Using Off-Path and On-Path Signaling for Internet Security

Saikat Guha, Paul Francis

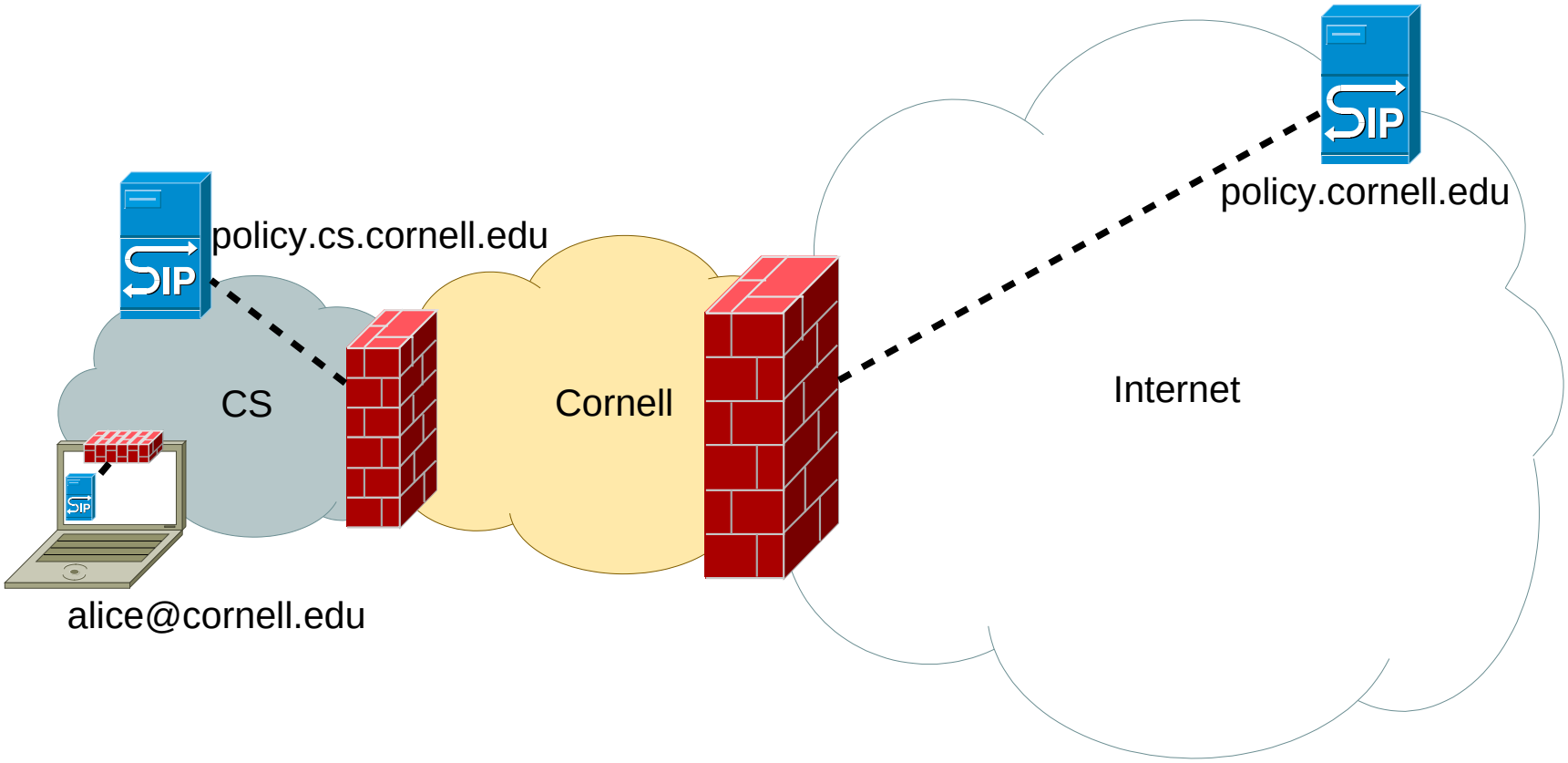
Cornell University

IETF 66 Off-path BoF

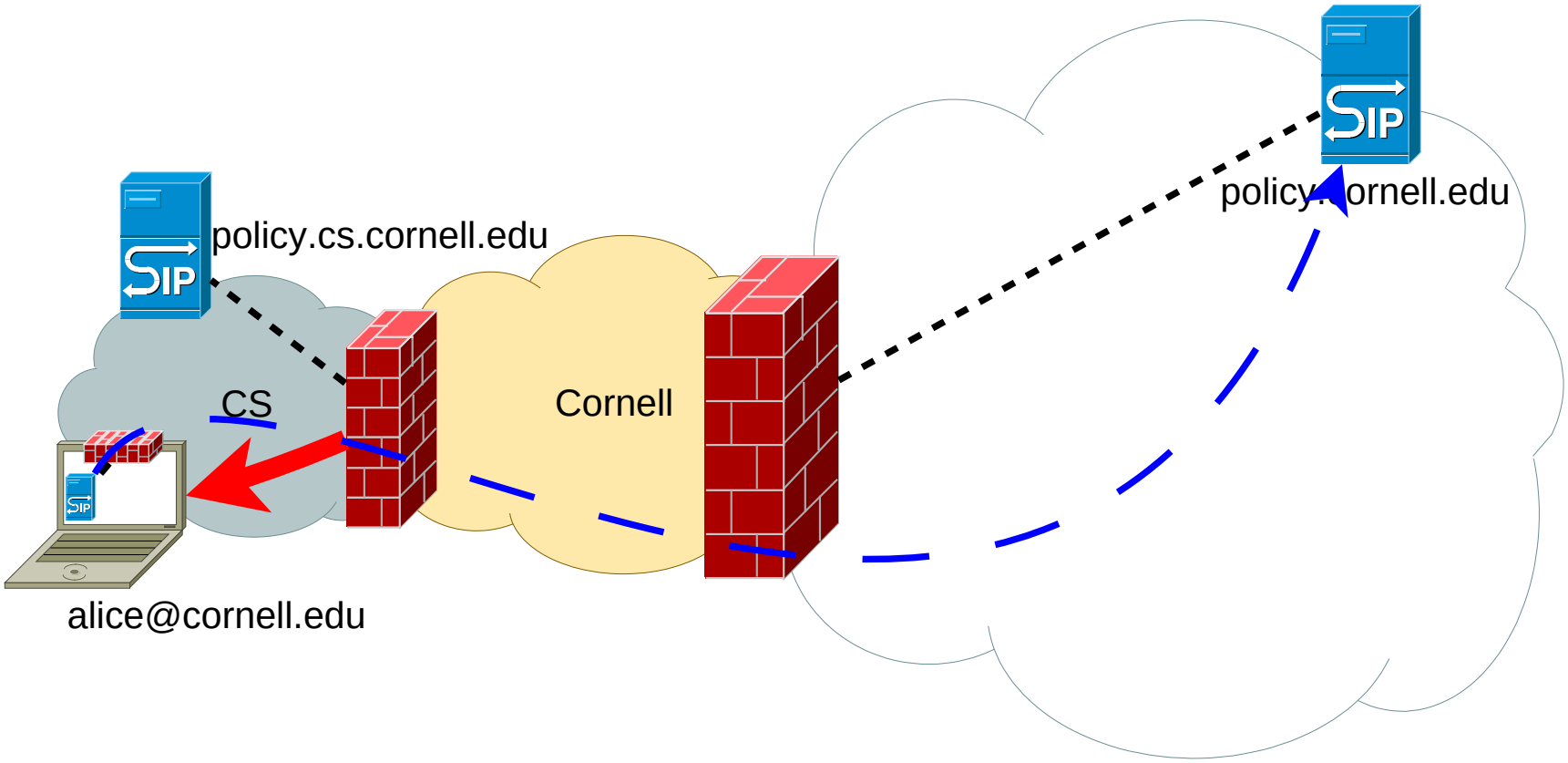
Architecture

- Default-Off Data-Path
  - Turned “on” after off-path negotiation
- Default-On Off-Path Signaling
  - Rate-limited
  - Mediated by intermediaries
  - Heavily Secured
- On-Path Signaling
  - Coupled Off-Path negotiation with Data-Path

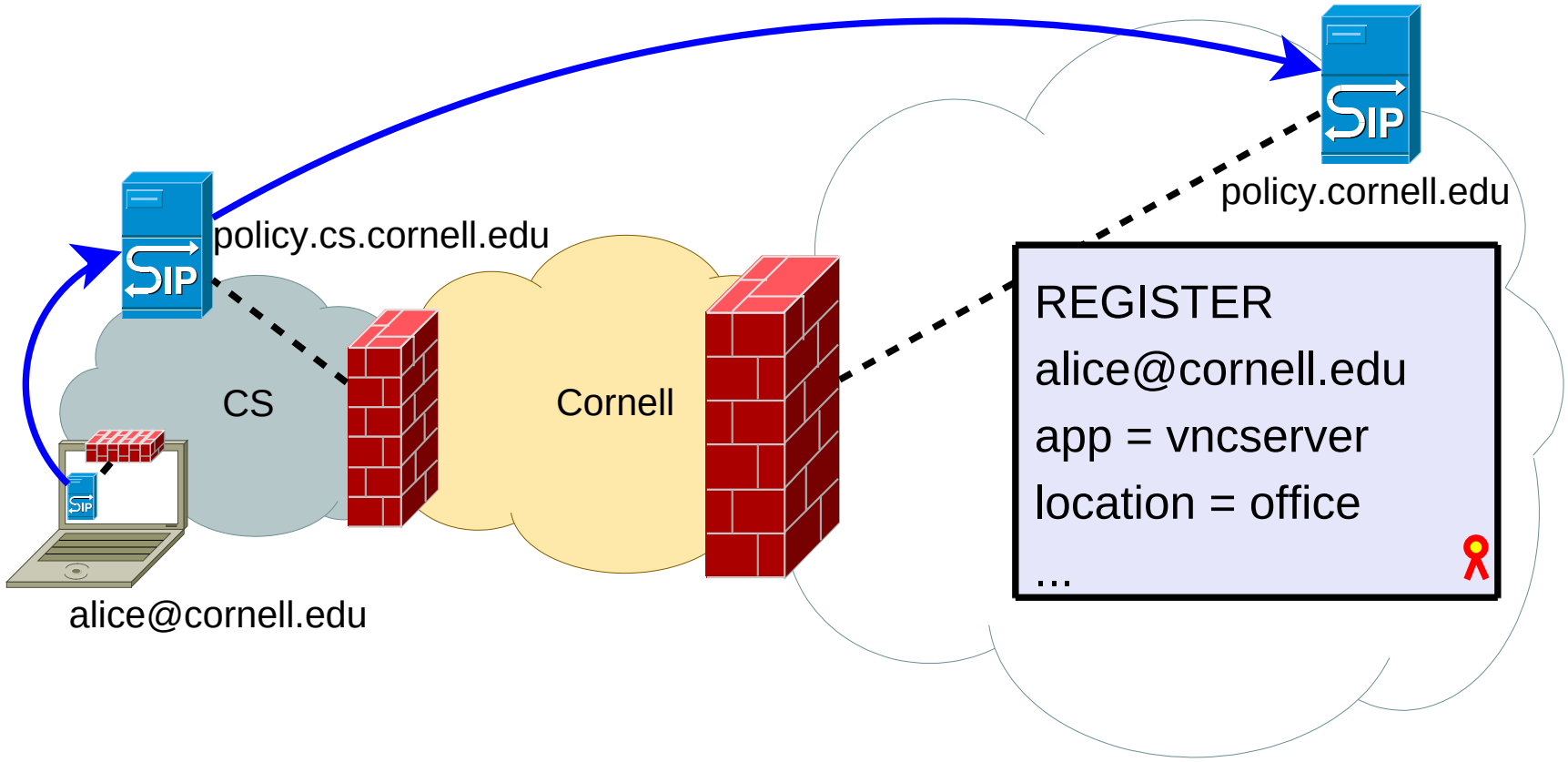
Network Elements



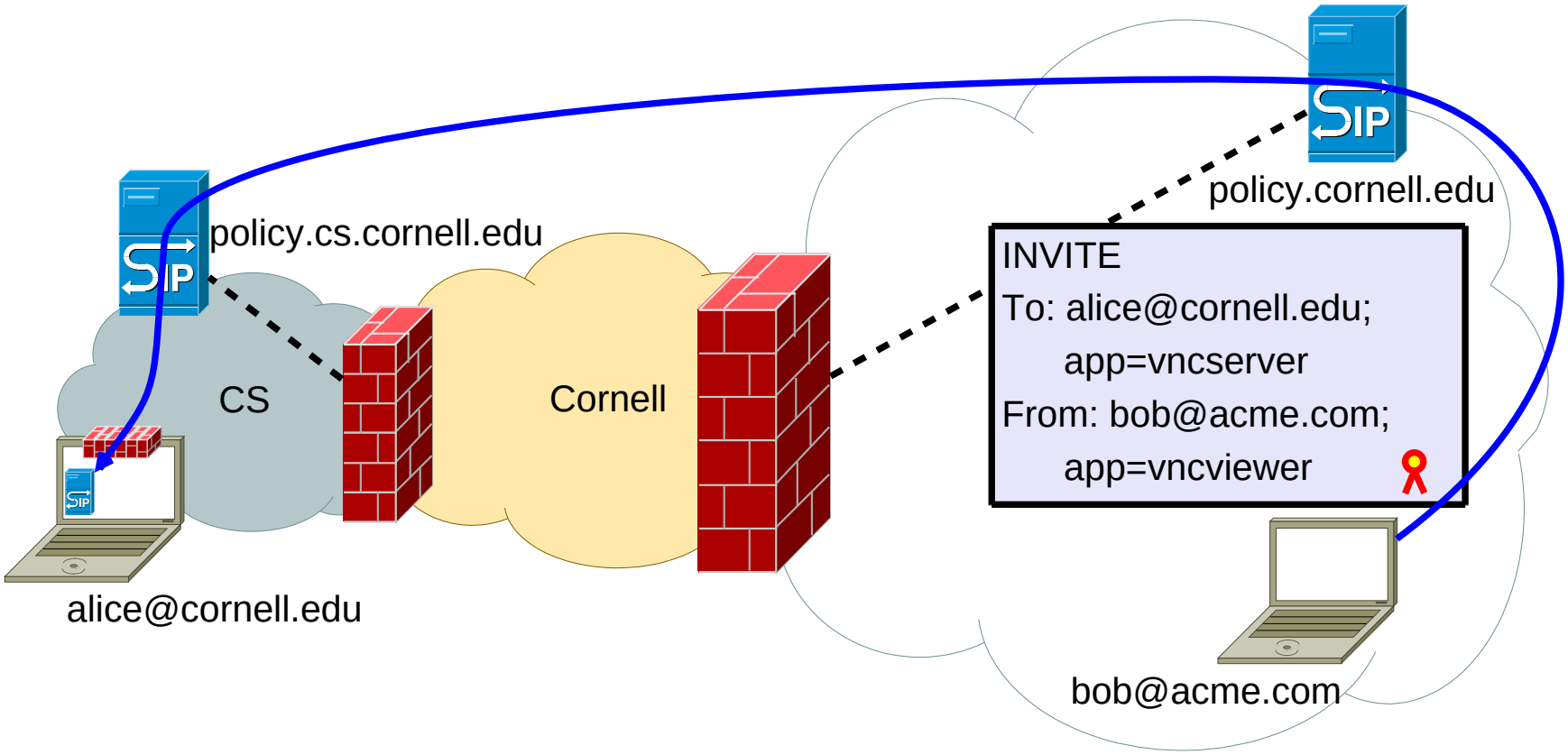
Discover P-Box



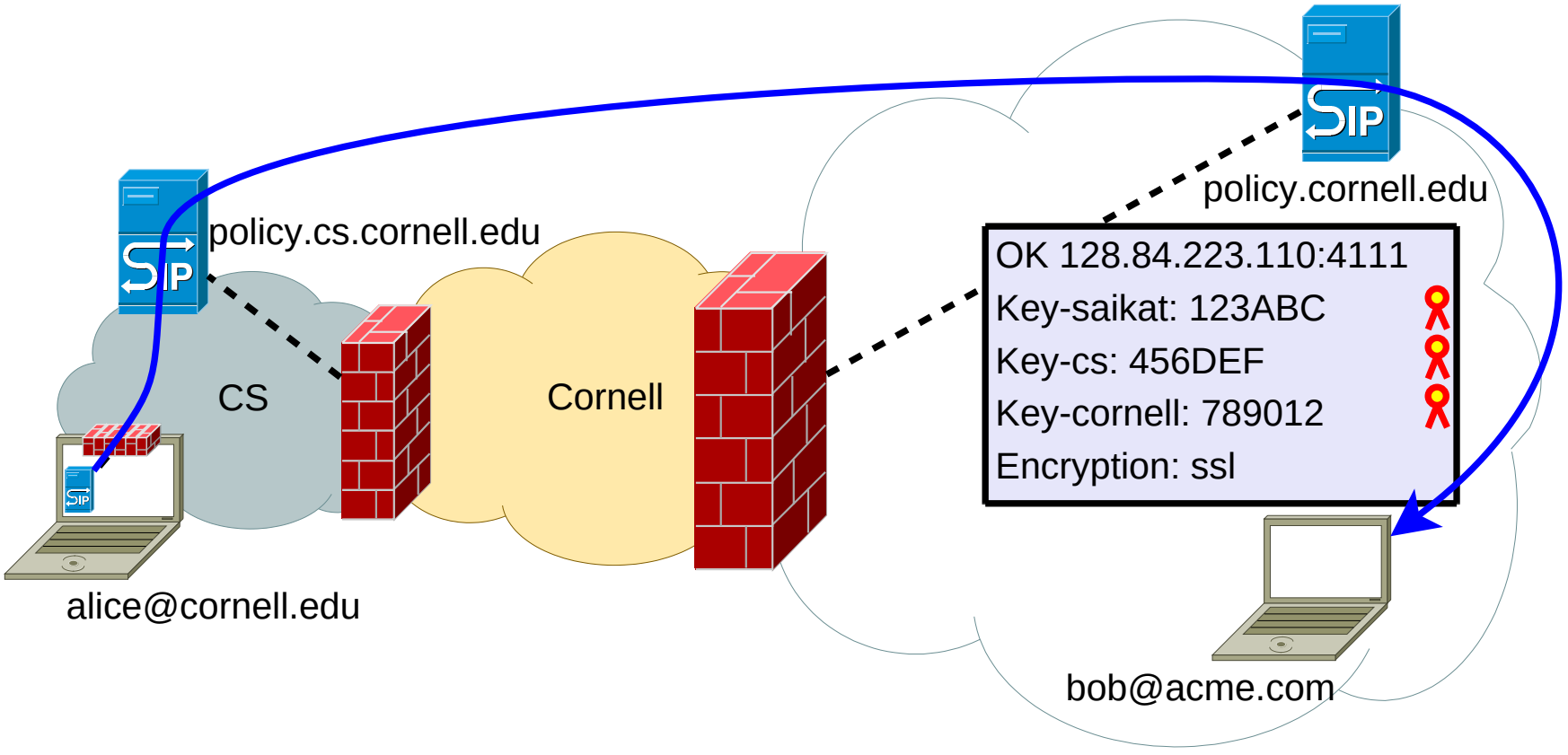
Register Off-path



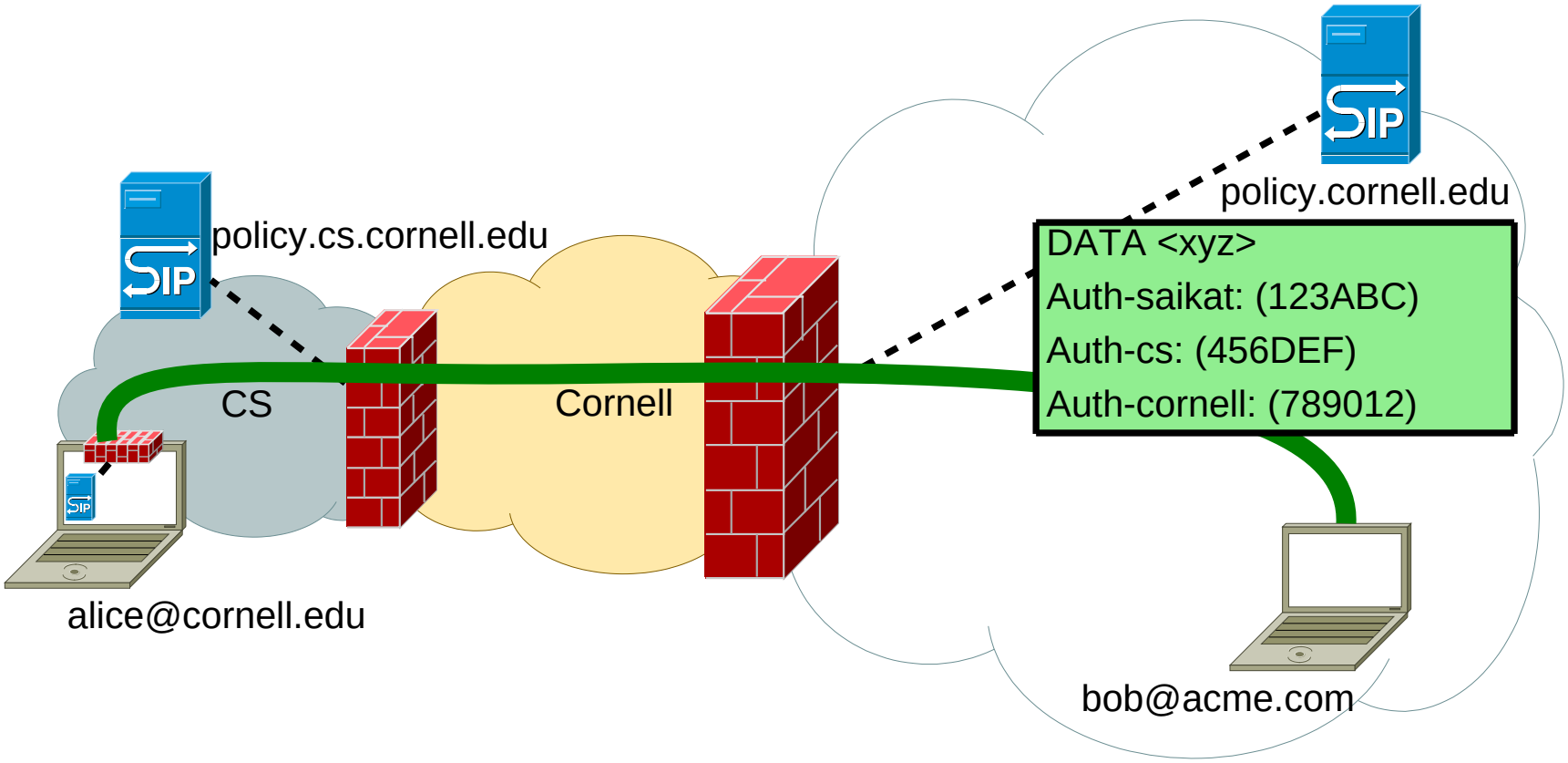
Request Data-Path



Data-Path with Keys



Authorized Data



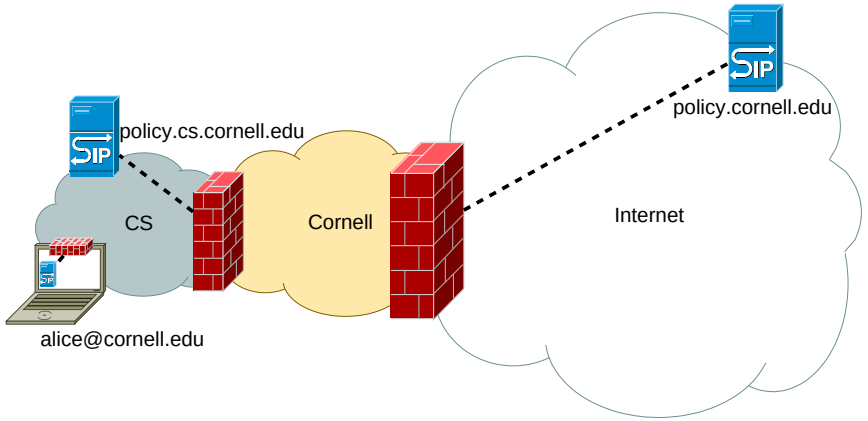
Network Elements

Off-path

- Policy
- Presence
- Messaging

On-Path

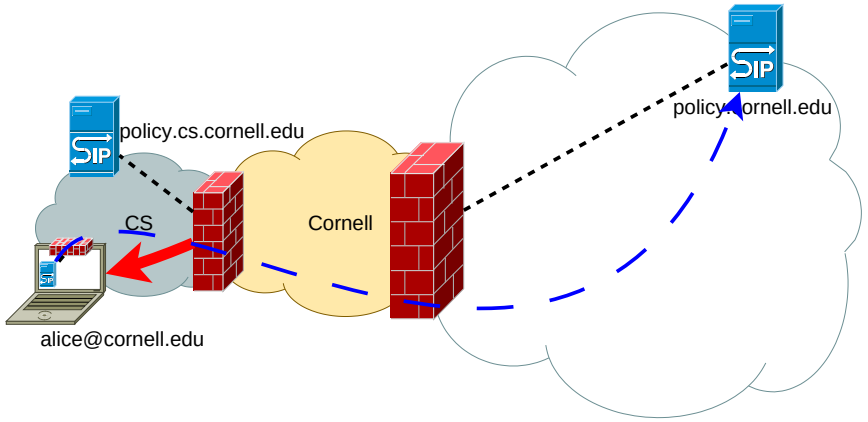
- Firewall
- TURN Relay
- Auditor



Discover P-Box

P-Box Discovery

- Static
- DHCP (at boot)
- Off-Path Query
- On-Path Query



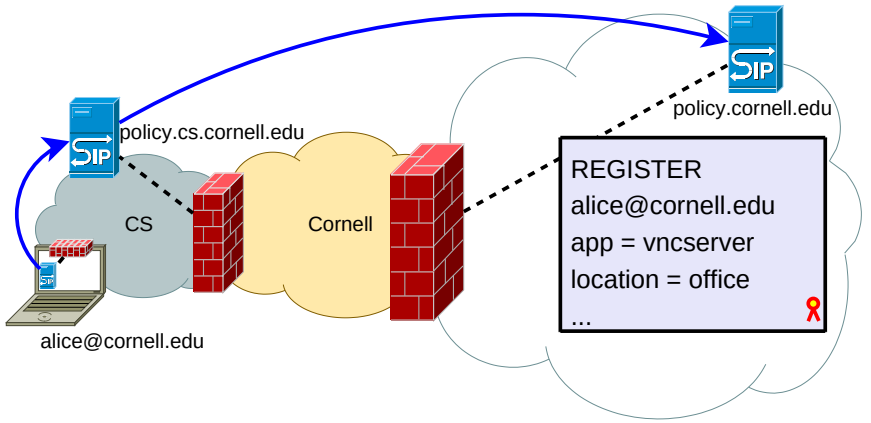
Register Off-path

Authenticate

- User, Domain
- Application
- Location

Mechanism

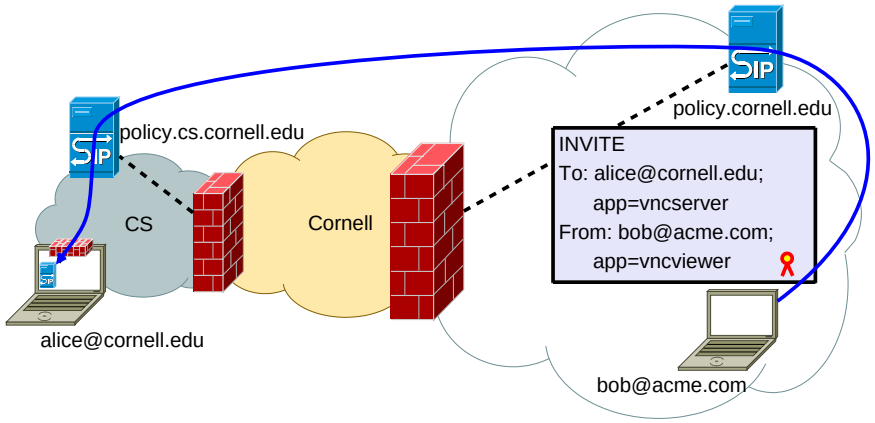
- Certificates
- Trusted Computing



Request Data-Path

Request

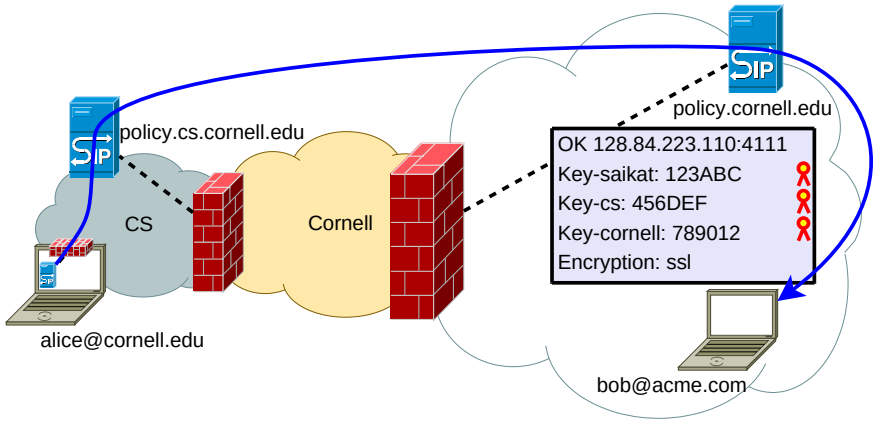
- Authentication
- Off-Path DoS
- Off-Path MitM



Data-Path with Keys

Response Token

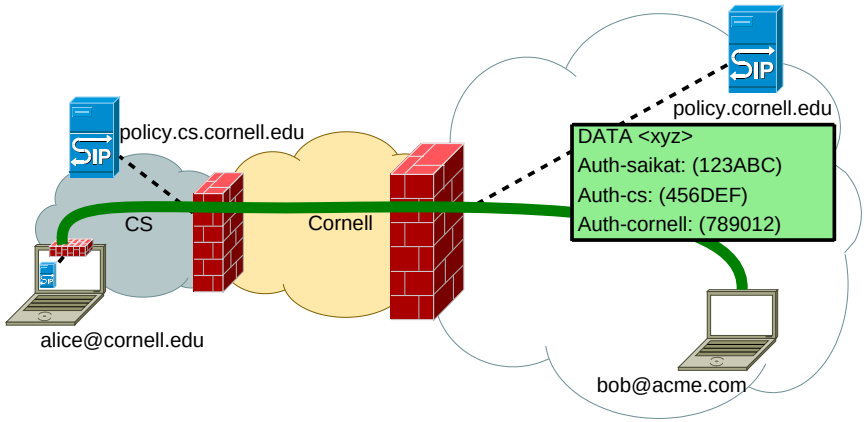
- Contents
  - IP:port
  - Firewall Key
  - # bytes
  - Time valid
- Replay Attack



Authorized Data

On-Path Signaling

- Out-of-Band (NSIS)
- In-Band (framing)



Implementation

- **P-Box:** SER SIP Proxy, static policy rules
- **P-Box Discovery:** Static Configuration
- **Registration:** SIP REGISTER (with user authorization)
- **Rendezvous:** SIP INVITE (with SDP)
- **Response:** 200 OK (with SDP, local address, STUN addresses, TURN address and TURN server authorization key)
- **Data-Path:** In-band (framing inside TCP), TURN path must include authorization

Callflows at: `nutss.net/bof/cf.txt`