

IPTables basics

An IPTables based firewall is made of three different basic “objects”.

1. Rules
2. Chains
3. Tables

Please read through the next three chapters to get a short description about those objects. Note that this is just a briefly introduction to the IPTables. For more detailed documentation have a look at the IPTables Manpage or www.iptables.org.

Rules

The lowest level objects are the ‘rules’ that are performing the packet filtering or manipulation. A rule is made of several parts.

The Table to which this rule should be added. If no table is defined the rule will be added to the “filter” table.

The Chain to which this rule should be added. (i.e. INPUT or FORWARD)

The filtering or manipulation instructions.

The target of the rule. This target decides what should be done with the packet if it matches the rule. The most important targets are “DROP”, which drops the packet without any further action, “ACCEPT”, which will let the packet pass the firewall and the data is sent to the receiver and “LOG” that simply writes some information (src. IP, ports etc.) about the packet that matches to the Syslog.

Chains

Those rules are organized in ‘chains’ which are simple ordered list of rules. There are some built-in chains that are always available for the user like the INPUT or the OUTPUT chain in the filter table. Built-in chains do also have a so called ‘Default Target’ which decides what to do with a packet that didn't match any of the rules defined in that chain.

For large configurations it's often required to setup rules for packets that are common in some pieces of their attributes. When you setup a firewall that also provides routing functionality you may want to have different kind of rules for packets coming from the internal network than for packets coming from the evil Internet.

To make it easier to manage such configurations you have the possibility to create your own chains. Those user defined chains don't have a ‘Default Target’.

User defined chains must be fed by rules that have the name of the user defined chain as their target. When a packet passes the whole user defined chain without matching any of its rules the

packet will be sent back to the chain that fed this chain just right after the rule that sent the packet to the user defined chain.

The packets will be compared to the rules in the order as they are defined in the chain. This means that the packet will no longer be tested if a rule before matched. So please pay attention to the order of the rules as a wrong rule order may end up in an very hard to find bug in the configuration.

Tables

Because of the lots of possibilities that IPTables rules give you to filter and/or manipulate the packets that are checked the chains themselves are organized in so called 'tables'. Each table has its own set of built-in chains that are available for direct use.

There are three tables available: 'filter', 'nat' and 'mangle'.

1. The "filter" table that is used for packet filtering as we all think about when we are talking about firewalls
2. The "nat" table is made for all kind of "Network Address Translation" which is a technology used to change the source and destination attributes of the packet. The well known "IP Masquerading" is the most common way to use this feature.
3. The "mangle" table is designed to hold chains and rules that change other attributes of the packets or sending them into the user space to be processed by any other application. If you are not thinking about really complicated things you shouldn't need to use this table.

Information Source: (12/10/2003)

http://kmyfirewall.sourceforge.net/kmf_doc/iptables-concept.html