نقش و اهمیت شماره پورت‌ها در عملکرد سرورها و سرویس‌های شبکه‌ای

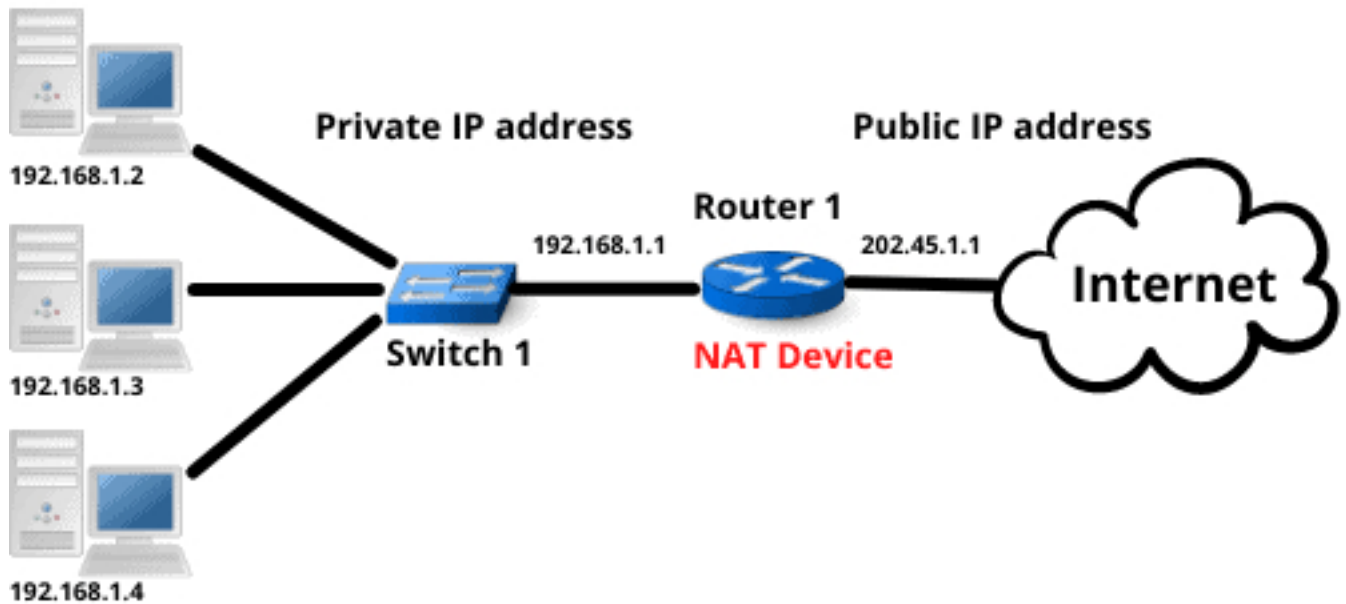
عرفان عبدی

40114141054300

پورت چیست و چرا هر سرویس شبکه‌ای نیاز به پورت منحصربه‌فرد دارد؟

- در دنیای شبکه، **پورت (Port)** یک عدد ۱۶ بیتی است که برای شناسایی برنامه یا سرویس خاصی که روی یک دستگاه در حال اجراست استفاده می‌شود. وقتی داده‌ای به یک آدرس IP ارسال می‌شود، شماره پورت مشخص می‌کند که این داده باید به کدام سرویس یا اپلیکیشن تحویل داده شود.
- بدون استفاده از پورت‌ها، دستگاه مقصد قادر نخواهد بود تشخیص دهد کدام سرویس باید به درخواست پاسخ دهد. به همین دلیل هر سرویس شناخته‌شده یک شماره پورت خاص و استاندارد دارد (مثلاً پورت ۸۰ برای HTTP).

Network Address Translation

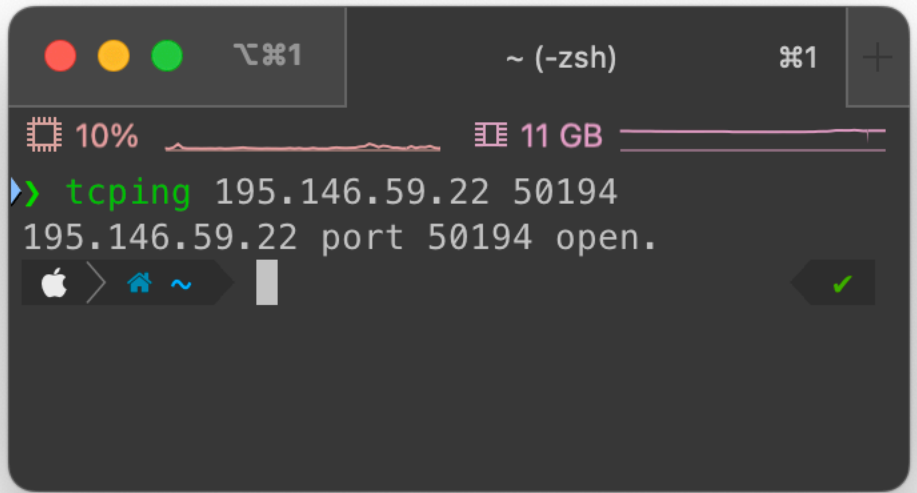


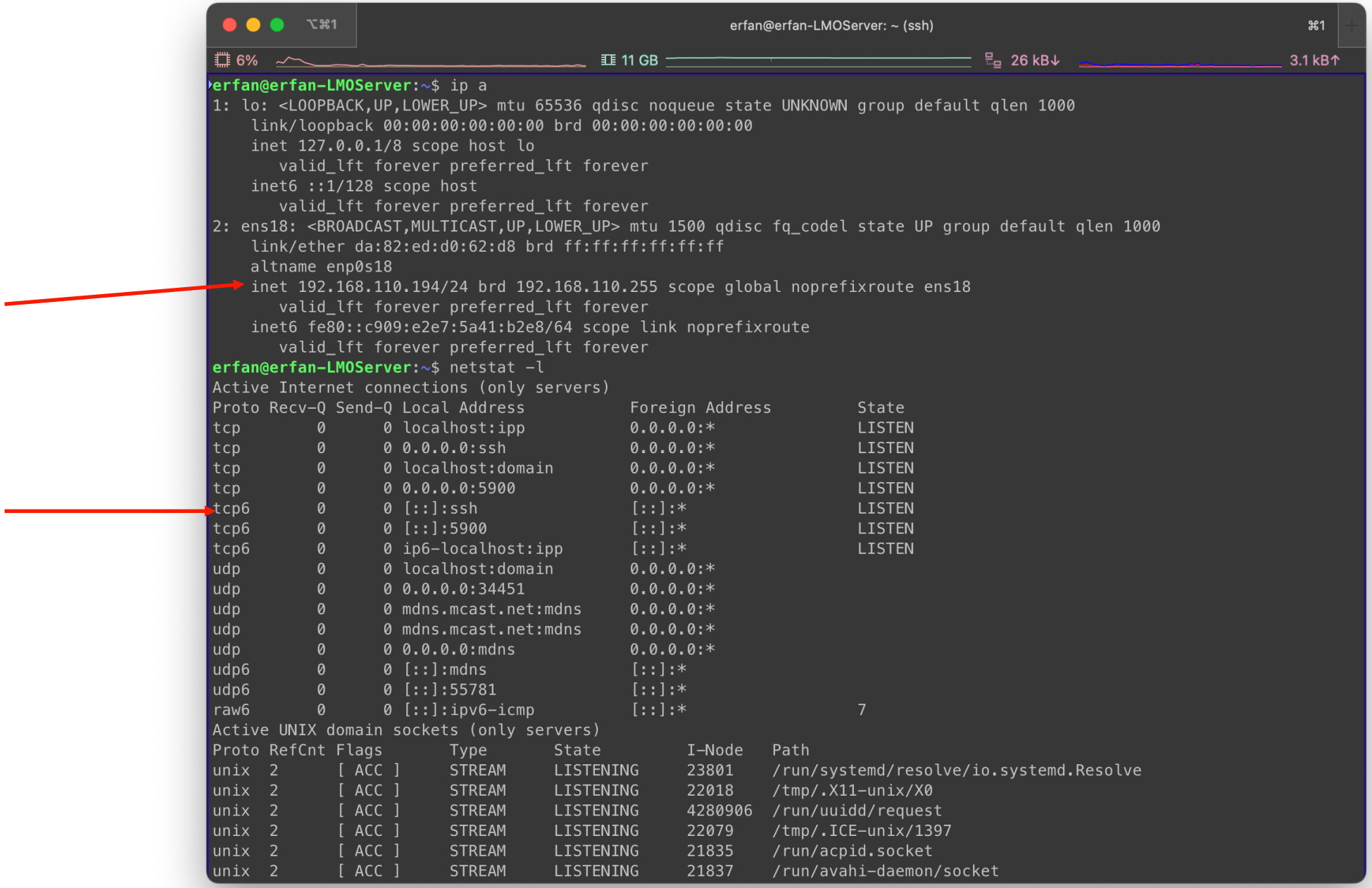
Firewall / NAT / Port Forward

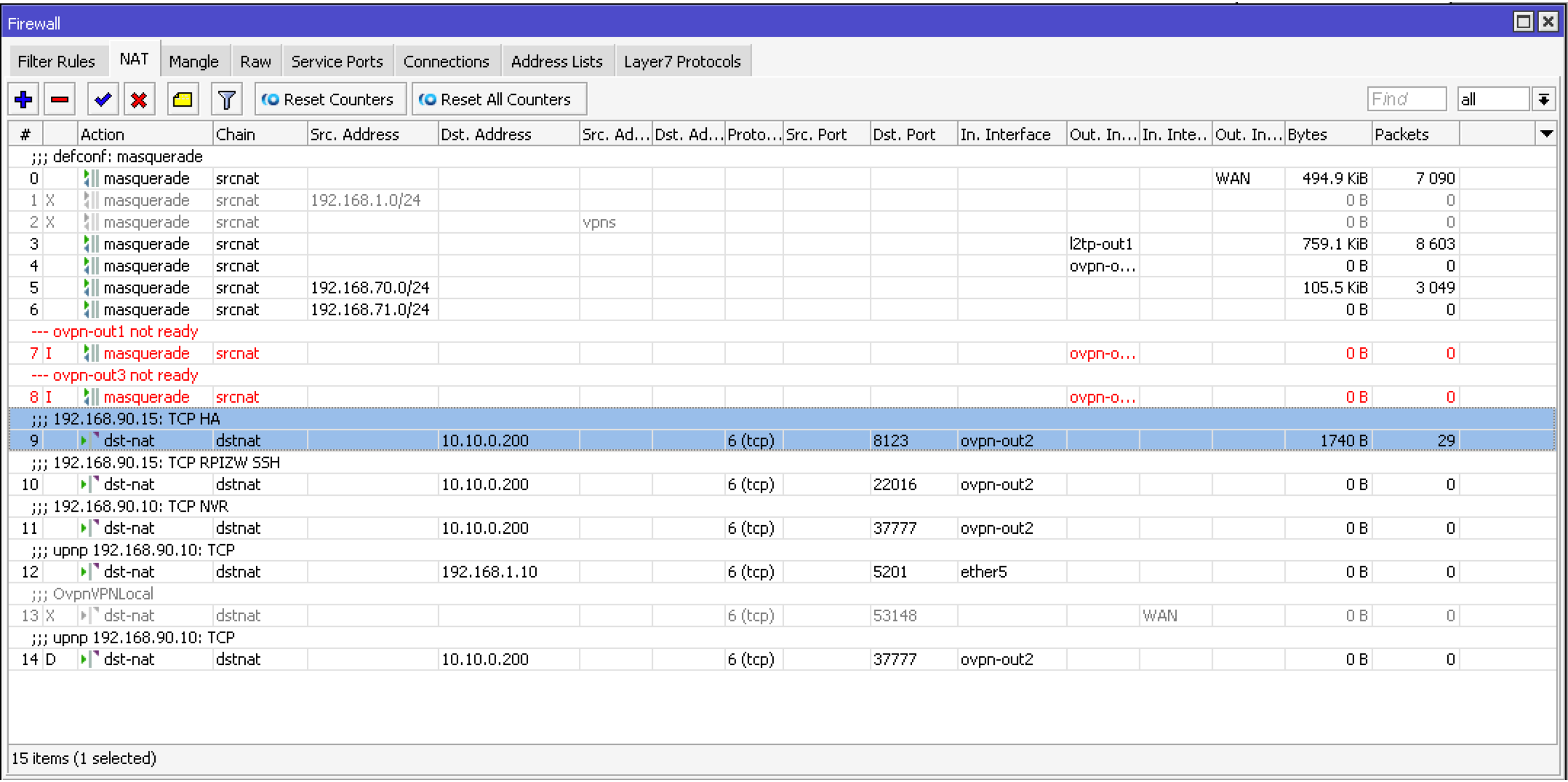
Port Forward | 1:1 | Outbound | NPt

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
☐	WAN	TCP	*	*	195.146.59.22	50189	192.168.110.189	22 (SSH)	LMO-Tadi-Personal-SSH	
☐	WAN	TCP	*	*	195.146.59.22	50193	192.168.110.193	22 (SSH)	GR-SSH	
☐	WAN	TCP	iranacc	*	195.146.59.22	50120	192.168.110.120	22 (SSH)	Jfrog-SSH	
☐	WAN	TCP	*	*	195.146.59.22	50194	192.168.110.194	22 (SSH)	Erfan-UbuntuDesktop-SSH	
☐	WAN	TCP	*	*	195.146.59.22	60194	192.168.110.194	5900 (VNC)	Erfan-UbuntuDesktop-VNC	
☐	WAN	TCP	*	*	195.146.59.22	50192	192.168.110.192	22 (SSH)	LMO-Shayan-Personal	


⌥⌘1
~ (-zsh)
⌘1
10%
11 GB
tcping 195.146.59.22 50194
195.146.59.22 port 50194 open.
~


erfan@erfan-LMOServer: ~ (ssh)
6%
11 GB
26 kB↓
3.1 kB↑
erfan@erfan-LMOServer:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether da:82:ed:d0:62:d8 brd ff:ff:ff:ff:ff:ff
altname enp0s18
inet 192.168.110.194/24 brd 192.168.110.255 scope global noprefixroute ens18
valid_lft forever preferred_lft forever
inet6 fe80::c909:e2e7:5a41:b2e8/64 scope link noprefixroute
valid_lft forever preferred_lft forever
erfan@erfan-LMOServer:~$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 localhost:ipp 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:ssh 0.0.0.0:* LISTEN
tcp 0 0 localhost:domain 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:5900 0.0.0.0:* LISTEN
tcp6 0 0 [::]:ssh [::]:* LISTEN
tcp6 0 0 [::]:5900 [::]:* LISTEN
tcp6 0 0 ip6-localhost:ipp [::]:* LISTEN
udp 0 0 localhost:domain 0.0.0.0:*
udp 0 0 0.0.0.0:34451 0.0.0.0:*
udp 0 0 mdns.mcast.net:mdns 0.0.0.0:*
udp 0 0 mdns.mcast.net:mdns 0.0.0.0:*
udp 0 0 0.0.0.0:mdns 0.0.0.0:*
udp6 0 0 [::]:mdns [::]:*
udp6 0 0 [::]:55781 [::]:*
raw6 0 0 [::]:ipv6-icmp [::]:* 7
Active UNIX domain sockets (only servers)
Proto RefCnt Flags Type State I-Node Path
unix 2 [ACC] STREAM LISTENING 23801 /run/systemd/resolve/io.systemd.Resolve
unix 2 [ACC] STREAM LISTENING 22018 /tmp/.X11-unix/X0
unix 2 [ACC] STREAM LISTENING 4280906 /run/uuidd/request
unix 2 [ACC] STREAM LISTENING 22079 /tmp/.ICE-unix/1397
unix 2 [ACC] STREAM LISTENING 21835 /run/acpid.socket
unix 2 [ACC] STREAM LISTENING 21837 /run/avahi-daemon/socket


Firewall
Filter Rules
NAT
Mangle
Raw
Service Ports
Connections
Address Lists
Layer7 Protocols
Reset Counters
Reset All Counters
Find
all
Action Chain Src. Address Dst. Address Src. Ad... Dst. Ad... Proto... Src. Port Dst. Port In. Interface Out. In... In. Inte.. Out. In... Bytes Packets
;;; defconf: masquerade
0 masquerade srcnat WAN 494.9 KiB 7 090
1 X masquerade srcnat 192.168.1.0/24 0 B 0
2 X masquerade srcnat vpns 0 B 0
3 masquerade srcnat l2tp-out1 759.1 KiB 8 603
4 masquerade srcnat ovpn-o... 0 B 0
5 masquerade srcnat 192.168.70.0/24 105.5 KiB 3 049
6 masquerade srcnat 192.168.71.0/24 0 B 0
--- ovpn-out1 not ready
7 I masquerade srcnat ovpn-o... 0 B 0
--- ovpn-out3 not ready
8 I masquerade srcnat ovpn-o... 0 B 0
;;; 192.168.90.15: TCP HA
9 dst-nat dstnat 10.10.0.200 6 (tcp) 8123 ovpn-out2 1740 B 29
;;; 192.168.90.15: TCP RPIZW SSH
10 dst-nat dstnat 10.10.0.200 6 (tcp) 22016 ovpn-out2 0 B 0
;;; 192.168.90.10: TCP NVR
11 dst-nat dstnat 10.10.0.200 6 (tcp) 37777 ovpn-out2 0 B 0
;;; upnp 192.168.90.10: TCP
12 dst-nat dstnat 192.168.1.10 6 (tcp) 5201 ether5 0 B 0
;;; OvpnVPNLocal
13 X dst-nat dstnat 6 (tcp) 53148 WAN 0 B 0
;;; upnp 192.168.90.10: TCP
14 D dst-nat dstnat 10.10.0.200 6 (tcp) 37777 ovpn-out2 0 B 0
15 items (1 selected)

معرفی سرویس‌های پرکاربرد و پورت‌های مربوطه

سرویس	شماره پورت
HTTP	80
HTTPS	443
DNS	53
SMTP	25
FTP	20 (Data), 21 (Control)
SSH	22

چگونه سرورها به‌کمک پورت‌ها به درخواست‌های مختلف پاسخ می‌دهند

- هر سرور برای گوش دادن به درخواست‌های خاص، پورت‌هایی را **باز** نگه می‌دارد. وقتی یک کلاینت (مثلاً مرورگر) درخواستی ارسال می‌کند:

۱. سیستم عامل سرور درخواست را بر اساس آدرس IP دریافت می‌کند.

۲. با نگاه به شماره پورت، تصمیم می‌گیرد که این داده به کدام برنامه یا سرویس تحویل داده شود.

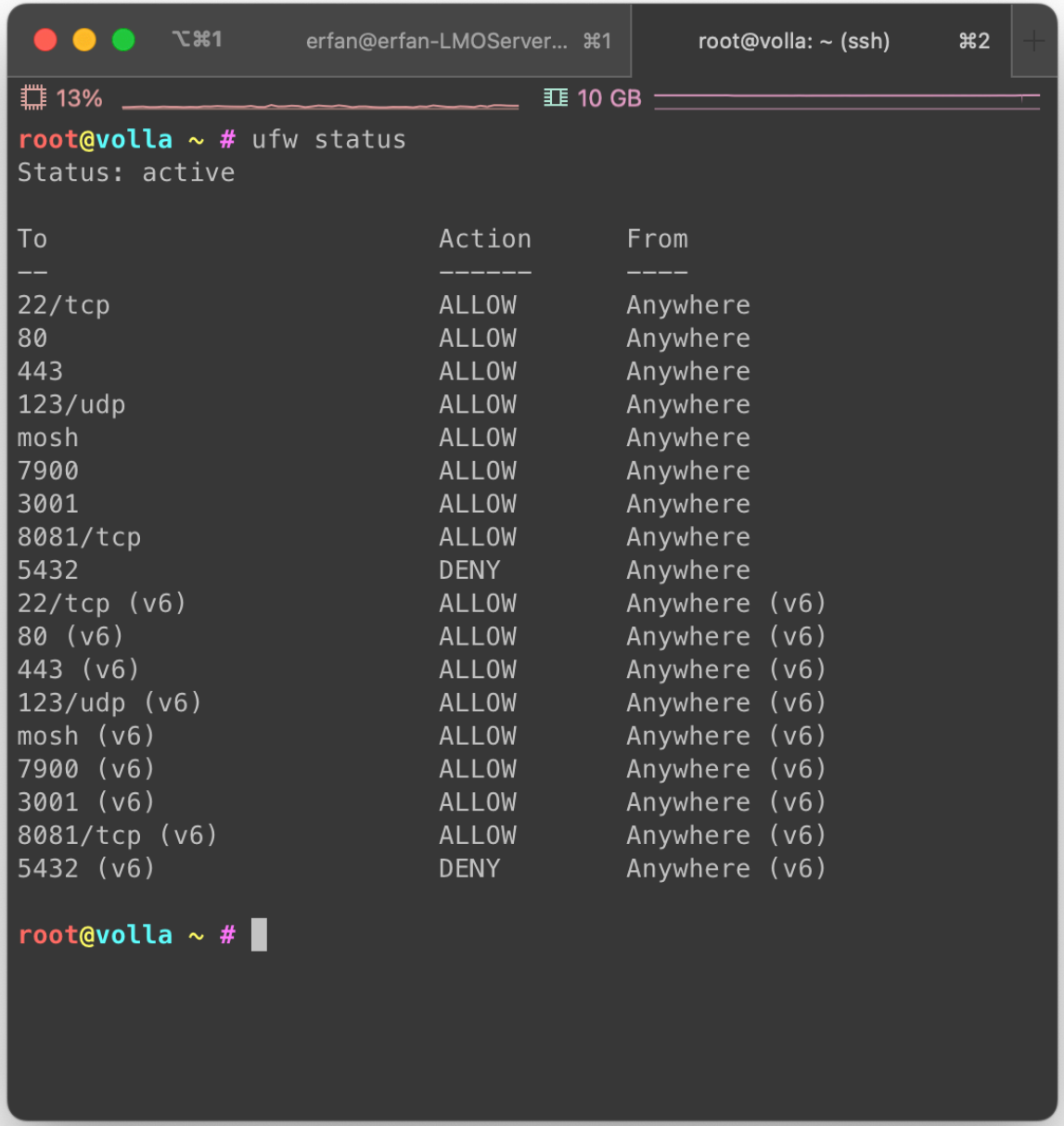
۳. مثلاً اگر درخواست به پورت ۴۴۳ برسد، به سرور HTTPS تحویل داده می‌شود.

اهمیت پورت‌ها در تنظیمات Firewall، NAT و Load Balancer

- **Firewall**: فایروال‌ها بر اساس شماره پورت تصمیم می‌گیرند که ترافیک را اجازه دهند یا مسدود کنند. مثلاً بستن پورت ۲۲ می‌تواند از دسترسی SSHجلوگیری کند.
- **NAT (Network Address Translation)**: برای ترجمه آدرس‌های داخلی به آدرس عمومی اینترنت، شماره پورت برای متمایز کردن ارتباط‌ها ضروری است.
- **Load Balancer**: لود بالانسر با استفاده از پورت‌ها درخواست‌ها را به سرورهای مختلف هدایت می‌کند (مثلاً تمام درخواست‌های پورت ۴۴۳ را بین چند سرور پخش می‌کند).

چه اتفاقی می‌افتد اگر پورت اشتباهی بسته یا باز باشد؟

- **اگر پورت اشتباهی بسته باشد:** فرض کنید پورت ۸۰ (HTTP) روی سرور وب بسته شده باشد. در این صورت کاربران نمی‌توانند سایت را مشاهده کنند، چون مرورگر نمی‌تواند به سرور متصل شود.
- **اگر پورت اشتباهی باز باشد:** باز بودن پورت ۳۳۰۶ (MySQL) در سروری که فقط از داخل شبکه باید قابل‌دسترسی باشد، می‌تواند امنیت را به خطر بیندازد و راه نفوذ هکرها باز بماند.


⌥⌘1
erfan@erfan-LMOServer... ⌘1
root@volla: ~ (ssh)
⌘2
13%
10 GB
root@volla ~ # ufw status
Status: active
To Action From
-- ------ ----
22/tcp ALLOW Anywhere
80 ALLOW Anywhere
443 ALLOW Anywhere
123/udp ALLOW Anywhere
mosh ALLOW Anywhere
7900 ALLOW Anywhere
3001 ALLOW Anywhere
8081/tcp ALLOW Anywhere
5432 DENY Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
80 (v6) ALLOW Anywhere (v6)
443 (v6) ALLOW Anywhere (v6)
123/udp (v6) ALLOW Anywhere (v6)
mosh (v6) ALLOW Anywhere (v6)
7900 (v6) ALLOW Anywhere (v6)
3001 (v6) ALLOW Anywhere (v6)
8081/tcp (v6) ALLOW Anywhere (v6)
5432 (v6) DENY Anywhere (v6)
root@volla ~ #

ممنون از توجه شما