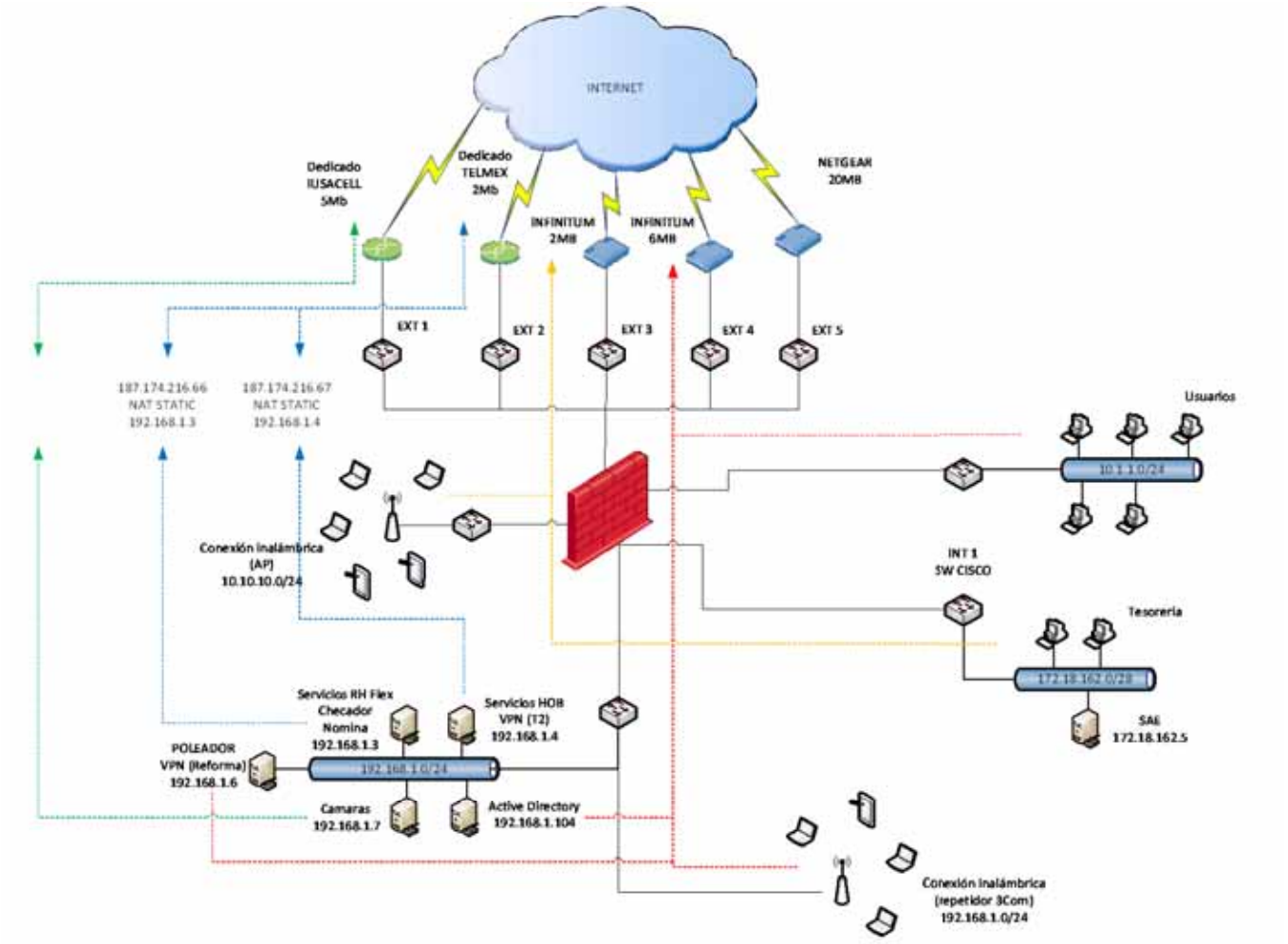



**Diagrama 1.1. Red corporativa.**

### Analizar e identificar vulnerabilidades que existan en la red corporativa

Teniendo en cuenta que es lo que vamos a proteger, es importante analizar e identificar cuáles son las vulnerabilidades que vamos a contrarrestar y al final saber cómo vamos a proteger dichos recursos de manera que se evalué y elija distintos productos y políticas para la seguridad. Es necesario definir algunos términos para analizar e identificar las vulnerabilidades que existan en la red corporativa y nos ayuden a proporcionar seguridad:

**¿Qué es una amenaza?**

Una posibilidad de violación de la seguridad, que existe cuando se da una circunstancia, capacidad, acción o evento que pudiera romper la seguridad y causar perjuicio[15]. Es decir, una amenaza es un peligro posible que podría explotar una vulnerabilidad.

**¿Qué es un ataque?**

Un asalto a la seguridad del sistema derivado de una amenaza inteligente; es decir, un acto inteligente y deliberado (especialmente en el sentido de método o técnica) para eludir los servicios de seguridad y violar la política de seguridad de un sistema.

**Amenazas**

Las redes de datos son atacadas principalmente por personas, quienes intencionalmente o no, pueden afectar a los elementos o recursos interconectados. Sin embargo, no se puede destacar a aquellas amenazas lógicas que fueron creadas para dañar (software malicioso o malware[16]) o incluso fallas en la programación de las aplicaciones (bugs[17] o agujeros), que aún no siendo su fin, pueden ocasionar daños o perdidas para la empresa.
También se pueden considerar como amenazas a las catástrofes naturales o artificiales, ya que nadie se escapa de la probabilidad de sufrir un terremoto, una inundación o una falla en el suministro de corriente eléctrica.

Las amenazas contra un sistema de comunicación de datos, de acuerdo a la recomendación ITU X.805, son las siguientes:

- Destrucción de información y/o de otros recursos
- Corrupción o modificación de información
- Robo, supresión o pérdida de información y/o de otros recursos
- Revelación de información
- Interrupción de servicios

[15] Ocasionar daño o deterioro material o moral.
[16] Programa maligno. Son todos aquellos programas diseñados para causar daños al hardware, software o redes, como los virus, troyanos y gusanos. Es un término común que se utiliza al referirse a cualquier programa malicioso.
[17] Error en la codificación de un programa que provoca inconvenientes diversos al usuario. Defecto de sistema. Un Bug es un fallo del disco de un sistema que sus creadores no han detectado. Puede producirse por un error en una fórmula matemática o por un defecto en la forma de leer y tratar la información que se recibe.

A su vez las amenazas pueden clasificarse en:

- **Amenazas accidentales.** Las amenazas accidentales son las que existen sin que haya premeditación. Ej. Fallos del sistema, equivocaciones en la operación y errores en los programas.
- **Amenazas intencionales.** Las amenazas intencionales pueden ir desde el examen ocasional, mediante el empleo de instrumentos de monitorización de fácil adquisición, hasta ataques sofisticados, gracias a un conocimiento especial del sistema. Una amenaza intencional que se concretiza puede considerarse como un «ataque».
- **Amenazas pasivas.** Las amenazas pasivas son las que no producirían ninguna modificación de la información contenida en el(los) sistema(s) y que tampoco modifican el funcionamiento ni el estado del sistema. La interceptación pasiva para observar la información transmitida por una línea de comunicaciones es un ejemplo.
- **Amenazas activas.** Las amenazas activas contra un sistema conllevan la alteración de información contenida en el sistema, o las modificaciones del estado o de la operación del sistema. La modificación maliciosa de las tablas de enrutamiento por un usuario no autorizado es un ejemplo de amenaza activa.

**Origen de las amenazas**

Las amenazas no se originan desde una sola fuente, pueden provenir de una persona (o varias), de una falla de programación o configuración, e incluso de una catástrofe natural, basándose en esto podemos definir tres grupos:

- Personas
- Amenazas lógicas
- Catástrofes

**Personas**

Las personas generalmente se dividen en dos grande grupos:

- Los atacantes pasivos. Son aquellos que fisgonean por el sistema pero no lo modifican o destruyen.
- Los atacantes activos. Son aquellos que dañan el objetivo atacado, o lo modifican a su favor.

En la siguiente tabla podemos ver algunos ejemplos de personas que atacan las organizaciones y se describe la forma en que lo hacen.

| Ejemplo | Descripción |
|---|---|
| Empleados | Rara vez son tomadas en cuenta las amenazas provenientes del personal de la propia organización, por lo que se puede pasar por alto el hecho de que casi cualquier persona de la organización puede comprometer la seguridad de los equipos.<br><br>Aunque los ataques pueden ser intencionados, lo normal es que se trate de accidentes causados por un error o por desconocimiento de las políticas de seguridad. |
| Hackers y Crackers | Estos términos se aplican a los entusiastas del estudio de las computadoras que sienten placer en conseguir acceso a las computadoras o las redes.<br>Otros designados a menudo como "crackers" son más maliciosos, pudiendo tomar el control de un sistema, robar o dañar datos confidenciales, desconfigurar las páginas Web, e incluso interrumpir el servicio. |
| Intrusos Remunerados | Este es el grupo de atacantes más peligroso, teniendo como principal blanco a las grandes empresas o a organismos de defensa.<br><br>Son piratas con gran experiencia en asuntos de seguridad así como un amplio conocimiento de la red y los sistemas, son pagados por una tercera parte (la competencia o un organismo de inteligencia), generalmente para robar secretos o simplemente para dañar la imagen de la entidad afectada. |

**Tabla 1.2. Ejemplos de personas atacantes.**

Una forma útil de clasificar los ataques a la seguridad, empleada en la recomendación X.805 y RFC 2828 (Internet Security Glossary), es la distinción entre ataques **pasivos** y **activos**. Un ataque pasivo intenta conocer o hacer uso de información del sistema, pero no afecta a los recursos del mismo. Un ataque activo, por el contrario, intenta alterar los recursos del sistema o afectar a su funcionamiento.

### Ataques pasivos

Los ataques pasivos se dan en forma de escucha o de observación no autorizadas de las transmisiones. El objetivo del oponente es obtener información que se esté transmitiendo. Dos tipos de ataques pasivos son la obtención de contenidos de mensajes y el análisis de tráfico.

La obtención de contenidos de mensajes se entiende fácilmente. Una conversación telefónica, un mensaje por correo electrónico y un fichero enviado pueden contener información confidencial. Queremos evitar que un oponente conozca los contenidos de estas transmisiones.

Un segundo tipo de ataque pasivo, el análisis de tráfico, es más sutil. Supongamos que hemos enmascarado los contenidos de los mensajes u otro tráfico de información de forma que el oponente, incluso habiendo capturado el mensaje, no pueda extraer la información que contiene.

La técnica común para enmascarar los contenidos es el cifrado. Incluso si tuviésemos protección mediante cifrado, un oponente podría observar el patrón de los mensajes, determinar la localización y la identidad de los servidores que se comunican y descubrir la frecuencia y la longitud de los mensajes que se están intercambiando. Esta información puede ser útil para averiguar la naturaleza de la comunicación que está teniendo lugar.

Los ataques pasivos son muy difíciles de detectar ya que no implican alteraciones en los datos. Normalmente, el mensaje se envía y se recibe de una forma aparentemente normal y ni el emisor ni el receptor son conscientes de que una tercera persona ha leído los mensajes o ha observado el patrón del tráfico. Sin embargo, es posible evitar el éxito de estos ataques, normalmente mediante el uso del cifrado. Así, al tratar con los ataques pasivos, el énfasis se pone más en la prevención que en la detección.

**Ataques activos**

Los ataques activos implican alguna modificación del flujo de datos o la creación de un flujo falso y se pueden dividir en cuatro categorías: suplantación de identidad, repetición, modificación de mensajes e interrupción de servicio.

Una suplantación se produce cuando una entidad finge ser otra. Un ataque de este tipo incluye habitualmente una de las otras formas de ataque activo.

Por ejemplo, las secuencias de autentificación pueden ser capturadas y repetidas después de que una secuencia válida de autentificación haya tenido lugar, permitiendo así, que una entidad autorizada con pocos privilegios obtenga privilegios extra haciéndose pasar por la entidad que realmente los posee.

La repetición implica la captura pasiva de una unidad de datos y su retransmisión posterior para producir un efecto no autorizado.

La modificación de mensajes significa que una parte de un mensaje original es alterada, o que los mensajes se han retrasado o reordenado, para producir un efecto no autorizado.

La interrupción de servicio impide el uso o la gestión normal de las utilidades de comunicación. Este ataque podría tener un objetivo específico; por ejemplo, una entidad podría suprimir todos los mensajes dirigidos a un destino en particular. Otra forma de este tipo de ataque es la interrupción de una red completa, ya sea inhabilitándola o sobrecargándola con mensajes para reducir su rendimiento.

Los ataques activos representan las características opuestas a los pasivos. Aunque los ataques pasivos son difíciles de detectar, existen medidas para prevenir su éxito. Sin embargo, es bastante difícil prevenir por completo los ataques activos, debido a que se requerirían la protección física de todas las herramientas de comunicación y las rutas en todo momento.

Por lo contrario, el objetivo es el de detectarlos y recuperarse de cualquier irrupción o retraso de originen. Como la detección tiene un efecto disuasivo, también podría contribuir a la prevención.

**Amenazas lógicas**

Bajo la etiqueta de amenaza lógica, se encuentran todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (malware) o simplemente por error (bugs o agujeros).

| Ejemplo | Descripción |
|---|---|
| Software incorrecto | Las amenazas más habituales a un sistema provienen de errores cometidos de forma involuntaria por los programadores de sistemas.<br>A estos errores de programación se les denomina bugs, y a los programas utilizados para aprovechar estos fallos y atacar al sistema se les denomina exploits[18]. |
| Herramientas de seguridad | Cualquier herramienta de seguridad representa un arma de doble filo. Ya que de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa; un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. |
| Puertas traseras | Durante el desarrollo de grandes aplicaciones o de sistemas operativos es habitual entre los programadores insertar 'atajos' en los sistemas de autenticación del programa. |

18 Fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

| | |
|---|---|
| | Algunos programadores pueden dejar estos atajos en las versiones definitivas de su software para facilitar un mantenimiento posterior, para garantizar su propio acceso, o simplemente por descuido. Sí un atacante descubre una de estas puertas traseras, va a tener acceso a datos que no debería poder leer. |
| Canales cubiertos | Los canales cubiertos son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; dicho de otra forma, un proceso transmite información a otros (locales o remotos) que no están autorizados a leer dicha información. |
| Virus | Un virus es una secuencia de código que se inserta en un archivo ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose así mismo en otros programas.<br><br>Cuando una computadora en la red ha sido infectada, es muy probable que las otras computadoras se infecten. |
| Gusanos | Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de la red, en ocasiones portando virus o aprovechando bugs de los sistemas a los que se conecta para dañarlos.<br><br>En un ataque a la red, mientras que una persona puede tardar como mínimo horas en tomar el control (tiempo razonable para detectarlo), un gusano puede hacer eso mismo en pocos minutos. |
| Caballos de troya | Los troyanos o caballos de Troya son instrucciones escondidas en un programa, de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario. |

**Tabla 1.3. Ejemplos de amenazas lógicas.**

### Catástrofes

Las catástrofes (naturales o artificiales) son las amenazas menos probables contra los entornos habituales. Sin embargo, el hecho de que estas amenazas sean las menores, no implica que contra ellas no se tomen unas medidas básicas, ya que si se produjeran, generarían los mayores daños. Algunos ejemplos de amenazas por catástrofes, son:

- Terremotos
- Inundaciones
- Incendios
- Humo
- Cortes eléctricos
- Atentados de baja magnitud

**Diseñar un plan de protección**

Para diseñar el plan de protección que requiere la empresa y contrarrestar todas las vulnerabilidades, ya sean amenazas o ataques, donde la empresa se pueda ver afectada nos apoyaremos en el estándar X.805 de la ITU-T[19], la cual nos habla de la arquitectura de seguridad que responde a las exigencias generales de seguridad de los proveedores de servicio, las empresas y los consumidores, y es válida para redes de voz, de datos y convergentes de tecnología inalámbrica, óptica o de cable. Esta arquitectura de seguridad integra las consideraciones de gestión, control y utilización de la infraestructura, los servicios y las aplicaciones de red.

La arquitectura de seguridad establece un plan y un conjunto de principios que constituyen una estructura de seguridad para la solución de seguridad extremo a extremo. La arquitectura identifica elementos de seguridad a considerar para evitar amenazas intencionales y accidentales.

La arquitectura de seguridad proporciona una visión global, de arriba abajo y extremo a extremo, de la seguridad de red y puede aplicarse a elementos de red, servicios y aplicaciones para detectar, estimar y remediar vulnerabilidades de seguridad. La arquitectura de seguridad divide lógicamente a una serie compleja de características de seguridad de red extremo a extremo, en distintos componentes de arquitectura.

Esta segmentación permite considerar la seguridad de extremo a extremo de forma sistemática, lo que permite planificar nuevas soluciones de seguridad y evaluar la seguridad de las redes actuales.

La arquitectura de seguridad integra tres consideraciones esenciales, para la seguridad extremo a extremo:

1. ¿Qué tipo de protección se necesita, y contra qué amenazas?
2. ¿Cuáles son los diferentes conjuntos de equipos e instalaciones de red que es necesario proteger?
3. ¿Cuáles son las diferentes actividades de red que es necesario proteger?

[19] El Sector de Estandarización de Telecomunicaciones (ITU-T) de la Unión Internacional de Telecomunicaciones (ITU) es una agencia financiada por las Naciones Unidas que desarrolla estándares, denominados recomendaciones, relativos a las Telecomunicaciones y a la interconexión de sistemas abiertos (OSI).

Para responder a estas preguntas hay que considerar tres componentes de la arquitectura:

- **Dimensiones de Seguridad**
- **Capas de Seguridad**
- **Planos de Seguridad**

Los principios descritos por la arquitectura de seguridad se pueden aplicar a una gran diversidad de redes, siendo indiferente la tecnología de red y la posición en la jerarquía de protocolos. A continuación se describen en detalle los elementos de la arquitectura y sus funciones frente a las amenazas.

**Dimensiones de seguridad**

Una dimensión de seguridad es un conjunto de medidas de seguridad que responden a un determinado aspecto de la seguridad de red. En esta recomendación se identifican ocho conjuntos de medidas contra las principales amenazas. Las dimensiones de seguridad incluyen a la red, las aplicaciones y la información de usuario. Estas son las dimensiones de seguridad:

1) Control de acceso
2) Autenticación
3) No repudio
4) Confidencialidad de datos
5) Seguridad de la comunicación
6) Integridad de los datos
7) Disponibilidad
8) Privacidad

| Dimensión de seguridad | Descripción | Ejemplos |
|---|---|---|
| Control de acceso | Límites y control en el acceso a los elementos de red, servicios y aplicaciones. | Password[20], listas de acceso, firewall[21], etc. |
| Autenticación | Garantía de la procedencia de la información. | Password compartido, firmas digitales, certificados digitales, etc. |
| No repudio | Garantía de que no se pueda negar cualquier tipo de actividad en la red. | Bitácoras, sistemas de registros de eventos, firmas digitales, etc. |
| Confidencialidad de los datos | Garantía de que la información solo es accesible por las entidades, sistemas o personas autorizadas. | DES,AES,RSA,etc. |
| Comunicación segura | Garantía de que la información fluye desde la fuente al destino. | Frame Relay, MPLS, IPSec, etc |
| Integridad de los datos | Garantía de que la información no ha sido modificada o corrompida de manera alguna, desde su transmisión hasta su recepción. | MD5, firmas digitales, software antivirus, etc. |
| Disponibilidad | Garantía de que los elementos de red, servicios y aplicaciones, se mantengan disponibles para los usuarios legítimos. | IDS, IPS, redundancia en la red, etc. |
| Privacidad | Garantía de que la información que fluye en la red se mantenga privada. | NAT, DES, AES, RSA, etc. |

**Tabla 1.4. Dimensiones de seguridad.**

### Control de acceso

Garantiza que sólo las personas y los dispositivos autorizados pueden acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y aplicaciones.

### Autenticación

La autenticación garantiza la validez de la identidad que se atribuyen las entidades de una comunicación (por ejemplo, personas, dispositivos, servicios o aplicaciones) y que una entidad no interviene usurpando una identidad o reproduciendo una comunicación anterior sin autorización.

[20] Se denomina así al método de seguridad que se utiliza para identificar a un usuario. Es frecuente su uso en redes. Se utiliza para dar acceso a personas con determinados permisos.

[21] Mecanismo que permite que las comunicaciones entre una red local e Internet se realicen conforme a las políticas de seguridad de quien los instala. Estos sistemas suelen incorporar elementos que garantizan la privacidad, autentificación, etc., con lo que se impide el acceso no autorizado desde Internet.

**No repudio**

Evita que una persona o una entidad niegue que ha realizado una acción de tratamiento de datos, proporcionando la prueba de distintas acciones de red (por ejemplo, de obligación, de intención o de compromiso; prueba de origen de datos; prueba de propiedad; prueba de utilización del recurso).

Garantiza la disponibilidad de pruebas que se pueden presentar a terceros y utilizar para demostrar que un determinado evento o acción si ha tenido lugar.

**Confidencialidad de datos**

Impide que los datos sean divulgados sin autorización.

**Seguridad de la comunicación**

Garantiza que la información solo circula entre los puntos extremo autorizados (no hay desviación ni interceptación de la información que circula entre estos puntos extremo).

**Integridad de los datos**

Garantiza la exactitud y la veracidad de los datos. Protege los datos contra acciones no autorizadas de modificación, supresión, creación o reactuación, y señala estas acciones no autorizadas.

**Disponibilidad**

Garantiza que las circunstancias de la red no impiden el acceso autorizado a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones. Esta categoría incluye soluciones para recuperación en caso de anomalía.

**Privacidad**

Protege la información que sería posible conocer observando las actividades de la red. Por ejemplo: los sitios Web visitados por un usuario, la posición geográfica del usuario y las direcciones IP y los nombres de dominio (DNS) de los dispositivos en la red de un proveedor de servicio.

**Capas de seguridad**

Para realizar una solución de seguridad extremo a extremo, es necesario aplicar las dimensiones de seguridad antes descritas a una jerarquía de equipos de red y dispositivos, es decir, las capas de seguridad. En esta recomendación se definen tres capas de seguridad:

1) Capa de seguridad de infraestructura
2) Capa de seguridad de servicios
3) Capa de seguridad de aplicaciones

Las capas de seguridad son sistemas de potenciación que permiten realizar soluciones de red seguras: la capa infraestructura potencia la capa servicios, y esta potencia la capa aplicaciones. La arquitectura de seguridad tiene en cuenta que las vulnerabilidades de seguridad de cada capa son diferentes, y ofrece la flexibilidad necesaria para reaccionar a las posibles amenazas de la forma más apropiada para una determinada capa de seguridad.

| Capa | Descripción | Ejemplo |
|---|---|---|
| Seguridad de infraestructura | La capa de seguridad de infraestructura, comprende los dispositivos de transmisión y los elementos de red. Esta capa constituye la base fundamental de las redes, sus servicios y aplicaciones. | Enrutadores, centros de conmutación, servidores, enlaces de comunicación, etc. |
| Seguridad de servicios | La capa de seguridad de servicios, tiene que ver con la seguridad de los servicios que los proveedores presentan a sus clientes. | Servicios básicos de transporte y conectividad, plataformas auxiliares para el acceso de Internet ( servicios AAA, DHCP, DNS, etc), o servicios de valor añadido como QoS, mensajería instantánea, etc. |
| Seguridad de aplicaciones | La capa de seguridad aplicaciones tiene que ver con la seguridad de las aplicaciones de la red a las que acceden los clientes de proveedores de servicios. Son aplicaciones soportadas por servicios de red. | Aplicaciones básicas como FTP o HTTP, aplicaciones como mensajería en red y correo electrónico y aplicaciones más elaboradas, como comercio electrónico o móvil, colaboración en video, etc. |

**Tabla 1.5. Capas de seguridad.**

Obsérvese que estas capas de seguridad constituyen una categoría aparte, y las tres capas de seguridad se pueden aplicar a cada capa del modelo de referencia OSI. El sistema de capas proporciona una perspectiva secuencial de la seguridad de red, que determina dónde hay que intervenir para la seguridad en los productos y las soluciones.

Por ejemplo, inicialmente se tratan las vulnerabilidades de seguridad en la capa de infraestructura, luego en la capa de servicios y finalmente en la capa de aplicaciones. En la figura 1.1 se ha representado la aplicación de las dimensiones de seguridad a las capas de seguridad para limitar las vulnerabilidades de cada una y así controlar los ataques contra la seguridad.
La arquitectura de seguridad tiene en cuenta que las vulnerabilidades de seguridad de cada capa son diferentes, y ofrece la flexibilidad necesaria para reaccionar a las posibles amenazas de la forma más apropiada para una determinada capa de seguridad.

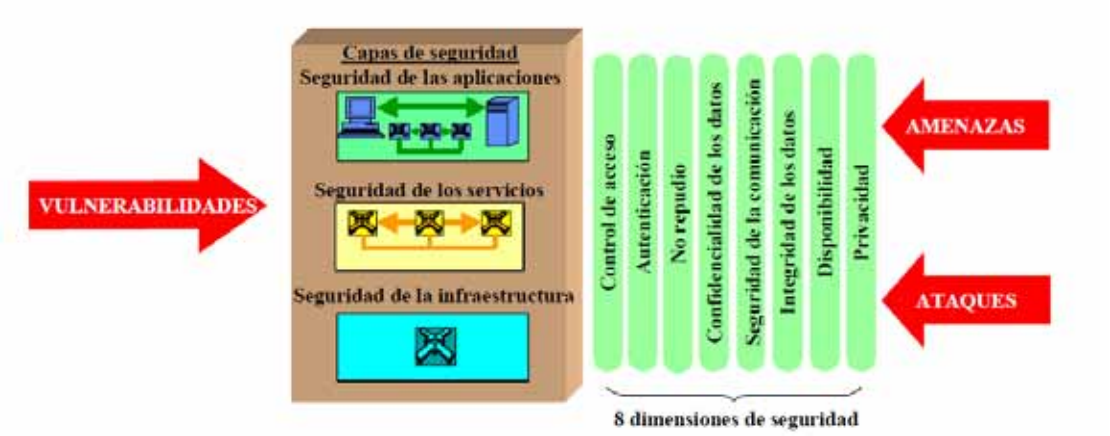



**Figura 1.2. Capas de seguridad.**

### Capa de seguridad servicios

La capa de seguridad servicios tiene que ver con la seguridad de los servicios que los proveedores prestan a sus clientes: desde servicios básicos de transporte y conectividad, hasta plataformas potenciadoras para el acceso a Internet (servicios AAA, servicios de dinámicos de configuración de anfitrión, servicios de nombre de dominio, etc.), o servicios de valor añadido como la telefonía gratuita, QoS, RPV, servicios de geodeterminación, mensajería instantánea, etc. La capa de seguridad servicios se utiliza para proteger a los proveedores de servicio y a sus clientes, que están expuestos unos y otros a amenazas contra la seguridad. Por ejemplo, alguien puede tratar de impedir que el proveedor preste los servicios, o tratar de interrumpir el servicio que se presta a un determinado cliente del proveedor (una empresa por ejemplo).

**Capa de seguridad aplicaciones**

La capa de seguridad aplicaciones tiene que ver con la seguridad de las aplicaciones de red a las que acceden los clientes de proveedores de servicios. Son aplicaciones potenciadas por servicios de red: aplicaciones básicas de transporte de ficheros (por ejemplo FTP) y de navegación Web, aplicaciones fundamentales como la asistencia de directorio, mensajería vocal en red y correo electrónico, y también las aplicaciones más elaboradas, como la gestión de relaciones con los clientes, comercio electrónico o móvil, formación en red, colaboración en vídeo, etc.

Las aplicaciones de red pueden ser productos de terceros: proveedores de servicio de aplicaciones (ASP), proveedores de servicios que intervienen como ASP o empresas que los albergan en centros de datos propios o alquilados.
Hay cuatro objetivos de ataques contra la seguridad en esta capa: el usuario de la aplicación, el proveedor de la aplicación, los programas intermedios de terceros que intervienen como integradores (por ejemplo, servicios de albergue en la Web) y el proveedor del servicio.

**Planos de seguridad**

Un plano de seguridad es una determinada actividad de red protegida por las dimensiones de seguridad. En la recomendación ITU X.805 se definen tres planos de seguridad que representan los tres tipos de actividades protegidas realizadas en la red:

1) El plano de gestión
2) El plano de control
3) El plano de usuario de extremo

Estos planos de seguridad corresponden a necesidades de seguridad particulares relativas a las actividades de gestión de red, control de red o señalización, así como las actividades de usuario de extremo correspondientes.

Es importante que el sistema de red separe totalmente los eventos de dos planos de seguridad. Por ejemplo, una gran cantidad de consultas de DNS[22] en el plano usuario de extremo, iniciadas por peticiones de usuarios, no debería bloquear la interfaz OAM&P[23] en el plano de gestión, para que el gestor pueda resolver el problema.

[22] Servicio de nombres de dominio (Domain Name Service).
[23] Operaciones, administración, mantenimiento y configuración (Operations, Administration, Maintenance & Provisioning).

En la figura 1.2 se representa la arquitectura de seguridad con sus planos de seguridad. Cada actividad de red tiene necesidades de seguridad particulares. El concepto de planos de seguridad permite distinguir los riesgos de seguridad de cada actividad y tratarlos separadamente. Considérese el caso de un servicio de VoIP[24], incluido en la capa de seguridad servicios.

La gestión del servicio VoIP (por ejemplo la configuración de usuarios) tiene que ser independiente del control del servicio (por ejemplo, protocolos como SIP[25]) y también de la seguridad de los datos del usuario de extremo transportados por el servicio (por ejemplo, voz de usuario).

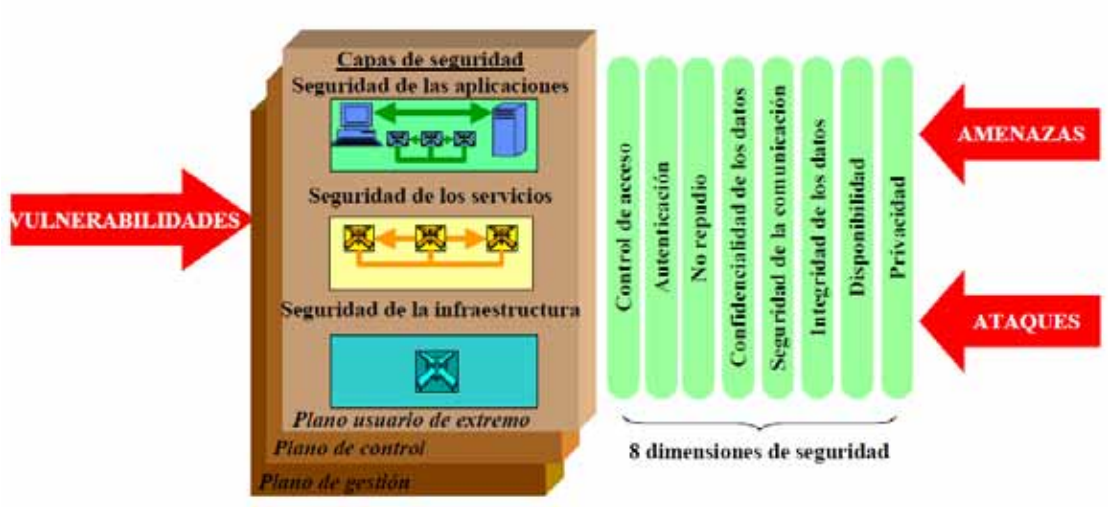



**Figura 1.3. Planos de seguridad.**

**Plano de seguridad gestión**

El plano de seguridad gestión tiene que ver con la protección de las funciones OAM&P de elementos de red, dispositivos de transmisión, sistemas administrativos (soporte de operaciones, soporte comercial, atención de clientes, etc.) y centros de datos. El plano de gestión soporta las funciones FCAPS (anomalía, capacidad, administración, configuración y seguridad). Obsérvese que el tráfico para estas actividades puede transportarse en la red dentro o fuera de la banda, con respecto al tráfico de usuario del proveedor de servicio.

**Plano de seguridad control**

El plano de seguridad control tiene que ver con la protección de las actividades que permiten una distribución eficiente de información, servicios y aplicaciones en la red.

[24] Voz sobre el protocolo Internet (Voice over IP).
[25] Protocolo de iniciación de sesión (Session Initiation Protocol).

Generalmente consiste en la comunicación máquina a máquina de información (por ejemplo centros de conmutación o encaminadores) que permite determinar la mejor forma de encaminar o conmutar el tráfico en la red de transporte subyacente. Se habla de información de control o información de señalización.

Estos mensajes se pueden transportar en la red dentro o fuera de la banda, con respecto al tráfico de usuario del proveedor de servicio. Por ejemplo, las redes IP transportan la información de control dentro de la banda, pero las redes RTPC lo hacen fuera de banda, en una red de señalización separada (la red SS7). Los protocolos de encaminamiento, DNS, SIP, SS7, Megaco/H.248, etc., son ejemplos de este tráfico.

**Plano de seguridad usuario de extremo**

El plano de seguridad usuario de extremo tiene que ver con la seguridad cuando los clientes acceden y utilizan la red del proveedor de servicio. En este plano también se incluyen flujos de datos efectivos del usuario de extremo. El usuario de extremo puede utilizar una red que sólo proporciona conectividad, puede utilizar redes para servicios de valor añadido como las RPV, o redes para acceder a aplicaciones de red.

**Implementación del plan de protección**

Es claro que el establecimiento de políticas de seguridad es un proceso dinámico sobre el cual tenemos que estar actuando permanentemente, de manera tal que no se quede desactualizado, que cuando se descubran debilidades, éstas sean subsanadas y finalmente, que su práctica por los integrantes de la empresa no caiga en desuso.

Este documento se convierte en el primer paso para construir barreras de protección efectivas. La definición de una política de seguridad de red no es algo en lo que se pueda establecer un orden lógico o secuencia aceptada de estados, debido a que la seguridad es algo muy subjetivo, cada departamento dentro de la empresa tiene diferentes expectativas, diferentes metas, diferentes formas de valorar lo que circula por su red, tiene distintos requerimientos para almacenar, enviar y comunicar información de manera electrónica; por esto nunca existe una sola política de seguridad aplicable a dos departamentos diferentes. Además, así como los negocios evolucionan para adaptarse a los cambios en las condiciones del mercado, la política de seguridad debe evolucionar para satisfacer las condiciones cambiantes de la tecnología.

Una política de seguridad de red efectiva es algo que todos los usuarios y administradores pueden aceptar y están dispuestos a reforzar, siempre y cuando la política no disminuya la capacidad de la organización, es decir la política de seguridad se debe implementar de tal forma que no interfiera con las tareas de los usuarios. En general, el costo de proteger las redes de una amenaza debe ser menor que el costo de la recuperación, si es que se ve afectado por la amenaza de seguridad.

Las políticas de seguridad las implementamos en el dispositivo ***FortiGate 200B***, este dispositivo hace uso de la *UTM*[26], ofrece altísimos niveles de escalabilidad, rendimiento, y seguridad. El dispositivo integra una completa gama de funciones y servicios de seguridad para proteger la red corporativa de las sofisticadas amenazas combinadas. Estos servicios de seguridad funcionan conjuntamente para prevenir que los ataques mixtos afecten a la red corporativa.


**Figura 1.4. FortiGate 200B.**

**Conexión y configuración de FortiGate en la red corporativa**

Conectamos y configuramos el dispositivo *FortiGate* para poder aplicar todas las políticas de seguridad que se requieren en la empresa para su óptimo funcionamiento. Cabe mencionar que *FortiGate* se utiliza como gateway[27] o router entre una red privada e Internet, opera en modo *NAT*[28]*/Route* con el fin de ocultar las direcciones de la red privada de miradas indiscretas, mientras que todavía permite que cualquier persona en la red privada pueda conectarse libremente a la Internet.

26 Unified Threat Management (Gestión Unificada de Amenazas).
27 Dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red inicial al protocolo usado en la red de destino.
28 Network Address Translation (Traducción de dirección de red).

En la figura 1.4 podemos ver los componentes que tiene *FortiGate 200B*, el primer paso fue conectarnos a la red privada de la empresa, posteriormente se conecto al *ISP*[29].

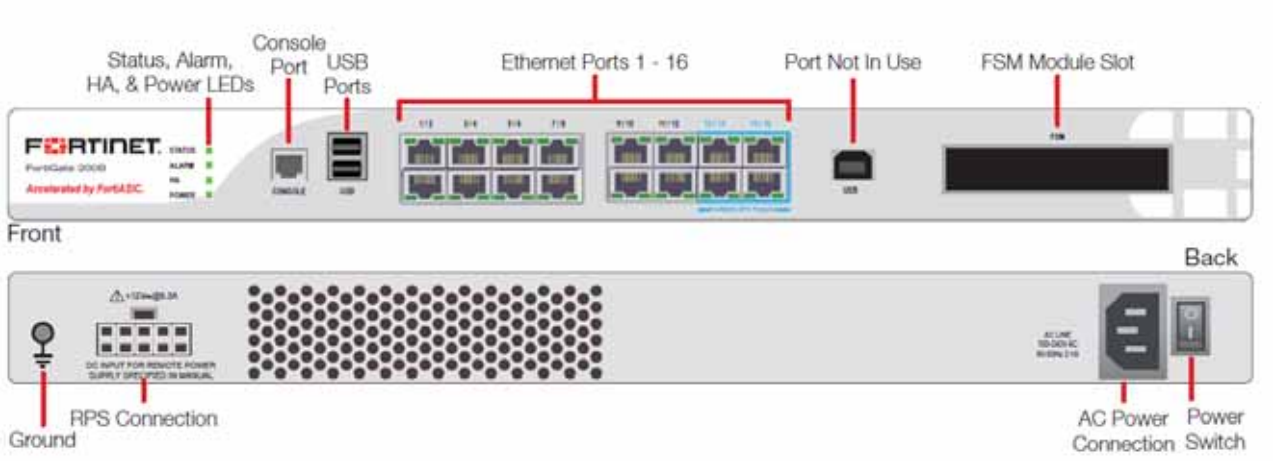



**Figura 1.5. Componentes de FortiGate.**

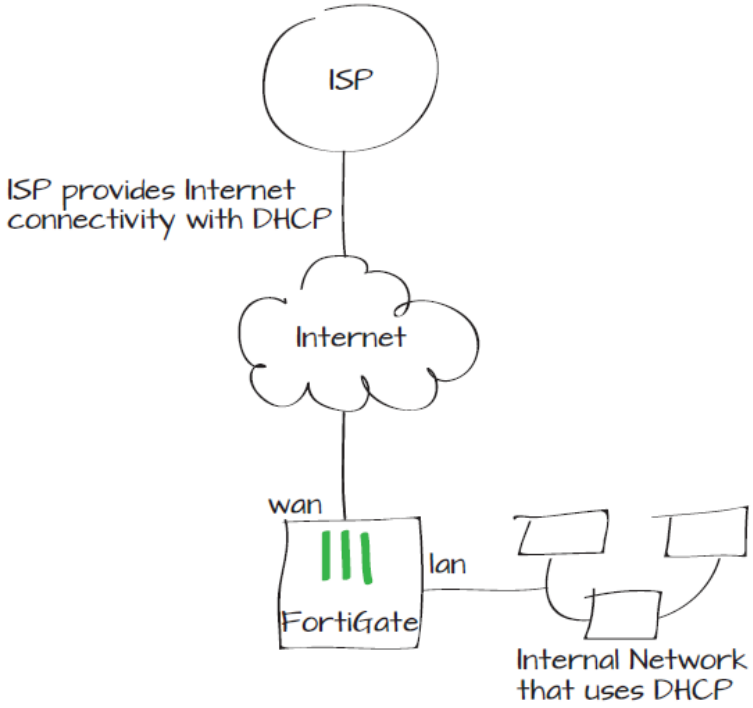



**Diagrama 1.2. Conexión ISP.**

Para poder acceder a la interfaz de *FortiGate* haciendo uso del navegador, desde cualquier computadora que se encuentre dentro de la red privada de la empresa, lo único que hicimos fue obtener la dirección *IP* automáticamente mediante DHCP[30].

[29] Internet Service Provider (Proveedor de servicios de Internet).
[30] Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de host).

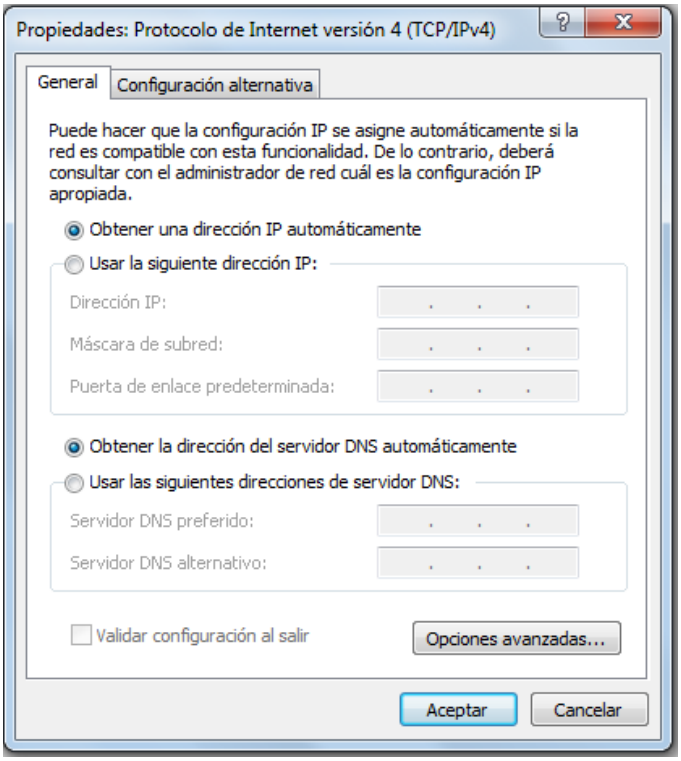



**Figura 1.6. Configuración IP.**

Una vez teniendo lo anterior, tecleamos *ipconfig* en símbolo de sistema y visualizaremos la dirección *192.168.1.99* que es la puerta de enlace predeterminada junto con la dirección que nos asignó dinámicamente, de igual forma como su máscara de subred.

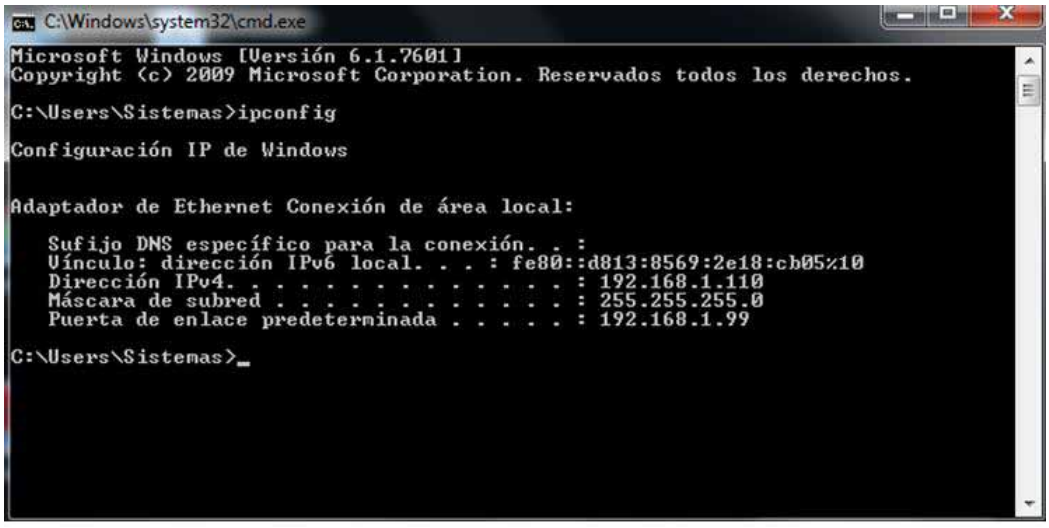



**Figura 1.7. Visualización de configuración IP.**

Si tecleamos la dirección *192.168.1.99* en el navegador de la computadora que estamos utilizando podremos acceder a la interfaz de *FortiGate*, para acceder es necesario utilizar una cuenta de administrador (la cuenta de administrador por defecto tiene el nombre de usuario *admin* y no lleva contraseña).

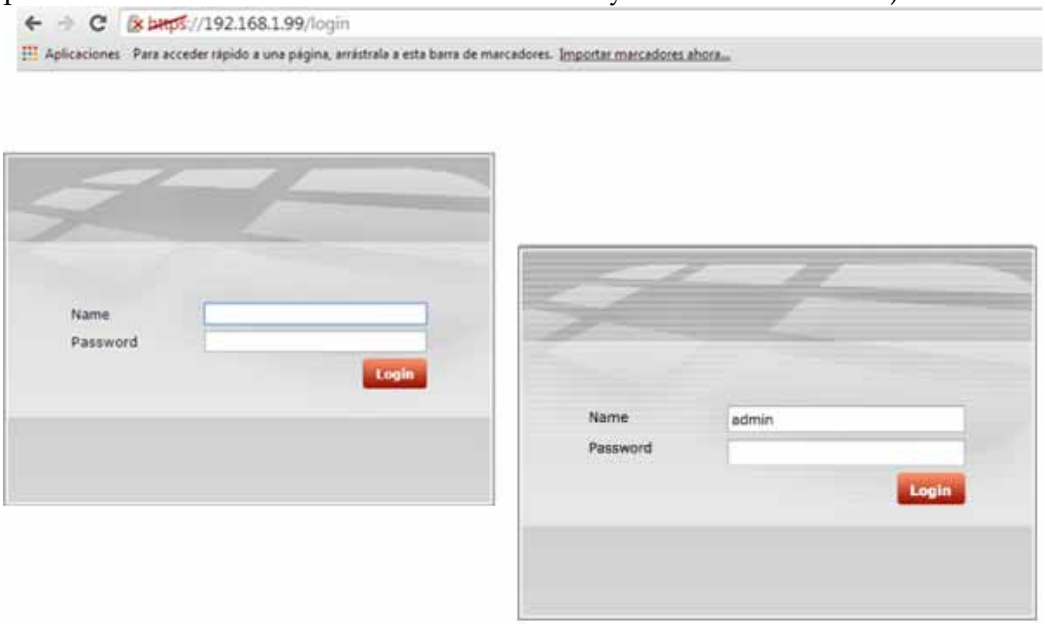



**Figura 1.8. Inicio de sesión.**

A continuación se muestra la interfaz con la cual trabajamos y es de vital importancia para la configuración de cada una de las políticas de seguridad.

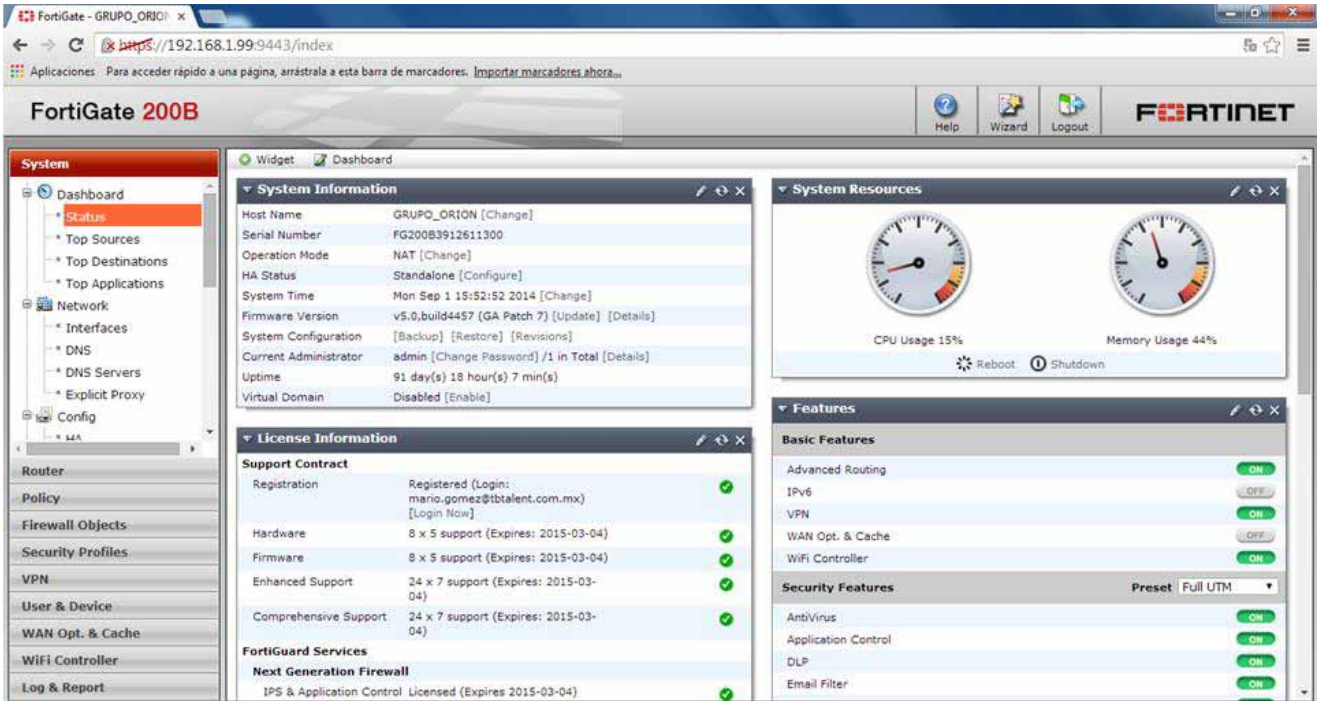



**Figura 1.9. Interfaz FortiGate.**

**Creación de política de seguridad para permitir el tráfico**

Ya estando dentro del sistema de *FortiGate* comenzamos a configurar las diferentes políticas de seguridad una de estas es habilitar el modo NAT/Route.

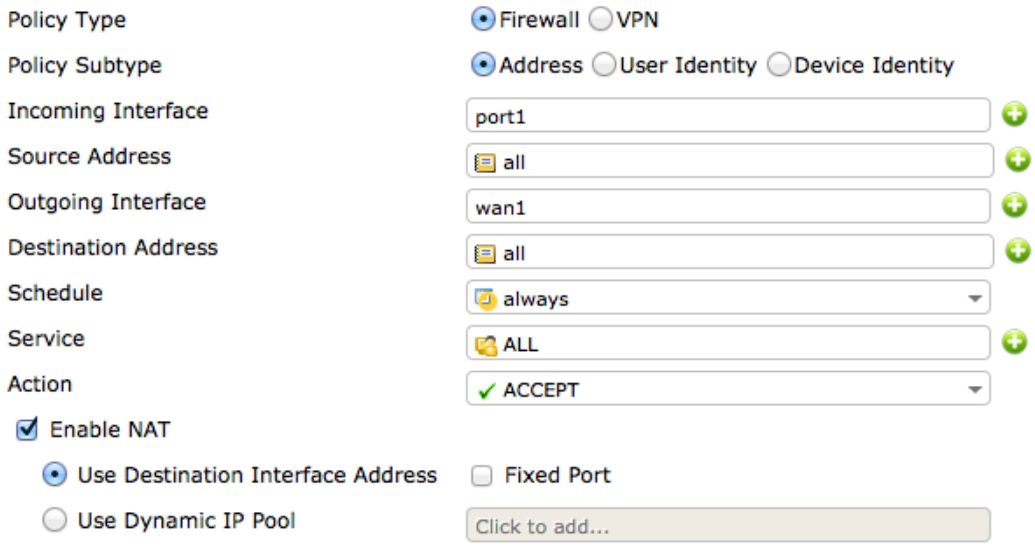



**Figura 1.10. NAT/Route.**

**Autenticación de los usuarios**

Este servicio permite garantizar que nadie ha falsificado la comunicación.

Podemos distinguir dos tipos de autenticación:

- La ***autenticación de mensaje*** o ***autenticación de origen de datos*** permite confirmar que el originador A de un mensaje es auténtico, es decir, que el mensaje no ha sido generado por un tercero Z que quiere hacer creer que lo ha generado A.

  Como efecto adicional, la autenticación de mensaje proporciona implícitamente el servicio de ***integridad de datos***, que permite confirmar que nadie ha modificado un mensaje enviado por A.

- La ***autenticación de entidad*** permite confirmar la identidad de un participante A en una comunicación, es decir, que no se trata de un tercero Z que dice ser A.

A continuación veremos cómo se puede conseguir cada uno de estos dos tipos de autenticación, la autenticación de mensaje o autenticación de origen de datos y autenticación de entidad.

**Autenticación de mensaje**

Existen dos grupos de técnicas para proporcionar autenticación de mensaje:

- Los ***códigos de autenticación de mensaje*** o ***MAC***[31], basados en claves simétricas.
- Las ***firmas digitales***, que se basan en la criptografía de clave pública.

**Códigos de autenticación de mensaje (MAC)**

Un ***código de autenticación de mensaje*** o ***MAC*** se obtiene con un algoritmo *a* que tiene dos entradas: un mensaje *M* de longitud arbitraria, y una clave secreta *k* compartida por el originador y el destinatario del mensaje.

Como resultado da un código $C_{MAC}$ = a (k, M) de longitud fija. El algoritmo MAC debe garantizar que sea computacionalmente inviable encontrar un mensaje $M' \neq M$ que de el mismo código que *M*, y también obtener el código de un mensaje cualquiera sin conocer la clave.

**Firmas digitales**

Los códigos MAC, dado que se basan en una clave secreta, sólo tienen significado para quienes conozcan dicha clave. Si A envía mensajes a B autenticados con una clave compartida, solo B podrá verificar la autenticidad de estos mensajes.

Por otro lado, en caso de un conflicto en que *A* denegase la autoría de un mensaje autenticado, *B* no podría demostrar delante de un tercero imparcial (por ejemplo, un árbitro o un juez) que el mensaje lo generó *A*. Revelar la clave secreta no sería prueba suficiente ya que, por el hecho de ser conocida por las dos partes, siempre habrá la posibilidad que el mensaje en disputa y el su código de autenticación los hubiera generado *B*.

En cambio, si *A* autentica los mensajes adjuntándoles la firma digital calculada con su clave privada, todo el mundo podrá verificarlos con su clave pública. Esta técnica de autenticación proporciona, como efecto adicional, el servicio de ***no repudio***.

Esto quiere decir que un destinatario *B* puede demostrar fehacientemente ante un tercero que un mensaje ha sido generado por *A*.

[31]Message Authentication Code (Código de Autenticación de Mensaje).

**Autenticación de entidad**

La autenticación de entidad se utiliza cuando en una comunicación una de las partes quiere asegurarse de la identidad de la otra. Normalmente, esta autenticación es un requisito para permitir el acceso a un recurso restringido, como, por ejemplo, una cuenta de usuario en un ordenador, dinero en efectivo en un cajero automático, acceso físico a una habitación, etc.

En general, las técnicas utilizadas para la identificación de un usuario A pueden estar basadas en:

- Algo que A sabe como, por ejemplo, una contraseña o una clave privada.
- Algo que A tiene como, por ejemplo, una tarjeta con banda magnética o con chip.
- Alguna propiedad inherente a A como, por ejemplo, sus características biométricas[32].

Algunas técnicas biométricas hacen uso de características fisiológicas humanas (como la huella dactilar, el iris, la retina, la cara o la mano) o características del comportamiento humano (como el habla, la firma manual o la pulsación de teclas).

Una diferencia entre la ***autenticación de mensaje*** y la ***autenticación de entidad*** es que la primera puede ser intemporal (es posible verificar la autenticidad de un documento firmado, por ejemplo, diez años atrás) mientras que la segunda normalmente se realiza en tiempo real. Esto quiere decir que para la autenticación de entidad se puede llevar a cabo un protocolo interactivo, en el que ambas partes se intercambien mensajes hasta que la identidad en cuestión quede confirmada.

A continuación veremos dos grupos de técnicas que se pueden utilizar para la autenticación de entidad:

- Las basadas en ***contraseñas*** (o ***passwords***, en inglés), también llamadas ***técnicas de autenticación débil.***
- Las basadas en ***protocolos de reto-respuesta (challenge-response,*** en inglés), también llamadas ***técnicas de autenticación fuerte.***

Nosotros utilizaremos las técnicas anteriormente mencionadas para poner en práctica las políticas de seguridad que requiere la empresa, este proceso realiza el acto de confirmación de la identidad de una persona o dispositivo. Cuando se utiliza la autenticación, las identidades de los usuarios o equipos host se deben establecer para garantizar que sólo las personas autorizadas puedan acceder a la red corporativa.

[32] Estudio mensurativo o estadístico de los fenómenos o procesos biológicos.

La autenticación de usuarios y la autenticación de dispositivos proporcionan un acceso diferente para los miembros del personal en función de si son a tiempo completo o tiempo parcial, al tiempo que niega todo el tráfico de los teléfonos móviles.

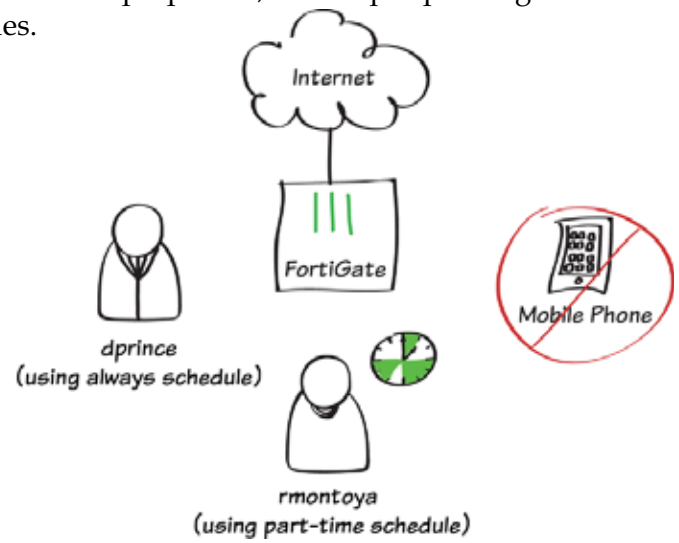



**Diagrama 1.3. Autenticación de usuarios.**

Ir a **User & Device > User > User Definitions** y crear dos nuevos usuarios como lo muestra la figura 1.11 los usuarios ejemplo seran *dprince* y*rmontoya.*

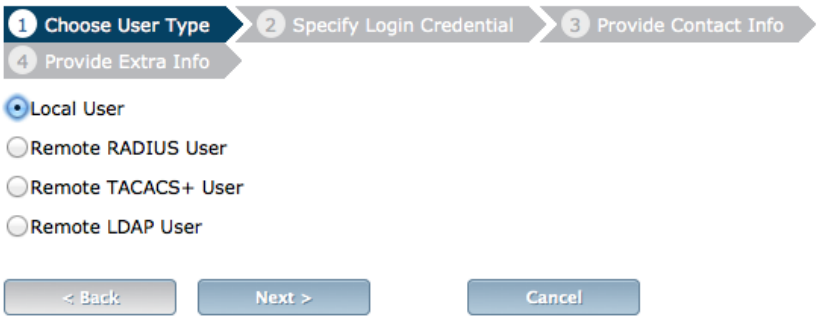



**Figura 1.11. Paso 1 de la autenticación.**

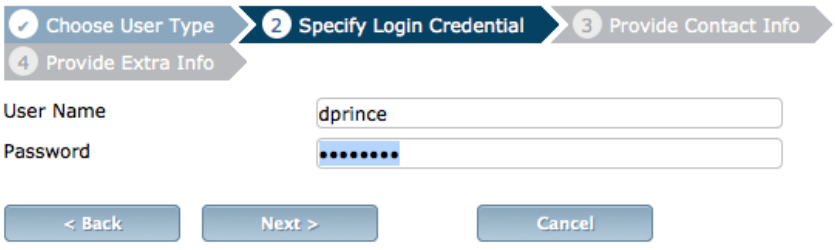



**Figura 1.12. Paso 2 de la autenticación.**

La idea básica de la autenticación basada en contraseñas es que el usuario *A* manda su identidad (su identificador de usuario, su nombre de *login*, etc.) seguida de una contraseña secreta $X_A$ (una palabra o combinación de caracteres que el usuario pueda memorizar). El verificador *B* comprueba que la contraseña sea válida, y si lo es da por buena la identidad de *A*.

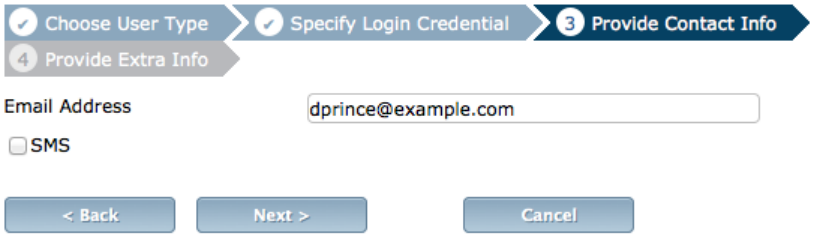



**Figura 1.13. Paso 3 de la autenticación.**

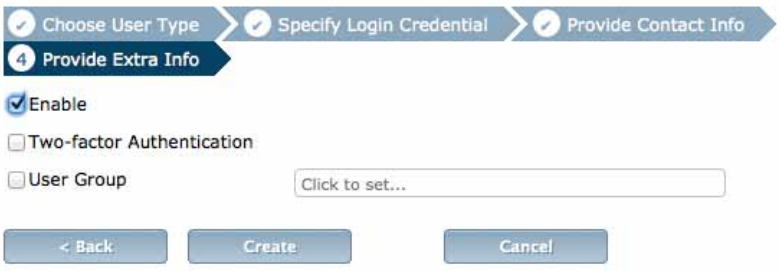



**Figura 1.14. Paso 4 de la autenticación.**

### Protocolos de reto-respuesta

El problema que tienen los esquemas de autenticación basados en contraseñas es que cada vez que se quiere realizar la autenticación se tiene que enviar el mismo valor al verificador (excepto en las contraseñas de un solo uso, como acabamos de ver). Cualquier atacante que consiga interceptar este valor fijo podrá suplantar la identidad del usuario a quien corresponda la contraseña.

Hay otro grupo de mecanismos donde el valor que se envía para la autenticación no es fijo, sino que depende de otro, generado por el verificador. Este último valor se llama **reto**, y se debe enviar al usuario *A* como primer paso para su autenticación. Entonces *A*, haciendo uso de una clave secreta, calcula una **respuesta** a partir de este reto, y lo envía al verificador *B*. Por este motivo, estos mecanismos de autenticación reciben el nombre de **protocolos de reto-respuesta**.

El algoritmo para calcular la respuesta debe garantizar que no se pueda obtener sin saber la clave secreta. Esto permite al verificador confirmar que la respuesta sólo ha podido enviarla *A*. Si se utiliza un reto distinto cada vez, un atacante no podrá sacar provecho de la información que descubra interceptando la comunicación.

En la figura 1.16 se muestra la autenticación de los usuarios ejemplo, junto con su tipo de usuario.

| User Name | Type | Two-factor Authentication | Ref. |
|---|---|---|---|
| dprince | LOCAL | | 0 |
| guest | LOCAL | | 1 |
| rmontoya | LOCAL | | 0 |

**Figura 1.15. Visualización de la autenticación.**

Para implementar grupos de trabajo de tiempo completo y tiempo parcial nos vamos a **User & Device > User > User Groups.**


**Figura 1.16. Usuarios de tiempo completo.**

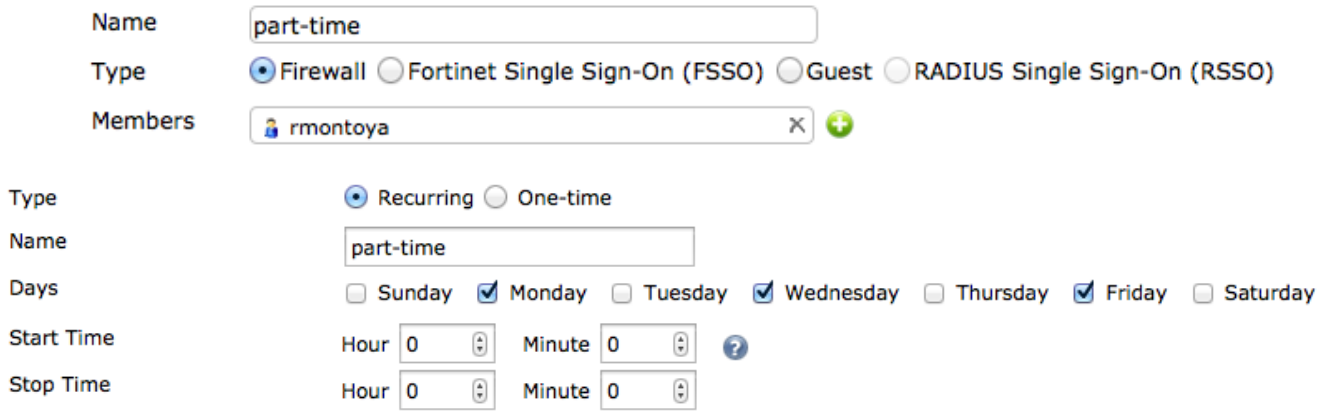



**Figura 1.17. Usuarios de medio tiempo.**

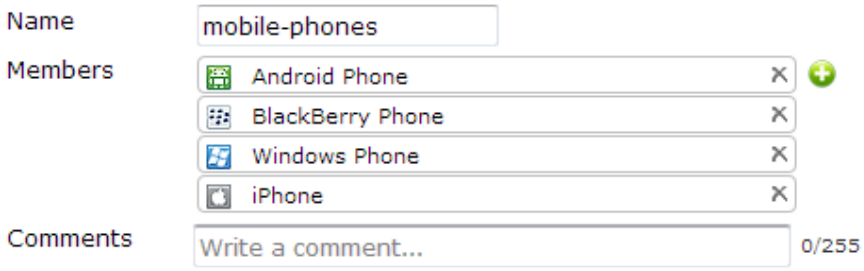



**Figura 1.18. Negación de servicio teléfonos móviles.**

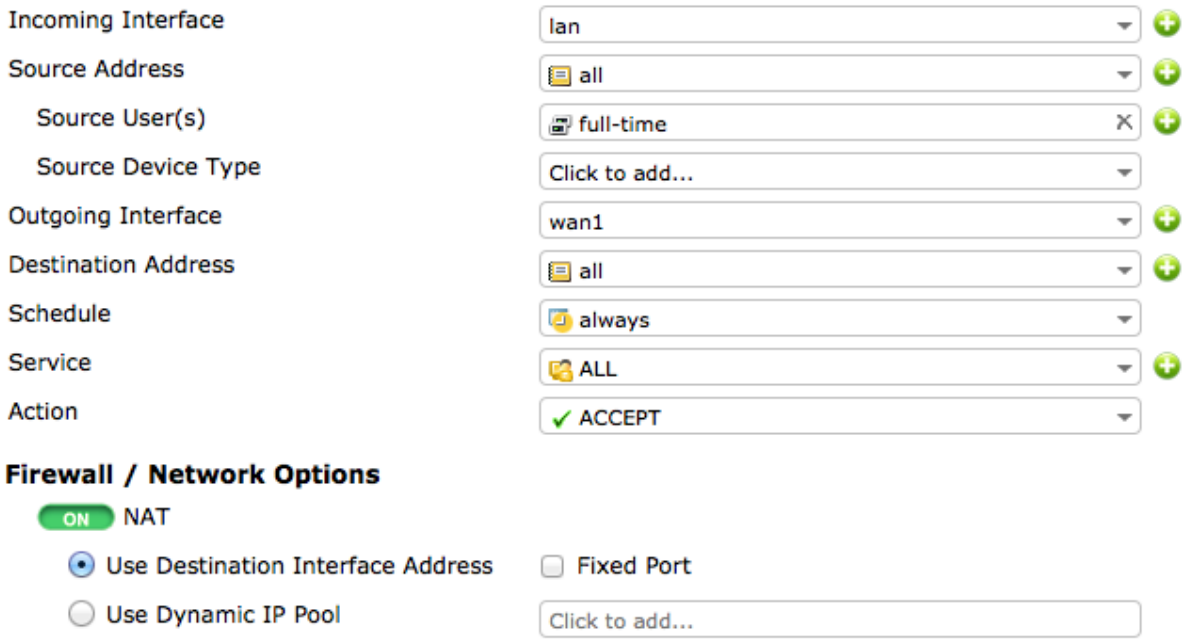



**Figura 1.19. Política de seguridad para usuarios de tiempo completo.**

La autenticación garantiza que sólo las personas y los dispositivos autorizados pueden acceder a los elementos de la red corporativa, la información almacenada, los flujos de información, los servicios y aplicaciones, implementando el control de acceso y la autenticación como políticas de seguridad. También garantiza la validez de la identidad de cada usuario de la red corporativa identificando los que no intervienen, los que usurpan y los que entran sin autorización.

Los usuarios son consientes de todo lo que se genera en la red es información de la empresa, así que la confidencialidad de los datos es un hecho. Ya que la información solo circula entre los puntos autorizados no hay desviación ni interceptación de la información que circula entre estos puntos.

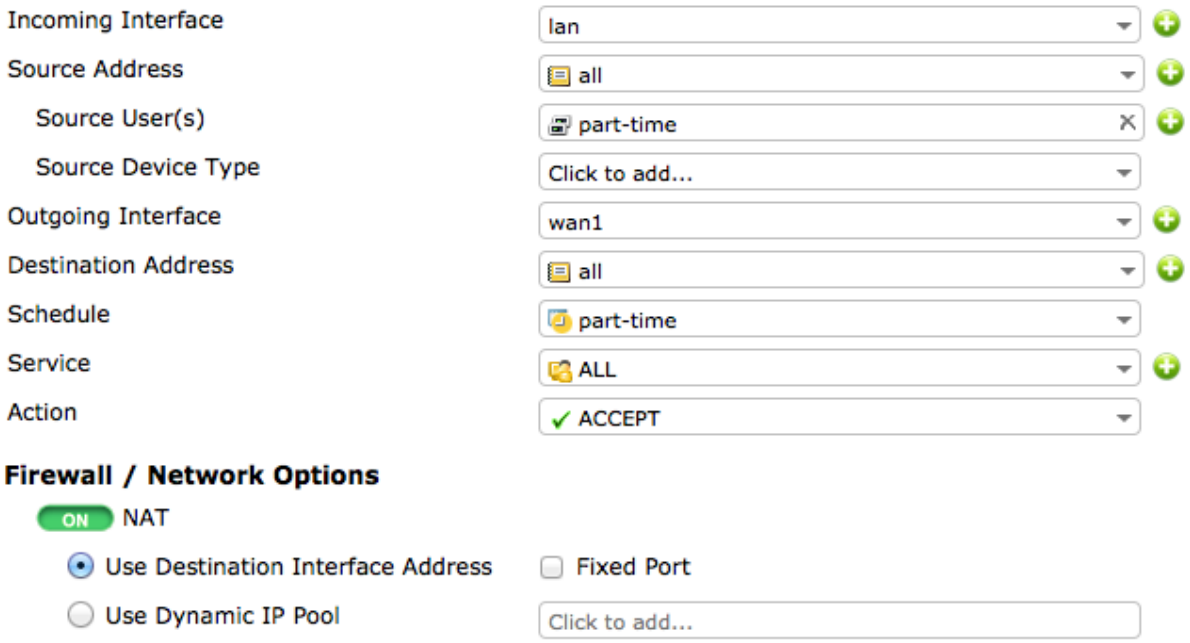



**Figura 1.20. Política de seguridad para usuarios de medio tiempo.**

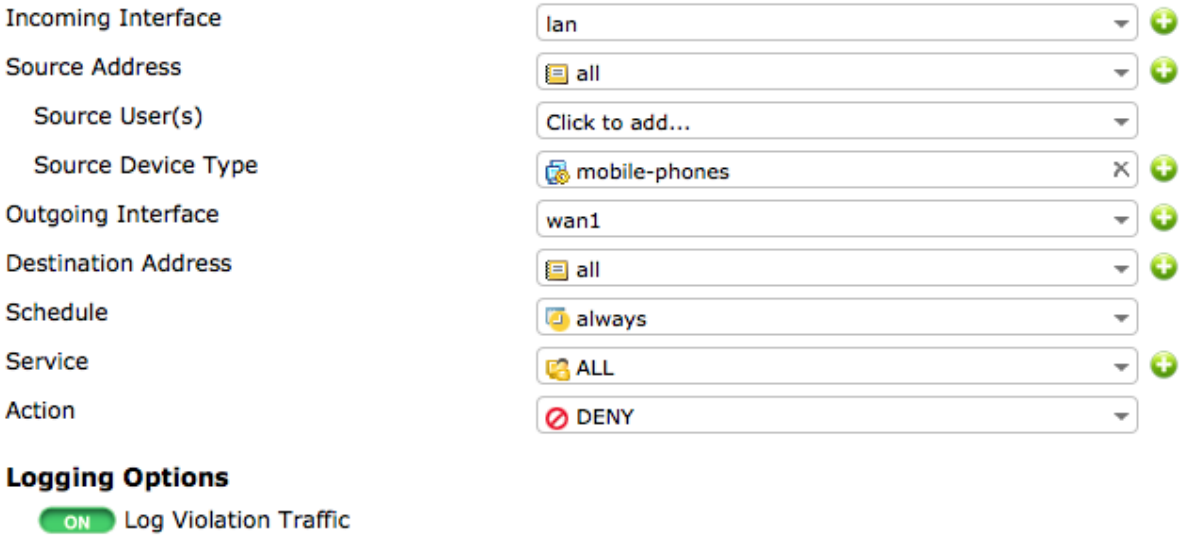



**Figura 1.21. Política de seguridad para teléfonos móviles.**

| Seq.# | From | To | Devices | Groups | Action |
|---|---|---|---|---|---|
| 3 | lan | wan1 | Mobile Devices | | DENY |
| 1 | lan | wan1 | | full-time | ACCEPT |
| 2 | lan | wan1 | | part-time | ACCEPT |
| 4 | any | any | | | DENY |

**Figura 1.22. Políticas de seguridad aplicadas.**

**FortiGate como sistemas cortafuegos**

Los sistemas cortafuegos[33] son un mecanismo de control de acceso sobre la capa de red. La idea básica es separar nuestra red (donde los equipos que intervienen son de confianza) de los equipos del exterior (potencialmente hostiles). FortiGate actúa como una barrera central, para reforzar el control de acceso a los servicios que se ejecutan tanto en el interior como en el exterior de la red. FortiGate intentará prevenir los ataques del exterior contra las máquinas internas de nuestra red denegando intentos de conexión desde partes no autorizadas.

El control de FortiGate consiste, en última instancia, en permitir o denegar el paso de la comunicación de una red a otra mediante el control de los protocolos TCP/IP.

En el momento configurar e implementar FortiGate en nuestra red, vimos las siguientes características:

1. Todo el tráfico que sale del interior hacia el exterior de la red que se quiere proteger, y viceversa, debe pasar por el cortafuego. Esto se puede conseguir bloqueando físicamente todo el acceso al interior de la red a través del sistema.

2. Solo el tráfico autorizado, definido en las políticas de seguridad locales del sistema, podrá traspasar el bloqueo.

3. El propio cortafuego debe estar protegido contra posibles intrusiones. Esto implica el uso de un sistema operativo de confianza con suficientes garantías de seguridad.

Una vez que sabemos cómo autenticar y saber un poco mas de FortiGate debemos esta consientes que hay más herramientas con las que podemos hacer uso y estas tienen que ver con la criptografía.

Esta herramienta que nos permite evitar que alguien intercepte, manipule o falsifique los datos transmitidos, cuya finalidad básica es el envío de información secreta. Si aplicamos una transformación, conocida como cifrado, a la información que queremos mantener en secreto, aunque un adversario consiga ver qué datos estamos enviando le serán completamente ininteligibles. Sólo el destinatario legítimo será capaz de realizar la transformación inversa y recuperar los datos originales.

[33] En inglés, *firewalls.*

La **criptografía** estudia, desde un punto de vista matemático, los métodos de protección de la información. Por otro lado, el criptoanálisis estudia las posibles técnicas utilizadas para contrarrestar los métodos criptográficos, y es de gran utilidad para ayudar a que estos sean más robustos y difíciles de atacar. El conjunto formado por estas dos disciplinas, criptografía y criptoanálisis, se conoce como criptología.

Esta protección que estamos implementando se puede obtener en distintos niveles de la arquitectura de comunicaciones. A nivel red, el mecanismo principal en un entorno de interconexión basado en IP es el conjunto de protocolos conocido como IPSec o a nivel de transporte, aprovechando así la infraestructura IP existente, principalmente los encaminadores o routers. Como ejemplo de protección a nivel de transporte están los protocolos SSL/TLS/WTLS. Hasta este punto tenemos mecanismos básicos de protección, que proporcionan servicios como la confidencialidad o la autenticación.

Ahora veremos la arquitectura IPSec, diseñada para proteger el protocolo de red usado en Internet, es decir, el protocolo IP. Veremos mecanismos para proteger las comunicaciones a nivel de transporte, y en el módulo de aplicaciones seguras veremos ejemplos de protección de los protocolos a nivel de aplicación.

**La arquitectura IPSec**

La arquitectura IPSec (RFC 2401) añade servicios de seguridad al protocolo IP (versión 4 y versión 6), que pueden ser usados por los protocolos de niveles superiores (TCP, UDP, ICMP, etc.).

IPSec se basa en el uso de una serie de protocolos seguros, de los cuales hay dos que proporcionana la mayor parte de los servicios:

- El **protocolo AH** (*Authentication Header*, RFC 2402) ofrece el servicio de autenticación de origen de los datagramas IP (incluyendo la cabecera y los datos de los datagramas).

- El **protocolo ESP** (*Encapsulating Security Payload*, RFC 2406) puede ofrecer el servicio de confidencialidad, el de autenticación de origen de los datos de los datagramas IP (sin incluir la cabecera), o los dos a la vez.

Cuando IPSec se implementa en FortiGate, proporciona una gran seguridad que se puede aplicar a todo el tráfico que lo cruza. El tráfico en esta empresa no provoca costes adicionales de procesamiento relativo a la seguridad.

IPSec es seguro en FortiGate si se obliga a que todo el tráfico que proviene del exterior use IP, y FortiGate es el único medio de entrada desde Internet a la organización.

IPSec está por debajo de la capa de transporte (TCP, UDP) y, por ello, es transparente a las aplicaciones. No es necesario cambiar el software en el sistema de un usuario o de un servidor cuando IPSec se implementa en FortiGate. Incluso si IPSec se implementa en sistemas finales, el software de nivel superior, incluyendo aplicaciones, no se ve afectado.

IPSec puede ser transparente a usuarios finales. No es necesario entrenar a los usuarios para la utilización de mecanismos de seguridad, ni suministrar material relativo al uso de claves por cada usuario, ni inhabilitar dicho material cuando los usuarios abandonan la organización.

IPSec puede proporcionar seguridad a usuarios individuales sí es necesario, lo cual es útil para trabajadores externos y para establecer una subred virtual segura en una organización para las aplicaciones confidenciales.

**Bloqueo del acceso a sitios Web específicos**

Bloquearemos el sitio *www.fortinet.com* para ejemplificar esta política de seguridad, la cual nos ayuda a tener un mejor control sobre que sitios deben de ver los usuarios de la red corporativa para evitar amenazas.


**Diagrama 1.4. Bloqueo de sitios específicos**

Nos vamos a Security *Profiles* > *Web Filter* > *Profiles*, le damos clic *Enable Web Site Filter y* creamos un nuevo perfil, *e*n *URL* le damos el sitio Web que queremos bloquear, es importante mencionar que utilizamos asterisco al principio del nombre del sitio Web para bloquear todos los subdominios del sitio Web.

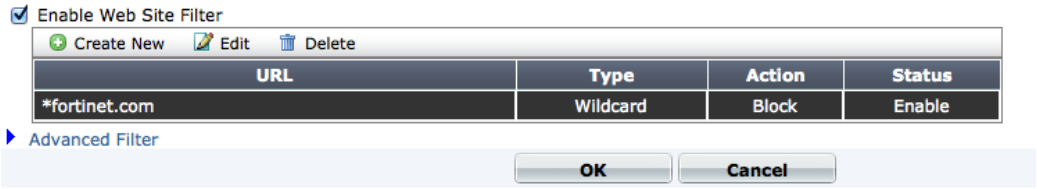



**Figura 1.23. Bloqueo del sitio Fortinet**

Agregamos por ultimo la política de seguridad que controlara el flujo de los datos, como se muestra en la figura 1.13.

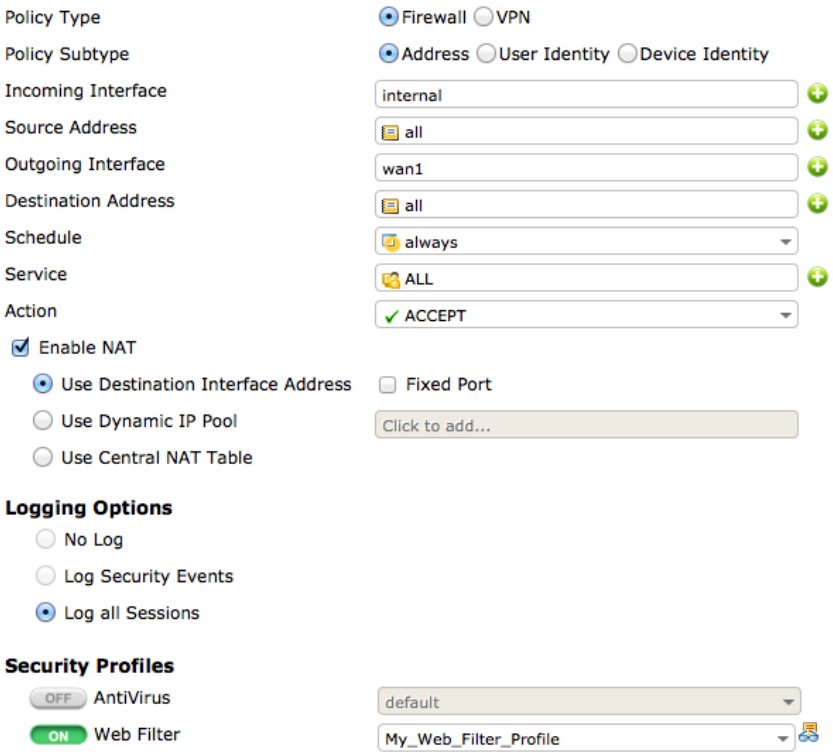



**Figura 1.24. Política de seguridad**

**Bloqueo de tráfico HTTP y HTTPS con filtrado Web**

Ahora se bloquearan sitios que hacen uso de *streaming*, serán bloqueados a partir de filtrado Web, los protocolos HTTP y HTTPS serán bloqueados.

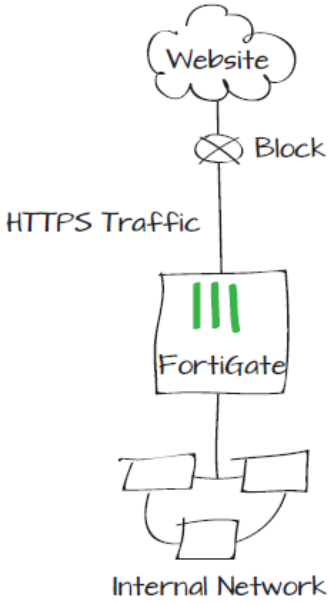



**Diagrama 1.5. Bloqueo de trafico HTTPS**

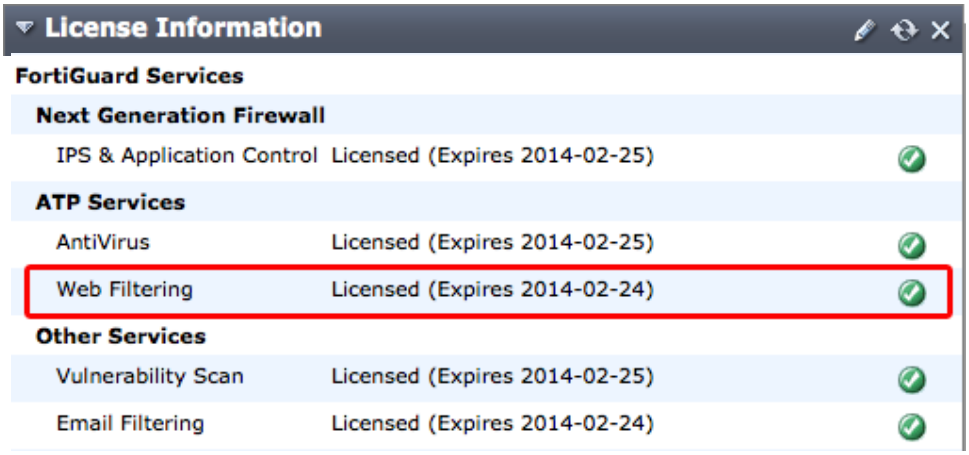



**Figura 1.25. Verificación de servicios FortiGuard**

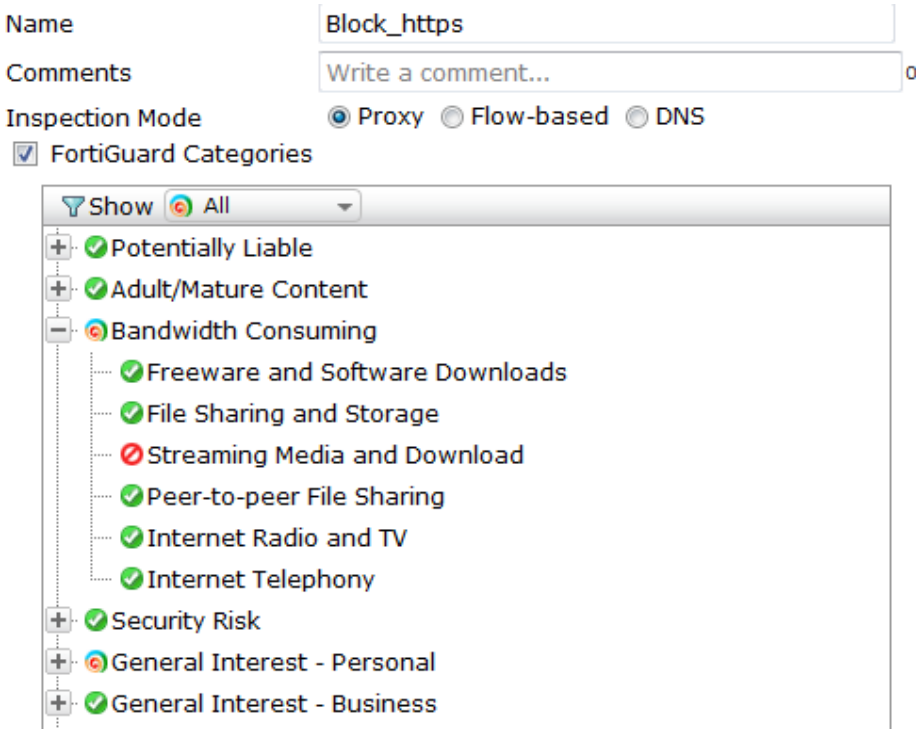



**Figura 1.26. Creación de un perfil de filtrado Web**

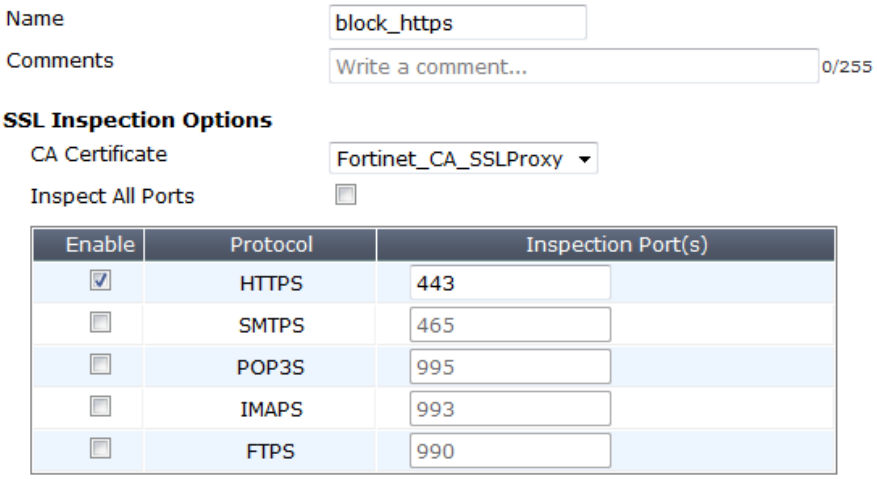



**Figura 1.27. Creación de un perfil de inspección SSL**

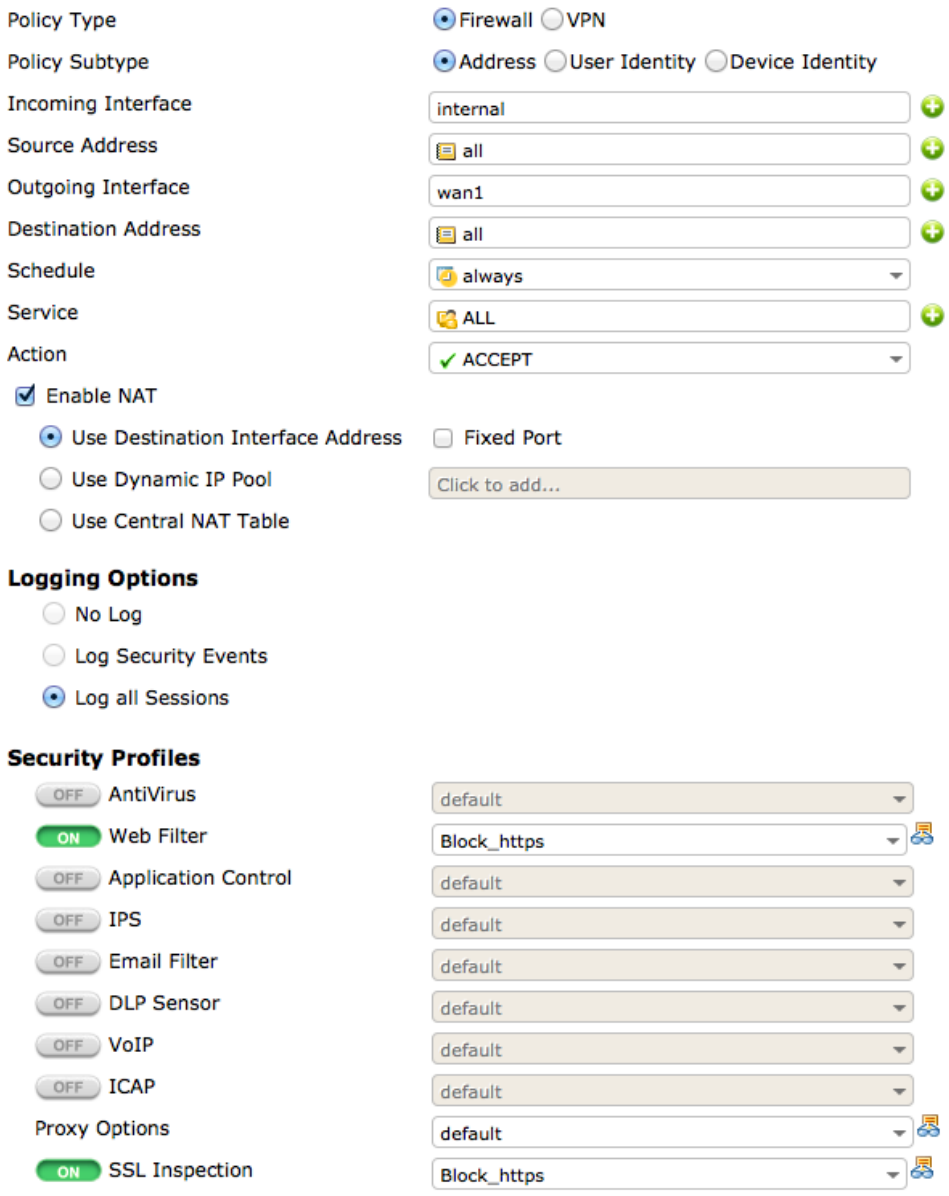



**Figura 1.28. Creación de política de seguridad**

La política de seguridad en esta parte tiene que ver con el tráfico que bloquearemos y nos dará una idea de tener el control del flujo que se transmite en la red corporativa.

**Bloqueo de Facebook**

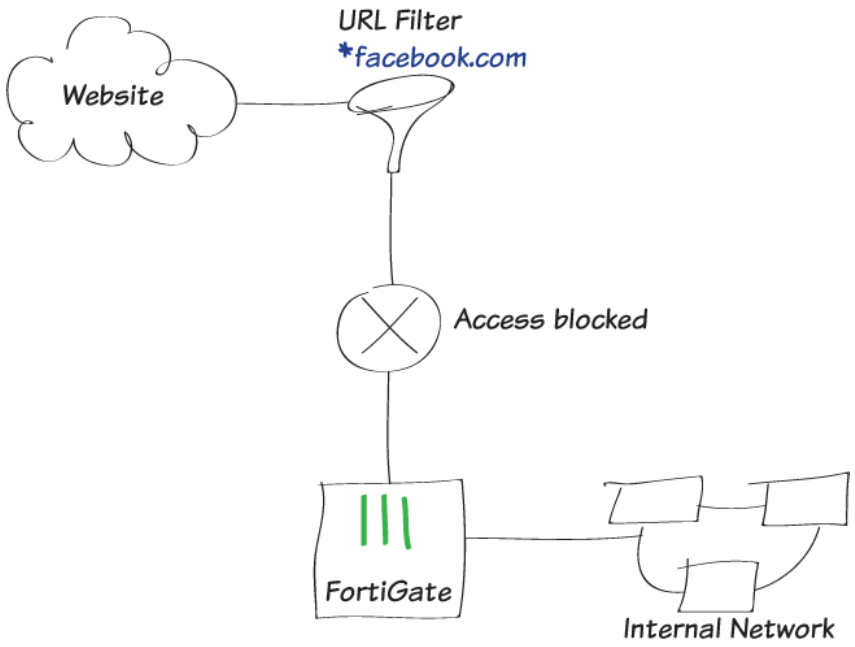



**Diagrama 1.6. Bloqueo de Facebook**

Configuramos FortiGate para impedir el acceso a un sitio Web específico de redes sociales, incluyendo sus subdominios.


**Figura 1.29. Verificación de suscripción FortiGuard.**

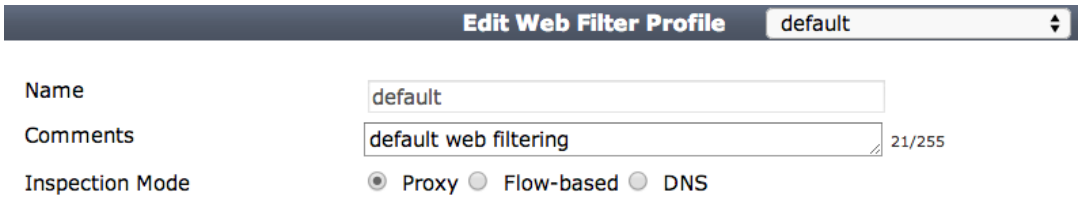



**Figura 1.30. Edición de perfil de Filtro Web.**

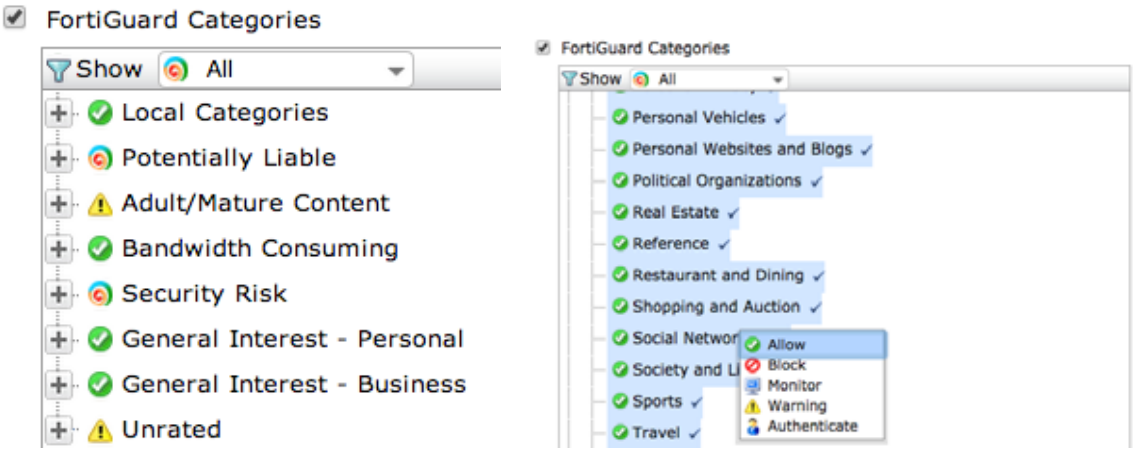



**Figura 1.31. Habilitación de acciones FortiGuard.**

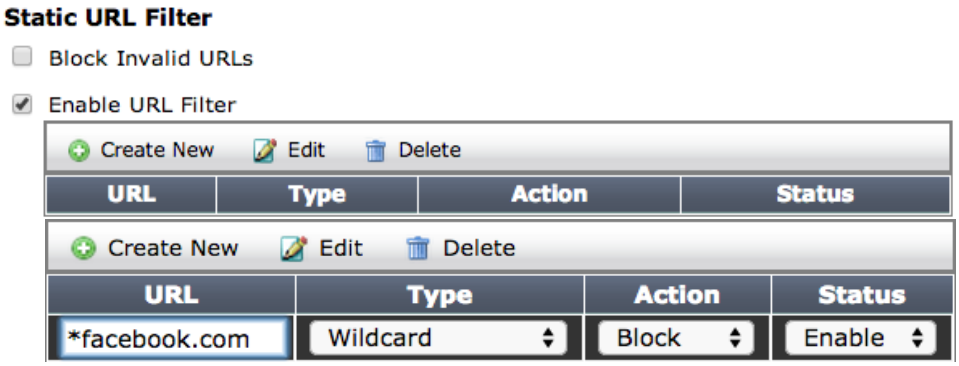



**Figura 1.32. Creación de filtro para bloquear Facebook.**

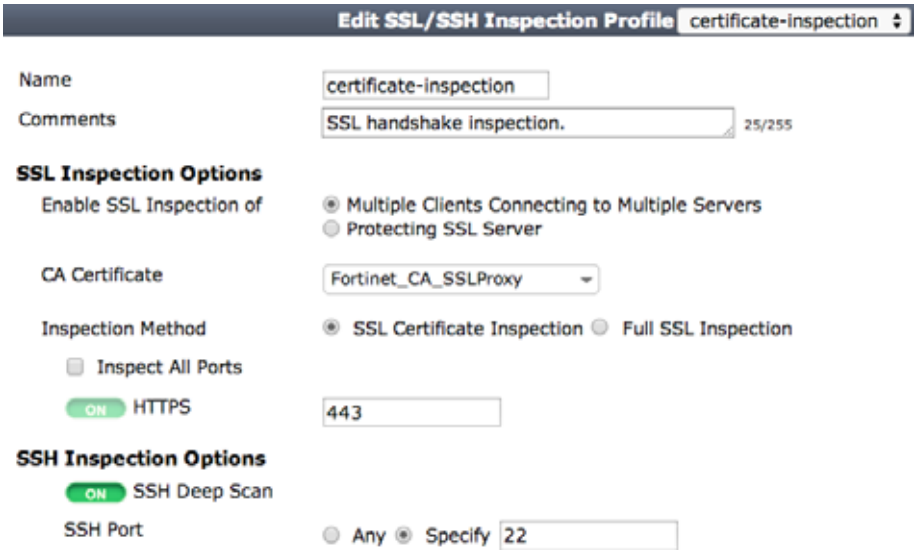



**Figura 1.33. Verificación de la inspección SSL[34].**

[34] En inglés, Secure Sockets Layer.

El objetivo inicial del diseño del protocolo SSL fue proteger las conexiones entre clientes y servidores web con el protocolo HTTP. Esta protección debía permitir al cliente asegurarse que se había conectado al servidor auténtico, y enviarle datos confidenciales, como por ejemplo un número de tarjeta de crédito, con la confianza que nadie más que el servidor sería capaz de ver estos datos. Las funciones de seguridad, pero, no se implementaron directamente en el protocolo de aplicación HTTP, si no que se optó por introducirlas a nivel de transporte. De este modo podría haber muchas más aplicaciones que hicieran uso de esta funcionalidad.

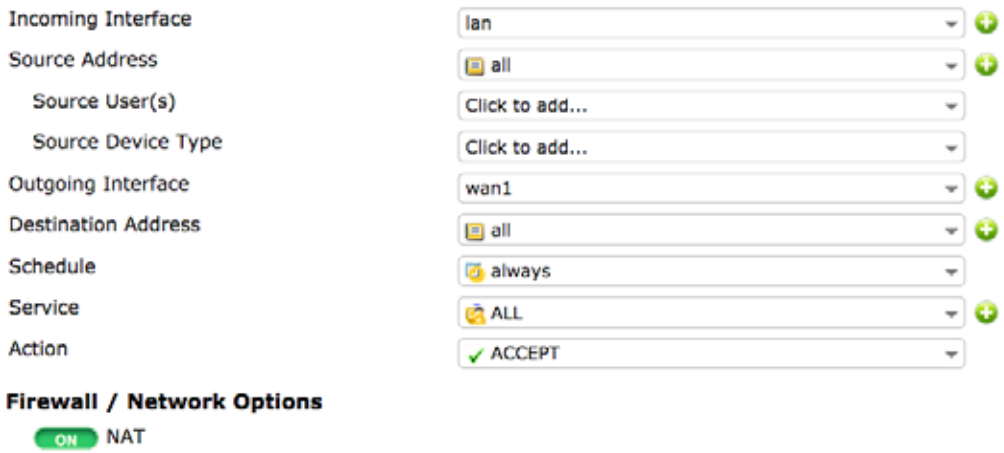



**Figura 1.34. Implementación de la política de seguridad.**

**VPN**

Una red privada virtual (VPN) es una configuración que combina el uso de dos tipos de tecnologías:

- Las tecnologías de seguridad que permiten la definición de una red privada, es decir, un medio de comunicación confidencial que no puede ser interceptado por usuarios ajenos a la red corporativa.

- Las tecnologías de encapsulamiento de protocolos que permiten que, en lugar de una conexión física dedicada para la red privada, se pueda utilizar una infraestructura de red pública, como Internet, para definir por encima de ella una red virtual.

Por tanto, una VPN es una red lógica o virtual creada sobre una infraestructura compartida, pero que proporciona los servicios de protección necesarios para una comunicación segura, que es lo que buscamos.

Dependiendo de la situación de los nodos que utilizan esta red, podemos considerar tres tipos de VPN:

- **VPN entre redes locales o intranets.** Este es el caso habitual en que una empresa dispone de redes locales en diferentes sedes, geográficamente separadas, en cada una de las cuales hay una red privada o intranet, de acceso restringido a sus empleados. Si interesa que desde una de sus sedes se pueda acceder a las intranets de otras sedes, se puede usar una VPN para interconectar estas redes privadas y formar una intranet única.

- **VPN de acceso remoto.** Cuando un empleado de la empresa quiere acceder a la intranet des de un ordenador remoto, puede establecer una VPN de este tipo entre este ordenador y la intranet de la empresa. El ordenador remoto puede ser, por ejemplo, un PC que el empleado tiene en su casa, o un ordenador portátil des del cual se conecta a la red de la empresa cuando está de viaje.

- **VPN extranet.** A veces, a una empresa le interesa compartir una parte de los recursos de su intranet con determinados usuarios externos, como por ejemplo proveedores o clientes de la empresa. La red que permite estos accesos externos a una intranet se llama extranet, y su protección se consigue mediante una VPN extranet.

A cada uno de los tipos de VPN que acabamos de ver le suele corresponder una configuración específica.

En las VPN entre intranets, la situación más habitual es que en cada intranet hay una **pasarela VPN**, que conecte la red local con Internet. Esta pasarela se comunica con la de las otras intranets, aplicando el cifrado y las protecciones que sean necesarias a las comunicaciones de pasarela a pasarela a través de Internet. Cuando los paquetes llegan a la intranet de destino, la pasarela correspondiente los descifra y los reenvía por la red local hasta el ordenador que los tenga que recibir.

De esta manera se utiliza la infraestructura pública de Internet, en lugar de establecer líneas privadas dedicadas, que supondrían un coste más elevado. También se aprovecha la fiabilidad y redundancia que proporciona Internet, ya que si una ruta no está disponible siempre se pueden encaminar los paquetes por otro camino, mientras que con una línea dedicada la redundancia supondría un coste aún más elevado.

En las VPN de acceso remoto, a veces llamadas VPDN, un usuario se puede comunicar con una intranet a través de un proveedor de acceso a Internet, utilizando tecnología convencional como por ejemplo a través de un módem ADSL. El ordenador del usuario ha de disponer de software **cliente VPDN (***Virtual Private Dial Network)*.

Para comunicarse con la pasarela VPN de la intranet y llevar a cabo la autenticación necesaria, el cifrado, etc. De este modo también se aprovecha la infraestructura de los proveedores de Internet para el acceso a la intranet, sin necesidad de llamadas a un módem de la empresa, que pueden llegar a tener un coste considerable.

El caso de las VPN extranet puede ser como el de las VPN entre intranets, en que la comunicación segura se establece entre pasarelas VPN, o bien como el de las VPN de acceso remoto, en que un cliente VPN se comunica con la pasarela de la intranet. La diferencia, pero, es que en este caso normalmente el control de acceso es más restrictivo para permitir solamente el acceso a los recursos autorizados.

La definición de una red virtual lleva a cabo mediante el establecimiento de **túneles**, que permiten encapsular paquetes de la red virtual, con sus protocolos, dentro de paquetes de otra red, que normalmente es Internet, con su protocolo, es decir IP.

Para la comunicación entre las distintas intranets, o entre el ordenador que accede remotamente y la intranet, se pueden utilizar los protocolos que sean más convenientes. Los paquetes de estos protocolos, para poderlos hacer llegar a su destino a través de Internet, se pueden encapsular en datagramas IP, que dentro suyo contendrán los paquetes originales. Cuando lleguen a su destino, se desencapsulan estos datagramas para recuperar los paquetes con el formato "nativo" del protocolo correspondiente.

Hay protocolos que pueden ser utilizados para establecer los túneles, dependiendo del nivel de la comunicación al cual se quiera realizar la protección.

**Túneles a nivel de red.** El protocolo utilizado en la gran mayoría de configuraciones VPN es IPsec en modo túnel, generalmente con ESP para cifrar los datos, y opcionalmente con AH para autenticar los paquetes encapsulados. Las pasarelas VPN son, en este caso, pasarelas seguras IPsec.

**Túneles a nivel de enlace.** En el caso de las VPN de acceso remoto o VPDN, existe la posibilidad de encapsular tramas PPP, que son las que transmite normalmente un cliente VPN de este tipo, sobre datagramas IP.

**Túneles a nivel de transporte.** El protocolo SSH (Secure Shell), como veremos en el módulo de aplicaciones seguras, ofrece la posibilidad de redirigir puertos TCP sobre un canal seguro, que podemos considerar como un túnel a nivel de transporte. Des de este punto de vista, también se podría considerar una conexión SSL/TLS como un túnel a nivel de transporte que proporciona confidencialidad y autenticación. Habitualmente, este último tipo de túnel no sirve para cualquier tipo de tráfico si no solamente para datos TCP, y por tanto no se considera parte integrante de una VPN.

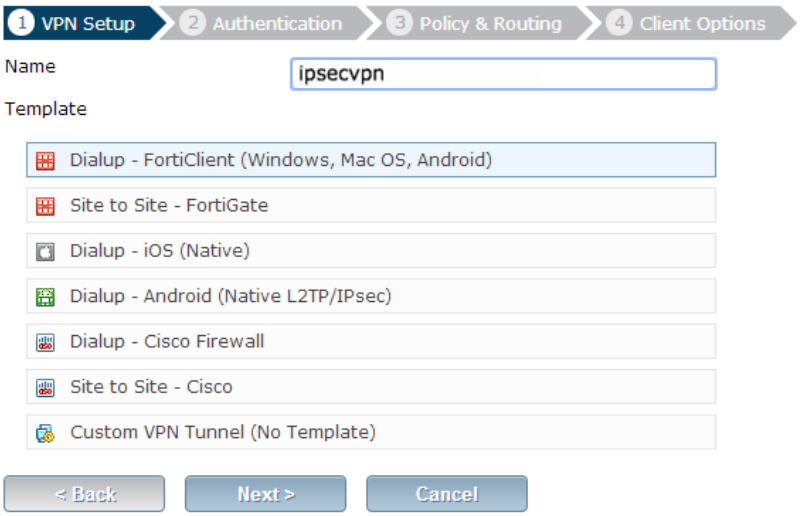



**Figura 1.35. Implementación de VPN en FortiGate.**

# Resultados

**Realizando pruebas de conectividad**

Observamos que al navegar por Internet mediante cualquier ordenador que este dentro de la red corporativa, se le pedirá la autenticación, eso se hace a través de un usuario y contraseña, cabe mencionar que por causas de privacidad de la empresa solo implementamos ejemplos y la autenticación real no se ve plasmada en imágenes de este reporte.

Introduciremos las credenciales de autenticación, esta es una forma de referirnos que cada usuario cuenta con un nombre de usuario y contraseña. Es por eso que para entrar al sistema usaremos el ejemplo de *dprince* como Username (cuenta), para poder acceder.

Con esto controlamos el acceso a los usuarios implementamos políticas de seguridad y verificamos la identidad de las personas o dispositivos que son los autorizados para ver información, compartirla, modificarla.


**Figura 2.1. Autenticación de usuarios.**

| Date/Time | User | Device | Destination | Action |
|---|---|---|---|---|
| 09:10:21 | | iPhone | 208.91.112.53 | deny |
| 09:10:21 | | Mac Mini | 157.55.56.159 | deny |
| 09:10:21 | | Mac Mini | 111.221.74.30 | deny |
| 09:10:21 | | Mac Mini | 111.221.77.159 | deny |
| 09:10:21 | | iPhone | 208.91.112.52 | deny |
| 09:10:20 | | iPhone | 208.91.112.53 | deny |
| 09:10:20 | | iPhone | 208.91.112.53 | deny |
| 09:10:19 | | Mac Mini | 157.55.56.159 | deny |
| 09:10:19 | | Mac Mini | 157.56.52.30 | deny |
| 09:10:17 | | iPhone | 208.91.112.52 | deny |
| 09:10:17 | dprince | Mac Mini | 54.231.0.33 (s3-1-w.amazonaws.com) | accept |
| 09:10:16 | dprince | Mac Mini | 54.231.0.33 (s3-1-w.amazonaws.com) | accept |
| 09:10:16 | dprince | Mac Mini | 54.231.0.33 (s3-1-w.amazonaws.com) | accept |
| 09:10:15 | dprince | Mac Mini | 64.94.107.34 (map-pb.quantserve.com.akadns.net) | accept |
| 09:10:15 | dprince | Mac Mini | 174.36.240.82 (api.mixpanel.com) | accept |

**Figura 2.2 Denegación de servicio de teléfonos móviles.**

Podemos denegar el servicio a dispositivos móviles que no queremos en nuestra red corporativa. Creamos registros de las personas y dispositivos autorizados en la figura 2.3, se muestra a los usuarios autorizados para estar dentro de la red corporativa.

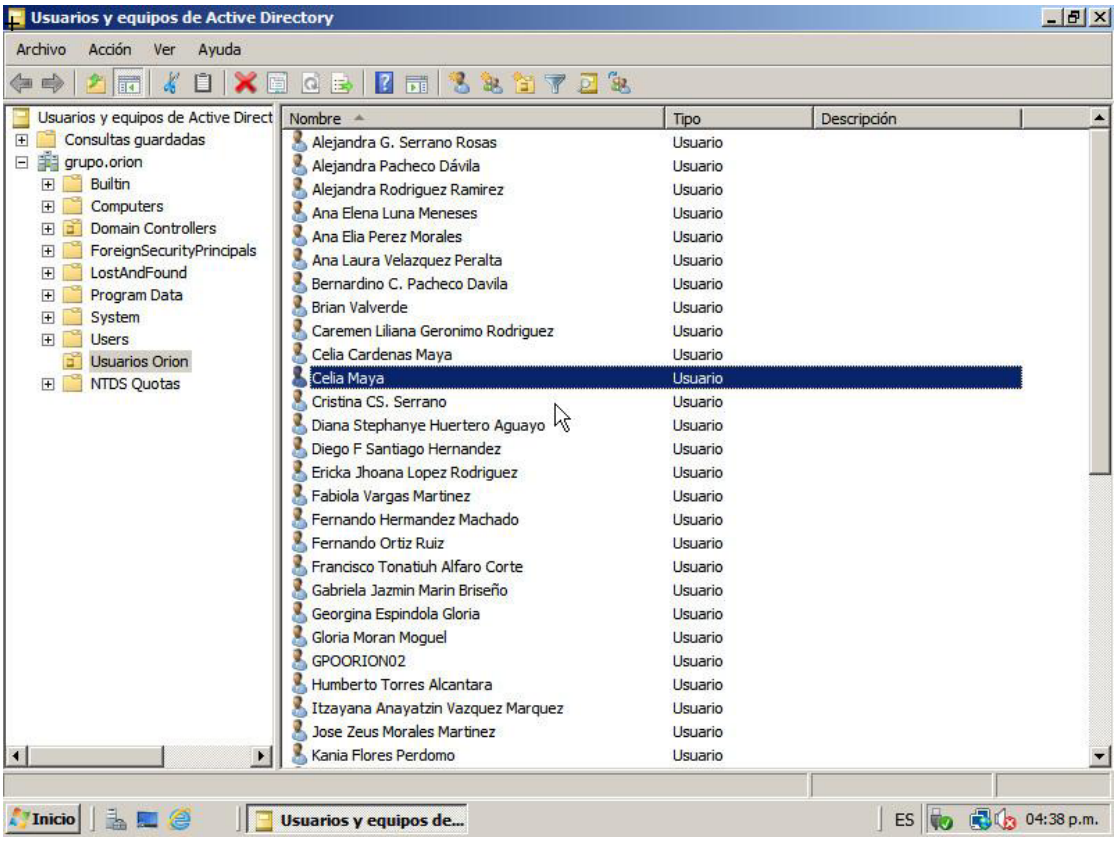



**Figura 2.3. Usuarios autorizados.**

Al aplicar la política de seguridad para el bloqueo especifico de sitios Web, podemos ver como resultado la figura 2.1 que muestra el bloqueo.

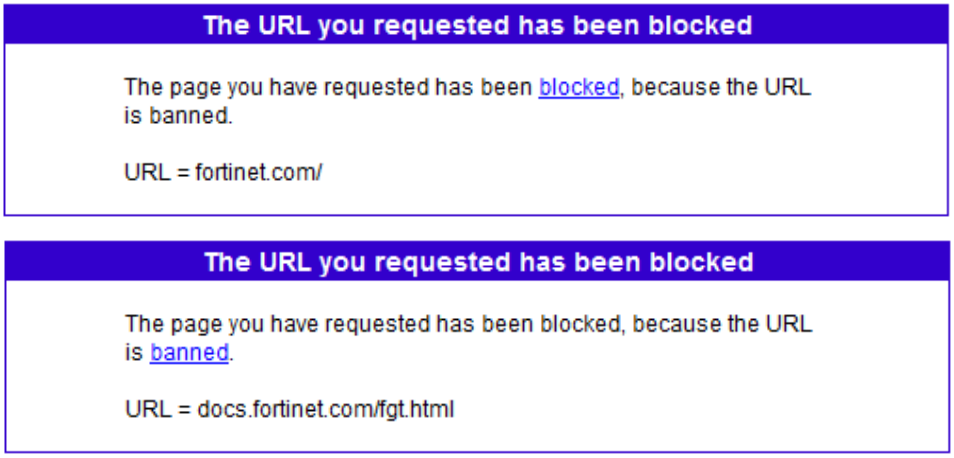



**Figura 2.4. Bloqueo especifico de sitios Web.**

Podemos visualizar que el sitio *www.fortinet.com* como el sitio *docs.fortinet.com* están bloqueados, lo cual nos hace ver que podemos hacer lo mismo para otros sitios no deseados.
Al aplicar la política de seguridad que bloquea el acceso el uso de *streaming* y protocolos *HTTPS* y *HTTP*, podemos ver que los resultados son contundentes y lo podemos visualizar en la figura 2.2.

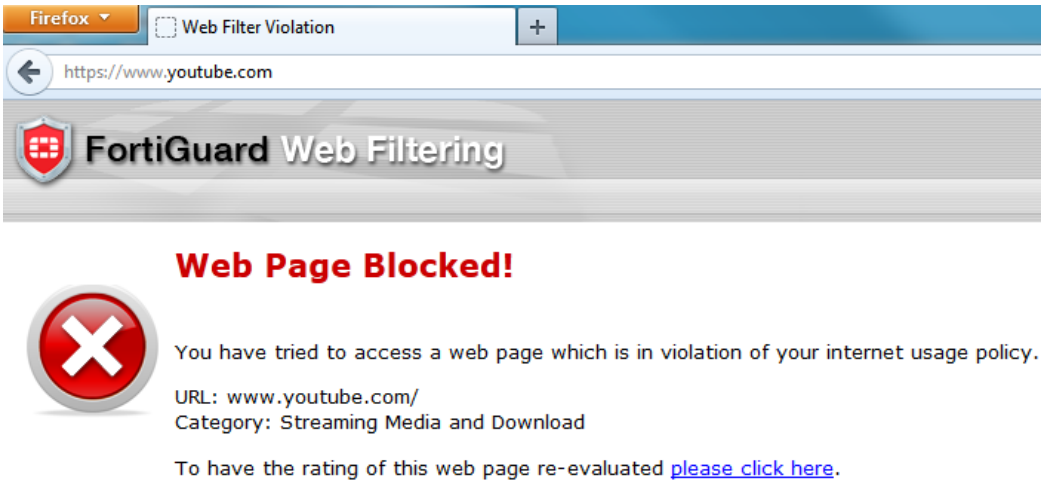



**Figura 2.5. Pagina Web bloqueada.**

Podemos ver el bloqueo a la página Web de Facebook, esto nos ayuda a un mejor rendimiento del usuario.


**Figura 2.6. Bloqueo de Facebook 1**

Cabe mencionar que podemos bloquear cualquier otro sitio Web que la empresa no desee accesar o que sus usuarios no debe de ver por políticas de seguridad internas que en posteriores acuerdos se establezcan.


**Figura 2.7. Bloqueo de Facebook 2**

## Análisis y discusión de resultados

Los resultados obtenidos garantizaron la procedencia de la información (autenticación), marcaron un límite y control de acceso a los elementos de la red corporativa, servicios y aplicaciones (control de acceso), la información solo es accesible por las entidades, sistemas o personas autorizadas (confidencialidad de los datos). Garantizamos que toda la información fluyera desde una fuente hacia un destino (comunicación segura), esta información no ha sido modificada o corrompida de manera alguna, desde su transmisión hasta su recepción (integridad de los datos), todos los elementos de red, los servicios y aplicaciones, se mantienen disponibles para todos los usuarios legítimos (disponibilidad) y sobre todo la información se mantiene como privada (privacidad).

Negar el servicio de páginas Web nos ayudara ahora y en un futuro a contrarrestar todas aquellas amenazas que intentan entrar a nuestra red corporativa. Es importante mencionar que estos ejemplos mostrados en este reporte final solamente se mencionan y se pretende ver cómo es que se deniega el servicio de cualquier página Web, partiendo de esta idea podemos negar el servicio a todas aquellas amenazas o ataques. Lo mostrado en este trabajo, es un estudio y aplicación de políticas de seguridad que a simple vista se vean sencillos pero la dificultad radica en la organización y el tomar las decisiones correctas y que se adecuen a la empresa para un mejor funcionamiento.

# Conclusiones

Todo esto nos llevó a una mejor comunicación interna y una mejor gestión centralizada de toda la información, nos ayudó a controlar los elementos de software y de hardware para garantizar el intercambio de información y ofrecer servicios de seguridad confiables.

FortiGate focaliza las decisiones de seguridad en un único punto de choque, tratando de rechazar cualquier conexión que no esté expresamente permitida. Así pues, la utilización de FortiGate supone una barrera de control que mantendrá la red protegida de todos aquellos accesos no autorizados, actuando como un punto central de control y facilitando las tareas de administración.

Por otro lado, por el hecho de situarse en un punto intermedio, FortiGate ofrece otras funciones de seguridad interesantes como podrían ser la monitorización de las conexiones de red, el análisis de contenidos, la realización de controles de autenticación adicionales, la construcción de redes privadas virtuales, etc. También pueden realizar funciones no relacionadas directamente con la seguridad de la red, como la traducción de direcciones IP (NAT), la gestión de servicios de red, el control del ancho de banda, etc.

Finalmente, debemos tener presente que FortiGate es únicamente un mecanismo de prevención y que no son una solución única para solventar todos los problemas de seguridad de una red conectada a Internet.

FortiGate no podrán proteger nunca a la red de aquellos ataques que se produzcan en su interior y es posible que un atacante externo pueda ser ayudado por un usuario interno para colaborar en un posible ataque.

Tampoco podrán evitar ataques contra servicios con acceso global, ni podrán proteger a la red contra la transferencia de aplicaciones maliciosos (virus, gusanos, etc.) Sería impracticable la utilización de un dispositivo que se dedicara a analizar todo el tráfico que circula a través suyo. Por este motivo, serán necesarios mecanismos de protección adicionales.

- **Prevención y protección.** Mediante la instalación de sistemas cortafuegos y de mecanismos criptográficos pudimos garantizar la privacidad y la integridad de la información en las comunicaciones, será posible llegar a conseguir un primer nivel de prevención y de protección contra la mayor parte de los ataques que hemos visto.

- **Autenticación.** La autenticación es posiblemente una de las necesidades más importantes, dado que el hecho de conseguir privacidad e integridad no tendría ningún sentido si no se garantizara la identificación del destinatario. Mediante la utilización de protocolos criptográficos de autenticación fuerte fue posible garantizar esta necesidad.

- **Detección y respuesta.** Así como los elementos anteriores los hemos identificado como básicos e imprescindibles para poder ofrecer un nivel de seguridad mínimo, fue necesaria la utilización de mecanismos complementarios para detectar los ataques que no se hayan podido evitar y tomar las acciones adecuadas para neutralizarlos.

Tenemos que recordar siempre que la seguridad no es un producto, es un proceso constante que se debe ir buscando, por medio de revisiones constantes de nuestras políticas de seguridad, de tal manera que cada día respondan favorablemente ante los nuevos retos que plantea la seguridad en redes de datos.

Nunca podremos mantener una seguridad al máximo solamente podremos aproximarnos a un nivel óptimo, principalmente porque cada día que se avanza en la creación de nuevas tecnologías de la información se crean o existen nuevas vulnerabilidades, lo único que podemos hacer es minimizar esos ataques o amenazas y erradicarlas, aunque sabemos de antemano que esto es incierto. Se debe estar actualizado e informado constantemente de las nuevas herramientas que existen para una seguridad de calidad.

# Referencias bibliográficas

[1] Andrew S. Tanenbaum, "Redes de computadoras", cuarta edición, pp. 1, 2003.

[2] Cheswick, W.R.; Bellovin, S.M.; Rubin, A.D.(2003). Firewalls and Internet Security: Repelling the Wily Hacker. (5a ed.): Addison-Wesley Professional Computing.

[3] Oppliger, R. (2000). Security technologies for the Word Wide Web. 1a ed.: Artech House.

[4] Menezes, J.; van Oorschot, P.C.; Vanstone, S.A. (2001). Handbook of Applied Cryptography. (5a ed.): CRC Press.

[5] Anonymous (1998). Maximum Security: A Hacker's Guide to Protecting Your internet Site and Network. Sams.

[6] Northcutt, S. (2000). Network Intrusion Detection. An analyst's handbook. New Riders.

[7] Scambray, J.; McClure, S.; Kurtz, G. (2001). Hacking Exposed: Network security secrets and solutions, 2nd ed. Osborne-McGraw Hill.

[8] Siles Peláez, R. (2002). Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados.

[9] Verdejo Álvarez, G. (2003). Seguridad en redes IP. Universidad Autónoma de Barcelona.

[10] Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. A. (1996). *Handbook of Applied Cryptography.* Boca Raton: CRC Press.

[11] Stallings, W. (2003). *Cryptography and Network Security, Principles and Practice, 3rd ed.* Upper Saddle River: Prentice Hall.

[12] Yuan, R.; Strayer,W. T. (2001). *Virtual Private Networks, Technologies and Solutions.* Boston: Addison-Wesley.

# Apéndice

**Address Resolution Protocol (ARP):** protocolo de la familia TCP/IP que asocia direcciones IP a direcciones MAC.

**ARP:** ver *Address Resolution Protocol*.

**Denegación de servicio (DoS):** ataque que hace una apropiación exclusiva de un recurso o servicio con la intención de evitar cualquier acceso a terceras partes. En inglés, *deny of service*.

**Desbordamiento de *buffer*:** posibilidad de corromper la pila de ejecución para modificar el valor de retorno de una llamada a función y provocar la ejecución de código arbitrario.

**DoS:** ver *Denegación de servicio*.

**Huella identificativa:** información muy precisa que permite identificar un sistema o una red en concreto. En inglés, *fingerprinting*.

**Escáner de vulnerabilidades:** aplicación que permite comprobar si un sistema es vulnerable a un conjunto de deficiencias de seguridad.

**Exploit:** aplicación, generalmente escrita en C o ensamblador, que fuerza las condiciones necesarias para aprovecharse de un error de programación que permite vulnerar su seguridad.

**Exploración de puertos:** técnica utilizada para identificar los servicios que ofrece un sistema.
**Explotación de un servicio:** actividad realizada por un atacante para conseguir una escalada de privilegios, abusando de alguna deficiencia del servicio o del sistema.

**Fingerprinting:** ver *Huella identificativa*.

**Firewall:** ver *Cortafuegos*.

**Fragmentación IP:** proceso de división de un datagrama IP en fragmentos de menor longitud.

**Internet Control Message Protocol (ICMP):** protocolo encargado de realizar el control de flujo de los datagramas IP que circulan por la red.

**ICMP:** ver *Internet Control Message Protocol*.

**Internet Protocol (IP):** protocolo para la interconexión de redes.

**IP:** ver *Internet Protocolo*.

**IP flooding:** ataque de denegación de servicio basado en una saturación de la red mediante la generación masiva de datagramas IP.

**Maxim Transfer Unit (MTU):** medida máxima de un datagrama IP dentro de una red.

**MTU:** Ver *Maxim Transfer Unit*.

**Requests for Comments:** conjunto de documentos técnicos y notas organizativas sobre internet.

**Reensemblado IP:** proceso de reconstrucción de un datagrama IP a partir de sus fragmentos.

**RFC:** Ver *Requests for Comments*.

**Rootkit:** recopilación de herramientas utilizadas en un ataque de intrusión para garantizar la ocultación de huellas, garantizar futuras conexiones, realizar otros ataques al sistema, etc.

**Shellcode:** código ensamblador inyectado en memoria que un *exploit* tratará de ejecutar.

**Sniffer:** aplicación que intercepta toda la información que pase por la interfaz de red a la que esté asociado.

**SYN Flooding:** ataque de denegación de servicio que se basa en no complementar intencionadamente el protocolo de intercambio de TCP.

**Cortafuegos:** elemento de prevención que realizará un control de acceso para proteger una red de los equipos del exterior (potencialmente hostiles).

**Transmission Control Protocol (TCP):** protocolo de transporte de la arquitectura de protocolos TCP/IP.

**TCP:** ver *Transmission Control Protocol*.

**User Datagram Protocol (UDP):** protocolo de transporte de la arquitectura de protocolos TCP/IP.

**UDP:** ver *User Datagram Protocol*.

**Política de seguridad:** resultado de documentar las expectativas de seguridad de una red, tratando de plasmar en el mundo real los conceptos abstractos de seguridad.

**Túnel:** Asociación entre dos nodos de una red para intercambiarse paquetes de un protocolo determinado, posiblemente con origen y destino final en otros nodos, encapsulados en paquetes del protocolo de comunicación que utiliza la red (típicamente, la red es Internet y el protocolo de encapsulación es IP).

**VPN:** Ver *Red privada virtual*.

***Wireless Transport Layer Security* (WTLS):** Versión del protocolo TLS adaptada a las comunicaciones inalámbricas en un entorno WAP (*Wireless Application Protocol*).

**WTLS:** Ver *Wireless Transport Layer Security*.

**Red privada virtual (VPN):** Red lógica (virtual) definida sobre una red pública, como por ejemplo Internet, y que funciona, mediante túneles, como si fuera una red privada dedicada.