An iptables policy is built from an ordered set of rules, describe to the kernel the actions, should be taken against certain classes of packets

Each iptables rule is applied to a chain within a table

iptables chain is a Care and Feeding of iptables 11 collection of rules that are compared, in order, against packets that share a common characteristic (such as being routed to the Linux system, as opposed to away from it)

Tables- iptable construct, mô tả các chức năng

vd: packet filtering or Network Address Translation (NAT)

- có 4 bảng:

+ filter, nat, mangle, and raw

- Filtering rules are applied to the filter table, NAT rules are applied to the nat table

- specialized rules that alter packet data are applied to the mangle table

- rules that should function independently of the Netfilter connection-tracking subsystem are applied to the raw table.

Chains- Each table has its own set of built-in chains

- user-defined chains can also be created => user can build a set of rules that is related by a common tag such as INPUT\_ESTABLISHED or DMZ\_NETWORK

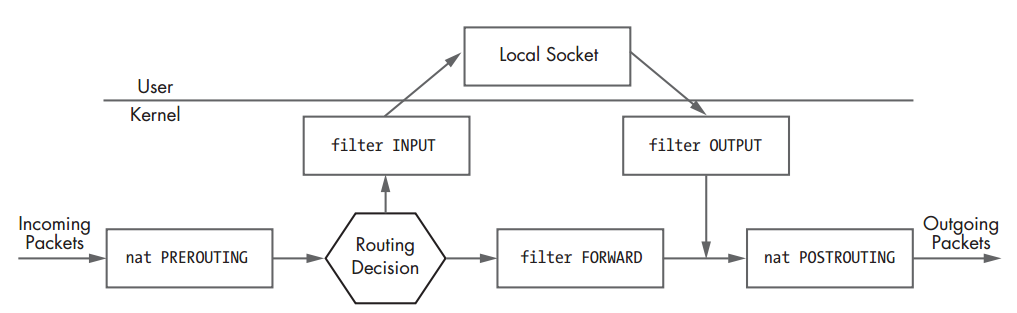
- most important built-in chains for our purposes are the INPUT, OUTPUT, and FORWARD chains in the filter table:

+ The INPUT chain is traversed by packets that are destined for the local Linux system after a routing calculation is made within the kernel

+ The OUTPUT chain is reserved for packets that are generated by the Linux system itself.

+ The FORWARD chain governs packets that are routed through the Linux system

- Two additional chains that are important:  
+ PREROUTING, POSTROUTING in the nat table, chúng sử dụng để used to modify packet headers before and after an IP routing calculation, made within the kernel.

+ 

Matches- set of matches along with a target that tells iptables what to do with a packet that conforms to the rule.

- iptables match is a condition that must be met by a packet in order for iptables to process the packet according to the action specified by the rule target

VD: apply a rule only to TCP packets, you can use the --protocol match.

- --source (-s) #Match on a source IP address or network

--destination (-d) #Match on a destination IP address or network

--protocol (-p) #Match on an IP value

--in-interface (-i) #Input interface (e.g., eth0)

--out-interface (-o) #Output interface

--state #Match on a set of connection states

--string #Match on a sequence of application layer data bytes

--comment #Associate up to 256 bytes of comment data with a

rule within kernel memory

Targets- set of targets that trigger an action when a packet matches a rule

- important targets used

ACCEPT Allows a packet to continue on its way.

DROP Drops a packet. No further processing is performed, and as far

as the receiving stack is concerned, it is as though the packet was never sent.

LOG Logs a packet to syslog.

REJECT Drops a packet and simultaneously sends an appropriate response

packet (e.g., a TCP Reset packet for a TCP connection or an

ICMP Port Unreachable message for a UDP packet).

RETURN Continues processing a packet within the calling chain

Default iptables PolicyPolicy Requirements- define the requirements for an effective firewall configuration for a network consisting of several client machines and two servers:

- servers (a webserver and a DNS server) must be accessible from the external network

- internal network should be allowed to initiate the following types of traffic through the firewall to external servers:

Domain Name System (DNS) queries

File Transfer Protocol (FTP) transfers

Network Time Protocol (NTP) queries

Secure SHell (SSH) sessions

Simple Mail Transfer Protocol (SMTP) sessions

Web sessions over HTTP/HTTPS

whois queries

- Except for access to the services listed above, all other traffic should be blocked.\\\

- Sessions initiated from the internal network or directly from the firewall should be statefully tracked by iptables

- NAT services should also be provided

- firewall should also implement controls against spoofed packets from the internal network being forwarded to any external IP address

- The firewall should accept ICMP Echo Requests from both the internal and external networks, but unsolicited ICMP packets that are not Echo Requests should be dropped from any source IP address

- firewall should be configured with a default log and drop stance so that any stray packets, port scans, or other connection attempts that are not explicitly allowed through will be logged and dropped

VD:

- external IP address on the firewall is statically assigned by the ISP

- single internal network with a non-routable network address of 192.168.10.0

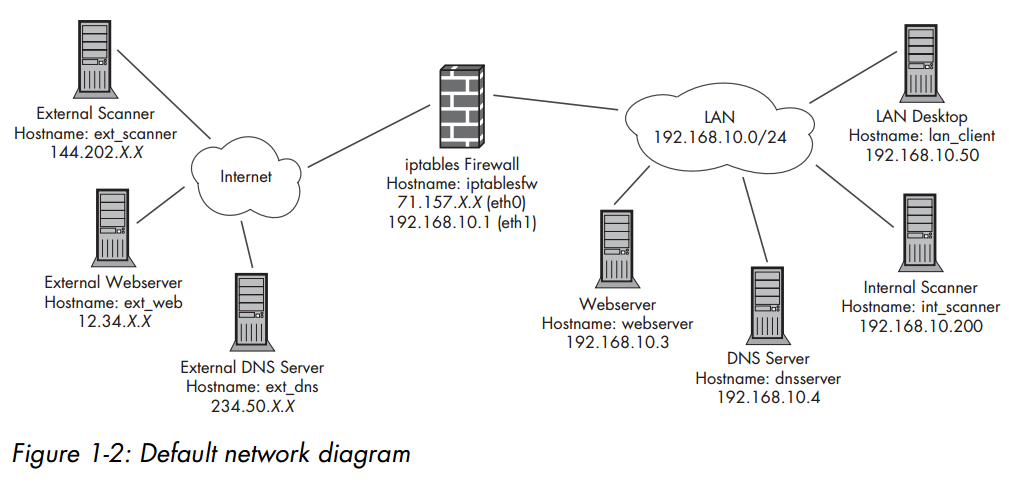
- Class C subnet mask 255.255.255.0 (or /24 in CIDR notation).

- internal network interface on the firewall (see Figure 1-2) is eth1 192.168.10.1,

- internal hosts have this address as their default gateway.

- allows internal systems to route all packets destined for systems that are not within the 192.168.10.0/24 subnet out through the firewall

- external interface on the firewall is eth0, we designate an external IP address of 71.157.X.X to this interface



iptables.sh Script Preamble

- Sử dụng script để tạo các rule trong ip tableIPTABLES and MODPROBE, INT\_NET

e