DISEÑO E IMPLEMENTACION DE UN SISTEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE COMERCIALIZADORA INTERNACIONAL OCEANOS S.A.

PAOLA ISABEL TORRES OSORIO

LAURA PATRICIA PATERNINA ALVAREZ

Director

Eduardo Gómez Vásquez
Magister en Ciencias Computacionales

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERIAS

ESPECIALIZACIÓN EN TELECOMUNICACIONES

CARTAGENA DE INDIAS, D. T. Y C

2011

DISEÑO E IMPLEMENTACION DE UN SISTEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE COMERCIALIZADORA INTERNACIONAL OCEANOS S.A.

PAOLA ISABEL TORRES OSORIO

LAURA PATRICIA PATERNINA ALVAREZ

Monografía presentada como registro de aprobación de la Especialización en Telecomunicaciones

Director

Eduardo Gómez Vásquez
Magister en Ciencias Computacionales

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERIAS

ESPECIALIZACIÓN EN TELECOMUNICACIONES

CARTAGENA DE INDIAS, D. T. Y C

2011

Cartagena de Indias, D. T. H. Y C. **18 de Octubre de 2011**

Señores:

Comité de Proyectos de Grado.
Universidad Tecnológica de Bolívar.
Cartagena de Indias, D. T. H. Y C.

Respetados Señores:

Presentamos para su consideración la monografía titulada: DISEÑO E IMPLEMENTACION DE UN SISTEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE COMERCIALIZADORA INTERNACIONAL OCEANOS S.A**.**

Como requisito para optar el titulo de Especialistas en Telecomunicaciones.

Atentamente,

Paola Isabel Torres Osorio
C.C Nº 45.533.169

Laura Patricia Paternina Álvarez
C.C Nº 64.696.874

Cartagena de Indias, D. T. H. Y C. **18 de Octubre de 2011**

Señores:

Comité de Proyectos de Grado.
Universidad Tecnológica de Bolívar.
Cartagena de Indias, D. T. H. Y C.

Respetados Señores:

Presentamos para su consideración la monografía titulada: **DISEÑO E IMPLEMENTACION DE UN SISTEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE COMERCIALIZADORA INTERNACIONAL OCEANOS S.A.** Como requisito para optar el titulo de Especialistas en Telecomunicaciones.

Espero que el contenido y las normas aplicadas cumplan con los requisitos exigidos por esta dirección.

Atentamente,

_____
Eduardo Gómez Vásquez
Magister en Ciencias Computacionales

CONTENIDO

LISTADO DE FIGURAS

LISTADO DE TABLAS

INTRODUCCIÓN

La seguridad informática va adquiriendo una importancia creciente con el aumento del volumen de información importante que se halla en las computadoras distribuidas. En este tipo de sistemas resulta muy sencillo para un usuario experto acceder de forma no autorizada a datos de carácter confidencial.

Toda organización debe estar a la vanguardia de los procesos de cambio. Estas deben disponer de información continua y confiable en el tiempo, esto constituye una ventaja fundamental.

La detección oportuna de fallas y el monitoreo de los elementos que conforman una red de cómputo son actividades de gran relevancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con un esquema capaz de notificarnos las fallas en la red y de mostrarnos su comportamiento mediante el análisis y recolección de tráfico.

La presente monografía propone la apropiación, desarrollo y la implementación de aspectos relacionados con la seguridad perimetral en la red de la entidad C.I Océanos S.A, lo que permitirá a la empresa y a los usuarios de la red, tener una mayor confianza, seguridad y efectividad en los procesos internos.

DESCRIPCION DEL PROBLEMA

La seguridad en los sistemas de comunicaciones no solo es un problema tecnológico sino que se extiende sobre la capacidad y honorabilidad de las personas y eficiencia de los procesos; para minimizar los riesgos de seguridad en las redes de comunicaciones, es imprescindible un servicio profesional especializado y experto, que transforme la defensa en un proceso continuo y dinámico. En la actualidad la entidad C.I OCEANOS S.A, no controla adecuadamente el nivel de seguridad perimetral de la empresa, provocando que los sistemas se hallen susceptibles a ataques informáticos, por consiguiente para la Red se realizará un análisis de la situación actual de la entidad, para luego implementar un diseño de un sistema de seguridad perimetral de tal manera de que se pueda analizar los servicios en su plataforma de red, tomando en cuenta aspectos como la infraestructura, los servicios, los protocolos, las aplicaciones que maneja la red y la forma de acceso al Internet, a la Intranet y a la Extranet. La detección oportuna de fallas y el monitoreo de los elementos que conforman una red de cómputo son actividades de gran relevancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con un esquema capaz de notificar las fallas en la red y de mostrar su comportamiento mediante el análisis y recolección de tráfico.

En conclusión, el problema consiste en abordar los temas fundamentales en el área de seguridad perimetral, a fin de proponer una metodología que facilite el diagnóstico, diseño e implementación de sistemas de seguridad perimetral en la red de comunicación de C.I. OCEANOS S.A.

OBJETIVO GENERAL

- Diseño e implementación de un Sistema de seguridad perimetral, que permita representar el funcionamiento y las soluciones basadas en las directrices necesarias para el desarrollo de políticas que contribuyan con la administración eficiente del sistema, basados en el diagnóstico de la red, criterios de diseño y escenarios de seguridad de C.I OCEANOS S.A.

OBJETIVOS ESPECIFICOS:

- Diseñar un esquema de seguridad perimetral para la entidad C.I. OCEANOS S.A.

- Proveer de una solución de seguridad perimetral integral para la red de datos de la Entidad C.I. OCEANOS S.A, lo que permitirá disponer de un nivel de confianza adecuado ante los riesgos que implican la interconexión de la red de datos a Internet

- Gestionar de manera eficiente y sencilla el conjunto de sistemas, garantizando un acceso rápido y fácil a la información que generan.

JUSTIFICACIÓN

Las amenazas de seguridad que enfrentan las redes de datos en Colombia son suficientes para pensar en las posibles soluciones que disponemos en la actualidad para enfrentar dichas amenazas, esto nos plantea el problema de cuál es la mejor manera para resolver esta situación. Estas intrusiones no deseadas pueden ser detenidas siempre y cuando las organizaciones definan e implementen de una manera clara sus opciones en seguridad perimetral, esto en concordancia con las políticas de seguridad previamente establecidas.

La seguridad en las redes de datos depende directamente de las amenazas a las que estén expuestas, con el acceso a Internet esa posibilidad se incrementa en forma exponencial. El ataque a una red de datos requiere por parte de quien lo realiza de mucho tiempo, conocimiento y paciencia. Curiosamente esas son las mismas características que debe tener quien la defiende, en realidad el perfil del administrador de una red y de un hacker o craker son muy parecidos, solo cambian sus intereses.

El nivel de amenaza de la entidad C.I. Océanos S.A está orientada básicamente a la información con la que cuenta de sus clientes, y cualquier acceso no autorizado o no detectado para llegar a dicha información puede ser de alto riesgo o tener un alto nivel de impacto en la imagen de la Institución.

Por tanto, es indispensable que se establezcan niveles y mecanismos básicos de control y seguridad para proteger la red de datos y la información que circula a través de ella.

En un alto porcentaje las organizaciones colombianas, carecen de profesionales y recursos en el tema de seguridad de redes de datos y por tal razón permanentemente están expuestas tanto a amenazas internas originadas desde el interior de la organización por medio de sus empleados, como a amenazas externas originadas por fuera de la organización, esto último se presenta especialmente cuando una organización se interconecta con otras organizaciones o con la Internet; por lo anterior el desarrollo del presente trabajo busca reforzar las políticas de seguridad de la entidad C.I OCEANOS y disminuir los riesgos de

seguridad presentes para los recursos tecnológicos de la organización, fortaleciendo la protección perimetral de la infraestructura tecnológica frente a amenazas de seguridad, a través de un firewall empresarial, sistema de protección de intrusos, el control de la navegación de los usuarios al interior de la organización, control de aplicaciones y la prestación de servicios de acceso seguro a través de VPNs SSL o IPsec.

TIPO DE INVESTIGACION

Se efectuará una investigación descriptiva y documental, dirigida hacia la aplicación de mecanismos de seguridad perimetral sobre la red de datos de C.I OCEANOS S.A, incorporando un dispositivo de seguridad integrado o administrador unificado en la plataforma tecnológica de la entidad.

1. FUNDAMENTOS TEÓRICOS DE SEGURIDAD EN REDES

Con el avance tecnológico experimentado en los últimos años, se han abierto nuevas formas de comprender al mundo, ya que la interconexión a diferentes redes y sistemas, permite la exploración de nuevos espacios fuera de los límites de una organización, lo cual conlleva al aparecimiento de nuevas amenazas inherentes a la expansión de una red aislada a una red compartida.

La seguridad de la información es un aspecto primordial en un sistema de red moderno, pero por ser considerado de forma errónea como un factor que no influye directamente en la productividad del sistema, no se proporciona la atención adecuada ni los recursos necesarios a esta labor.

Debido a que los datos constituyen recursos intangibles, el valor de los mismos gira en función de la importancia relativa que tienen para cada individuo, institución, empresa u entidad pertinente. Pero más allá del valor que alguien puede dar a la información, el problema real es el mal uso de la misma, ya que al exponerse a la red mundial puede ser interceptada o almacenada para realizar delitos informáticos y causar pérdidas económicas.

La inseguridad informática no se concentra solamente en el Internet, sino en toda forma de ataque electrónico como los accesos no autorizados, virus, falsificación y robo de información, violando las principales reglas de seguridad como lo es la integridad, privacidad y autenticidad.

A causa de los diferentes peligros a los que se exponen en la actualidad los sistemas informáticos, se considera necesario procedimientos que permitan el buen uso de recursos y contenidos, para garantizar la continuidad de operación y la seguridad de la información.

La seguridad es algo que comienza y termina en las personas, las mismas que son un componente importante dentro de un sistema; por tal motivo es importante inculcar los conceptos, usos y costumbres del manejo adecuado de los recursos informáticos a los usuarios; sin embargo esto requiere tiempo y esfuerzo.

1.1 SEGURIDAD INFORMÁTICA

Los sistemas de información y los datos almacenados son uno de los recursos más valiosos con los que puede contar cualquier organización. La necesidad imperante del flujo de información y el traslado de recursos de un sitio a otro hace que aparezcan vulnerabilidades que ponen en riesgo la seguridad de la infraestructura de comunicación y toda la información que contienen sus nodos. Proteger la información y los recursos tecnológicos informáticos es una tarea continua y de vital importancia que debe darse en la medida en que avanza la tecnología, ya que las técnicas empleadas por aquellos que usan dichos avances para fines delictivos aumentan y como resultado los atacantes son cada vez más numerosos, mejor organizados y con mejores capacidades. Las amenazas que se pueden presentar provienen tanto de agentes externos como de agentes internos, por eso es importante que toda organización que quiera tener una menor probabilidad de pérdida de recursos por causa de los ataques a los que se expone defina una estrategia de seguridad fundamentada en políticas que estén respaldadas por todos los miembros de la organización.

Se debe considerar que la violación de la seguridad en un sistema podría llegar a afectar gravemente las operaciones más importantes de la empresa y dejarla expuesta a la quiebra.
En este sentido y considerando la alta volatilidad y especialidad de las vulnerabilidades, es necesario establecer programas de verificación y validación de las prácticas de seguridad informática con el fin de persuadir a los intrusos y valorar el estado del arte de esta función en la organización, es decir, ejercicios como pruebas de vulnerabilidades, auditorías de seguridad y evaluaciones de seguridad deben ser parte integral de la manera como la organización estima su nivel de riesgo real, frente a acciones intrusitas de terceros o internos sobre los sistemas de información.

Las tendencias en inseguridad informática son tan variantes como las relaciones que se presenten entre los diferentes elementos que la componente: tecnología, procesos o individuos, por tanto la única predicción válida en inseguridad de la información se concentra más que todo en algunas vulnerabilidades tecnológicas, otros en procedimientos (cuando se roban o pierden elementos de Sistemas tecnología) o en comportamientos no deseados de los individuos frente a la información y sus usos autorizados.

El futuro de la inseguridad exige de los profesionales de la seguridad un constante estudio de los riesgos y relaciones cambiantes del entorno de negocios para mantener una posición vigilante frente los movimientos de los intrusos, pues "a la hora que menos pensemos llega el ladrón y nos sorprende". En este sentido, es preciso diseñar y proponer sistemas de inteligencia informática para aprender sobre los indicadores ambientales y tecnológicos que permitan visualizar cambios o vectores de ataques que mantengan nuestra motivación para continuar aprendiendo de la esencia misma de la protección de los activos: la inseguridad.

La seguridad de la información debe estar orientada a garantizar o mantener tres cualidades propias de esta última: disponibilidad, integridad y confidencialidad. En algunos entornos, especialmente en los dedicados a la Administración Electrónica, interesan, además, otros aspectos muy importantes de las transacciones on-line como son la autenticidad o la trazabilidad.

Por consiguiente se hace imprescindible, tomar conciencia de los riesgos a través de medidas a todos los niveles (legislativas, organizativas y técnicas) así como de la implantación de herramientas técnicas de seguridad (anti-virus, firewalls, software para autenticación de usuarios o para cifrado de la información) y del empleo de productos certificados, de inspecciones o auditorías de seguridad, etc.

Al abordar el tema de Seguridad Informática, se debe tener muy en claro que no existe una seguridad en términos absolutos. Sólo se pueden reducir las oportunidades de que un sistema sea comprometido o minimizar la duración y daños provocados a raíz de un ataque.

Al tratar el asunto, se está considerando que se encuentran en riesgo tres elementos:

a) Los datos: información guardada en las computadoras.
   Ellos tienen tres características a proteger:
- Confidencialidad
- Integridad
- Disponibilidad

b) Los recursos: el equipamiento en sí mismo
c) La reputación

Una de las actividades iniciales es el Análisis de riesgos, para lo cual, se debe realizar un modelado de amenazas. Se trata de una actividad de carácter recurrente. Un riesgo es una combinación de activos, vulnerabilidades y atacantes.

Elementos

- Lo que se quiere proteger: los activos
- Objetivos de seguridad: niveles y tipos de protección que requiere cada activo.
    - **Confidencialidad de los datos:** se garantiza que la información es accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
    - **Integridad de datos y sistemas:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
    - **Disponibilidad del sistema/red:** se garantiza que las personas usuarias autorizadas tengan acceso a la información y recursos relacionados con la misma toda vez que se requiera.
- Amenazas
- Motivos: financieros, políticos, personales/sicológicos.

Hay que tener en consideración que los ataques pueden ser direccionados a:

- Servidores
- Red
- Aplicaciones web

Estrategias generales para minimizar los ataques:

- Observar el principio del menor privilegio
- Defensa a fondo o en profundidad
- Redundancia: utilizar más de un mecanismo de seguridad
- Punto de choque
- Eslabón más débil
- Postura de falla segura
- Definición y uso de políticas y procedimientos
- Mantenerse informado/actualizado

SERVIDORES

Ataques a servidores

- **Servidores Web:** Utilización de vulnerabilidades conocidas que posibilitan ejecutar código arbitrario, acceso no autorizado a archivos o denegación de servicio (DoS).
- **Servicios de administración remota:** Telnet, SSH, Microsoft Terminal Server.
- **Servicios de administración de contenidos:** FTP, SSH/SCP, etc.
- **Servidores de Nombres:** ataque al servidor, modificación de zonas, *cache poisoning*, etc.
- **Servidor de correo electrónico:** intercepción de datos confidenciales; *spam*; propagación de virus, apropiación del servidor de correo para lanzar otros tipos de ataque, etc.
- **Servidor de bases de datos:** problemas tales como compromiso del servidor (por ej. por desbordamientos de búfer); robo de datos; corrupción de datos o pérdida, denegación de servicio (DoS), etc.
- **Navegadores:** fallas que permiten ejecutar código arbitrario en el cliente, controlando parcial o totalmente el equipo: Cross site scripting, manipulación de cookies, robo de código fuente, etc.

Es el estudio y aplicación de métodos y medios de protección para los sistemas de información y comunicación, contra revelación, modificación o destrucción de la información; o contra fallos de proceso, almacenamiento o transmisión que se lleva a cabo de forma accidental o intencional.

1.2 AMENAZAS

Es cualquier cosa que pueda alterar la operación, funcionalidad, integridad o disponibilidad de una red o sistema.

- **Formas de la Amenaza**
  - ✓ ***Interrupción:*** Provoca que un objeto del sistema se pierda, quede inutilizable o no disponible, su detección es inmediata.
  - ✓ ***Interceptación:*** Cuando un elemento no autorizado consigue acceso a un elemento del sistema, su detección es difícil a veces no deja huellas.

- ✓ ***Modificación:*** Cuando a más de conseguir el acceso, consigue modificar un objeto del sistema con el fin de obtener beneficios. Se considera también como la destrucción del objeto si el mismo queda inutilizable.
- ✓ ***Generación:*** Cuando se crea o modifica un objeto con el fin de asemejarse a uno original, para pretender engañar al sistema, constituyen delitos de falsificación y su detección es difícil.

➢ **Tipos de Amenaza**

- ✓ **Amenaza Pasiva:** Atenta contra la confidencialidad de la información sin cambiar el estado del sistema. Consiste en el acceso no autorizado a la información protegida, mediante la escucha o monitoreo con el fin de obtener la información transmitida y así averiguar o utilizar información del sistema, sin afectar los recursos del mismo.

  Estos ataques son muy difíciles de detectar, ya que no alteran los datos ni la funcionalidad del sistema; para impedir el éxito de estos se puede utilizar cifrado de datos. La defensa ante estos ataques se orienta a la prevención mediante cifrado, antes que a la detección.

- Divulgación del contenido. Consiste en publicar información de carácter sensible o confidencial.

- Análisis de tráfico. Consiste en estudiar la información (plana / cifrada) transmitida, para averiguar la naturaleza de la comunicación.

Un atacante podría observar el patrón de los mensajes o las cabeceras de paquetes y así determinar la localización e identidad de los computadores, o la longitud y frecuencia de los mensajes; aun cuando la información viaje cifrada podría calcular la cantidad de tráfico que circula por la red o que entra y sale de un sistema, para determinar la naturaleza de la comunicación.

- **Amenaza Activa:** Provoca un cambio no autorizado y deliberado del estado del sistema; intenta alterar los recursos del sistema o influir en su normal funcionamiento; busca modificar el flujo de datos o crear flujos falsos.

  Es difícil impedirlos de forma absoluta, para lograrlo sería necesario protección física permanente de todos los recursos y rutas de comunicación. La clave es la detección de ataques y la recuperación de interrupciones o retardos causados por estos; además la detección puede contribuir con la prevención.

  - ***Enmascaramiento.*** Consiste en suplantar a una entidad, mediante la captura de secuencias de autenticación, y retransmisión de las mismas; con el fin de obtener privilegios adicionales dentro del sistema.
  - ***Retransmisión.*** Consiste en la captura de datos y su posterior retrasmisión para provocar efectos no autorizados.
  - ***Modificación de mensajes.*** Consiste en la modificación, retraso, reordenamiento de algún fragmento de un mensaje legítimo con el fin de provocar efectos no autorizados.
  - ***Denegación de Servicio.*** Consiste en impedir el normal funcionamiento de equipos, redes y servicios de comunicación. Interrupción de un servidor o de toda una red, al deshabilitar el servidor o sobrecargarlo para degradar su rendimiento. Suprimir todos los mensajes dirigidos a un destino concreto, entonces si no hay petición no hay respuesta.

- **Origen de las Amenazas**
  - ***Humanas:*** Las personas son el eslabón más débil en la seguridad, ya que está en la naturaleza humana factores como la curiosidad, el bien y el mal que puede afectar a cualquier sistema de seguridad por más sofisticado que este sea.
  - ***Personal.*** Son los integrantes de una organización, los mismos que se supone son confiables, pero pueden comprometer gravemente la seguridad del sistema de forma intencional o accidental; cuando los ataques son intencionados pueden causar efectos extremadamente dañinos, ya que el personal conoce los sistemas y sus debilidades mejor que cualquier persona externa a la organización y es frecuente también los accidentes causados por errores o desconocimiento de las normas básicas de seguridad.

- ***Ex empleados.*** Se trata de personas separadas de la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente para dañarlo por algún hecho que no consideran justo.
- ***Curiosos.*** Son los atacantes más habituales de un sistema; pues las personas son curiosas por naturaleza y con el amplio acceso a la tecnología que se tiene en la actualidad, potencialmente se convierten en profesionales y expertos de sistemas informáticos y telecomunicaciones, así exploran los sistemas en busca de mayores privilegios o accesos de los que ya tienen.
- ***Crackers.*** Son las personas que intentan de forma ilegal romper la seguridad de un sistema por diversión o interés. Su objetivo típico son los sistemas de seguridad media y redes generalmente abiertas. Mediante un escáner de seguridad detectan las vulnerabilidades de los sistemas para finalmente atacarlos.
- ***Hackers.*** Personas con altos conocimientos en informática, que crean programas que permiten eliminar limitaciones o candados y así desproteger programas y evitar pagar licencias de uso o comprarlos.
- ***Terroristas.*** Personas que atacan un sistema con el fin de causar algún tipo de daño.
- ***Intrusos remunerados.*** Constituyen el grupo más peligroso, ya que son personas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, pagados por una tercera parte (empresa de la competencia) para robar secretos o dañar la imagen de la entidad atacada.
- ***Script Kiddie.*** Persona inexperta, generalmente un adolescente que usa programas que descarga de Internet para atacar sistemas.

➢ **Amenazas Lógicas:** Constituyen todo tipo de programas que de una forma u otra pueden dañar un sistema, creados de forma intencional (software malicioso) o errónea (bugs).

- Software incorrecto. Son los errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones, se los llama bugs y son explotados mediante programas llamados exploits.
- Herramientas de seguridad. Son utilizadas para detectar fallos en los sistemas o redes, pero representan un arma de doble filo, ya que un administrador de red puede solucionar las falencias encontradas, mientras que un intruso puede explotar las mismas.

- Malware. Es cualquier software creado con la intención de molestar o dañar el normal funcionamiento de una computadora. Tenemos los virus, spywares, gusanos, etc.

➢ **Amenazas Físicas:** Las catástrofes (naturales o artificiales) son la amenaza menos probable, sin embargo es importante tomar medidas básicas de protección, ya que si se produjeran generarían daños de gran impacto. Como ejemplos de catástrofes tenemos: terremotos, inundaciones, incendios, humo o atentados de baja magnitud.
También existe un subgrupo de catástrofes con posibilidad de ocurrencia mínima, denominados riesgos poco probables, por lo tanto no vale la pena tomar medidas de seguridad contra éstas, ya que el sistema de prevención resultaría costoso e innecesario.

1.3 VULNERABILIDADES

Es una debilidad inherente al diseño, configuración o implementación de una red o sistema, que lo deja susceptible a ataques.

- **Diseño pobre**
  Se presenta en los sistemas hardware y software que contienen fallas de diseño que pueden ser explotadas, es decir que el sistema ha sido creado con huecos de seguridad.
- **Implementación pobre**
  Se presenta en los sistemas configurados incorrectamente y por lo tanto son vulnerables a un ataque; estos tipos de vulnerabilidades son el resultado de desconocimiento, inexperiencia, entrenamiento insuficiente o descuido en el trabajo.
- **Administración pobre**
  Son el resultado de procedimientos inadecuados, controles y verificaciones insuficientes. Las medidas de seguridad no pueden operar en un vacío, necesitan ser documentadas y monitoreadas.

1.4 MECANISMOS

La seguridad informática en las redes y sistemas requiere de un ciclo continuo de protección, detección y respuesta.

- **Mecanismos de Prevención**

  Consiste en cerrar las brechas de seguridad para aumentan la fiabilidad de un sistema durante su funcionamiento normal, previniendo la ocurrencia de violaciones a la seguridad.

- **Mecanismos de autenticación e identificación**

  Permiten identificar entidades del sistema de una forma única para posteriormente autenticarlas (comprobar que la entidad es quien dice ser).

- **Mecanismos de control de acceso**

  Controlan todos los tipos de acceso sobre cada objeto por parte de cualquier entidad del sistema.

- **Mecanismos de separación**

  Se utilizan cuando un sistema maneja diferentes niveles de seguridad, para evitar el flujo de información entre objetos y entidades de diferentes niveles sin la exigencia de una autorización expresa del mecanismo de control de acceso. Tenemos mecanismos de separación física, temporal, lógica y criptográfica.

- **Mecanismos de seguridad en las comunicaciones**

  Se utilizan para garantizar la privacidad e integridad de los datos cuando se transmiten por la red. Algunos de estos mecanismos se basan en la criptografía como el cifrado de clave pública, de clave privada, firmas digitales, etc. Otros utilizan protocolos seguros como SSH, Kerberos, etc.

  Los mecanismos de prevención se detallan más adelante en el subcapítulo Tecnologías de Seguridad Informática.

- **Mecanismos de Detección**

  Son aquellos que se utilizan para detectar violaciones a la seguridad o intentos de violación, ya que si no nos damos cuenta del ataque el daño va a ser mayor. Como ejemplo tenemos los programas de auditoría.

- **Mecanismos de Respuesta**

  Son aquellos que se aplican cuando una violación del sistema se ha detectado, ya que busca minimizar los efectos de un ataque o problema y finalmente retornar al sistema a su modo de trabajo normal. Como ejemplo tenemos las copias de seguridad o el hardware adicional (respaldos).

- **Mecanismo de análisis forense**

  Su objetivo es averiguar el alcance de la violación, las actividades del intruso en el sistema y la puerta utilizada para entrar; así se podrá prevenir ataques posteriores y detectar ataques a otros sistemas de nuestra red.

1.5 MODELOS DE SEGURIDAD

- **Seguridad por Oscuridad**

  Consiste en esconderse o pasar desapercibido para protegerse, así si nadie conoce de la existencia de la red o sistema, entonces éste no estaría sujeto a ataques.
- **Perímetro de defensa**

  Consiste en cercar la red o sistema a proteger, generalmente mediante un firewall que separe la red protegida de la red no confiable.
- **A nivel de red**

  Busca proteger al sistema informático de los ataques de hackers, intrusiones o robo de información en conexiones remotas.
- **A nivel de contenidos**

  Busca proteger al sistema de amenazas como los virus, gusanos, troyanos, spyware, phishing y demás clases de malware, del spam o correo basura y de los contenidos web no apropiados.
- **Defensa en profundidad**

  Es el modelo más robusto y consiste en la protección y monitoreo de cada sistema aisladamente, dotándoles de la capacidad de defenderse por si mismos.

1.6 SEGURIDAD EN EMPRESAS

Las redes y sistemas pertenecientes a empresas teóricamente son las que representan mayores ventajas en lo relativo a su protección ya que suelen ser muy aislables.

Las empresas disponen de una red LAN en el edificio donde están ubicadas, la misma que puede aislarse del exterior mediante un Firewall; pero si se ofrecen servicios hacia el exterior (correo electrónico y web), se pueden situar los servidores en una zona desmilitarizada entre el Router y la red interna. Además se tiene la conexión a Internet que brinda acceso hacia el exterior. Así la idealización de red aislada no sería posible con lo cual nos enfrentaríamos a los problemas de seguridad inherentes a esta apertura.

Las empresas cuentan con varias sucursales separadas geográficamente, para conectarlas tenemos dos opciones, hacerlo mediante una red propia (muy costoso) protegida por los técnicos de la misma compañía o mediante un enlace arrendado a través de una red de propósito general como base de comunicaciones (red telefónica, Internet, etc.), así la protección de la red ya no depende exclusivamente de la propia organización, entonces es indispensable recurrir a VPN (Redes Privadas Virtuales), estableciendo canales de comunicación seguros dentro de redes inseguras.

El personal de las empresas cuenta con estaciones de trabajo móviles, las mismas que potencialmente pueden causar problemas de conectividad y seguridad, ya que una estación móvil puede entrar en contacto con ambientes inseguros y comprometer la información o infectarse, para seguidamente, introducirse en la organización y comprometer la seguridad de la misma.

Finalmente hay que considerar los ataques internos, que puede sufrir la organización por parte del personal propio de la empresa.

1.7 POLÍTICAS DE SEGURIDAD INFORMÁTICA

En la actualidad la gestión de la seguridad es algo crítico para cualquier organización, igual de importante que los sistemas de calidad o las líneas de producto que desarrolla.

Las políticas de seguridad son el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema, que indica lo que está y lo que no está permitido en el área de seguridad durante la operación general del sistema.

Sin una política de seguridad correctamente implantada en la organización no sirven de nada los controles de acceso (físicos y lógicos) implementados en la misma.

1.8 POLÍTICAS Y PROCEDIMIENTOS

Las políticas y procedimientos de seguridad en una red o sistema sirven para asegurar la seguridad de la información, definen los niveles aceptables de seguridad de la información, mediante el planteamiento de aspectos como: ¿qué constituye la seguridad de la información?, ¿por qué es importante? y ¿cómo mantenerla?.

Para determinar el nivel de seguridad adecuado para cierta organización, se debe considerar los elementos de seguridad de la información: confidencialidad, integridad, disponibilidad, autenticación y control de acceso, de acuerdo a los requerimientos de la organización.

- **Políticas de seguridad:** Son el conjunto de reglas y procedimientos que regulan cómo una organización administra, usa, protege y distribuye toda la información que directa o indirectamente le pertenece. Las políticas deben estar orientadas a qué posesiones proteger y por qué necesitan ser protegidos, son amplias en su alcance y son diseñadas para fijar el tono y la dirección. Son documentos que exhiben el ¿qué? y ¿por qué? de la seguridad de la información para una organización, además deben ser simples de entender y fáciles de recordar.

- **Procedimientos de seguridad:** El desarrollo de los procedimientos debe fluir desde las políticas de seguridad, estos deben ser más precisos y detallados, centrarse en las medidas específicas necesarias para proteger las posesiones de la organización. Son documentos que contienen el ¿quién?, ¿cuándo? Y ¿cómo? de la seguridad de la información dentro de una organización.

1.8.1 OBJETIVOS DE LAS POLÍTICAS DE SEGURIDAD

El desarrollo de políticas y procedimientos de seguridad para redes y sistemas de una organización proporciona beneficios directos como prevenir o detectar fraudes o disuadir hackers, también beneficios indirectos como proteger a la organización de potenciales responsabilidades o salvarla de posibles vergüenzas.

- ✓ **Administración de riesgos:** Es necesario identificar los riesgos que enfrenta una organización y desarrollar medidas preventivas y de recuperación para minimizar el impacto de éstos.
- ✓ **Asegurar la continuidad del negocio:** Las políticas y procedimientos deben asegura la reanudación del negocio mediante un esquema apropiado de las acciones necesarias en respuesta a un incidente o desastre.

- ✓ **Definición de responsabilidades, expectativas y comportamientos aceptables:** Para que cualquier política o procedimiento sea eficaz, las personas involucradas con éstas deben entender, qué se requiere de ellas para cumplirlas. El acatamiento de una política se consigue llegando a un acuerdo de, qué constituye el acatamiento. Los empleados necesitan entender sus responsabilidades dependiendo de las circunstancias.

- ✓ **Proteger a la organización de la responsabilidad:** La existencia de políticas y procedimientos son esenciales para demostrar que la organización no aprobó las acciones de un usuario final, o que un empleado actuó o no con la autorización de la organización.

- ✓ **Asegurar la integridad y confidencialidad de la información:** La protección de los recursos informáticos de la organización constituye un componente clave de la seguridad de la información. Sin la integridad de la información la organización no puede tomar decisiones de negocios. Sin la confidencialidad de la información la organización perderá su ventaja competitiva por la pérdida de la información reservada de productos, clientes, compañeros, proveedores, etc.

1.9 TÉCNICAS DE ATAQUES Y PROTECCIONES

1.9.1 AMENAZAS Y ATAQUES

1.9.1.1 Virus

Son una sección oculta y auto-replicable de software, por lo general con una lógica maliciosa, que se propaga mediante la infección, es decir, la inserción de una copia de sí

mismo y convertirse en parte de - otro programa. Un virus no se puede ejecutar por sí mismo, sino que requiere que su programa anfitrión sea ejecutado para lograr que el virus se active.[1]

Un virus informático es un tipo de malware que se propaga de una computadora a otra, dejando infecciones a medida que viaja. Los virus pueden variar en gravedad desde provocar efectos ligeramente molestos a los datos o programas hasta causar condiciones de Denegación-de-Servicio (DoS). Casi todos los virus se unen a un archivo ejecutable, lo que significa que el virus puede existir en un sistema, pero no se activa o es capaz de propagarse hasta que un usuario ejecute o abra el archivo anfitrión o programa malicioso. Cuando el código del anfitrión se ejecuta, el código del virus es ejecutado también. Normalmente, el programa anfitrión sigue funcionando después de ser infectado por el virus. Sin embargo, algunos virus sobrescriben otros programas con copias de sí mismos, que destruye por completo el programa donde se hospeda. Los virus se propagan cuando el software o el documento al que se adjuntan es traslado de un computador a otro a través de la red, un disco, el uso compartido de archivos, o al adjuntar archivos de correo electrónico infectados.

1.9.1.2 Worms – Gusanos

Es un programa de computador que puede funcionar de forma independiente, puede propagar una versión funcional completa de sí mismo en otras máquinas en una red, y puede consumir recursos del computador destructivamente.[2]

Los gusanos son similares a los virus porque realizan copias funcionales de sí mismos y pueden causar el mismo tipo de daño. A diferencia de los virus, que requieren la propagación de un archivo anfitrión infectado, los gusanos son programas independientes y no necesitan la ayuda humana ni un programa anfitrión para propagarse. Para propagarse, los gusanos explotan una vulnerabilidad del sistema objetivo o utilizan algún tipo de ingeniería social para engañar a los usuarios en la ejecución de ellos. Un gusano entra a un computador a través de una vulnerabilidad en el sistema y toma ventaja de archivos de

[1] Definición de Virus. (http://www.sans.org/security-resources/glossary-of-terms/v).
[2] Definición de Worms o gusanos. (http://www.sans.org/security-resources/glossary-of-terms/w).

transporte o de características de transporte de información en el sistema, permitiéndole que viaje sin ayuda.

1.9.1.3 Caballo De Troya

Son aquellos programas de computador que parecen tener una función útil, pero también poseen una función oculta y potencialmente maliciosa que evade los mecanismos de seguridad, a veces mediante la explotación de autorizaciones legítimas de una entidad sistema que invoca el programa.[3]

Este tipo de malware lleva el nombre del caballo de madera que los griegos usaron para infiltrarse en Troya. Es una pieza de software dañino que parece legítimo. Los usuarios suelen ser engañados para cargarlos y ejecutarlos en su sistema. Después de que se activa, se puede conseguir cualquier cantidad de ataques en el anfitrión, desde irritar al usuario (con ventanas emergentes o cambiando el escritorio) hasta dañar al anfitrión (eliminando archivos, recolectando datos, o activando y difundiendo otros tipos de malware, como virus). Los troyanos son también conocidos por crear puertas traseras (back doors) para que los usuarios malintencionados tengan acceso al sistema.

A diferencia de los virus y los gusanos, los troyanos no se reproducen infectando otros archivos ni se auto-replican. Los troyanos se propagan a través de la interacción de los usuarios, al abrir un archivo adjunto de correo electrónico o descargar y ejecutar un archivo desde Internet.

1.9.1.4 Bot

"Bot" se deriva de la palabra "Robot" y es un proceso automatizado que interactúa con otros servicios de red. Los Bots a menudo automatizan tareas y proporcionan información o servicios que de otra manera se llevaría a cabo por un ser humano. Este software se encarga de realizar labores rutinarias del sistema y puede ser utilizado para generar algún tipo de daño cuando se accede a él de forma indebida. Un uso típico de los bots es la recolección de información (tales como los restreadores web – web crawlers) o la interacción automática con la mensajería instantánea (IM), Internet Relay Chat (IRC), u otras interfaces web. También se pueden utilizar para interactuar dinámicamente con sitios web.

[3] Definición de Trojan Horse. (http://www.sans.org/security-resources/glossary-of-terms/t).

Los bots pueden ser usados para el bien o con intenciones maliciosas. Un bot malicioso es un malware que se autopropaga, diseñado para infectar a un anfitrión y conectarse de nuevo a un servidor central o servidores que actúan como un centro de comando y control de toda la red de dispositivos comprometidos o "botnet". Con una botnet (red de zombies), los atacantes pueden realizar ataques tipo inundaciones contra su objetivo o controlarlos remotamente. Además de la capacidad que tiene de auto propagarse como un gusano, un robot puede incluir la capacidad de grabar las pulsaciones del teclado, obtener contraseñas, capturar y analizar paquetes, recopilar la información financiera, lanzar ataques de Denegación de Servicios (DoS) o abrir puertas traseras en la máquina infectada.

Los Bots tienen todas las ventajas de los gusanos, pero son mucho más versátiles en su vector de infección y se modifican con frecuencia en horas de la publicación de publicación de un nuevo exploit. Son conocidos por explotar las puertas traseras que abren los virus y gusanos, lo que les permite acceder a redes que tienen un buen control de perímetro. Los bots rara vez se anuncian con altas tasas de exploración, que dañan la infraestructura de la red, sino que infectan las redes de manera que escapa a la percepción inmediata.

1.9.1.5 Bomba Lógica o de Tiempo

Son básicamente un troyano, con la diferencia de que no es el cliente quien toma la iniciativa de activación, sino ella misma partir de determinada fecha y hora, o número de ejecuciones de la bomba de tiempo, y por reunir determinados requisitos el sistema en su lógica. Son programas independientes que no necesitan de ningún agente externo y carecen de la capacidad para autorreplicarse.

1.9.1.6 Bomba de Correo

Este tipo de malware tiene una filosofía de actuación similar al SPAM, aunque realmente el fin que persigue no es el mismo. Básicamente las bombas de correo son una serie de aplicaciones que tienen como objetivo atacar el buzón de correo de un usuario hasta conseguir la saturación del mismo. Consiguiendo así la denegación de servicio del buzón, y evitando por lo tanto que el atacado pueda enviar o recibir más correo hasta que la amenaza no sea eliminada.

La metodología utilizada, por lo tanto, es el uso de una serie de aplicaciones que se encargan de construir los correos y enviarlos hacia Internet. Una de las medidas de protección contra estos mail bomber consiste en configurar el servidor de correo para que no acepte series de ellos cuando procede de la misma fuente. A pesar de ello aplicaciones más avanzadas son capaces de buscar diferentes pasarelas de correo SMTP desprotegidas para reenviar desde allí los e-mails y aparentar de esta forma que los correos proceden de diferentes orígenes evitando la medida de protección y cumpliendo así el objetivo propuesto. Adicionalmente son capaces de encolar mensajes haciendo posible que estos queden dispersos por Internet. De este modo, aún cuando se realice la tarea de limpieza de la bandeja de entrada, éstos seguirían entrando y por lo tanto colapsando el sistema de correo.

Si por algún motivo el ataque fuera prolongado y lanzado contra un gran número de buzones de correo de un determinado servidor, no se descarta la posibilidad de que se produzca denegación de servicio completa de todo el servidor. Una evolución natural en este tipo de ataque contra servidores se produce no con el envío masivo de correo, sino con el envío de bombas lógicas o gusanos de correo.

La mejor protección contra estas amenazas es la precaución. Hay que desconfiar de aquellos correos de dudosa procedencia o de contenido incierto. Por ejemplo, si recibimos un correo de un amigo con un asunto en inglés tipo Hi!, debemos desconfiar del mismo, o desechar correos con adjuntos si no podemos confirmar su procedencia.

1.9.1.7 Keyloggers

Sin lugar a dudas un virus es peligroso, pero al final de una u otra forma se conoce de su existencia y se puede remediar la situación (o al menos intentarlo). Pero ¿qué pasaría si algo en la máquina estuviera recogiendo lo que hacemos y lo enviara a otra persona? Por supuesto las repercusiones serían más graves. El espionaje informático es una operación lucrativa utilizada por algunos hackers y que supone un gran peligro. Imaginemos qué una persona conoce cada golpe de teclado que realizamos en nuestra máquina. Conocería nuestros passwords, tendría acceso a nuestro correo, sería capaz de predecir nuestras acciones, detectaría y anticiparía nuestros modos de operación, tendría acceso a toda nuestra información, etc. Los keyloggers son aplicaciones malware que tienen este objetivo.

Estas aplicaciones normalmente llegan al usuario de forma camuflada, algo similar a como sucede con los troyanos, y una vez instalados en la máquina ejecutan las acciones correspondientes para recoger cada pulsación que se produzca en el teclado del computador. Algunos sitios web (principalmente bancos) conocedores de estos programas han rediseñado sus accesos para introducir las claves a través de números que son pulsados por ratón en un tablero de la página web. Para sobreponerse a estas técnicas los keylogger han ido evolucionando, recogiendo también las comunicaciones de los navegadores y almacenando las pulsaciones de ratón e intentando identificar en qué posición de pantalla fueron accionadas.

Un problema al que se enfrenta un atacante que utiliza un programa de este tipo es la de recoger la información obtenida. Algunos de ellos pegan la información en un texto plano y el hacker debería tener acceso físico al mismo para recogerlo, pero los más avanzados pueden ser configurados para reenviar la información vía correo a un buzón específico, o establecer una comunicación contra una dirección IP y enviar los datos necesarios.
Algunos de estos programas han pasado a ser comerciales y se ha extendido su uso para el control y predicción de acciones. Algunos padres los utilizan para conocer qué lugares de Internet visitan sus hijos, que conversaciones mantienen a través de Messenger, etc.

1.9.1.8 Back Door

Software que permite el acceso al sistema sin la debida autentificación o facilitando la entrada de información no deseada desde fuera, pues han abierto algún puerto en el equipo. Se trata de un agujero - trampa y su funcionamiento en el primer caso se asemeja al de un troyano, en el segundo caso al de un gusano.

1.9.1.9 Rootkit

Rootkit es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers con el objetivo de acceder ilícitamente a un sistema informático
Hay rootkits para una amplia variedad de sistemas operativos, como Linux, Solaris o Microsoft Windows. Por ejemplo, el rootkit puede esconder una aplicación que lance una consola cada vez que el atacante se conecte al sistema a través de un determinado puerto.

Los rootkits del kernel o núcleo pueden contener funcionalidades similares. Tratan de encubrir a otros procesos que están llevando a cabo acciones maliciosas en el sistema. Por ejemplo, si en el sistema hay una puerta trasera para llevar a cabo tareas de espionaje, el rootkit ocultará los puertos abiertos que delaten la comunicación; o si hay un sistema para enviar spam, ocultará la actividad del sistema de correo.

Los rootkits, al estar diseñados para pasar desapercibidos, no pueden ser detectados. Si un usuario intenta analizar el sistema para ver qué procesos están ejecutándose, el rootkit mostrará información falsa, mostrando todos los procesos excepto él mismo y los que está ocultando.

Un rootkit necesita llevar a cabo algunas tareas que se podrían considerar "típicas", como adquirir derechos de root, modificar llamadas básicas al sistema operativo, falsear sistemas de reporte de datos del sistema. Todas estas tareas, una a una, entrañan poco peligro. Pero todas ellas, juntas y en el mismo momento, llevadas a cabo por el mismo programa, proporcionan información clara de que algo extraño está pasando en la computadora. Si las soluciones antivirus fracasan definitivamente a la hora de detectar un rootkit, las nuevas tecnologías de detección de amenazas por comportamiento tienen su mejor prueba de eficacia en la detección y bloqueo de rootkits. Estas tecnologías no basan su funcionamiento en condicionantes previamente aprendidos sobre patrones cerrados de identificación de amenazas. Su éxito se basa en la investigación inteligente y automática de la situación de un proceso en una computadora.

Cuando una serie de acciones se llevan a cabo sobre el sistema y todas ellas (o, al menos, alguna) pueden suponer un riesgo para la integridad de la información o el correcto funcionamiento de la máquina, se evalúan una serie de factores que sirven para calificar la peligrosidad de esa tarea. Por ejemplo, que un proceso quiera tomar derechos de administración en un sistema puede ser más o menos habitual. Y tiene un cierto riesgo, sin duda, pero no hay que alertar por ello.

1.9.1.10 Spyware

El término spyware se refiere a los programas de software espía que tienen la capacidad de auto instalarse en las computadoras personales de los usuarios, con objeto de conocer su identidad y monitorear su comportamiento al usar sistemas de cómputo o navegar en Internet. El software espía al igual que las famosas cookies es capaz de crear bases de datos y proporcionar información y updates sobre las preferencias y hábitos personales de los usuarios.

La denominación spyware fue idea del creador de software norteamericano Steve Gibson, quien al realizar una investigación descubrió algunos mecanismos espías en una gran cantidad de programas de software, comúnmente utilizado por empresas e individuos. Al respecto, Steve Gibson señala: "si una persona regularmente utiliza una computadora personal, es muy probable que ésta contenga algunos programas de spyware escondidos en la misma".

El software espía, tal y como algunas enfermedades del ser humano, se manifiesta en distintas formas dependiendo de los sistemas y computadoras utilizados por los usuarios.

Actualmente, no se conoce una causa específica relacionada con el spyware que permita controlar su crecimiento, sin embargo, los principales síntomas pueden ser: (i) lentitud del sistema operativo, tanto al abrir programas como al guardar documentos en el disco duro; (ii) funcionamiento inadecuado del teclado y otras funciones primordiales de la computadora y en general, cambios sorpresivos en las barras de herramientas de la computadora; (iii) desplegar una dirección en Internet o URL distinta a la que originalmente se tecleó, o incluir direcciones Web en la lista de sitios favoritos del navegador; (iv) el navegador baja e instala programas de manera automática o cambia constantemente la página principal e inclusive.

1.9.1.11 Adware

El Adware es software que durante su funcionamiento despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes o a través de una barra que aparece en la pantalla. Esta

práctica se utiliza para subvencionar económicamente la aplicación, permitiendo que el usuario la obtenga por un precio más bajo e incluso gratis y, por supuesto, puede proporcionar al programador un beneficio, que ayuda a motivarlo para escribir, mantener y actualizar un programa valioso.

Algunos programas adware son también shareware, y en estos los usuarios tiene la opción de pagar por una versión registrada o con licencia, que normalmente elimina los anuncios.

Algunos programas adware han sido criticados porque ocasionalmente incluyen código que realiza un seguimiento de información personal del usuario y la pasa a terceras entidades, sin la autorización o el conocimiento del usuario.

Existen programas destinados a ayudar al usuario en la búsqueda y modificación de programas adware, para bloquear la presentación de los anuncios o eliminar las partes de spyware. Para evitar una reacción negativa, como toda la industria publicitaria en general, los creadores de adware deben equilibrar sus intentos de generar ingresos con el deseo del usuario de no ser molestado.

1.9.1.12 Dialers

Los Dialers son programas maliciosos, o código maligno escondido en webs, que hace que el módem marque a un sitio web de pago.
Por este mismo motivo, ya no se dan tanto, pues la mayoría de gente utiliza Router, y no módem, por lo que se han reducido las infecciones por este tipo de amenazas.
Los antivirus actuales ya están preparados para prevenir este tipo de ataques, de marcación telefónica.
Lo que conseguían con los dialers era que el módem, se conectara a líneas de pago, como podían ser líneas eróticas, de videncia, etc. No importaba el sitio al que se conectaran, solo que era de pago. Pues bien, la gente que infectaba con dialers, se beneficiaba de ellos, y mucho. El dinero que se estuviera gastando en las líneas de pago, iba para ellos y, claro está, en la factura aparecía un alto importe. Aún así, dichos programas siguen intentando infectar a gente que sigue con módem, aunque cada vez, gracias a la información, son menos los que sufren sus ataques.

Actualmente la mayoría de páginas web que utilizaban el dialer, utilizan otros sistemas, como pedir al usuario que marque por voluntad propia un número de tarificación adicional para acceder a los contenidos de pago.

1.9.1.13 Jokes

Los Jokes son pequeños programas que no son virus, sino bromas cuyo objetivo es hacer creer a los usuarios que su computador ha resultado afectado por algún tipo de código malicioso. No son capaces de provocar daños en los equipos (como pérdida de datos, envíos de correo electrónico no deseado, etc.) pero, indirectamente, si pueden perjudicar a los usuarios.

Cuando un Joke es ejecutado, muestra una imagen con el árbol de archivos que se encuentran en el disco duro del computador.

En la práctica, la medida básica para no ser víctimas de los jokes es no abrir mensajes de correo electrónico no solicitados, ya que es la principal vía que utilizan para llegar a los sistemas. A su vez, si se ha recibido uno, y se tiene conocimiento de que se trata de un joke, lo más conveniente es no distribuirlo.

En cualquier caso, lo mejor es contar con un buen antivirus actualizado para protegerse de los jokes, así como de todo tipo de malware, como el spam, los dialers, el spyware, etc.

1.9.1.14 Spoofs

Buscan falsificar la identidad de alguien o enmascararse como algún otro individuo o entidad para ganar acceso a sistemas o redes y obtener información para propósitos no autorizados.

1.9.1.15 Ip Address Spoofing:

Cada dispositivo tiene una dirección IP única en una red TCP / IP. Este ataque toma ventaja de sistemas y redes que confían en la dirección IP del sistema o dispositivo que se conecta para autenticarlo y permitir el acceso; pero si un hacker enmascara una dirección válida logrará acceso a la red interna.

1.9.1.16 Sequence Number Spoofing.

Las conexiones en redes TCP / IP usan números de secuencia, que son parte de cada transmisión y son intercambiados con cada transacción. Un hacker puede monitorear la conexión de red para registrar los números de secuencia intercambiados y predecir los números de secuencia futuros, lo cual le permitirá insertarse y adueñarse de la conexión de red o insertar información incorrecta.

1.9.1.17 Sesión Hijacking.

Un hacker se encarga de la conexión de sesión entre un cliente y un servidor, una de las muchas técnicas empleadas es mediante la obtención de acceso a un router o dispositivo de red que actúe como gateway entre un usuario legítimo y el servidor.

1.9.1.18 Man in the Middle Attack (MITM).

Alguno de estos ataques se llevan a cabo mediante el DNS spoofing o hyperlink sppoofing; consiste en registrar una URL que es muy similar a una URL existente. Así un atacante se inserta entre un programa cliente y un servidor en una red, para interceptar información ingresada por un cliente (números de tarjetas de crédito, contraseñas, información de cuentas), puede insertarse entre un browser y un servidor Web (Web Spoofing).

1.9.1.19 Dns Poisoning.

Explota una vulnerabilidad de bind, que permite ingresar entradas a la tabla de un servidor DNS con información falsa, así un atacante puede dirigir al usuario a una dirección IP incorrecta; haciendo que una URL legítima apunte al sitio web del hacker.

1.9.1.20 Redirección.

Es otro método de ataque DNS, consiste en comprometer links de una página web con links falsos, aparentemente estos enlaces son legítimos, pero re- direccionan al usuario a un sitio controlado por el hacker. También puede tratar de manipular el sistema de registro de nombres de dominio para alterar su funcionamiento normal, al

transferir un nombre de dominio propietario a otra dirección IP provocando la re-dirección.

1.9.1.21 Ataque de Repetición

Consiste en interceptar y almacenar una transmisión legítima entre dos sistemas y retransmitirla un tiempo después.

1.9.1.22 Password Cracking

Es una técnica que se vale de un programa para descifrar archivos de contraseña utilizando el mismo algoritmo usado para generar la contraseña cifrada, empleando un diccionario de palabras o frases conocidas y cifradas con el algoritmo de contraseña. Entonces comparan cada registro del archivo de contraseña con los registros del archivo diccionario hasta encontrar una coincidencia que revele la contraseña.

1.9.1.23 Ingeniería Social

Son métodos no técnicos que emplea un hacker para obtener acceso al sistema, pueden ser sorprendentemente efectivos; consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían, como revelar información (contraseñas).

1.9.1.24 Sniffing

Consiste en monitorear los paquetes de una red en busca de información (contraseñas o direcciones IP) que pueda ser útil para un ataque; también el análisis de tráfico puede proveer información útil.

1.9.1.25 Modificación de Sitios Web

Consiste en modificar los sitios web de alguna organización, se consigue mediante la explotación de configuraciones incorrectas y/o vulnerabilidades conocidas del software o sistema operativo del servidor Web. Para contrarrestar este ataque hay que actualizar las

versiones del software y sistema operativo del servidor Web o implementar servidores caché de red que actualicen al servidor Web.

1.9.1.26 War Dialing

Es un método de fuerza bruta para descubrir puertas traseras en una red perteneciente a una organización, atenta de manera efectiva contra el perímetro de defensa; utiliza un sistema de marcado automático para llamar a cada número de teléfono de la organización en busca de conexiones de módem, para intentar irrumpir en el sistema al cual el módem está conectado y obtener acceso a la red.

1.9.1.27 Negación del Servicio

Son diseñados para apagar o presentar inoperable un sistema, el objetivo es hacer a una red o sistema no disponible.

1.9.1.28 Ping de la Muerte.

Ping es un comando TCP / IP que envía un paquete IP a una dirección IP específica para ver si existe respuesta y determinar si el host está en la red (está activo).
Algunos sistemas operativos fueron o son vulnerables a paquetes ICMP más grandes de lo normal, entonces especificando un paquete grande en un comando ping se puede causar un desbordamiento interno en algunos sistemas dejándolos inhabilitados. Normalmente se requiere inundar de pings a un sistema para colapsarlo.

1.9.1.29 Inundación de Syn.

Explota la negociación de tres vías que TCP / IP utiliza para establecer una conexión, deshabilita un determinado sistema creando muchas conexiones entreabiertas.
Consiste en inicializar una conexión a un servidor con el bit número SYN, sin embargo la dirección de retorno asociada con el SYN no es una dirección válida, entonces el servidor envía un SYN-ACK a una dirección no válida que no existe y no responde, por lo tanto permanece en espera del ACK de retorno. Así muchas conexiones entreabiertas no permiten el acceso de usuarios legítimos y también pueden colapsar el sistema.

1.9.1.30 Ataque Smurf.

Emplea paquetes ICMP ECHO_REQUEST falsificados, enviando como dirección IP origen la dirección IP de un determinado sistema (víctima) y la dirección destino de estos paquetes son direcciones IP de broadcast de red; de ésta manera las máquinas de la red responden e inundan al sistema apuntado, consecuentemente se degradará el rendimiento de la red que conecta a la red intermediaria con el sistema

1.9.2 PROTECCIONES

1.9.2.1 Secure Sockets Layer (Ssl)

Fue desarrollado para brindar seguridad en la transmisión de información por Internet, ofrece confidencialidad al momento de ingresar o trasmitir datos por la Web. Se utiliza la encriptación asimétrica para preparar la sesión SSL y la encriptación simétrica para transmitir datos de forma segura sobre una red insegura.

1.9.2.2 HTTPS

Consiste en usar el servicio http sobre SSL, SSL establece una conexión segura mediante el uso de un túnel encriptado entre el cliente browser y el servidor Web, así los paquetes de datos viajan seguros. La integridad de la información se establece mediante algoritmos hash, la confidencialidad de la información es asegurada mediante la encriptación, la autenticación de las entidades se asegura mediante el uso de certificados digitales y encriptación asimétrica.
El proceso consiste en preparar una sesión SSL:

1. Ambos extremos intercambian números aleatorios.
2. El servidor envía su clave pública y un ID de sesión.
3. El cliente browser crea una clave denominada pre_master_secret, la cifra con la clave pública del servidor y la envía al servidor.
4. Ambos extremos generan una clave de sesión utilizando la pre_master_secret y los números aleatorios.
5. Utilizan la clave de sesión para trabajar con encriptación simétrica.

1.9.2.3 Seguridad E-Mail

Consiste en no revelar el contenido del mensaje e-mail mediante el uso de encriptación; asegurar la integridad del mensaje mediante el empleo de algoritmos hashing o message digest; verificar la identidad del transmisor mediante el empleo de firmas digitales y finalmente verificar la identidad del receptor mediante el uso de encriptación de clave pública.

1.10 TECNOLOGÍAS DE SEGURIDAD INFORMÁTICA

1.10.1 FIREWALL

Es un sistema o dispositivo de control de acceso que se utiliza para separar una red interna de una red externa, se encuentra en el límite entre el espacio protegido denominado perímetro de seguridad y la red externa denominada zona de riesgo, filtra tráfico de entrada y salida, y también esconde la configuración de la red hacia el exterior.
La función del firewall, por tanto, es bloquear el tráfico no autorizado entre un sistema de confianza y un sistema de dudosa confianza.

Un firewall es, a menudo, instalado en el punto donde una red interna se conecta con Internet. Todo tráfico externo de Internet hacia la red interna pasa a través del firewall, así puede determinar si dicho tráfico es aceptable de acuerdo a sus políticas de seguridad.

Aunque el propósito principal de los firewall es mantener a los intrusos fuera del alcance de la información que es propiedad de un ente determinado, ya sea un usuario, una empresa o un gobierno, su posición dentro del acceso a distintas redes le vuelve muy útil para controlar estadísticas de situaciones como usuarios que intentaron conectarse y no lo consiguieron, tráfico que atravesó la misma, etc... Esto proporciona un sistema muy cómodo de auditar la red. Algunas de sus funciones son las siguientes:

- Restringir la entrada a usuarios a puntos cuidadosamente controlados.
- Prevenir los ataques
- Dividir una red en zonas con distintas necesidades de seguridad
- Auditar el acceso a la red.

Algunos firewall solamente permiten tráfico de correo a través de ellos, de modo que protegen de cualquier ataque sobre la red distinto de un servicio de correo electrónico. Otros firewall proporcionan menos restricciones y bloquean servicios que son conocidos por sus constantes problemas de intrusión. De los servicios ya hablaremos más adelante. Generalmente, los firewalls están configuradas para proteger contra "logins" sin autorización. Esto ayuda principalmente a prevenir actos de vandalismos en máquinas y software de nuestra red. Redes firewalls más elaboradas bloquean el tráfico de fuera a dentro, permitiendo a los usuarios del interior comunicarse libremente con los usuarios del exterior. Los firewall pueden protegernos de cualquier tipo de ataque a la red, siempre y cuando se configuren para ello.

1.10.1.1 Características de un Firewall

Un firewall, debido a su funcionalidad, debe ser capaz de ofrecer una serie de características mínimas como puede ser el empleo de una adecuada política de seguridad. Por consiguiente, esto sólo no basta, sino que el firewall además debe de ser capaz de poder ofrecer otros servicios como pueden ser el registro de las operaciones que vaya realizando y el poseer una interfaz fácil e intuitiva que reduzca al mínimo la posibilidad de que el operario se equivoque a la hora de configurarlo y mantenerlo. Algunas de las características que definen a un firewall son:

1.10.1.2 Política de Seguridad

Consiste en determinar los principios generales en los que debe basarse el diseño de un sistema de seguridad, en nuestro caso un firewall:

- **Política Principal:** Todo aquello que no está expresamente permitido está prohibido
- **Política de Diseño:** Encaminada a la minimización y la simplicidad.
- **Política de Escepticismo:** Tras dotar al firewall de todas las protecciones disponibles se toma en consideración que se pueden desarrollar nuevas técnicas y que ningún grado de seguridad es absoluto.

1.10.1.3 Registro de Operaciones

El firewall podía ser utilizado para obtener datos estadísticos acerca de la afluencia entre ambas redes. Pues bien, para poder realizar esta estadística deberá recoger, como mínimo, la siguiente información y almacenarla en algún fichero:

- **Service Information** - fecha, y hora.
- **Remote Information** - dirección IP del presunto intruso, así como el puerto y el protocolo utilizado.
- **Local Information** - dirección IP de destino y puerto.
- **Filter Information** - actuación del filtro y qué adaptador de red lo hizo.
- **Packet Information** - encabezamiento e información del paquete.

Esta información también es muy útil en caso de producirse un ataque para poder conocer por donde se ha intentado entrar, cuándo y porqué, cuál ha sido la estrategia que ha seguido el firewall, si el ataque ha sido o no exitoso. Estos datos nos van a permitir poder hacer un seguimiento sobre el funcionamiento del firewall.

1.10.1.4 Interfaces

Con una política de seguridad lo suficientemente hermética y un firewall eficaz, el mayor riesgo provendrá de un error humano del administrador del firewall. Estos pueden incorporar un gran número de funciones que complican su trabajo de administración. Los firewall que cuentan con una buena interfaz reducen la posibilidad de errores humanos y simplifican el trabajo del administrador del firewall.

Una interfaz fácil de utilizar y con un número mínimo de opciones de configuración reduce la posibilidad de que se produzcan errores de administración. Naturalmente, un número menor de opciones de configuración puede significar también menor flexibilidad de configuración.

Existen tres clases de interfaz del administrador de firewalls:

- Administración basada en ficheros de texto.
- Administración basada en menús de texto.
- Administración basada en GUI.

La interfaz basada en ficheros de texto es la de uso más extendido en lo que respecta a los firewalls de elaboración propia. Este tipo de interfaces permiten al administrador editar un archivo específico donde puede introducir parámetros de configuración específicos. Se trata de la interfaz de elección para los administradores de sistemas UNIX tradicionales, dado que ofrece una interfaz de control a bajo nivel con los mecanismos del firewall. La desventaja de dicho control a bajo nivel es que resulta mucho más fácil cometer errores, ya que, al editar un fichero, pueden producirse errores de escritura u otros errores técnicos que, en un sistema basado en menús, es menos probable que ocurran.

La interfaz de administrador basada en menús de texto presenta un menú basado en texto que reduce la probabilidad de producirse errores pero que proporciona menor capacidad de control para el administrador. Sin embargo, la posibilidad de error no queda totalmente excluida, dado que el administrador no siempre puede ver el efecto de algunos cambios.

La interfaz gráfica de usuario, o GUI, para administradores incorpora ventanas, botones, menús desplegables y pantallas de ayuda que facilitan el trabajo de configuración. La mayoría de proveedores ha optado por incluir esta interfaz en sus productos, puesto que tiende a ser más fácil de utilizar y no es susceptible a muchos de los errores que pueden producirse en los otros dos tipos de interfaz.

1.10.1.5 Autenticación de Usuarios

La dirección IP del host origen se emplea para efectuar el control básico de acceso. Sin embargo, esta dirección puede ser suplantada fácilmente, especialmente por hosts que forman parte de la misma red. Además, en el caso de conexiones procedentes de hosts multiusuario, la dirección de éstos no permite distinguir un usuario de otro. La mayoría de firewalls a nivel de aplicación soportan la autenticación de usuarios para algunos servicios de red. Para ello, el firewall interrumpe la conexión y solicita a los usuarios que se identifiquen antes de continuar la conexión hacia el destino deseado.

Sin embargo, la mayoría de protocolos de servicio de red no toleran dicha interrupción y, por lo tanto, no pueden soportar los métodos de autenticación, como contraseñas y tarjetas inteligentes. Otros protocolos como el correo electrónico o los grupos de noticias no

establecen una conexión directa con el usuario, por lo que no es posible solicitar información para la identificación.

Los servicios de red estándar que contemplan la posibilidad de que un firewall pueda realizar funciones de autenticación son Telnet y FTP. Algunos firewall soportan también la autenticación para los servicios X11 y HTTP.
Los mecanismos estándar de autenticación que ofrecen los firewalls en la actualidad son contraseñas convencionales, tarjetas inteligentes y servicios S/Key. El mecanismo de contraseñas convencional emplea contraseñas multiuso y no es recomendable utilizarlo en Internet porque las contraseñas pueden ser interceptadas y empleadas más adelante por un intruso. Las tarjetas inteligentes verifican la identidad de un usuario devolviendo una respuesta única basada en un número aleatorio, que proporciona el firewall. Los usuarios responden introduciendo el número en un dispositivo autentificador, que calcula la respuesta apropiada.

1.10.1.6 Correlación de Direcciones

Antes de producirse el auge de Internet, muchas organizaciones poseían redes privadas desprovistas de conexión con otras redes también privadas. Como estaban aisladas entre sí, no tenían que solicitar a las autoridades de Internet direcciones de red no utilizadas. En lugar de ello, escogían cualquier clase de dirección IP que les apetecía.
Con el advenimiento de la Internet como parte de la infraestructura global, estas organizaciones han comenzado a conectarse a Internet y no pueden utilizar las mismas direcciones porque probablemente ya han sido asignadas a otro usuario.
Naturalmente, las organizaciones podrían solicitar una clase de dirección única, pero resultaría muy costoso cambiar todas sus computadoras y es difícil obtener las direcciones IP.
Otra solución consistiría en que el firewall correlacionara direcciones origen legales con direcciones de Internet legales en el momento que abandonan la intranet interna. En esta situación, es necesario descorrelacionar la dirección de destino de los paquetes de retorno o restaurarla a la dirección original.
En realidad, la correlación de direcciones no es una cuestión de seguridad, pero el firewall está situado generalmente en el punto ideal de la arquitectura de la red, a fin de proporcionar este servicio.

Una razón plausible para tener o mantener direcciones ilegales en la red es que puede poner trabas a los intrusos que hayan podido entrar en la misma evitando el firewall. En este caso, los paquetes del intruso pueden encontrar dificultades para llegar a la red, ya que los protocolos de direccionamiento estándar los dirigirán hacia el propietario de la dirección real. Ésta es una protección adicional mínima y, probablemente, no compensa la reducción de la velocidad y el aumento de la complejidad al tener que correlacionar todas las direcciones.

1.10.1.7 Restricciones de Día y Hora

La política de seguridad puede variar en función de del día de la semana y la hora del día. Por ejemplo, es posible permitir transferir archivos a Internet durante las horas laborales normales, aunque no durante los fines de semana o después de las 6 de la tarde. Algunos firewall permiten basar las reglas de acceso o listas de acceso en la hora del día y el día de la semana.

1.10.1.8 Control de la Carga

El control de la carga es una característica que ofrecen muy pocos firewalls. Para la mayoría de estos, cuando se permite el acceso, el host o la red pueden efectuar un número ilimitado de conexiones. Es útil poder establecer limitaciones al número de conexiones simultáneas con un host o una red de hosts que puede haber activas. Esta característica puede ayudar a impedir ataques por inundación, mediante los cuales un pirata informático inunda la red con conexiones a fin de ocultar el ataque real.

1.10.1.9 Canalización

La canalización es la capacidad de combinar múltiples servicios de aplicación en una única conexión. Los intrusos emplean en ocasiones esta técnica para disfrazar un servicio no autorizado (por ejemplo, FTP) como servicio autorizado (como el correo electrónico).

Un firewall puede proporcionar también la característica de canalización para permitir a dos sitios de una compañía compartir servicios en Internet que no serían autorizados normalmente a través del mismo.

1.10.1.10 Servidor Proxy

El proxy es una solución software que se ejecuta sobre el Firewall para permitir la comunicación entre dos redes de una forma controlada.
Proxy a nivel de aplicación. Son aplicaciones software (servicios proxy) para bloquear o reenviar conexiones a servicios como finger, telnet, http, smtp o ftp; la máquina donde corren estas aplicaciones se denomina pasarela de aplicación.
Los servicios proxy permiten únicamente la utilización de servicios para los que existe un proxy, además entiende el protocolo para el que fue diseñado lo que hace posible mayor capacidad de análisis y restricción; pero esto puede ser costoso, limitar el ancho de banda efectivo de la red o disminuir la funcionalidad de aplicaciones.
La pasarela de aplicación permite un grado de ocultación de la estructura de la red protegida, ya que es el único sistema que se presenta hacia el exterior, todas las conexiones se originan y terminan en las interfaces del Firewall.

1.11 VPN

Es una red de datos privada creada a partir de una red de datos pública como Internet, transporta tráfico de una manera segura sobre una red insegura, mediante el uso de encriptación, autenticación y encapsulamiento (tunneling), con el fin de asegurar la integridad y privacidad de los datos. Existen varias razones para la implantación de VPNs:

- Bajo costo de implementación.
- Privacidad de los datos.
- Acceso desde todas partes.
- Flexibilidad.
- Escalabilidad.

1.11.1 Seguridad

- **Privacidad de los datos**
  - ✓ **Modo Encriptación.** Consiste en cifrar la porción de datos del paquete usando encriptación simétrica o asimétrica, la cabecera del paquete no es modificada.

- ✓ **Modo Túnel.** Todo el paquete de datos incluida la cabecera es encapsulado dentro de un nuevo paquete el mismo que es encriptado y finalmente se le añade una nueva cabecera, este modo es usado para transmitir protocolos no IP sobre el backbone IP o IP dentro de IP por razones de seguridad.

- **Integridad de los datos**

Para asegurar la integridad de los datos las soluciones VPN utilizan los algoritmos hash.

- **Autenticación**

Las soluciones VPN soportan varios esquemas de autenticación de usuarios como:
User / Password.

- **Autenticación vía token.**

- Smartcards.
- Certificados X.509.

- **Autorización**

Las soluciones VPN permiten definir perfiles de usuario con su correspondiente nivel de autorización y acceso.

- **Control de acceso**

Las soluciones VPN proveen un control de acceso por razones de seguridad y auditoría basado en:

- UserID.
- HostID.
- IPaddress.
- Subnetwork address.

- **Auditoría**

Las soluciones VPN definen un registro de actividad del usuario.

- **Rendimiento**

El tiempo de respuesta entre una red segura y una red insegura deben ser semejantes, para brindar transparencia a la solución VPN, el trabajo adicional que acarrea el uso de VPNs incrementa la latencia y disminuye la velocidad efectiva de los datos. Entonces es importante considerar los siguientes parámetros al comprar o diseñar una solución VPN:

- Calidad de servicio (QOS).
- Acuerdos de nivel de servicio (SLAs).
- Soporte de múltiples protocolos.

- Confiabilidad y resistencia.

1.12 MODELOS DE AUTENTICACIÓN

Los sistemas de una organización deben tener la capacidad de restringir el acceso a sus diferentes recursos dependiendo de la identificación y autorización que posee el usuario.

- ✓ **Contraseñas**

  Cualidad que el individuo conoce, las contraseñas brindan una seguridad débil ya que una contraseña puede ser adivinada, robada u obtenida.

- ✓ **Tarjetas inteligentes**

  Cualidad que el individuo tiene, las tarjetas inteligentes proporcionan una seguridad mayor pero no completa, evitan el riesgo de que una contraseña sea descubierta, pero si una tarjeta es robada y constituye el único medio de autenticación una atacante explotará esta vulnerabilidad del sistema para tener acceso al mismo.

1.13 SOFTWARE ANTIMALWARE

Son programas que escanean los virus, son muy efectivos contra virus conocidos, pero son incapaces de reconocer y adaptarse a nuevos virus.

Su funcionamiento radica en el reconocimiento de la firma de un virus conocido, el programa detecta un virus cuando encuentra una coincidencia entre los resultados escaneados y las firmas de virus almacenadas en la base de datos. La base de datos que contiene las firmas de virus debe ser actualizada regularmente caso contrario el programa antivirus se vuelve obsoleto rápidamente.

Constituye un componente necesario para una buena solución de seguridad, ya que si está implementado y configurado apropiadamente, puede reducir la exposición de una organización a programas mal intencionados.

Sin embargo no protegerá a una organización de un intruso que haga mal uso de un programa legítimo para obtener el acceso al sistema, tampoco si un usuario legítimo intenta obtener acceso a archivos a los que no tiene acceso.

1.14 SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

Constituyen sistemas administradores competentes que auditan y monitorean continuamente sus sistemas en busca de intrusiones. La detección de intrusiones es el arte de detectar actividades no autorizadas, inapropiadas o extrañas.

Los IDS son capaces de detectar ataques en progreso, generar alarmas en tiempo real y contrarrestar un ataque mediante el lanzamiento de un evento o la reconfiguración del router o Firewall.

Actúan como guardianes de seguridad o centinelas, constantemente están escaneando el tráfico de red o los logs de auditoría de un host.

1.14.1 Sistemas de detección de intrusos para host (HIDS)

Reside en el host y es capaz de monitorear y negar servicios automáticamente si una actividad sospechosa es detectada; usan los archivos log y los agentes de auditoría del sistema para realizar el monitoreo.

- **Verificadores de integridad del sistema (SIV).** Es un mecanismo encargado de monitorizar archivos de una máquina en busca de posibles modificaciones no autorizadas.
- **Monitores de registros (LFM).** Monitorizan los archivos de log generados por los programas de una máquina en busca de patrones que puedan indicar un ataque o una intrusión.
- **Sistemas de decepción.** Son mecanismos encargados de simular servicios con problemas de seguridad de forma que un pirata piense que realmente el problema se puede aprovechar para acceder a un sistema, cuando realmente se está aprovechando para registrar todas sus actividades.

1.14.2 Sistemas de detección de intrusos para red (NIDS)

Monitoriza los paquetes que circulan por la red en busca de elementos que denoten un ataque contra alguno de los sistemas ubicados en ella; el IDS puede situarse en cualquiera de los hosts o en un elemento que analice todo el tráfico (como un HUB o un enrutador); éste analiza los siguientes elementos:

- Campos de fragmentación IP.
- Dirección origen y destino.
- Puerto origen y destino.
- Flags TCP.
- Campo de datos.

1.14.3 Detección de anomalías

La base del funcionamiento de estos sistemas es suponer que una intrusión se puede ver como una anomalía de nuestro sistema, estos modelos de detección conocen lo que es normal en nuestra red o nuestras máquinas a lo largo del tiempo, desarrollando y actualizando conjuntos de patrones contra los que se compararán los eventos que se producen en los sistemas, se tiene:

- Métodos estadísticos que determinan los perfiles de comportamiento habitual.
- Especificación de reglas que establecen los perfiles de comportamiento normal.

1.14.4 Detección de usos indebidos

El funcionamiento de los IDS basados en la detección de usos indebidos presupone que podemos establecer patrones para los diferentes ataques conocidos y algunas de sus variaciones, este esquema se limita a conocer lo anormal para poder detectar intrusiones, se tiene:

- Sistemas expertos.
- Transición de estados.
- Comparación y emparejamiento de patrones.
- Detección basada en modelos.

1.15 SEGURIDAD FÍSICA DE RED

La seguridad física de los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y detección contra las amenazas a los recursos y a la información confidencial. Éste suele ser un aspecto olvidado frecuentemente, lo cual motiva a los atacantes a explotar las vulnerabilidades físicas del sistema.

Entonces implementar cierta seguridad física es importante para garantizar la seguridad global de la red y los sistemas conectados a ella; pues se podría implementar un sistema sofisticado de seguridad lógica pero no serviría de nada si un intruso accede físicamente al sistema u ocurre una catástrofe que puede causar mucho más daño que una amenaza lógica.

Para establecer un sistema de seguridad física se ha de analizar el valor de lo que se quiere proteger y la probabilidad de las amenazas potenciales, para en función de los resultados obtenidos diseñar un plan de seguridad adecuado.

1.15.1.1 PROTECCIÓN DEL HARDWARE

Las medidas encaminadas a asegurar la integridad del hardware son parte importante de la seguridad física de cualquier organización, ya que frecuentemente constituye el componente más caro de todo sistema informático.

1.15.1.1.1 Acceso Físico

Comprende la protección de zonas o elementos físicos que pueden comprometer la seguridad del sistema, es así que el nivel de seguridad física depende completamente del entorno donde se ubiquen los puntos a proteger, ya que se tendrán equipos bien protegidos dentro de la organización y otros ubicados en lugares de acceso casi público. La posibilidad de acceder físicamente a un sistema hace inútiles casi todas las medidas de seguridad que se hayan aplicado.

- **Prevención.** Consiste en implementar mecanismos de control de acceso, para prevenir un ingreso físico no autorizado. Los más adecuados para la seguridad física son los biométricos y los basados en algo que el individuo posee, así entre los más comunes tenemos videocámaras, geometría de la mano, huellas digitales, tarjetas inteligentes, control de las llaves que abren determinada puerta.
- **Detección**. Consiste en implementar mecanismos que permitan conocer la presencia de accesos no autorizados, entre los más comunes tenemos cámaras de vigilancia, alarmas o personal de la organización.

1.15.1.1.2 Desastres del entorno

- Electricidad. Se pueden presentar los siguientes problemas con el sistema eléctrico que alimenta a los equipos: cortocircuitos, picos de tensión, bajas de tensión, cortes de flujo, que continuamente amenazan la integridad de hardware y los datos.
- Para contrarrestar estas amenazas puede implementarse tomas de tierra, acondicionadores de tensión o utilizar un SAI (Servicio de Alimentación Ininterrumpido) como los UPS o plantas generadoras de energía privadas.
- Para protegerse contra los problemas que puede causar la corriente estática se puede utilizar spray antiestático, o simplemente no tocar directamente ninguna parte metálica, protegerse si debe hacer operaciones con el hardware o no mantener el entorno excesivamente seco.
- Ruido eléctrico. Es generado por motores, ordenadores u otros dispositivos, y puede perjudicar el normal funcionamiento de un equipo, para contrarrestarlo hay que situar los aparatos que causan ruido eléctrico un poco alejado de las instalaciones y equipos del sistema, caso contrario se puede instalar filtros en las líneas de alimentación y mantener alejados equipos emisores de ondas (teléfonos móviles, transmisores de radio, etc.).
- Incendios y humo. Pueden ser causados por problemas eléctricos (cortocircuitos o recalentamiento de equipos) debido a la sobrecarga de la red por el gran número de aparatos conectados al tendido. Para contrarrestar esta amenaza se puede colocar extintores adecuados (de dióxido de carbono) que se activen automáticamente al detectar humo o calor.
- Temperaturas extremas. Es recomendable evitar el frío intenso o el calor excesivo, tanto para los equipos como para las personas.

1.15.1.2 PROTECCIÓN DE LOS DATOS

La seguridad física también implica una protección a la información del sistema, tanto a la que está almacenada como a la que se transmite entre diferentes equipos.

- **Interceptación**. Es un proceso mediante el cual un agente capta información (plana o cifrada) que no le pertenece. Mediante el sniffing un atacante puede

capturar tramas que circulan por la red, para contrarrestar esta amenaza hay que evitar tener segmentos de red de fácil acceso o tomas de red libres y usar aplicaciones de cifrado para las comunicaciones o almacenamiento de la información (hardware de cifrado).

También puede filtrarse la información (reuniones) mediante teléfonos fijos o móviles, para evitar esto se pueden desconectar los teléfonos fijos y bloquear la señal de los móviles mediante un sistema de aislamiento que bloquea cualquier transmisión en los rangos de frecuencias en los que trabajan las operadoras telefónicas.

- **Backups.** Consiste en la protección de los diferentes medios donde residen las copias de seguridad, ya que contienen toda la información, hay que protegerlas igual que a los sistemas en si; se puede realizar backups cifrados y controlar más el acceso al lugar donde se guardan.

1.16 UTM (UNIFIED THREAT MANAGEMENT)

1.16.1 ESTUDIO DE LA TECNOLOGÍA UTM

Los avances de la tecnología y el desarrollo de amenazas cada vez más peligrosas y complejas, a determinado que las soluciones de seguridad perimetral evolucione a los sistemas de seguridad multi-amenazas, que constituyen la nueva generación de los sistemas de protección de red en tiempo real.

Los sistemas unificados de administración de amenazas (UTM) detectan y eliminan las más dañinas amenazas basadas en el contenido e-mail o tráfico web tales como virus, gusanos, intrusiones, contenido web inapropiado y más en tiempo real, sin degradar el rendimiento de la red.

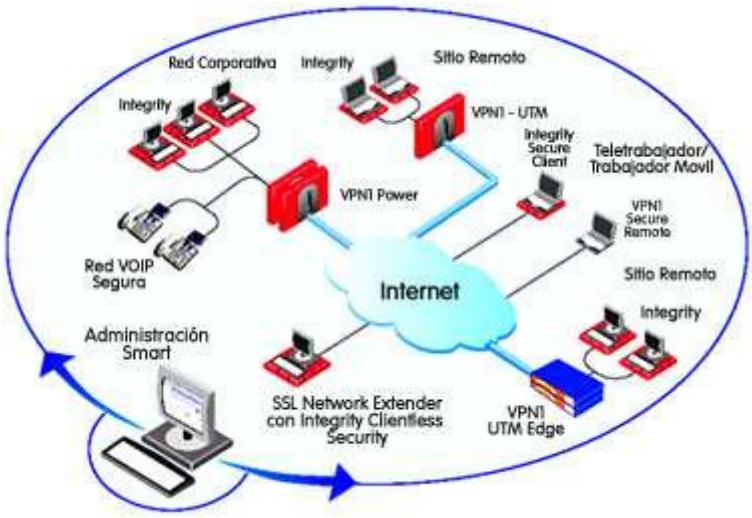


Figura 1: Características de los sistemas UTM.

Un sistema de seguridad debe poseer varios componentes que trabajen conjuntamente con el fin de aproximarse a un sistema seguro, es así, que los sistemas UTM incorporan varias técnicas y *componentes* de seguridad para lograr el acercamiento a este objetivo.

Los sistemas reinantes actualmente como los Firewall, VPNs e IDS resultan efectivos proporcionando protección a nivel de red, sin embargo no cubren las necesidades de protección actual en los ámbitos telemáticos, ya que su capacidad permite el análisis de la cabecera de los paquetes pero no el análisis del contenido de los mismos.

Estos sistemas no pueden comprobar el contenido del paquete y procesarlo para identificar virus, gusanos u otras amenazas, por lo tanto son ineficaces contra ataques basados en contenido. Así los virus, gusanos, troyanos, etc, transmitidos por correo electrónico y tráfico http atraviesan fácilmente los Firewall, VPN o IDS.

Toda esta evolución de tecnología ha acelerado la necesidad de implantación de soluciones de defensa en profundidad a nivel de contenido. Aparentemente el reto de los fabricantes y proveedores de seguridad es la gestión eficiente de respuesta ante los nuevos ataques que nacen en el Internet y en proporcionar firmas actualizadas y efectivas para controlar dichos ataques.

Los sistemas UTM constituyen el software y hardware específico para la seguridad de redes, sus más comunes y principales características son el uso de tecnología ASIC (Application-Specific Integrated Circuit) y la integración de diferentes módulos de seguridad que garantizan la adecuada protección de la red sin degradar su rendimiento.

Finalmente para complementar la seguridad en entornos extremadamente críticos se incluye HIDS sistemas de seguridad en profundidad encargados de detectar y proteger a un sistema en particular de intrusiones; así se puede controlar de manera exhaustiva los datos, aplicaciones y accesos que se procesan en una determinada máquina.

Los dispositivos UTM combinan las funciones de diferentes dispositivos de seguridad, administración y análisis dentro de un solo ambiente más flexible lo cual permite desarrollar en forma integral múltiples características de seguridad (políticas de seguridad) en una sola plataforma.

Estos sistemas están ganando popularidad rápidamente debido al rendimiento que ofrecen en aplicaciones de seguridad, costo de operación e inversión de capital.

2. ANÁLISIS SOLUCIÓN DE IMPLEMENTACIÓN: FORTIFGATE DE FORTINET

En el mercado existen muchas soluciones UTM como lo son las ofrecidas por los fabricantes Fortinet, SonicWall, Check Point Software Technologies, Watchguard, Juniper, Cisco, Netgear, entre otros. El análisis de la solución UTM FORTIGATE del fabricante FORTINET, para el caso puntual de C.I OCEANOS S.A, entidad en la que se desarrolla el presente proyecto, obedece a que esta es la solución que han implementado otras unidades de negocios del grupo al que pertenece esta entidad y el grupo corporativo la ha tomado como solución estándar, para todas sus empresas. A pesar de esta limitante en la selección de un UTM, se realiza un análisis del comparativo del Cuadrante mágico para UTMs realizados por la entidad Gartner en Octubre del 2010, ver figura N° 2.

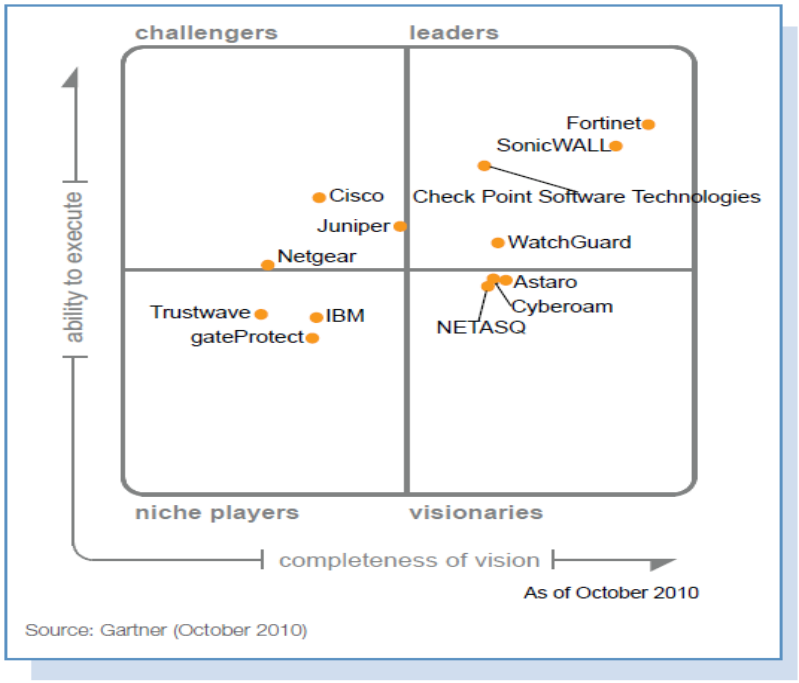


Figura 2: Cuadrante mágico para UTMs realizados por la entidad Gartner en Octubre del 2010.

En la anterior figura se detalla que la entidad Gartner sitúa la solución UTM de FORTINET cómo líder en el mercado, con la mayor habilidad de ejecución y visión completa frente a las funcionalidades que ofrece las soluciones UTM, a diferencia de otras soluciones del mercado.

A continuación se detallan las fortalezas y debilidades, de acuerdo a los lineamientos de la entidad Gartner en el informe Magic Quadrant for Unified Threat Management respecto a la solución UTM Fortinet:

FORTALEZAS

- ✓ Fortinet se presenta en la mayoría de listas de candidatos y sigue innovando. En el mercado de medianas empresas, se considera una "opción segura", debido a su fuerte presencia en este mercado.
- ✓ El uso de Fortinet de hardware a la medida, combinada con precios agresivos, sigue ofreciendo un alto nivel de precio / rendimiento.

- ✓ Tiene aplicación flexible y fácil de conocer las capacidades políticas de firewall, estrechamente vinculada a las políticas de IPS.

DEBILIDADES:

- ✓ Fortinet IPS es difícil de ajustar con precisión.
- ✓ La interfaz de usuario (IU) no es la más intuitiva, especialmente onexperts forn.
- ✓ La falta de pruebas de rendimiento independientes dificulta la capacidad de los compradores más avanzados para verificar las afirmaciones acerca de su rendimiento.
- ✓ Las funciones de registros y presentación de informes del dispositivo son muy básicas. Los usuarios se quejan de que hay muy poca memoria en los dispositivos para realizar un análisis de estos registros, para esto se requiere de un producto por separado como es el FortiAnalyzer.

Por otro lado Fortinet ofrece una completa gama de productos (software y hardware), servicios de subscripción y soporte que trabajan conjuntamente para proporcionar soluciones de seguridad de red amplias, rentables y manejables; cuenta además con certificaciones FIPS (Federal Information Processing Standards) e ICSA (International Computer Security Association) y características NSS (Network Security Services) y EAL (Evaluation Assurance Level).

Los sistemas de seguridad multi-amenaza de Fortinet utilizan tecnología ASIC y constituyen la nueva generación de protección de red en tiempo real; detectan y eliminan las amenazas más perjudiciales de correo electrónico y tráfico web sin degradar el rendimiento de la red.

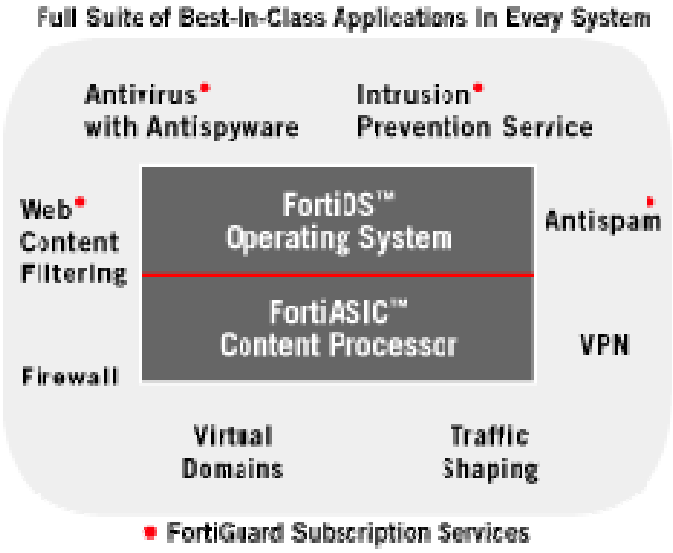


Figura 3: Tecnologías y ámbitos que envuelve Fortinet.

2.1 FORTIGUARD DISTRIBUTION NETWORK (FDN)

Es una red mundial de servidores FortiGuard distribuidos que permite actualizar las definiciones de ataques.

La infraestructura FortiGuard de Fortinet asegura la rápida identificación de nuevas amenazas y el desarrollo de firmas de nuevos ataques. Los servicios de FortiGuard constituyen un valioso recurso para el cliente e incluye actualizaciones automáticas de virus, motores IPS y definiciones a través de la FDN.

2.2 FORTIGUARD CENTER

Presenta la base de datos de vulnerabilidades y amenazas, la misma que es mantenida y actualizada por el equipo mundial de respuesta de amenazas de Fortinet y provee cobertura de 24x7x365 sobre las más recientes amenazas globales.

Estos servicios son creados con la más reciente tecnología de seguridad y diseñados para operar con el menor costo. Con la subscripción de servicios FortiGuard habilitada, los clientes pueden estar seguros que sus plataformas de seguridad FortiGate están

funcionando óptimamente y protegiendo sus activos corporativos con la última tecnología de seguridad y con el mejor precio posible.

- **Servicio Antivirus FortiGuard.** Proporciona protección automática para el Firewall Antivirus de FortiGate y lo mantiene actualizado con las últimas defensas antivirus contra amenazas basadas en red.

- **Servicio IPS FortiGuard.** Proporciona a los clientes FortiGate las últimas defensas contra actividades de red maliciosas, sospechosas o secretas, provenientes de nuevas y desconocidas amenazas y vulnerabilidades mediante las cuales se pretende ganar acceso a la red, a sus aplicaciones importantes o a la información; este servicio toma medidas de precaución y responde a los ataques que se propagan rápidamente en la actualidad.

- **Servicio de Filtrado Web FortiGuard.** Regula y proporciona una valiosa comprensión de las actividades web, permitiendo a los clientes satisfacer las nuevas regulaciones gubernamentales, cumplimiento educacional, políticas de recursos humanos y políticas de uso de Internet corporativo; así previene el uso inapropiado de Internet que provoca bajas en la productividad, utilización inadecuada de los recursos empresariales, hostigamiento, deuda legal y demás cuestiones de recurso humanos.

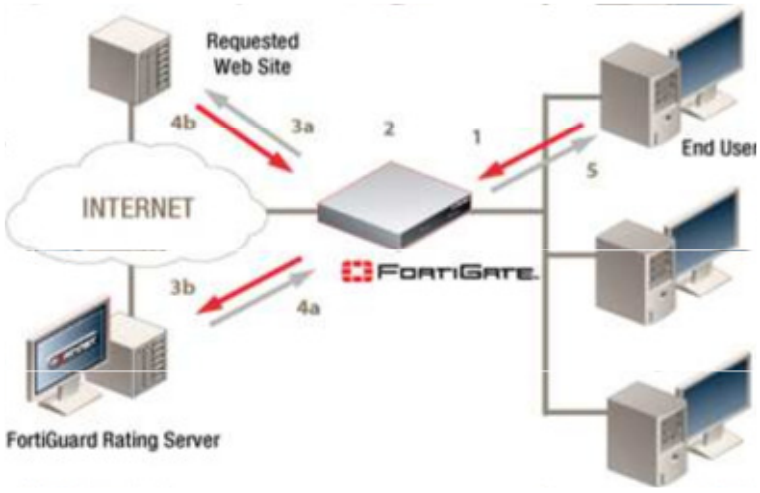


Figura 4: Servicio AntiSpam FortiGuard.

2.3 FORTIGATE

Es un sistema de administración de amenazas unificado (UTM) que mejora la seguridad de red, reduce el mal uso y abuso de la red y ayuda a utilizar más eficientemente los recursos de comunicaciones sin comprometer el rendimiento de la red. Los sistemas UTM FortiGate cuentan con certificaciones ICSA para firewall, IPSec y Antivirus.
FortiGate es un dispositivo de seguridad dedicado y de fácil administración que ofrece un paquete completo de capacidades entre las cuales se incluye:

- Servicios a nivel de aplicación. Ofrecen protección contra virus y filtrado de contenido.
- Servicios a nivel de red. Ofrecen protección mediante firewall, detección / prevención de intrusiones, VPN y modelado de tráfico.

El sistema UTM FortiGate utiliza tecnología DTPS (Dynamic Threat Prevention System), que aprovecha los avances tecnológicos en:

- Diseño del chip.
- Red.
- Seguridad.
- Análisis de contenido.

La arquitectura basada en tecnología ASIC analiza el contenido y el comportamiento en tiempo real lo que permite que aplicaciones de seguridad claves sean desplegadas justo en el límite de red donde son más eficaces para la protección de la misma.

2.3.1 Estado del sistema

- Página de Estado. Expone información del sistema, información de licencias, recursos del sistema, consola CLI, estado de la interfaz, consola de mensajes de alerta, estadística de tráfico y protección.
- Información del sistema. Permite cambiar la hora, el nombre y el modo de operación para el VDOM.
- Firmware FortiGate. Permite actualizar a una nueva versión o regresar a una versión antigua del software FortiOS.

- Historial de operación. Permite visualizar seis gráficos que presentan los recursos del sistema y la actividad de protección.
- Definiciones FortiGuard. Permite actualizar las bases de datos de las diferentes herramientas FortiGuard:
  - ✓ Antivirus.
  - ✓ Prevención de Intrusiones.
  - ✓ AntiSpam.
  - ✓ AntiSpyware.
  - ✓ Visor de estadísticas. Muestra información sobre sesiones, archivos de contenido y actividad de protección de red.
  - ✓ Visor de Topología. Permite diagramar y documentar las redes conectadas a la unidad FortiGate, para establecer un control y monitoreo de las mismas.

Figura 5: Visor de estadísticas FortiGate.

2.3.2 Uso de Dominios Virtuales

Los dominios virtuales (VDOMs) permiten a la unidad FortiGate funcionar como múltiples unidades virtuales independientes; una sola unidad puede servir separadamente a varias redes y ser la base de la administración del servicio de seguridad. Los VDOMs proporcionan diferentes dominios de seguridad que permiten separar zonas, autenticar usuarios, aplicar políticas de firewall / ruteo y configurar VPNs. Por defecto cada unidad tiene un VDOM llamado root, que incluye todas las interfaces

físicas, sub interfaces VLAN, zonas, políticas de firewall, configuraciones router y VPN.

2.3.3 Configuración FortiGate

Modo NAT / Router

En este modo la unidad FortiGate es visible para la red, sus interfaces están en diferente subred. Se puede establecer políticas de firewall para controlar las comunicaciones a través de la unidad FortiGate que controla el tráfico basado en la dirección origen, dirección destino y servicio de cada paquete.

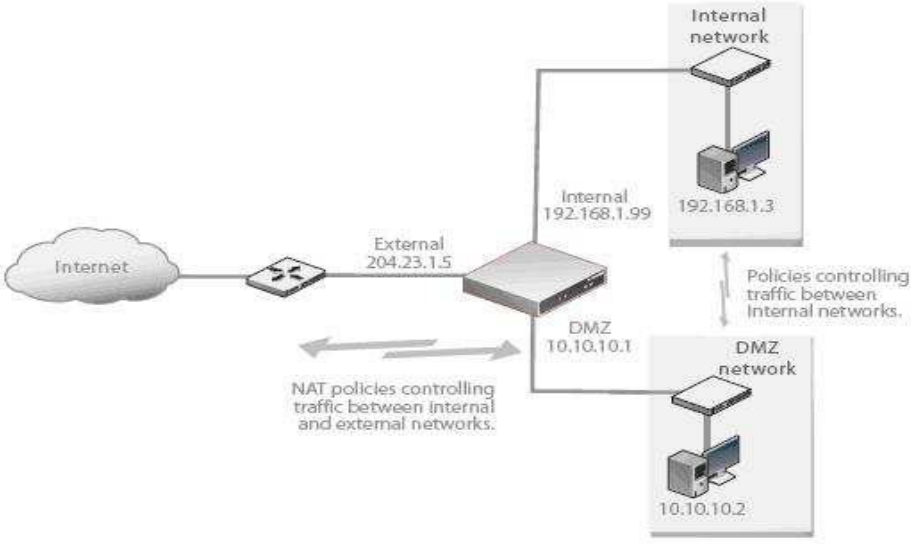


Figura 6: Configuración Modo NAT / Router.

En el modo NAT FortiGate realiza la traducción de la dirección de red antes de enviar el paquete a la red destino; en el modo Router no hay traducción de dirección. Se usa el modo NAT/Router cuando la unidad FortiGate está operando como un Gateway entre las redes pública y privada, se crean políticas de firewall en modo NAT para controlar el tráfico entre la red interna y la red externa y políticas de firewall en modo Router para controlar el tráfico entre las redes internas.

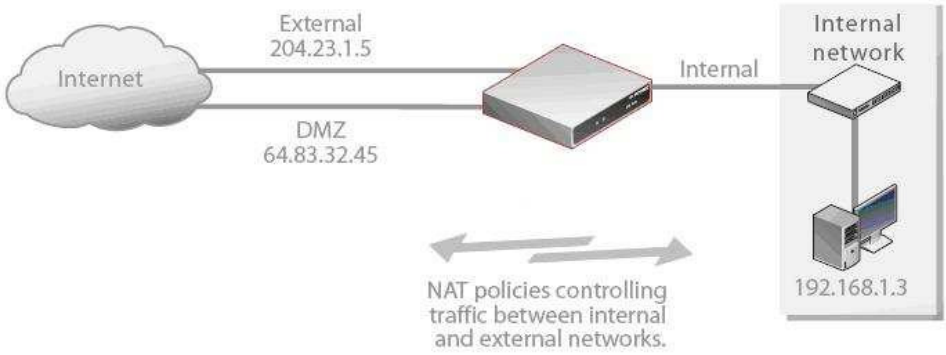


Figura 7: Configuración Modo NAT / Router con conexiones a Internet múltiple.

2.3.4 Modo Transparente

En el modo transparente la unidad FortiGate no es visible para la red, su comportamiento es similar a un puente de red y todas las interfaces de la unidad deben estar en la misma subred; solamente se configura una dirección IP de administración para poder realizar cambios en la configuración, actualizar el antivirus y las amenazas.

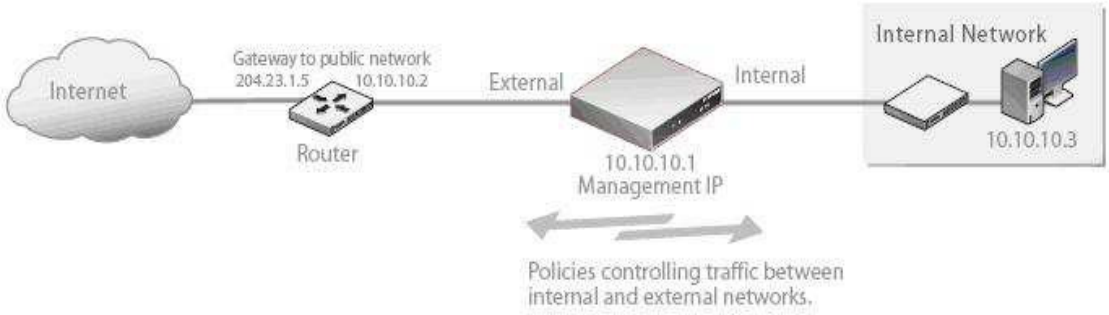


Figura 8: Configuración Modo Transparente.

El modo transparente se usa en redes privadas detrás de un firewall existente o detrás de un router.

La unidad FortiGate realiza las funciones de firewall, IPSec VPN, escaneo de virus, filtrado web, IPS y filtrado Spam; pueden conectarse hasta doce segmentos de red a la unidad FortiGate para controlar el tráfico de red entre éstos.

2.3.5 Sistema de red

2.3.5.1 Interfaz

- ✓ Cambio de Modo. En el modo switch la interfaz interna es configurada como una interfaz compartida por todos los puertos.

En el modo interfaz se puede configurar cada interfaz interna de forma separada, esto permite asignar diferentes subredes y máscaras de red a cada interfaz interna.

- ✓ Estándar IEEE 802.3ad. Permite agregar o combinar dos o más interfaces físicas para incrementar el ancho de banda o proporcionar redundancia de enlace.

- ✓ Configuración. Las interfaces de la unidad pueden ser configuradas para establecer enlaces ADSL, inalámbrico, PPPoE, PPPoA e IPSec, o para utilizar servicios como DHCP y DNS dinámico.

2.3.5.2 Zonas

Agrupan interfaces y sub interfaces VLAN relacionadas, con el fin de simplificar la creación de políticas que se aplicarán a las conexiones desde y hacia las zonas, mas no a las conexiones entre las interfaces de una misma zona.

2.3.5.3 Opciones de Red

- ✓ Servidor DNS. Varias funciones de la unidad FortiGate usan el servicio DNS, incluyendo las alertas e-mail y el bloqueo URL; se puede especificar la dirección IP del servidor DNS al cual se conecta la unidad.

- ✓ Detección del Gateway. Para confirmar la conectividad de red periódicamente se ejecutan pings hacia el servidor ping, que por lo general es el siguiente salto del router que se expone a la red externa o al Internet.

2.3.5.4 Tabla de ruteo estática

En el modo transparente se añaden rutas estáticas desde la unidad FortiGate hacia los routers locales.

2.3.5.5 Interfaz Módem

La interfaz módem puede ser usada como una interfaz de respaldo o como una interfaz independiente en el modo NAT/Route.
En el modo redundante, la interfaz módem automáticamente toma el control de la interfaz Ethernet no disponible (averiada).
En el modo independiente, la interfaz módem establece la conexión desde la unidad FortiGate hacia el Internet.

2.3.5.6 Soporte IPv6

Se puede asignar direcciones IPv4 e IPv6 a cualquier interfaz de la unidad FortiGate, la interfaz funciona como dos interfaces una para paquetes con dirección IPV4 y otro para paquetes con dirección IPV6.
La unidad FortiGate soporta ruteo estático, informes periódicos de ruteo, políticas firewall y tunneling de tráfico con direccionamiento IPv6 sobre una red direccionada con IPv4.

2.3.5.7 Sistema Inalámbrico

- ✓ Interfaz LAN inalámbrica FortiWiFi. Ésta interfaz puede ser configurada para:
- ✓ Proporcionar un punto de acceso al cual los usuarios con tarjetas de red inalámbricas pueden conectarse.
- ✓ Conectar la unidad FortiWiFi a otra red inalámbrica.

Las unidades FortiWiFi soportan los siguientes estándares de red inalámbricas:

- ✓ IEEE 802.11a (Banda 5 GHz).
- ✓ IEEE 802.11b (Banda 2.4 GHz).
- ✓ IEEE 802.11g (Banda 2.4 GHz).
- ✓ WEP (Wired Equivalent Privacy).
- ✓ WAP acceso protegido Wi-Fi usando pre-shared key o servidor RADIUS.

- ✓ Filtro MAC inalámbrico. Permitir o niega el acceso a la red inalámbrica basándose en la dirección MAC de cada tarjeta inalámbrica.

2.3.5.8 Sistema DHCP

El protocolo DHCP habilita a los host para obtener automáticamente su dirección IP asignada, además pueden obtener el Gateway y servidor DNS.
Una interfaz FortiGate o sub interfaz VLAN pueden proporcionar los siguientes servicios DHCP:

- Servidores DHCP regulares para conexiones Ethernet regulares.
- Servidores DHCP IPSec para conexiones IPSec (VPN).
- Transmisión DHCP para conexiones Ethernet o IPSec.

2.3.5.9 Configuración del Sistema

Alta disponibilidad (HA)

Mejora la confiabilidad e incrementa el rendimiento, la unidad FortiGate puede unirse a un cluster de alta disponibilidad.

2.3.5.10 SNMP

SNMP es un protocolo de administración simple que permite monitorear el hardware en la red; se puede configurar el hardware o el agente snmp de la unidad FortiGate para que reporte la información del sistema y envíe traps (alarmas o mensajes de eventos) al administrador SNMP. El administrador SNMP es una computadora corriendo una aplicación que puede leer las traps provenientes del agente y rastrear la información.
La implementación SNMP en FortiGate es de solo lectura, mediante la administración SNMP se puede tener acceso a las traps SNMP y a los datos de cualquier interfaz de la unidad FortiGate o sub interfaz VLAN configurada para el acceso de administración SNMP, lo que hace posible el monitoreo de la información de este sistema; pero para estar en capacidad de recibir traps FortiGate se debe compilar las MIBs propietarias de Fortinet así como las MIBs estándares soportadas por Fortinet en el administrador SNMP.

- ✓ **Comunidad snmp.** Una comunidad snmp consiste en la agrupación de equipos con el propósito de administrar la red, el administrador SNMP puede conectarse a la unidad FortiGate para observar la información del sistema y recibir traps SNMP; se puede añadir hasta tres comunidades SNMP y hasta ocho direcciones IP de administradores SNMP a cada comunidad.

- ✓ **MIBs Fortinet.** El agente SNMP de FortiGate soporta MIBs propietarias de Fortinet así como las MIBs estándar (RFC 1213 y RFC 2665); para comunicarse con el agente SNMP hay que compilar todas las MIBs estándar y privadas dentro del administrador SNMP.

- ✓ **Traps FortiGate.** El agente FortiGate puede enviar traps a los administradores SNMP que se agreguen a la comunidad SNMP; para recibir traps se debe cargar y compilar la MIB Fortinet 3.0 en el administrador SNMP. Las traps contienen el mensaje trap, el número serial de la unidad FortiGate y el Hostname.

Mensajes de reemplazo

La unidad FortiGate genera mensajes de reemplazo a una variedad de cadenas de contenido tales como mensajes e-mail infectados o bloqueados por spam, páginas web bloqueadas, sesiones FTP, etc, cuando detecta una amenaza.

Modo de operación y administración VDOM

Se puede cambiar el modo de operación de cada VDOM independientemente, así se puede combinar el modo de operación (NAT/Route o transparente) para cada una de las VDOMs de la unidad FortiGate; el acceso a la administración de cada VDOM puede ser restringida basándose en la interfaz y protocolo usado para la conexión con la interfaz.

2.4 ADMINISTRACIÓN DEL SISTEMA

Existen dos niveles de cuentas de administradores:

- **Administrador regular.** Es asignado a una VDOM y no puede tener acceso a la configuración global o a la configuración de otro VDOM al cual no haya sido asignado.
- **Administrador de sistema.** Tiene acceso completo a la configuración de la unidad FortiGate.

2.4.1 Perfil de acceso

Cada cuenta de administrador pertenece a un perfil de acceso; el perfil de acceso separa en categorías el control de acceso a las características de la unidad FortiGate, se puede habilitar accesos de lectura y/o escritura.

2.4.2 FortiManager

La unidad FortiGate se comunica con el servidor FortiManager mediante un enlace IPSec VPN que es transparente y viene pre configurado en la unidad FortiGate.

2.4.3 Mantenimiento del sistema

Respaldo y Restauración

Se puede respaldar la configuración del sistema, incluyendo los archivos de contenido web y archivos de filtrado spam a la computadora que administra o a un disco USB; también se puede restaurar la configuración del sistema de archivos de respaldo descargados con anterioridad.

2.4.4 Centro FortiGuard

El centro FortiGuard configura a la unidad FortiGate para acceder a la red de distribución FortiGuard (FDN) y a los servicios FortiGuard.

La red de distribución FortiGuard proporciona actualización de antivirus, definiciones de ataques, lista negra de direcciones IP en línea, lista negra de URL y otras herramientas de filtrado spam.

La lista negra de direcciones IP contiene direcciones IP de servidores e-mail que se conoce son usados para generar spam.

La lista negra de URL contiene URLs de sitios web encontrados en e-mails spam; también proporciona cientos de millones de páginas web clasificadas en un amplio rango de categorías que el usuario puede permitir, bloquear o monitorear.

2.4.5 Ruteo estático

Una ruta proporciona a la unidad FortiGate la información necesaria para enviar un paquete a un destino particular en la red; una ruta estática hace que los paquetes se envíen a un destino diferente del configurado por defecto. Opcionalmente se pueden definir políticas de ruteo, que permiten especificar criterios adicionales para examinar las propiedades de los paquetes entrantes, mediante el uso de políticas de ruteo se puede configurar a la unidad FortiGate para que dirija paquetes basándose en la dirección IP de origen y/o destino, la interfaz por la cual el paquete fue recibido, el protocolo (servicio) y/o el puerto que está siendo usado para transportar el paquete.

2.4.6 Ruteo dinámico

Trabaja con protocolos dinámicos para enrutar el tráfico a través de redes grandes y complejas; los protocolos dinámicos habilitan a la unidad FortiGate para que comparta información de ruteo automáticamente con routers vecinos y aprenda sobre rutas y redes anunciadas por sus routers vecinos. La unidad FortiGate soporta los siguientes protocolos de enrutamiento dinámico:

- Routing Information Protocol (RIP).
- Open Shortest Path First (OSPF).
- Border Gateway Protocol (BGP).
- Protocol Independet Multicast (PIM).

2.4.7 Políticas Firewall

Las políticas firewall controlan todo el tráfico que pasa a través de la unidad FortiGate, son instrucciones usadas para decidir qué hacer con una petición de conexión.
Cuando el Firewall recibe una petición de conexión en forma de paquete, éste es analizado para extraer la dirección origen, la dirección destino y el servicio (número de puerto), para ser evaluado con las políticas de firewall y tomar acciones sobre el paquete, como permitir

la conexión, negar la conexión, pedir autenticación antes de permitir la conexión o procesar al paquete como un paquete VPN IPSec.

2.4.8 Virtual IP – Firewall

- ✓ **Virtual IPs:** Las direcciones IP virtuales pueden ser usadas para permitir conexiones a través de la unidad FortiGate usando políticas firewall de tipo NAT. Las IPs virtuales usan un proxy ARP para que la unidad FortiGate pueda responder a peticiones ARP pertenecientes a un servidor que actualmente está instalado en otra red; así la unidad FortiGate se presenta como el servidor y la red interna permanece oculta al público.

- ✓ **Pool de IPs:** Son utilizadas para añadir políticas NAT que traduzcan dinámicamente direcciones origen de los paquetes salientes a direcciones aleatorias seleccionadas del pool IP antes que limitarse a la dirección IP de la interfaz de destino. Un pool IP define una dirección o un rango de direcciones IP que responden a las peticiones ARP en la interfaz a la cual ha sido asignado el pool IP.

- ✓ **Perfil de protección Firewall:** El perfil de protección es un grupo de configuraciones que pueden modificarse para ajustarse a un propósito particular; se pueden usar perfiles de protección para cada tipo de tráfico que maneja una política firewall, se tiene:
  - Configurar la protección antivirus para políticas HTTP, FTP, IMAP, POP3, SMTP e IM.
  - Configurar el filtrado web para políticas HTTP y HTTPS.
  - Configurar el filtrado web por categorías para políticas HTTP y HTTPS.
  - Configurar el filtrado spam para políticas IMAP, POP3 y SMTP.
  - Habilitar IPS para todos los servicios.
  - Configurar el archivo de contenido para políticas HTTP, HTTPS, FTP, IMAP, POP3, SMTP e IM.
  - Configurar filtrado IM y control de acceso para mensajería instantánea AIM, ICQ, MSN, Yahoo y SIMPLE.
  - Configurar acceso P2P y control del ancho de banda para clientes punto a punto Bit

- Torrent, eDonkey, Gnutella, Kazaa, Skype, WinNY, Emule y Ares.
- Configurar cuales acciones del perfil de protección serán registradas.
- Configurar la capacidad para los protocolos VoIP, SIP y SCCP.

Mediante los perfiles de protección se puede personalizar los tipos y niveles de protección para diferentes políticas firewall.

La unidad FortiGate tiene pre-configurados cuatro perfiles de protección:

- Estricto. Aplica máxima protección al tráfico HTTP, FTP, IMAP, POP3 y SMTP.
- Escanear. Aplica escaneo de virus al tráfico HTTP, FTP, IMAP, POP3 y SMTP.
- Web. Aplica escaneo de virus y bloqueo de contenido web para el tráfico HTTP.
- No filtrado. No aplica escaneo, bloqueo o IPS.

2.4.9 IPSec (Internet Protocol Security)

La unidad FortiGate implementa el protocolo ESP (Encapsulated Security Payload), donde los paquetes encriptados aparecen como paquetes ordinarios que pueden ser enrutados a través de cualquier red IP, el procedimiento IKE (Internet Key Exchange) es realizado automáticamente basándose en pre-shared keys o certificados digitales X.509, aunque también se pueden especificar claves manualmente.
Cuando se define una ruta basada en un túnel IPSec, una interfaz IPSec virtual es creada automáticamente como una sub-interfaz en la interfaz física, agregada o VLAN de la unidad FortiGate esto es conocido como IPSec modo interfaz.

Una interfaz virtual IPSec es considerada en funcionamiento cuando puede establecer una conexión de fase 1 con un punto similar VPN o un cliente; sin embargo la interfaz virtual IPSec no puede ser usada para enviar tráfico a través de un túnel hasta pasar a la fase 2 de definición; después de que una interfaz virtual IPSec ha sido asignada a un túnel, el tráfico puede ser enrutado a la interfaz usando métricas específicas tanto para rutas estáticas como para políticas de rutas, además se pueden crear políticas de firewall considerando a la interfaz virtual IPSec como la interfaz origen o destino.

Cuando el tráfico IP se origina detrás de la unidad FortiGate local busca una interfaz FortiGate de salida que actúe como el punto final local del túnel IPSec, el tráfico es encapsulado por el túnel y enviado a través de la interfaz física a la cual pertenece la interfaz virtual IPSec.

Cuando el tráfico encapsulado de un punto VPN remoto o de un cliente busca una interfaz física local de la unidad FortiGate, ésta determina si una interfaz virtual IPSec está asociada a la interfaz física a través de selectores en el tráfico; si el tráfico coincide con los selectores predefinidos, éste es des-encapsulado y enviado a la interfaz virtual IPSec.

En la dirección saliente, la unidad FortiGate realiza un lazo de ruteo para encontrar la interfaz a través de la cual debe enviar el tráfico para alcanzar el siguiente router, si la unidad encuentra una ruta a través de una interfaz virtual que está ligada a un túnel VPN específico, el tráfico es encriptado y enviado a través del túnel VPN.

En la dirección entrante, la unidad identifica un túnel VPN usando la dirección IP de destino y el SPI (Security Parameter Index) en el datagrama ESP, luego para completar la fase 2 se analiza la SA (Security Association); si una coincidencia SA es encontrada, el datagrama es des encriptado y el tráfico IP asociado es re direccionado a través de la interfaz virtual IPSec.

- Fase uno. En la fase 1 los dos puntos VPN se autentican uno al otro e intercambian claves para establecer un canal de comunicación segura entre ellos.
- Intercambio de información de autenticación encriptado o no encriptado.
- Uso de pre-shared key o certificados digitales para la autenticación de las entidades de los puntos VPN.
- Uso de un identificador especial, un certificado de nombre distinguido o nombre de grupo para identificar el punto VPN remoto o cliente remoto.

Fase dos. Los parámetros de la fase 2 definen los algoritmos que la unidad FortiGate puede usar para cifrar y transferir los datos por el resto de la sesión; durante la fase 2, las asociaciones de seguridad específicas de IPSec requeridas para implementar servicios de seguridad son seleccionadas y un túnel es establecido.

2.4.10 PPTP

La unidad FortiGate soporta PPTP para túneles con tráfico PPP entre dos puntos VPN, los clientes PPTP de Windows o Linux pueden establecer un túnel PPTP con una unidad FortiGate configurada para actuar como servidor PPTP, también se puede configurar la unidad para enviar los paquetes PPTP al servidor PPTP de la red detrás de la unidad FortiGate.

Las VPN PPTP son posibles solo en el modo NAT/Route y se permiten hasta 254 sesiones PPTP y L2TP.

2.4.11 SSL

La unidad FortiGate permite establecer sesiones SSL en el modo NAT/Route, para operaciones en modo túnel o modo web y si se requiere se puede habilitar el uso de certificados digitales para la autenticación de usuarios remotos.

2.4.12 Autenticación de usuarios

Servidor RADIUS

Si el usuario requiere autenticarse usando un servidor RADIUS, la unidad FortiGate envía las credenciales del usuario al servidor RADIUS para su autenticación; si el servidor RADIUS puede autentificar al usuario, el mismo es autentificado exitosamente con la unidad FortiGate, caso contrario la conexión es rechazada por la unidad FortiGate.

2.4.13 Servidor LDAP

Si el usuario requiere autenticarse usando un servidor LDAP, la unidad FortiGate contacta al servidor LDAP para la autenticación. Para autenticarse con la unidad FortiGate el usuario ingresa un nombre y contraseña, los mismos que son enviados al servidor LDAP, donde se realiza el procedimiento de autenticación, si el usuario es autenticado positivamente obtiene el accesos a la unidad FortiGate, caso contrario la

conexión es rechazada. Adicionalmente FortiGate LDAP soporta LDAP sobre SSL / TLS.

2.4.14 Autenticación PKI

Utiliza una biblioteca de certificados de autenticación, así los usuarios necesitan solamente un certificado válido para su autenticación.

2.4.15 Servidor AD de Windows

En las redes que usan servidores Windows Active Directory (AD) para la autenticación, la unidad FortiGate puede autenticar a los usuarios de forma transparente sin necesidad de preguntarles su nombre de usuario y contraseña, para lo cual se debe instalar FSAE (Fortinet Server Authentication Extensions) en la red y configurar la unidad FortiGate para recuperar información del servidor Windows AD.

2.4.16 Grupo de usuario

Es una lista de identidades de usuario, donde una identidad puede ser:

- Una cuenta de usuario local (nombre de usuario y contraseña) almacenado en la unidad FortiGate.
- Una cuenta de usuario local con una contraseña almacenada en un servidor
- RADIUS o LDAP.
- Un servidor RADIUS o LDAP (todas las identidades almacenadas en el servidor pueden ser autentificadas).
- Un grupo de usuarios definidos en un servidor Microsoft Active Directory.

En la mayoría de los casos la unidad FortiGate autentica a los usuarios mediante su nombre de usuario y contraseña, primero chequea las cuentas de usuarios locales, luego los servidores RADIUS o LDAP que pertenecen al grupo de usuario; la autenticación es exitosa cuando encuentra una coincidencia. Para el grupo de usuario de AD la autenticación se realiza cuando el usuario entra a la red

mediante el agente de FSAE la unidad FortiGate recibe el nombre de usuario y la dirección IP.

2.4.17 AntiVirus

El procedimiento antivirus engloba varios módulos y motores que realizan tareas separadas; los elementos antivirus trabajan en secuencia para proporcionar un método de escaneo eficiente para los archivos entrantes; estos elementos trabajan para ofrecer a la red una protección antivirus incomparable.
Además para asegurar la mejor protección disponible, todas las definiciones y firmas de virus son actualizadas regularmente mediante los servicios antivirus FortiGuard.

2.4.18 Archivo patrón

Una vez que un archivo es aceptado, la unidad FortiGate aplica el filtro de reconocimiento de patrón de archivo y compara el archivo entrante con el patrón de archivo configurado, si el archivo tiene un patrón de bloqueo, éste es detenido y un mensaje de reemplazo es enviado al usuario final, además ningún otro nivel de protección es aplicado; pero si el archivo no es bloqueado entonces otros niveles de protección son aplicados.
El patrón de archivos sirve para bloquear archivos que constituyen una potencial amenaza y prevenir los ataques de virus; los archivos pueden ser bloqueados por nombre, extensión o cualquier otro patrón, así se proporciona la flexibilidad para bloquear potencial contenido dañino. La lista de archivos patrón está pre configurada con una lista por defecto de archivos patrón:

- Archivos ejecutables (*.bat, *.com y *.exe).
- Archivos comprimidos (*.gz, *.rar y *.tar, *.tgz y *.zip).
- Librerías de enlace dinámico (*.dll).
- Aplicaciones html (*.hta).
- Archivos Microsoft Office (*.doc, *.ppt y *.xl?).
- Archivos Microsoft Works (*.wps).
- Archivos Visual Basic (*.vb?).
- Archivos screen saver (*.scr).

- Archivos de información de programa (*.wps).

2.4.19 Escáner de virus

Si el archivo ha pasado el módulo archivo patrón, entonces se le se aplica el scanner de virus; las definiciones de virus son almacenadas y actualizada periódicamente a través de FDN. La unidad FortiGate usa las definiciones de virus para detectar y remover virus, gusanos, troyanos y otras amenazas de contenido.
La lista de virus muestra en orden alfabético las definiciones de virus FortiGuard actualizadas que se encuentran instaladas en la unidad FortiGate.

2.4.20 Grayware

Una vez que el archivo entrante ha pasado los módulos archivo patrón y escáner de virus, será chequeado por el módulo grayware.
Los programas grayware son software comercial no solicitado que se instalan en computadoras generalmente sin el conocimiento o consentimiento del usuario; estos programas son considerados una molestia ya que causan problemas en el rendimiento del sistema o son usados para fines maliciosos. La lista de categorías y contenidos grayware son añadidos o actualizados cuando la unidad FortiGate recibe los paquetes de actualización de virus.
Las categorías grayware que se pueden habilitar para que la unidad FortiGate los bloquee son:

- Adware.
- Dial.
- Download.
- Game.
- Hacker Tool.
- Hijacker.
- Joke.
- RAT (Remote Administration Tools).
- NMT (Network Management Tools).

- Keylog.
- Misc.
- P2P.
- Plugin.
- Spy.
- Toolbar.
- BHO (Block browser Helper Objects, son archivos dll).

Heurístico

Finalmente, luego de haber pasado los tres módulos anteriores, el archivo entrante es sometido al módulo heurístico. El motor heurístico de la unidad FortiGate realiza pruebas en el archivo para detectar virus basándose en indicadores de comportamiento o en virus conocidos, es así que se puede detectar nuevos virus pero también se pueden producir resultados falsos positivos.

Cuarentena

La unidad FortiGate con disco duro puede poner en cuarentena a archivos bloqueados e infectados para ver el nombre y la información de estado de éstos; además pueden ser cargados automáticamente al análisis Fortinet. Para las unidades FortiGate que no cuentan con disco duro, se puede configurar para que los archivos bloqueados e infectados sean enviados a la unidad FortiAnalyzer.

Protección contra intrusos

El sistema de prevención de intrusos (IPS) FortiGuard combina la detección de firmas y anomalías para descubrir y prevenir las intrusiones al sistema, con baja latencia y excelente confiabilidad. La unidad FortiGate puede grabar el tráfico sospechoso en logs, puede enviar alertas e-mail al sistema administrador y puede registrar, comunicar, soltar, restaurar y limpiar sesiones o paquetes sospechosos. También es posible habilitar o deshabilitar todas las firmas o anomalías en cada perfil de protección firewall.

Firmas

El IPS FortiGate compara el tráfico de red con los patrones contenidos en las firmas de ataques, las firmas de los ataques protegen la red de los ataques conocidos. La unidad FortiGate permite modelar nuevas firmas de acuerdo a las necesidades de la red además de las firmas predefinidas.

Decodificador de protocolo

El IPS FortiGate usa la detección de anomalías para identificar el tráfico de red que intenta tomar ventaja de debilidades conocidas.

Anomalías

El IPS FortiGate usa la detección de anomalías para identificar el tráfico de red que no encaja en los patrones de tráfico predefinidos o conocidos; identifica cuatro tipos de anomalías estadísticas para los protocolos TCP, UDP e ICMP:

- Flooding.
- Scan.
- Source session limit.
- Destination session limit.

Las siguientes son las acciones de respuesta cuando se detecta un patrón de firma o una anomalía:

Action	Description
Pass	When a packet triggers a signature, the FortiGate unit generates an alert and allows the packet through the firewall without further action. If logging is disabled and action is set to Pass, the signature is effectively disabled.
Drop	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The firewall session is not touched. Fortinet recommends using an action other than Drop for TCP connection based attacks.
Reset	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The FortiGate unit sends a reset to both the client and the server and drops the firewall session from the firewall session table. This is used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset action is triggered before the TCP connection is fully established, it acts as Clear Session.
Reset Client	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The FortiGate unit sends a reset to the client and drops the firewall session from the firewall session table. This is used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Client action is triggered before the TCP connection is fully established, it acts as Clear Session.
Reset Server	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The FortiGate unit sends a reset to the server and drops the firewall session from the firewall session table. This is used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Server action is triggered before the TCP connection is fully established, it acts as Clear Session.
Drop Session	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. For the remainder of this packet's firewall session, all follow-up packets are dropped.
Pass Session	When a packet triggers a signature, the FortiGate unit generates an alert and allows the packet through the firewall. For the remainder of this packet's session, the IPS is bypassed by all follow-up packets.
Clear Session	When a packet triggers a signature, the FortiGate unit generates an alert and the session to which the packet belongs is removed from the session table immediately. No reset is sent. For TCP, all follow-up packets could be dropped. For UDP, all follow-up packets could trigger the firewall to create a new session.

Tabla 1: Respuestas ante amenazas detectadas por el dispositivo UTM.

Filtro web

Los filtros web son aplicados en el siguiente orden:

1. URL de excepción.
2. URL bloqueada.
3. URL patrón bloqueada.
4. Categoría URL web bloqueada.
5. Contenido web bloqueado.
6. Filtro script.
7. Escaneo de virus.

Bloqueo de contenido

Controla el contenido web al bloquear palabras o patrones específicos; si se habilita en el perfil de protección, la unidad FortiGate busca las palabras o patrones en las páginas web solicitadas, una coincidencia es encontrada cuando los valores asignados a las palabras son totales, si el valor de umbral definido de un usuario es excedido, la página web es bloqueada.

Filtro URL

Permite o bloquea el acceso a URLs específicas, las cuales han sido añadidas a la lista de filtrado; se añaden los patrones usando texto o expresiones regulares (caracteres wildcard). La unidad FortiGate permite o bloquea páginas web comparándolas con las URLs o patrones especificados y despliega un mensaje de reemplazo a cambio indicando que la página no es accesible de acuerdo a las políticas de uso de Internet.

Filtro web FortiGuard

Es una solución de filtrado web administrada y provista por Fortinet que clasifica cientos de millones de páginas web dentro de un amplio rango de categorías que los usuarios pueden permitir, bloquear o monitorear.

La unidad FortiGate accede al punto de servicio FortiGuard - Web más cercano para determinar la categoría de una página solicitada, entonces continúa a la política firewall configurada por el usuario en la interfaz.

FortiGuard - Web abarca millones de valoraciones individuales de sitios web aplicándose a cientos de millones de páginas; las páginas son clasificadas y valoradas en 56 categorías

que los usuarios pueden permitir, bloquear o monitorear; las categorías pueden ser añadidas o actualizadas según como el Internet evolucione.

La valoración de FortiGuard - Web es realizada mediante la combinación de métodos propietarios como análisis de texto, explotación de la estructura web y la intervención humana en la clasificación; los usuarios pueden notificar a los puntos de servicio FortiGuard - Web si piensan que una página no está categorizada correctamente además nuevos sitios son clasificados rápidamente. Si se necesita acceder a un sitio web restringido se puede anular temporalmente la regla.

AntiSpam

Esta funcionalidad puede ser configurada para manejar e-mails comerciales no solicitados, mediante la detección de mensajes e-mail spam e identificación de transmisiones spam provenientes de servidores spam conocidos o sospechosos.

FortiGuard - AntiSpam es una de las características diseñadas para manejar el spam; incluye una lista negra de direcciones IP, una lista negra de direcciones URL y herramientas de filtrado spam.
El orden en el cual los e-mails entrantes pasan a través de los filtros AntiSpam de FortiGate está determinado por el protocolo usado para transferir el e-mail.

- **Para SMTP:**

1. Verificación BWL (Black / White List) de la dirección IP con el último brinco IP.
2. Verificación RBL (Realtime Blackhole List) & ORDBL (Open Relay Database List), FortiGuard verifica la dirección IP, mediante HELO DNS lookup.
3. Verificación BWL de la dirección e-mail.
4. Verificación de la cabecera MIME (Multipurpose Internet Mail Extensions).
5. Verificación BWL de la dirección IP (para IPs extraídas de las cabeceras recibidas).
6. Verificación DNS de retorno de e-mails, verificación FortiGuard – AntiSpam (para IPs extraídas de las cabeceras recibidas y URLs en el contenido e-mail).
7. Verificación de palabras prohibidas en el asunto e-mail.
8. Verificación de palabras prohibidas en el contenido e-mail.

- **Para POP3 e IMAP:**

1. Verificación BWL de la dirección e-mail.
2. Verificación de la cabecera MIME, verificación BWL de la dirección IP.
1. 3. Verificación DNS de retorno de e-mails, verificación FortiGuard - AntiSpam, verificación RBL & ORDBL.
3. Verificación de palabras prohibidas en el asunto e-mail.
4. Verificación de palabras prohibidas en el contenido e-mail.

Para SMTP, POP3 e IMAP los filtros requieren preguntar a un servidor (servicio FortiGuard-AntiSpam, DNSBL/ORDBL) y una respuesta es ejecutada simultáneamente; para evitar retardos, las interrogantes son enviadas mientras otros filtros se están ejecutando, la primera respuesta a un trigger es una acción spam que toma efecto tan pronto como la respuesta es recibida. Cada filtro spam pasa el e-mail al siguiente filtro si no se encuentran coincidencias o problemas. Si la acción en un filtro es "Mark as Spam", la unidad FortiGate etiquetará o desechará (solo en SMTP) el e-mail de acuerdo a las configuraciones del perfil de protección. Si la acción en un filtro es "Mark as Clear", el e- mail estará exento de cualquier filtro restante. Si la acción en un filtro es "Mark as Reject", la sesión e-mail es dada de baja. Los mensajes e-mail SMTP rechazados son substituidos con mensajes de reemplazo configurables.

Palabras prohibidas

El control spam por bloqueo de mensajes e-mail contiene palabras o patrones específicos, si se habilita en el perfil de protección, la unidad FortiGate busca palabras o patrones en el mensaje e-mail.

La unida FortiGate usa una lista de direcciones IP y una lista de direcciones e-mail para filtrar los e-mail entrantes; cuando se realiza la verificación en la lista de direcciones IP, la unidad FortiGate compara la dirección IP del que envía el mensaje con la lista de direcciones IP en forma secuencial, si se encuentra una coincidencia se toma la acción asociada con la dirección IP caso contrario el mensaje pasa al siguiente filtro spam habilitado. Cuando se realiza la verificación en la lista de direcciones e-mail, la unidad FortiGate compara la dirección e-mail del que envía el mensaje con la lista de direcciones e-mail en forma secuencial, si se encuentra una coincidencia se toma la acción

asociada con la dirección e-mail caso contrario el mensaje pasa al siguiente filtro spam habilitado.

IM, P2P & VoIP

La unidad FortiGate puede controlar y monitorear el uso de aplicaciones IM/P2P y protocolos VoIP (SIP y SCCP).

Fortinet reconoce que estas aplicaciones son parte de los negocios pero si se abusa de las mismas pueden degradar la productividad y el rendimiento de la red.

El sistema FortiGate permite configurar la lista de usuarios para permitir o bloquear el uso de este tipo de aplicaciones a más de asignar el ancho de banda a ser usado por las mismas.

SOFTWARE PARA PROTECCIÓN

FortiClient

Es un software para seguridad host, provee un ambiente de computación seguro para computadoras de escritorio y portátiles que corren el sistema operativo Microsoft Windows y brinda las siguientes funcionalidades:

- Creación de conexiones VPN con redes remotas.
- Configuración de protección en tiempo real contra virus.
- Protección contra la modificación del registro de Windows.
- Escaneo de virus.

FortiMail

Es una plataforma de mensajes segura, provee escaneo heurístico flexible e informa de la capacidad de entrada y salida del tráfico e-mail. La unidad FortiMail utiliza el escaneo DCC (Distributed Checksum Clearinghouse) y Bayesiano que brindan alto rendimiento y confiabilidad para la detección y bloqueo de anexos maliciosos.

Gracias a la tecnología FortiASIC y FortiOS, el antivirus FortiMail extiende las capacidades de inspección de contenido para detectar las amenazas de correo electrónico más avanzadas.

FortiBridge

Estos productos son diseñados para proveer tráfico de red continuamente en caso de un corte de energía o un fallo en el sistema FortiGate; son productos fáciles de usar e implementar y se pueden personalizar las acciones a tomar en caso de fallos.
La unidad FortiBridge evita la unidad FortiGate para asegurarse que la red pueda continuar procesando tráfico.

FortiManager

Es un sistema diseñado para cubrir las necesidades de empresas grandes responsables de establecer y mantener las políticas de seguridad de varias instalaciones FortiGate dispersas. Con este sistema se puede configurar múltiples dispositivos FortiGate y monitorear su estado, también se puede ver el historial de logs y logs en tiempo real, incluyendo la actualización de imágenes de los dispositivos FortiGate administrados. Este sistema es de fácil uso y se integra fácilmente a otros sistemas.

2.5 FORTIANALYZER

Es un dispositivo de red que provee herramientas para la obtención de reportes, ejecución de análisis de datos y recopilación integrada de logs. Los informes de log detallados proveen el análisis tanto histórico como en tiempo real del tráfico de red, e-mail, FTP, actividad web, actividad de virus, actividad spam y actividad de ataques de intrusión, para ayudar a identificar las cuestiones de seguridad y reducir el mal uso y abuso de la red.
Provee a los administradores de red una visión exhaustiva del uso de red y la información de seguridad, cubre las necesidades de empresas y proveedores de servicios responsables por descubrir y direccionar las vulnerabilidades a través de los sistemas FortiGate dispersos.

Los dispositivos FortiAnalyzer minimizan el esfuerzo requerido para monitorear y mantener políticas de uso aceptable, identificar patrones de ataques, enjuiciar a los atacantes, obedecer reglamentos gubernamentales respecto a la privacidad y develación de la información. Aceptan y procesan un amplio rango de registros (logs) proporcionados por los sistemas FortiGate, provee funciones de administración de seguridad avanzadas como

archivos en cuarentena, correlación de eventos, valoración de vulnerabilidades, análisis de tráfico y de archivos de contenido.

Los registros log de los sistemas FortiGate / FortiMail son transmitidos al sistema FortiAnalyzer usando túneles VPN encriptados para garantizar la seguridad en la transmisión de archivos log y archivos puestos en cuarentena. Su capacidad varía desde 250GB hasta 4.8TB de datos log y niveles RAID (Redundant Array of Inexpensive Disks) de 0, 1, 5, 10 y 50 que pueden ser seleccionados para soportar el nivel deseado entre capacidad y seguridad de los datos.

2.5.1 Características

FortiAnalyzer recibe los archivos log de varios dispositivos FortiGate, FortiMail, FortiManager, FortiClient y demás servidores syslog; además por su capacidad de reportes robusta puede monitorear el tráfico, los ataques y el mal uso de la red por parte de los usuarios.

2.5.2 Registros

La unidad FortiAnalyzer crea sus propios mensajes log del sistema en relación a su actividad, eventos de seguridad y negociaciones IPSec para la transmisión segura de los paquetes que contienen los mensajes log.

- **Registros locales.** Permite almacenar los mensajes log en el disco duro de la unidad FortiAnalyzer local.
- **Registros para un host**. Permite enviar los mensajes log de la unidad FortiAnalyzer a un servidor Syslog.

2.5.3 Reportes

- **Análisis log y reportes.** Analiza logs presentados por múltiples dispositivos y genera una variedad de reportes que hacen posible una seguridad de red proactiva, ya que permite conocer las amenazas que aparecen, evitar el abuso de red, administrar los requerimientos de ancho de banda y monitorear los sitios web visitados a fin de asegurar el uso apropiado de la red.

- Reportes de vulnerabilidades. Presenta las debilidades potenciales ante ataques que podrían existir para un dispositivo seleccionado. FortiAnalyzer consulta los puertos abiertos y la información sobre el servicio que se ejecuta, para dar a conocer las vulnerabilidades existentes para este servicio.

2.5.4 Significado de los datos

Permite fácil acceso a reportes simples para obtener información sobre los intentos de intrusión y el tipo de tráfico en la red. Los resúmenes de eventos de seguridad proporcionan una vista rápida del tráfico no deseado que intenta romper la seguridad del Firewall (virus, intrusiones y actividad sospechosa) y los creadores de tráfico excesivo en la red, mientras que los resúmenes de tráfico proporcionan una vista rápida del tráfico que atraviesa el Firewall e ingresa a la red.

2.5.5 Analizador de red

Actúa como un sniffer que captura datos del tráfico de red para almacenarlos en el disco duro o generar reportes en base a éstos.
El analizador de red usa un puerto dedicado de la unidad FortiAnalyzer que se conecta al switch, permite alcanzar áreas de red donde el Firewall de FortiGate no se esté utilizando o si no se tiene un FortiGate como Firewall.

2.5.6 Visor de Logs

El navegador de logs permite visualizar los mensajes log enviados al FortiAnalyzer desde los dispositivos registrados; permite ver cualquier mensaje o archivo log guardado en el disco duro. Todos los archivos y mensajes pueden ser explorados y filtrados para localizar información específica.

- Visor de logs en tiempo real. Provee registros en tiempo real de tráfico Web, FTP y correo electrónico mediante registros de contenido.
  El visor de contenidos ofrece una visualización en tiempo real de la información meta de los dispositivos registrados. La información meta incluye la fuente y el

destino de la información, lo que permite seguir en tiempo real las tendencias de uso de la red.

- Visor del historial de logs. Permite visualizar la información log de un rango de tiempo específico y filtrarla para encontrar información de eventos específicos.

2.5.7 Agregación de Logs

Es un método que permite recopilar datos log de dispositivos FortiAnalyzer remotos u otros dispositivos de red que soporten el formato syslog a una unidad FortiAnalyzer central.

La unidad FortiAnalyzer actúa como cliente cuando envía logs a un servidor de agregación, y como servidor cuando recibe los logs de los clientes de agregación.

2.5.8 Cuarentena

Para los FortiGate que no tienen disco duro, FortiAnalyzer ofrece la habilidad de poner en cuarentena archivos sospechosos o infectados que entran en el ambiente de red. Mediante el explorador de cuarentena se puede observar los archivos para determinar si son peligrosos o no.

2.5.9 Almacenamiento en red

FortiAnalyzer actúa como un dispositivo NAS, se lo usa como un medio de respaldo para almacenar información importante en el espacio extra del disco duro, como un servidor de archivos o repositorio.

2.5.10 RAID

FortiAnalyzer utiliza múltiples discos duros para almacenar los datos log usando un arreglo RAID para ofrecer almacenamiento redundante, protección de los datos, rápido acceso al disco duro o una gran capacidad de almacenamiento.

2.5.11 LDAP

La unidad FortiAnalyzer usa LDAP para consultar al servidor Active Directory de Windows sobre los nombres usuarios o grupos para generar los reportes.

2.5.12 Análisis Forense

Proporciona un método de vigilancia y reportes sobre individuos o grupo de personas a cerca de su tráfico de red, correo electrónico y mensajes instantáneos; permitiendo al administrador reducir la información a determinados individuos o grupos de personas.
Además permite ejecutar reportes con información detallada sobre el acceso a sitios web, accesos web bloqueados, correo electrónico, FTP y mensajes instantáneos durante un periodo específico en la red.

2.5.13 Alertas

Informan sobre los asuntos que se originan en un FortiGate, en la red o en el mismo FortiAnalyzer, tales como fallas del sistema o ataques de red, permitiendo reaccionar inmediatamente ante el evento; puede enviar los mensajes de alerta a direcciones de correo electrónico, servidores syslog o como traps SNMP, para informar a los administradores sobre los sucesos y su origen.

2.5.14 Escáner de vulnerabilidades

La unidad FortiAnalyzer genera un informe de las vulnerabilidades de los host que están en riesgo ante los ataques de hackers y spyware.
El escáner de vulnerabilidades entra al host y escanea los puertos, el software y las aplicaciones instaladas; esta exploración revela posibles puntos de ataque que pueden ser explotados para acceder a la información del computador o afectar su operación. El informe de la vulnerabilidad provee la información sobre la gravedad de la amenaza de seguridad y los parches disponibles o las soluciones conocidas para eliminar la amenaza.
El escáner de vulnerabilidades usa conexiones Remote Vulnerability Scan (RVS) y un motor RVS que es actualizado a través de la red de distribución Fortinet (FDN).

2.6 FORTIREPORTER

Es un software de análisis de seguridad, que genera informes de fácil comprensión y puede recopilar logs de cualquier unidad FortiGate y de otros dispositivos de seguridad (otros vendedores).

2.6.1 Análisis Forense

Proporciona un método de vigilancia y reportes sobre individuos o grupo de personas a cerca de su tráfico de red, correo electrónico y mensajes instantáneos; permitiendo al administrador reducir la información a determinados individuos o grupos de personas.
Además permite ejecutar reportes con información detallada sobre el acceso a sitios web, accesos web bloqueados, correo electrónico, FTP y mensajes instantáneos durante un periodo específico en la red.

2.6.2 Alertas

Informan sobre los asuntos que se originan en un FortiGate, en la red o en el mismo FortiAnalyzer, tales como fallas del sistema o ataques de red, permitiendo reaccionar inmediatamente ante el evento; puede enviar los mensajes de alerta a direcciones de correo electrónico, servidores syslog o como traps SNMP, para informar a los administradores sobre los sucesos y su origen.

2.6.3 Escáner de vulnerabilidades

La unidad FortiAnalyzer genera un informe de las vulnerabilidades de los host que están en riesgo ante los ataques de hackers y spyware.
El escáner de vulnerabilidades entra al host y escanea los puertos, el software y las aplicaciones instaladas; esta exploración revela posibles puntos de ataque que pueden ser explotados para acceder a la información del computador o afectar su operación. El

informe de la vulnerabilidad provee la información sobre la gravedad de la amenaza de seguridad y los parches disponibles o las soluciones conocidas para eliminar la amenaza.

El escáner de vulnerabilidades usa conexiones Remote Vulnerability Scan (RVS) y un motor RVS que es actualizado a través de la red de distribución Fortinet (FDN).

La tecnología ofrecida por Fortinet se presenta como la más apropiada al momento de hablar sobre UTM, siendo este proveedor el que lidera actualmente el mercado.

Los UTM de Fortinet ayudan a frustrar ataques combinados1, mediante una amplia variedad de funcionalidades y servicios de seguridad; además, soportan sólidamente aplicaciones exigentes, mediante sistemas hardware de alto rendimiento ya que utilizan microprocesadores ASIC, exclusivamente diseñados para soportar el análisis que requieren los temas de seguridad.

3. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED DE C.I. OCEANOS S.A

3.1 DESCRIPCIÓN DE LA ENTIDAD.

C.I. Océanos S.A. es una empresa que hace parte del Grupo Manuelita desde 1987. Es la mayor compañía colombiana productora de camarones de cultivo. Cuenta con 1.052 hectáreas en cultivos y con una planta de procesos capaz de procesar más de 7.000 toneladas anuales de camarón. Su principal mercado es el europeo, mediante canales de distribución de grandes superficies y mayoristas.

C.I. Océanos S.A. está ubicada en Cartagena, ciudad que cuenta con el puerto más importante del país que le ofrece la posibilidad de atender eficazmente a los mercados de Estados Unidos y la Unión Europea. La entidad cuenta con una fábrica de hielo propia que abastece la demanda de su cadena de producción.

C.I. Océanos S.A. cuenta con tres ubicaciones físicas las cuales son:

- **Finca Camaronera:** Ubicada en la Isla de Covado a 25 km de la ciudad de Cartagena
- **Planta de Procesos**: Ubicada en Mamonal zona industrial de Cartagena.
- **Fábrica de hielo:** Ubicada en el barrio Ceballos de Cartagena. *Ver Figura 8.*

Figura 9. Ubicaciones Geográficas Sedes de C.I. OCEANOS S.A.

3.2 INFRAESTRUCTURA DE LA RED DE DATOS

La red de datos de C.I. OCEANOS S.A., se considera una red LAN a pesar de encontrarse dispersa entre varias sedes físicas con ubicaciones geográficas diferentes distantes en más de 25 Kilómetros entre sí; esto debido a que las sedes se han interconectado con la implementación de radio enlaces microondas en frecuencias libres al público, el cual ha permitido extender la red principal de datos y servicios de C.I. OCEANOS S.A. ubicada en la sede Planta a las sedes finca camaronera y fábrica de hielo. *Ver Figura 9.*

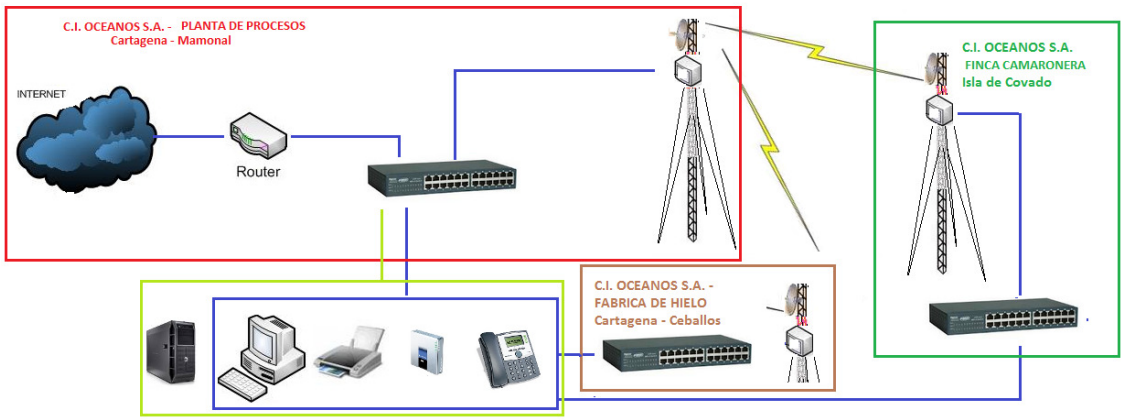


Figura 10. Radio enlaces microondas C.I. OCEANOS S.A.

Los enlaces microondas son soportados por equipos del fabricante Mikrotik, trabajan en la banda libre 5 GHz empleando la frecuencia 5,18 Ghz en el enlace Planta-Finca para una cobertura de 25 KM en línea recta empleando antenas parabólicas grilladas de 32DBi de ganancias ubicadas en torres de 55mt de altura aproximadamente, también se usa la frecuencia 5,7Ghz en el enlace planta-Fabrica para una cobertura en línea recta de más de 2km, se emplean antenas grilladas direccionales de 28DBi.

La red LAN Ethernet de C.I. OCENOS S.A. presenta una topología física y lógica en estrella con un centro de computo principal en la sede Planta en la cual se encuentra el centro de cableado principal y el conjunto de todos los servidores, adicionalmente en esta sede, y también en la finca camaronera y fábrica de hielo se encuentran centros de cableado adicionales que albergan equipos de comunicaciones que proporcional localmente conectividad a equipos de computo más no servidores de aplicaciones.
El backbone de datos está conformado por switches marca Cisco y algunos switches de otras marcas menos reconocidas.

3.3 ACCESO A INTERNET

El acceso a internet es realizado a través de un canal de datos de 3M contratado con Telmex quien posee un router modelo cisco 2800 en las ubicaciones del cliente, adicionalmente C.I. OCEANOS S.A. cuenta con otro canal disponible proporcionado por el ISP redes Integrales el cual no se encontraba en uso hasta antes del desarrollo del presente proyecto, por no poseerse ningún equipo que realice un balanceo de cargas entre enlaces o router que realice el enrutamiento hasta la red de datos de este ISP.

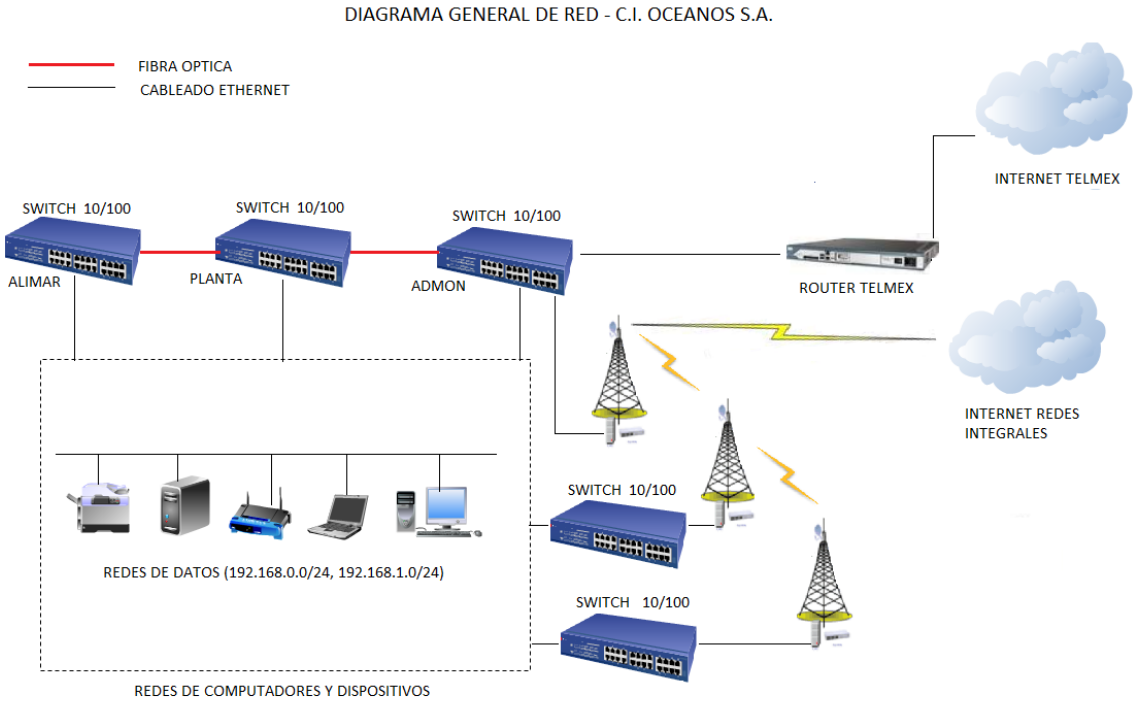


Figura 11: Canales de Internet.

Las revisión de los gráficos MRGT de una semana y un mes ver Figuras 10 y Figura 11 respectivamente, consultadas desde el sitio proporcionado por el proveedor Telmex, dan a conocer que el canal actual de datos presenta saturación en algunas ocasiones aunque por lo general es suficiente para la navegación a internet actual en C.I. OCEANOS S.A., mencionamos que C.I. océanos S.A. no cuenta con ningún control para navegación de los usuarios.

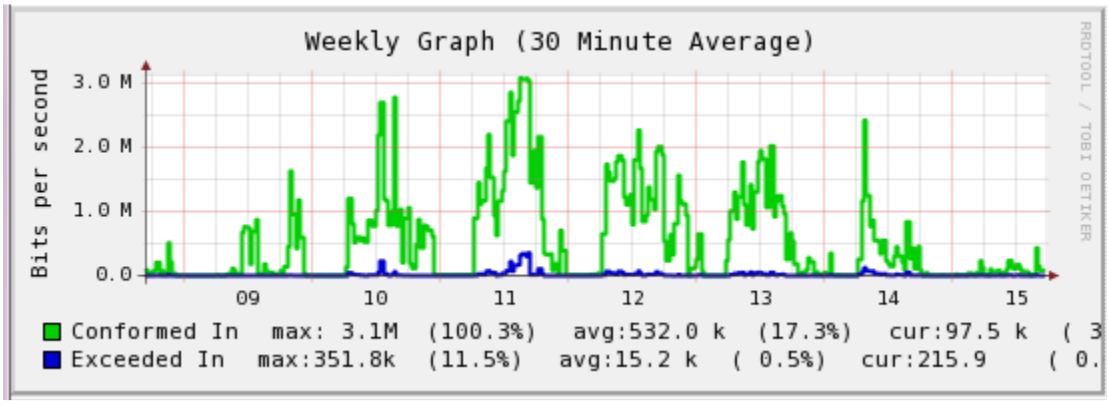


Figura 12: Consumo canal dedicado del 08 al 15 de octubre del 2011.

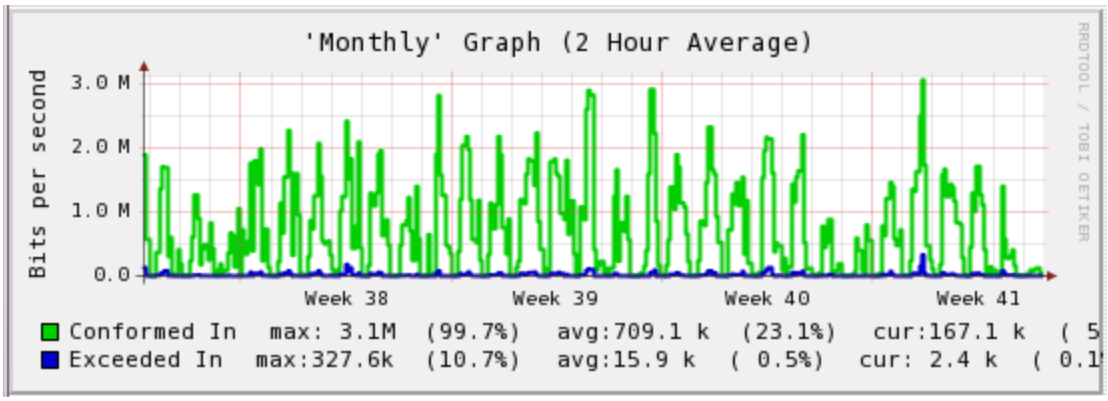


Figura 13: Consumo canal dedicado del 15 de septiembre al 15 de octubre del 2011.

A pesar de esto se desea el uso del otro canal disponible de 2M con Redes Integrales para la navegación como respaldo del canal de datos principal.

3.4.1 Direccionamiento de la red de datos C.I. OCEANOS S.A.

En la tabla a continuación el direccionamiento público entregados por los dos ISP actuales de la entidad:

PROVEEDOR	SERVICIO	CAPACIDAD	MEDIO	DIRECCIONAMIENTO PÚBLICO (REDES)	SERVICIOS
TELMEX	CANAL DE DATOS DEDICADO	3M	FIBRA OPTICA	190.144.033.008/29 190.190.233.080/29 190.144.131.000/30	INTERNET, CORREO HOSTEADO, DNS
REDES INTEGRALES	CANAL DE DATOS DEDICADO	2M	ENLACE MICROONDAS	201.201.200.096/29	INTERNET

Tabla 2. Direccionamiento Publico disponible por ISP.

En la actualidad C.I. océanos S.A. posee una gran cantidad de dispositivos Ethernet aproximadamente 200 en los que se incluyen (PCs, impresoras de red, Acces Points, etc.). En la tabla a continuación el direccionamiento privado en uso al inicio del proyecto y direcciones publicas empleadas en NAT.

3.4 DIRECCIONAMIENTO PRIVADO

RED	PUERTA DE ENLACES	DISPOSITIVO PUERTA DE ENLACE	OBSERVACION	DIRECCION PUBLICA NAT
192.168.0.0/24	192.168.0.1	ROUTER TELMEX	Direccionamiento para Servidores, PCs cliente y equipos de comunicaciones (Acces Point), impresoras y terminales inalámbricas	190.144.33.9
192.168.1.0/24	192.168.1.1	ROUTER TELMEX	Direccionamiento para PCs clientes.	190.144.131.41

Tabla 3. Direccionamiento privado Red C.I. Océanos S.A.

El router de Telmex en la entidad, se encarga actualmente del direccionamiento público y privado de la red la red de C.I. Océanos S.A., este router es administrado exclusivamente por el ISP y cualquier cambio que desee el cliente debe ser informado y solicitado a esta entidad. El direccionamiento se coloca de forma manual en cada dispositivo dentro de la red ya que no se cuenta con servidor DHCP en la entidad.

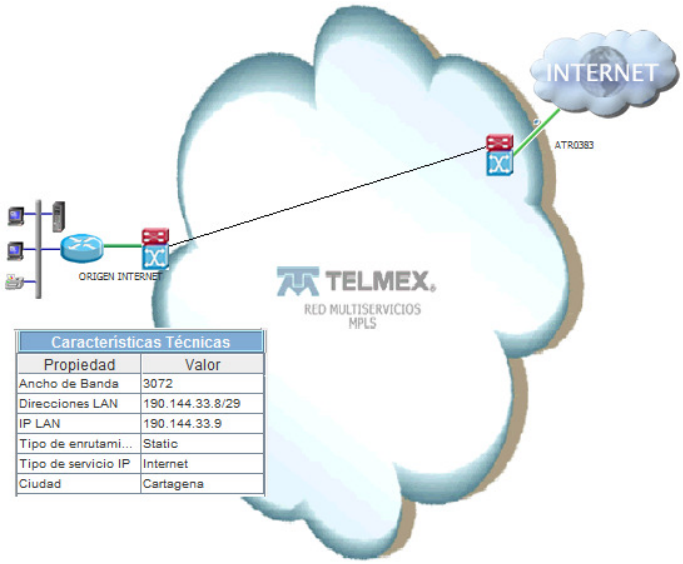


Figura 14: Topología de Red C.I. Océanos S.A.

En esta punto cabe mencionar que en la sede planta de la entidad C.I. OCEANOS se presentan una cantidad de equipos con tarjetas Ethernet (40 equipos aprox.) que no

pertenecen a la entidad pero que emplean la red de datos de C.I. OCEANOS S.A., esto debido a que dentro de la sede se encuentran prestadas muchas oficinas a terceros conocidos como los outsourcings de Océanos S.A. , los cuales están autorizados por la gerencia para el empleo de este tipo de recursos , estas otras entidades tienen la administración local de sus máquinas, las cuales no son responsabilidad de C.I. OCEANOS S.A., pero afectan la administración de las redes de datos y deben ser considerados en cualquier proyecto que se teja alrededor de la infraestructura de redes.

3.5 SISTEMAS DE INFORMACIÓN C.I. OCEANOS S.A.

En C.I. OCEANOS S.A., se emplean diferentes aplicaciones cabe recalcar que la mayoría soportada en sistemas Microsoft, de modo que los equipos de los usuarios y servidores poseen sistemas operativos Windows en diversas versiones y hacen uso de las herramientas ofimáticas conocidas como Microsoft Office (Word, Excel, Outlook, Power Point etc.) también en diferentes versiones.

Entre las aplicaciones las más importantes para cualquier entidad son aquellas que corresponden a sistemas de información que como su nombre lo indican almacenan información relevante al negocio de la entidad, a continuación se detallan los sistemas de información actuales en C.I. OCEANOS S.A.

3.5.1 Sistemas De Información Principales

Software de gestión empresarial funcionalidades contabilidad, venta inventario, compras, mantenimiento etc.

Módulos implementados (MM, CO, PM, FI).

Sistema para registro de producto terminado, desde diferentes etapas de la cadena de producción en planta (Empaque, congelación y conservación) y despacho a clientes.

Sistema para registro de actividades de operarios, base para el pago actual por actividades realizadas; y control de producción de operarios.

Software para registro y pago de nomina de empleados de C.I. OCEANOS S.A. y sus colaboradores asociados a cooperativas

3.5.2 Otros Sistemas De Información

Sistema para registro de procedimientos internos. Herramienta base para el sistema de gestión ambiental.

Software de contabilidad de cooperativas asociadas a C.I. OCEANOS

Sistema de Administración de Cuentas de Compensación, base para generación y envío de reportes al banco de la republica y DIAN.

3.5.3 Otros Sistemas De Propósito Específico

De igual forma también se dispone en la entidad de otras aplicaciones o software de propósito específico que aunque no almacenan información relevante al negocio, proporcionan operatividad a los usuarios de la red como son:

Sistema de antivirus centralizado para computadores de usuarios y computadores servidores.

Sistema central de administración de telefonía IP, permite la administración de extensiones telefónicas y control de permisos de llamadas.

Sistema de impresiones para control de impresiones de usuarios.

Sistema de correos electrónicos.

3.6 HARDWARE

El hardware de la entidad C.I. OCEANOS S.A. se clasifica principalmente en 3 categorías, a continuación se detallas las categorías en cuestión.

3.6.1 Equipos de cómputo.

Se incluyen en esta categoría PCs de escritorio y portátiles asignados a los empleados para la realización de sus labores, periféricos tales como impresoras, video beams, así como equipos de cómputo servidores. Los servidores de la entidad se detallan a continuación:

SERVIDORES	APLICACIONES Y/O SERVICIOS	S.O.	CARACTERISTICAS DEL HARDWARE
TECNOCEDI	SQL SERVER 2005, IIS, ESCRITORIO REMOTO, CARPETAS COMPARTIDAS	WINDOWS SERVER 2003	- DELL POWER EDGE T410 - INTEL XEON G5 2.53 GHZ - 4.00 GB RAM - 2 DISCOS SAS DE 250GB (RAID 1) - UNIDAD DVD/RW
PXP	ORACLE , IIS, ESCRITORIO REMOTO, CARPETAS COMPARTIDAS	WINDOWS SERVER 2003	- DELL POWER EDGE T410 - INTEL XEON G5 2.53 GHZ - 4.00 GB RAM - 2 DISCOS SAS DE 250GB (RAID 1) - UNIDAD DVD/RW
SRHOCEANOS	ORACLE 9I, CARPETAS COMPARTIDAS	WINDOWS SERVER 2000	- HP SERVER TC2110 - INTEL PENTIUM IV 2.40GHZ - 256MB M - 2 40GB DISCO - CD ROM
SRHBDCOOP	ORACLE 9I, CARPETAS COMPARTIDAS	WINDOWS SERVER 2003	- DELL POWER EDGE T410 - INTEL XEON G5 2.53 GHZ - 4.00 GB RAM - 2 DISCOS SAS DE 250GB (RAID 1) - UNIDAD DVD/RW
SRHAPLICACOOP	ESCRITORIO REMOTO, CARPETAS COMPARTIDAS	WINDOWS SERVER 2003	- HP PROLIANT ML110 - INTEL PENTIUM IV 3.20 GHZ - 256 MB RAM - 80 GB DE ALMACENAMIENTO - CD ROM
ZEUS	SQL SERVER EXPRESS, ESCRITORIO REMOTO, CARPETAS COMPARTIDAS	WINDOWS SERVER 2003	- DELL POWER EDGE SC440 - INTEL CELERON 2.80 GHZ - 1.00GB - 160 GB - Unidad de DVD/CD RW

COUNTEX	SQL SERVER EXPRESS 2005, IIS, ESCRITORIO REMOTO , CARPETAS COMPARTIDAS	WINDOWS VISTA BUSINESS	- DELL VOSTRO 1700 - INTEL DUAL CORE 2.30 GHZ - 1.00GB - 160 GB - Unidad de DVD/CD RW
IMPRESIÓN	DISPOSITIVOS COMPARTIDOS Y ESCRITORIO REMOTO.	WINDOWS SERVER 2003	- CLON - INTEL CORE 2 DUO 2.80GHZ - 1.00GB RAM - 150 GB DE DISCO DURO - UNIDAD DE CD/DVD RW
ANTIVIRUS	TRENDMICRO	WINDOWS XP PROFESIONAL	- HP DC5750 - AMD ATHLON 64 1.80GHZ - 512 MB RAN - 80 GB - CD ROM

Tabla 4. Equipos servidores C.I. OCEANOS S.A.

3.6.2 Dispositivos de propósito específico.

Varias aplicaciones hacen uso de dispositivos de propósito específico tal es el caso de los mostrados en la tabla a continuación:

SISTEMA	SISTEMA	DISPOSITIVOS
Telefonía IP		**Convertidor o Gateway de telefonía análoga a telefonía IP**. Empleado para aprovechar las redes telefonía tradicional en el uso de telefonía IP
		**Convertidor o Gateway de telefonía celular a telefonía IP.** Permite la salida de llamadas por tarjetas de telefonía celular o GSM
		**Teléfonos IP:** Dispositivos diseñados para el trabajo con redes de VozIP.
		**Dispositivos ATA** adaptadores terminales de teléfonos análogos a telefonía IP
PXP		**Terminales portables** para registro de tiempos de operarios.
SERVIBARRAS		**Terminales portables** para registro de inventario de producto terminado.

Tabla 5. Equipos de propósito específico

3.6.3 Equipos de comunicaciones.

Aquí se incluyen dispositivos activos de la red de comunicaciones como son Switches, Routers, Acces Points, transceiver (convertidores de medios) y radios microondas etc.

3.7 ADMINISTRACIÓN DE LA RED Y SEGURIDAD

La red de C.I. OCEANOS S.A. carece de sistemas que permitan la administración y monitoreo de la red, no cuenta con herramientas que faciliten la recolección, presentación y el análisis de logs a fin de conocer sobre la existencias, cambios en el sistema o modificaciones de hardware y software.

El mantenimiento a equipos de computo es realizado por el personal del área de sistemas a excepción del mantenimiento a equipos servidores y de radio comunicaciones que es realizado por el contratista REDES INTEGRALES y el mantenimiento a impresoras que es realizado por el contratista Ricoh Colombia.

3.7.1 Gestión del Software.

la instalación del software para computadores es realizado manualmente por el personal del área de sistemas, la información de licencias, aplicaciones, contraseñas y otros, se registra manualmente en archivos de Excel, haciendo que las operaciones de sistemas no sean estandarizada y o sean modificables sin dejar registro alguno.

3.7.2 Gestión del Hardware.

Los dispositivos del área de sistemas son registrados manualmente en un archivo de Excel, pero esta información es susceptible a errores debido a la falta de actualización.

3.7.3 Gestión de usuarios.

La creación y administración de usuarios se crea localmente en cada máquina respectiva, de forma manual por el personal de sistemas, ya que no se cuenta con servidor de directorio activo. De forma similar se realiza la administración de usuarios en las aplicaciones las aplicaciones internas.

3.8 Diagnóstico de la Red de Datos C.I OCEANOS S.A.

Las vulnerabilidades identificadas en la Red de Datos de C.I OCEANOS S.A fueron valoradas, mediante observación y experiencia del administrador de la Red, las cuales se detallan a continuación:

- ✓ **Navegación a Internet:** Los usuarios navegan libremente en internet poniendo en riesgo de infección de Malware a la plataforma tecnológica de la entidad. A pesar de que se encuentra con una solución Antimalware local en cada máquina. Se han identificado personal accediendo a sitios no relacionados con el entorno laboral, es el caso de páginas de Redes Sociales, páginas de Juegos y páginas Streaming Multimedia.

- ✓ **Mensajería Instantánea:** Los usuarios de la Red emplean aplicaciones de mensajería instantánea que constituyen un riesgo de seguridad para los equipos de cómputo, ya que se han confirmado en años anteriores que son fuente de propagación Malware.

- ✓ **Control de Aplicaciones:** La entidad no cuenta con un directorio activo y tiene algunas máquinas con usuarios que poseen perfiles de administrador, los cuales pueden realizar cualquier tipo de instalación de programas que presenten riesgos para la seguridad de la empresa, como es el caso de los programas Peer to Peer, los cuales no pueden ser controlados ya que no se tienen mecanismos de control de aplicaciones. Semestralmente el área de sistemas realiza una revisión máquina a máquina de las aplicaciones instaladas encontrándose equipos con programas como Ares, Vnc, Teamviewer.

- ✓ **Direccionamiento IP**: La entidad no cuenta con administración propia para el direccionamiento público y privado de las redes, estos están a cargo del proveedor de servicios de internet, que continua siendo un tercero, de modo que el grado de confidencialidad que se pueda tener con este no es el mismo que se presentaría si la administración estuviera únicamente limitada al personal de Sistema de la Entidad.

- ✓ **Equipos de Computo de Terceros**: Los Equipos de cómputo de los outsourcing e invitados, no son administrados por C.I Océanos S.A, pero se encuentran adscritos a la red de la entidad, lo que aumenta el riesgo que utilicen los recursos de la Red de

Océanos, como es el caso de las impresoras y que sean fuentes de infección y propagación de Malware.

- ✓ **Monitoreo de Red:** La entidad C.I Océanos no cuenta con sistemas que permitan monitorear el estado de los canales de datos dedicados con los ISP.

- ✓ **Firewall:** El único mecanismo de apertura o cerrado de puertos de las máquinas lo constituye únicamente el firewall incorporado del sistema operativo, por lo tanto no se pueden aplicar políticas de firewall entre grupos de máquinas de Océanos.

4. DISEÑO DEL SISTEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE C.I. OCEANOS S.A

CI OCÉANOS S.A actualmente presenta muchas riesgos en su seguridad informática debido a la carencia de controles frente al acceso a los recursos de la red incluido el servicio de internet, siendo este ultimo el mayor problema de seguridad que afecta las empresas modernas, ocasionadas a su vez por la ausencia de una política de Seguridad establecida e implementada en mecanismos hardware o software en la entidad y por la desconocimiento de la alta gerencia de los riesgos que esto representan para la operación y productividad de toda la entidad ocasionando que no se comprendan, aprueben y apoyen económicamente nuevos proyectos de seguridad.

Esta situación ha ocasionado el uso inadecuado e innecesario de diferentes recursos de la entidad por parte de los empleados principalmente del servicio de Internet disminuyendo el rendimiento productivo del recurso humano. La libre navegación por la red mundial, expone a su vez a los sistemas informáticos de C.I OCEANOS S.A. a diferentes amenazas como Virus, Spyware, Spam, entre otros; lo cual puede provocar serios daños en aspectos de seguridad como disponibilidad, privacidad, confidencialidad e integridad.

De igual forma la falta de controles ha incurrido en que la administración de la seguridad al interior de la entidad resulte muy manual y por ende más compleja para el responsable

de la red, así como demoras significativas para la identificación y solución de incidentes asociados a un ataque o explotación de riesgos informáticos.

Por lo anterior, de acuerdo al análisis del sistema y los riegos que presenta la red de datos de CI OCEANOS S.A se consideró necesario establecer mecanismos de control perimetral, por ello la empresa aprueba y adquiere un dispositivo para manejo unificado de amenazas UTM que proporciona muchas funcionalidades adicionales para la administración del acceso a los recursos de la red.

La marca evaluada y seleccionada de UTM **FORTINET** obedeció a que otras empresas del grupo al cual pertenece C.I. OCEANOS S.A. han seleccionado este fabricante para la incorporación y protección en su redes de datos, y por lo cual se estableció un estándar para todas las demás empresas del grupo, solución que brinda la adecuada seguridad al sistema en torno a muchos de los asuntos concernientes a la seguridad de su información; debido a que cuenta con los siguientes módulos de seguridad de cualquier UTM: Firewall, Antivirus, AntiSpyware, AntiSpam, IDS, IPS y VPN, permitiendo así el incremento de la funcionalidad de la Red de Datos y el ágil desempeño en sus procesos.

En aras de proteger de forma integral, eficiente y efectiva la Red de CI OCEANOS S.A; se presenta a continuación un esquema final de la implementación del Dispositivo de Seguridad Perimetral, el cual permite brindar una protección integral y a profundidad contra las más sofisticadas amenazas que se lanzan a la red mundial continuamente.

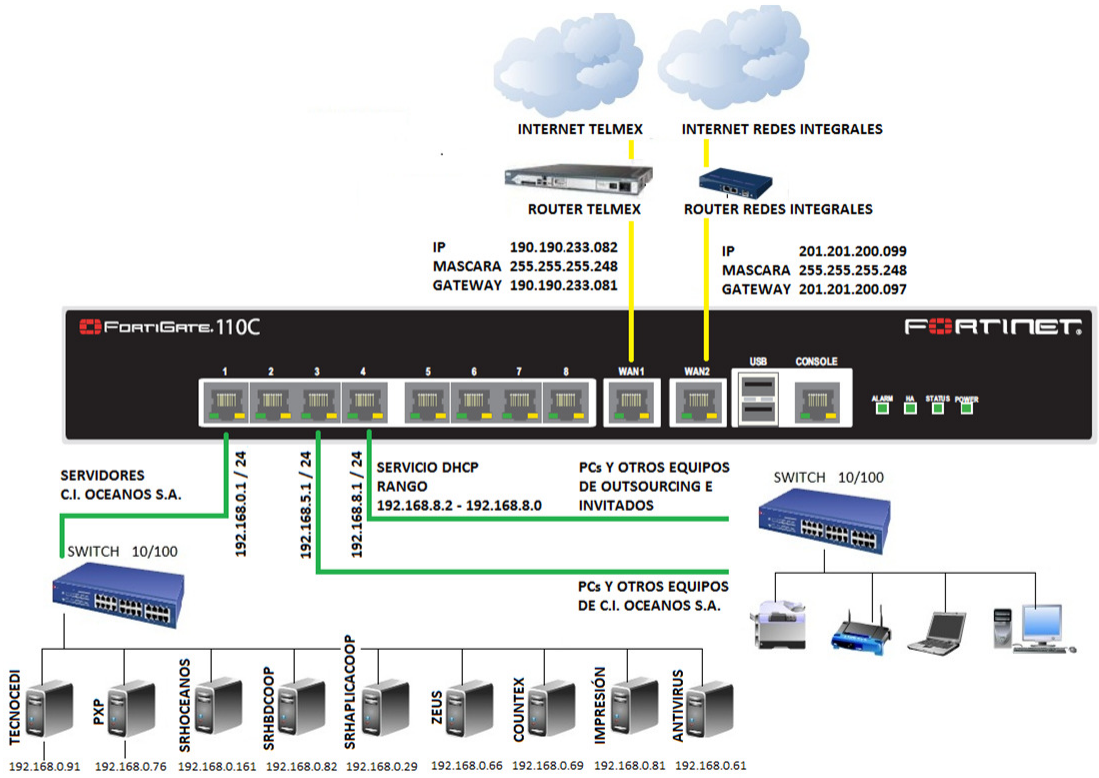


Figura 15. Esquema Final de RED implementación Fortinet C.I. OCEANOS S.A.

4.1 PROCEDIMIENTO DE LA IMPLEMENTACIÓN GENERAL DE FORTINET.

La implementación del sistema de seguridad perimetral de C.I. OCEANOS S.A, se realizó en un esquema de alta disponibilidad con el empleo de dos dispositivos FORTIGATE 110C, y un dispositivo Fortianalizer 100C. Las etapas o pasos realizados se especifican a continuación:

1. Se definió un diseño inicial de la red para la infraestructura presente en C.I. OCEANOS S.A. de acuerdo a las necesidades de seguridad perimetral en la entidad, como se muestra en la figura 12. Este diseño inicialmente propuesto sufrió cambios durante la etapa de implementación, siendo los objetivos principales del mismo:

   - Independizar la red de datos para los equipos de outsourcings e invitados de tal forma que no presentaran comunicación alguna con las redes de datos asignados para los equipos propiedad de C.I. OCEANOS S.A. empleados por usuarios finales y aquellos en el rol de servidores de aplicaciones.

- Independizar la red de datos de los usuarios de la compañía.

- Aislar los servidores en una red de datos independiente a la empleada por los usuarios finales de C.I. OCEANOS S.A. a fin de realizar una detección y prevención de intrusiones identificando el origen de los mismos tanto desde internet como de la red de clientes interna y habilitando solo los puertos de las aplicaciones empleadas entre una red y otra.

- Usar el canal de datos proporcionado por redes Integrales., y habilitar los dos canales actuales de C.I. OCEANOS S.A. para balanceo de cargas y fileover en caso de caída de alguno de los canales.

- Realizar un filtrado web y bloqueo de aplicaciones para todos los equipos que acceden a internet, restringiendo el acceso a sitios y aplicaciones no relacionados con el trabajo de los empleados, outsourcing e invitados.

- Realizar un bloqueo de envío de correos smtp, los cuales estuvieran destinados a equipos diferentes a los servidores de correo de C.I. OCEANOS S.A., hostiados en el ISP Telmex, a fin de evitar listado de direcciones publicas en servidores RBL garantizando la entrega de los correos de la entidad.

- Habilitar VPN SSL para el acceso seguro de usuarios desde la extranet a los servicios WEB y escritorio remoto de los servidores Tecnocedi y PXP específicamente.

- Habilitar servicio DHCP para un rango de direcciones IP de la red destinada para Outsourcing para ser empleado por los invitados de la entidad, de modo que se evita la configuración manual de direcciones IP.

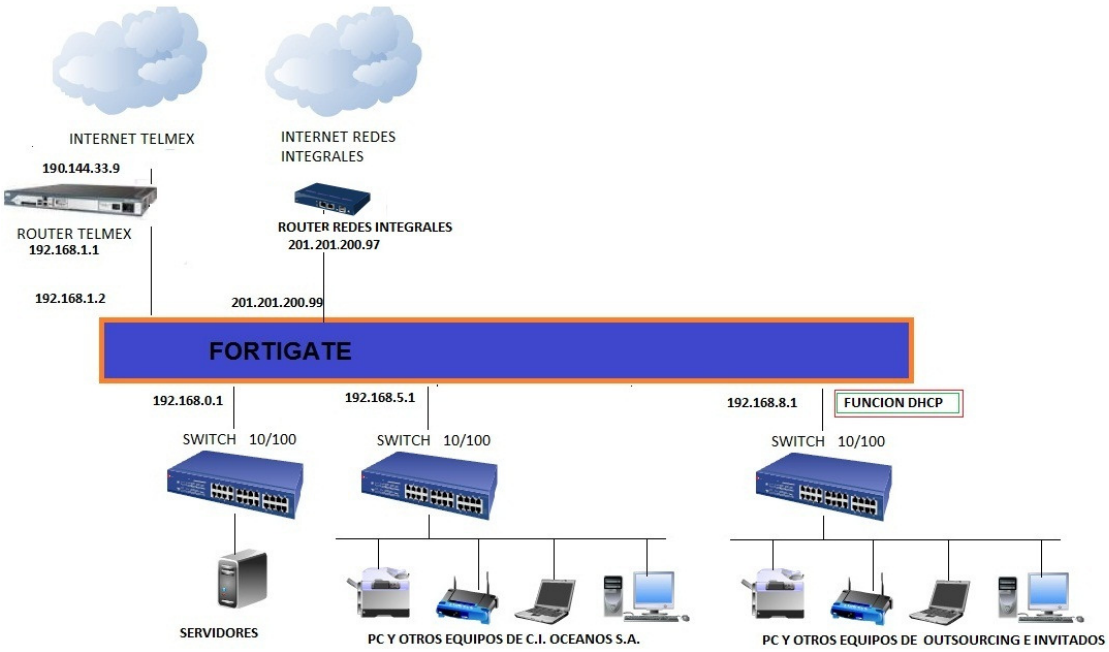


Figura 16. Esquema de RED propuesto pre implementación Fortinet

2. Se configuró temporalmente una interfaz del dispositivo con una IP local de C.I. OCEANOS con acceso a internet y se procedió con la instalación y actualización de Firmware de los dos equipos fortigate empleados llevándolos a la versión MR3 Patch.

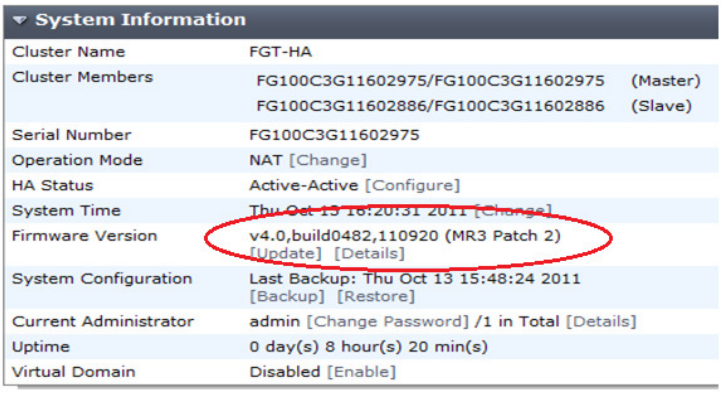


Figura 17. Actualización de Firmware.

3. Se realizó la configuración de la Segmentación y Direccionamiento en las interfaces del dispositivo Fortigate como se muestra en la figura a continuación, mediante la opción Interfaces del menú **System – Network** del dispositivo:

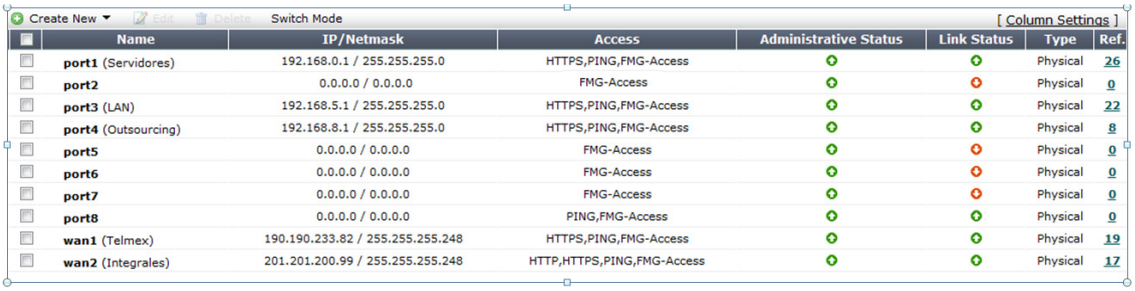


Figura 18. Configuración de interfaz del dispositivo.

- La interfaz port1 fue configurada como puerta de enlace de la red 192.168.0.0 / 24 definida para ser empleada para servidores.

- La interfaz port3 fue configurada como puerta de enlace de la red 192.168.5.0 / 24 definida para equipos de propiedad de C.I. OCEANOS S.A (Pcs de usuarios, acces point, impresoras, terminales, etc).

- La interfaz port 4 fue configurada como puerta de enlace de la red 192.168.8.0 / 24 destinada para equipos propiedad de Outsourcings y invitados de la empresa.

- Se configura la interfaz de red Wan 1 con la dirección pública 190.190.233.82 /29 destinada para acceso a internet por el canal de datos contratado con Telmex.

- Se configura interfaz de red Wan 2 con la dirección pública 201.201.200.99 /29 destinada para acceso a internet por el canal de datos contratado con redes Integrales.

4. Se realizó configuración de los DNS como se muestra en la figura a continuación. Cabe recalcar que el DNS 200.26.137.100 corresponde al DNS primario de Telmex y el DNS secundario 201.219.193.253 corresponde al DNS primario especificado por Redes integrales. Esto debido a que de lo contrario se mostraba errores de DNS en el equipo.

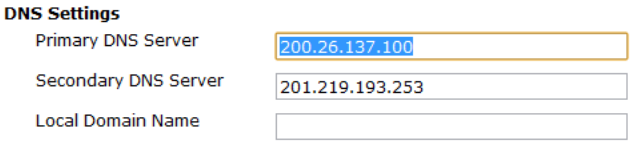


Figura 19. Configuración DNSs

5. Se configuró en el menú System - Network – DHCP Server, el rango de direcciones IP a entregar asociándolo a la interfaz port 4 ya definida para Outsourcings e invitados. Ver Figura 19.

Interface	Mode	Type	Options	Enable
port4(Outsourcing)	Server	Regular	192.168.8.2 - 192.168.8.50	✓

Figura 20. Configuración DHCP Server

6. Se probó el esquema de alta disponibilidad el cual se configuró en la interfaz 8 de cada uno de los dos dispositivos Fortigate empleados, y el cual fue especificado como modo activo-activo en ambos equipos. Se resalta que la configuración inicial se realiza en único equipo el cual replica la configuración en el otro equipo especificado como esclavo. Ver Figura 20.

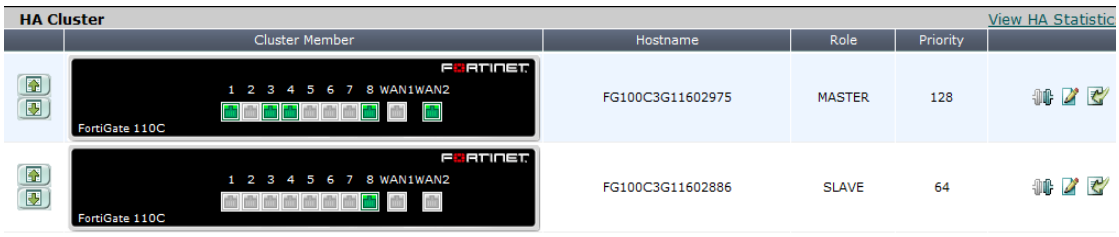


Figura 21. Configuración Alta Disponibilidad de dispositivos.

7. Se crearon los usuarios para administración y monitoreo del dispositivo.

Name	Trusted Hosts	Profile	Type
admin	0.0.0.0/0	super_admin	Local
emorales	0.0.0.0/0	auxsistemas	Local
ptorres	0.0.0.0/0	jfsistemas	Local

Figura 22. Configuración de Usuarios

8. A través del menú **Router - Static - Route** Se crearon las rutas estáticas respectivas para las direcciones públicas y dirección adicional 10.0.0.0 a emplear en el uso de la VPN que se configuró para C.I. OCEANOS S.A.

IP/Mask	Gateway	Device
0.0.0.0/0.0.0.0	190.144.233.81	wan1
0.0.0.0/0.0.0.0	201.219.200.97	wan2
10.0.0.0/255.255.255.0		ssl.root

Figura 23. Configuración de rutas estáticas.

9. A través del menú **Router – Static - Policy Route** Se crearon las políticas de Rutas y así establecer el balanceo de carga. Una política de ruta se crea entre una interfaz y otra. Y no en un rango de dirección IP explicito.

Incoming	Outgoing	Source	Destination
port1	port3	192.168.10.0 / 255.255.255.0	192.168.5.0 / 255.255.255.0
port1	port1	192.168.0.0 / 255.255.255.0	192.168.10.0 / 255.255.255.0
port1	port3	192.168.0.0 / 255.255.255.0	192.168.5.0 / 255.255.255.0
port1	wan1	192.168.0.0 / 255.255.255.0	0.0.0.0 / 0.0.0.0
port2	wan1	192.168.3.0 / 255.255.255.0	0.0.0.0 / 0.0.0.0
port3	port1	192.168.5.0 / 255.255.255.0	192.168.10.0 / 255.255.255.0
port3	port1	192.168.5.0 / 255.255.255.0	192.168.0.0 / 255.255.255.0
port3	wan1	192.168.5.0 / 255.255.255.0	0.0.0.0 / 0.0.0.0
port4	wan2	192.168.8.0 / 255.255.255.0	0.0.0.0 / 0.0.0.0

Figura 24. Configuración de políticas de rutas.

10. Se configuró la redundancia para las dos interfaz WAN correspondiente al balanceo de carga y fileover de canales de internet a través de l menú Router – Static – Settings. Ver figura 24.

ECMP Load Balancing Method

Source IP based Weighted Load Balance Spillover

Dead Gateway Detection

Create New Edit Delete

Interface	Ping Server	Detect Protocol	Interval	Failover
wan2	4.2.2.2	ICMP Ping	5	5
wan1	8.8.8.8	ICMP Ping	5	5

Figura 25. Configuración de fileover de canales.

11. Se definieron todas los host y redes requeridos para posterior aplicación de reglas de firewall. Esto a través del menú **Firewall Objets - Address – Address**. Ver figura 25.

Name	Address/FQDN	Interface	Type	Ref.
CORREO	200.26.137.33/255.255.255.255	Any	Subnet	6
FG_INTEGRALES	201.219.200.99/255.255.255.255	Any	Subnet	1
HOST_ANTIVIRUS	192.168.0.61/255.255.255.255	Any	Subnet	2
HOST_COUNTEX	192.168.0.69/255.255.255.255	Any	Subnet	2
HOST_IMPRESION	192.168.0.81/255.255.255.255	Any	Subnet	2
HOST_ISOQCS	192.168.0.92/255.255.255.255	Any	Subnet	2
HOST_PXP	192.168.0.76/255.255.255.255	Any	Subnet	2
HOST_SRHAPLICACOOP	192.168.0.29/255.255.255.255	Any	Subnet	2
HOST_SRHBDCOOP	192.168.0.82/255.255.255.255	Any	Subnet	2
HOST_SRHOCEANOS	192.168.0.161/255.255.255.255	Any	Subnet	2
HOST_TECNOCEDI	192.168.0.91/255.255.255.255	Any	Subnet	2
HOST_TELEFONIAIP	192.168.0.54/255.255.255.255	Any	Subnet	1
HOST_ZEUS	192.168.0.66/255.255.255.255	Any	Subnet	2
RED_LAN_OCEANOS	192.168.5.0/255.255.255.0	Any	Subnet	10
RED_LAN_OUTSOURCING	192.168.8.0/255.255.255.0	Any	Subnet	6
RED_SERVIDORES	192.168.0.0/255.255.255.0	Any	Subnet	11
RED_TELEFONIA	192.168.3.0/255.255.255.0	Any	Subnet	2
ROUTER_SAP	192.168.0.45/255.255.255.255	Any	Subnet	1
SAP	192.168.10.0/255.255.255.0	Any	Subnet	2
all	0.0.0.0/0.0.0.0	Any	Subnet	23

Figura 26. Definición de objetos de firewall.

12. Se crearon las políticas de firewall requeridas de acuerdo al esquema que se planteó en la pre implementación a través del menú Policy - Policy –Policy. Ver figura 26.

Seq.#	Source	Destination	Authentication	Schedule	Service	Action	Log	ID
port1(Servidores) -> port3(LAN) (1)								
1	SAP RED_SERVIDORES	all		always	ANY	✓ ACCEPT		18
port1(Servidores) -> ssl.root (1)								
2	RED_SERVIDORES	SSLVPN_TUNNEL_ADDR1		always	ANY	✓ ACCEPT		12
port1(Servidores) -> wan1(Telmex) (4)								
3	wparra	all		always	ANY	✓ ACCEPT		19
4	RED_SERVIDORES	CORREO		always	SMTP POP3	✓ ACCEPT		20
5	RED_SERVIDORES	all		always	SMTP	⊘ DENY		21
6	RED_SERVIDORES	all		always	ANY	✓ ACCEPT		24
port1(Servidores) -> wan2(Integrales) (3)								
7	RED_SERVIDORES	CORREO		always	SMTP POP3	✓ ACCEPT		27
8	RED_SERVIDORES	all		always	SMTP	⊘ DENY		26
9	RED_SERVIDORES	all		always	ANY	✓ ACCEPT		5
port2(Telefonia) -> wan1(Telmex) (1)								
10	RED_TELEFONIA	all		always	ANY	✓ ACCEPT		10
port2(Telefonia) -> wan2(Integrales) (1)								
11	RED_TELEFONIA	all		always	ANY	✓ ACCEPT		6

Figura 27. Definición de Políticas de firewall.

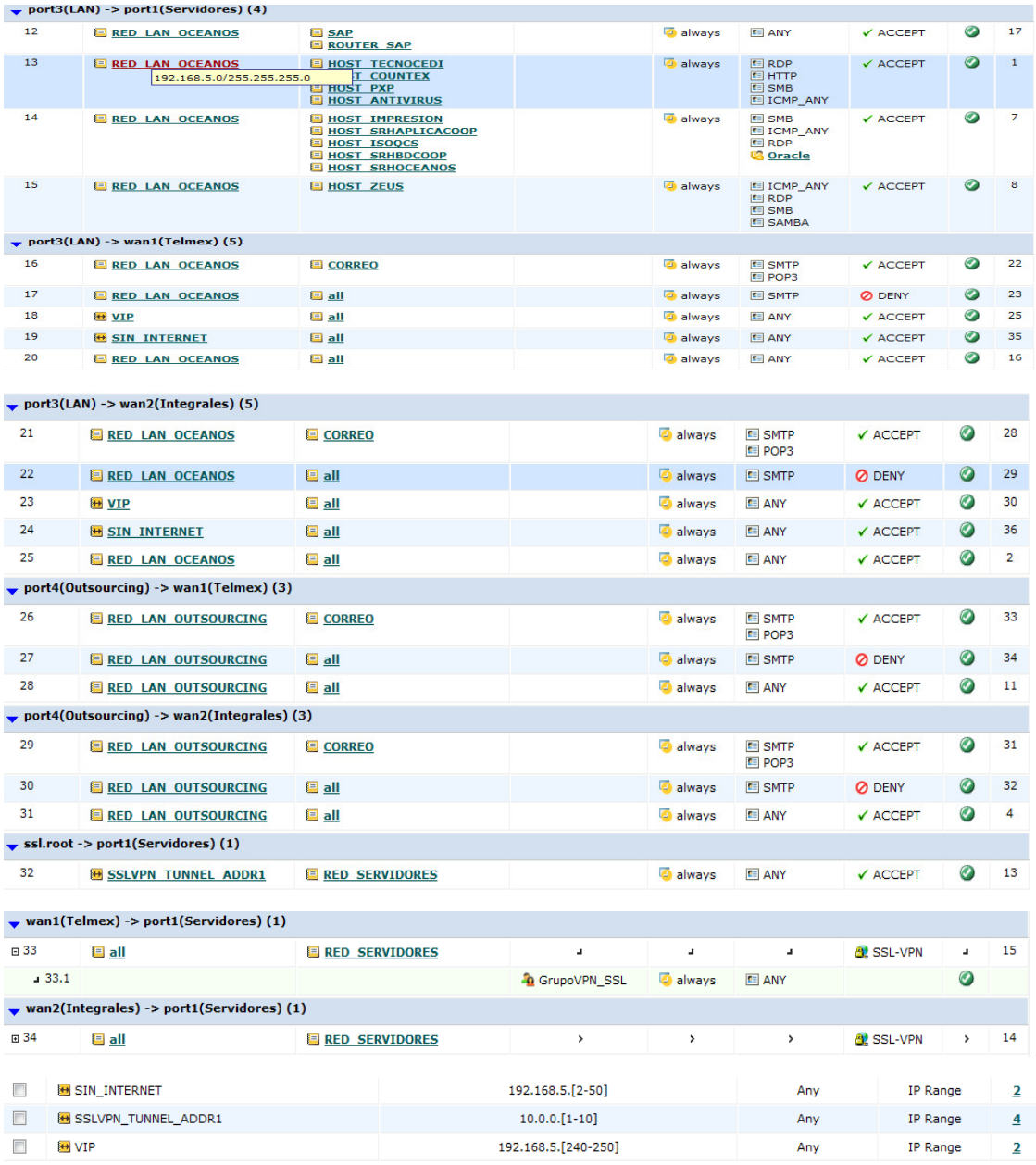
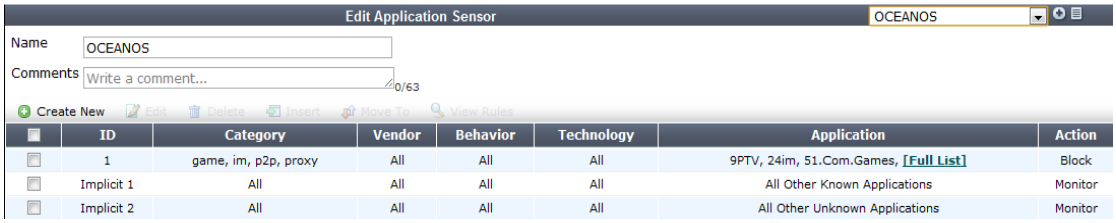


Figura 28. Configuración de políticas de firewall.

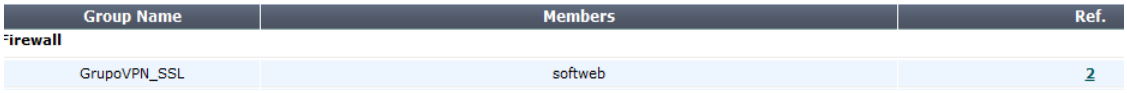
13. se crearon y aplicaron dos perfiles para la navegación web y uno de aplicaciones.

Name	Comments	Ref.
OCEANOS		9
VIP		0

Figura 29. Definición de Perfiles.



14 Se creó, configuró y se probó la VPN SSL para acceso de manera segura por RDP y servicio web a los SERVIDORES (TECNOCEDI y PXP). Se creó un usuario y el grupo respectivo a través del menú.



15. Se instaló, actualizó y configuró el dispositivo FortiAnalizer 100C para almacenamiento de logs de los dispositivos fortigate.

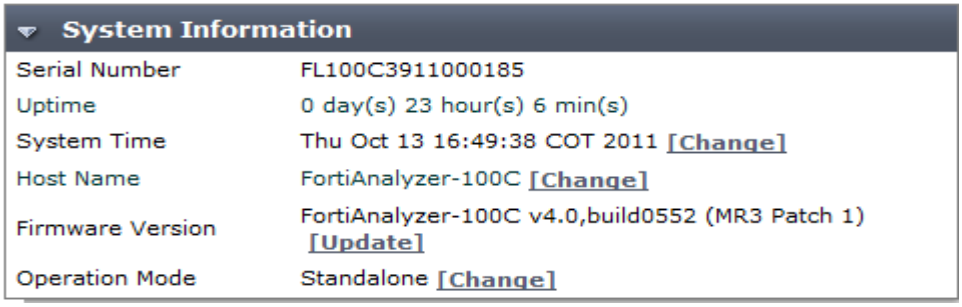


Figura 30. Actualización de firmware Fortianalizer.

15. Se configuró el direccionamiento, los DNS y la ruta respectivas del fortianalizer.

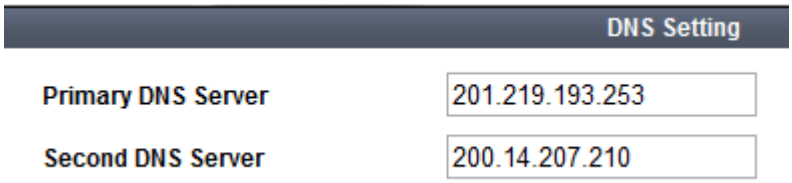
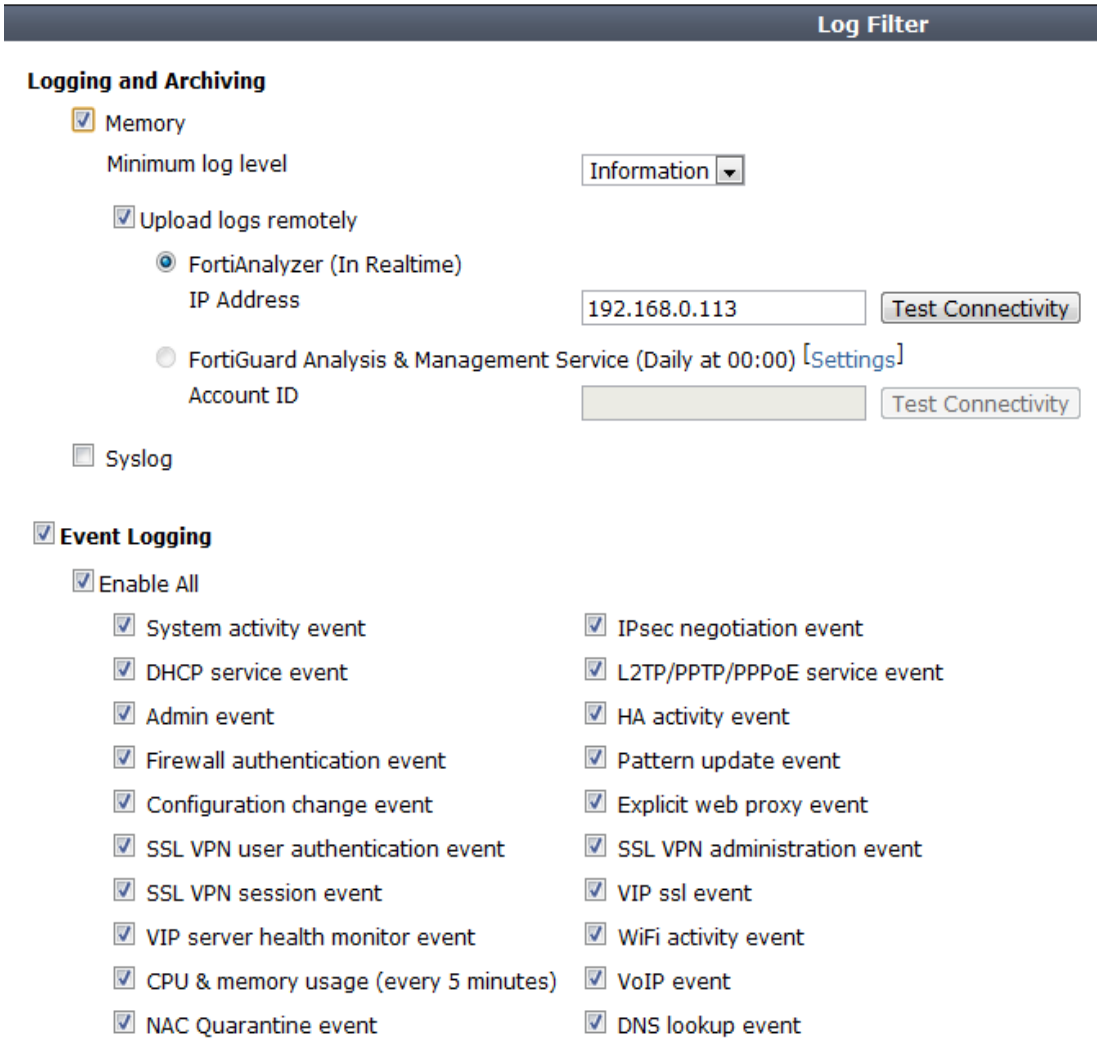


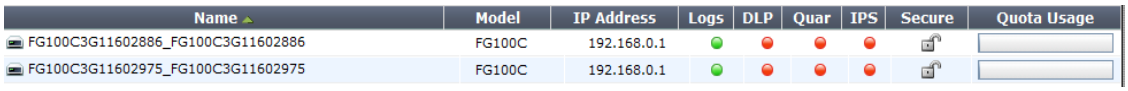
Figura 31. Configuración de DNSs Fortianalizer.

Figura 32. Configuración de ruta Fortianalizer.

16 Se configuró el Fortigate para la entrega de logs y así sincronizarse con el fortianalizer.



Se verifica la sincronización en el FAZ de los Fortigates.



Name	Model	IP Address	Logs	DLP	Quar	IPS	Secure	Quota Usage
FG100C3G11602886_FG100C3G11602886	FG100C	192.168.0.1						
FG100C3G11602975_FG100C3G11602975	FG100C	192.168.0.1						

Figura 33. Configuración de Fortianalizer en equipo Fortigate.

CONCLUSIONES

Luego del diseño e implementación del sistema de seguridad perimetral en C.I. OCEANOS S.A. se pueden realizar las siguientes conclusiones:

1. La integración de un dispositivo UTM fue una medida adecuada que aumentó la seguridad perimetral de la entidad, proporcionando controles a los administradores de la red para monitoreo y restricción del acceso a la red desde la extranet e incluso la intranet.

2. Se logró independizar la red de datos de los servidores de la entidad de todos los usuarios e invitados de la red, permitiendo únicamente un acceso controlado a los servicios que estos proporcionan a través de la aplicación de políticas de firewall en el UTM, que disminuyen los riesgos de seguridad asociados.

3. Se habilitó el uso de un canal de datos dedicado para acceso a internet que la entidad no había logrado usar con la funcionalidad adicional de ser un canal de respaldo ante el fallo del canal de datos principal.

4. Se logró restringir y controlar la navegación que los usuarios realizan hacia internet y con esto se garantiza un uso adecuado del recurso informático constituido por el servicio de internet y la disminución de los riesgos asociados a una navegación descontrolada hacia sitios públicos.

RECOMENDACIONES

A pesar de los controles que se han establecido con la implementación del dispositivo UTM de Fortigate en la red de C.I. OCEANOS S.A., se realizan las siguientes recomendaciones a la entidad:

1. Redacción y divulgación de una política de seguridad informática al interior de la entidad que especifique y describa los controles que se deben realizar en la administración de los recursos informáticos.

2. Incorporación de mecanismos de control adicionales en la intranet como es el caso de uso de VLAN en los dispositivos switch de la entidad para disminuir aun más los riesgos asociados a esta red.

3. Incorporación de los servicios de Directorio Activo, DNS en la intranet.

4. Monitoreo constante de Logs de los dispositivos de seguridad implementados para identificación de ataques o amanezcas presentes en la red y de los cuales el dispositivo Fortigate está realizando detección y bloqueo.

5. Evaluación constante y periódica de los controles a seguridad informática de la entidad para detección temprana de amenazas debido a que los riegos informáticos evolucionan muy rápidamente.

6. Se debe crear conciencia en la alta gerencia de que los riesgos a la seguridad informática representan para la empresa y la necesidad constante de implementación de controles que disminuyan y en lo posible minimicen estos riesgos, para que aprueben y apoyen económicamente las soluciones planteadas.

BILBIOGRAFIA

[1] BARRETO Gustavo Adolfo, Estudio de seguridad en computadoras con sistemas operativos conectados a una red TCP/IP, Universidad del Valle 2001.

[2] VILLALÓN Huerta, Antonio. "Seguridad en Unix y Redes". Versión 2.1. Julio.

[3] STALLINGS, William. "Comunicaciones y Redes de Computadores". 7ma Edición. Prentice Hall. New Jersey. 2004.

[4] CANAVAN, John. "Fundamentals of Network Security". Artech House. United States of America. 2001.

[5] ARGENTINA. ArCERT. "Manual de Seguridad en Redes" [en línea]. 1999. Disponible en Web: http://www.arcert.gov.ar/

[6] MAIWALD, Eric. "Fundamentos de seguridad de redes". Segunda Edición. McGraw-Hill. 2005.

[7] ZHOW Lidong, Haas Zygmunt J. "Securing Ad Hoc Nectworks", IEEE Network, Vol. 13, No. 6, pp 24-30, Junio 1999.

[8] ARBAUGH William A., Shankar Narendar, Wan Juustin Y. C., "Your 802.11 Wireless Network has No Clothes" IEEE Wireless Communications, Vol. 9, No. 6, pp. 44-51, Diciembre 2002.

[9] MADRID Molina Juan Manuel, "Seguridad en Redes inalámbricas 802.11", Revista Sistemas y Telemática, Universidad Icesi, Cali (Colombia), ISSN 1692-5238, pp. 13-28, Enero 2004.

[10] Network Working Group, "Site Security Handbook", Request for Comments 2196, Septiembre 1997.

[11] Instituto Argentino de Normalización, "Código de práctica para la administración de la seguridad de la información", IRAM-ISO IEC 17799, Buenos Aires, febrero 2002.

[12] Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina, Manual de Seguridad en Redes.

[13] Jesús Herney Cifuentes, César Augusto Narváez, Manual de detección de vulnerabilidades de sistemas operativos en redes TCP/IP, Universidad del Valle 2004.

[14] FORTINET. "FortiGate Unified Threat Management" [en línea]. Disponible en Web:
http://www.fortinet.com/
http://www.fortinet.com/products/fortigate_overvie.html
http://www.fortinet.com/doc/FGT1000-3800DS.pdf

[15] GONCALVES Marcus, "Firewalls Complete", Mc Graw Hill Beta Books, Cap 6, Enero 1997, Recuperado de Internet: <URL: http://www.ods.com.ua/win/eng/security/firewall/preface.htm>

ANEXOS

GLOSARIO

- **Abuso de privilegio**: se produce cuando un usuario realiza una acción que no tiene asignada de acuerdo a la política organizativa o a la ley.
- **Ataque interior**: es un ataque originado desde dentro de la propia red protegida.
- **Autentificación**: proceso que determina la identidad de un usuario que está intentando acceder a un sistema.
- **Autorización**: proceso destinado a determinar que tipos de actividades se permiten. Normalmente la autorización se encuentra en el contexto de la autentificación: una vez autentificado el usuario en cuestión, se les puede autorizar realizar diferentes tipos de acceso o actividades.
- **Amenaza:** Situación o evento con que puede provocar daños en un sistema. Análisis de vulnerabilidades: Análisis del estado de la seguridad de un sistema o sus componentes mediante el envío de pruebas y recogida de resultados en intervalos. Análisis dinámico, o en tiempo real: Análisis desarrollado en tiempo real, o de forma continúa.
- **Análisis sin acreditaciones:** En análisis de vulnerabilidades, enfoque de monitorización pasiva en los que las contraseñas u otro tipo de credenciales no son necesarias. Normalmente implica el lanzamiento de ataques contra el sistema, provocando algún tipo de reacción.
- **Aplicación engañosa:** Aplicación cuya apariencia y comportamiento emulan a una aplicación real. Normalmente se utiliza para monitorizar acciones realizadas por atacantes o intrusos. Ataque por interceptación: Estrategia de ataque en la que el atacante intercepta una comunicación entre dos partes, substituyendo el tráfico entre ambas a voluntad y controlando la comunicación.
- **Bastion Host**: un sistema que ha sido configurado para resistir los ataques y que se encuentra instalado en una red en la que se prevé que habrá ataques. Normalmente, un bastion host está ejecutando alguna aplicación o sistema operativo de propósito general (como: UNIX o WNT) más que un sistema operativo de firewall.
- **Basado en testigo:** Sistemas que emplean elementos especiales como tarjetas inteligentes, llaves, o discos para la autenticación de usuario.

- **Base de reglas:** Conjunto de reglas utilizadas para analizar los registros de datos.
- **Caballo de Troya, troyano:** Programa informático de aspecto inofensivo que oculta en su interior un código que permite abrir una "puerta trasera" en el sistema en que se ejecuta. Capacidad de ser registrado: Habilidad de relacionar una determinada actividad o evento con la parte responsable.
- **Cifrado:** Proceso mediante el cual se toma un mensaje en claro, se le aplica una función matemática, y se obtiene un mensaje codificado.
- **Composición:** 1. En detección de intrusiones, proceso de combinar información procedente de distintas fuentes en un flujo de datos coherente. 2. En seguridad informática, combinar un conjunto de componentes en un sistema para obtener los atributos de seguridad del sistema, según las propiedades de los componentes.
- **Comprobador de integridad:** Herramienta de seguridad que utiliza funciones resumen basadas en algoritmos de cifrado para detectar alteraciones en objetos de sistema. Control de acceso: Limitar el acceso a objetos de acuerdo a los permisos de acceso del sujeto. El control de acceso puede ser definido por el sistema (Control de accesos obligatorio, MAC) o por el propietario del objeto (Control de accesos discrecional, DAC).
- **Control de acceso discrecional (DAC):** Política de acceso a los datos en la que el propietario del objeto, de forma voluntaria (discrecional), concede o deniega el acceso a éste a otros sujetos.
- **Control de accesos obligatorio (MAC):** Política de acceso a los datos en la que el sistema comparte de forma obligatoria tanto los objetos como los sujetos. A partir de dicha forma de compartir los elementos, se establecen unas reglas de acceso.
- **Cortafuegos:** Herramienta de seguridad que proporciona un límite entre redes de distinta confianza o nivel de seguridad mediante el uso de políticas de control de acceso de nivel de red. Criterio de Evaluación de Sistemas Informáticos Fiables (TCSEC): Conocido comúnmente como Libro Naranja, describe las propiedades que deben cumplir los sistemas para contener información sensible o clasificada. Este criterio fue desarrollado por el Centro de Seguridad Informática Nacional (NCSC).

- **Detección de intrusión**: detección de rupturas o intentos de rupturas bien sea manual o vía sistemas expertos de software que atentan contra las actividades que se producen en la red o contra la información disponible en la misma.
- **Dual Homed Gateway**: es un sistema que tiene 2 o más interfaces de red, cada uno de los cuales está conectado a una red diferente. En las configuraciones firewall, un "dual homed gateway" actúa generalmente, como bloqueo o filtrador de parte o del total del tráfico que intenta pasar entre las redes.
- **Datagrama:** Mensaje que se envía en una red de comunicaciones de ordenadores por intercambio de paquetes.
- **Denegación de servicio distribuida (DDoS):** Estrategia de ataque que coordina la acción de múltiples sistemas para saturar a la víctima con información inútil para detener los servicios que ofrece. Los sistemas utilizados para el ataque suelen haber sido previamente
- **Deslizamiento sigiloso de sesión:** Técnica utilizada por un usuario que consiste en modificar gradualmente su comportamiento para entrenar al detector de anomalías. De esta forma, se consigue que el detector diagnostique como actividad normal un posible ataque. Detección de intrusiones: Proceso de monitorizar los eventos de un sistema o red en busca de signos que indiquen problemas de seguridad.
- **Detector de Intrusiones de Nodo de Red:** Detector de intrusiones basado en red que se instala en una máquina. Esta medida ayuda a solventar problemas como los asociados a entornos conmutados, o cifrado en las comunicaciones.
- **Enmascarado:** Atacante que accede a un sistema utilizando identificadores de usuario y contraseñas de usuarios legítimos.
- **Error de Tipo I:** En detección de intrusiones, error producido cuando el sistema diagnostica como ataque una actividad normal. También conocido como falso positivo.
- **Error de Tipo II:** En detección de intrusiones, error producido cuando el sistema diagnostica como actividad normal un ataque. También conocido como falso negativo.
- **Escaneo sigiloso de puertos:** Barrido de puertos mediante diversas técnicas con el fin de evadir los métodos de detección comunes. Algunas de estas técnicas

implican un escaneo intencionadamente lento, o el envío de paquetes especiales aprovechando particularidades del protocolo.

- **Firma, patrón:** En detección de intrusiones, patrones que indican los usos indebidos de un sistema.
- **Formato de registro binario:** Formato de registro utilizado por herramientas basadas en las librerías "libpcap", como por ejemplo "tcpdump". Se aplica para registrar el tráfico de red. Algunas de las ventajas del formato binario sobre el formato ASCII son que ocupa menos, y la información que contiene puede ser accedida en menor tiempo.
- **Gestión de redes:** Controlar diversos aspectos de una red para optimizar su eficiencia. Las cinco categorías de gestión de red son: seguridad, fallo, auditoría, configuración y gestión de rendimiento.
- **Gestión de seguridad: 1.** Proceso de establecer y mantener la seguridad en un sistema o red de sistemas informáticos. Las etapas de este proceso incluyen la prevención de problemas de seguridad, detección de intrusiones, investigación de intrusiones, y resolución. 2. En gestión de redes, controlar (permitir, limitar, restringir, o denegar) acceso a la red y recursos, buscar intrusiones, identificar puntos de entrada de intrusiones, y reparar o cerrar estas posibles vías de acceso.
- **Identificación y autenticación (I&A):** Mecanismo de seguridad que asigna una identidad única a cada usuario (identificación) y la comprueba (autenticación).
- **Lista de Control de Acceso (ACL):** Conjunto de datos que indican al sistema operativo qué permisos tiene un usuario o grupo sobre un determinado objeto de sistema. Cada objeto tiene atributos de seguridad únicos que indican qué usuarios pueden accederlo, y la Lista de Control de Acceso contiene una descripción de los privilegios de acceso de cada objeto y usuario. Módulo de Seguridad Básico (BSM): Paquete de seguridad de Sun Microsystem proporcionado por los sistemas operativos de Sun para cumplir con los requisitos del documento TCSEC (la clase C2).
- **Logging**: el proceso de almacenamiento de información sobre eventos que ocurren en el firewall o en la red.
- **Política**: reglas de gobierno a nivel empresarial / organizativo que afectan a los recursos informáticos, prácticas de seguridad y procedimientos operativos.

- **Proxy**: un agente software que actúa en beneficio de un usuario. Los proxies típicos, aceptan una conexión de un usuario, toman una decisión al respecto de si el usuario o cliente IP es o no un usuario del proxy, quizás realicen procesos de autentificación adicionales y entonces completan una conexión entre el usuario y el destino remoto.
- **Paquete:** Estructura de datos con una cabecera que puede estar o no lógicamente completa. Más a menudo, se refiere a un empaquetamiento físico de datos que lógico. Se utiliza para enviar datos a través de una red conmutada de paquetes.
- Política de seguridad: 1. Conjunto de estatutos que describen la filosofía de una organización respecto a la protección de su información y sistemas informáticos. 2. Conjunto de reglas que ponen en práctica los requisitos de seguridad del sistema.
- **Puerta trasera:** Mecanismo que permite a un atacante entrar y controlar un sistema de forma oculta. Suelen instalarse justo después de comprometer un sistema.
- **Router - Encaminador:** dispositivo destinado a conectar 2 o más redes de área local y que se utiliza para encaminar la información que atraviesa dicho dispositivo.
- **Screened Host**: un host detrás de un router protegido. El grado en que el host puede ser accesible depende de las reglas de protección del router.
- **Screened Subnet**: una subred detrás de un router protegido. El grado en que la subred puede ser accesible depende de las reglas de protección del router.
- **Sistema de prevención de intrusiones (IPS):** Sistema que combina las capacidades de bloqueo de un cortafuegos y las de análisis de un IDS. Está diseñado para detener ataques antes de que tengan éxito.
- **Virus polimórfico:** Virus informático que cambia de aspecto con cada ejecución. Esta característica tiene el objeto de evitar los detectores de virus.
- **Vulnerabilidades:** Debilidades en un sistema que pueden ser utilizadas para violar las políticas de seguridad.
- **Zona desmilitarizada, red perimétrica (DMZ):** Máquina o pequeña subred situada entre una red interna de confianza (como una red local privada) y una red externa no confiable (como Internet). Normalmente en esta zona se sitúan los dispositivos accesibles desde Internet, como servidores Web, FTP, SMTP o DNS, evitando la necesidad de acceso desde el exterior a la red privada. Este término es de origen militar, y se utiliza para definir un área situada entre dos enemigos.

FortiAnalyzer Report

Report Name: Scheduled-Application_Usage_Report-2011-10-19-1623
Report Title: Bandwidth_and_Application_Usage
Generated on: Wed Oct 19 16:23:53 2011
Scheduled Period: 2011-10-12 00:00 - 2011-10-18 23:59 COT
(FortiAnalyzer local) Devices: 2

Cover Page

FortiAnalyzer
Application Usage Report
FortiAnalyzer Host Name: FortiAnalyzer-100C
FortiAnalyzer Serial Number: FL100C3911000185

Application Usage

Bandwidth consumption and application usage data can be an important indicator of your organization's security status. Inordinately high bandwidth consumption or the presence of unauthorized applications traversing your network could be due to inappropriate behavior on the part of the user or evidence that malware has infected your systems.

To help you assess the status of your bandwidth consumption and application utilization, this report provides data on the following:

* Bandwidth consumption by user

* Top users by number of sessions

* Top application categories by bandwidth usage

* Top application categories by number of sessions

* WAN optimization and cache performance

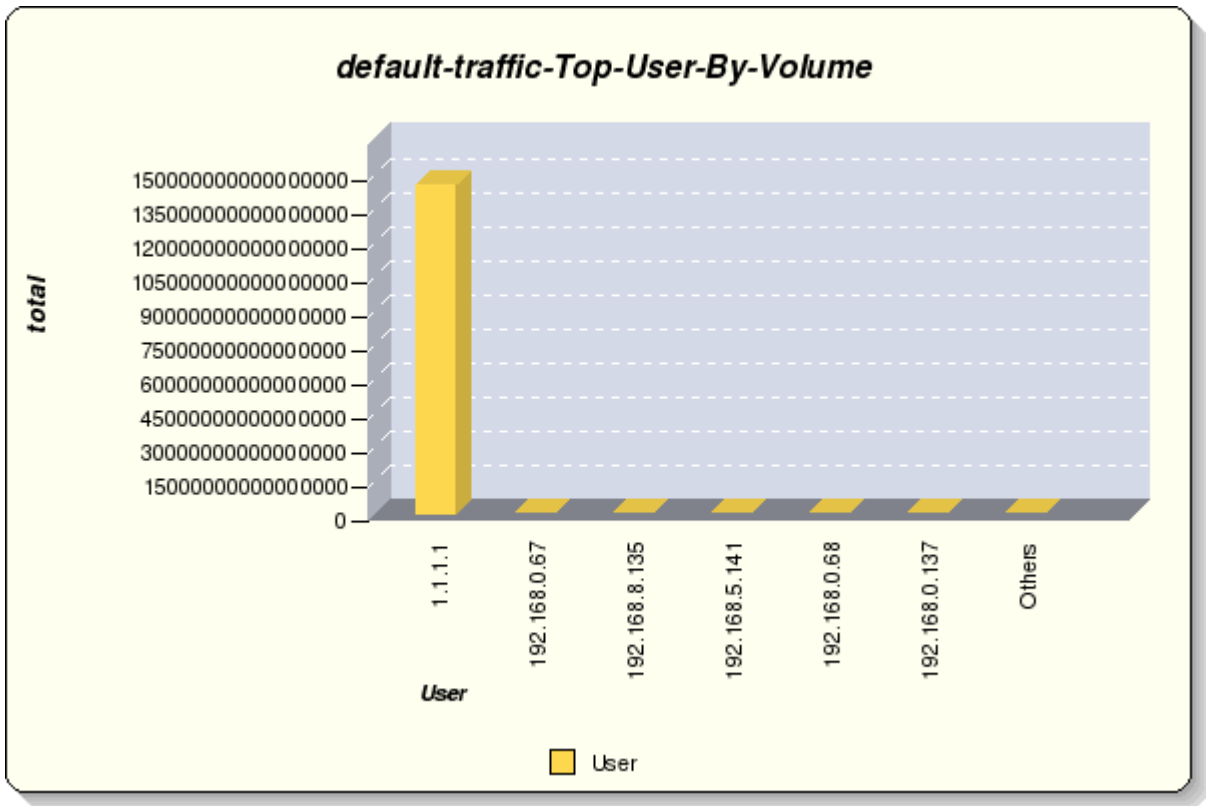
Top Users By Bandwidth

default-traffic-Top-User-By-Volume

Top Users By Bandwidth

All FortiGates

Period: 2011-10-12 00:00:00 - 2011-10-18 23:59:59COT (FortiAnalyzer Local)



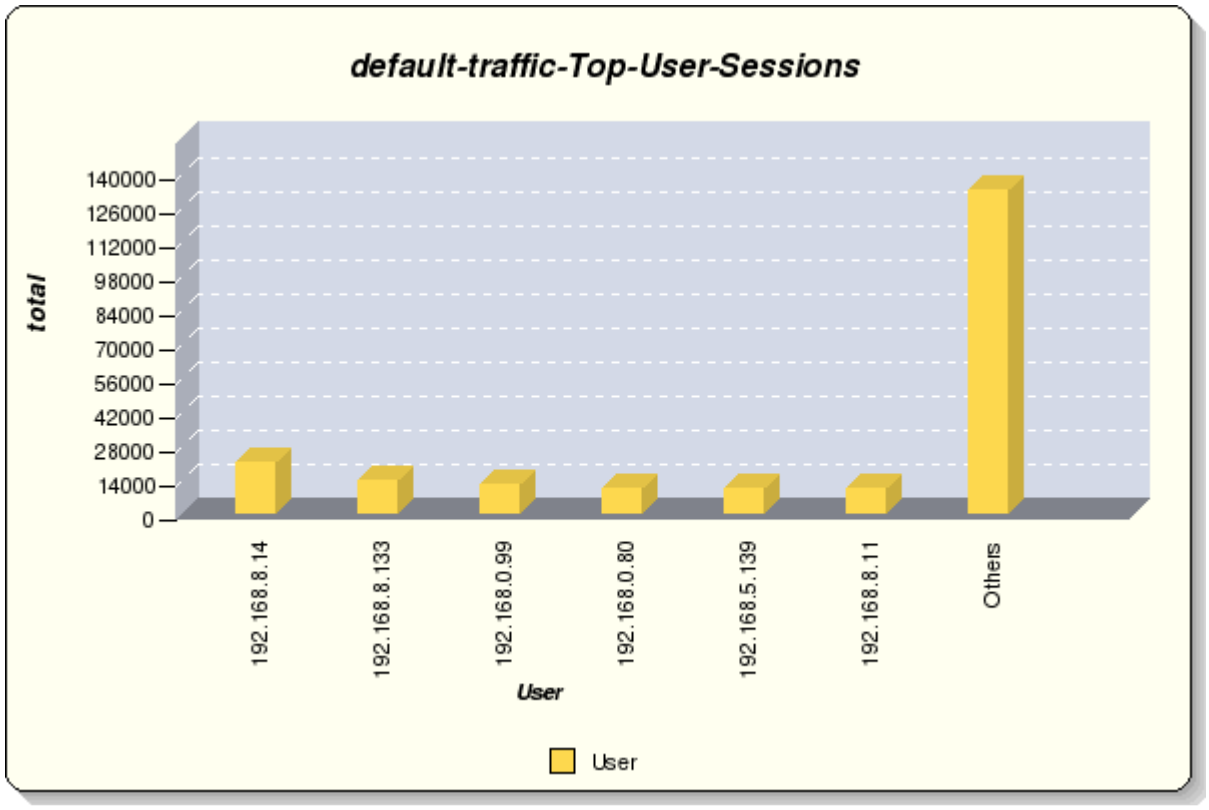
Top Users By Session

default-traffic-Top-User-Sessions

Top Users by Sessions

All FortiGates

Period: 2011-10-12 00:00:00 - 2011-10-18 23:59:59COT (FortiAnalyzer Local)



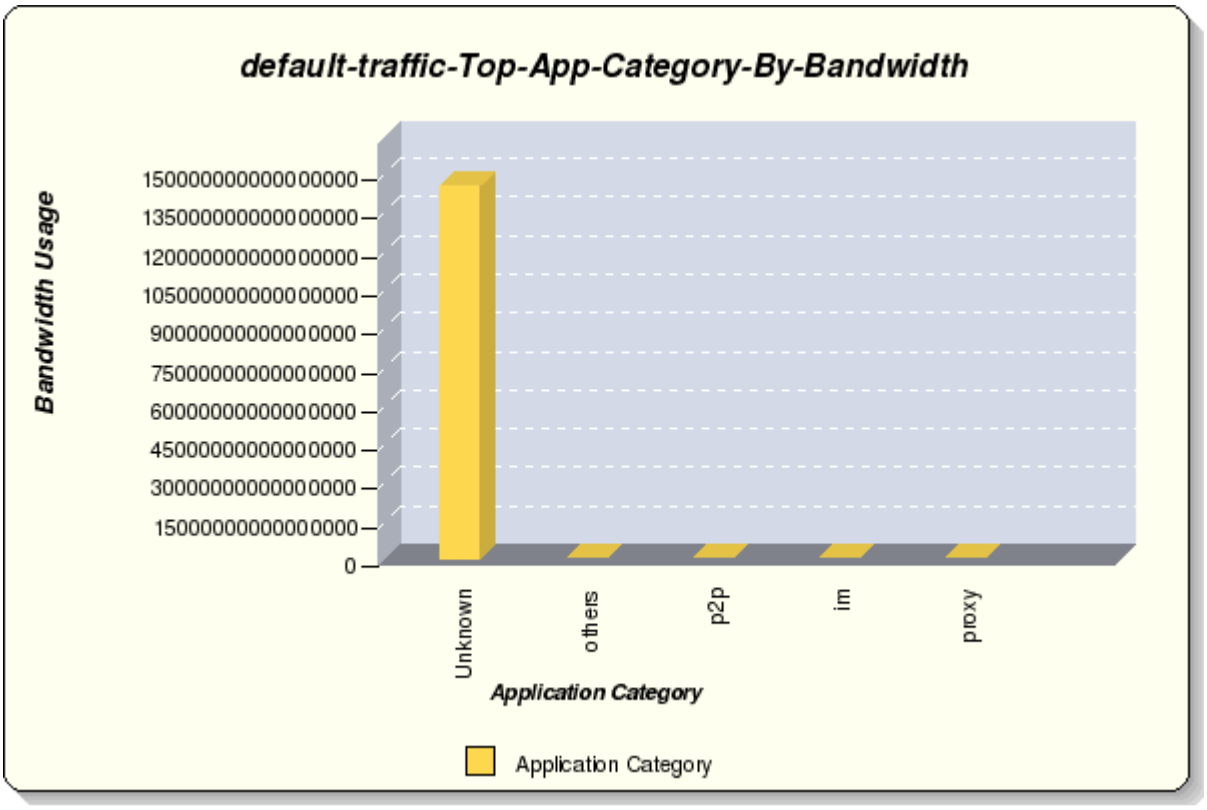
Top Application Categories By Bandwidth

default-traffic-Top-App-Category-By-Bandwidth

Top Application Categories by Bandwidth

All FortiGates

Period: 2011-10-12 00:00:00 - 2011-10-18 23:59:59COT (FortiAnalyzer Local)



default-traffic-Top-App-Category-By-Bandwidth		
Application Category	Bandwidth Usage	% of Total
Unknown	144680345676153346	100.00
others	5337837900	0.00
p2p	6050410	0.00
im	123936	0.00
proxy	10976	0.00
Total	**144680351020176568**	**100.00**

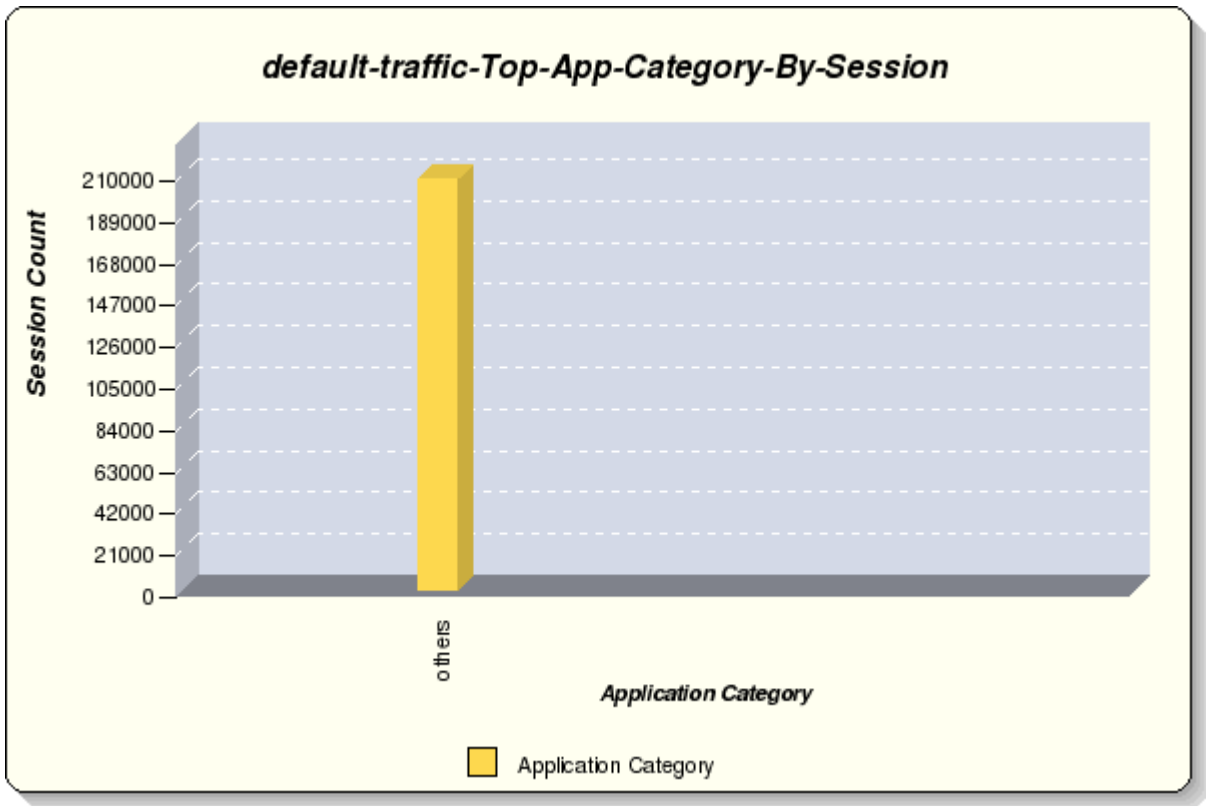
Top Application Categories By Session

default-traffic-Top-App-Category-By-Session

Top Application Categories by Sessions

All FortiGates

Period: 2011-10-12 00:00:00 - 2011-10-18 23:59:59COT (FortiAnalyzer Local)



default-traffic-Top-App-Category-By-Session		
Application Category	Session Count	% of Total
others	207341	100.00
Total	**207341**	**100.00**

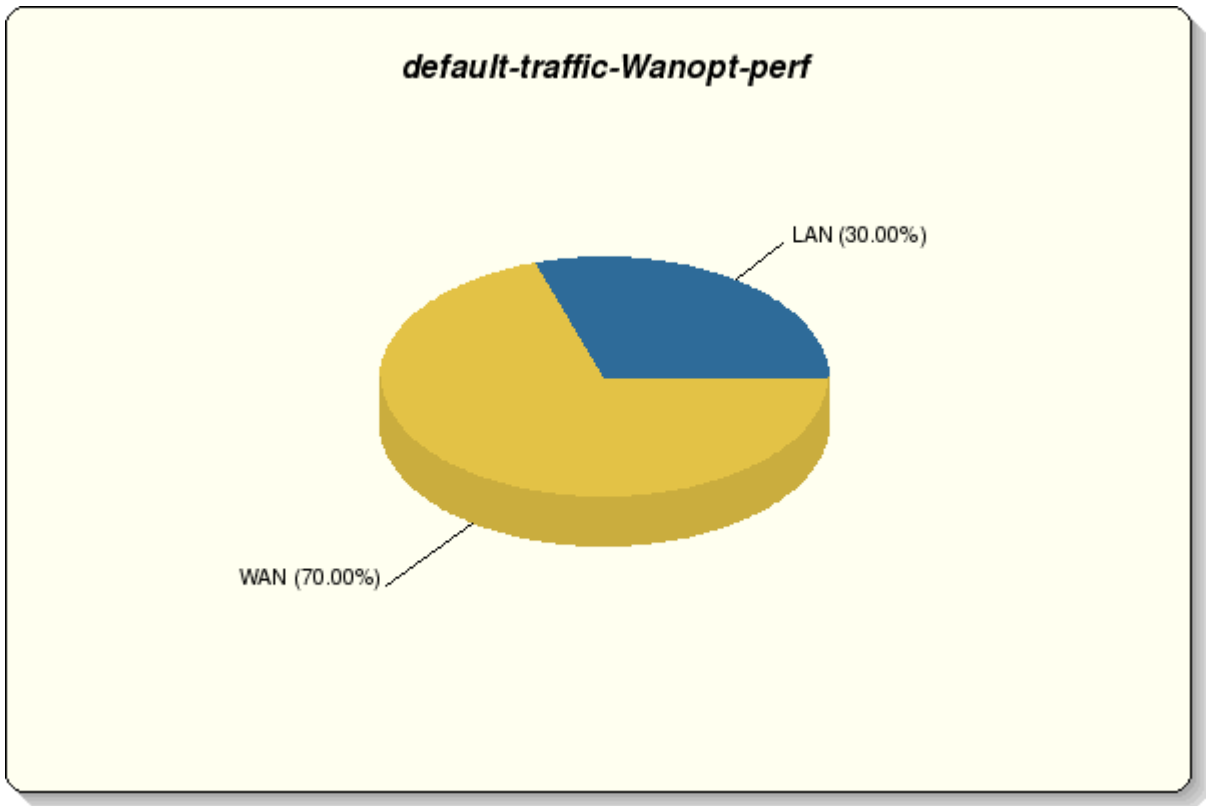
Wan Optimization & Cache Performance

default-traffic-Wanopt-perf

Wan Optimization & Cache Performance

All FortiGates

Period: 2011-10-12 00:00:00 - 2011-10-18 23:59:59COT (FortiAnalyzer Local)



Cover Page

FortiAnalyzer

Web Filtering and Usage Report

FortiAnalyzer Host Name: FortiAnalyzer-100C

FortiAnalyzer Serial Number: FL100C3911000185

Web Filtering and Usage

Understanding how individuals in your organization are utilizing the web assists in improving employee productivity, meeting regulatory requirements and identifying possible infections and security breaches. To help you assess the status of your bandwidth consumption and application utilization, this report provides data on the following:

*** Blocked users for web site**

*** Allowed users for web site**

*** Allowed web categories**

*** Blocked web categories**

*** Top search phrases**

*** Top allowed web sites**

*** Top blocked web sites**

*** Top websites by bandwidth**

*** Video streaming sites by bandwidth**

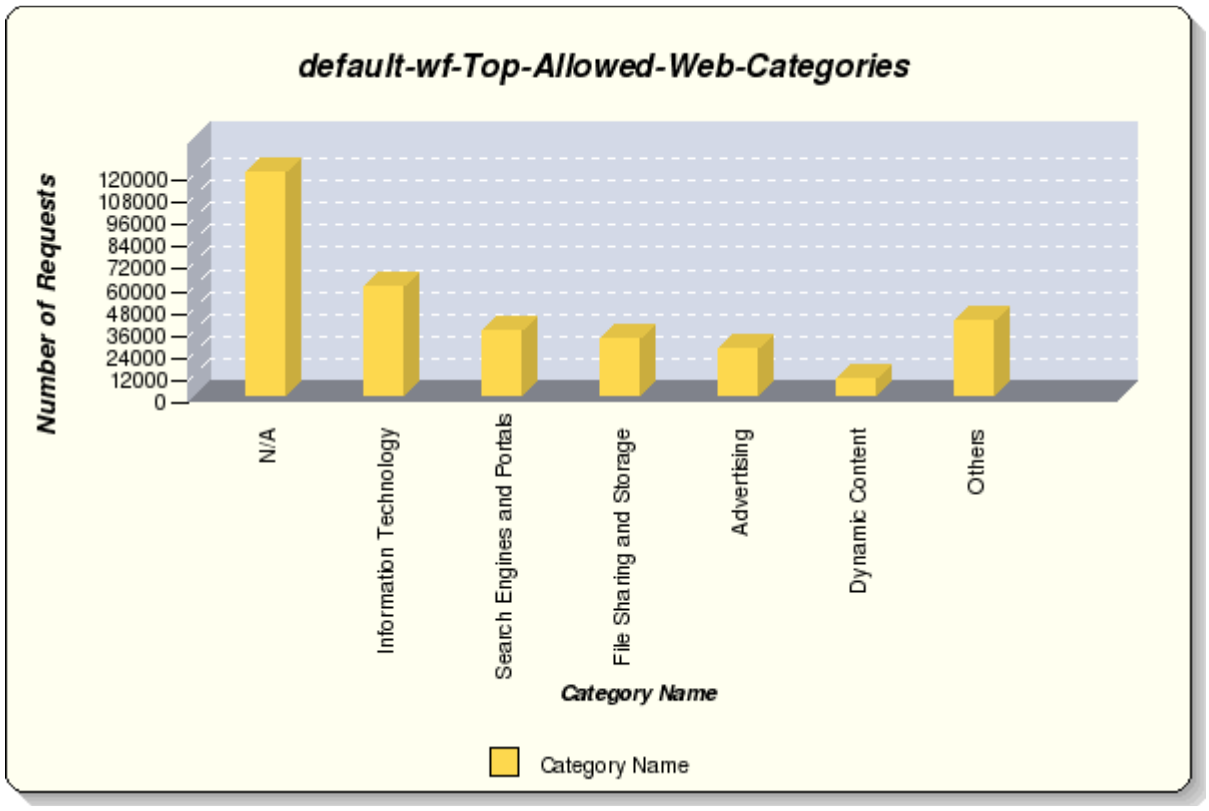
Top Allowed Web Categories (Requests)

default-wf-Top-Allowed-Web-Categories

Top Allowed Web Categories by Requests

All FortiGates

Period: 2011-10-12 00:00:00 - 2011-10-18 23:59:59COT (FortiAnalyzer Local)



default-wf-Top-Allowed-Web-Categories		
Category Name	Number of Requests	% of Total
N/A	119693	37.67
Information Technology	58766	18.49
Search Engines and Portals	34820	10.96
File Sharing and Storage	30095	9.47
Advertising	25345	7.98
Dynamic Content	8872	2.79
Others	40163	12.64
Total	**317754**	**100.00**

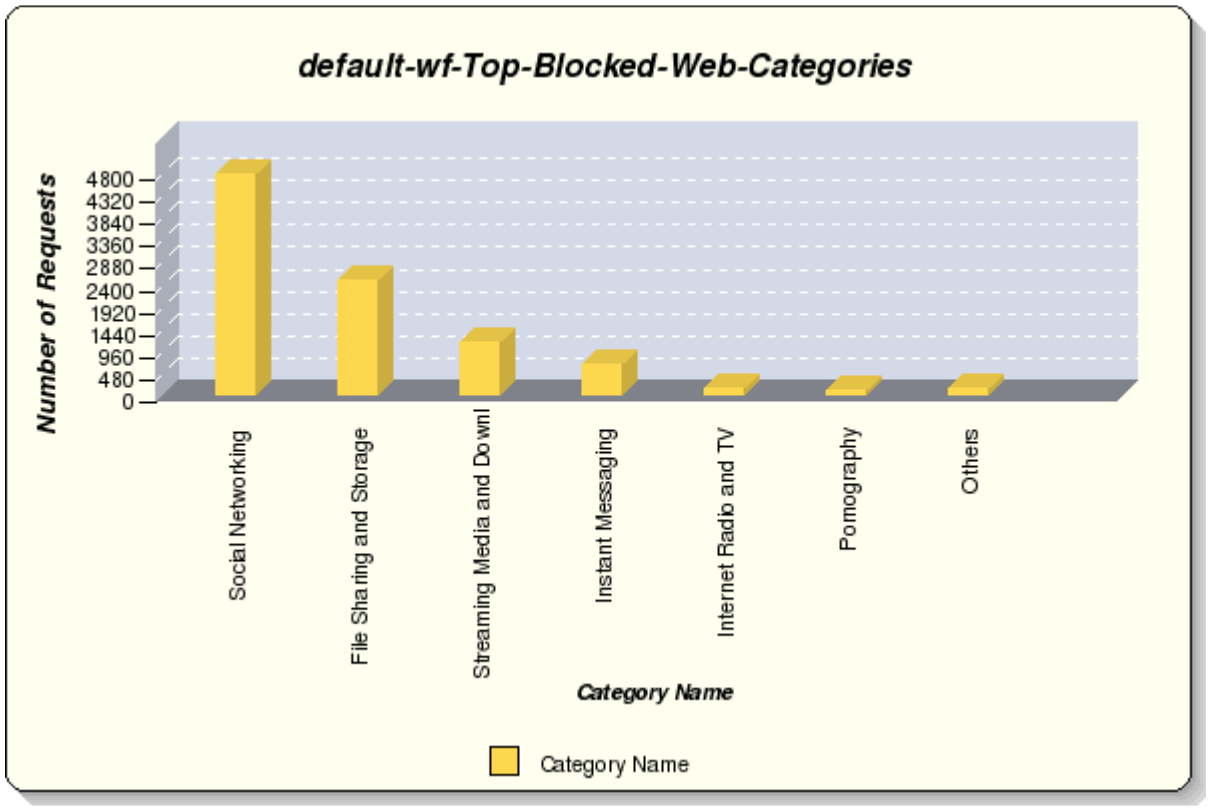
Top Blocked Web Category(Request)

default-wf-Top-Blocked-Web-Categories

Top Blocked Web Categories

All FortiGates

Period: 2011-10-12 00:00:00 - 2011-10-18 23:59:59COT (FortiAnalyzer Local)



default-wf-Top-Blocked-Web-Categories		
Category Name	Number of Requests	% of Total
Social Networking	4743	51.01
File Sharing and Storage	2445	26.30
Streaming Media and Download	1141	12.27
Instant Messaging	633	6.81
Internet Radio and TV	121	1.30
Pornography	85	0.91
Others	130	1.40
Total	**9298**	**100.00**

Top Search Phrases

default-wf-Top-Search-Phrases

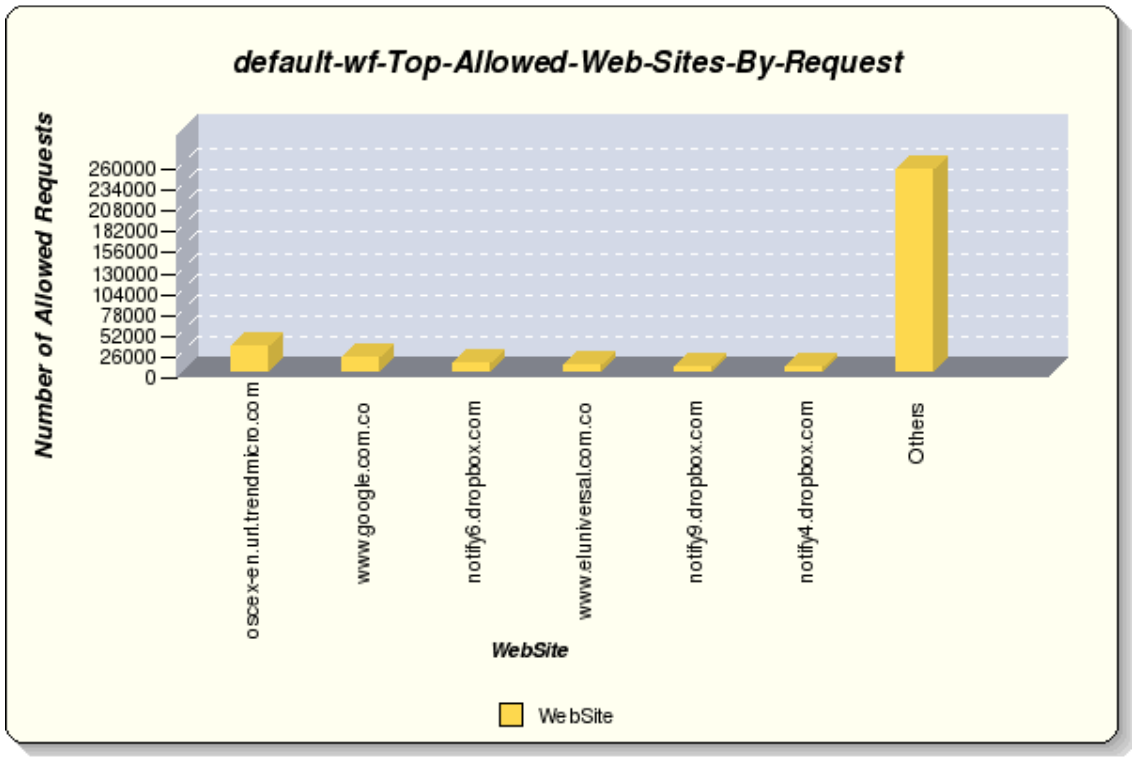
All FortiGates
Period: 2011-10-12 00:00:00 - 2011-10-18 23:59:59COT (FortiAnalyzer Local)
No matching log data for this report

Top Allowed Web Sites (Requests)

default-wf-Top-Allowed-Web-Sites-By-Request

Top Allowed Web Sites

All FortiGates
Period: 2011-10-12 00:00:00 - 2011-10-18 23:59:59COT (FortiAnalyzer Local)



default-wf-Top-Allowed-Web-Sites-By-Request		
WebSite	Number of Allowed Requests	% of Total
oscex-en.url.trendmicro.com:80	29340	9.12
www.google.com.co	17369	5.40
notify6.dropbox.com	8782	2.73
www.eluniversal.com.co	6782	2.11
notify9.dropbox.com	4225	1.31
notify4.dropbox.com	3965	1.23
Others	251112	78.09
Total	**321575**	**100.00**

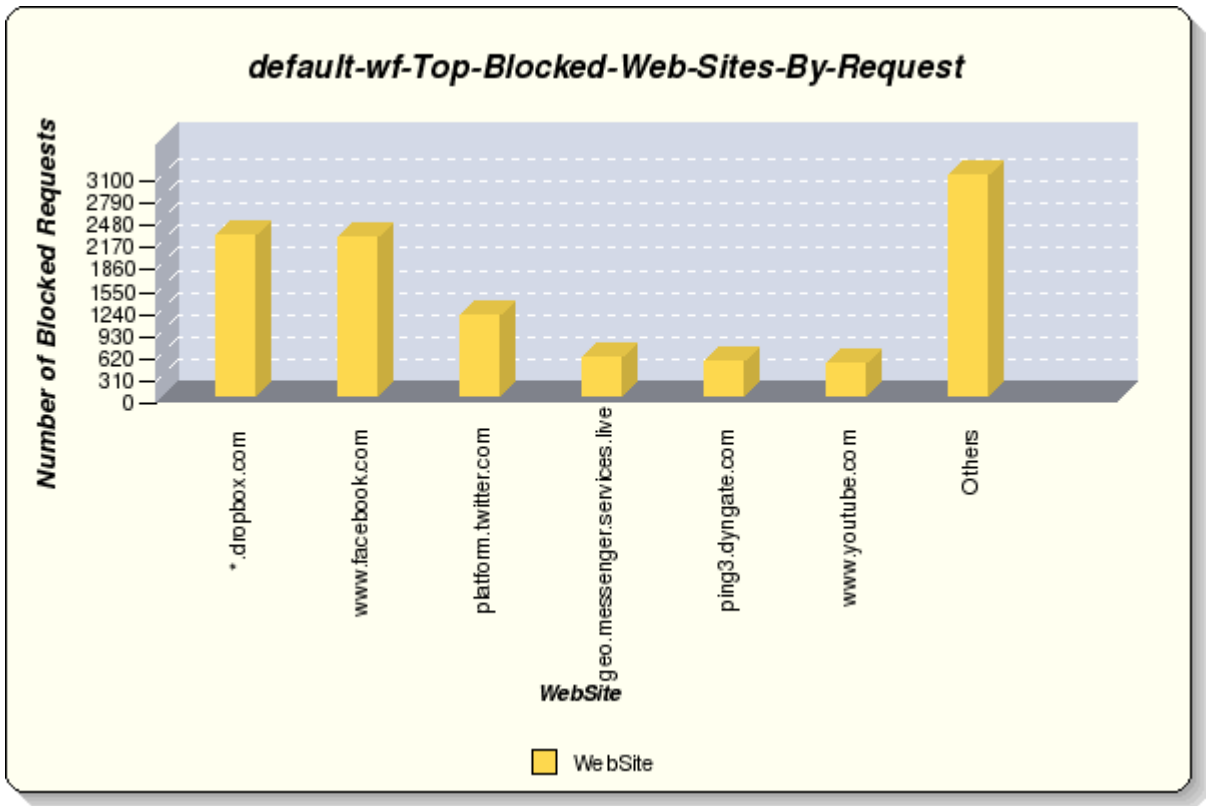
Top Blocked Web Sites

default-wf-Top-Blocked-Web-Sites-By-Request

Top Blocked Web Sites By Request

All FortiGates

Period: 2011-10-12 00:00:00 - 2011-10-18 23:59:59COT (FortiAnalyzer Local)



default-wf-Top-Blocked-Web-Sites-By-Request		
WebSite	Number of Blocked Requests	% of Total
*.dropbox.com	2232	22.18
www.facebook.com	2195	21.82
platform.twitter.com	1111	11.04
geo.messenger.services.live.com	525	5.22
ping3.dyngate.com	471	4.68
www.youtube.com	442	4.39
Others	3085	30.66
Total	**10061**	**100.00**

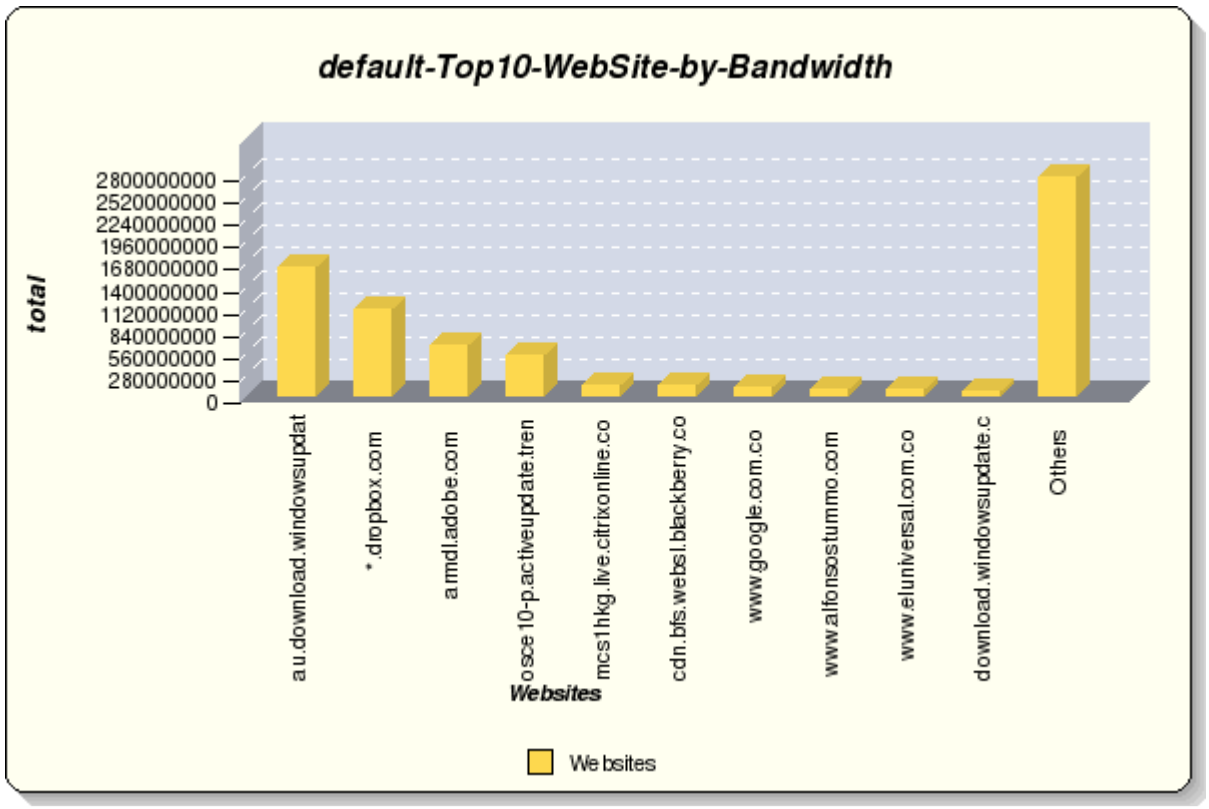
Top Web Sites (Bandwidth)

default-Top10-WebSite-by-Bandwidth

Top Web Sites

All FortiGates

Period: 2011-10-12 00:00:00 - 2011-10-18 23:59:59COT (FortiAnalyzer Local)



Top Video Streaming Web Sites (Bandwidth)

default-Top10-Video-Streaming-By-WebSites-By-Bandwidth

Top Video Streaming Web Sites

All FortiGates
Period: 2011-10-12 00:00:00 - 2011-10-18 23:59:59COT (FortiAnalyzer Local)