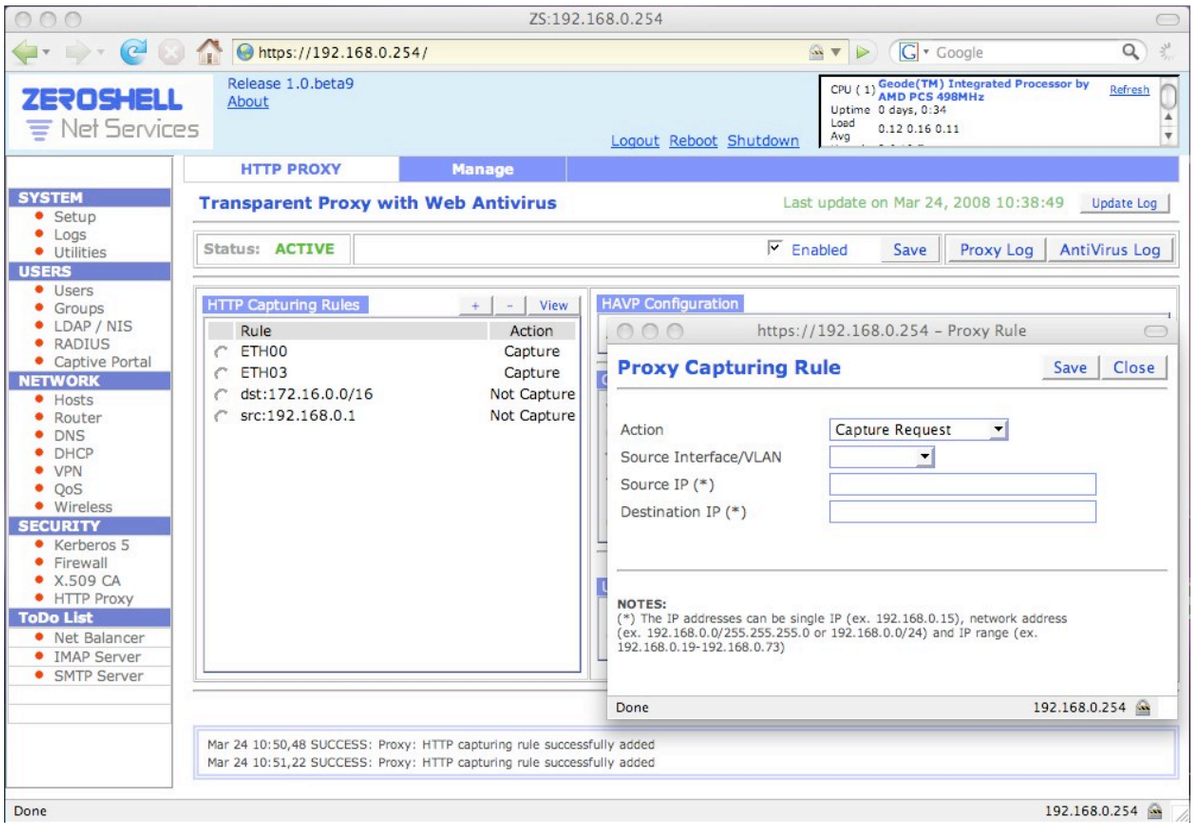
Mengapa menggunakan web proxy yang terintegrasi dengan AntiVirus…???

Halaman web sangat rentang sekali terserang worm dan virus yang tersebar di Internet. Situs Web, baik sengaja atau tidak sengaja dan karena mereka rentang sehingga dapat diubah tanpa sepengetahuan penulis yang sah, kadang-kadang mempunyai referensi script program yang dapat digunakan untuk menginfeksi pengguna komputer. Selain itu, situasi telah memburuk sejak beberapa kerentanan dalam sistem berbasis gambar yang telah memungkinkan virus untuk dieksekusi dalam format file JPEG. Terakhir, meningkatnya penggunaan applet Java adalah meningkatkan jumlah multiplatform virus menyebar melalui http dan operasi terlepas dari platform (PC, Palmtop, ponsel) atau sistem operasi di tempat mereka bekerja. Solusi terbaik untuk jenis masalah ini adalah untuk menyediakan semua perangkat klien yang terhubung ke internet dengan program antivirus yang baik dengan real-time perlindungan, memeriksa setiap file yang masuk. Namun, ini mungkin tidak cukup untuk dua alasan: tidak ada program antivirus, bahkan mereka memiliki mekanisme tanda tangan untuk memperbarui diri, dapat memberikan 100% jaminan terhadap setiap virus; real-time memeriksa konten masuk adalah sangat membebani dalam istilah komputasi dan terutama pada perangkat yang kinerjanya tidak terlalu baik, ia dapat memperlambat sistem sampai membuat pengguna menonaktifkan antivirus secara real-time perlindungan. Untuk alasan ini, virus semakin dilakukan check adalah hulu, sebelum virus potensial dapat menjangkau pengguna klien. Dengan kata lain, sistem antivirus terpusat digunakan pada server-server yang menawarkan layanan tertentu. Contoh yang paling luas adalah bahwa e-mail server, yang memiliki sistem yang menganalisis pesan yang masuk dan keluar melalui SMTP dan lampiran untuk memindai virus. Dalam hal ini, aplikasi antivirus memeriksa gateway SMTP sangat wajar, karena e-mail wajib untuk melewati itu, sebelum mencapai kotak masuk pengguna. Untuk layanan http, ini tidak begitu signifikan, karena klien LAN dapat berpotensi menghubungkan langsung ke salah satu server web yang tersedia di Internet. Solusi untuk masalah ini memperkenalkan aplikasi yang melibatkan tingkat-pintu gerbang ke LAN untuk mengumpulkan http permintaan klien dan maju mereka ke server web yang relevan. Gateway aplikasi ini disebut sebagai Web Proxy dan karena ia mampu menafsirkan protokol http, bukan hanya filter berdasarkan URL, tetapi juga merinci materi yang sedang dilakukan (HTML, JavaScript, Java Applet, gambar, ...) dan untuk scan virus. Salah satu fungsi yang paling umum dari proxy sejauh ini web cache, yaitu pada disk pengarsipan halaman web yang telah dikunjungi, dalam rangka mempercepat menampilkan alamat URL yang sama untuk permintaan pengguna berikutnya. Tujuan dari hal ini juga untuk mengurangi konsumsi bandwidth di Internet dan salah satu yang paling dikenal sistem proxy, mampu melakukan fungsi-fungsi web cache adalah Squid, didistribusikan dengan lisensi Open Source. ZEROSHELL tidak memadukan Squid karena tidak mengumpulkan halaman web. Tugas web yang berfokus pada program antivirus dan filter konten, menggunakan blacklist URL, ditangani oleh HAVP sebagai sistem proxy dan ClamAV sebagai perangkat lunak antivirus. Keduanya didistribusikan di bawah lisensi GPL.

Proxy Mode Transparan

Salah satu masalah terbesar ketika menggunakan server proxy adalah bahwa mengkonfigurasi semua web browser untuk menggunakannya. Oleh karena itu, perlu menetapkan alamat IP atau nama host dan port TCP yang merespon (biasanya port 8080). Hal ini bisa memberatkan dalam kasus LAN dengan banyak pengguna, tapi lebih buruk lagi, mungkin tidak menjamin terhadap pengguna menghapus konfigurasi ini untuk mendapatkan akses langsung ke web, sehingga menghindari antivirus memeriksa, akses penebangan dan blacklist. Untuk mengatasi masalah ini, ZEROSHELL Transparent Proxy menggunakan modus yang melibatkan klien secara otomatis menangkap permintaan pada TCP port 80. Jelas, untuk ZEROSHELL untuk dapat menangkap permintaan web ini, maka harus dikonfigurasi sebagai sebuah gateway jaringan, sehingga lalu lintas internet klien berjalan melewatinya. ZEROSHELL akan secara otomatis mengambil http permintaan apakah ini adalah tingkat 2 gateway (jembatan antara Ethernet, WIFI atau antarmuka VPN) atau lapisan 3 gateway (router). Hal ini tetap penting untuk menentukan di mana antarmuka jaringan atau subnet IP permintaan ini harus diarahkan. Hal ini dilakukan dengan menambahkan apa yang disebut HTTP Menangkap Aturan seperti ditunjukkan pada gambar di bawah ini:

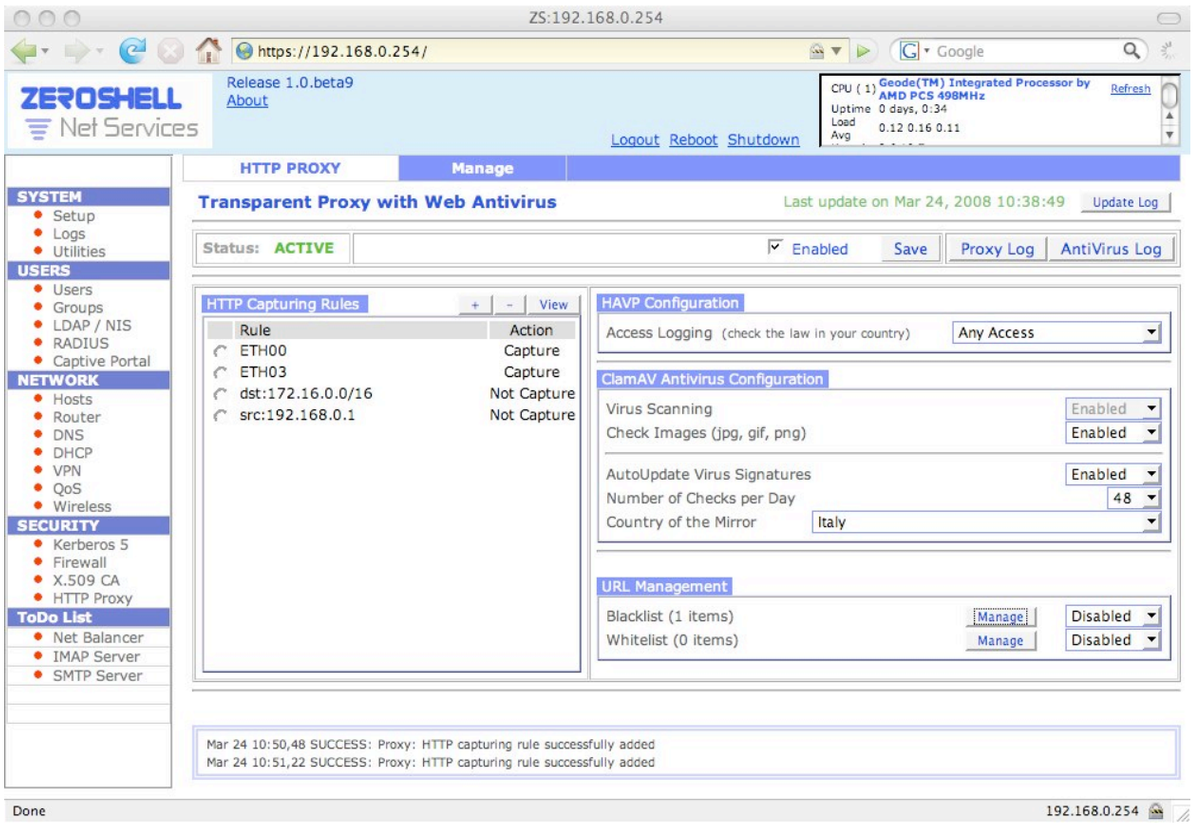


Konfigurasi rule http

Dalam contoh pada gambar diatas, http ETH00 dan permintaan dari antarmuka jaringan ETH03 dicapture. Dikeluarkan dari kunjungan ini adalah mereka yang diarahkan pada server web milik 172.16.0.0/16 IP subnet dan mereka yang berasal dari klien dengan alamat IP 192.168.0.1. Mungkin ada beberapa alasan mengapa perlu untuk mengecualikan intervensi dari transparent proxy pada beberapa klien dan beberapa web server. Sebagai contoh, salah satu server web dapat membatasi akses hanya untuk klien dengan IP tertentu pada ACLs. Dalam kasus ini, jika capturing permintaan proxy di atas server, maka akan dicapai melalui IP-nya dan ini akan mencegah akses. Di sisi lain, hal itu tidak akan dapat diotorisasi alamat IP dari proxy di web server ACLs, karena hal ini akan berarti tanpa pandang bulu memungkinkan akses ke semua klien yang menggunakan proxy. Jelas, kemudian, bahwa satu-satunya solusi adalah menghindari capturing permintaan oleh transparent proxy. Terakhir, perhatikan bahwa aturan iptables untuk mengarahkan ke arah layanan proxy (8080 tcp) ditempatkan di hilir dari campur tangan mereka di Captive Portal. Berkat ini, Captive Portal dan Transparent Proxy dapat diaktifkan secara bersamaan pada antarmuka jaringan yang sama.

Konfigurasi dan Aktivasi Servis Proxy

Seperti diilustrasikan dalam gambar di bawah ini, konfigurasi layanan dari proxy dengan antivirus check adalah sangat sederhana. Setelah mengkonfigurasi mesin ZEROSHELL untuk bertindak sebagai router dan setelah mengkonfigurasi pada klien sebagai default gateway, atau konfigurasi sebagai jembatan dan interposing pada titik di mana LAN arus lalu lintas ke dan dari Internet, cukup aktifkan flag [Enabled] sehingga proxy dapat mulai bekerja. Seperti disebutkan dalam paragraf sebelumnya, web permintaan yang sebenarnya dicegat dan diserahkan ke proxy adalah mereka yang ditentukan melalui konfigurasi [HTTP sesuai aturan].



Konfigurasi proxy melalui interface web

Perhatikan bahwa, *start up* layanan dari proxy sangat lambat dibandingkan dengan layanan lain, dan pada hardware yang tidak terlalu cepat dapat berlangsung hingga 30-40 detik. Hal ini disebabkan oleh kebutuhan **antivirus ClamAV** menscan sejumlah file dalam memori mereka. Untuk mencegah hal ini menghalangi konfigurasi web interface dan *start-up scripts* untuk interval waktu yang panjang, layanan dimulai *asynchronously*. Karena itu, ketika proxy diaktifkan atau mengkonfigurasi ulang, item Status tidak ditampilkan sebagai ACTIVE (hijau) langsung, tapi pertama-tama ketika *STARTING* tandanya (oranye) yang menunjukkan bahwa layanan ini telah memuat *the signature*. Untuk memahami ketika proxy sebenarnya mulai tampil, klik pada [Manage] untuk mereload halaman konfigurasi, atau cukup klik pada [proxy log] untuk melihat havp daemon's start-up pesan. Selama periode awal dari havp daemon, aturan iptables untuk menangkap permintaan http sementara dihapus, lalu lintas Web memungkinkan mengalir secara teratur, tetapi tanpa di scan virus. Beberapa item konfigurasi dianalisis secara lebih rinci dalam paragraf berikut.

Akses Log dan Privasi

Menjadi *application gateway http* mampu menafsirkan permintaan, agar bekerja dengan benar, web proxy decrypts URL yang dikunjungi oleh pengguna. Secara default, ZEROSHELL tidak mengirimkan informasi ini ke log sistem, yang, jika terkait dengan alamat IP klien meminta halaman web, dapat membantu untuk menelusuri konten mengunjungi dari para pengguna. Namun demikian, penebangan informasi ini dapat diaktifkan dengan memodifikasi item [Access Logging] dari "Hanya URL yang mengandung Virus" untuk "Ada Akses". Dengan melakukan ini, setiap URL yang dikunjungi tersebut tercatat dalam log yang terkait dengan alamat IP klien. Hal ini perlu, sebelum mengaktifkan opsi ini, untuk berkonsultasi undang-undang lokal di negara Anda untuk memastikan bahwa penebangan dari URL yang dikunjungi tidak bertentangan dengan hukum privasi nasional. Selain itu, penting untuk menyadari bahwa, seperti memungkinkan NAT di router akses Internet , setiap klien permintaan eksternal dibuat oleh router itu sendiri, dengan cara yang sama permintaan http melewati proxy tampaknya dibuat dari alamat IP dari server proxy. Ini dapat menyebabkan kesulitan dalam menelusuri identitas pengguna yang telah melakukan tindakan ilegal pada remote server. Sebuah solusi untuk masalah ini, yang kurang invasif dalam istilah privasi, bisa untuk mengaktifkan penebangan dari Connection Tracking (dari antarmuka web ZEROSHELL [Firewall] [Connection Pelacakan]). Dengan cara

ini, TCP / UDP koneksi tercatat dalam log yang menunjukkan sumber IP, port sumber, IP tujuan dan port tujuan. Oleh karena itu, tidak akan mungkin untuk melacak aktivitas pengguna konten, namun jejak akan disimpan koneksi dibuat. Sekali lagi, dalam kasus ini adalah perlu untuk berkonsultasi dengan undang-undang setempat sebelum sambungan memungkinkan pelacakan.

Antivirus mengecek tiap File Gambar

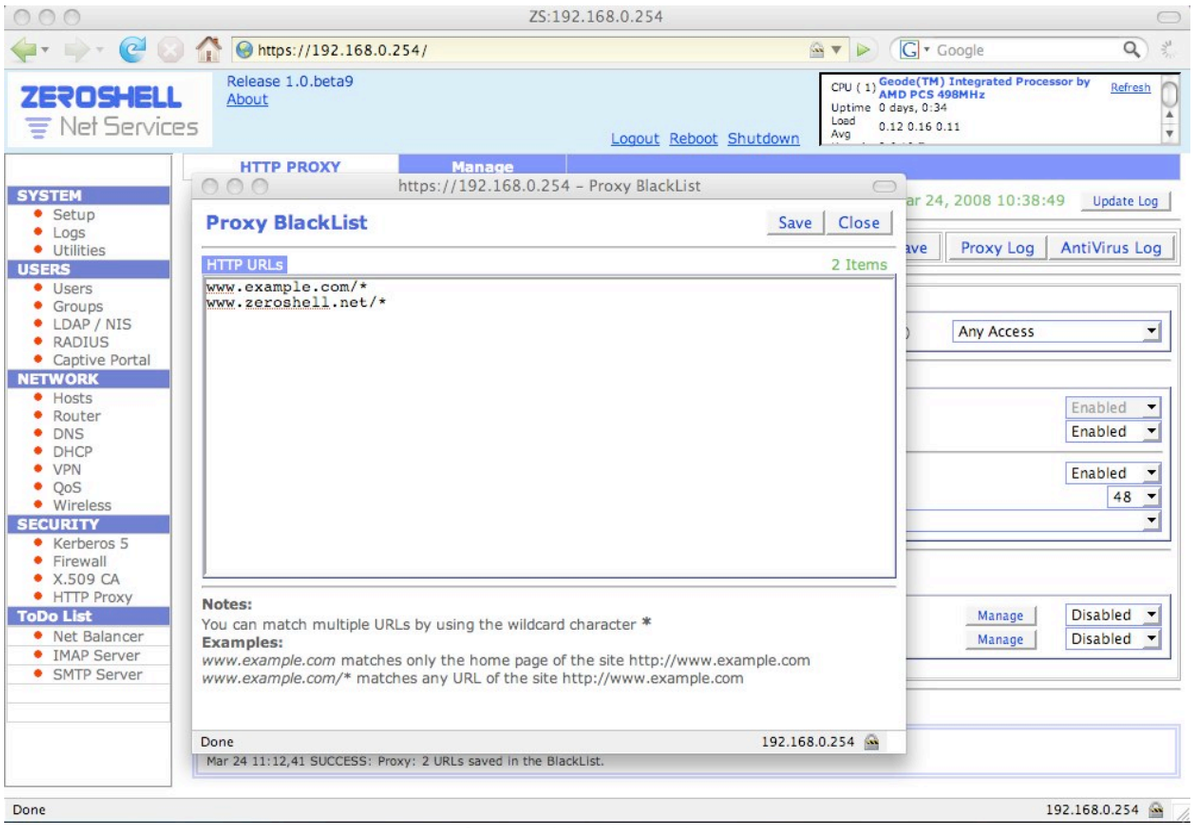
Untuk waktu yang lama itu mengira bahwa file yang berisi gambar JPEG atau GIF tidak bisa mengandung virus, karena hanya terdiri atas data diformat dalam format yang telah ditetapkan, ditafsirkan oleh sistem melihat sistem operasi. Baru-baru ini, beberapa komponen rendering gambar telah menunjukkan bahwa mereka rentan jika mereka tidak diperbarui dengan tambalan. Sebuah gambar yang dibangun sesuai dapat menciptakan sebuah *Buffer overrun* dan menjalankan kode **arbitrer** pada sistem. Sangat mudah untuk memahami keseriusan ini, mengingat sebagian besar konten hypertext di WWW dalam bentuk gambar. HAVP proxy yang dikonfigurasi di ZEROSHELL, secara default gambar di scan menggunakan program antivirus ClamAV. Namun demikian, pada hardware lambat, scanning gambar bisa menunda pembukaan halaman web dengan banyak gambar. Dalam hal ini mungkin untuk menonaktifkan pemindaian file berisi gambar, dengan mengatur [Periksa Images (jpg, gif, png)] pilihan dari "Diaktifkan" ke "Disabled"

Otomatis update of ClamAV

Kecepatan dari virus baru diletakkan di internet dan diidentifikasi, bertanda antivirus meningkat dan sering dimodifikasi. Pada database ClamAV ada pengecualian, berkat freshclam daemon, bisa diupdate online kapan saja secara teratur. ZEROSHELL mengkonfigurasi freshclam secara default untuk memeriksa database terbarunya sebanyak 12 kali dalam sehari. Interval ini dapat diatur menggunakan [Jumlah Cek per Hari] parameter, dari minimal 1 sampai maksimal 48 cek per hari. Hal ini juga penting untuk mengatur [*Country of the Mirror*] dengan benar, melalui mana freshclam memilih situs yang terdekat untuk men-download virus database. Namun, perlu diketahui bahwa update secara teratur adalah operasi cepat yang tidak menghasilkan banyak lalu lintas, karena sistem update diferensial digunakan.

Daftar webstite blacklist dan whitelist

Hal ini sering diperlukan untuk memblokir menampilkan sejumlah situs web karena konten mereka dianggap tidak cocok untuk para pengguna layanan web. Contohnya adalah orang dewasa-hanya materi, yang tidak boleh ditampilkan pada komputer untuk anak-anak yang memiliki akses. Salah satu solusi yang sangat efektif untuk masalah ini adalah web memaksa klien untuk mengakses internet melalui proxy, yang melalui perangkat lunak *Content Filtering* seperti **DansGuardian**, memeriksa isi dari halaman *html* memblokir mereka yang diduga milik kategori yang tidak diinginkan. Mekanisme filter ini dapat dibandingkan dengan sistem *antispamming*. Sayangnya, tidak jelas apakah lisensi rilis **DansGuardian** kompatibel untuk integrasi dalam suatu sistem seperti ZEROSHELL dan, karenanya, tidak digunakan demi menghindari risiko pelanggaran lisensi. Pada saat ini, satu-satunya cara untuk memblokir atau memungkinkan tampilan halaman web adalah daftar hitam dan membolehkan akses halaman web seperti yang ditunjukkan pada gambar.



Konfigurasi blacklist web proxy

Whitelists dan blacklist terdiri dari rangkaian URL yang diatur pada baris yang berbeda. Setiap baris dapat berhubungan dengan beberapa halaman web ketika karakter * yang digunakan. Untuk memblokir situs tempat http://www.example.com, www.example.com/* pada di *blacklist*, sedangkan garis www.example.com, tanpa *, hanya akan memblokir halaman home dari situs tersebut. Situs yang terdapat di daftar *whitelist* lebih diprioritaskan ketimbang situs yang terdaftar di *Blacklist*. Dengan kata lain, jika halaman Web yang sesuai dengan item pada daftar *blacklist* dan pada saat yang sama ditemukan pada daftar *whitelist*, maka akses diperbolehkan ke halaman web tersebut. Selain itu, perhatikan bahwa tujuan dari *whitelist* tidak hanya memberikan akses ke halaman yang seharusnya dapat dilarang oleh daftar *blacklist*, tetapi juga untuk mem-bypass antivirus memeriksa. Harap mencatat dengan cermat tentang hal ini. Jika administrator LAN ingin mengadopsi kebijakan menyediakan akses ke sejumlah situs / ia dapat menentukan * / * baris dalam daftar hitam, yang akan mencegah akses ke semua halaman kecuali yang termasuk pada daftar putih.

Pengujian proxy dan fungsi antivirus

Pada dasarnya ada dua alasan mengapa proxy biasanya tidak bekerja dengan semestinya. Pertama-tama, kita perlu memastikan apakah mesin ZEROSHELL dikonfigurasi sebagai router atau *bridge*, dan juga bahwa lalu lintas *ke* dan *dari* internet benar-benar berjalan melewatinya. Kedua, Anda harus yakin konfigurasi yang benar dari [HTTP sudah sesuai dengan Aturan], yang menentukan permintaan http benar-benar diarahkan terhadap proses proxy (havp mendengarkan di 127.0.0.1:8080). Secara khusus, jika menangkap *http request* dikenakan pada antarmuka jaringan yang merupakan bagian dari sebuah bridge (jembatan), Anda harus yakin bahwa setidaknya satu alamat IP Anda telah didefinisikan. Cara termudah untuk mengecek apakah proxy bekerja dengan benar adalah untuk memungkinkan penebangan sementara semua akses dan menampilkan log proxy setelah meminta halaman web dari klien. Setelah yakin bahwa web proxy menangkap permintaan seperti yang diharapkan, pastikan perangkat lunak antivirus ClamAV bekerja dengan benar. Untuk melakukan ini, pertama-tama periksa log **freshclam** apakah telah di set untuk diperbarui secara teratur. Lalu, ke URL http://www.eicar.org/anti_virus_test_file.htm untuk memeriksa apakah EICAR-AV-Test pengujian virus (kata tidak berbahaya oleh penulis) yang ditangkap dan diblokir. Terakhir, perhatikan bahwa proxy tidak dapat melayani permintaan https (http dienkripsi dengan SSL / TLS) yang diberikan itu, tidak memiliki kunci pribadi server web, tidak dapat mendekripsi konten dan URL permintaan ini dikemas dalam terowongan dienkripsi.