Next-Generation SecureDrop: Protecting Journalists from Malware

Usenix Enigma, January 2020
Jennifer Helsby (@redshiftzero)
Lead Developer

Today

1. Security Goals
2. Current architecture: The story so far
3. Challenges
4. Next generation architecture
5. What’s next

Current Team

100% time on SecureDrop

Jen
Engineering

Kushal
Engineering

Kevin
Support, Engineering

Allie
Engineering

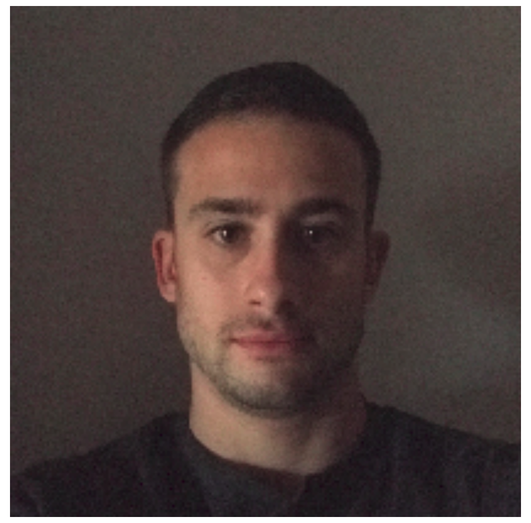
John
Engineering

Rowen
Support

>= 50% time on SecureDrop

Conor
Engineering

Erik
Project Manager


Mickael
Engineering

Nina
UX

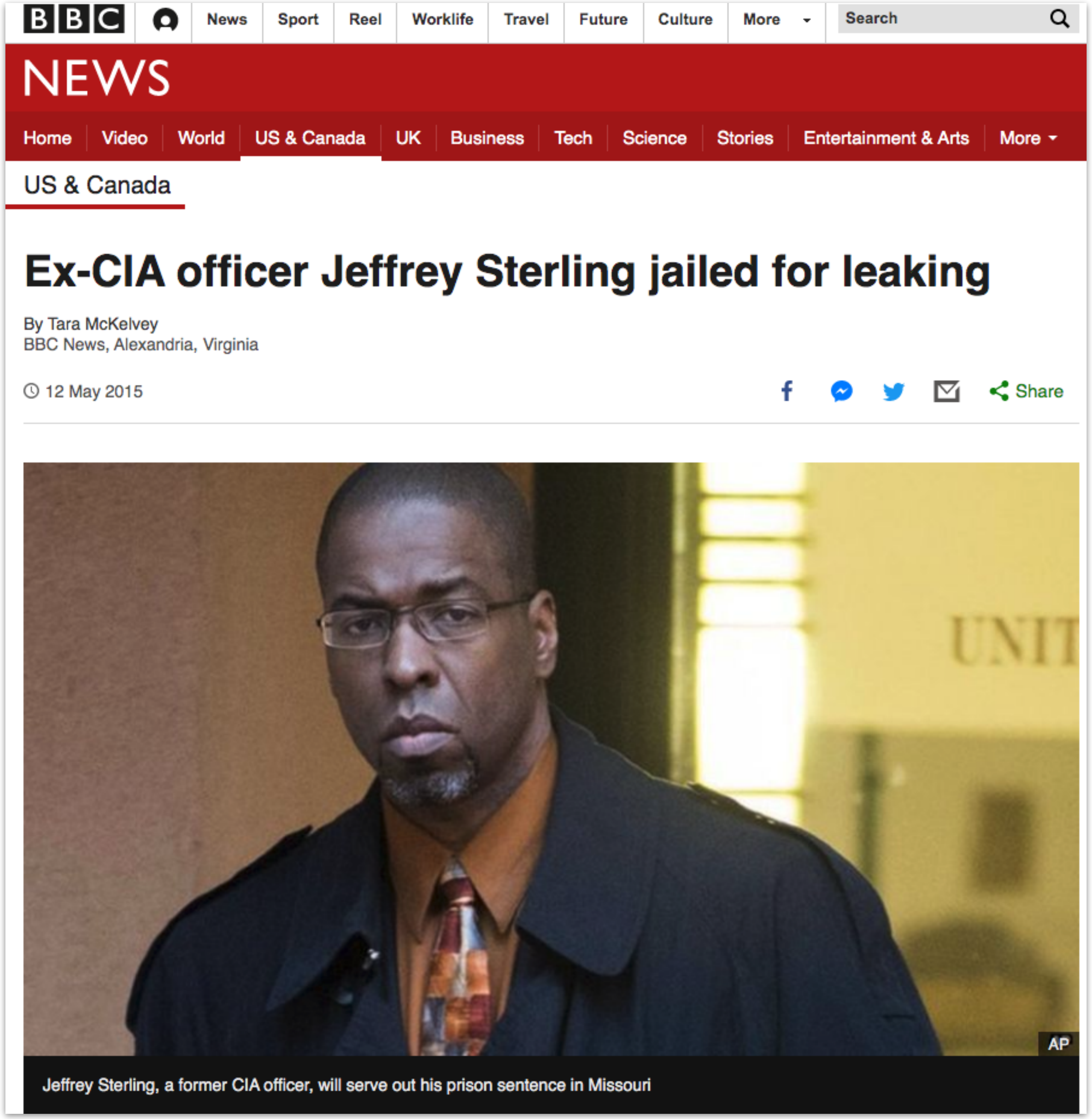
>= 25% time on SecureDrop

Harlo
Training

Olivia
Training

David
Training

A tale of a whistleblower



Ex-CIA officer Jeffrey Sterling jailed for leaking

By Tara McKelvey
BBC News, Alexandria, Virginia

12 May 2015

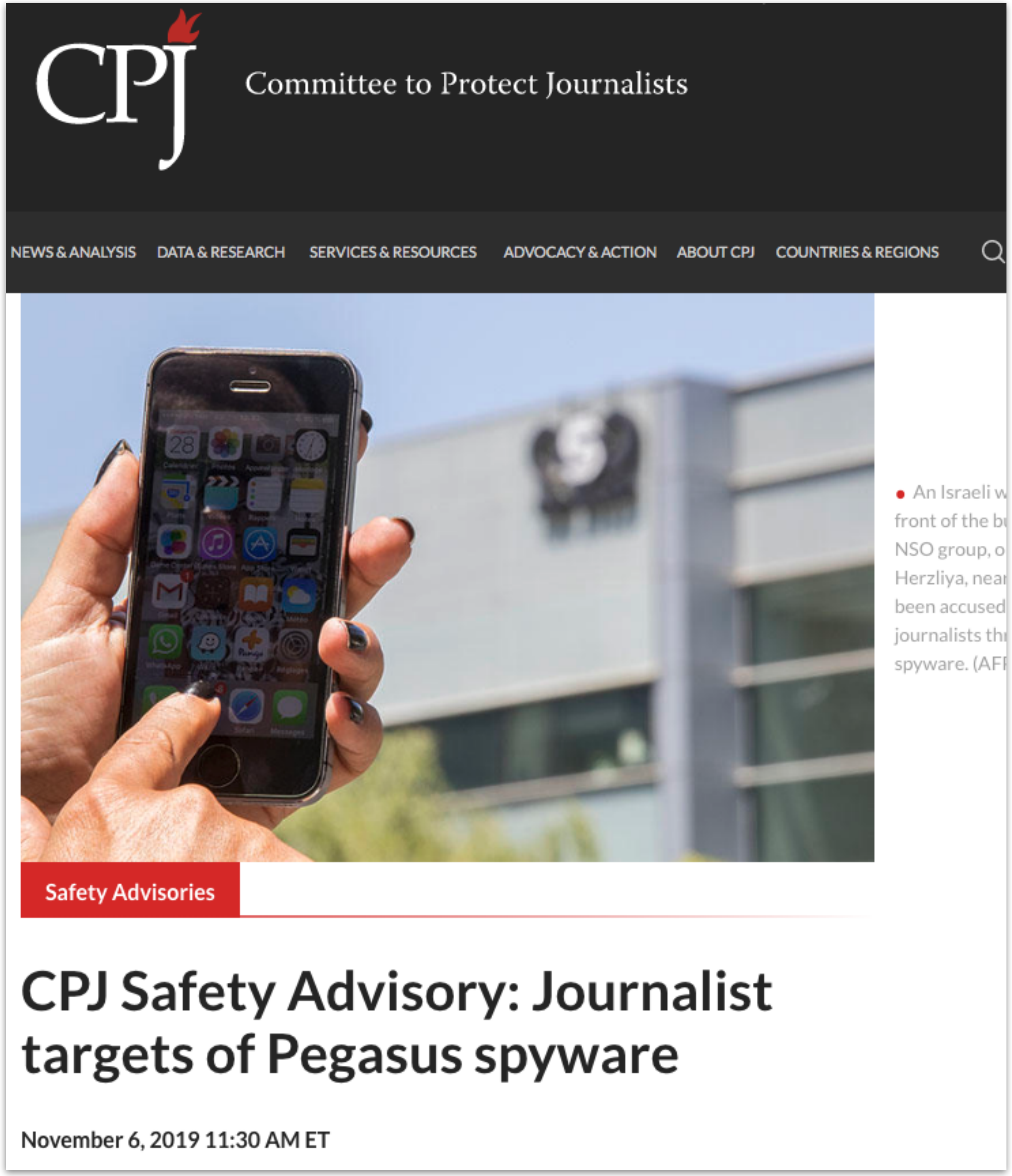
Jeffrey Sterling, a former CIA officer, will serve out his prison sentence in Missouri

Trial by metadata

Security Goals

1. Prevent identification of journalistic sources.

2. Preserve confidentiality of source materials.

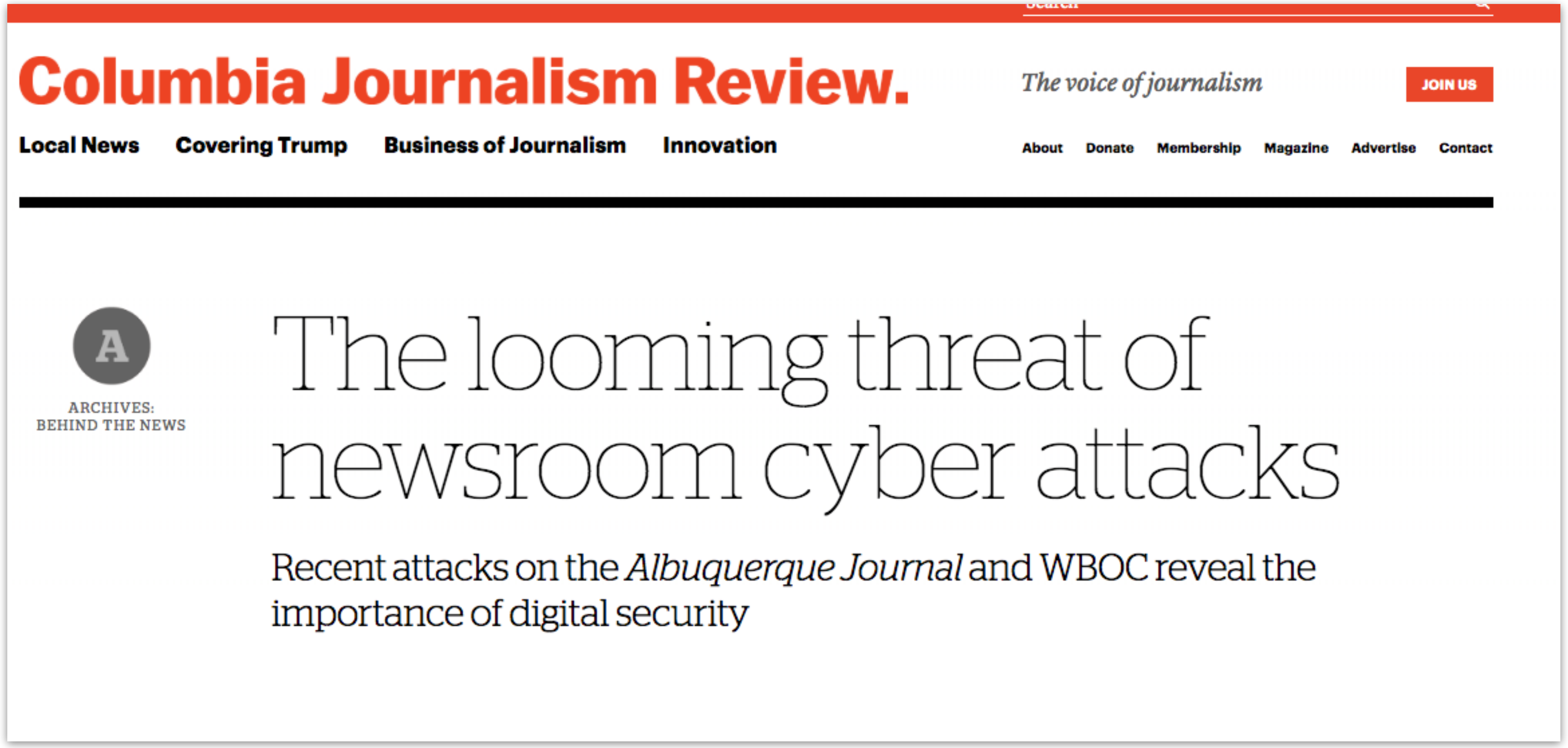


An Israeli w
front of the bu
NSO group, o
Herzliya, near
been accused
journalists thr
spyware. (AFP

Safety Advisories

CPJ Safety Advisory: Journalist targets of Pegasus spyware

November 6, 2019 11:30 AM ET



The looming threat of newsroom cyber attacks

Recent attacks on the *Albuquerque Journal* and WBOC reveal the importance of digital security

Trial by metadata

Security Goals

1. Prevent identification of journalistic sources.
2. Preserve confidentiality of source materials.
3. Prevent journalists from being hacked via malicious submissions.

Security Goals

1. Prevent identification of journalistic sources.

2. Preserve confidentiality of source materials.

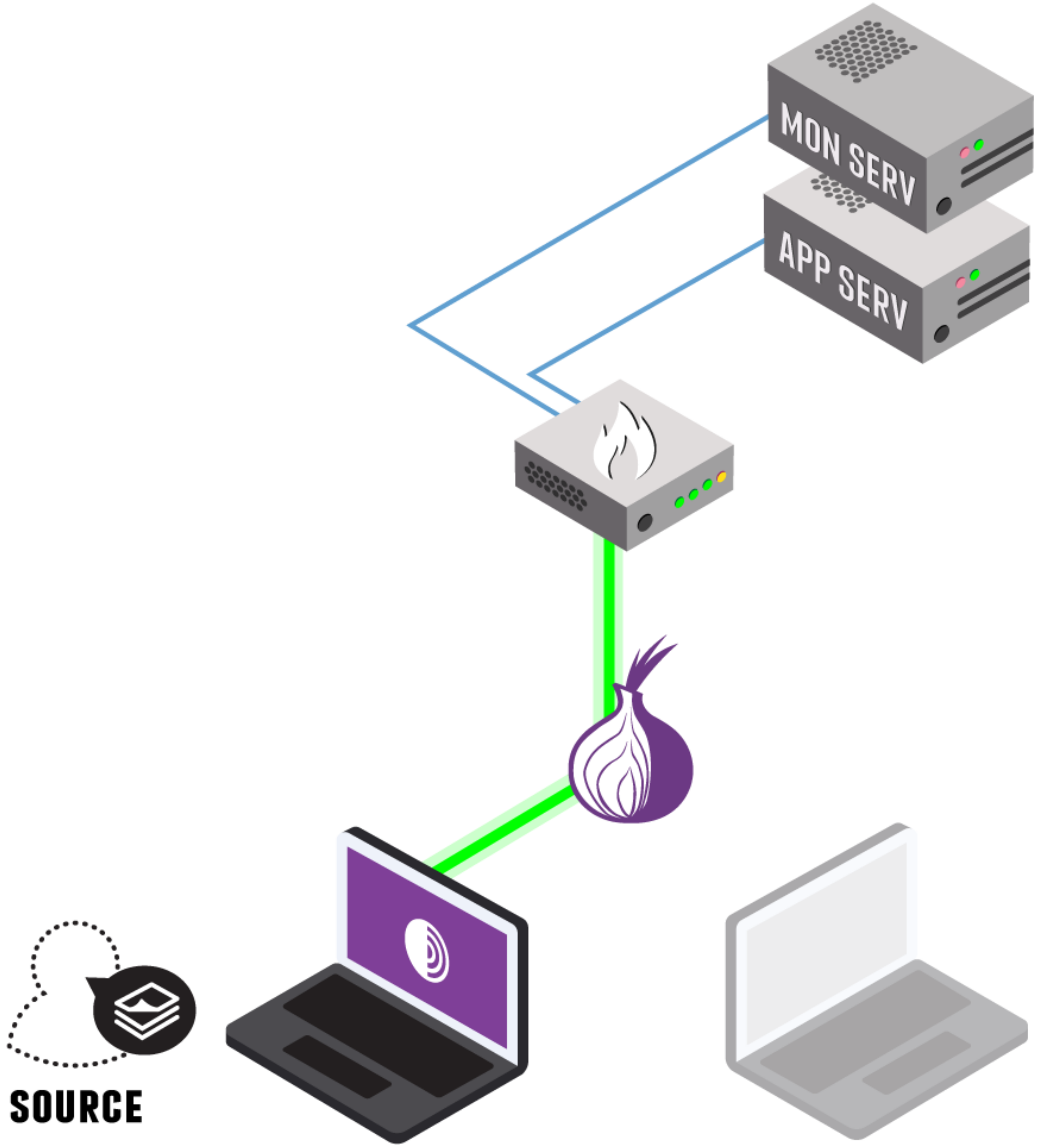
3. **Prevent journalists from being hacked via malicious submissions.**

The story so far…

The Intercept_
WIRED
POLITICO
Bloomberg
FT
FINANCIAL TIMES
HUFFPOST
USA TODAY NETWORK
npr
The Washington Post
THE GLOBE AND MAIL
REUTERS
CBC
THE WALL STREET JOURNAL
AP Associated Press
The Guardian
SLATE
The Telegraph
NBC NEWS
Reveal
from The Center for Investigative Reporting
BuzzFeed
Forbes
The New York Times
DAILY BEAST
BUSINESS INSIDER
ALJAZEERA
LPL
Gizmodo Media Group
VOX MEDIA
ICIJ The International Consortium of Investigative Journalists
Aftenposten
Süddeutsche Zeitung
WHISTLEBLOWER AID
THE TRUTH & TRANSPARENCY FOUNDATION

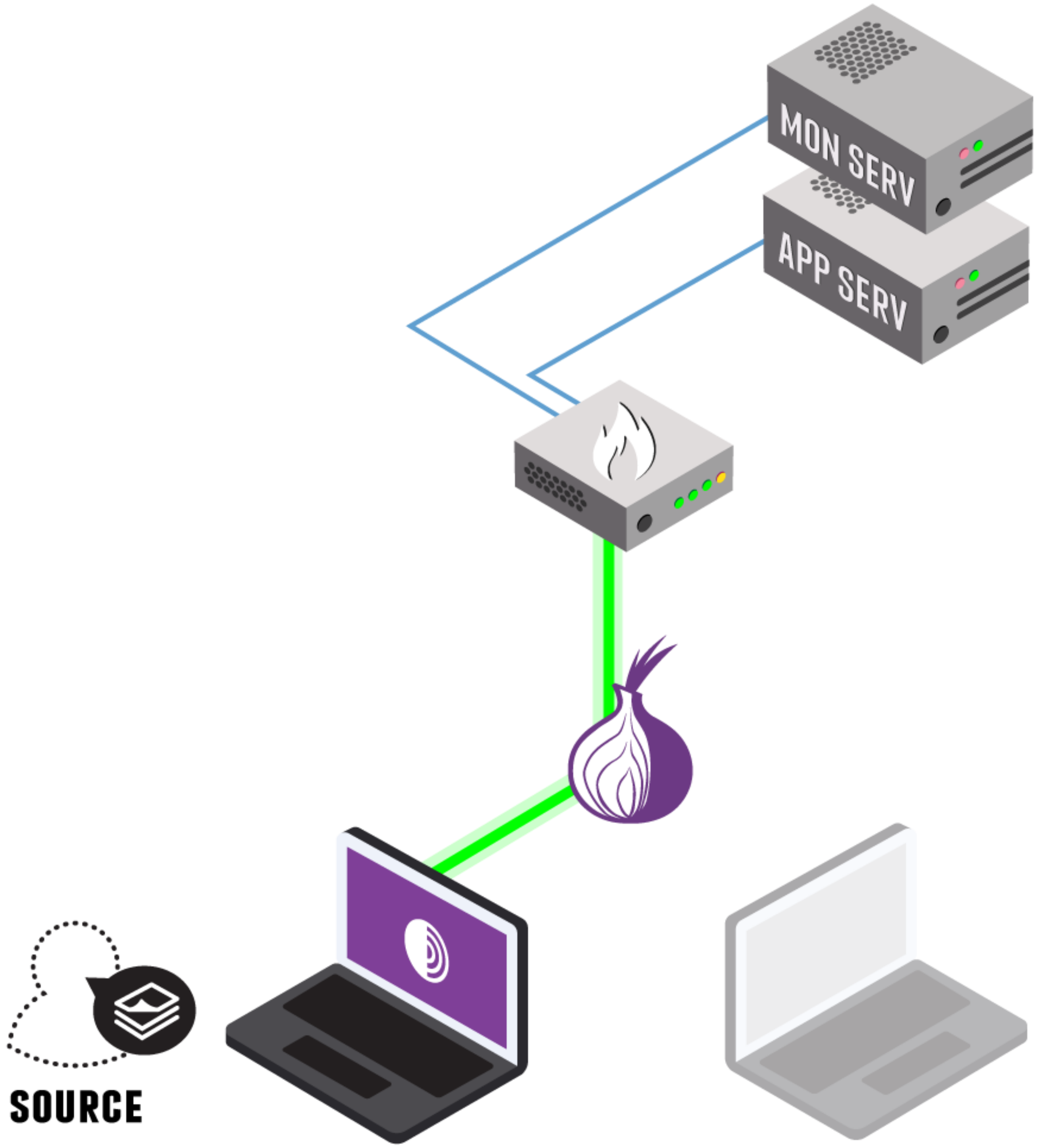
Some organizations that use SecureDrop for source communication

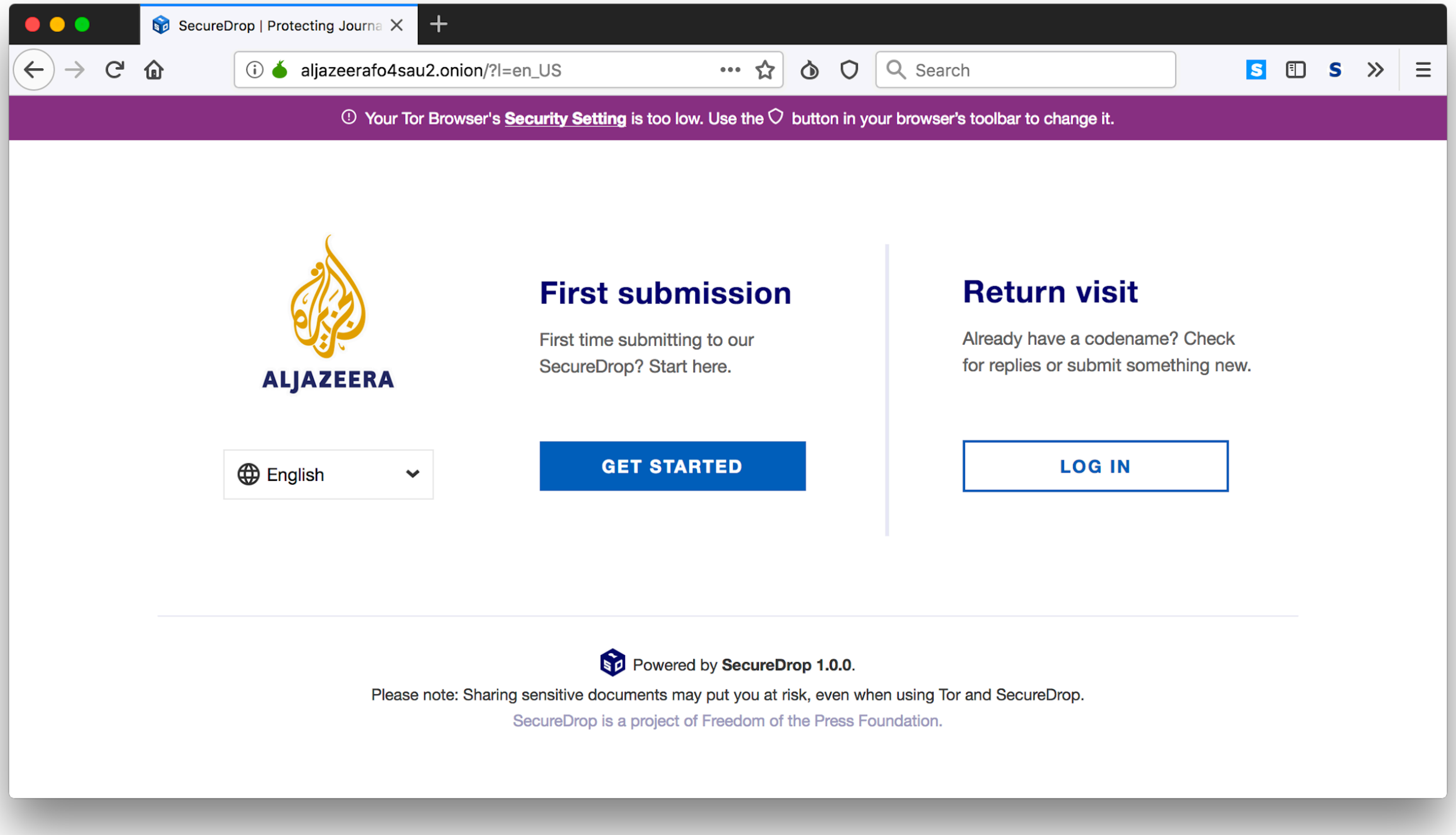
Current Architecture



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

Current Architecture




SecureDrop | Protecting Journa
aljazeerafo4sau2.onion/?l=en_US
Search
ALJAZEERA
English
GET STARTED
LOG IN

Your Tor Browser's **Security Setting** is too low. Use the button in your browser's toolbar to change it.

First submission

First time submitting to our SecureDrop? Start here.

Return visit

Already have a codename? Check for replies or submit something new.

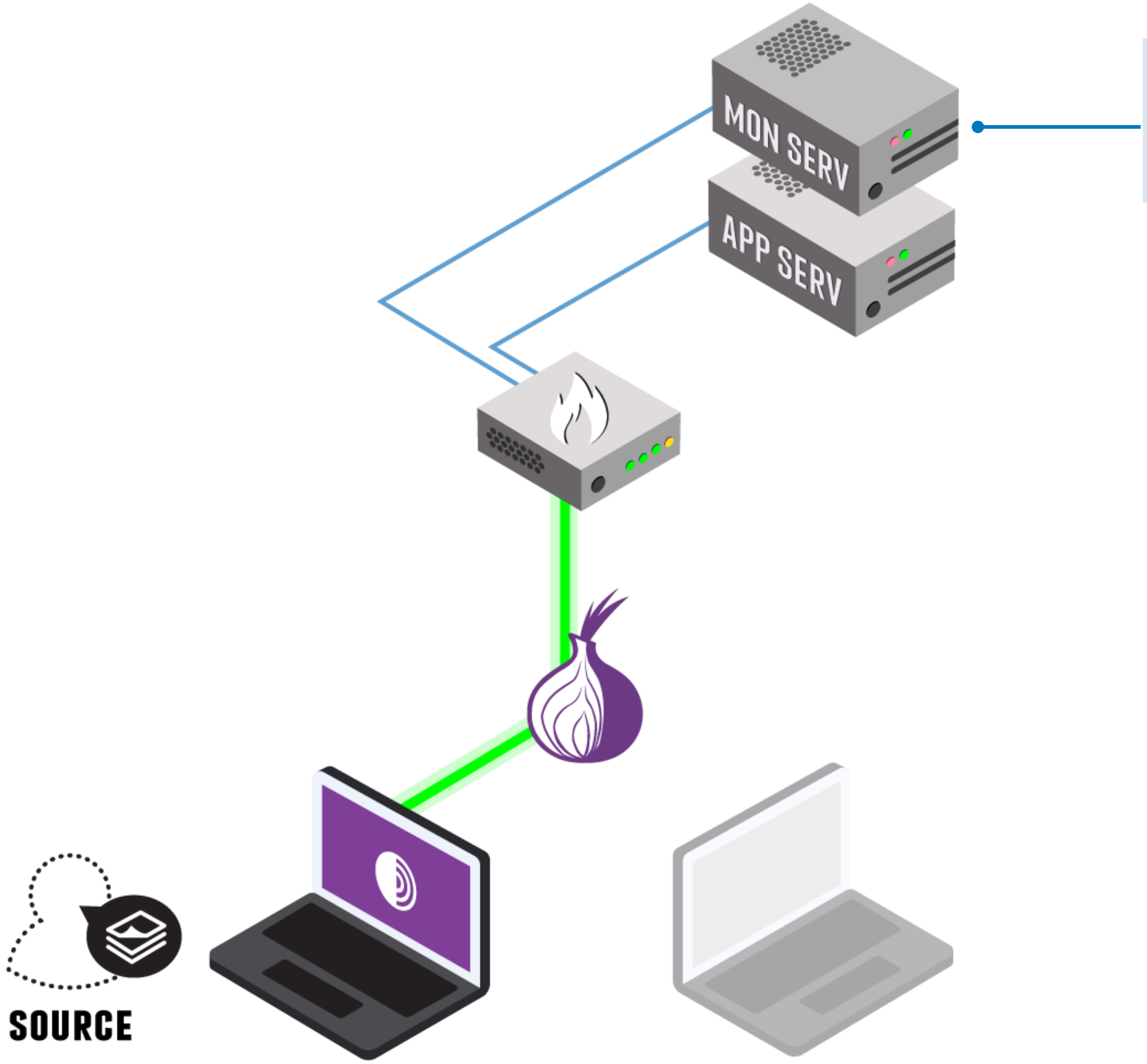
Powered by **SecureDrop 1.0.0**.

Please note: Sharing sensitive documents may put you at risk, even when using Tor and SecureDrop.

SecureDrop is a project of Freedom of the Press Foundation.

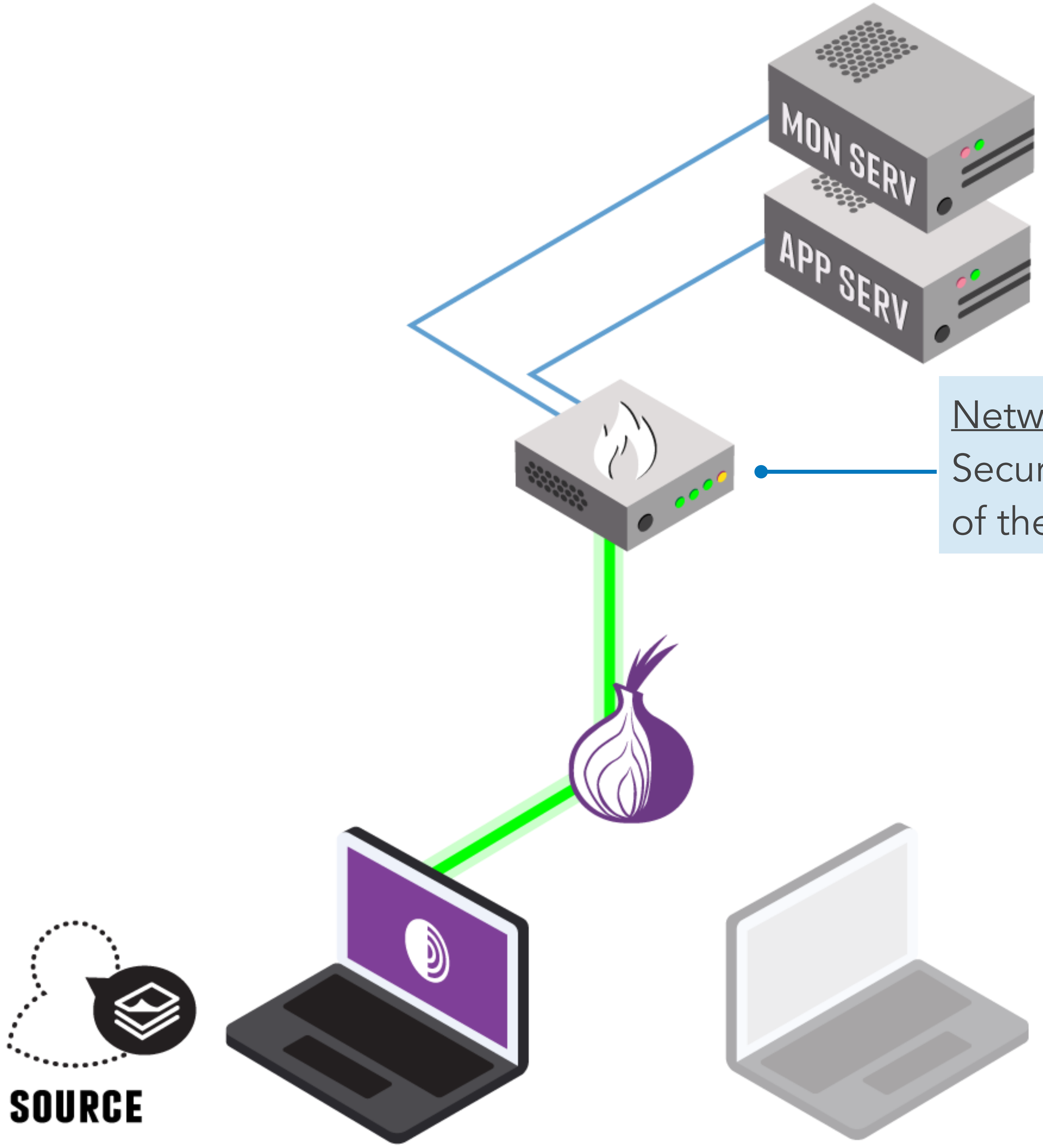
SECUREDROP

Current Architecture



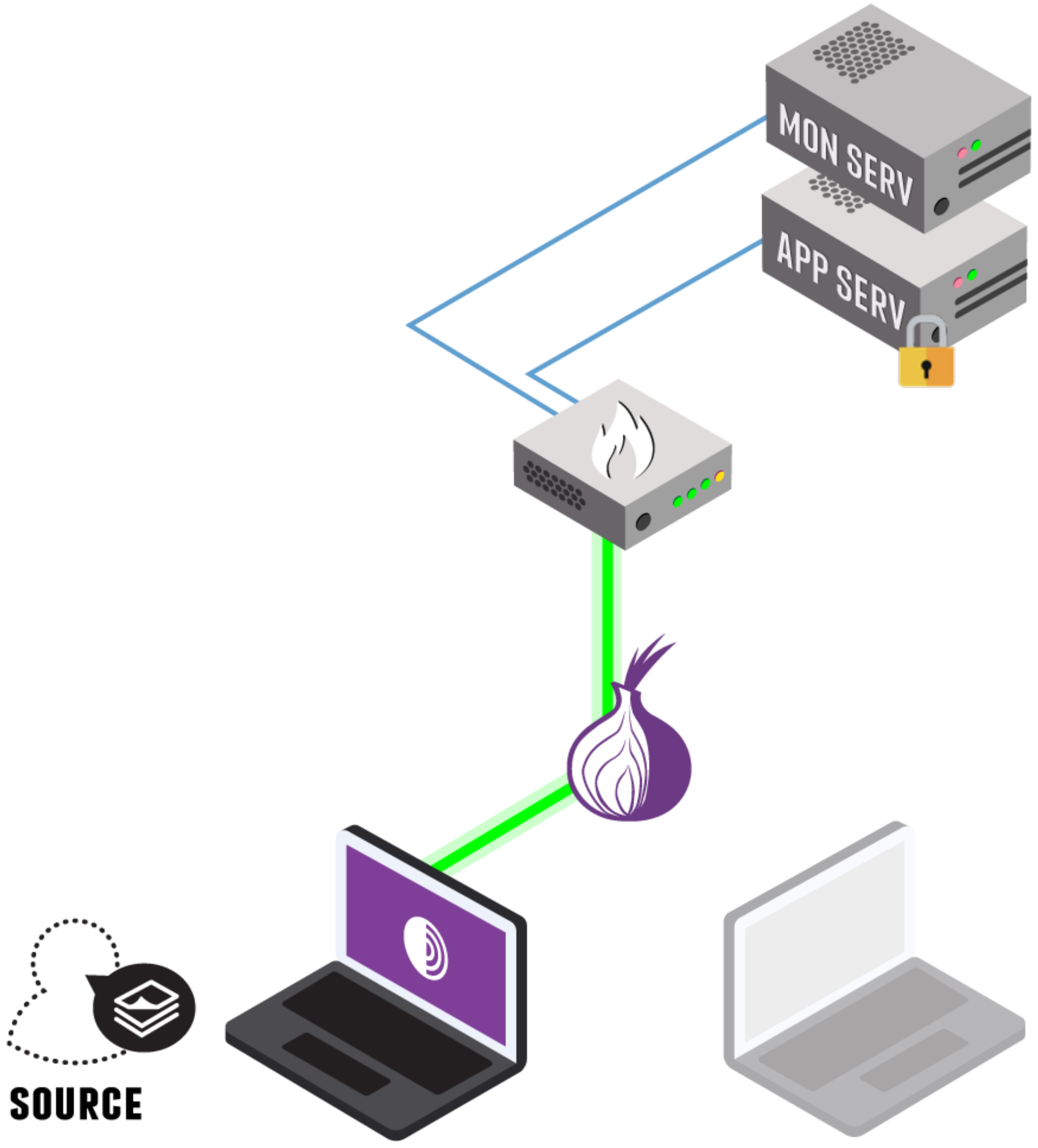
Monitoring server: Runs a host-based IDS (OSSEC) to monitor the application server and send alerts to administrators

Current Architecture



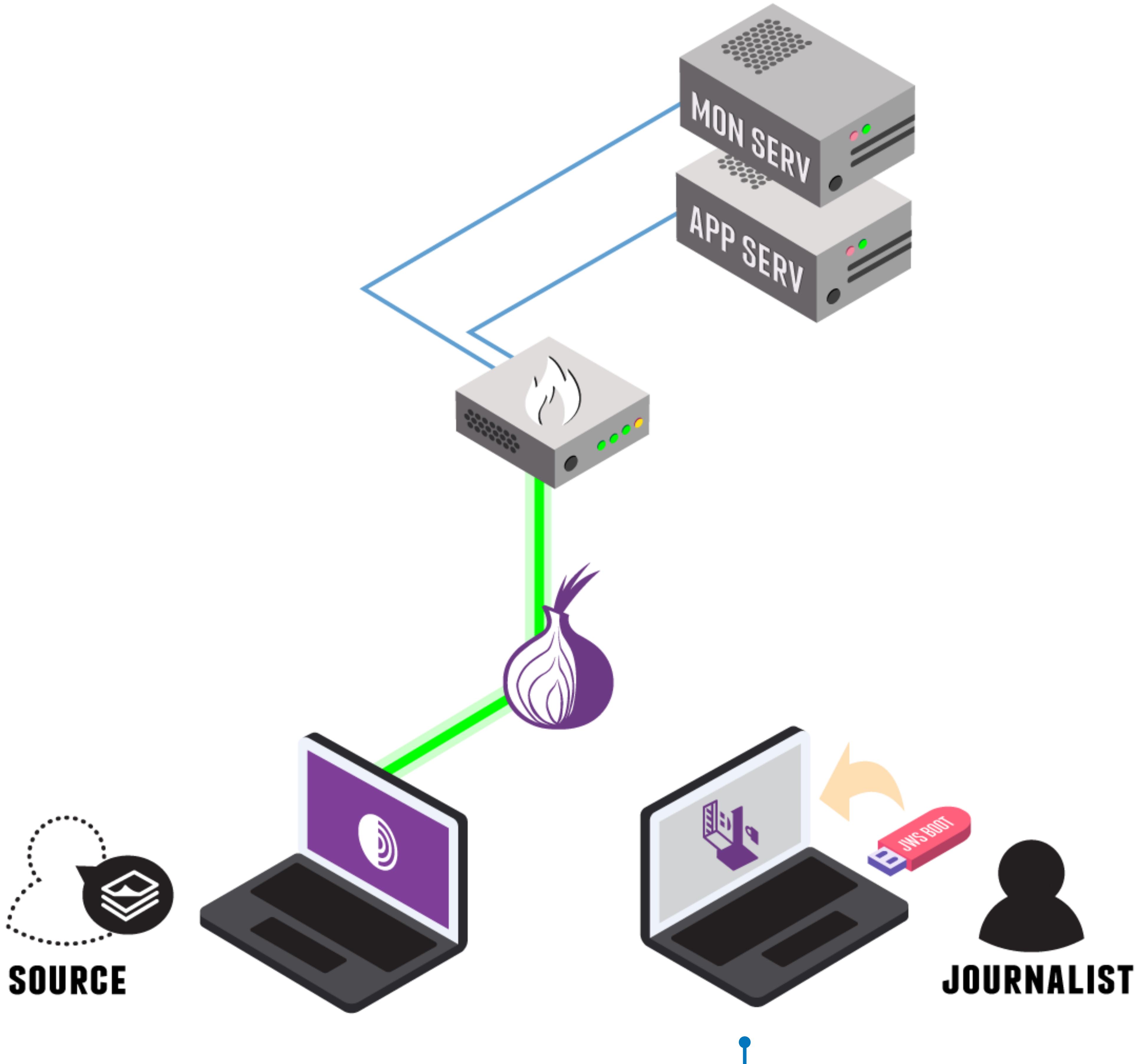
Network firewall: pfSense used to isolate the SecureDrop area of the network from the rest of the news organization

Current Architecture



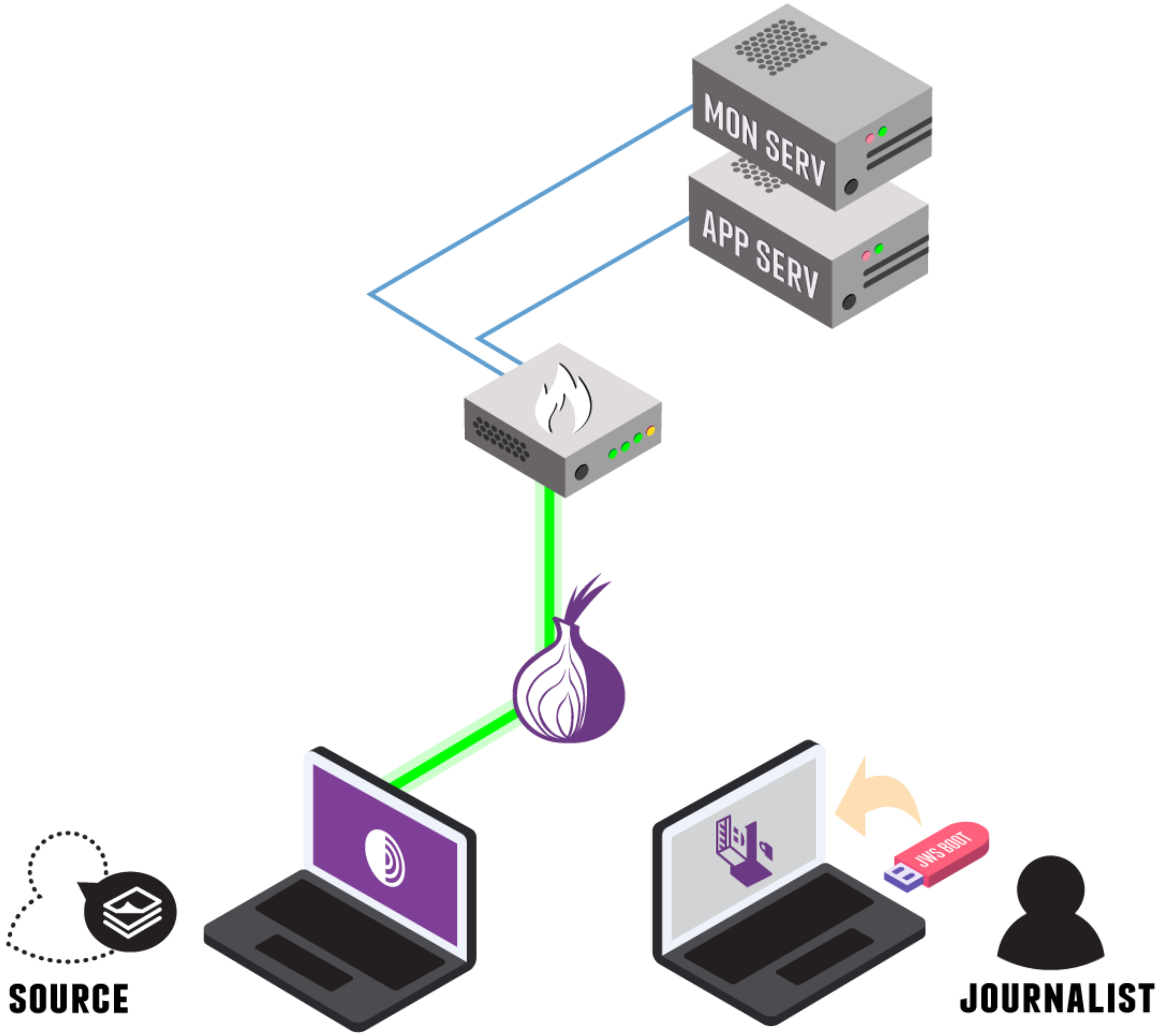
Documents stored encrypted to the instance’s public key

Current Architecture

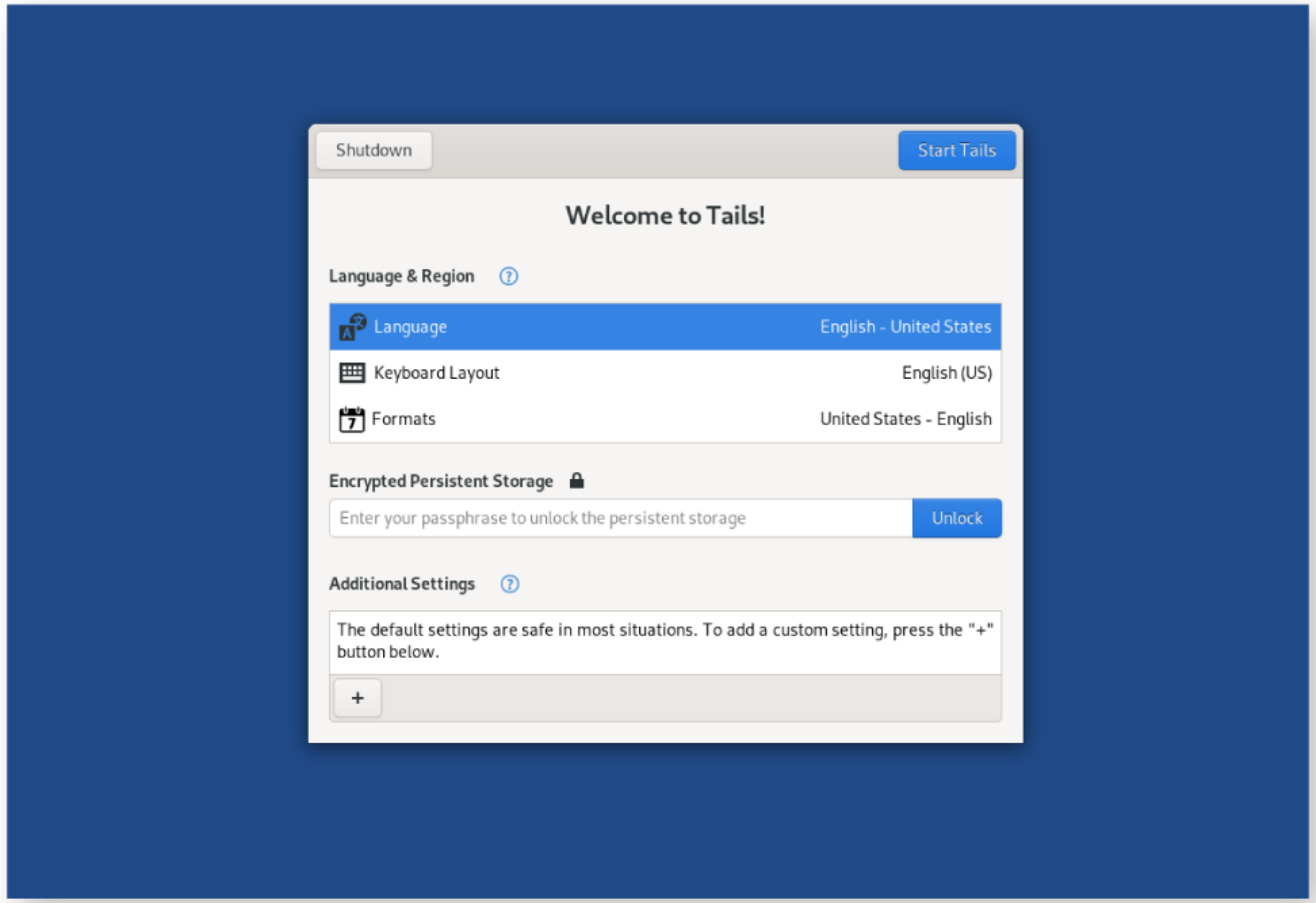


Journalists log on using TailsOS

Current Architecture



Journalists log on using TailsOS



Welcome to Tails!

Language & Region

Language English - United States

Keyboard Layout English (US)

Formats United States - English

Encrypted Persistent Storage

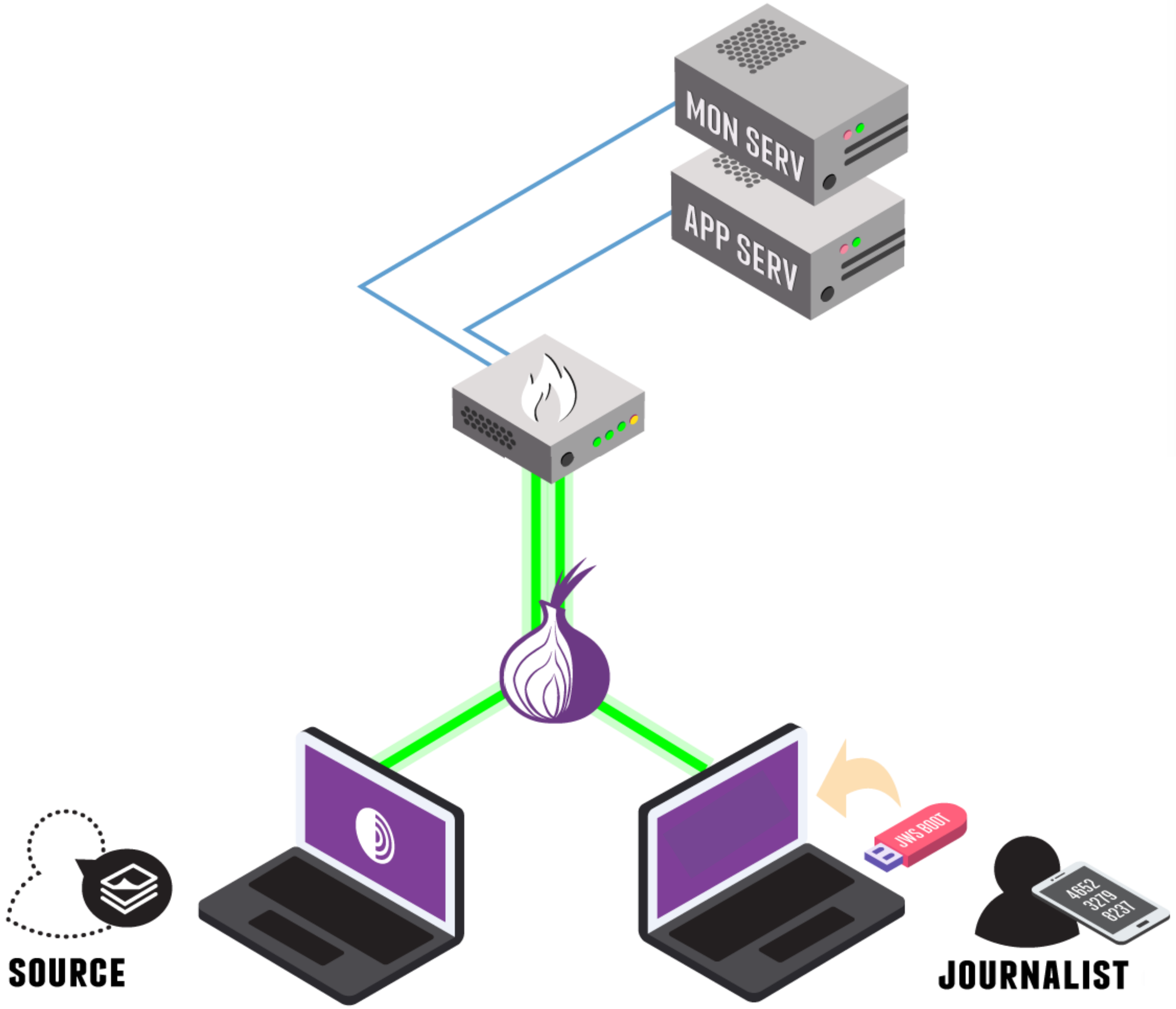
Enter your passphrase to unlock the persistent storage

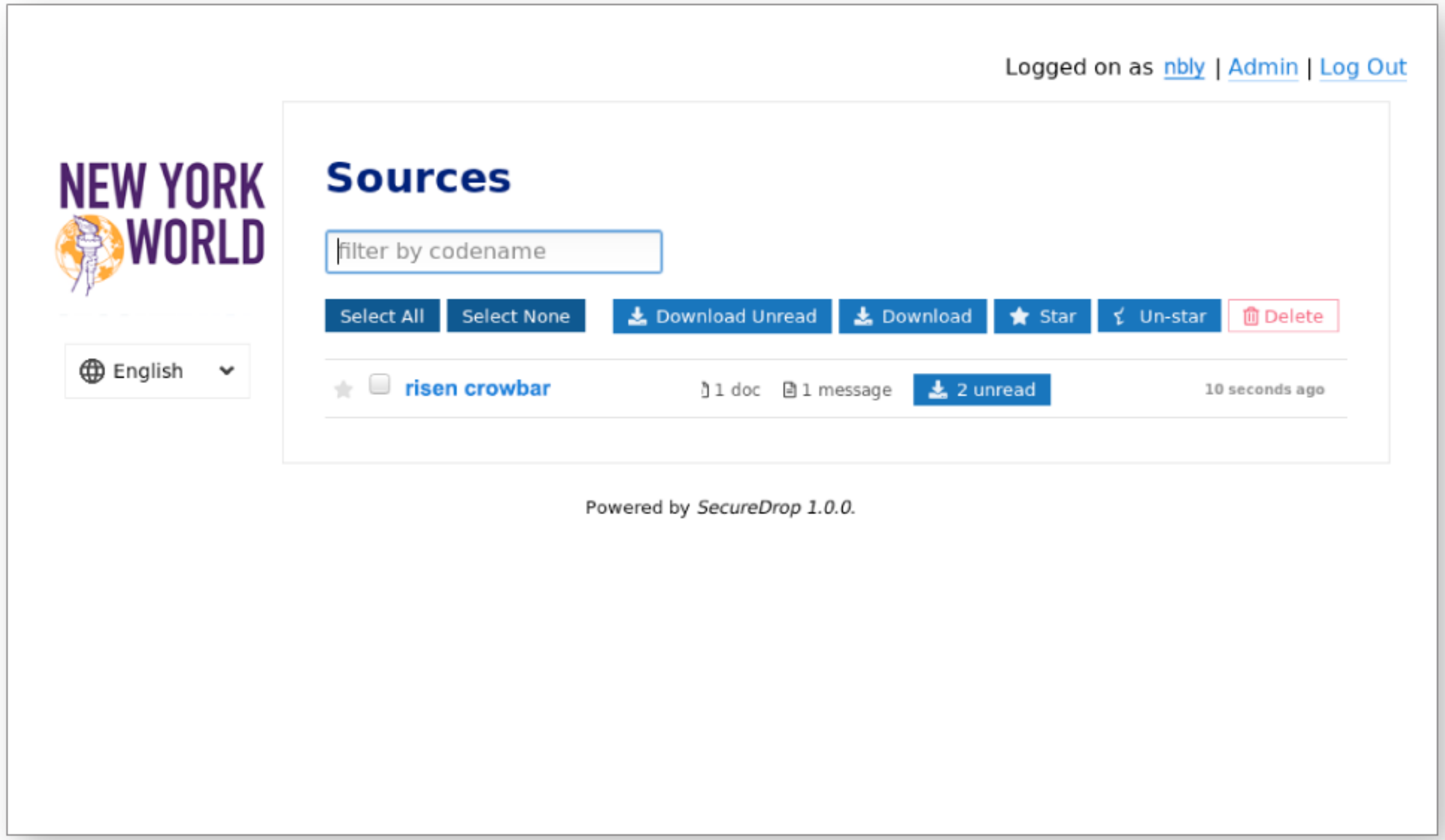
Additional Settings

The default settings are safe in most situations. To add a custom setting, press the "+" button below.

SECUREDROP

Current Architecture




Logged on as nbly | Admin | Log Out

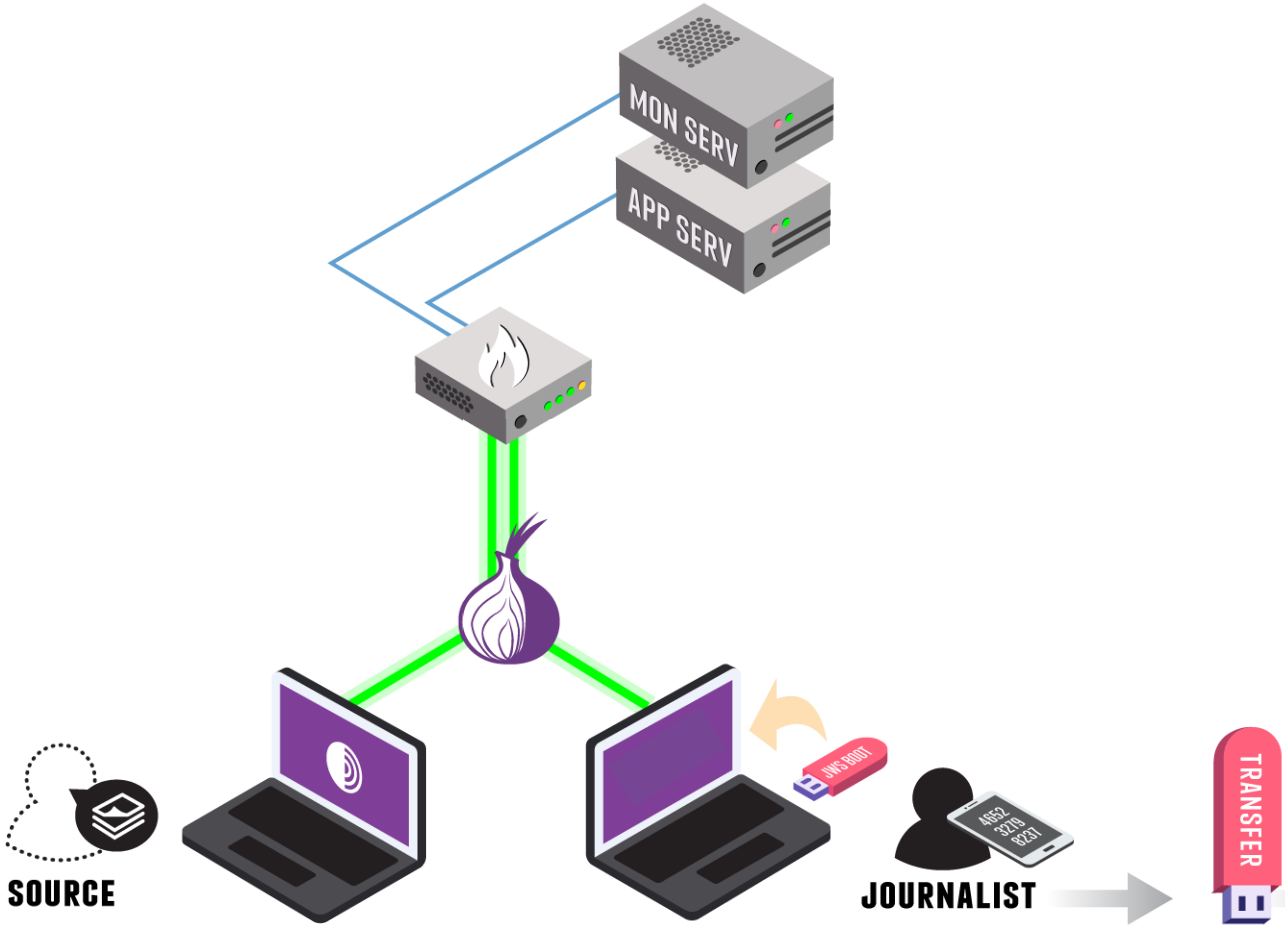
Sources

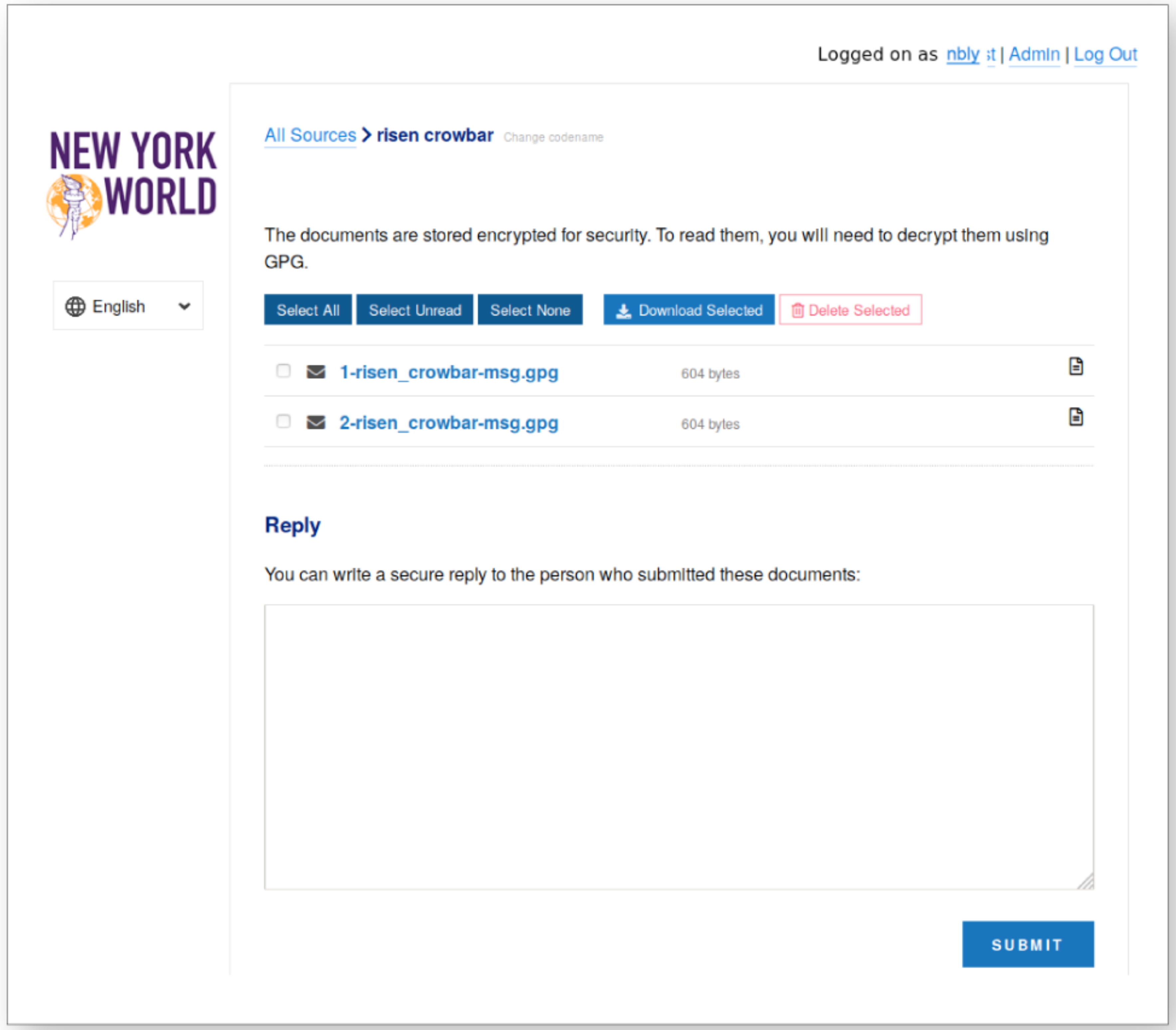
Filter by codename

risen crowbar 1 doc 1 message 2 unread 10 seconds ago

Powered by *SecureDrop 1.0.0.*

Current Architecture




Logged on as nbly :t | Admin | Log Out

NEW YORK WORLD

English

All Sources > **risen crowbar** Change codename

The documents are stored encrypted for security. To read them, you will need to decrypt them using GPG.

Select All | Select Unread | Select None | Download Selected | Delete Selected

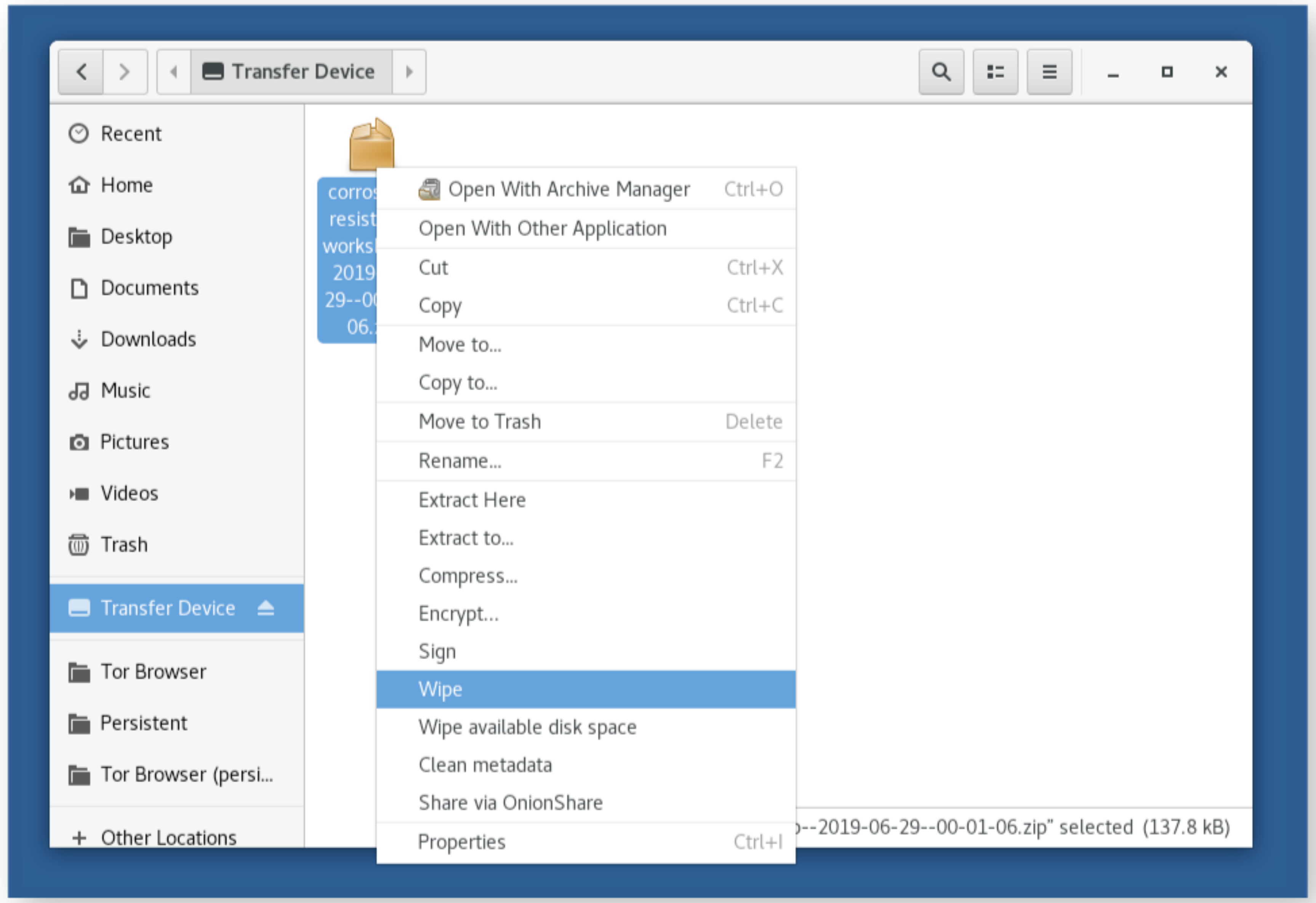
□	✉	1-risen_crowbar-msg.gpg	604 bytes
□	✉	2-risen_crowbar-msg.gpg	604 bytes

Reply

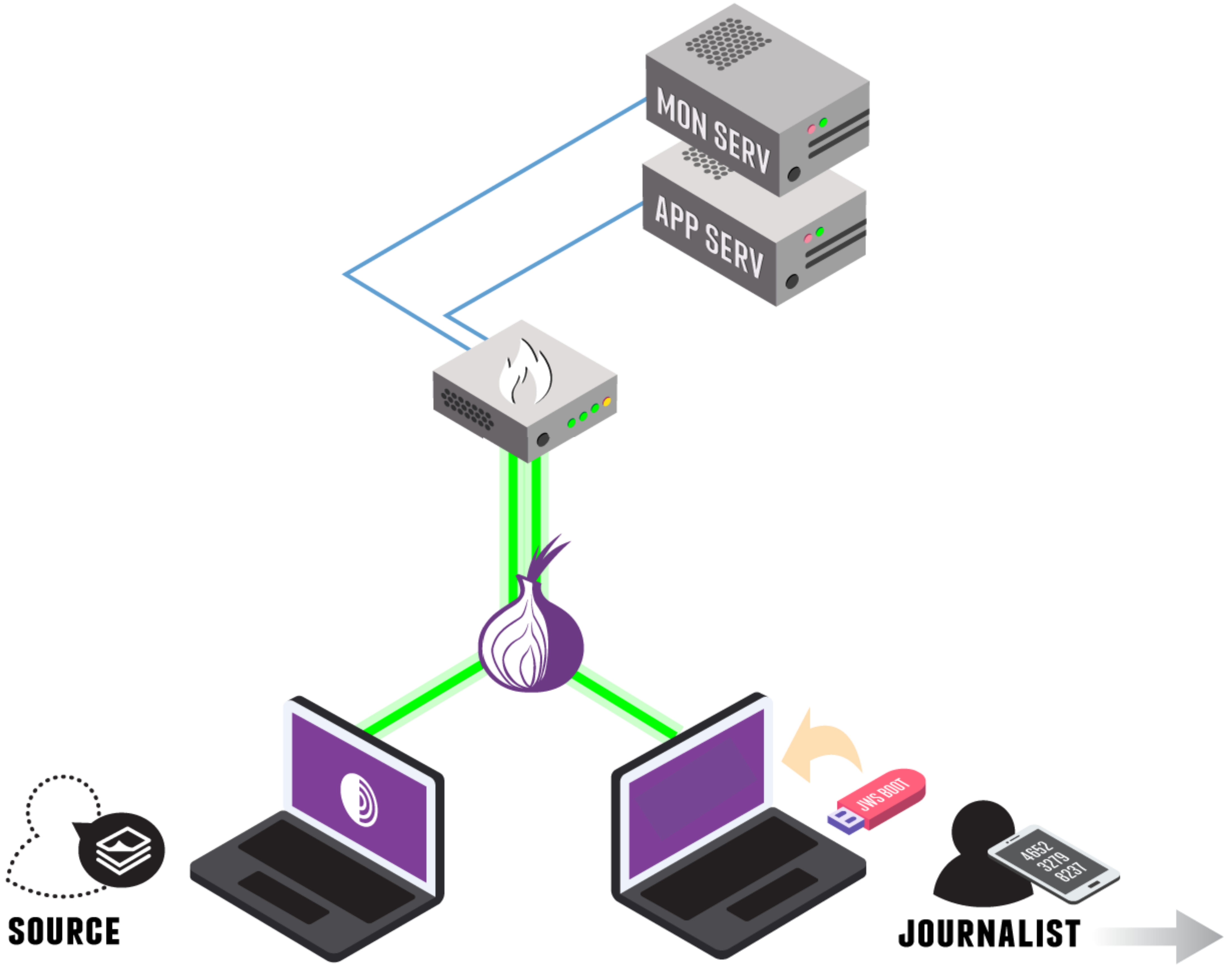
You can write a secure reply to the person who submitted these documents:

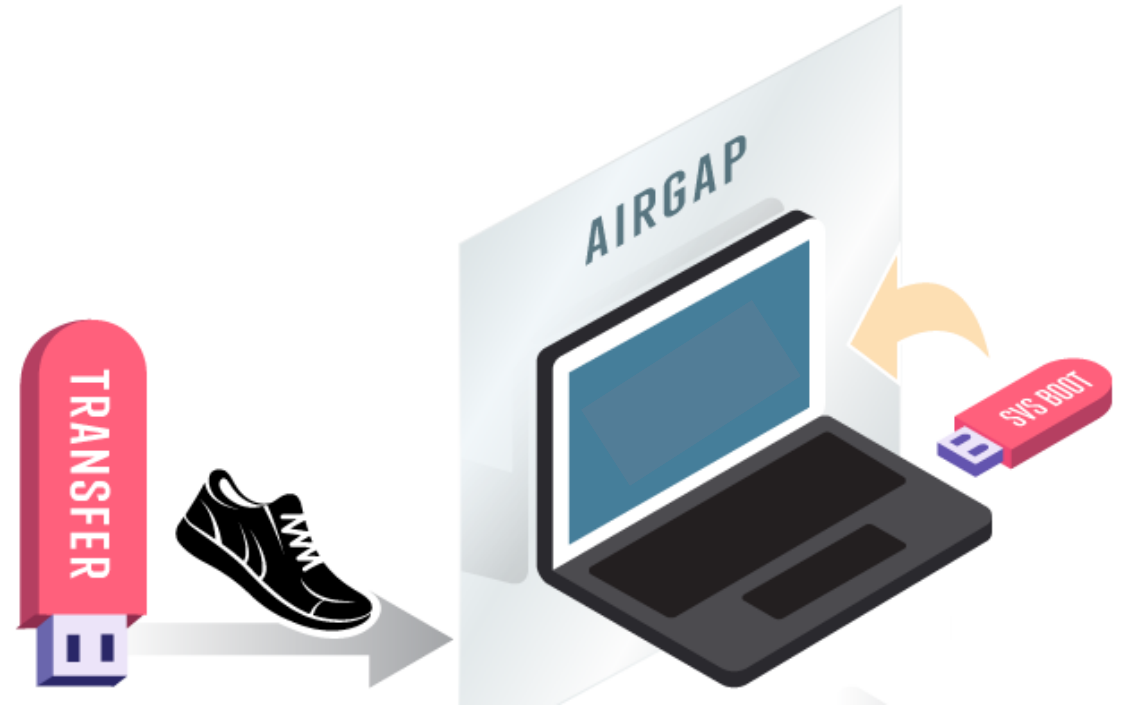
SUBMIT

Current Architecture

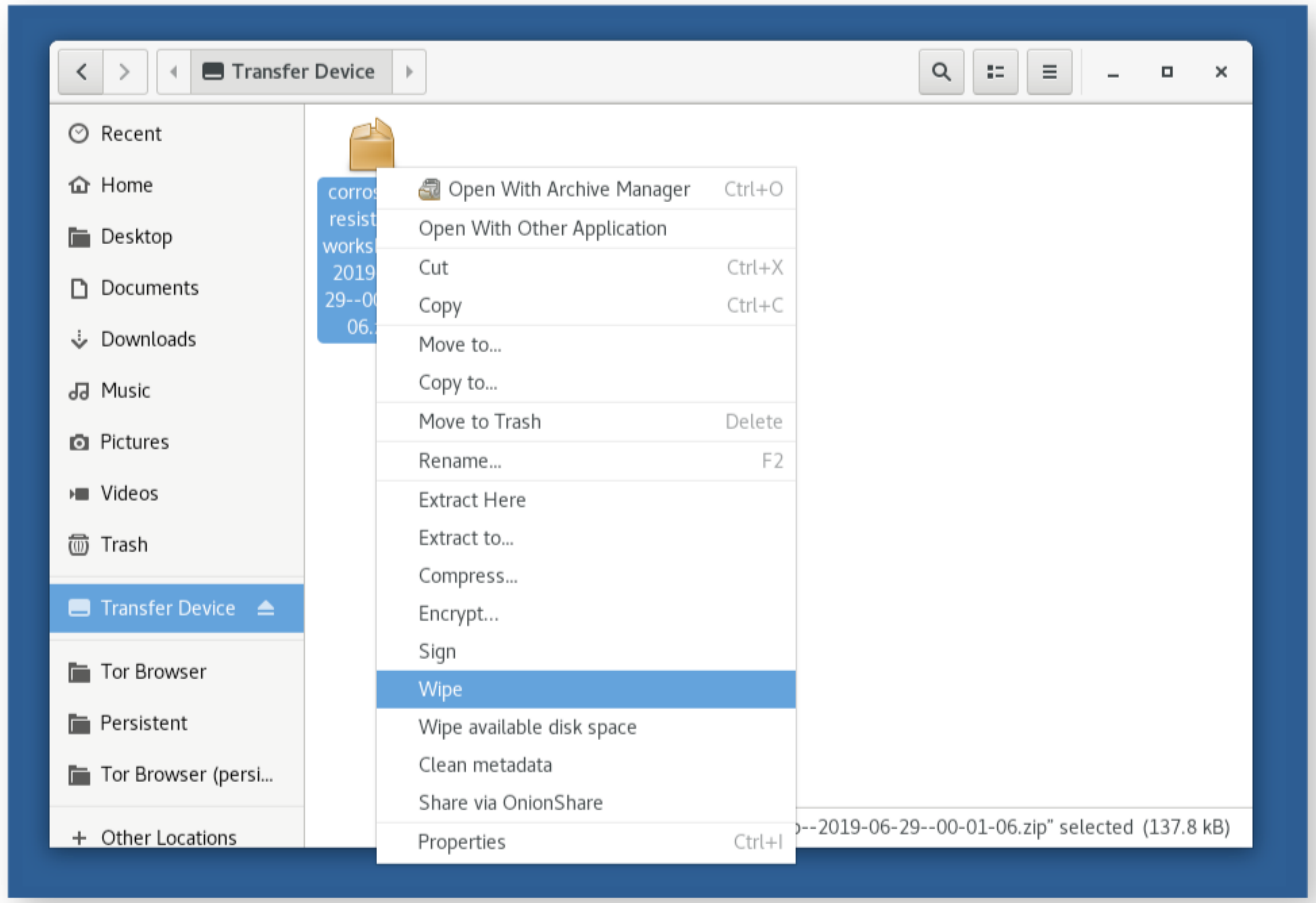


)--2019-06-29--00-01-06.zip" selected (137.8 kB)





Current Architecture



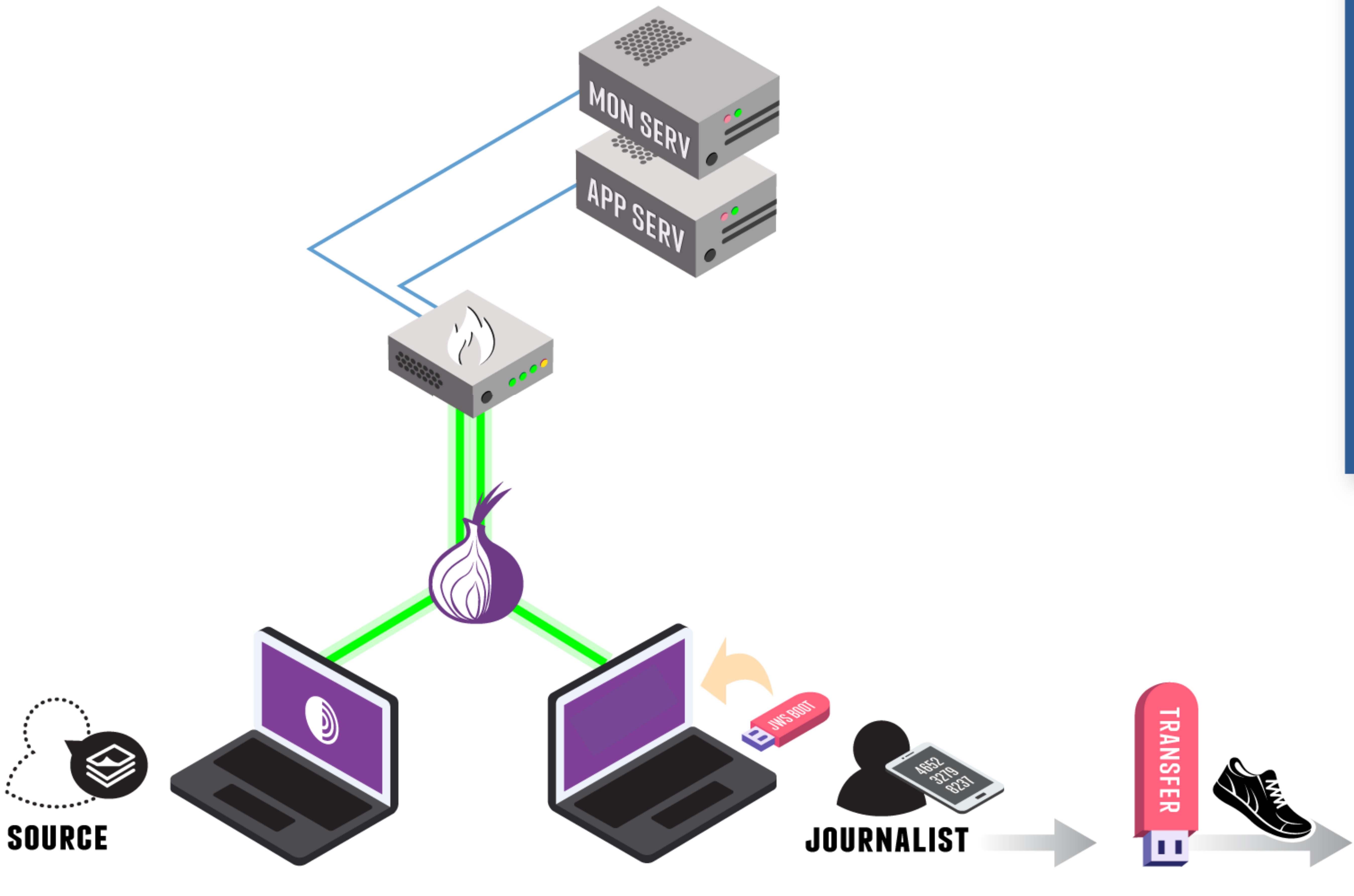
Transfer Device

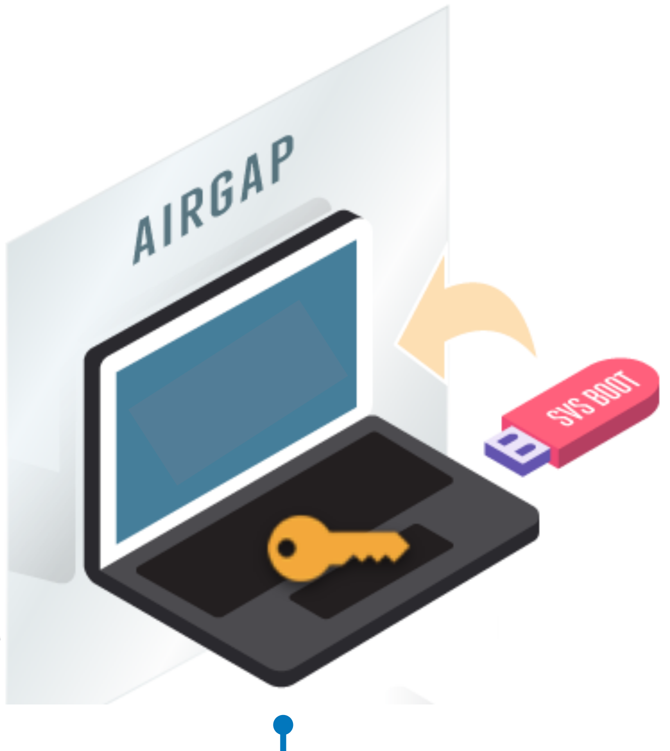
- Recent
- Home
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Trash
- Transfer Device
- Tor Browser
- Persistent
- Tor Browser (persi...
- + Other Locations

corro resist works 2019 29--0 06.

Open With Archive Manager	Ctrl+O
Open With Other Application	
Cut	Ctrl+X
Copy	Ctrl+C
Move to...	
Copy to...	
Move to Trash	Delete
Rename...	F2
Extract Here	
Extract to...	
Compress...	
Encrypt...	
Sign	
Wipe	
Wipe available disk space	
Clean metadata	
Share via OnionShare	
Properties	Ctrl+I

--2019-06-29--00-01-06.zip" selected (137.8 kB)

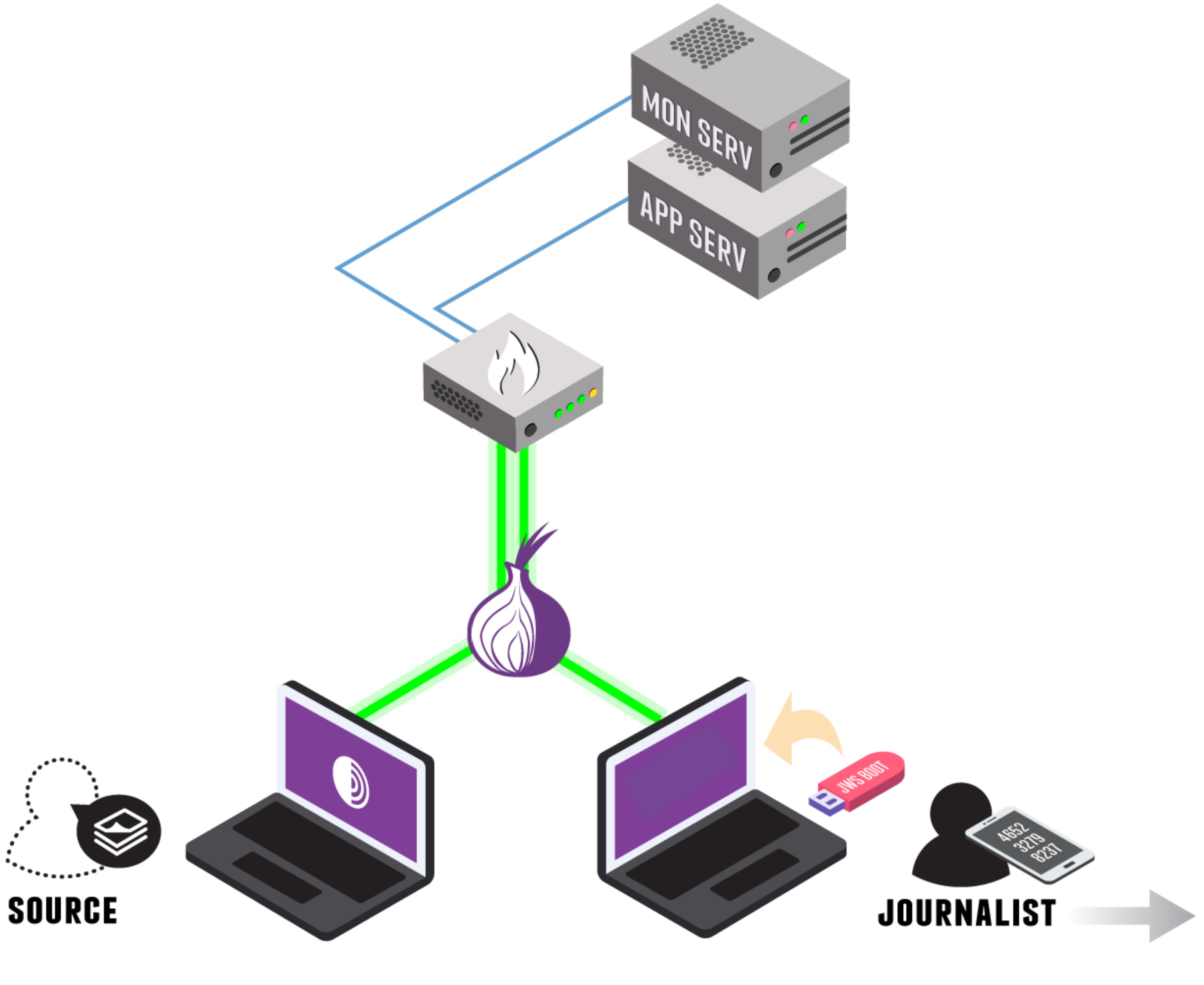


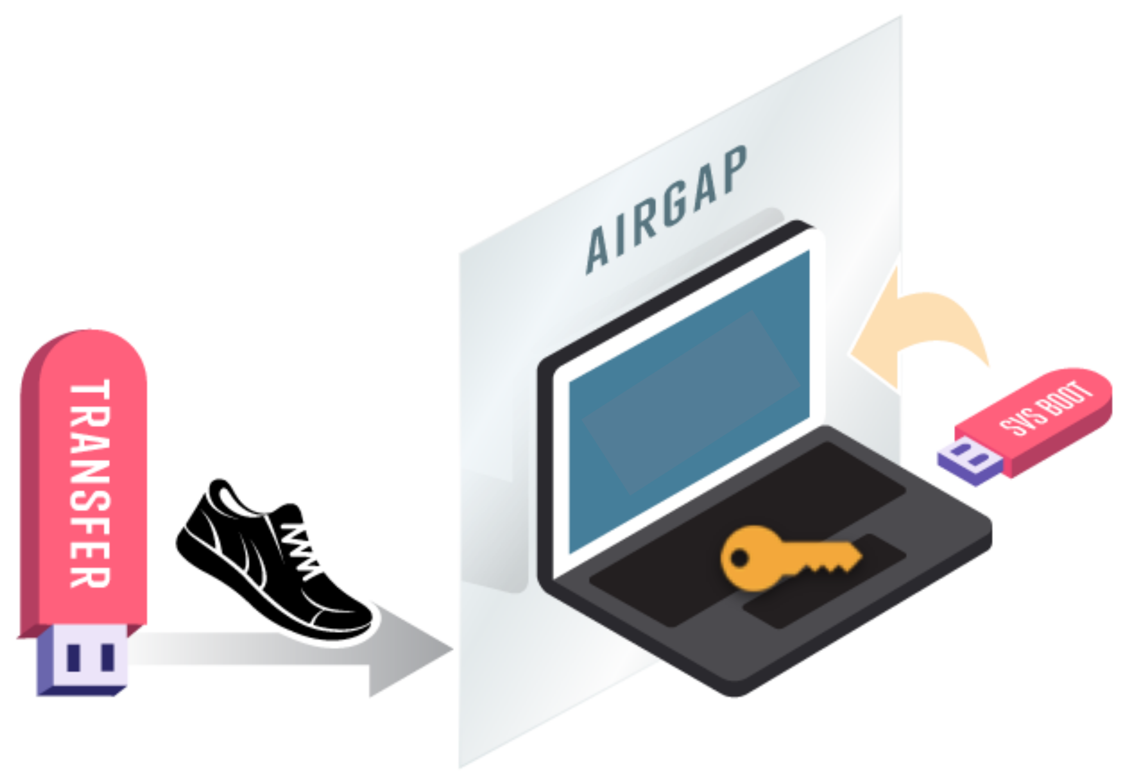


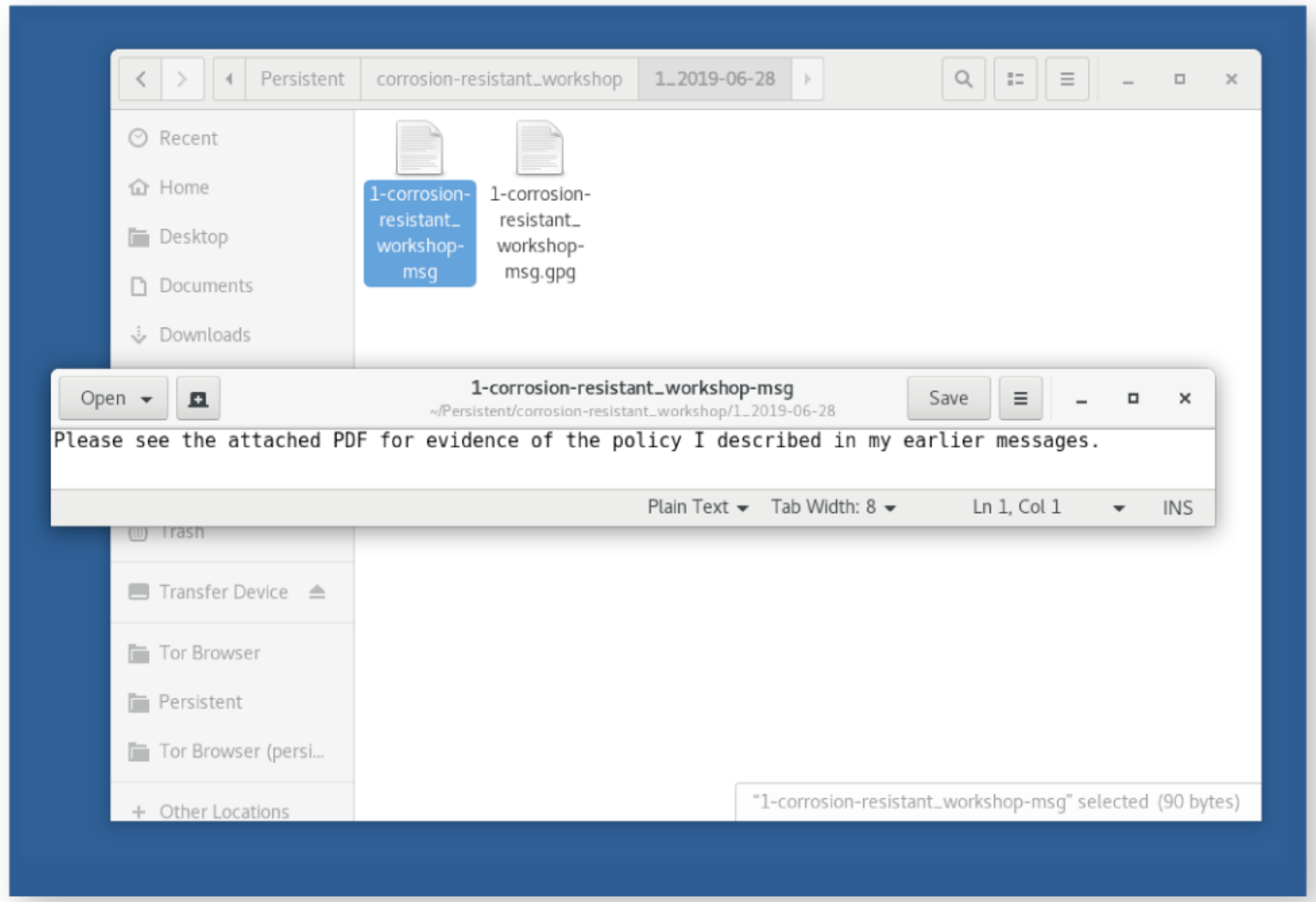
Private key to decrypt documents only in the air-gap environment.

SECUREDROP

Current Architecture






Persistent
corrosion-resistant_workshop
1_2019-06-28
Recent
Home
Desktop
Documents
Downloads
Trash
Transfer Device
Tor Browser
Persistent
Tor Browser (persi...
+ Other Locations
1-corrosion-resistant_workshop-msg
1-corrosion-resistant_workshop-msg.gpg
Open
Save
1-corrosion-resistant_workshop-msg
~/Persistent/corrosion-resistant_workshop/1_2019-06-28
Plain Text
Tab Width: 8
Ln 1, Col 1
INS

```
Please see the attached PDF for evidence of the policy I described in my earlier messages.
```

"1-corrosion-resistant_workshop-msg" selected (90 bytes)

Accomplishments

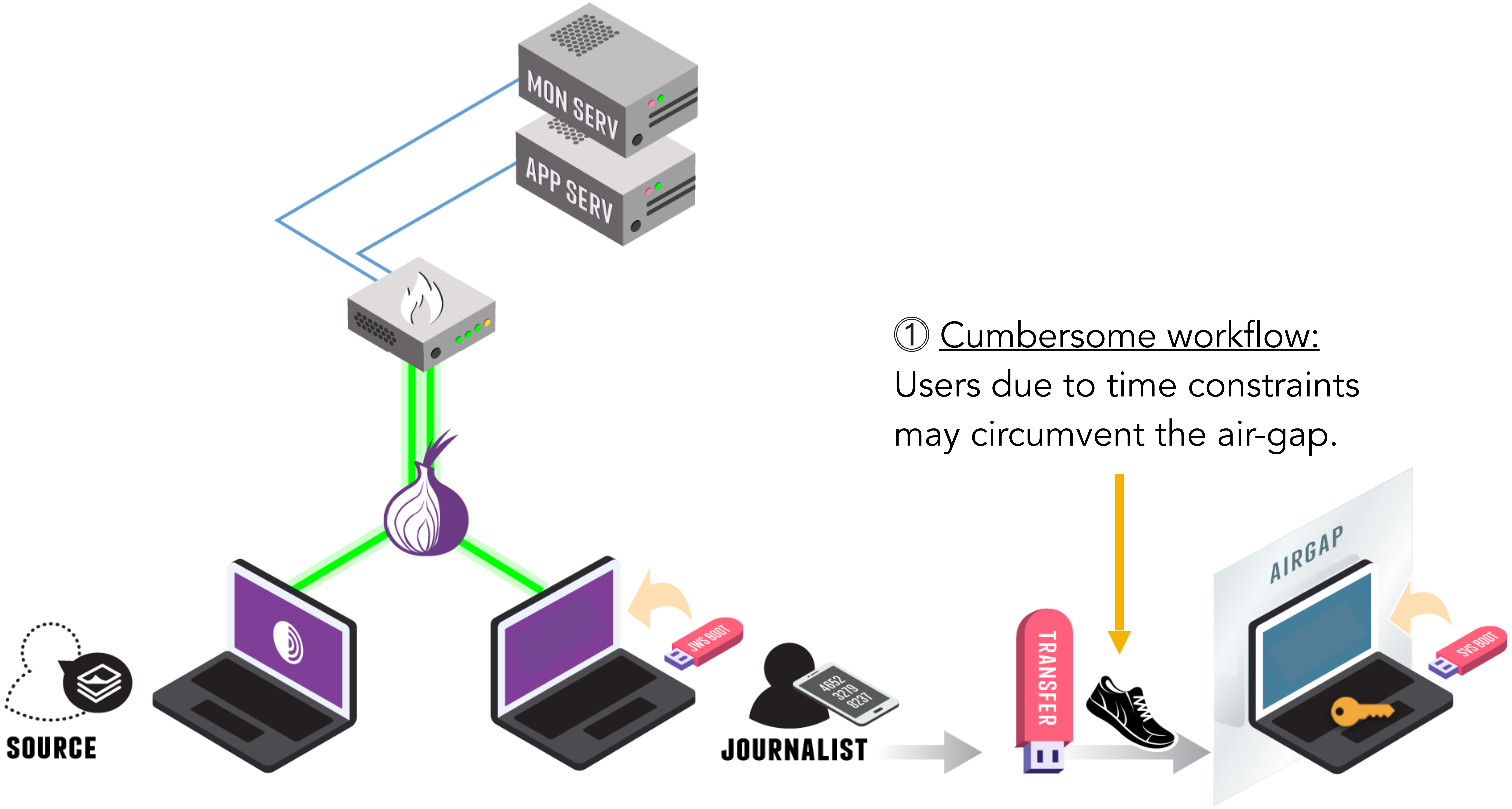
1. Minimized the metadata trail between sources and journalists (source traffic is routed through Tor).

2. No third parties to subpoena.

3. If an attacker gets code execution on the workstation with source data, they need to jump the airgap to exfiltrate any data.

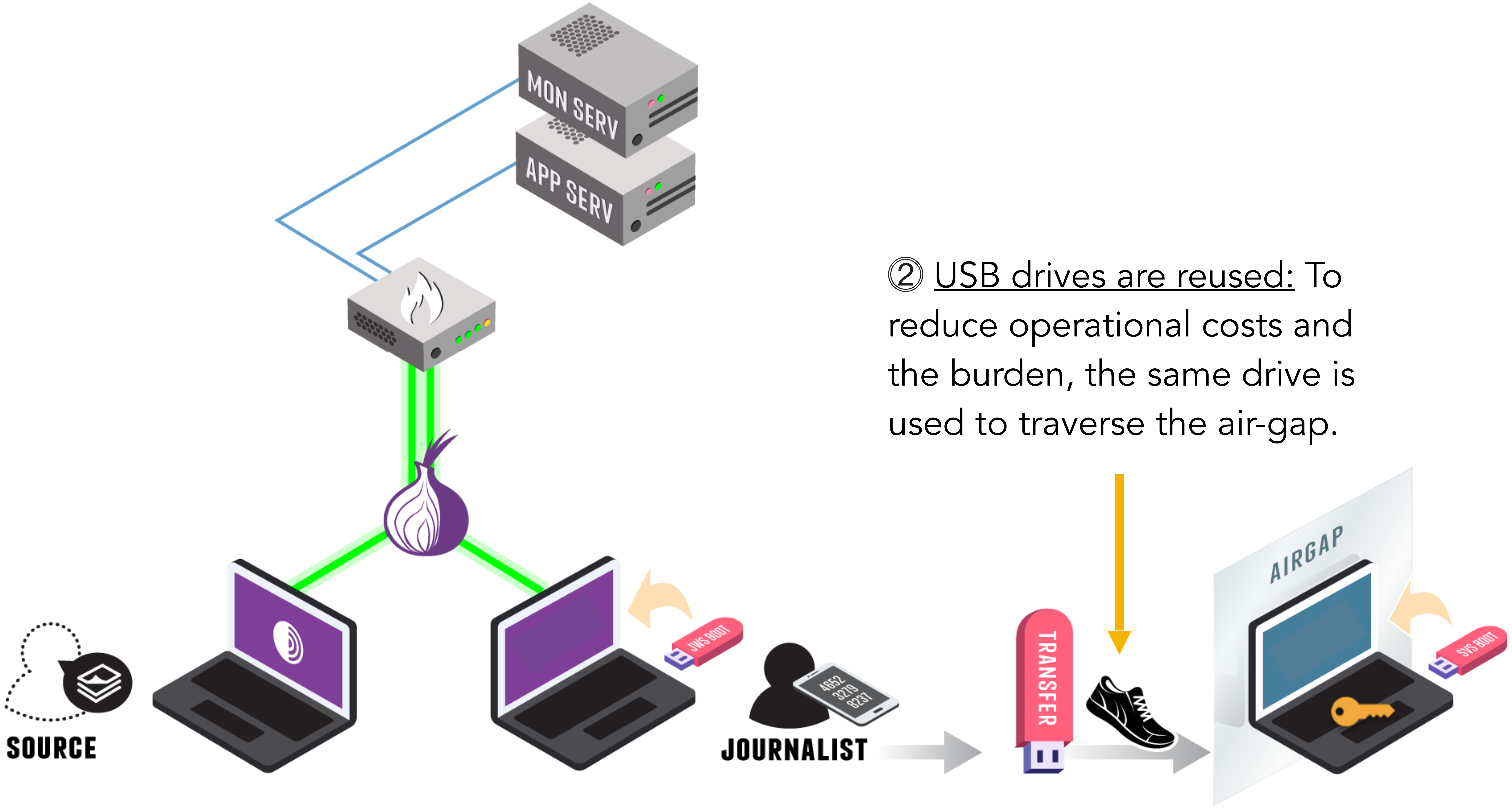
Challenges with the airgap

Current Architecture



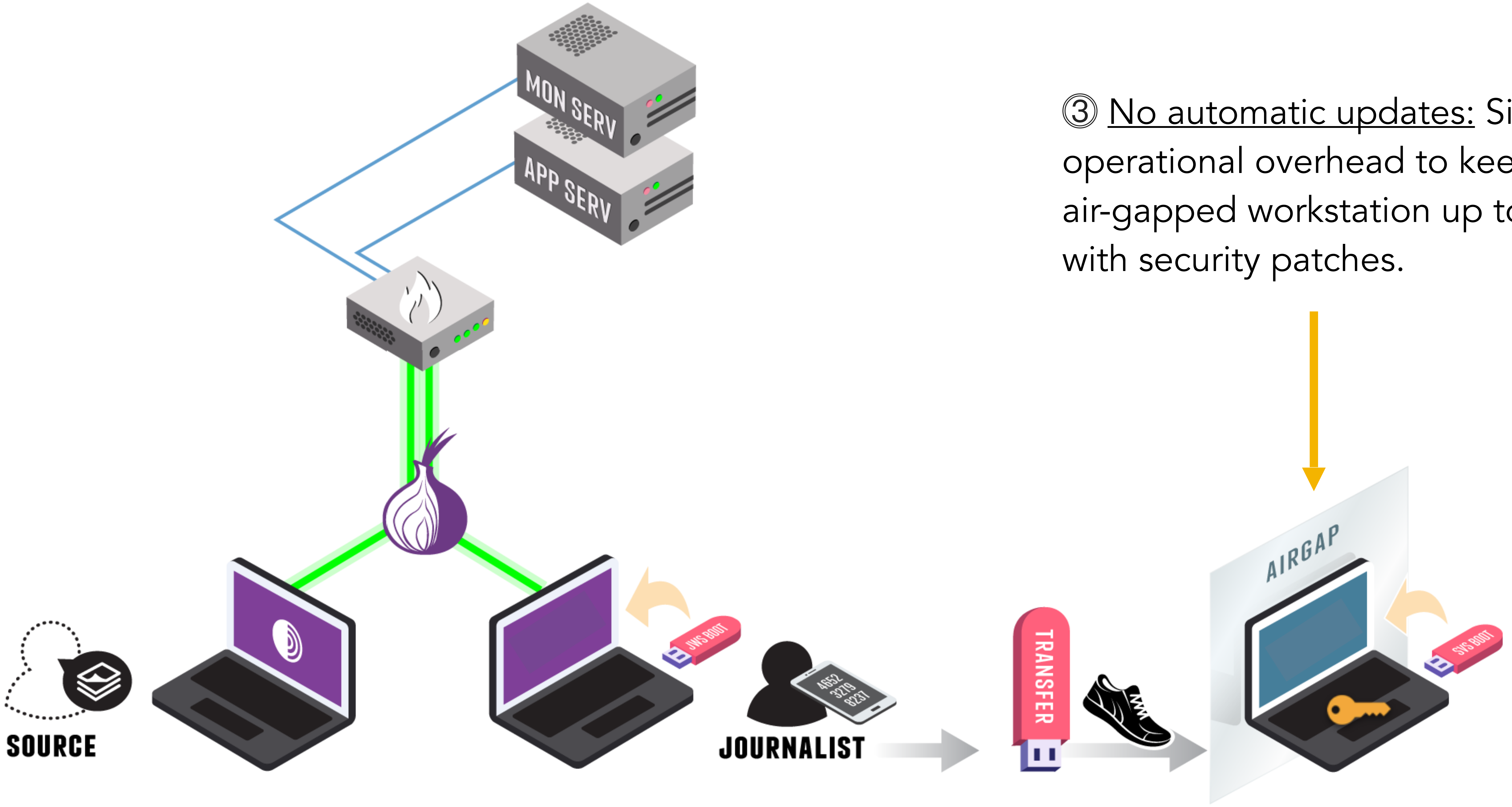
① Cumbersome workflow:
Users due to time constraints may circumvent the air-gap.

Current Architecture



② USB drives are reused: To reduce operational costs and the burden, the same drive is used to traverse the air-gap.

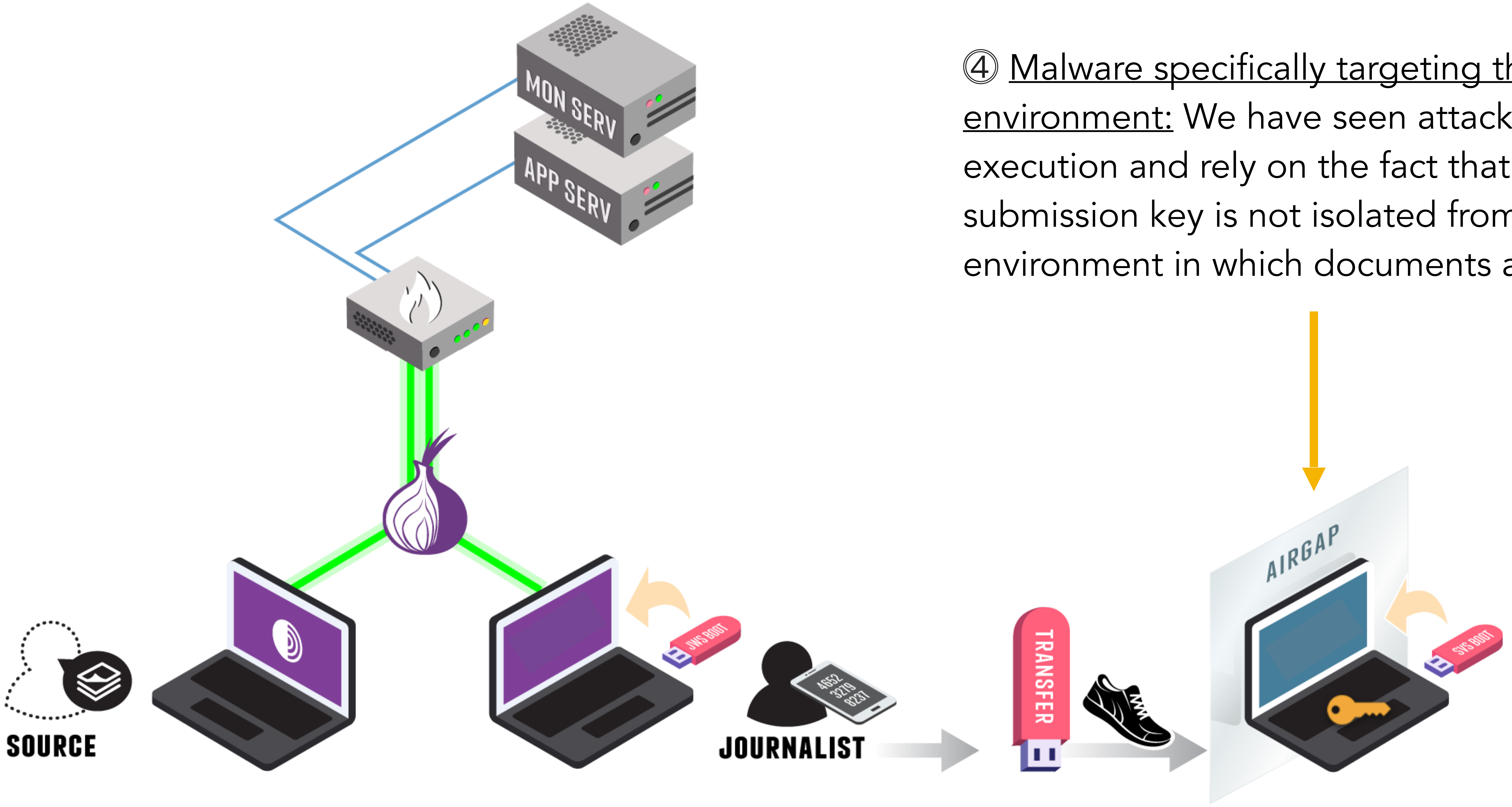
Current Architecture



③ <u>No automatic updates:</u> Significant operational overhead to keeping an air-gapped workstation up to date with security patches.

Current Architecture

④ Malware specifically targeting the air-gap environment: We have seen attacks get code execution and rely on the fact that the submission key is not isolated from the environment in which documents are opened.



Take 2

Technical Goals

1. Ensure known vulnerabilities are patched.
2. Isolate the submission private key from potentially malicious submissions.
3. Isolate each source’s documents.
4. Recover from an attacker getting code execution in the VM used to open submissions.
5. Provide defense in depth to defend against unknown vulnerabilities.

SECUREDROP

Design considerations

1. Needs to be maintainable by non-specialist IT staff at a news organization.

2. Needs to be usable by journalists.

QubesOS: single-user desktop-based Xen distribution

QUBES OS

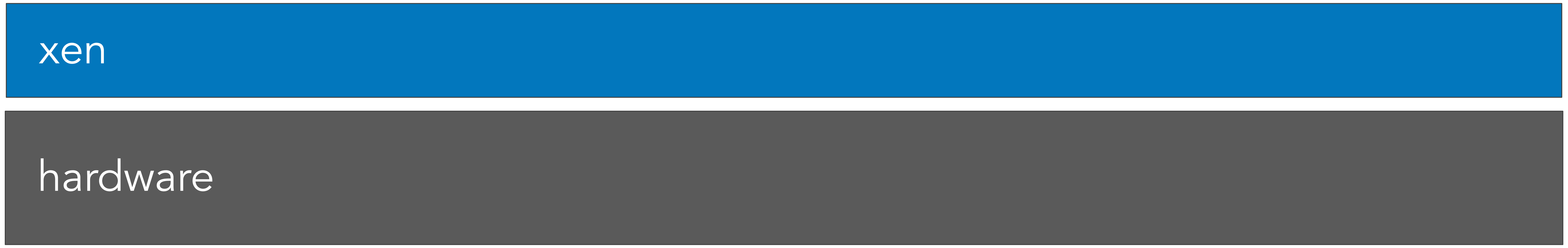
A REASONABLY SECURE OPERATING SYSTEM

QubesOS: single-user desktop-based Xen distribution

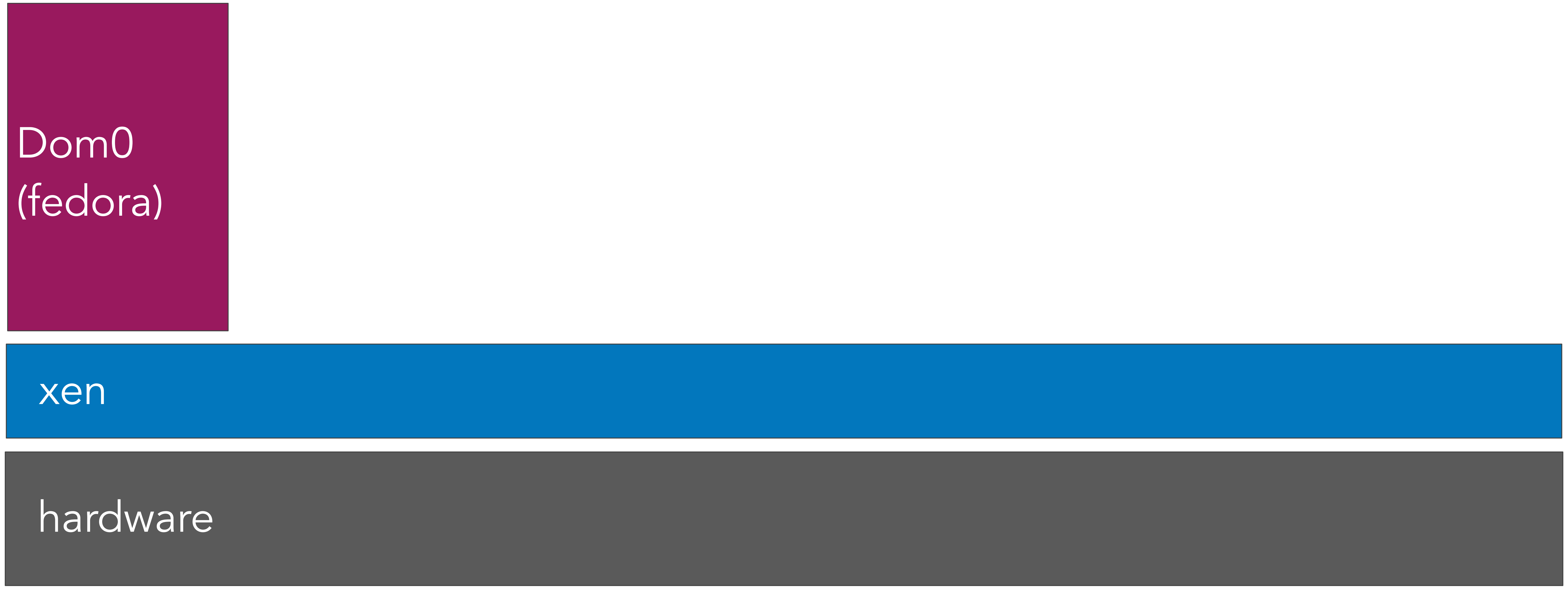
QubesOS: single-user desktop-based Xen distribution

QUBES OS

A REASONABLY SECURE OPERATING SYSTEM

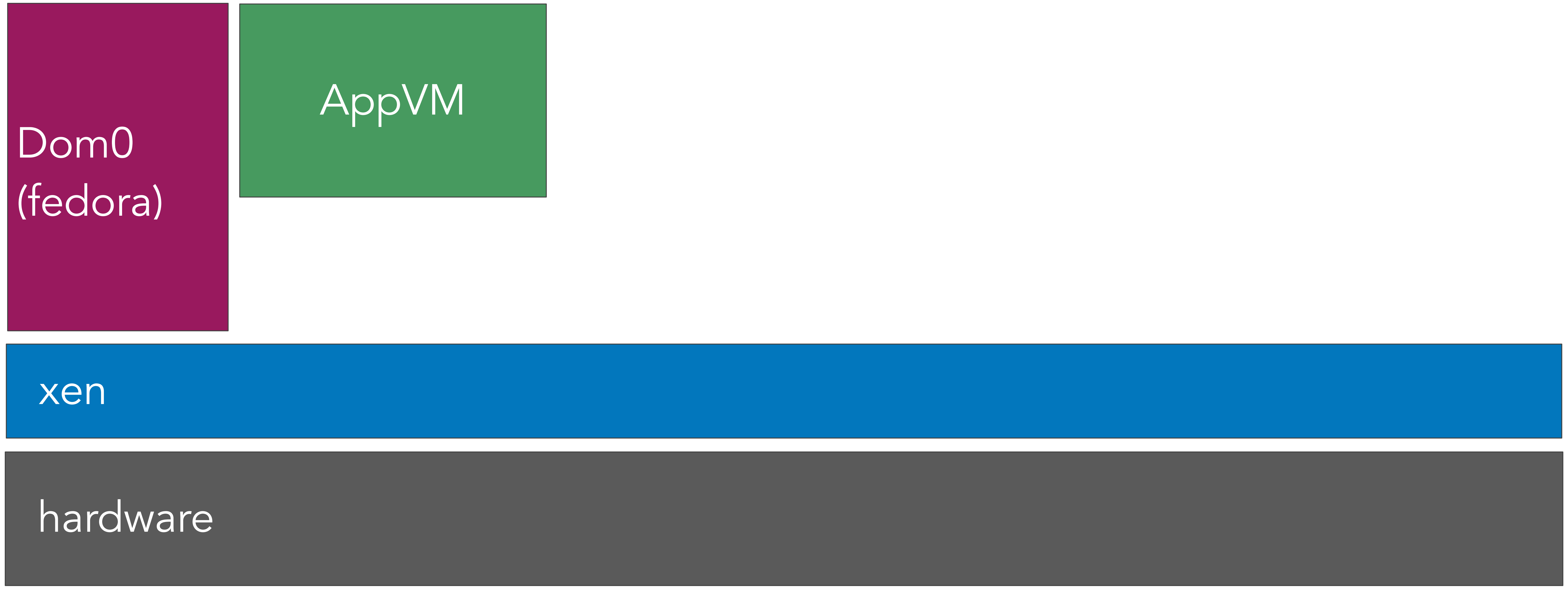


QubesOS: single-user desktop-based Xen distribution



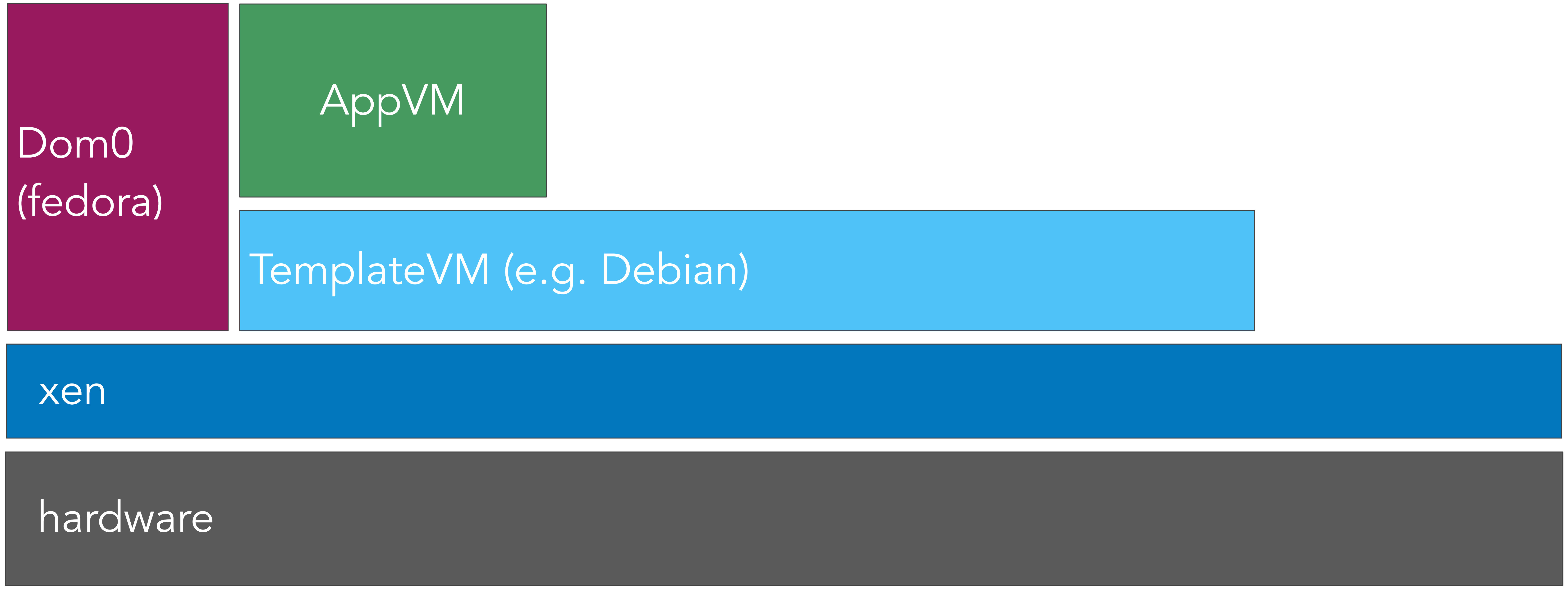
QubesOS: single-user desktop-based Xen distribution

QUBES OS
A REASONABLY SECURE OPERATING SYSTEM



SECUREDROP

QubesOS: single-user desktop-based Xen distribution



Dom0 (fedora)

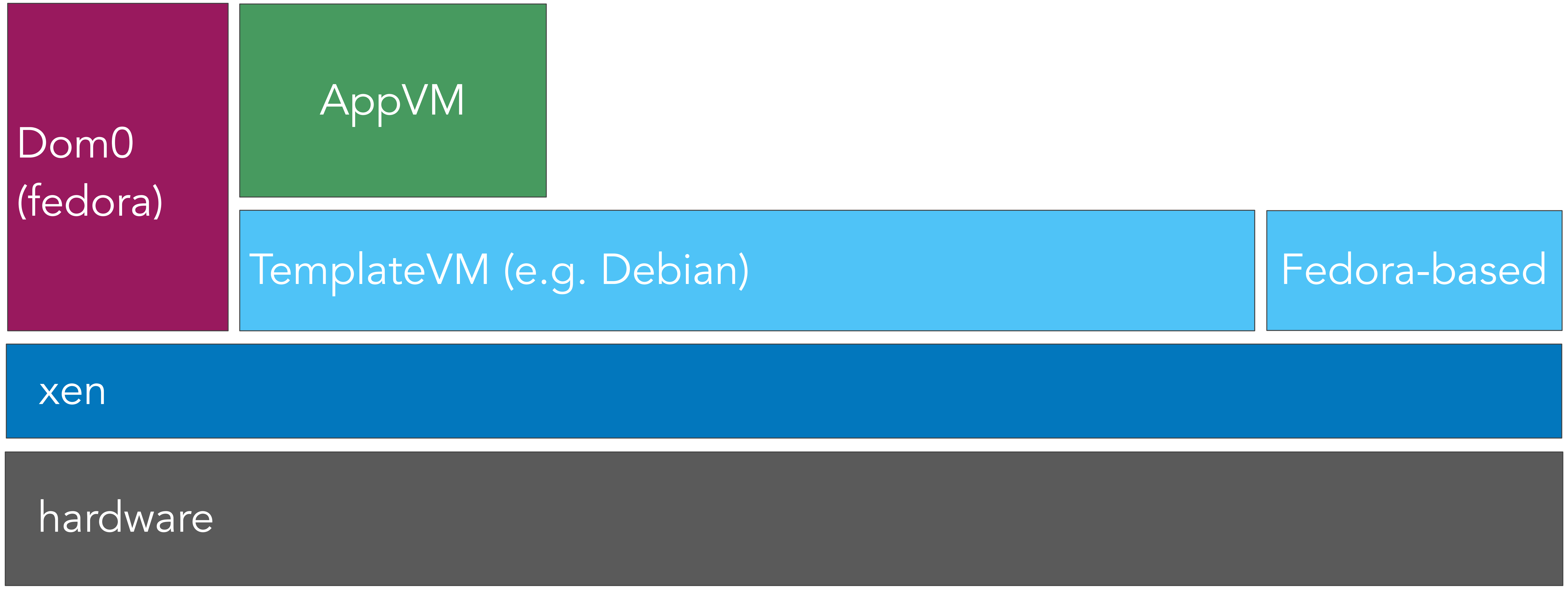
AppVM

TemplateVM (e.g. Debian)

xen

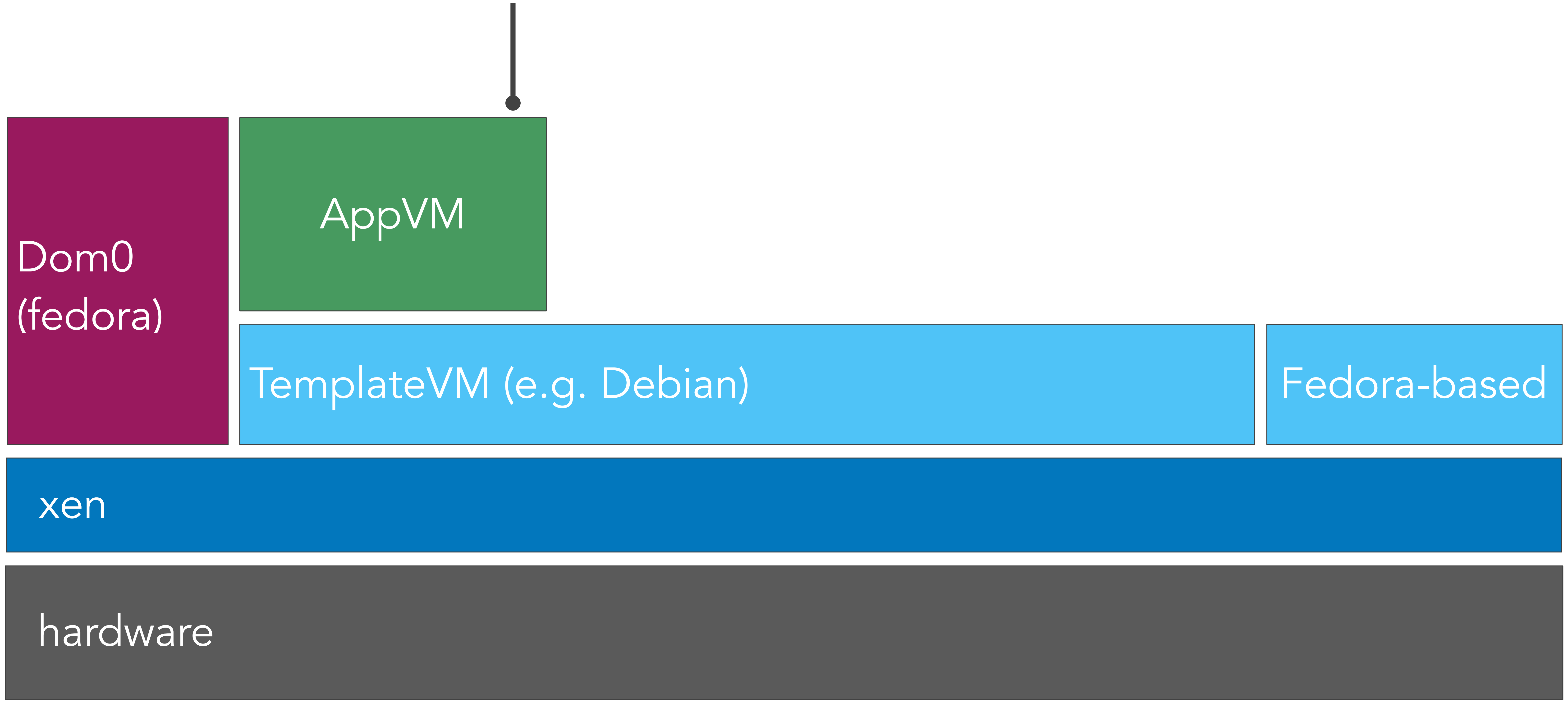
hardware

QubesOS: single-user desktop-based Xen distribution

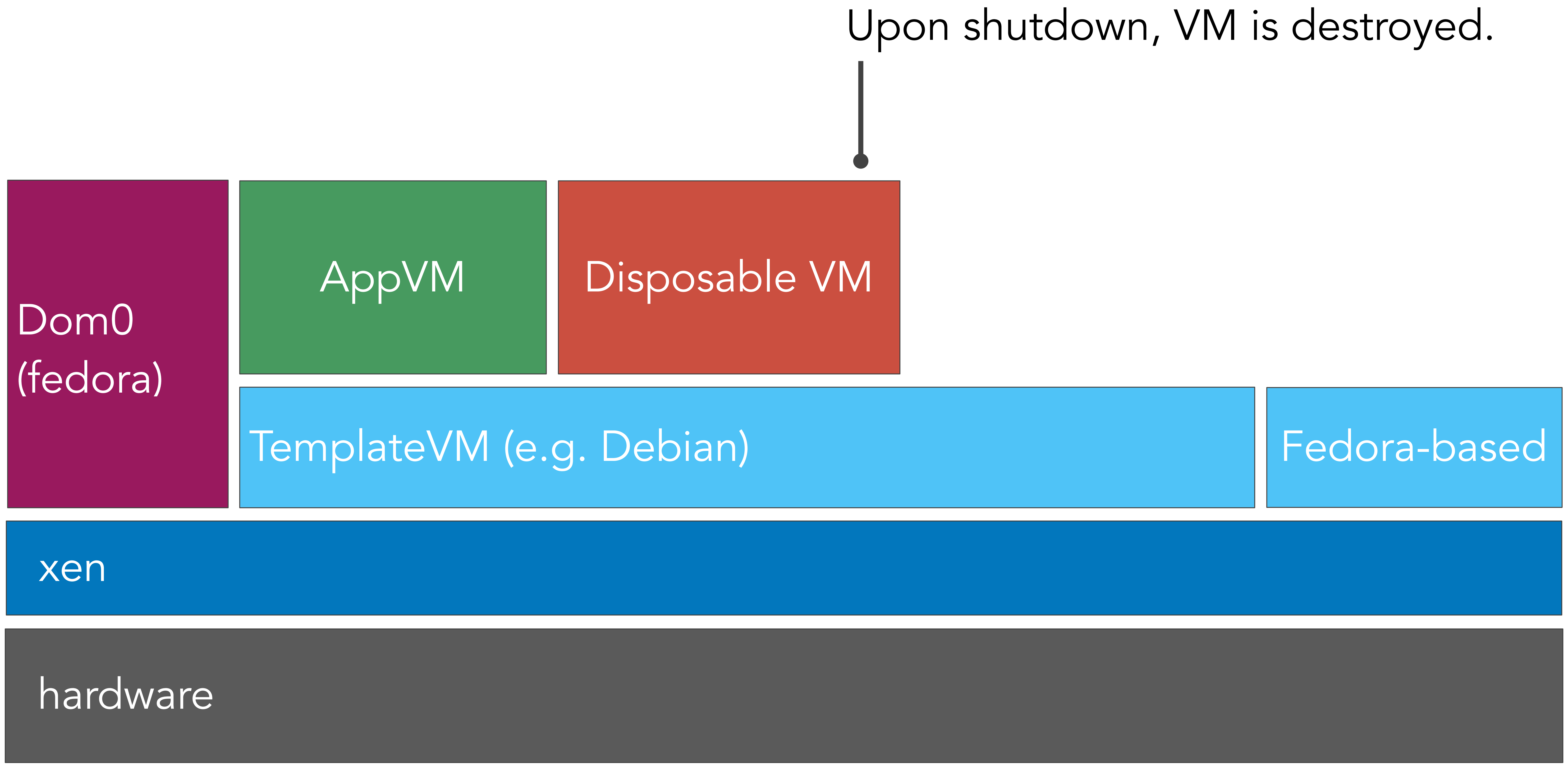


QubesOS: single-user desktop-based Xen distribution

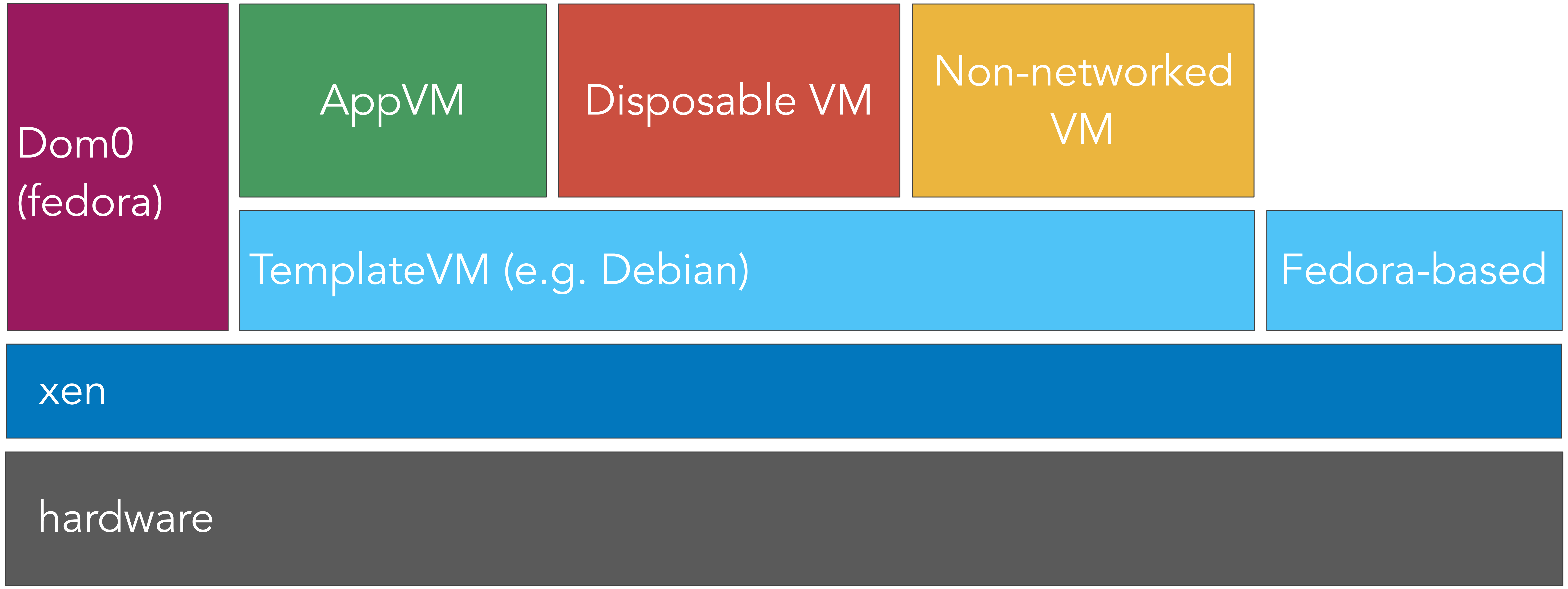
Only `/home`, `/usr/local`, `/rw/config` will persist through a reboot, otherwise AppVM state is reset to the base TemplateVM



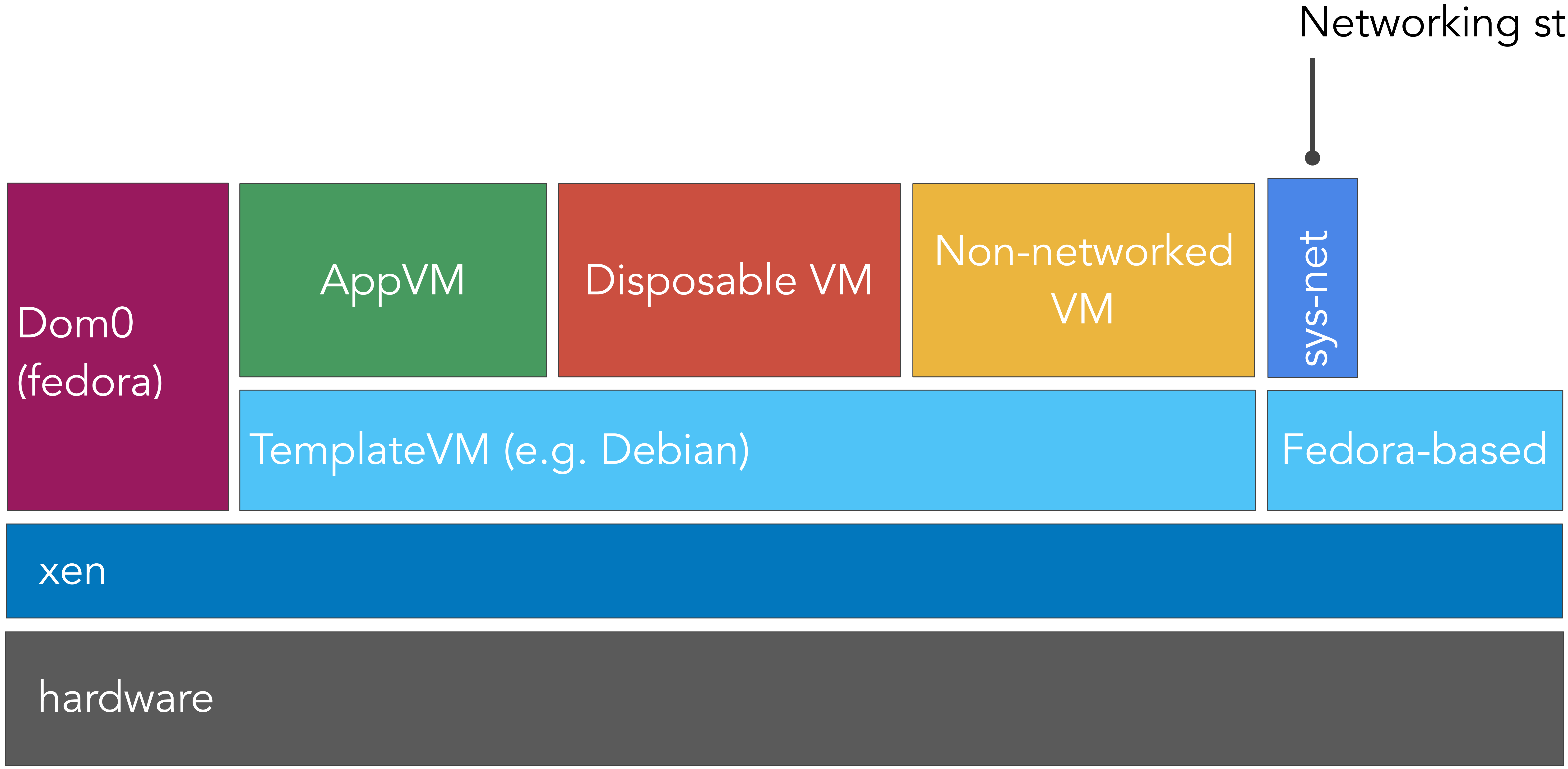
QubesOS: single-user desktop-based Xen distribution



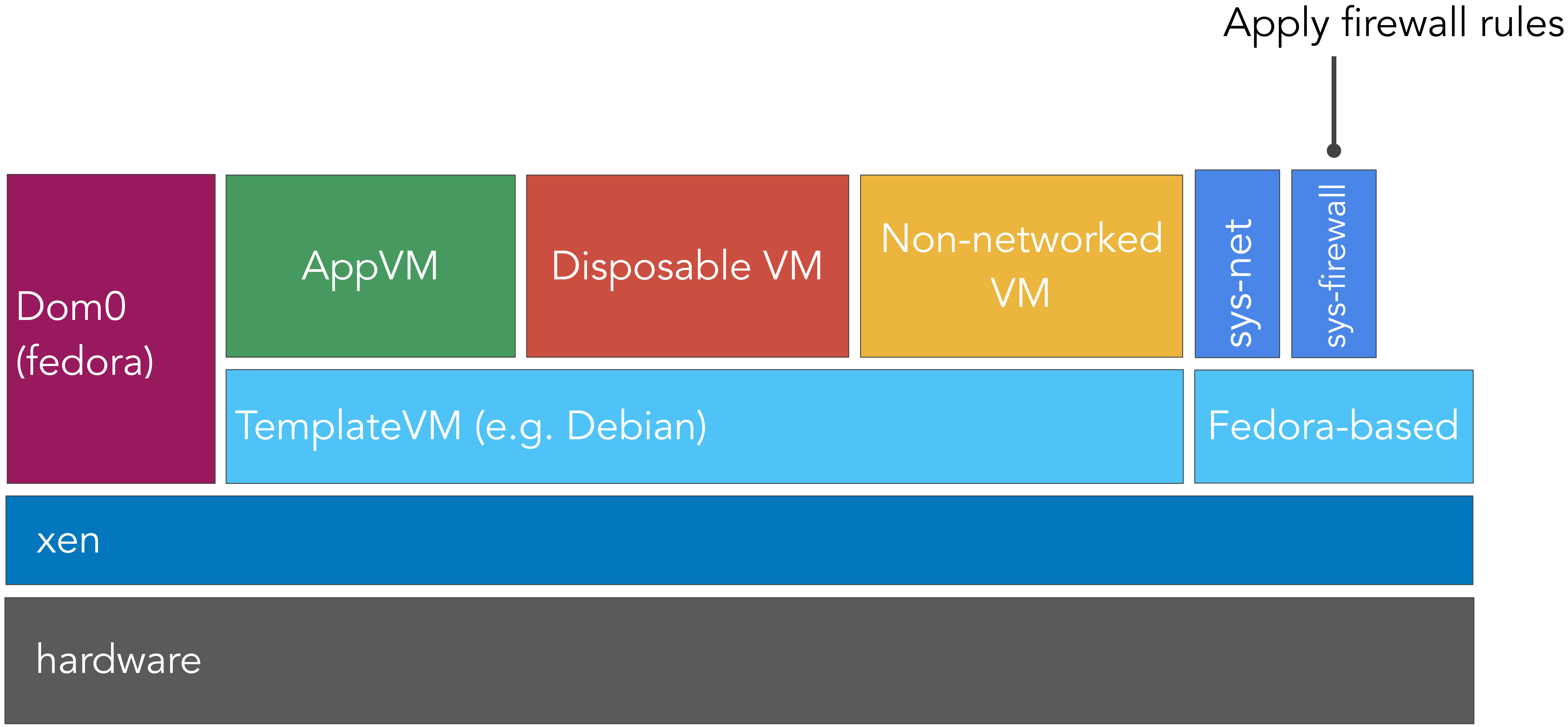
QubesOS: single-user desktop-based Xen distribution



QubesOS: single-user desktop-based Xen distribution



QubesOS: single-user desktop-based Xen distribution

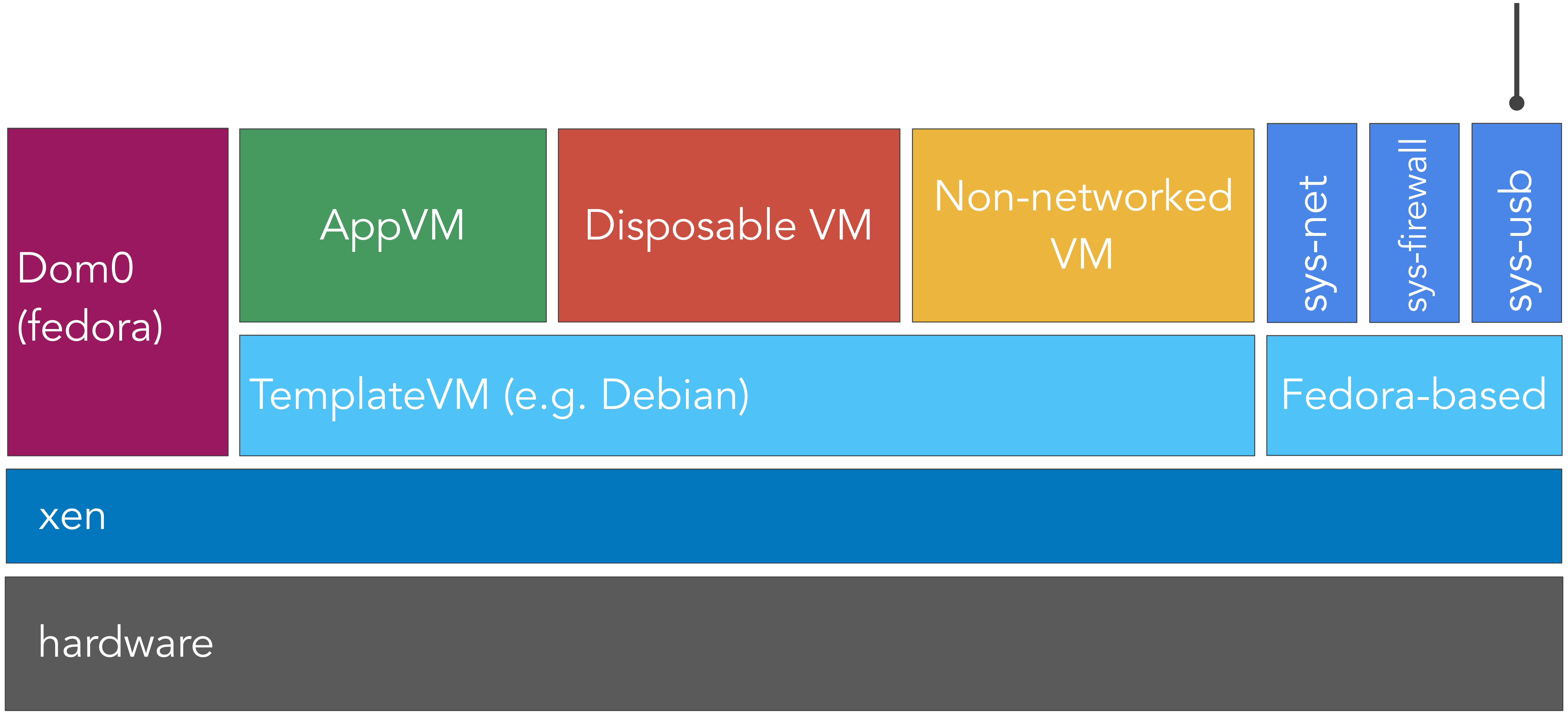


QUBES OS
A REASONABLY SECURE OPERATING SYSTEM

SECUREDROP

QubesOS: single-user desktop-based Xen distribution

USB controllers
by default
attached here



Dom0 (fedora)

AppVM

Disposable VM

Non-networked VM

sys-net

sys-firewall

sys-usb

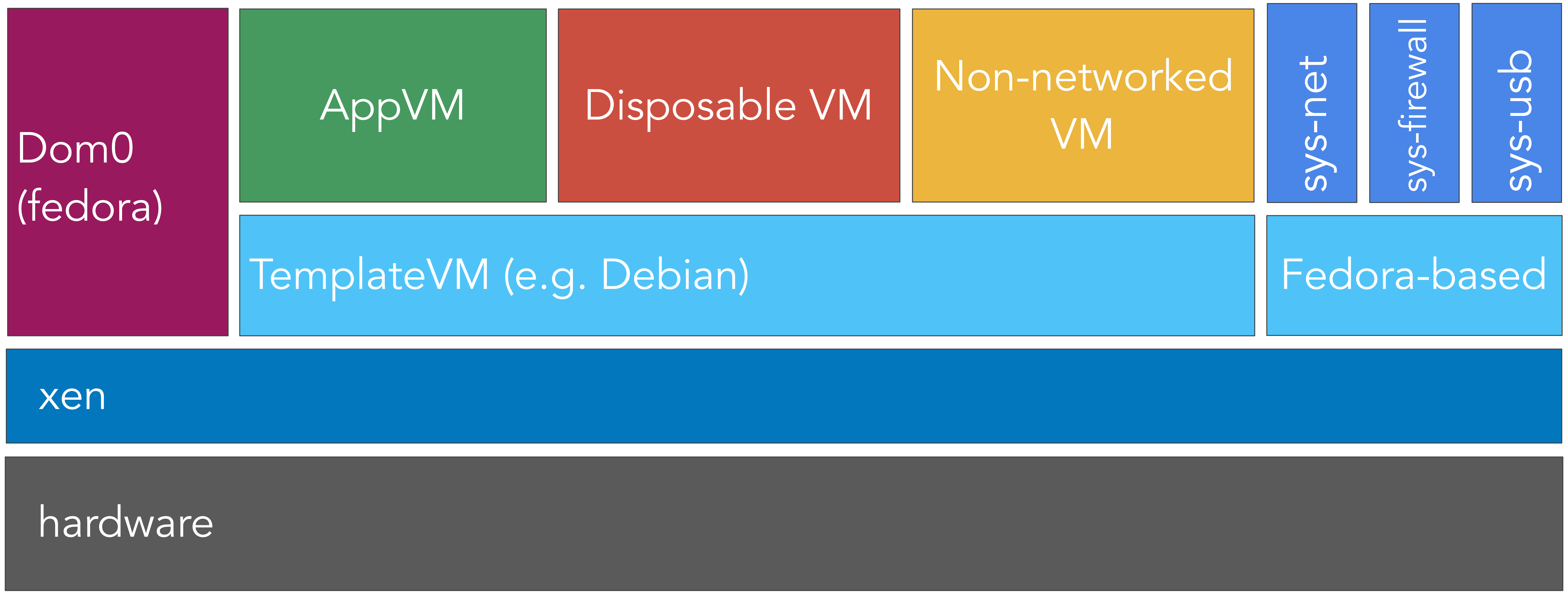
TemplateVM (e.g. Debian)

Fedora-based

xen

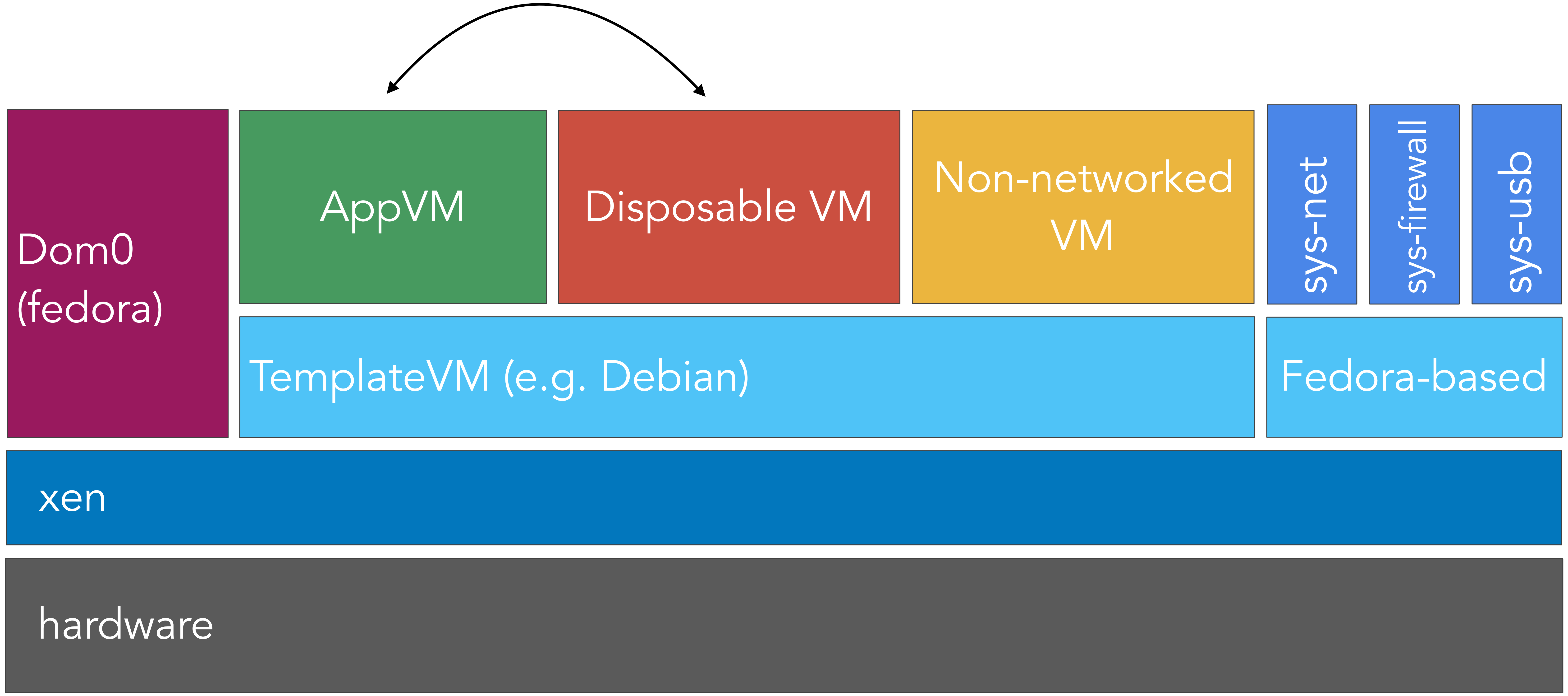
hardware

QubesOS: single-user desktop-based Xen distribution

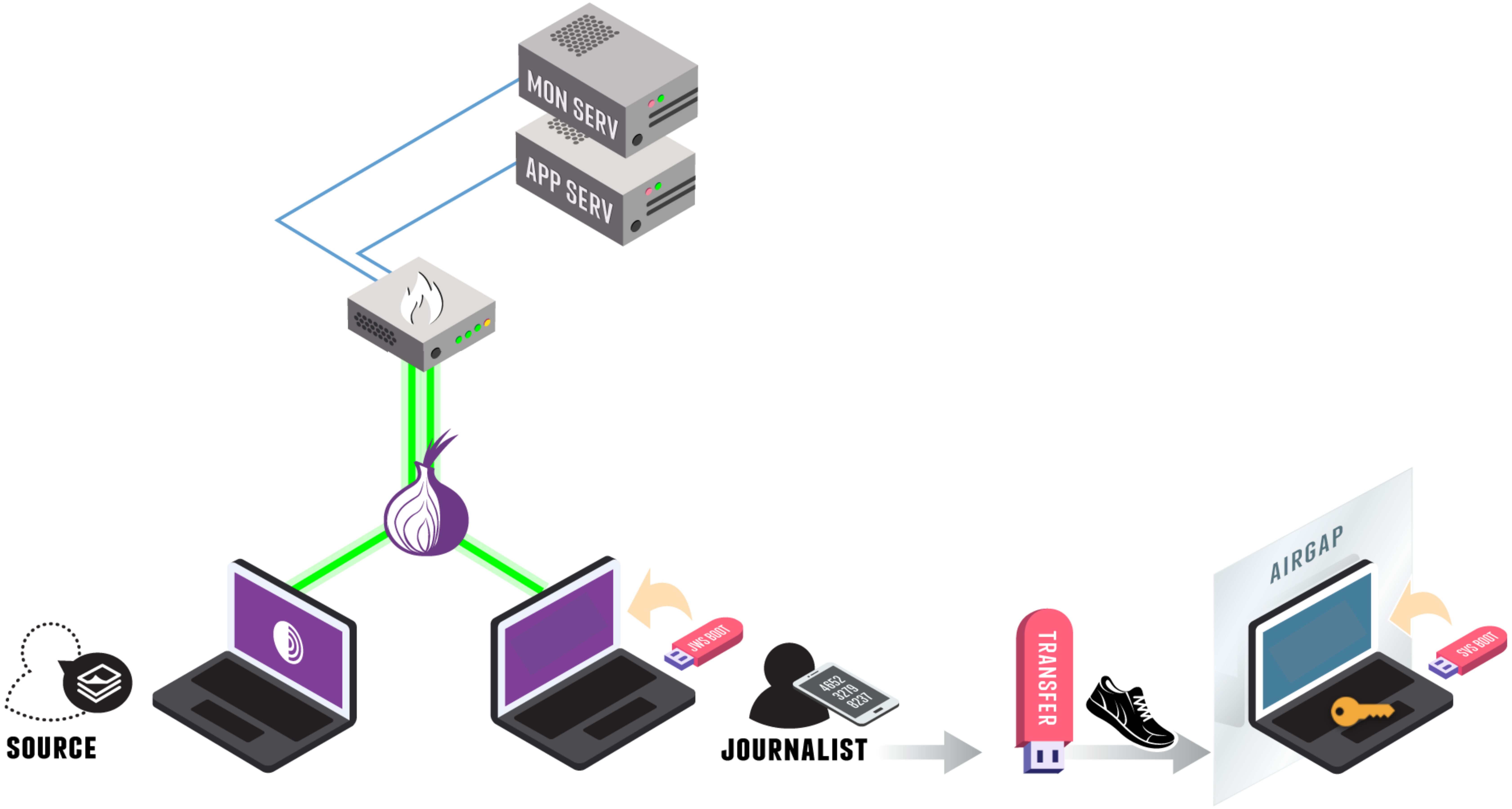


QubesOS: single-user desktop-based Xen distribution

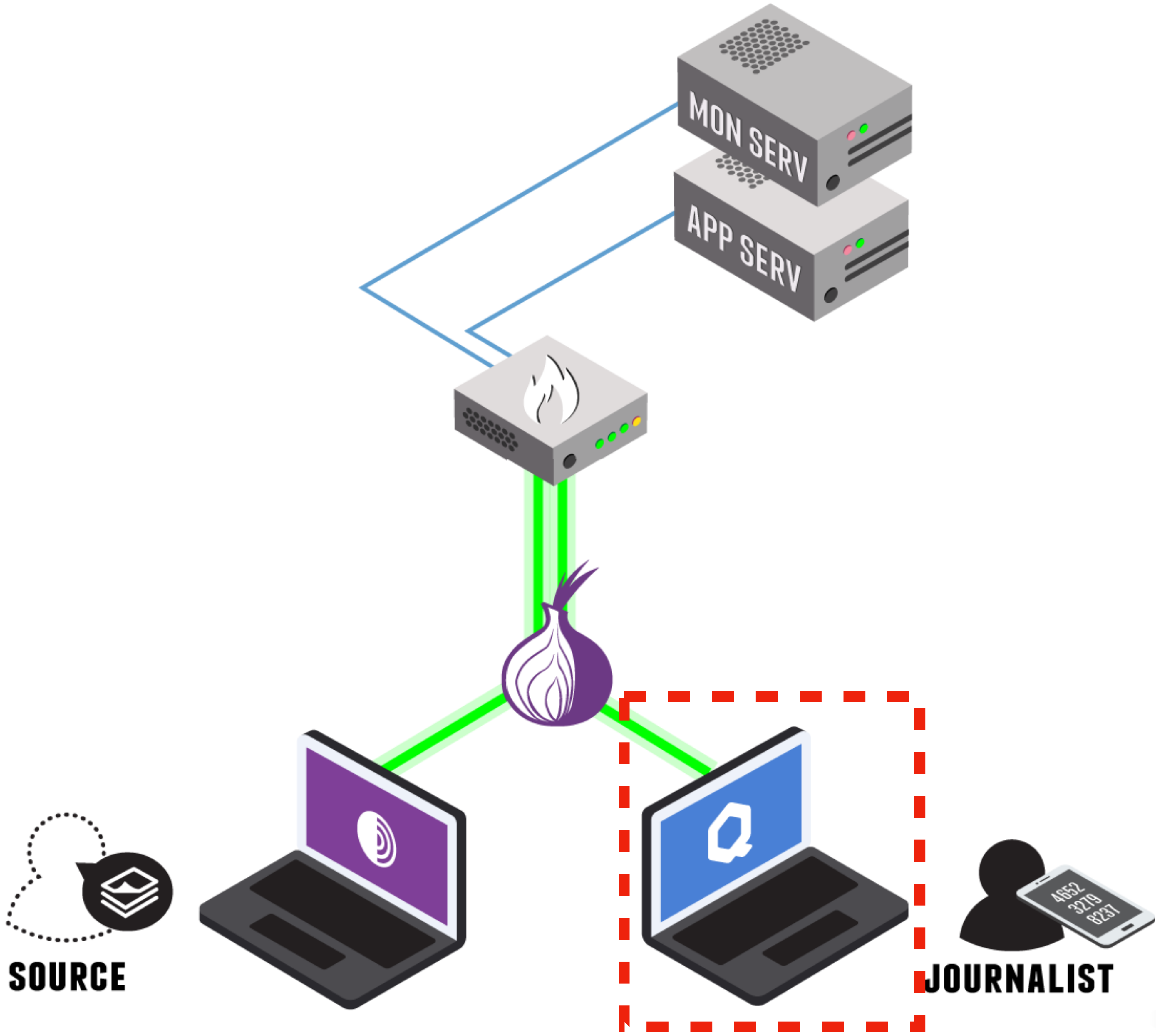
InterVM communication via `qrexec`, based on Xen's `vchan`



Current Architecture



New Architecture



New Architecture

Legend

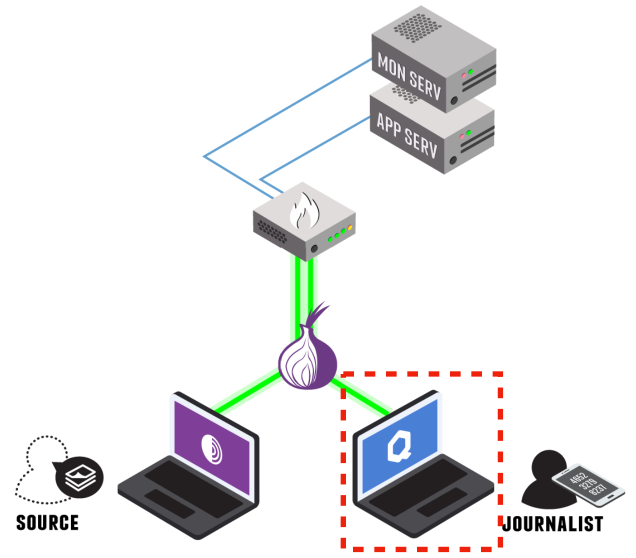
━ qrexec (interVM communication)

🟧 Disposable *and* non-networked AppVM

🟩 Networked AppVM

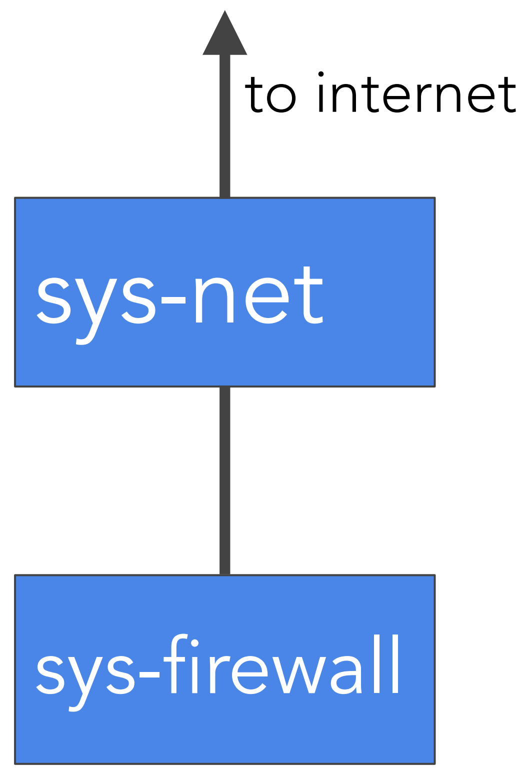
🟨 Non-networked AppVM

🟦 System VM



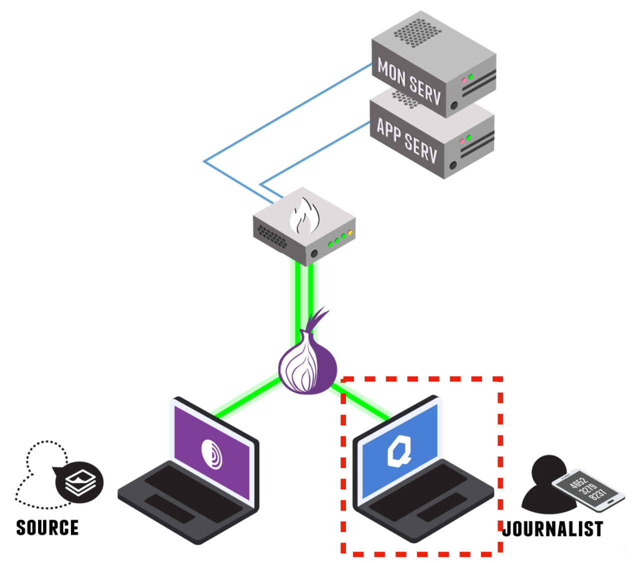
SECUREDROP

New Architecture



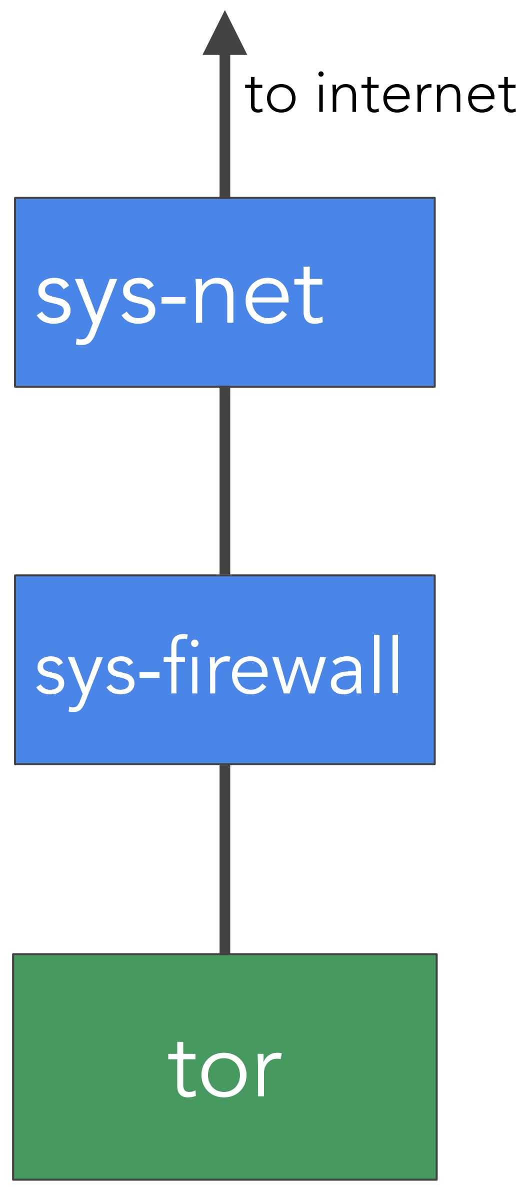
Legend

- ━ qrexec (interVM communication)
- 🟧 Disposable *and* non-networked AppVM
- 🟩 Networked AppVM
- 🟨 Non-networked AppVM
- 🟦 System VM



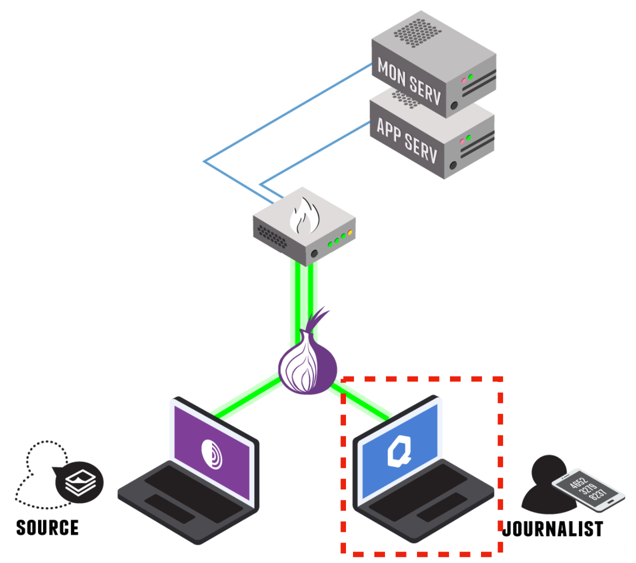
SECUREDROP

New Architecture

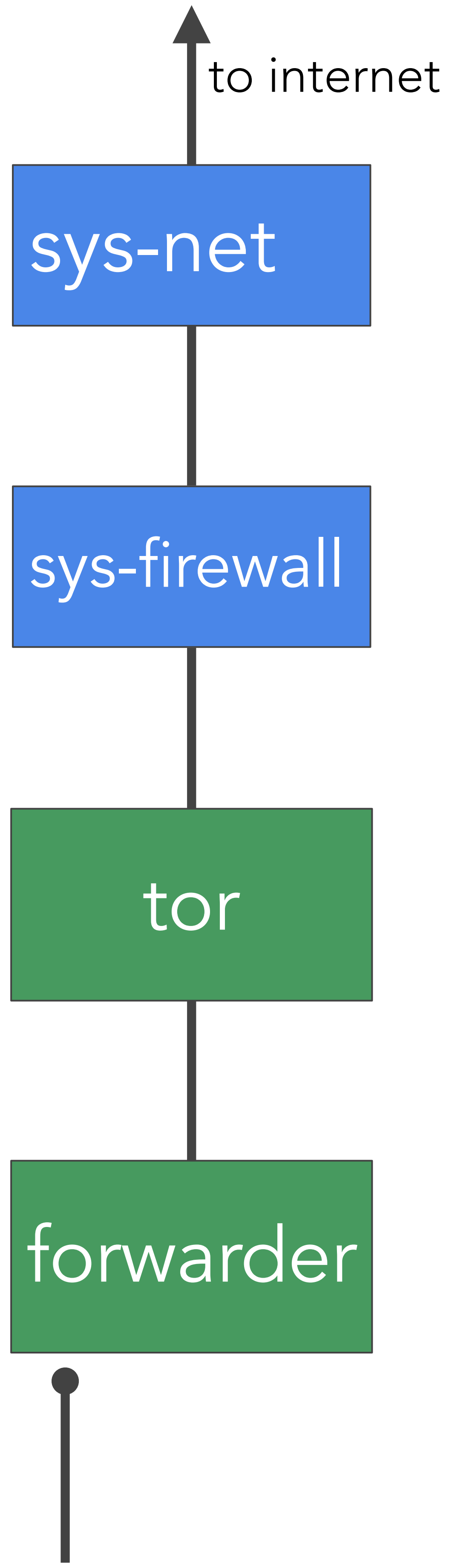


Legend

- ▬ qrexec (interVM communication)
- 🟧 Disposable *and* non-networked AppVM
- 🟩 Networked AppVM
- 🟨 Non-networked AppVM
- 🟦 System VM



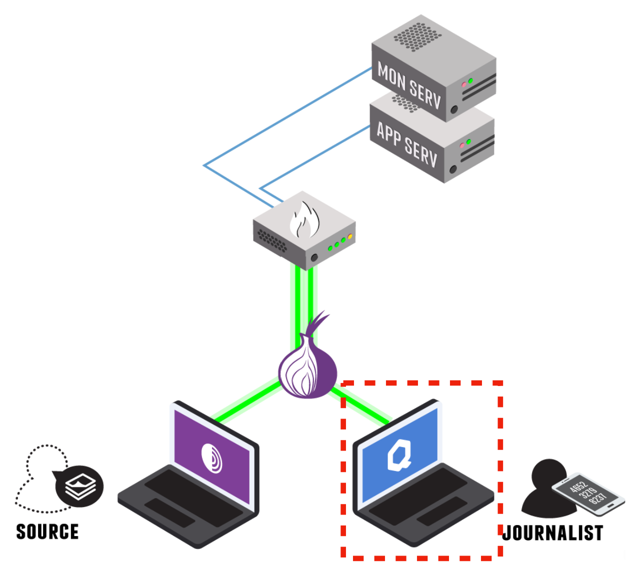
New Architecture



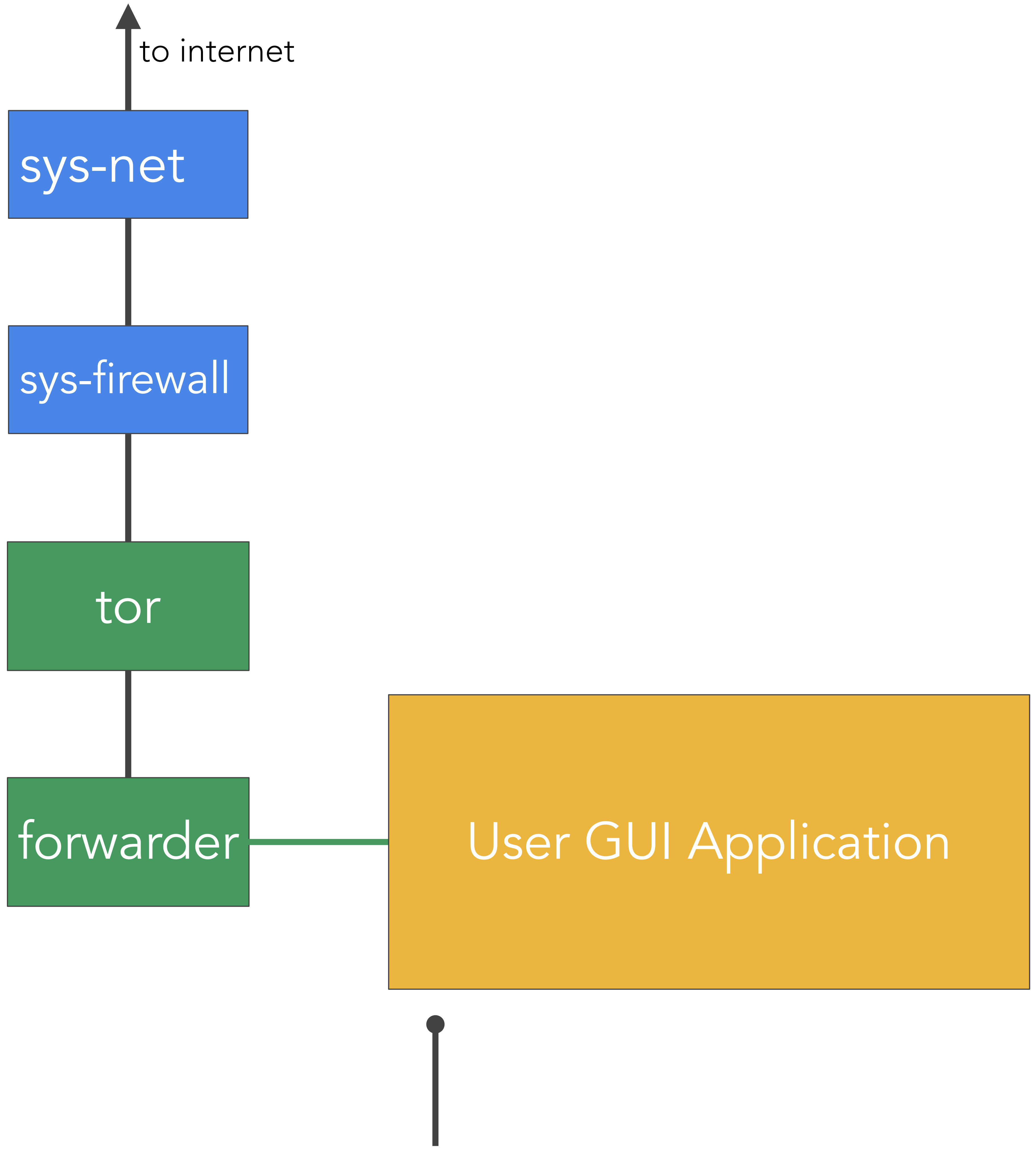
Passes API requests/responses from the SecureDrop server/to the user

Legend

- ━ qrexec (interVM communication)
- 🟧 Disposable *and* non-networked AppVM
- 🟩 Networked AppVM
- 🟨 Non-networked AppVM
- 🟦 System VM



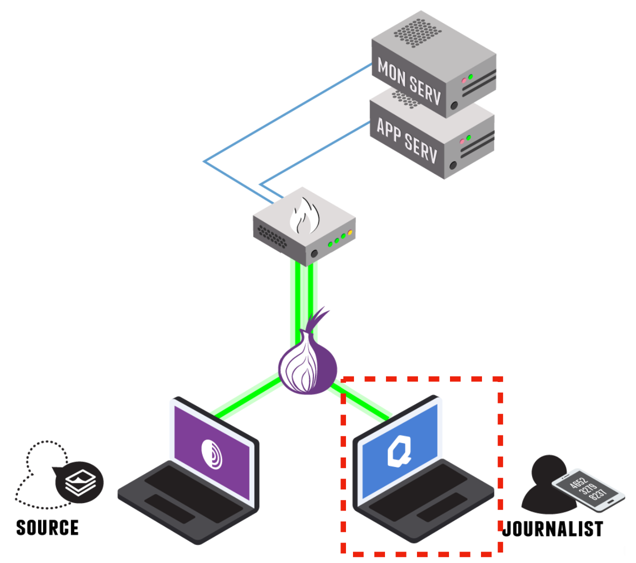
New Architecture



Non-networked VM used to run a chat-like interface

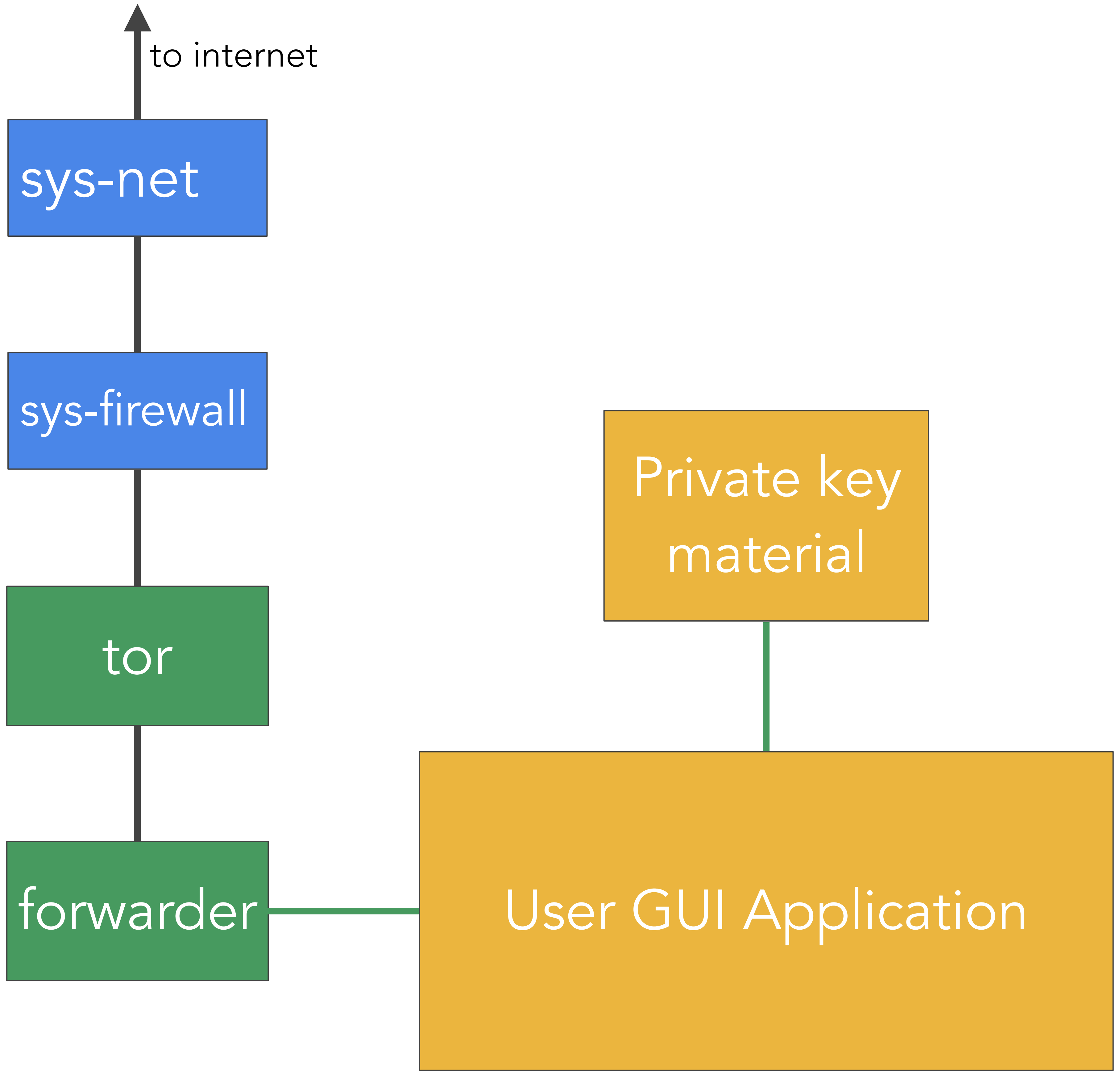
Legend

▬	qrexec (interVM communication)
🟧	Disposable *and* non-networked AppVM
🟩	Networked AppVM
🟨	Non-networked AppVM
🟦	System VM



SECUREDROP

New Architecture



to internet

sys-net

sys-firewall

tor

forwarder

Private key material

User GUI Application

Legend

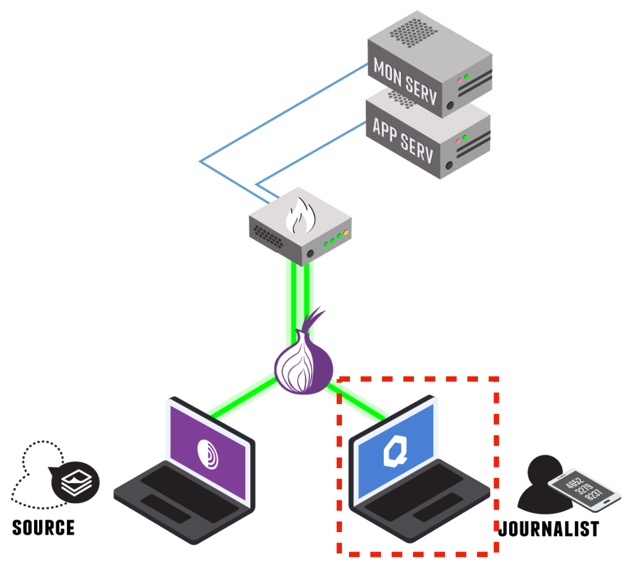
▬ qrexec (interVM communication)

🟧 Disposable *and* non-networked AppVM

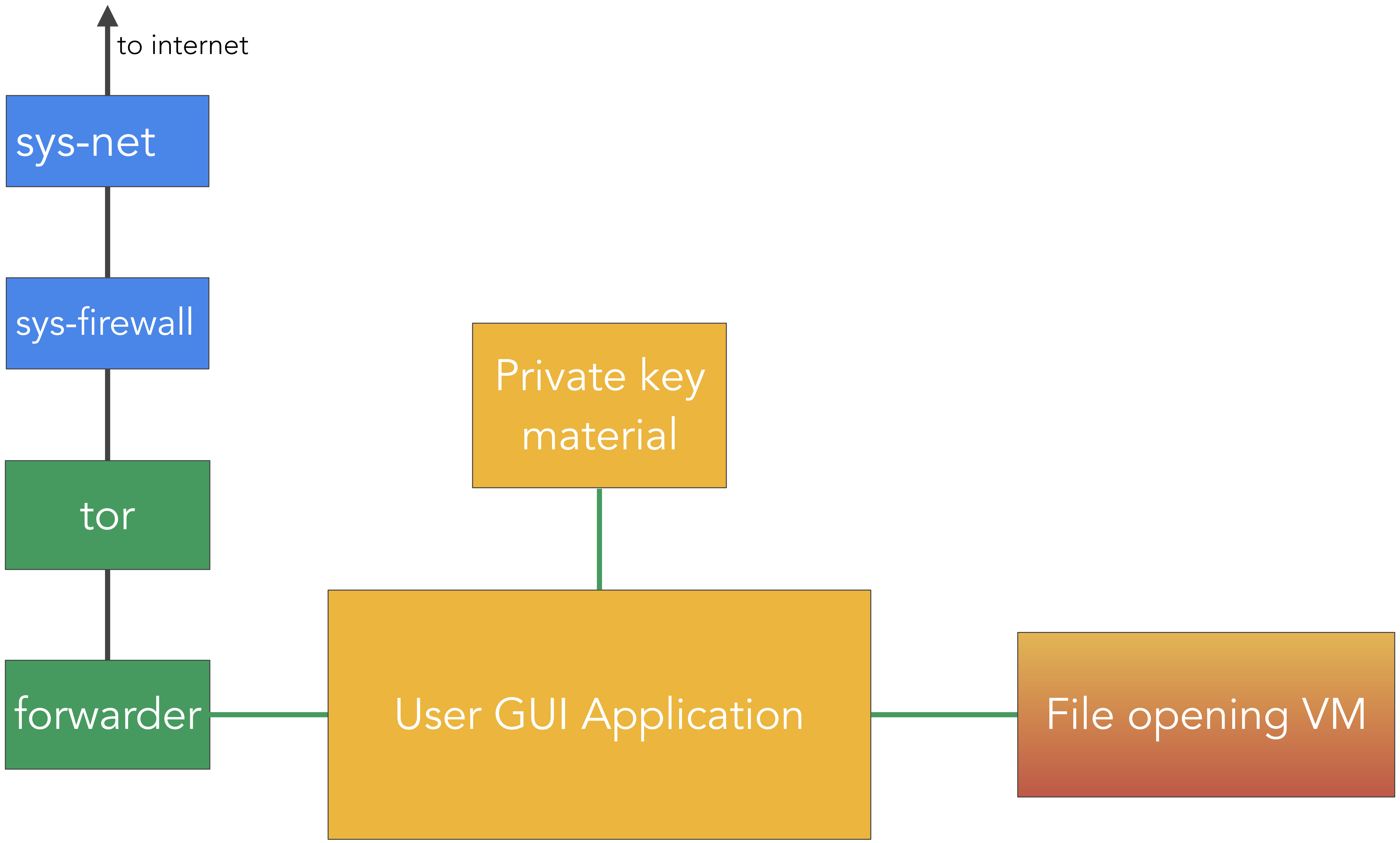
🟩 Networked AppVM

🟨 Non-networked AppVM

🟦 System VM



New Architecture



to internet

sys-net

sys-firewall

tor

forwarder

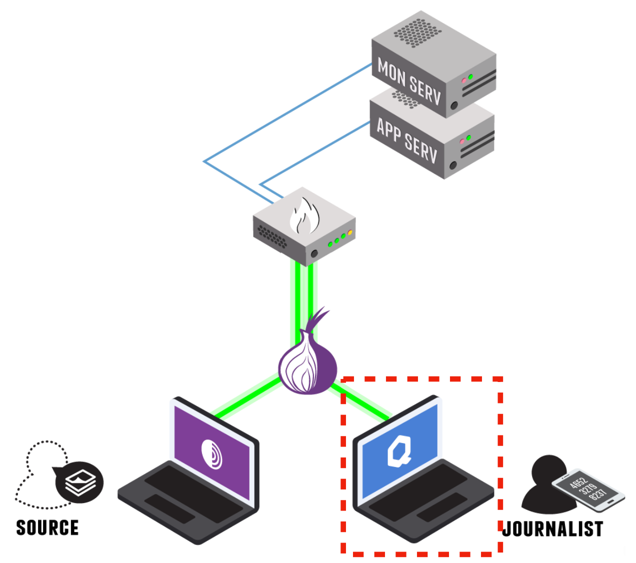
Private key material

User GUI Application

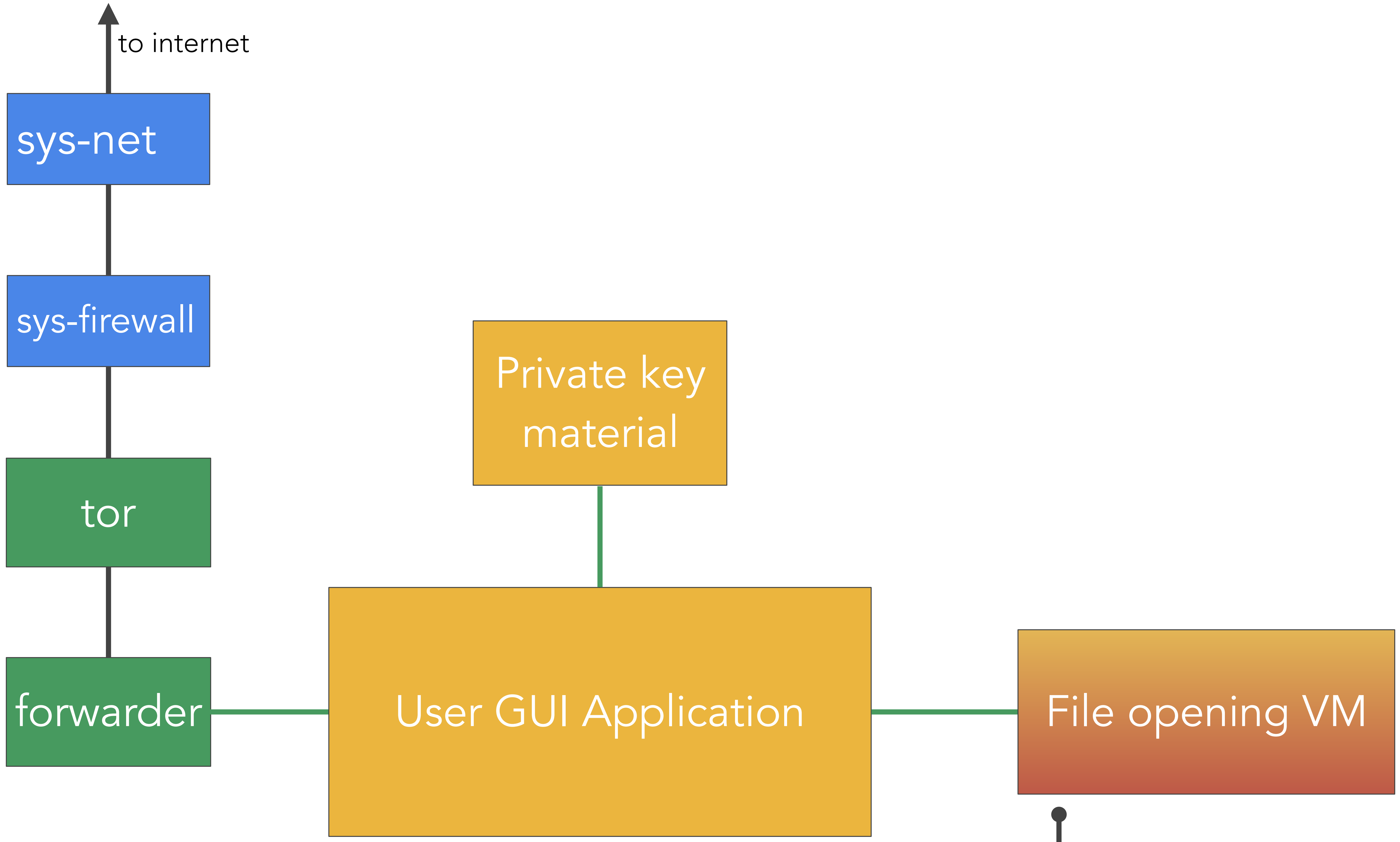
File opening VM

Legend

- ━ qrexec (interVM communication)
- 🟧 Disposable *and* non-networked AppVM
- 🟩 Networked AppVM
- 🟨 Non-networked AppVM
- 🟦 System VM



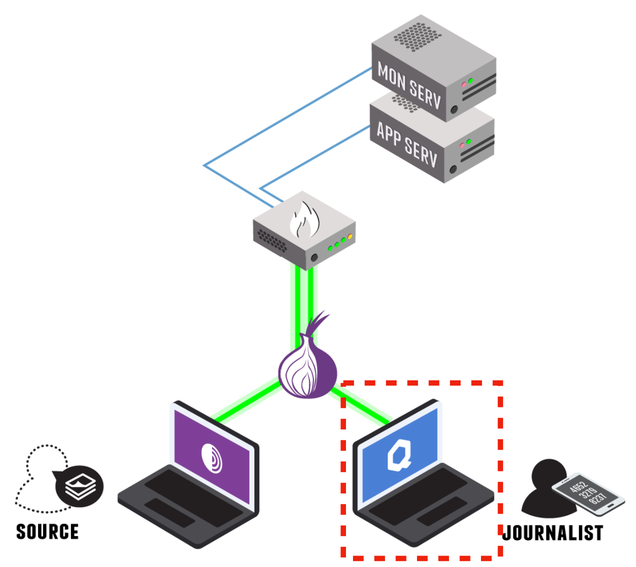
New Architecture



Uses a hardened kernel (grsecurity) in order to provide additional generalized exploit mitigations for memory corruption vulns

Legend

- ▬ qrexec (interVM communication)
- 🟧 Disposable *and* non-networked AppVM
- 🟩 Networked AppVM
- 🟨 Non-networked AppVM
- 🟦 System VM



SECUREDROP

Technical Goals

1. Ensure known vulnerabilities are patched.

    - Autoupdates in all VMs (via updating the base templates).

2. Isolate the submission private key from potentially malicious documents.

    - Submission private key is isolated in its own VM.

3. Isolate each source's documents.

    - Each document is isolated in its own VM.

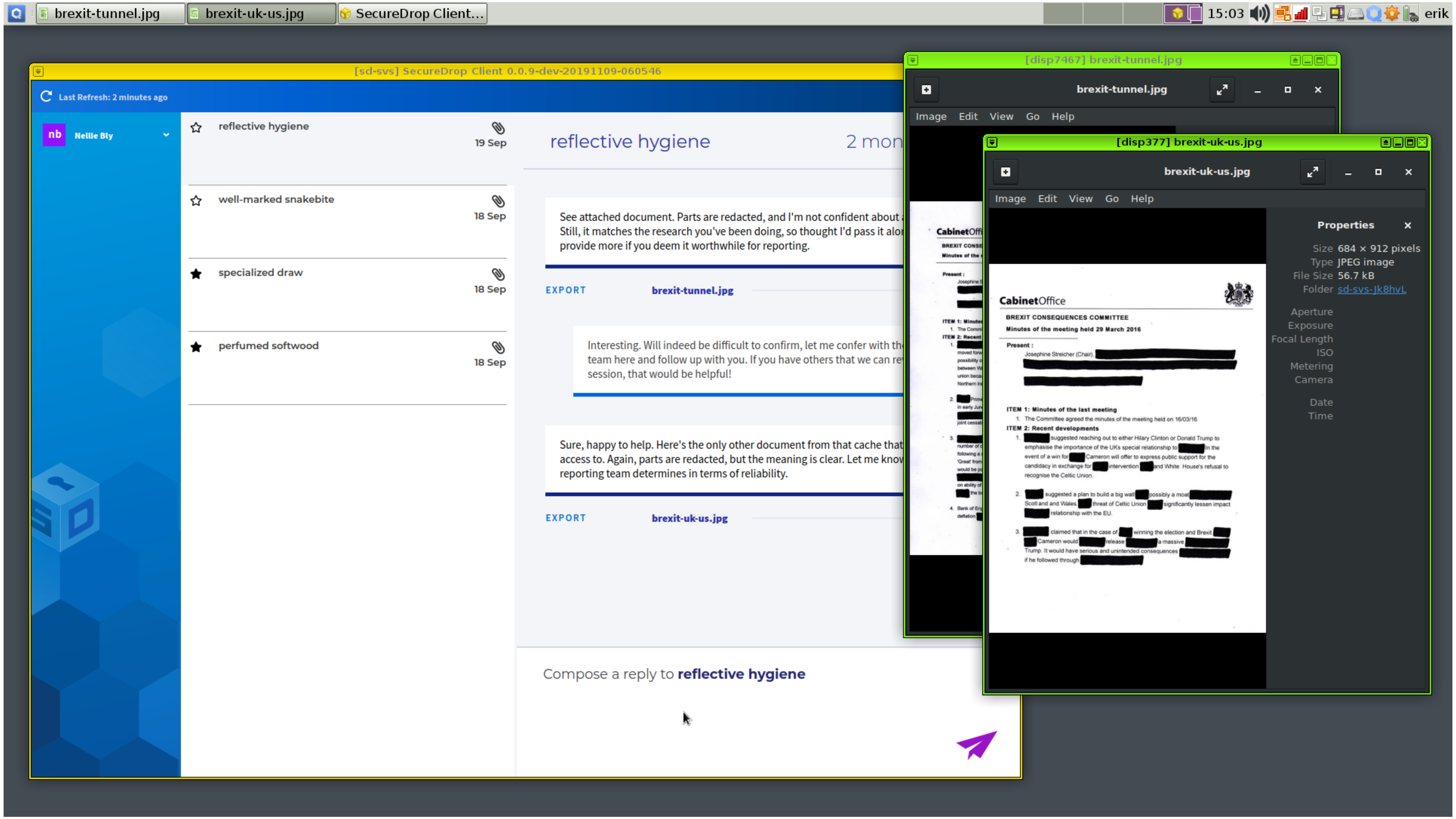
4. Recover from an attacker getting code execution in the VM used to open submissions.

    - Each file viewing VM is destroyed after shutdown.

5. Provide defense in depth against unknown vulnerabilities.

    - Kernel hardening complicates exploitation of memory corruption-based vulnerabilities.

Journalist Perspective



See attached document. Parts are redacted, and I'm not confident about
Still, it matches the research you've been doing, so thought I'd pass it alo
provide more if you deem it worthwhile for reporting.

EXPORT brexit-tunnel.jpg

Interesting. Will indeed be difficult to confirm, let me confer with th
team here and follow up with you. If you have others that we can re
session, that would be helpful!

Sure, happy to help. Here's the only other document from that cache that
access to. Again, parts are redacted, but the meaning is clear. Let me kno
reporting team determines in terms of reliability.

EXPORT brexit-uk-us.jpg

Compose a reply to **reflective hygiene**

CabinetOffice

BREXIT CONSEQUENCES COMMITTEE

Minutes of the meeting held 29 March 2016

Present :

Josephine Streicher (Chair), [redacted]

ITEM 1: Minutes of the last meeting

1. The Committee agreed the minutes of the meeting held on 16/03/16

ITEM 2: Recent developments

1. [redacted] suggested reaching out to either Hilary Clinton or Donald Trump to emphasise the importance of the UKs special relationship to [redacted] In the event of a win for [redacted] Cameron will offer to express public support for the candidacy in exchange for [redacted] intervention [redacted] and White House's refusal to recognise the Celtic Union.

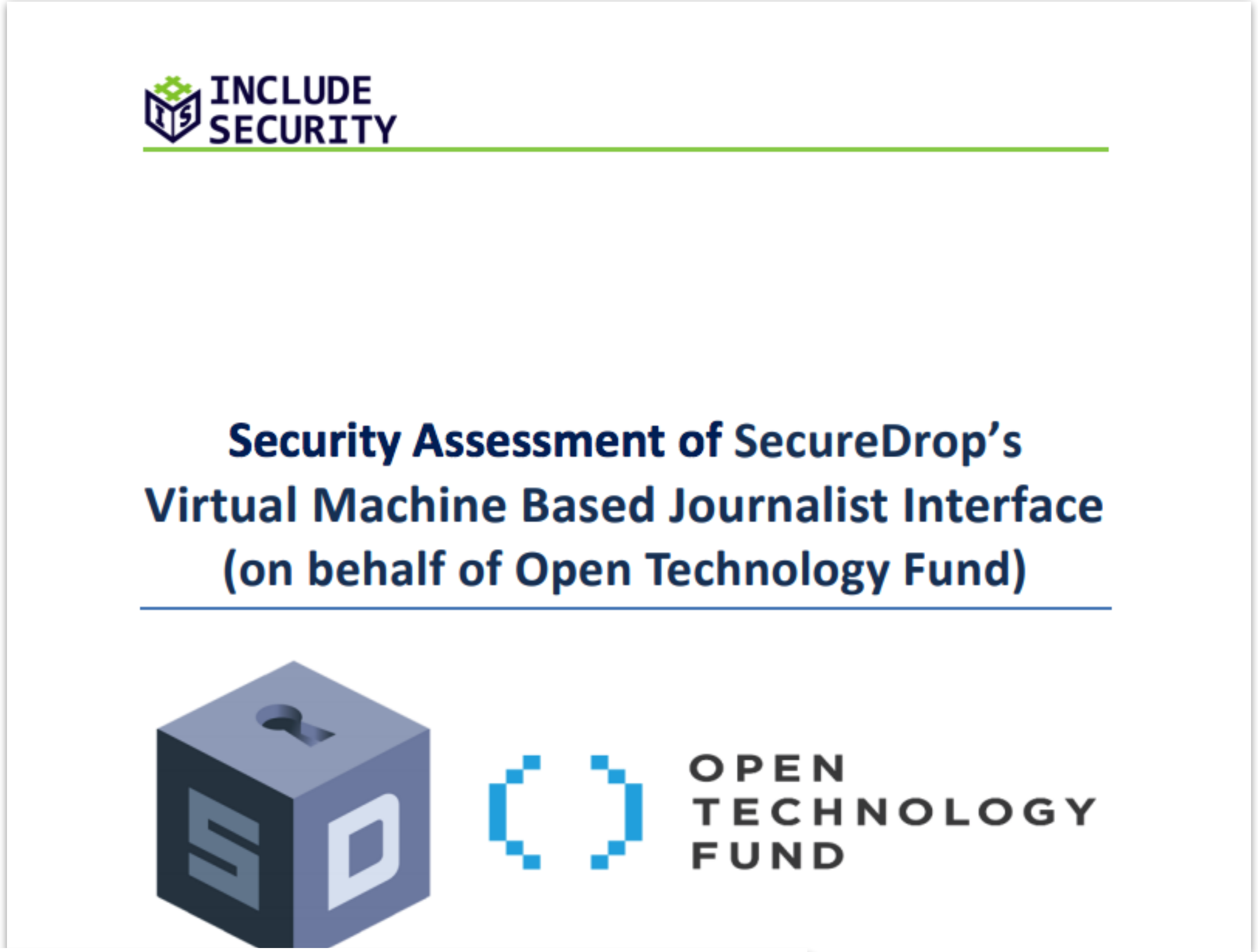
2. [redacted] suggested a plan to build a big wall [redacted] possibly a moat [redacted] Scotland and Wales. [redacted] threat of Celtic Union [redacted] significantly lessen impact [redacted] relationship with the EU.

3. [redacted] claimed that in the case of [redacted] winning the election and Brexit [redacted] Cameron would [redacted] release [redacted] a massive [redacted] Trump. It would have serious and unintended consequences [redacted] if he followed through [redacted]

Current status

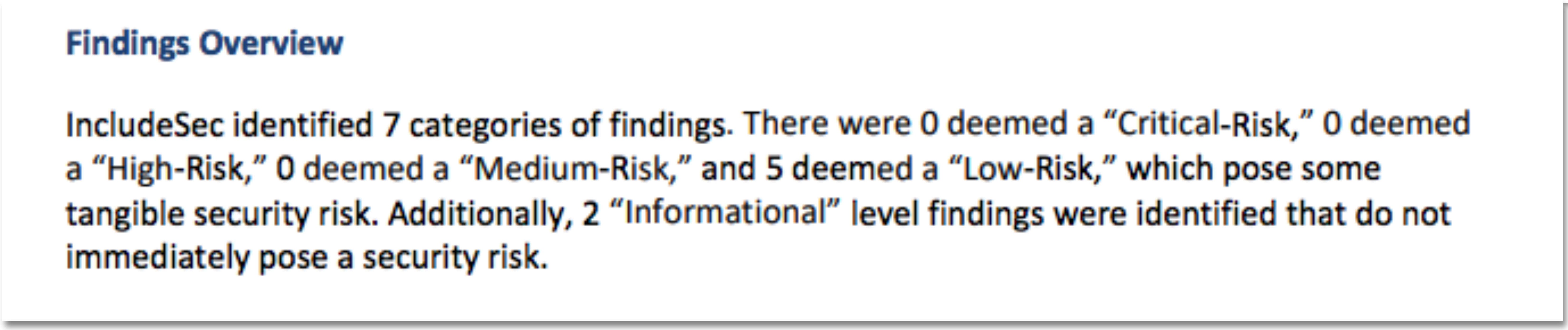
1. Audit performed late 2018 of the alpha version of this project (full audit report PDF available on securedrop.org)

2. Beta test beginning in the next few weeks with targeted news organizations



INCLUDE SECURITY

Security Assessment of SecureDrop's Virtual Machine Based Journalist Interface (on behalf of Open Technology Fund)



Findings Overview

IncludeSec identified 7 categories of findings. There were 0 deemed a "Critical-Risk," 0 deemed a "High-Risk," 0 deemed a "Medium-Risk," and 5 deemed a "Low-Risk," which pose some tangible security risk. Additionally, 2 "Informational" level findings were identified that do not immediately pose a security risk.

Takeaways

1. Journalists and their sources face growing challenges due to malware, phishing, and other electronic threats.

2. User-friendly tools for working with potentially malicious documents are critical for journalists.

3. We have built one solution based on QubesOS, but more work in this area is needed.

Interested?

Check out our repositories: `https://github.com/freedomofpress/securedrop-workstation`

Check out our bug bounty program: `https://bugcrowd.com/freedomofpress`