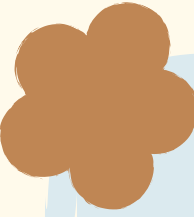


Day 3

Networking and Package Management



agenda

- 
- Package Management
 - Networking commands
 - Archiving and File Transfer (FTP, scp, rsync)
 - SSH Architecture, Flows and Administering Remote Machines
 - Interfaces Management and Network Routing
 - Firewall Management



Package manager

Helps you install, update, configure, and remove software on your system. Instead of manually downloading and compiling programs, the package manager automatically fetches them from trusted repositories, installs required dependencies, and keeps everything up to date.

widely used *package managers*

dpgk

low level package
manager

Need to specify the deb
file to install

dependency issues

apt

high level package
manager

specify only the package
name, it will fetch
automatically

resolve dependency by
automatically fetching the
required packages

aptitude

high level package
manager

snap



Method of installing, updating,
configuring, and removing software
on the system in a controlled way

What happens under the hood?? *apt...*

apt

apt update

apt install

Repository

There will be lot of repository available

- Can edit the sources to get packages from custom repositories if needed
- default sources are specified from the parrot repo

commands

apt install <package-name>

apt edit-sources

apt update

apt list

apt remove

apt upgrade

Networking *commands*

curl

- To interact with API (GET, POST, and more)
- Used to transfer data to or from a server using a variety of protocols such as HTTP, HTTPS, FTP, SCP and more
- To get the content of the webpage



REST APIs before tools like Postman existed.

wget for “offline Google”

wget

- To download files from the internet/web
- You can stop a download halfway, and resume it later without starting over
- With the right flags, wget can mirror an entire website, including all linked pages, images, and assets

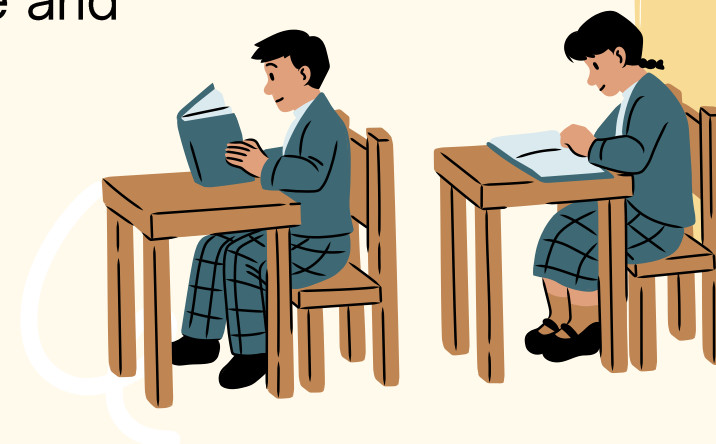
Can send emails, even download YouTube videos

curl is in space 🚀

Archiving and File Transfer

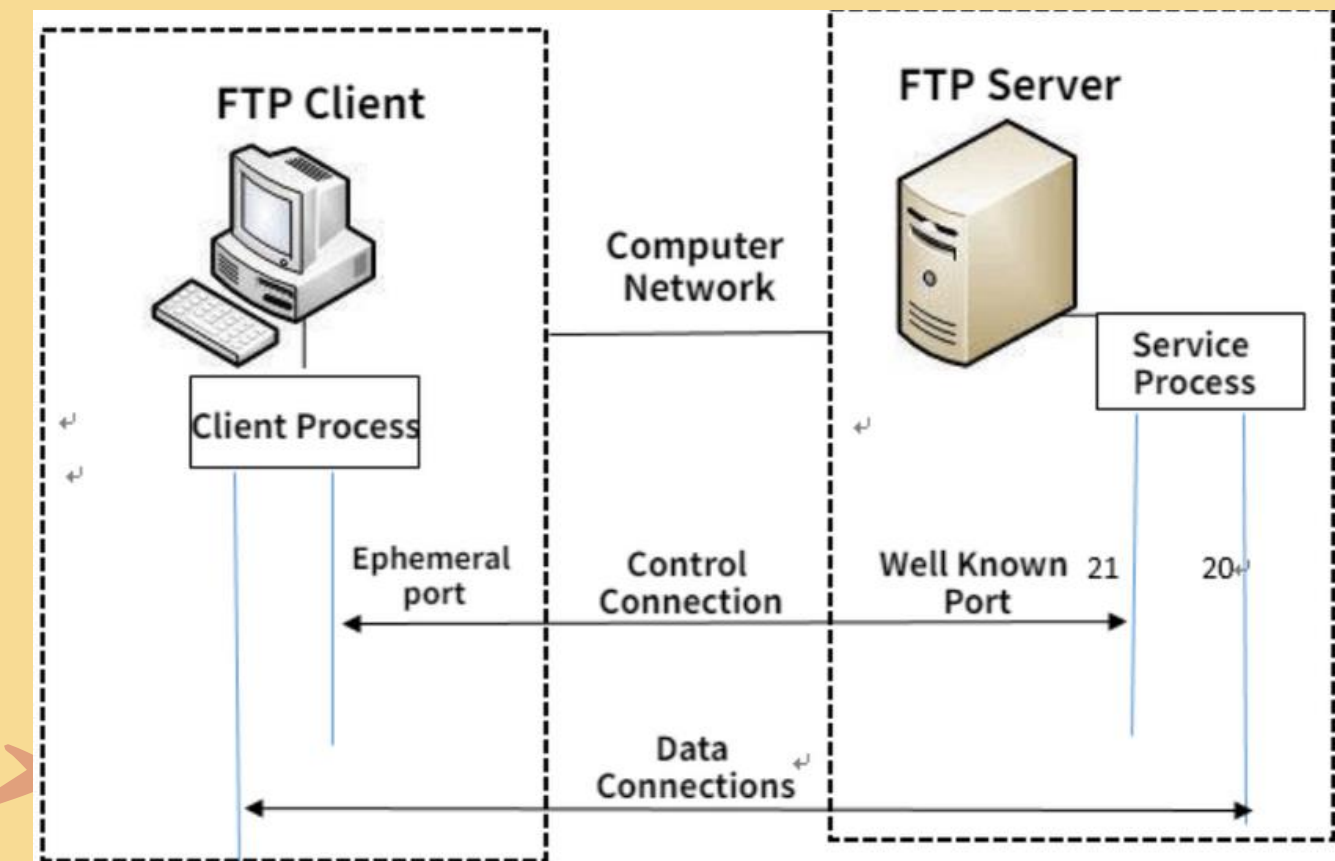
rsync (Remote Sync)

- Transfer files from one place to another
- `rsync dir1 dir2` (`dir*` can be local dir or can be NFS mounted system)
- One directional utility and not for syncing the files between two directories
- Use SSH by default
- When a file is updated at the source and pushed again, the existing data at the destination is not overwritten; instead, a new copy of the file is created at the destination
- By default, the meta between the source and target will not be the same



FTP (File Transfer Protocol)

- Used to transfer files between a client and a server over a network
- Client-server model
- TCP port (20, 21)
- Have active and passive modes

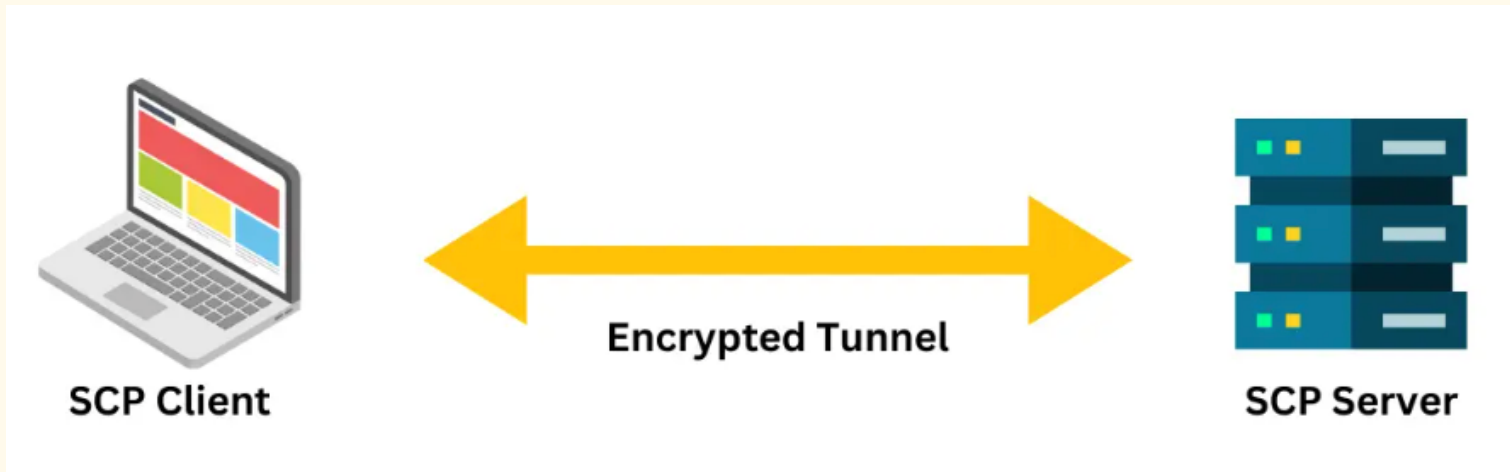


Archiving and File Transfer



SCP (Secure Copy Protocol)

- Transfer files securely between Linux/Unix systems over SSH (port 22)
- It encrypts Authentication, commands and content



Aspect	FTP
Security	Transmits data in plain text (insecure). FTPS adds TLS/SSL for encryption.
Functionality	Full file management: browse, rename, delete, move, list files.
Speed	Can be faster (less encryption overhead, uses port 21 for control & data transfer).



ssh protocol

secure shell

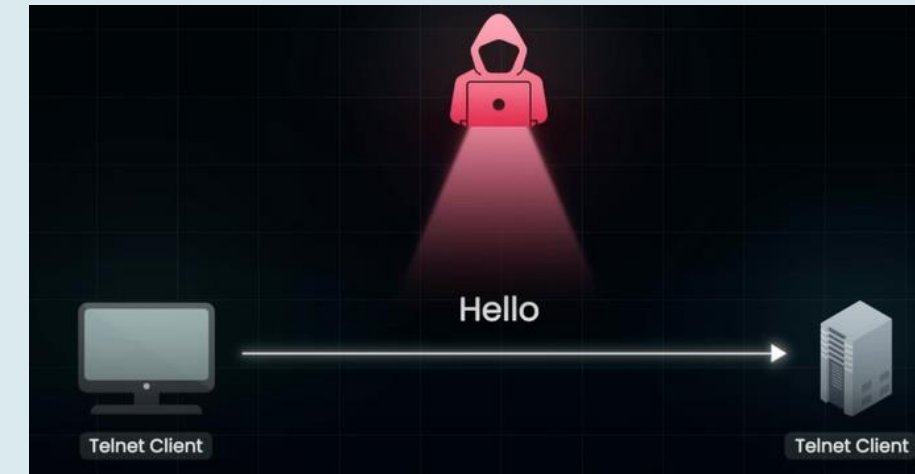
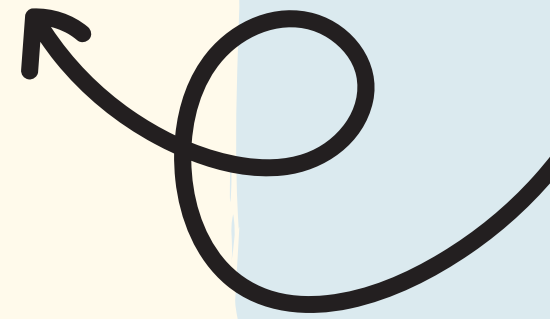
- Atfirst initiates the TCP connection
 - Create a secure tunnel
 - Package the data
 - Encrypt the data
-
- Send to the client
 - Client decrypts that and use that data

Cryptography

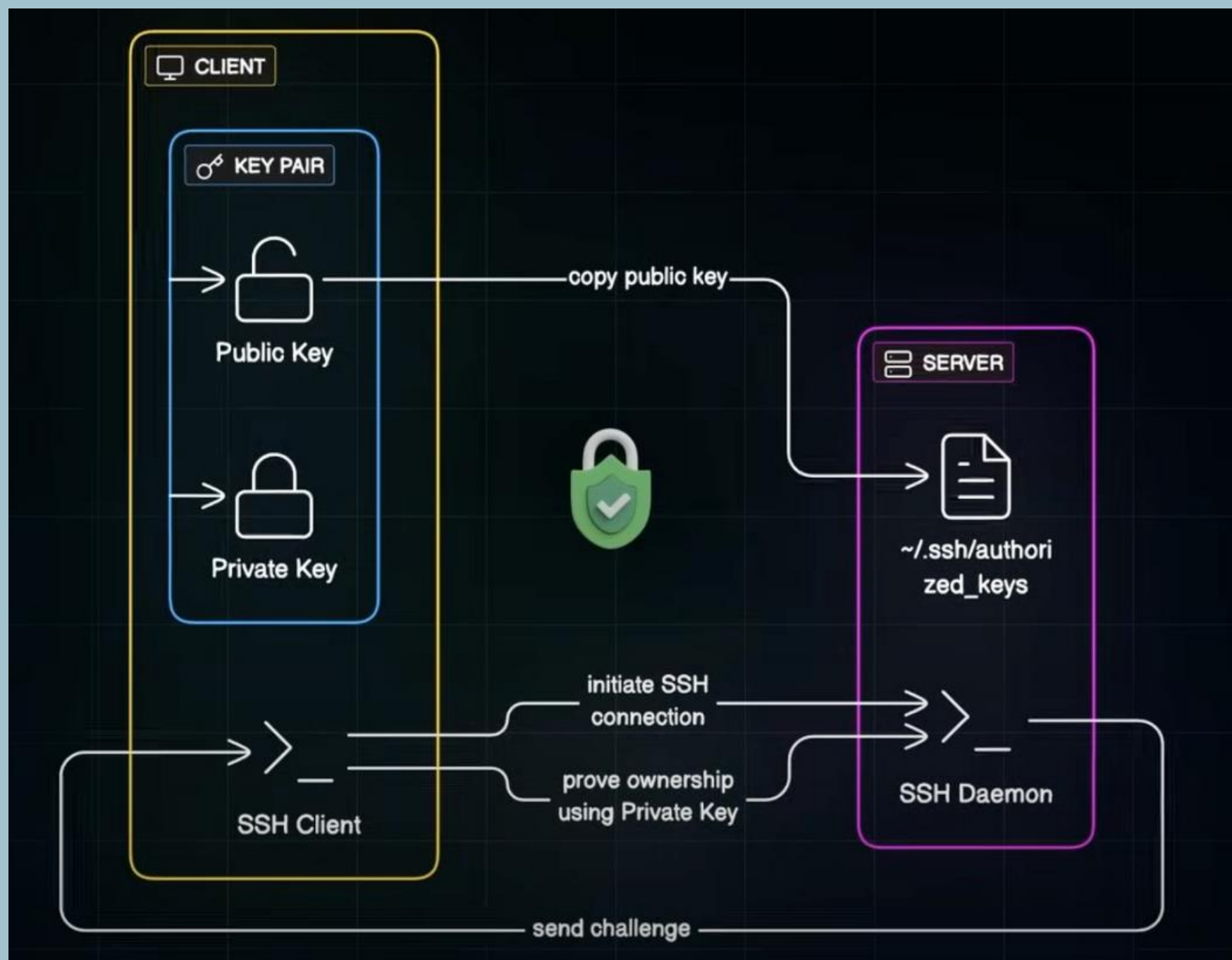
Symmetric
Encryption

Asymmetric
Encryption

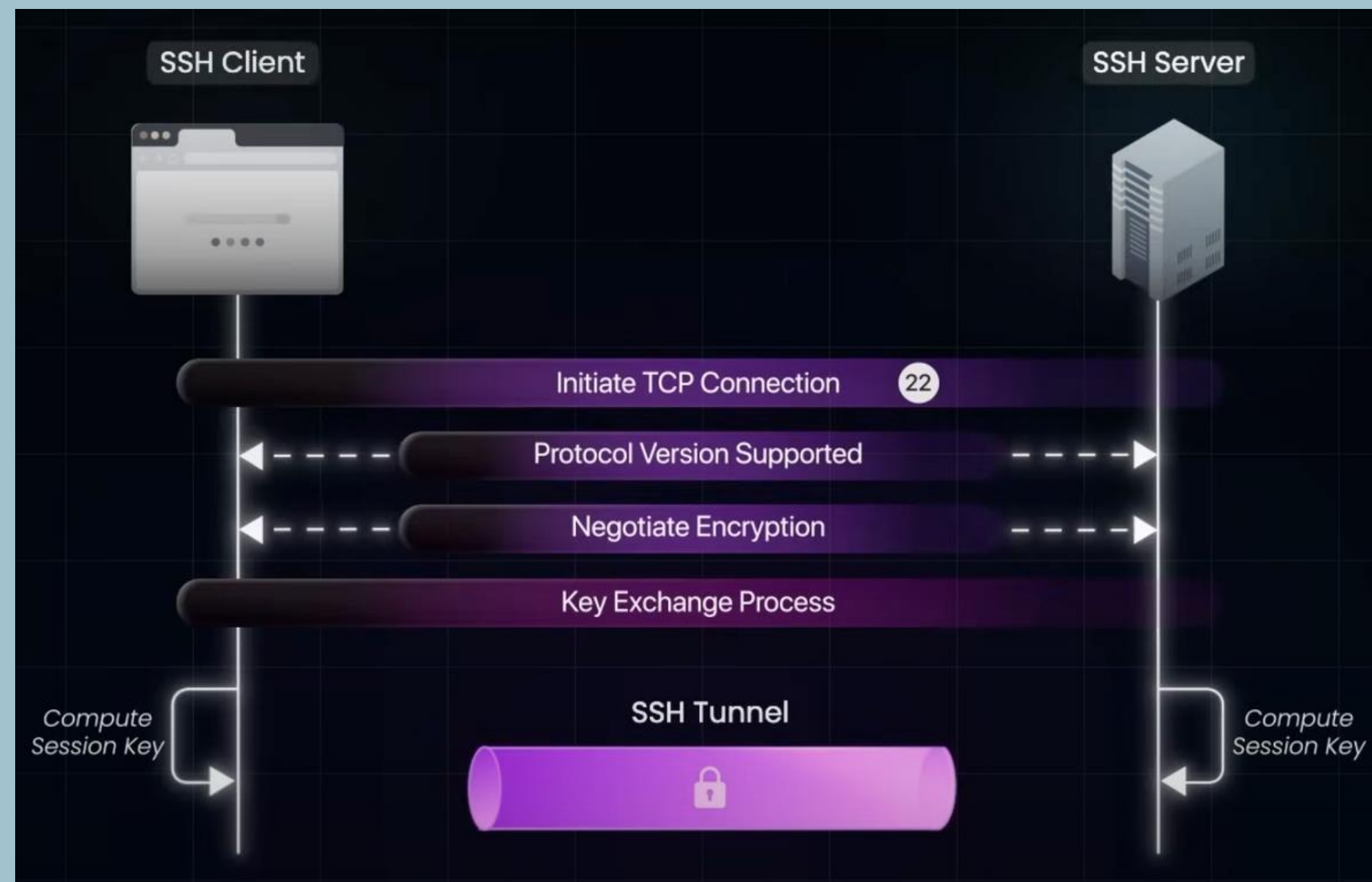
telnet



Key based Authentication

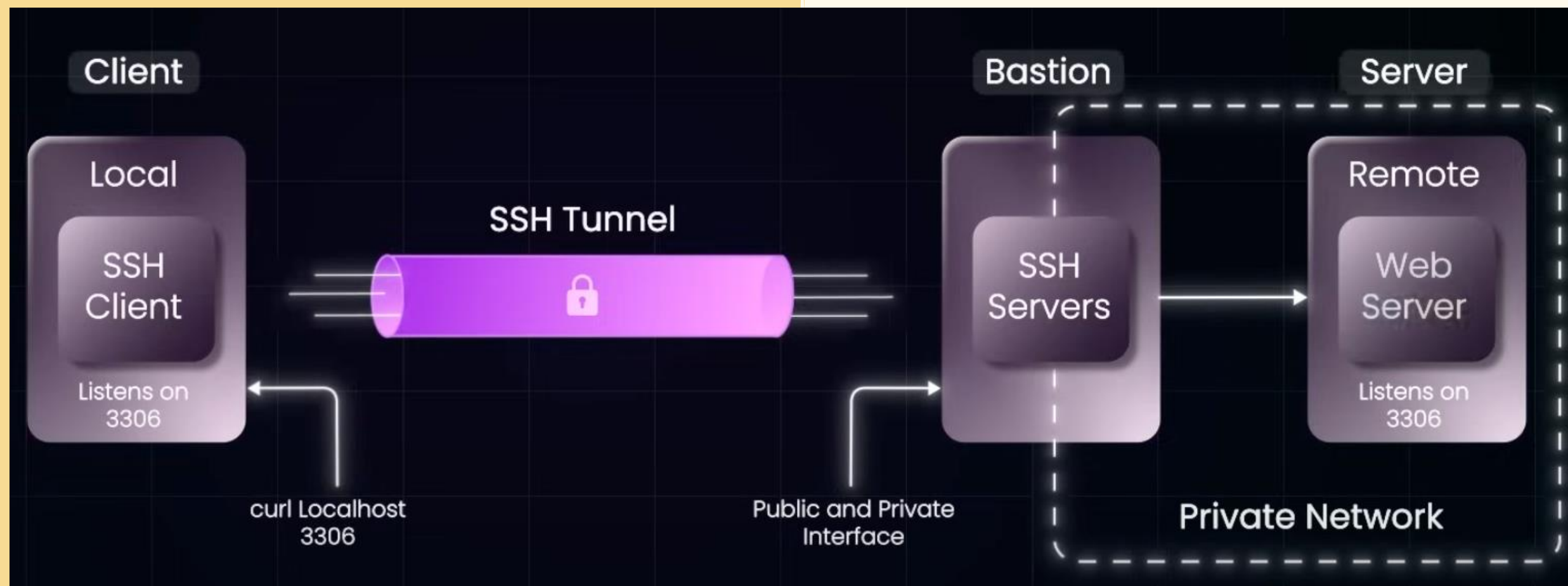


SSH Connection Flow



Local forwarding

- Establish a secure SSH session to the Bastion host, which provides controlled access to private network instances that are otherwise inaccessible externally



Network interfaces and routing

Network interface:

- A door through which your system communicates with the outside world.
- Can be physical or virtual endpoint
- Each interface has name, hardware id, software id and status

Routes:

- Route tells the system where to send the traffic it received
- It holds all the routes in the route table



```
ip route add <network>/<prefix> via <gateway-ip> dev <interface>
```

```
ip route
```

```
ifconfig
```

```
ip link show
```

Commands

Ping

- Checks connectivity between your machine and a remote host by sending ICMP echo requests.

telnet

- Tests connectivity to a host on a specific port
- telnet <hostname or IP> <port>

route -n

- Displays the kernel's IP routing table.
- -n flag shows numerical addresses instead of resolving hostnames (faster).

dig

- dig (Domain Information Groper) queries DNS servers to get information about domain names (IP resolution, mail servers, etc.)
- dig <domain>

Firewall Management

- Security guard for your server
- Checks every packet of data coming in (ingress) or going out (egress) of your system
- Based on rules we set, it decides whether to allow or block that packet
- Configure the rules properly

Why ?

- Security & compliance
- Traffic filtering
- Service control

ufw allow/deny from <source_ip> to
<dest_ip> port <port> proto <protocol>

ufw status

ufw allow/deny <port>

ufw enable

