Miniguida su come consentire solo specifiche porte su Zeroshell

Nota: non raccomando l'uso di questo metodo per controllare l'accesso alle risorse di Internet da parte degli utenti della vostra LAN. Un utente un po' più furbo della media potrebbe configurare infatti un server VPN o SSH che risponda su una delle porte lasciate aperte, eludendo così il blocco. Allo stesso modo, alcuni software come Skype e TeamViewer sono progettati per tentare di superare gli eventuali firewall e quindi nel caso la loro porta specifica sia bloccata comunicano sulla porta 80 o 443, ignorando nuovamente le restrizioni che avete impostato.
Inoltre le regole potrebbero causare problemi per alcuni usi: ad esempio, se consentite solo le canoniche 80, 8080, 25, 110, 53 e qualcuno dovrà scaricare un file via FTP (porta 21), non potrà farlo. Idem se qualche programma usa una porta non-standard.

Detto questo, passiamo alla configurazione.

La rete di test che ho creato per questa miniguida è siffatta:

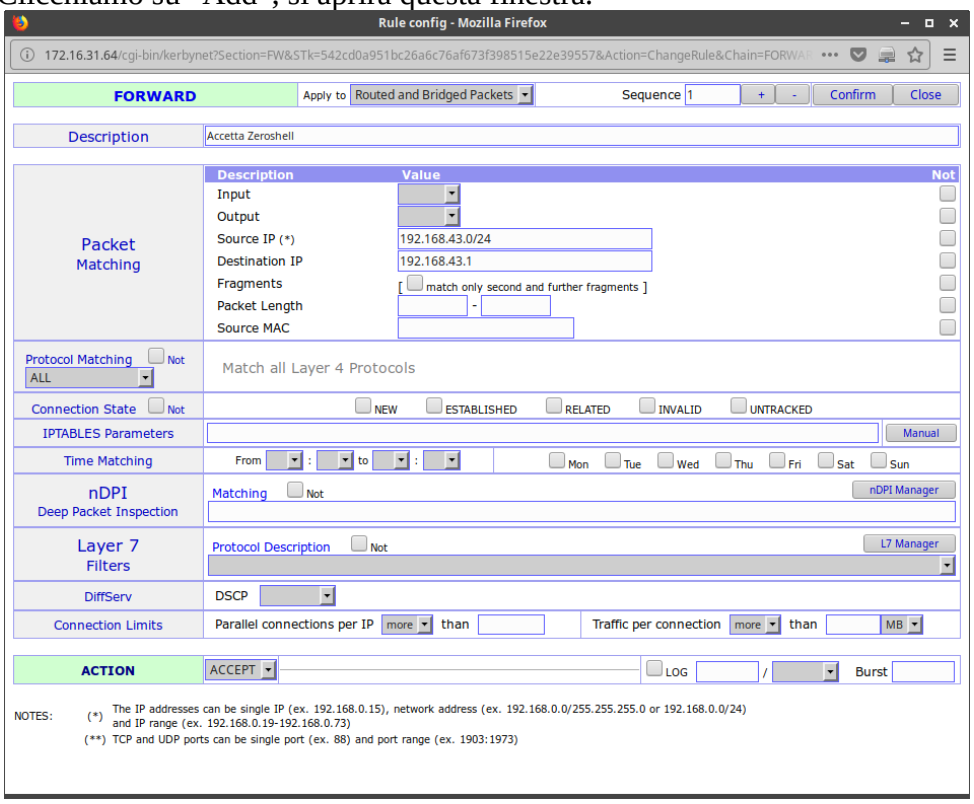
- Zeroshell fa da router, server DHCP e firewall e ha due schede di rete
- La scheda N°1 (eth00) è collegata ad un altro router e ottiene l'indirizzo via DHCP
- La scheda N°2 (eth01) ha come indirizzo 192.168.43.1/24
- La LAN che vogliamo filtrare è quindi 192.168.43.0/24

Tralascio la descrizione di come impostare la funzione di router e server DHCP in quanto ci sono già ottime guide sul web per configurarli :-)

Nella pagina "Firewall" **NON tocchiamo la "policy" mettendola su "DROP"** come verrebbe intuitivo fare! In questo modo ci si chiude fuori da Zeroshell (serve accedere fisicamente alla macchina e riavviare in failsafe mode)!

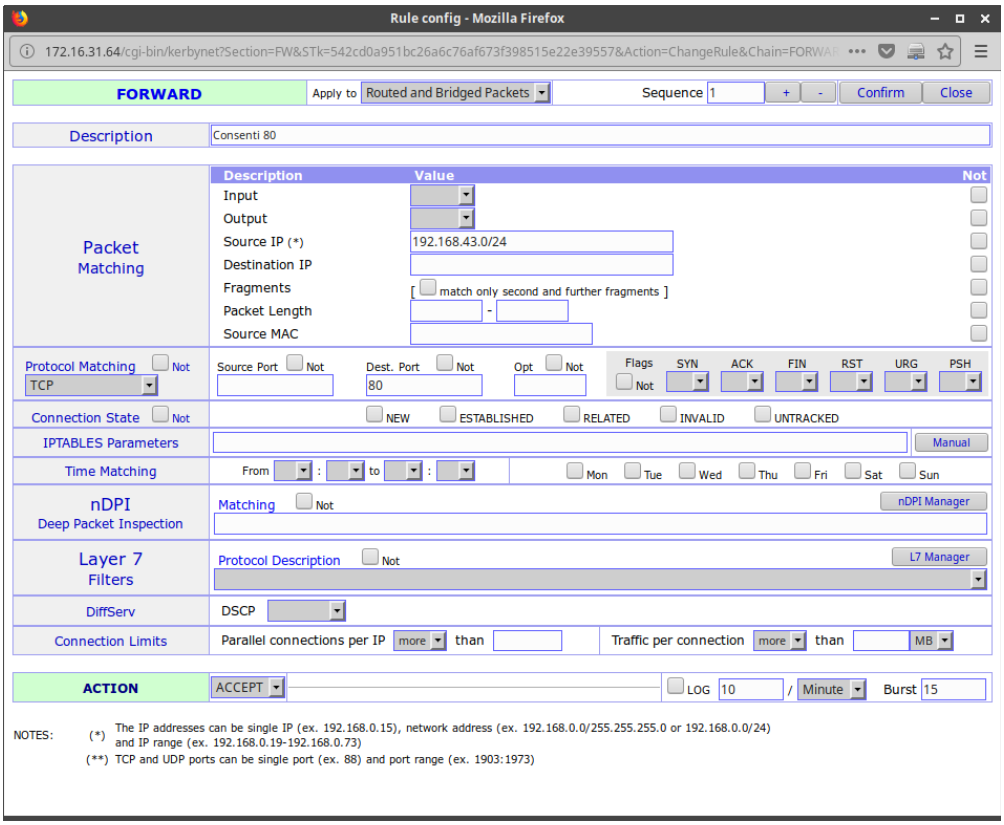
Supponiamo di voler consentire solo le porte 80, 443 e 53 (benvenuti nel 1984 ;-)). L'operazione è semplicissima.

Prima di tutto dobbiamo consentire l'accesso dalla LAN a Zeroshell, altrimenti ci chiudiamo fuori. Clicchiamo su "Add", si aprirà questa finestra.



- In “**Description**” mettete qualcosa che vi aiuti a capire la regola :-)
- In “**Source IP**” mettete la subnet della vostra LAN (qui **192.168.43.0/24**)
- In “**Destination IP**” mettete l’IP di Zeroshell (qui **192.168.43.1**)
- In “**Action**” impostate **ACCEPT.**

Passiamo ora alla configurazione delle regole vere e proprie. Fate nuovamente clic su Add:



- In “**Description**” mettete qualcosa che vi aiuti a capire la regola :-)
- In “**Source IP**” mettete la subnet della vostra LAN (qui **192.168.43.0/24**)
- In “**Protocol Matching**” selezionate **TCP** e impostate la porta che desiderate consentire nel campo **Dest. Port** (si può usare una porta singola tipo 80 oppure un range di porte come 1000:1200 ma NON tutti e due)
- Aggiungere, volendo, dei parametri di orario in “**Time Matching**”
- In “**Action**” impostate **ACCEPT.**

Aggiungete altre regole identiche per consentire ulteriori porte.
Allo stesso modo, per consentire le porte **UDP**, aggiungete regole identiche ma selezionate “**UDP**” in “**Protocol Matching**” anziché **TCP.**

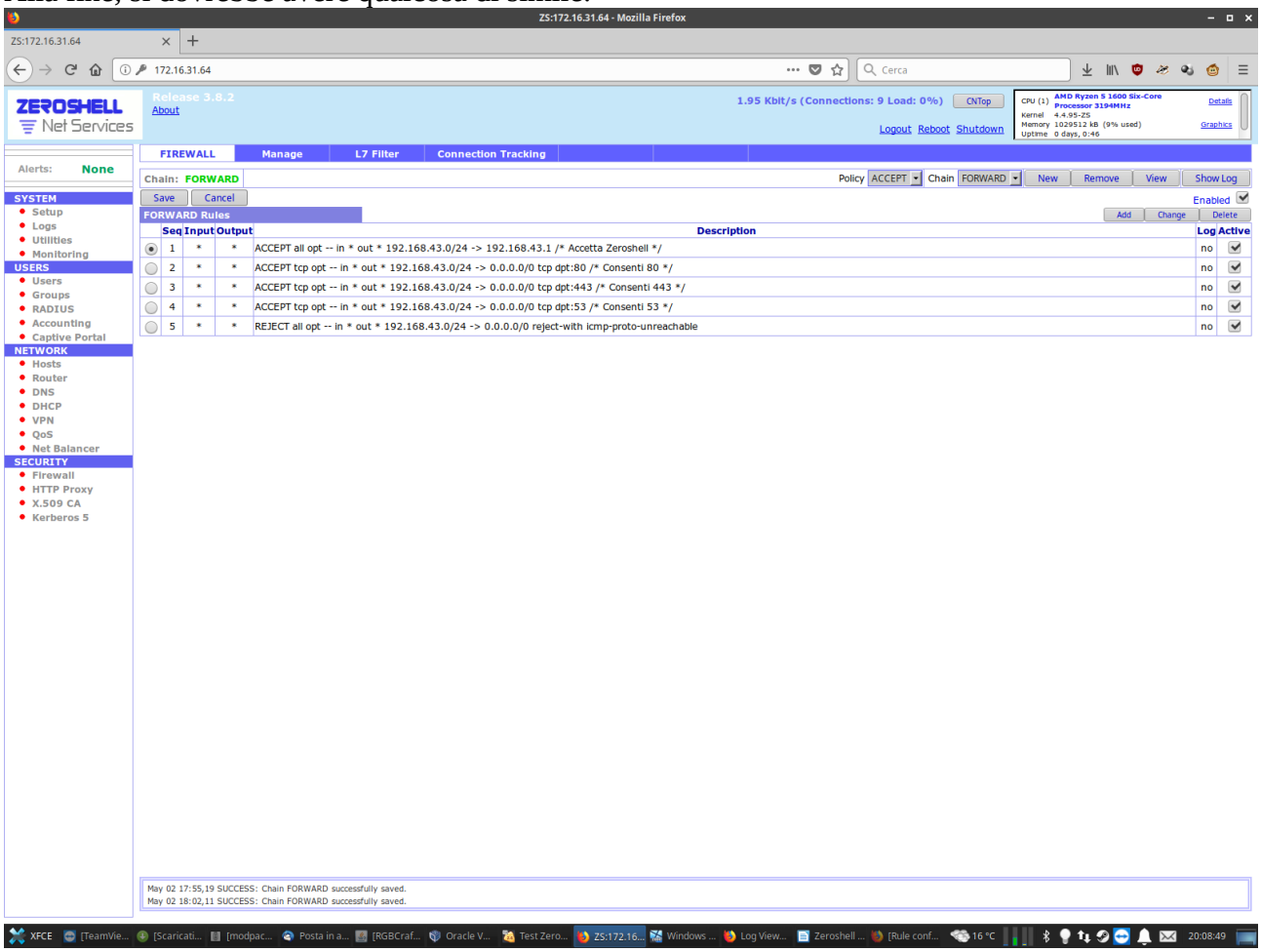
A questo punto, dopo aver aggiunto tutte le regole che consentono l’accesso alle porte autorizzate, configuriamo una regola generale che blocchi tutto ciò che non rientra nelle regole precedenti.

Facciamo nuovamente clic su “Add”.

- In “**Source IP**” mettete la subnet della vostra LAN (qui **192.168.43.0/24**)
- In “**Action**” impostate **DROP** o **REJECT**. Consiglio di impostare **REJECT.** Il motivo di questa scelta è spiegato in quest’ottimo articolo: https://www.achab.it/achab.cfm/it/blog/achablog/drop-vs-reject-qual-e-la-differenza

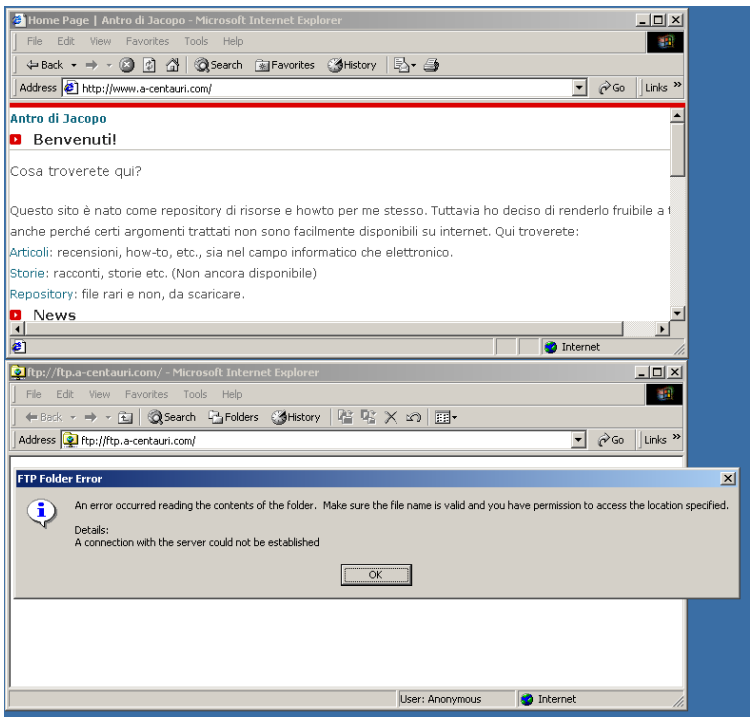
Potete anche spuntare la casella “**LOG**” che registrerà tutti gli utenti che tentano di forzare il firewall.

Alla fine, si dovrebbe avere qualcosa di simile:



A questo punto fate clic su **“Save”** e controllate che tutto funzioni. Se per caso vi siete chiusi fuori da Zeroshell, accedete fisicamente alla macchina e premete il tasto Z (fail-safe mode).

Ed ecco qui il risultato: la macchina collegata alla LAN riesce a navigare in Internet perché le porte 80, 53 e 443 sono aperte, ma non riesce ad accedere al server FTP perché la 21 è chiusa.



Tutto qui :-)