ITSON
Educar para
Trascender

INSTITUTO TECNOLÓGICO DE SONORA

DISEÑO DE UNA PLATAFORMA DE SEGURIDAD Y GESTIÓN DE RED BASADA EN EL TIPPING POINT 3COM X5.

TITULACIÓN POR TESIS
QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN ELECTRÓNICA

PRESENTA:

JESÚS IGNACIO BRICEÑO RUÍZ

CD. OBREGÓN, SONORA JULIO-2009

Resumen

En este trabajo se describe el procedimiento utilizado en la instalación y configuración del Tipping Point 3com x5 3crtpx5-u-96 en la empresa Siselec (Sistemas Electrónicos Sulu S. A. de C. V.) como plataforma de seguridad y gestión de red.

En el capítulo I, se expone principalmente al lector el problema de estudio, las razones por las cuales se llevo a cabo este trabajo, así como los alcances y limitaciones del mismo.

El capítulo II, ofrece una breve introducción a las redes de computadoras, seguida de una breve perspectiva actual referente a la seguridad en redes computacionales y se finaliza con el estudio de las principales características de los protocolos de comunicaciones.

En el capítulo III, en una primera instancia se ofrece al lector una breve descripción de las características y prestaciones del Tipping Point x5 como objeto principal de estudio, posteriormente se aborda el procedimiento utilizado en la inicialización por primera vez del Tipping Point x5, su integración física a la red Local, su configuración, la conexión del dispositivo a la Internet y la integración total y funcional del dispositivo en la red.

El capítulo IV, indica las pruebas realizadas para comprobar y evaluar el funcionamiento del Tipping Point x5 y de su configuración así como los resultados obtenidos a partir de estas.

Por último se exponen las conclusiones obtenidas al finalizar el trabajo.

INDICE

Lista de figuras

CAPÍTULO I
INTRODUCCIÓN

1.1 Antecedentes

Actualmente el uso de dispositivos electrónicos orientados a garantizar la seguridad en una red computacional es tan difundido que las compañías desarrolladoras de este tipo de tecnologías se encuentran en clara competencia por el dominio del mercado.

Diversas marcas ofrecen al consumidor gran variedad en plataformas de seguridad que se ajustan a las necesidades de protección de cada empresa, tales necesidades pueden ir desde un simple firewall hasta un complejo dispositivo que brinde además entre otras prestaciones la capacidad de crear zonas de seguridad en una red VPN (Virtual Prívate Network).

Con la aparición del primer computador personal lanzado por IBM (International Business Machines) el 12 de agosto de 1981 se abrió una amplia gama de

posibilidades para el uso de está tecnología, tiempo después surgió la necesidad de conectar dos o más dispositivos entre sí, dando pie a la creación de las redes de computadoras; con el desarrollo de las primeras redes surgieron otras necesidades de gestión, es decir, establecer las características internas de red como el tráfico y la clase de información que en esta se maneja, privilegios y restricciones de los usuarios, etc., en ese momento los nombres de usuario y claves de acceso eran más que suficientes como garantía de seguridad y nadie podía concebir un ataque malicioso con el fin de crear un caos.

Cuando apareció el primer virus informático llamado “Elk Cloner” (creado en 1982 por Rich Skrenta) que se propagaba a través de disquetes infectados del sistema operativo del Apple II y que no representaba una amenaza a los equipos de computo, nadie podía imaginar las consecuencias que traería años más adelante el desarrollo de este tipo de ataques y amenazas.

Con el desarrollo del Internet las posibilidades de conectividad se ampliaron de manera exponencial y a la vez la seguridad en las redes comenzó a verse amenazada por virus aun más complejos, estos virus dieron pie a que se presentaran ataques más poderosos y que las pérdidas de información y de tiempo de trabajo se empezarán a traducirse en pérdidas monetarias para las empresas, los desarrolladores de redes tomaron cartas en el asunto y se enfocaron a la tarea de desarrollar medidas de seguridad aplicables en las redes empresariales.

Las medidas de seguridad, han ido desde simples ruteos físicos por medio de hardware hasta complejos dispositivos que en base a programación pueden realizar una infinidad de funciones.

Los primeros Firewalls si es que podía llamárseles de esa manera, no eran más que simples routers que separaban redes; una vez que los nombres de usuario y claves de seguridad no fueron suficientes se comenzó a aplicar algoritmos de cifrado de información para garantizar que la información transmitida a través de la Internet y la red no fuera corrompida; además de las necesidades de seguridad existen también necesidades de gestión de red, en algunas redes se priorizan ciertos servicios o características por sobre otros, por ejemplo destinar un mayor rango del ancho de

banda para la transmisión de VoIP (Voice over IP) por encima de la transmisión de mensajería instantánea o aplicar políticas de filtrado de contenido Web entre otras.
Los desarrolladores de redes ponen especial énfasis en garantizar que la red que se implementa sea confiable y de rendimiento óptimo, es decir, garantizar que la conectividad este al alcance de cada uno de los usuarios, que la información manejada esté protegida ante amenazas de cualquier tipo y que la red utilice de manera óptima los recursos de los que dispone.
Actualmente y a beneficio de todos existen múltiples opciones en tecnología desarrollada específicamente para dar soluciones a los puntos mencionados anteriormente, en los ingenieros recae la responsabilidad de elegir de manera correcta e inteligente la opción que satisfaga las necesidades de la red, existen dispositivos que como uno solo brindan soluciones por separado de Cortafuegos, Anti-Spam, Filtrado Web, Modulación de ancho de banda, etc., más sin embargo lo ideal seria contar con un dispositivo tan versátil que pueda reunir todas estás características en uno solo tal como lo hace el Tipping Point x5 3crtpx5-u-96 de 3com y en el cual se centra la realización de este trabajo.

1.2 Definición del problema

Los requerimientos de seguridad y gestión de una red computacional determinan las características del hardware y del software a utilizar, es decir, será un gran desperdicio utilizar dispositivos muy complejos cuyas prestaciones excedan en mucho las necesidades de una red muy sencilla, así como será un gran riesgo y un grave error de diseño utilizar dispositivos que no brinden las medidas adecuadas en seguridad y gestión que requiera una red compleja en la que la accesibilidad, confiabilidad y el manejo de información critica sean prioridad.
Una vez expuesto estos puntos importantes reducimos el problema a una simple acción, la elección y diseño inteligente de una plataforma de seguridad y gestión que satisfaga los requerimientos de una red específica.

1.3 Justificación

La importancia de este trabajo recae en el hecho de que su realización busca presentar las bases para un plan de acción que sirva para brindar una solución a una necesidad real presente dentro de la empresa Siselec (Sistemas Electrónicos Sulu S.A. de C.V.).

El cliente desea resultados, el cliente desea una conectividad de red accesible en todo momento, desea que su información este completamente segura, desea además tener control absoluto en la gestión de su red; por ejemplo: priorizar servicios unos sobre otros, como podría ser VoIP sobre tráfico Web, establecer políticas de tráfico de red, características de filtrado de contenido Web, etc., en pocas palabras el cliente tiene el privilegio de dictaminar las características de su red y el ingeniero tendrá la responsabilidad y la capacidad de llevar todo esto a cabo en la medida que sea posible.

Debido a las necesidades del cliente se llevará a cabo el diseño de una plataforma de seguridad y gestión de red basada en el Tipping Point x5 3crtpx5-u-96 de 3com en la empresa Siselec, el cual vendrá a dar solución a los requerimientos de la red específicos, este trabajo proveerá además una gran experiencia laboral, proporcionará habilidades prácticas y herramientas útiles al momento de llevar a cabo este tipo de proyectos.

1.4 Objetivo

El objetivo general de este trabajo consiste en el Diseño de una plataforma de seguridad y gestión de red basada en el Tipping Point 3com x5, esto implica la integración física del dispositivo a la red empresarial en la que se está trabajando además de la configuración necesaria para llevar esto acabo.

Como objetivos específicos podemos señalar los siguientes:

- Configuración del Tipping Point x5 como plataforma de seguridad que implica la configuración del dispositivo para satisfacer las necesidades de seguridad que la empresa necesita
- Configuración del Tipping Point x5 como plataforma de gestión que Implica la configuración del dispositivo para satisfacer las necesidades de gestión de información y servicios que la empresa necesita.

La motivación de llevar a cabo este trabajo viene precedida de la conjunción de estos objetivos mencionados.

1.5 Limitaciones

Una de las limitaciones más criticas y que considero la más importante que enfrentará el desarrollo de este trabajo será la falta de experiencia en la configuración e instalación práctica de este tipo de dispositivos, lo que conllevará una investigación y estudio exhaustivo de las características del dispositivo utilizado.
La falta de trabajos relacionados con este tipo de problemáticas añade otra limitación ya que no es posible tomar investigaciones anteriores como base para la realización de este trabajo y a pesar de que la compañía desarrolladora de este dispositivo cuenta con un soporte técnico altamente capacitado, al ser este de tipo remoto limita en cierta medida la calidad del mismo.

1.6 Alcances

El desarrollo de este trabajo incluye el diseño de la plataforma de seguridad y gestión de red, así como la configuración necesaria para la instalación e integración física del Tipping Point 3com x5 3crtpx5-u-96 en la red empresarial en donde se llevan a cabo las prácticas profesionales.

Una vez instalado el dispositivo en la red, se realizará la configuración necesaria que de solución a las necesidades de seguridad de la red, tales como aplicación de políticas de Cortafuegos, políticas de Anti-Spam entre otros ajustes solicitados por el supervisor de proyecto, además se realizará la configuración del dispositivo para permitir una gestión de red acorde a los requerimientos solicitados, tales como habilitación de Servidores Virtuales, creación y negación de privilegios a usuarios externos e internos de la red y Filtrado de Contenido Web.

Los alcances están sujetos a cambios, es posible que durante la realización de este trabajo los requerimientos cambien e incluso sean solicitados otros que no se tenían contemplados y por lo tanto serán incluidos en el desarrollo del proyecto con previa evaluación y autorización.

CAPÍTULO II
FUNDAMENTACION TEORICA

2.1 Introducción a las redes de Computadoras

Podemos definir una red computacional, como la agrupación de computadoras interconectadas entre sí con la finalidad principal de crear un grupo de trabajo en donde se comparta información.

Las primeras redes construidas permitieron la comunicación entre una computadora central y terminales remotas. Se utilizaron líneas telefónicas, ya que estas permitían un traslado rápido y económico de los datos. Se utilizaron procedimientos y protocolos ya existentes para establecer la comunicación y se incorporaron moduladores y demoduladores para que, una vez establecido el canal físico, fuera posible transformar las señales digitales en analógicas adecuadas para la transmisión por medio de un módem.

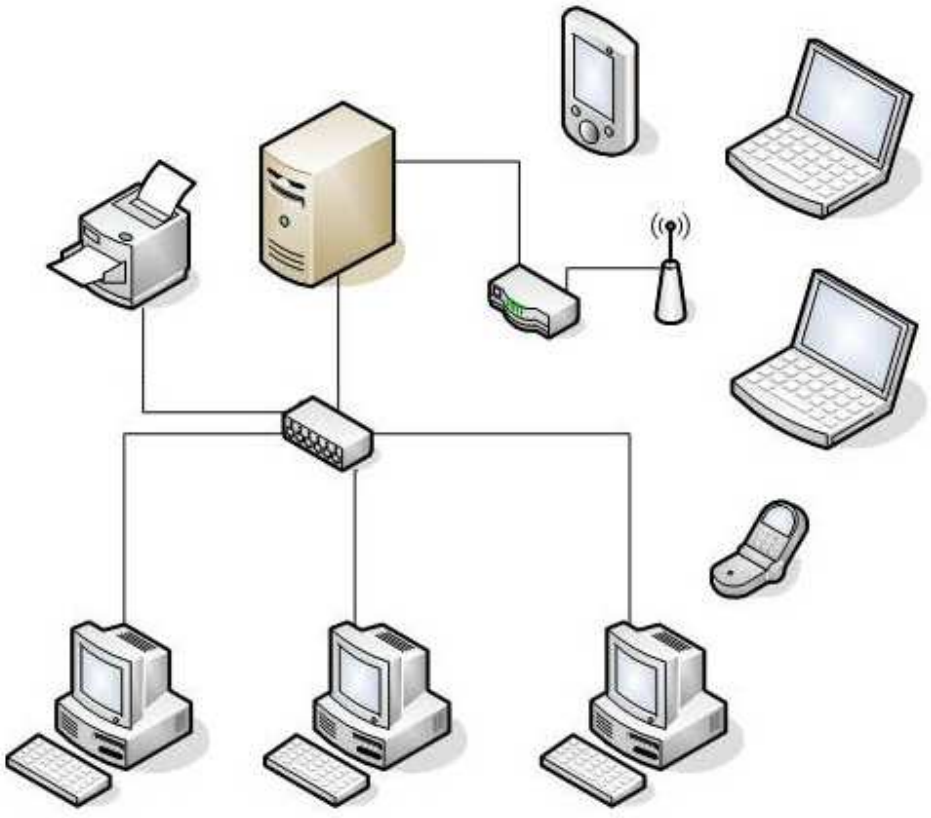

Figura 2-1. Ejemplo de red de computadoras.

2.2 Seguridad en Redes Computacionales

2.2.1 Introducción

La aparición de las redes computacionales, trajo consigo una amplia gama de posibilidades para la comunicación, transmisión e intercambio de información pero estas ventajas implicaron nuevas complicaciones.

En la actualidad, las pérdidas de información crítica para las empresas y corporativos se ven reflejadas en grandes pérdidas de dinero, hasta un simple usuario particular puede verse afectado con la pérdida de información personal o algún tipo de daño a su equipo computacional, es por esto que continuamente nuevas herramientas son

desarrolladas y lanzadas al mercado para brindar soluciones de seguridad que garanticen a los usuarios que su información no sea corrompida por personas no autorizadas.

Las características de las herramientas o procedimientos a utilizar son determinados por las necesidades de seguridad de los usuarios implicados.

2.2.2 Herramientas de Seguridad

Actualmente, existen en el mercado diferentes herramientas y/o procedimientos orientados a ofrecer medidas de seguridad a las empresas, lo cierto es que ninguna de estas podrá proporcionar la seguridad total a una organización. Es necesario tener muchos productos y tipos de productos diferentes para proteger completamente los activos de información de una organización [1].

Entre los tipos más comunes de tecnologías de seguridad, podemos destacar los Softwares Antivirus, Controles de Acceso, Muros de Fuego (mejor conocidos como Firewalls o Cortafuegos), Sistemas de Detección de Intrusiones, entre otros [1].
Estas herramientas ofrecen un nivel de seguridad aceptable acorde a su nivel de complejidad pero como se señaló al principio ninguna podrá proporcionar seguridad total.

2.2.3 Ataques

Cualquier equipo conectado a una red informática puede ser vulnerable a un ataque. Un "ataque" consiste en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, programa de software o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causan un daño [10].

Una gran cantidad de ataques se producen desde Internet, a razón de varios ataques por minuto en cada equipo conectado. En su mayoría, se lanzan automáticamente desde equipos infectados (a través de virus, troyanos, gusanos, etc.) sin que el

propietario sepa lo que está ocurriendo. En casos atípicos, son ejecutados por piratas informáticos [10].

Para bloquear estos ataques, es importante estar familiarizado con los principales tipos y tomar medidas preventivas [10].

Los ataques pueden ejecutarse por diversos motivos:

- Para obtener acceso al sistema;
- Para robar información, como secretos industriales o propiedad intelectual;
- Para recopilar información personal acerca de un usuario;
- Para obtener información de cuentas bancarias;
- Para obtener información acerca de una organización (la compañía del usuario, etc.);
- Para afectar el funcionamiento normal de un servicio;
- Para utilizar el sistema de un usuario como un "rebote" para un ataque;
- Para usar los recursos del sistema del usuario, en particular cuando la red en la que está ubicado tiene un ancho de banda considerable [10].

2.2.4 Tipos de Ataques

Los riesgos se pueden clasificar de la siguiente manera:

- **Acceso físico**: El atacante tiene acceso a las instalaciones e incluso a los equipos:
    - Interrupción del suministro eléctrico.
    - Apagado manual del equipo.
    - Vandalismo.
    - Apertura de la carcasa del equipo y robo del disco duro.
    - Monitoreo del tráfico de red.

- **Intercepción de comunicaciones**:
  - Secuestro de sesión.
  - Falsificación de identidad.
  - Redireccionamiento o alteración de mensajes.
- **Denegaciones de servicio**: El objetivo de estos ataques reside en interrumpir el funcionamiento normal de un servicio. Por lo general, las denegaciones de servicio se dividen de la siguiente manera:
  - Explotación de las debilidades del protocolo TCP/IP *(*Transmission Control Protocol/Internet Protocol*).*
  - Explotación de las vulnerabilidades del software del servidor.
- **Intrusiones**:
  - Análisis de puertos.
  - Elevación de privilegios: Este tipo de ataque consiste en aprovechar una vulnerabilidad en una aplicación al enviar una solicitud específica (no planeada por su diseñador). En ciertos casos, esto genera comportamientos atípicos que permiten acceder al sistema con derechos de aplicación. Los ataques de **desbordamiento de la memoria intermedia (búfer)** usan este principio.
  - Ataques malintencionados (virus, gusanos, troyanos).
- **Ingeniería social**: En la mayoría de los casos, el eslabón más débil es el mismo usuario. Muchas veces es él quien, por ignorancia o a causa de un engaño, genera una vulnerabilidad en el sistema al brindar información (la contraseña, por ejemplo) al pirata informático o al abrir un archivo adjunto. Cuando ello sucede, ningún dispositivo puede proteger al usuario contra la falsificación: sólo el sentido común, la razón y el conocimiento básico acerca de las prácticas utilizadas pueden ayudar a evitar este tipo de errores.
- **Puertas trampa**: Son puertas traseras ocultas en un programa de software que brindan acceso a su diseñador en todo momento [10].

Es por ello, que los errores de programación de los programas son corregidos con bastante rapidez por su diseñador apenas se publica la vulnerabilidad. En consecuencia, queda en manos de los administradores (o usuarios privados con un

buen conocimiento) mantenerse informados acerca de las actualizaciones de los programas que usan a fin de limitar los riesgos de ataques. Además, existen ciertos dispositivos (Firewalls, sistemas de detección de intrusiones, antivirus) que brindan la posibilidad de aumentar el nivel de seguridad [10].

2.3 Protocolo de comunicaciones

Los protocolos son reglas de comunicación que permiten el flujo de información entre computadoras distintas que manejan lenguajes distintos, por ejemplo, dos computadores conectados en la misma red pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas "hablen" el mismo idioma, por tal sentido, el protocolo TCP/IP fue creado para las comunicaciones en Internet, para que cualquier computador se conecte a Internet, es necesario que tenga instalado este protocolo de comunicación[9].

Pueden estar implementados bien en hardware (tarjetas de red), software (drivers), o una combinación de ambos.

2.3.1 Propiedades Típicas

- Detección de la conexión física sobre la que se realiza la conexión (cableada o sin cables).
- Pasos necesarios para comenzar a comunicarse (Handshaking).
- Negociación de las características de la conexión.
- Cómo se inicia y cómo termina un mensaje.
- Formato de los mensajes.
- Qué hacer con los mensajes erróneos o corruptos (corrección de errores)
- Cómo detectar la pérdida inesperada de la conexión, y qué hacer en ese caso.
- Terminación de la sesión de conexión.
- Estrategias para asegurar la seguridad (autenticación, cifrado) [9].

2.3.2 Estandarización

Los protocolos implantados en sistemas de comunicación con un amplio impacto, suelen convertirse en estándares, debido a que la comunicación e intercambio de información (datos) es un factor fundamental en numerosos sistemas, y para asegurar tal comunicación se vuelve necesario copiar el diseño y funcionamiento a partir del ejemplo pre-existente. Esto ocurre tanto de manera informal como deliberada [9].

Existen consorcios empresariales, que tienen como propósito precisamente el de proponer recomendaciones de estándares que se deben respetar para asegurar la interoperabilidad de los productos [9].

2.3.3 Niveles de abstracción

En el campo de las redes informáticas, los protocolos se pueden dividir en varias categorías, una de las clasificaciones más estudiadas es la OSI (Open System Interconnection) . Según la clasificación OSI, la comunicación de varios dispositivos ETD (Data Terminal Equipment) se puede estudiar dividiéndola en 7 niveles [9]. A su vez, esos 7 niveles se pueden subdividir en dos categorías, las capas superiores y las capas inferiores. Las 4 capas superiores trabajan con problemas particulares a las aplicaciones, y las 3 capas inferiores se encargan de los problemas pertinentes al transporte de los datos [9].

Los protocolos de cada capa tienen una interfaz bien definida. Una capa generalmente se comunica con la capa inmediata inferior, la inmediata superior, y la capa del mismo nivel en otros computadores de la red. Está división de los protocolos ofrece abstracción en la comunicación. Una aplicación (capa nivel 7) por ejemplo, solo necesita conocer como comunicarse con la capa 6 que le sigue, y con otra aplicación en otro computador (capa 7). No necesita conocer nada entre las capas de la 1 y la 5. Así, un navegador Web (HTTP (HyperText Transfer Protocol), capa 7) puede utilizar una conexión Ethernet o PPP(Point-to-Point Protocol) (capa 2) para acceder a la Internet, sin que sea necesario cualquier tratamiento para los

protocolos de este nivel más bajo. De la misma forma, un router sólo necesita de las informaciones del nivel de red para enrutar paquetes, sin que importe si los datos en tránsito pertenecen a una imagen para un navegador Web, un archivo transferido vía FTP(File transfer protocol) o un mensaje de correo electrónico [9].

2.3.4 Ejemplos de Protocolos de Red por Capa

- **Capa 1: Nivel físico**
  - Cable coaxial o UTP (Unshielded Twisted Pair) categoría 5, categoría 5e, categoría 6, categoría 6a Cable de fibra óptica, Cable de par trenzado, Microondas, Radio, RS-232 [9].

- **Capa 2: Nivel de enlace de datos**
  - Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface), ATM(Asynchronous Transfer Mode), HDLC(High-Level Data Link Control), CDP(Cisco Discovery Protocol) [9].

- **Capa 3: Nivel de red**
  - ARP(Address Resolution Protocol), RARP(Reverse Address Resolution Protocol), IP (IPv4, IPv6), X.25, ICMP(Internet Control Message Protocol), IGMP(Internet Group Management Protocol), NetBEUI(NetBIOS Extender Interface), IPX(Internetwork Packet Exchange), Appletalk [9].

- **Capa 4: Nivel de transporte**
  - TCP, UDP (User Datagram Protocol), SPX (Sequenced Packet Exchange) [9].

- **Capa 5: Nivel de sesión**
  - NetBIOS (Network Basic Input/Output System), RPC (Remote Procedure Call), SSL (Secure Sockets Layer) [9].

- **Capa 6: Nivel de presentación**
  - ASN.1 (Abstract Syntax Notation One) [9].

- **Capa 7: Nivel de aplicación**
  - SNMP(Simple Network Management Protocol), SMTP(Simple Mail Transfer Protocol), NNTP(Network News Transport Protocol), FTP(File transfer protocol), SSH(Secure Shell), HTTP, SMB(Server Message Block)/CIFS(Common Internet File System), NFS(Network File System), Telnet(TELecommunication NETwork), IRC(Internet Relay Chat), ICQ(I seek you), POP3(Post Office Protocol), IMAP(Internet Message Access Protocol) [9].

CAPÍTULO III
ANÁLISIS Y CONFIGURACIÓN

3.1 El Tipping Point x5 3crtpx5-u-96

Las plataformas de seguridad unificada de 3Com® ofrecen una protección sin precedentes frente a amenazas para las pequeñas empresas y organizaciones con varias sucursales o numerosos teletrabajadores ayudando a impedir las interrupciones del negocio, la pérdida de ingresos y los daños para la reputación de una organización causados por rupturas en la seguridad.

Estas plataformas de seguridad unificada, construidas en base a la galardonada arquitectura del sistema de prevención de intrusiones (IPS) TippingPoint" de 3Com, combinan las capacidades del IPS líder de la industria con soporte de red privada virtual (VPN), firewall de inspección de estado de paquetes, administración de ancho de banda de aplicación, routing IP multicast para audio/vídeo, y filtrado de contenidos Web.

Esta completa solución de seguridad protege la red frente a ataques y usos incorrectos, y ofrece una conectividad multi-emplazamientos basada en políticas para las aplicaciones en tiempo real críticas para la empresa, como por ejemplo de VoIP. Las funcionalidades de alta disponibilidad ayudan a garantizar un flujo de tráfico a velocidad de cable, incluso en caso de un error de la red o de un dispositivo interno, o de un fallo de alimentación en el dispositivo primario [6].

El objeto principal de estudio de este trabajo es el Tipping Point 3com x5 3crtpx5-u-96, este dispositivo perteneciente a la familia de dispositivos de seguridad Tipping Point reúne todas las características antes mencionadas y ofrece una solución inteligente a los requerimientos de seguridad y gestión para pequeñas y medianas empresas.

Figura 3-1. Vista del Tipping Point 3com x5 3crtpx5-u-96

3.2 Conexión y Configuración Inicial

Este apartado es suma importancia, en este punto se tiene la oportunidad de familiarizarse con el dispositivo para que posteriormente sea llevada a cabo la conexión del mismo.

El primer paso que se lleva a cabo en la inicialización por primera vez del Tipping Point x5 consiste en la conexión del dispositivo a la fuente de alimentación y en el paquete de fábrica se incluye un adaptador de 5 volts para llevar a cabo está acción. La figura 3-2 muestra un diagrama de referencia de la vista posterior del dispositivo necesario para llevar a cabo las debidas conexiones.

Figura 3-2. Diagrama de entradas.

Una vez que se conecta el dispositivo a la red eléctrica con su debido adaptador, el led de estatus presenta un color naranja y parpadeante, esto es indicador de que el dispositivo se está inicializando, pasado unos cuantos minutos el tono del led se estabiliza en un color verde claro, esto es indicador de que el dispositivo está listo para usarse, a continuación se lleva a cabo la configuración de la conexión de red en la PC utilizada para la comunicación con el Tipping Point. Una vez en la PC se accede a Mis sitios de Red-Ver conexiones de red, tal y como se muestra en la figura 3-3.

Figura 3-3. Accediendo a la configuración de área local.

Se ingresa a las propiedades de Conexión de red de área local posicionándose sobre Protocolo Internet (TCP/IP) tal y como se muestra en la figura 3-4.

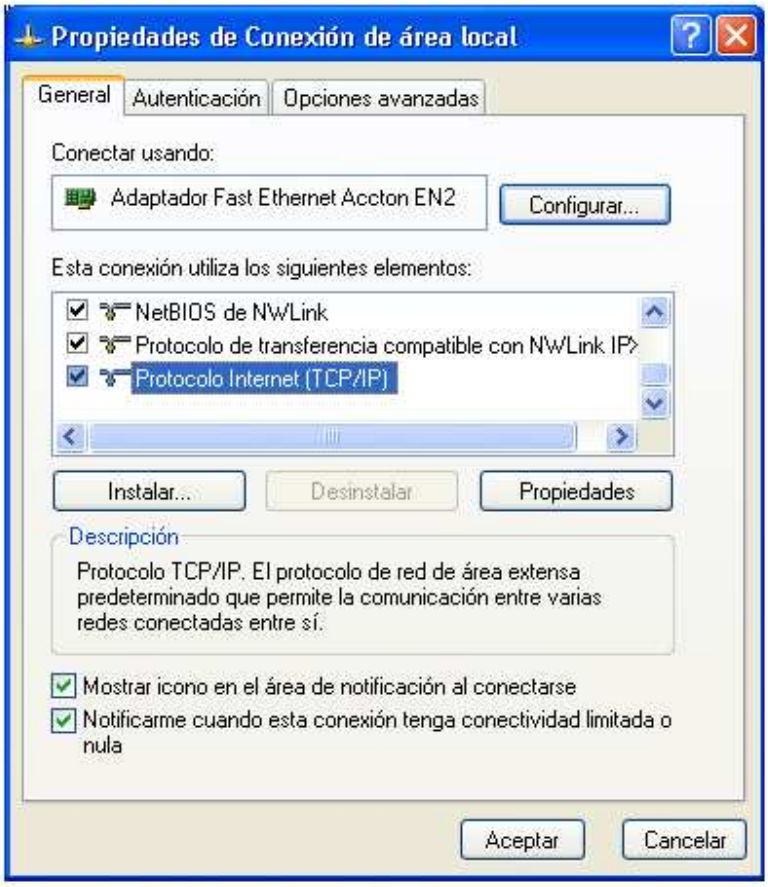

Figura 3-4. Configuración del Protocolo de Internet (TCP/IP).

Una vez ahí se ingresa a las propiedades del Protocolo de Internet (TCP/IP), en la figura 3-5 se muestra de que manera se lleva a cabo la configuración para que la conexión de red reciba automáticamente una dirección IP por medio de DHCP (Dynamic Host Configuration Protocol).

Figura 3-5. Configuración para recibir una dirección IP por medio de DHCP.

3.3 Conexión del Tipping Point x5 a la red local

Una vez que se llevan a cabo estos pasos se procede a la conexión del Tipping Point con la PC, utilizando un cable ethernet se conecta el puerto LAN(Local Area Network) del Tipping Point con el puerto de la tarjeta de red de la PC, automáticamente se recibe la dirección IP por default 192.168.1.17 con la que el dispositivo es capaz de reconocer a la PC, después se accede a la interfaz de configuración en nuestro navegador de Internet por medio de la dirección por default https://192.168.1.254. Automáticamente aparece un asistente de configuración, tal y como recomienda el fabricante en una instalación por primera vez se acepta el nivel

de seguridad 2 por default y además se crea una cuenta de Súper usuario en donde se especifica un nombre de usuario y nuestra contraseña. Se aceptan los ajustes por default que se presentan a través del asistente de configuración sin hacer ningún tipo de ajuste personal cuando el asistente lo solicita, es importante señalar que todos estos ajustes mencionados se pueden reajustar más adelante, esta metodología aplica únicamente al momento de conectar el Tipping Point por primera vez. Una vez que se acepta la configuración por default se decide integrar el equipo a la red local para que los usuarios autorizados tengan acceso a la interfaz del Tipping Point desde cualquier PC, así pues se accede a la dirección https://192.168.1.254 proporcionando usuario y contraseña como se muestra en la figura 3-6.

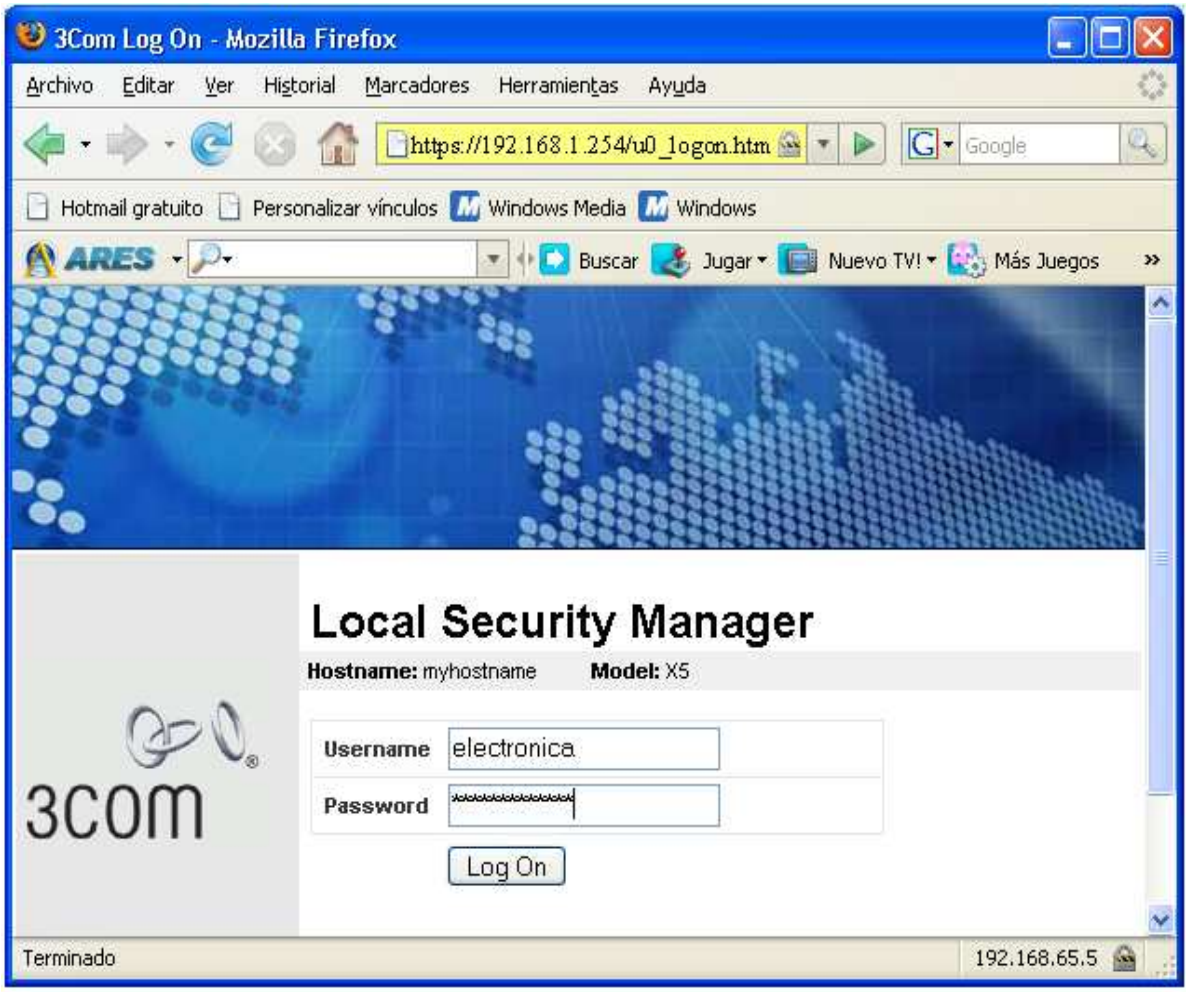

Figura 3-6. Accediendo a la interfaz de usuario por medio de la dirección IP de fabrica.

Dentro de la interfaz de configuración del Tipping Point, y por medio de la ruta Network-DHCP Server-Configure DHCP, se procede a desactivar el servidor DHCP, por default esta característica viene habilitada en el dispositivo y podría ocasionar conflictos con el servidor DHCP de la red local, por recomendación no se permite tener 2 servidores DHCP en una misma red, si se conectara el Tipping Point como servidor DHCP el antiguo servidor lo reconocería y automáticamente intentaría darse de baja, y tomando en cuenta que el Tipping Point hasta este punto no está debidamente configurado esto podría ocasionar conflictos en la red.

Se deshabilita está característica y se aplican los cambios como se muestra en la figura 3-7, una vez realizada está acción se procede a integrar el Tipping Point de forma segura a la red local.

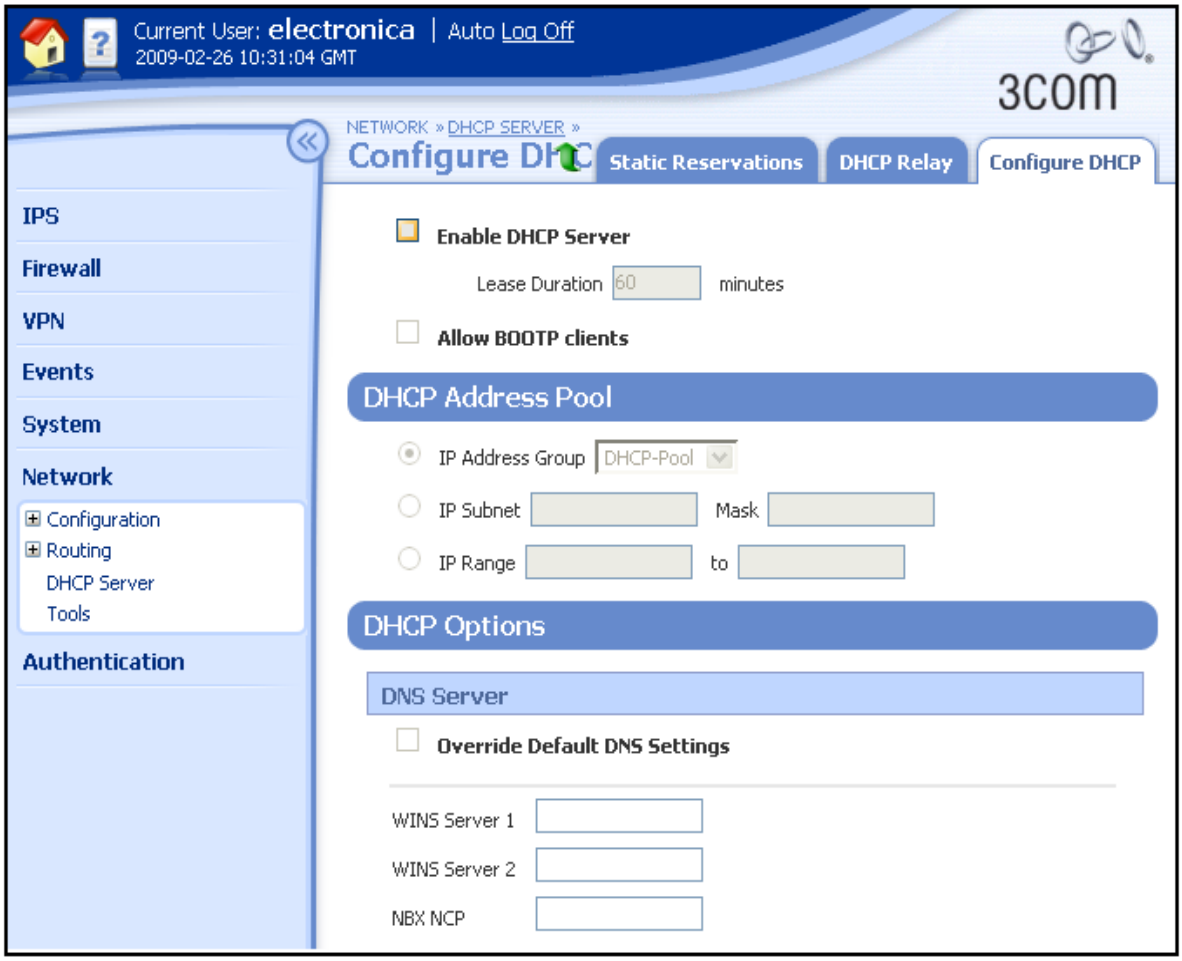

Figura 3-7. Dehabilitando el servidor DHCP del Tipping Point x5.

Como siguiente paso se asigna una nueva dirección IP al dispositivo, está dirección está dentro del rango de direcciones de la empresa para que el dispositivo sea reconocido en la red local. Se accede en el menú izquierdo a Network-Configuration-IP Interfaces y se elige la interfaz interna para acceder a ella y editarla tal como se muestra en la figura 3-8.

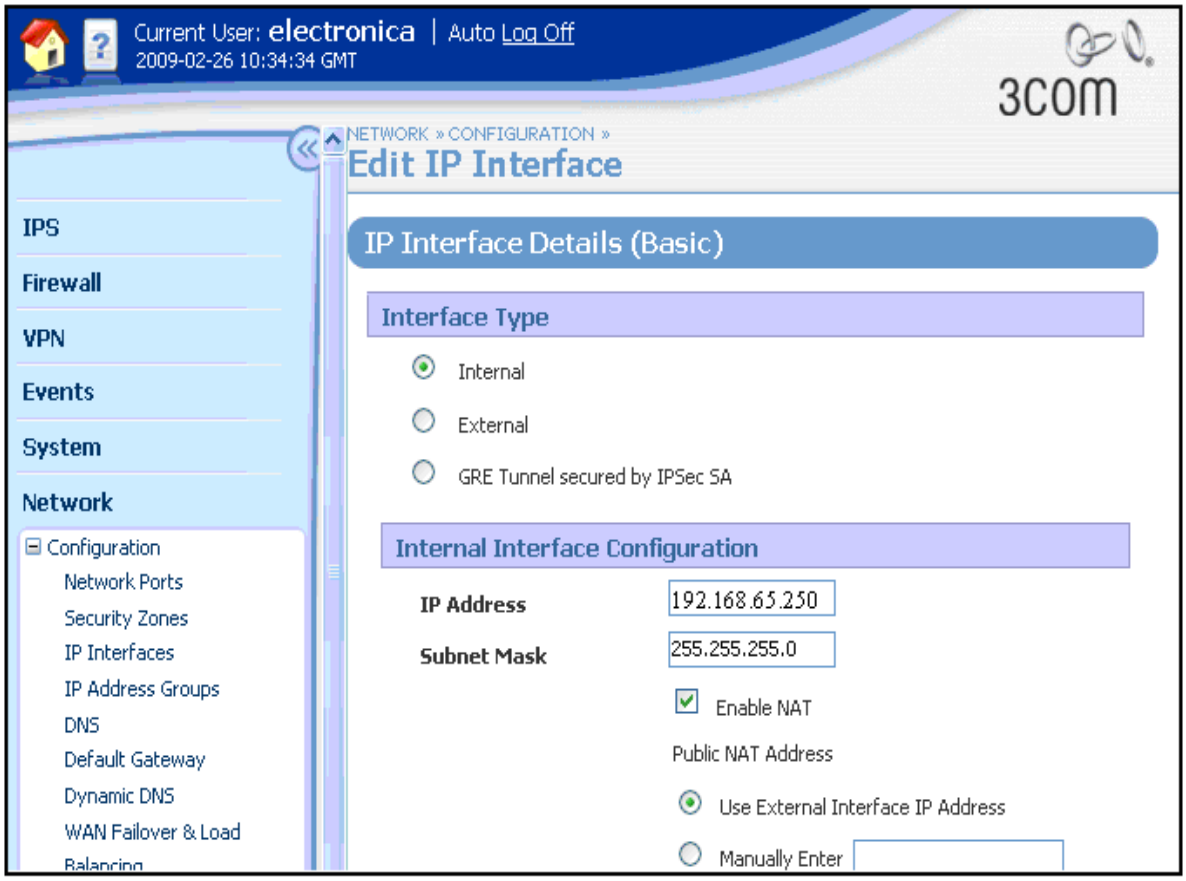

Figura 3-8. Configurando la Interfaz Interna.

Automáticamente se elige el tipo de interfaz interna y se indica la nueva dirección IP del dispositivo con su respectiva máscara de subred tal y como se muestra en la figura anterior, la nueva dirección a la que se deberá acceder al dispositivo será la 192.168.65.250 con máscara de subred 255.255.255.0, está dirección está dentro del rango de direcciones de la red de la empresa y se encuentra libre.

Posteriormente el dispositivo es integrado a la red local, por medio de un cable ethernet se conecta el puerto LAN del Tipping Point a un nodo disponible en la red y se continúa con su configuración.

3.4 Creación de Servidores Virtuales

Antes de realizar la conexión a Internet es necesario dar de alta como servidores virtuales a los puertos IP necesarios para activar los servicios de: POP3, HTTP, HTTPS (Hypertext Transfer Protocol Secure), SMTP, MS-WBT-Server-TCP y MS-WBT-Server-UDP; estos servidores permitirán que los equipos autorizados que se conecten vía externa a la red local tengan acceso a los servicios ya mencionados.
Para dar de alta los servidores virtuales se ingresa a la interfaz de configuración y se sigue la ruta Firewall-Virtual Servers-Create Virtual Server.

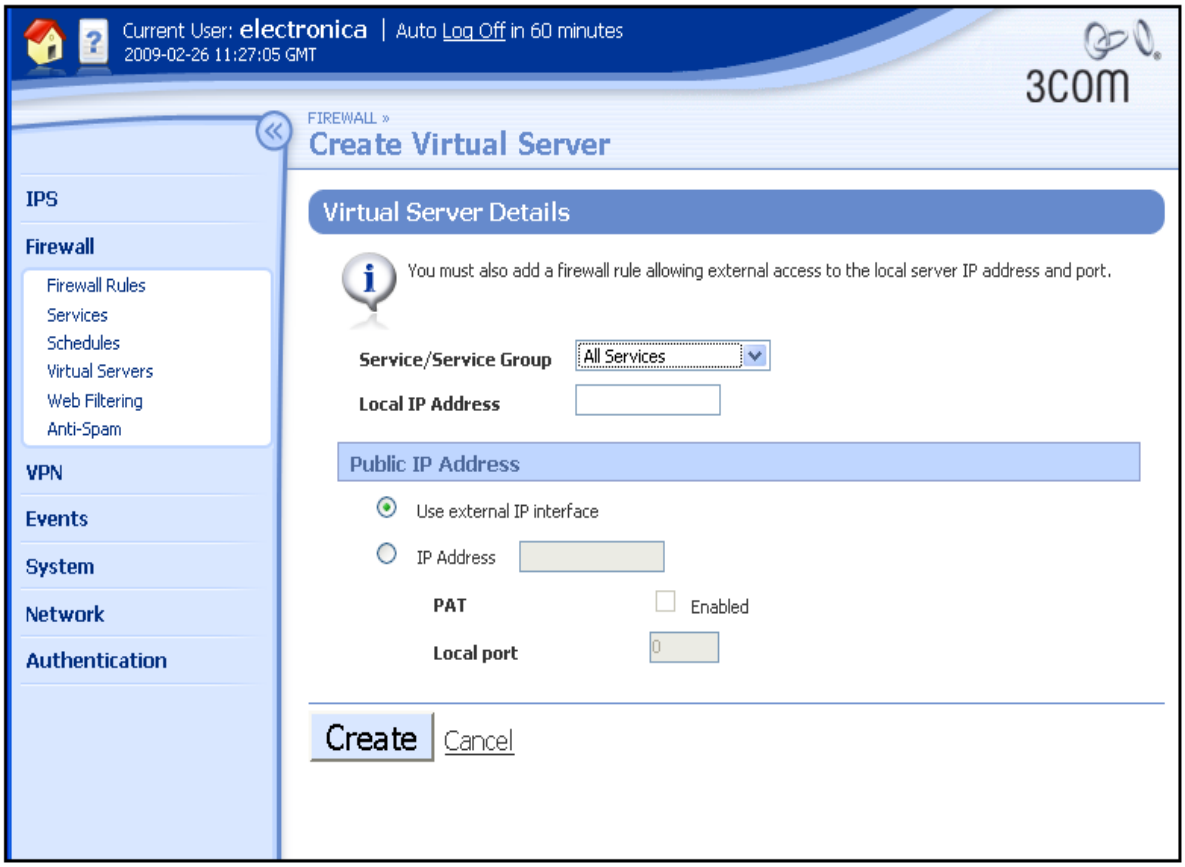

Figura 3-9. Creando Servidores Virtuales.

En la figura 3-9 se muestra de que manera se elige el servicio que se desea aplicar, en dirección IP local se ingresa la dirección del servidor de la empresa 192.168.65.10 y se elige usar una interfaz IP externa como dirección publica IP, puesto que las peticiones a los servidores virtuales llegarán hacia el servidor local desde equipos externos. Se sigue el mismo procedimiento para cada uno de los servidores virtuales que se desean dar de alta, los servicios MS-WBT-Server-TCP y MS-WBT-Server-UDP no vienen dentro de la lista de servicios que trae el dispositivo por default, es necesario darlos de alta de manera manual.

Se sigue la ruta Firewall-Services-Add Service, se declara el nombre del servicio, el protocolo utilizado y el puerto IP al que corresponde, se crea y con esto ya es posible dar de alta el servidor virtual puesto que ya se encontrara dentro de las opciones a elegir, en la figura 3-10 se muestra la configuración realizada para dar de alta los servicios MS-WBT-Server-TCP y MS-WBT-Server-UDP.

Figura 3-10. Añadiendo un nuevo servicio al Cortafuegos.

La figura 3-11 muestra todos los servidores virtuales que fueron creados.

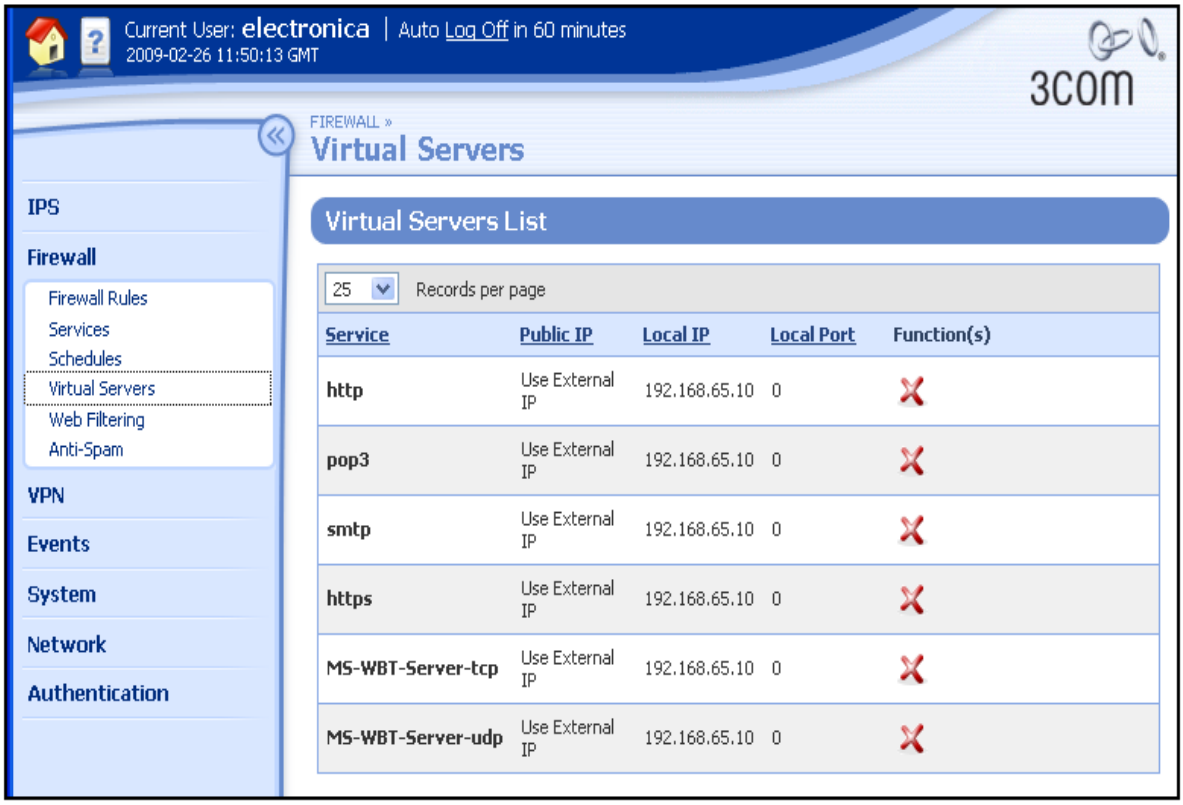

Figura 3-11. Lista de Servidores Virtuales creados.

3.5 Creación de las reglas del Cortafuegos, habilitación del Filtrado Web y Servicio Anti-Spam.

La creación de servidores virtuales se lleva a cabo con la finalidad de permitir que equipos externos autorizados tengan la capacidad de ingresar a la red local y hacer uso de servicios contenidos dentro del servidor de la empresa, por lo tanto; es necesaria la creación de reglas de cortafuegos para cada uno de los servicios declarados y así evitar posibles ataques o infecciones provenientes desde WAN (Wide Area Network). Para llevar esto a cabo se sigue la ruta Firewall-Firewall Rules-Create Firewall Rule, por ejemplo para el servicio de navegación Internet seguro HTTPS, la acción deseada será: permitir el servicio (puede ser bloqueado de ser necesario), se elige el servicio HTTPS de la lista de opciones y las demás opciones se dejan sin modificación alguna por el momento como se observa en la figura 3-12.

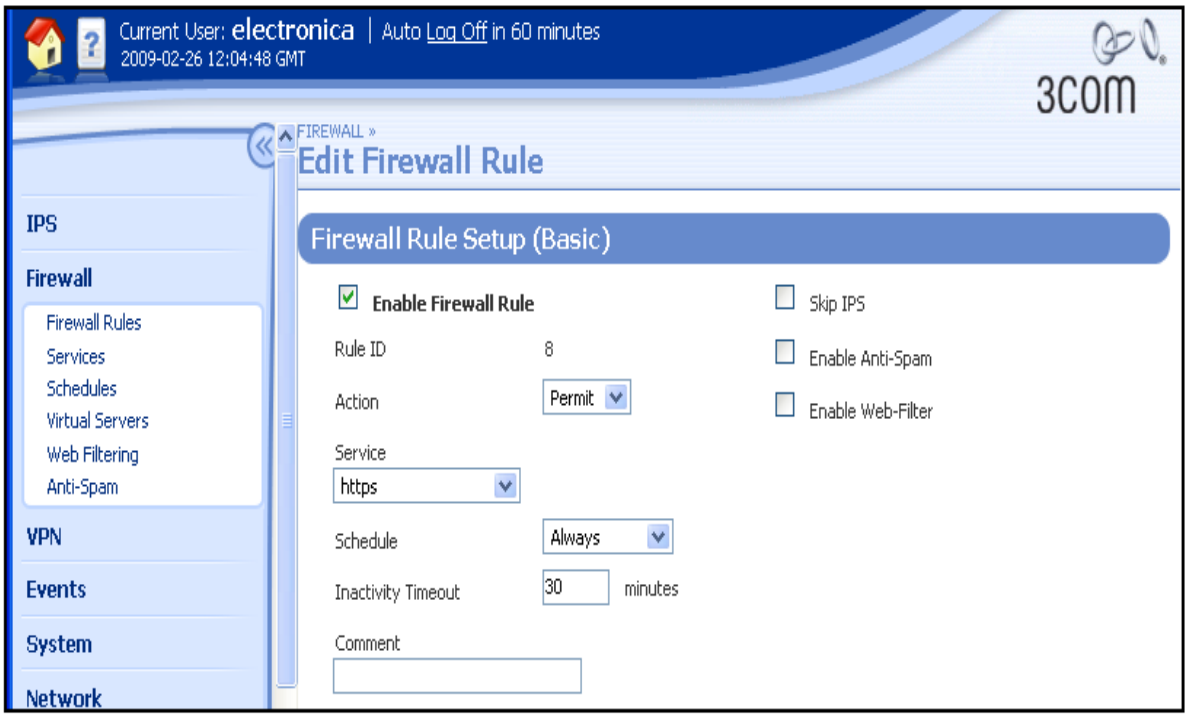

Figura 3-12. Creando y editando una Regla de Cortafuegos.

En esa misma pantalla hacia abajo continuando con la configuración.

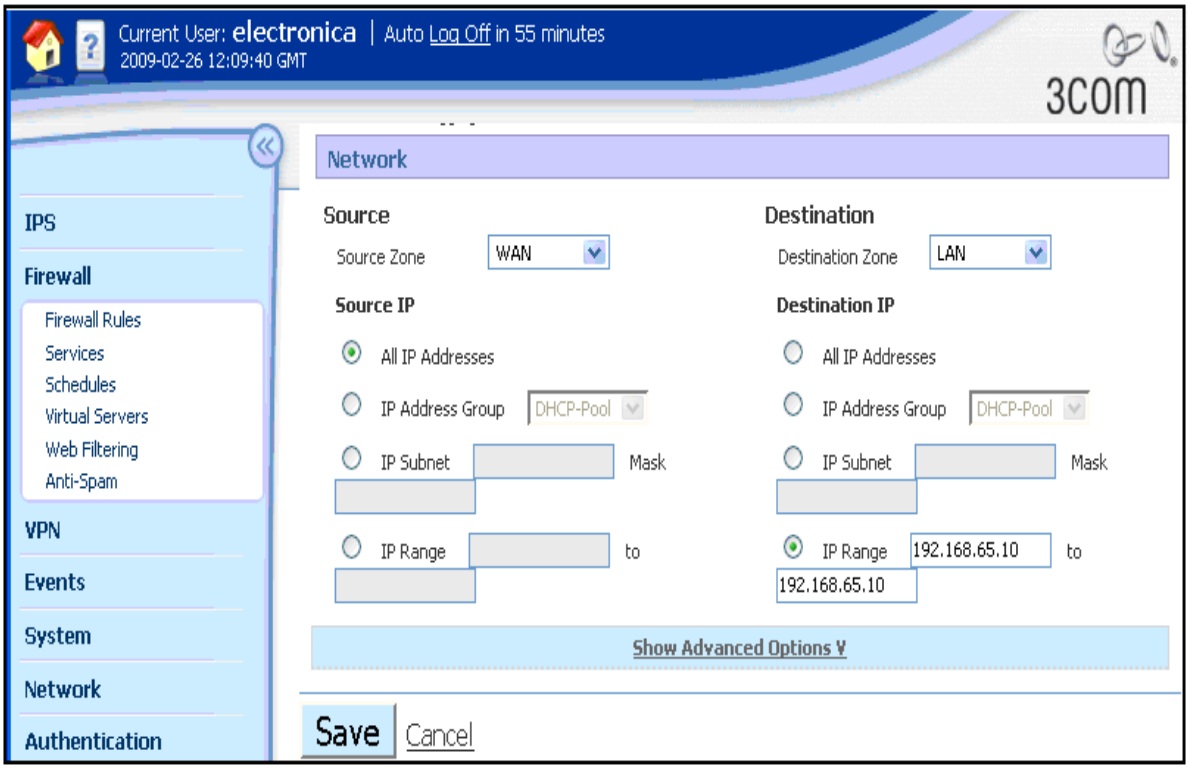

Figura 3-13. Creando y editando una Regla de Cortafuegos.

En la figura 3-13 se declara cual es la fuente de petición del servicio, como se señala que se conectarán equipos externos desde Internet, por lo tanto la fuente será WAN, se tiene la capacidad de indicar un rango de direcciones IP a las que se aplicará esta regla, un grupo e incluso una sola dirección, para este caso particular se indica que sean todas las direcciones IP. Después se define al destino, como las peticiones de servicio van a la red local el destino es LAN, igualmente se tiene la capacidad de elegir las direcciones IP del destino, en este caso particular las peticiones van directamente al servidor local de la empresa y por lo tanto el destino especifico es la dirección del servidor 192.168.65.10, por último se salvan los cambios.

Ya se ha creado nuestra regla de seguridad para el servicio HTTPS y de la misma manera se crean las demás reglas correspondientes a cada uno de los servicios declarados, algunas reglas tendrán además opciones avanzadas de configuración y

características adicionales, algunas de esas características adicionales son el Filtrado Web, Anti-Spam, entre otras.

Para poder aplicar el Filtrado Web es necesario crear antes un archivo de filtrado en el que se contengan todas las características de dicho filtro, se sigue la ruta Firewall-Web filtering y se tiene una ventana como en la figura 3-14.

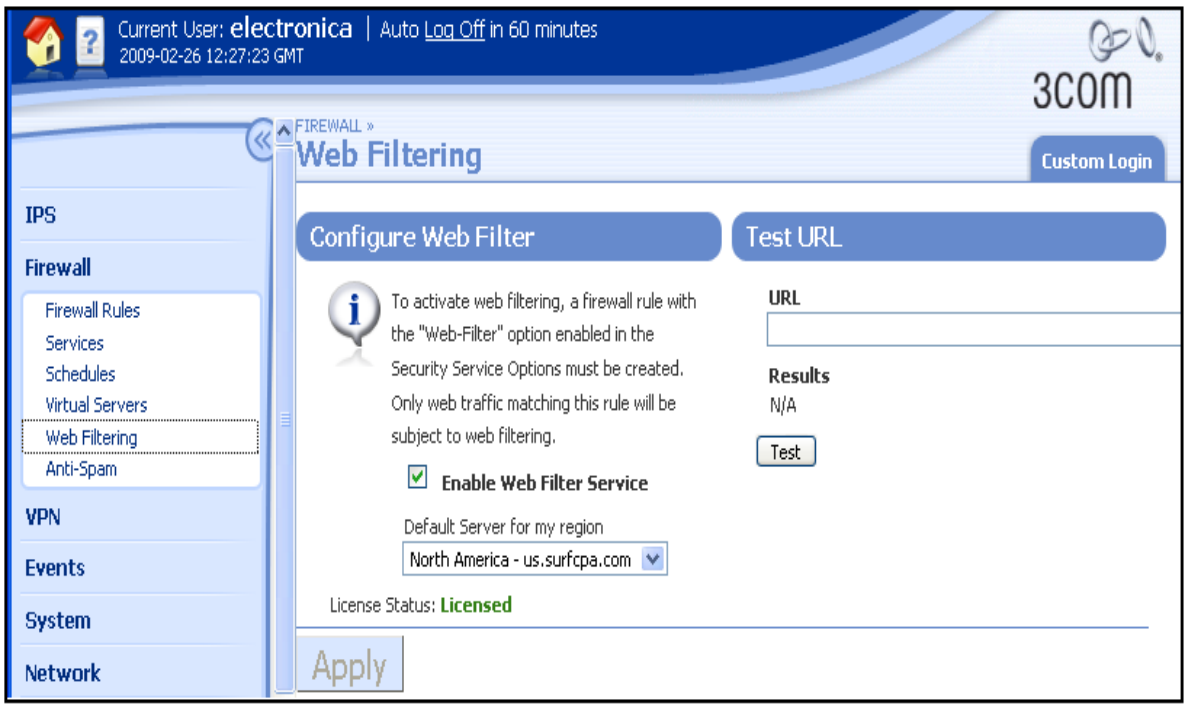

Figura 3-14. Activando el Filtrado de contenido Web.

En la ventana mostrada en la imagen anterior se activa “Activar el Servicio de Filtro Web”, además se elige un servidor de región por default tal y como se muestra, se aplican cambios, esto por sí solo no activa el Filtro Web, además es necesario editar al archivo de Filtro Web.

En esa misma ventana hacia abajo, en la sección de Lista de archivos de Filtro Web.

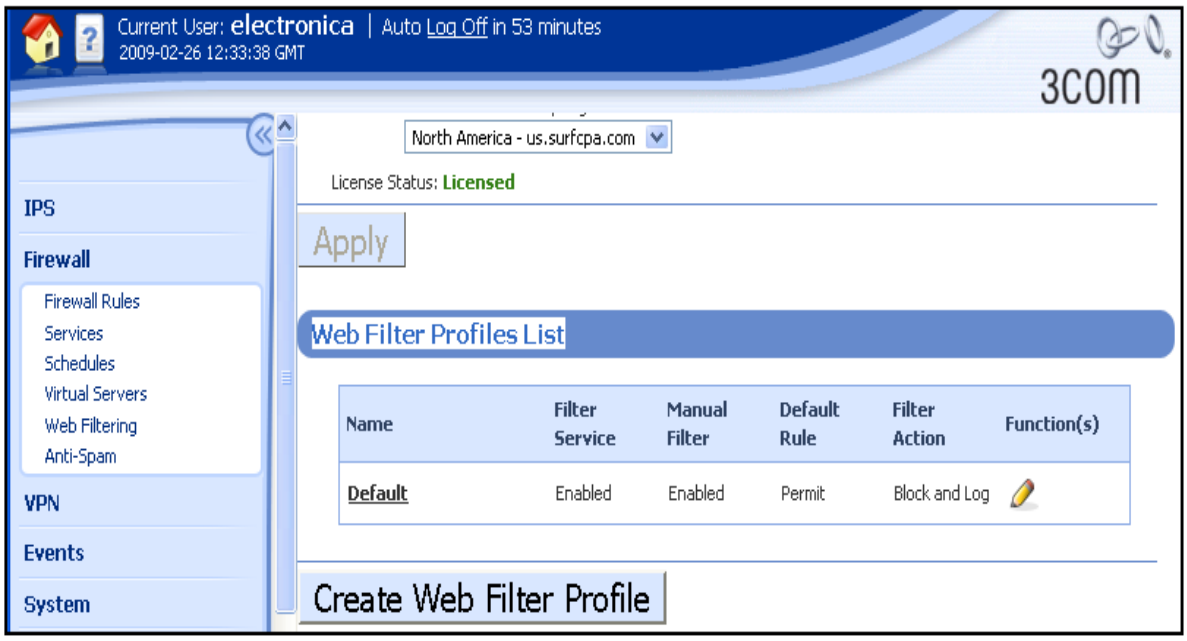

Figura 3-15. Editando el Filtrado de contenido Web.

En la figura 3-15 es posible ver que ya existe un archivo por default, se tiene la capacidad de crear tantos archivos como creamos necesarios, para este caso en particular solo se limitará a editar y configurar el archivo mostrado en la imagen anterior, para llevar esto acabo se accede a su edición por medio de un clic sobre la figura del lápiz que aparece justo a la derecha y se tiene una ventana como en la figura 3-16.

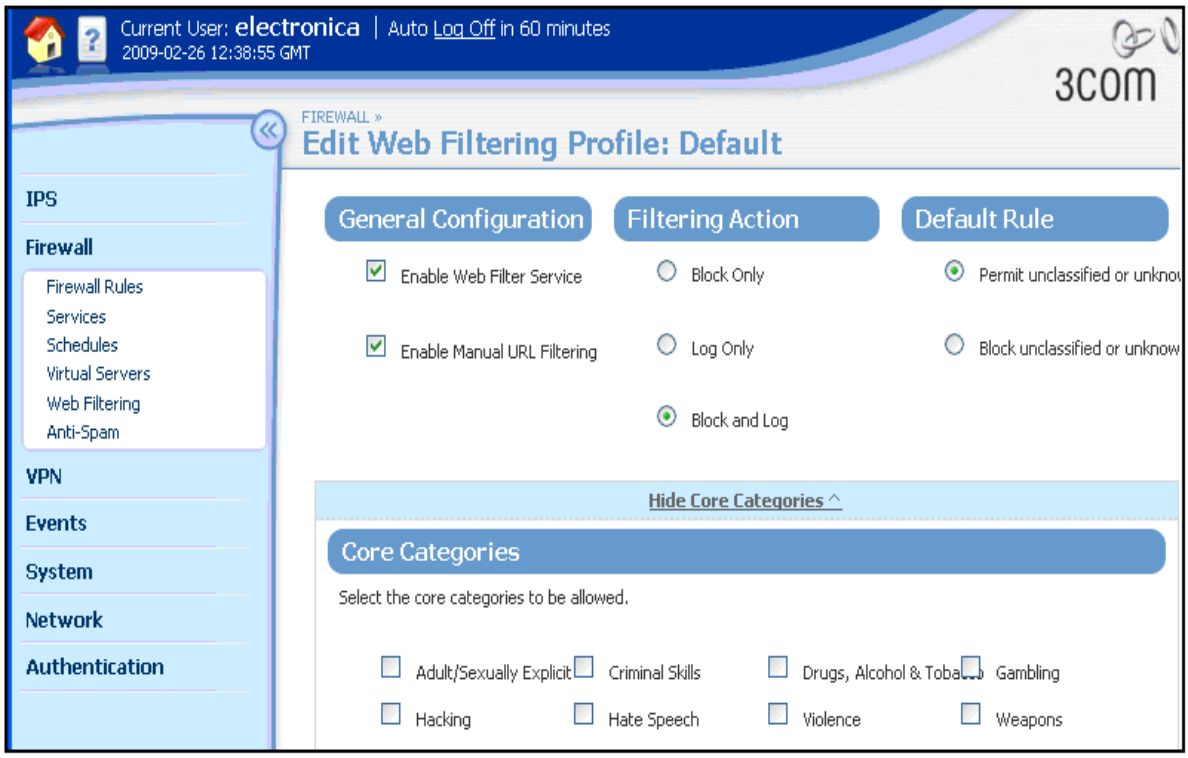

Figura 3-16. Editando el Filtrado de contenido Web.

En está ventana se habilita de nuevo el servicio de Filtro Web, el filtrado manual de URL(permite ingresar una dirección Web y conocer que clasificación le otorga el Tipping Point en cuanto a los sitios permitidos y no permitidos), las demás opciones se dejan si modificación alguna.

En esa misma ventana hacia abajo se encuentran algunos menús desplegables como se muestra en la figura 3-17.

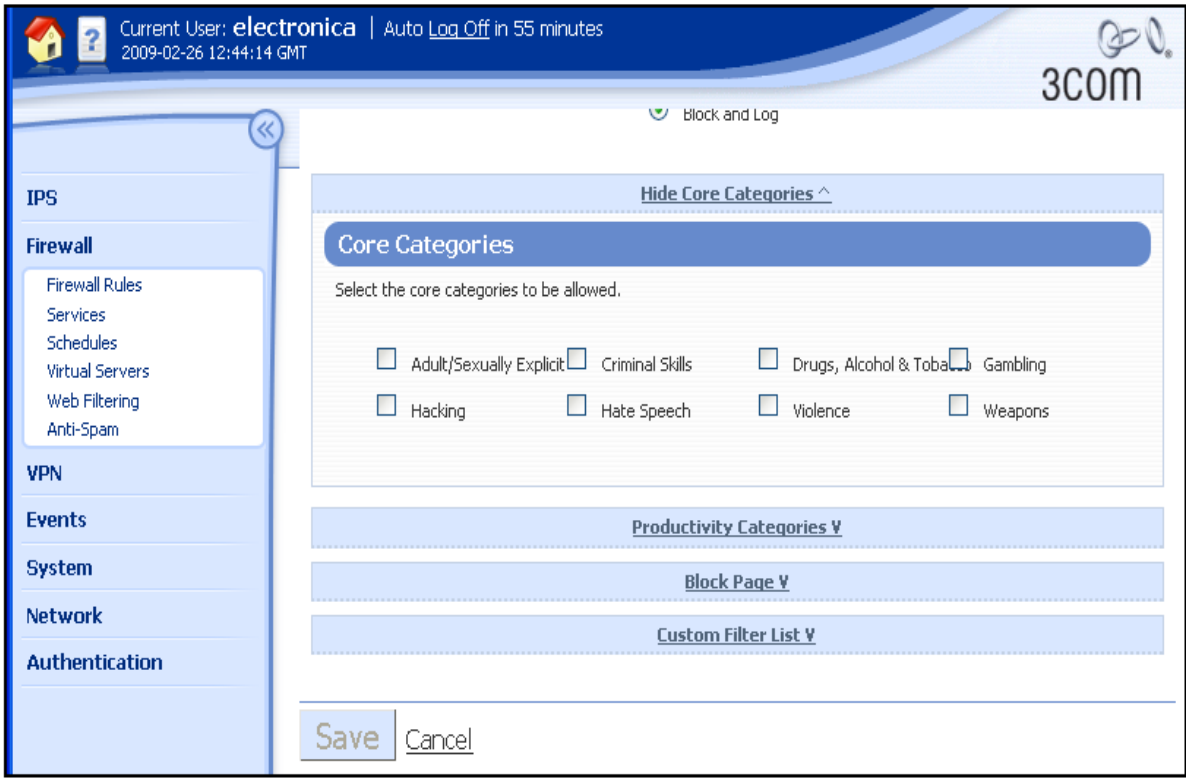

Figura 3-17. Editando el Filtrado de contenido Web.

Si se despliega cada uno los menús mostrados se podrá tener acceso a diferentes opciones y categorías de contenido Web que pueden ser bloqueadas o permitidas según sea el caso, en ese momento se limitará a permitir todas las categorías contenidas dentro del menú Categorías de Productividad y se deshabilitan las contenidas dentro de Categorías Core, además es posible denegar acceso desde una sola página Web en particular hasta una lista creada por el usuario, así como la capacidad de editar el mensaje mostrado al momento de bloquear la Web, solo resta salvar los cambios.

A través de la ruta Firewall-Anti-Spam se activa el servicio de Anti-Spam y se verá frente a una ventana como se observa en la figura 3-18.

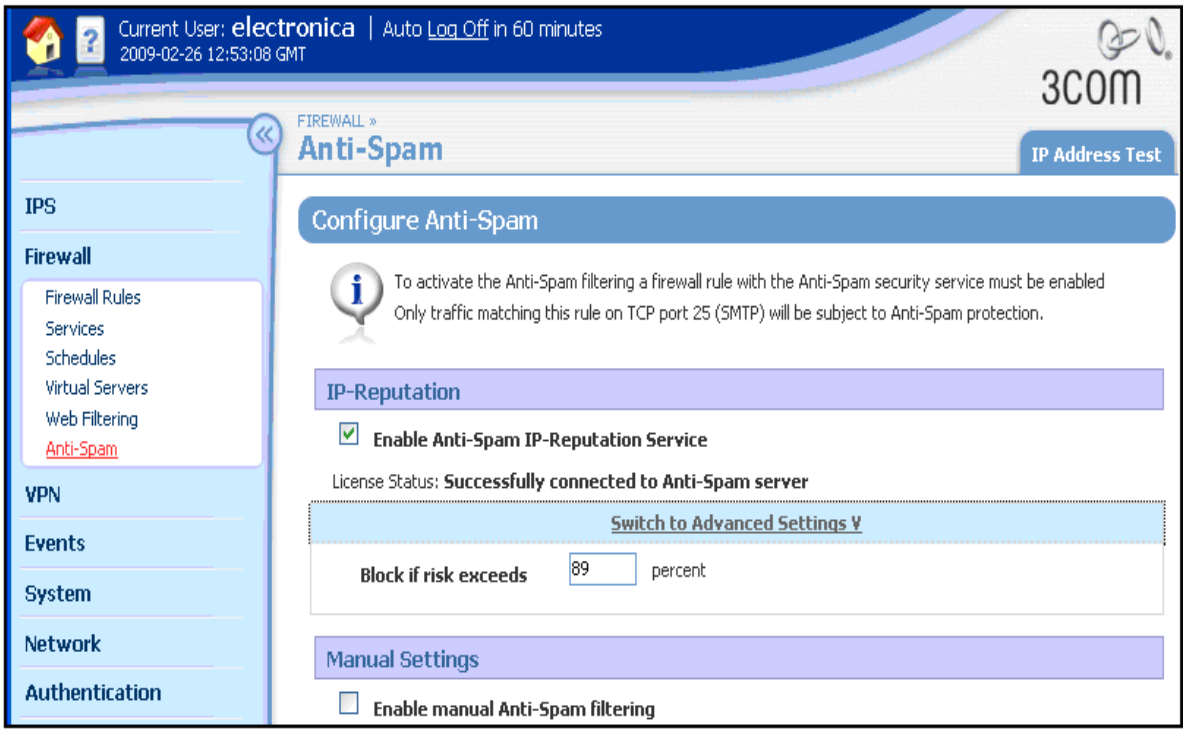

Figura 3-18. Activando el Servicio Anti-Spam.

Aquí no se realizan muchos cambios, solo se habilita el servicio de Anti-Spam, se dejan las demás opciones por default y se salvan los cambios.

Una vez configurados debidamente los servicios de Filtrado Web y de Anti-Spam, se podrá añadir estás características si así se desea dentro de las reglas de seguridad que se quieran crear, al momento de editar dicha regla, del lado derecho se mostrarán las opciones de habilitación de Filtrado Web (también se mostrará una lista de archivos de filtrado disponibles) y de Anti-Spam como se aprecia en la figura 3-19.

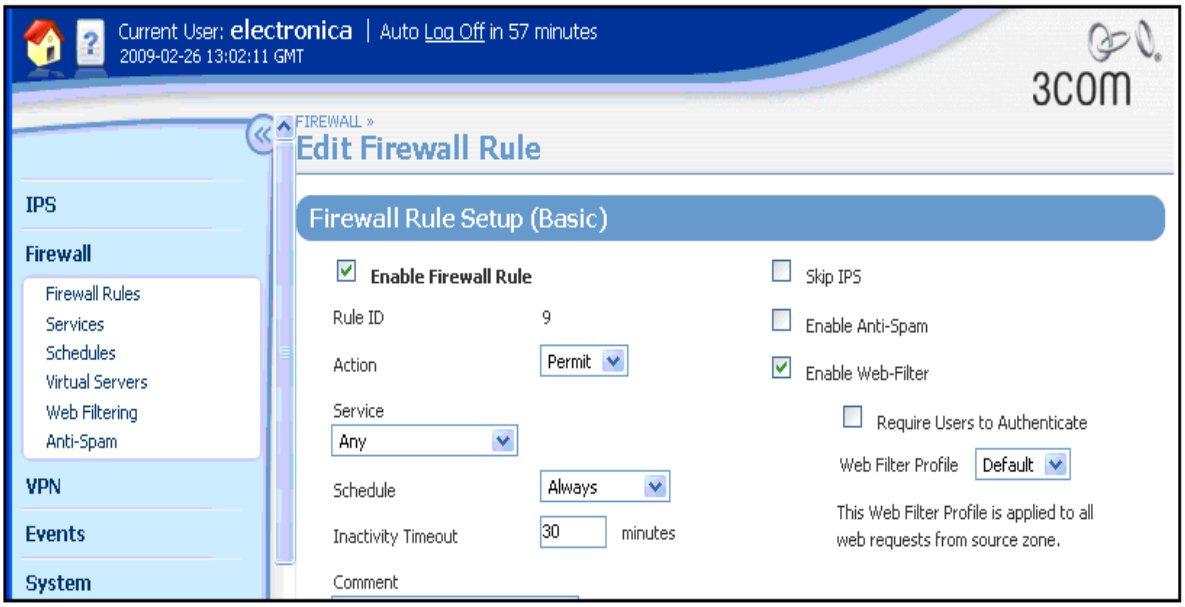

Figura 3-19. Añadiendo el Servicio de Filtrado Web a una regla de cortafuegos especifica.

Del lado derecho puede ver que ahora se es posible habilitar las opciones ya mencionadas.

Además de la creación de las reglas para cada uno de los servidores virtuales creados y de las reglas por default contenidas dentro del Tipping Point, se crea una regla especial que permite todo tipo de servicios desde la red local LAN con fuente específica en la dirección 192.168.65.111, esto se puede observar en la figura 3-20.

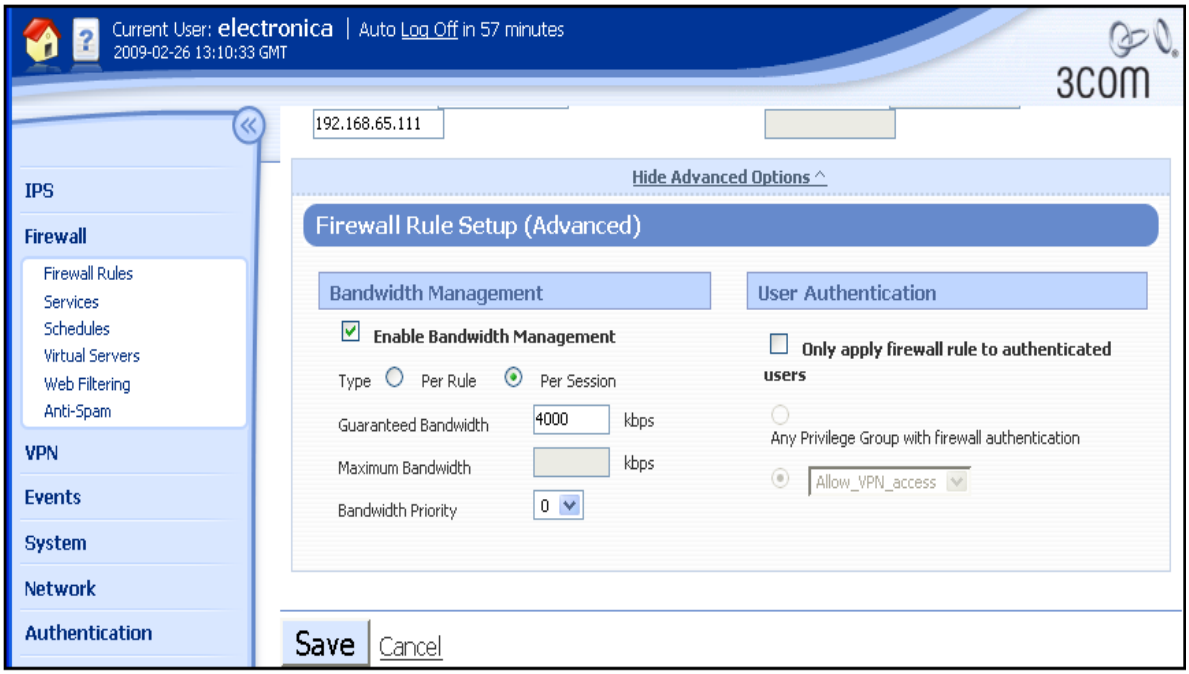

Figura 3-20. Creación de una regla especial con Gestión de Ancho de Banda.

El procedimiento es el mismo que se utiliza en la creación de las reglas anteriores a diferencia que en la parte inferior de la pantalla se despliega el menú de Configuración de regla de cortafuegos avanzada, se habilita la gestión del ancho de banda por sesión además se asigna un ancho de banda garantizado de 4000 kbps, por último se salvan los cambios.

Las figuras 3-21 y 3-22 muestran todas aquellas reglas de cortafuegos que fueron creadas.

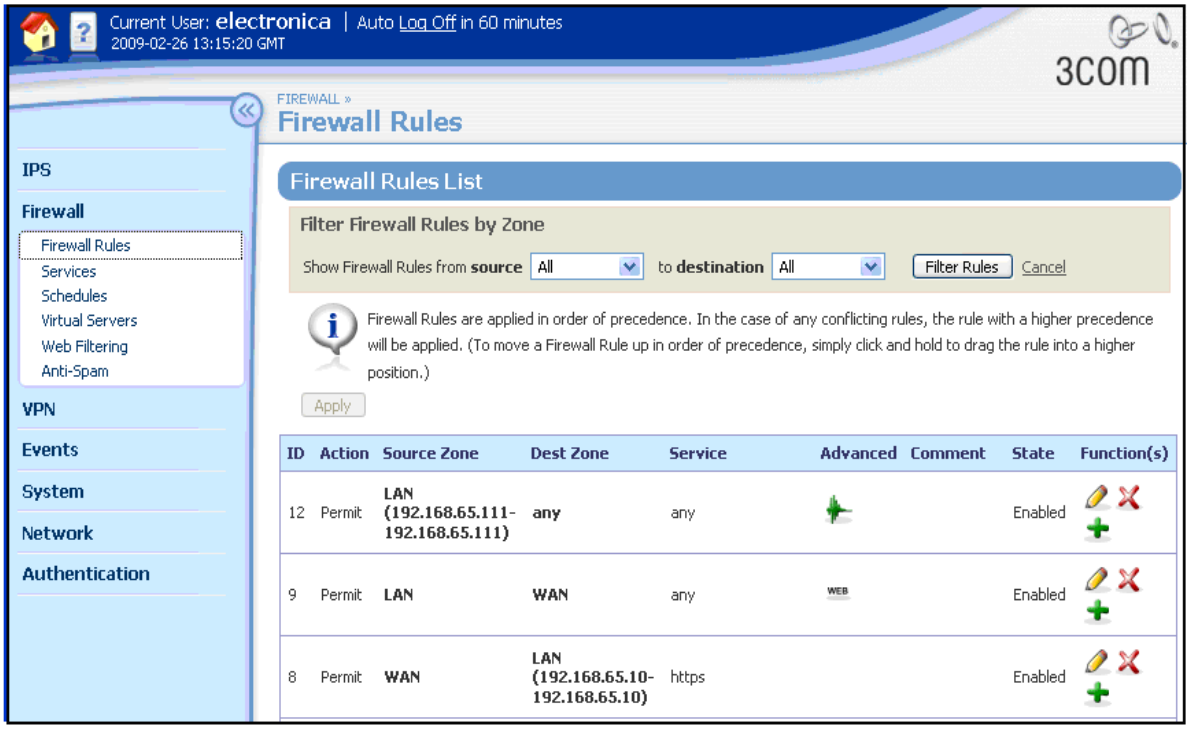

Figura 3-21. Lista de Reglas de Cortafuegos creadas.

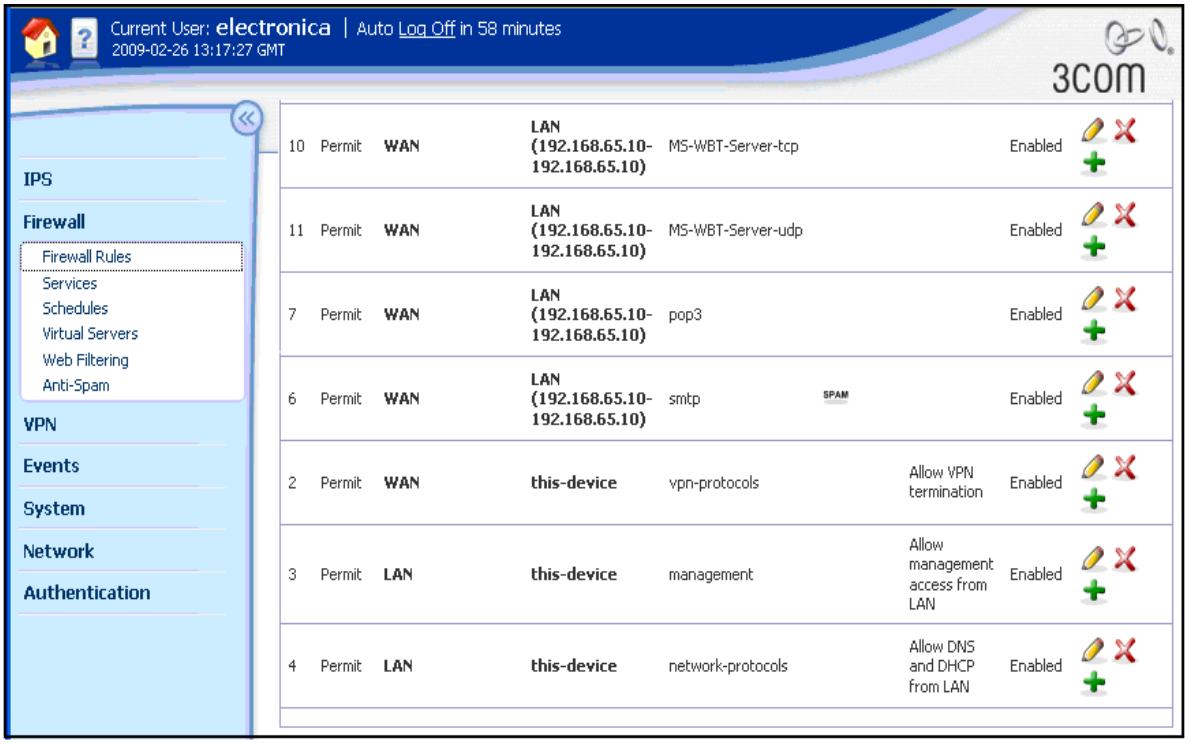

Figura 3-22. Lista de Reglas de Cortafuegos creadas.

Es importante señalar que el orden de las reglas si afecta, el dispositivo toma como prioridad la regla que se encuentra posicionada en la parte más alta de la lista, en caso de existir conflicto entre 2 reglas declaradas el dispositivo aplicara la que tenga una posición más alta. Para cambiar de lugar una regla basta con hacer clic sobre ella y arrastrar hacia la posición deseada.

3.6 Conexión del Tipping Point x5 a Internet

Ya que se han habilitado los servidores virtuales y se han establecido las reglas de cortafuegos necesarias, es momento de llevar a cabo la conexión del Tipping Point a Internet y así tener la oportunidad de aprovechar al máximo las prestaciones del dispositivo.

Antes de llevar a cabo está acción es necesario declarar que tipo de interfaz externa usara el Tipping Point a la hora de conectarse a Internet, para esto se sigue la ruta Network-Configuration-IP Interfaces-External y estará frente a una ventana como la que se observa en la figura 3-23.

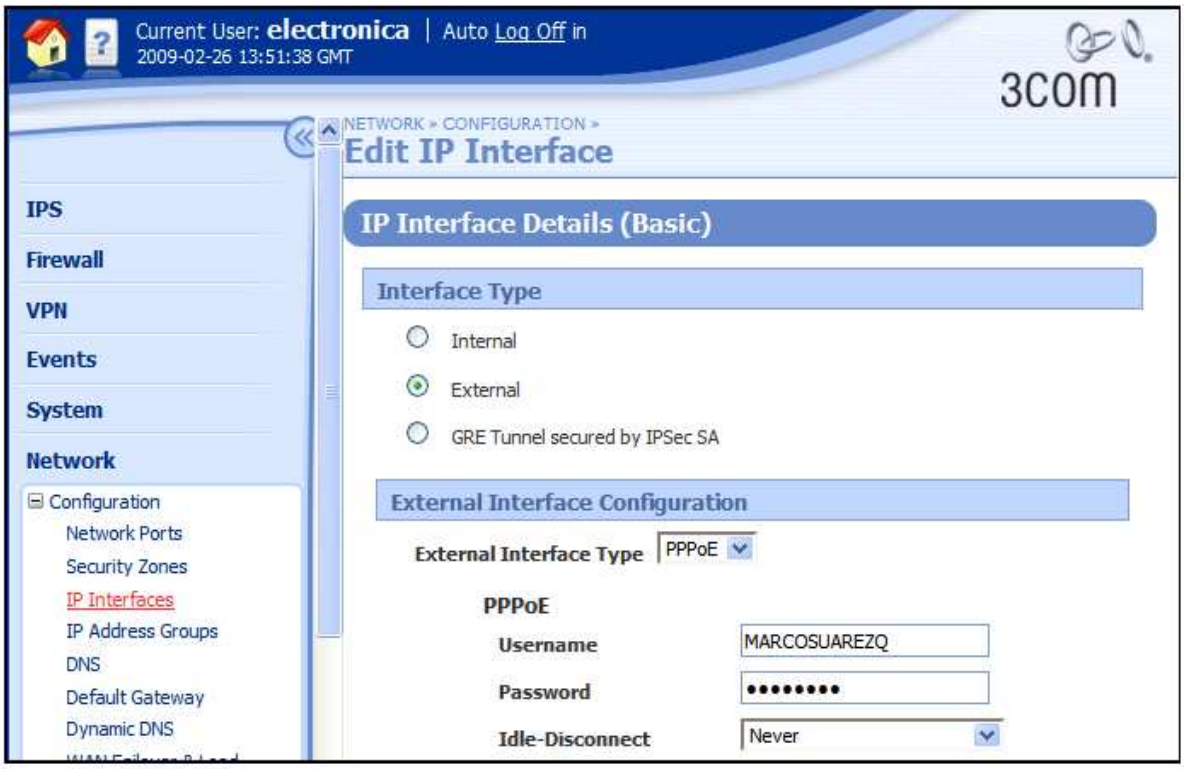

Figura 3-23. Configurando la Interfaz de usuario Externa.

Se elige la opción el tipo de interfaz externa PPPoE (Point-to-Point Protocol over Ethernet), se ingresa el nombre de usuario y contraseña correspondiente, las demás opciones se dejan tal y como están, se salvan los cambios y ahora el Tipping Point está listo para ser conectado a Internet.

Actualmente la red local en la empresa cuenta con un Modem/Router 2wire 2700HG que proporciona una conexión a Internet de banda ancha a través de PPPoE además de la función de ruteo, al momento de conectar el Tipping Point a Internet y debido a la configuración de interfaz externa aplicada este entrará en modo de ruteo lo que podría crear conflictos con el 2wire, ya que también tiene la función de ruteador. Para impedir que se presenten este tipo de inconvenientes fue necesario habilitar el modo bridge dentro del 2wire, al hacer esto habilitamos una configuración especial del Módem-Router en la cual se anula precisamente la parte de router quedando de esta forma en funciones de un simple módem, por lo tanto en modo bridge el 2wire únicamente servirá de pasarela para los datos provenientes de Internet y no llevará a cabo la función NAT, no es necesario hacer algún tipo de gestión ya que todo pasará sin restricciones y ahora la responsabilidad del ruteo recaerá en el Tipping Point instalado

Una vez que el 2wire ha entrado en modo bridge, es posible conectar el Tipping Point de forma segura a Internet, el diagrama de la figura 3-24 muestra la estructura actual de la red local en la empresa.

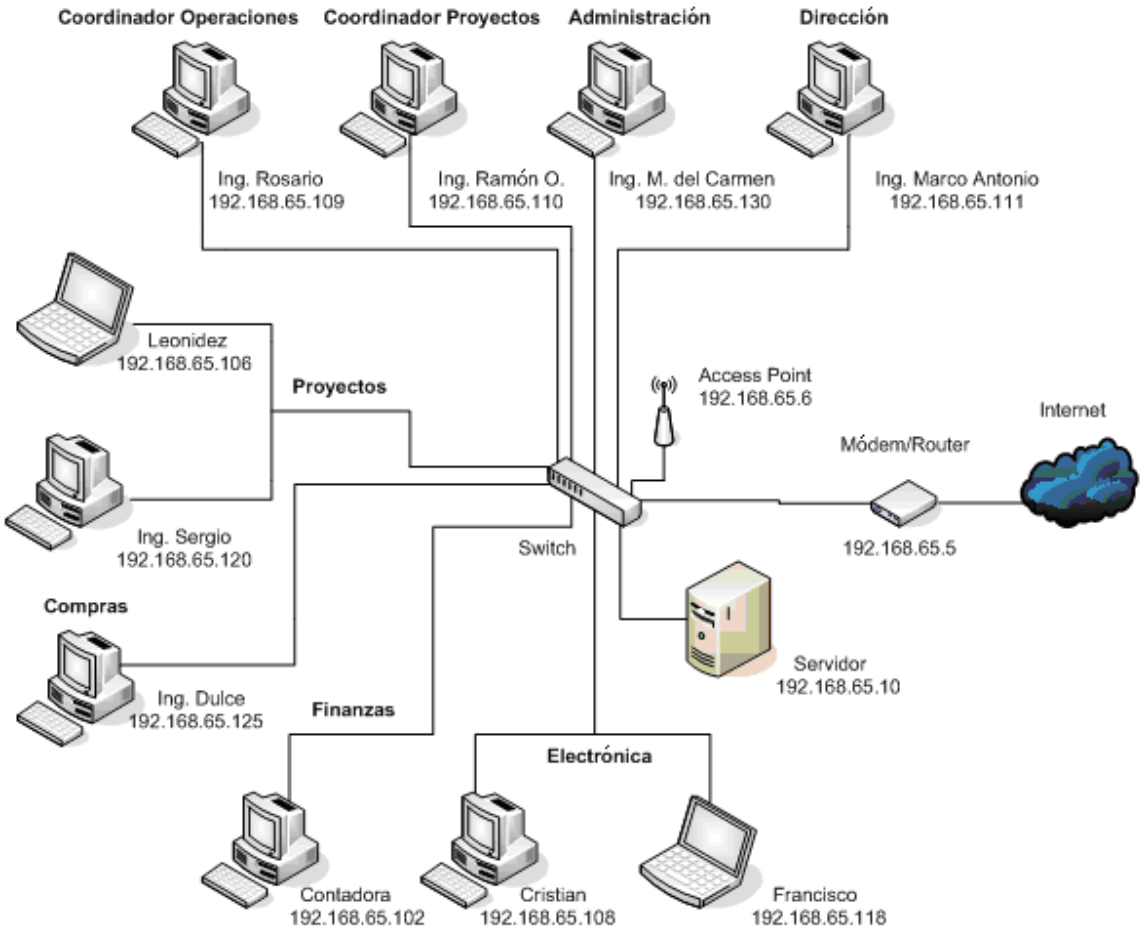

Figura 3-24. Diagrama lógico de la red actual en la empresa.

Por medio de un cable ethernet se conecta la salida del Modem 2wire a la entrada del puerto WAN del Tipping Point x5, a su vez el puerto LAN del Tipping Point es conectado al Switch de la empresa para cerrar la conexión. Una vez terminada la conexión del Tipping Point a Internet, este queda colocado justo en medio del 2wire y el switch.

Al poner el 2wire en modo Bridge se le asigna una dirección IP diferente a la que tenía quedando libre la anterior, ahora el 2wire tiene la dirección de fábrica por default y la interfaz interna del Tipping Point es modificada con el mismo procedimiento antes mencionado de tal manera que se asigna la nueva dirección IP 192.168.65.5.

Una vez que el Tipping Point es conectado a Internet, el diagrama de la red local se ve modificado tal y como se muestra en la figura 3-25.

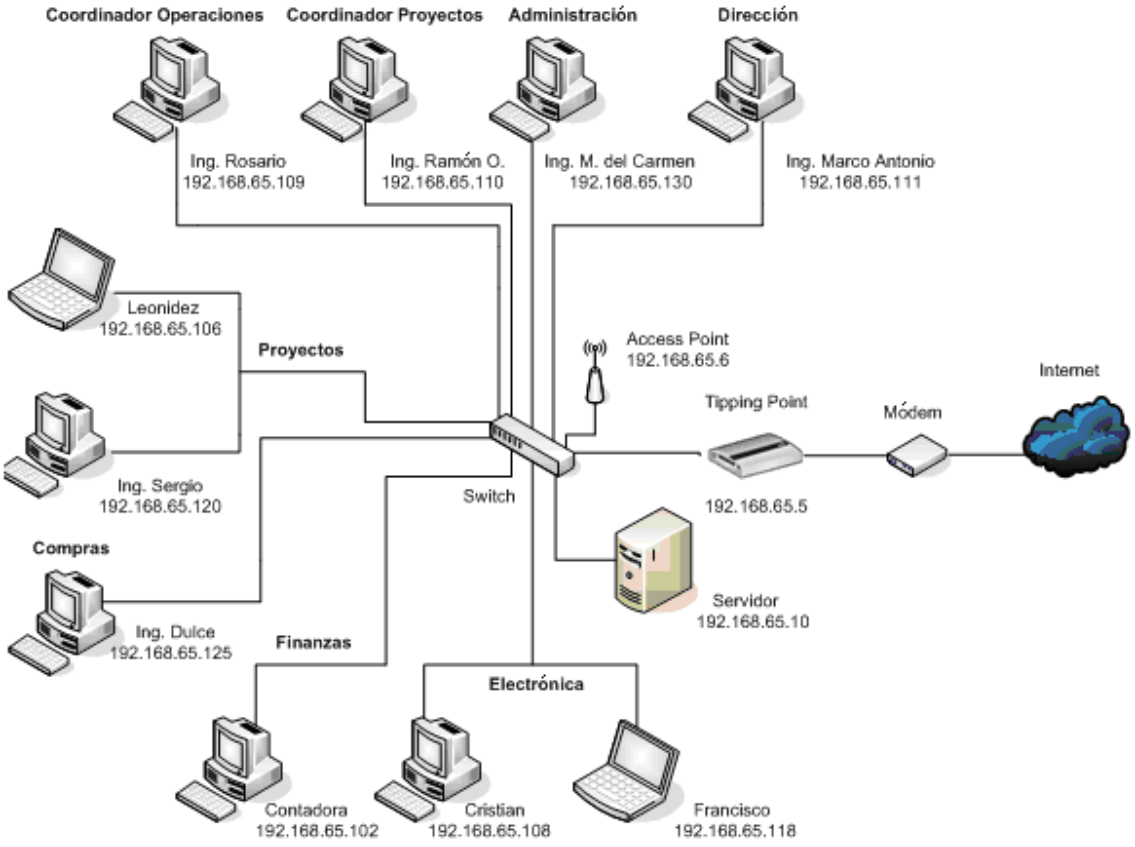

Figura 3-25. Diagrama lógico de la red una vez instalado el Tipping Point x5.

CAPÍTULO IV
PRUEBAS Y RESULTADOS

4.1 Introducción

En el siguiente capítulo, se describen las pruebas que se llevaron a cabo, con el fin de probar el funcionamiento de las diversas configuraciones realizadas en el Tipping Point x5, también se describen los resultados obtenidos de dichas pruebas.

4.2 Funcionamiento General

La primera prueba a llevar a cabo consiste en revisar el funcionamiento general del Tipping Point x5, para esto accedemos al apartado de Salud mediante la ruta Events-Health-Monitor como se aprecia en la figura 4-1.

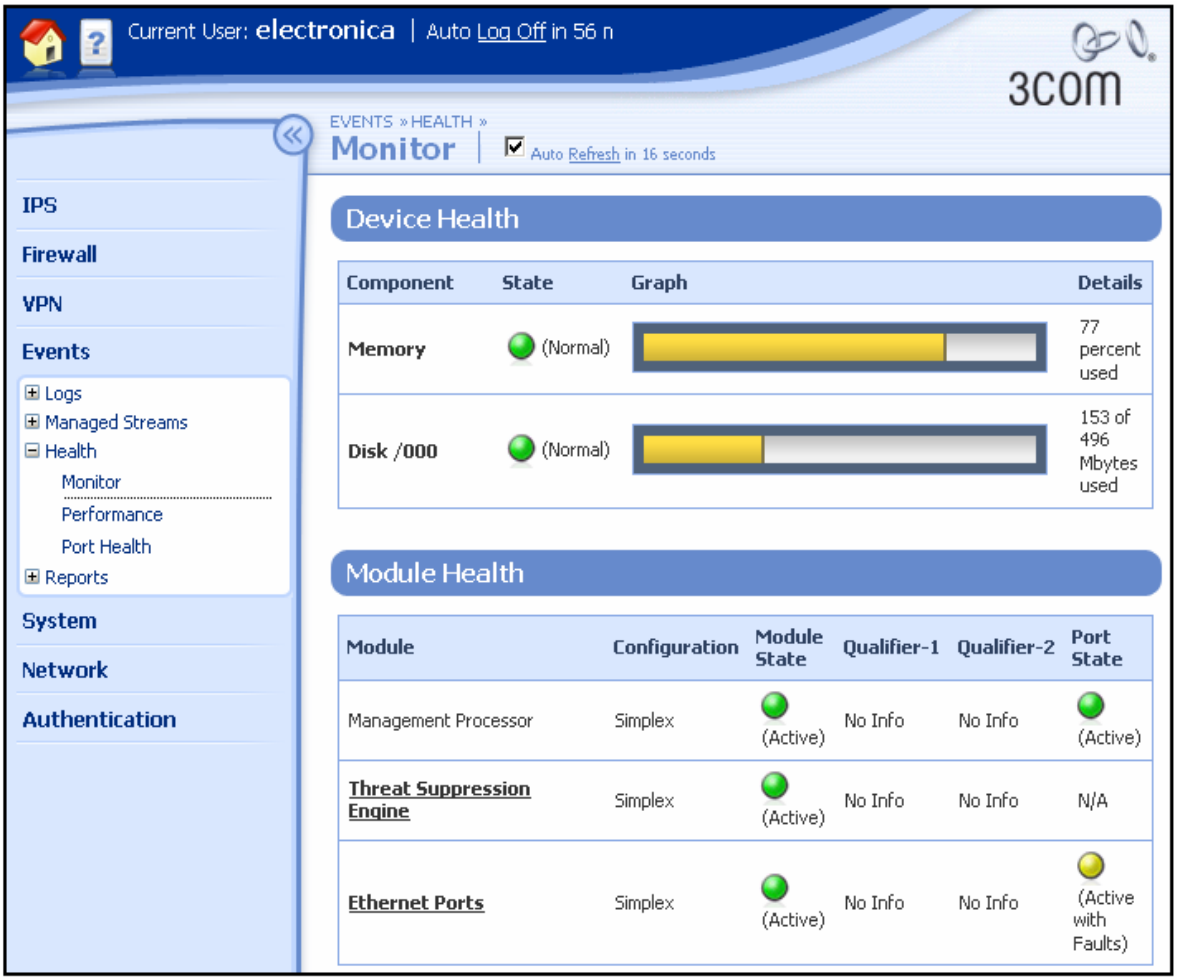

Figura 4-1. Monitior de dispoitivo.

En este apartado es posible dar un vistazo general al estado de salud del dispositivo, más específicamente a la memoria, al disco, y a los módulos de Supresión de Amenazas, Procesador y Puertos Ethernet, como se puede apreciar el estado en color verde es indicativo de que estas funciones están funcionando sin problema alguno.

Siguiendo la ruta Events-Health-Port Health accedemos al estatus de los puertos como se muestra en la figura 4-2.

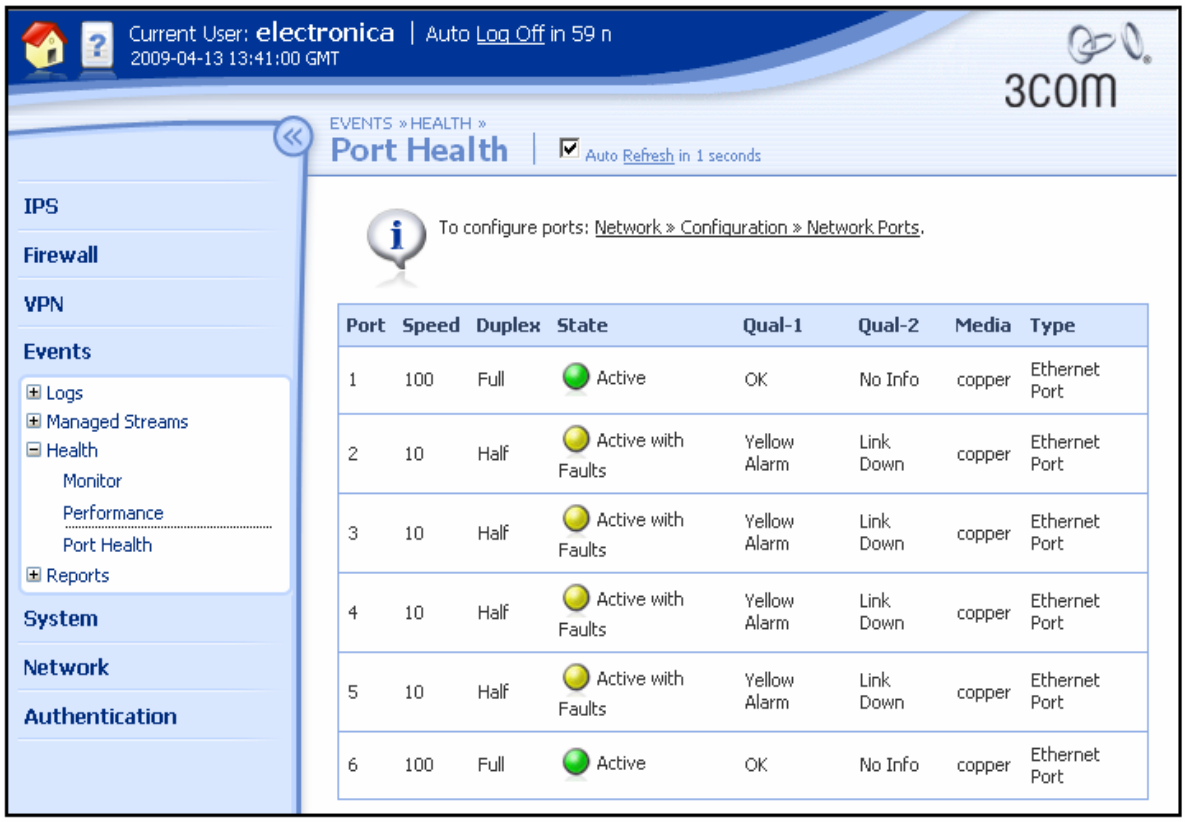

Figura 4-2. Estatus de Puertos.

En este apartado es posible corroborar el correcto funcionamiento de los puertos del Tipping Point x5, se puede observar que únicamente los puertos Ethernet 1 y 6, LAN y WAN respectivamente, se encuentran activados.

Posteriormente por medio de la ruta Events-Traffic-Port verificaremos que los puertos LAN y WAN estén recibiendo tráfico de red y por lo tanto se encuentren funcionando, esto se muestra en la figura 4-3.

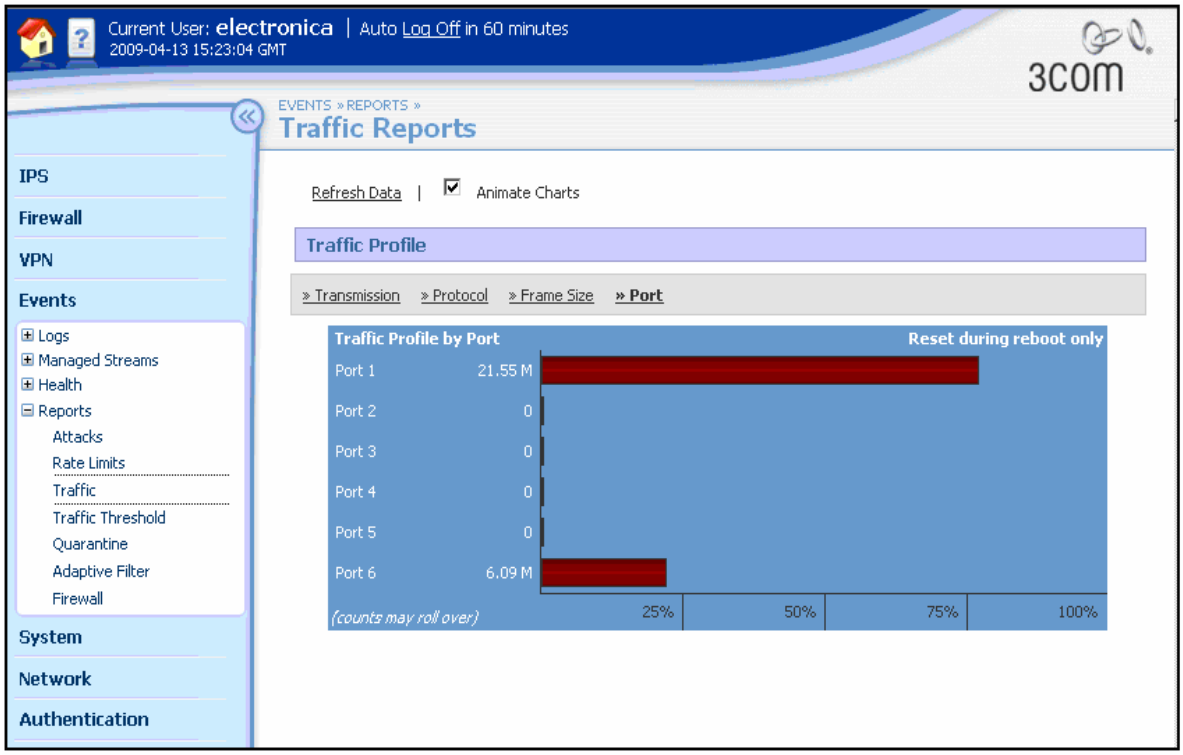

Figura 4-3. Tráfico en puertos Ethernet.

En la figura 4-3 podemos observar que los puertos 1 y 2, se encuentran recibiendo tráfico.

Una vez que se da una revisión al funcionamiento general del dispositivo, lo siguiente consiste en probar el funcionamiento de características más específicas.

4.3 Reglas de Firewall y Servidores Virtuales

Recordemos que una Regla de Firewall consiste en establecer políticas de seguridad a las solicitudes de servicios desde distintas zonas, sean LAN, WAN u otra en específico, además mediante una Regla de Firewall es posible administrar el ancho

de banda consumido por los usuarios o por los mismos servicios, adicionalmente se tiene la capacidad de añadir otras herramientas como el Filtrado Web y Anti-Spam.
Las Reglas de Firewall tienen una estrecha relación con los Servidores Virtuales creados en el Tipping Point x5, cada Servidor Virtual implica la creación de una Regla de Firewall específica es por eso que al probar el funcionamiento de las Reglas directamente probamos el funcionamiento de los Servidores.
Debido a los puntos anteriores las pruebas realizadas serán en conjunto con estas 2 características.

4.3.1 Servidores Virtuales

El Tipping Point x5 fue configurado de tal manera que se habilitarán servidores virtuales para los servicios de POP3, SMTP, HTTP, HTTPS, MS-WBT-Server-TCP y MS-WBT-Server-UDP, como se aprecia en la figura 4-4.

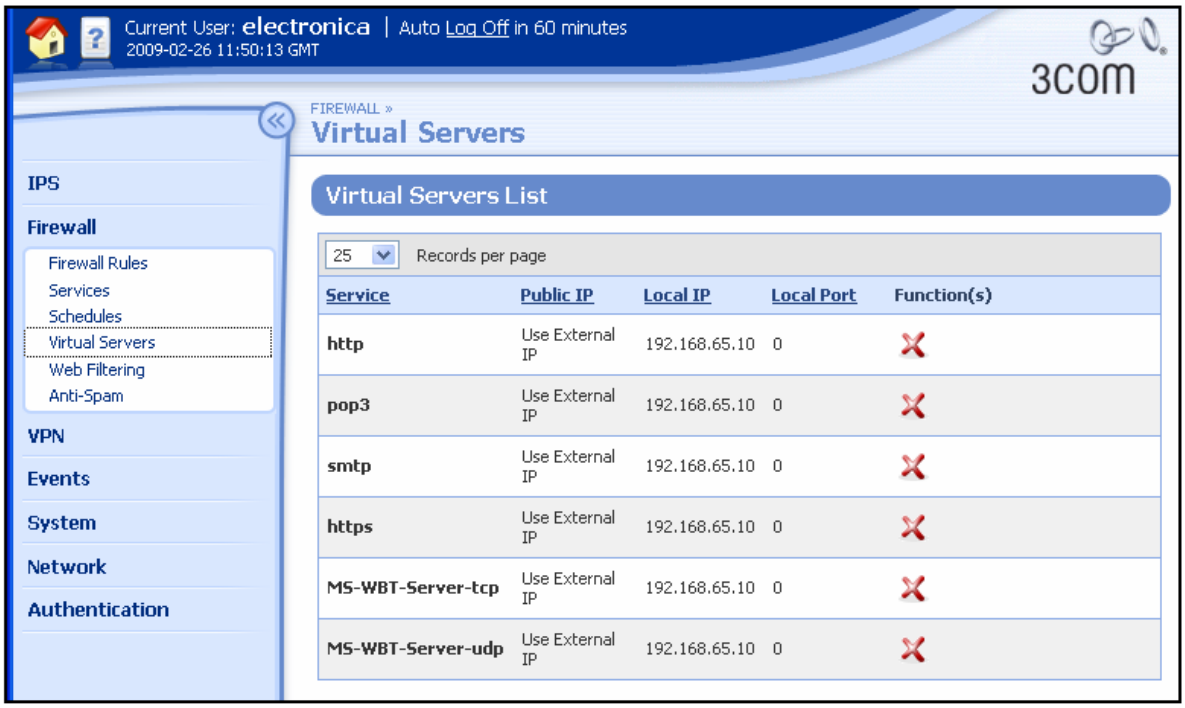

Figura 4-4. Lista de Servidores Virtuales creados.

Estas configuraciones fueron llevadas a cabo con la finalidad de permitir que los usuarios previamente autorizados puedan conectarse con el servidor de la empresa vía externa y hacer uso de los servicios mencionados; por lo tanto es de suma importancia que estás características funcionen correctamente para asegurar que los usuarios autorizados que se encuentren trabajando de manera externa puedan tener acceso a los recursos.

4.3.1.1 Funcionamiento de los Servidores Virtuales

Las pruebas realizadas con el fin de comprobar el funcionamiento de los servidores virtuales son sencillas, estás consisten únicamente en hacer uso de los servicios POP3, SMTP, HTTP, HTTPS, MS-WBT-Server-TCP y MS-WBT-Server-UDP desde cualquier PC dentro y fuera de la empresa.

Las pruebas anteriores fueron llevadas a cabo de manera exitosa sin ningún tipo de complicaciones, esto lo podemos comprobar si seguimos la ruta Events-Reports-Firewall-Services.

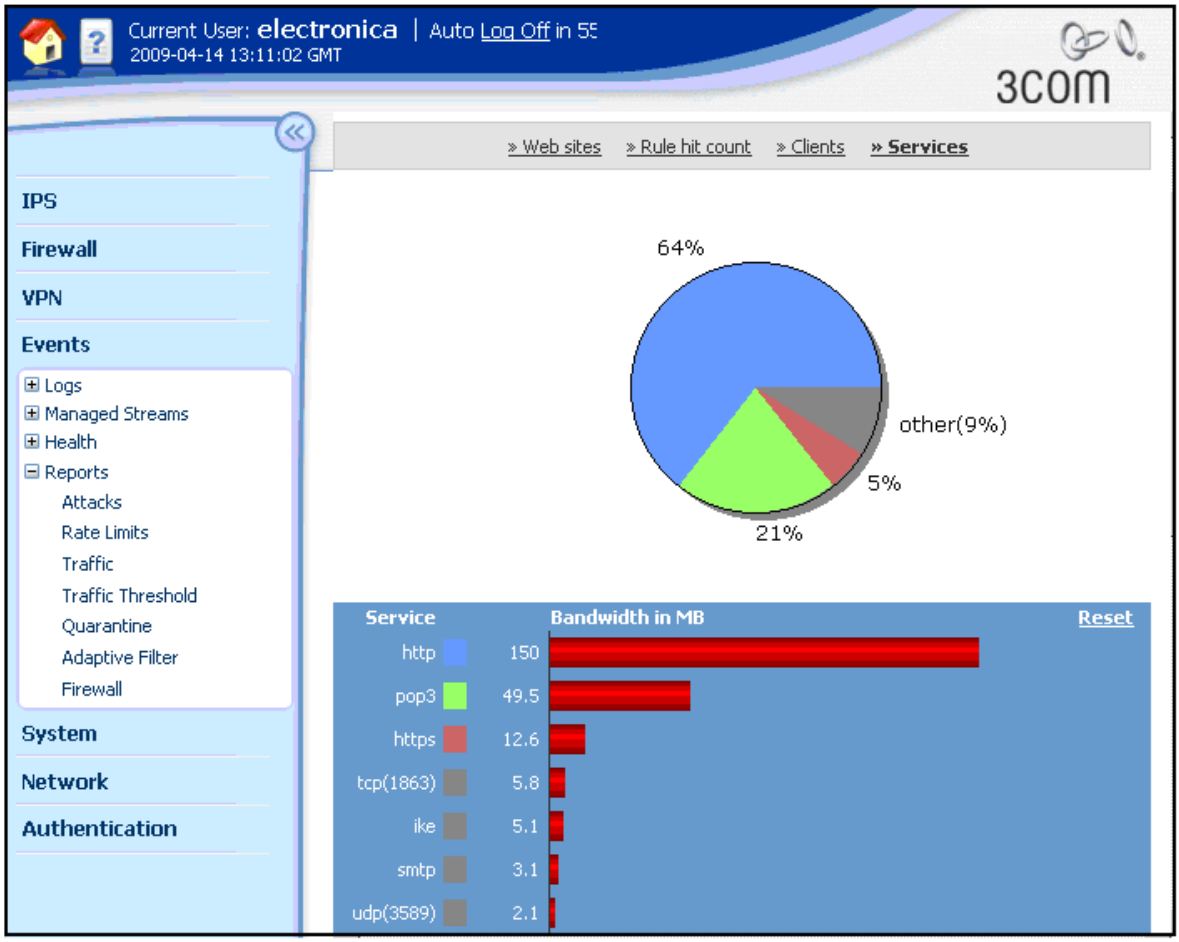

Figura 4-5. Gráfica de uso de los servicios contenidos en los Servidores Virtuales.

La figura 4-5 da fe del buen funcionamiento de los servidores virtuales, en ella podemos determinar que servicio de los Servidores Virtuales es el que consume más ancho de banda y por lo tanto el más utilizado, el consumo del ancho de banda se muestra en MB (Megabytes), en base a estas estadísticas podemos tener control sobre el ancho de banda consumido por cada servicio, se tiene la capacidad de crear una Regla de Firewall que limite el ancho de banda consumido por cada servicio, incluso es posible establecer un ancho de banda predeterminado para cada servicio utilizado por los usuarios, de esta manera podemos hacer uso óptimo del ancho de banda y optimizar al máximo los recursos de la red.

4.3.2 Funcionamiento de las Reglas de Firewall

Las Reglas de Firewall fueron creadas con el propósito de mantener al máximo la seguridad en la red local, por lo tanto es primordial asegurar que estas tengan un desempeño óptimo.

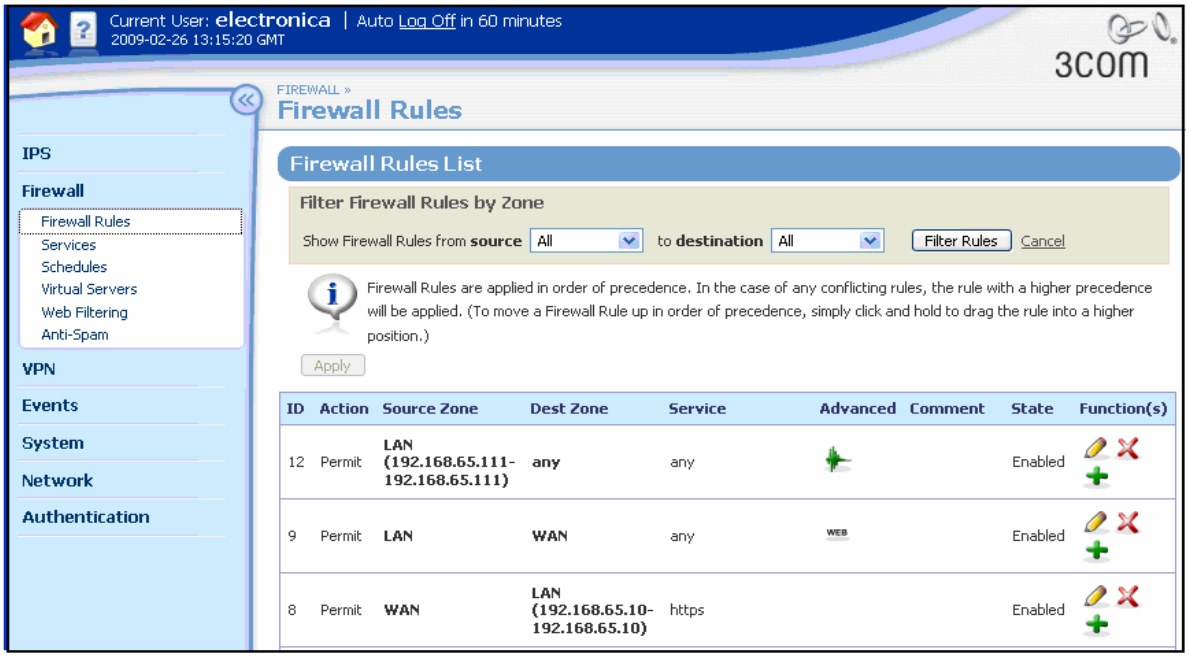

Figura 4-6. Lista de Reglas de Cortafuegos creadas.

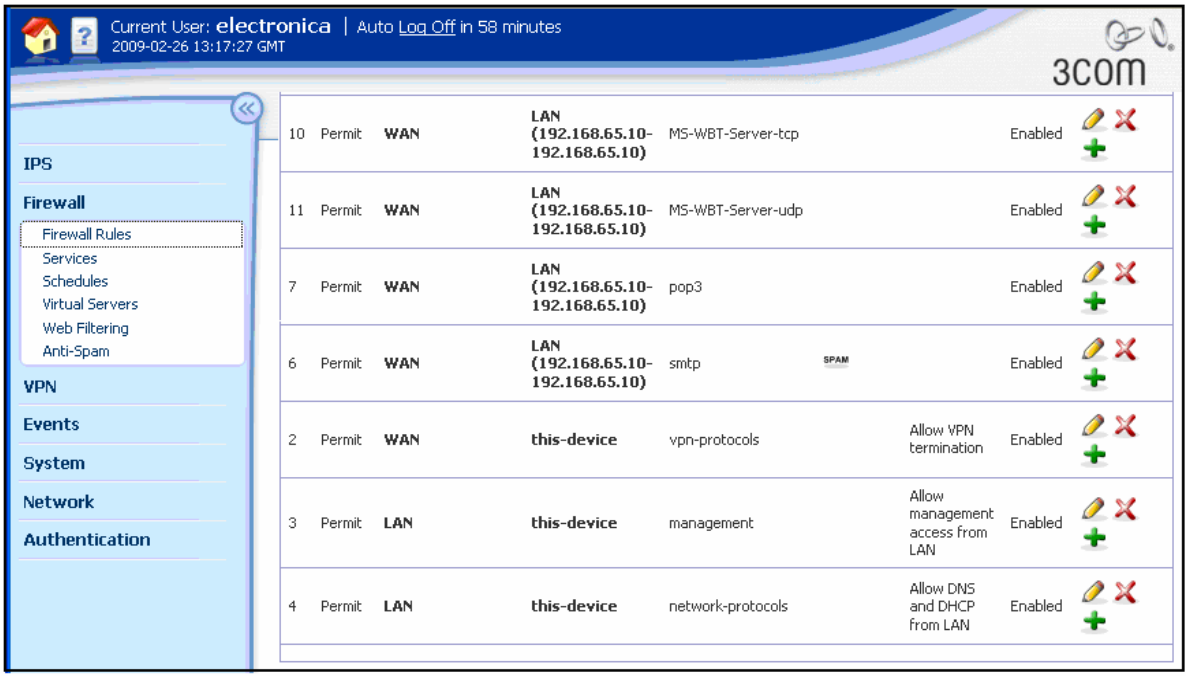

Figura 4-7. Lista de Reglas de Cortafuegos creadas.

En las figuras 4-6 y 4-7, se muestran todas aquellas Reglas de Firewall que fueron creadas.

Las Reglas de Firewall funcionaron sin contratiempos, todos los usuarios involucrados dentro de las reglas no tuvieron problema alguno al momento de hacer las solicitudes de servicios, además el Tipping Point x5 permite al administrador llevar una estadística del uso de las Reglas de Firewall, para acceder a este característica es necesario seguir la ruta Events-Reports-Firewall-Rule hit count, como se observa en las figuras 4-8 y 4-9.

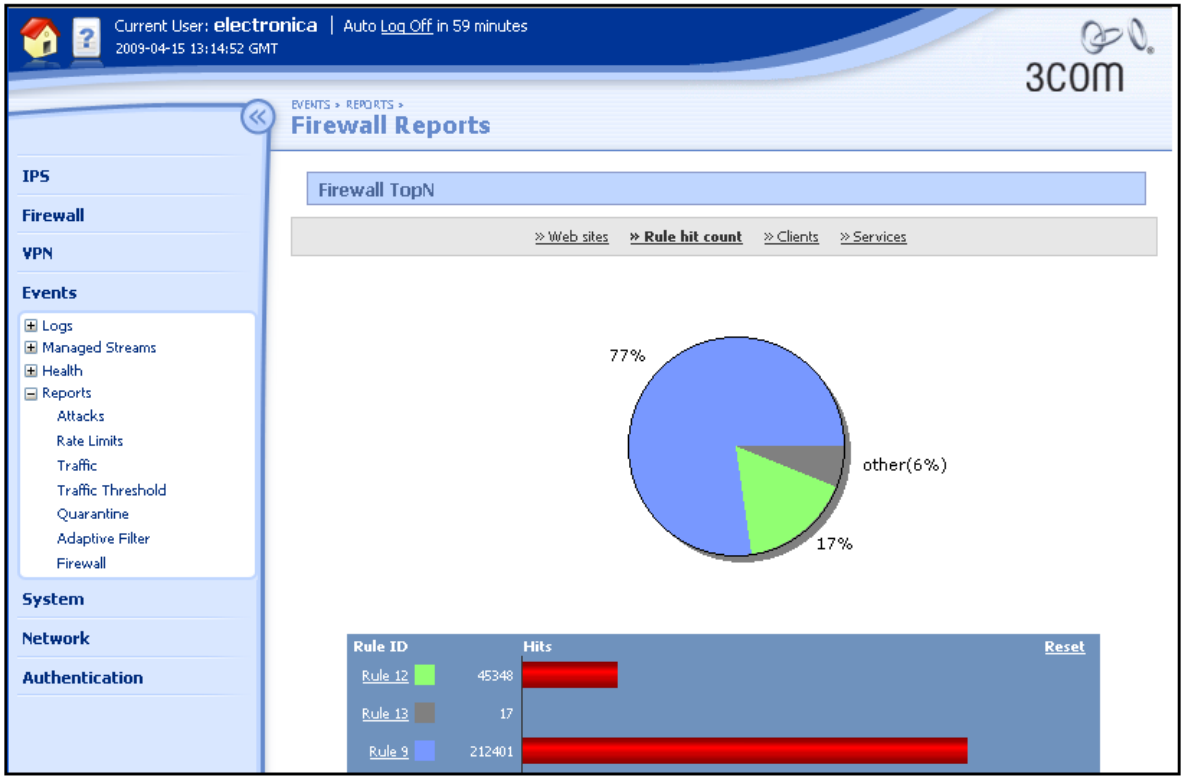

Figura 4-8. Frecuencia de uso de las Reglas de Firewall.

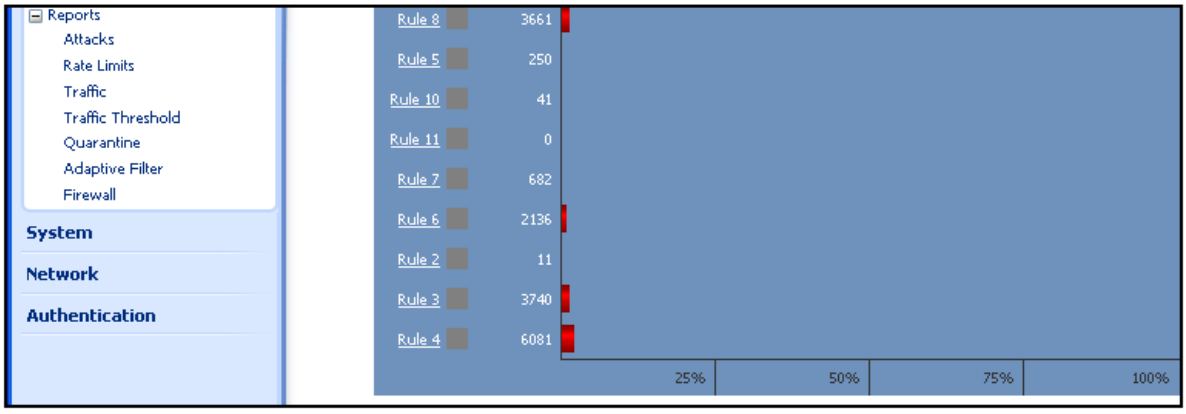

Figura 4-9. Frecuencia de uso de las Reglas de Firewall.

La herramienta Rule hit count le permite al administrador de la red tener un control de la aplicación de las Reglas de Firewall, en la ventana se muestra cual de las Reglas es la que más se aplica a los usuarios cuando estos se encuentran haciendo uso de los recursos de la red, en este caso se trata de la regla 9 correspondiente a uso de todo tipo de servicios con fuente en LAN y destino en WAN, el orden se muestra de manera descendente, posicionando en la parte más alta aquella regla que se aplica de manera más frecuente.

4.4 Funcionamiento del Filtrado Web

El Filtrado Web es una poderosa herramienta que le permite al administrador de la red tener el control del contenido Web al que acceden los usuarios, este servicio funciona mediante una clasificación de sitios Web que pueden ser permitidas o no permitidas según sean las especificaciones.

Al intentar acceder a sitios Web que se encuentren dentro de la clasificación de sitios no permitidos el usuario se vera frente a una ventana como la de la figura 4-10.

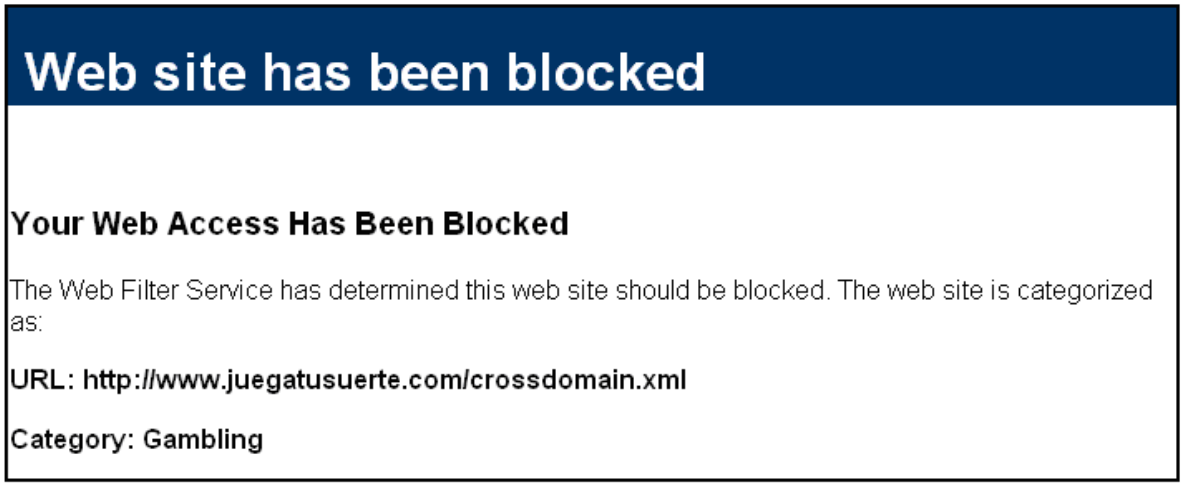

Figura 4-10. Pagina de mensaje de sitio bloqueado.

Como se puede observar en la figura 4-10, el mensaje que recibirá el usuario será una notificación de que el sitio Web ha sido bloqueado, se mostrará la dirección del sitio al que se intentó acceder además de la categoría al cual pertenece.

Adicional a esto es posible tener un registro de todas aquellas entradas a sitios que han sido bloqueados, para esto seguimos la ruta Events-Logs-Firewall Blog Log como se aprecia en la figura 4-11.

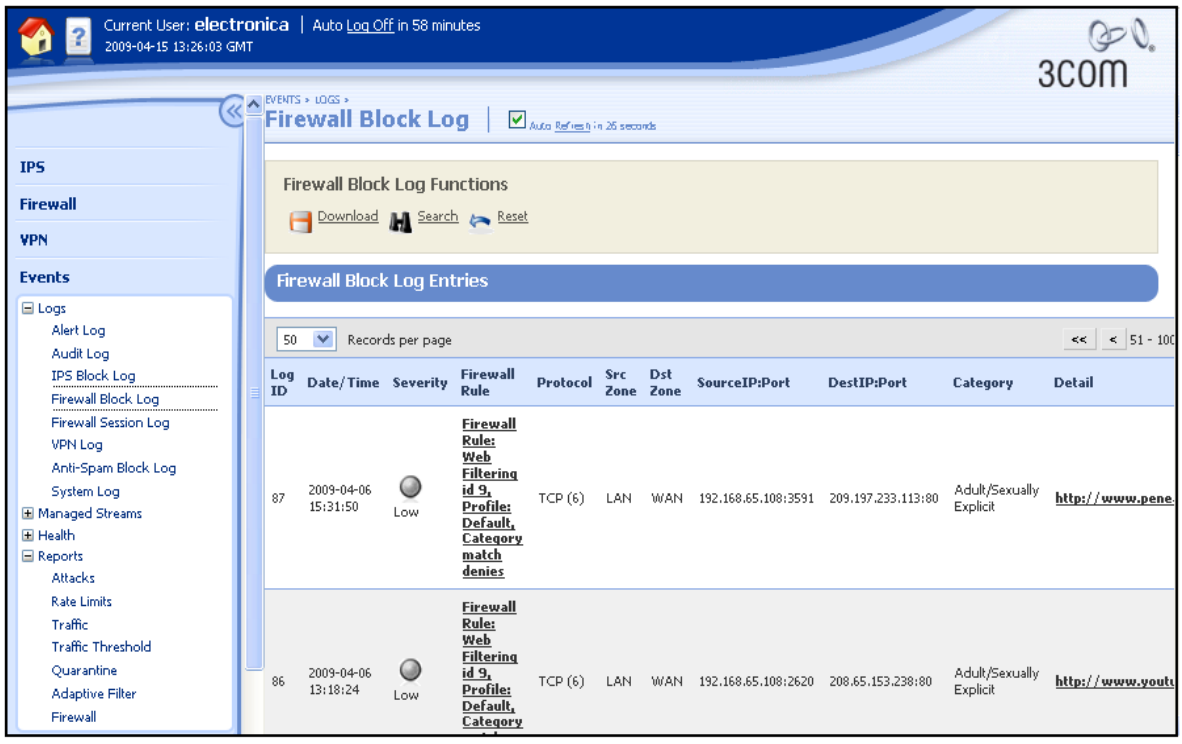

Figura 4-11. Registro de sitios web visitados.

En esta ventana accedemos al registro de los sitios Web que fueron bloqueados cuando los usuarios intentaron accesarlos, en ella se muestra el número de entrada, la fecha y hora del bloqueo, el nivel de seguridad, la Regla de Firewall aplicada al momento de hacer el bloqueo, el protocolo utilizado, la fuente y el destino de la petición, el destino IP del puerto, la categoría del sitio bloqueado y por último la dirección de Internet correspondiente al sitio.
El uso de está herramienta y el conocer estás estadísticas es de gran utilidad para el administrador de la red, el llevar este registro le permitirá tomar las medidas correctivas que considere pertinentes.

4.5 Gestión de ancho de banda

Una de las tareas más importantes consiste en gestionar de manera adecuada los recursos de los que dispone la red para que esta funcione de manera óptima.
El Tipping Point x5 incorpora herramientas que le permiten al administrador tener control sobre el ancho de banda que se utiliza en la red, estas características permiten tomar decisiones y aplicar acciones en búsqueda de optimizar la red, además el Tipping Point x5 permite la asignación de uso de ancho de banda desde un simple usuario, se tiene la característica de conocer el consumo de ancho de banda por cada usuario o dispositivo en la red, para esto seguimos la ruta Events-Reports-Firewall-Clients.

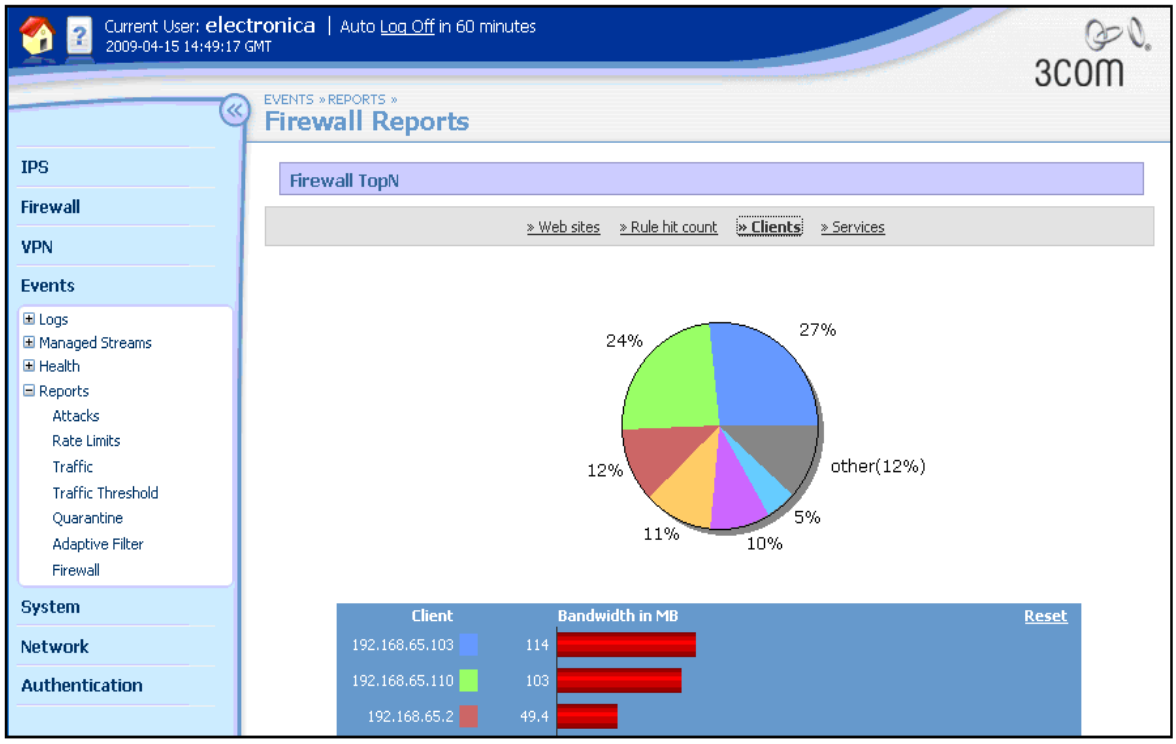

Figura 4-12. Consumo de ancho de banda por usuario.

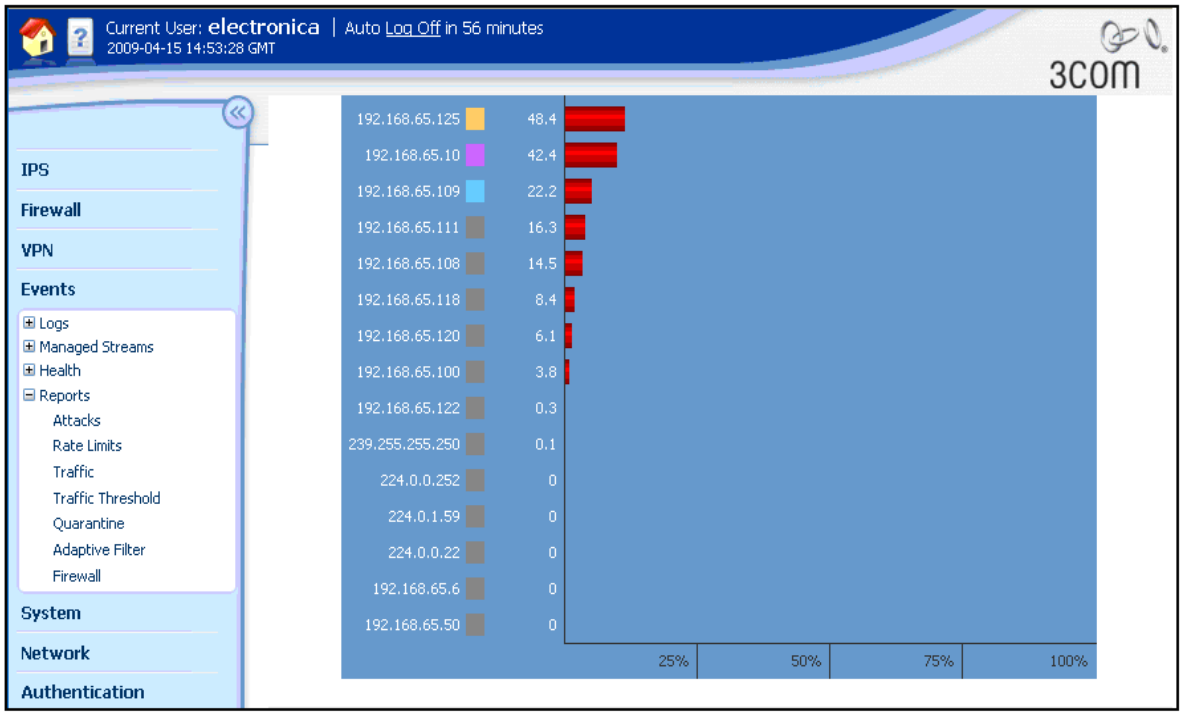

Figura 4-13. Consumo de ancho de banda por usuario.

En las figuras 4-12 y 4-13 podemos ver que usuario de la red consume más ancho de banda medido en MB, en este caso particular el usuario de la PC con dirección 192.168.65.3 es el que más recursos consume, está característica es de gran utilidad si se desea establecer un ancho de banda permitido a cada usuario en particular.
Para poder llevar a cabo lo anterior, es necesario crear una regla de cortafuegos que involucre al usuario o grupo de usuarios a los que se les limitará el ancho de banda permitido, el procedimiento para llevar esto a cabo fue descrito en el capítulo 3.

Es importante agregar que todas las herramientas vistas dentro de este capítulo y que contienen estadísticas son actualizadas de manera automática y en tiempo real.

CONCLUSIONES

Inicialmente la instalación del Tipping Point x5 se plantea como la solución de integrar una plataforma de seguridad y gestión dentro de una red computacional, las prestaciones de este dispositivo permiten satisfacer las necesidades que se plantean al momento de iniciar el trabajo, si bien es cierto existen diversos dispositivos que como uno solo brindan soluciones por separado, el hecho de contar con una herramienta que integre todas estás características resulta de gran utilidad para dar solución a la problemática principal.

Como bien se expuso en el inicio de este documento, la seguridad y la gestión de ancho de banda son dos de las necesidades más importantes en una red computacional, el funcionamiento óptimo de estás dos características garantiza en gran medida la optimización de los recursos de los que dispone nuestra red y esto a su vez optimiza el rendimiento de la misma, la experiencia de trabajar e involucrarse

en este ámbito permite comprender de una mejor manera cuan importante resulta satisfacer esas dos características en particular.

El inicio de este proyecto implica la dificultad de no contar con la experiencia práctica en lo que se refiere a la instalación de dispositivos de conectividad de red, para esto es necesario llevar a cabo una capacitación en lo que se refiere a esta actividad, consistiendo esta en la búsqueda de información referente a equipos de red, características de dispositivos, configuraciones, instalación. Además, si bien se contaba con conocimientos teóricos referente a Redes LAN y WAN, el hecho de tener la oportunidad de participar en la instalación y configuración del Tipping Point x5 implica además una mayor capacitación teórica referente al tema.

A lo largo de este trabajo, me enfrenté a complicaciones que debido a mi falta de experiencia no me era posible solucionar de manera correcta e inmediata, pero el estudio, la capacitación y la colaboración tanto de compañeros como de asesores dentro y fuera de la empresa me ayudaron a superar las complicaciones que se presentaron.

Las pruebas realizadas y los resultados obtenidos de las mismas permiten concluir que el proyecto alcanzo las expectativas y las metas que se generaron en su planeación e inicio.

La realización de este trabajo brinda la valiosa experiencia para en un futuro tener las herramientas necesarias en la elaboración de proyectos y la realización de trabajos con la seguridad de contar con un respaldo que garantiza que el procedimiento seguido es el correcto.

Bibliografía

1. Eric Maiwald, 2005, Fundamentos de seguridad de Redes, Mc Graw Hill, México.

2. Corina Schmelkes, 2001, Manual para la presentación de anteproyectos, 2da. Edición, Oxford, México.

3. Diciembre 2007, 3Com® X Family Concepts Guide.

4. Noviembre 2007, 3Com® X5 Quick Start Guide.

5. Jesús Arámbula Trejo, Seguridad en redes de computadoras.
Ver (http://www.monografias.com/trabajos30/seguridad-redes/seguridad-redes.shtml)

6. 3com®, Plataformas de seguridad unificada de 3Com®.
Ver(http://www.3com.com/prod/es_LA_AMER/detail.jsp?tab=features&sku=WEBXFAMILYSYS)

7. Anónimo, 2007, 25 Años desde el primer virus informático.
Ver (http://www.kriptopolis.org/25-aniversario-del-primer-virus-informatico)

8. Anónimo, 2006, El computador personal cumple 25 años.
Ver(http://es.wikinews.org/wiki/El_computador_personal_cumple_veinticinco_a%C3%B1os)

9. Anónimo, 2009, Protocolo de comunicaciones.
Ver (http://es.wikipedia.org/wiki/Protocolo_de_red)

10. Anónimo, 2008, Introducción a los ataques.
Ver (http://es.kioskea.net/contents/attaques/attaques.php3)

Apéndice A. Glosario de términos

Appletalk. Conjunto de protocolos desarrollados por Apple Inc. para la conexión de redes.

ARP. Siglas en inglés de Address Resolution Protocol (Protocolo de resolución de direcciones).

ASN.1. Siglas en inglés de Abstract Syntax Notation One (Notación sintáctica abstracta 1).

ATM. Siglas en inglés de Asynchronous Transfer Mode (Modo de Transferencia Asíncrona).

Búfer. En informática, ubicación de la memoria en una computadora o en un instrumento digital reservada para el almacenamiento temporal de información digital, mientras que está esperando ser procesada.

CDP. Siglas en inglés de Cisco Discovery Protocol (Protocolo de descubrimiento de Cisco).

Cortafuegos. Elemento de hardware o software que se utiliza en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización

DHCP. Siglas en inglés de Dynamic Host Configuration Protocol (Protocolo Configuración Dinámica de Anfitrión).

Driver. Controlador de dispositivo, llamado normalmente controlador (en inglés, device driver) es un programa informático que permite al sistema operativo interactuar con un periférico, haciendo una abstracción del hardware y proporcionando una interfaz -posiblemente estandarizada- para usarlo.

ETD. Siglas en inglés de Data Terminal Equipment (Equipo terminal de datos).

Ethernet. Estándar de redes de computadoras de área local con acceso al medio por contienda CSMA/CD.

Fast Ethernet. Serie de estándares de IEEE de redes Ethernet de 100 Mbps

FDDI. Siglas en inglés de Fiber Distributed Data Interface (Interfaz de datos distribuidos por fibra).

Firewalls. Elemento de hardware o software que se utiliza en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización

FTP. Siglas en inglés de File transfer protocol (Protocolo de transferencia de archivos).

Gigabit Ethernet. Tecnología que incrementa diez veces la velocidad de Fast Ethernet, 1 gigabit por segundo (Gbps) o 1000 Mbps. Toma ventaja de la alta velocidad de la tecnología de interface física de ANSI X3T11 FibreChanel mientras que mantiene el mismo formato que IEEE 802.3.

Gusanos. Subclase de virus. Por lo general, los gusanos se propagan sin la intervención del usuario y distribuye copias completas (posiblemente modificadas) de sí mismo por las redes. Un gusano puede consumir memoria o ancho de banda de red, lo que puede provocar que un equipo se bloquee.

Handshaking. Protocolo de comunicación se usa para transferir datos entre dos dispositivos asíncronos (como puertas serie RS232). Se usan normalmente dos líneas. Una de éstas es para la señal de datos preparados desde el dispositivo que manda al que recibe. Cuando el que recibe ha aceptado los datos, manda una señal de datos recibidos al dispositivo original, que sabe así que puede mandar otro grupo de datos, y así sucesivamente.

HDLC. Siglas en inglés de High-Level Data Link Control

HTTP. Siglas en inglés de HyperText Transfer Protocol (Protocolo de transferencia de hipertexto).

HTTPS. Siglas en inglés de Hypertext Transfer Protocol Secure (Protocolo seguro de transferencia de hipertexto).

IBM. Siglas en inglés de International Business Machines

ICMP. Siglas en inglés de Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet).

ICQ. Siglas en inglés de I seek you" o "te busco" es un servicio de mensajería instantánea y el primero de su tipo en ser ampliamente utilizado en Internet, mediante el cual es posible chatear y enviar mensajes instantáneos a otros usuarios conectados a la red.

IGMP. Siglas en inglés de Internet Group Management Protocol

IMAP. Siglas en inglés de Internet Message Access Protocol (Protocolo de acceso a mensajes electrónicos).

IP. Siglas en inglés de Internet Protocol (Protocolo de Internet).

IPv4. Versión 4 del Protocolo IP (Internet Protocol) versión anterior de ipv6. Está fue la primera versión del protocolo que se implementó extensamente, y forma la base de Internet. IPv4 usa direcciones de 32 bits, limitándola a 2^{32} = 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs).

IPv6. El protocolo **IPv6** es una nueva versión de IP (Internet Prococol), diseñada para reemplazar a la versión 4 (IPv4) RFC 791, actualmente en uso. IPv6 admite 340.282.366.920.938.463.463.374.607.431.768.211.456 (2^{128} o 340 sextillones) direcciones —cerca de $3{,}4 \times 10^{20}$ (340 trillones) direcciones por cada pulgada cuadrada ($6{,}7 \times 10^{17}$ o 670 mil billones direcciones/mm^2) de la superficie de La Tierra.

IPS. Siglas en inglés de Intrusión Prevention System (Sistema de prevención de intrusiones).

IPX. Siglas en inglés de Internetwork Packet Exchange.

IRC. Siglas en inglés de Internet Relay Chat.

Kbps. Kilobits por Segundo, velocidad de trasferencia de archivos.

LAN. Siglas en inglés de Local Area Network (Red de área local).

Modem. Dispositivo que sirve para modular y desmodular (en amplitud, frecuencia, fase u otro sistema) una señal llamada portadora mediante otra señal de entrada llamada moduladora

Modo bridge. Configuración especial de algunos Modem-Router en la cual se anula la parte de router quedando de está forma en funciones de un simple modem y no llevará a cabo la función NAT.

Multicast. Multidifusión (multicast) es el envío de la información en una red a múltiples destinos simultáneamente, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red sólo una vez y creando copias cuando los enlaces en los destinos se dividen.

NAT. Siglas en inglés de Network Address Translation (Traducción de Dirección de Red).

NetBEUI. NetBIOS Extender Interface. Versión mejorada del protocolo NetBIOS utilizado por sistemas operativos de red como LAN Manager, LAN Server, Windows para grupos de trabajo y Windows NT. NetBEUI formaliza la capa de transporte y agrega funciones. NetBEUI implementa el protocolo OSI LLC2.

NetBIOS. Network Basic Input/Output System. API (Application Programming Interface) utilizada por aplicaciones en redes LAN de IBM para peticiones de

servicios de los procesos de red de niveles inferiores. Estos servicios deben incluir el establecimiento y terminación de las sesiones y transferencia de información.

NFS. Siglas en inglés de Network File System (Sistema de archivos de red).

NNTP. Siglas en inglés de Network News Transport Protocol

OSI. Siglas en inglés de Open System Interconnection (Modelo de referencia de Interconexión de Sistemas Abiertos).

PC. Siglas en inglés de Personal computer (Computadora personal).

POP3. Siglas en inglés de Post Office Protocol, diseñado para recibir correo no para enviarlo.

PPP. Siglas en inglés de Point-to-Point Protocol (Protocolo punto a punto).

PPPoE. Siglas en inglés de Point-to-Point Protocol over Ethernet (Protocolo Punto a Punto sobre Ethernet).

Protocolo. Conjunto de estándares que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red. Protocolo de red para la comunicación de datos a través de paquetes conmutados.

RARP. Siglas en inglés de Reverse Address Resolution Protocol (Protocolo de resolución de direcciones inverso

Routing. Routing o encaminamiento se refiere a la selección del camino en una red de computadoras por donde se envían datos.

RPC. Siglas en inglés de Remote Procedure Call (Llamada a Procedimiento Remoto).

RS-232. También conocido como Electronic Industries Alliance RS-232C) es una interfaz que designa una norma para el intercambio serie de datos binarios entre un

DTE (Equipo terminal de datos) y un DCE (Data Communication Equipment, Equipo de Comunicación de datos).

Server. Equipo destinado a proveer servicios usados por otras computadoras.

Servidores virtuales. Partición dentro de un servidor que habilita varias máquinas virtuales dentro de dicha máquina por medio de varias tecnologías.

SMB. Siglas en inglés de Server Message Block.

CIFS. Siglas en inglés de Common Internet File System.

SMTP. Siglas en inglés de Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo).

SNMP. Siglas en inglés de Simple Network Management Protocol (Protocolo Simple de Administración de Red).

Spam. Mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor

SPX. Siglas en inglés de Sequenced Packet Exchange

SSH. Siglas en inglés de Secure Shell (Intérprete de órdenes seguro).

SSL. Siglas en inglés de Secure Sockets Layer (Protocolo de Capa de Conexión Segura).

Switch. Dispositivo de Networking situado en la capa 2 del modelo de referencia OSI

TCP/IP. Siglas en inglés de Transport Control Protocol/ Internet Protocol. Los dos protocolos de Internet más conocidos que erróneamente suelen confundirse con uno solo. TCP, corresponde a la capa 4 (capa de transporte) del modelo OSI y ofrece transmisión confiable de datos, IP corresponde a la capa 3 (capa de red) del modelo

OSI y ofrece servicios de datagramás sin conexión. Comúnmente TCP/IP se utiliza para hacer referencia a la suite de protocolos de Internet.

Telnet. TELecommunication NETwork es el nombre de un protocolo de red (y del programa informático que implementa el cliente), que sirve para acceder mediante una red a otra máquina, para manejarla remotamente.

Token Ring. Tecnología de LAN basada en la transmisión de estafeta y soportada por IBM. Corre a 4 o 16 Mbps sobre una topología de anillo. Es similar a IEEE 802.5.

Troyanos. Programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona.

UDP. Siglas en inglés de User Datagram Protocol (Protocolo de Datagrama de Usuario).

URL. Siglas en inglés de Uniform Resource Locator(Llocalizador uniforme de recurso).

UTP. Siglas en inglés de Unshielded Twisted Pair (Cable trenzado sin apantallar).

VoIP. Voice over IP. La habilidad de transportar voz, al estilo de la telefonía normal, sobre Internet basado en IP con funcionalidad, confiabilidad y calidad de voz similar a la tecnología POTS.

VPN. Siglas en inglés de Virtual private network (Red privada virtual).

WAN. Siglas en inglés de Wide area network (Red de área amplia).

X.25. Estándar UIT-T para redes de área amplia de conmutación de paquetes.

Apéndice B. Especificaciones técnicas del Tipping Point 3com x5 3crtpx5-u-96

SPECIFICATIONS

Information in this section is relevant to all versions of the 3Com X5 and X506 Unified Security Platforms, unless stated otherwise.

CONNECTORS
6 auto-negotiating 10BASE-T/100BASE-TX configured as auto MDI/MDIX

1 serial (RJ-45)

CONCURRENT SESSIONS
3Com X5 (25 user license): 20,000

3Com X5 (unlimited license): 60,000

3Com X506 (unlimited license): 128,000

INTRUSION PREVENTION
TippingPoint Threat Suppression Engine

IPS performance:
- X5: 20 Mbps
- X506: 60 Mbps

Automated Digital Vaccine Attack Filter Update Service‡ by TippingPoint

Recommended settings for Intrusion Prevention System (IPS) filters

Zero-day filters

Level 4–7 rate limiting

Automatic quarantine

2,300+ attack filters protecting against spyware, worms, viruses, trojans, phishing, VoIP threats, DoS, P2P, IM

FIREWALL
Firewall performance:
- X5: 70 Mbps
- X506: 100 Mbps

Firewall policies:
- X5 (25 user): 50
- X5 (unlimited user): 100
- X506: 500

Security zones:
- X5: 16
- X506: 32

Virtual servers:
- X5: 25
- X506: 100

Time-based schedules

User authentication

VIRTUAL PRIVATE NETWORK (VPN)
VPN performance (168-bit DES):
- X5: 40 Mbps
- X506: 95 Mbps

Concurrent VPN client sessions:
- X5 (25 user): 50
- X5 (unlimited user): 128
- X506: 1,000

Security Associations:
- X5: 50
- X506: 512

Keying modes: manual key, IKE-PSK, IKE-X509

Encryption: DES, 3DES, AES128, AES-192, AES-256

VPN client support: native IPSec, L2TP/IPSec, PPTP/MPPE

User-based zone-specific VPN termination via LDAP

WEB CONTENT FILTERING
Annual subscription service*:
- Provider: WebSense; onbox subscription service*
- URLs filtered: 15+ million*
- Content filter categories: 40*

Custom URL black/white lists

User-based content filtering via LDAP

Keyword, wildcard, regular URL matching

ANTI-SPAM†
GlobalView Mail Reputation Service

Automated SMTP email Spam rating service

Greater than 80% detection rate

Industry's lowest false positives

TRAFFIC SHAPING
Inbound and outbound rate limiting

Policy-based shaping

Traffic shaping inside VPN tunnels

NETWORKING
Deployment modes: IP transparent, route, NAT

IP router interfaces:
- X5: 6
- X506: 32

IP address groups:
- X5: 25
- X506: 200

Static routes:
- X5: 100
- X506: 500

Dynamic routing RIP v1 and 2, OSPF v2 including NSSA

OSPF routes:
- X5: 50,000
- X506: 200,000

PPPoE, L2TP, PPTP IP assignment

DHCP client

IEEE 802.1Q VLAN support

Internal multi-scope DHCP server

DHCP relay over VPN

GRE tunneling

IP multicast routing PIM-DM

IGMP v1 and 2

HIGH AVAILABILITY
Dual-box active-standby pair

Dual-box automatic configuration synchronization

Dual WAN links in active-standby fail-over pair

Dual WAN links in active-active load-balancing pair

Primary and secondary VPN peers

Configurable load-balancing

SYSTEM AND ADMINISTRATION
Web interface via HTTPS

Command line interface via console, telnet, SSH

TippingPoint Security Management System (SMS) support

RADIUS server and local database authentication

DNS support for dynamic IP allocation

Configuration snapshot and restore

Software upgrade via web interface or SMS

Software rollback

SNMP v1, 2 and 3; SNMP Enterprise MIB

Fully-integrated AdventNet Firewall Analyzer support

DIMENSIONS
X5

Height: 4.3 cm (1.7 in)

Width: 29.5 cm (11.6 in)

Depth: 17.5 cm (6.9 in)

Weight: 1.1 kg (2.5 lb)

X506

Height: 4.3 cm (1.7 in)

Width: 44.5 cm (17.5 in)

Depth: 30.5 cm (12.0 in)

Weight: 4.1 kg (9.0 lb)

POWER SUPPLY
X5

100-240 VAC auto-ranging, 50/60 Hz

Current rating: 0.8–1.2 Amps, max

Power consumption: 30 W, max

X506

100-240 VAC auto-ranging, 50/60 Hz

Current rating: 1–2 Amps, max

Power consumption: 50 W, max

ENVIRONMENTAL REQUIREMENTS
Operating temperature: 0° to 40°C (32° to 104°F)

Storage temperature: -20° to 80°C (-4° to 176°F)

Humidity: 5% to 95% non-condensing

RELIABILITY
(MTBF @25°C)

X5: 22 years (193,000 hours)

X506: 13 years (115,000 hours)

EMISSIONS / AGENCY APPROVALS
FCC Part 15 Class B

EN 55022 Class B

ICES-003 Class B

VCCI Class B

EN 61000-3-2

EN 61000-3-3

IMMUNITY
Product conforms to EN 55024

SAFETY AGENCY CERTIFICATIONS
UL 60950-1

IEC 60950-1

EN 60950-1

CAN/CSA-C22.2 No. 60950-1-03

STANDARDS AND PROTOCOLS
IEEE standards

IEEE 802.1Q (VLANs)

IEEE 802.3 Ethernet

IEEE 802.3i (10BASE-T)

IEEE 802.3u (Fast Ethernet)

RFC standards

RFC 0768 (User Datagram Protocol)

RFC 0791 (Internet Protocol)

RFC 792, 950, 1256 (Internet Control Message Protocol)

RFC 0793 (Transmission Control Protocol)

RFC 1157 (Simple Network Management Protocol)

RFC 1213 (Management Information Base for Network Management of TCP/IP-based Internets: MIB-II)

RFC 1722, 2082, 2453 (RIP)

RFC 2131 (DHCP)

RFC 2236 (IGMP)

RFC 2403 (Use of HMAC-MD5-96 within ESP and AH)

RFC 2404 (Use of HMAC-SHA-1-96 within ESP and AH)

RFC 2405 (ESP DES-CBC Cipher Algorithm With Explicit IV)

RFC 2410 (NULL Encryption Algorithm and Its Use With IPsec)

RFC 2516 (PPPoE)

RFC 2541 (ESP CBC-Mode Cipher Algorithms)

RFC 2637 (PPTP)

RFC 2661 (L2TP)

RFC 2784 (Generic Routing Encapsulation)

RFC 3022 (Network Address Translation)

RFC 3164 (Syslog)

RFC 3193 (Securing L2TP using IPsec)

RFC 3261 (SIP)

RFC 3947 (Negotiation of NAT-Traversal in the IKE)

RFC 3948 (UDP Encapsulation of IPsec ESP Packets)

RFC 3973 (PIM-DM)

RFC 4109 (Algorithms for Internet Key Exchange version 1)

RFC 4301 (Security Architecture for the Internet Protocol)

RFC 4302 (IP Authentication Header)

RFC 4303 (IP Encapsulating Security Payload)

PACKAGE CONTENTS
X5

3Com X5 Unified Security Platform

Power adapter

X506

3Com X506 Unified Security Platform

Power cord

WARRANTY
One Year Limited Hardware Warranty

Limited Software Warranty for 90 days

90 days free technical support

Refer to www.3com.com/warranty for details.

‡ 1 year of updates included with purchase of device; purchase additional licenses to extend protection

* 30-day trial included; requires purchase of content filter license for continued protection

† 30-day trial included; requires purchase of anti-Spam filter license for continued protection