SECUREDROP

SecureDrop Workstation:

Handling unsafe documents safely

LibrePlanet, 2021

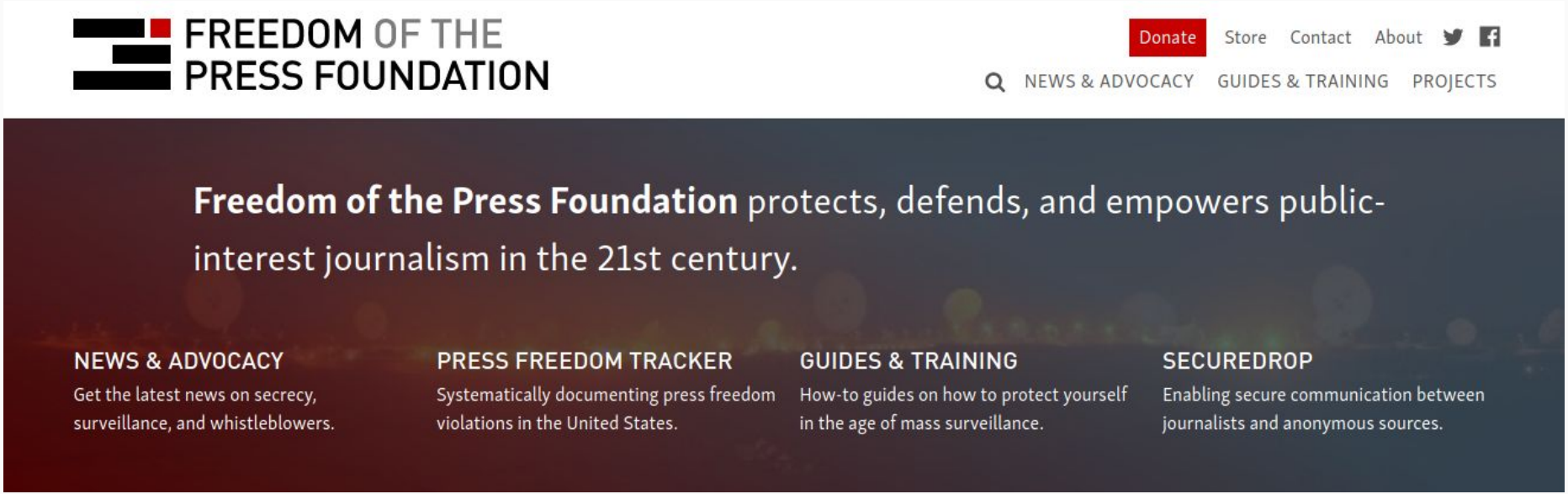
Conor Schaefer
Chief Technology Officer, Freedom of the Press Foundation

[META] Overview

- Intro
  - About FPF
  - About PFT
- SecureDrop
  - What it is
  - Who uses it
  - Motivations
  - How it works
    - Arch diagram
    - Highlight journo area
- Workstation
  - Before, in Tails, photo of airgap
  - Now, in Qubes
  - Xen arch diag (from Jen)
- Benefits:
  - Updates
  - Tooling
  - Real-time comms
- Audit review
  - “SecureDrop Workstation system represents a complex but well researched product that has been thoughtfully designed”
- Next steps
- Audit

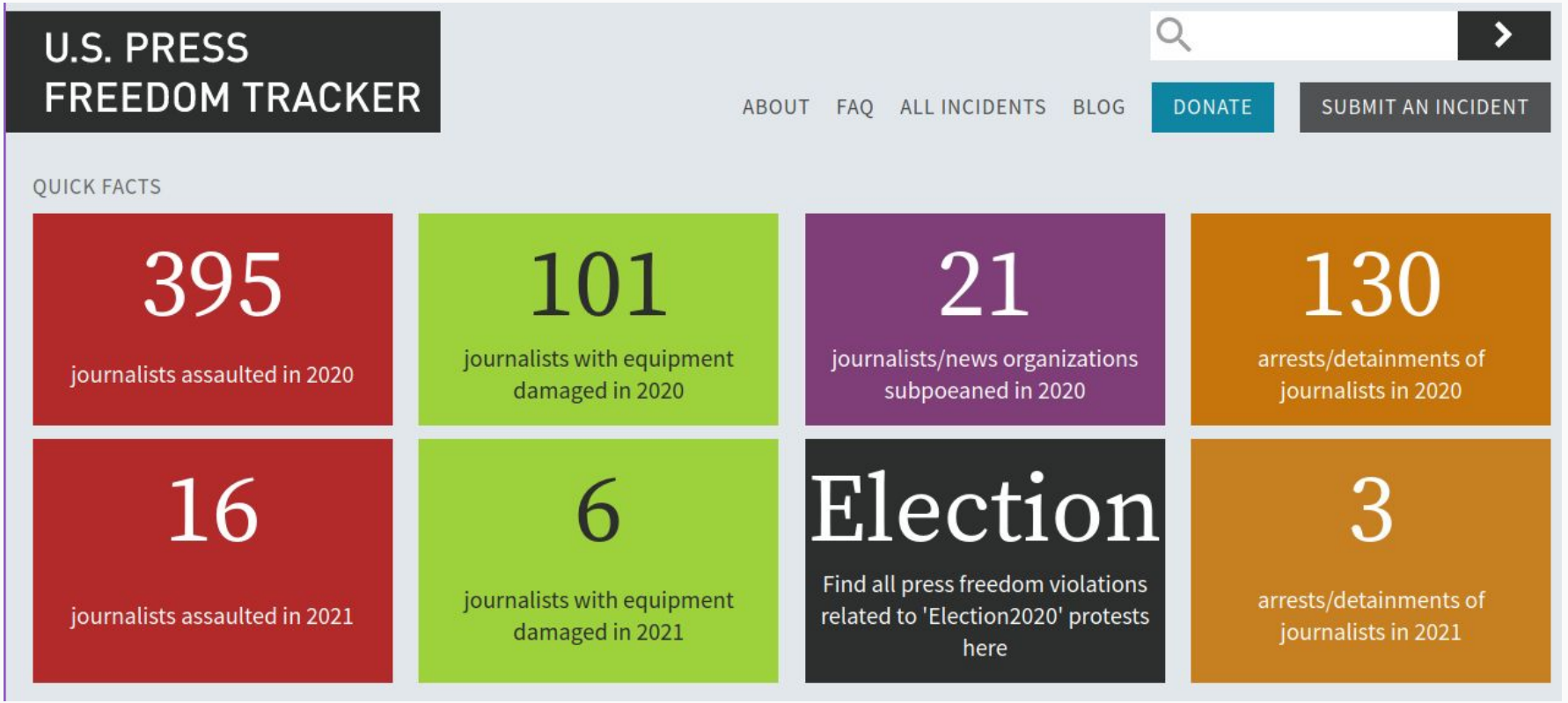
Overview

- Intro, about FPF
- SecureDrop
  - What it is
  - Who uses it
  - Motivations
  - How it works today
- Workstation
  - Qubes OS
  - How isolation works
  - Pilot program
- Security audit
- Next steps


FREEDOM OF THE PRESS FOUNDATION
Donate
Store
Contact
About
NEWS & ADVOCACY
GUIDES & TRAINING
PROJECTS
Freedom of the Press Foundation protects, defends, and empowers public-interest journalism in the 21st century.
NEWS & ADVOCACY
Get the latest news on secrecy, surveillance, and whistleblowers.
PRESS FREEDOM TRACKER
Systematically documenting press freedom violations in the United States.
GUIDES & TRAINING
How-to guides on how to protect yourself in the age of mass surveillance.
SECUREDROP
Enabling secure communication between journalists and anonymous sources.

US Press Freedom Tracker

https://pressfreedomtracker.us



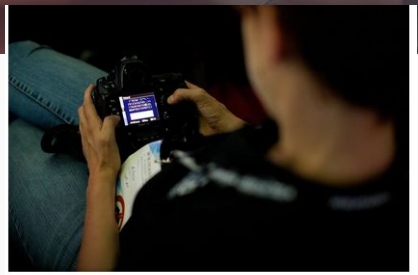
Guides & Training

Our training team delivers digital security trainings to news organizations, freelance and citizen journalists, and other at-risk groups. With education and advocacy, we aim to protect press freedoms through the adoption of the tools and practices included in our trainings.

FROM FPF

What to do if your phone is seized by police

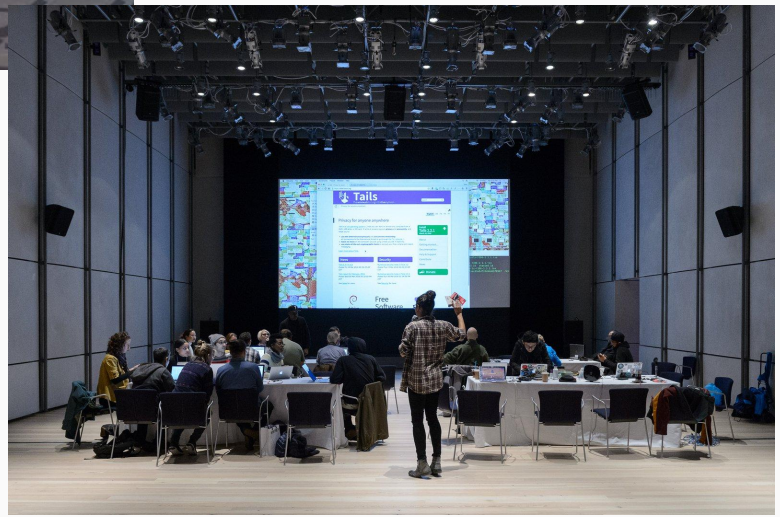
So, you've been arrested at an event. You're taken to the police station and your phone is confiscated. When you're let out, you realize someone has gone through your digital belongings. What now?



FROM FPF

Everything you wanted to know about media metadata, but were afraid to ask

Take a crash course in some of the tools you can use to analyze, manipulate, and scrub media metadata.



SecureDrop is an online whistleblowing platform, hosted on-premise by news organizations. It uses Tor Onion services for anonymity and GPG for encryption. The code is free software, under the AGPL.

Some of the organizations that currently use SecureDrop

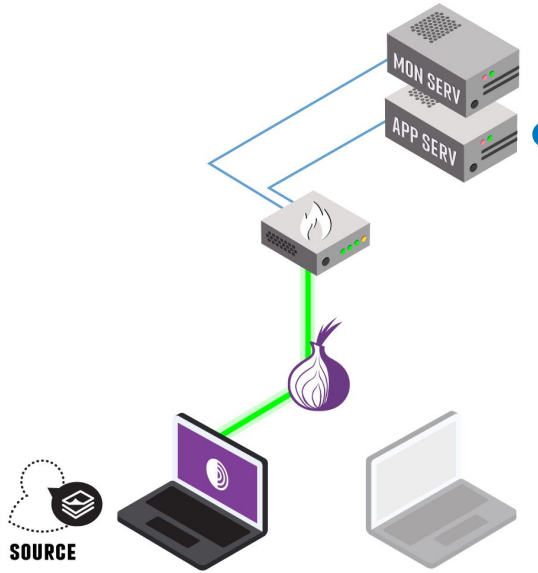
SECUREDROP

Why?

Motivations for SecureDrop

- Journalists have an inherently risky job
- Not every source is Ed Snowden!
- Free software implementation provides a stable, well-reviewed solution

How it works

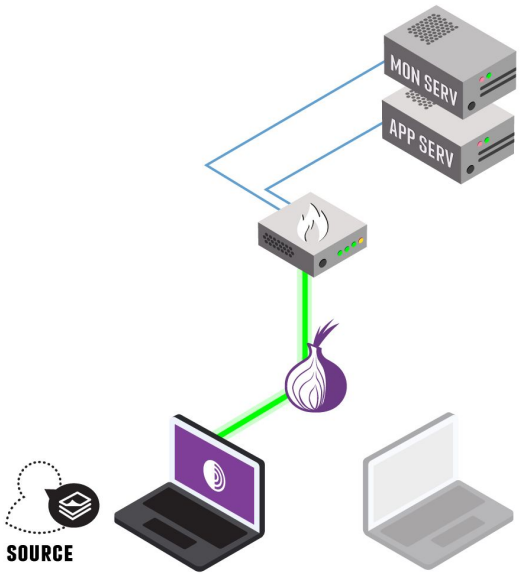


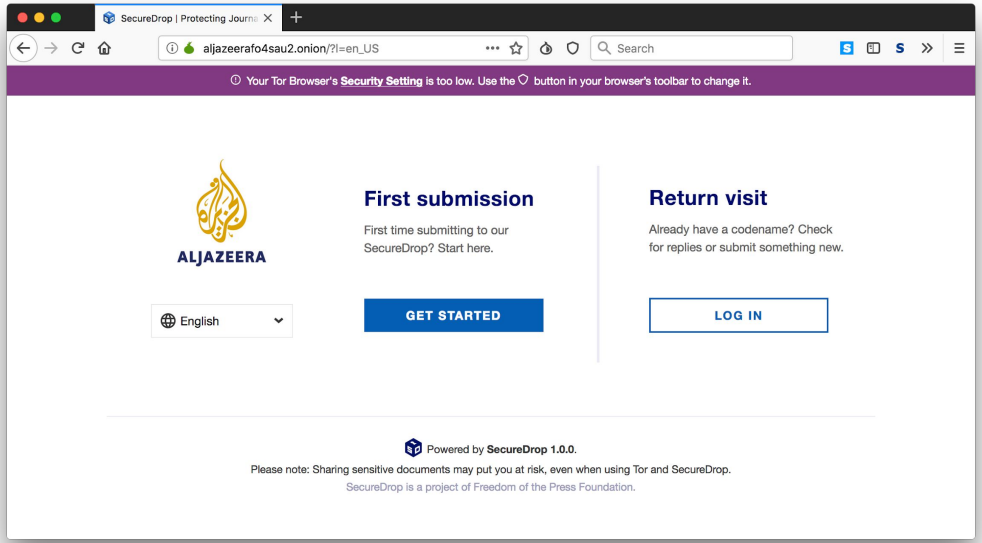
Application server: Runs two Python web applications (one for sources, one for journalists) exposed via Tor Onion Services.

Source Interface: Public v3 Onion URL, accessible by anyone in Tor Browser

Journalist Interface: Authenticated v3 Onion URL. Requires key-based auth to resolve. Only accessible to journalists.

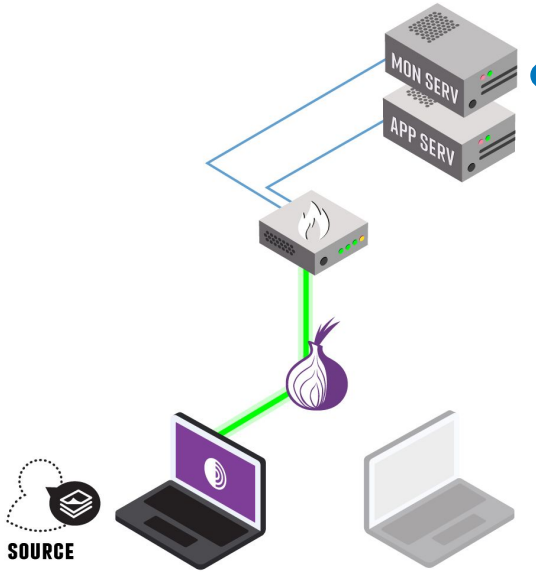
SECUREDROP





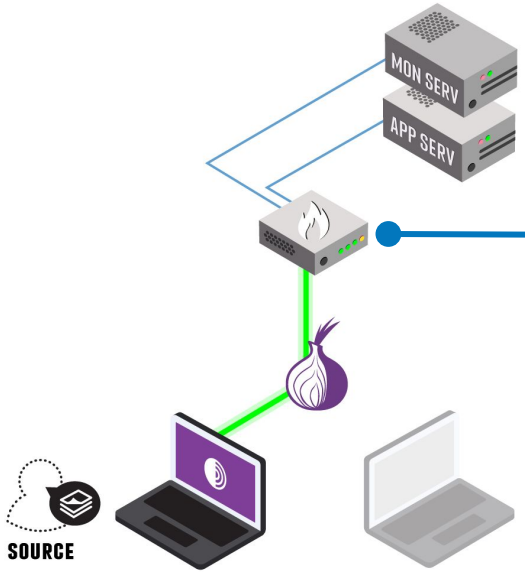
What the source sees

SECUREDROP



Monitoring server: Runs a host-based IDS (OSSEC) to monitor the application server and send alerts to administrators

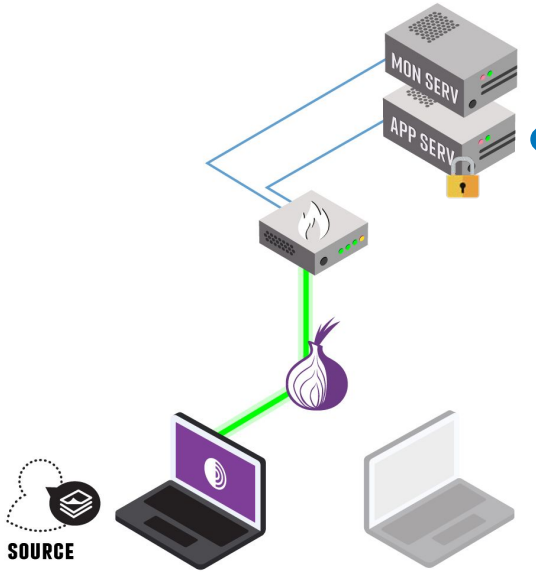
SECUREDROP



Network firewall: pfSense used to isolate the SecureDrop area of the network from the rest of the news organization

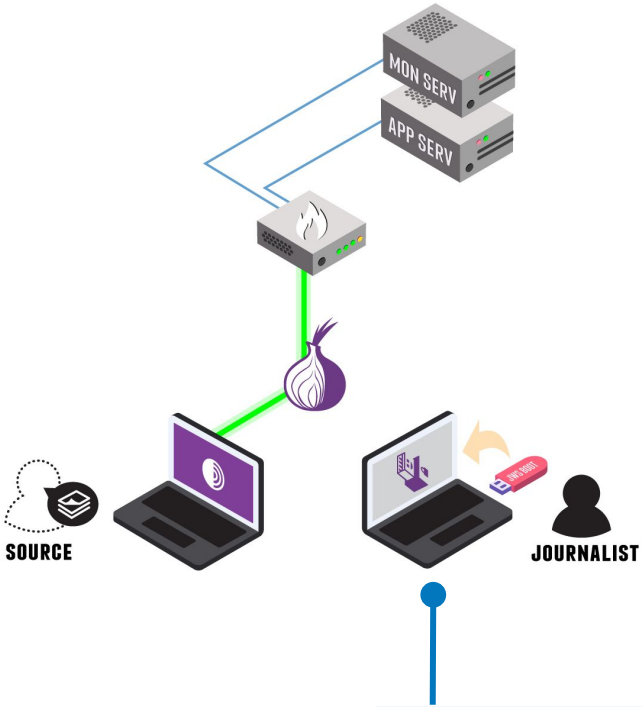
Drops all inbound traffic, except established/related. Tor Onions provide NAT-punching.

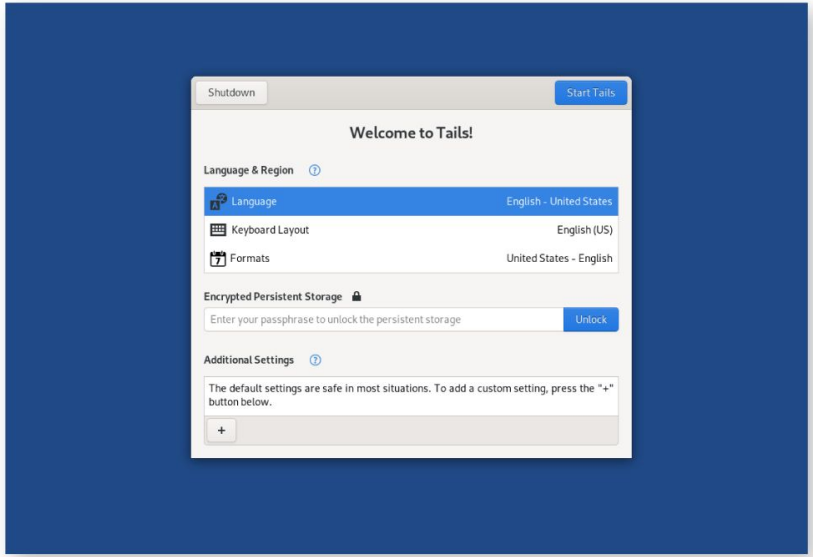
SECUREDROP



Documents stored encrypted to the instance's public key

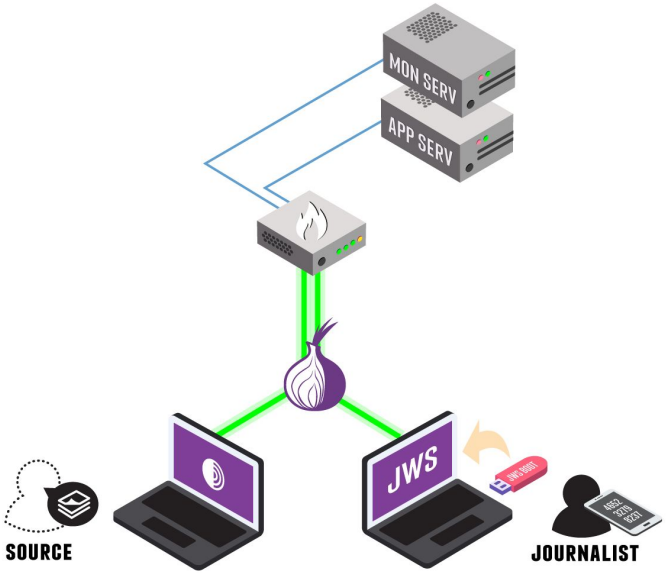
SECUREDROP

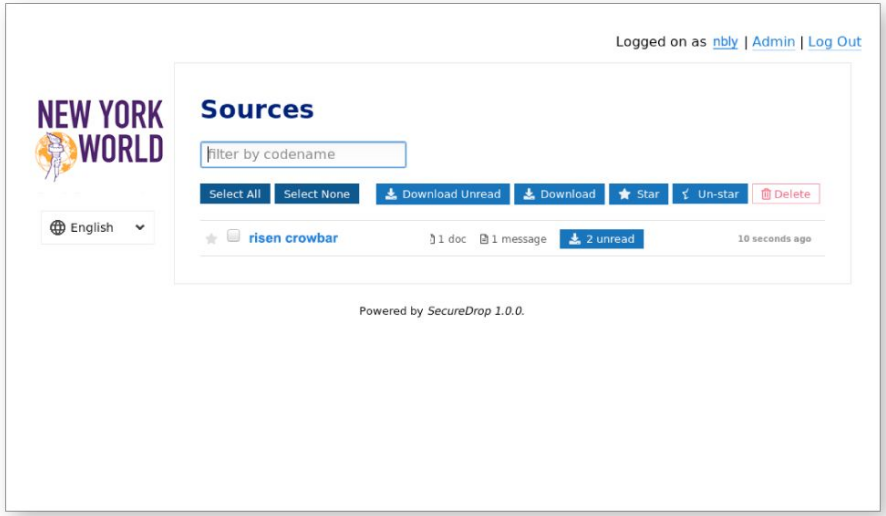




Journalists log in to Tails OS

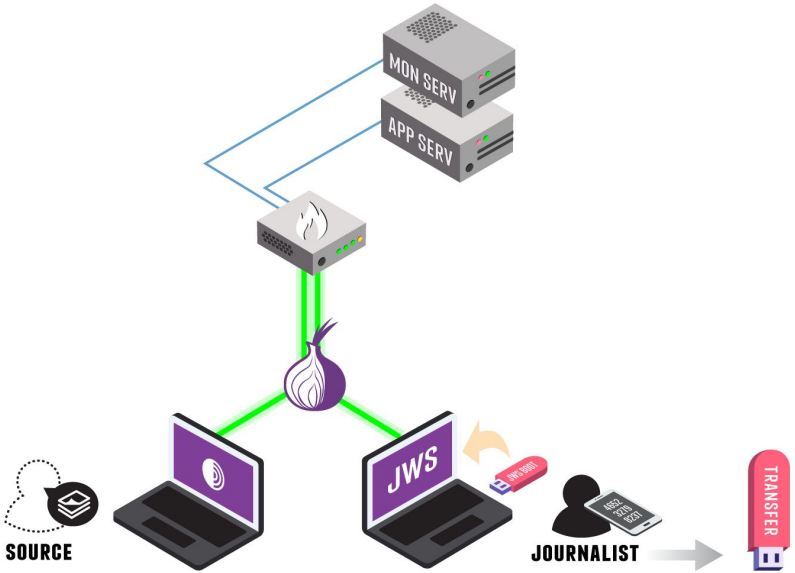
SECUREDROP

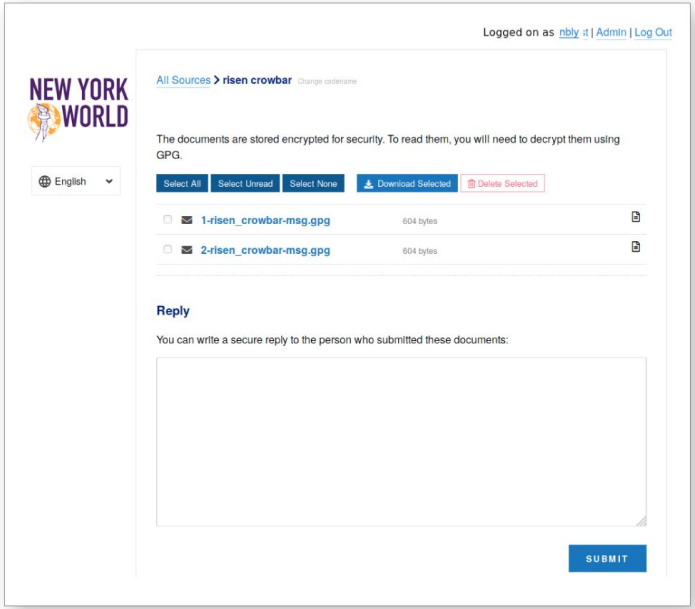




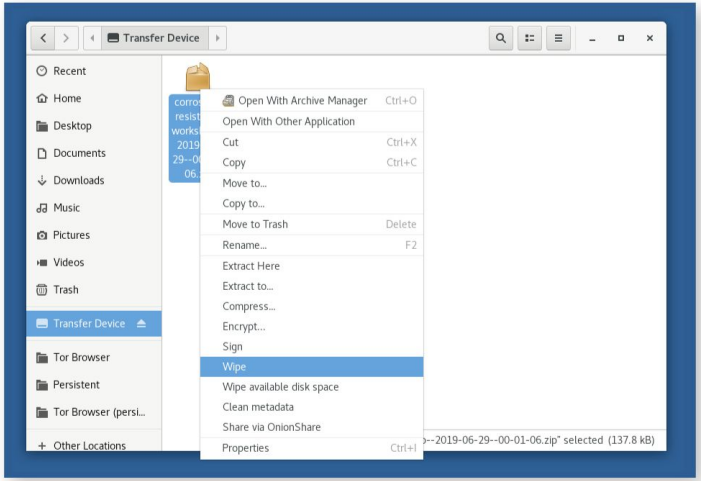
What the journalist sees

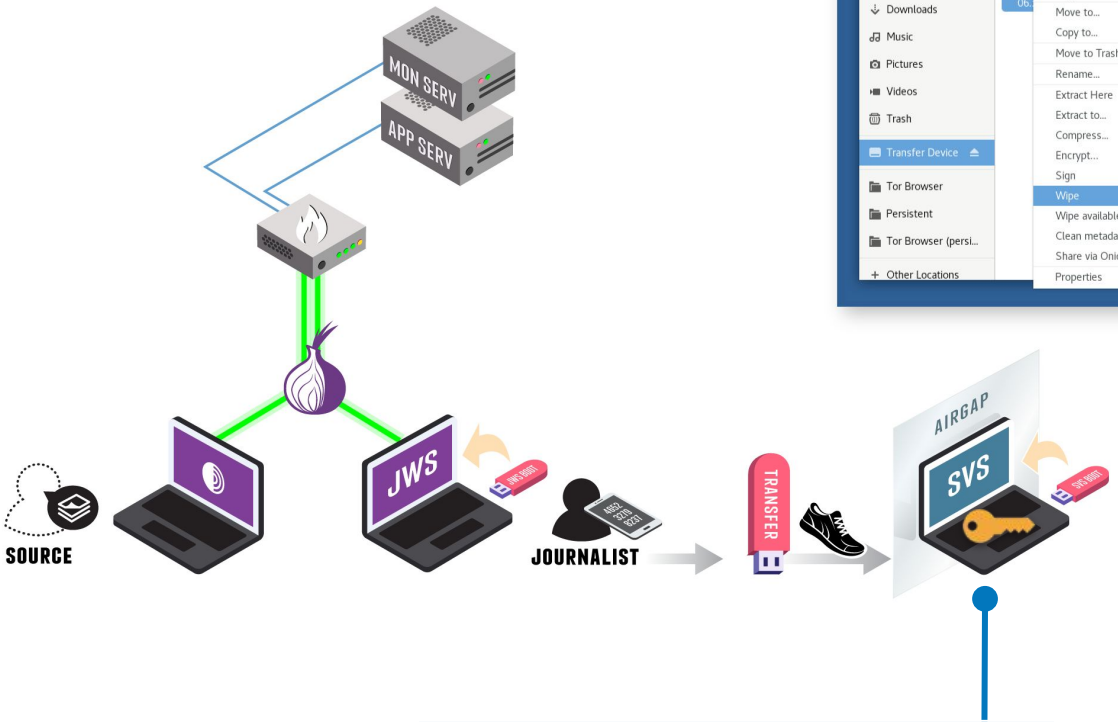
SECUREDROP


MON SERV
APP SERV
JWS
SOURCE
JOURNALIST
TRANSFER


Logged on as nbly it | Admin | Log Out
NEW YORK WORLD
All Sources > risen crowbar Change codename
The documents are stored encrypted for security. To read them, you will need to decrypt them using GPG.
English
Select All
Select Unread
Select None
Download Selected
Delete Selected
1-risen_crowbar-msg.gpg 604 bytes
2-risen_crowbar-msg.gpg 604 bytes
Reply
You can write a secure reply to the person who submitted these documents:
SUBMIT

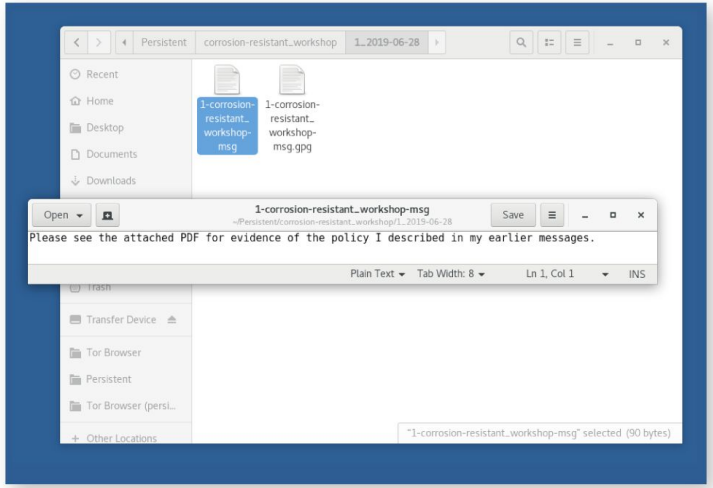
SECUREDROP

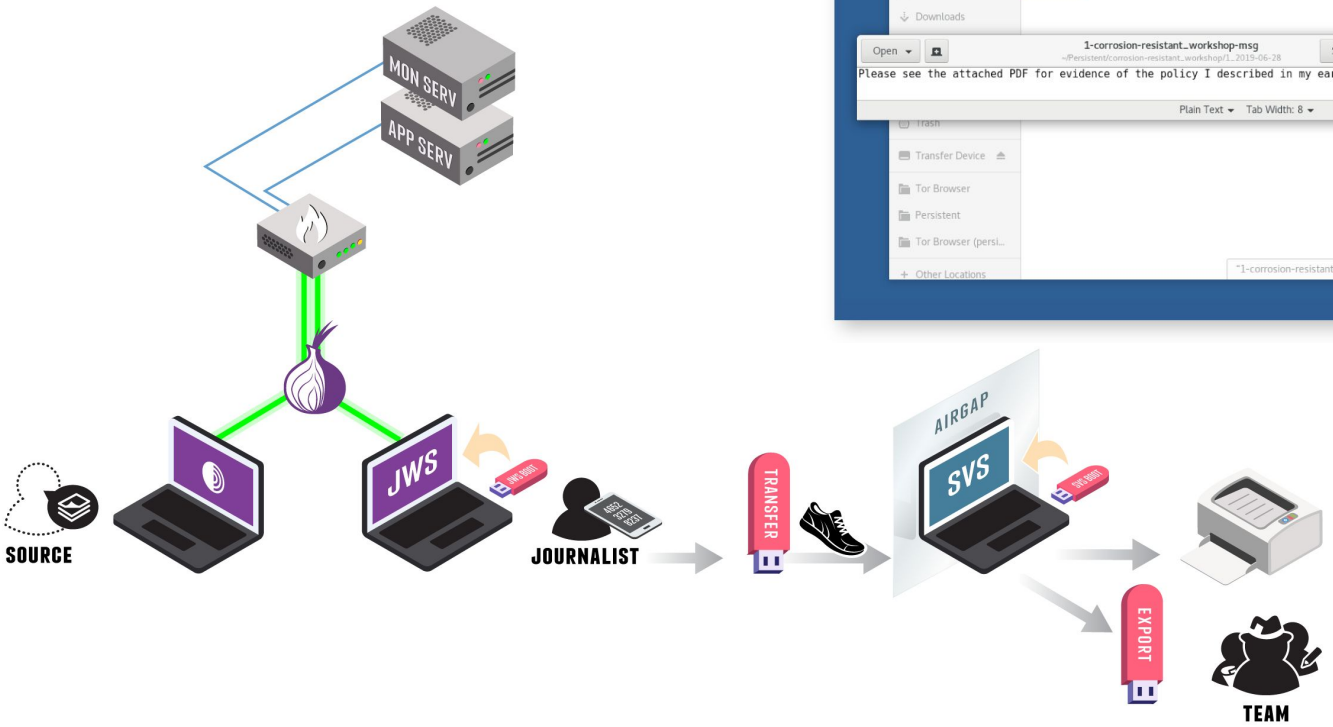




Private key to decrypt documents only in the air-gap environment.

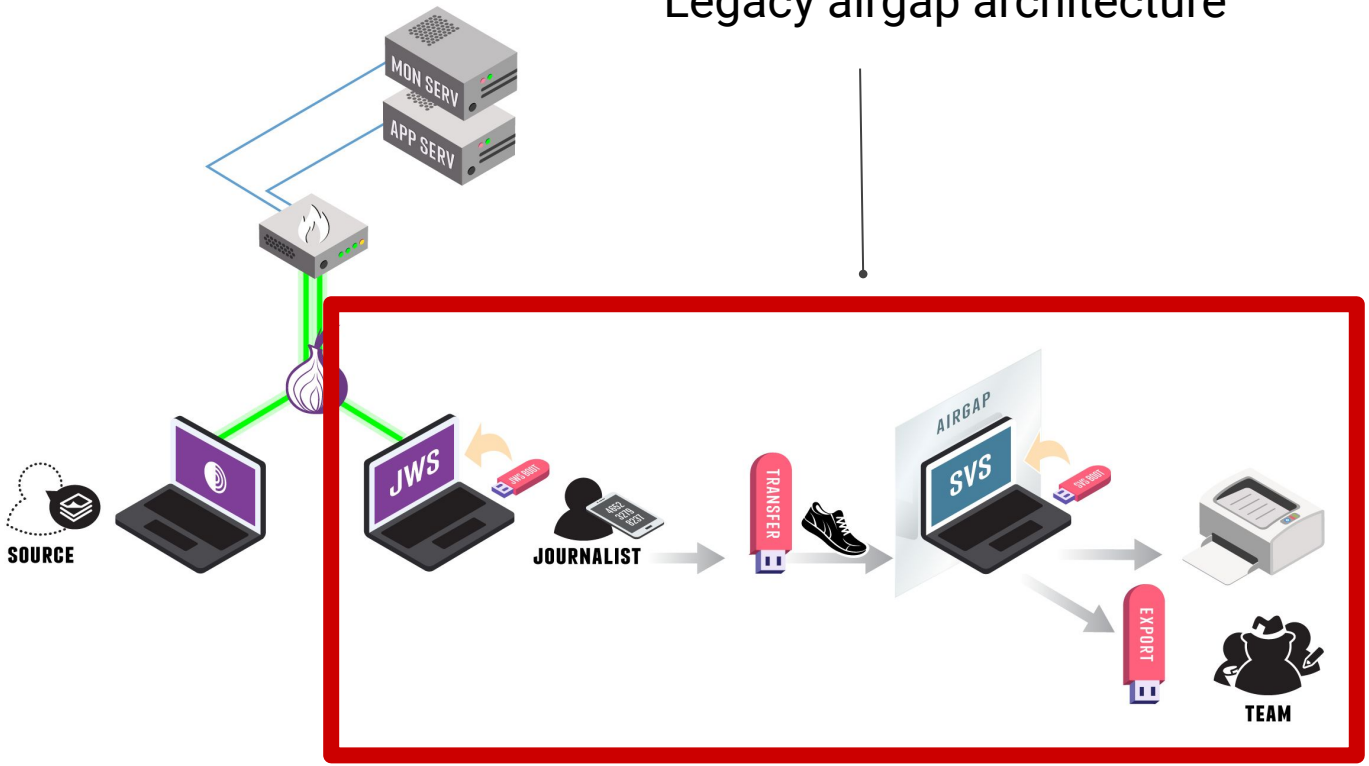
SECUREDROP


Persistent
corrosion-resistant_workshop
1_2019-06-28
Recent
Home
Desktop
Documents
Downloads
1-corrosion-resistant_workshop-msg
1-corrosion-resistant_workshop-msg.gpg
Open
1-corrosion-resistant_workshop-msg
~/Persistent/corrosion-resistant_workshop/1_2019-06-28
Save
Please see the attached PDF for evidence of the policy I described in my earlier messages.
Plain Text
Tab Width: 8
Ln 1, Col 1
INS
Trash
Transfer Device
Tor Browser
Persistent
Tor Browser (persi...
Other Locations
"1-corrosion-resistant_workshop-msg" selected (90 bytes)


MON SERV
APP SERV
JWS
SOURCE
JOURNALIST
TRANSFER
AIRGAP
SVS
EXPORT
TEAM

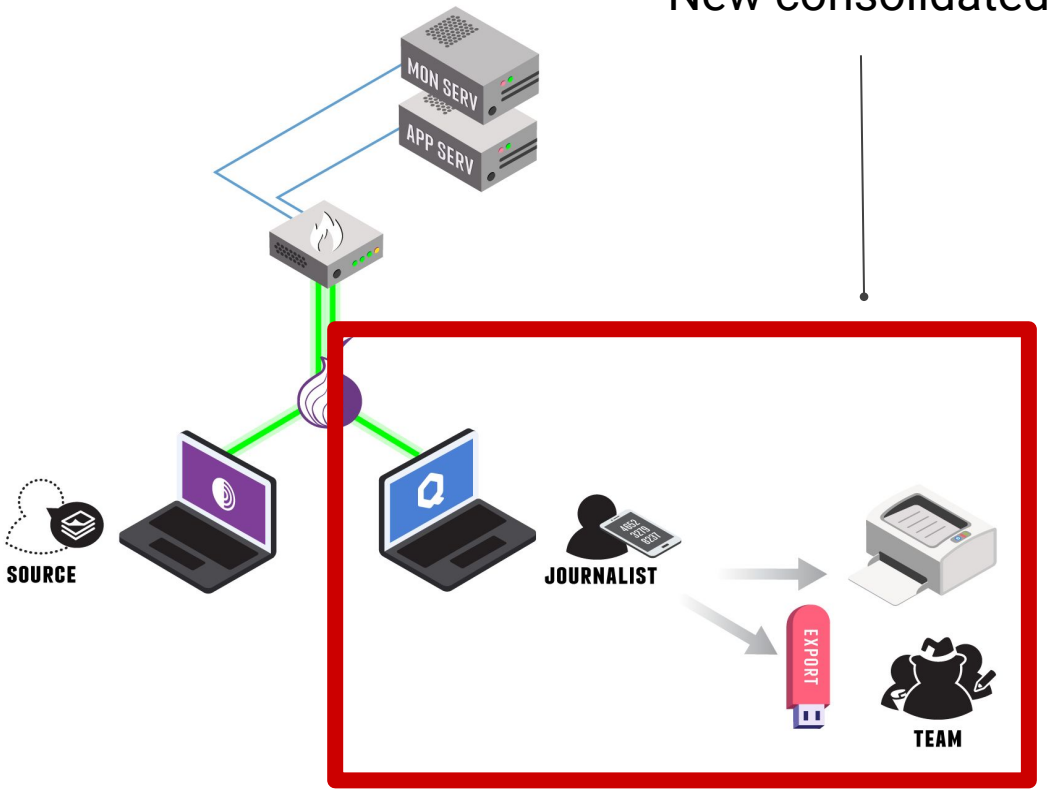
SECUREDROP

Legacy airgap architecture



SECUREDROP

New consolidated architecture



SECUREDROP

SecureDrop Workstation

Motivations for SecureDrop Workstation

- Existing workflows are slow (~1 hour round-trip)
- It's hard to patch an airgapped system
- Airgap is not perfect isolation
- Journalists need more tools than just viewing

Qubes OS

- Hypervisor-based isolation, via Xen
- Template & disposable environments to combat malware persistence
- Strict controls for inter-VM communication

How Qubes OS works

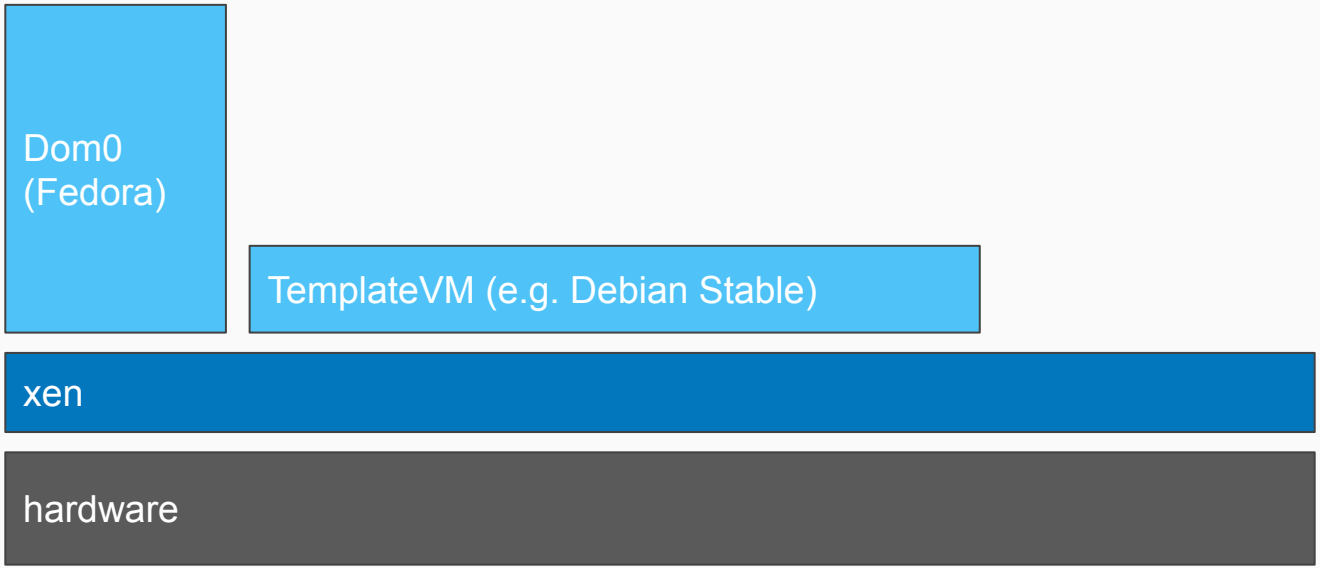
Qubes OS: single-user desktop-based Xen distribution

hardware

Qubes OS: single-user desktop-based Xen distribution

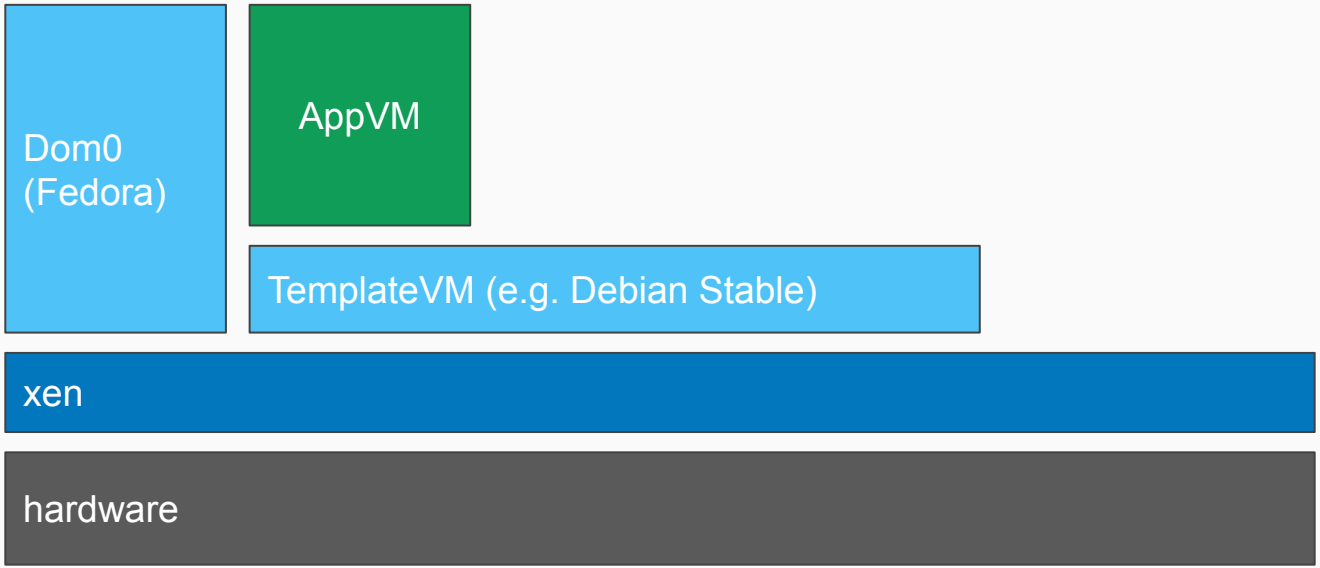
Qubes OS: single-user desktop-based Xen distribution

Qubes OS: single-user desktop-based Xen distribution

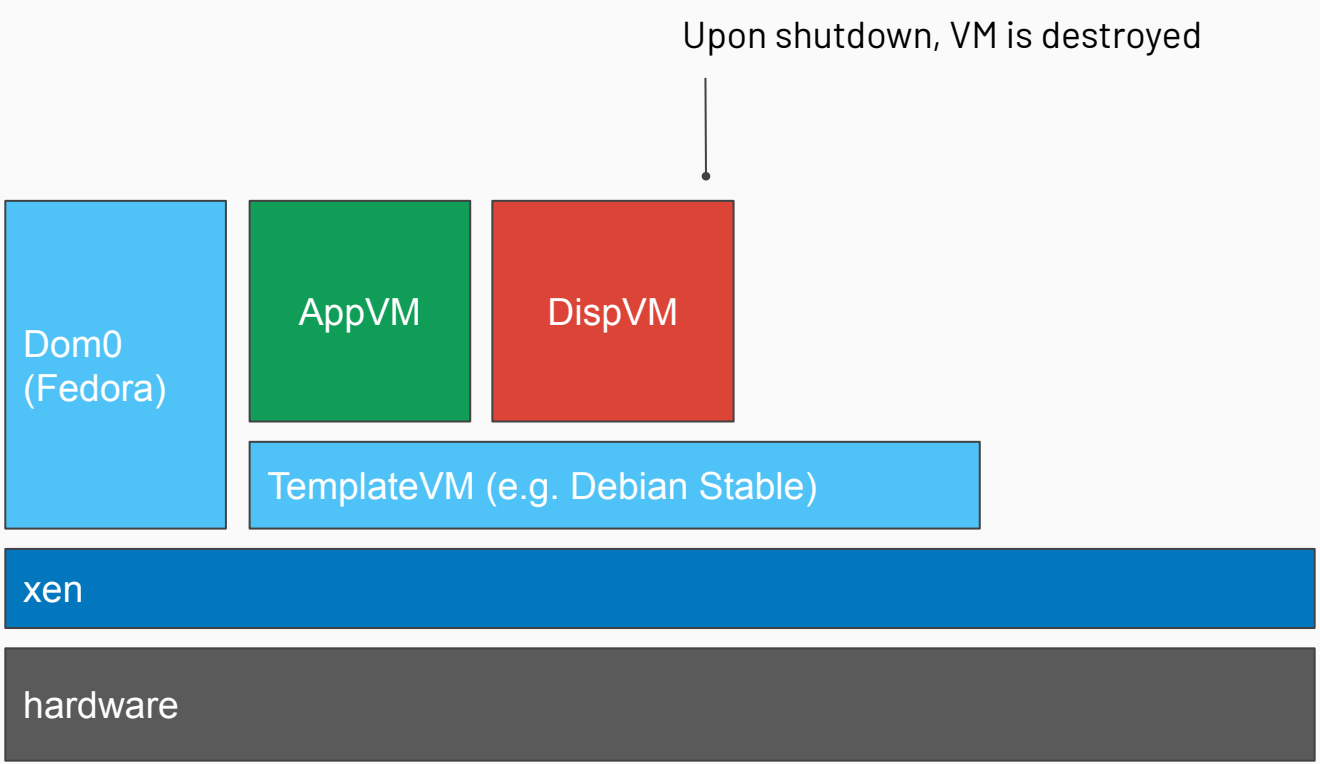


Qubes OS: single-user desktop-based Xen distribution

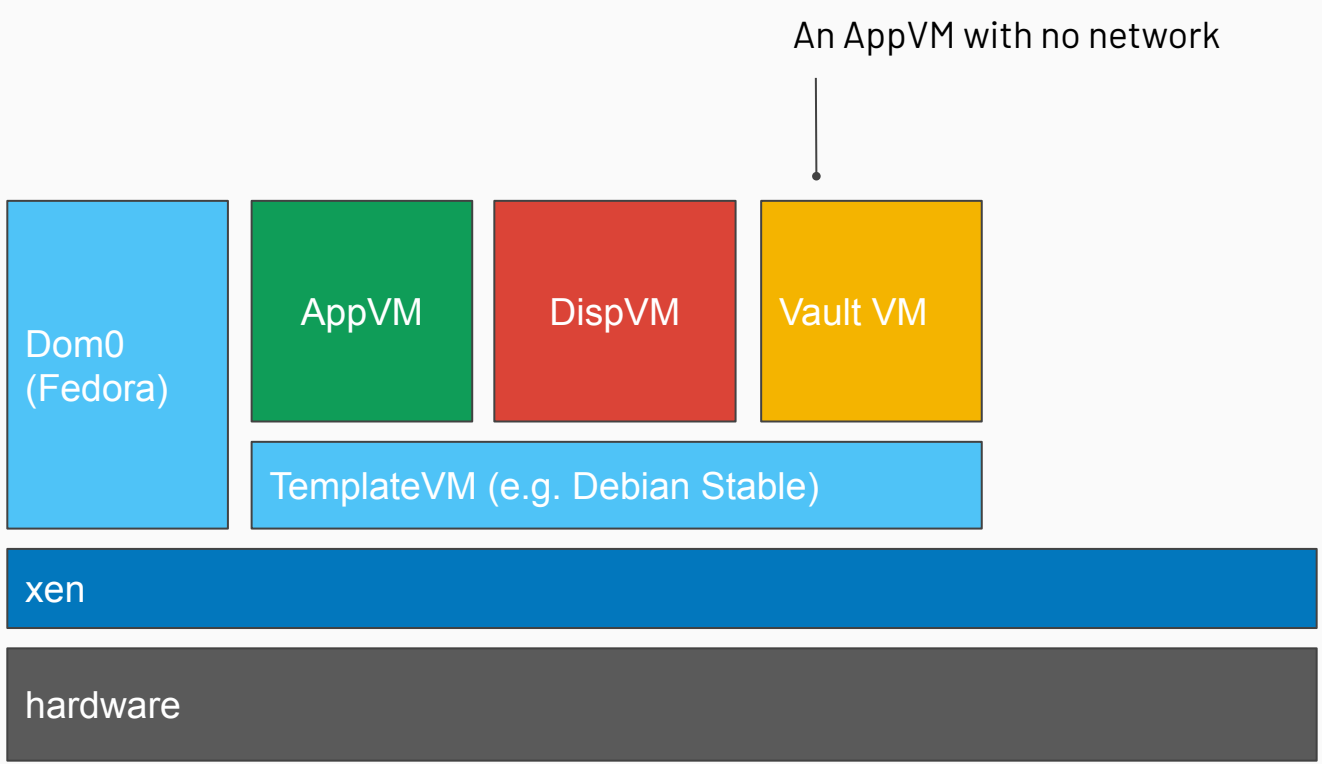
Only `/home`, `/usr/local`, `/rw/config` will persist a reboot, otherwise state is reset to the base TemplateVM



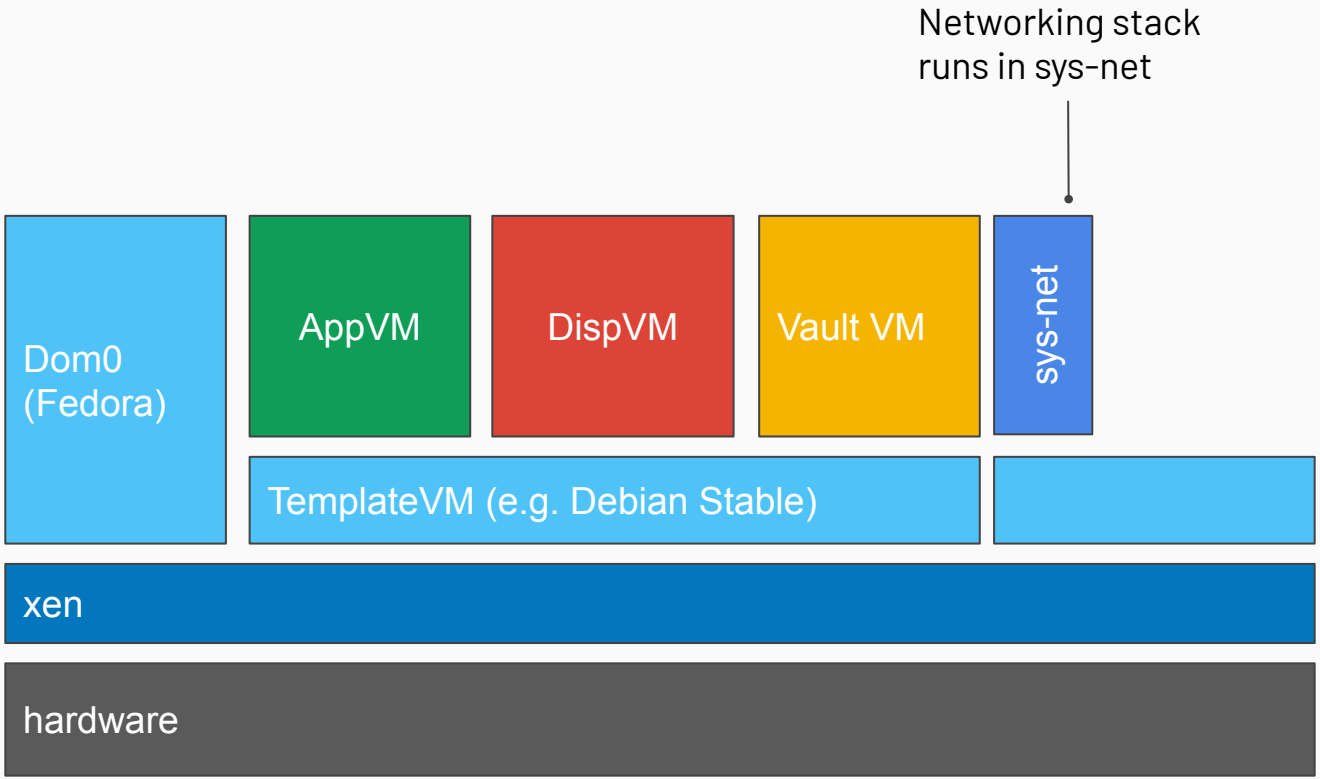
Qubes OS: single-user desktop-based Xen distribution



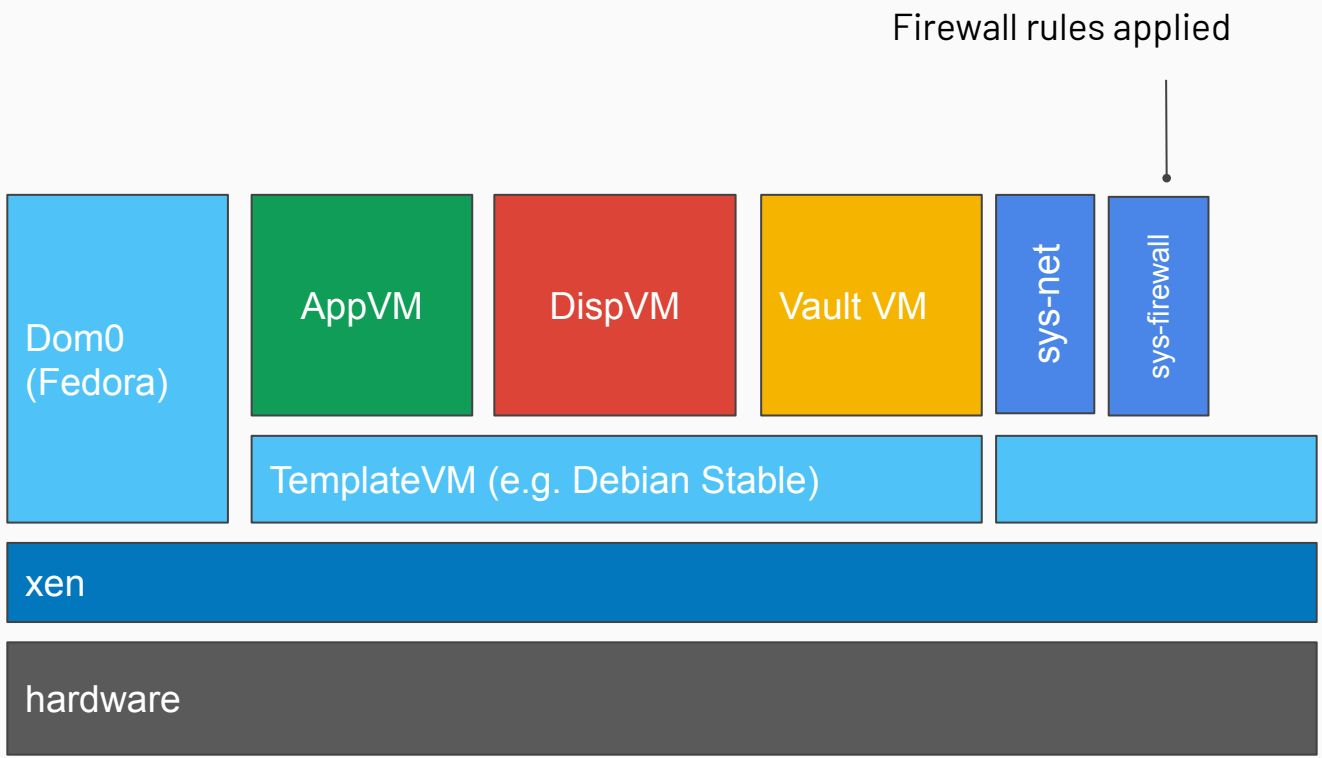
Qubes OS: single-user desktop-based Xen distribution



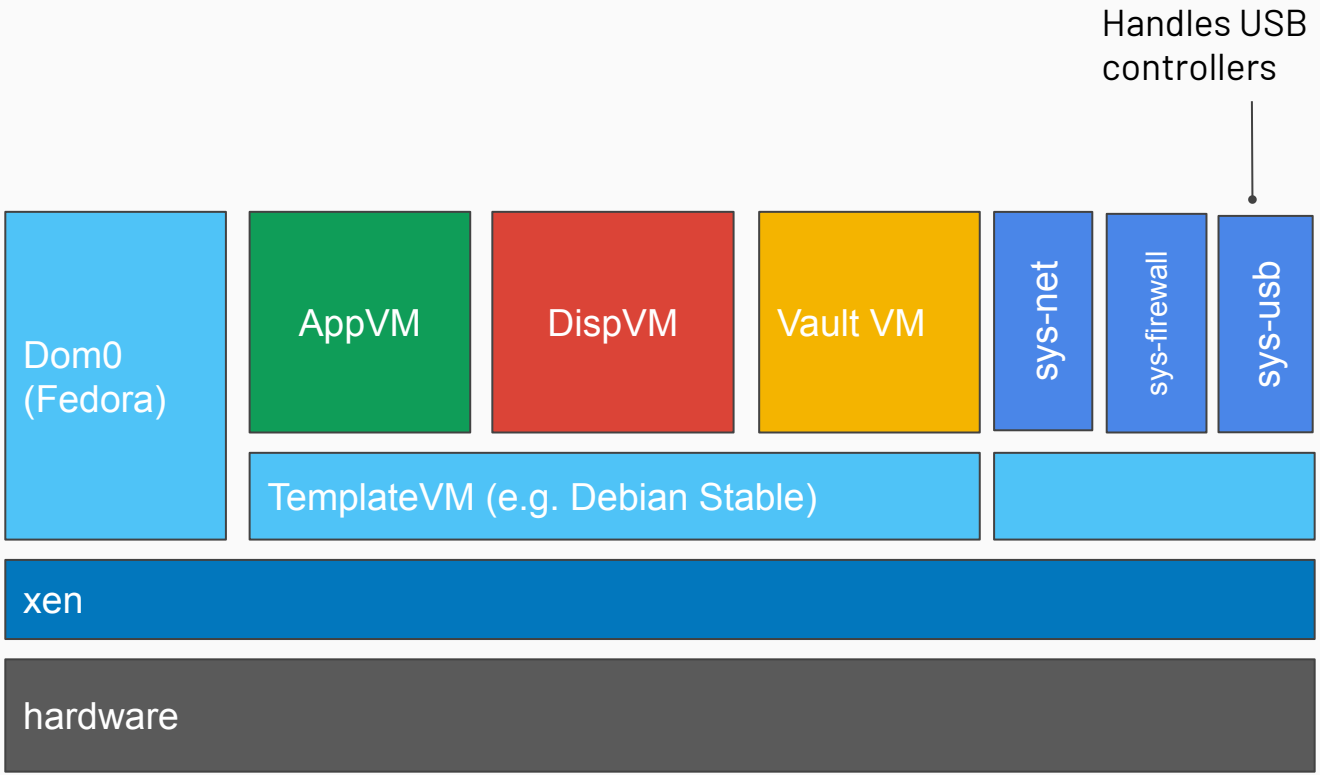
Qubes OS: single-user desktop-based Xen distribution



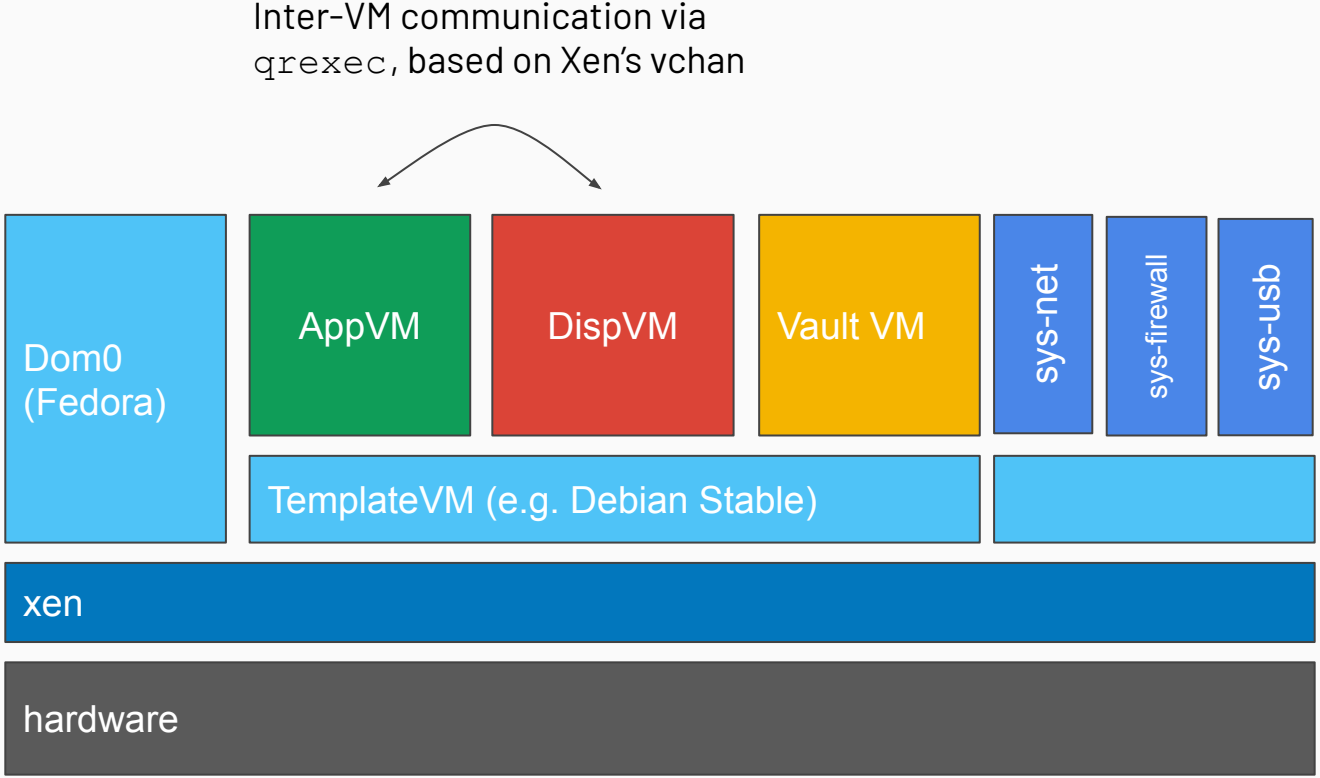
Qubes OS: single-user desktop-based Xen distribution



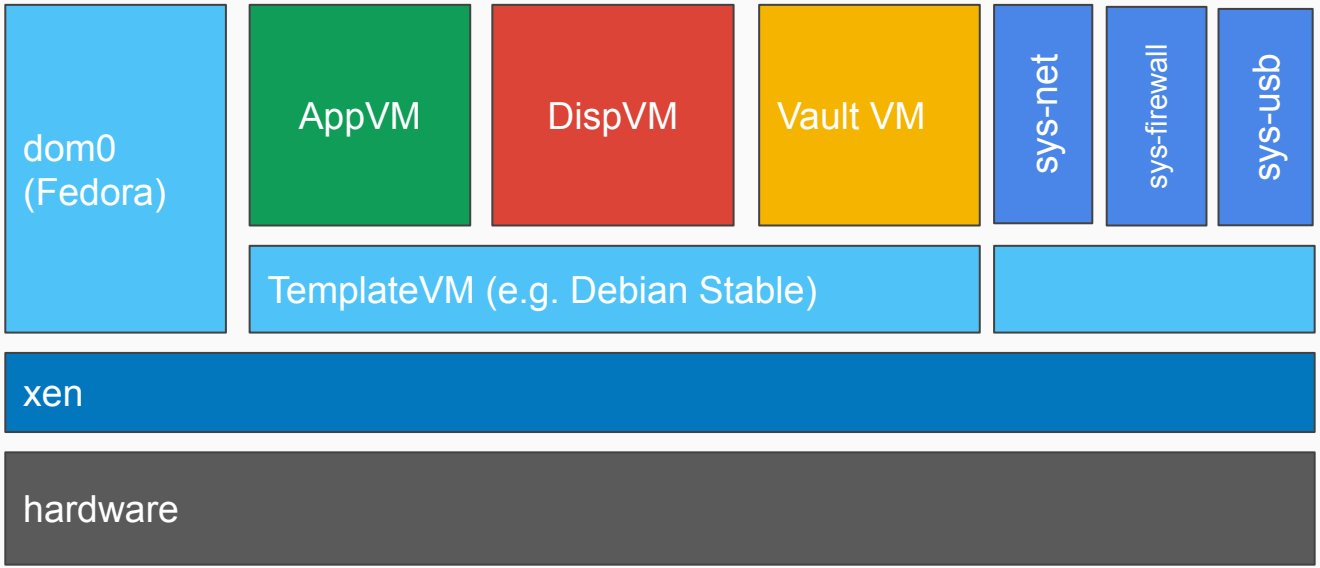
Qubes OS: single-user desktop-based Xen distribution



Qubes OS: single-user desktop-based Xen distribution

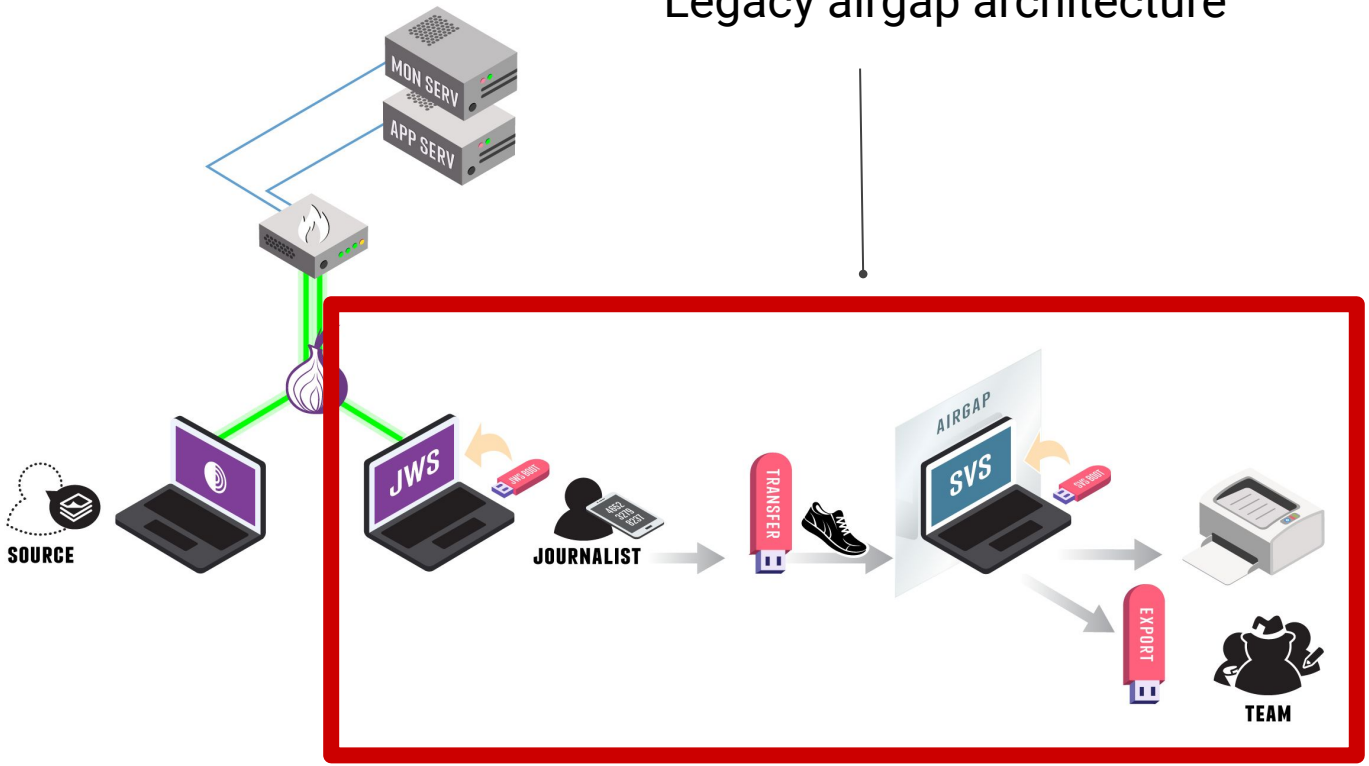


Qubes OS: single-user desktop-based Xen distribution



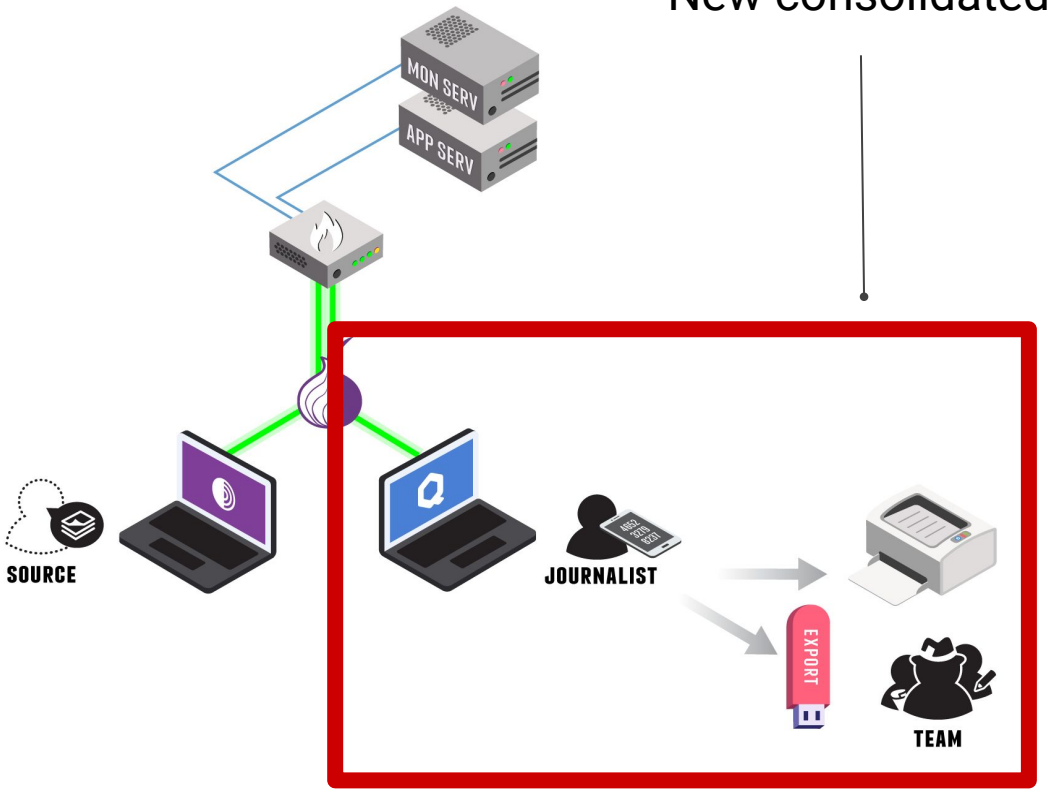
SecureDrop Workstation architecture

Legacy airgap architecture

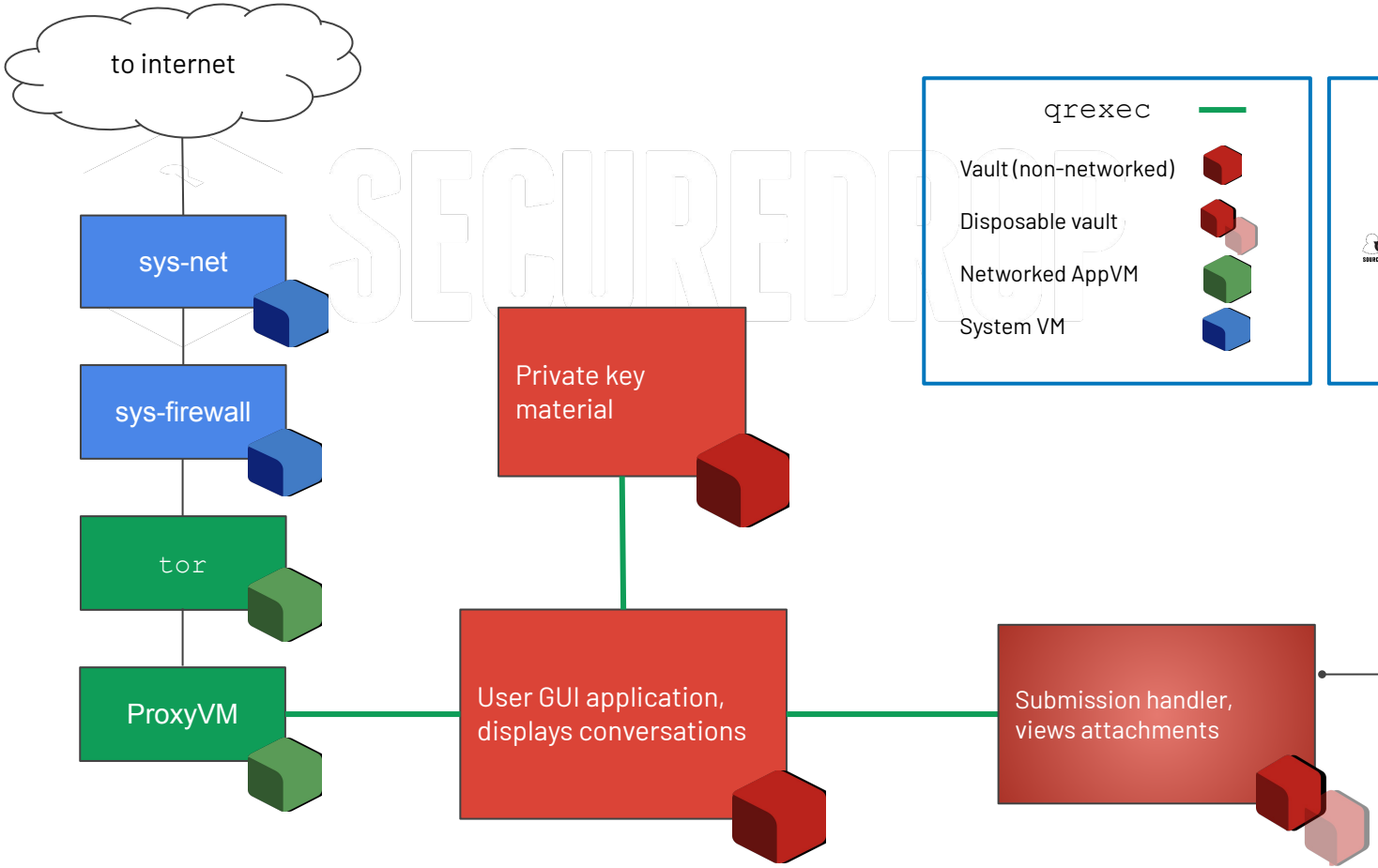


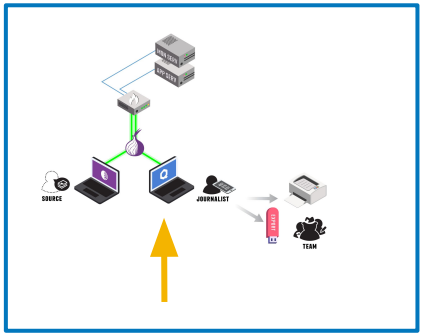
SECUREDROP

New consolidated architecture



SECUREDROP





Use a hardened template with grsecurity-patched kernel to provide additional generalized exploit mitigations for memory corruption vulnerabilities

"Overall, the SecureDrop Workstation system represents a complex but well researched product that has been thoughtfully designed."

- Trail of Bits, 2020

SECUREDROP

What’s next?

Future work

- Additional export tooling (e.g. Signal, Onionshare)
- Metadata redaction
- Malware detection

Questions?

Get involved:

- Our repos: https://github.com/freedomofpress/
- Qubes OS: https://qubes-os.org/
- Tor: https://torproject.org/
- Want to donate? https://freedom.press/donate/

Contact:

Conor Schaefer
Chief Technology Officer
conor@freedom.press

SECUREDROP