Cheatsheet iptables

Table	Function	Chain	Function
Filter	Packet filtering	FORWARD	Filters packets destined for other machines
		INPUT	Filters all packets destined for local machine
		OUTPUT	Filters all packets created by local machine
Nat	Network Address Translation	PREROUTING	Address translation occurs before routing. Changes the destination IP also known as **destination NAT** or **DNAT**.
		POSTROUTING	Address translation occurs after routing. Changes the source IP also known as **source NAT**, or **SNAT**.
		OUTPUT	Address Translation for packets generated by the firewall.
Mangle	TCP header modification, TTL, TOS, and MARK to change routing	PREROUTING	Packets arriving at an interface transit this chain.
		INPUT	Packets destined for local machine enter here
		OUTPUT	Packets created by local machine exit here
		FORWARD	Packets not destined for local machine transit this chain
		POSTROUTING	Packets exiting transit this chain

FILTER Rule Specifications

Tables are made of of chains. Chains are made up of rules. Rules are made up of matches and actions

Matches and Actions	Description
-s <source IP>	Match on <source IP> - can be IP, Network (192.168.2.0/24), hostname.
-d <destination IP>	Match on <destination IP> - can be IP, Network (192.168.2.0/24), hostname.
-i <ingress interface>	Match on ingress interface. For INPUT, FORWARD and PREROUTING
-o <egress interface>	Match on exit interface. For OUTPUT, FORWARD and POSTROUTING
-p tcp | udp | icmp | all	Match on protocol, default is *all*
--dport <port>	Match on <destination port> - can be a number, range (137:139 or 1024:) or a name from /etc/services
--sport <port>	Match on <source port> - can be a number, range (137:139 or 1024:) or a name from /etc/services
--tcp-flags <mask> <match>	Match on tcp flags . Mask shows which flags to look at, match shows which have to be on. Mask/match can be one or more of SYN, ACK, PSH, URG, RST, FIN, ALL or NONE. **Must be preceded by -p tcp**
--icmp-type <type>	Match on icmp-type <type>. Type can be a numeric ICMP type or a name (to see list iptables -p imcp -h). **Must be preceded by -p icmp**
-m state --state <statespec>	Load state module (-m) and match on statespec. Statespec can be one or more of NEW, ESTABLISHED, INVALID or RELATED.
-j accept | drop | log | reject [chain_name]	Jump to specific action or a custom chain [chain_name]. Actions can be one of ACCEPT, DROP, LOG or REJECT

Firewall Function	Command
List all rules [chain]	iptables -L INPUT
List rules with line numbers	iptables -L --line-numbers INPUT
List rules in short format	iptables -S
Flush rules in chain	iptables -F INPUT
Create a new chain	iptables -N BOBSCHAIN
Send traffic to chain	iptables -A INPUT -j BOBSCHAIN
Delete chain	iptables -X BOBSCHAIN
Insert rule in chain	iptables -I INPUT 2 -p tcp --dport 80 -m state --state NEW -j ACCEPT
Append rule to chain	iptables -A INPUT -p tcp --dport 80 -m state –state NEW -j ACCEPT
Delete rule from chain	iptables -D INPUT 2
Replace rule in chain	iptables -R INPUT 1 -s 192.168.0.1 -j DROP
Set default policy of chain	iptables -P INPUT DROP
Specify table to operate on	iptables -t filter

Firewall Task	Example Rule
Allow inbound web traffic	iptables -A INPUT -p tcp --dport 80 -i eth0 -j ACCEPT
Drop from one IP address	iptables -A INPUT -s 202.54.1.2 -j DROP
Drop incoming traffic only	iptables -A INPUT -m state --state NEW,ESTABLISHED -j ACCEPT
Drop traffic from a network	iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
Drop traffic to port	iptables -A INPUT -p tcp --dport 80 -j DROP
Drop outgoing traffic to ip	iptables -A OUTPUT -d 75.126.153.206 -j DROP
Drop packets from MAC	iptables -A INPUT -m mac --mac-source 00:0F:EA:91:04:08 -j DROP
Log packets from network	iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j LOG --log-prefix "SPOOF"
Log and limit packets from network	iptables -A INPUT -s 10.0.0.0/8 -m limit --limit 5/m --limit-burst 7 -j LOG --log-prefix "SPOOF"
Show Logged packets	grep 'SPOOF' /var/log/messages
Drop ping requests	iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
Allow ping from network	iptables -A INPUT -s 192.168.1.0/24 -p icmp --icmp-type echo-request -j ACCEPT
Allow from port range	iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 7000:7010 -j ACCEPT
Allow from IP range	iptables -A INPUT -p tcp --destination-port 80 -m iprange --src-range 192.168.1.100-192.168.1.200 -j ACCEPT
Set default INPUT policy	iptables -P INPUT DROP
Flushes rules in [chain]	iptables -F INPUT
Save rules to file	Iptables -S > /etc/sysconfig/iptables