06-09-21

Firewall on desktop (linux-fedora)

Commands:

>>id # check user

>>ping www.google.com

------------systemctl-------

#check status of firewalld on fedora

>>systemctl status firewalld

#stop the service

>>systemctl stop firewalld

>>systemctl start firewalld

------------iptables list rules--------

# list all the rules in iptables

>>iptables -L

# list rules for input chain

>>iptables -L INPUT

#input chain of filter table

>>iptables -L INPUT -t filter

-------------backup, restore and flush---------

#save the rules to a files as backup

>>iptables-save > fw

#view fw file on terminal

>>less fw

#flush iptables rules in filter table

>>iptables -F

# restore old rules back from fw file

>>iptables-restore fw

#flush all the chains from filter table

>>iptables -X

--------------default: block everything---

#block input and output chains

#-P => policy

>>iptables -P INPUT DROP

>>iptables -P OUTPUT DROP

-----allow all traffic to go out-------

#allow all traffic to go out

#-j => target

>>iptables -A OUTPUT -j ACCEPT

------filter incoming traffic-------

#allow established, related traffic

#-m => module

#--ctstate => states in conntrack

>>iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

# ping and browser will work in above step

------delete a rule------

#delete output chain rule defined above

>>iptables -D OUTPUT -j ACCEPT

----------allow tcp, udp packets to go out-----

#-p => protocol

>>iptables -A OUTPUT -p tcp -j ACCEPT

#with above step browser and ping will not work

#ping => icmp

#browser => http, https => tcp, udp

## allow udp

>>iptables -A OUTPUT -p udp -j ACCEPT

#ping will not work with above step=> not established connection; uses icmp

#browser will work

##### allow udp packets of port number 53 to go out

#-m udp => udp module

#--dport => destination port

>>iptables -A OUTPUT -p udp -m udp --dport 53 -j ACCEPT

-------allow only web browsing traffic -----------

>>iptables -D OUTPUT -p tcp -j ACCEPT

>>iptables -A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT

>>iptables -A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT

----------allow icmp echo request to go out----

>>iptables -A OUTPUT -p icmp -m icmp --icmp-type echo-request -j ACCEPT

#ping will work after above step

Router

08-09-21

Firewall on router

Default:

>>iptables -P FORWARD DROP

1) LAN -> I, allow all

>>iptables -A FORWARD -i eth0 -o eth1 -s 10.0.0.1/8 -j ACCEPT

2) I -> LAN, allow related traffic

>>iptables -A FORWARD -i eth1 -o eth0 -d 10.0.0.1/8 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

3) LAN -> WS, allow 80, 443, tcp

>>iptables -A FORWARD -i eth0 -o eth2 -s 10.0.0.1/8 -p tcp -m tcp --dport 80 -j ACCEPT

>>iptables -A FORWARD -i eth0 -o eth2 -s 10.0.0.1/8 -p tcp -m tcp --dport 443 -j ACCEPT

----------or

>>iptables -A FORWARD -i eth0 -o eth2 -s 10.0.0.1/24 -p tcp -m multiport --dports 80,443 -j ACCEPT

4) WS -> LAN, allow related traffic

>>iptables -A FORWARD -i eth2 -o eth0 -d 10.0.0.1/24 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

5) I -> WS, allow 443, tcp

>>iptables -A FORWARD -i eth1 -o eth2 -p tcp -m tcp --dport 443 -j ACCEPT

6) WS -> I, allow related traffic

>>iptables -A FORWARD -i eth2 -o eth1 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT