Securing Your Linux Server

David Clinton
LINUX SYSTEM ADMINISTRATOR

bootstrap-it.com/linux-admin | @davidbclinton | linkedin.com/in/dbclinton

Overview

Overview

Permissions

Overview

Permissions

Software patches

Overview

Permissions

Software patches

Managing network ports

Overview

- Permissions
- Software patches
- Managing network ports
- Data encryption

Applying Object Permissions

Permissions: Numeric Notation

Permissions: Numeric Notation

Read	r	
Write	w	
Execute	x	

Permissions: Numeric Notation

Read	r	4
Write	w	2
Execute	x	1

Permissions: Numeric Notation

Read	r	4
Write	w	2
Execute	x	1

Full permissions: 7

Permissions: Numeric Notation

Read	r	4
Write	w	2
Execute	x	1

Full permissions: 7
Read/execute: 5

Permissions: Numeric Notation

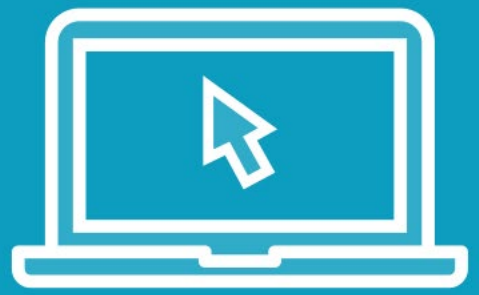
Read	r	4
Write	w	2
Execute	x	1

Full permissions: 7
Read/execute: 5
Execute: 1

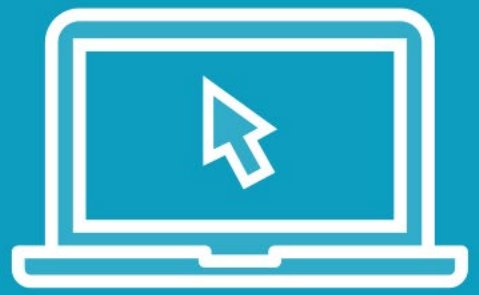
Extending Object Usability

Hardening Your Server

Demo

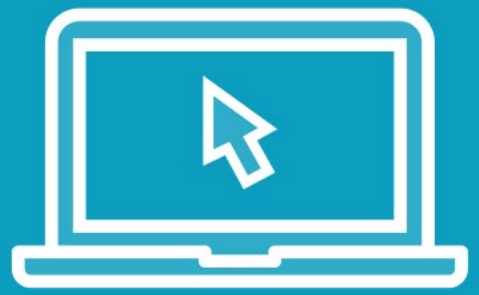


Demo



Reducing vulnerability

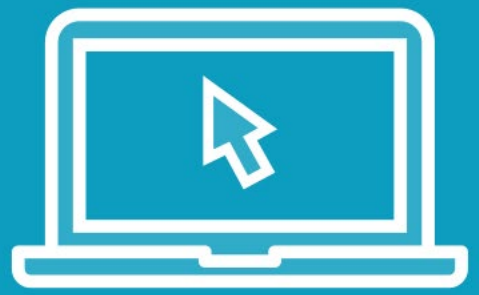
Demo



Reducing vulnerability

Patching systems

Demo

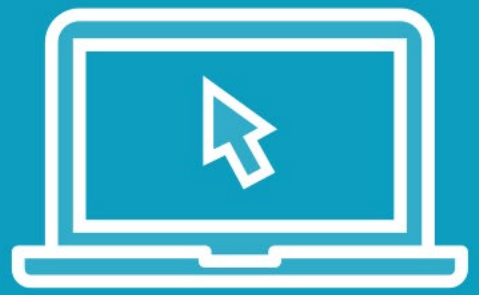


Reducing vulnerability

Patching systems

Understanding network ports

Demo



Reducing vulnerability

Patching systems

Understanding network ports

Managing network ports

Software Updates

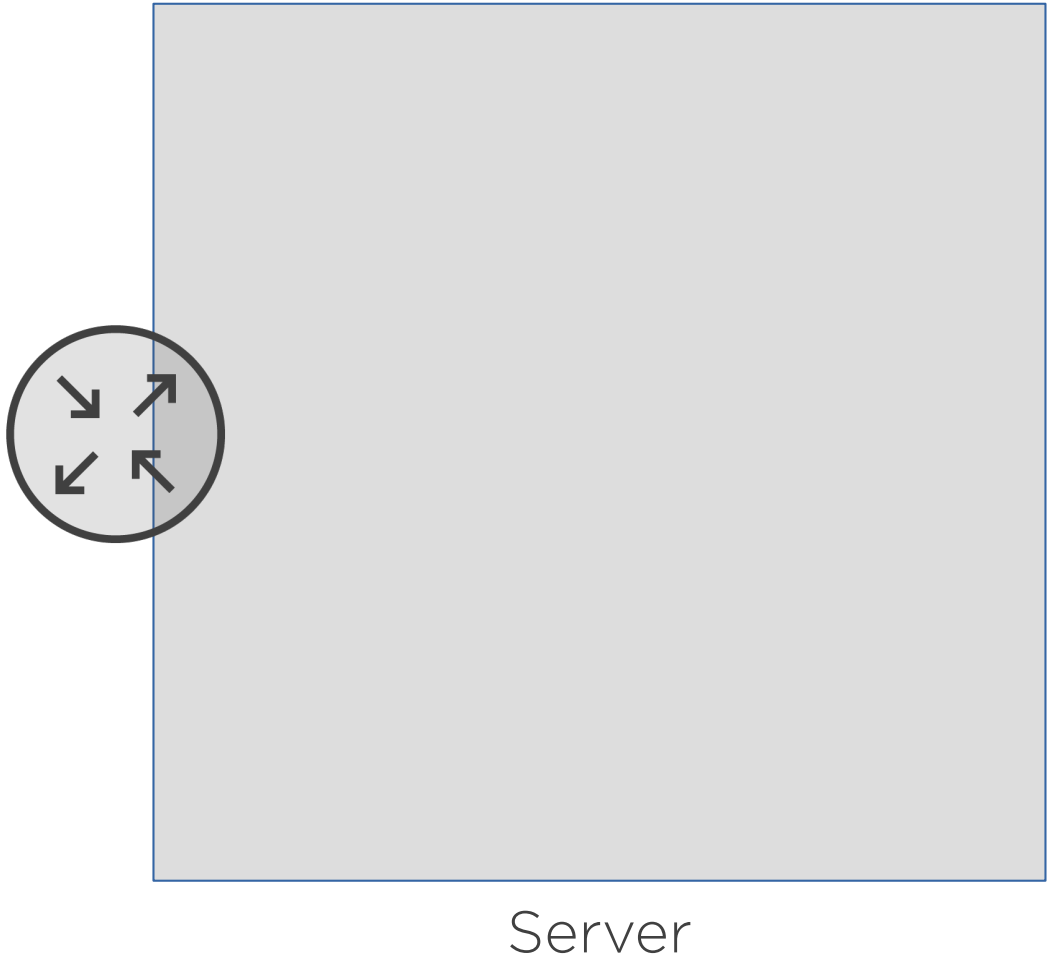
Software Updates

sudo apt update

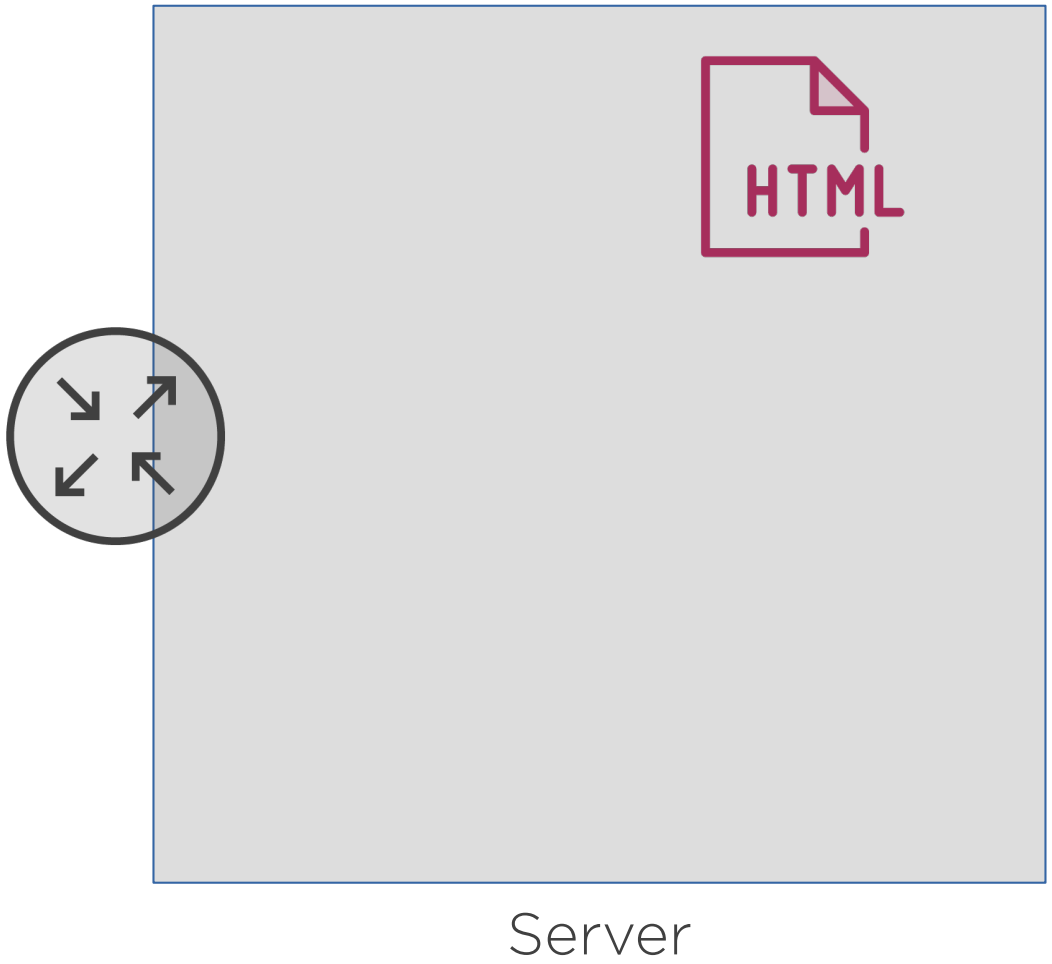
sudo apt upgrade

yum update

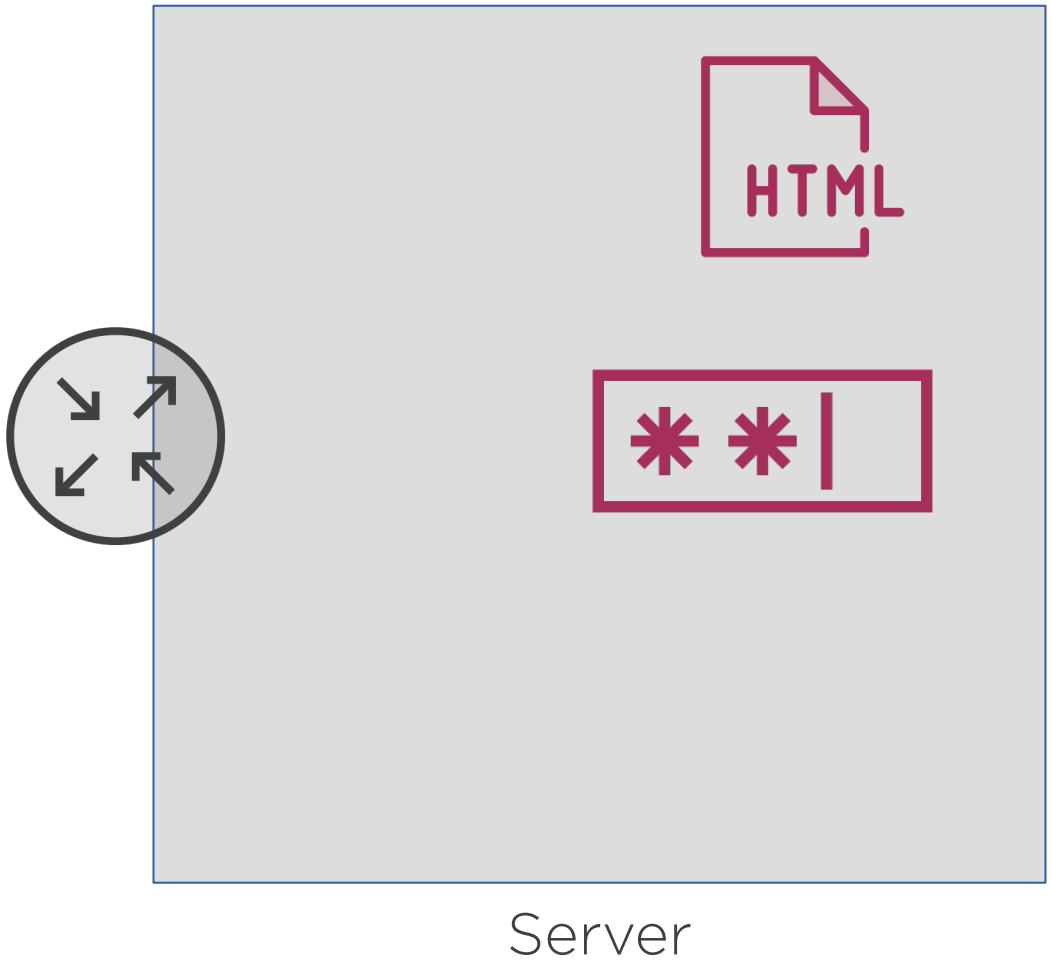
Network Ports



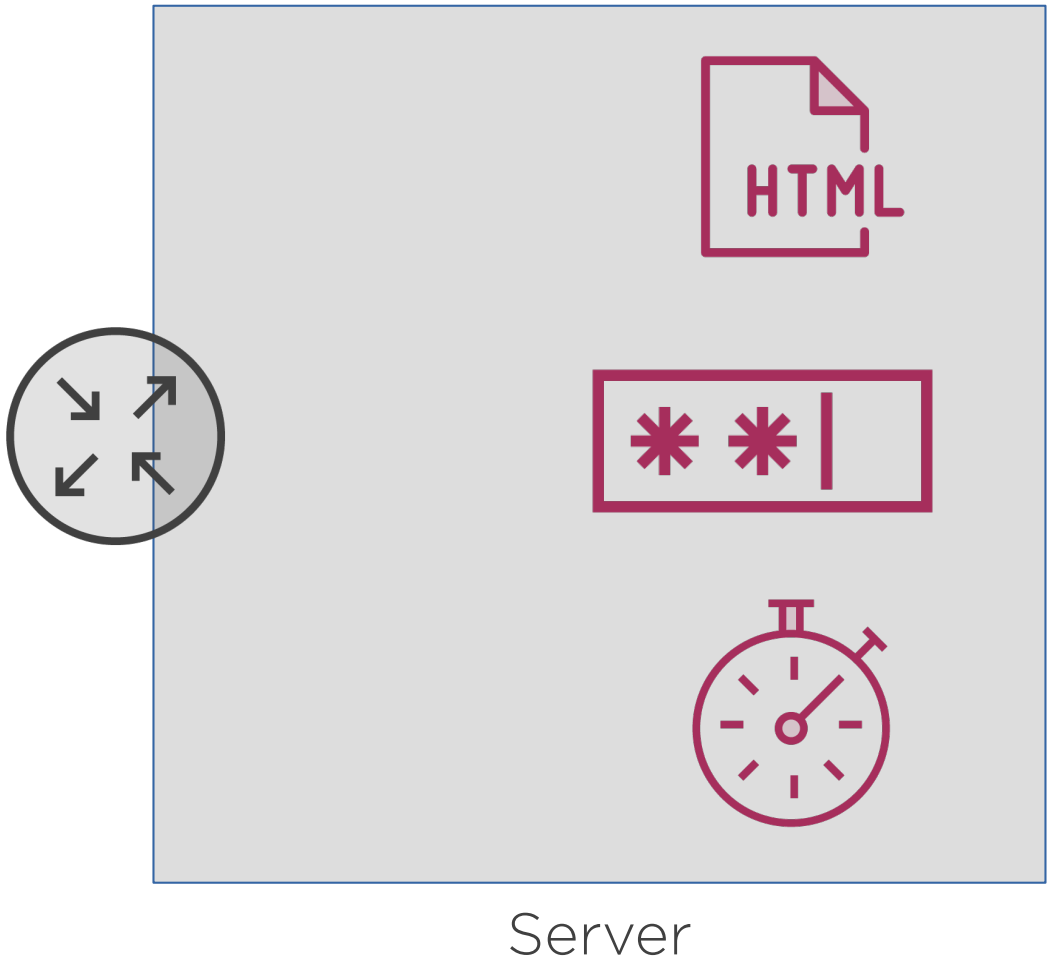
Network Ports



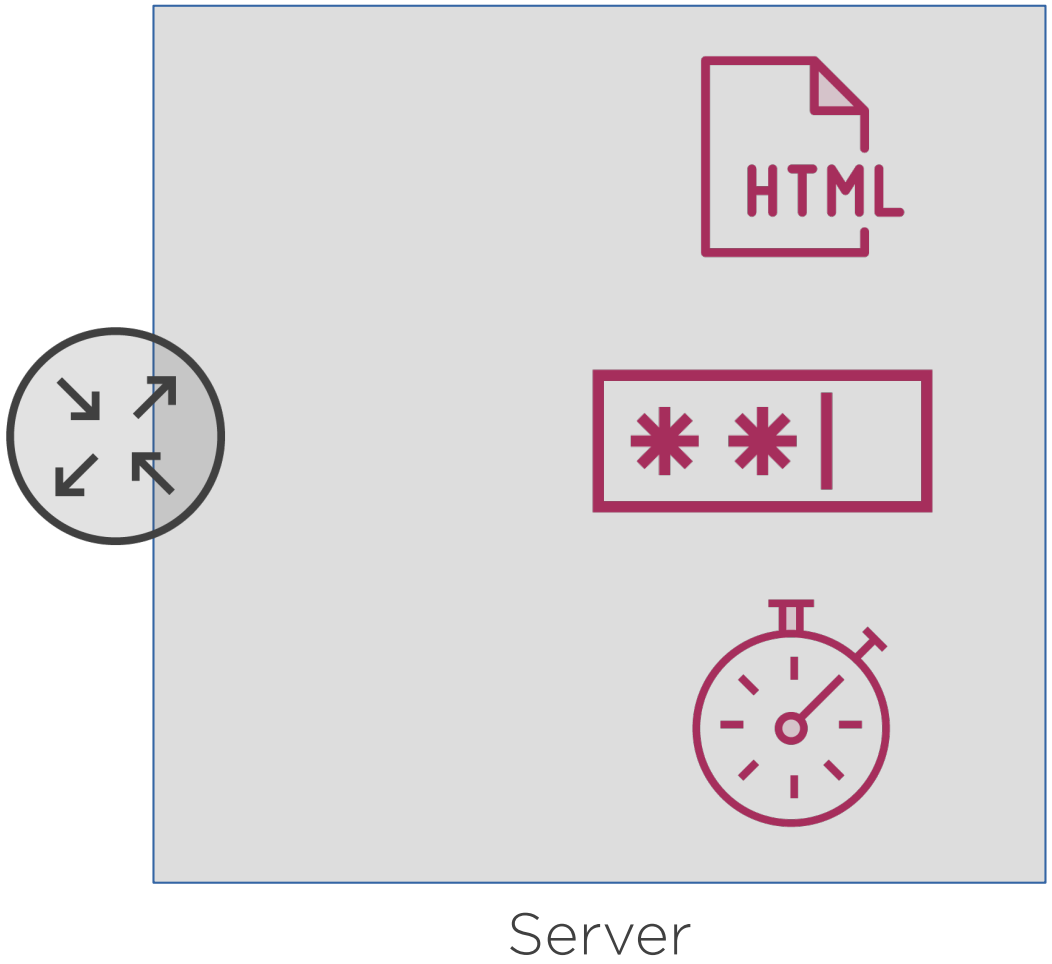
Network Ports



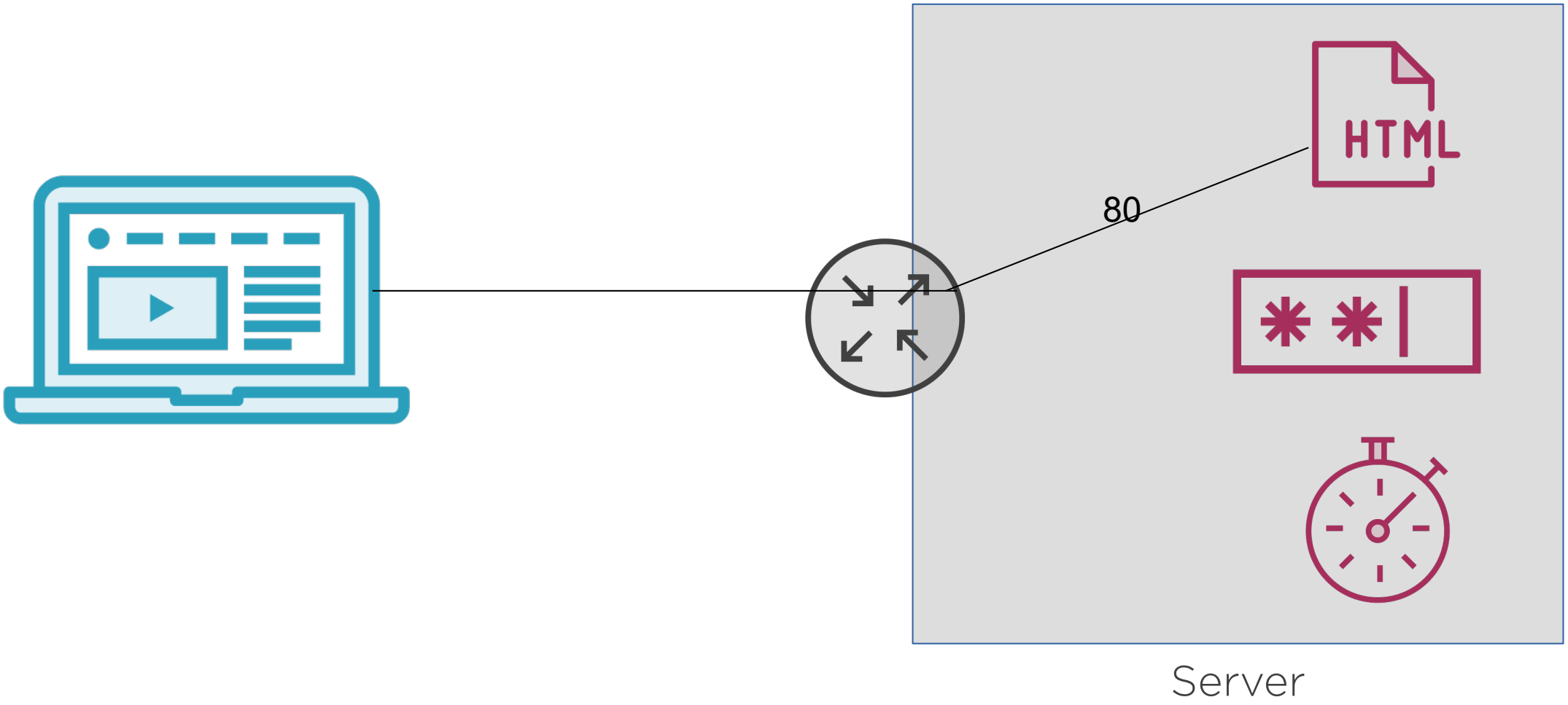
Network Ports



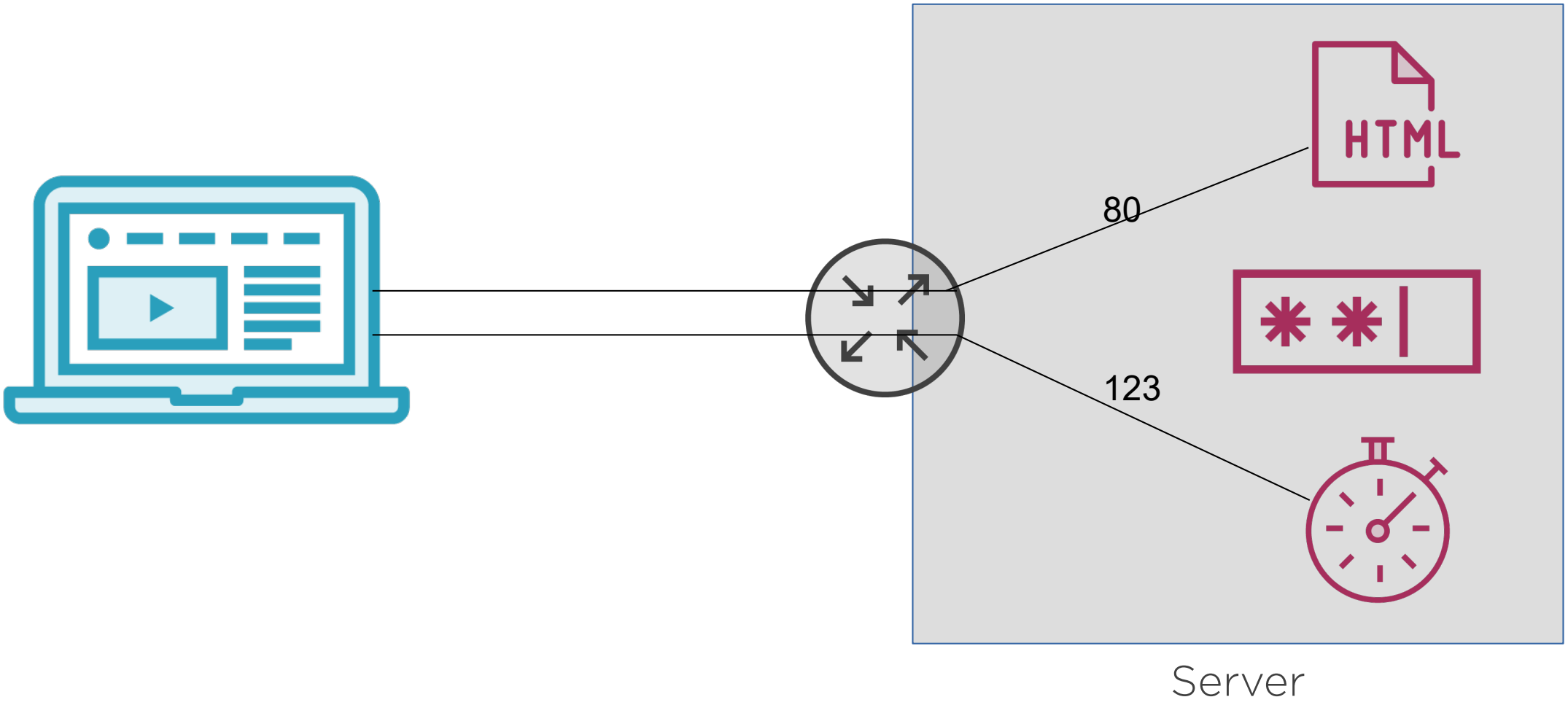
Network Ports



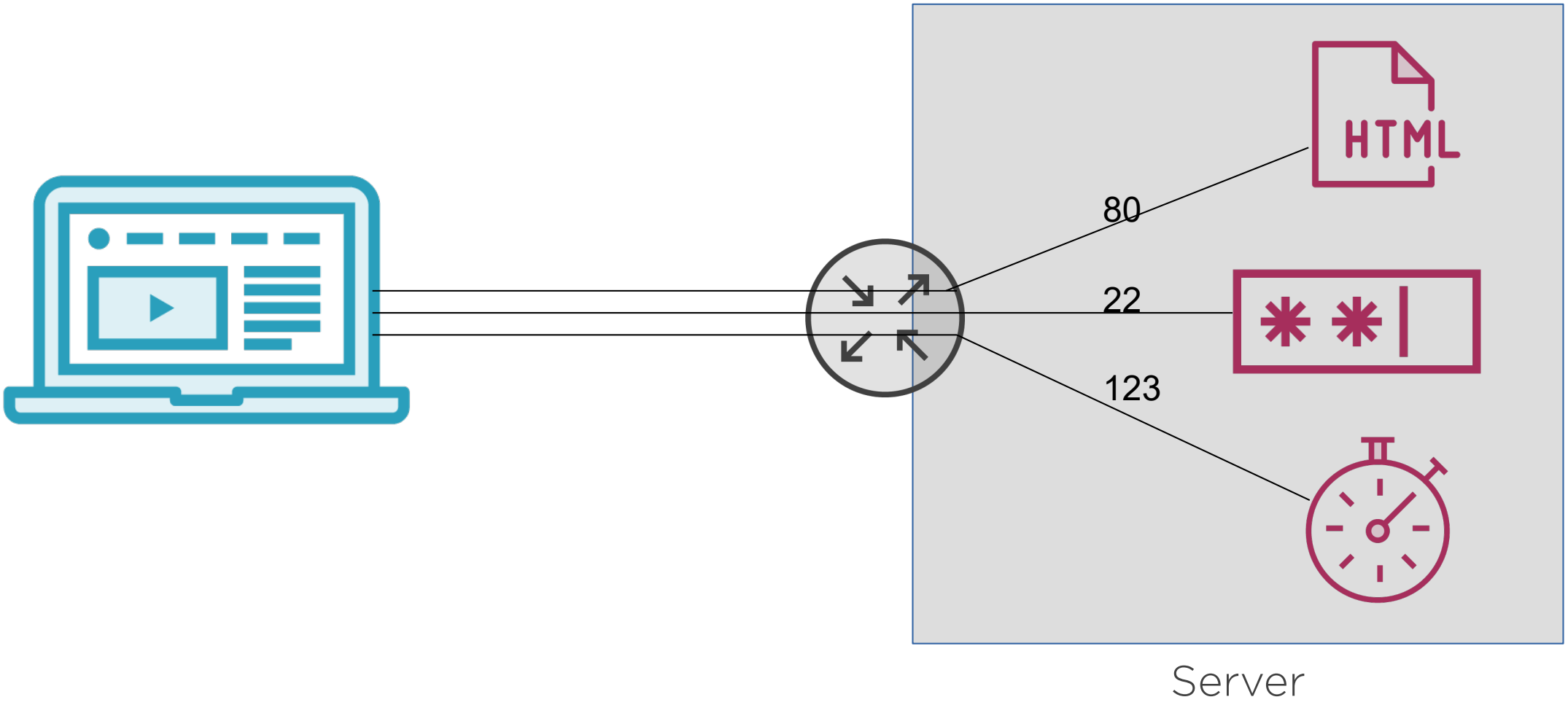
Network Ports



Network Ports



Network Ports



Service Access Controls

Service Hardening

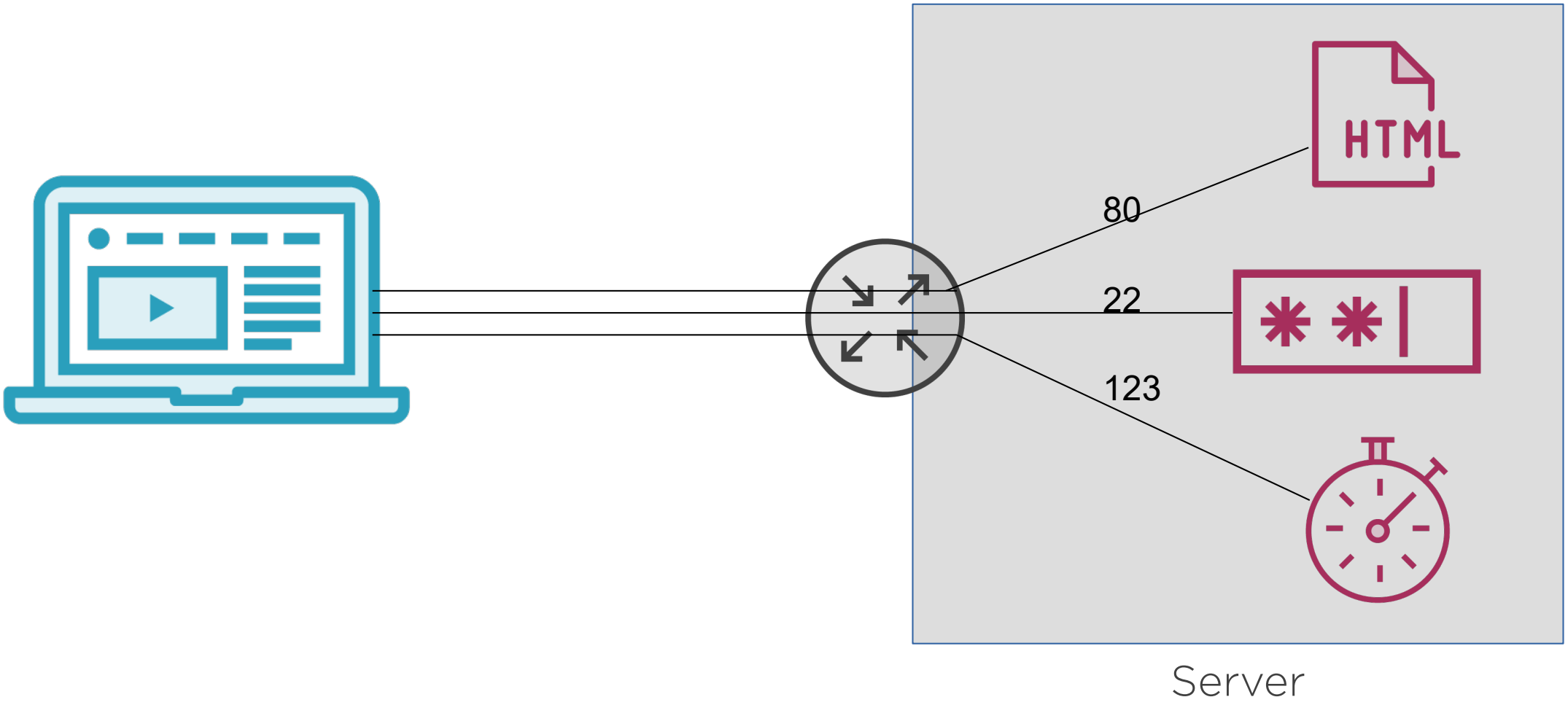
Port control

Firewall rules

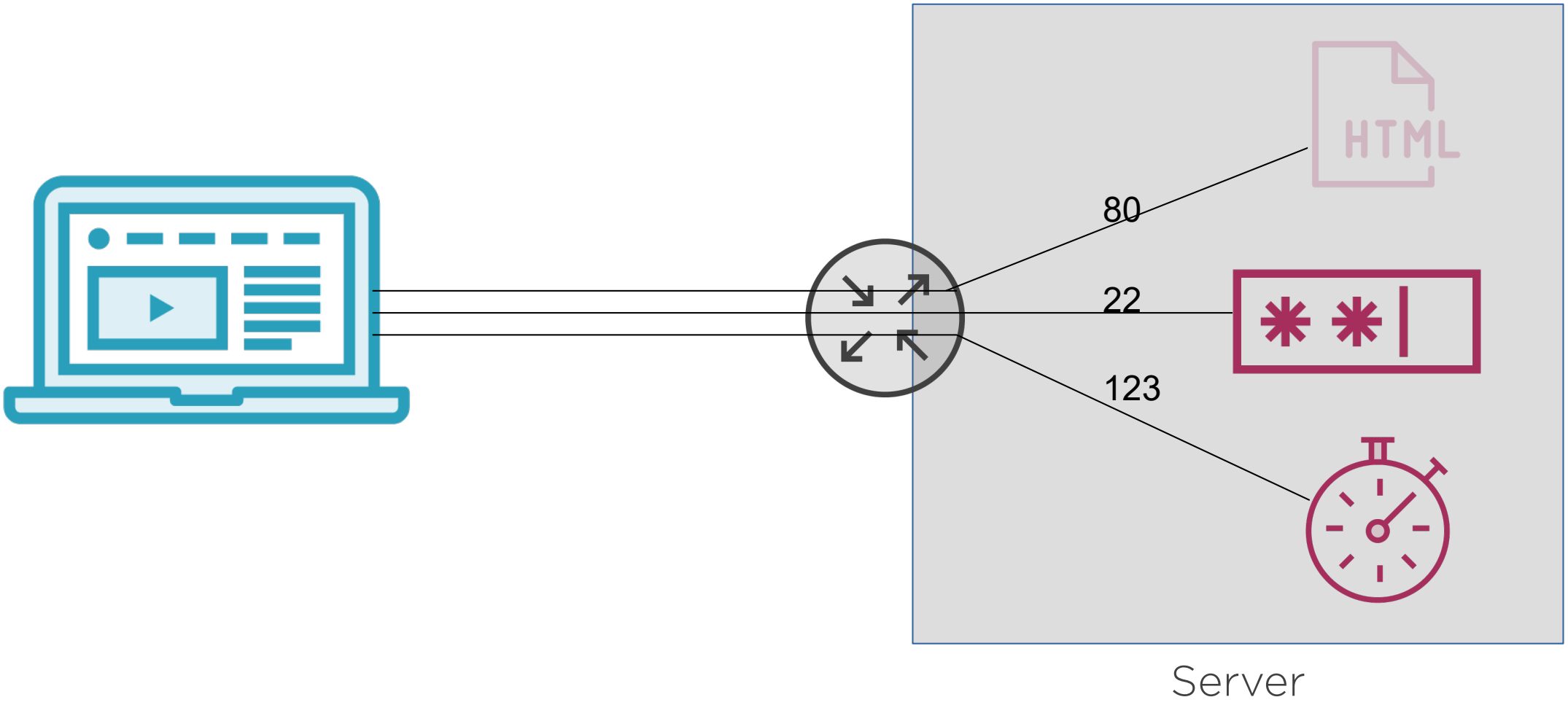
Service Access Controls

Service Access Controls

Network Ports

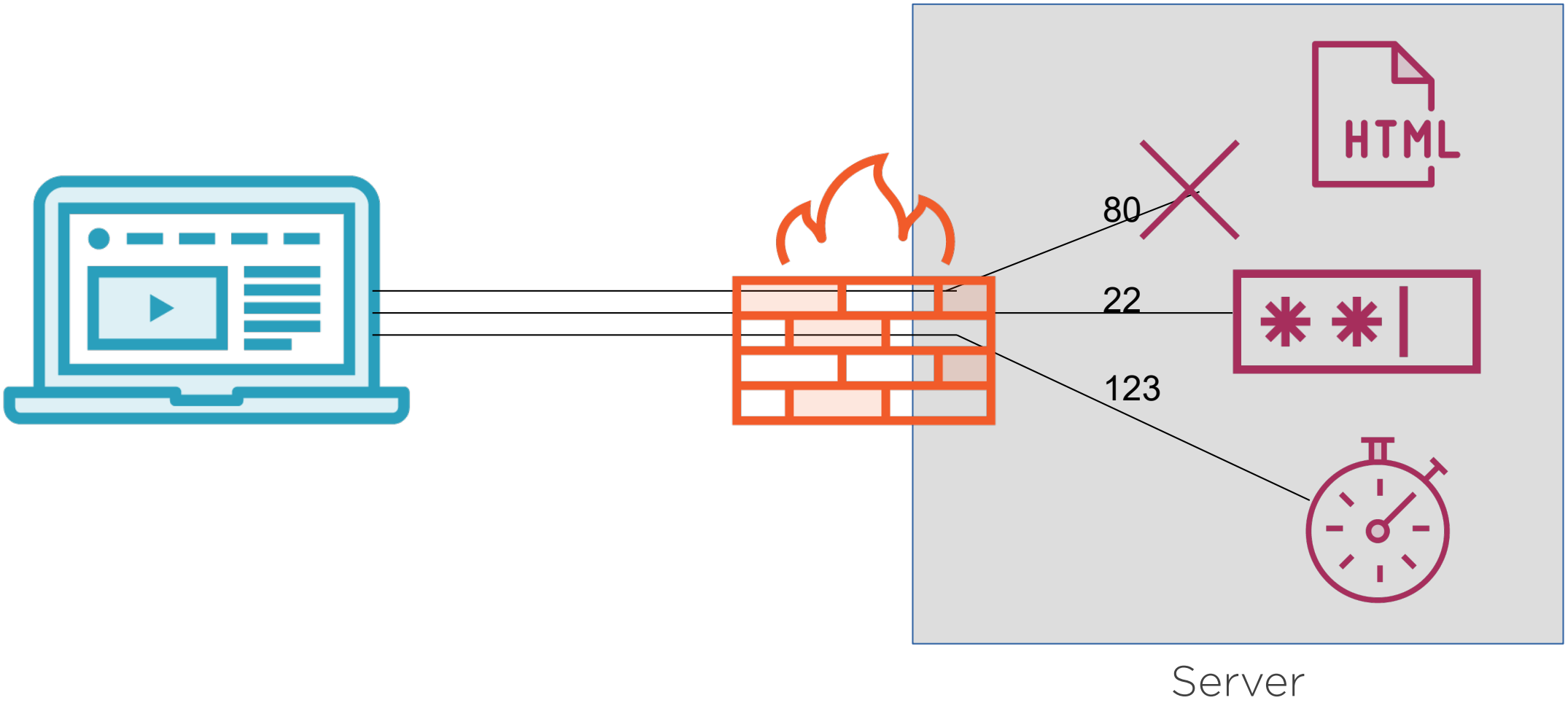


Network Ports



Service Access Controls

Firewall Filtering



Admin Powers: Best Practices

Avoid using the root account

Create unique accounts for each user

Assign only necessary authority to each user

Use admin power only via sudo

Data Encryption

Overview

Why encrypt

Overview

Why encrypt

Disk encryption

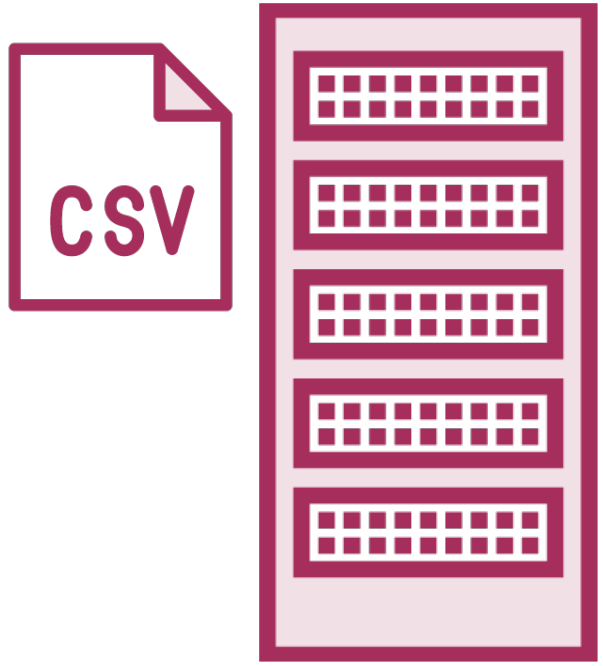
Overview

- Why encrypt
- Disk encryption
- SSL/TSL encryption

Overview

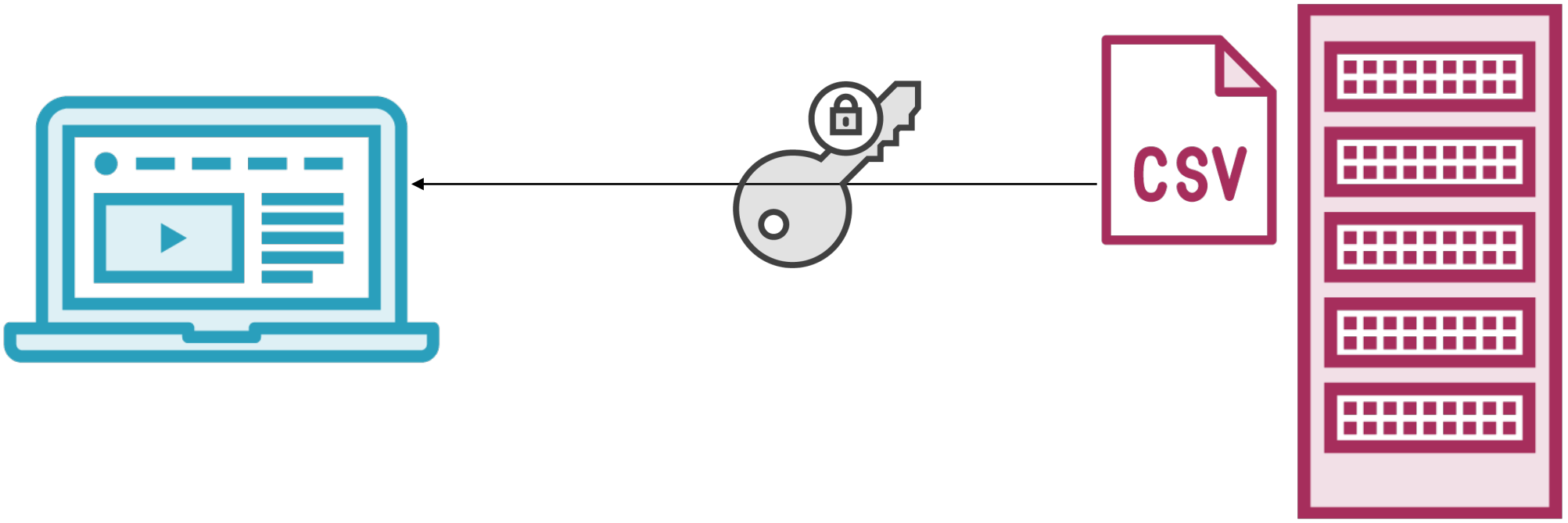
- Why encrypt
- Disk encryption
- SSL/TSL encryption
- Email encryption

Encryption

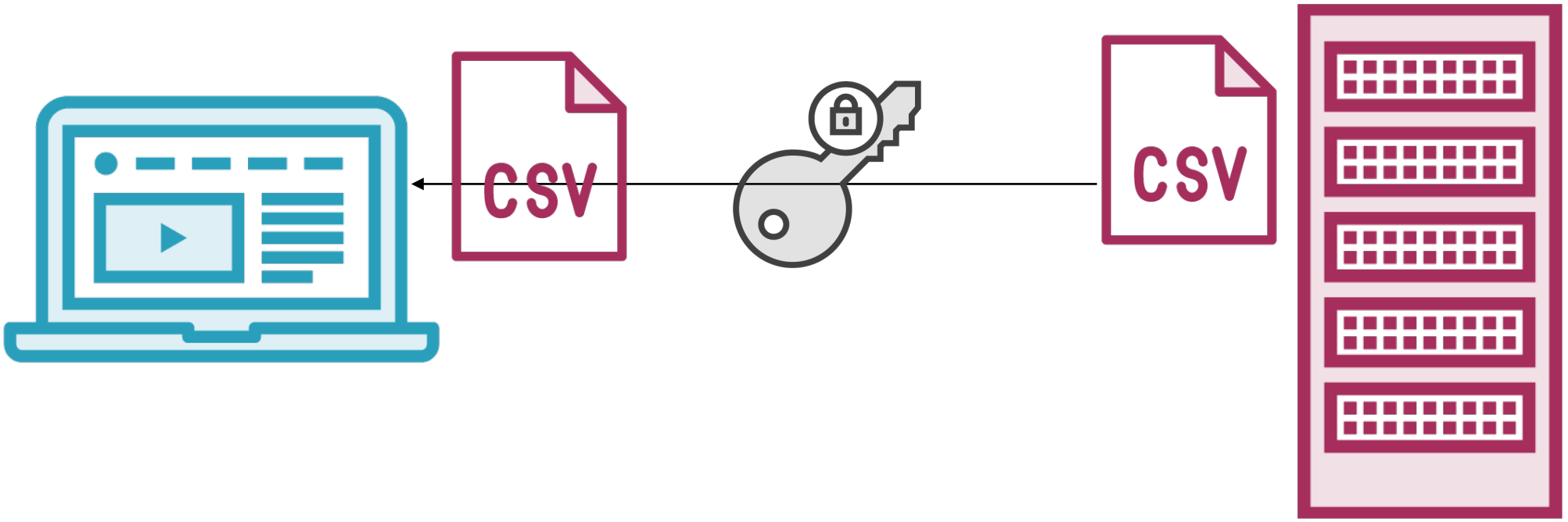


Encryption

Encryption



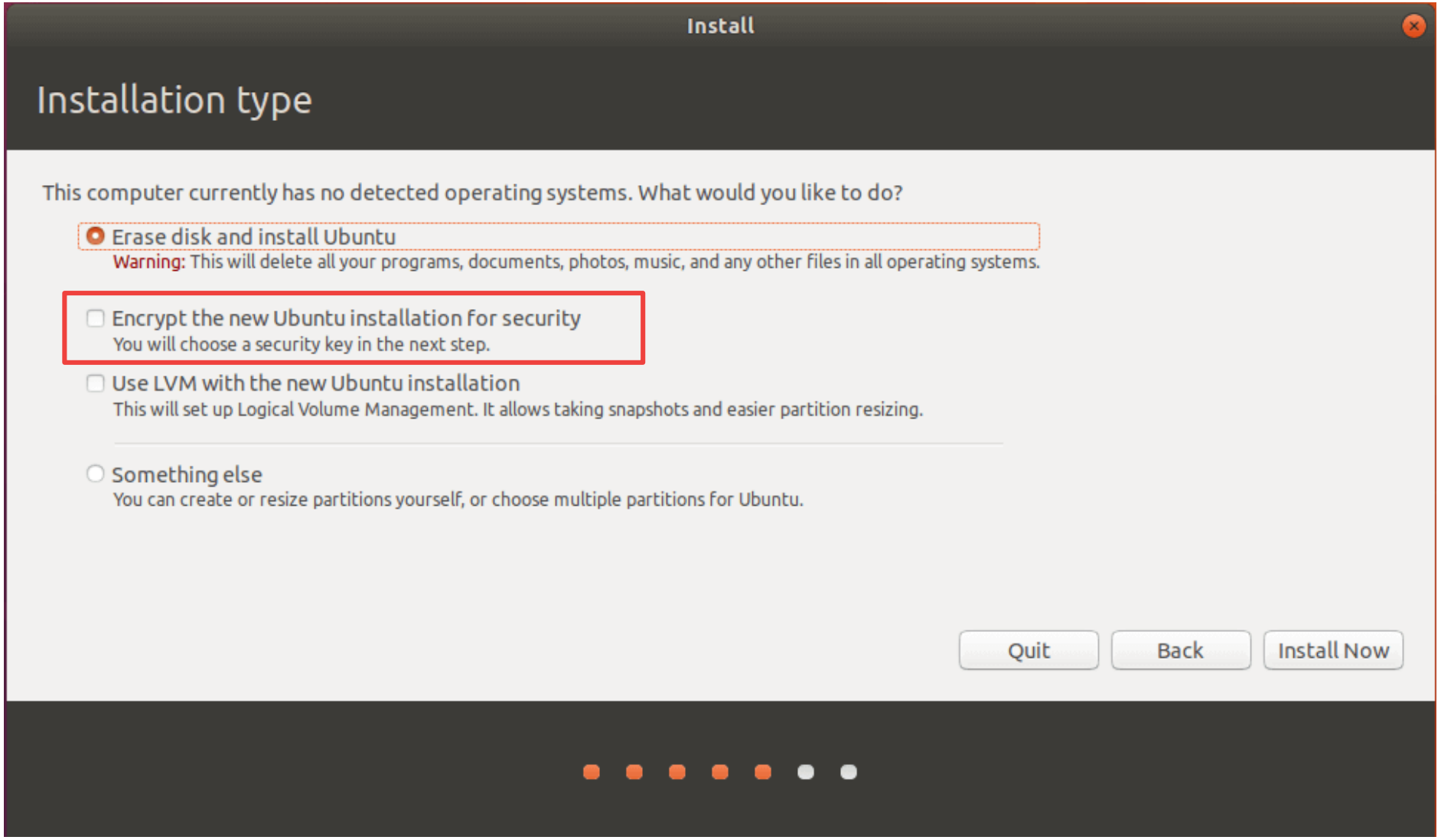
Encryption



Encryption

Encryption

Disk Encryption (Installation Choice)



TLS Encryption

Email Server Elements

Email Server Elements

Mail transport agent (MTA)

Postfix, Sendmail

Email Server Elements

Mail transport agent (MTA)

Postfix, Sendmail

Mail delivery agent (MDA)

Dovecot

Email Server Elements

Mail transport agent (MTA)

Postfix, Sendmail

Mail delivery agent (MDA)

Dovecot

Mail user agents (MUA)

Thunderbird

Review

drwxrwxr-x 2 root secret-group 4096 Jan 20

Review

Review

drwxrwxr-x 2 root secret-group 4096 Jan 20

$ chmod o+x data.txt

Review

drwxrwxr-x 2 root secret-group 4096 Jan 20

$ chmod o+x data.txt

chown ubuntu:secret-group /var/secret

Review

drwxrwxr-x 2 root secret-group 4096 Jan 20

$ chmod o+x data.txt

chown ubuntu:secret-group /var/secret

$ chmod 777 myfile

Review

drwxrwxr-x 2 root secret-group 4096 Jan 20

$ chmod o+x data.txt

chown ubuntu:secret-group /var/secret

$ chmod 777 myfile

chmod +s /var/secret

Review

drwxrwxr-x 2 root secret-group 4096 Jan 20

$ chmod o+x data.txt

chown ubuntu:secret-group /var/secret

$ chmod 777 myfile

chmod +s /var/secret

ln -s /home/ubuntu/scripts/myscript.sh \
/var/secret/data/

Review

drwxrwxr-x 2 root secret-group 4096 Jan 20

$ chmod o+x data.txt

chown ubuntu:secret-group /var/secret

$ chmod 777 myfile

chmod +s /var/secret

```
# ln -s /home/ubuntu/scripts/myscript.sh \
    /var/secret/data/
```

apt upgrade

Review

drwxrwxr-x 2 root secret-group 4096 Jan 20

$ chmod o+x data.txt

chown ubuntu:secret-group /var/secret

$ chmod 777 myfile

chmod +s /var/secret

```
# ln -s /home/ubuntu/scripts/myscript.sh \
    /var/secret/data/
```

apt upgrade

$ nmap -v -sT localhost

Review

drwxrwxr-x 2 root secret-group 4096 Jan 20

$ chmod o+x data.txt

chown ubuntu:secret-group /var/secret

$ chmod 777 myfile

chmod +s /var/secret

```
# ln -s /home/ubuntu/scripts/myscript.sh \
    /var/secret/data/
```

apt upgrade

$ nmap -v -sT localhost

systemctl disable apache2

Review

drwxrwxr-x 2 root secret-group 4096 Jan 20

$ chmod o+x data.txt

chown ubuntu:secret-group /var/secret

$ chmod 777 myfile

chmod +s /var/secret

```
# ln -s /home/ubuntu/scripts/myscript.sh \
    /var/secret/data/
```

apt upgrade

$ nmap -v -sT localhost

systemctl disable apache2

Data encryption