Pengaturan OpenDNS

OpenDNS menyediakan pengguna internet dengan layanan Domain Name System bebas diakses dari host manapun, terlepas dari alamat IP jaringan yang digunakan untuk mengirim permintaan. Sistem DNS ini adalah mendapatkan popularitas dengan jutaan pengguna karena menawarkan serangkaian keuntungan yang tidak disediakan oleh layanan DNS tradisional yang ditawarkan oleh Internet Service Provider.
Dokumen ini berisi daftar keuntungan menggunakan OpenDNS dan memberikan petunjuk konfigurasi untuk ZEROSHELL Router / Firewall. Selain itu, ZEROSHELL memiliki updater yang update OpenDNS dengan IP dinamis ditugaskan ke router. . Berkat fitur ini Anda dapat menyesuaikan fungsi pada web dashboard OpenDNS untuk sepenuhnya memanfaatkan fitur-fitur canggih seperti, misalnya, filter konten web dan kontrol orangtua Dokumen ini dipecah menjadi bagian-bagian berikut:

OpenDNS untuk meningkatkan waktu respon Web navigasi

Salah satu alasan untuk lambat web navigasi dan penggunaan layanan internet lainnya adalah kecepatan respon DNS lambat. Harus memenuhi seperti sejumlah besar permintaan, OpenDNS memiliki cache yang sangat besar dan diperbarui. Ini berarti bahwa jika klien meminta resolusi nama di IP, OpenDNS kemungkinan besar sudah tahu jawabannya, tanpa harus meminta DNS otoritatif untuk menerimanya. Selain itu, OpenDNS menyediakan DNS rekursif yang dapat langsung menanggapi permintaan klien. Tidak harus menerima tanggapan untuk loop selanjutnya membantu mengurangi waktu tunggu klien.

OpenDNS dan Anti Phishing perlindungan

Salah satu perangkap navigasi paling berbahaya disebut *Phishing* . Seorang pengguna mungkin akan tertipu untuk memberikan data sensitif seperti informasi kartu kredit atau online kredensial rekening bank login pada situs yang tampaknya aslinya tapi benar-benar hanya dimaksudkan untuk memperoleh informasi ini untuk penggunaan terlarang. Nama-nama situs phishing ini hampir persis sama dengan yang asli untuk membingungkan pengguna. Mereka dibuka dengan mengklik hyperlink dalam pesan spam atau salah memasukkan nama alamat di browser web Anda. Jelas, situs-situs tersebut tidak menggunakan protokol https terenkripsi sehingga pengguna bahkan tidak menerima valid peringatan sertifikat digital. Sejak OpenDNS memiliki database yang berisi daftar yang akurat dari situs yang digunakan untuk Phishing, hal ini membantu Anda untuk mencegah Phishing karena blok itu resolusi alamat IP dan dengan demikian layar.

Filter konten Web dan kontrol orangtua

Cukup menggunakan dua DNS, *208.67.222.222* dan *208.67.220.220* untuk menggunakan OpenDNS untuk meningkatkan waktu respon dan mendapatkan ptotection anti Phishing tanpa ada kekhawatiran lain. Namun, Anda dapat membuat account OpenDNS untuk membuka dashboard web di mana Anda dapat mengatur layanan yang terbaik untuk memenuhi kebutuhan Anda dan menggunakan layanan OpenDNS canggih. Khususnya, Anda dapat menyaring situs-situs membagi mereka ke dalam kategori yang dianggap tidak pantas bagi pengguna internet Anda. Sebagai contoh, Anda dapat menonaktifkan resolusi nama situs diklasifikasikan sebagai mengandung materi pornografi, yang membahas subyek ilegal atau jaringan sosial seperti Facebook atau pesan instan hanya menggunakan dashboard. Selain mengontrol konten menggunakan kategori default, Anda dapat setup sendiri *blacklist* dan *whitelist* untuk memblokir atau mengizinkan akses ke situs tertentu.
Jelas, jika Anda ingin menggunakan fitur-fitur canggih OpenDNS, Anda harus membuat hubungan antara akun pribadi Anda dan OpenDNS alamat IP pengguna internet '. Jika alamat IP yang statis, hanya mengatur mereka di Dashboard. Jika tidak, Anda dapat menggunakan updater DNS untuk alamat IP dinamis untuk mengirim perubahan alamat IP ke database OpenDNS. ZEROSHELL dapat melakukan tugas-tugas ini dan kami akan melihat bagaimana untuk memasangnya di bawah ini.

Penggunaan Internet statistik

Salah satu cara terbaik untuk melihat mana layanan Internet yang paling banyak digunakan pada LAN Anda adalah untuk mendapatkan statistik pada permintaan resolusi domain. Jelas, apa pun layanan yang diminta adalah (WWW, e-mail, VoIP, dll), sulit untuk mengakses layanan melalui alamat IP, yang sulit untuk mengingat dan bahkan bisa berubah secara dinamis, tapi hampir selalu dapat diakses melalui nama host .
OpenDNS memungkinkan Anda melihat statistik akses domain. Ingat bahwa statistik harus diaktifkan pada dashboard berikut OpenDNS pendaftaran.

URL cek ejaan

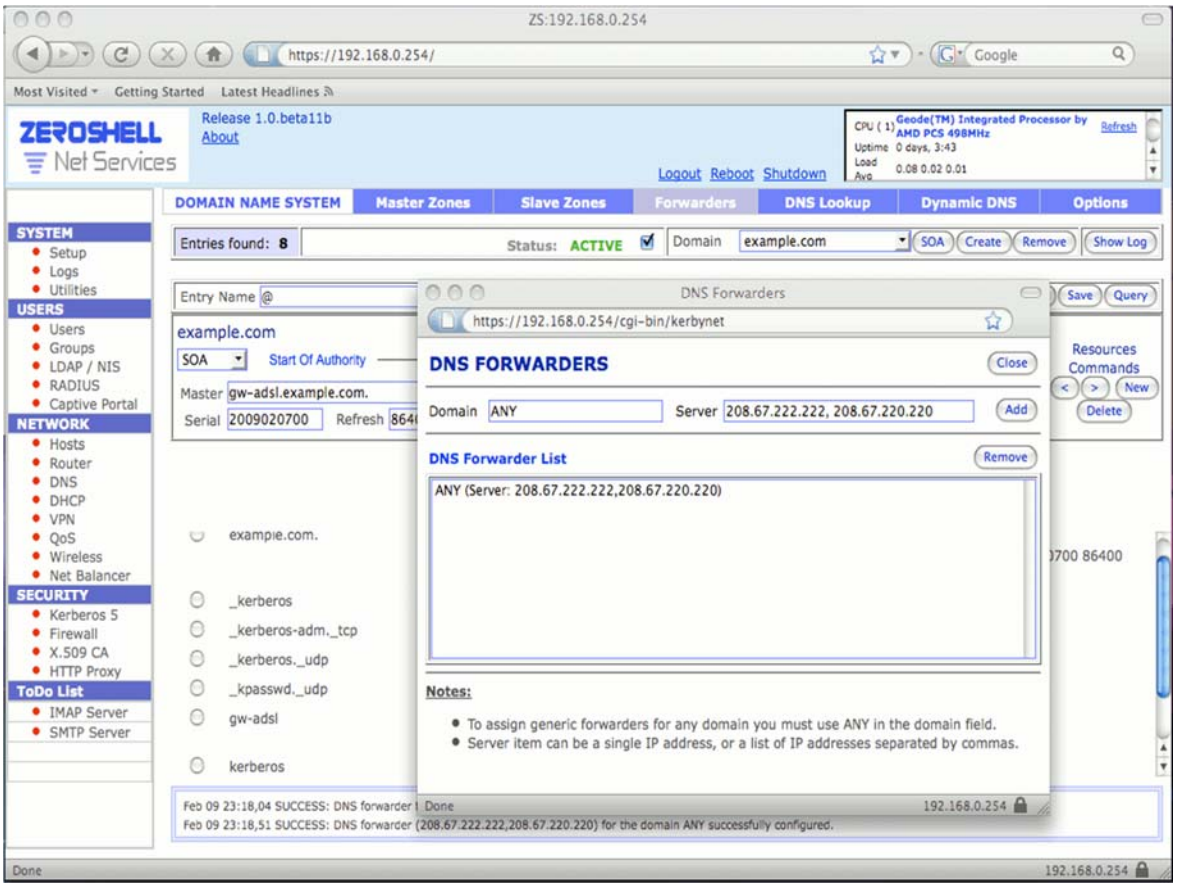
Membantu meskipun fitur lain tidak penting OpenDNS adalah hostname ejaan cek. Jika Anda memasukkan URL inexistent, OpenDNS mencoba untuk menafsirkan permintaan pengguna dan, bila mungkin, secara otomatis memperbaiki sebelum menanggapi dengan halaman pencarian web.

Pintas URL

Dengan account OpenDNS Anda dapat membuat shortcut pada dashboard untuk menetapkan mudah diingat nama panggilan ke alamat web yang panjang dan rumit.Anda akan otomatis diarahkan ke situs web terkait ketika Anda memasukkan cara pintas di address bar browser. Fitur ini tidak penting tetapi mungkin membantu alat navigasi web.

Menyiapkan ZEROSHELL untuk OpenDNS

Untuk memanfaatkan fitur OpenDNS, cukup tambahkan dua DNS (208.67.222.222 dan 208.67.220.220) ke pengaturan pada setiap klien pengguna internet. Jika tidak, Anda dapat mengatur server DHCP untuk secara otomatis mengatur mereka. Kemungkinan lain, jika Anda memiliki sebuah server DNS pada LAN Anda, adalah memiliki pekerjaan server sebagai DNS cache diatur untuk menggunakan OpenDNS sebagai *Forwarders* untuk menyelesaikan setiap domain non otoritatif. Dengan cara ini, ketika respon klien tidak di cache DNS LAN, hanya meneruskan permintaan ke server OpenDNS bukan *ROOT DNS* . Selain memiliki cache lokal, solusi ini memungkinkan Anda mengelola fitur OpenDNS canggih, membuat account tunggal dan dan hanya memperbarui alamat IP server DNS lokal dalam database OpenDNS.

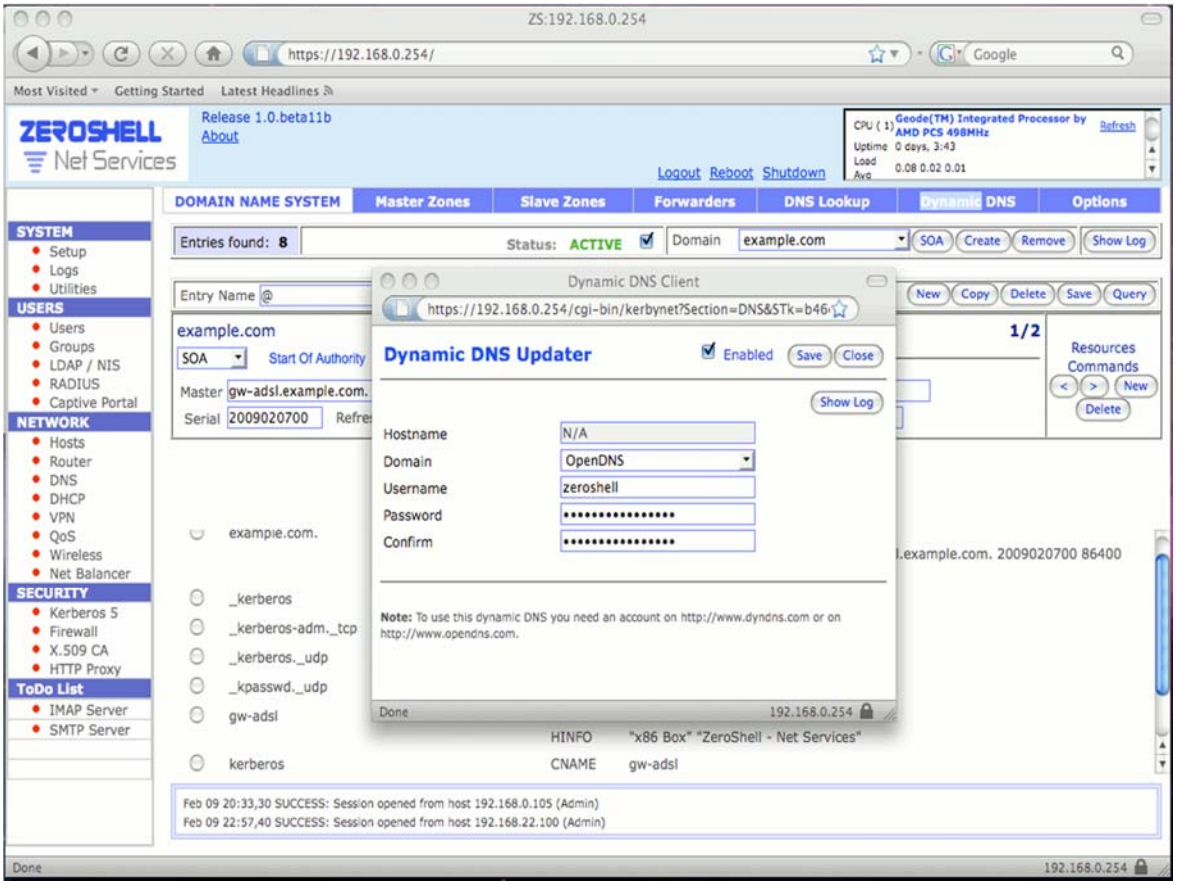


Menyiapkan server OpenDNS sebagai DNS forwarders

Untuk mengatur server DNS ZEROSHELL seperti yang dijelaskan untuk menggunakan OpenDNS sebagai forwarders, hanya menampilkan [DNS] [Forwarders] bagian dan memperbarui layanan dengan IP 208.67.222.222 dan 208.67.220.220 dipisahkan oleh koma dan menentukan *APAPUN* sebagai domain. Hasilnya adalah yang digambarkan di atas.

Mengatur Dynamic DNS Updater untuk OpenDNS

Pada titik ini, setelah dua forwarders DNS ditetapkan, OpenDNS sudah digunakan oleh klien LAN. Namun, seperti yang sudah disebutkan, untuk menggunakan layanan canggih seperti disesuaikan filter web dan kontrol orangtua, statistik akses Internet dan cara pintas, Anda harus memberitahukan OpenDNS alamat IP yang digunakan untuk mengirim permintaan. Jika Anda memiliki alamat IP statis, Anda hanya perlu mengaturnya sekali pada dashboard OpenDNS saat Anda harus menggunakan*Dynamic DNS Updater* untuk alamat IP dinamis.

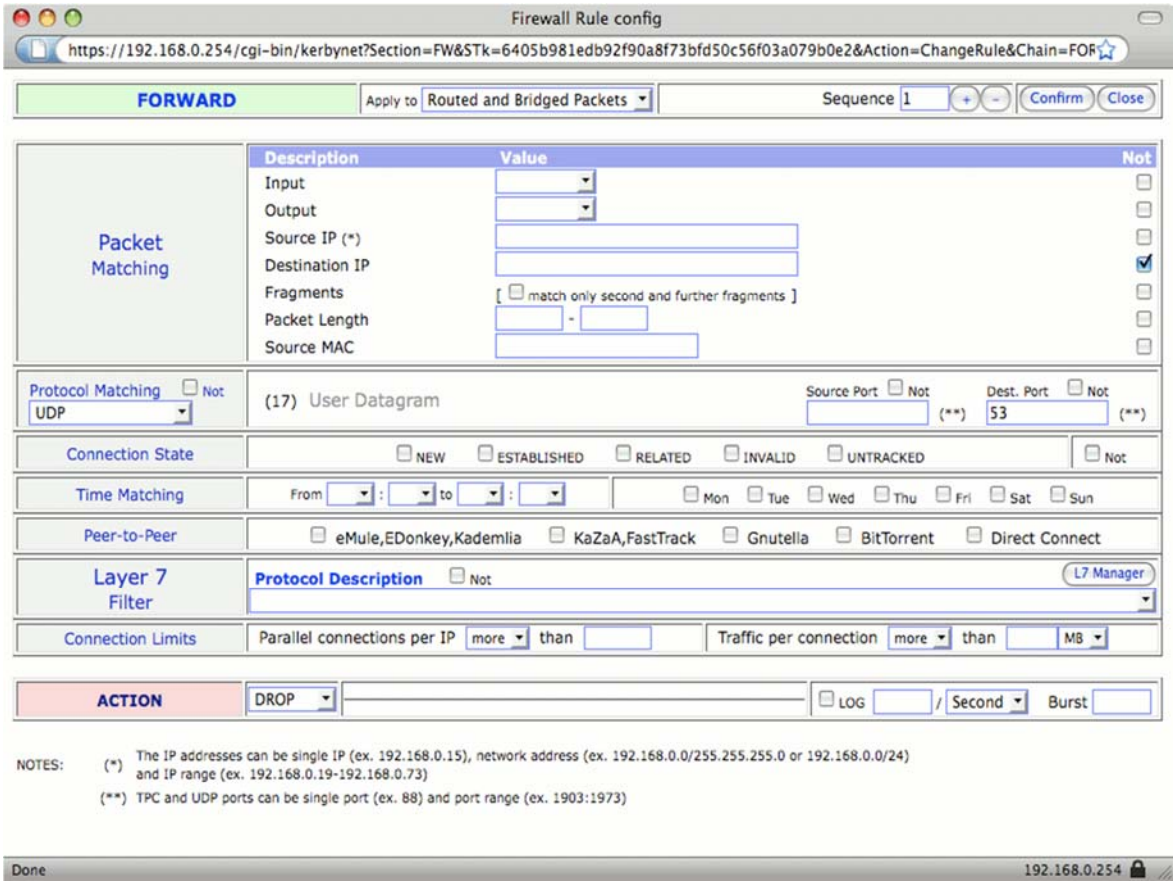


OpenDNS updater untuk menjaga alamat IP dinamis diperbarui dalam database OpenDNS.

ZEROSHELL memiliki klien DNS dinamis kompatibel dengan OpenDNS. Untuk mengaturnya, cukup pilih *OpenDNS* sebagai domain dalam [DNS] [Dynamic DNS] bagian (seperti yang digambarkan di atas), masukkan OpenDNS akun username dan password dan mengaktifkan layanan tersebut.

Pengaturan firewall untuk mencegah penggunaan non OpenDNS DNS

Jika Anda berniat untuk mengaktifkan filter web untuk mencegah akses ke kategori situs tertentu, Anda harus memastikan bahwa satu-satunya DNS klien gunakan adalah ZEROSHELL salah satu yang menggunakan OpenDNS sebagai forwarder. Dengan cara ini, pengguna tidak dapat mengubah DNS klien mereka untuk menghindari pembatasan. Untuk melakukan hal ini, jika ZEROSHELL adalah akses internet gateway default atau jembatan transparan, blok komunikasi ke port 53 UDP / TCP di Firewall.



Pengaturan firewall untuk mencegah penggunaan DNS selain OpenDNS.

Blok ini harus ditetapkan dalam *MAJU* rantai untuk memproses lalu lintas router. Server DNS ZEROSHELL masih dapat menghubungi server OpenDNS karena lalu lintas yang dihasilkan oleh proses lokal tidak dipengaruhi oleh rantai FORWARD.