Auditoría WatchGuard®

Equipo de Vigilancia de Tráfico

Control de Aplicaciones, Filtrado web, Logs, Informes

WatchGuardXTM
XTM2, 5, 8, 10, 20

EMPRESA QUE HACE LA AUDITORIA »

DESCRIPCION DE LA EMPRESA QUE HACE LA AUDITORIA.

1. WatchGuard Technologies Inc.

WatchGuard desarrolla soluciones de seguridad integradas para proporcionar a las empresas una protección eficaz a un precio asequible. Las soluciones de seguridad en red XTM (Extensible Threat Management, es decir, Gestión de Amenazas Extensible) ofrecen una completa solución firewall, VPN y servicios de seguridad para proteger las redes contra spam, virus, malware e intrusiones. Los nuevos equipos XCS (Extensible Content Security, es decir, Seguridad de Contenidos Extensible) permiten asegurar el contenido del correo electrónico y las páginas web junto con la prevención de la pérdida de datos para la protección integral de los contenidos.

Las soluciones de WatchGuard son escalables para garantizar la seguridad desde las pequeñas empresas hasta los grandes grupos con más de 10.000 empleados. Desde nuestros inicios en 1996, hemos desplegado más de 600.000 dispositivos de seguridad de la firma WatchGuard en todo el mundo. Hoy en día, más de 15.000 socios dedicados a nuestros productos en más de 120 países.

WatchGuard dispone de sede en Seattle, en el estado de Washington, y oficinas en Norteamérica, Sudamérica, Europa y la región Asia-Pacífico.

2. Ejecución de la auditoría

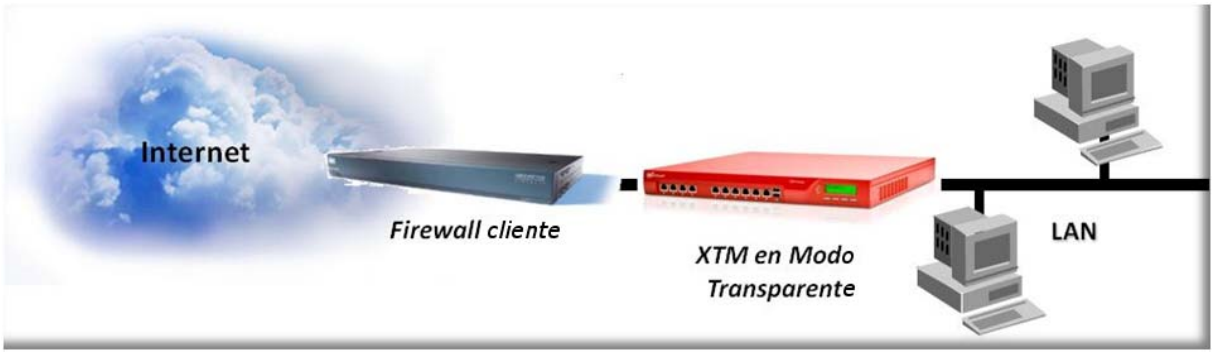
2.1. Objectivo de la auditoría

Este documento tiene como objetivo analizar y presentar los resultados de la auditoría que se llevó a cabo durante 15 días en el "***nombre del cliente***".

Los resultados se basan en la arquitectura, que se llevó a cabo de manera transparente, para permitir la captura y el seguimiento del tráfico de los usuarios de Internet. Este tráfico ha sido registrado y almacenado para permitir la creación de informes. Estos informes se presentan y analizan en este documento.

El propósito de este documento es proporcionar recomendaciones sobre el tráfico de filtrado para optimizar el uso de Internet, tanto desde el punto de vista de la productividad de los usuarios, como el uso del ancho de banda para las necesidades del negocio.

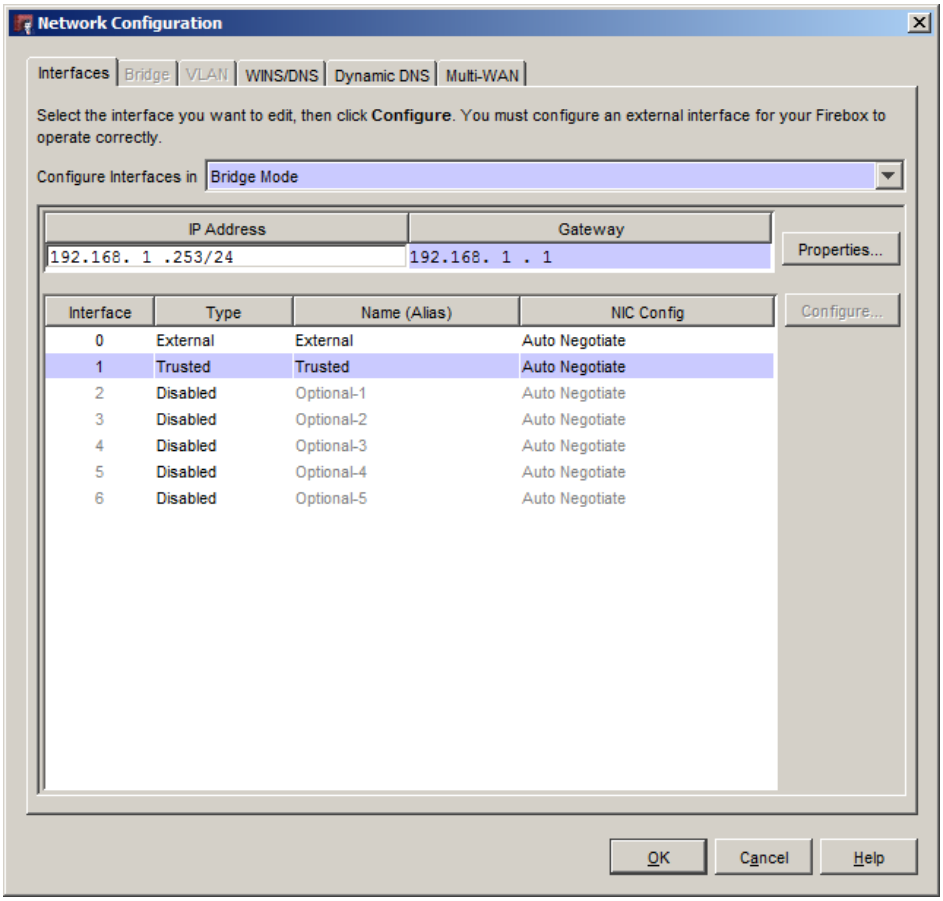
2.2. Arquitectura de la auditoría



Arquitectura Transparente

Para habilitar la ejecución de la auditoría, un equipo de WatchGuard Technologies es configurado en modo transparente entre el firewall actual y la red de usuarios (u otro segmento a auditar).En el modo transparente, el XTM no requiere la configuración exhaustiva de la red IP, sólo tiene que conectar la interfaz LAN entre el firewall y los activos existentes de la red.

Todos los puestos de trabajos mantendrán la misma configuración IP (dirección y puerta de enlace predeterminada).



Mode Bridge para en análisis transparente

En términos de reglas, el XTM de Supervisión está configurado en modo abierto(ver próxima sección) para que todo el tráfico sea permitido por el cortafuegos hasta el cliente. El XTM permite rastrear el flujo y generar una visualización del uso de la red a nivel de aplicación.

El firewall existente debe estar configurado para permitir que el XTM pueda acceder a sus servicios y actualizaciones de bases de datos (WebBlocker, IPS, AV,Application Control). La forma más fácil es crear una regla para permitir la IP del equipo de gestión para salir. Puede, sin embargo, restringir el tráfico al no especificarlos puertos que sean de utilidad.

2.3. Configuración del equipo XTM

Todas las reglas del cortafuegos debe estar configurado para permitir el tráfico en todos los niveles:

- Reglas
- Proxies
- Servicios

El propósito de esta configuración particular no es bloquear todo el tráfico del usuario. El papel del aparato es ser completamente transparente para el tráfico legítimo como ilegítimo.

Reglas de Salida:

En las reglas de salida se configurarán los siguientes servicios:

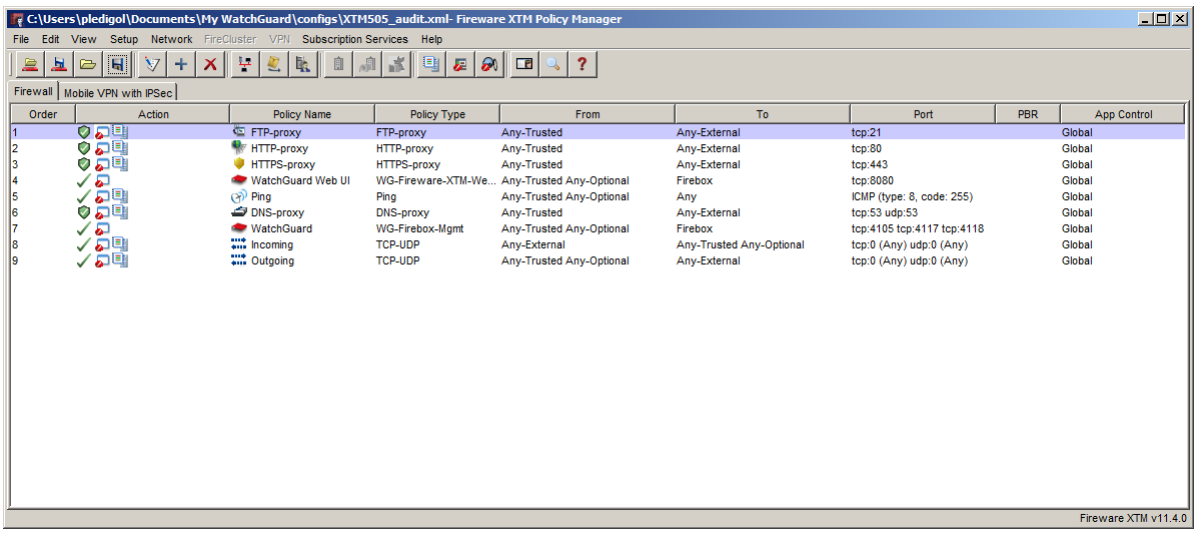
Proxies: ftp, http, https, dns

Packet Filter: ping, outgoing

Reglas de entrada:

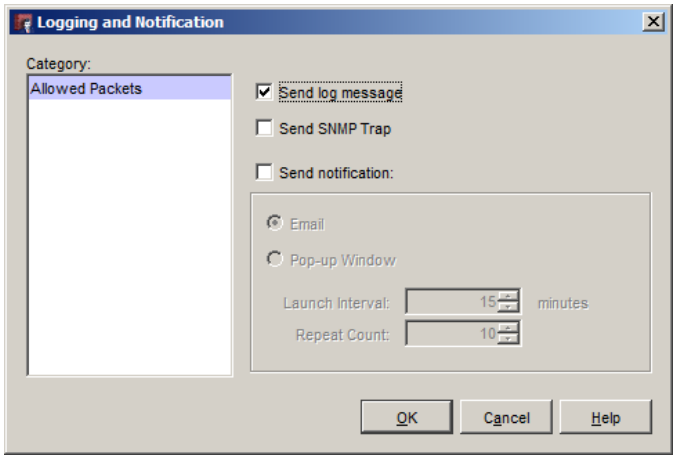
Para el flujo de entrada, una regla de incoming será establecida para todo TCP/UDP.

Nota : En caso de tener correo pasando por el appliance, será necesario añadir reglas de proxy SMTP.



Reglas sobre el equipo XTM en modo transparente

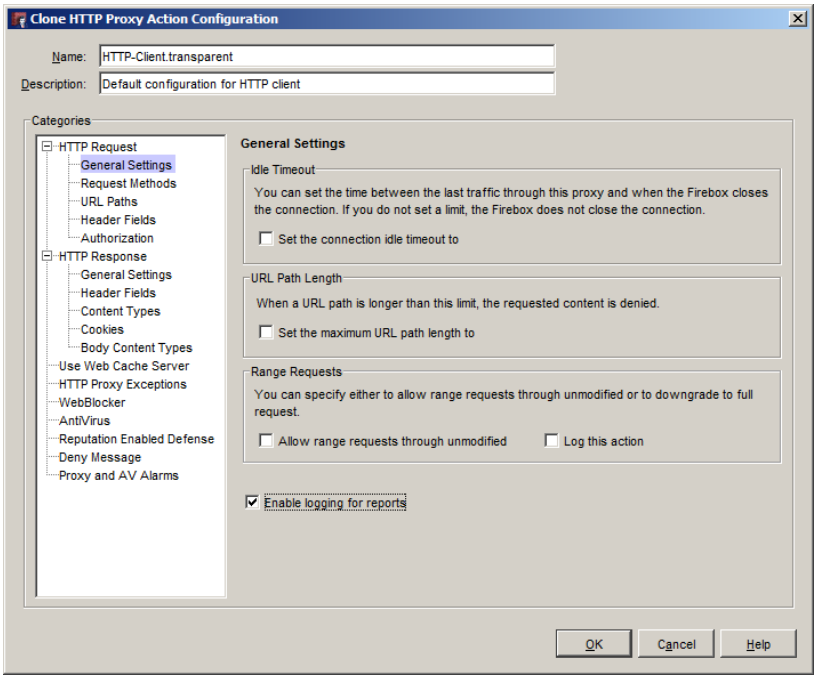
Todas las reglas logarán su actividad para tener total trazabilidad del sistema y poder obtener los informes sobre los usuarios, amenazas, etc…



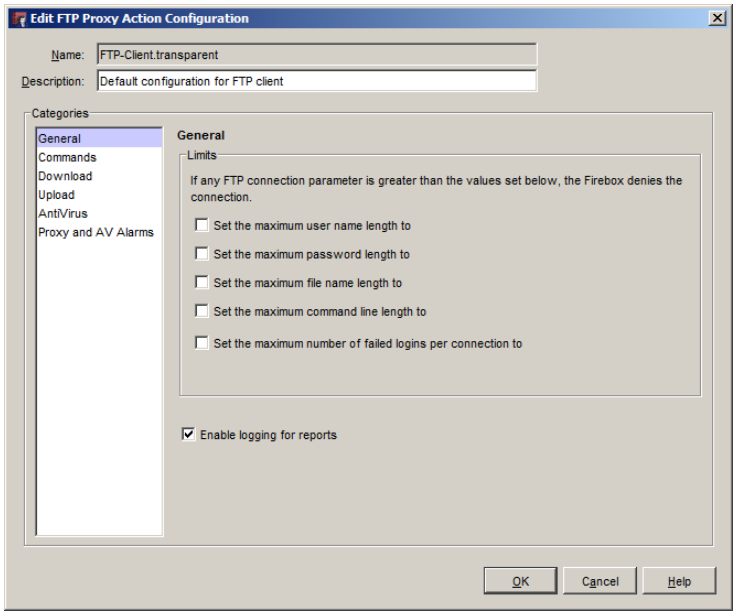
Activación del log en las reglas

Las acciones de proxy ftp, http, https y dns se deben configurar para no bloquear nada, dejándolos “abiertos”, configurando todo en « Allow » y eliminando todos los límites.

Por otro lado, deberemos forzar su logado («enable logging for reports »desde el tab de « general settings »).



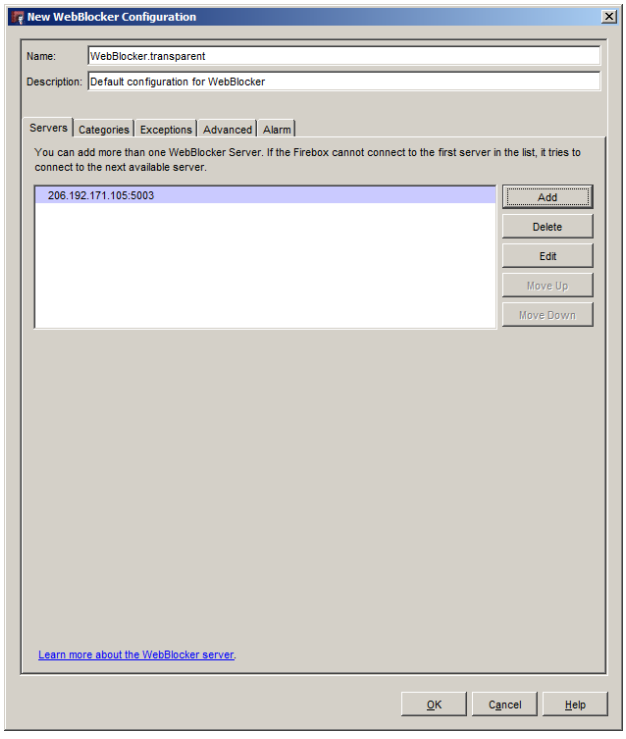
Activación de logs en el proxy HTTP



Eliminación de límites y restricciones en el proxy FTP

El filtrado URL será configurado pero sin realizar ningún bloqueo de categorías, para de este modo, tener registradas cuáles son las mismas que se visitan

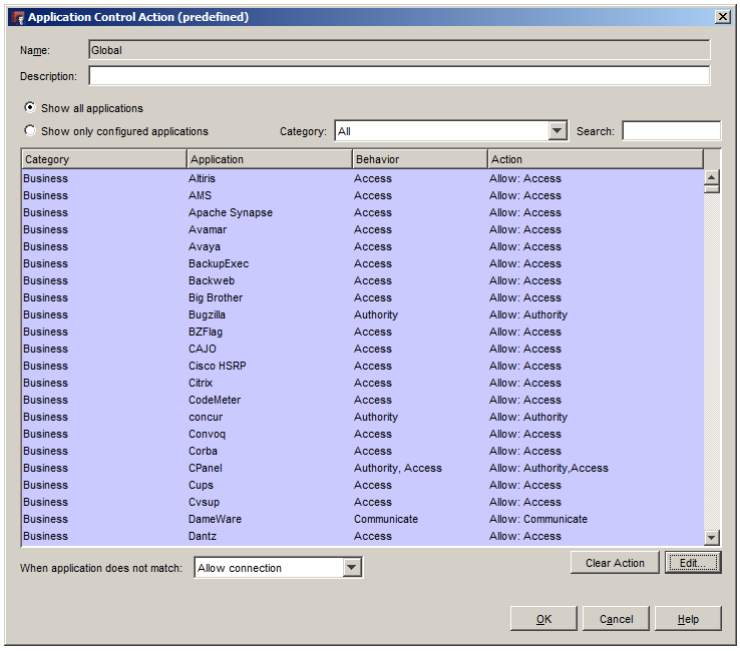
Para evitar configurar un servidor de WebBlocker local, usaremos un sistema en la nube alojado por WatchGuard, para lo que resolveremos swb.watchguard.com e introduciremos su IP.



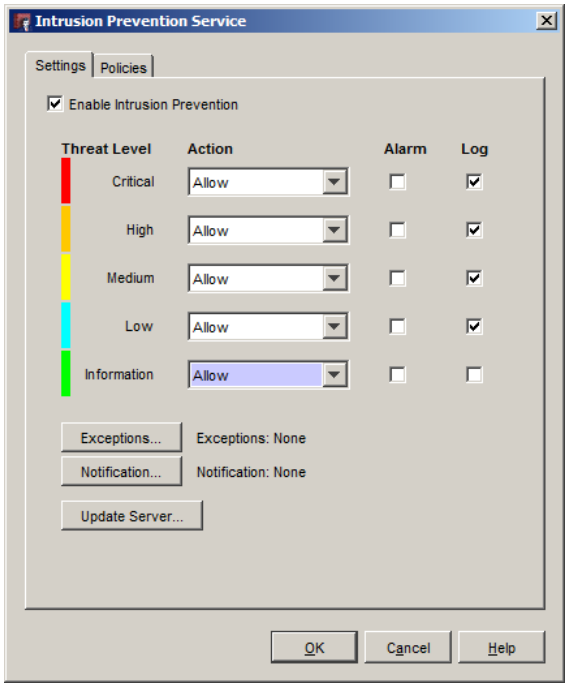
Configuración del servidor en nube de WebBlocker

El servicio de control de aplicaciones será configurado en modo abierto, permitiendo explícitamente todas las aplicaciones de la base de datos. La acción “global” será configurada para que se aplique en todas las reglas.

El servicio de IPS (de prevención de intrusión) será configurado de forma análoga.

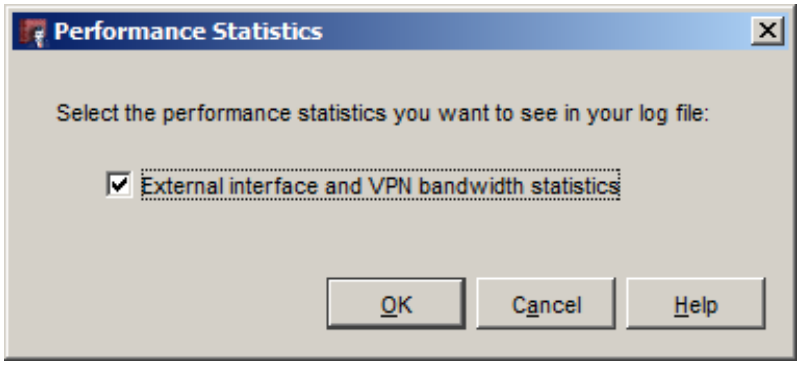


Autorización de las aplicaciones



Autorización de las firmas de IPS/IDS

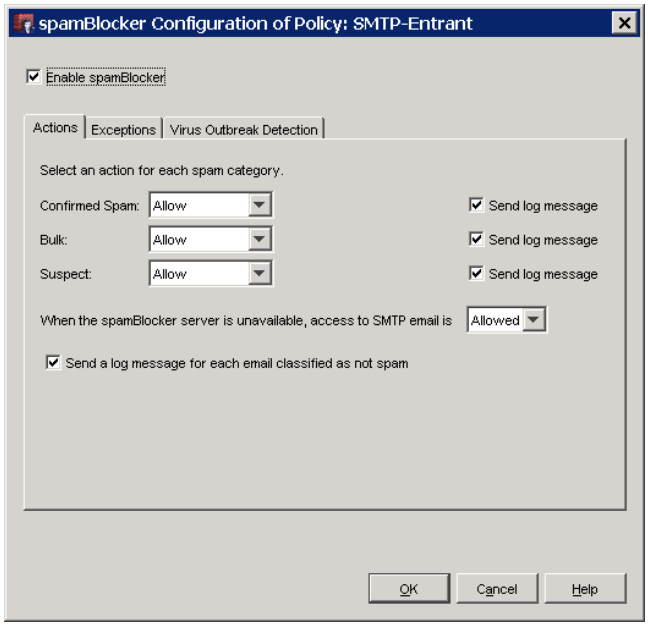
Finalmente, se activará la obtención de estadísticas de ancho de banda consumido por la interfaz externa (« performance statistics »).



Activación de las estadísticas de ancho de banda consumido

Tráfico de Mensajería

Es posible considerar el SMTP también en la auditoría, pero es más complicado en términos de arquitectura, porque el servidor SMTP estará, probablemente, en la interfaz DMZ de un corta-fuegos existente. Puede ser posible hacerlo en un segundo tiempo una vez que la auditoría se ha llevada a cabo en la LAN. En este caso, se agregará el proxy SMTP entrante y saliente en modo transparente y abierto con los registros habilitados.
En este caso, también vamos a agregar el SpamBlocker antispam para demostrar que el servicio podría ser filtrado. Sin embargo, se comprobará la presencia o ausencia de un firewall antispam dedicado entre el servidor de correo existente (o software en el servidor de correo).



Configuración antispam transparente

2.4. WatchGuard Log Server

Implantación del servidor de logs

Todos los registros durante la auditoría serán almacenados en un servidor de logs de WatchGuard.

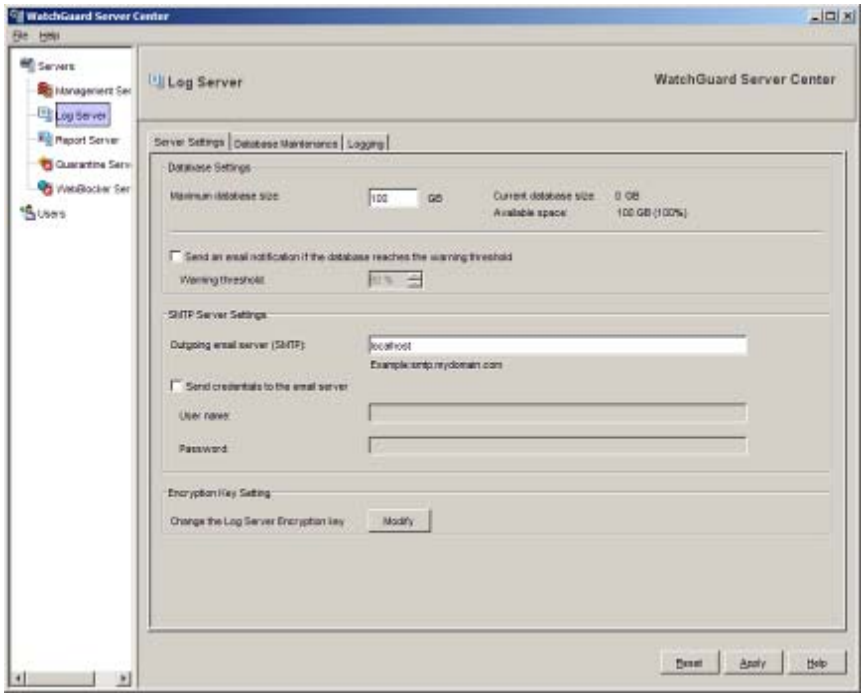
El servidor de logs puede ser instalado localmente en un servidor físico o en una máquina virtual Windows. También es posible enviar los registros directamente en un servidor remoto alojado. En este segundo caso, debemos asegurar que los logs enviados no son bloqueados por el firewall existente. También se asegurará de que hay suficiente espacio en disco para la duración de la auditoría.

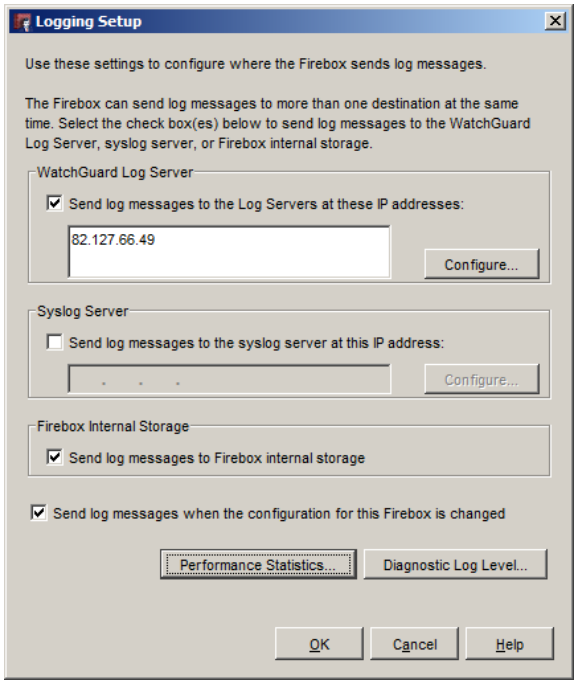
Descripción del servidor de logs

WatchGuard ha incorporado una arquitectura de registros completos para superarlas deficiencias de las herramientas comunes del mercado, tales como syslog. De hecho, Syslog es un protocolo utilizado para registrar la información, pero basado en UDP. UDP es un protocolo sin conexión y no garantiza la retransmisión de las tramas perdidas, WatchGuard ha elegido para desarrollar su propio protocolo de registros. Para hacer esto, WatchGuard ha desarrollado un protocolo basado enTCP registra con un servidor de registro proporciona como estándar. Por otra parte, no proporciona ninguna Syslog estándar de cifrado de datos que hace difícil el uso de un protocolo para construir una arquitectura para la gestión remota segura.

Así, el Firebox envía al servidor de registro de los logs de WatchGuard para garantizar la fiabilidad de la comunicación, la conectividad permanente a los registros del servidor con cualquier copia de seguridad y encriptación de datos transferidos.

El registro del servidor viene con una base de datos integrada de SQL (PostgreSQL) en el que almacena los registros.





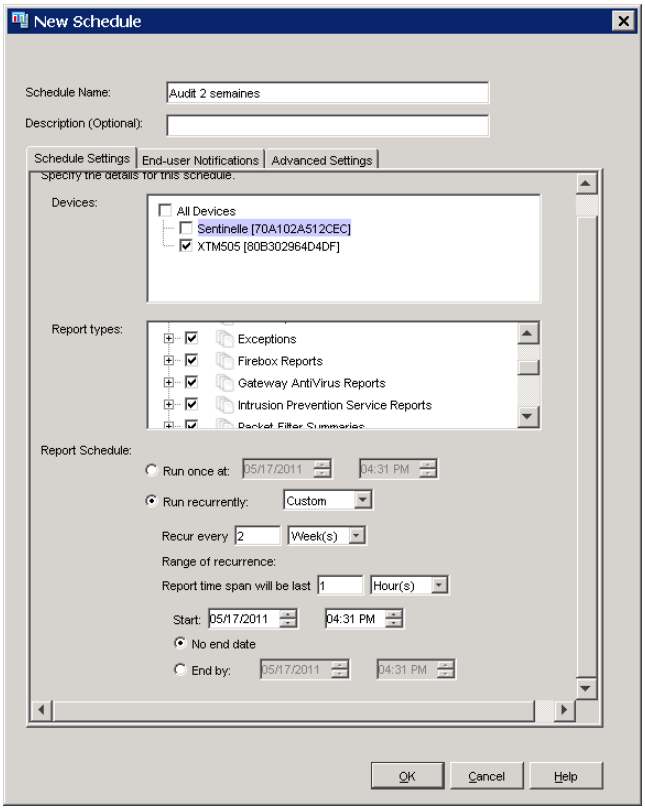
Configuración del servidor de logs, en el propio servidor y su integración con WatchGuard

2.5. Report Server, Report Manager y Report Web UI

Implementación del servidor de informes

De los registros almacenados en el periodo de la auditoría, se generan varios informes utilizando el servidor de informes. Esto asegurará que los informes diarios, informes semanales y la duración completa de la auditoría. Informes más específicos se pueden generar cuando sea necesario para un análisis más detallado de algunos períodos con un comportamiento anormal.

El servidor de informes se instalará en la misma máquina que el servidor de logs en función de la arquitectura seleccionada (máquina física o virtual alojado).



Generación de informes de dos semanas

Descripción del servidor de informes

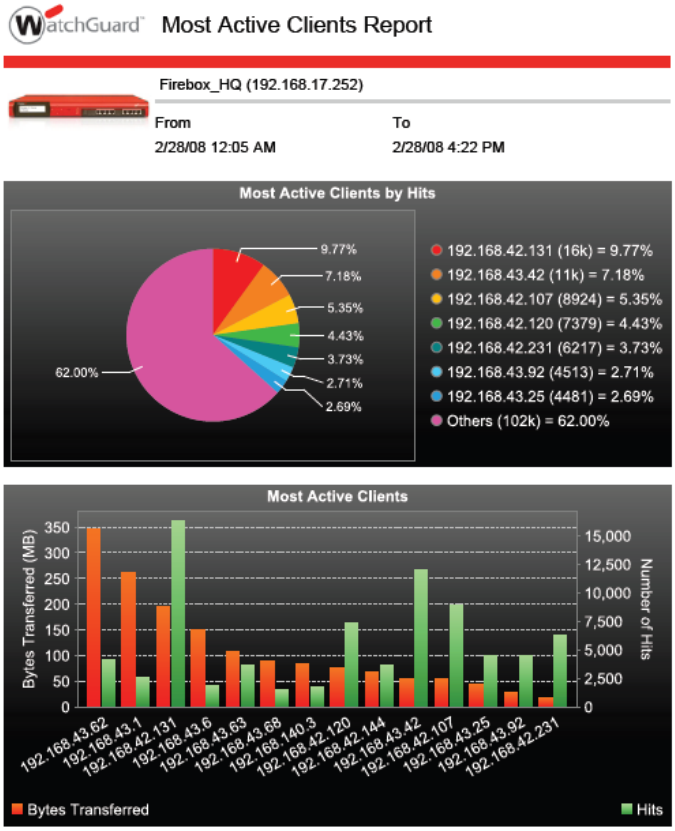
El servidor de informes es el módulo que proporcionará más rápido de los datos estadísticos sobre la actividad de red importante.

El servidor de informes utiliza los datos almacenados en los registros de base de datos para generar informes de forma automática o bajo demanda. Por defecto, el servidor de informes genera un informe diario y un resumen semanal. El administrador puede generar informes sobre la demanda durante un período determinado.

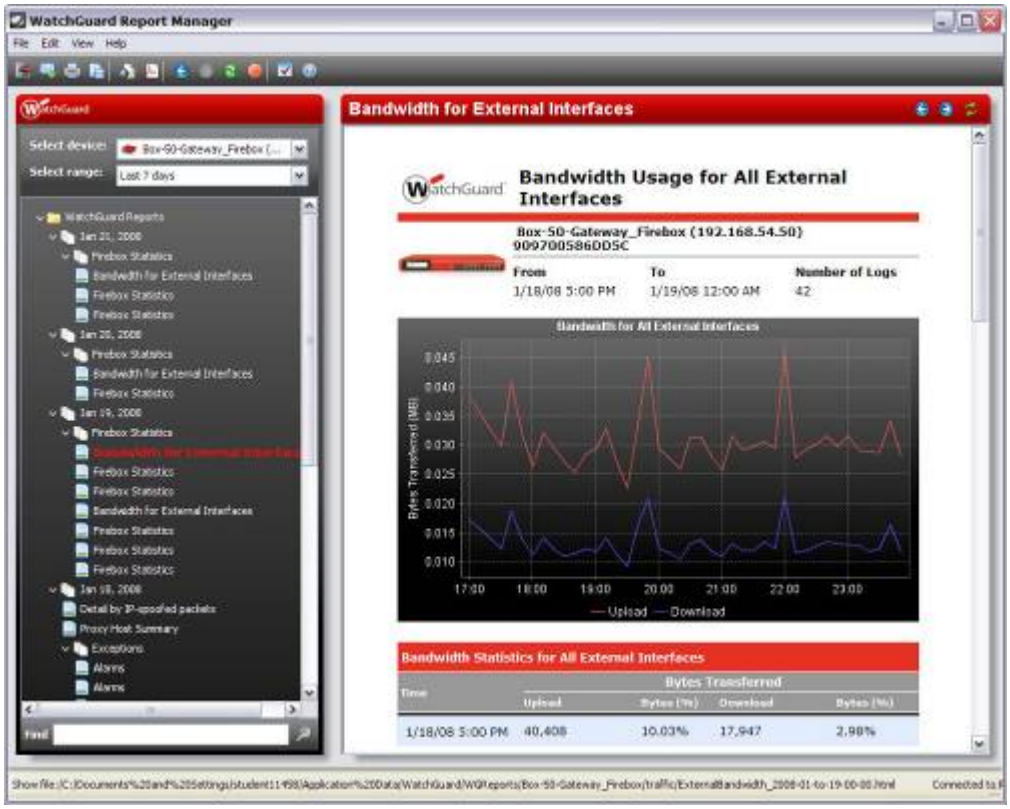
Los informes se pueden ver a través del Administrador de informes (incluido en elWSM) o desde la interfaz web (WebUI informe). El informe de WebUI también se puede utilizar para proporcionar acceso a información remota o integrado en un portal de consulta.

Una función de filtro también se puede ver que máquinas o protocolos que desea.

Los informes se pueden exportar a PDF o HTML.



Visualización de informes con el ReportManager



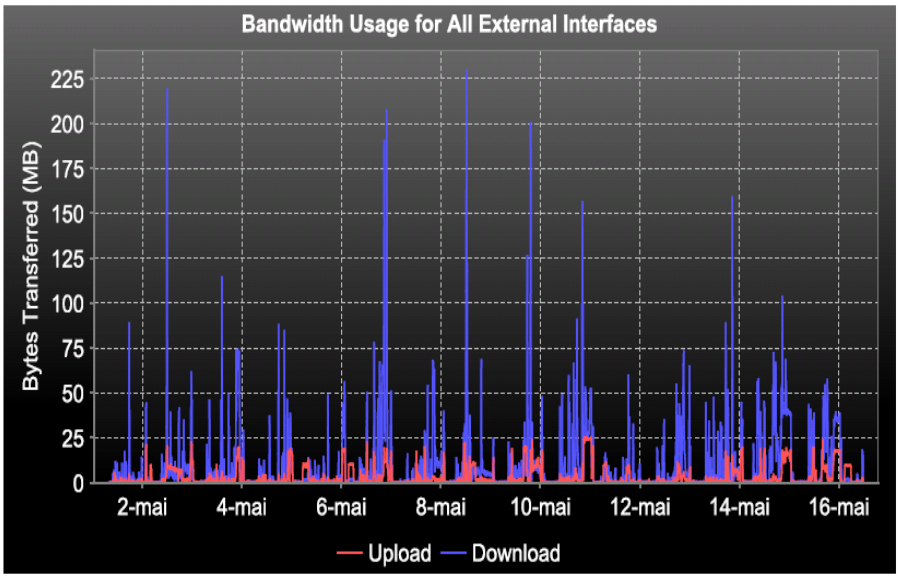
Visualización del ancho de banda consumido

3. Análisis de los datos de la auditoría

3.1. Capacidad de las interfaces externas

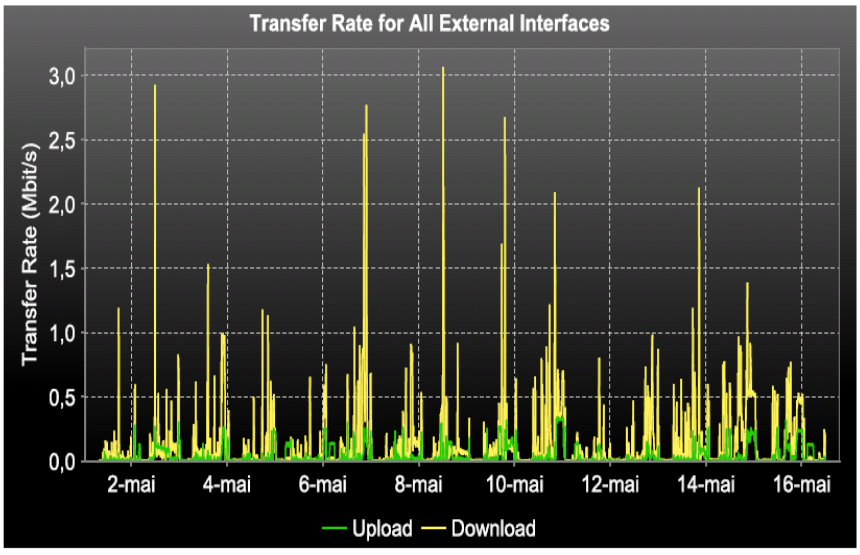
Sentinelle (172.16.10.1) 70A102A512CEC

From	To	Number of Logs
01/05/11 08:00	16/05/11 18:00	2 182



Sentinelle (172.16.10.1) 70A102A512CEC

From	To	Number of Logs
01/05/11 08:00	16/05/11 18:00	2 182



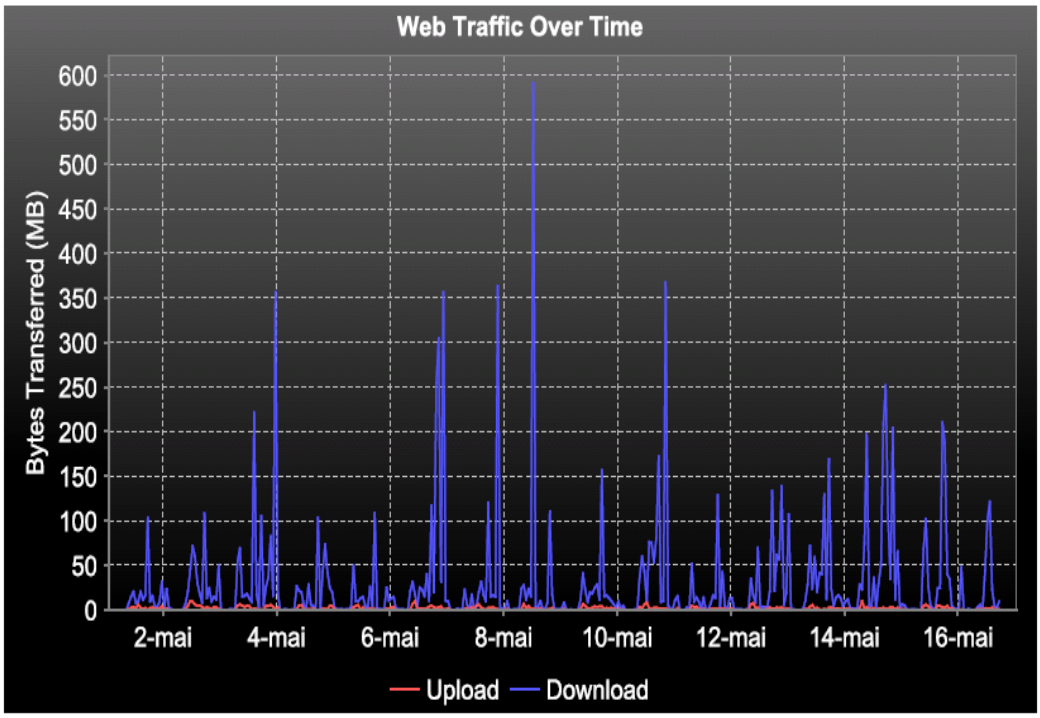
Los puntos a considerar son:

- Línea de la congestión de Internet
- Ancho de banda anormal en comparación con el número de usuarios y el uso de Internet
- Ancho de banda anormal de ciertos días o periodos (descarga ilegal, botnet copias de seguridad automáticas, etc…)
- Sospecha de un comportamiento anormal en el interior o exterior (DDoS) en ciertos momentos
- Fallas supuesta operador

3.2. Tráfico Web

Sentinelle (172.16.10.1) 70A102A512CEC

From	To	Number of Logs
01/05/11 08:00	16/05/11 18:00	1 035 838



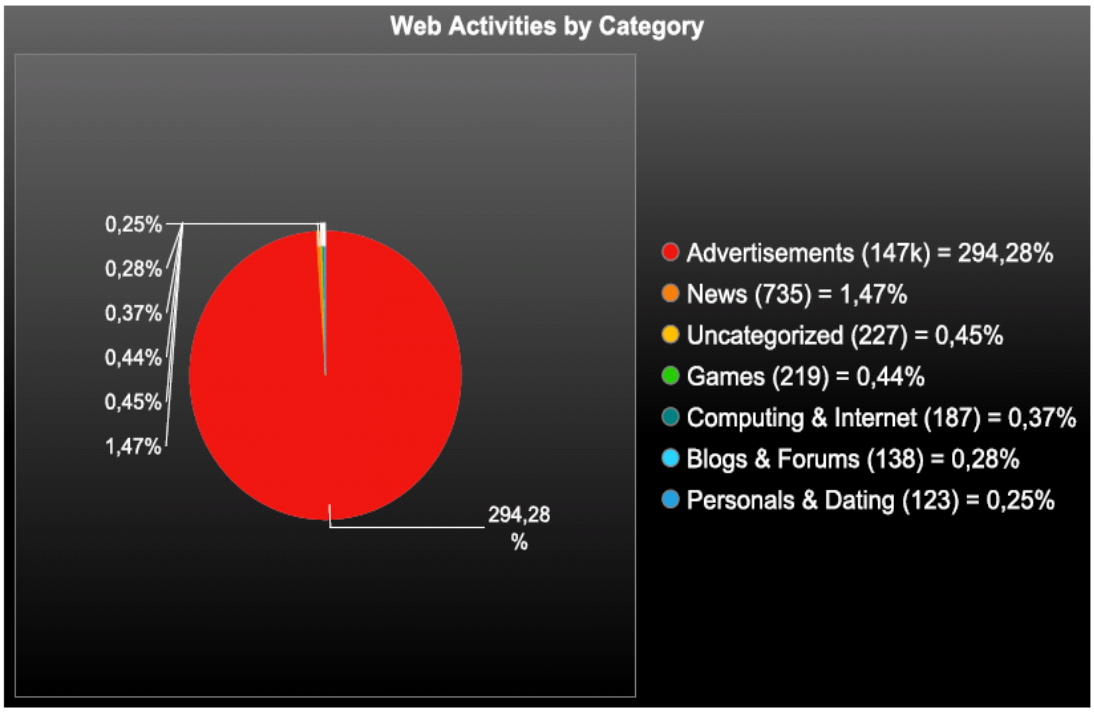
Los puntos a considerar son:

- Ancho de banda se utiliza de forma desproporcionada con respecto al número de usuarios y el uso de Internet
- Ancho de banda anormalmente utiliza para ciertos días períodos (o botnets sospecha descarga ilegal)

Sentinelle (172.16.10.1) 70A102A512CEC

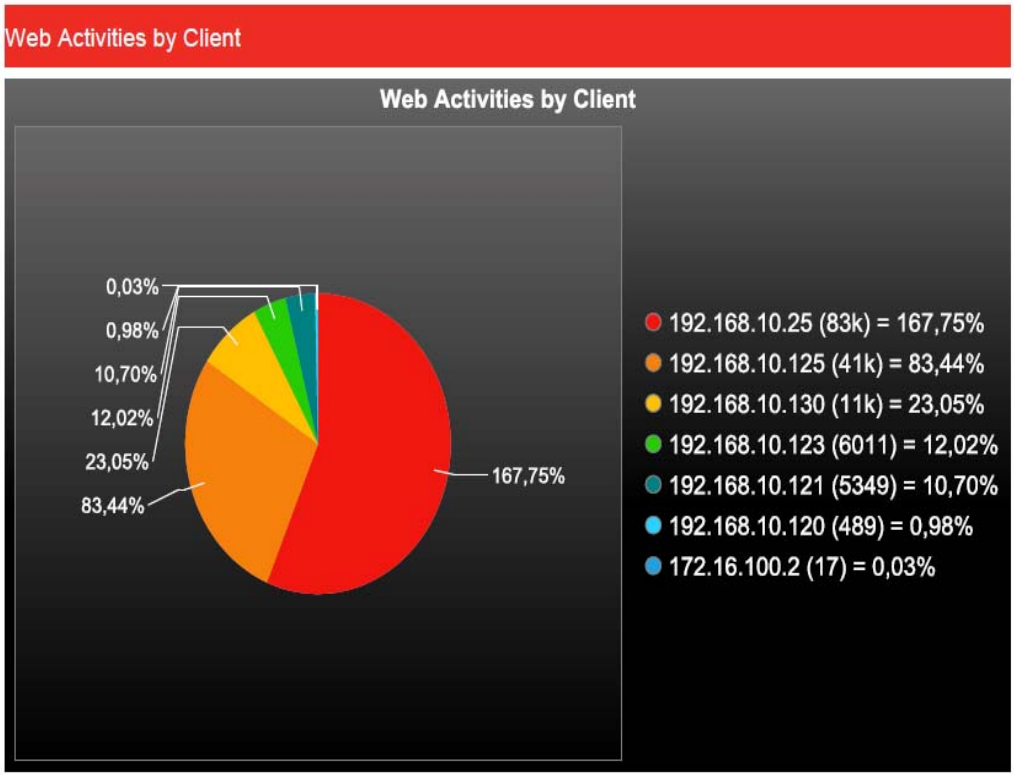
From	To	Number of Logs
01/05/11 08:00	16/05/11 18:00	50 000

Web Activities by Category



Los puntos a considerar son:

- Categorías y por lo tanto, innecesarios para bloquear como "juegos" o "personales y citas"
- Categorías toleradas para actividades personales, pero que son demasiado, en proporción a la actividad general: la limitación de ciertas actividades o recomendación de los intervalos temporales para establecer (en función de la programación del servidor de seguridad, tales como sólo permitir el acceso a Facebook durante las horas del almuerzo).



Los puntos a considerar son:

- La actividad anormal de un usuario (ver "auditoría por cliente web" para dar más detalles de la actividad del usuario y el abuso)
- La actividad anormal de un servidor (servidor interno el uso ilegal botnet o el servidor)

Ejemplo de anomalía en web: posible descarga de contenido ilegal

Domain Name/IP Address	Bytes Transferred	%
update.nai.com	1,62 GB	21,05%
img.playa-games.com	381,09 MB	4,84%
www86.megaupload.com	350,62 MB	4,46%
www1259.megaupload.com	350,01 MB	4,45%
www865.megaupload.com	350 MB	4,45%
www1028.megaupload.com	350 MB	4,45%
www22.megaupload.com	349,62 MB	4,44%
proxy-48.dailymotion.com	290,19 MB	3,69%
Total 8	7,68 GB	51,83%

Los datos muestran un mal uso del sitio de descargas **Megaupload** para la recuperación de archivos de gran tamaño.
Este sitio alberga una gran cantidad de vídeo en general, sujetos a derechos de autor. Esta actividad puede estar prohibida por diversas leyes, con riesgo de interrupción de la conexión a Internet o una multa. Se recomienda encarecidamente a cortar el acceso a este tipo de sitios por razones legales y también por el impacto de este tipo de descarga en el ancho de banda corporativo.

Ejemplo de anomalía en web: sitios de pornografía

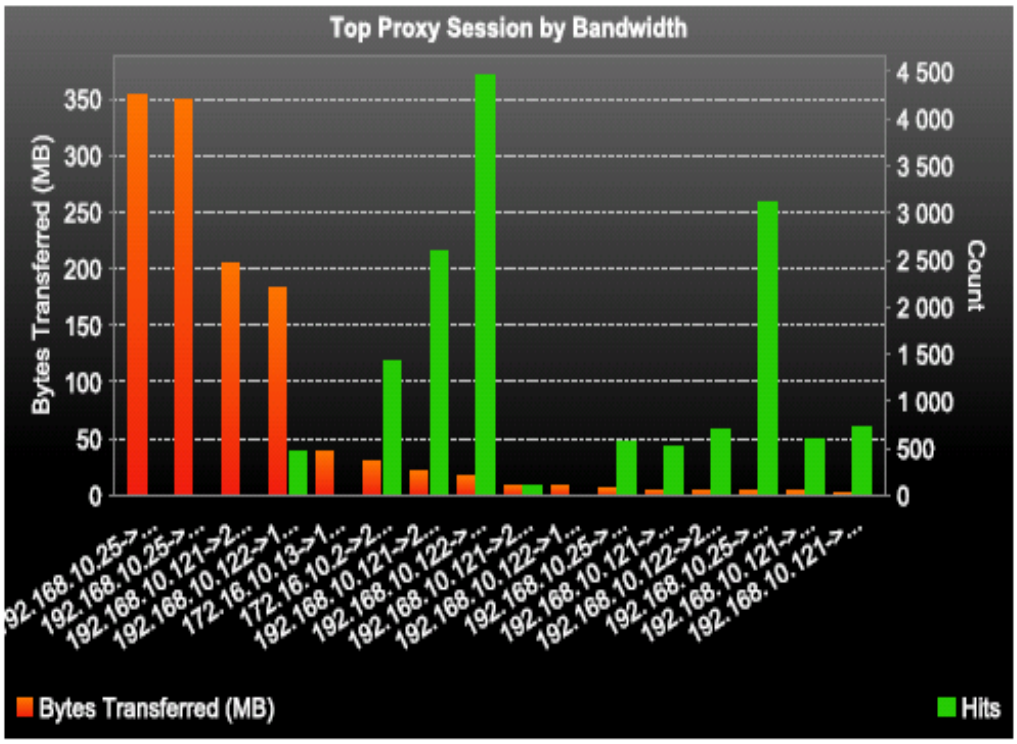
Similares resultados a los anteriores, pero con webs que incluyen estos contenidos.

Ejemplo de anomalía en web: sitios de juego online

Similares resultados a los anteriores, pero con webs que incluyen estos contenidos.

3.3. Top Proxy Session

Top Proxy Session by Bandwidth



Host	Bytes Transferred	%	Count	%
192.168.10.25->87.255.33.136:http	353,5 MB	26,83%	1	0,01%
192.168.10.25->95.211.91.237:http	350 MB	26,56%	1	0,01%
192.168.10.121->206.191.171.102:ftp	204,1 MB	15,49%	5	0,03%
192.168.10.122->188.165.60.30:http	183,87 MB	13,96%	470	2,52%
172.16.10.13->173.194.20.150:http	39,27 MB	2,98%	6	0,03%
Total 5	1,29 GB	85,82%	18657	2,59%

Los resultados de la auditoría reveló algunas descargas sobre http y ftp. Será necesario controlar este tipo de descargas.

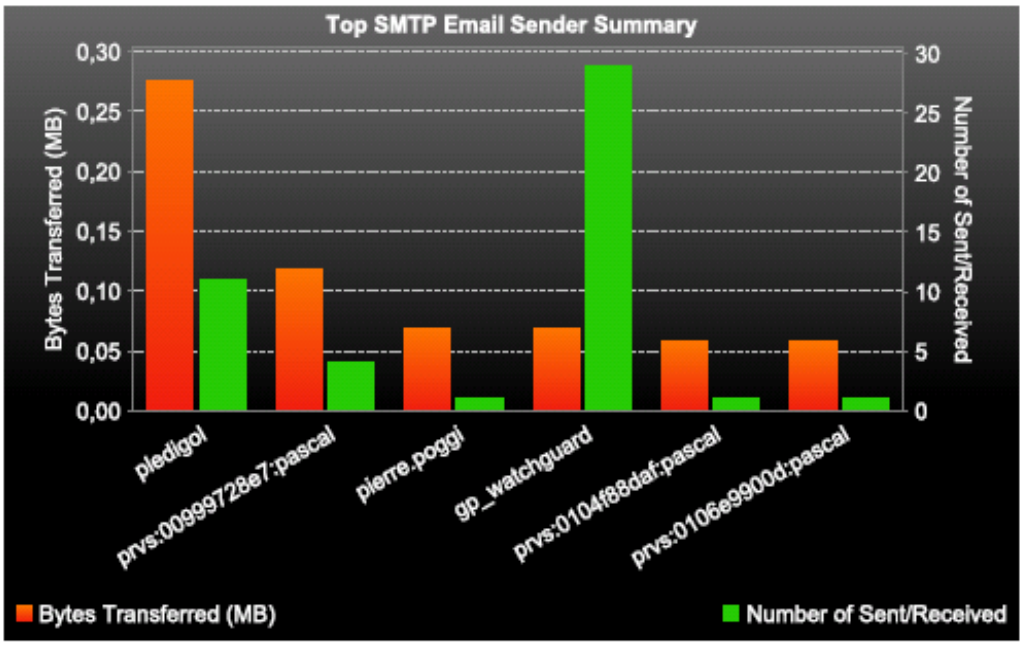
También es muy recomendable para poner en práctica mecanismos de QoS para evitar este tipo de descarga se lleve todo el ancho de banda en comparación con el flujo de negocios.

3.4. Trafico de Mensajería y antispam transparente

Sentinelle (172.16.10.1) 70A102A512CEC

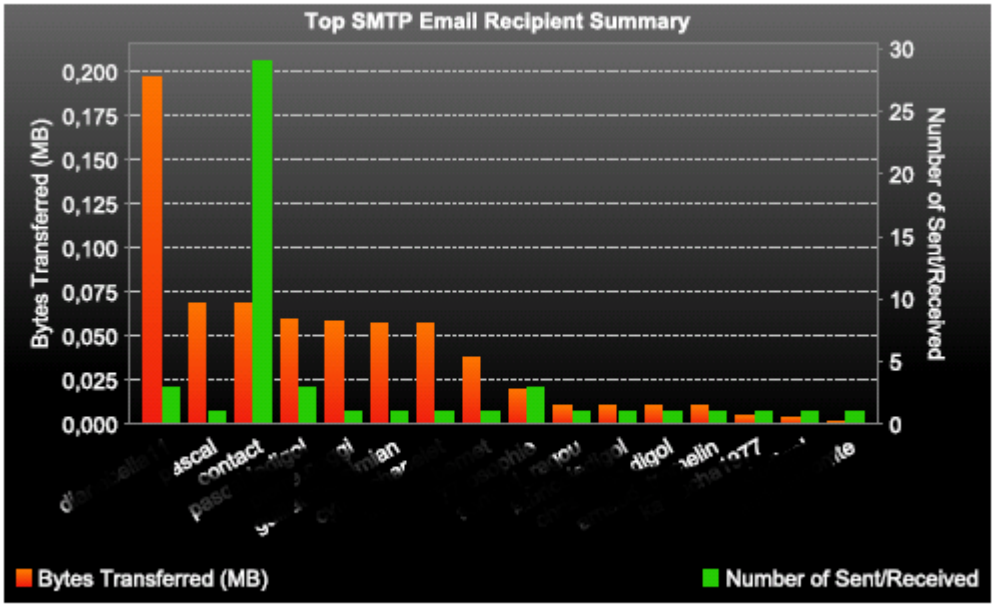
From	To	Number of Logs
17/04/11 17:40	17/05/11 17:40	47

SMTP Email by Sender Summary



Email	Bytes Transferred		Sent/Received	
	Bytes	%	Count	%
pledigol@yahoo.fr	281,88 KB	42,62%	11	23,40%
prvs:00999728e7:	121,1 KB	18,31%	4	8,51%
pierre.poggi@watchguard.com	70,61 KB	10,67%	1	2,13%
gp_watchguard@rapsodie.fr	70,15 KB	10,61%	29	61,70%
prvs:0104f88daf:	58,86 KB	8,90%	1	2,13%
prvs:0106e9900d:	58,85 KB	8,90%	1	2,13%
Total 6	0,65 MB	100,00%	47	100,00%

SMTP Email Summary by Recipient



SMTP Proxy Detail

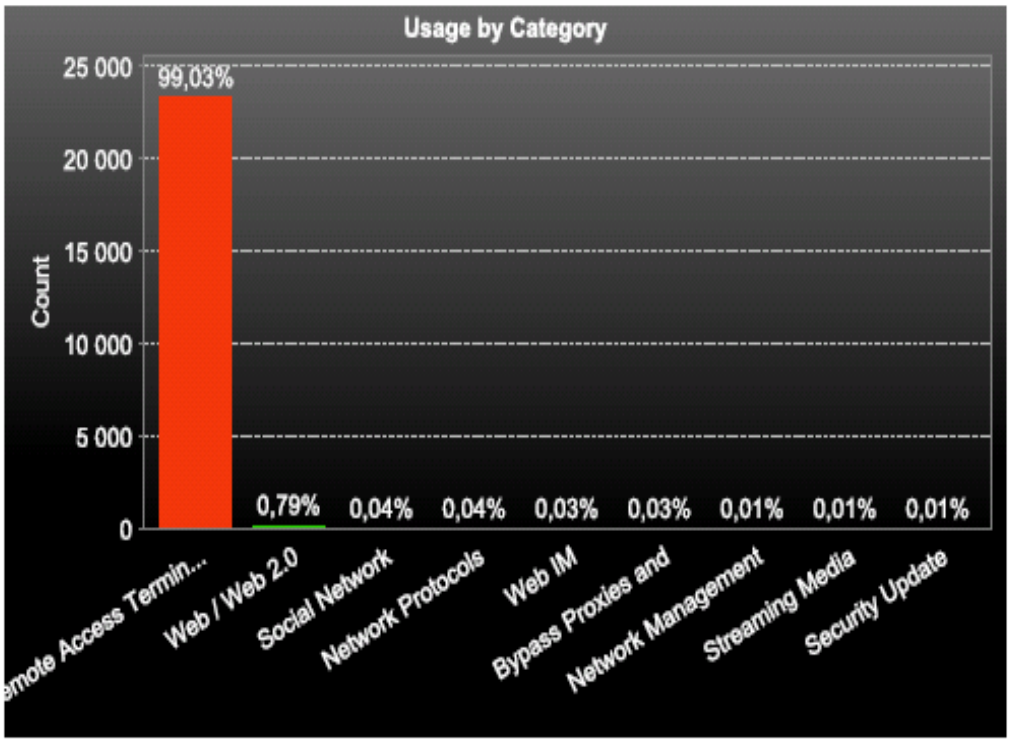
Event Time	Bytes Transferred
28/04/11 10:57	1,34 KB
Sender: prvs:00999728e7:pascal@watchguardenfrance.com	
Recipient(s): pascal.ledigol@watchguard.com	
28/04/11 10:59	58,89 KB
Sender: prvs:00999728e7:pascal@watchguardenfrance.com	
Recipient(s): pascal.ledigol@watchguard.com	

Puntos a considerar en el envío / recepción de mensajes de correo electrónico son los siguientes:

- El uso indebido de enviar archivos por correo electrónico.
- Adjuntos demasiado grandes.
- Recomendación cuota / limitación de tamaño

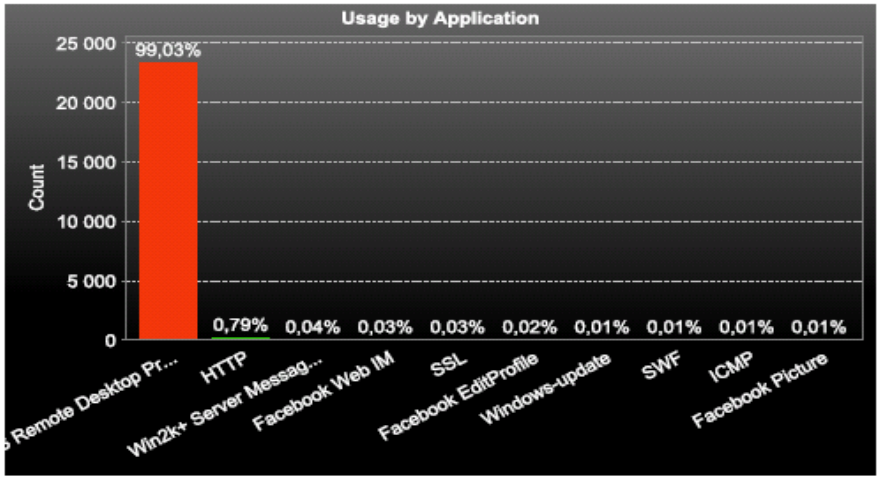
3.5. Tráfico de las aplicaciones

Usage by Category



Category	Count	%
Remote Access Terminals	23 306	99,03%
Web / Web 2.0	186	0,79%
Social Network	10	0,04%
Network Protocols	9	0,04%
Web IM	8	0,03%
Bypass Proxies and Tunnels	7	0,03%
Network Management	3	0,01%
Total 7	23 529	99,97%

Usage by Application



Application	Count	%
MS Remote Desktop Protocol (RDP)	23 306	99,03%
HTTP	185	0,79%
Win2k+ Server Message Block	9	0,04%
Facebook Web IM	8	0,03%
SSL	7	0,03%
Facebook EditProfile	5	0,02%
Windows-update	3	0,01%
SWF	3	0,01%
Total 8	23 526	99,96%

Los puntos a considerar son:

- Comparación de la utilización por categoría de negocios frente a la categoría deuso personal
    - Mucho de redes sociales→Recomendación total o parcial, se puede limitar a una mera consulta, evitar mensajes de vídeo, etc. Establecer franjas temporales para su uso.
    - Mucho de mensajería instantánea→ Recomendación de filtrado total o parcial. Es posible para permitir que el chat, pero no las transferencias de archivos y el uso de multimedia (vídeo / micrófono) para maximizar el impacto en el ancho de banda y reducir los posibles usos de la mensajería instantánea. Recordemos los riesgos de la transferencia de archivos a través de mensajería instantánea que pueden contener virus u otro malware
- Actividad anormal de un servidor (posible uso ilegal o parte de una botnet)
- La categoría de BypassProxies& Tunnelse debe supervisar. Si no hay ninguna razón por la que los túneles se establecen dentro de la red hacia el exterior, pues se puede tratar de un problema muy serio de seguridad mediante su elusión.
- Windows Update demasiado lento →Todos los PC's lo usan de forma independiente. Recomendación del uso de un servidor de actualizaciones.

Ejemplo de software de bypass firewall: Ultrasurf

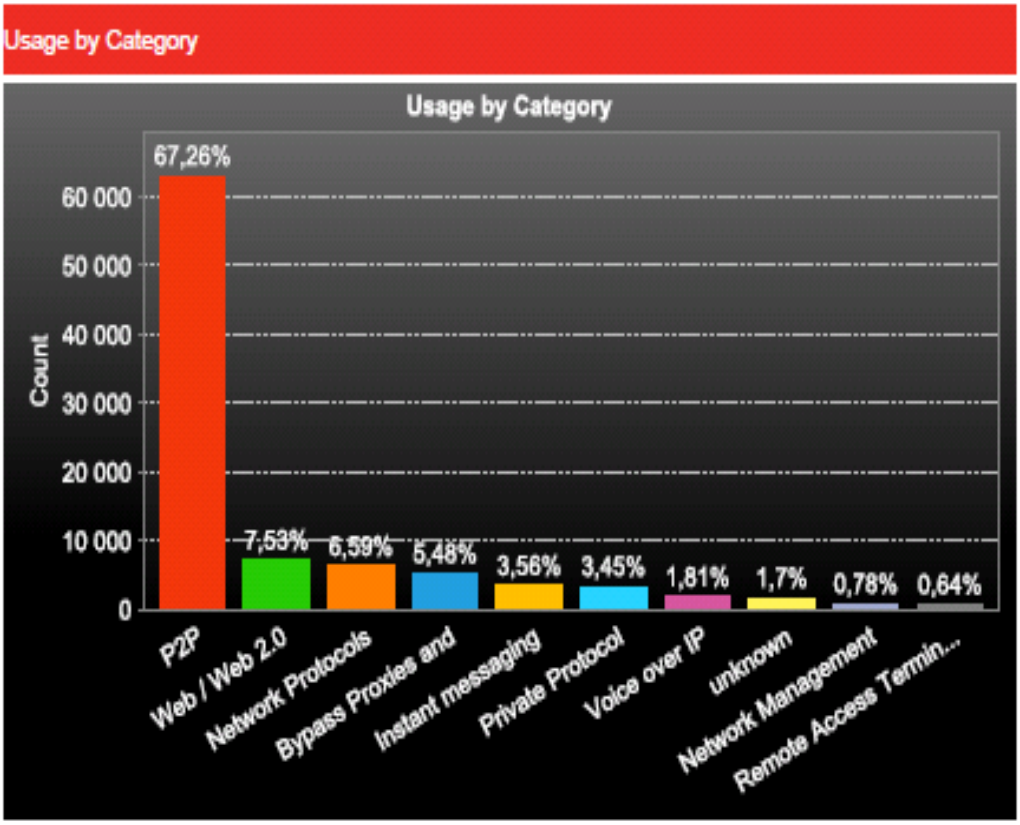
El análisis del tráfico de aplicaciones pone de manifiesto el uso de herramientas tales como Ultrasurf sin pasar por la seguridad del servidor de seguridad. Estas herramientas pueden permitir al usuario acceder a los recursos bloqueados en Internet como la descarga ilegal, juegos, videos, etc.

Esta herramienta ha sido detectado varias veces en la red durante el período auditado (n veces), y que a partir de varias estaciones de trabajo diferentes.

Es absolutamente recomendable para bloquear esta aplicación en la red, sino también para erradicar las estaciones de trabajo.

Application		Count	%
Wujie/UltraSurf		10	100,00%
Total	1	10	100,00%

Ejemplo de anomalía en aplicaciones : P2P

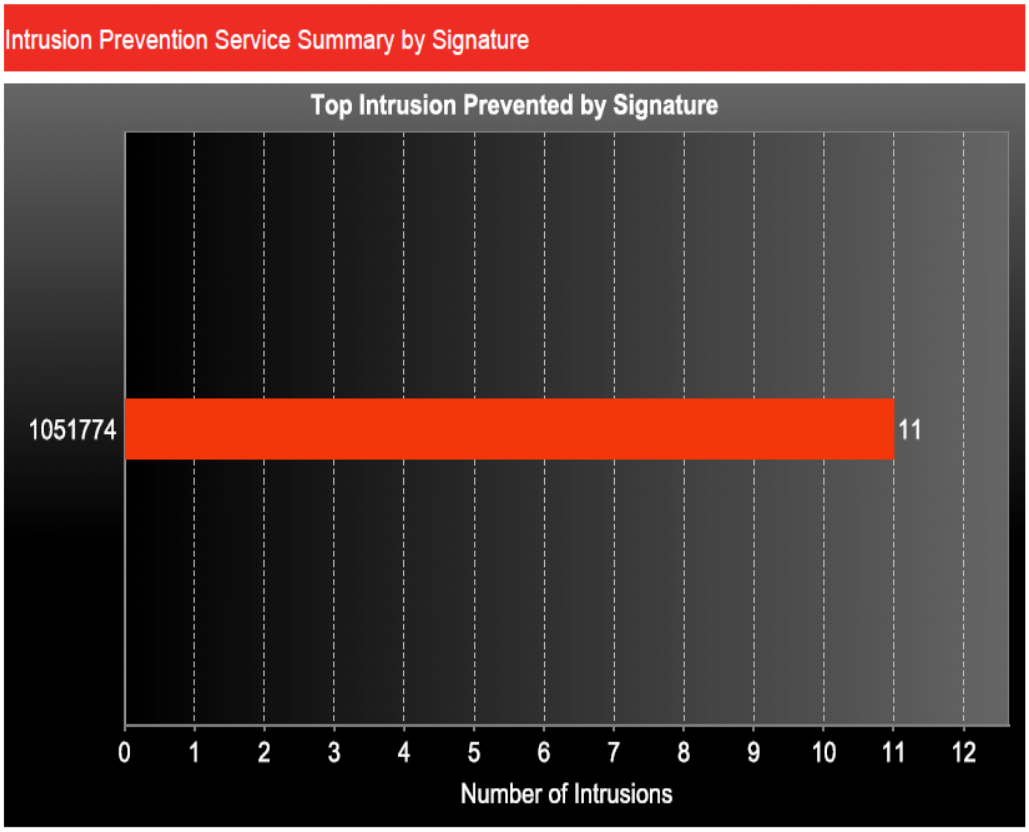


Category	Count	%
P2P	62 966	67,26%

3.6. Prevención de intrusión

XTM505 (172.16.10.154) 80B302964D4DF

From	To	Number of Logs
09/05/11 18:06	16/05/11 18:06	11



Aunque el propósito de la actividad de auditoría no es auditar el nivel de seguridad, la auditoría ha revelado un ataque, no filtrado por el firewall hoy en día.

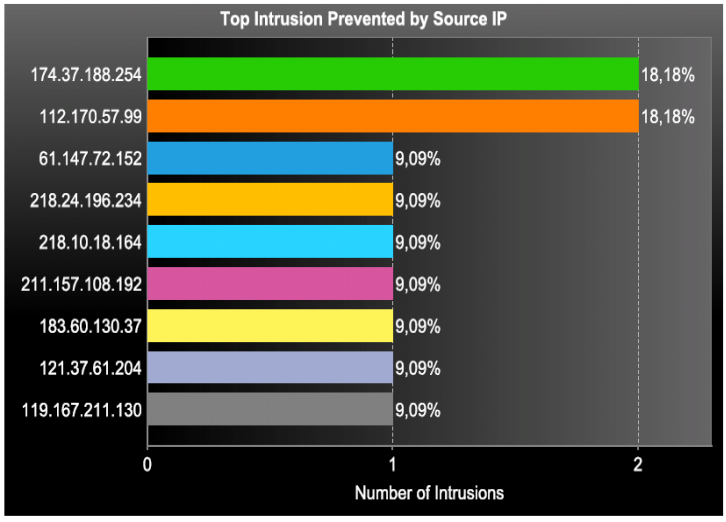
Intrusion Prevention Service by Signatures

Risk	Event Time	Protocol	Source IP:Port	Destination IP:Port
	10/05/11 02:55	rdp/tcp	211.157.108.192:6000	172.16.100.2:3389
	Policy: RDP-00		Proxy Action:	
	Message: Possible DoS HGOD SynKiller Flooding			
	10/05/11 05:21	rdp/tcp	174.37.188.254:6000	172.16.100.2:3389
	Policy: RDP-00		Proxy Action:	
	Message: Possible DoS HGOD SynKiller Flooding			
	11/05/11 09:12	rdp/tcp	218.10.18.164:6000	172.16.100.2:3389
	Policy: RDP-00		Proxy Action:	
	Message: Possible DoS HGOD SynKiller Flooding			
	12/05/11 05:31	rdp/tcp	121.37.61.204:6000	172.16.100.2:3389
	Policy: RDP-00		Proxy Action:	
	Message: Possible DoS HGOD SynKiller Flooding			
	13/05/11 12:53	rdp/tcp	119.167.211.130:6000	172.16.100.2:3389
	Policy: RDP-00		Proxy Action:	
	Message: Possible DoS HGOD SynKiller Flooding			

XTM505 (172.16.10.154) 80B302964D4DF

From	To	Number of Logs
09/05/11 18:09	16/05/11 18:09	11

Intrusion Prevention Service Summary by Source IP



Este ataque es un ataque a través de la regla de reenvío de puerto RDP de varias direcciones IP en Internet, que potencialmente podría evitar que los servidores se refiere para que funcione correctamente, o peor aún a tomar el control remoto. En este caso, sería aconsejable que el acceso remoto RDP sólo a través de un portal SSL VPN para prevenir este tipo de intrusión.

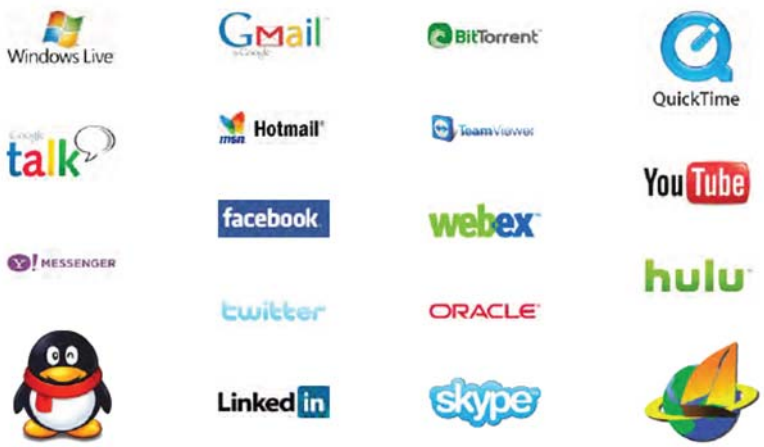
3.7. Conclusiones

Recordar las diversas recomendaciones fundamentales para la salud de la red de acuerdo con lo que se ha identificado en los informes.
Recomendamos el control de las aplicaciones para aumentar el nivel de seguridad existente. El siguiente capítulo trata sobre el control de las aplicaciones y sus beneficios.

4. Control de Aplicaciones

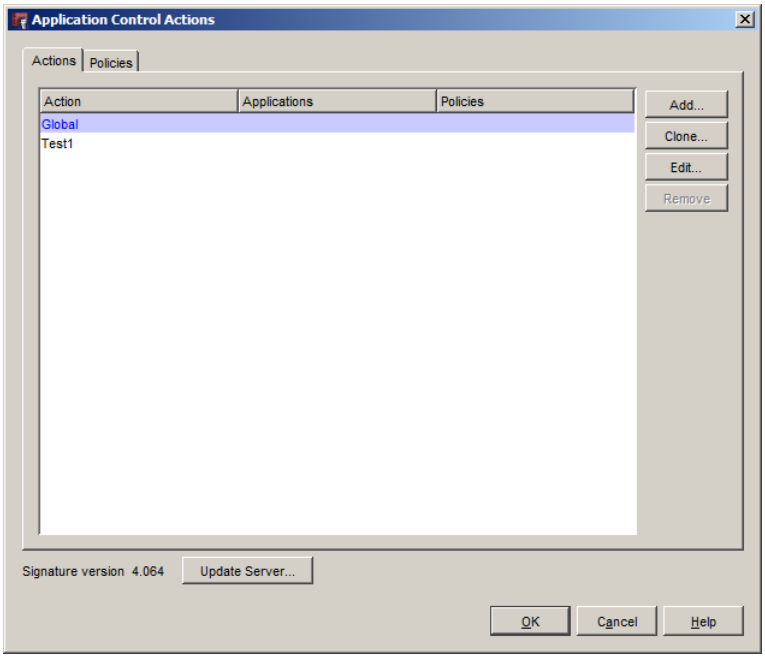
El Control de Aplicaciones en WatchGuard es una suscripción de seguridad integrada para dispositivos WatchGuard XTM. Permite a los administradores supervisar y controlar el acceso a las aplicaciones web y empresariales para hacer cumplir la política de seguridad y proteger la productividad y el ancho de banda de red.

El Control de Aplicaciones de WatchGuard mejora la seguridad de sus redes locales y remotas, logrando un mejor uso de sus recursos de TI.



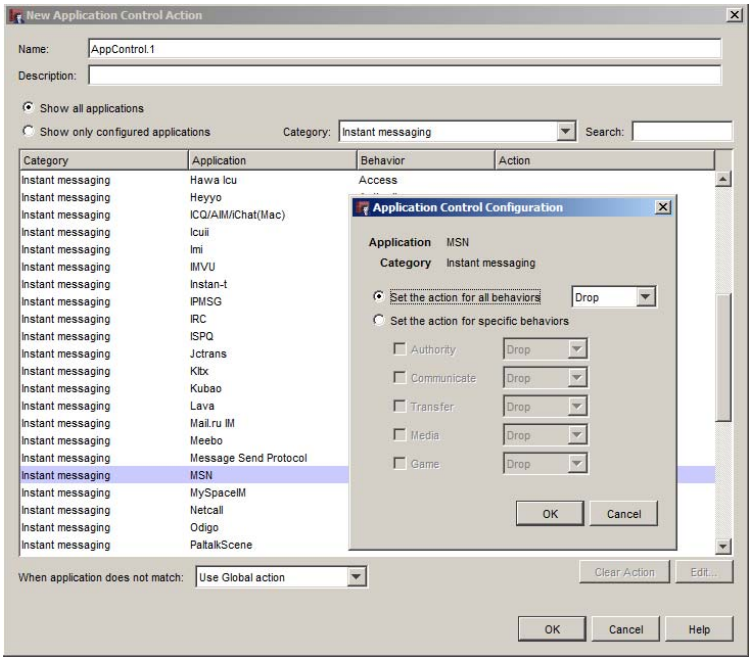
Con el Control de Aplicaciones, puede permitir, bloquear o denegar el acceso a aplicaciones basadas en un grupo de usuarios, sus tareas y la hora del día, y generar informes de uso. Por ejemplo, usted puede optar por:

- bloquear el uso de YouTube, Skype y MSN en cualquier momento durante las horas de oficina
- bloquear el uso de todas las aplicaciones P2P pero para parte del equipo de gestión
- autorizar el acceso al departamento de marketing de Facebook y otras redes sociales
- autorizar el lanzamiento de Windows Live Messenger para mensajería instantánea, pero denegar su uso para la transferencia de archivos
- limitar la transmisión de las aplicaciones de los medios de comunicación en momentos específicos del día
- Obtener el top 10 aplicaciones que se utilizan en la empresa
- Informe del uso (o intento de uso) las aplicaciones por usuario dentro de la empresa



Creación de acciones de Application Control

El administrador puede configurar varias acciones de control de aplicaciones que se aplicarán las reglas que ellos quieren. La acción de control de aplicaciones puede heredar una acción predeterminada (global) o ser independientes. Esta acción será definir las aplicaciones con control de flujo de tráfico. Para cada flujo de tráfico, el administrador puede asociar acciones diferentes y por lo tanto el control de las aplicaciones de forma diferente dependiendo de la fuente / destino, protocolo, horarios, etc…



Configuración de una acción y sus comportamientos

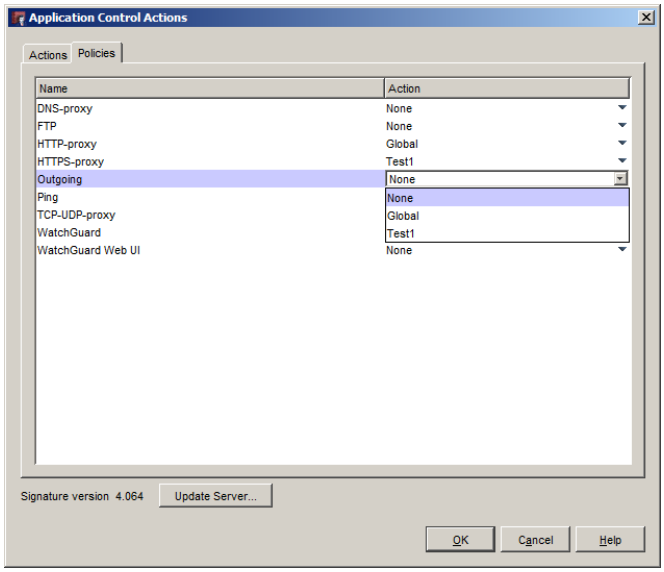
La base de aplicaciones permite encontrar éstas mediante:

- Categoría de la aplicación
- Aplicación
- Comportamiento de la aplicación

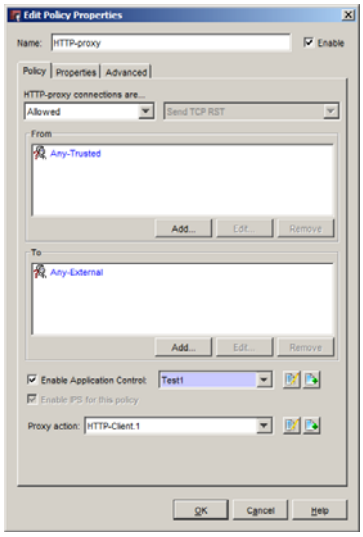
Hay más de 20 categorías diferentes de aplicaciones en las que se reparten las más de 1800 soportadas actualmente, así como firmas para diferenciar sus distintos comportamientos. Ciertas aplicaciones, como por ejemplo, MSN, permiten un control altamente granular:

- Autenticación
- Transferencia de ficheros
- Chat
- Media (webcam)
- Juegos integrados en la aplicación

La interfaz de administración permite buscar rápidamente una aplicación con sólo comenzar a escribir su nombre en la herramienta de búsqueda integrada.

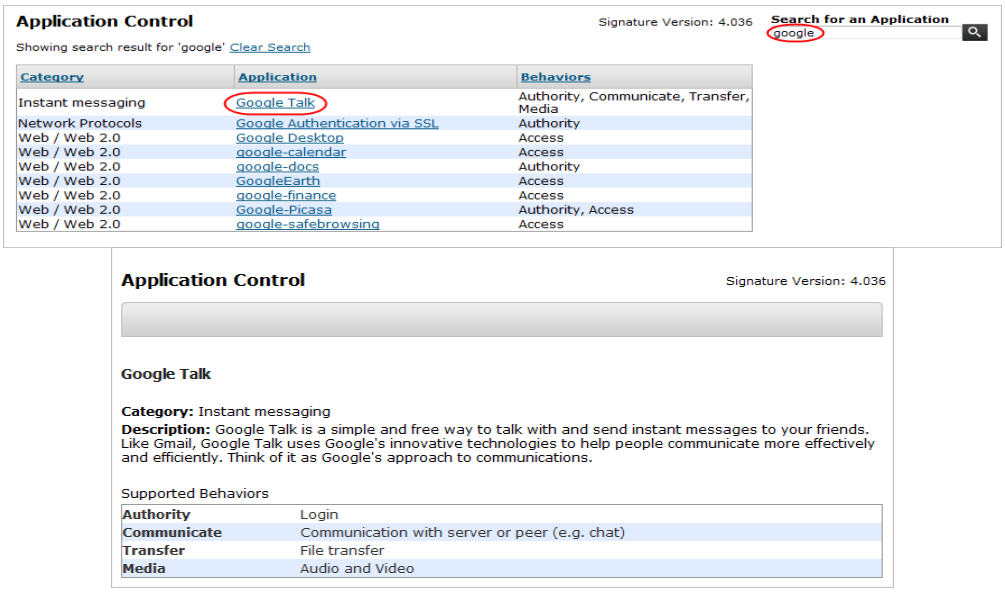


Aplicación de las acciones de Application Control a las reglas.



Activación o desactivación de Application Control en una regla

Por otro lado, WatchGuard publica un portal web en la que consultar las aplicaciones soportadas y sus comportamientos disponibles. Un administrador podrá verificar en todo momento si una aplicación es detectada.



SecurityPortal de WatchGuard con un detalle de aplicación

Finalmente, la función de informes integrada con los appliances de WatchGuard proporciona 5 tipos diferentes de informes respecto al Control de Aplicación.

Esto permite a un administrador saber exactamente cómo se utiliza su red y qué aplicaciones y modificar la política de seguridad en consecuencia. Este informe aporta realmente una herramienta nueva y muy potente para los administradores de red que ya no se contentan con ver cómo la red está ocupada en términos de flujos, pero en realidad en términos de aplicaciones lanzadas por los usuarios.