VyOS initial boot

Default pass	vyos:vyos
Change passwords	sudo su passwd root XXXX configure set system login user vyos authentication plaintext-password ‘XXXX’
Check running services	sudo su service --status-all
Disable SSH (if running)	pkill ssh pkill sshd
Disable telnet	
Interface mapping	show [tab] interface

Configure [commit; save; exit]

Enabling SSH	mkdir /var/run/sshd/ sudo chown root:root /var/run/sshd vim /etc/ssh/sshd_config ListenAddress <LAN **IP ADDRESS**> TTY: sudo /usr/sbin/sshd -D
Interface Mapping:	su vyos configure show [tab] interface
Setting WAN interface	**this should be already set**
Setting LAN interface	configure set interfaces ethernet eth1 address ‘x.x.x.x/24’ set interfaces ethernet eth1 description ‘INSIDE’ set interfaces ethernet eth1 duplex ‘auto’ set interfaces ethernet eth1 speed ‘auto’ commit save
Removing entries	delete interfaces ethernet eth1 delete interfaces ethernet eth1 description commit save

setting host name	set system host-name <hostname>
show default route	show ip route 0.0.0.0

Important note on usage of terms: The firewall makes use of the terms in, out, and local for firewall policy. Users experienced with netfilter often confuse **in** to be a reference to the **INPUT** chain, and **out** the **OUTPUT** chain from netfilter. This is not the case. These instead indicate the use of the **FORWARD** chain and either the input or output interface. The **INPUT** chain, which is used for local traffic to the OS, is a reference to as local with respect to its input interface.

Firewall rules

Ports	TCP: 20 - FTP 21 - FTP 22 - SSH 25 - SMTP 80 - HTTP 110 - POP3 443 - HTTPS UDP: 53 - DNS (in/out)
Setting groups	set firewall group network-group NET-INSIDE network x.x.0.0/24 set firewall group network-group NET-INSIDE x.x.1.0/24
Setting port groups	set firewall group port-group PORT-TCP-SERVER1 port 80 set firewall group port-group PORT-TCP-SERVER1 port 443 set firewall group port-group PORT-TCP-SERVER1 port 5000-5010
Rule-sets	set firewall name INSIDE-OUT default-action drop set firewall name INSIDE-OUT rule 1010 action accept set firewall name INSIDE-OUT rule 1010 state established enable

	set firewall name INSIDE-OUT rule 1010 state related enable set firewall name INSIDE-OUT rule 1020 action drop set firewall name INSIDE-OUT rule 1020 tate invalid enable
Applying rule-set to an interface	set interfaces ethernet eth1 firewall out name INSIDE-OUT
Applying rule-set to a zone	set zone-policy zone INSIDE from OUTSIDE firewall INSIDE-OUT
Port forwarding	set nat destination rule 10 description ‘Port Forward: HTTP to x.x.x.x’ set nat destination rule 10 destination port ‘80’ set nat destination rule 10 inbound-interface ‘eth0’ set nat destination rule 10 protocol ‘tcp’ set nat destination rule 10 translation address ‘x.x.x.x’
Applying a Rule-Set to an Interface	set interfaces ethernet eth1 firewall out name INSIDE-OUT

Monitoring

Send to background	kill %
Check for listening ports	sudo lsof -i
Netstat	netstat -anp -t (tcp) -u (udp)
TCP Dump	CTRL + ALT [+ FUNC] + F2, F3, etc. (or screen) sudo tcpdump -i <interface WAN> -w /var/dump.1
SSH	/etc/ssh/ssh_config /etc/ssh/sshd_config /user/bin/ssh
Log Monitoring	var/log/auth.log history cat ~/.bash_history

Misc. Commands

clear screen	ctrl+l
network	sudo su ifconfig

```
vi /etc/network/interfaces

      auto eth0

      iface eth0 inet static

      address 10.10.10.69

      netmask 255.255.255.0

      gateway 10.10.10.1

      dns-nameservers 10.10.10.1
```