Remedy

Relay Monitoring and Deployment

“server-side circumvention”

https://github.com/ProjectRemedy/Remedy

Addressed Issue

- Content/service blocking (censorship)
- **Not** surveillance (and associated repression)

Content & service blocking

- DNS level (domain name)
- IP level
- Content-based (DPI, transparent proxy)

Circumvention

- By end-user action:
  - Changing config (e.g. DNS)
  - Using circumvention tools
  - Accessing other service
- By server admin action:
  - Registering new domain
  - Changing IP
  - Setting up reverse proxies
  - Setting up SSL

Concerns

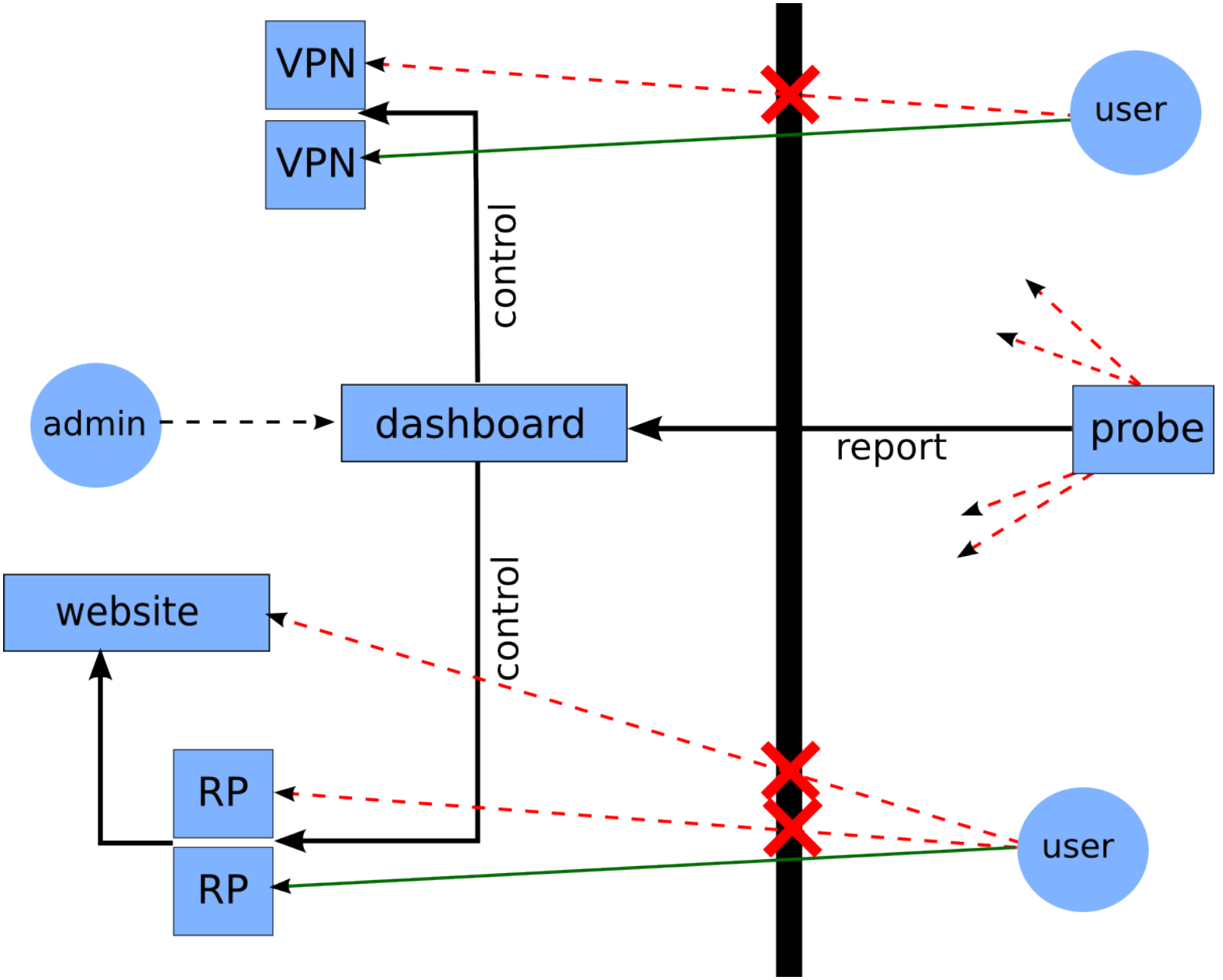
- End-user circumvention:
  - Knowledge
  - Availability of tools
  - Mistakes (e.g. tango.me, cleartext proxies, Ultrasurf)
- Server-side circumvention:
  - Admin knowledge
  - Time required for setup
  - Time required for censors to find out

Remedy idea

Speed up & ease server-side circumvention

(i.e. faster mouse in cat-and-mouse game)

Remedy overview



How?

- Web frontend “dashboard” to monitor & take action
- Deployment of relays through SaltStack to minimize manual actions (dashboard backend)
- Use of AMI and OpenStack for VM deployment
- Early blockade detection and report with OONI probes
- Try to hide dashboard (security): Tor

Current status

- Dashboard backend bootstrapping (Salt, Tor) for Ubuntu systems
- Web relays bootstrapping
- Preliminary Salt recipes web relays
- Frontend – not yet connected to Salt backend
- Early testing of OONI

Interrogations/difficulties

- Salt through Tor: not so good
- Salt's SSL implementation?
- OONI under heavy development
- Some tasks uneasy to automate

- Tell censored people (but not censors) about a new IP/domain name/...?

Source

https://github.com/ProjectRemedy/Remedy