The Sunbeam Architecture

Splintercon 2023

Operator Foundation

- 501(c)3 non-profit, grant-funded
- Specializing in technology development
  - For human rights organizations
  - We work exclusively with partners
- Software and hardware
- Design and manufacturing
  - Stealth case design

Problem

- Splinternets break Internet connectivity
- Federated services can still work
  - However, they could be detected and blocked
  - They are not designed for adversarial networks

- Example federated services:
  - Matrix Chat
  - Mastodon
  - SimpleX

Proposed Solution

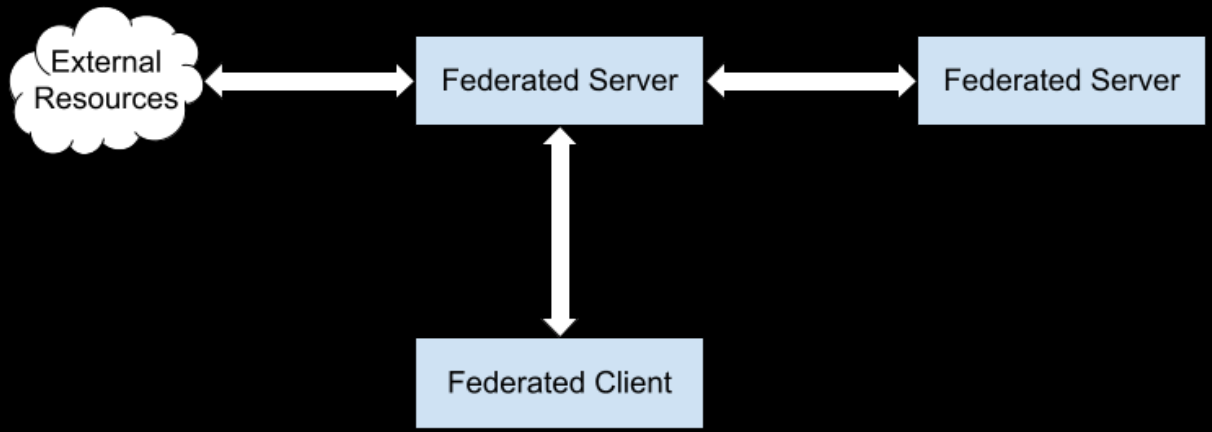
- Remove dependency on full Internet
- Protect federated services from discovery
- Offer a smooth upgrade/downgrade path
- No modification to client or server code
- Services that “just work” during shutdowns
  - International communication will be disabled

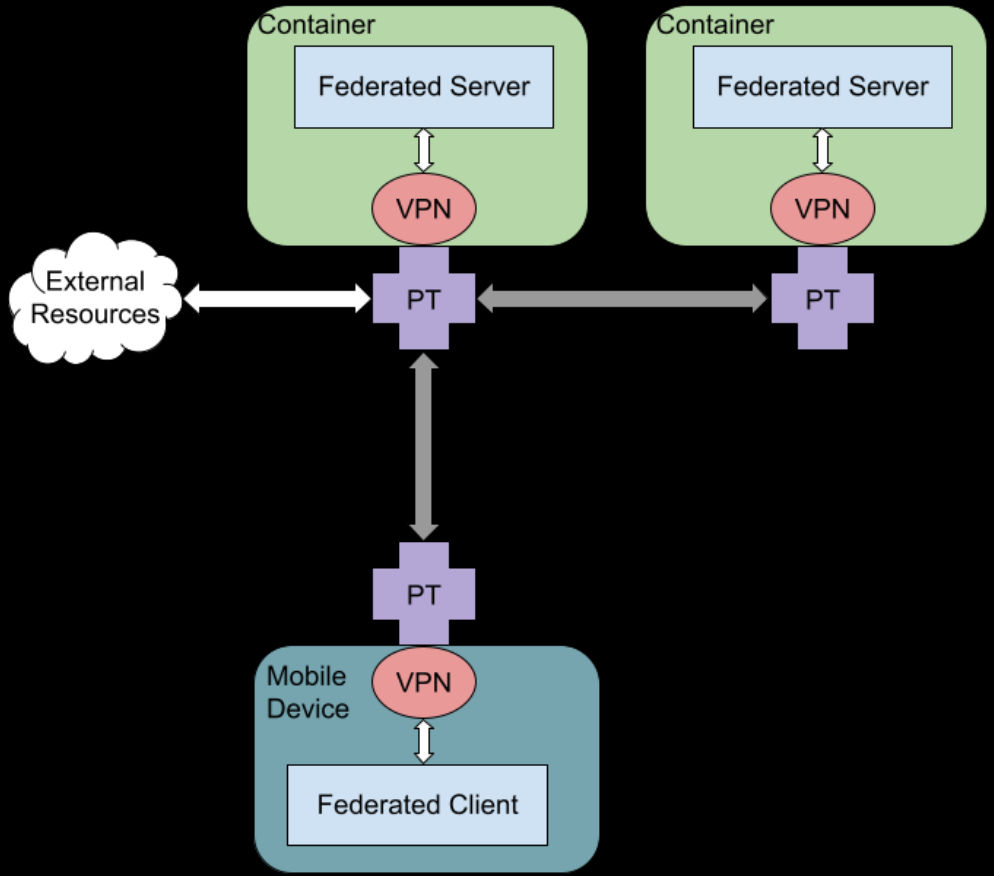
Threat Model

- No international Internet available
- DNS will not be reliable
- The network will be fully monitored
- Federated services will be shut down
  - If discovered through monitoring
- Encrypted traffic will be blocked

Architecture Overview

- Pluggable Transports
- Intercepting Federated Service Traffic
- Handling DNS
- Incoming Connections
- Outgoing Connections
- Updating PT Server Addresses


External Resources
Federated Server
Federated Server
Federated Client


Container
Federated Server
VPN
Container
Federated Server
VPN
External Resources
PT
PT
PT
Mobile Device
VPN
Federated Client

Intercepting Federated Service Traffic

- OS-level VPN services
- “split proxy” mode support
- Pluggable Transports
  - Encryption
  - Obfuscation

Handling DNS

- Splinternet DNS resolvers are unreliable
- Revert to /etc/hosts model for DNS
  - “pet names”
- Our DNS returns the IP of the Pluggable Transport server, not the application server

Handling Incoming Connections

- Federated service DNS resolves to PT servers
- Automatically added to splitproxy config
- PT servers forward incoming connections to federated service servers
- PT connections are encrypted and obfuscated

Handling Outgoing Connections

- Containers used to capture outgoing connections
- Pluggable Transports used to move the outgoing connection to another machine
- This hides the location of the federated service

Updating PT Server Addresses

- As PT servers are discovered, they are blocked
- How do we distribute new PT servers?
- Many options
- One option is the Wreath automated server discovery framework

Prior Art

- VPN = “Virtual **Private** Network”
- Hamachi
- TailScale
- Moonbounce / Persona
- Lantern, Psiphon, TunnelBear, Tor

Conclusion

- The Sunbeam Architecture
- Is a Virtual **Private** Network
- Providing private communication
  - Between clients and service instances
  - Between service instances
- Federated services might have a bright future on splinternets