Iptables - Traversing of tables and chains!

Πίνακας περιεχομένων

1. General

When a packet first enters the firewall, it hits the hardware and then gets passed on to the proper device driver in the kernel.

Then the packet starts to go through a series of steps in the kernel, before it is either sent to the correct application (locally), or forwarded to another host - or whatever happens to it.

2. Destination local host (our own machine)

Table 1. Destination local host

Step	Table	Chain	Comment
1			On the wire (e.g., Internet)
2			Comes in on the interface (e.g., eth0)
3	raw	PREROUTING	This chain is used to handle packets before the connection tracking takes place. It can be used to set a specific connection not to be handled by the connection tracking code for example.
4			This is when the connection tracking code takes place

5	mangle	PREROUTING	This chain is normally used for mangling packets, i.e., changing TOS and so on.
6	nat	PREROUTING	This chain is used for DNAT mainly. Avoid filtering in this chain since it will be bypassed in certain cases.
7			Routing decision, i.e., is the packet destined for our local host or to be forwarded and where.
8	mangle	INPUT	At this point, the mangle INPUT chain is hit. We use this chain to mangle packets, after they have been routed, but before they are actually sent to the process on the machine.
9	filter	INPUT	This is where we do filtering for all incoming traffic destined for our local host. Note that all incoming packets destined for this host pass through this chain, no matter what interface or in which direction they came from.
10			Local process or application (i.e., server or client program).

3. Source local host (our own machine)

Table 2. Source local host

Step	Table	Chain	Comment

1			Local process/application (i.e., server/client program)
2			Routing decision. What source address to use, what outgoing interface to use, and other necessary information that needs to be gathered.
3	raw	OUTPUT	This is where you do work before the connection tracking has taken place for locally generated packets. You can mark connections so that they will not be tracked for example.
4			This is where the connection tracking takes place for locally generated packets, for example state changes et cetera.
5	mangle	OUTPUT	This is where we mangle packets, it is suggested that you do not filter in this chain since it can have side effects.
6	nat	OUTPUT	This chain can be used to NAT outgoing packets from the firewall itself.
7			Routing decision, since the previous mangle and nat changes may have changed how the packet should be routed.
8	filter	OUTPUT	This is where we filter packets going out from the local host.

9	mangle	POSTROUTING	The POSTROUTING chain in the mangle table is mainly used when we want to do mangling on packets before they leave our host, but after the actual routing decisions. This chain will be hit by both packets just traversing the firewall, as well as packets created by the firewall itself.
10	nat	POSTROUTING	This is where we do SNAT as described earlier. It is suggested that you don’t do filtering here since it can have side effects, and certain packets might slip through even though you set a default policy of DROP.
11			Goes out on some interface (e.g., eth0)
12			On the wire (e.g., Internet)

4. Forwarded packets

In this example, we’re assuming that the packet is destined for another host on another network. The packet goes through the different steps in the following fashion:

Table 3. Forwarded packets

Step	Table	Chain	Comment
1			On the wire (i.e., Internet)
2			Comes in on the interface (i.e., eth0)

3	raw	PREROUTING	Here you can set a connection to not be handled by the connection tracking system.
4			This is where the non-locally generated connection tracking takes place.
5	mangle	PREROUTING	This chain is normally used for mangling packets, i.e., changing TOS and so on.
6	nat	PREROUTING	This chain is used for DNAT mainly. SNAT is done further on. Avoid filtering in this chain since it will be bypassed in certain cases.
7			Routing decision, i.e., is the packet destined for our local host or to be forwarded and where.
8	mangle	FORWARD	The packet is then sent on to the FORWARD chain of the mangle table. This can be used for very specific needs, where we want to mangle the packets after the initial routing decision, but before the last routing decision made just before the packet is sent out.

9	filter	FORWARD	The packet gets routed onto the FORWARD chain. Only forwarded packets go through here, and here we do all the filtering. Note that all traffic that’s forwarded goes through here (not only in one direction), so you need to think about it when writing your rule-set.
10	mangle	POSTROUTING	This chain is used for specific types of packet mangling that we wish to take place after all kinds of routing decisions have been done, but still on this machine.
11	nat	POSTROUTING	This chain should first and foremost be used for SNAT. Avoid doing filtering here, since certain packets might pass this chain without ever hitting it. This is also where Masquerading is done.
12			Goes out on the outgoing interface (i.e., eth1).
13			Out on the wire again (i.e., LAN).

ℹ *Reminder*

Caminante, no hay camino,
se hace camino al andar.

Wanderer, there is no path,
the path is made by walking.

Antonio Machado Campos de Castilla