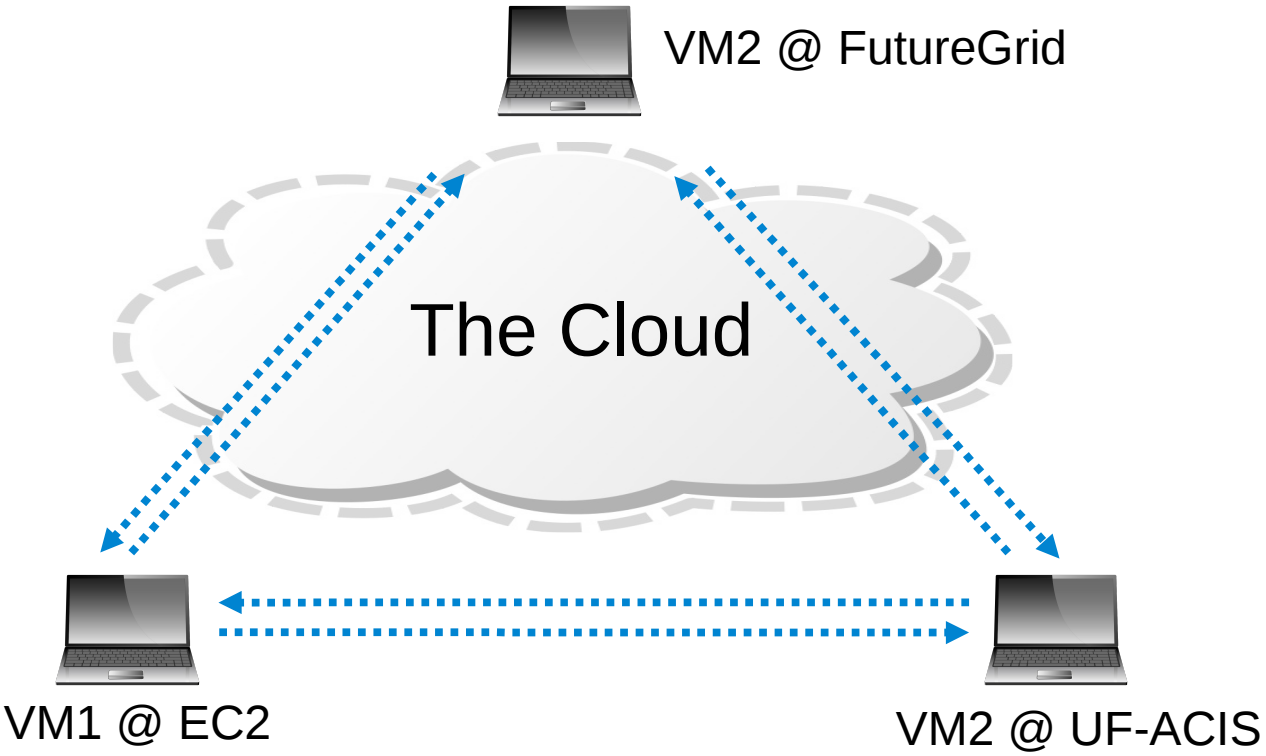
IPOP and SocialVPN Demonstrations

Pierre St Juste, Renato Figueiredo
Advanced Computing and Information Systems Lab
University of Florida
March 22, 2013

Motivation

Virtual machines **want to communicate as if they are part of the same LAN**, this can be difficult when they are **located at different cloud providers** or administrative domains

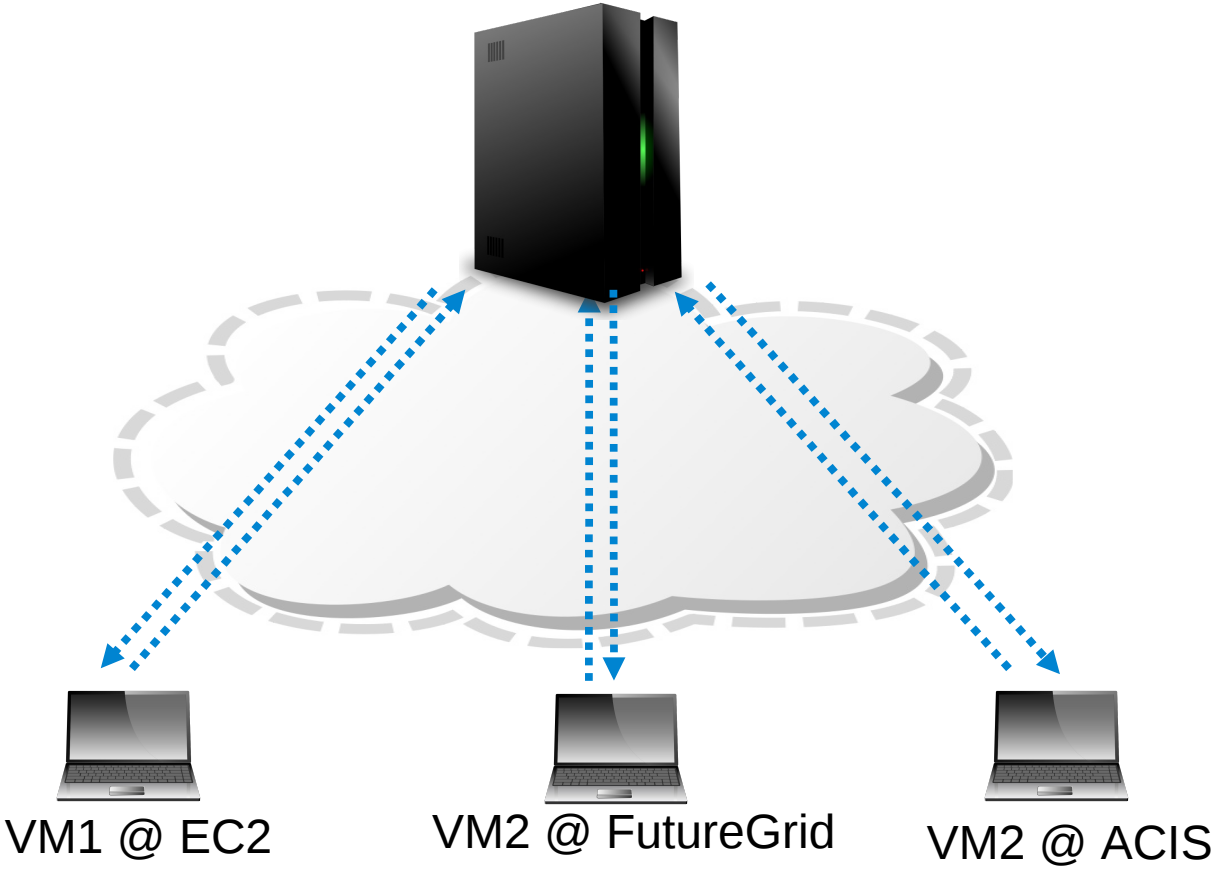


ACIS

UF UNIVERSITY of FLORIDA
The Foundation for The Gator Nation

Motivation

Naive Centralized VPN Gateway (OpenVPN)



1. Performance

All IP packets are routed through the gateway causing extra latency and bandwidth bottlenecks

2. Lack of trust

All IP packets are encrypted and decrypted at the gateway possibly leading to undetectable packet spoofing

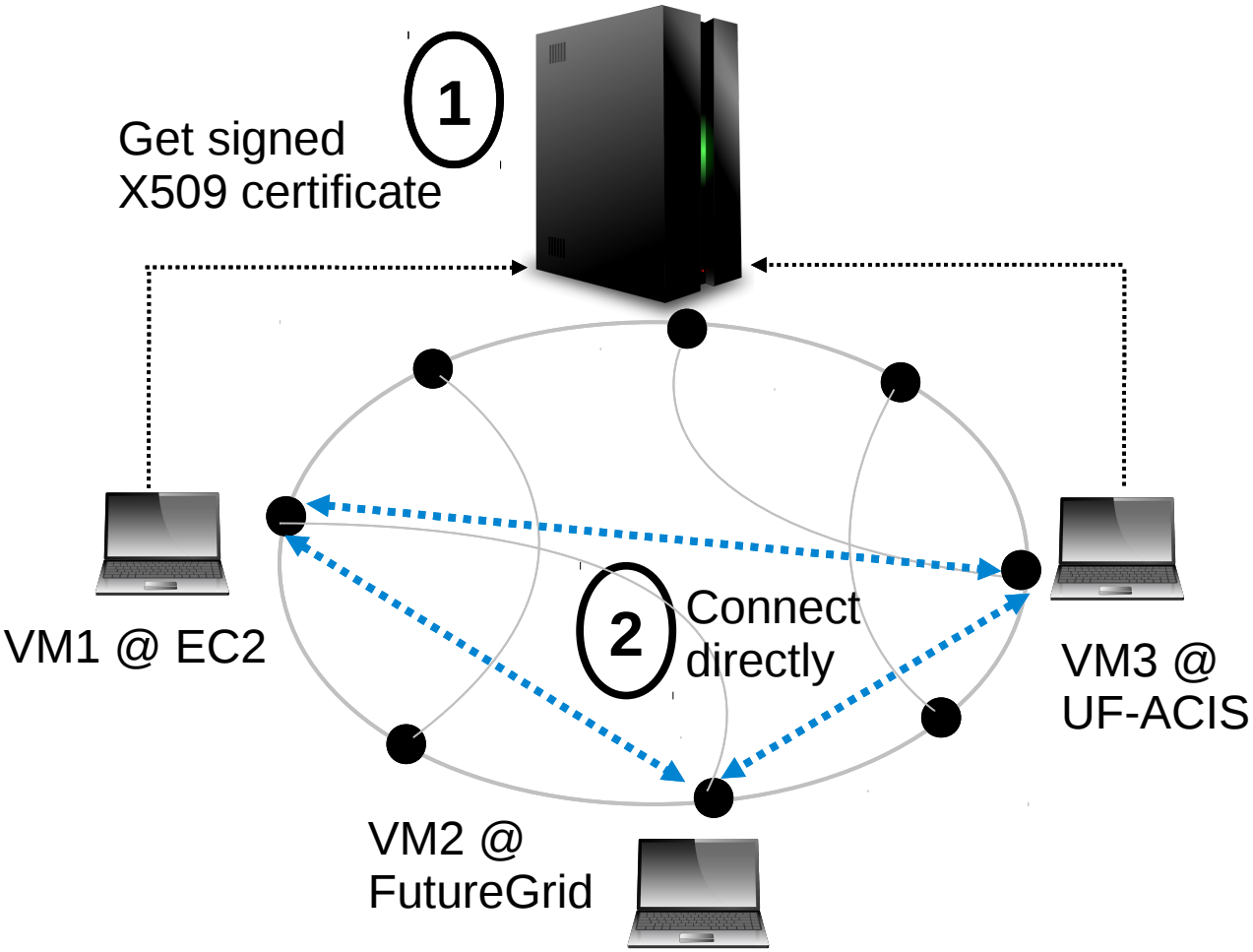
3. Single Point

Gateway maintains all routing state, along with assignment of IP address thus creating a single point of failure

ACIS

UF UNIVERSITY of FLORIDA
The Foundation for The Gator Nation

The Peer-to-Peer Approach



1. Performance

IP packets are sent over direct P2P tunnels thus removing the extra latency and bandwidth limitations of the gateway approach

2. Security

End-to-end encryption (e.g. IPSec) ensures no middleman can modify a packet unnoticed

3. Low maintenance

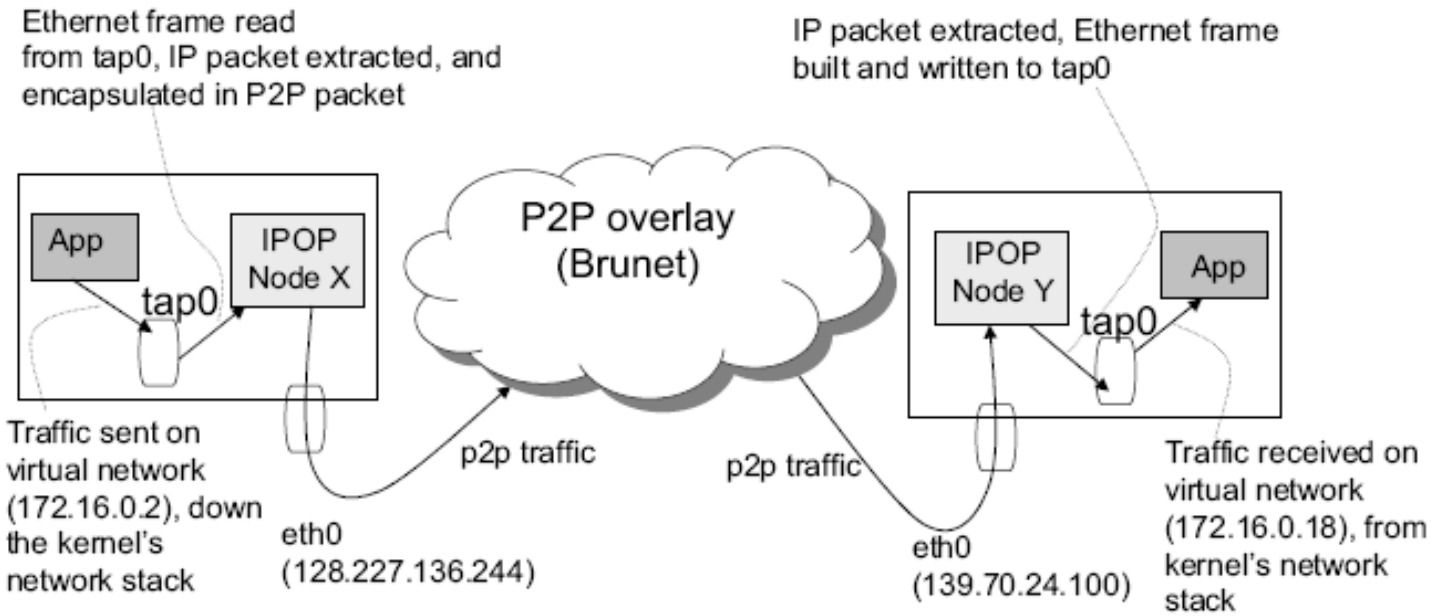
P2P technology provides self-managing/self-adapting network with no single-point of failure

Use **P2P technology to remove the inefficiencies** of the centralized approach, the gateway simply **functions as a certificate authority**

ACIS

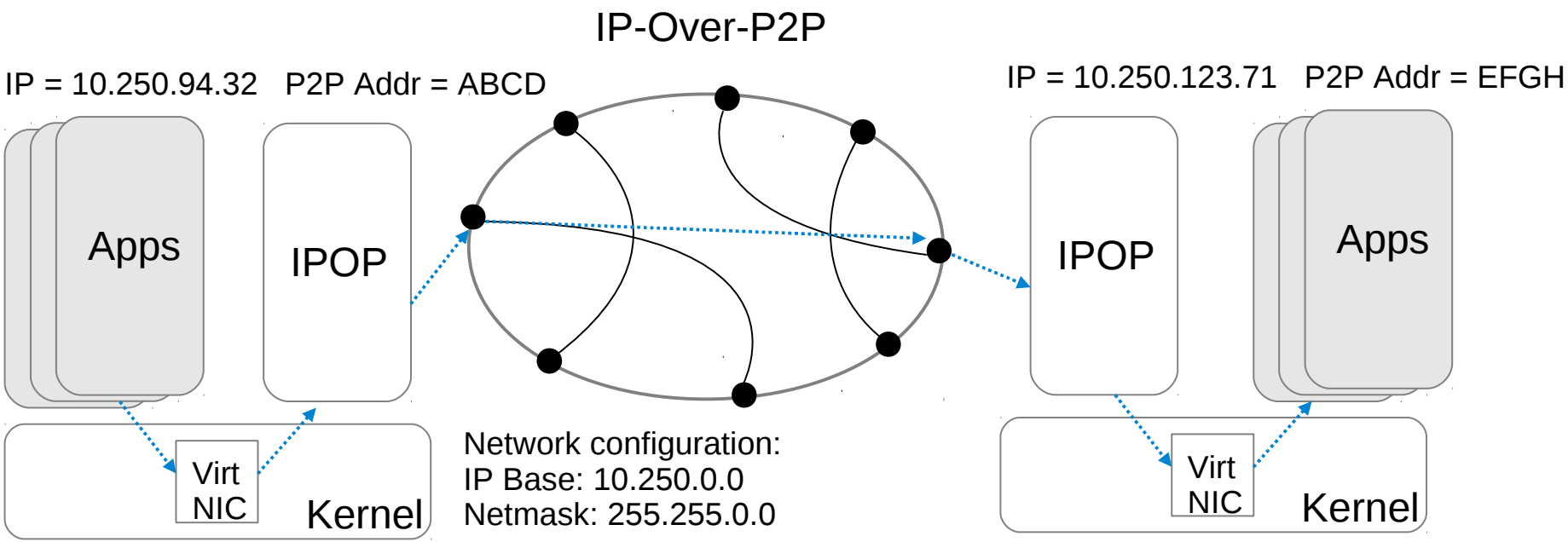
UF UNIVERSITY of FLORIDA
The Foundation for The Gator Nation

IPOP Design (1)



- Virtual LAN
  - **Self-configuring, decentralized virtual network**
  - P2P VPN routes IP packets over P2P overlay
  - Builtin security stack (or IPSec)
- P2P Overlay
  - Structured P2P overlay
  - NAT/firewall traversal
  - **Robust, scalable, and self-organizing system**

IPOP Design (2)



IP Allocation

IP addresses are assigned to nodes through the use of a DHT by performing a lookup to see if the key already exists, if so a different IP is looked up until an unallocated IP is found

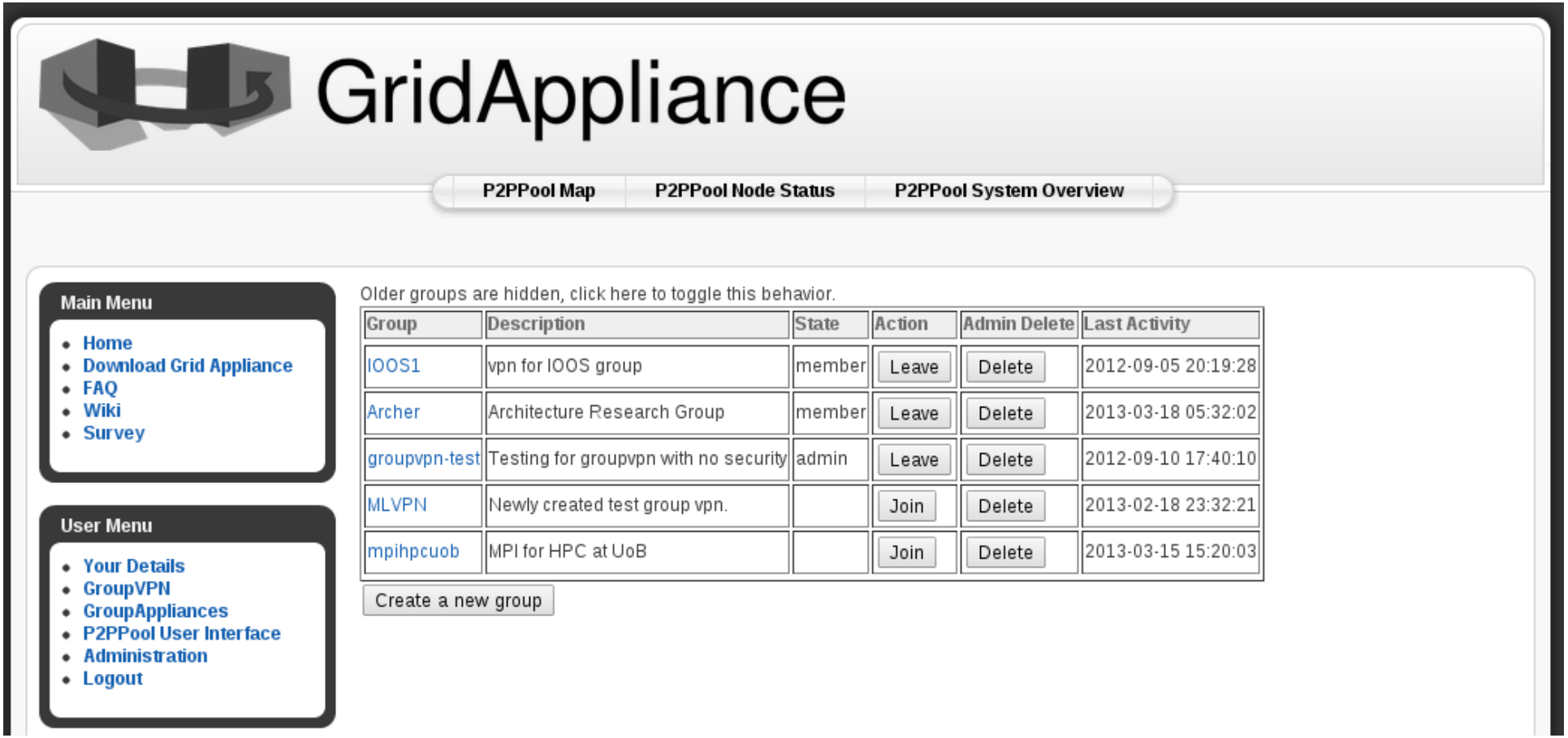
IP Resolution

IPOP uses the DHT to lookup the P2P address belonging to the destination virtual IP address

IP Tunneling

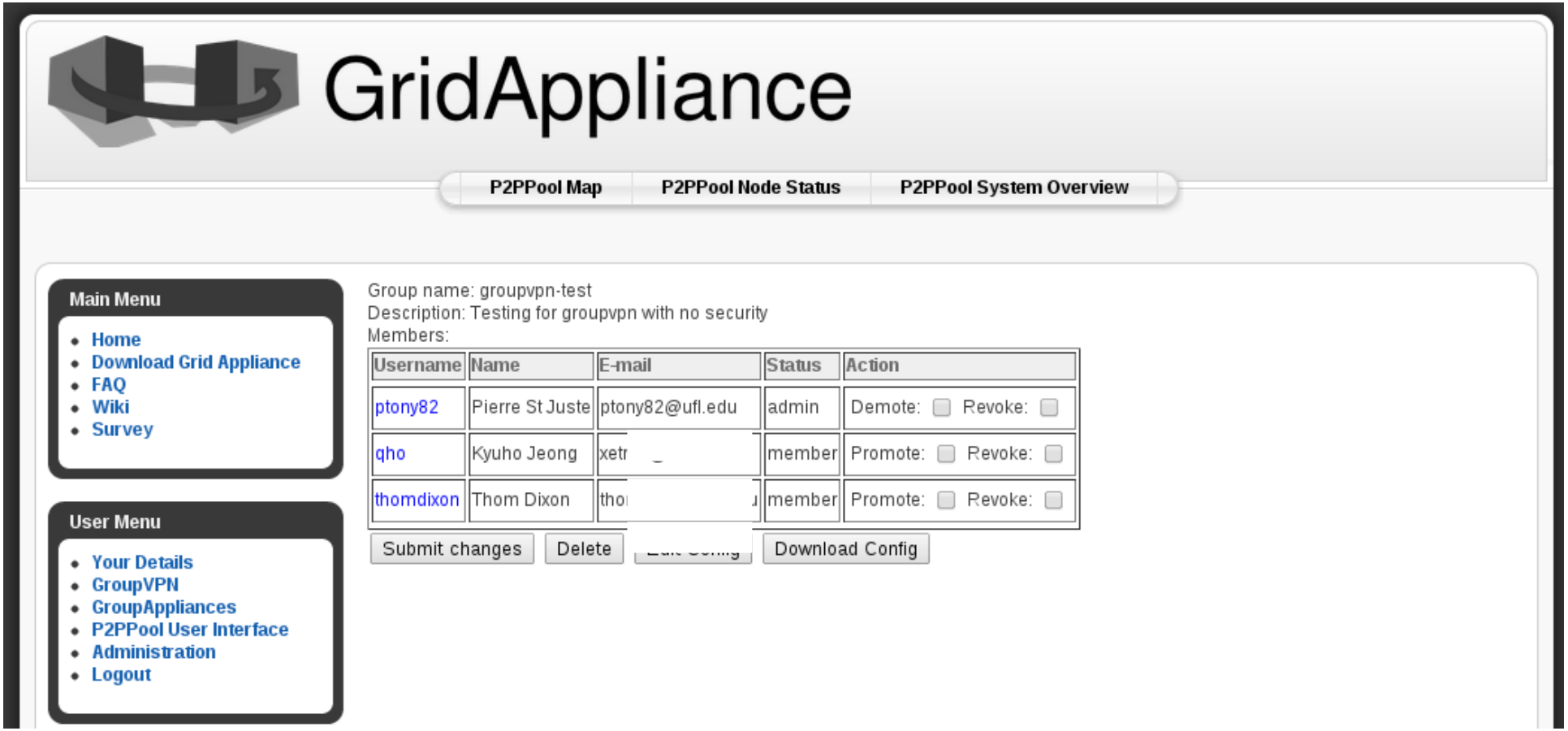
IP packets addressed to the virtual IP range are captured by virtual NIC, given to IPOP and tunneled through Brunet

GroupVPN (1)



Membership to the network is managed through the grid-appliance.org website or users can run their down web service (the code is freely available on github)

GroupVPN (2)



Each user has to go to the management site to download their configuration which includes a signed X.509 certificate, a list of bootstrap nodes for the P2P overlay, and the namespace for the DHT

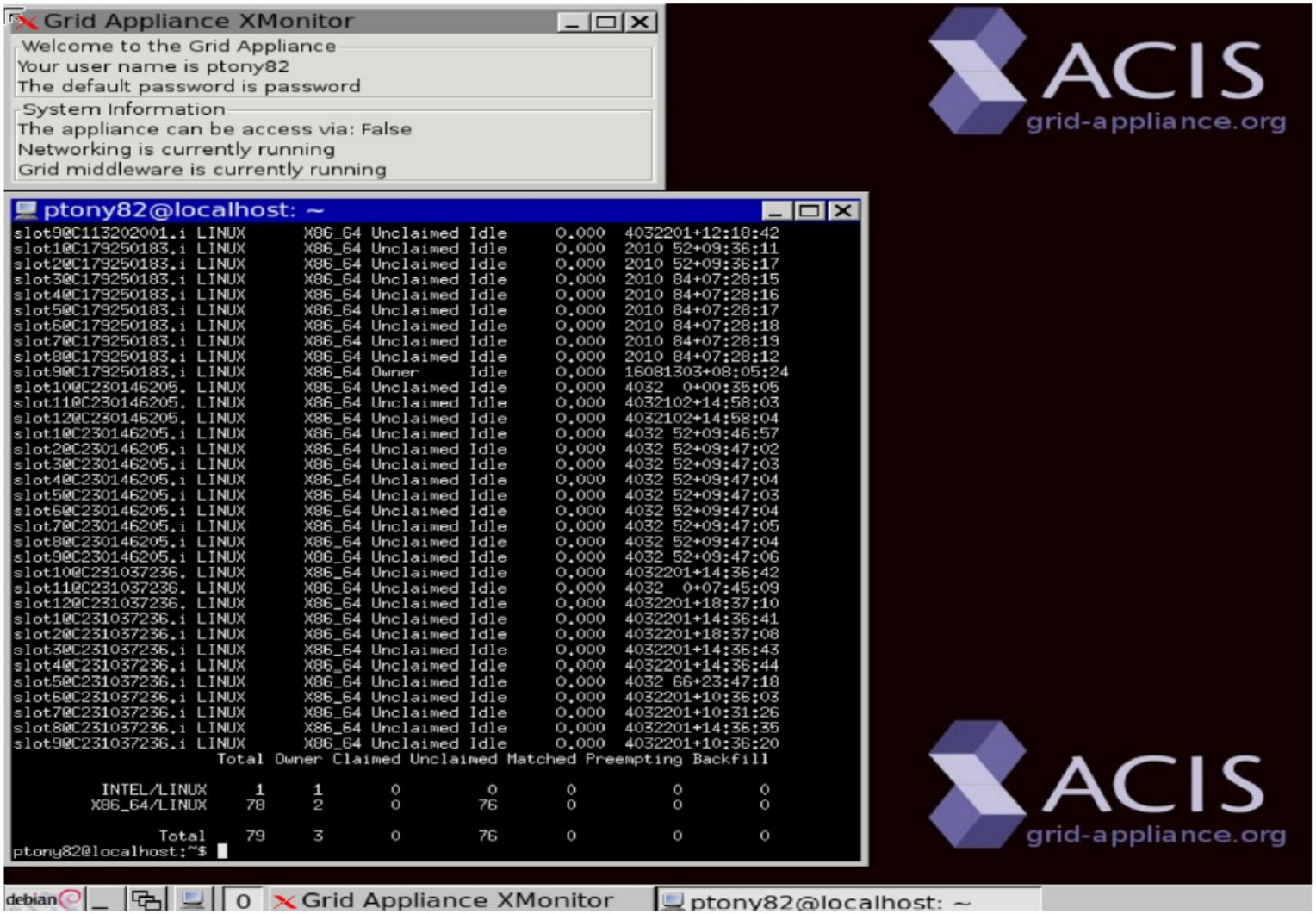
Grid-appliance.org

Condor over Wide Area

Packaged as virtual machine

Supports Vmware, Xen, Virtualbox, KVM, EC2, FutureGrid

VMs join the same VPN over wide area

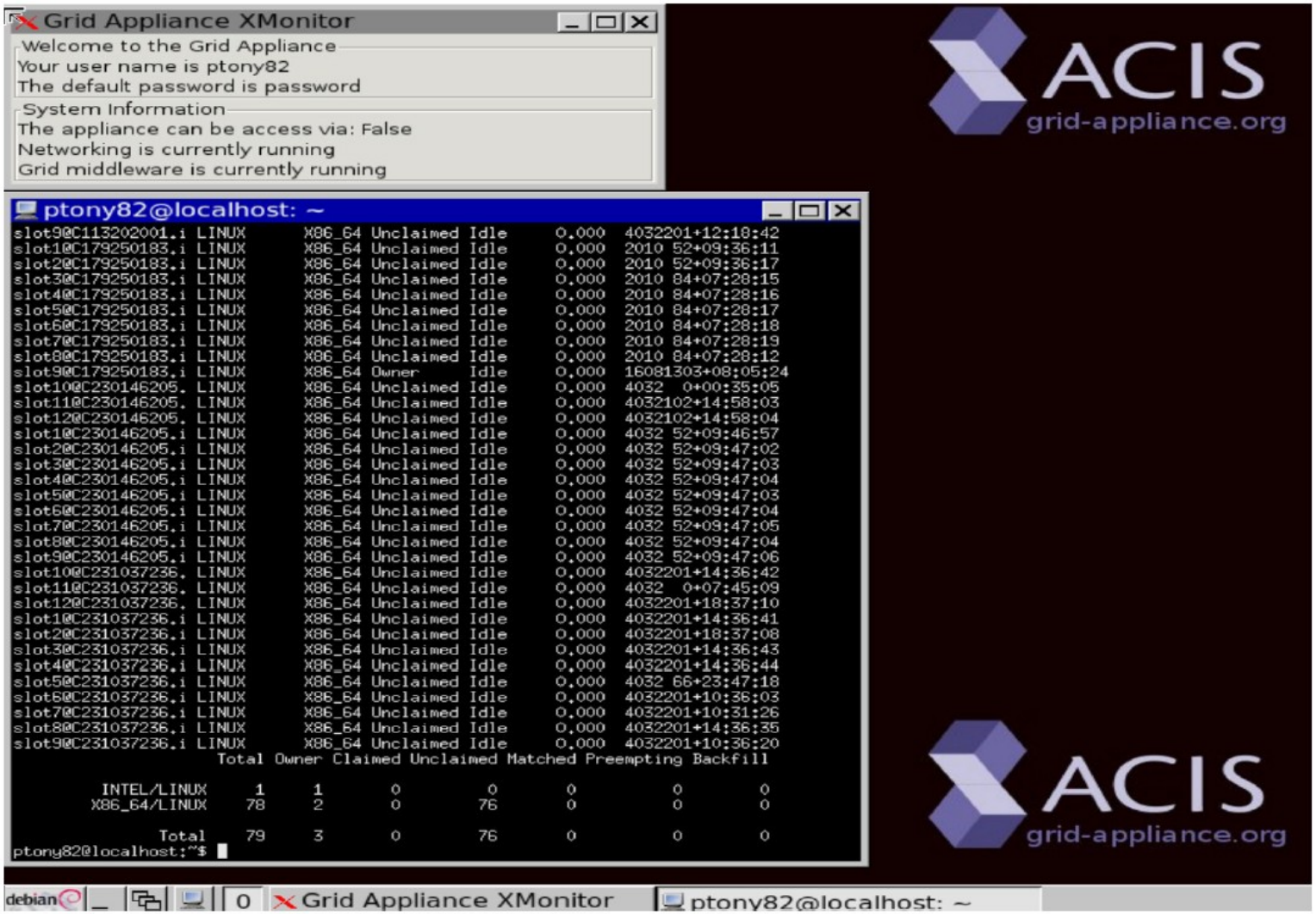


Grid-appliance.org

1) Download GridAppliance VM with Condor pre-installed

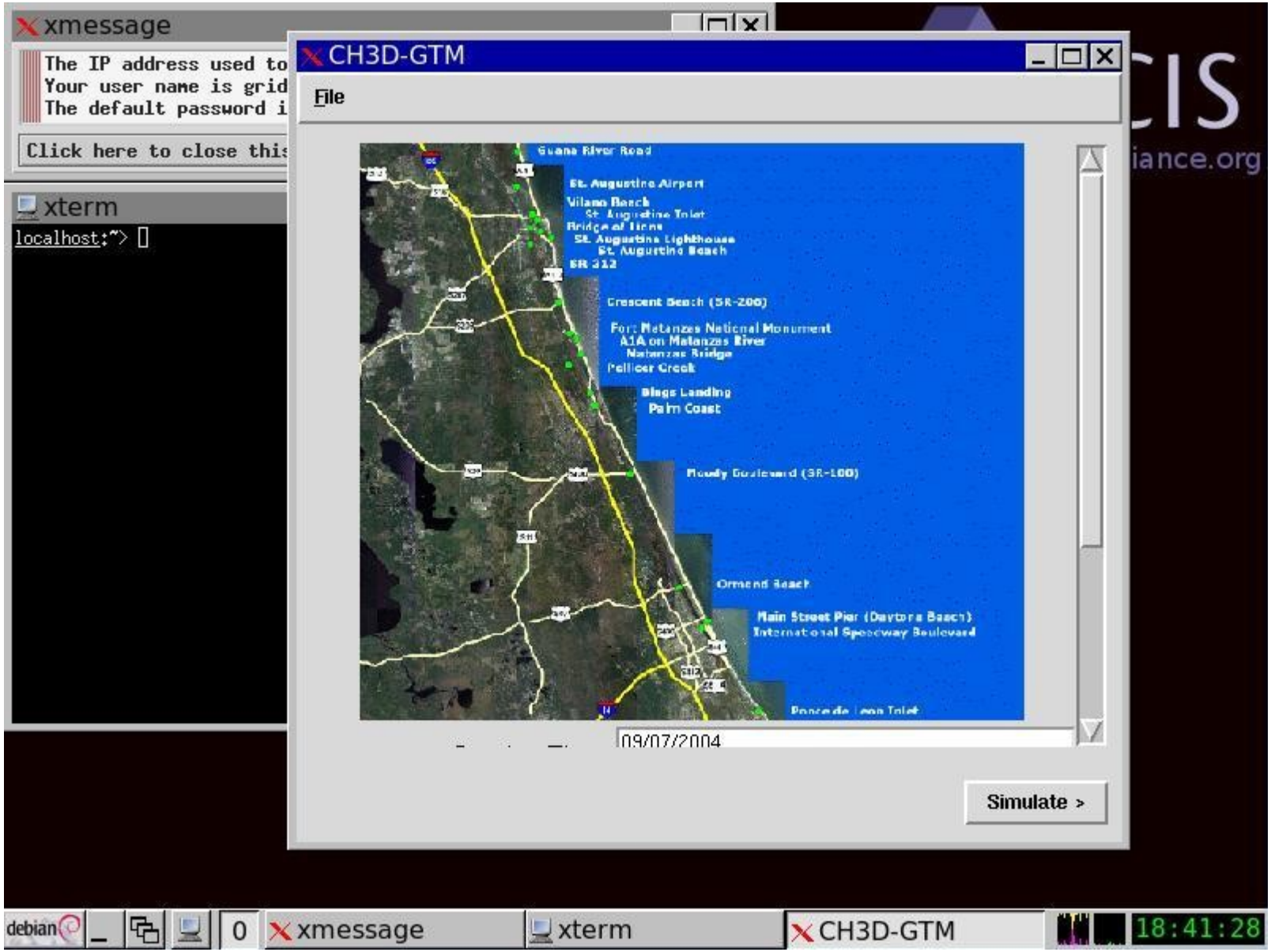
2) Download customized floppy from GridAppliance website

3) Start your VM and run condor_status

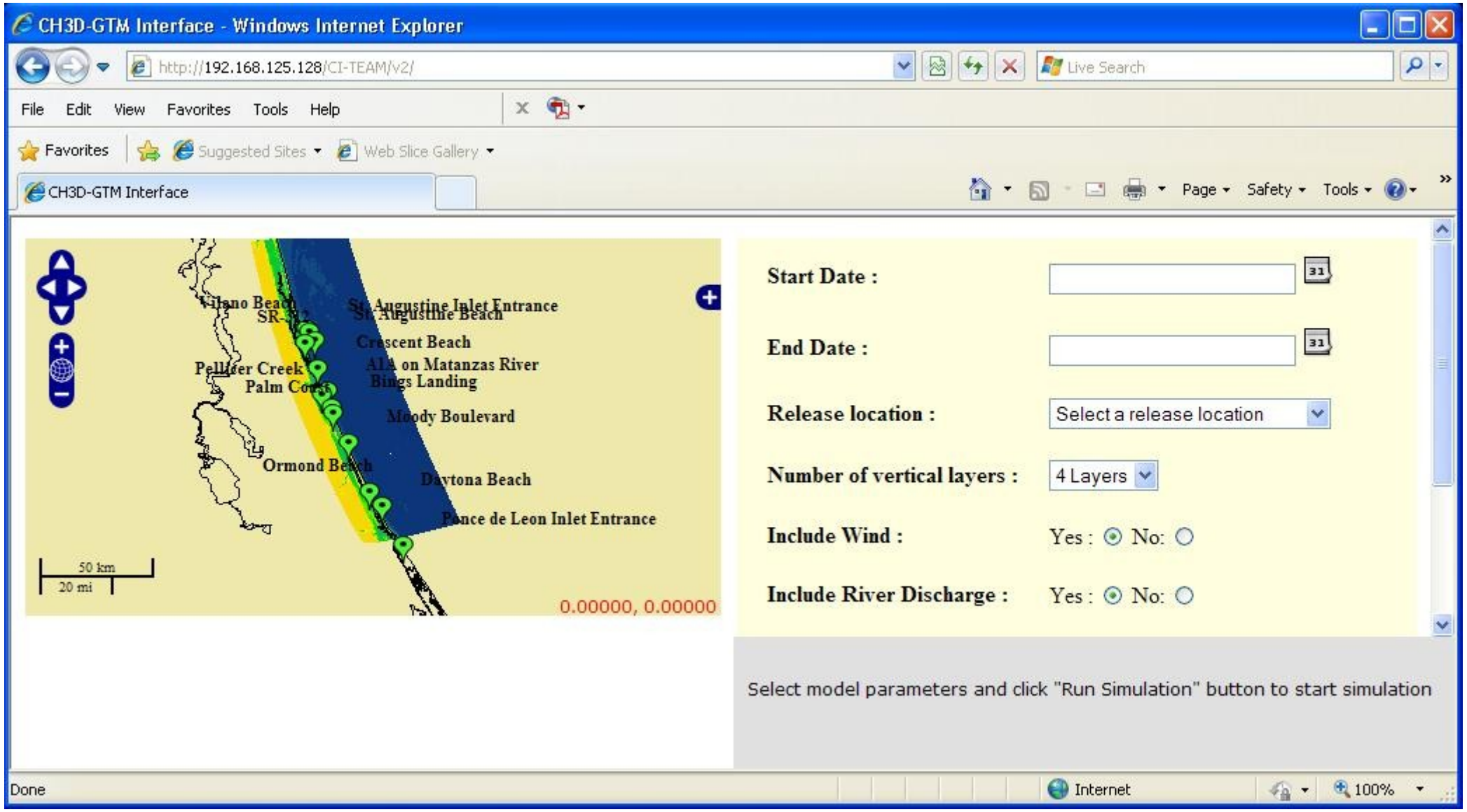


Easy with very little management

Coastal Ocean Observing and Prediction with Grid-Appliance



Coastal Ocean Observing and Prediction with Grid-Appliance



ACIS

UF UNIVERSITY of FLORIDA
The Foundation for The Gator Nation

IPOP/Grid-appliance Talking Points

1) Grid-appliance image running on EC2 and FutureGrid

2) Networking without a gateway using P2P technology

3) Self-managing for years

IPOP Demo Details

1. Create/Join virtual network group on grid-appliance.org
2. Download configuration from grid-appliance.org
3. Start Ubuntu 12.04 LTS instance on EC2
4. Add Debian repository to Ubuntu package manager
5. Install ipop using apt-get
6. Upload configuration to EC2
7. Start IPOP and connect over VPN

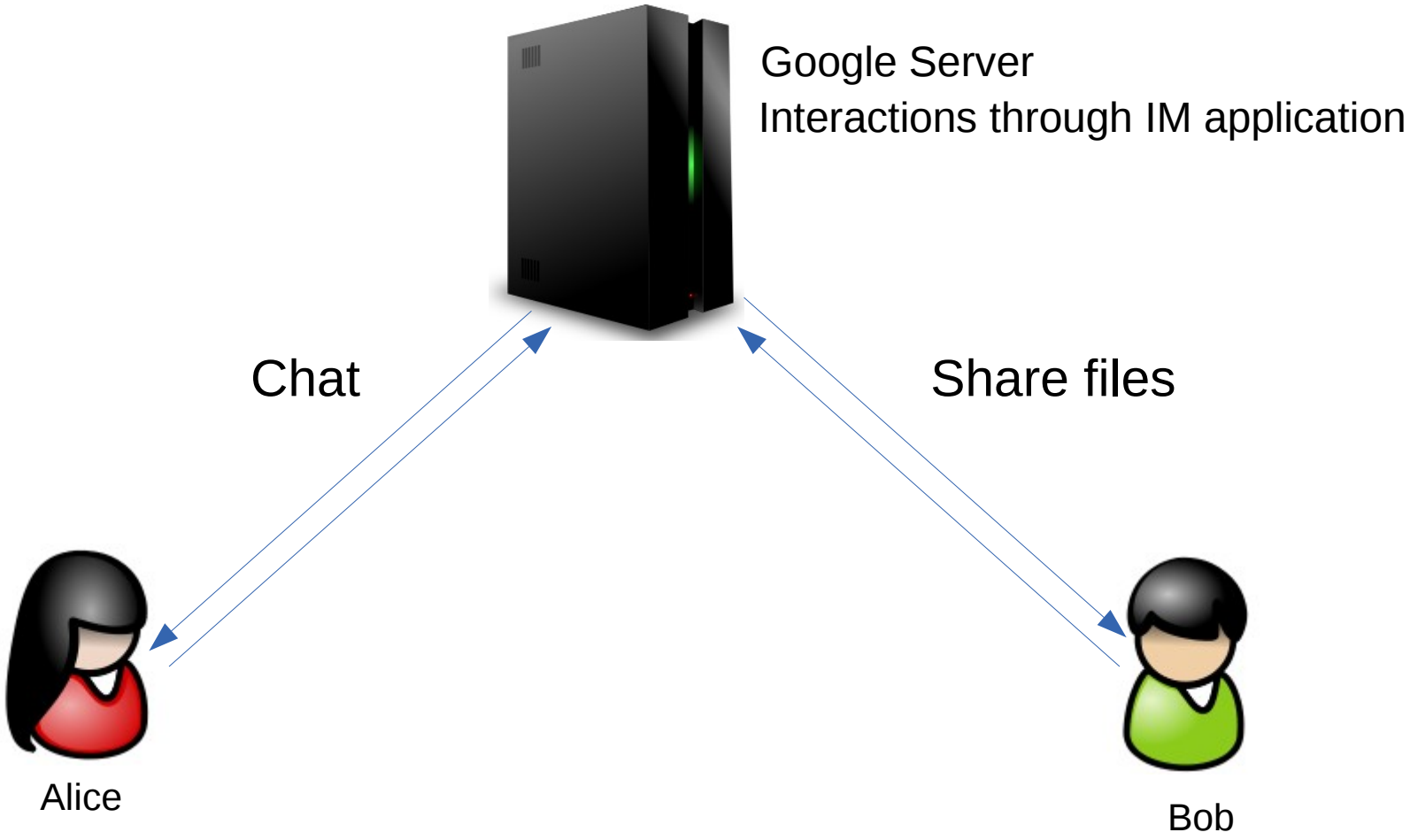
What is SocialVPN?

SocialVPN is a free and open-source **P2P Social Virtual Private Network** that seamlessly networks your computer with your friends' computers

ACIS

UF UNIVERSITY of FLORIDA
The Foundation for The Gator Nation

Alice and Bob are Google Chat buddies

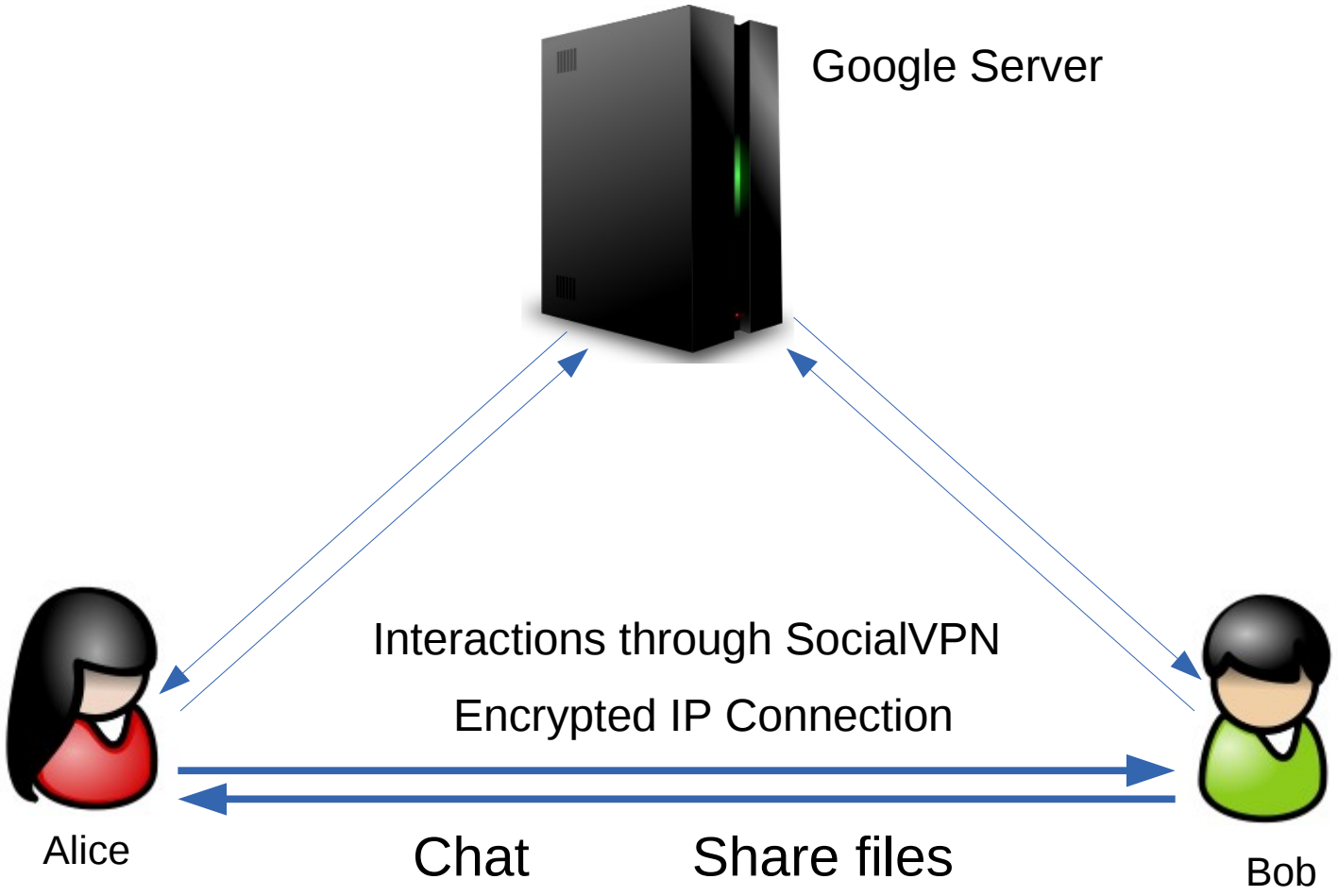


Other desktop applications cannot take advantage of this communication link between Alice and Bob

ACIS

UF UNIVERSITY of FLORIDA
The Foundation for The Gator Nation

Alice and Bob are Google Chat buddies



SocialVPN extends this social link between Alice and Bob into an encrypted network level connection so that **other applications such as iTunes can also communicate through this link**.

ACIS

UF UNIVERSITY of FLORIDA
The Foundation for The Gator Nation

What you can do with SocialVPN:

Access a folder on your friend's PC directly from your PC without installing any new software

Share your iTunes playlist with your friends

Play multi-player LAN games with your friends

Access your home PC from anywhere

Run a website on your computer that only your friends can access

And much more...

What makes SocialVPN different?

Distributed NAT Traversal

- P2P overlay is used as a distributed STUN server

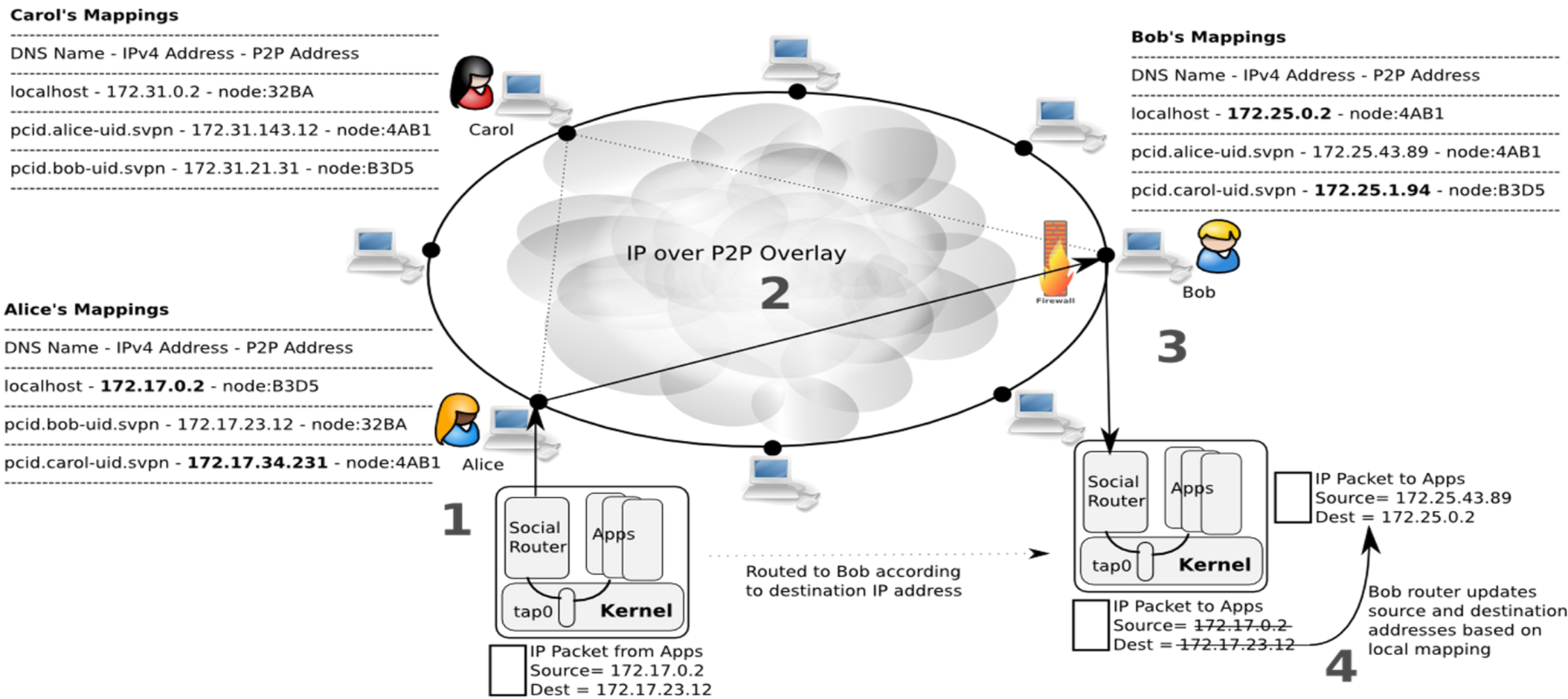
Centralized backend is not required

- Peers can exchange certificate fingerprints over the phone

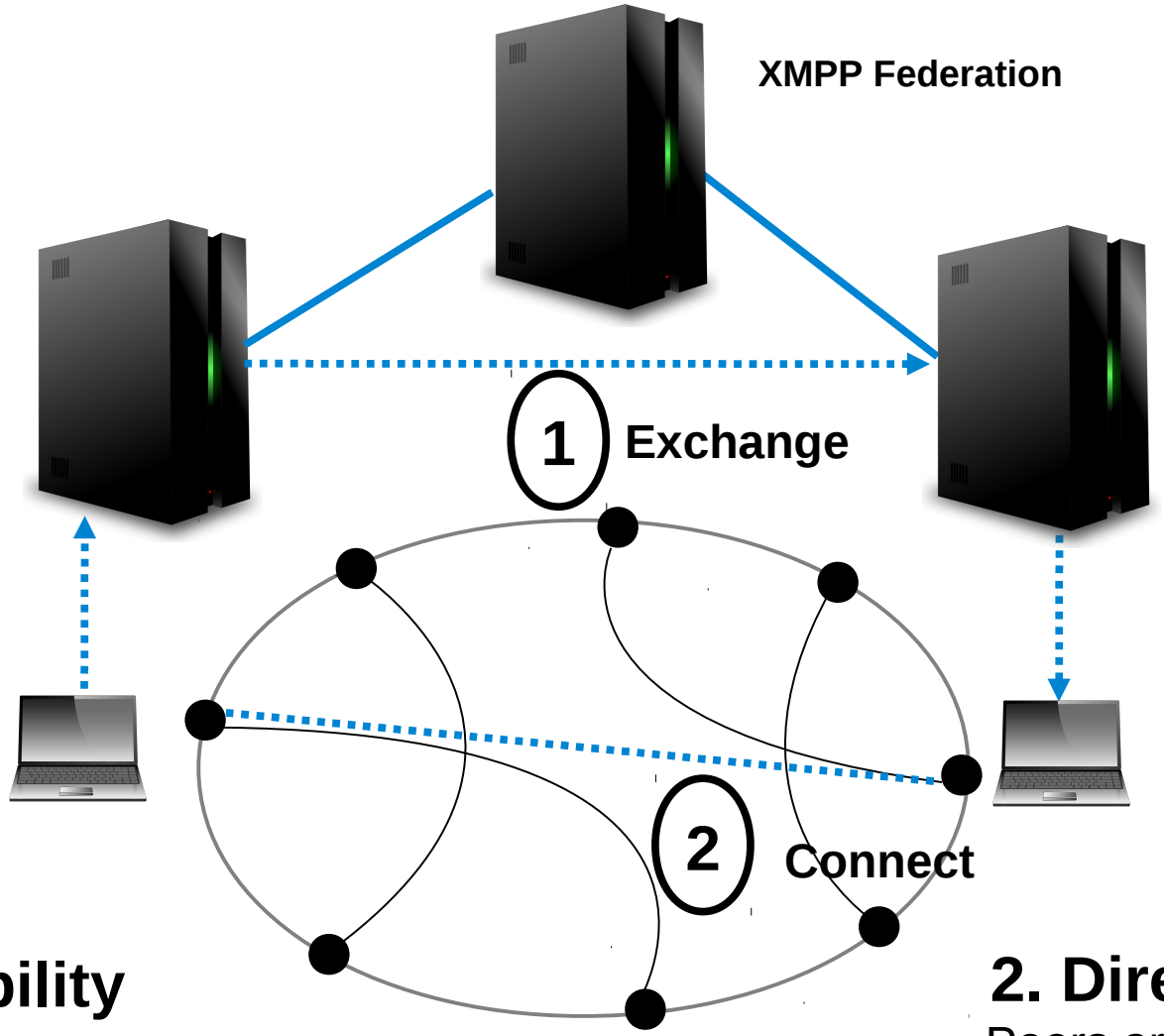
Open-source, and mature code base

- Has been running on Planetlab for over 5 years
- Anyone can contribute

SocialVPN Design (1)



SocialVPN Design (3)



1. Communication

XMPP servers maintains buddy lists for users and route XML messages

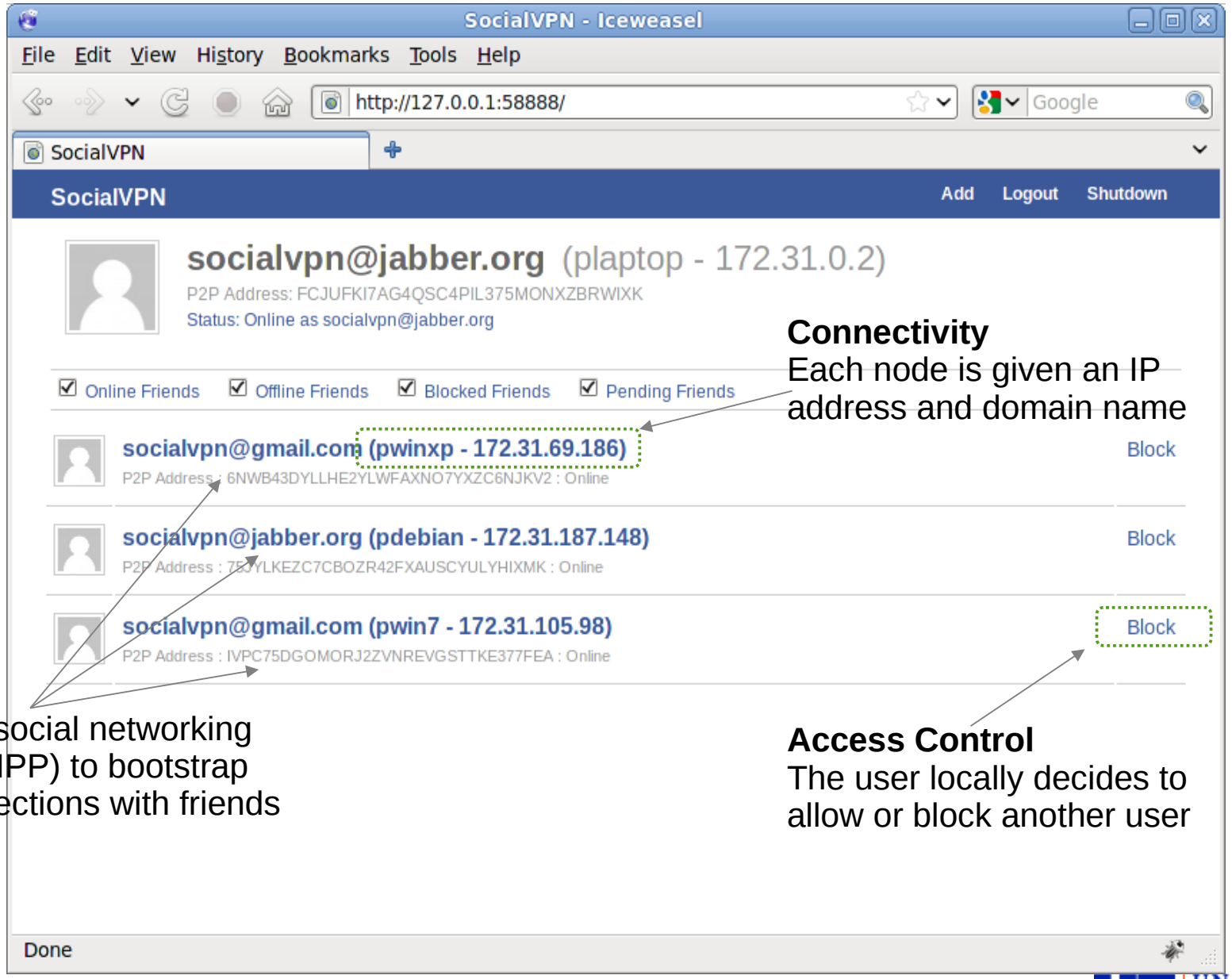
2. Direct Exchanges

Peers are able to discover each other and change X.509 certificates directly through XMPP

3. Stability

XMPP protocol is an open-standard and more stable than the Facebook API

SocialVPN Design (2)



Connectivity
Each node is given an IP address and domain name

Trust
Use current social networking systems (XMPP) to bootstrap secure connections with friends

Access Control
The user locally decides to allow or block another user

SocialVPN Design (2)

The code is **open-source** (socialvpn.org) and runs on Windows and Linux; it has been **downloaded over 10,000 times** since September 2009, there are between **80 – 120 users at any given time**

Trust
Use current social networking systems (XMPP) to bootstrap secure connections with friends

Access Control
The user locally decides to allow or block another user

SocialVPN Demo Details

1. Download SocialVPN from socialvpn.org
2. Extract and run SocialVPN
3. Login using Google credentials
4. Ping machine