Configurar OpenDNS – Zeroshell

OpenDNS les proporciona a los usuarios de Internet un servicio gratuito de "**Sistema de Nombres de Dominio - DNS**" accesible desde cualquier host, independientemente de la dirección IP de la red usada para hacer la petición. Este sistema de DNS esta ganando gran popularidad ya que ofrece una serie de ventajas, las cuales no son ofrecidas por los tradicionales servicios de DNS que proporcionan los "**Proveedores de Servicio de Internet – ISP**".
Este documento muestra las ventajas de utilizar OpenDNS y provee instrucciones de configuración para Zeroshell Router/Firewall. Adicionalmente, Zeroshell cuenta con un "Updater", el cual actualiza a OpenDNS con la IP dinámica asignada al router o modem que provee el ISP. "Esto se da, si usted no cuenta con una IP estática"
Gracias a esta característica, usted puede personalizar funciones en el "**Dashboard**" de la página web de OpenDNS, para utilizar en su totalidad características avanzadas tales como: filtrado de contenidos web y control parental.

Este documento esta dividido en las siguientes secciones:

OpenDNS para mejorar los tiempos de respuesta en la navegación web

Una de las razones para que la navegación en Internet sea lenta además de otros servicios que requieren de Internet para su funcionamiento, es la lenta respuesta que tiene el servicio de DNS. Teniendo que satisfacer un gran numero de peticiones, OpenDNS tiene una extensa y actualizada memoria cache. Esto significa que si un cliente pregunta por la resolución de un nombre a su respectiva IP, OpenDNS probablemente ya conoce la respuesta sin necesidad de solicitar a la autoridad DNS correspondiente esta petición. Mas aun, OpenDNS provee un DNS recursivo que puede directamente responder las peticiones de los clientes, sin tener que recibir las respuestas de los bucles

posteriores, se obtiene eficiencia en el proces amiento y así se reducirá el tiempo de espera del cliente.

OpenDNS y protección Anti-Phishing

Una de las mas peligrosas trampas de navegación es llamada “Phishing”. Un usuario puede ser fácilmente engañado y de esta forma llevado a proveer información confidencial tal como: Información de tarjetas de crédito, datos de cuenta en sitios web de sucursales virtuales de bancos que parecen ser reales pero que en realidad solo intentan adquirir esta información para usos ilícitos.
Los nombres de estos sitios de “Phishing” son casi exactamente iguales que los de los sitios reales, para así poder fácilmente confundir a los usuarios. Estos son abiertos haciendo click en links spam que se envían en los mensajes e-mail o que aparecen digitando de forma incompleta e incorrecta en el navegador la dirección URL del banco real. Obviamente, estos sitios no usan protocolo encriptado https por lo que el usuario ni siquiera recibe mensajes de advertencia por certificado digital invalido. Por lo tanto, OpenDNS cuenta con una base de datos que contiene una lista muy completa de sitios usados para “Pishing”, la cual le ayudará a prevenir el “Pishing” ya que estos sitios son bloqueados en la resolución de nombres a IP y de esta forma no podrán ser exhibidos.

Filtro de contenido web y control parental

Simplemente se debe usar las 2 direcciones IP del los servidores DNS, 208.67.222.222 y 208.67.220.220 así, se usará OpenDNS para obtener mejor respuesta en los tiempos de búsqueda y conseguir protección “Anti - Pishing”. Por otra parte, usted puede crear una cuenta O penDNS para obtener acceso al Deshboard que está en el sitio web de OpenDNS, donde podrá configurar los servicios que mejor satisfagan sus necesidades y usar los servicios avanzados de OpenDNS. Específicamente, usted puede filtrar sitios web dividiéndolos en categorías inapropiadas para sus usuarios. Por ejemplo, usted puede deshabilitar la resolución de nombres de sitios, clasificándolos como sitios con contenido pornográfico. Todo esto se puede realizar utilizando las opci ones del Deshboard. También es posible bloquear o permitir la resolución de nombres de páginas individuales como por ejemplo: “www.facebook.com”, configurándolas con las opciones “Blacklist” o “Whitelist” en el Deshboard según sea el caso.
Obviamente, si usted quiere utilizar todas las opciones avanzadas, debe crear un enlace entre la cuenta OpenDNS y la dirección IP de la Red que se quiere configurar con los servicios de OpenDNS. Si la dirección IP de la red es estática, simplemente se debe configurar en el Deshboard. También usted puede usar un actualizador DNS para direcciones IP dinámicas, para enviar los cambios de la dirección IP publica de la red que se está configurando a la base de datos de OpenDNS.

Zeroshell puede ayudarlo con esta tarea y más adelante se verá como hacerlo.

Estadísticas de uso de Internet

La mejor forma para ver cual es el servicio de Internet mas utilizado en su red, es obtener estadísticas en las peticiones de resolución de dominios. Obviamente, las peticiones de servicio son: (WWW, e-mail, VoIP, etc.), es difícil acceder a los servicios por medio de la dirección IP puesto que es muy complejo recordarlas y además pueden cambiar dinámicamente, pero son casi siempre accesibles por medio del nombre del host del sitio web. OpenDNS le permite a usted ver las estadísticas de los accesos a los dominios. Recuerde que las estadísticas pueden ser activadas en el Deshboard después de registrarse en OpenDNS.

Corrección de escritura de URL

Otra opción de OpenDNS tal vez no tan importante, es la corrección de escritura de URL. Si usted ingresa una URL inexistente, OpenDNS estará atento a interpretar la petición del usuario y si es posible automáticamente la corrige antes de enviar la página web buscada.

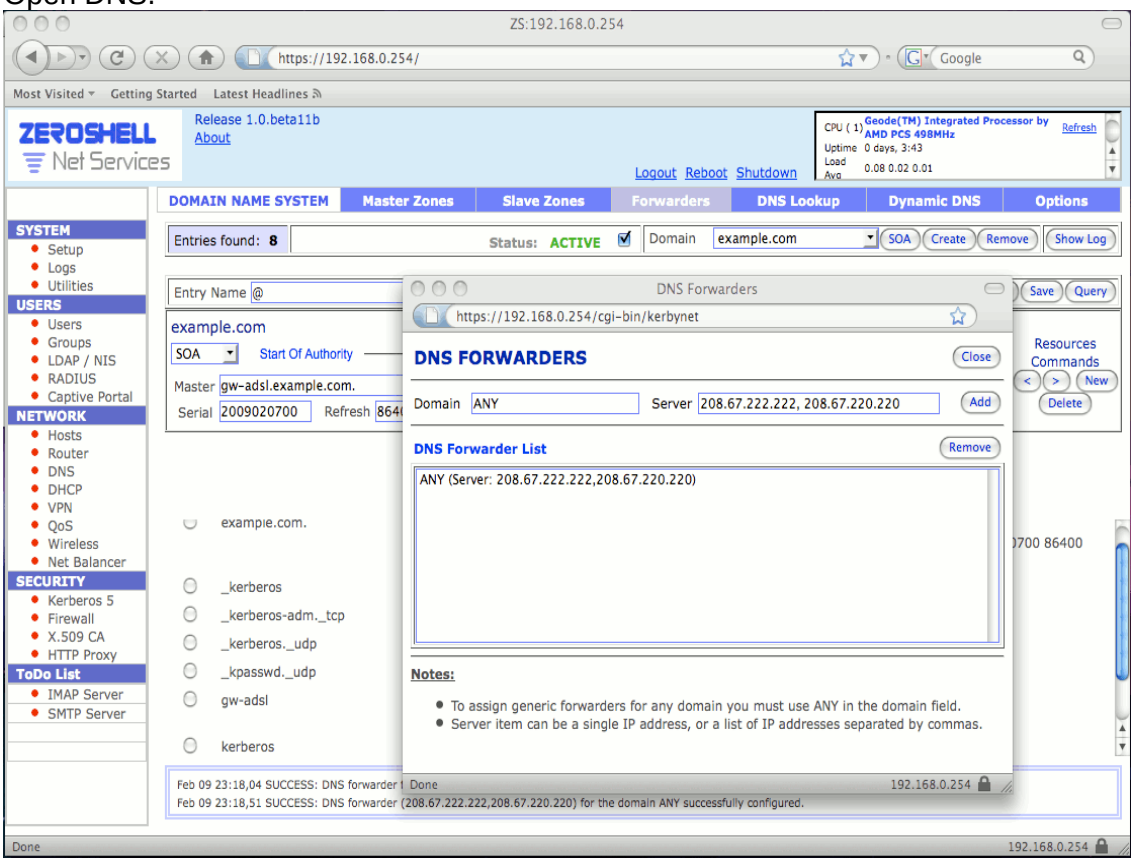
Abreviación de escritura de URL

Con una cuenta OpenDNS usted también puede crear abreviaciones para así, asignar fácilmente nombres cortos a direcciones web largas y complejas. Usted será automáticamente redireccionado a la dirección web asociada al nombre corto, cuando usted digite esta abreviación en la barra de direcciones del navegador. Está herramienta no es esencial pero puede ser de gran ayuda en la navegación.

Configuración de Zeroshell para trabajar con OpenDNS

Con la intención de tomar ventaja de las características que OpenDNS ofrece, simplemente se debe agregar las 2 direcciones de DNS (208.67.222.222 y 208.67.220.220) y configurarlas manualmente en cada usuario de Internet. También, usted puede configurar un servidor DHCP para configurar las direcciones DNS de forma automáticas. Otra posibilidad seria, si usted tiene un servidor DNS en su LAN, configurarlo para trabajar como servidor DNS cache y también configurar a OpenDNS en modo "*Forwarders"* y así resolver cualquier dominio no autorizado. De esta forma, cuando las respuestas a las peticiones de los clientes no estén en el DNS cache de la LAN, de inmediato envía las peticiones al servidor OpenDNS en lugar de *ROOT DNS*.

También para tener cache local, esta solución le permite manejar características de OpenDNS avanzadas, creando una cuenta sencilla y solo actualizando la dirección IP del servidor DNS local en la base de datos de Open DNS.



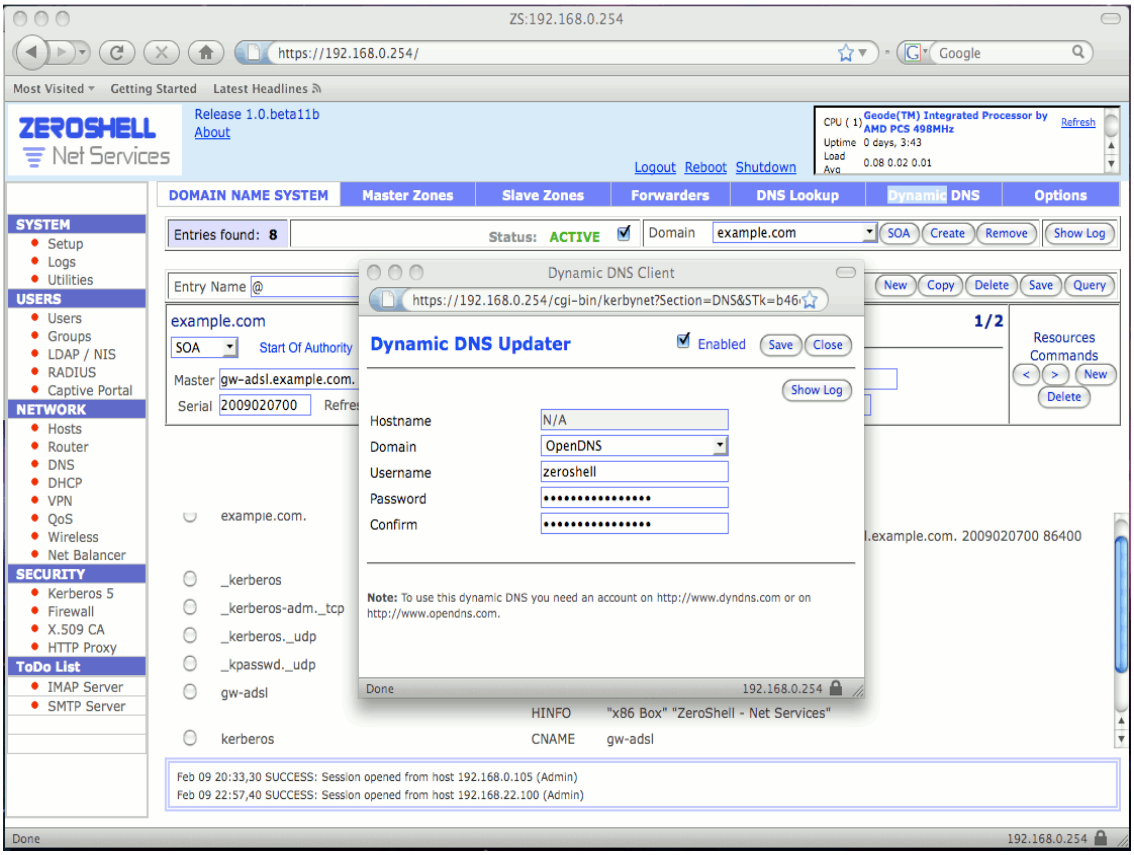
Configurar OpenDNS como DNS Forwarders

Para configurar el servidor DNS de Zeroshell como se ha descrito para usar OpenDNS como "Forwarders", simplemente diríjase a la sección [DNS][Forwarders] para actualizar los servicios con las IPs 208.67.222.222 y 208.67.220.220 separadas por una coma y digitando ANY como el dominio. El resultado es como el que se muestra en la imagen que está arriba de este texto.

Configuración del actualizador dinámico de DNS para OpenDNS

En este punto, una vez que los 2 DNS "Forwarders" son configurados, OpenDNS está en disposición de ser usado por los clientes. Sin embargo como ya se ha mencionado, para usar los servicios avanzados tales como: personalizar filtros web y control parental, estadísticas de acceso a Internet y nombres cortos a las direcciones web complejas; usted puede informarle a OpenDNs la dirección IP usada para hacer las peticiones. Si usted tiene una dirección estática, usted solo tiene que configurarla una sola vez en el

“Deshboard”, pero si no es así, usted podría usar un actualizador dinámico de DNS para las direcciones ÏP dinámicas.



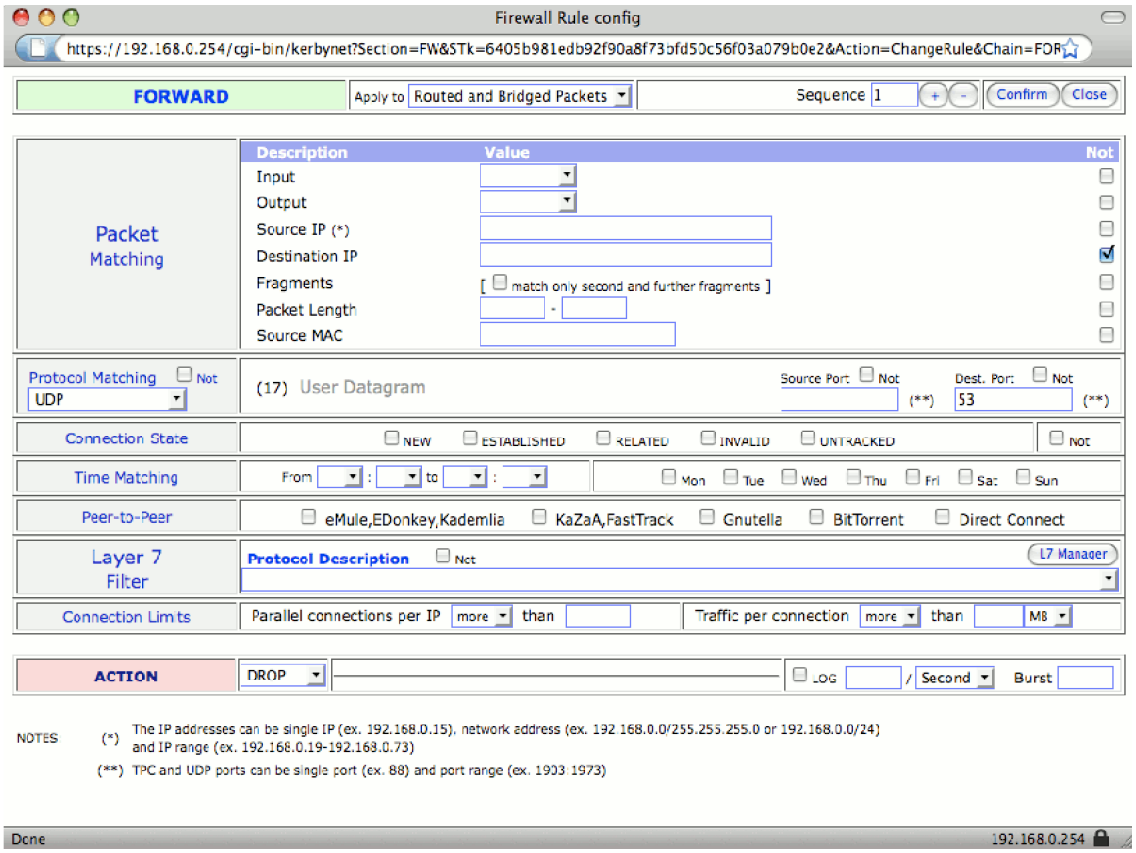
Actualizador OpenDNS para mantener actualizada la dirección IP dinámica en la base de datos de OpenDNS

Zeroshell tiene un cliente de DNS dinámico compatible con OpenDNS . Para configurarlo, solo seleccione OpenDNS como dominio en la sección [DNS][Dynamic DNS] (como se muestra en la imagen de arriba), luego ingrese el usuario y la contraseña de su cuenta OpenDNS y active el servicio.

Configuración del firewall para prevenir la no utilización de OpenDNS

Si usted intenta habilitar el filtro web para prevenir acceso a ciertos sitios categorizados, usted debería asegurarse que el cliente DNS usado en Zeroshell sea OpenDNS y este se utilice en modo “Forwarder”. De esta forma, los usuarios no podrán cambiar sus clientes DNS para burlar las restricciones que usted ha configurado en el “Deshboard” de OpenDNS . Ademas usted deberá asegurarse de que Zeroshell sea usado como el “ Gateway por defecto

para dar acceso a Internet" o como "Bridge transparente" luego debe bloquear las comunicaciones al puerto TCP/UDP 53 en el firewall.



Configuración del Firewall para prevenir el uso de otros DNS diferentes a OpenDNS.

Este bloqueo puede ser configurado en la chain *FORWARD* para procesar el tráfico del router. El servidor DNS de Zeroshell no se verá afectado por esta regla de Firewall.