

Miniguia 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 miniguia 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.

The screenshot shows the 'Rule config' window in Mozilla Firefox. The rule is named 'Accetta Zeroshell' and is set to 'FORWARD' with 'Apply to Routed and Bridged Packets'. The 'Sequence' is 1. The 'Description' is 'Accetta Zeroshell'. The 'Packet Matching' section is expanded, showing the following configuration:

Description	Value	Not
Input		<input type="checkbox"/>
Output		<input type="checkbox"/>
Source IP (*)	192.168.43.0/24	<input type="checkbox"/>
Destination IP	192.168.43.1	<input type="checkbox"/>
Fragments	<input type="checkbox"/> match only second and further fragments]	<input type="checkbox"/>
Packet Length	-	<input type="checkbox"/>
Source MAC		<input type="checkbox"/>

The 'Protocol Matching' section is set to 'ALL' and 'Match all Layer 4 Protocols'. The 'Connection State' section is set to 'NEW', 'ESTABLISHED', 'RELATED', 'INVALID', and 'UNTRACKED'. The 'Time Matching' section is set to 'From' and 'to' with 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat', and 'Sun' options. The 'nDPI' section is set to 'Matching' and 'Deep Packet Inspection'. The 'Layer 7 Filters' section is set to 'Protocol Description' and 'L7 Manager'. The 'DiffServ' section is set to 'DSCP'. The 'Connection Limits' section is set to 'Parallel connections per IP' and 'Traffic per connection'. The 'ACTION' section is set to 'ACCEPT' and 'LOG'.

NOTES: (*) The IP addresses can be single IP (ex. 192.168.0.15), network address (ex. 192.168.0.0/255.255.0 or 192.168.0.0/24) and IP range (ex. 192.168.0.19-192.168.0.73)
(**) TCP and UDP ports can be single port (ex. 88) and port range (ex. 1903:1973)

- 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:

The screenshot shows the 'Rule config' window in Mozilla Firefox. The rule is named 'Consenti 80' and is applied to 'Routed and Bridged Packets' with sequence number 1. The description is 'Consenti 80'. Under 'Packet Matching', 'Source IP (*)' is set to '192.168.43.0/24'. Under 'Protocol Matching', 'TCP' is selected and 'Dest. Port' is set to '80'. The 'Action' is set to 'ACCEPT'. There are also fields for 'LOG', 'Minute', and 'Burst'.

- 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:

Seq	Input	Output	Description	Log	Active
1	*	*	ACCEPT all opt -- in * out * 192.168.43.0/24 -> 192.168.43.1 /* Accetta Zeroshell */	no	<input checked="" type="checkbox"/>
2	*	*	ACCEPT tcp opt -- in * out * 192.168.43.0/24 -> 0.0.0.0/0 tcp dpt:80 /* Consenti 80 */	no	<input checked="" type="checkbox"/>
3	*	*	ACCEPT tcp opt -- in * out * 192.168.43.0/24 -> 0.0.0.0/0 tcp dpt:443 /* Consenti 443 */	no	<input checked="" type="checkbox"/>
4	*	*	ACCEPT tcp opt -- in * out * 192.168.43.0/24 -> 0.0.0.0/0 tcp dpt:53 /* Consenti 53 */	no	<input checked="" type="checkbox"/>
5	*	*	REJECT all opt -- in * out * 192.168.43.0/24 -> 0.0.0.0/0 reject-with icmp-proto-unreachable	no	<input checked="" type="checkbox"/>

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 :-)