

Climenole's rules set Version 3 - Introduction

One of the most frequent question about rules set firewall is: "Where I put that rule in the list?" I'll try to find a solution by adding to each rule name a code giving the relative position of the rule in the list.

| | | | | | |
|--|--|--|--|--|--|
| | | | | | {B. 01}; [ALL] << Invalid IP ! > |
| | | | | | {B. 02}; [ALL] << Invalid IP ! > |
| | | | | | {B. 03}; [ALL] << Non-routable IP ! > |
| | | | | | {B. 04}; [ALL] << Non-routable IP ! > |
| | | | | | {B. 05}; [ALL] << Non-routable IP ! > |
| | | | | | {B. 06}; [ALL] << Non-routable IP ! > |
| | | | | | {B. 07}; [ALL] << Non-routable IP ! > |
| | | | | | {B. 08}; [ALL] << Multicast IP ! > |
| | | | | | {B. 09}; [ALL] << Reserved IP ! > |
| | | | | | {C. 01}; [ICMP] << Fragmented ! > |
| | | | | | {C. 02}; [ICMP] << + Fragments ! > |
| | | | | | {C. 03}; [ICMP] { Request } |
| | | | | | {C. 04}; [ICMP] { Reply } |
| | | | | | {C. 05}; [ICMP] { Trace route } |
| | | | | | {C. 33}; [ICMP] < Port Unreachable ! >> |
| | | | | | {C. 80}; [ICMP] << Ping Scan ! > |
| | | | | | {C. 310}; [ICMP] << Host - Communication Forbidden ! > |
| | | | | | {C. 313}; [ICMP] << Filtering - Comm. Forbidden ! > |
| | | | | | {C. 999}; [ICMP] << Icmp Lock ! >> |
| | | | | | {E. 01}; [T/U] << Src Port 0 Invalid ! > |
| | | | | | {E. 02}; [T/U] << Dst Port 0 Invalid ! > |
| | | | | | {E. 03}; [T/U] << Fragmented ! > |
| | | | | | {E. 04}; [T/U] << + Fragments ! > |
| | | | | | {G. 53.01}; [UDP] { Names Resolution } |
| | | | | | {H. 01}; [TCP] << SRC & DST = @IP ! >> |
| | | | | | {H. 02}; [TCP] << NULL ! > |
| | | | | | {H. 03}; [TCP] << FULL ! > |
| | | | | | {H. 04}; [TCP] << FIN & 15 Variants ! > |
| | | | | | {H. 05}; [TCP] << SYN RST & 4 Variants ! > |
| | | | | | {H. 06}; [TCP] << SYN PSH & 2 Variants ! > |
| | | | | | {H. 07}; [TCP] << SYN URG ! > |

The general syntax for the rule name will be easy to understand with this example of a basic rule:

Name of the rule:

{R. 80,01}; [TCP] { HTTP }

Description of the rule:

[S/optional: else {S..0000000} or G]

[Hyper Text Transfer Protocol]

Firefox, Opera, IE

The "*{R. 80,01}*" means: a rule in the rules subset R , remote port 80, one remote port only.

The "*; [TCP] { HTTP }*" means : a rule using TCP protocol (The "Transport layer of the TCP-IP protocols) and using the port related to the HTTP (the "Application level layer" of the tcp-IP protocols).

The description: "*[S/optional: else {S..0000000} or G]*" means : this is a specific rule (one program must be included at least in this rule otherwise the more general rule {S..0000000} will be used instead.

The "**or G**" means: you may leave it as a general rule anyway... [This will be more clear later...]

There is an **other coded indication in the rule name**:

{{ rule name }} means: packets authorised in and out for general rule
{ rule name } means : packets authorised in and out for specific rule
{{ rule name } } means : packets authorised incoming only
{ rule name }} means: packets authorised outgoing only
{ * rule name } means: packets authorised in and out for a Server rule

<< rule name ! >> means: packets blocked in and out
<< rule name ! > means packets blocked incoming only
< rule name ! >> means : packets blocked outgoing only

In the rule description there is also some codes:

G = general rule or for any program

S = specific rule: at least one program must be listed in that rule
(this is mandatory for server rules and Udp rules ...)[Exception: the DNS rule...]

S/C means Specific rule and must be configured: most of the time the port used in the rule must be configured also in the program like utorrent for example.

u+e = if needed, this rule must be unblocked (remove the red dot) and enable (check the first column...)

experimental = self obvious. This rule was not fully tested and may require some fixes...

recommended: not a mandatory rule but it's better to have it.

mandatory: you must have this rule!

optionnal: mostly for TCP applications.

Normally TCP application used the general rule “*{S..0000000}; [TCP] {{ Common Internet Applications }}*” and you don't need more. Used these rules if you want it.

testing: some rules are created for testing or learning.

This is for “Geek” fun !!! Mostly about the TCP flags used in connections.

See rules {S. 0}; [TCP] {{ ACK }} to {S. 7}; [TCP] {{ RST }}.

Needed: rule for a server or for Udp protocol. The rule must be specific!!!

That's all for now. The *next articles* will explained the rules for each *rule's subsets* and give you some hints about the Internet packets filtering and the methodology used to create a “*well built*” rules set. **In subsequent articles** I will give you a more accurate details about routers and LAN configuration rules. Finally I will finished with an *UNofficial Frequently Asked Questions* for Look'n'Stop and firewalls in general ...

Stay tunes for the next articles !