UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

"MODERNIZACIÓN Y PROTECCIÓN DE LOS SERVICIOS DE INTERNET PARA LA SECRETARÍA DE GOBERNACIÓN"

T R A B A J O E S C R I T O

EN LA MODALIDAD DE DESARROLLO DE UN CASO PRÁCTICO

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A :

M I R O S L A B A B E R E N I C E
Z Ú Ñ I G A T A M A Y O

ASESOR: ING. OSCAR ESTRADA GARCIA

MÉXICO, 2012

AGRADECIMIENTOS

A mi madre Leticia Zúñiga por ser un ejemplo:

La mujer que con su entereza me enseñó lo que es vivir; a saborear el triunfo y levantarme de las derrotas, que con sus consejos volvió a darme el empuje para seguir adelante.
A ti que supiste ser Madre y Padre, aunque hubo momentos difíciles, siempre tuve tu apoyo ante todo.

A mi hermana Michelle Zúñiga:

Por ser la mejor hermana que dios me pudo dar, mi mayor motivación y por su cariño incondicional…

"Debí esforzarme mucho para ser todo lo buena, protectora y segura que mi hermana menor pensaba que yo era. El desafío de estar a la altura de sus fantasías fue tan grande, que es la gran responsable de que yo me superara en muchas cosas."

A Rosalí Sabre:

"Prima, como las ramas de un árbol, crecemos en distintas direcciones pero nuestra raíz continúa siendo una sola. Así, la vida de cada una será siempre una parte esencial de la de la otra."

Al Lic. José Oscar Vega M:

Por confiar en mí, darme la oportunidad de crecer profesionalmente y sobre todo por brindarme su sincera amistad.

A todos mis profes:

No sólo de la carrera sino de toda la vida, mil gracias porque forman parte de lo que ahora soy, Especialmente a mi asesor Oscar Estrada por tu amistad, apoyo y paciencia para la elaboración de este trabajo.

A todos mis amigos:

Sin excluir a ninguno pero en especial a Solecito, Iselita, Eli, Perita, Nathali, Pakito, George, Hiram, Vincho, Javi, Serch, William Kelleher, Rene Villa y Alejandro Cuevas por todo su apoyo, amistad y compañía.

ÍNDICE

INTRODUCCIÓN

La Secretaría de Gobernación (SEGOB) es la dependencia del Ejecutivo Federal responsable de atender el desarrollo político del país y de coadyuvar en la conducción de las relaciones del Poder Ejecutivo Federal con los otros poderes de la Unión y los demás niveles de gobierno, para fomentar la convivencia armónica, la paz social, el desarrollo y el bienestar de los mexicanos en un Estado de Derecho.[1]

MISIÓN

Tiene a su cargo el ejercicio de las atribuciones que le asignan las leyes, así como los reglamentos, decretos, acuerdos y órdenes del Presidente de los Estados Unidos Mexicanos.

VISIÓN

Ser el motor principal para que México tenga una sociedad abierta, libre, plural, informada y crítica, con una sólida cultura democrática y una amplia participación ciudadana; reconociendo que el Estado de Derecho es la única vía que permite a los mexicanos vivir en armonía.

Al frente de la SEGOB está un Secretario del Despacho, titular de la misma, quien para el desahogo de los asuntos de su competencia, se auxiliará de:

A. Los servidores públicos siguientes:

I. Subsecretario de Gobierno;

II. Subsecretario de Enlace Legislativo;

III. Subsecretario de Asuntos Jurídicos y Derechos Humanos;

IV. Subsecretario de Población, Migración y Asuntos Religiosos;

V. Subsecretario de Normatividad de Medios, y

VI. Oficial Mayor.

B. Las unidades administrativas siguientes:

I. Coordinación General de Protección Civil;

II. Unidad para el Desarrollo Político;

[1] SEGOB http://www.segob.gob.mx/es_mx/SEGOB/Mision

III. Dirección General de Comunicación Social;

IV. Unidad de Gobierno;

V. Unidad de Enlace Federal;

VI. Unidad para la Atención de las Organizaciones Sociales;

VII. Dirección General de Coordinación con Entidades Federativas;

VIII. Unidad de Enlace Legislativo;

IX. Dirección General de Estudios Legislativos;

X. Dirección General de Información Legislativa;

XI. Dirección General de Cultura Democrática y Fomento Cívico;

XII. Unidad de Asuntos Jurídicos;

XIII. Unidad para la Promoción y Defensa de los Derechos Humanos;

XIV. Dirección General de Compilación y Consulta del Orden Jurídico Nacional;

XV. Dirección General del Registro Nacional de Población e Identificación Personal;

XVI. Dirección General de Asociaciones Religiosas;

XVII. Dirección General de Radio, Televisión y Cinematografía;

XVIII. Dirección General de Medios Impresos;

XIX. Dirección General de Normatividad de Comunicación;

XX. Dirección General de Programación y Presupuesto;

XXI. Dirección General de Recursos Humanos;

XXII. Dirección General de Recursos Materiales y Servicios Generales;

XXIII. Dirección General de Tecnologías de la Información;

XXIV. Dirección General de Protección Civil, y

XXV. Dirección General para el Fondo de Desastres Naturales.

C. Los órganos administrativos desconcentrados se conforman de la siguiente manera:

- Archivo General de la Nación
- Centro de Investigación y Seguridad Nacional
- Centro de Producción de Programas Informativos Especiales
- Centro Nacional de Prevención de Desastres
- Comisión Nacional para Prevenir y Erradicar la Violencia contra las Mujeres
- Coordinación General de la Comisión Mexicana de Ayuda a Refugiados
- Instituto Nacional de Migración
- Instituto Nacional para el Federalismo y el Desarrollo Municipal
- Secretaría General del Consejo Nacional de Población
- Secretaría Técnica de la Comisión Calificadora de Publicaciones y Revistas Ilustradas
- Secretaría Técnica del Consejo de Coordinación para la Implementación del Sistema de Justicia Penal

La Secretaría cuenta con una Unidad de Contraloría Interna, Órgano Interno de Control (OIC), que depende de la Secretaría de la Función Pública encargado de promover la transparencia y el apego a la legalidad de los servidores públicos mediante la atención de quejas; denuncias y peticiones ciudadanas; realización de auditorías; resolución de procedimientos administrativos de responsabilidades y de inconformidades derivadas de procesos licitatorios; así como la recomendación de acciones de mejora relacionadas con los controles internos y operación de procesos.

En materia de administración e implementación de Tecnologías de la Información en la dependencia, se encuentra la Dirección General de Tecnologías de la Información, perteneciente a la Oficialía Mayor, área desde donde se abordará la problemática del presente trabajo, cuyas atribuciones son las siguientes:

I. Proponer políticas, normas y lineamientos en materia de informática y telecomunicaciones de observancia general a todas las unidades administrativas de la Secretaría;

II. Integrar y dar seguimiento al programa institucional de desarrollo informático y de telecomunicaciones de las unidades administrativas de la Secretaría;

III. Apoyar a los órganos administrativos desconcentrados de la Secretaría en el desarrollo e implantación de los sistemas de información;

IV. Desarrollar e instrumentar los sistemas de información de las unidades administrativas de la Secretaría;

V. Administrar y operar los servidores de cómputo, sistemas de almacenamiento central y equipos de telecomunicaciones de la Secretaría;

VI. Planear, establecer, coordinar y supervisar los sistemas de seguridad lógica de las aplicaciones y de los sistemas de transmisión de voz y datos, así como proveer de los servicios de Internet a la Secretaría;

VII. Dictaminar los estudios de viabilidad que presenten las unidades administrativas de la Secretaría, para la adquisición de bienes y servicios informáticos y de telecomunicaciones;

VIII. Participar en los procedimientos de contratación de bienes y servicios informáticos y de telecomunicaciones de la Secretaría;

IX. Coordinar el desarrollo y operación de los servicios de los medios de comunicación electrónica, intercambio y consulta de información y la operación remota de sistemas administrativos en las unidades administrativas de la Secretaría, garantizando la confidencialidad de la información y accesos autorizados a las bases de datos institucionales;

X. Fungir como Secretariado Técnico del Comité de Informática y Telecomunicaciones de la Secretaría;

XI. Planear, establecer, coordinar y supervisar los servicios de mantenimiento preventivo y correctivo de los equipos de informática y telecomunicaciones, instalados en las unidades administrativas de la Secretaría;

XII. Vigilar el cumplimiento de las garantías otorgadas por los proveedores de bienes y servicios informáticos y de telecomunicaciones adquiridos por la Secretaría;

XIII. Instalar, supervisar y garantizar la operación de las redes de telecomunicaciones instaladas en la Secretaría;

XVI. Proporcionar los medios necesarios para la transmisión de voz, información e imágenes que requieran las unidades administrativas de la Secretaría;

XVII. Analizar en forma permanente las tecnologías de punta en materia de informática y de telecomunicaciones, para su eventual aplicación en la Secretaría;

XVIII. Ser el enlace de la Secretaría con dependencias, entidades, instituciones y empresas tanto nacionales como internacionales relacionadas con la informática y las telecomunicaciones;

XIX Coordinar, apoyar y supervisar los servicios en materia de informática y telecomunicaciones, de las entidades del sector coordinado, cuando éstas así lo requieran al Oficial Mayor.

Se ha organizado la presentación de este caso práctico en tres capítulos, previamente se expone el marco teórico y la problemática de la Institución con su servicio de Internet; los capítulos constituyen el análisis, implementación y solución de la problemática. Se procede a exponer de forma sintética el contenido de los capítulos que conforman este trabajo para que el lector pueda realizarse una primera representación mental del mismo.

Marco Teórico

En este apartado se muestra la perspectiva de la Secretaría de Gobernación ante la evolución y el crecimiento de la Web y las prioridades de la institución en lo que a Seguridad Lógica se refiere.

Problemática

En este capítulo, partiendo de las deficiencias en infraestructura y servicios, se expondrán los riesgos que hicieron necesaria la modernización y protección de los servicios de Internet para la Secretaria de Gobernación, ante la navegación libre y sin protección que existía al interior.

Marco Referencial del Servicio de Internet de la Secretaría de Gobernación

Para comprender la problemática que enfrentaba la Secretaría de Gobernación, durante este capítulo se exponen las características de la infraestructura anterior en la dependencia con la que se proveía el servicio de Internet, así como la dinámica de operación en el área.

Capítulo 1 "Análisis de las opciones y elección de la solución"

En este apartado se analizaran las opciones disponibles para solventar la problemática que enfrenta la Secretaría de Gobernación respecto a su servicio de Internet y la modernización de la infraestructura del mismo.

Capítulo 2 "Implementación de la Solución 8e6"

En este capítulo se muestra como fue implementada la solución que ayudó a resolver la problemática con la navegación en la web; así como la adquisición de la nueva infraestructura.

Capítulo 3 "Pruebas y Adecuación de la Solución 8e6 a las condiciones imprevistas"

En este capítulo se detallan las pruebas de funcionalidad realizadas a la solución de los equipos 8e6 ya implementados en la Red de la SEGOB, asimismo se da a conocer los resultados mediante la operación diaria.

Conclusión

En este apartado se plasmará si las mejoras implementadas cubrieron las necesidades en materia de seguridad, así como los beneficios logrados para la dependencia.

MARCO TEÓRICO

Actualmente las administraciones Públicas se enfrentan a varios problemas complejos, en los que destacan los requisitos de Tecnologías de la Información (TI).

Internamente, las políticas se deben aplicar, procurando cumplir con las normas, pero de una manera que no inhiba o bloquee el servicio y los accesos que requiera el usuario para sus tareas desempeñadas. Es un reto difícil, por las distintas naturalezas de las áreas y sus actividades, así que realizar una segmentación en el servicio sin considerarlas, puede beneficiar a un área y perjudicar a otra. Pero, sin estas medidas de control, un uso indebido del internet por parte de los usuarios de SEGOB podría ser sujeto al escrutinio público, mermando la credibilidad institucional de no cumplirse con las normas que regulan el acceso a la Web.

Desde esta perspectiva, las prioridades de la Secretaría de Gobernación en lo que a Seguridad Lógica se refiere cuya operación y atención recaen en la Dirección General de Tecnologías de la Información son:

- Protección frente a aplicaciones complejas y cada vez más sofisticadas.
- Amenazas de seguridad cibernética como bots / botnets, virus, spyware, malware, phishing, anonimizadores Proxy, ataques a la red.
- Hacer cumplir las políticas de uso de los recursos informáticos de manera aceptable.
- Maximizar la productividad de los empleados, facilitándoles la información que requieren.
- Prevención de fugas de información.
- Asegurar el cumplimiento normativo (en los Estados Unidos, la Federal Información Security Management Act, o FISMA) como practicas aceptadas de seguridad.
- Mitigación de exposición a responsabilidades legales.
- Preservar y optimizar el ancho de banda de red.

PLANTEAMIENTO DEL PROBLEMA

La Modernización y Protección de los servicios de Internet para la Secretaría de Gobernación surge de la necesidad de proteger la información de la institución, ya que al ser el órgano encargado de atender el desarrollo político del país y de coadyuvar en la conducción de las relaciones del Poder Ejecutivo Federal con los otros poderes de la Unión y de los demás niveles de gobierno, el hurto de la información o ataques informáticos podría ocasionar consecuencias de inestabilidad política y desorden social.

En lo que compete a las atribuciones de la Secretaría de Gobernación, desde 2008 se han hecho esfuerzos para controlar el acceso a Internet con el que cuentan los empleados, usuarios y proveedores de la RED de la Secretaría, para proteger la información y asegurar la operación diaria.

Dichos esfuerzos han abarcado desde la modernización de la infraestructura, ya que no se contaba equipos de seguridad de filtrado de contenido Web, hasta de carácter normativo, mismo que da marco para establecer los lineamientos de operación y uso del acceso a Internet, dando pauta al establecimiento de una política sobre Tecnologías de la Información y las Comunicaciones al interior de la dependencia.

A continuación se describirán las problemáticas existentes antes de la implementación de las mejoras en materia de Tecnologías de la Información en la Secretaría de Gobernación.

POLÍTICAS DE NAVEGACIÓN OBSOLETAS

Los permisos para este recurso estaban controlados a través de las políticas en el Reglamento Interno publicado por el Diario Oficial de la Federación el 9 de marzo de 2000 y los Proxys Squid, los cuales operaban desde el año 2001; sin embargo era necesario actualizar los lineamientos de navegación adaptándolos a las nuevas necesidades y a la evolución del Internet para evitar el consumo de páginas web con contenidos inapropiados como chats, ocio, con posibles virus, etc.

Uno de principales obstáculos, como se mencionó, eran lineamientos de navegación obsoletos que no respondían a las atribuciones de la Dirección General de Tecnologías de la Información en cuanto a la importancia de observar la nueva dinámica y crecimiento de la web como un componente estratégico, así como para establecer parámetros para el acceso a contenidos y protección de información de la dependencia.

Reglamento de navegación de 2000 a 2008

Los usuarios ubicados en edificios que ya se encuentran incorporados a la Red Metropolitana de la Secretaria, deberán utilizar la conexión a Internet que ofrece la Red Internet. El acceso a Internet mediante servicio “Dial Up” o el uso de módem para acceso a aplicaciones de cómputo e Internet, se realizará bajo la autorización de la Dirección General de Tecnologías de la Información, previa solicitud y análisis de su uso.

Para el acceso remoto a la red de la SEGOB se cuenta con los servicios de usuarios móviles y usuarios permanentes fijos, mismos que pueden solicitarse a través del CAT (Centro de Atención Técnica).

El servicio de Acceso Remoto debe ser instalado en equipos propiedad de la SEGOB designados a funcionarios de la Secretaria, por lo que la instalación de software de autentificación remota a aquellos equipos que no permanezcan a la Secretaria, requerirá de la autorización por escrito de la Dirección de Servicios de la DGTI.

Cuando se termine el lapso solicitado para el servicio de acceso remoto, la DGTI será la encargada de desinstalar el software que respalda el servicio y será obligación del usuario, notificar dicha terminación.

Queda prohibida la consulta de cuentas de correo electrónico personal utilizando el servicio de Internet Institucional.

No se permite el tráfico de Web “http” directo, es decir todas las computadoras que integran la Red de la Secretaria deben de transitar por un punto central, “El Servidor Proxy”.[2]

Resultaba tarea difícil proteger diferentes frentes cuando los servidores públicos y usuarios no tenían consciencia de que podrían ser objeto de algún tipo de fraude u hostigamiento al navegar en páginas no seguras. Sin embargo, es muy común que el usuario solicite permisos para acceder libremente a la web, sin entender

[2] Un servidor proxy es un equipo intermediario entre el usuario e Internet. Puede utilizarse para registrar el uso de Internet y también para bloquear el acceso a una sede Web.

que puede ser flanco de una infinidad de amenazas; la menos graves quizás virus y spyware o backdoors, las más graves tal vez fraudes en sus cuentas de banco o robos de identidad.

El control sobre las visitas a sitios no autorizados se complicaba más cuando el usuario en su afán de libertad, incurría en prácticas ilegales desde la RED de la SEGOB, como descargas de: software, música, obras literarias, películas, imágenes, video, etc., con derechos de Autor. Hasta el momento no se han presentado quejas por Derechos de Autor ante la dependencia, por ello las nuevas políticas e infraestructura abonan para evitar riesgos de esta naturaleza.

El establecimiento de nuevas políticas responde a la necesidad de tener un mayor control respecto a la navegación. Desde luego todo acceso a la web está permitido en los parámetros de operación y utilización razonables y racionales de la SEGOB para cumplir con sus actividades, por lo que aquello que es ilegal, que representa un riesgo, viola los derechos de otros o no compete a las atribuciones del trabajo de la Unidad Responsable, no podrá ser visitado.

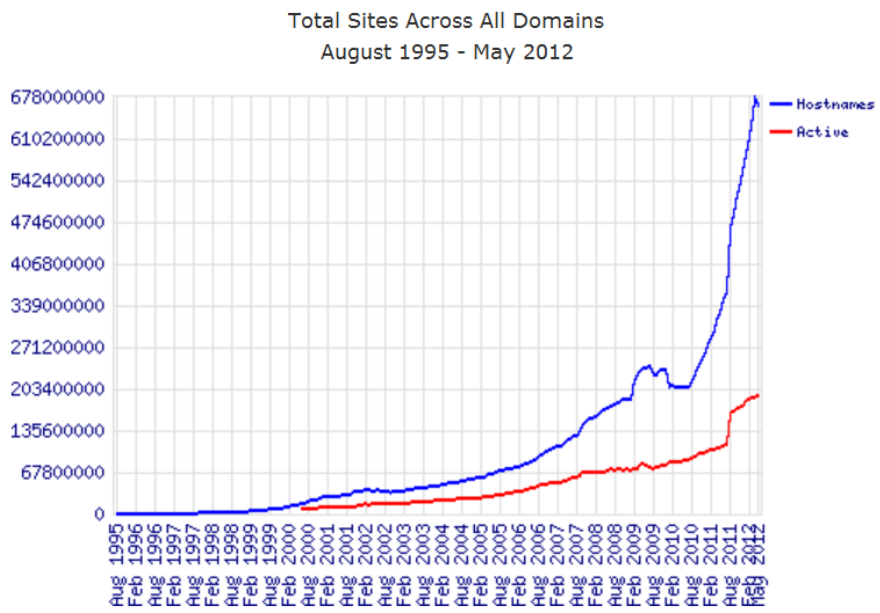
INFRAESTRUCTURA OBSOLETA

Toda la infraestructura con la que operaba la SEGOB para proveer el servicio de Internet funcionaba sobre computadoras personales PC´s (éstas no contaban con características de servidor, tales como: fuentes de poder redundantes, discos duros de alta velocidad, arreglos de discos para protección de la información, etc.), incapaces de soportar el tráfico en la red ocasionada por la demanda de los usuarios.

CRECIMIENTO DE INTERNET

Con el desenfrenado crecimiento de la web con casi 204 millones de sitios de Internet, de acuerdo con un estudio de Netcraft[3] hasta febrero de 2012 -16% más con respecto al año anterior-, resultaba imposible mantener el control de acceso a páginas inadecuadas para los usuarios, ya que la negación de acceso a las mismas se realizaba dando de alta cada sitio en los Proxys.

[3] http://news.netcraft.com/ (Investigación de Internet, Anti-phishing y Servicios de Seguridad)



Gráfica 1.0 Crecimiento de la WEB

Como se puede apreciar en la gráfica el incremento de Sitios Webs activos (línea roja) fue el siguiente:

AÑO	SITIOS	PORCENTAJE	% ACUMULADO
2009	68 millones	0%	-----
2010	80 millones	17%	-----
2011	136 millones	70%	-----
2012	204 millones	50%	300%

Tabla 1.0 Crecimiento de la WEB 2009-2012

Tomando como referencia del año 2009 a la fecha (incremento anual).

Es decir se veía rebasado el número de páginas a filtrar ante el surgimiento diario de nuevas, por lo que el reto para el equipo de seguridad (Proxy) era mayúsculo o imposible de cumplir porque cada una se tenía que agregar manualmente.

Cabe mencionar que la constante creación de páginas web trae consigo un incremento sustancial en la publicación de materiales ilegales como: Pornografía infantil, Terrorismo, Sitios de Fraudes, Sitios de Armas, Publicación de Material con Derechos de Autor, Discriminación y Racismo, Violencia, Phishing, Hacking y Cracking, entre otros.

CRECIMIENTO DE LAS UNIDADES ADMINISTRATIVAS DENTRO DE LA SEGOB

Ante la ampliación de las atribuciones de la SEGOB, con la absorción de nuevas unidades administrativas y órganos desconcentrados, tales como la Comisión Nacional para Prevenir y Erradicar la Violencia contra las Mujeres (CONAVIM, 2009) y el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública y (SESNSP 2009), por mandato presidencial para que la SEGOB encabezara los trabajos del Consejo Nacional de Seguridad Pública, se ha generado un crecimiento importante en el número de usuarios de Internet en la dependencia, además del aumento en otras áreas ya existentes.

FALLAS EN EL SERVICIO DE INTERNET

Las fallas en el servicio Internet son reportadas por el usuario a través de una mesa de servicio la cual envía los reportes a los correo electrónico de los encargados del área con un tiempo de respuesta de no más de dos horas; Una vez concluido el reporte, las actividades realizadas tenían que registrarse en el sistema que administra los tickets de la mesa, en este caso footprints.

Entre las fallas más comunes que se presentaban en el día a día iban desde lentitud para navegar, intermitencias hasta pérdida del servicio.

El número de reportes de falla de Internet era tan alto (60 a 100 reportes por día) que con el poco personal del área conformada por 2 personas y con los equipos Proxy Squid era casi imposible resolverlos. Dicha situación originaba que el personal no pudiera invertir tiempo en otras actividades propias del área de Seguridad Lógica, entre las que destacan actividades gerenciales y de estrategia (encaminadas a la mejora y a la innovación de procesos y de infraestructura que ayudara a completar los ciclos de renovación tecnológica).

En numerosas ocasiones se caía el servicio debido a:

Fallas del Firewall con las múltiples peticiones que tenía al no ser un equipo de propósito específico, ya que era una PC con software de servidor firewall Iptables. Las interfaces de red se bloqueaban, este equipo era punto sensible de falla, al no tener redundancia todo el servicio de Internet se veía interrumpido.

Fallas en los Proxys debido a la saturación de memoria y bloqueo de las interfaces de red.

Fallas en el Balanceador (bloqueo de las interfaces de red y de sincronización en el algoritmo de balanceo).

Fallas en los en los enlaces y equipos de comunicación del proveedor del servicio de Internet, dicho punto era responsabilidad del proveedor del servicio en la SEGOB (AXTEL).

LENTITUD CON EL SERVICIO DE VPN (Red Virtual Privada)

En la salida principal a Internet ubicada en Bucareli se encuentra nuestro servicio de VPN (Red Virtual Privada), el cual permite la conexión desde el exterior a la RED de SEGOB. Ésta presentaba lentitud para acceder a ella lo que generaba un problema para algunos de los webmasters, ya que a través de dicho servicio se actualiza información de casi 100 portales web publicados en Internet.

EQUIPOS SIN SOPORTE

Los Proxys no contaban con soporte ya que tenían software OPEN SOURCE (squid)[4], estaban instalados sobre PC´s, sin manuales o líneas telefónicas de soporte técnico que facilitaran recuperar el servicio de Internet en caso de perderlo.

ANCHO DE BANDA LIMITADO

Con nuestros más de 6,000 usuarios de Internet distribuidos en dos enlaces:

Bucareli abasteciendo a un total de 7 edificios y Reforma abasteciendo a un total de 12 edificios

Cada enlace de Internet tenía una capacidad de 5 Megabytes, lo que quiere decir que el ancho de banda estaba limitado respecto a la cantidad de usuarios, circunstancia que propiciaba que el servicio de Internet fuera ineficiente para la institución.

BAJA SUPERVISIÓN

Dada la necesidad de intercomunicación entre las dependencias gubernamentales, el 85 por ciento de los trabajadores requiere conexión a Internet, por lo que crece la importancia de supervisar los sitios y las actividades que desarrollan en su tiempo laboral para asegurar que esas visitas sean utilizadas para el desarrollo de las actividades de la dependencia.

El registro de los Proxys, alimentado de forma manual, no permitía tener un control de los sitios a los que accedían los usuarios, por lo que era imposible para el área de Seguridad identificar quién incurría en una navegación inadecuada o detectar prácticas ilegales con la herramienta.

[4] http://www.telecom.segob/pac y http://proxy2.segob.gob.mx

Además la supervisión era nula puesto que los Proxys no alertaban ni detenían al usuario en caso de estar haciendo mal uso de Internet.

Se tenían quejas recurrentes de algunos mandos altos quienes reportaban usos indebidos de la web por parte de sus subordinados para cuestiones personales u ocio, por lo que solicitaban a la Dirección de Tecnología de la Información denegar el acceso a dichos sitios e incluso algunas veces requerían se les proporcionaran reportes para apreciar los sitios a los que ingresaban los usuarios observados, pedimentos que no se podían cumplir por ausencia de una herramienta para ello.

APARICIÓN DE NUEVOS SERVICIOS EN INTERNET

Hasta el año 2008 el chat en sus diferentes modalidades (Internet Relay Chat, Salas de chat montadas en páginas web, MSN, etc.) era la forma más popular de comunicación en Internet, por lo que los usuarios de la SEGOB invertían mucho tiempo en esta actividad.

El acceso al servicio de chat se administraba mediante los Proxys.

El boom de YouTube con sus innovaciones de contenidos multimedia, la creciente difusión de videos y películas, el auge del nuevo chat con VIDEO (video llamadas, video conferencias), la aparición de nuevas redes sociales y los juegos en Internet con participantes en diferentes lugares del mundo, ocasionaron que se incrementara exponencialmente el número de servicios a administrar en la RED de SEGOB.

JUSTIFICACIÓN

Al utilizar Internet como herramienta de comunicación entre las dependencias gubernamentales y el exterior, permitiendo una mayor accesibilidad a la información y los servicios mediante la publicación de Sitios Web pertenecientes a la Institución, se deben tomar en cuenta muchos factores a considerar para el correcto y seguro funcionamiento del servicio, para la alta disponibilidad, el resguardo y protección de la información y el usuario, así como para prevenir la pérdida de tiempo o el uso indebido del servicio de Internet de la Secretaria de Gobernación.

El proyecto de Modernización y Protección de los Servicios de Internet surge de la necesidad de corregir y mejorar deficiencias en el servicio, a través del diagnostico de los problemas más frecuentes para su corrección, así como en la infraestructura disponible, para, a partir de él, visualizar la implementación de una

herramienta que solucionara de manera eficiente y transparente los conflictos existentes, sin arriesgar la seguridad de la institución.

Una vez realizado el análisis de las mejoras por el departamento de Seguridad Lógica, había que considerar el factor económico para sujetar la viabilidad del proyecto de acuerdo al presupuesto disponible, así como observar los lineamientos para la obtención de nuevo equipo y cambio de la infraestructura de la institución.

Las principales mejoras de este proyecto son las siguientes:

- Brindar niveles de navegación óptima y segura de Internet a los más de 8,000 usuarios de la Secretaria de Gobernación, para mejorar la transferencia de la información, ya que se recibían muchos reportes donde el usuario se quejaba de lentitud en la navegación, intermitencias o falta del servicio, que entorpecía la realización de su trabajo.
- Reducir el riesgo en interrupciones del servicio de Internet por cortes de energía, falla de hardware y actualizaciones del sistema, a través del nuevo equipo con software licenciado y pólizas de mantenimiento.
- Otro beneficio es que se podrá dividir a los usuarios en grupos con los privilegios para el acceso a Internet que cada área requiera, así se disminuirán los tiempos de respuesta en la atención a fallas, ya que será más fácil identificar el problema y determinar la solución.

OBJETIVO GENERAL

Modernizar y Proteger los Servicios de Internet en la Secretaria de Gobernación para asegurar la disponibilidad del servicio y para proteger la información que se genera dentro de la Institución y aquella que se comparte con otras dependencias del gobierno federal.

Lo anterior implica proveer a la Secretaría de un instrumento que funcione en perfectas condiciones, en el que se puedan realizar cambios en el servicio de Internet de manera transparente para el usuario, con la certeza de que se contará con soporte de mantenimiento para mitigar fallas del servicio, así como con toda la documentación de la infraestructura implementada para consulta de futuras generaciones.

Además contribuirá a reducir riesgos provenientes de la navegación inadecuada, al impedir que los usuarios en su afán de libertad para navegar podrían incurran en prácticas ilegales desde la RED de la SEGOB, a través de descargas de material como: software, música, obras literarias, películas, imágenes, video, etc., protegidos derechos de autor. Afortunadamente no se han presentado quejas por parte de los dueños de esos derechos hacia la SEGOB, pero no se debe esperar a que este riesgo se presente.

OBJETIVOS ESPECÍFICOS

- Análisis del esquema de Internet actual.
- Investigación de mercado para definir la solución más viable para resolver la problemática.
- Elaboración del plan de trabajo para la modernización del servicio de Internet.
- Medir impacto del cambio.
- Realizar la traducción de las políticas y reglas de filtrado de los equipos actuales a los nuevos.
- Migración del esquema anterior a la nueva infraestructura.
- Modernizar los servicios de Internet que brinda la Secretaria de Gobernación para obtener mejoras en el servicio y proveer a los usuarios de una navegación segura, así como la alta disponibilidad de los portales web de la Secretaria.
- Monitorear el uso de los servicios y recursos de Internet que provee la Secretaría de Gobernación.

MARCO REFERENCIAL DEL SERVICIO DE INTERNET DE LA SECRETARIA DE GOBERNACION

Para el cumplimiento de las funciones de la Secretaría de Gobernación en un contexto donde las tecnologías de la información se convierten en un elemento importante para la consulta e intercambio de información, la implementación del servicio, por atribución, corre a cargo de la Dirección General de Tecnologías de la Información.

Para entender la importancia del Internet en la Secretaria de Gobernación en el contexto actual , es trascendente conocer el número de edificios a los que se proporcionaba el servicio, ya que al contar con acceso a la web, el envió y recepción de información a través del correo electrónico institucional o la consulta de información en los sitios web, permite la interacción entre las Unidades Administrativas de la dependencia, lo que ayuda a reducir tiempos de respuesta y agiliza la operación en sus actividades sustantivas, ya sea dentro del conjunto Bucareli o en las áreas que están ubicadas en otros edificios.

Además de sus oficinas centrales ubicadas en Abraham González No.48, colonia Juárez, delegación Cuauhtémoc, (Conjunto Bucareli) y su edificio corporativo ubicado en Avenida Reforma 99, ambas en el Distrito Federal; En 2008 la SEGOB contaba con 15 edificios para albergar a las distintas áreas que la conforman.

El número de usuarios de Internet era de más de 6,000, servicio que se proveía a través de dos salidas como se muestra en el siguiente diagrama:

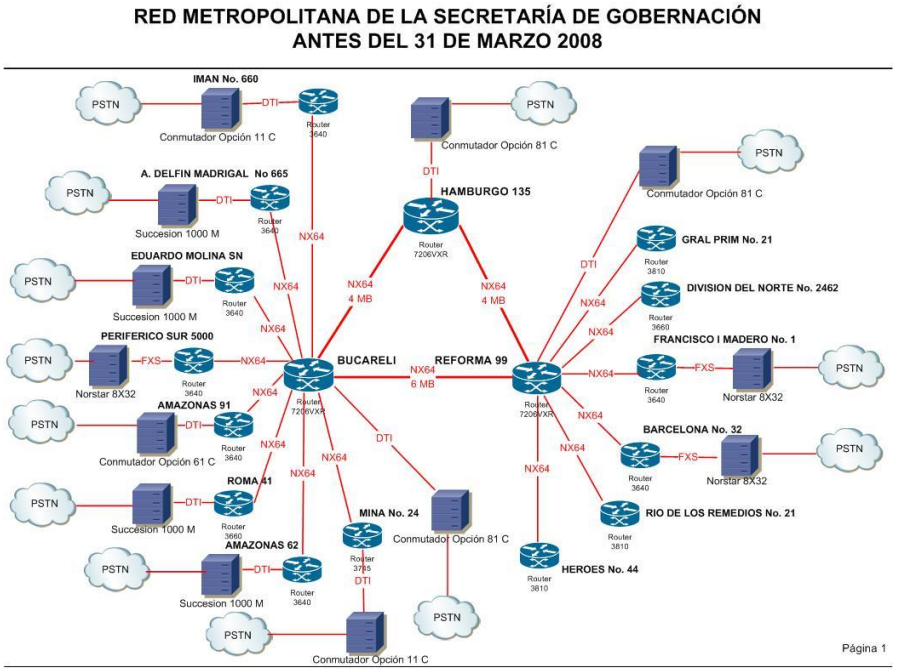


Diagrama 1.0 Red Metropolitana de la SEGOB al 31/03/2008

La distribución de la Red metropolitana de la Secretaría de Gobernación, antes del 31 de marzo de 2008, tenía dos enlaces ubicados en el edificio de Reforma 99 con un E1 y Bucareli con dos E1, proveídos por el operador de TELECOM AVANTEL.

En el siguiente diagrama se describe enlace de Internet de Bucareli y Reforma 99:

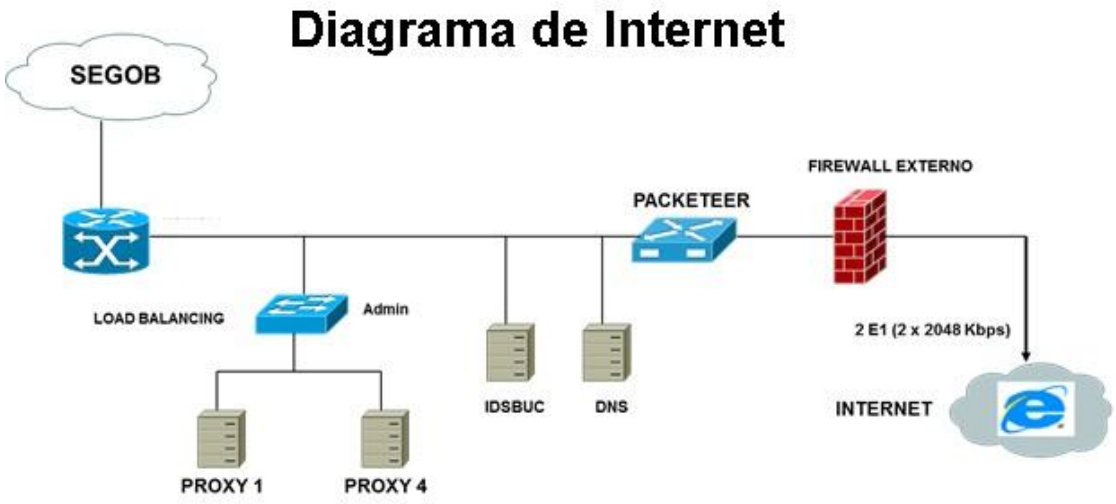


Diagrama 2.0 Esquema de Internet de la SEGOB 2008

Características técnicas de los equipos:

- **Router 2800** Cisco (2 interfaces de E1´s).
- **Firewall HP Proliant ML350** con 4 procesadores Intel Xeon, memoria RAM de 2 GB, Disco Duro de 135 GB, 2 interfaces de red.
- Dispositivo de control de tráfico **Packeteer** series 2500.
- **DNS HP Proliant ML350** con 4 procesadores Intel Xeon, memoria RAM de 2 GB, Disco Duro de 135 GB, 2 interfaces de red.
- **Balanceador** de tráfico para la salida de Internet Alteon AD4
- **Servidores Proxy 1 y 4 Proliant** ML350 con 4 procesadores Intel Xeon, memoria RAM de 2 GB, Disco Duro de 135 GB, 2 interfaces de red.
- **Router 7200** para distribución de la salida de Internet para todos los usuarios de la red interna.

Las funciones realizadas por los equipos:

Router 2800 Cisco (2 interfaces de E1´s)

Este equipo era proporcionado por el proveedor de servicios, las puntas de entrada eran 2 interfaces G703 (BNC´s), cuya salida de Internet se daba a través de un cable RJ45, balanceado con los 2 E1´s (4096 KB), conectado a la entrada de la interfaz del Firewall.

Firewall HP Proliant ML350

Con 4 procesadores Intel Xeon, memoria RAM de 2 GB, Disco Duro de 135 GB, 2 interfaces de red, este firewall estaba configurado con software libre Linux Mandrake reléase 10.1, cuya función consistía en detener ataques de DOS, Spoofing, Spyware, aplicaciones como P2P.

Interfaces de Red

Dos interfaces para configurar la red externa (Internet) y la red Interna. Para la red externa se configuraban direcciones IP virtuales para proporcionar servicios de entrada o salida desde Internet.

Para la salida de Internet, en el firewall se configuraba los DNS´s del proveedor de servicios y de la red interna.

Scripts de Reinicio

Mediante el uso de scripts se ejecutaban permisos de rutas estáticas, reglas de firewall, bloqueo o acceso a aplicaciones desde Internet tales como FTP´s, servidores con puerto distinto al 80, 443 etc. Se usaban scripts, ya que si se tenía una descarga eléctrica o interrupción de energía eléctrica, el servidor tendría que reiniciarse.

Packeteer serie 2500

Su función consistía en reportar el tráfico que se tenía durante el día, así como también dar estadísticas por día, semana, mes y año de las páginas consultadas. Además, los ataques de virus que se tenían y otras navegaciones maliciosas por Internet.

Servidores Proxy

Servidores Proxy 1 y 4 Proliant ML350 con 4 procesadores Intel Xeon, memoria RAM de 2 GB, Disco Duro de 135 GB, 2 interfaces de red.

Los servidores Proxy estaba configurado con software libre Linux Mandrake reléase 10.1, mediante el software SQUID STABLE, cuya función básica consistía en proporcionar el servicio de Internet mediante caché, es decir una vez consultada una página, éste la guardaba y se la proporcionaba a otro usuario que la requiera, sin necesidad de realizar una nueva búsqueda.

Además el Proxy filtraba el contenido como páginas de juegos, contenido para adultos y bloqueaba el acceso a Internet a los usuarios, así como correos externos, Chat y/o Messenger y descargas de material con derecho de autor.

Partiendo del diagrama que muestra la conexión para Internet de la SEGOB, funcionaba de la siguiente manera: toda la información electrónica entraba a través del router capaz de direccionar los paquetes de datos hacia el switch alteon, que hacía un balance de todo el tráfico proveniente de la navegación de los usuarios, dividiéndolo en 2 partes y distribuyéndolo hacia los dos Proxys.

En el switch Alteon se configuraba la dirección IP virtual 10.2.2.249, teniendo como IP real la 10.2.3.100. Lo que hacía el switch era un address translation, es decir balancear el tráfico y entregarle la posibilidad de permitir o denegar la navegación a Internet a los Proxys (1 y 4).

Para que los usuarios pudieran navegar en Internet era necesario que tuvieran en su navegador la configuración de la IP virtual del Proxy; como se muestra en la imagen:

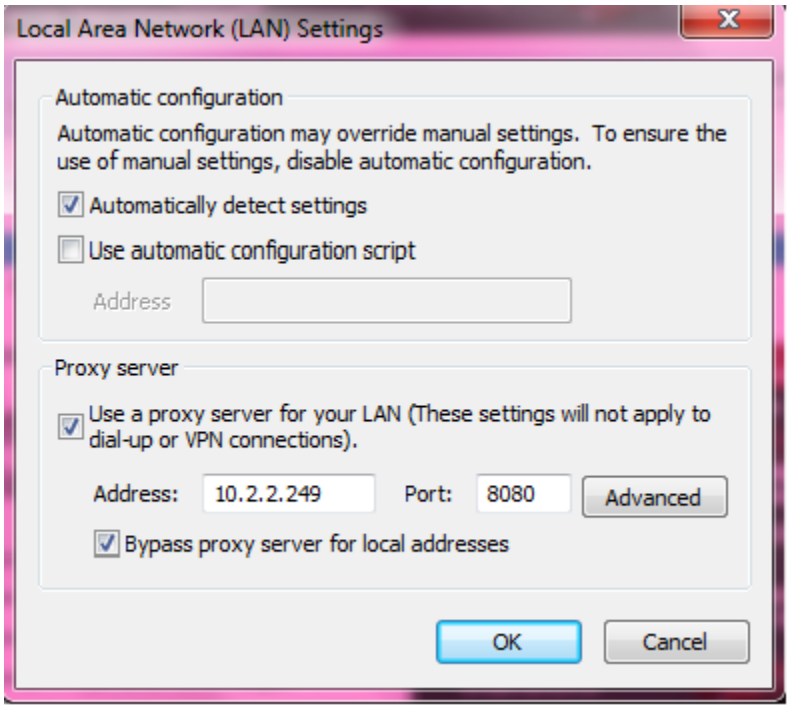


Imagen 1.0 Configuración de PROXY

Esta configuración era indispensable para que el usuario navegara por Internet. Como se visualiza la dirección IP del navegador era la 10.2.2.249, (IP virtual de los servidores Proxy).

La dirección virtual de la IP respondía a la necesidad de contener ataques informáticos y por lo tanto, que el atacante no conociera direcciones IP's reales de cada dispositivo involucrado en el diagrama de Internet.

Los servidores Proxy hacían la función de cachés y filtradores de contenido web, mediante la configuración del squid caché. En este punto se definían los privilegios de navegación de los usuarios de la SEGOB, entre los que desacataban solicitudes para acceder a chat, sitios de música, juegos y video.

En el Proxy se ejecutaba el comando tail –xvzf /var/log/squid/access.log para ver en tiempo real la navegación de los usuarios y conocer los sitios web a los que ingresaban; con el propósito de detectar si alguno estaba haciendo uso indebido de Internet.

Para filtrar los contenidos no deseados de las URL´s se implementaban las siguientes acciones:

Con la información resultante de access.log el área de seguridad revisaba cada URL visitada, consultando una por una en el navegador para poder categorizarlas.

Al categorizar cada URL´s, se escribían las que debían ser denegadas dentro de un archivo en el Proxy.

En los servidores Proxy no se catalogaba el tráfico por Unidades Administrativas, por tal motivo cada usuario tenía navegación libre; por ejemplo un usuario de la Unidad Asuntos Jurídicos podía tener las mismas opciones de navegación que uno de la Unidad de Comunicación Social, aunque el primero por sus necesidades, no requiere una navegación con accesos a chat, video, juegos; sin embargo el segundo, por sus funciones y necesidades de comunicación sí requería del servicio de chat o video.

Cabe destacar que aunque se tenía conocimiento del uso indebido de Internet era difícil detectar al usuario que incurría en esta práctica, debido a que no se tenía un registro confiable de IP´s; además dicho comportamiento sólo se podía apreciar al consultar en tiempo real los logs del Proxy.

Con el uso de los Proxy´s únicamente se tenían dos grupos de autorización para la navegación:

1. Permitir correos y Chats
2. Permitir todas aplicaciones y todas las páginas web

CONFIGURACIÓN DEL PROXY

Los principales parámetros de configuración del Proxy con los que operaba la SEGOB son los siguientes:

A continuación se muestra el contenido del archivo raíz “Squid.conf” que definía todos los parámetros de configuración tales como el puerto de navegación del Proxy, el tamaño de la memoria cache, nombre de los directorios, scripts de reinicio, entre otros.

```
#  WELCOME TO SQUID 2

# NETWORK OPTIONS

  http_port 8080

# OPTIONS WHICH AFFECT THE CACHE SIZE

cache_mem  1500 MB

maximum_object_size 8000 KB

# LOGFILE PATHNAMES AND CACHE DIRECTORIES

cache_dir ufs /var/spool/squid 25000 16 256

cache_access_log /var/log/squid/access.log

cache_log /var/log/squid/cache.log

cache_store_log none

mime_table /usr/local/squid-2.5.STABLE6/etc/

pid_filename /var/run/squid.pid

# ACCESS CONTROLS

acl aclname myport   3128 ...          # (local socket TCP port)

acl all src 0.0.0.0/0.0.0.0

acl getonly method GET

acl segob src 10.0.0.0/8 172.16.0.0/16 192.168.0.0/16

acl manager proto cache_object

acl localhost src 127.0.0.1/255.255.255.255
```

```
# Acceso a toda las páginas web

acl sinrestricciones src "/usr/local/squid-2.5.STABLE6/etc/Ipsinrestric

# Bloqueo Spyware

acl Spyware dstdomain .gator.com ad.doubleclick.net ad.mx.doubleclick.net .yesky.com

# (Debido a que los sitios que se tenían bloqueados para spyware eran 4, no era necesario generar un archivo, ya que se colocaban directamente en el acl).

# Bloqueo a correos

acl Mail dstdomain "/usr/local/squid-2.5.STABLE6/etc/CorreoExterno

#  (En el archivo “CorreoExterno” se agregaban todas aquellas páginas de mail no institucional).

# Bloqueo a Chat´s

acl Chat dstdomain "/usr/local/squid-2.5.STABLE6/etc/ChatExterno

# (En el archivo “ChatExterno” se agregaban todas aquellas páginas de donde se podía descargar MSN y las páginas de chats).

# Bloqueo a Juegos en línea

acl Juegos dstdomain "/usr/local/squid-2.5.STABLE6/etc/JuegosExterno"

# (En el archivo “JuegosExterno” se incluían todas aquellas páginas con categoría de juegos).

# Bloqueo de contenido para adulto.

acl Porn dstdomain "/usr/local/squid-2.5.STABLE6/etc/PornoExterno"

# Para bloquear los contenidos con categoría de pornografía, se agregaban todas aquellas páginas  en el archivo “PornoExterno”).

# Bloqueo de descargas y música en línea

acl Music dstdomain "/usr/local/squid-2.5.STABLE6/etc/MusicaExterna"

# (En el archivo “MusicaExterna” se agregaban todas aquellas páginas con categoría de descarga y reproducción de música).

# Bloqueo de P2P

acl PeertoPeer dstdomain "/usr/local/squid-2.5.STABLE6/etc/P2P"

# (En el archivo P2P se agregaban todas aquellas páginas con categoría de compartición de archivos).
```

Bloqueo de Páginas por el Puerto 443.

acl Port443 dstdomain "/usr/local/squid-2.5.STABLE6/etc/Pagesport443"

(En el archivo “Pagesport443” se agregaban todas aquellas páginas cuya publicación era por el puerto 443).

acl CONNECT method CONNECT (con este ACL se utiliza el método connect , como lo dice el nombre conecta acl´s involucrados y mencionados en el script).

“deny” (Con la siguiente configuración se denegaba el acceso a Spyware, Chat, Juegos, Pornografía, Descargas de música y PeertoPeer basándose en los archivos de los acl’s previamente mencionados).

http_access deny Spyware

http_access deny Chat

http_access deny Juegos

http_access deny Porn

http_access deny Music

http_access deny PeertoPeer

“SINRESTRICCIONES” En dicho grupo se encontraban todas las Ips que tenían permitido la consulta de correos externos como Hotmail, Gmail, Yahoo, etc. y Chats.

http_access allow sinrestricciones

http_access deny Mail (En esta sección se restringe el acceso a correos externos y chat a toda aquella Ip que no cuente con dicha autorización)

http_access allow Port443 (Se permiten las páginas 443 incluidas en el archivo “Pagesport443”

http_access deny SSL_ports (Se restringen las páginas publicadas por el Puerto 443 que no se encuentren en el archivo anterior)

“SEGOB” Era el grupo de ip´s que tenían navegación completamente libre, es decir no estaban sujetas a ninguna restricción.

http_access allow segob

http_access deny all (aquí es donde se deniega todo para los usuarios que no tienen permiso para ciertas páginas).

NOTA: Las páginas que se agregaban a los diferentes archivos mencionados eran únicamente las que se conocían u obtenían de la revisión de los logs del Proxy.

CAPÍTULO 1. ANÁLISIS DE LAS OPCIONES Y ELECCIÓN DE LA SOLUCIÓN

Actualmente la Secretaria de Gobernación cuenta con 21 edificios albergando sus distintas áreas y proveyendo del servicio de Internet a más de 8000 usuarios, a través de 2 enlaces de Internet de 100 Mbps cada uno; ubicados en Reforma y Bucareli proveídos por el operador de TELECOM METRONET.

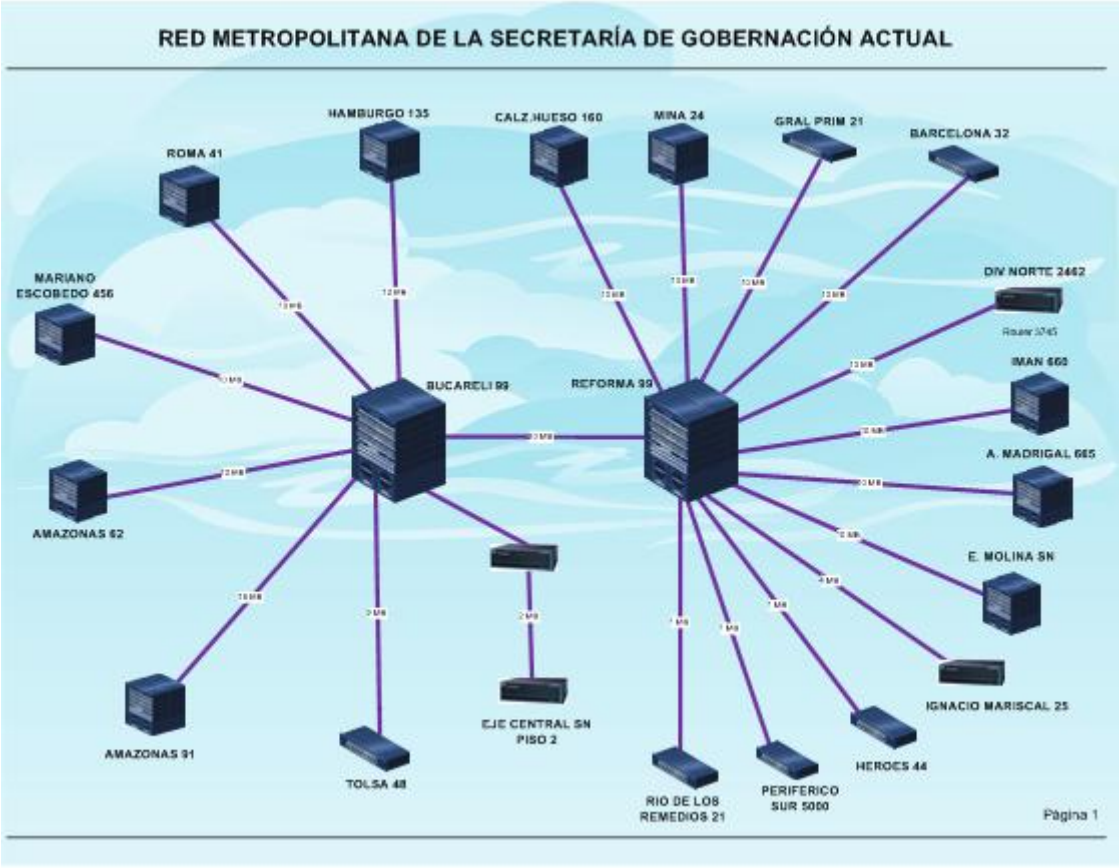


Diagrama 3.0 Red Metropolitana de la SEGOB Actual

1.1 ANALISIS DE LA SOLUCIÓN

Con el propósito de dar solución a los problemas suscitados con el servicio de internet de la Secretaría de Gobernación y con la intención de dimensionar nuevos retos en el camino, como Proxys anónimos, boom de redes sociales y otros trucos que son diseñados continuamente para evitar el filtrado de contenido, se pensó en una solución de Filtrado para Internet debido a que este tipo de soluciones tiene cuatro objetivos simples, los cuales atacan de manera directa nuestra problemática:

1. Reducir las responsabilidades jurídicas debido a sitios Web inapropiados.

   La solución provee una administración con una herramienta capaz de hacer cumplir las políticas de la empresa, evitando daños y responsabilidad legal debido a acoso sexual y comportamientos inapropiados dentro de la ley.

2. Eliminar distracciones en Internet y así incrementar la productividad de los usuarios.

   Al administrar accesos de usuarios finales a Internet se evita perdida de tiempo en sitios no autorizados como, Mensajería instantánea, Redes sociales, Peer to Peer, etc.

   Ofrece libre de mantenimiento para proyectos de misión crítica, en lugar de ingresar constantemente información en el firewall o Proxy.

3. Proteger la Red de amenazas debido a los servicios y aplicaciones usadas en Internet.

   Lo anterior asegura la confidencialidad de la información contra el spyware y phishing.

4. Preservar los recursos de la Red.

   Limita el acceso a sitios de alto consumo de ancho de banda, manteniendo al Firewall (s) disponibles y concentrados en sus funciones principales.

La solución de Filtrado para Internet brinda una experiencia positiva en la navegación protegiendo al usuario de material ofensivo e inapropiado y alentado hábitos apropiados de navegación, para mantener un ambiente positivo de trabajo y aprendizaje.

Para encontrar la solución que se ajustara en su totalidad a los requerimientos se analizaron varios Filtradores de Contenido Web que actualmente lideran las soluciones de filtrado, entre los que se encuentran los de las siguientes marcas:

COMPARATIVO WEBFILTERS	M86 WebMarshal	WEBSENSE Triton	FORTINET FG400
Características	Filtrado Web Reporting Suite	Gateways de Seguridad Web	Seguridad Integral en Tiempo Real
Actualizaciones de Software disponibles	Si	Si	Si
Pagina de bloqueo institucional personalizada	Si	*no disponible*	*no disponible*
modos de Operación Invisible, Router, Firewall, ICAP, Mobile Only Disponibles?	Si	Si	Si
protocolos de bloqueo	Si	Si	Si
modos de bloqueo via tabla de ARP	Si	*no disponible*	*no disponible*
Protocolo de Bloqueo	Si	Si	Si
Modo de bloqueo a una direccion MAC especifica	Si	Si	Si
capacidad de hacer backup de la configuracion y del sistema	Si	*no disponible*	*no disponible*
capacidad de hacer backup de la configuracion y del Sistema manual	Si	*no disponible*	*no disponible*
capacidad de hacer backup de la configuracion y del Sistema Automatico	Si	*no disponible*	*no disponible*
Capacidad de autenticacion por Radius	Si	*no disponible*	Si
capacidad de monitoreo del sistema por SNMP	Si	*no disponible*	Si
deteccion y monitoreo de fallas de HW (discos duros y fuentes)	Si	*no disponible*	*no disponible*
Capacidad de sincronizacion con equipos remotos en modalidad maestro - esclavo	Si	*no disponible*	Si
Notificacion por correo electronico de incidentes de emergencia	Si	*no disponible*	*no disponible*
Capacidad de diagnostico para detectar fallas en el equipo	Si	*no disponible*	*no disponible*
Capacidad de visualizar en tiempo real logs de trafico en tiempo real	Si	Si	Si
Capacidad de visualizar en tiempo real logs de usuarios conectados	Si	Si	Si
Capacidad de visualizar en tiempo real logs de errores	Si	*no disponible*	*no disponible*
Capacidad de visualizar en tiempo real logs de autenticacion	Si	Si	Si
capacidad de poner el equipo en modo de Troubleshooting para diagnosticar problemas del equipo	Si	*no disponible*	*no disponible*
capacidad de generar reporte detallados por hora	Si	Si	Si
capacidad de generar reporte detallados por dia	Si	Si	Si
capacidad de generar reporte detallados por semana	Si	Si	Si
capacidad de generar reporte detallados por mes	Si	Si	Si
capacidad de generar reporte detallados por año	Si	Si	Si
capacidad de sincronizar el equipo con servidores NTP	Si		Si
Capacidad de bloqueo por patrones	Si	Si	Si
Capacidad de de crear cuentas Override para validacion de paginas	Si	*no disponible*	*no disponible*
Capacidad de monitorear en tiempo real el trafico de internet por indicadores, catalogados por categorias de navegacion	Si	Si	Si
Capacidad de intervenir en tiempo real el trafico de internet	Si	Si	Si
FiltroWeb	Si	Si	Si
Filtra todo el tráfico Web en todos los puertos TCP por URL y / o dirección IP	Si	Si	Si
Afecta a la conexión de red o de Internet si se retrasa o se cae ?	No es punto de falla	No es punto de falla	No es punto de falla
Introduce latencia de la red	No	No	No
Firewall	No	Si	Si
VPN IPSec	No	Si	Si
VPN SSL	No	Si	Si
Traffic Shaping – por política y subinterfaz	No	Si	Si
Antivirus	No	Si	Si
Antispam	No	Si	Si
capacidad de Seguridad VoIP	Si	*no disponible*	Si
Bloquea Mensajeria Instantanea & P2P	Si	Si	Si
Web Proxy Clandestinos	Si	Si	Si
X-Strikes Bloqueo	Si	Si	Si
Clasificación de contenido en tiempo real	Si	Si	Si
Autenticación de usuarios	Si	Si	Si
Escalablilidad y flexiblilidad	Si	Si	Si
Capacidad de Usuarios	Cantidad máx. de usuarios por appliance Hasta 10,000	Cantidad máx. de usuarios por appliance Hasta 10,000	Sesiones Concurrentes(TCP) 400000 / Nuevas Sesiones/Sec (TCP) 10000

Tabla 2.0 Comparativo WEBFILTERS

Como se puede apreciar en la tabla anterior la solución M86 Web Marshall cumplió con la mayoría de los requerimientos a través del comparativo entre las principales marcas.

A su vez se tuvieron reuniones con M86 Web Marshall, WEBSENSE y FORTINET para que presentaran sus productos, aclarar dudas y conocer las características más a fondo; Durante este proceso se dejaron en la contienda únicamente a las empresas M86 y WEBSENSE para solucionar a la problemática.

Cabe destacar que M86 Web Marshall proporcionó e instaló un filtrador de contenido Web 8e6 en instalaciones de SEGOB para la realizar una prueba de concepto con el propósito de conocer a fondo las capacidades del equipo, la cual se llevó a cabo con éxito.

1.2 ELECCIÓN DE LA SOLUCIÓN PARA EL FILTRADO DE CONTENIDO

A pesar de que M86 Web Marshall y WEBSENSE tienen características similares se eligió al primero como proveedor de la solución debido a tres razones principales:

A. MENOR PRECIO

La propuesta económica que presentó M86 Web Marshall a la SEGOB era 20% más económica que la de WEBSENSE.

Cabe mencionar que para las adquisiciones de equipos y/o servicios deben cumplir con el artículo 36 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público:

"*CUANDO LAS DEPENDENCIAS Y ENTIDADES REQUIERAN OBTENER BIENES, ARRENDAMIENTOS O SERVICIOS QUE CONLLEVEN EL USO DE CARACTERISTICAS DE ALTA ESPECIALIDAD TECNICA O DE INNOVACION TECNOLOGIA, DEBERAN UTILIZAR EL CRITERIO DE EVALUACION DE PUNTOS Y PORCENTAJES O DE COSTO BENEFICIO. "*

"A QUIEN OFERTE EL PRECIO MAS BAJO QUE RESULTE DEL USO DE LA MODALIDAD DE OFERTAS SUBSECUENTES DE DESCUENTOS, SIEMPRE Y CUANDO LA PROPOSICION RESULTE SOLVENTE TECNICA Y ECONOMICAMENTE."

B. EVALUACIÓN DE LA MEJOR TECNOLOGÍA.

En la presentación de soluciones, la compañía WEBSENSE mostró como modelo de solución un servicio sustentado en Servidores Windows 2003, que en su momento presentaban inestabilidad y vulnerabilidad sobre el sistema operativo, que requeriría constantes actualizaciones de software y parches.

C. M86 Web Marshall con equipos de propósito especifico

Esta solución está basada en Appliance de propósito específico lo que hace que no tenga un sistema operativo susceptible a infecciones de virus y con capacidad suficiente para soportar la cantidad de usuarios concurrentes de salida a internet.

La solución basada en equipos no requieren la compra de software o hardware extra, es decir un precio cubría la solución total.

1.3 SOLUCIÓN 8e6 R3000 “M86 WEB MARSHALL”

El 8e6 usa equipos de alto rendimiento especializados en el monitoreo, filtrado y reportes, alojados en hardware 1U con procesadores Xeon de cuatro núcleos, arreglos de disco RAID (Hot Swap), diseñados para soportar desde 1,500 hasta 30,000 usuarios con un servicio consistente.

Filtrar el acceso a Internet es una parte de la solución; los reportes permiten a los administradores entender las tendencias de acceso, determinar “áreas problemáticas” con necesidades de mayor atención, donde se originan las amenazas para efectuar ajustes necesarios. Sin monitoreo y reportes no existe una manera de cuantificar el retorno de la inversión de filtrado o su contribución general para incrementar la productividad.

La tecnología de 8e6 R3000 ofrece dos soluciones eficientes para el monitoreo y reporteo; El reporteador empresarial y el reporteador de análisis de amenazas usados en conjunto con el Filtrador de contenido de Internet, trabajan juntos para proporcionar la administración completa sobre el uso indebido del acceso a Internet.

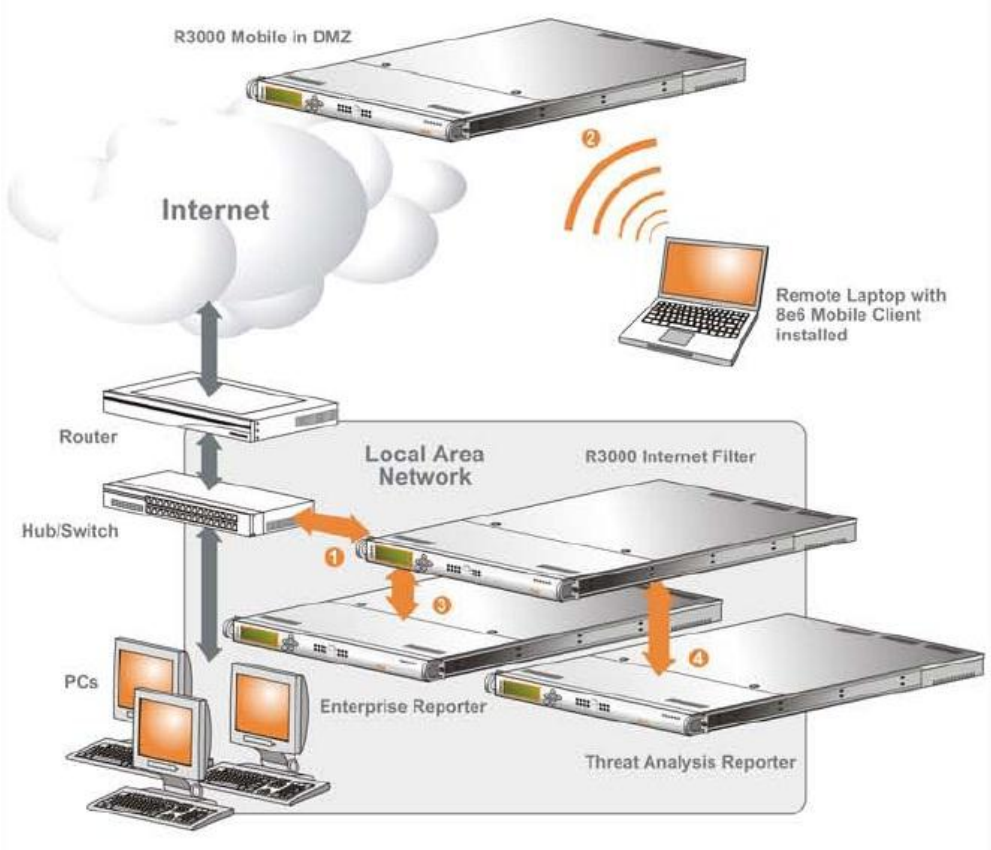


Imagen 2.0 Integración de equipos 8e6

1.3.1 Filtrador de Contenido de Internet (WebFilter)

EL R3000 Filtrador de Internet, es un Appliance dedicado que administra los accesos de usuarios finales fundamentándose en el contenido de Internet. Hecho con el propósito de ser escalable y ofrecer alta velocidad de filtrado, cada R3000 está basado en Linux Red Hat y provee el acceso a más de 100 categorías y millones de sitios Web en su base de datos.

Características

- Filtrado de Internet
  Incluyendo URL´s y /o direcciones IP, archivos tales como MP3, MPEG, zip, HTTP, HTTPS, FTP, grupos de noticias NNTP y puertos TCP.
  Bloquea amenazas de Internet incluyendo spyware, código malicioso, sitios de phishing y sitios de IRC.
- Bloquea Mensajería instantánea y Peer-to-peer
  Utilizando tecnología intelligent foot-print IFT para bloquear servidores de IM y P2P por patrón o por firma.

- Monitoreo en tiempo real
  Permite a los administradores monitorear la actividad de internet al momento que esta ocurriendo.
- Bloqueo “X-Strikes”
  Bloquea el equipo de cómputo de un usuario, cuando el administrador define un límite para accesar a sitios inapropiados y los intentos han sido excedidos.
- Implementación “SafeSearch”
  Fuerza el uso del modo “SafeSearch” en todas las búsquedas, incluyendo imágenes con los motores de búsqueda (Google, Yahoo, AOL, Ask).
- Bloqueo por patrón de Proxys
  Bloquea Proxys anónimos usando un detector de patrón de firmas único.
- Filtrado de palabras clave en motores de búsqueda.
  Bloquea el uso de palabras clave o frases en motores de búsquedas, para el acceso a sitios Web inapropiados.
- Categorización automática de URL´s
  Envió frecuente de URL´s no categorizadas de participantes quienes envían dicha información. Esta es seleccionada y añadida a la librería de 8e6.
- Consola central de administración
  Permite a los administradores sincronizar y administrar múltiples R3000´s sin tener que configurar uno por uno.
- Personalizable
  Personalizable para usuarios y perfiles de usuarios, pueden ser creados usando la base de datos de 8e6 con más de 100 categorías, abarcando más de diez millones de URL´s y direcciones IP.
- Mantenimiento bajo
  Mantenimiento bajo y transparente para los usuarios, al ser un equipo de propósito específico no requiere mantenimientos periódicos, en caso de necesitar alguno no se tiene afectación del servicio.
- Tecnología Pass-By
  El filtrado Pass-By elimina el desempeño ineficiente debido al volumen de tráfico y logra un filtrado rápido. El equipo R3000 se encuentra del lado del tráfico de la red, observando y comparando peticiones con la base de datos de sitios Web y URL´s de 8e6. Otorga compatibilidad y performance sin impacto negativo.
- Filtrado Móvil
  Utilizando el 8e6 Mobile Client posibilita el filtrado web remoto a usuarios fuera de la red.

- BASE DE DATOS 8e6

  El 8e6 cuenta con una base de datos alimentada con la información de sus analistas de internet, los cuales clasifican el contenido web, categorizando cada sitio que aparece y la añade, además el R3000 tiene CFM (Customer Feedback Module) el cual captura los accesos a sitios no categorizados y envía los datos a 8e6 donde son analizados y categorizados.

  La base de datos de 8e6 tiene más de 100 categorías, incluyendo diez millones de sitios Web y URL´s, con actualización de categorización.

1.3.2 Reporteador Empresarial (Reporter)

El reporteador empresarial procesa los datos del filtrador de contenido de internet y proporciona reportes predefinidos, modificables desde una red hasta un individuo en particular.

Posterior al procesamiento despliega bitácoras de filtrado de internet sin impactar las funciones de red y filtrado, construido sobre base de datos dedicada MySQL, usa una interfaz gráfica interactiva de procesamiento de datos para la generación de los reportes.

Características

- Metodología de procesamiento de Reportes:

Maneja grandes cantidades de tráfico de Internet, pre-procesamiento, indexación y presentación.

El pre-procesamiento le permite al reporteador almacenar datos, la indexación conserva espacio de almacenamiento al capturar solamente elementos únicos de los datos para ejecutar reportes con información en tiempo real.

- Reportes Forenses detallados

Permite el conocimiento de la intención en la navegación de los usuarios al medir y documentar la longitud completa de las URL´s visitadas, así como las palabras clave usadas dentro de un motor de búsqueda; Por ejemplo, un usuario puede ser bloqueado varias veces al tratar de acceder a diferentes URL´s restringidas pero éste puede intentar usar un motor de búsqueda para burlar el filtrado de contenido. El reporteador empresarial busca este tipo de comportamiento para que el administrador tenga la documentación necesaria para validar y remediar el problema.

- Agenda y reportes modificables

Las investigaciones de datos específicos pueden ser memorizadas o almacenadas en un menú de reportes definido por usuario para tener un acceso continuo y futuro. Estos reportes pueden ser entonces agendados, ejecutados y distribuidos automáticamente por medio de correo electrónico en una frecuencia (Ej. diaria, semanal, mensual).

- Panel gráfico intuitivo

Los administradores pueden identificar rápidamente actividad anómala de internet a través del panel gráfico.

El panel contiene 7 reportes de fácil lectura para escoger entre:

  - Las 20 categorías más altas
  - Los 20 usuarios más altos por conteo de páginas.
  - Los 20 usuarios más altos por Spyware
  - Los 20 sitios más altos
  - Los 10 grupos de usuarios
  - Comparación de categorías

- Reportes a fondo

Permite a los administradores documentar la actividad de usuarios anómalos específicos, los reportes pueden ser modificados por una ventana de tiempo específica, complementados con la capacidad de analizar los detalles a distintas opciones de alto nivel tales como:

Categorías, IP’s, Usuarios, Sitios, Grupos de usuario.

1.3.3 Reporteador de Análisis de Riesgos (TAR)

Entrega representaciones gráficas instantáneas del tráfico de Internet y está soportada por herramientas administrativas de tiempo real para identificar y controlar las amenazas web generadas por usuarios.

Características

- Panel de amenazas en tiempo real

Proporciona medidores gráficos en tiempo real que permite a los administradores identificar rápidamente múltiples categorías de amenazas, las categorías más ofensivas y los usuarios, basados en métricas y políticas.

- Análisis de amenazas a la medida

Los administradores pueden crear medidores adicionales al panel para modificar su propio sistema de alerta de amenazas, (Ej. de medidores modificables pueden monitorear un sitio Web de tráfico alto tal como Facebook), un grupo de categorías o grupo de usuarios o incluso un individuo que requiere un escrutinio más a detalle.

- Clasificación y calificación de amenazas

Los administradores pueden ajustar las calificaciones de las amenazas al configurar un peso a la categoría basado en requerimientos de las políticas.

Al usar una tabla de clasificación global, un administrador puede tener una vista rápida de toda la actividad Web de los usuarios, y configurar un rango de alertas basados en las altas calificaciones.

- Capacidad a detalle

Proporciona una interfaz intuitiva y analítica que puede obtener datos de los medidores principales de las categorías y las subcategorías que son monitoreadas para obtener la actividad específica de un usuario, permitiendo obtener la ruta directa al origen de una actividad inusual.

- Reportes de tendencias

Provee de gráficas de tendencias ocupadas para determinar el pico de tráfico de internet; Son usadas para optimizar las configuraciones de los medidores de amenazas para que concuerden con niveles de actividades de red únicos.

- Notificaciones de Alertas

Las notificaciones de las alertas permiten a los administradores configurar acciones predefinidas, basadas en opciones de las políticas de las alertas.

Con el administrador de alertas, un administrador puede ser alertado automáticamente de la violación de una política por medio de correo electrónico, o por medio de una alarma en la bandeja de sistema.

- Bloqueo y remediación

Los administradores pueden bloquear manualmente un usuario o configurar bloqueos automáticos por medio del administrador de alertas.

El mecanismo de bloqueo incluye los siguientes niveles de negación de acceso, (baja severidad (bloqueo de categorías), media severidad (bloqueo de acceso a internet) y alta severidad (cuarentena, sin acceso a la red).

CAPÍTULO 2. IMPLEMENTACIÓN DE LA SOLUCIÓN 8e6

2.1 ADQUISICIÓN

En el mes de febrero de 2009 la Secretaria de Gobernación adquirió la Solución de Filtrado de contenido de Internet 8e6 mediante la empresa de telecomunicaciones Axtel que a su vez subcontrato a la empresa Protektnet[5] con un contrato de 3 años el cual contempló la entrega y cumplimiento de lo siguiente:

Modelo	Descripción	Cantidad
RM3000-SL	Equipo de Filtrado de Contenido Web.	2
ERSL-200	Equipo Reporteador Empresarial.	2
TAR-SL	Equipo Reporteador de Análisis de Riesgos.	2
320000A	Licencias, Suscripción de Servicio y soporte por 36 meses.	10000
Install 8e6	Instalación e implementación de los equipos 8e6.	1
Capacitación Básica 8e6	Capacitación básica de un día para filtrado de contenido 8e6. El curso se imparte en las oficinas de Proteknet. Con duración de 6 horas las cuales se impartirán 3 horas de teoría y 3 horas de práctica. En la pare práctica se instalara un equipo de demo para usarse de laboratorio. (hasta 4 participantes)	1

Tabla 3.0 Equipo adquirido con la Solución 8e6

[5] Protektnet www.protektnet.com (Especialistas en Soluciones de Seguridad Informática)

Soporte

El 8e6 cuenta con soporte integrado con una línea de contacto para resolver problemas de Hardware, Software, consulta de consejos para resolver problemas; a través de las siguientes modalidades:

- Soporte vía Mail que permite a elementos de SEGOB previamente definidos, tener una línea abierta de soporte con ingenieros especializados en seguridad.
- Soporte Telefónico para consultar información acerca de virus o amenazas informáticas y recibir asesoría sobre posibles anomalías que pudieran causar indisponibilidad de los productos.
- Soporte vía Internet con herramienta RemoteCall

2.2 PLAN DE TRABAJO

Actividades de pre-implementación

Paso	Tiempo estimado	Instrucciones	Criterio de aceptación	¿Funcionó? SI/NO	Implementador (Iniciales y Fecha)
1	1 Mes	Instalación de un equipo DEMO dentro de la SEGOB.	SI	SI	SEGOB/ ProtektNet
2	2 días	Capacitación en la herramienta WEBFILTER	SI	SI	SEGOB/ ProtektNet
3	2 días	Generación del nuevo reglamento para navegación en Internet	SI	SI	SEGOB
4	1 semana	Junta para notificar y difundir la noticia del apagado del PROXY a los enlaces informáticos. Para que ellos tomen consideraciones para la migración de sus equipos.	SI	SI	SEGOB

Tabla 4.0 Plan de Trabajo (Pre implementación)

Actividades para la Implementación

Paso	Tiempo estimado	Instrucciones	Criterio de aceptación	¿Funcionó? SI/NO	Implementador (Iniciales y Fecha)
1	1 Semana	Planeación para la instalación del equipamiento en el SITE de Telecomunicaciones	SI	SI	SEGOB / ProtektNet
2	1 semana	Configuración de los equipos 8e6	SI	SI	SEGOB/ ProtektNet
3	1 Semana	Definición de grupos de navegación a internet	SI	SI	SEGOB
4	1 Semana	Captura de todas las direcciones IP de los equipos de la SEGOB a WEBFILTER.	SI	SI	SEGOB
5	1 semana	Capacitación de los equipos del CAT (centro de atención técnica) para recepción de quejas.	SI	SI	SEGOB
6	1 semana	Pruebas de funcionalidad del filtrado de contenido Web	SI	SI	SEGOB
7	1 semana	Configuración de los navegadores de los equipos de la SEGOB	SI	SI	SEGOB (enlaces informáticos)
8	15 minutos	Apagado del PROXY	SI	Si	SEGOB
9	1 Semana	Adecuación de los equipos 8e6 a las condiciones imprevistas de la navegación de la SEGOB	SI	SI	SEGOB
10	1 mes	Monitoreo y control de cambios.	SI	SI	SEGOB

Tabla 4. 1 Plan de Trabajo (Implementación)

2.3 REGLAMENTO DE NAVEGACIÓN VIGENTE A PARTIR DEL AÑO 2009

Con la adquisición de los equipos 8e6 y con el propósito de cubrir la problemática con la implementación de los mismos fue necesario definir nuevas políticas de uso de Internet desde equipos propiedad de la Secretaría de Gobernación y de aquellos equipos que no son propiedad de la Institución, pero requieren servicio de acceso a Internet, desde la RED SEGOB, para lo que se designo a la DGTI y esta a su vez a la Subdirección de Seguridad Lógica; Lo anterior llevó a establecer el nuevo reglamento de navegación.

NORMAS GENERALES

Con base en el cumplimiento a las normas legales vigentes: Ley Federal de Responsabilidades de los Servidores Públicos, Capitulo I, Título Segundo, Capitulo I, Artículos 7,8,9,10,11,12 y 13; Ley Federal de Derechos de Autor. Capitulo Único, Articulo 1, 3, 12, 13, a la Ley Federal de Acceso a la Información y a las Recomendaciones Sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales y el Reglamento Interno de la Secretaría de Gobernación, Articulo 31 fracción I, IV, V, VI, VII, IX, XV, XVII y XVIII. Es desde donde se parte para el establecimiento de un Reglamento de navegación al interior de la SEGOB.

El eje rector de dicha normatividad interna radica en que los recursos y servicios de Internet deben ser utilizados de manera racional y consciente, teniendo en cuenta que se trata de un servicio para beneficio general de los empleados y las funciones de la Secretaría.

Uso indebido de Internet

Se define como uso indebido de Internet a todo aquello que represente contenidos de bajo valor para la dependencia; atente contra las reglas de comportamiento general establecidas en el Código de Conducta Institucional; se relacione con la ilegalidad y, por ende, que contravenga las leyes de los Estados Unidos Mexicanos. Se muestra de manera gráfica las zonas Prohibidas, Excepciones y los Permitidos este último esta dentro de los parámetros normales de navegación y uso de Internet.

Prohibido	Pornografía, Phishing, Cracking, Hacking, Racismo, Odio, Muerte, Terrorismo, Violencia, Descarga de Material con Derechos de Autor o licenciamiento, Proxys Clandestinos, Tunnels, etc.
Permitido	Páginas de Gobierno, Cultura, Salud, Educación, Bancos, Librerías, Bibliotecas, Deportes y Noticias
Excepciones	Radio y Televisión por Internet, Chat, Redes Sociales, Streaming.

Tabla 5.0 Uso de Internet

Prohibiciones hacia Internet

Está totalmente prohibido el ingreso a páginas de contenido pornográfico, pederastia, zoofilia, fraudes, armas, terrorismo, descarga de programas que permitan realizar conexiones automáticas e ilegales, a través de la Web.

a. Queda prohibida la utilización del Internet para distribución o reproducción, de material que cuenta con derechos de autor, marcas o patentes, ya sea vía la RED SEGOB, Internet o medios de almacenamiento (USB, ópticos, magnéticos, electrónicos, etc.), El material descargado con derechos de autor por el usuario es responsabilidad de cada Usuario (a título Personal) y no de la Secretaría, ya que esto se castiga por la ley por lo que deberá observarse o referirse a la Ley Federal de Derechos de Autor, a la Ley Federal de Responsabilidades de los Servidores Públicos y a todas aquellas leyes involucradas.

b. Queda prohibido Descargar música y video con servicios como KaZaa, Morpheus, GNUtella, Torrents, Sitios Web o cualquier otro software Peer to Peer. El material descargado con derechos de autor por el usuario es responsabilidad de cada Usuario (a título Personal) y no de la Secretaría, ya que esto se castiga por la ley por lo que deberá observarse o referirse a la Ley Federal de Derechos de Autor, a la Ley Federal de Responsabilidades de los Servidores Públicos y a todas aquellas leyes involucradas.

c. Queda Prohibido participar en juegos de entretenimiento en línea de manera individual o en la modalidad multiusuario.

d. Queda Prohibido participar en Sitios de apuestas, juegos de azar o lotería, etc.

e. Queda Prohibida la utilización de los servicios de Radio y TV por demanda (Todito.com, TV Azteca, Televisa, MVS noticias etc.), excepto cuando los usuarios justifiquen de manera amplia su uso, ejemplo RTC y Comunicación Social. Así mismo la justificación no obliga a la liberación de estos servicios y quedará sujeta a la disponibilidad del servicio.

f. Queda Prohibidos Servicios de Multimedia como son YouTube, etc.; excepto cuando los usuarios justifiquen de manera amplia su uso, ejemplo RTC y Comunicación Social. Asimismo la justificación no obliga a la liberación de estos servicios y quedará sujeta a la disponibilidad del servicio.

g. Queda Prohibido entrar a sitios de Hacking, Cracking, etc., así como a foros de esta misma categoría.

h. El uso del Servicio de Internet es para las actividades institucionales y laborales, queda prohibido el uso de Internet con fines de entretenimiento, publicidad, campaña política o comercial, etc.

Acceso a sitios de Internet

a. Si se requiere acceso a sitios especiales, como son correo público como Yahoo, Hotmail, Gmail, etc. Deberá de justificarse ampliamente su utilización. Así mismo la justificación no obliga a la liberación de estos servicios.

b. Los únicos puertos por los cuales deberá de navegar el personal serán el 80 y 443, cualquier otro puerto distinto a estos deberán de solicitarse a la DGTI a través de la Subdirección de Seguridad de Tecnologías de la Información, indicando el tiempo que estará abierto, el objetivo de porque estará abierto, el servicio y todos los detalles de porque se necesita esta apertura. La DGTI y en particular la Subdirección de Seguridad de Tecnologías de la Información, se reservan el derecho de abrir o no estos puertos, por lo que ninguna justificación representa obligación alguna de abrir los puertos si estos representan un riesgo o una amenaza y/o vulnerabilidad de la red de SEGOB.

c. El Usuario no debe interferir en el Tráfico de la RED e Internet de la SEGOB mediante acciones deliberadas que disminuyan el desempeño o la capacidad de los equipos instalados, por ejemplo escaneo de puertos, pings, tracerts, etc.

d. Bajo ningún pretexto debe intentar burlar los esquemas de seguridad de los sistemas de la SEGOB.

e. Todos los usuarios tienen la obligación de reportar a la DGTI a través del CAT (Centro de Atención Técnica) y este a su vez a la Subdirección de Seguridad de Tecnologías de la Información el uso incorrecto o inapropiado del servicio de Internet por parte de los usuarios.

Sobre el uso de Internet para proveedores e invitados especiales.

De acuerdo a la naturaleza del trabajo y actividad del personal de la empresa proveedora o invitado especial, deberá de solicitar los accesos a la red de datos, tomando en cuenta las siguientes consideraciones:

a. El equipo de cómputo del proveedor se conectara a una VLAN diferente de las institucionales para evitar tráfico malicioso o posibles infecciones a los equipos de la RED SEGOB.

b. En caso de requerir acceso a la RED SEGOB el área responsable deberá solicitar los permisos de acceso a la Subdirección de Seguridad de Tecnologías de la Información a los sistemas indicando objetivo, tipo de permisos, tiempo en el que estarán habilitados los servicios.

c. El área responsable deberá validar que el equipo del proveedor está libre de virus y de software malicioso.

d. Queda prohibido el uso de software para el escaneo de puertos, sniffers, implementaciones de Túnel (http-tunnel), el personal que sea sorprendido implementando este tipo de software en la Red de la SEGOB, se le suspenderá el Servicio de Internet, será reportado al área responsable y se notificara a seguridad institucional.

e. Respecto al acceso al área responsable que haya contratado o este al frente de la supervisión del proveedor solicitara dichos permisos al área de Seguridad de la DGTI (Subdirección de Seguridad de Tecnologías de la Información).

f. El personal del proveedor es responsable de su información y de su equipo de cómputo, por lo que la Secretaría no se hará responsable por daños lógicos o pérdida de información de los equipos de cómputo del proveedor.

g. El mal uso de los servicios de red será reportado al área responsable, dicha área tendrá la obligación de notificar la anomalía al responsable de la empresa proveedora.

h. La Secretaría se reserva el derecho de autorizar o no dichos servicios y accesos de red al considerarlos una amenaza o considerarlos no competentes a la actividad o trabajo del proveedor o por falta de disponibilidad.

i. El personal de la empresa proveedora quedará sujeto a los lineamientos de protección de datos personales y cuando sea necesario se le harán firmar cartas de confidencialidad en las cuales se detallará el objeto de la información que está utilizando, así como el compromiso de no divulgarla o utilizarla con otros fines que no sea el del trabajo o actividad para el cual fue contratado.

Cancelación del servicio de Internet

La cancelación del servicio de Internet podrá realizarse de manera parcial o definitiva en los siguientes casos.

a. Cuando se compruebe que el usuario ha incurrido en mal uso del Internet, mencionadas en la Sección I PROHIBICIONES HACIA INTERNET, en este documento.

b. Cuando exista un riesgo potencial que dañe la infraestructura de la RED SEGOB.

c. Cuando el usuario incurra en prácticas ilegales de escaneo de puertos, instale programas para robar contraseñas usurpar sesiones o funciones en la RED.

d. Cuando se compruebe que el usuario descargo material con Derechos de autor, Marcas y/o Patentes.

e. Cuando instale software tales como túneles, Proxys, para evadir la seguridad de Internet y poner en riesgo la Organización.

f. Cuando el equipo del usuario sea fuente de infección de Virus, Spyware, BackDoor, o ataques a la RED SEGOB o a otras Redes de Internet.

g. Por solicitud expedita de su Jefe Inmediato o Jefe de UR mediante Oficio o Atenta Nota.

Sanciones

- El incumplimiento de las políticas aquí presentadas puede acarrear consecuencias, tales como: la cancelación temporal o definitiva del acceso de Internet y el reporte de lo sucedido al Órgano Interno de Control (OIC).
- En otros casos y dependiendo de la naturaleza de la acción se analizará el caso en particular y será reportado al OIC para proceder conforme lo marca la ley.
- La DGTI a través de la Subdirección de Seguridad de Tecnologías de la Información, se reservan el derecho de permitir el uso de Internet de los usuarios.

Nota: Cualquier punto no contemplado en el presente Documento, será evaluado y resuelto por Personal DGTI a través de la Subdirección de Seguridad de Tecnologías de la Información.

2.4 REUNIÓN CON ENLACES INFORMÁTICOS DE LAS UNIDADES ADMINISTRATIVAS

Cada Unidad Administrativa de la SEGOB cuenta con un Enlace Informático quienes son los encargados de recibir y atender las peticiones correspondientes a Tecnologías de la Información (TI).

Posterior a la creación del nuevo Reglamento de navegación se realizó una reunión con los Enlaces Informáticos para dar a conocer los siguientes puntos:

La existencia de un nuevo Reglamento de navegación a Internet al cual todas las Unidades Administrativas tendrían que apegarse:

- Adquisición de los equipos 8e6 y sus funciones
- Requerimiento de un listado de las Ips de los equipos con nombre de los responsables de estas.
- Cambio en la navegación, la cual a partir de la instalación y configuración de los equipos 8e6 seria sin Proxy.

2.5 INSTALACIÓN DE LOS EQUIPOS 8e6 EN SEGOB

La SEGOB adquirió dos soluciones 8e6 por lo que dichos equipos fueron instalados en sus Sites de las oficinas de Bucareli y Reforma debido a que ahí se encuentran los dos enlaces de Internet.

Los equipos fueron instalados en un rack por el proveedor considerando las siguientes especificaciones eléctricas:

Equipo	Fuente de alimentación	Consumo de energía
WEBFILTER	AC: 100V-240V 50-60Hz	150W
REPORTER	AC: 100V-240V 50-60Hz	150W
TAR	AC: 100V-240V 50-60Hz	150W

Tabla 6.0 Especificaciones Eléctricas de los equipos 8e6

2.6 CONFIGURACIÓN DE LOS EQUIPOS 8e6

Para configurar los equipos 8e6 una vez conectados a la electricidad se conecto una laptop que cuenta con un puerto serial DV9; para comenzar la configuración inicial se requirió del programa de Windows XP HyperTerminal como se muestra a continuación:

a) Para abrir el programa HyperTerminal Inicio → Programas → Accesorios → Comunicaciones → HyperTerminal

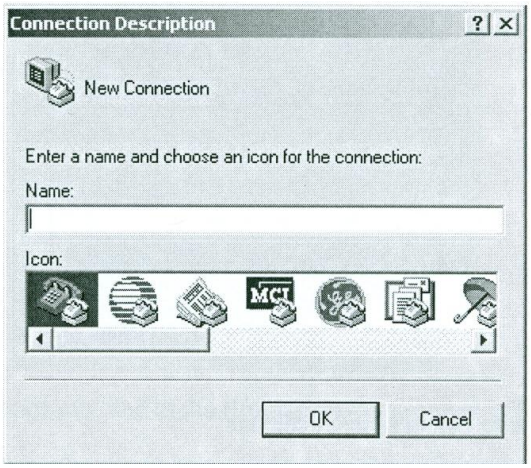


Imagen 3.0 Descripción de nueva conexión para HyperTerminal

b) En el recuadro “descripción de conexión” se debe ingresar cualquier nombre de sesión.

c) La conexión se realizara usando el puerto COM asignado al puerto de serie de las computadoras portátiles (probablemente COM1)

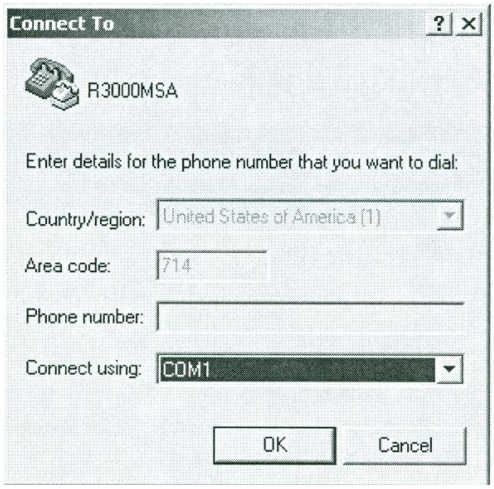


Imagen 3.1 HyperTerminal “Definición de puerto COM”

d) Especifique los valores de la sesión siguientes:

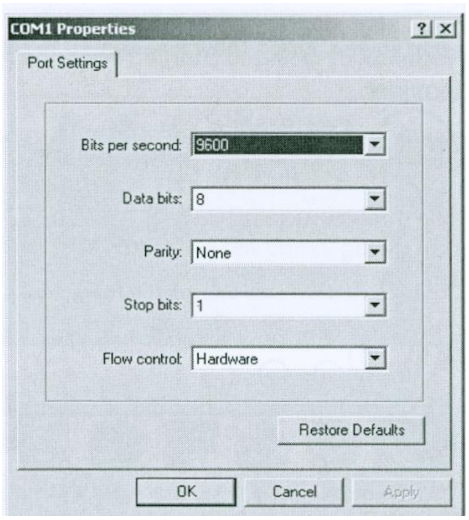


Imagen 3.2 HyperTerminal “Parámetros de la Sesión”

e) En la ventana de sesión de HyperTerminal Archivo →Propiedades → para abrir el cuadro de diálogo Propiedades, que muestra la conexión y configuración.

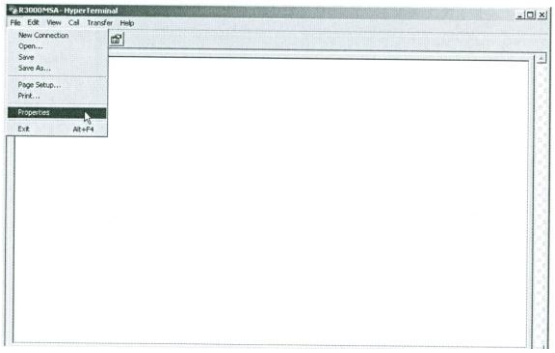


Imagen 3.3 HyperTerminal "Cuadro de diálogo de propiedades"

f) En la pestaña de configuración y el menú de emulación seleccionaremos "VT100"

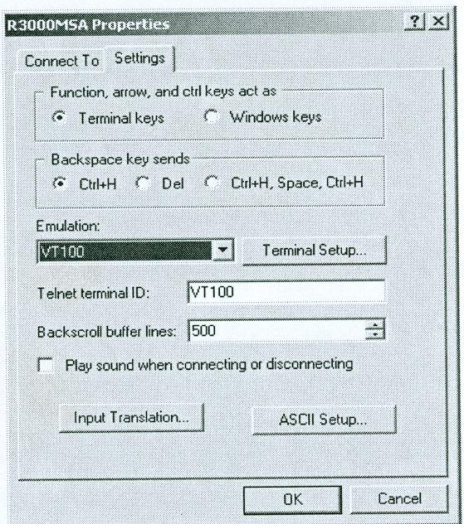


Imagen 3.4 HyperTerminal "Emulación VT100"

g) Haciendo clic en Aceptar cerraremos el cuadro de diálogo y se podrá ir a la pantalla de inicio de sesión

La HyperTerminal nos permite ingresar a las siguientes pantallas de configuración:

Configuración Inicial

Donde se ingresará la contraseña de administración genérica

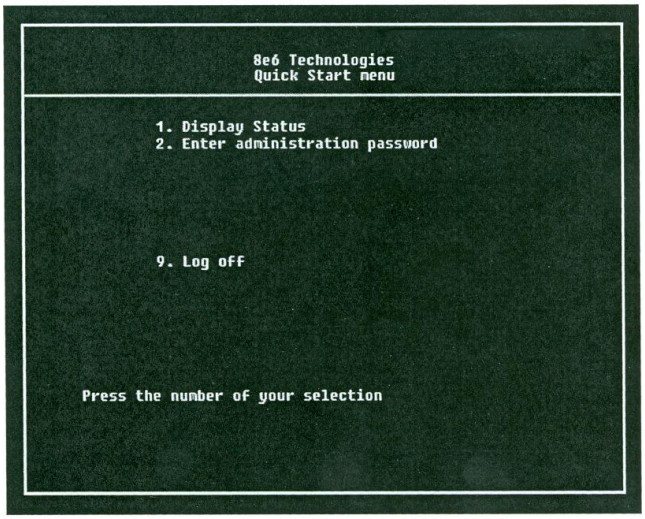


Imagen 4.0 Configuración Inicial

Seleccionamos la **opción "2"** para el proceso de inicio de instalación rápida; en el inicio de sesión del sistema, pedirá nuevamente introducir la contraseña genérica.

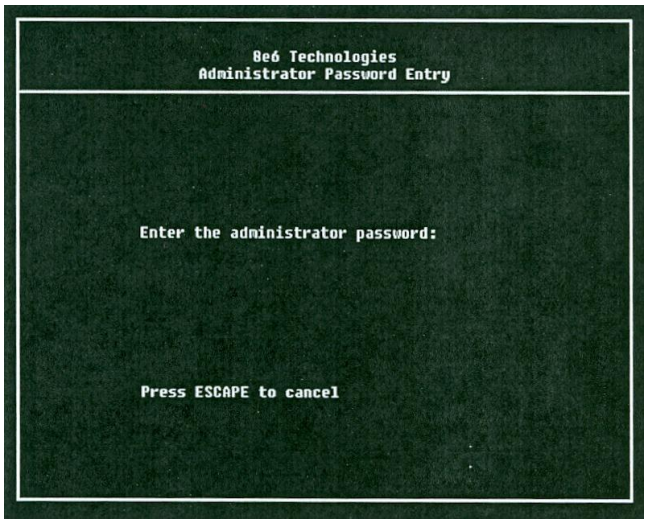


Imagen 4.1 Contraseña

Después se podrá visualizar el menú de administración para comenzar a utilizar los procedimientos de configuración de inicio rápido.

El menú de administración mostrará las pantallas de configuración siguientes:

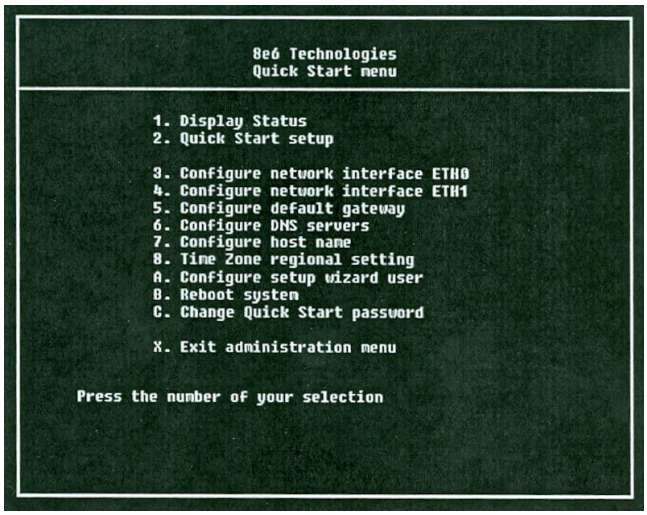


Imagen 4.2 Menú de Administración

Donde seleccionaremos la **opción "2"** para acceder a la configuración de inicio rápido, este proceso nos dirige a la pantalla de configuración de interfaz de red.

Configuración de Interfaz de Red

En el campo "LAN1" (interfaz para el acceso web) indicáremos la dirección IP elegida para el equipo a configurar.

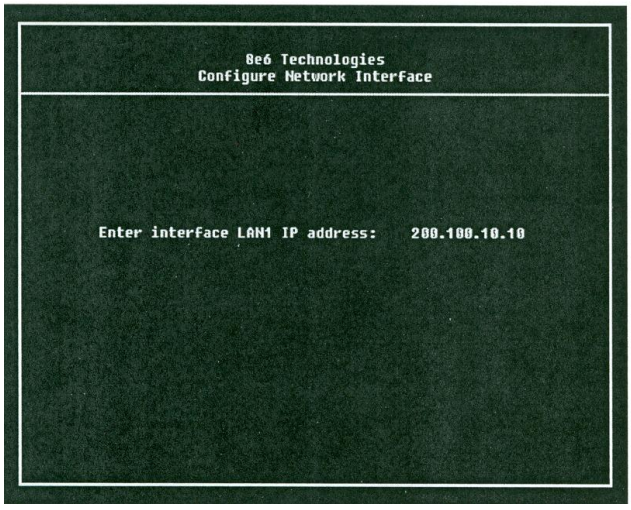


Imagen 4.3 Configuración de Red

Mascara de Red para LAN1

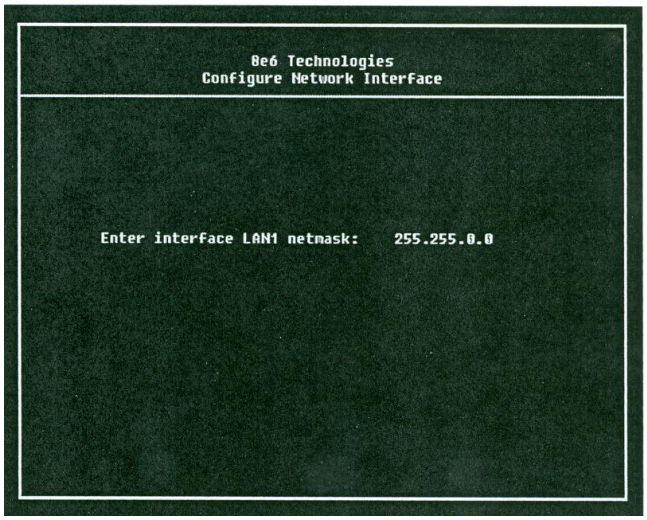


Imagen 4.4 Configuración de Mascara de Red para LAN1

Imagen 4.5 Configuración de Gateway

Configuración de DNS de la SEGOB Primario y Secundario.

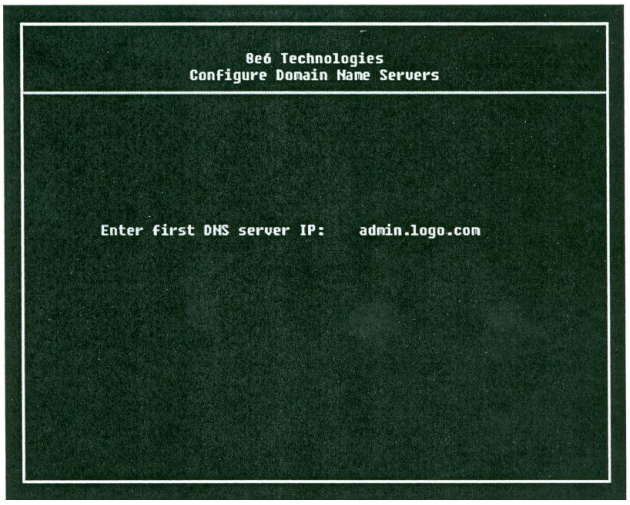


Imagen 4.6 Configuración de DNS Primario

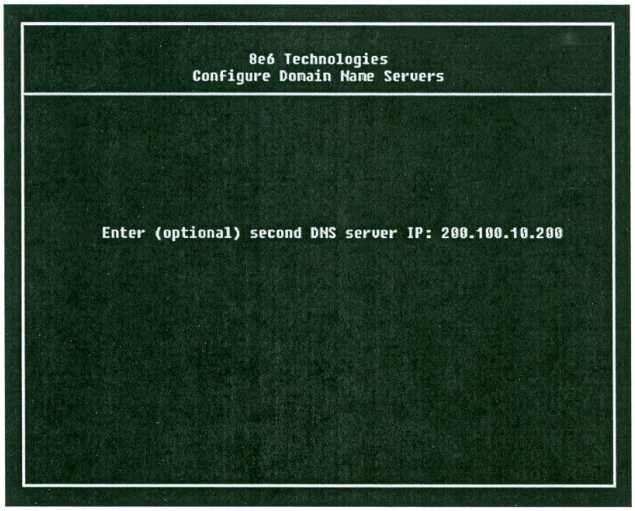


Imagen 4.7 Configuración de DNS Secundario

Host Name del Servidor

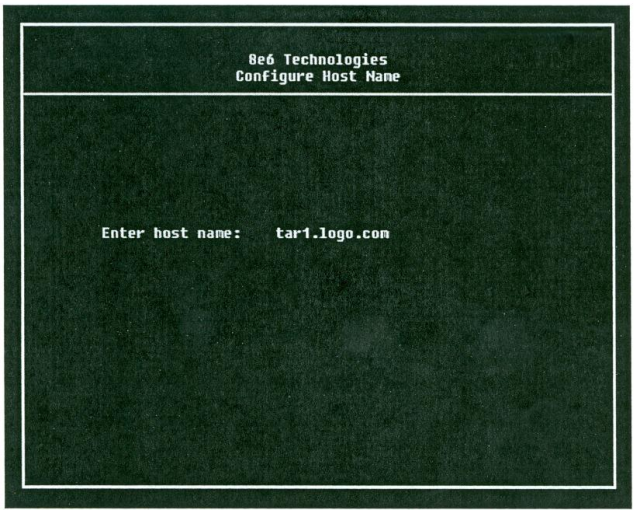


Imagen 4.8 Configuración de Host Name

Configuración de Zona horaria

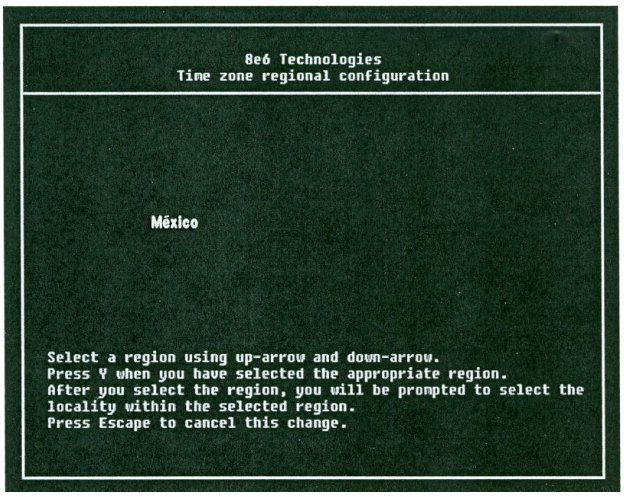


Imagen 4.9 Configuración de Zona horaria

Configuración de Usuario y Contraseña

(Para su administración vía web)

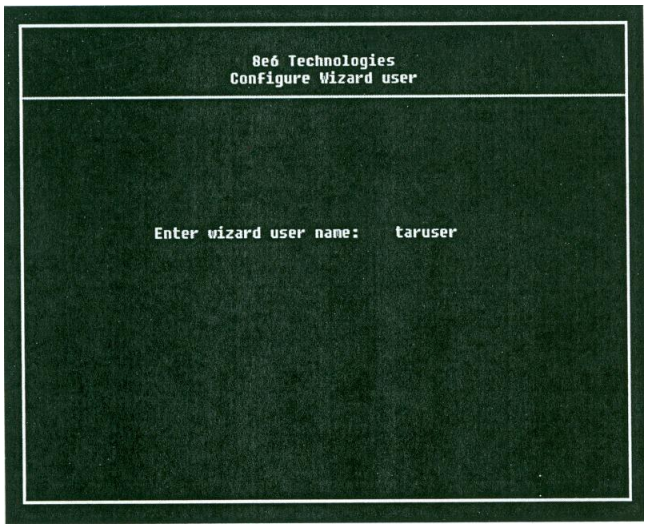


Imagen 4.10 Configuración de Usuario para administración vía web

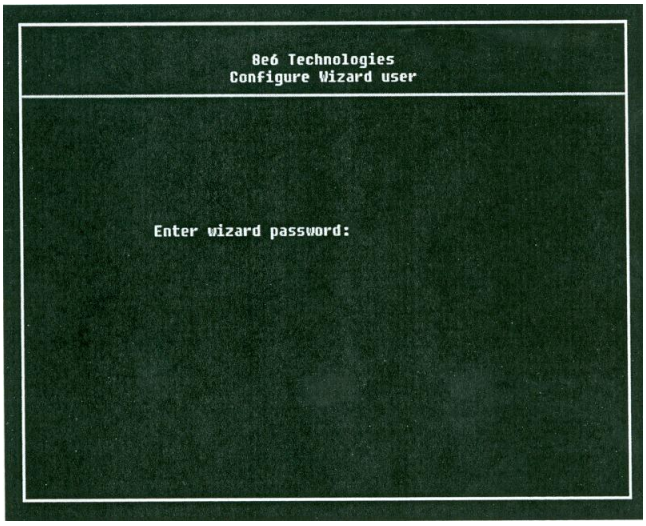


Imagen 4.11 Configuración de Contraseña para administración vía web

Estado del Sistema

Una vez terminada la configuración en consola al presionar la tecla “1” se podrá verificar el estado del equipo y revisar las entradas realizadas con la configuración de inicio rápido.

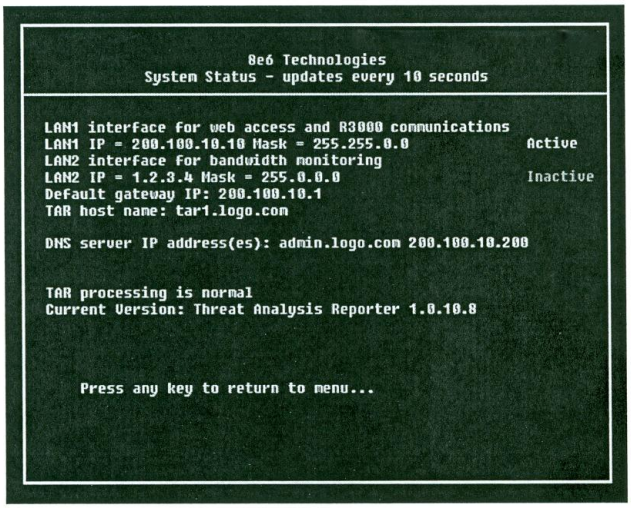


Imagen 4.12 Estado del Sistema

Completados los procedimientos de configuración de inicio se procede a conectar físicamente la unidad a la Red de la SEGOB.

Nota: La configuración inicial para los 3 equipos 8e6 (WebFilter, Reporter y TAR) se realiza de la misma manera, como se mostró en las pantallas anteriores.

2.6.1 CONFIGURACIÓN FILTRADOR DE CONTENIDO (WebFilter)

El ingreso a la interfaz gráfica del WebFilter se realiza mediante un navegador de internet poniendo https://la ip que destinamos a la interfaz: y el puerto 1443

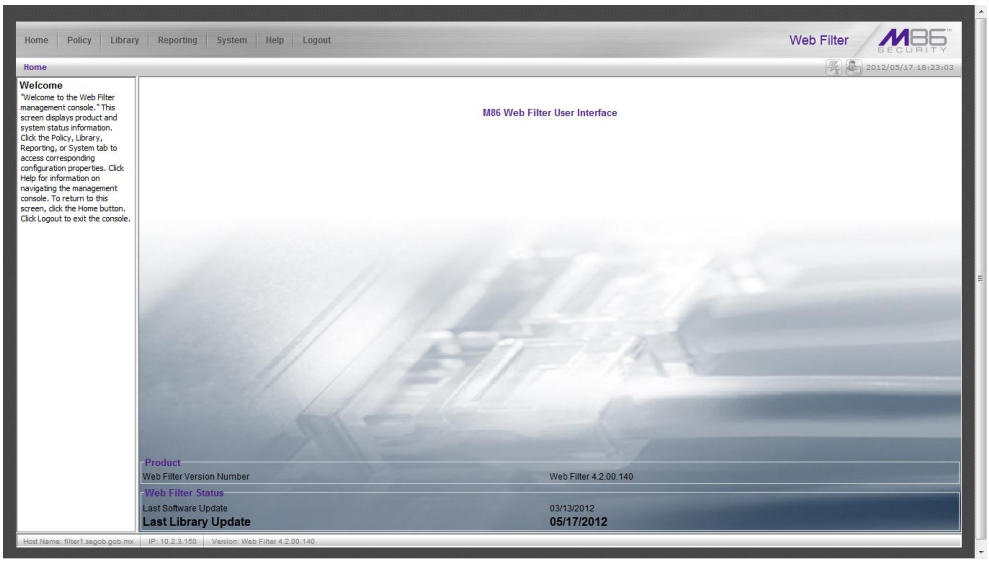


Imagen 5.0 Pantalla representativa de WebFilter

Modo de Operación

System→Mode→Operation Mode

En esta pantalla definimos el modo de operación el cual debe estar habilitado en "Invisible" para que no sea punto sensible de falla.

En el modo Invisible por default la interfaz LAN1 que se configuró previamente es por la que escucha el tráfico de los usuarios que va hacia Internet y ejecuta el filtrado.

LAN2 Es la interfaz utilizada para bloqueo de los paquetes y administración.

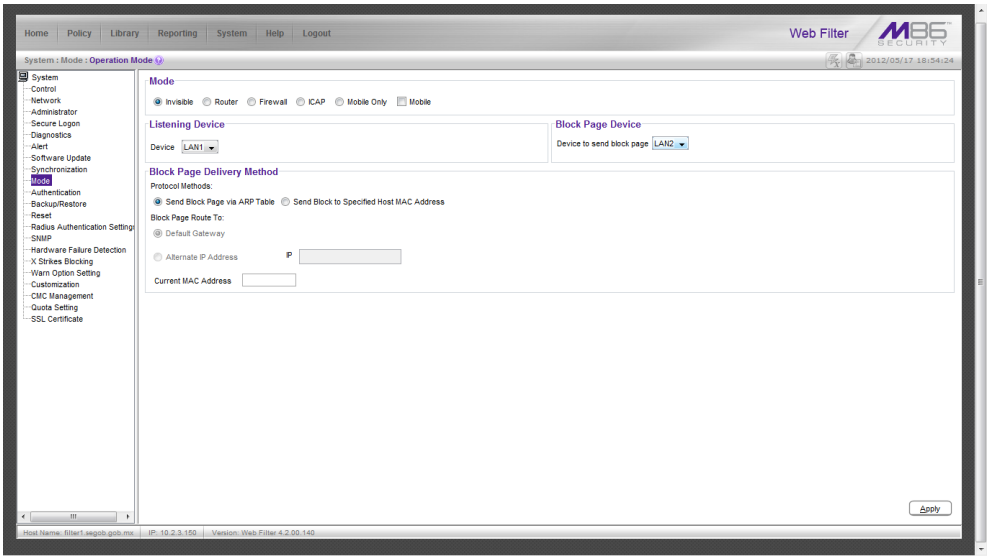


Imagen 5.1 Modo de operación del WebFilter

Configuración de Red para la Interfaz Gráfica

Previamente en consola elegimos una IP para LAN1 la cual es necesario colocar nuevamente en la interfaz gráfica del WebFilter.

Network→LAN Settings

Imagen 5.2 Configuración de LAN1 para WebFilter

Además de la Ip la cual colocaremos en la sección LAN1, debemos ingresar el Host Name del equipo el cual debe incluir el nombre del dominio (filter.segob.gob.mx), los DNS primario y secundario de la SEGOB; así como el Gateway.

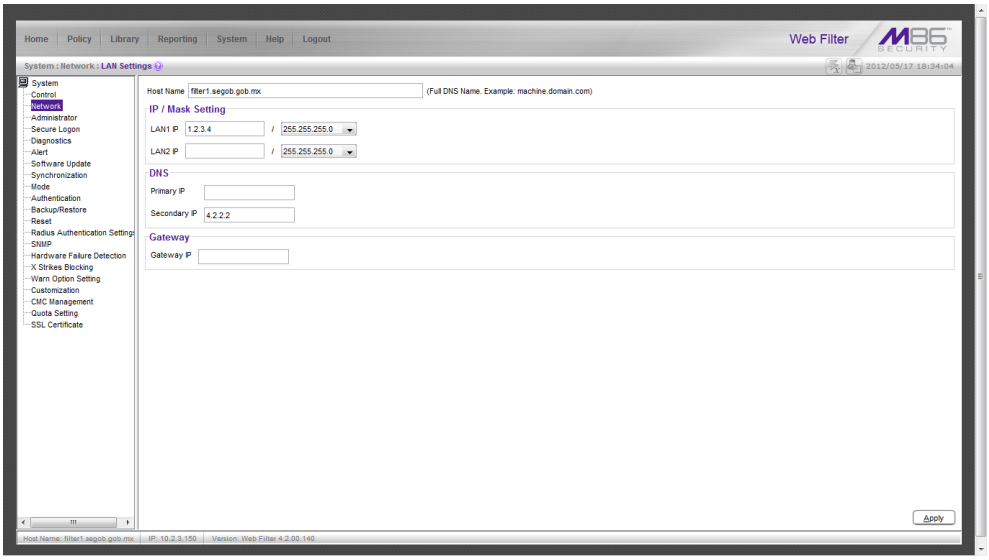


Imagen 5.3 Configuración de Host Name, DNS y Gateway para LAN1 de WebFilter

NTP Servers

En esta pantalla **System→Network→ NTP Servers** se configura el Servidor de NTP (Network Time Protocol) el cual sirve para mantener al equipo en la hora del país o de zona adecuada.

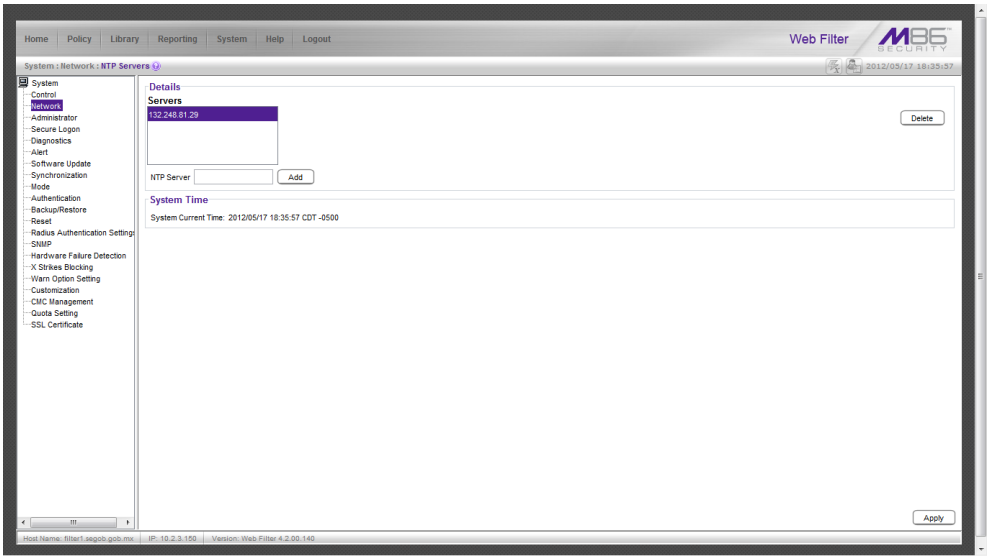


Imagen 5.4 Configuración de Servidor NTP para WebFilter

Configuración Regional

System→Network→Regional Setting

En esta pantalla se configura el País o Región, la Ubicación y el Idioma.

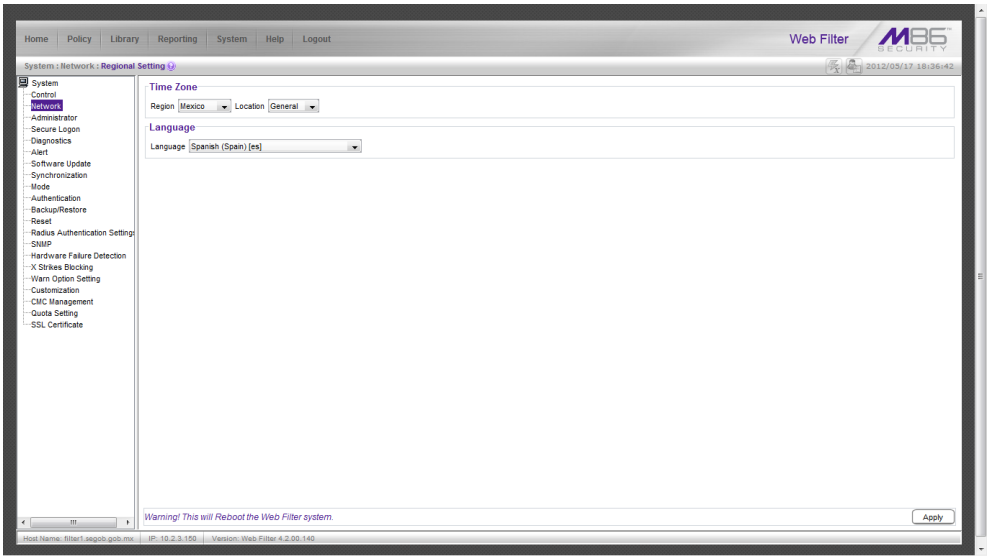


Imagen 5.5 Configuración de Región para WebFilter

Activación de Filtrado

Para activar el filtrado en el equipo debemos ingresar a **System→Control → Filter** como la siguiente pantalla:

Imagen 5.6 Activación de Filtrado para WebFilter

Una vez estando en la sección de Filtrado la opción mas importante a configurar es “Local Filtering” la cual debe estar en **“ON”**

HTTPS/SSL Filtering se recomienda que esté en el nivel **“low**” ya que de lo contrario tiraría todo el tráfico https por ejemplo los servicios de banca electrónica o pagos por internet.

La opción **Service Control →Pattern Blocking** se debe habilitar esta opción para evitar que todos los usuarios utilicen algún WebProxys o Anonimizadores para evadir la seguridad implementada.

Por último **Target(s) Filtering →Fuerza** el filtrado mediante la actualización de los perfiles o firmas del M86.

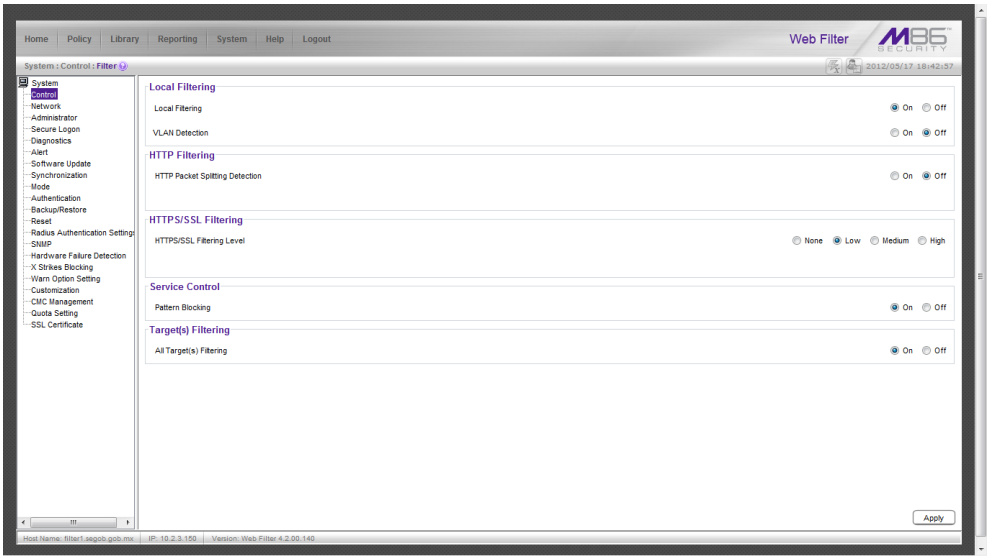


Imagen 5.7 Target(s) Filtering para WebFilter

Cuentas de Administrador

System→ Administrator→

En esta pantalla se definen los Usuarios para ingresar a la interfaz gráfica y el tipo de permisos de los mismos.

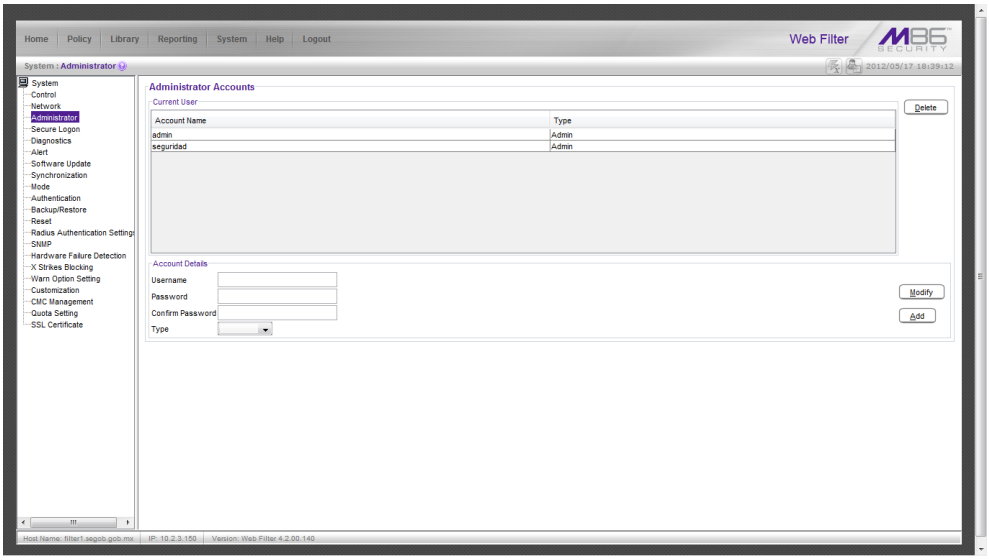


Imagen 5.8 Cuentas de Administrador para WebFilter

Alertas

System→Alert→Alert Settings

Se definen las cuentas de correo electrónico donde se enviarán las alertas del equipo y el emisor de las mismas.

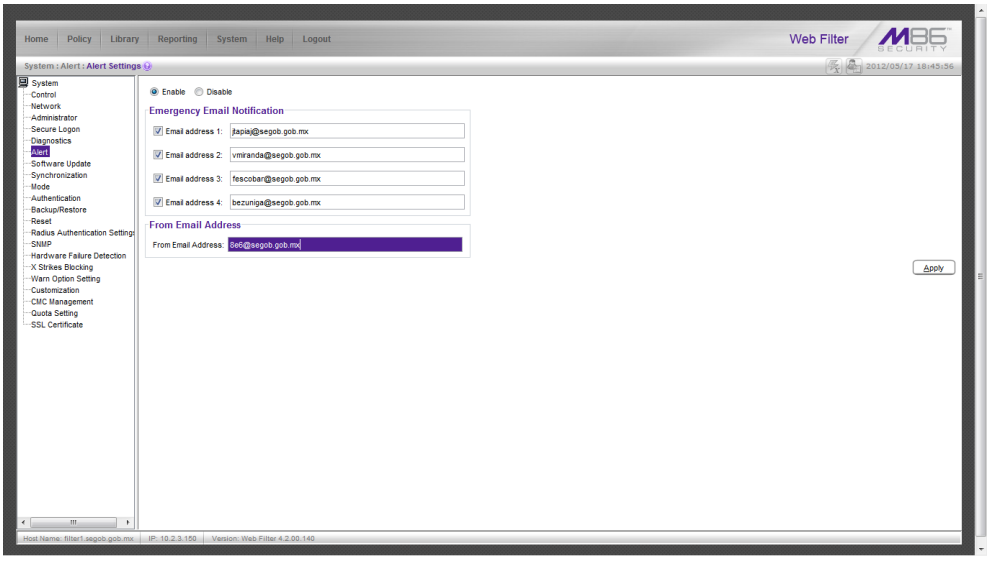


Imagen 5.9 Configuración de Alertas para WebFilter

Configuración de Servidor SMTP

System→Alert→SMTP Server Settings

En esta pantalla se configura el servidor de correo electrónico de SEGOB a través del cual estará enviando las alertas del equipo.

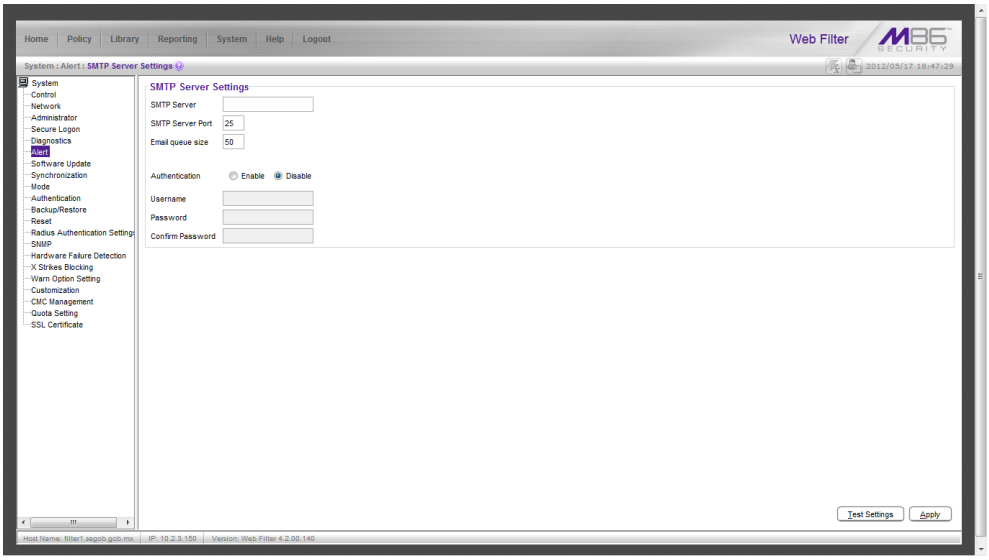


Imagen 5.10 Configuración de Servidor de Correo Electrónico en WebFilter

Actualización de Software

System→Software Update →Local Software Updates

En dicha pantalla se valida si existen actualizaciones del software de filtrado disponibles para aplicar, además queda registrado el histórico de las actualizaciones aplicadas.

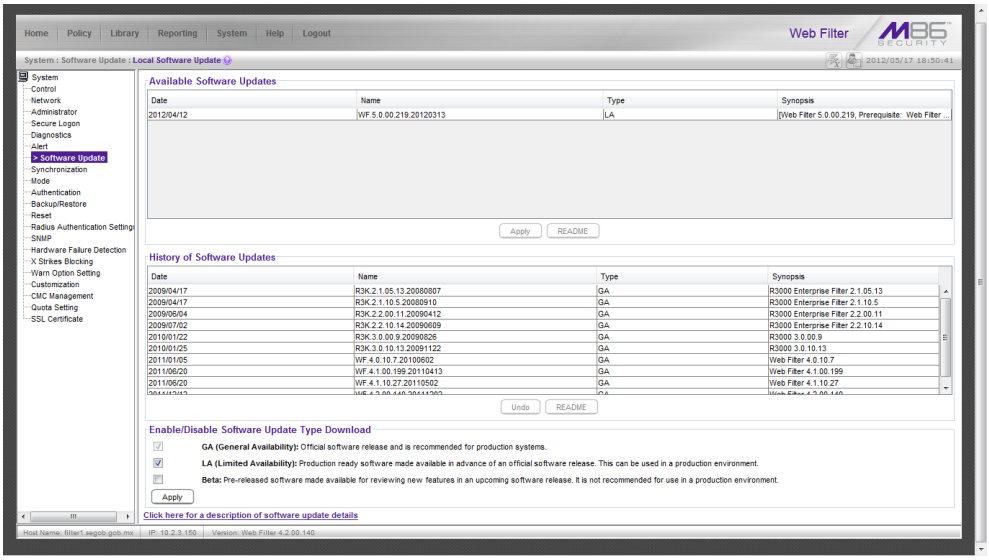


Imagen 5.11 Actualización de Software de WebFilter

Sincronización

System→Synchronization→Setup

En esta pantalla se realiza la configuración de modo Esclavo o modo Maestro; al seleccionar la opción “source” significa que se encuentra en modo Maestro, es decir el equipo que se encuentra en Reforma 99 viene a leer la base de datos de permisos de navegación de los usuarios del equipo de Bucareli.

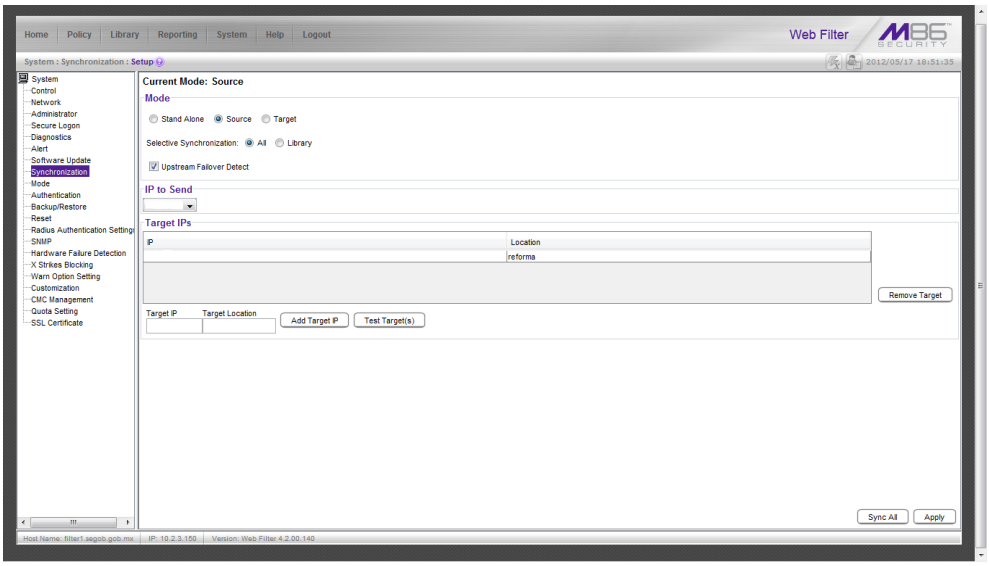


Imagen 5.12 Sincronización de equipos WebFilter

X Strikes Blocking

System→X Strikes Blocking→Categories

En esta opción se definen las categorías que estarán bloqueadas en el equipo para todos los grupos de navegación desde el comienzo de la operación.

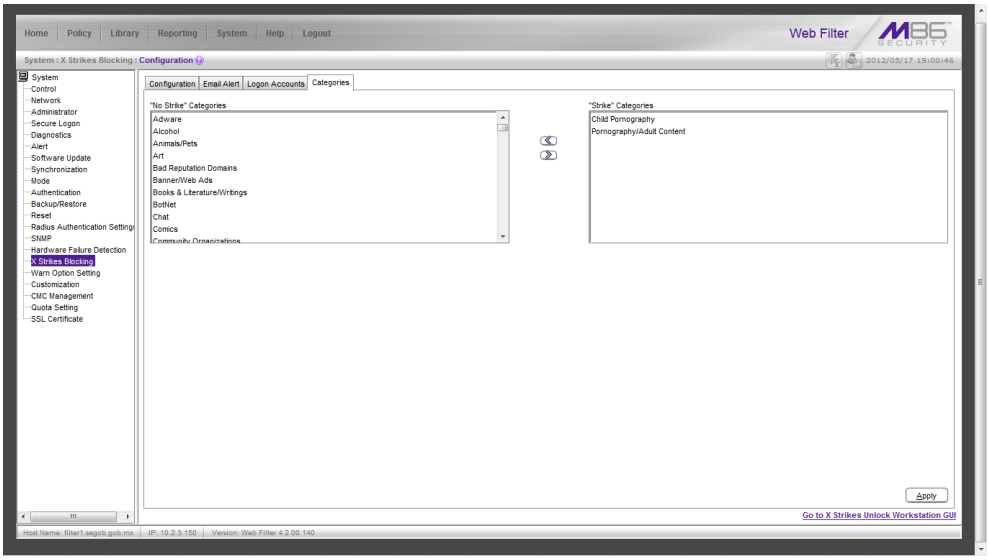


Imagen 5.13 Definición de Categorías bloqueadas para WebFilter

Página de bloqueo

System→Customization→Block Page

En esta sección se define URL de la página institucional que se muestra a los usuarios en su intento de burlar las políticas establecidas para la navegación Web.

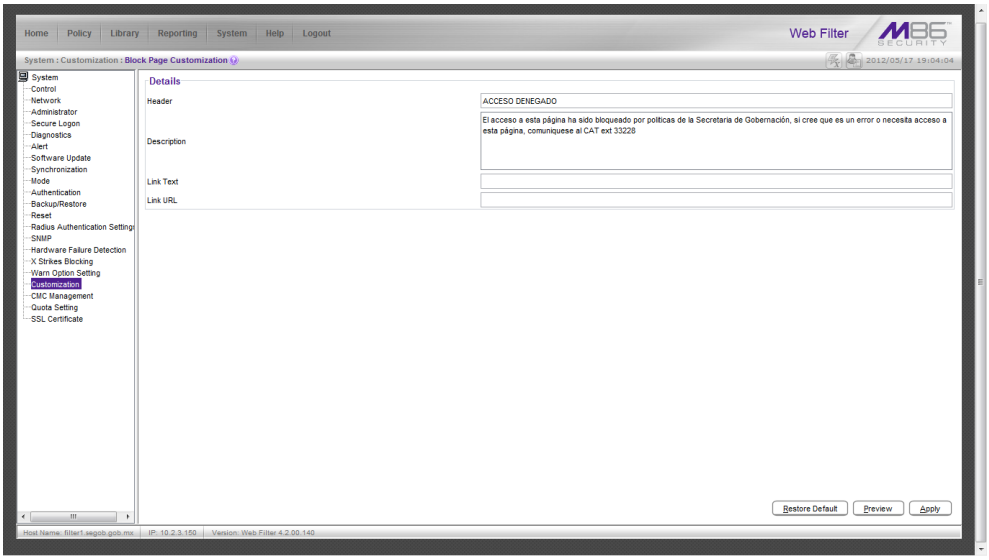


Imagen 5.14 Configuración de la página de bloqueo en WebFilter

Imagen 5.15 Página de Bloqueo

2.6.2 CONFIGURACIÓN REPORTEADOR EMPRESARIAL (Reporter)

Para configurar el Reporteador Empresarial es necesario ingresar a la interfaz gráfica de administración mediante un navegador http:// la ip que destinamos a la interfaz gráfica: y el puerto 88.

Configuración de Red para la Interfaz Gráfica

Previamente en consola elegimos una IP para LAN1 la cual se colocara nuevamente en la interfaz gráfica; además se deben completar otros campos, como se aprecia en la imagen.

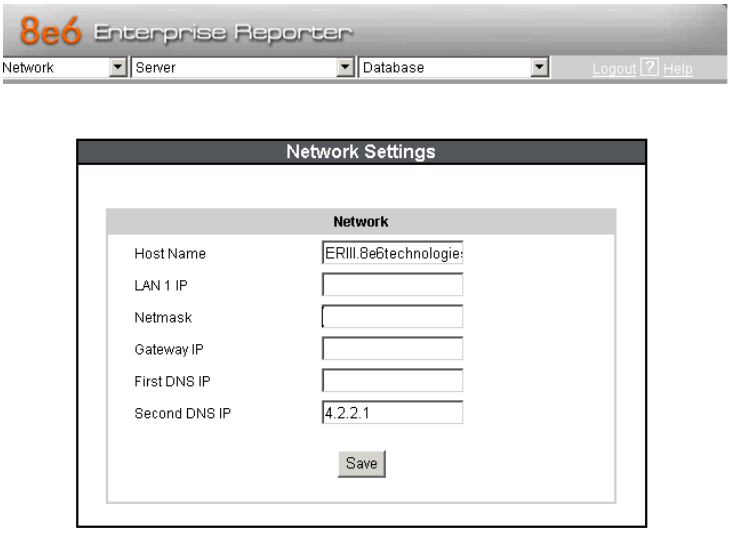


Imagen 6.0 Configuración de Red para la interfaz gráfica del Reporter

Cuentas de Usuario

Previo a la utilización del Reporteador Empresarial se deben generar cuentas de usuario en la modalidad de Administrador o Consultor.

Network→Administrators

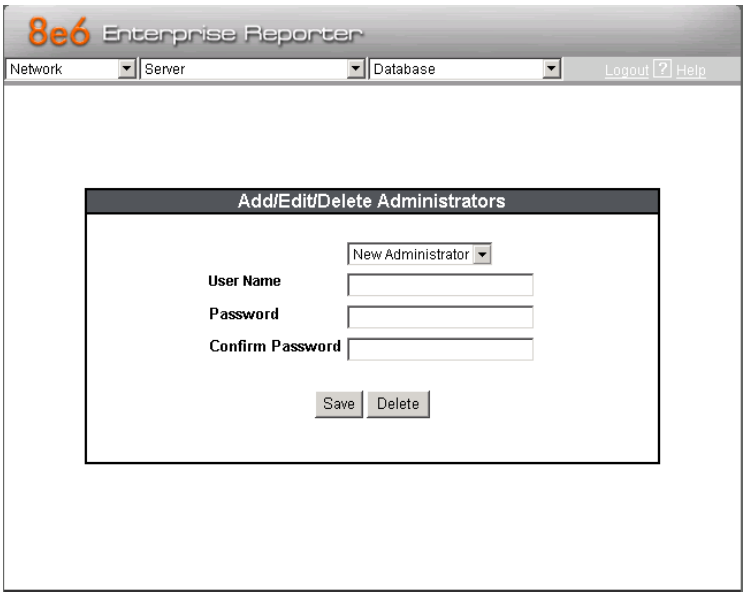


Imagen 6.1 Cuentas de Usuario para Reporter

Configuración Regional

Network→Regional Setting

En esta pantalla se configura el País o Región, el Idioma y el Servidor de NTP (Network Time Protocol) el cual sirve para mantener al equipo en la hora del país o de zona adecuada.

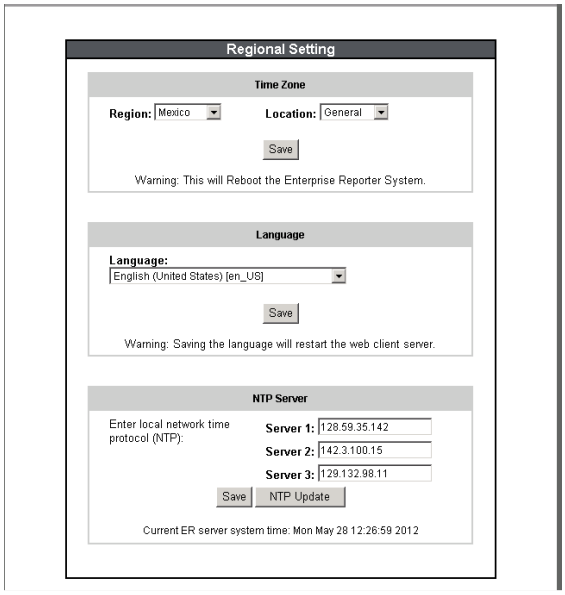


Imagen 6.2 Configuración Regional para Reporter

2.6.3 CONFIGURACIÓN REPORTEADOR DE ANÁLISIS DE RIESGOS (TAR)

El ingreso a la interfaz gráfica del Reporteador de Análisis de Riesgos (TAR) se realiza mediante un navegador de internet poniendo https:// la ip que destinamos a la interfaz gráfica: y el puerto 8443

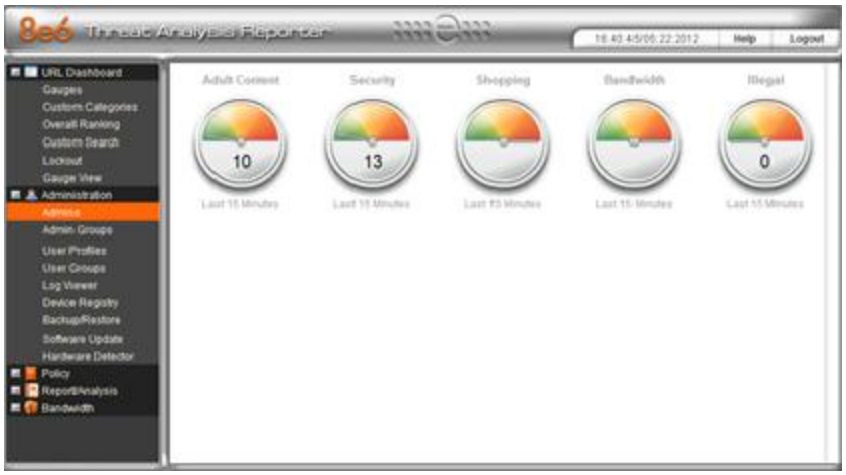


Imagen 6.0 Pantalla representativa de TAR

Configuración de Administrador del Sistema

Administration →Admins

En esta pantalla vamos a definir al administrador o grupo de administradores del sistema, los cuales podrán consultar en tiempo real el monitoreo del tráfico de la red de SEGOB.

Imagen 7.1 Configuración de Administradores de Sistema

Indicadores

En el reporteador de análisis de riesgos se pueden definir nuevos indicadores, los cuales se agregan de la siguiente manera:

Gauges→ Gauges Management →Add Gouge Group

Antes de proceder a editar el nuevo indicador se elije la categoría a agregar.

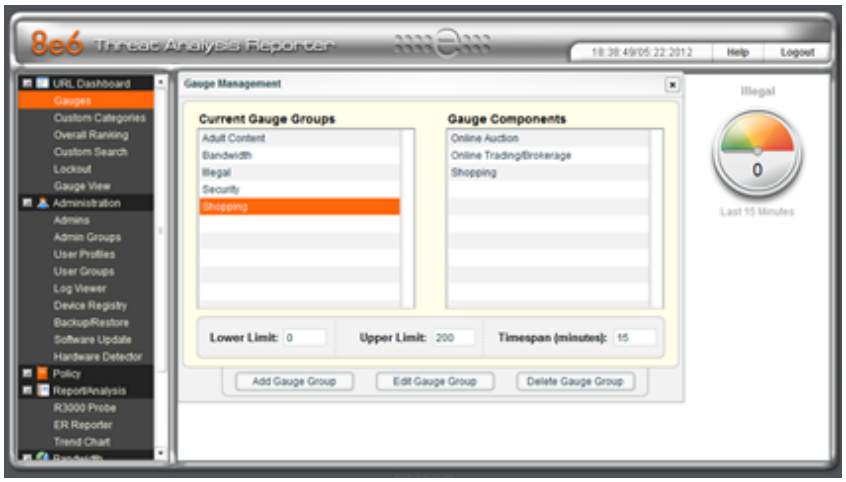


Imagen 7.2 Indicadores de riesgos de TAR

Posteriormente se define el nombre del nuevo indicador y los limites de intentos en un intervalo de tiempo.

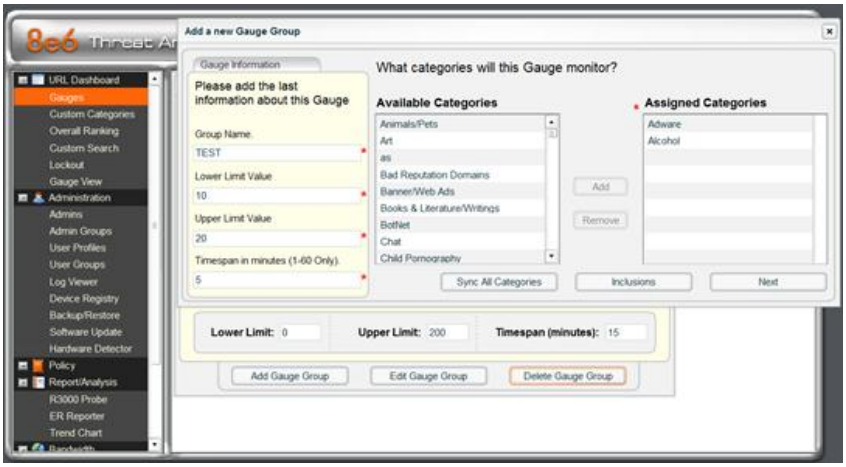


Imagen 7.3 Nombre de Indicador de Riesgo

Una vez elegida la categoría del nuevo indicador, podremos ver las subcategorías a agregar.

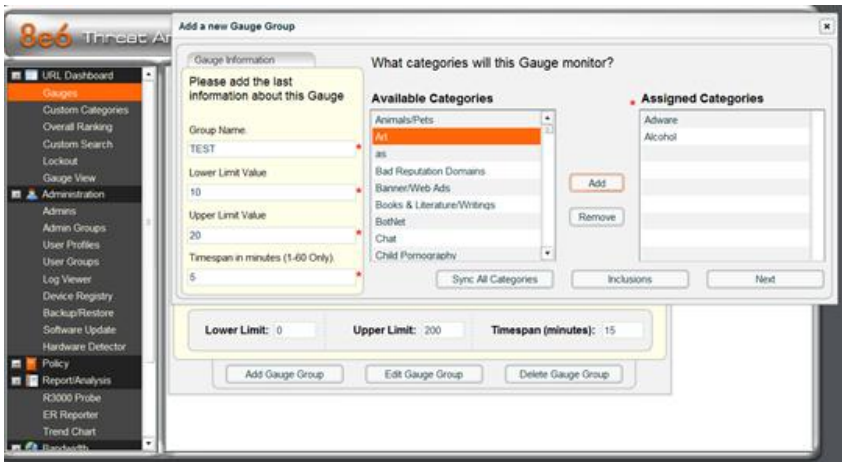


Imagen 7.4 Categoría de Indicador de Riesgo

Agregamos la nueva subcategoría al indicador llamado **"TEST"** para este caso en particular y seleccionamos **Add → Next**

Imagen 7.5 Subcategoría de Indicador de Riesgo

Nuestro nuevo indicador ya podrá entregar reportes de las subcategorías seleccionadas.

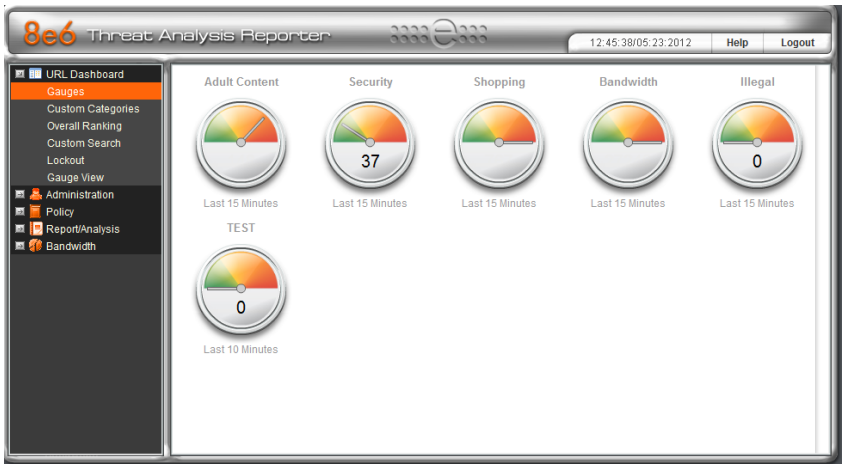


Imagen 7.6 Nuevo Indicador de Riesgo de TAR

Registro de Dispositivos

En esta pantalla se verifica la conexión de la solución 8e6; es decir se comprueba el estado de los equipos conectados WebFilter, Reporter y TAR.

Administration→Device Registry

Imagen 7.7 Registro de Dispositivos 8e6

Actualizaciones de Software

En la configuración inicial es necesario verificar si existen actualizaciones disponibles, debido a que el equipo debe estar actualizado en su versión mas reciente antes de comenzar su operación; las actualizaciones y sus bitácoras (logs) las encontramos en:

Administration→Software Update→ Install New Patches

Administration→Software Update→View Software Update Log

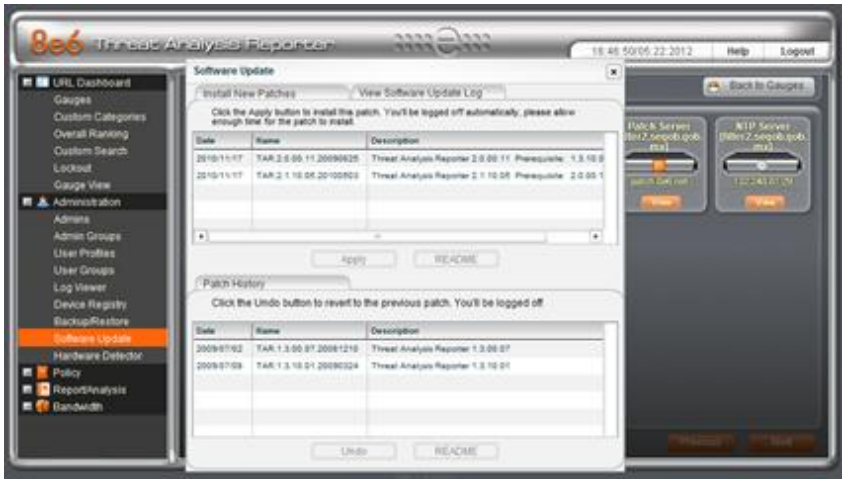


Imagen 7.8 Actualizaciones de Software

2.7 GENERACIÓN DE GRUPO DE CONTROL DE NAVEGACIÓN EN FILTRADOR DE CONTENIDO WEB (WebFilter)

Policy→IP (click secundario)

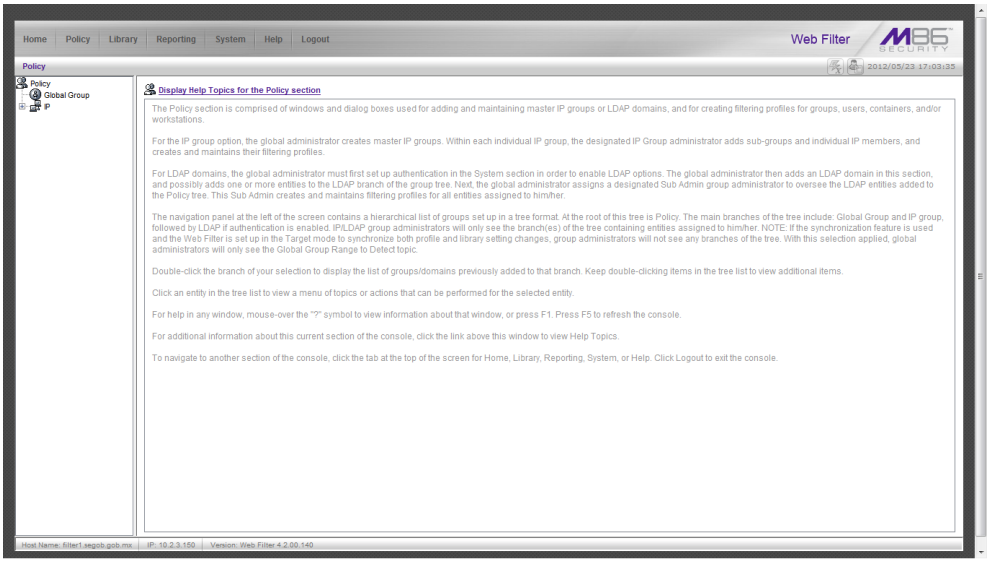


Imagen 7.0 Generación de Grupo de Control de Navegación WebFilter

Add Group

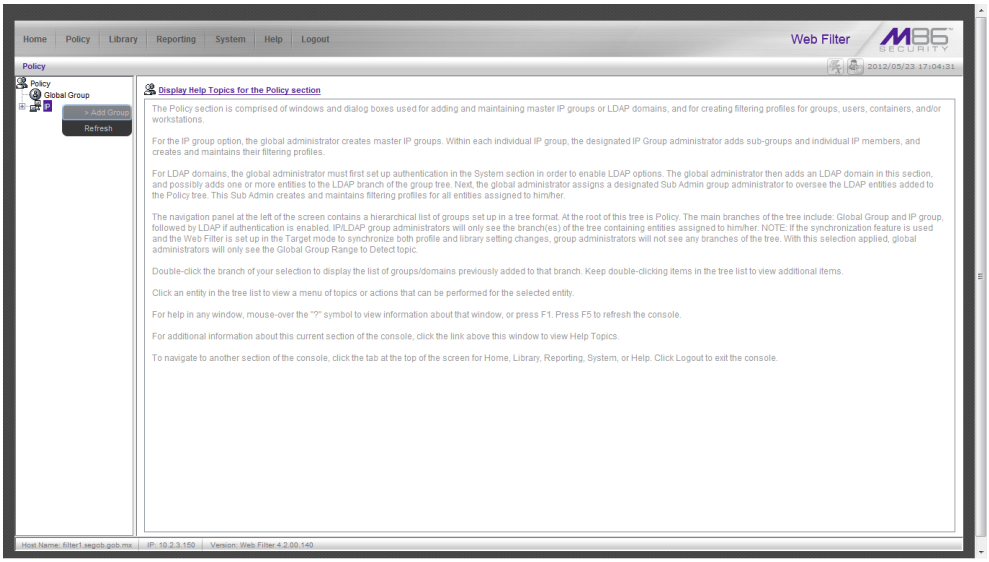


Imagen 8.1 Agregar Grupo de Control de Navegación

En esta sección se define el nombre de nuestro nuevo grupo y se le asigna una contraseña, la cual debe ser alfanumérica, de 8 caracteres incluyendo por lo menos un carácter especial.

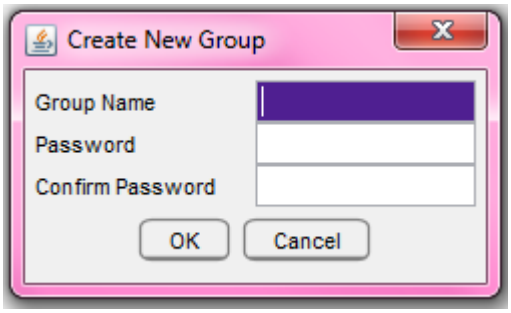


Imagen 8.2 Datos del Grupo de Control de Navegación

Perfil de Navegación

Una vez creado el grupo, se configura el perfil de navegación.

Posicionándonos sobre el grupo nuevo **TEST1→ Group Profile**

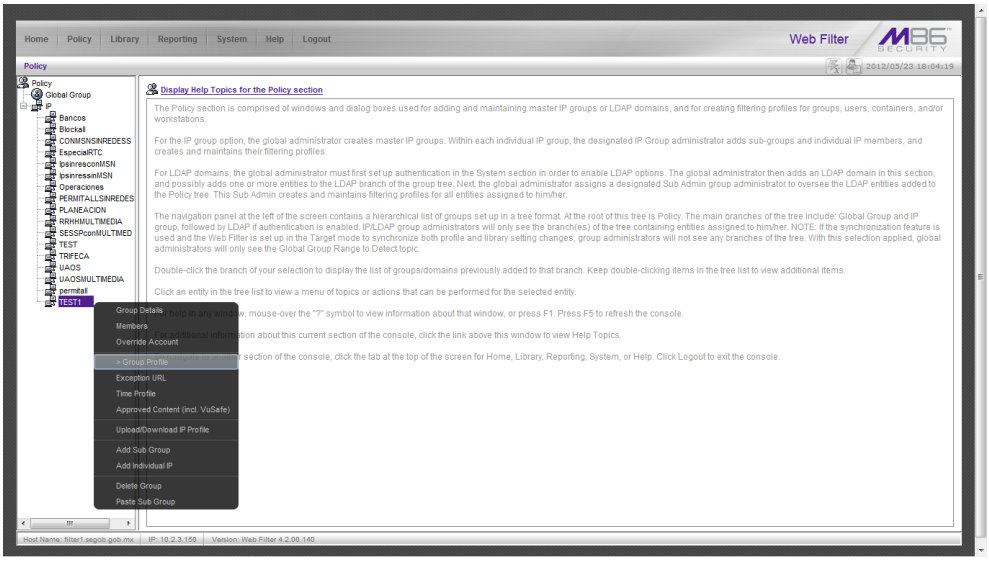


Imagen 8.3 Configuración de Perfil de Navegación

Como se puede apreciar en la siguiente pantalla todas las categorías y subcategorías de navegación están en nivel **"pass"** lo que permite personalizar el grupo de acuerdo a nuestras necesidades de filtrado; o bien en la sección **"Available Filter Levels"** podemos encontrar las reglas de los grupos anteriores en caso de querer que el nuevo grupo cuente con los mismos privilegios de navegación que uno anterior.

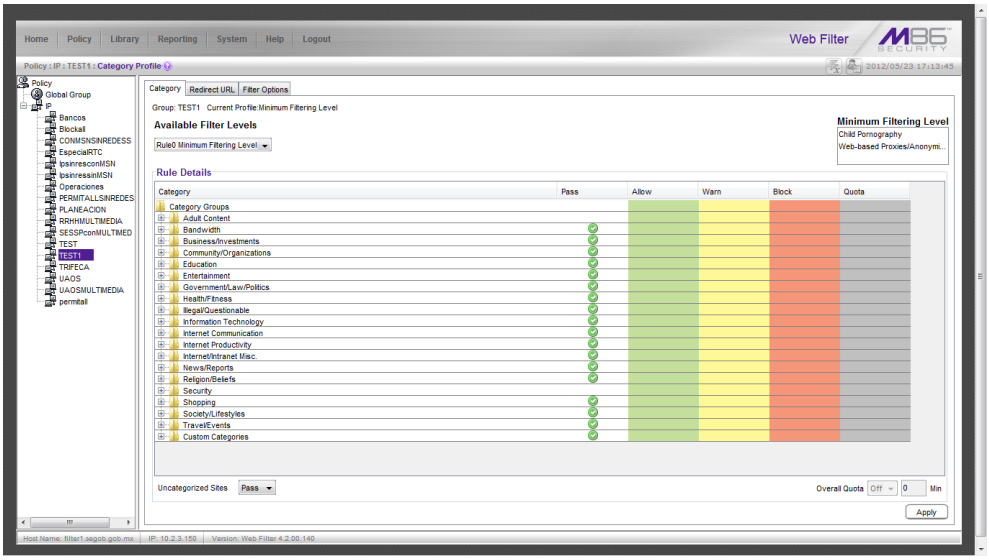


Imagen 8.4 Categorías de Control de Grupo de Navegación

Para personalizar el grupo debemos abrir cada una de las categorías y subcategorías para permitirlas o denegarlas; como se muestra en la imagen.

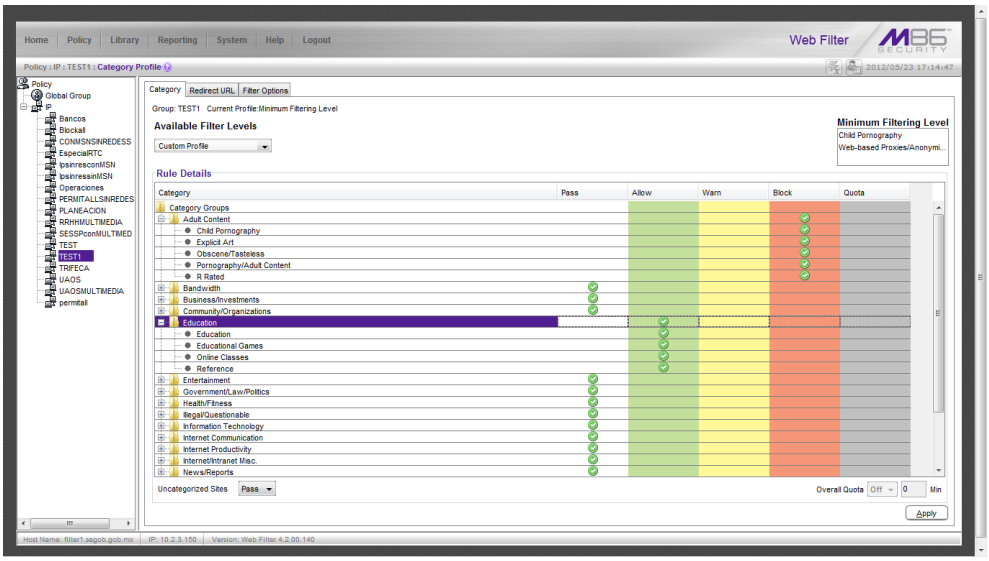


Imagen 8.5 Subcategorías de Control de Grupo de Navegación

El siguiente paso será agregar miembros al grupo.

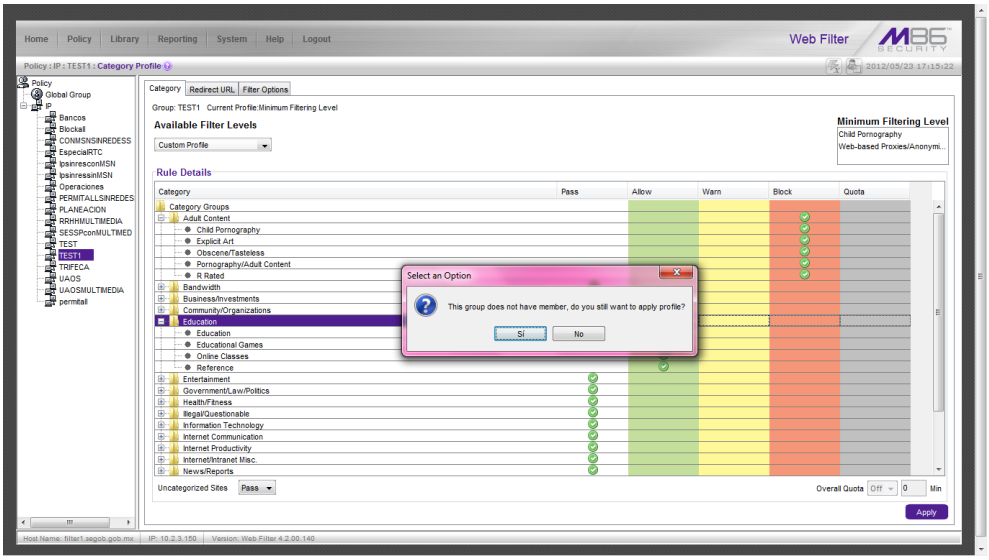


Imagen 8.6 Grupo de Control de Navegación Finalizado

Miembros de Grupo

Grupo al que se desea agregar→Members

En caso de ser solo una ip seleccionamos la opción **"Source IP"** colocamos la Ip en el recuadro, con su mascara de red; en caso de ser un segmento de red seleccionamos **"Source IP Start"** para colocar la Ip donde comienza el segmento y después de **"End"** la Ip donde termina.

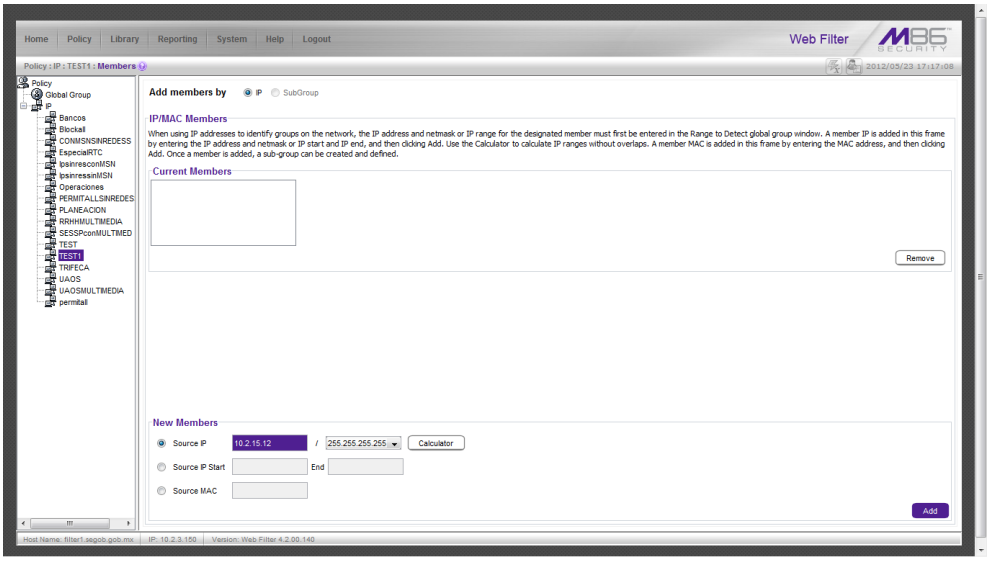


Imagen 8.7 Miembros de Grupo de Control de Navegación

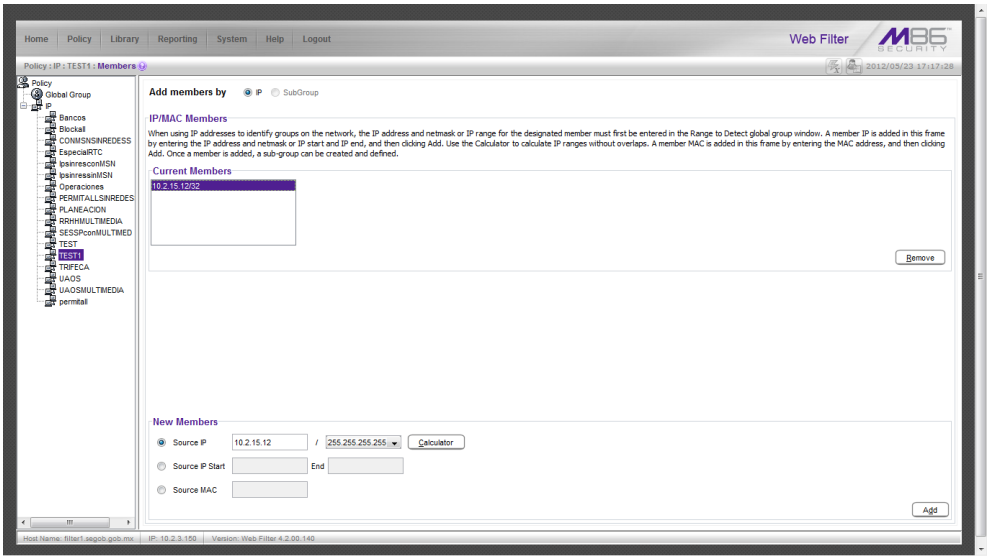


Imagen 8.8 Dirección Ip Asignada a un Grupo de Control de Navegación

2.7.1 PERSONALIZACIÓN DE UN GRUPO DE CONTROL DE NAVEGACIÓN EN FILTRADOR DE CONTENIDO WEB (WebFilter)

Ejemplo de Personalización para grupo de control SINMSN

Category			**Pass**	**Allow**	**Warm**	**Block**
Adult Content						true
	Child Pornography					true
	Explicit Art					true
	Obscene/Tasteless					true
	Pornography/Adult Content					true
	R Rated					true
Bandwidth						
	Image Servers & Image Search Engines			true		
	Internet Radio			true		
	March Madness Streaming		true			
	Peer-to-peer/File Sharing					true
	Video Sharing					true
	VoIP					true
	Web Based Storage			true		
	Streaming Media					
		Flash Video		true		
		Generic Streaming Media		true		
		March Madness Streaming	true			
		QuickTime Video		true		
		Real Time Streaming Protocol				true
		Windows Media Video				true
Business/Investments				true		

Category			Pass	Allow	Warm	Block
	Employment			true		
	Financial Institution			true		
	General Business			true		
	Online Trading/Brokerage			true		
	Real Estate			true		
Community/Organizations				true		
	Community Organizations			true		
	Local Community			true		
Education				true		
	Education			true		
	Educational Games			true		
	Online Classes			true		
	Reference			true		
Entertainment						
	Art			true		
	Comics			true		
	Entertainment			true		
	Gambling					true
	Humor			true		
	Kids			true		
	Movies & Television			true		
	Music Appreciation			true		
	Online Greeting Cards			true		
	Restaurant/Dining			true		
	Theater			true		
	Games					true
		Games				true

Category			Pass	Allow	Warm	Block
		Games Patterns				true
Government/Law/Politics				true		
	Government			true		
	Legal			true		
	Military Appreciation			true		
	Military Official			true		
	Political Opinion			true		
Health/Fitness				true		
	Fitness			true		
	Health/Medical			true		
	Holistic			true		
	Self Help			true		
Illegal/Questionable						true
	Criminal Skills					true
	Dubious/Unsavory					true
	Hate & Discrimination					true
	Illegal Drugs					true
	Terrorist/Militant/Extremist					true
Information Technology						
	Dynamic DNS Services			true		
	Freeware/Shareware					true
	Information Technology			true		
	Internet Service Provider			true		
	Portals			true		
	Search Engines			true		
	Web Based Newsgroups			true		

Category			Pass	Allow	Warm	Block
Internet Communication						
	Chat			true		
	Message Boards					true
	Online Communities			true		
	Translation Services			true		
	Web Based Email			true		
	Web Logs/Personal Pages			true		
	Web-Based Productivity Apps			true		
	Instant Messaging (IM)					
		Generic IM				true
		Google Chat		true		
		Google Talk		true		
		ICQ & AIM				true
		IRC				true
		Meebo				true
		My Space IM				true
		PoPo				true
		QQ				true
		ToToMoMo				true
		WangWang				true
		Windows Live Messenger		true		
		Yahoo IM		true		
Internet Productivity						
	Adware			true		
	Banner/Web Ads			true		
	Fantasy Sports			true		
	Free Hosts			true		

Category			Pass	Allow	Warm	Block
	Web Hosts			true		
	Remote Access					true
		Generic Remote Access				true
		GoToMyPC				true
		Remote Desktop				true
		Secure Shell (SSH)				true
		Virtual Network Computing				true
		pcAnywhere				true
Internet/Intranet Misc.				true		
	Domain Landing			true		
	Edge Content Servers/Infrastructure			true		
	Invalid Web Pages			true		
	Reviewed/Miscellaneous			true		
News/Reports						
	March Madness News		true			
	News			true		
	Sports			true		
	Weather/Traffic			true		
Religion/Beliefs				true		
	Paranormal			true		
	Religion			true		
Security						true
	Bad Reputation Domains					true
	BotNet					true
	Hacking					true
	Malicious Code/Virus					true
	Phishing					true

Category			Pass	Allow	Warm	Block
	Spyware					true
	Web-based Proxys/Anonymizers					true
Shopping				true		
	Online Auction			true		
	Shopping			true		
Society/Lifestyles				true		
	Alcohol			true		
	Animals/Pets			true		
	Books & Literature/Writings			true		
	Dating/Personals			true		
	Fashion			true		
	Lifestyle & Culture			true		
	Recreation			true		
	Self Defense			true		
	Weapons			true		
Travel/Events				true		
	Tickets			true		
	Travel			true		
	Vehicles			true		
Custom Categories						
	DECLARA			true		
	Intranet/Internal Servers			true		
	MicrosoftUpdate		true			
	Sitio Bloqueados					true
	sitios no bloqueados			true		

Tabla 7.0 Personalización de un Grupo de Control de Navegación en WebFilter

2.8 DEFINICIÓN DE GRUPOS DE NAVEGACIÓN

El sistema de filtrado en Proxy Squid´s, se basaba en reglas de acceso, en su principio cubría las necesidades básicas de la Secretaria.

Estos grupos delimitaban el acceso de la siguiente manera, detallados en el capítulo “Marco Referencial del Servicio de Internet de la Secretaria de Gobernación”

- Permitir correos y Chats
- Permitir todas aplicaciones y todas las páginas web

Grupos de control del equipo de filtrado Web 8e6

Tomando en cuenta las restricciones anteriores y las nuevas necesidades de Filtrado de la Web para la Institución, se llego a la conclusión que con los equipos 8e6 se tenia la capacidad para hacer grupos de control de navegación mas completos, por lo que se procedió a rediseñar los grupos existentes y crear nuevos grupos que cubrieran las expectativas de las áreas al usar el Internet.

Quedando creados los grupos de la siguiente manera:

- ☐ Bancos — Grupo con acceso exclusivo a Bancos.
- ☐ Blockall — Grupo con bloqueo de Internet.
- ☐ Conmsnsinredes — Grupo con acceso a MSN, sin redes sociales.
- ☐ EspecialRTC — Grupo especial para el área de RTC[6].
- ☐ IpsinresconMSN — Grupo con acceso a MSN y redes sociales.
- ☐ IpsinressinMSN — Grupo sin acceso a MSN, sin redes sociales.
- ☐ Operaciones — Grupo especial de DGTI[7].
- ☐ Permitallsinredessoc — Grupo con Multimedia, sin redes sociales.
- ☐ Planeacion — Grupo del C.Secretario y altos funcionarios.
- ☐ Rrhhmultimedia — Grupo especial para el área de Recursos Humanos.
- ☐ Sesspconmultimed — Grupo especial para el SESSP[8]
- ☐ Trifeca — Grupo especial para TRIFECA[9]
- ☐ Uaos — Grupo especial para la UAOS[10]
- ☐ Permitall — Grupo con acceso a MSN, Redes Sociales, Multimedia.

[6] RTC.- Radio, Televisión y Cinematografía.
[7] DGTI.- Dirección General de Tecnologías de la Información.
[8] SESSP.- Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública
[9] TRIFECA.- Tribunal Federal de Conciliación y Arbitraje.
[10] UAOS.- Unidad para la Atención de las Organizaciones Sociales.

Pantalla representativa del WebFilter donde se aprecian los grupos creados.

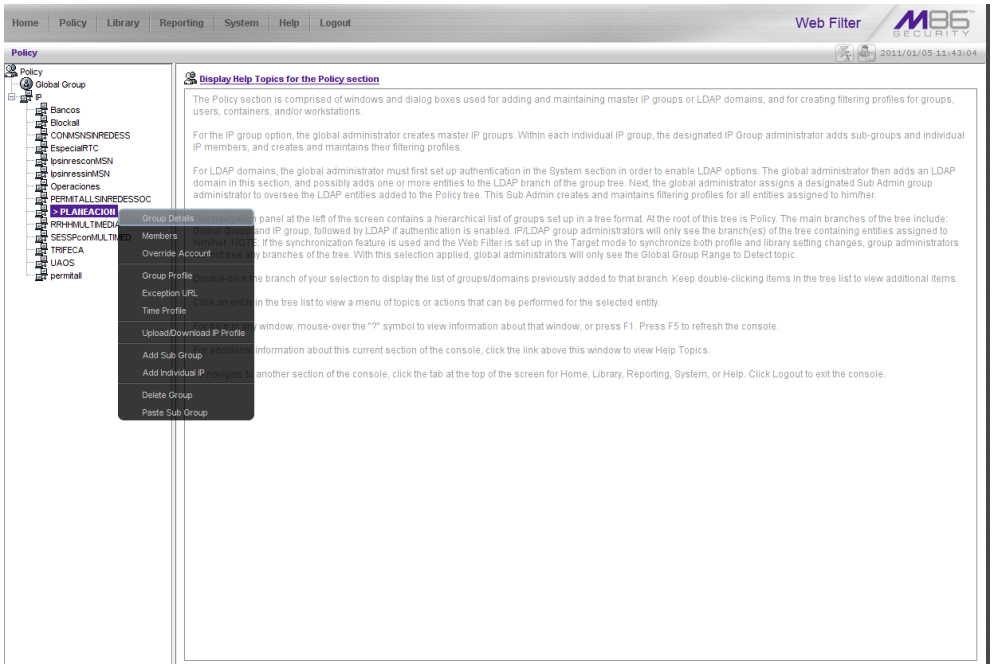


Imagen 8.0 Pantalla Representativa de WebFilter con Grupos de Control de Navegación

2.8.1 PRIVILEGIOS DE NAVEGACIÓN DE LOS GRUPOS DE CONTROL

Bancos

El grupo “BANCOS” fue creado para el área de Finanzas de la SEGOB debido a que el personal de dicha unidad presento un incidente de seguridad donde por phishing intentaron tomar las claves bancarias del área para realizar un fraude; por tal motivo se decidió restringir el acceso para que la unidad únicamente pudiera consultar en Internet sitios de bancos.

Blockall

En este grupo se encuentran todas aquellas Ips que no requieren acceso a internet por las funciones propias de su área, aunque originalmente fue diseñado con esa función en la actualidad también es utilizado para colocar aquellas Ips que contaban con privilegios de navegación pero que por alguna cuestión de seguridad se han colocado ahí temporalmente.

Conmsnsinredes

En este grupo se encuentran todas aquellas Ips que por sus funciones requieren acceso a mensajería instantánea, consulta de correos externos (Hotmail, Yahoo, Gmail, entre otros) y Motores de Búsqueda, sin acceso a Redes Sociales y contenido multimedia.

EspecialRTC

Este grupo fue creado para la unidad administrativa RTC (Radio, Televisión y Cinematografía) los cuales por sus actividades requieren constante navegación en páginas con contenido multimedia, incluso en páginas que pudieran estar catalogadas como ociosas; por lo cual las Ips contenidas en el grupo tienen acceso a Mensajería Instantánea, Correos Externos, Redes Sociales, Multimedia, motores de búsqueda, entre otras.

Ipsinresconmsn

En este grupo se encuentran todas las Ips que por sus actividades tienen acceso a Correos Externos, Mensajería Instantánea, Redes Sociales y Motores de Búsqueda.

Operaciones

El grupo fue creado para la unidad administrativa DGTI (Dirección General de Tecnologías de la Información), teniendo permitido el acceso a SSH (Secure Shell), Correos Externos, Mensajería Instantánea, Redes Sociales, Motores de Búsqueda y Contenido Multimedia.

Permitallsinredessoc

Dicho grupo fue creado para solventar la problemática de algunas unidades que requerían acceso a navegación amplia, ingresando a páginas con contenido Multimedia, Mensajería instantánea, Correos Externos pero que requerían restringir las Redes Sociales por el tiempo que invierten en ellas los usuarios.

Planeación

Es un grupo de navegación en el que se encuentra la Ip del Secretario de Gobernación y colaboradores más cercanos, sin restricciones para la consulta de páginas Web, debidas a las funciones que realizan los funcionarios.

Rrhhmultimedia

Grupo generado para personal de la Dirección de Recursos Humanos; el cual tiene acceso a Correos Externos, Mensajería Instantánea, Motores de Búsqueda y Contenido Multimedia.

Sesspconmultimedia

Originalmente el grupo de navegación fue creado para todas aquellas Ips provenientes del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, teniendo consultas a Correos Externos, Mensajería Instantánea, Motores de Búsqueda, Redes Sociales y Contenido Multimedia; pero ante la sobre explotación de los recursos para navegación se redujo, ingresando dichas Ips en alguno de los grupos de control antes mencionados, quedando aquí únicamente las direcciones Ip del Secretariado que por sus funciones requirieran el perfil de navegación establecido.

Trifeca

Grupo generado para la navegación del Tribunal Federal de Conciliación y Arbitraje, únicamente pueden consultar las páginas que mediante correo electrónico su enlace informático nos solicita, las cuales tienen información referente a leyes y códigos civiles, laborales.

Uaos

Grupo generado para las Ips pertenecientes a la Unidad para la Atención de las Organizaciones Sociales, con navegación a Motores de Búsquedas y a URL´s que mediante su enlace informático nos solicitan.

Permitall

Grupo generado para todas aquellas Ips que requieran navegación a páginas con Contenido Multimedia, Correos Externos, Mensajería Instantánea, Motores de Búsqueda y Redes Sociales.

2.9 MIGRACIÓN DE LOS EQUIPOS HACIA LA SOLUCIÓN 8E6

Con la creación de los grupos de control de navegación y los listados de las Ips del personal de SEGOB, donde definían responsable y necesidad de navegación los cuales fueron entregados por cada enlace informático se procedió a capturar todas las Ips al Filtrador de Contenido Web (WebFilter) en el grupo de control que les correspondía según la lista.

Cabe destacar que aunque todas las Ips fueron capturadas en el Filtrador aún se encontraban en los Proxys de la SEGOB puesto que era necesario capacitar al CAT (Centro de Atención Técnica) para la recepción y atención de comentarios o reportes respecto al nuevo servicio de navegación; la capacitación se llevo a cabo mediante una presentación *(Anexo1 "Implementación de Equipos de Seguridad para Internet")* donde se explicaba a detalle el funcionamiento de los equipos WebFilter, Reporter y TAR.

Simultáneamente se coordinó a los enlaces informáticos para que en el lapso de 2 semanas a partir de la captura de las Ips al filtrador de contenido eliminaran de los navegadores web de todos los equipos de la Secretaria la configuración del Proxy; ya que al concluir el tiempo establecido se apagarían los Proxys y de existir algún equipo que conservara la configuración anterior no tendría la posibilidad de navegar a Internet.

2.10 INFRAESTRUCTURA DEL SERVICIO DE INTERNET DE LA SEGOB ACTUAL

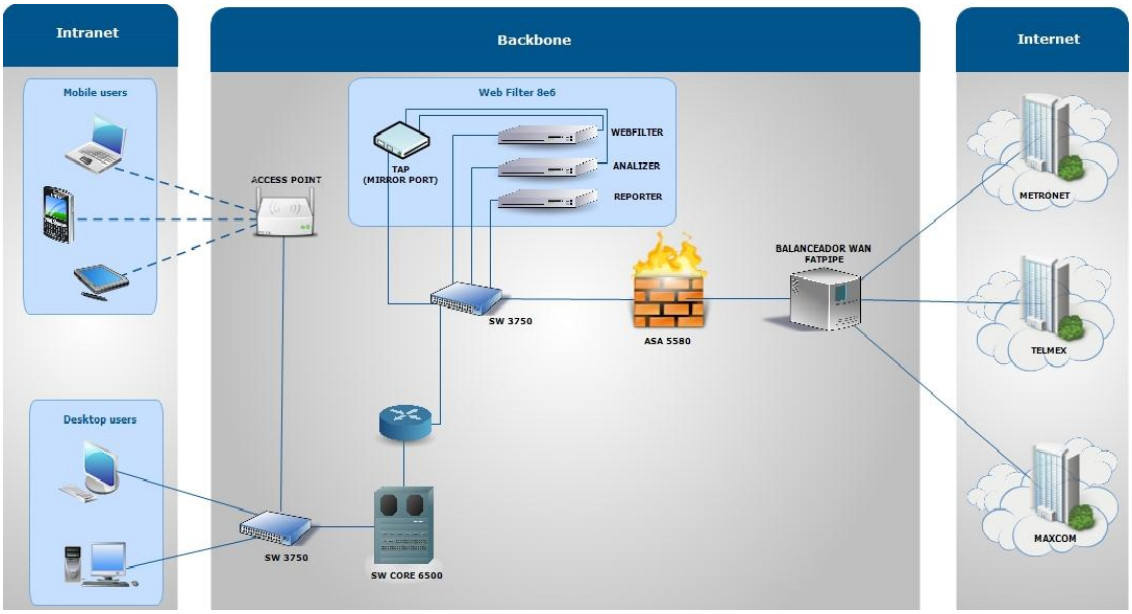


Diagrama 4.0 Infraestructura del Servicio de Internet de la SEGOB Actual

Como se puede apreciar el diagrama, muestra la conexión para Internet, donde se visualiza la red la SEGOB la cual funciona de la siguiente manera:

Todos los usuarios de la Red de SEGOB alámbricos o móviles para su salida a Internet están conectados a switch´s auxiliares los cuales a su vez se interconectan al site de Telecomunicaciones a un switch de core 6500 el cual se encarga de distribuir los paquetes clasificando el tipo de salida, en interna o hacia Internet, una vez clasificada la salida el router direcciona los paquetes de salida hacia internet al switch 3750.

El equipo tap se encarga de espejear el tráfico por diferentes puertos al WebFilter y Analizer equipos 8e6, alimentándose de la información del switch 3750; posteriormente el WebFilter analiza la ip origen, el destino del paquete y valida en su base de datos si tiene permitido el acceso a dicho destino; de ser así no hace nada; en caso contrario le manda un tcp reset a la conexión (deteniendo los paquetes de datos para que no lleguen a destino) y un redirect a nuestro sitio de seguridad.

Como comentamos si la conexión es válida el siguiente filtro es el Firewall que de igual forma valida (únicamente ip y puertos) en sus tablas si tiene permitida esa conexión en caso de ser así la deja pasar; caso contrario se interrumpe la conexión; las conexiones validas llegan al equipo fatpipe el cual no hace distinción de protocolo, origen o destino únicamente balancea las conexiones a nuestros 3 enlaces de internet.

Cabe destacar que el Filtrado de contenido Web sólo es aplicable a las peticiones externas a la red; ya que la navegación a sitios internos no se tiene restricción alguna; es decir no pasan por el equipo de filtrado.

CAPÍTULO 3. PRUEBAS Y ADECUACIÓN DE LA SOLUCIÓN 8e6 A LAS CONDICIONES IMPREVISTAS

3.1 PRUEBAS DE FUNCIONALIDAD DEL FILTRADO DE CONTENIDO (WebFilter)

Para realizar las pruebas de funcionalidad del WebFilter se eligieron 10 direcciones Ips, 5 pertenecientes al enlace de Internet de Reforma y 5 del enlace de Bucareli, se configurarían en equipos del área de Seguridad Lógica; mismas que serian ingresadas en los distintos grupos de control de navegación, en cada uno a la vez probando sus privilegios de navegación, de esta forma podríamos validar si el equipo filtraba el contenido web de la manera deseada.

Prueba #1 “Búsqueda Segura”

Como se puede apreciar en la siguiente imagen donde se intenta mediante un motor de búsqueda acceder a pornografía, WebFilter fuerza al usuario a realizar búsquedas seguras al no regresar resultado alguno a la búsqueda inadecuada.

Imagen 9.0 Búsqueda Segura con WebFilter

Prueba #2 “Sin Acceso a Navegación Web con Contenido Multimedia”

Al colocar una Ip en un grupo el cual tiene restringida la navegación multimedia ingresa a el sitio de Tvolución el cual sirve para ver contenido multimedia (http://tvolucion.esmas.com); WebFilter le permitirá ver la página principal;

Imagen 10.1 Página Web con Contenido Multimedia

Sin embargo cuando el usuario intente acceder a los videos; WebFilter no le permitirá visualizar estos.

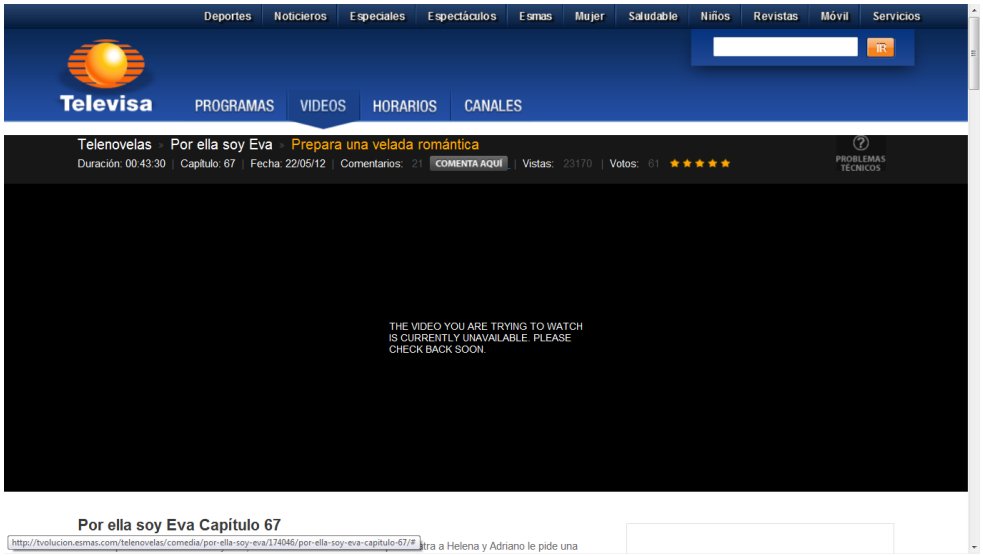


Imagen 10.2 Bloqueo de Visualización del Contenido Multimedia por WebFilter

Prueba #3 “Sin Acceso a Redes Sociales”

Al colocar una Ip en un grupo el cual tiene restringido el acceso a Redes Sociales y aunque el motor de búsqueda permita encontrar el sitio;

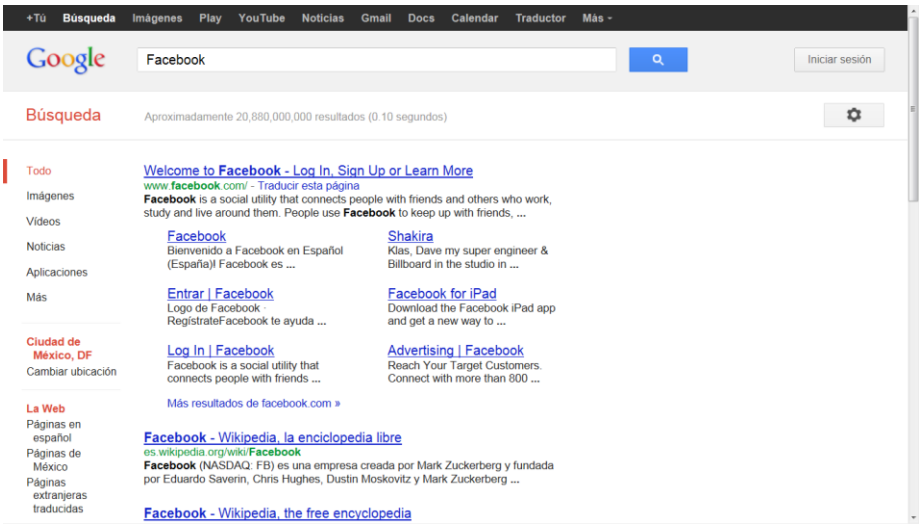


Imagen 10.3 Búsqueda de Red Social en Google

Al intentar ingresar, él usuario es redirigido a la página de seguridad de SEGOB.

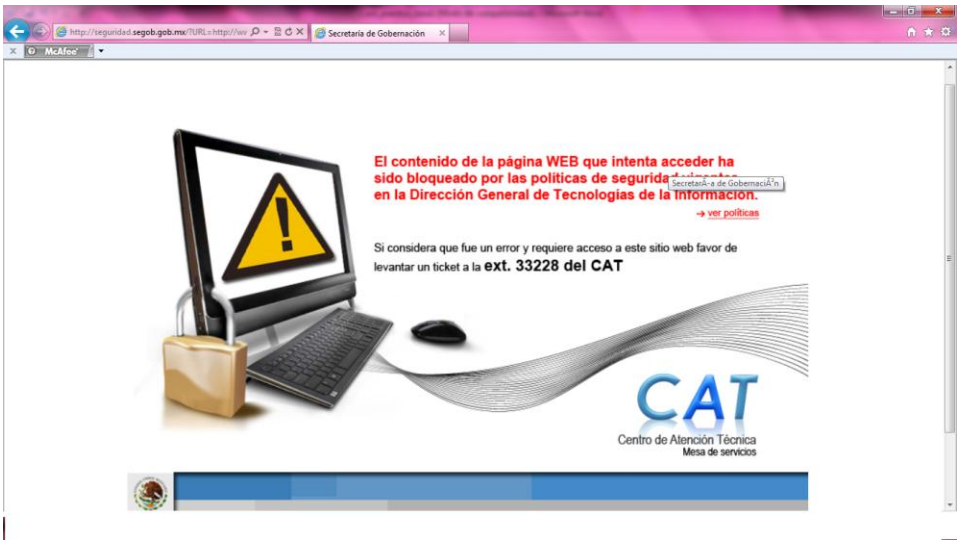


Imagen 10.4 Página de redirección del usuario cuando le faltan privilegios de Navegación

Nota: Las pruebas de filtrado para las 10 direcciones Ips fueron exitosas.

3.2 APAGADO DEL PROXY

El apagado del Proxy se realizó mediante una ventana de mantenimiento que contemplaba un fin de semana debido a que son días no laborables donde se podría identificar si el servicio de internet no tenía afectación.

Con el resultado exitoso de las pruebas de funcionalidad de filtrado con el WebFilter, y la confirmación de los enlaces informáticos de la eliminación de la configuración del proxy en los navegadores de todos los equipos de la SEGOB; se procedió a apagar el proxy.

Nuevamente se realizaron las pruebas mencionadas en el apartado “Pruebas de Funcionalidad del Filtrado de Contenido (WebFilter)” con el propósito de asegurar que el funcionamiento del WebFilter era el correcto sin estar de intermediario el proxy; Las pruebas fueron exitosas.

3.3 ADECUACIÓN DE LOS EQUIPOS 8e6 A LAS CONDICIONES IMPREVISTAS DE LA NAVEGACIÓN DE LA SEGOB

Como parte de la implementación de la solución del filtrado de contenido 8e6, se contempló un periodo de adaptación de los usuarios a la herramienta y viceversa con el objetivo de que la herramienta conociera la navegación de todos los usuarios para ir adecuando los parámetros según las necesidades inmediatas, con el fin de que esta solución no representará un bloqueo total para todas las áreas, sino una forma gradual para ir controlando los accesos a Internet con mínima supervisión y los accesos que requirieran permisos especiales de navegación.

Cabe resaltar que, durante el arranque de la solución, aun con los grupos ya formados, con los permisos establecidos y categorizados, se tomo la decisión que durante un tiempo razonable una o dos semanas por ejemplo, el filtrador de contenido trabajara en sus características mínimas permitiendo la mayoría del trafico cursado por la red, esto ayudaría primero a que el equipo de seguridad conociera nuevamente por área, el trafico que requiere para sus actividades, ajustar parámetros del equipo Filtrador de Contenido Web, Reporteador Empresarial y Reporteador de Análisis de Riesgos, dar tiempo de conocer más al equipo en tiempo real el trafico de la red y lo más importante que las solicitudes de desbloqueo de páginas y fallas detectadas por algún parámetro en el equipo, no

saturara al área de seguridad, ni al CAT (Centro de Atención Telefónica) con reportes que pudiera colapsar la solución con alguna decisión ejecutiva de quitar la herramienta y regresar a la solución anterior.

El caso más interesante que ejemplifica como se iba ajustando el equipo a la forma de navegación fue el siguiente:

Problema detectado:
No se pueden ver los videos de presidencia.gob.mx

Área afectada:
Todos los grupos de control del WebFilter con permisos multimedia.

Primera Validación:
Se validó con una red externa BAM/infinitum que los videos se visualicen correctamente y no sea una falla del sitio.

Prioridad:
Urgente, Se está dando un discurso importante del Presidente que requiere ser analizado por las aéreas interesadas.

Solución:
Como primer paso la liga www.presidencia.gob.mx se agregó a todos los grupos de control del WebFilter, esto con la finalidad de crear una excepción hacia ese sitio.

Se validó nuevamente que los usuarios pudieran entrar al sitio:

Respuesta negativa.

Se habilitaron los permisos de REAL PLAYER (esto analizando la página) con la finalidad que los permisos multimedia tuvieran acceso a ese tipo de transmisión.

Se validó nuevamente que los usuarios pudieran entrar al sitio:

Respuesta negativa.

Mediante una opción de ayuda del WebFilter llamada REAL TIME PROBE, se procedió a hacer el análisis del tráfico de UNA sola máquina dirigida hacia ese sitio, por 5 minutos que es el máximo tiempo que sugiere la marca para hacer esa captura de tráfico y no saturar el equipo.

El resultado de esa captura arrojo que había intentos de conexiones hacia un sitio diferente al de www.presidencia.gob.mx llamado USTREAM.US sitio que se encuentra dedicado a hacer transmisión en vivo.

Se agregó esa liga a los grupos de control del WebFilter y la **respuesta fue exitosa**, ya se podía ver los videos de Presidencia en internet, se llegó a la conclusión que Presidencia había alojado en una cuenta de USTREAM sus videos, por eso no podía visualizarlo los usuarios.

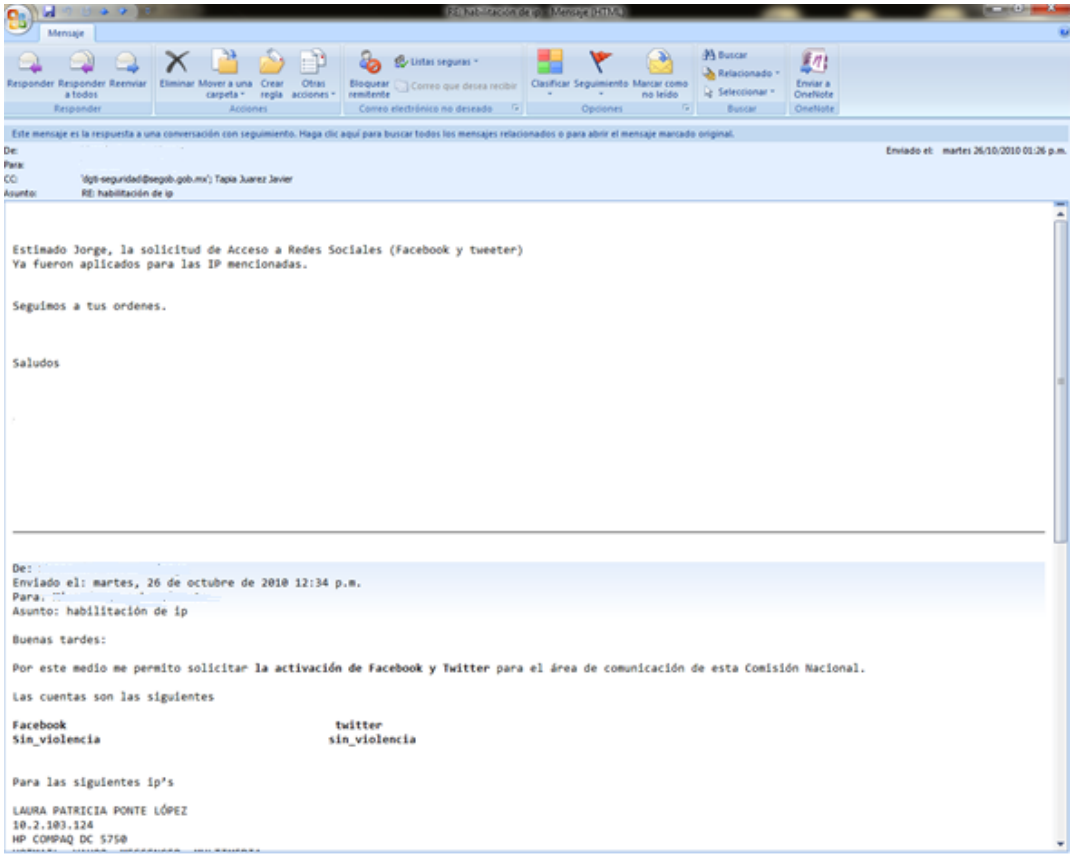
Posteriormente Presidencia alojo sus videos en YOUTUBE.COM como parte de su búsqueda de mejores opciones para hacer llegar sus videos a sus visitantes.

Se experimentó de este caso que con las herramientas y la capacitación adecuada se pueden resolver problemas que normalmente no se ven a simple vista.

3.4 MONITOREO Y CONTROL DE CAMBIOS

3.4.1 Filtrador de Contenido (WebFilter)

Solicitud de acceso a Redes Sociales para monitoreo de una cuenta de Twitter y Facebook de la CONAVIM (Comisión Nacional para Prevenir y Erradicar la Violencia contra las Mujeres).



Estimado Jorge, la solicitud de Acceso a Redes Sociales (Facebook y tweeter)
Ya fueron aplicados para las IP mencionadas.

Seguimos a tus ordenes.

Saludos

De:
Enviado el: martes, 26 de octubre de 2010 12:34 p.m.
Para:
Asunto: habilitación de ip

Buenas tardes:

Por este medio me permito solicitar **la activación de Facebook y Twitter** para el área de comunicación de esta Comisión Nacional.

Las cuentas son las siguientes

Facebook **twitter**
Sin_violencia **sin_violencia**

Para las siguientes ip's

LAURA PATRICIA PONTE LÓPEZ
10.2.103.124
HP COMPAQ DC 5750

Imagen 10.0 Justificación de Acceso a Redes Sociales

Se validan las Ips en el WebFilter y se cambian a un grupo de control con acceso a Redes Sociales.

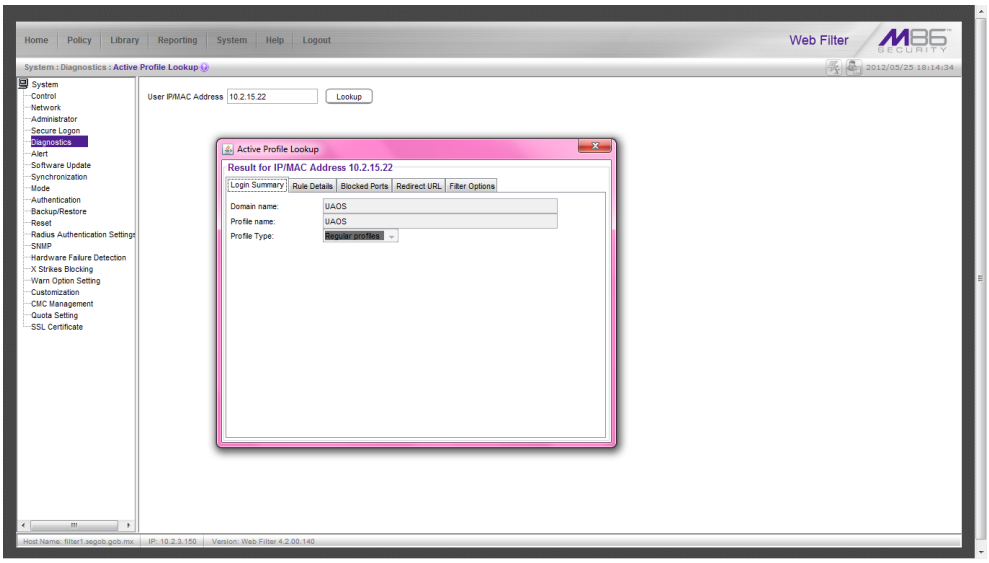


Imagen 11.1 Validación de Perfil de Navegación en WebFilter

En este correo se puede apreciar como el Enlace Informático de la UAOS (Unidad de Atención para las Organizaciones Sociales) requiere la liberación de una página para todo su grupo de control.

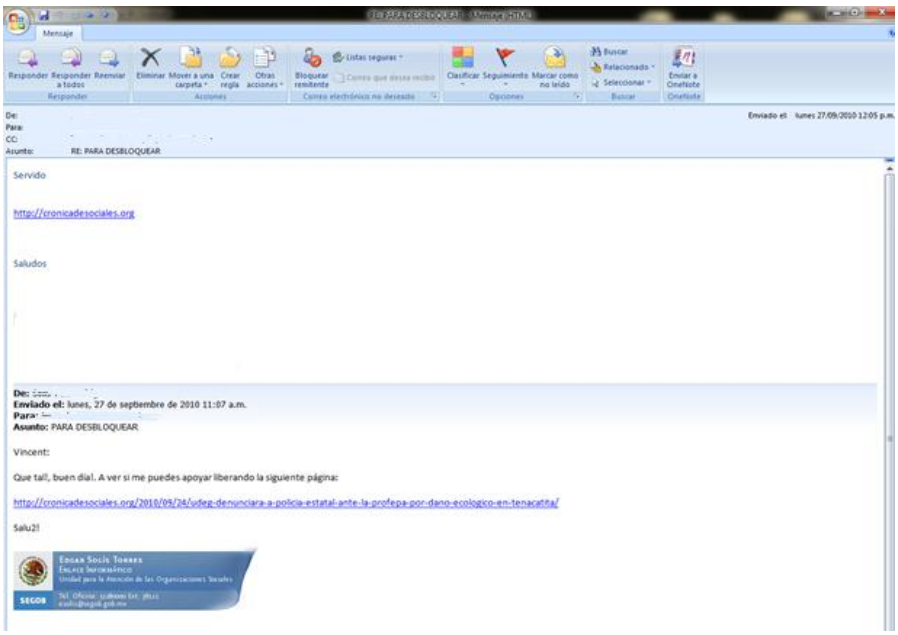


Imagen 11.2 Solicitud de Liberación de Página para Grupo de Control en WebFilter

En este caso se agrega la URL al grupo de control en cuestión; de la siguiente manera:

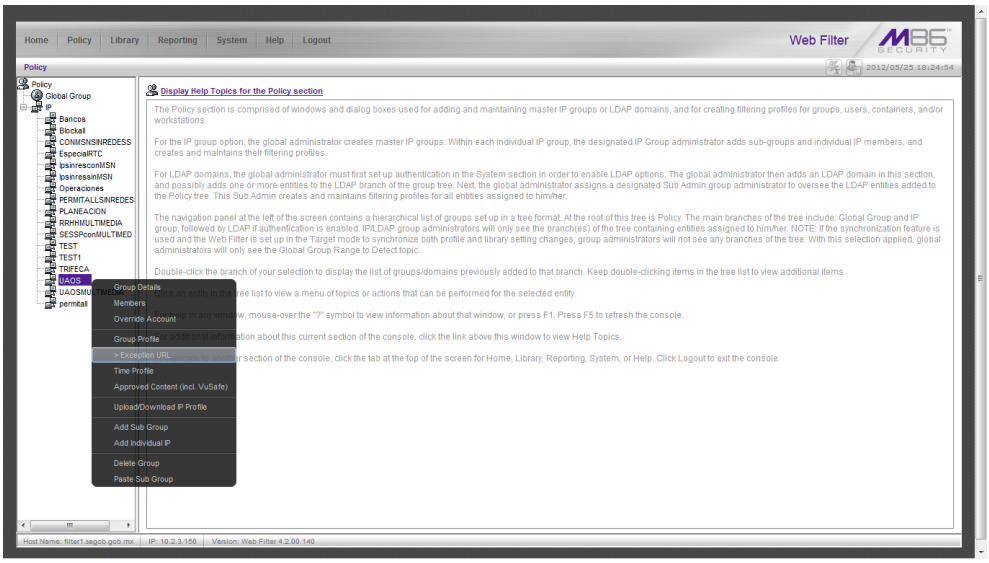


Imagen 11.3 Excepción a URL en Grupo de Control de Navegación en WebFilter

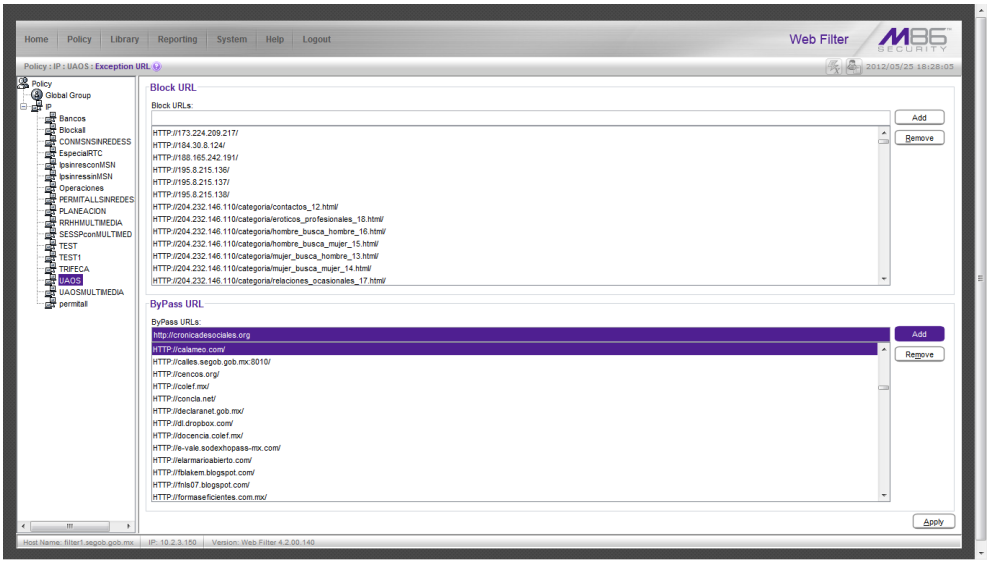


Imagen 11.4 Aplicación de la URL al Grupo de Control de Navegación

3.4.2 Reporteador Empresarial (Reporter)

Con el Reporteador empresarial podemos obtener reportes completos (diarios, semanales, mensuales) acerca del comportamiento de los usuarios que navegan en internet, gráficas de comportamiento en diferentes categorías, como las que se muestran a continuación.

Top 20 de los Usuarios que el equipo ha denegado el acceso a ciertas páginas.

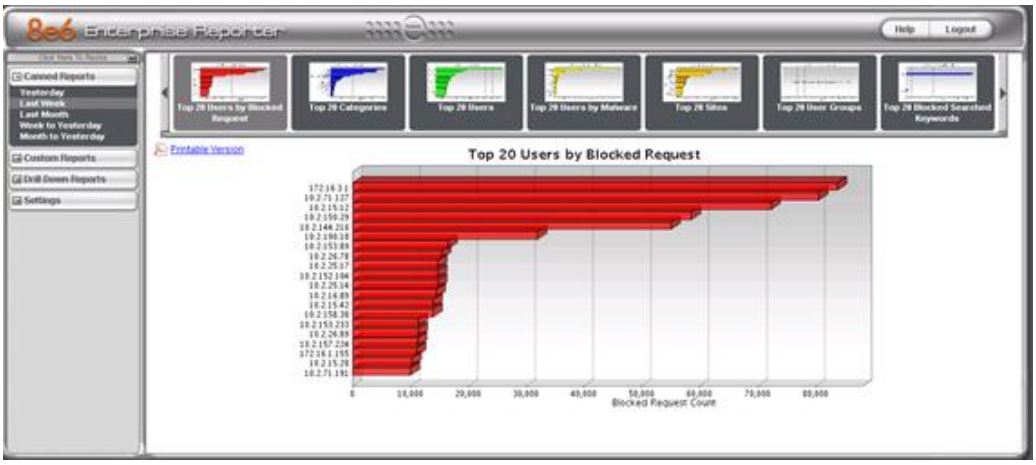


Imagen 12.0 Top 20 Usuarios con Peticiones Bloqueadas

Top 20 de las categorías de las páginas más consultadas por los usuarios; teniendo en primer lugar **"Noticias"**.

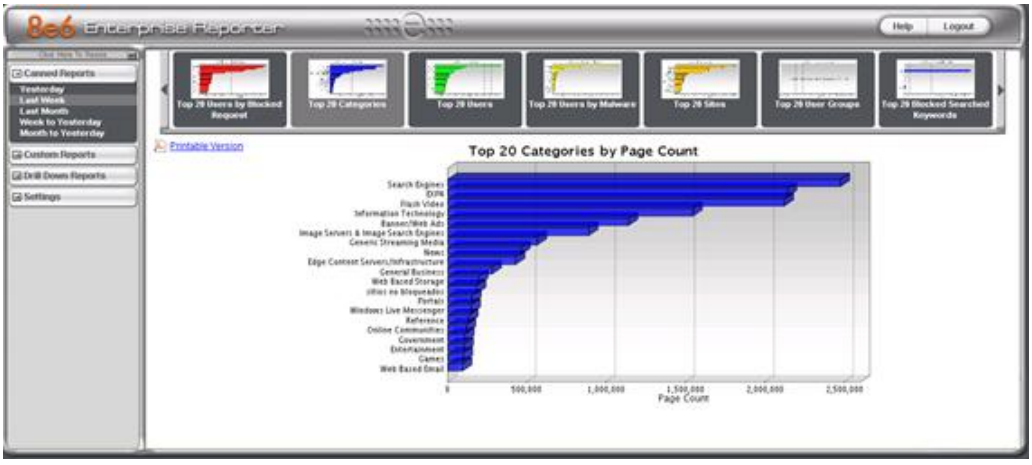


Imagen 11.1 Top 20 Categorías más consultadas

Top 20 de los Usuario que tienen mayor actividad en la Web.

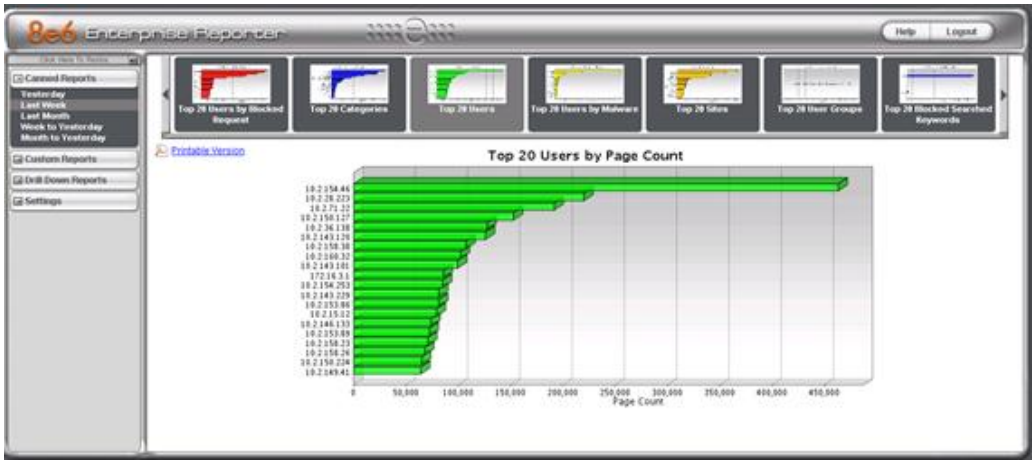


Imagen 12.2 Top 20 Usuarios con Mayor actividad en la Web

Top 20 de los Usuarios con descargas de Virus.

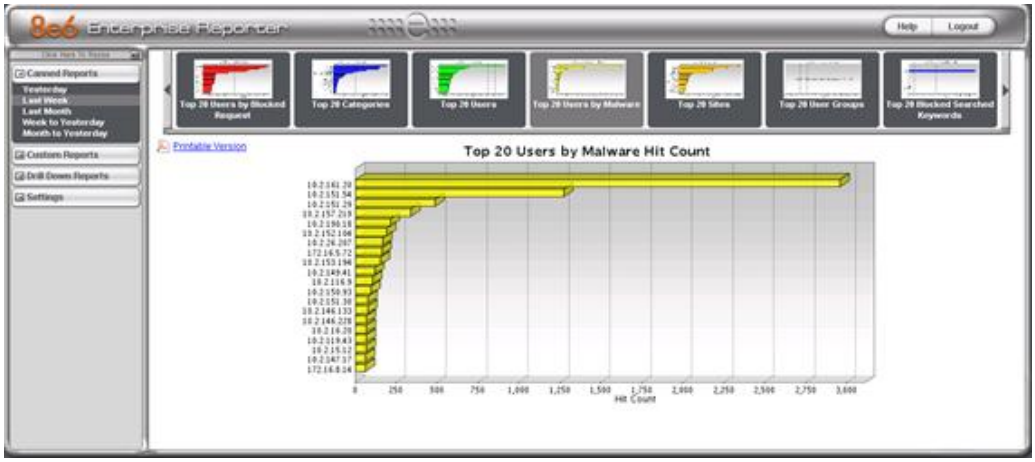


Imagen 12.3 Top 20 de los Usuarios con Descargas de Virus

Top 20 de los sitios más consultados en la Web teniendo en primer lugar a **"Google"**

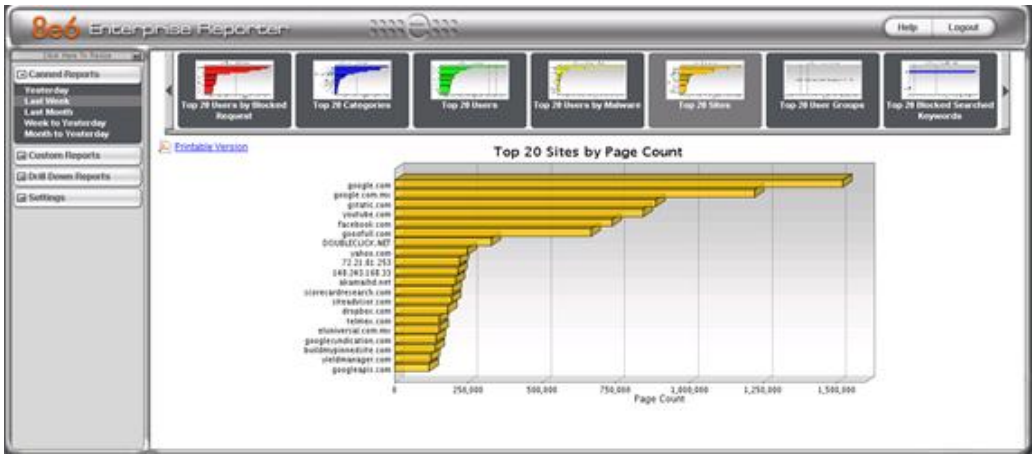


Imagen 12.4 Top 20 de los Sitios más consultados en la Web

3.4.3 Reporteador de Análisis de Riesgos (TAR)

Desde esta consola se pueden supervisar varios parámetros que pueden afectar la seguridad o el rendimiento de la red.

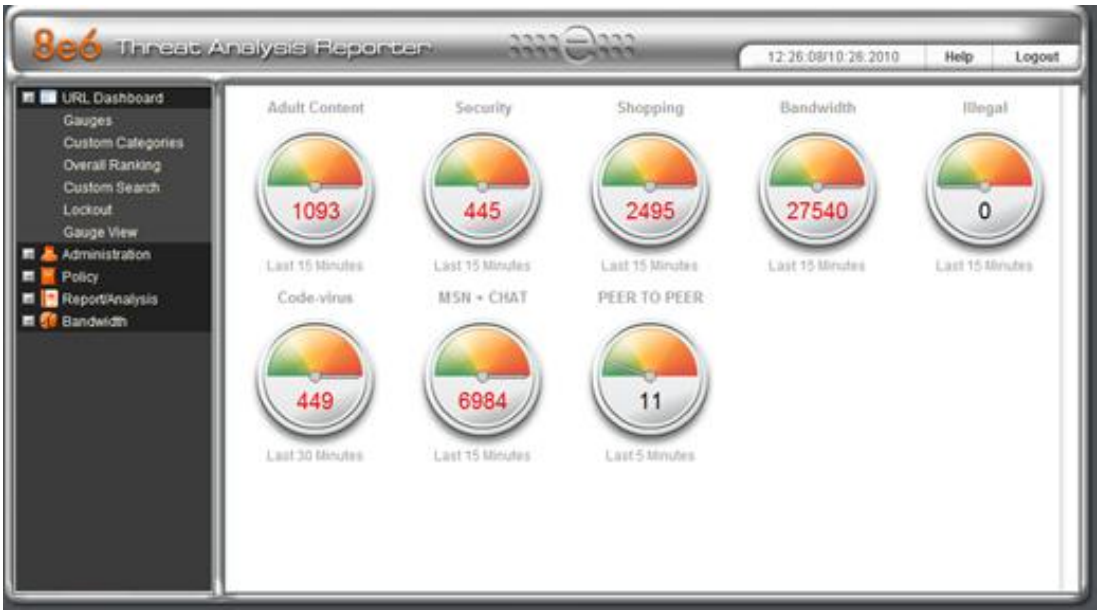


Imagen 12.0 Consola de supervisión de Rendimiento de la Red

Teniendo un monitoreo en tiempo real por dirección Ip y por página consultada.

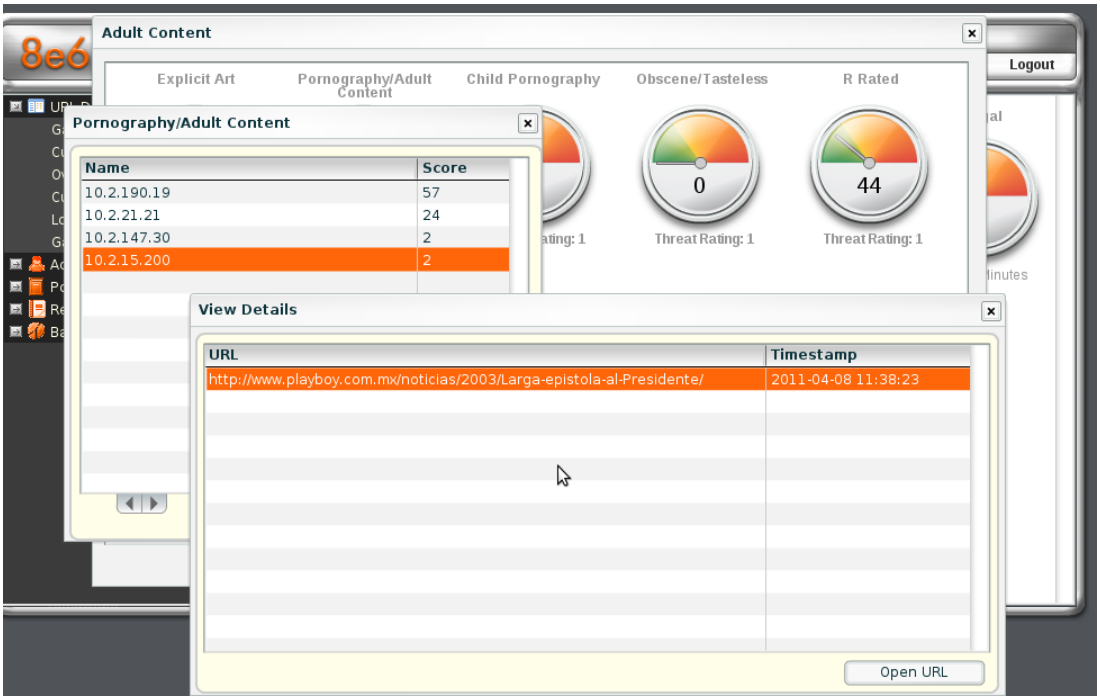
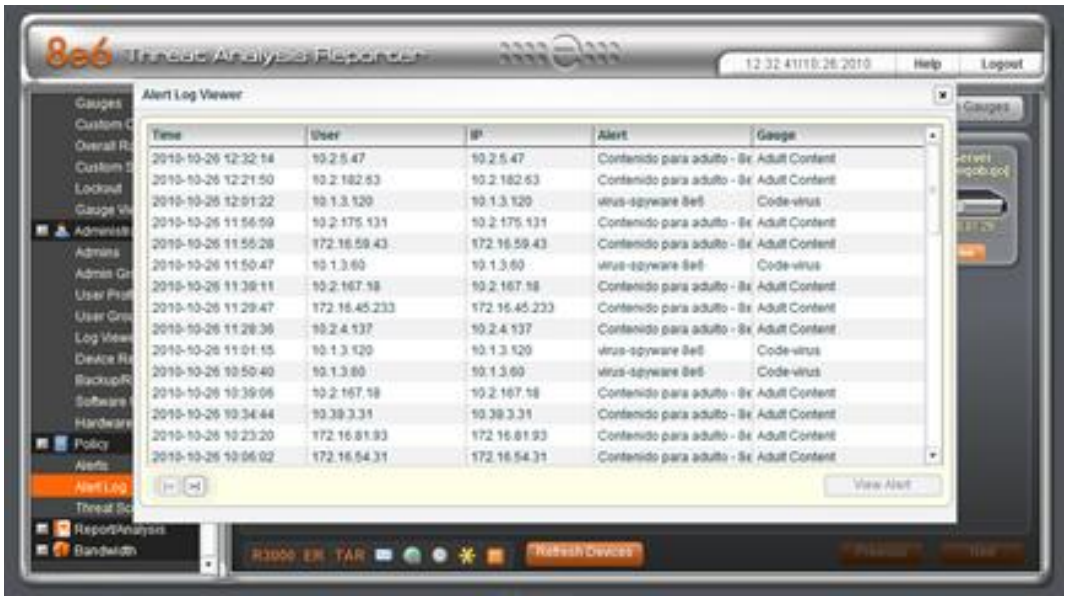


Imagen 13.1 Monitoreo de Consultas de dirección Ip en tiempo Real

Las alertas son enviadas vía correo electrónico, al rebasar los parámetros de seguridad establecidos para contenido para adultos y/o virus



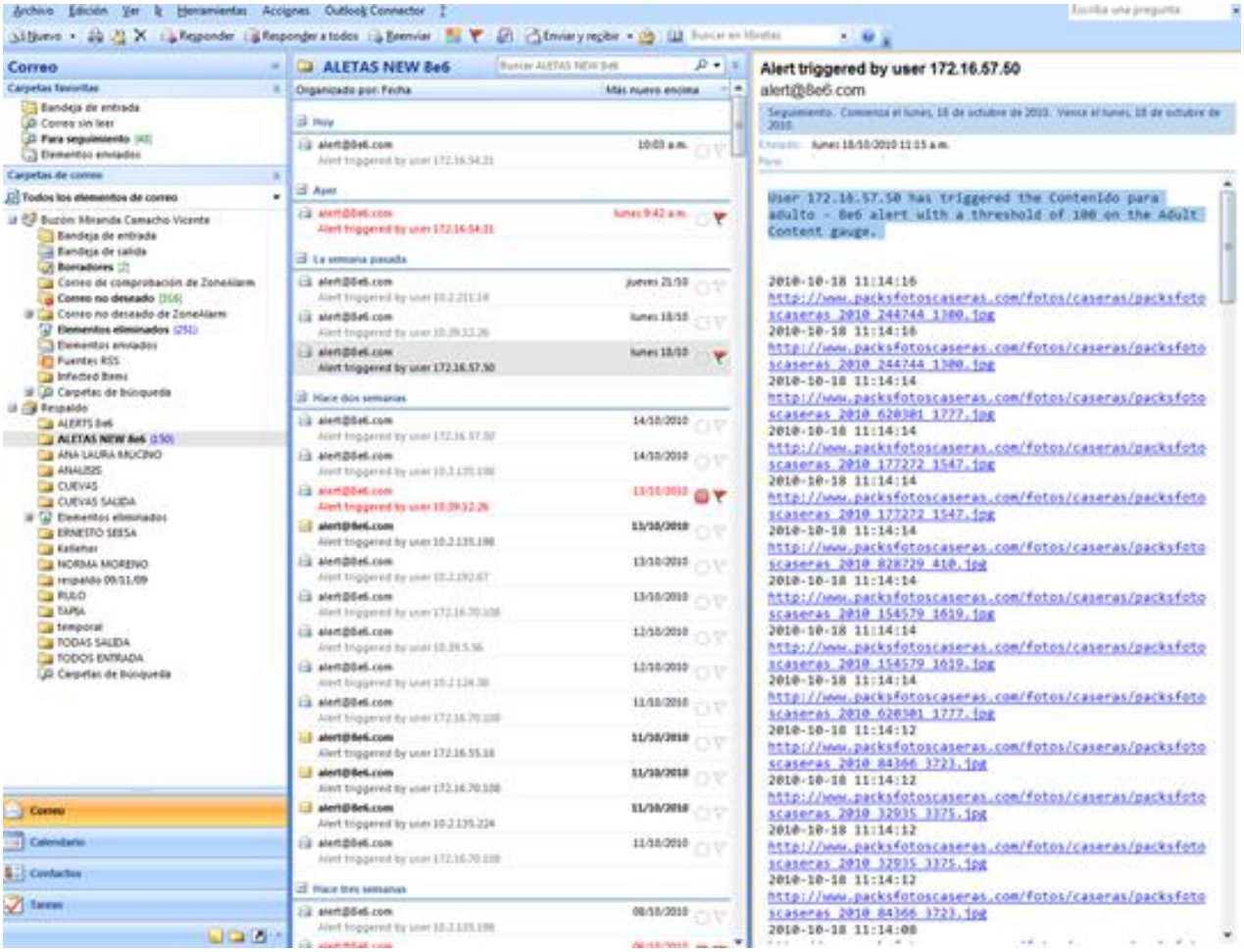


Imagen 13.2 Envió de Incidentes a Correo Electrónico

CAPÍTULO 4. CONCLUSIONES

Como elemento final se mencionan las conclusiones obtenidas durante el desarrollo del caso práctico.

Al final de la implementación del Filtrador de Contenido (WebFilter), se logró cubrir el objetivo principal de manera satisfactoria; con la modernización de los Servicios de Internet se consiguió asegurar la disponibilidad del servicio y proteger el uso y manejo de la información que se genera al interior de la Institución

Los objetivos específicos fueron cubiertos posteriores a la implementación completa de la solución provista por los equipos 8e6 que incluye Filtrador de Contenido Web (WebFilter), Reporterador Empresarial (Reporter), y Reporteador de Análisis de Riesgos (TAR) obteniendo las siguientes mejoras:

- Se modernizo la infraestructura al implementar un Filtrador de Contenido Web y eliminar el uso de los Proxys.
- Estabilidad en el servicio de Internet al tener un equipo de filtrado NO intrusivo.
- Posibilidad de dividir en grupos de control de navegación a las diversas Unidades Administrativas de la Secretaría de Gobernación, reduciendo los tiempos de ocio de los usuarios.
- Establecimiento de un nuevo Reglamento de Navegación el cual se encuentra adaptado al vertiginoso crecimiento de la Web y a la aparición de nuevos servicios; evitando incidentes relacionados a la fuga de información o reputación de la Institución.
- Protección de la integridad en la navegación de los usuarios eliminando accesos a sitios con contenido potencialmente dañino.
- Se brindaron niveles de navegación optima; eliminando por completo las fallas en el servicio de internet; puesto que esta segmentado de acuerdo a las necesidades de cada Unidad Administrativa sin el desperdicio del recurso.
- Capacidad de administrar los servicios de Internet para las nuevas Unidades Administrativas adjudicadas a SEGOB.

- Disminución de tiempo de respuesta en atención a solicitudes referentes al servicio de Internet.
- Proveer a la SEGOB del recurso para la supervisión del uso adecuado de Internet, mediante la obtención de reportes.

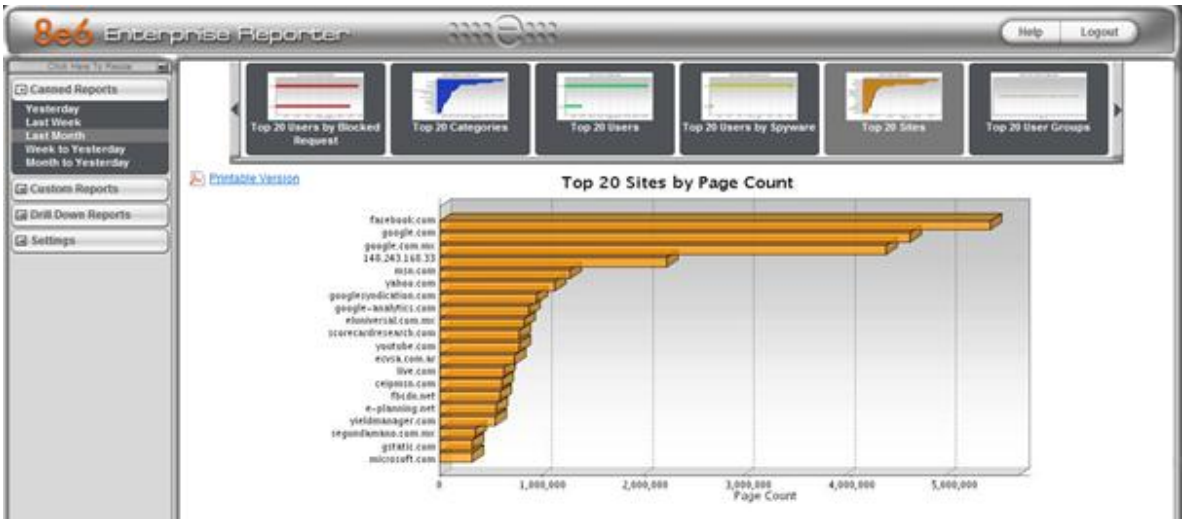
Cabe destacar que el uso del filtrador de contenido nos permitió realizar cambios en el servicio de Internet de manera transparente para el usuario, con la seguridad de tener soporte de mantenimiento.

Como observación se concluye que la implementación de la Solución 8e6 alcanzó las expectativas de la DGTI (Dirección General de Tecnologías de la Información) al eliminar los constantes reportes por fallas en el servicio de Internet; reflejando que las herramientas seleccionadas fueron las correctas, demostrando que el análisis de las opciones de solución fue elaborado de manera optima al igual que el plan de trabajo ya que durante la implementación no se tuvieron contratiempos.

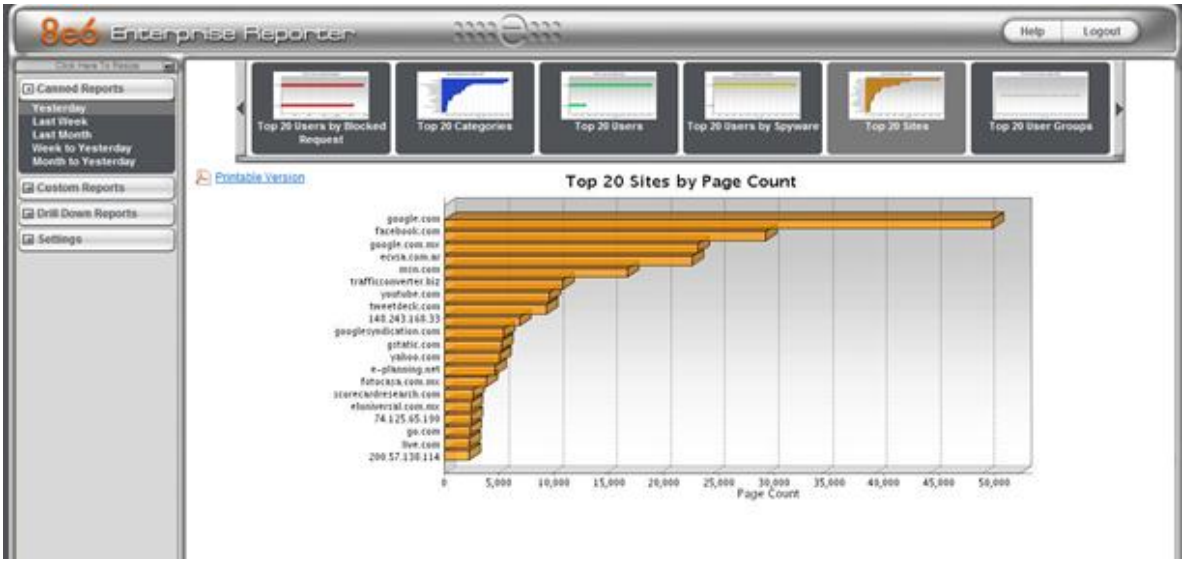
CASO ESPECIAL: FACEBOOK EN SEGOB

Durante el primer año de funcionamiento en producción el Filtrador de Contenido Web estaba enfocado a evitar mensajería instantánea ante la evolución de las Redes Sociales las cuales cambiaron de protocolo http a https y el crecimiento en su uso provocó que el filtrado fuera mas complejo agregando nuevas características al equipo.

Durante el mes de Noviembre del 2010 los accesos totales a Facebook en SEGOB sumaron 5.5 millones, 1 millón más de accesos que Google.



Gracias a la flexibilidad de los equipos 8e6 y al soporte técnico con el cual se cuenta se realizó una Actualización a la versión 4.0 del sistema con el objetivo de realizar ajustes y revalidar permisos de navegación, reduciendo los accesos totales de Facebook a 2.15 millones; teniendo menor cantidad de accesos que Google.



Trabajos a Futuro

A futuro con la implementación de la Solución 8e6 para la Secretaría de Gobernación se pretende fomentar una cultura de responsabilidad sobre el uso de Internet; ninguna solución seria suficiente si se intentara apartar a los usuarios de SEGOB de las nuevas tecnologías; la censura institucional no es una respuesta factible, por lo que se orienta al usuario con la premisa que el recurso de Internet debe estar dedicado siempre al servicio de la meta institucional.

ANEXO # 1

Dirección General de Tecnologías de la Información

SEGOB

Implementación de Equipos de Seguridad para Internet

2009

Dirección General de Tecnologías de la Información

SEGOB

SEGURIDAD EN INTERNET

Situación Actual:

En los últimos años se han hecho esfuerzos para controlar el acceso a Internet con el que cuentan los empleados, usuarios, proveedores de la RED de la SEGOB hacia Internet.

Los permisos hacia este recurso están controlados a través de las políticas en los proxys y el reglamento Interno, sin embargo con el crecimiento de la WEB con casi **187 millones** de sitios en total en Internet, tan solo en 2008 se crearon **30 millones** de sitios según el último estudio de **Netcraft**, es decir que en el último año el número de sitios WEB en Internet se incremento en 17 % con respecto al año 2007.

Cabe mencionarse que la creación de estos sitios trae consigo un incremento sustancial en la publicación de materiales ilegales tales como: Pornografía infantil, Terrorismo, Sitios de Fraudes, Sitios de Armas, Publicación de Material con Derechos de Autor, Discriminación y Racismo, Violencia, Hacking y Cracking, etc.

Dirección General
de Tecnologías de la Información

SEGURIDAD EN INTERNET

SEGOB

Resulta tarea difícil el proteger tantos frentes, cuando no se tiene la plena conciencia de que el mismo usuario puede ser victima de algún tipo de fraude o de hostigamiento, y en ocasiones cuando un usuario pide la libertad de navegar, realmente se esta exponiendo a ser flanco de una gran infinidad de amenazas, la menos graves quizás virus y spyware o backdors, las más graves quizás fraudes en sus cuentas de banco o robos de identidad.

Se complica más cuando el usuario en su afán de libertad, incurre en prácticas ilegales desde la RED de la SEGOB, como descargas de material tales como: software, música, obras literarias, películas, imágenes, video, etc., que cuenta con los derechos de Autor. Afortunadamente no se han hecho escándalos por parte de las personas que tienen esos derechos hacia la SEGOB, pero no podemos esperar a que esto se presente.

Por eso es necesario implementar las políticas que regirán la navegación en Internet, desde luego toda la navegación esta permitida en los parámetros de operación y utilización razonables y racionales de la SEGOB, por lo que aquello que es ilegal, representa un riesgo, viola los derechos de otros, o no entra en la atribuciones del trabajo de la Unidad Responsable, no podrá ser accedido.

Dirección General
de Tecnologías de la Información

SEGURIDAD EN INTERNET

SEGOB

¿Por qué es importante la Seguridad en Internet?

La Secretaría de Gobernación es la dependencia del Ejecutivo Federal responsable de atender el desarrollo político del país y de coadyuvar en la conducción de las relaciones del Poder Ejecutivo Federal con los otros poderes de la Unión y de los demás niveles de gobierno para fomentar la convivencia armónica, la paz social, el desarrollo y el bienestar de los mexicanos en un Estado de Derecho.

Los riesgos de hurto de información pueden traer consecuencias de inestabilidad política o social, desinformación y desorden social.

Precisamente las restricciones están fundamentadas dentro de los parámetros normales de navegación, todo aquello que no es legal o viola los derechos o la ley, queda prohibido.

Entendemos que la Seguridad siempre causa molestia o desacuerdo, pero también sabemos que este punto de vista cambia cuando el usuario se convierte en victima de un fraude o robo de identidad.

Dirección General
de Tecnologías de la Información

SEGURIDAD EN INTERNET

SEGOB

En Junio de 2007 se abrió un foro donde se trataron temas respecto a los sitios de Internet con pornografía Infantil, dicho foro llevo el nombre de **"Creando un Consejo Nacional para la seguridad en Línea"**
Participo la La Señora Margarita Zavala de Calderón

LA PRENSA

Llama Margarita Zavala a un frente común contra pornografía en Internet

Genoveva Ortiz

La señora Margarita Zavala de Calderón durante su participación en el foro "Creando un Consenso Nacional para la Seguridad en Línea". (Foto: Javier Narváez).

A pesar de que el Internet hoy en día es un factor determinante en el desarrollo económico y la educación del país, también representa una gran amenaza para los niños y las niñas, quienes a través de una computadora pueden tener acceso a materiales e información nociva para su desarrollo y bienestar.

Así lo alertó la señora Margarita Zavala de Calderón al manifestar que la responsabilidad del Estado y de la sociedad en su conjunto es proteger, vigilar y controlar la seguridad de Internet, porque la batalla contra la pornografía, la prostitución y la explotación sexual infantil no se detiene en el orden judicial y debe darse a través de todos los frentes.

Durante la ceremonia de inauguración del foro "Creando un Consenso Nacional para la Seguridad en Línea", organizado por Fundación Telmex, la presidenta del Consejo Ciudadano del Sistema Nacional DIF recordó que en México alrededor de 16,000 niños y niñas son víctimas de explotación sexual.

"No cerremos los ojos ante una realidad innegable", declaró la esposa del Presidente Felipe Calderón al señalar que el acceso a pornografía, drogas, comercio sexual infantil y [illegible] a través de Internet, "nos obliga a [illegible] común que impida que la delincuencia organizada atrape lo mejor que tienen los países, los niños y las niñas".

Al felicitar a las dependencias e instituciones civiles participantes en este foro, Margarita Zavala señaló que de acuerdo a la Convención de los Derechos de los Niños, la infancia tiene derecho a recibir y difundir información e ideas procedentes de diversas fuentes.

Pero al mismo tiempo, agregó, los niños y las niñas también tienen el derecho a estar protegidos frente a informaciones y materiales que puedan perjudicarlos y que son nocivos para su propio bienestar y desarrollo.

Anteriormente, recordó, los peores tipos de criminalidad estaban limitados a lugares o espacios físicos y restringidos casi más a los adultos, pero hoy, agregó, con Internet, la pornografía, violencia, crímenes y aficiones están al alcance y a la disponibilidad de cualquier niño que tenga acceso a una computadora.

"Hoy el crimen organizado se diversifica y busca, además, diferentes campos de negocios, donde la pornografía, la prostitución y la explotación sexual infantil tienen un alto índice de rentabilidad", alertó.

Ante este panorama, advirtió que la lucha que actualmente enfrenta el gobierno federal y estatales contra el crimen organizado, nos impulsa a no dar marcha atrás en esta pelea, porque la batalla que se da contra la delincuencia no se detiene en el orden judicial y debe darse a través de todos los frentes.

"Se trata de que cada mamá, cada papá que ve a su hijo o a su hija frente a la computadora, esté tranquilo y se sienta seguro", consumó Margarita Zavala al agradecer el esfuerzo que significa este foro, para que la tecnología esté siempre al servicio de la persona humana, de su desarrollo y de su felicidad.

Dirección General
de Tecnologías de la Información

SEGURIDAD EN INTERNET

SEGOB

La seguridad Empieza en CASA

FECHA 14 DIC 2007 PAGINA 1PP y 10 PPS

EXCELSIOR

REVISARÁ CONTENIDOS

Segob quiere regular internet

La libre expresión tiene sus límites, afirma el subsecretario de Normatividad de Medios

POR PAUL LARA

La Secretaría de Gobernación tiene planes para regular los contenidos de Internet a corto plazo.

Su postura la justifica en que existen páginas peligrosas en la red que ponen en riesgo a sectores considerados vulnerables (niños y adolescentes).

"La pornografía, la violencia y temas relacionados como Gobiernos hostiles y armas por parte de grupos terroristas como Al-Qaeda y Al Fatah, son riesgosos para los menores de edad, por lo que se debe regular lo que se lleva a internet", dijo Juan María Navaja, subsecretario de Normatividad de Medios de la Secretaría de Gobernación.

Durante su participación en el foro "Creando un consenso tecnológico para la seguridad en línea", organizado por la Fundación Telmex, Navaja comentó que no existen reglas en el mundo para controlar internet, y que la Segob ya analiza la posibilidad de que exista una autoridad que lo controle.

"Las redes deben ceñirse a un marco regulatorio. En los temas comerciales se deben cuidar os derechos de autor, las marcas, la piratería y los fraudes. En el bienestar, se deben identificar delitos específicos contra quien viole las disposiciones y atacar con virus las redes o computadoras personales", dijo.

FÉRREO CONTROL

- Estados Unidos supervisa mecanismos privados de vigilancia de contenidos contra Google y Yahoo.
- China es el país en el que existen más desarrolladas las tecnologías de intervención de comunicaciones de Internet, según Reporteros sin Fronteras.

Respecto a los temas de comercio, señaló que debe haber regulación económica, sin violar la libertad de expresión.

"No habrá censura o autocensura, pero sí deben supervisar los contenidos y la responsabilidad de los medios de comunicación. Debe haber un marco regulatorio, pero la ética no restringe el derecho. Como lo señaló en la Suprema Corte de Justicia de la Nación hace unos días, la libertad de expresión tiene sus límites", afirmó Navaja.

El subsecretario agregó que es una política del presidente Felipe Calderón no utilizar la censura en estos casos, pero alentó la creación de un marco regulatorio para Internet, con el fin de que no haya intervención del gobierno en el tema.

LLAMAN A ATACAR POR TODOS LOS FRENTES LA PORNOGRAFÍA INFANTIL

Dirección General
de Tecnologías de la Información

SEGURIDAD EN INTERNET

SEGOB

La seguridad Empieza en CASA

No esperemos a salir en el periódico con una mala nota.

La Jornada

Hay acceso libre a pornografía infantil, turismo sexual y páginas con contenidos violentos

Instan a crear frente para combatir delitos en Internet contra menores

Dirección General
de Tecnologías de la Información

SEGURIDAD EN INTERNET

SEGOB

Pasos a seguir para la implementación de los equipos:

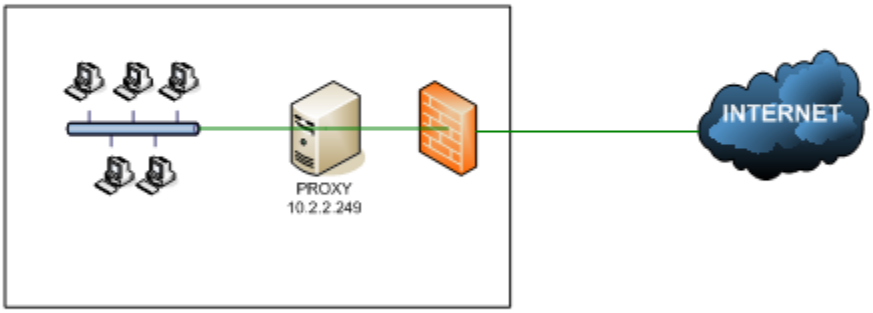
1. Configurar los equipos que tendrán las políticas de acceso a Internet
2. Tener las Políticas de acceso actualizadas y vigentes y en concordancia con la Dirección de Servicios
3. Montar Página Web con la notificación de bloqueo de sitios prohibidos de contenido prohibido
4. Citar a los enlaces informáticos para informales la fecha en la cual la navegación será sin Proxy
5. Hablar con la gente de la Dirección de Servicios para ponerle Fecha y explicarles el proceso de migración de Proxys al Web Filter.

Dirección General
de Tecnologías de la Información

SEGURIDAD EN INTERNET

SEGOB

Esquema de Internet Actual

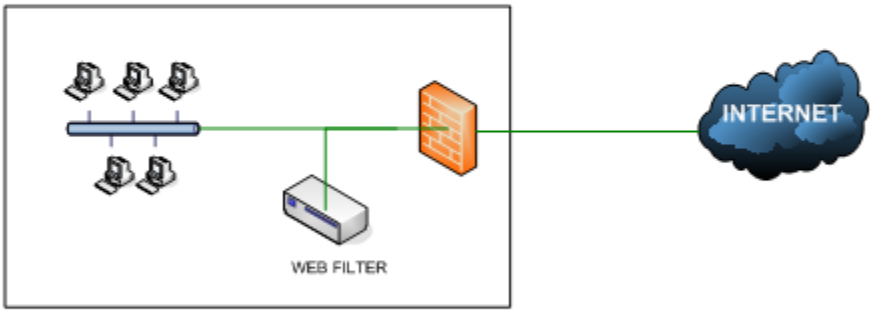


Dirección General
de Tecnologías de la Información

SEGURIDAD EN INTERNET

SEGOB

Esquema de Internet Nuevo



Dirección General
de Tecnologías de la Información

SEGURIDAD EN INTERNET

SEGOB

Pantalla con la indicación de que está entrando a un sitio Web Restringido:

Dirección General
de Tecnologías de la Información

SEGURIDAD EN INTERNET

SEGOB

¿Qué es lo que sigue?:

1. Contar con un inventario de todas las IP's, porque en ocasiones por premura estas IP's no tienen nombre o responsable. (Se les enviara relación de IP's de Sus áreas que no tienen nombre para que nos apoyen a darlas de baja o ponerles nombre).

2. Si se requieren permisos y están fuera de los parámetros de Navegación se les hará firmar una carta responsiva a los usuarios, ya que en caso de violación como lo marcan las políticas o en caso de afectación a la Red SEGOB serán las primeras IP's a auditar y será informado el OIC.

3. Comenzar a quitar el Proxy desde Mañana (23 de Abril de 2009) y como fecha limite tenemos hasta el 28 de Abril de 2009, es decir el Web Filter estará funcionando la mañana del 29 de Abril.

Desaparece:

http://www.telecom/segob.pac

proxy2.segob.gob.mx o 10.2.2.249 puerto 8080

¡¡¡¡ GRACIAS !!!!

DUDAS y COMENTARIOS

GLOSARIO DE TÉRMINOS

Adware:

Los programas de tipo adware muestran publicidad asociada a productos y/o servicios ofrecidos por los propios creadores o por terceros.

Ancho de banda:

Es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período dado. El ancho de banda se indica generalmente en bits por segundo (bps), kilobits por segundo (Kbps), o megabits por segundo (Mbps).

Anonimizadores:

Es un navegador (Página) que deja a los usuarios navegar escondiendo su IP.

Appliance:

Son dispositivos de hardware dedicados (se encargan de realizar un número determinado de funciones), debemos tener en cuenta un aspecto importante. En ningún caso estos appliances sustituyen al antivirus, sino que son un complemento de éste, descargándolo de trabajo y realizando funciones diferentes que el último no puede ejecutar (o lo hace peor). Incorporan a la seguridad de nuestra red lo que se ha denominado protección perimetral. Algunas de las funciones que pueden realizar son:

- Detección y bloqueo de SPAM
- Detección y eliminación de virus y malware
- Identificación de sitios web maliciosos (phishing, spyware,...)
- Filtrado de navegación web
- Protección contra intrusiones
- Firewall
- Gestión de VPN

Backdoors:

En la informática, una puerta trasera (o en inglés backdoor), en un sistema informático es una secuencia especial dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo (autentificación) para acceder al sistema.

Bots / botnets:

Es un término que hace referencia a un conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet (llamado pastor) puede controlar todos los ordenadores/servidores infectados de forma remota.

Caché:

Es una memoria más diminuta y rápida, la cual almacena copias de datos ubicados en la memoria principal que se utilizan con más frecuencia. Usada por la unidad central de procesamiento de una computadora para reducir el tiempo de acceso a la memoria.

Caché de web:

Cuando se accede por primera vez a un dato o una página web, se hace una copia en el caché; los accesos siguientes se realizan a dicha copia, haciendo que el tiempo de acceso medio al dato sea menor.

Cracking:

Es la modificación del software con la intención de eliminar los métodos de protección de los cuales este disponga: protección de copias, versiones de prueba, números de serie, claves de hardware, verificación de fechas, verificación de CD o publicidad y adware.

DNS:

Domain Name System o DNS (en español: sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Con el propósito de poder localizar y direccionar estos equipos mundialmente.

Filtrado Web:

El filtro para web escanea las páginas de un sitio para comprobar el contenido censurable, adulto o malicioso. En un servidor que utiliza un filtrado para la web, cada sitio web solicitado es escaneado antes de que el acceso al destino requerido sea permitido. Y sin embargo, si el sitio al que está tratando de adquirir acceso contiene contenido obsceno, para adultos o malicioso el acceso al mismo será bloqueado. Con un filtrado de contenido Web también se cuenta con un sistema de administración desde el cual podemos controlar a qué tipo de contenido podrán tener acceso a Internet. Un buen sistema de administración también nos presentará una bitácora en reportes con el registro de los sitios web al que los usuarios han tratado de tener acceso y si trataron de hacer una descarga y contenido del mismo, lo cual es también otro aspecto que puede prevenir al utilizar una solución para el filtrado de la web.

La descarga de música, aplicaciones y videos también pueden ser bloqueados a través de una solución para el filtrado de la web. Al bloquear las descargas así como ciertos sitios web se está asegurando que el ancho de banda no se desperdicia en vano, puesto que va a liberar recursos de TI y proteger a usuarios del acceso a material potencialmente ofensivo y por supuesto esto significa que todas las horas que los usuarios utilizan para navegar en Internet para su uso personal sean utilizadas de una manera más productiva.

Firewall:

Es usado para ayudar a mantener segura una red. Su principal objetivo es controlar la entrada y salida del trafico de red mediante el análisis de paquetes de datos y determinando cual deber ser permitido y cual no, basado en un predeterminado set de reglas. El firewall de una red construye un puente entre una red interna que se supone es segura y confiable, y otra red, usualmente una red externa, como lo es internet que es asumida como no segura y no confiable. Un firewall puede estar basado en software o hardware.

FTP:

File Transfer Protocol usado en internet. Permite transferir archivos locales hacia un servidor web.

Hacking:

Es la búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo.

HTTP:

Hypertext Transfer Protocol o HTTP (en español protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la World Wide Web. Es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores.

HTTPS:

Hyper Text Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), es un protocolo de aplicación, destinado a la transferencia segura de datos de Hiper Texto, es decir, es la versión segura de HTTP. Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas

Internet:

Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.

Uno de los servicios que más éxito ha tenido en Internet ha sido la World Wide Web (www).

IP:

Protocolo de Internet; la dirección IP es el número que identifica a cada dispositivo dentro de una red con protocolo IP.

Iptables:

Es el nombre de la herramienta de espacio de usuario mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red. Iptables es un software disponible en prácticamente todas las distribuciones de Linux actuales.

IP Virtuales:

Una IP virtual es un mecanismo por medio del cual el resto de usuarios no tiene acceso a nuestra IP real, sino que ve una IP que no se corresponde con la realidad.

Licencia GPL:

La Licencia Pública General de GNU, está orientada principalmente a proteger la libre distribución, modificación y uso de software. Su propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios.

Logs:

Son usados para registrar datos o información sobre quien, qué, cuándo, dónde, y por qué, un evento ocurre para un dispositivo en particular o aplicación

Malware:

Malware o software de actividades ilegales es una categoría de código malicioso que incluye virus, gusanos y caballos de Troya. El malware destructivo utiliza herramientas de comunicación conocidas para distribuir gusanos que se envían por correo electrónico y mensajes instantáneos, caballos de Troya que provienen de ciertos sitios Web y archivos infectados de virus que se descargan de conexiones P2P. El malware también buscará explotar en silencio las vulnerabilidades existentes en sistemas.

Medios de comunicación electrónica:

Agrupan los elementos y las técnicas usados en el tratamiento y la transmisión de la información, principalmente la informática, Internet y las telecomunicaciones.

NNTP:

Network News Transport Protocol (NNTP) es un protocolo inicialmente creado para la lectura y publicación de artículos de noticias en Usenet. Su traducción literal al español es "protocolo para la transferencia de noticias en red".

Open Source:

Código abierto es el término con el que se conoce al software distribuido y desarrollado libremente. El código abierto tiene un punto de vista más orientado a los beneficios prácticos de compartir el código que a las cuestiones éticas y morales las cuales destacan en el llamado software libre.

Packeteer:

Es un administrador de ancho de banda para enlaces de comunicación privados o enlaces hacia Internet que permite conocer qué aplicaciones circulan realmente por sus enlaces y así posteriormente dictar políticas de control y prioridad que le aseguren un desempeño adecuado a las aplicaciones importantes.

Peer to Peer:

Red de pares, red entre iguales, red entre pares o red punto a punto (P2P, por sus siglas en inglés) es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

Phishing:

Consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario. Consiste también en el robo de información personal y/o financiera del usuario, a través de la falsificación de un ente de confianza. De esta forma, el usuario cree ingresar los datos en un sitio de confianza cuando, en realidad, estos son enviados directamente al atacante. El phishing es una de las técnicas y tipos de Password Harvesting, forma en que se denominan los ataques que recolectan contraseñas de los usuarios. En su forma clásica, el ataque comienza con el envío de un correo electrónico simulando la identidad de una organización de confianza, como por ejemplo un banco o una reconocida empresa.

Protocolo:

Un protocolo es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red por medio de intercambio de mensajes.

Proxy:

Es un programa o dispositivo que realiza una acción en representación de otro, esto es, si una hipotética máquina A solicita un recurso a una C, lo hará mediante una petición a B; C entonces no sabrá que la petición procedió originalmente de A.

Red:

Una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Router:

Es un dispositivo que renvía paquetes de datos entre redes de computadoras creando una interconexión entre diferentes redes. Un router esta conectado a dos o más líneas de datos de diferentes redes. Cuando un paquete de datos viene de una de una de las líneas, el router lee la información de dirección en el paquete, para determinar su destino final. Entonces, usando información en esta tabla o políticas de ruteo, este dirige el paquete a la próxima red.

Scripts:

Un guion, archivo de órdenes o archivo de procesamiento por lotes, vulgarmente referidos con el barbarismo script, es un programa usualmente simple, que por lo regular se almacena en un archivo de texto plano.

Seguridad lógica:

Se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

Servicios informáticos:

Término general utilizado para describir toda la gama de servicios y empresas que participan en el desarrollo de software, diseño de hardware, sistemas informáticos en red, la y la prestación de servicios de tecnología de la información.

Servidores de cómputo:

Un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

Sitios de IRC:

Internet Relay Chat es un protocolo de comunicación en tiempo real basado en texto, que permite debates entre dos o más personas. Se diferencia de la mensajería instantánea en que los usuarios no deben acceder a establecer la comunicación de antemano, de tal forma que todos los usuarios que se encuentran en un canal pueden comunicarse entre sí, aunque no hayan tenido ningún contacto anterior.

Spam:

Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

Spoofing:

En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Spyware:

Programa espía es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

Squid:

Squid es un popular programa de software libre que implementa un servidor Proxy y un dominio para caché de páginas web, publicado bajo licencia GPL. Tiene una amplia variedad de utilidades, desde acelerar un servidor web, guardando en caché peticiones repetidas a DNS y otras búsquedas para un grupo de gente que comparte recursos de la red, hasta caché de web, además de añadir seguridad filtrando el tráfico. Está especialmente diseñado para ejecutarse bajo entornos tipo Unix.

TCP/IP:

En referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP).

Telecomunicaciones:

El término telecomunicación cubre todas las formas de comunicación a distancia, incluyendo radio, telegrafía, televisión, telefonía, transmisión de datos e interconexión de computadoras a nivel de enlace.

Troyanos:

El principal objetivo de este tipo de malware es introducir e instalar otras aplicaciones en el equipo infectado, para permitir su control remoto desde otros equipos.

URL:

Un localizador de recursos uniforme, más comúnmente denominado URL (sigla en inglés de uniform resource locator), es una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación, como por ejemplo documentos textuales, imágenes, vídeos, presentaciones digitales, etc.

Virus:

Es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

VPN:

Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada.

WEB:

La World Wide Web (www) o Red informática mundial es un sistema de distribución de información basado en hipertexto o hipermedios enlazados y accesibles a través de Internet.

Webmasters:

Son las personas responsables del mantenimiento o programación de un sitio web.

FUENTES ELECTRÓNICAS

http://segob.gob.mx

- ✓ http://segob.gob.mx/es_mx/SEGOB/Mision
- ✓ http://segob.gob.mx/es_mx/SEGOB/Atribuciones

[Consulta: 20 de mayo de 2012].

"REGLAMENTO INTERIOR DE LA SECRETARÍA DE GOBERNACIÓN".

AUTOR: VICENTE FOX QUESADA

Publicado por el Diario oficial de la federación 30/julio/2002

- ✓ http://segob.gob.mx/es_mx/SEGOB/Marco_juridico

[Consulta: 28 de mayo de 2012].

NETCRAFT "INVESTIGACIÓN DE INTERNET, ANTI-PHISHING Y SERVICIOS DE SEGURIDAD"

AUTOR: NETCRAFT

- ✓ http://news.netcraft.com/

[Consulta: 29 de mayo de 2012].

MANUALES M86 WEBMARSHALL
AUTOR: M86

- ✓ http://www.m86security.com/documents/pdfs/datasheets/web_security/DS_WebMarshal.pdf

[Consulta: 28 de mayo de 2012].

DEFINICIONES DE TÉRMINOS

Microsoft TechNet. «Defining Malware: FAQ» (en inglés).

- ✓ http://technet.microsoft.com/en-us/library/dd632948.aspx

[Consulta: 01 de junio de 2012].

Tipos de malware» (en español).

- ✓ www.infospyware.com.

[Consulta: 01 de junio de 2012].

SYMANTEC CORPORATION. «SYMANTEC INTERNET SECURITY THREAT REPORT: TRENDS FOR JULY-DECEMBER 2007 (EXECUTIVE SUMMARY)» (EN INGLÉS).

- ✓ http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf

  [Consulta: 05 de junio de 2012].

PANDA LABS. «LA CANTIDAD DE MALWARE CREADO AUMENTA EN 26% HASTA LLEGAR A MÁS DE 73,000 DIARIOS».

- ✓ http://prensa.pandasecurity.com/2011/03/la-cantidad-de-malware-creado-aumenta-en-26-hasta-llegar-a-mas-de-73000-diarios-informa-pandalabs/

  [Consulta: 05 de junio de 2012].

ESET. «TIPOS DE MALWARE Y OTRAS AMENAZAS INFORMÁTICAS» (EN ESPAÑOL).

- ✓ http://www.eset.com.mx/centro-amenazas/amenazas/2148-PayLoad

  [Consulta: 07 de junio de 2012].

- ✓ http://es.wikipedia.org/wiki/Servidor.

  [Consulta: 09 de junio de 2012].

- ✓ http://es.wikipedia.org/wiki/Spyware .

  [Consulta: 09 de junio de 2012].

- ✓ http://www.slideshare.net/acurbelo/seguridad-ciberntica

  [Consulta: 10 de junio de 2012].

- ✓ http://es.wikipedia.org/wiki/Backdoor

  [Consulta: 10 de junio de 2012].

- ✓ http://www.duiops.net/hacking/hacking-cracking.htm

  [Consulta: 10 de junio de 2012].

- ✓ http://en.wikipedia.org/wiki/Router_(computing) Consultado el 11/05/2012

  [Consulta: 10 de junio de 2012].

- ✓ http://en.wikipedia.org/wiki/Firewall_(computing) Consultado el 11/05/2012

  [Consulta: 10 de junio de 2012].