DOWNRANGE TECHNOLOGIES

RICOCHET

Advanced Communication Platform

DOWNRANGE TECHNOLOGIES

Problem

- Secure Communication Infrastructure is difficult to design, deploy, operate and maintain.
- No COTS orchestration tools are available to support the IC/DoD market
- Need a turn-key solution to provide immediate results

DOWNRANGE TECHNOLOGIES

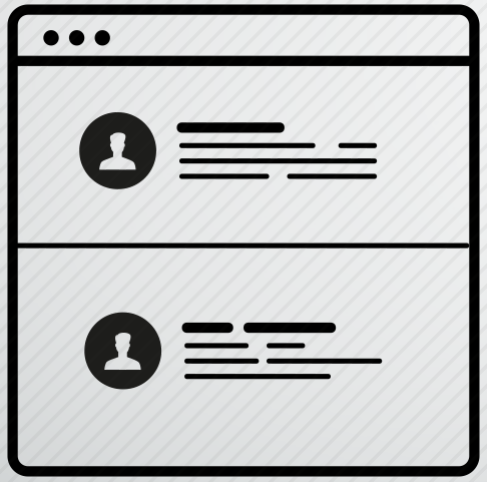
Solution

Ricochet is a web-based, software toolkit designed to dynamically provision, configure, and enable ephemeral, global, and secure communications on-demand. The toolkit allows users to quickly and easily standup multi-hop, global virtual communications infrastructure to enable secure data services using encrypted communication protocols and industry best-practices.

The software toolkit is designed for use by a beginner-to-intermediate operator and does not require in-depth technical knowledge to operate.

Components

GUI



Build Engine

Script Repo

Ricochet: Features

- **Strong Crypto:** AES-256-CBC, SHA512, TLS 1.2
- **Globally available:** Hosts/Hops can be provisioned in over a dozen countries
- **Hosts secure:** Hosts are automatically hardened with best practices; have been red-teamed by third-party
- **On-The-Fly Host Generation:** Hosts and keys are created on-demand and are never pre-staged
- **Self-Destruct:** Hosts are (optionally) securely destroyed after a user-specified period of time
- **Multi-Hop Capable:** The Operator is capable of choosing the number and location of redirect hops needed; Entry and exit points

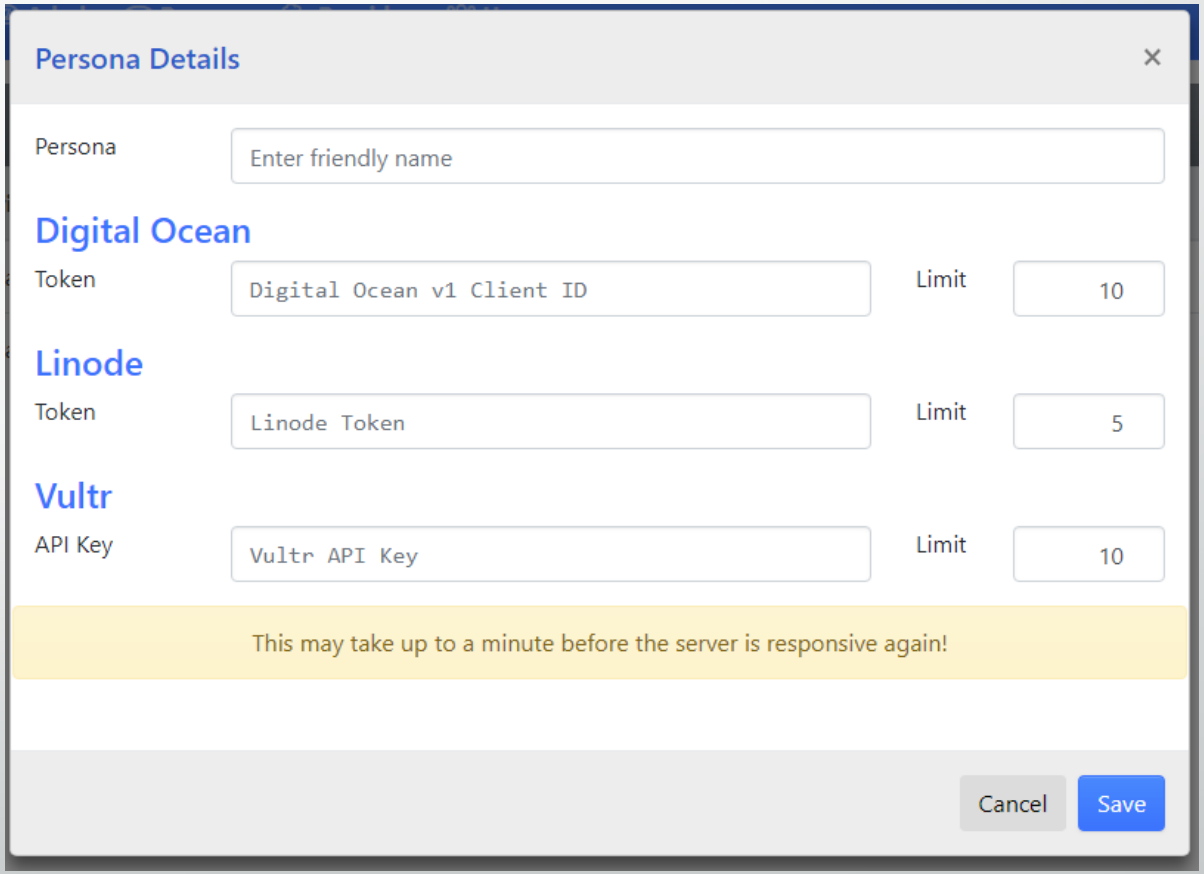
DOWNRANGE TECHNOLOGIES

Ricochet: Features

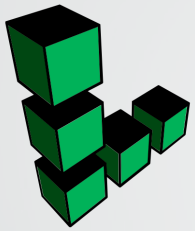
- **Communications are Encrypted End-to-End:** Hop-Hosts do not contain crypto keys and cannot decrypt traffic; They are blind redirectors
- **Multiple Vendors Diversity:** Currently support four (4) VPS providers, more being added
- **Active and Passive Countermeasures:** Client-side traffic production agent and adaptive firewall
- **Early-Warning-System capable:** Ricochet-created hosts contain an (optional) lightweight IDS (bro-ids) to monitor non-Secure communications for third-party probing and introspection.
- **Managed Attribution:** Designed with Persona Management functionality at the user level
- **Monitoring:** Uses m/monit and monit for active, passive, and proactive monitoring

Ricochet: Persona Management

- Ricochet exposes persona management functionality to the admin user
- This enables the user to control the associated persona they want to use when building Tunnels for their clients
- User can set limits for each provider



Current VPS Support



linode

amazon web services™ | EC2

DigitalOcean

VULTR

Planned

- Azure

Usage Modes

- **Research mode:** (Vertical) Allows for clients to anonymize their location and digital footprint (non-attribution)
- **Virtual Desktop:** (Vertical) Offers a Virtual Desktop to the user to manage a digital persona (ephemeral)
- **Collaboration mode:** (Horizontal) Multi-hop connectivity to secure, private communication services (chat, file, voice, email and video)
- **Platform Mode:** Root access to the end-node via SSH. Authentication via Public Key only. (advanced)

DOWNRANGE TECHNOLOGIES

Ricochet: Research Mode

When used in "Research" mode, a user will connect to the Tunnel at the entry point. All of their communications will be sent through the Tunnel, exiting through the exit node.

- To connect, the user needs VPN software, which we provide with Ricochet.
- VPN software is available on Windows, Mac, Linux, iOS and Android
  - The mobile application does not require root or jailbreak and a compatible VPN client is available in respective app stores
- In this mode, no collaborative services are offered at the endpoint

Ricochet: Collaborative Mode

When used in "Collaborative" mode, a user will connect to the Tunnel at the entry point. No communications are allowed outside of the tunnel and the user seemingly cannot access the internet.

- Multiple collaborative services are offered within the tunnel. For example, users can chat with one another using a jabber/xmpp compatible application.
  - This protocol also supports group chat and basic file transfers between two users.
- More advanced services are available, such as closed-domain email, voice and video services.
  - A user only needs a compatible SIP client to leverage communication services and/or an email client to send and receive email.

Ricochet: Platform Mode

When used in "Platform" mode, the server does not offer communication services or secure tunneling. The user accesses the end-node via SSH by connecting to the entry node.

The user is provided with a root shell on the end node and all commands are executed there.

This is optimal for Computer Network Operations.

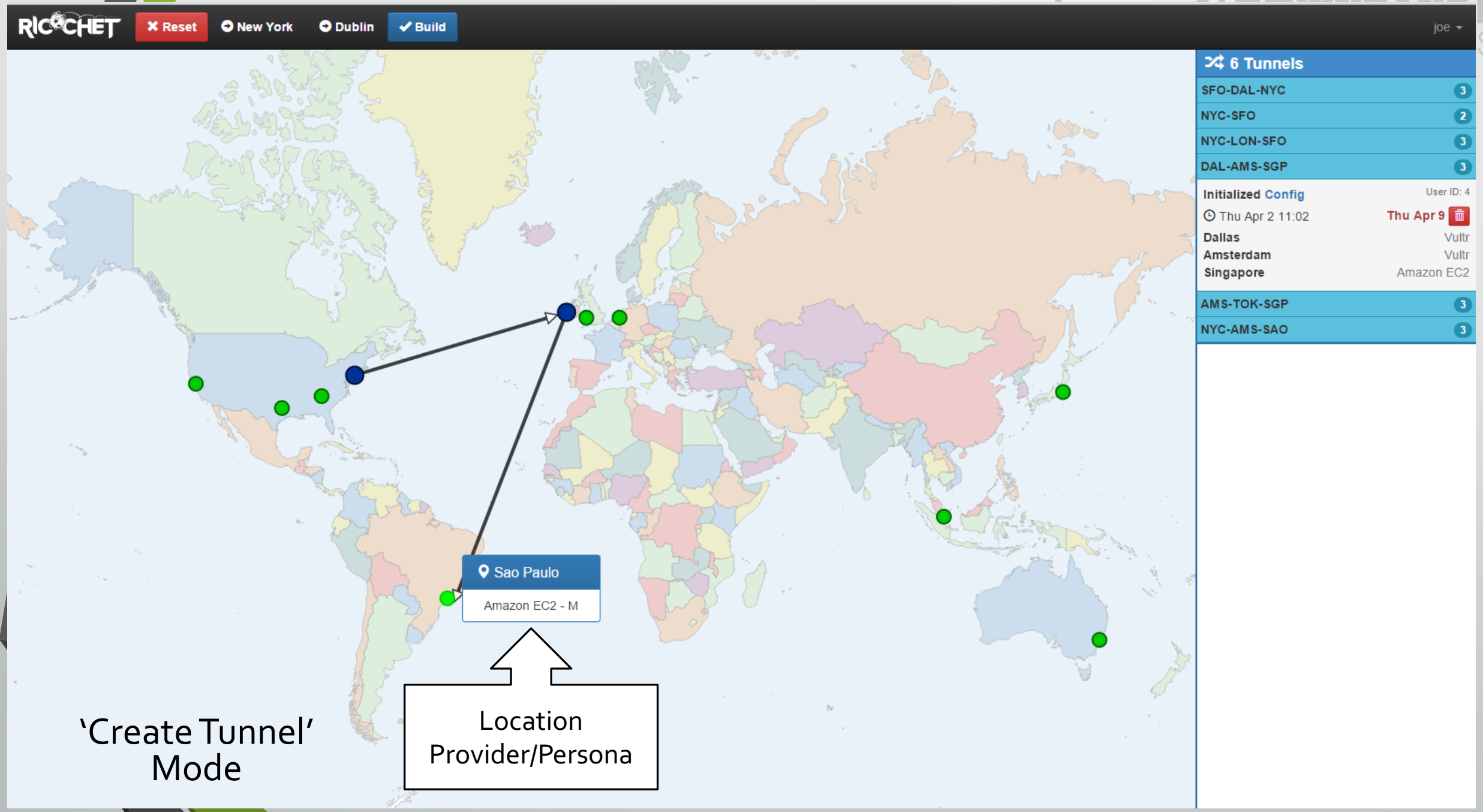
Ricochet: Virtual Desktop Mode

When used in "Virtual Desktop" mode, Ricochet will install and configure the *noMachine* Virtual Desktop daemon. This daemon is web accessible and does not require any specialized client software. *noMachine* is a very mature and stable COTS product

- Once the user is connected to the **Ricochet** Tunnel, the Virtual Desktop environment is accessible via a private IP address (e.g. https://10.1.1.1/).
- Once connected, the browser transforms into a highly configurable virtual desktop. Only the activity that occurs within the browser is routed through the tunnel. All other communications from the host machine are routed normally.
- Currently, noMachine can virtualize Linux and Windows environments. An (optional) client application is available for Windows, Mac, Linux, Android and iOS.

DOWNRANGE TECHNOLOGIES

Building a Tunnel


RICOCHET
Reset
New York
Dublin
Build
joe
6 Tunnels
SFO-DAL-NYC 3
NYC-SFO 2
NYC-LON-SFO 3
DAL-AMS-SGP 3
Initialized Config
User ID: 4
Thu Apr 2 11:02
Thu Apr 9
Dallas Vultr
Amsterdam Vultr
Singapore Amazon EC2
AMS-TOK-SGP 3
NYC-AMS-SAO 3
Sao Paulo
Amazon EC2 - M
'Create Tunnel' Mode
Location Provider/Persona

Ricochet Tunnel

Name: TOR-ATL-FRA-DEC3

Profile: (•) Research ( ) Platform ( ) Dispersive

Clients: 1 ▾ Lifetime in days: 7

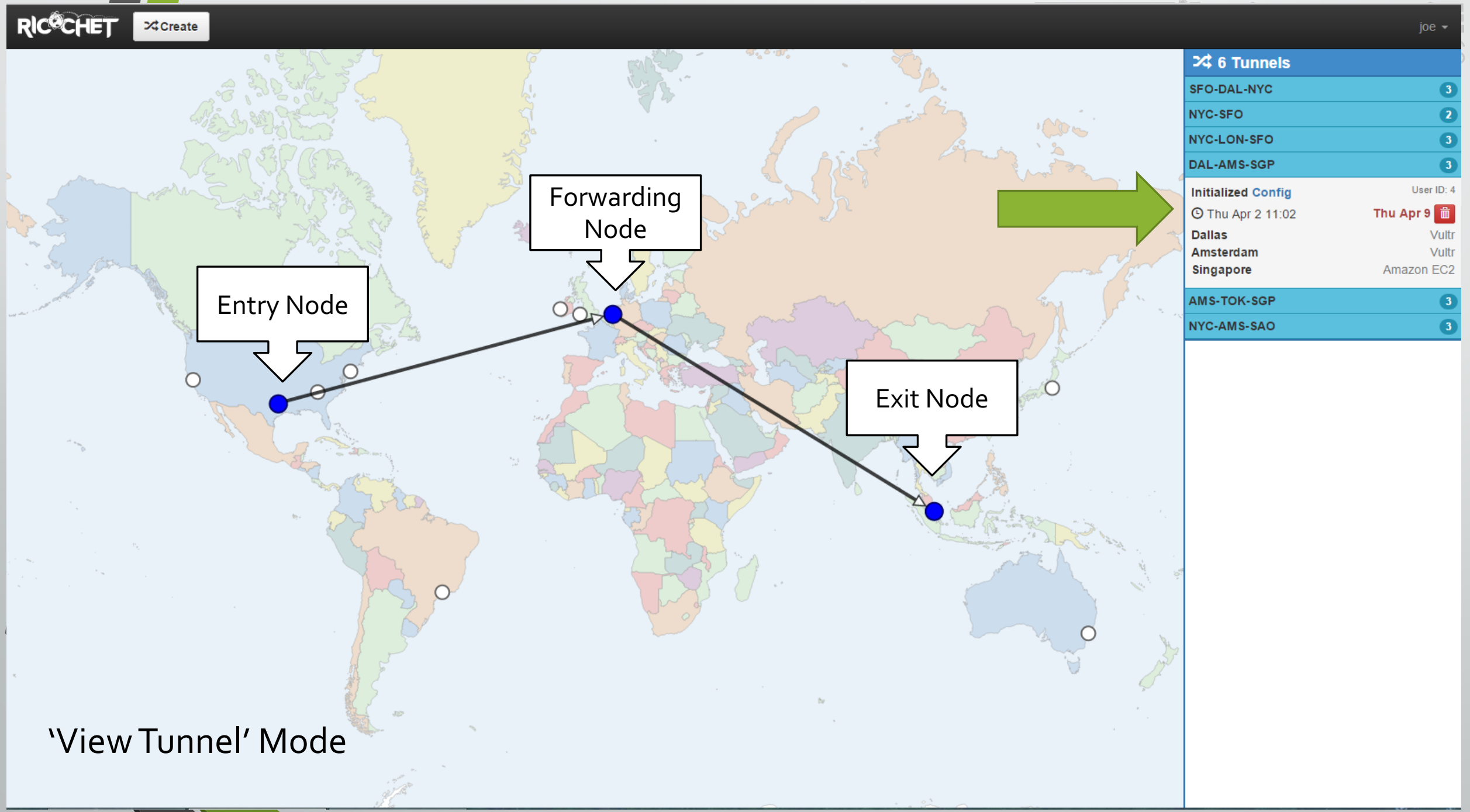
City	Status	Provider
Toronto	Planning	Digital Ocean - DO ▾
Atlanta	Planning	Vultr - DO ▾
Frankfurt	Planning	Digital Ocean - DO ▾

Cancel Build

Ricochet: Building a Tunnel

- Name: All Tunnels have a friendly name. By default, it is named based on the hops chosen in "Create Tunnel" mode.
- Mode: Determines what type of Tunnel you want to create
- Clients: The user can create multiple client configurations at once.
- Lifetime in Days: The Tunnel will self-destruct after the period of time set by the user. A lifetime of zero means, never self-destruct.
- Provider/Persona: Choose which persona you want each node to be associated with.

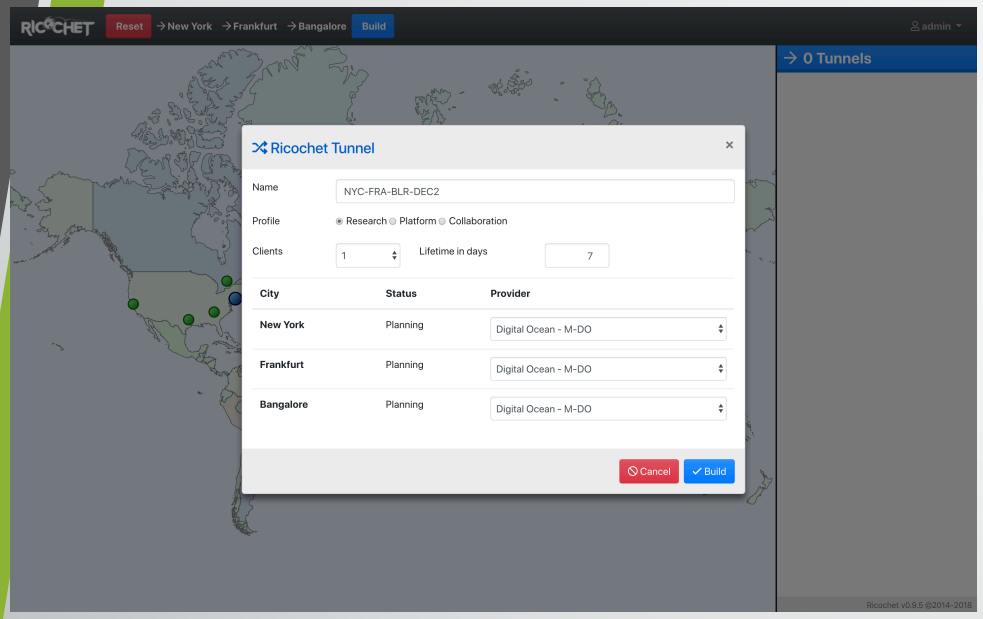
Normal Build time is between 2-4 minutes, depending on the provider used (Some are slower than others)


RICOCHET
Create
joe
6 Tunnels
SFO-DAL-NYC 3
NYC-SFO 2
NYC-LON-SFO 3
DAL-AMS-SGP 3
Initialized Config
User ID: 4
Thu Apr 2 11:02
Thu Apr 9
Dallas Vultr
Amsterdam Vultr
Singapore Amazon EC2
AMS-TOK-SGP 3
NYC-AMS-SAO 3
Forwarding Node
Entry Node
Exit Node
'View Tunnel' Mode

DOWNRANGE TECHNOLOGIES

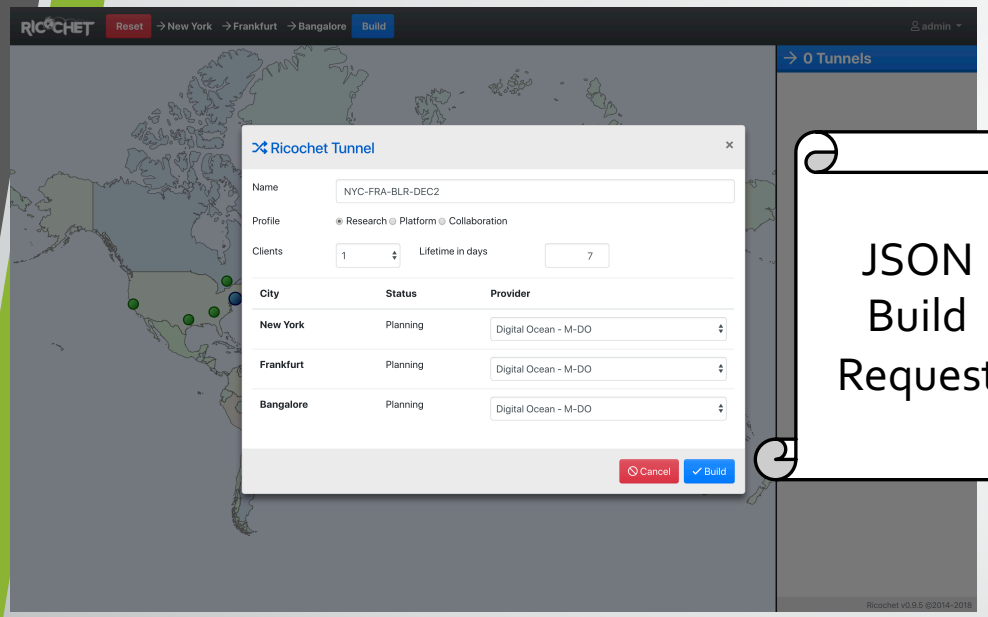
Some Technical Notes

- Comms are encrypted end-to-end, keys are generated on the controller server
  - CA private key is located on Ricochet server, can be moved
- Build Engine generates a unique CA for each Tunnel
- Ricochet is written in Python
  - Uses tornado, d3.js, and other common web frameworks
- Platform is Ubuntu 16.04 LTS
- Tunnels are (arbitrarily) limited to three hops. This can be changed, but increases latency
- Software used:
  - OpenVPN, fail2ban, OpenSSH, noMachine, ejabberd, Zimbra, Viscosity



Build Engine

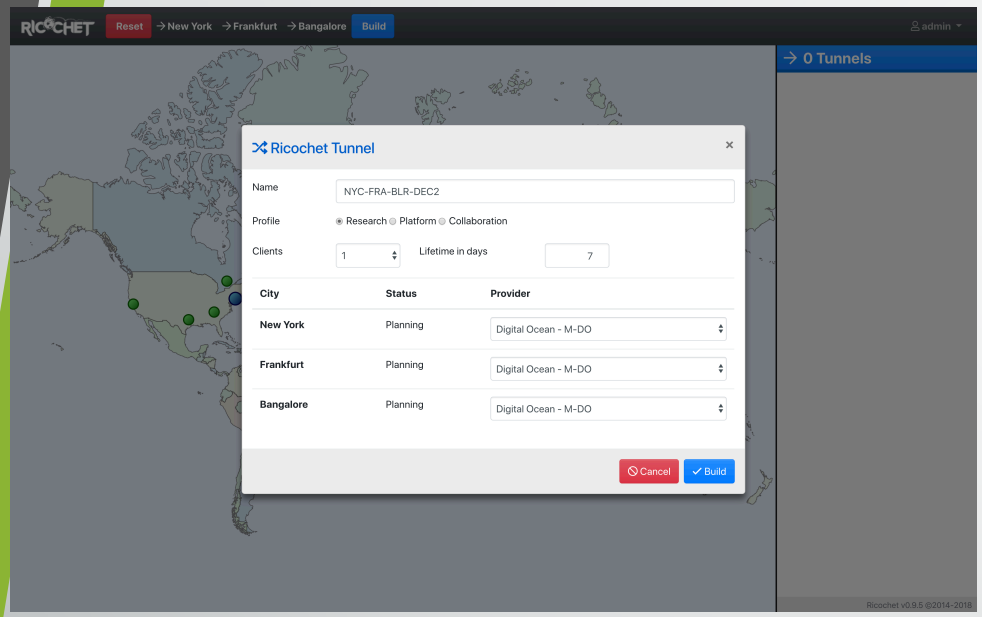
Script Repository

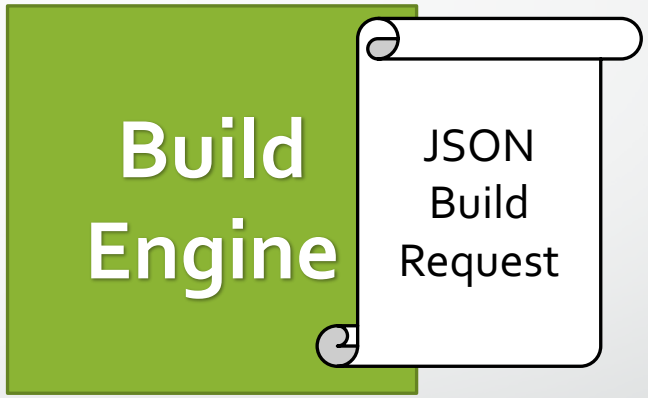


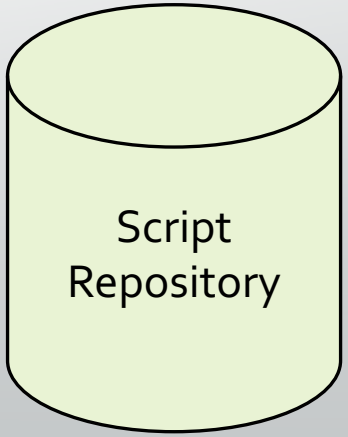
JSON Build Request

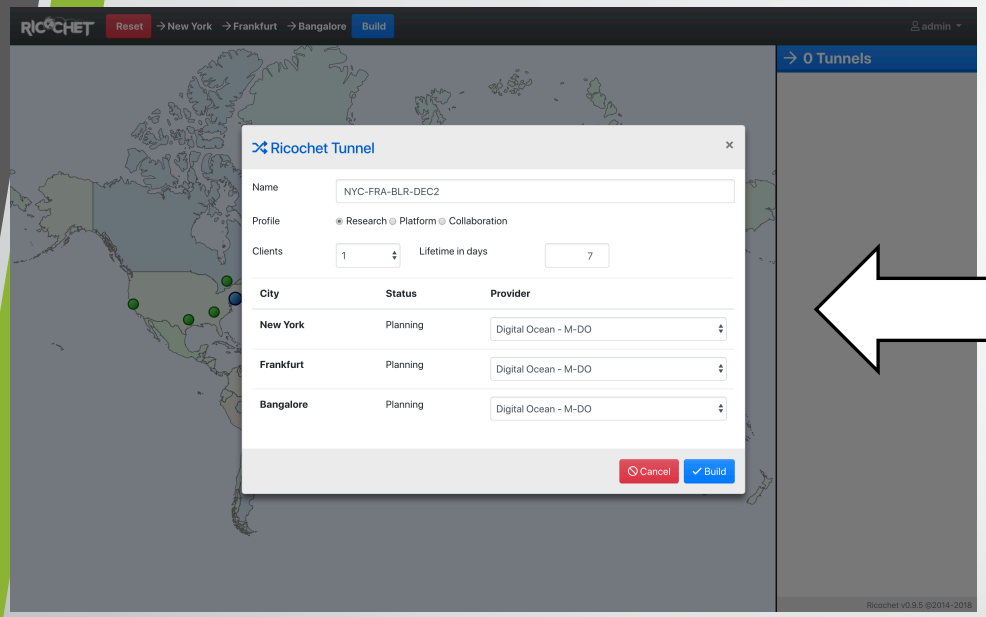
Build Engine

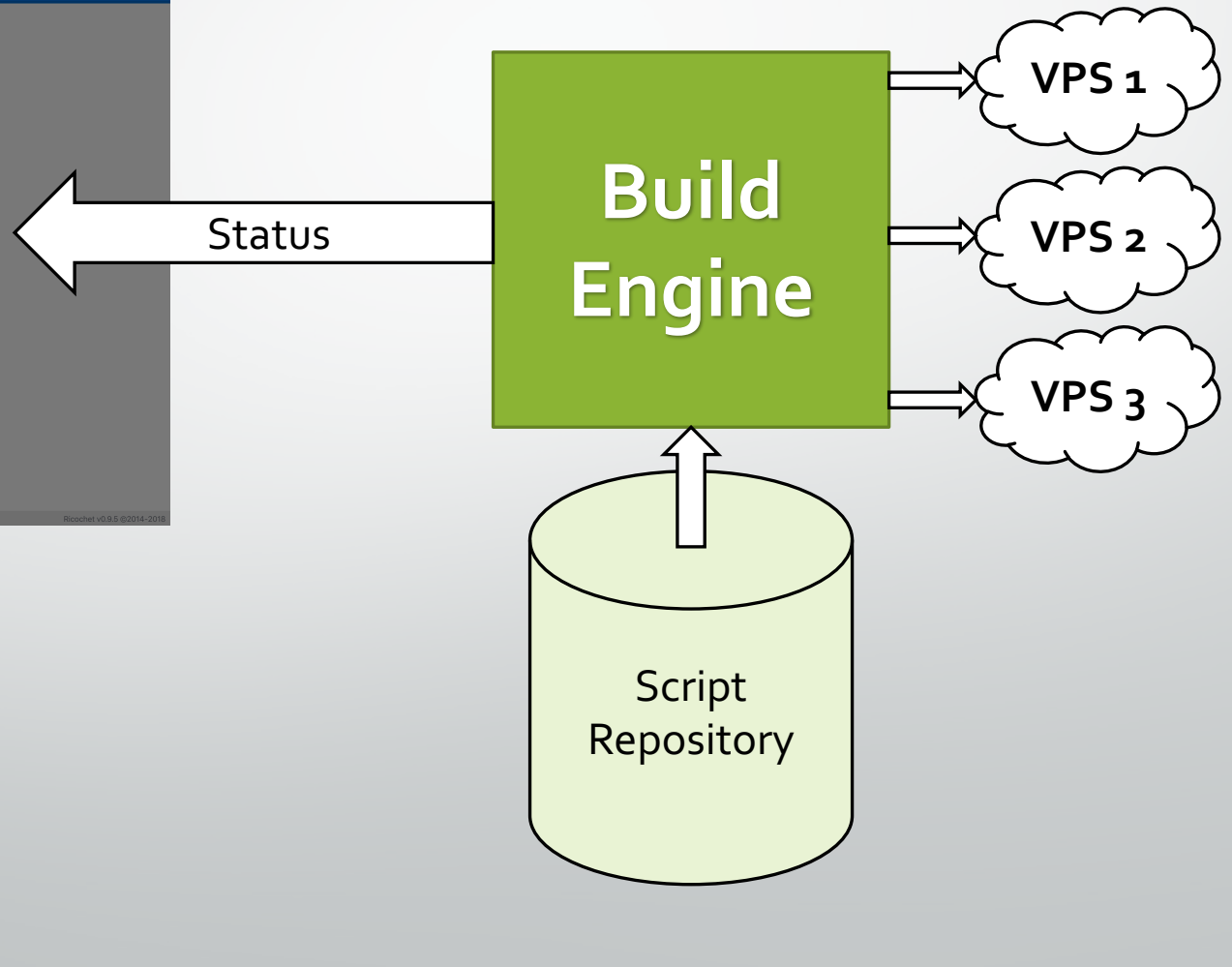
Script Repository

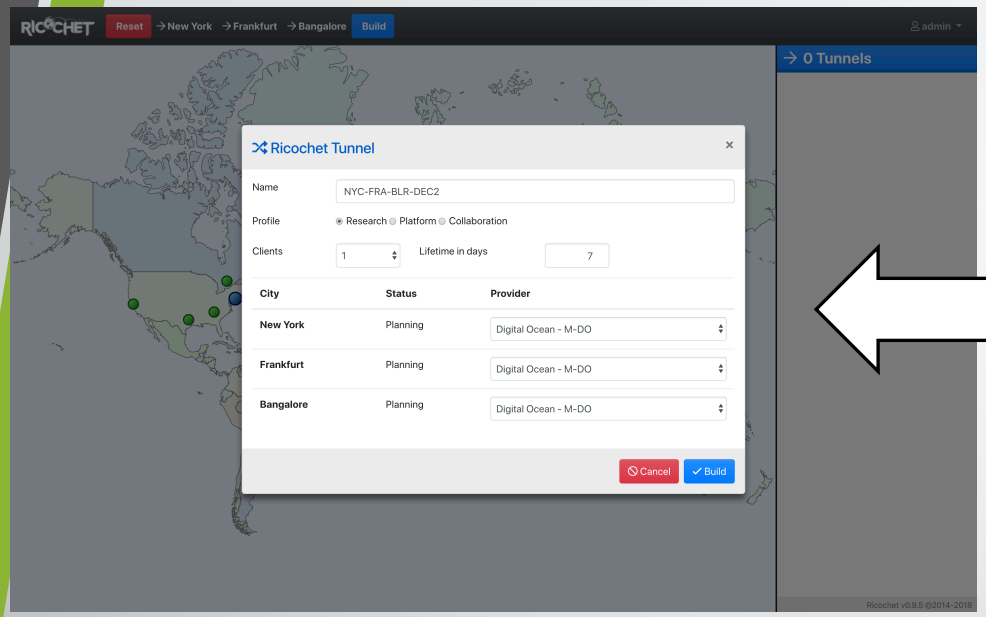

RICOCHET
Reset
New York
Frankfurt
Bangalore
Build
admin
0 Tunnels
Ricochet Tunnel
Name
NYC-FRA-BLR-DEC2
Profile
Research
Platform
Collaboration
Clients
1
Lifetime in days
7
City
Status
Provider
New York
Planning
Digital Ocean - M-DO
Frankfurt
Planning
Digital Ocean - M-DO
Bangalore
Planning
Digital Ocean - M-DO
Cancel
Build
Ricochet v0.9.5 ©2014-2018

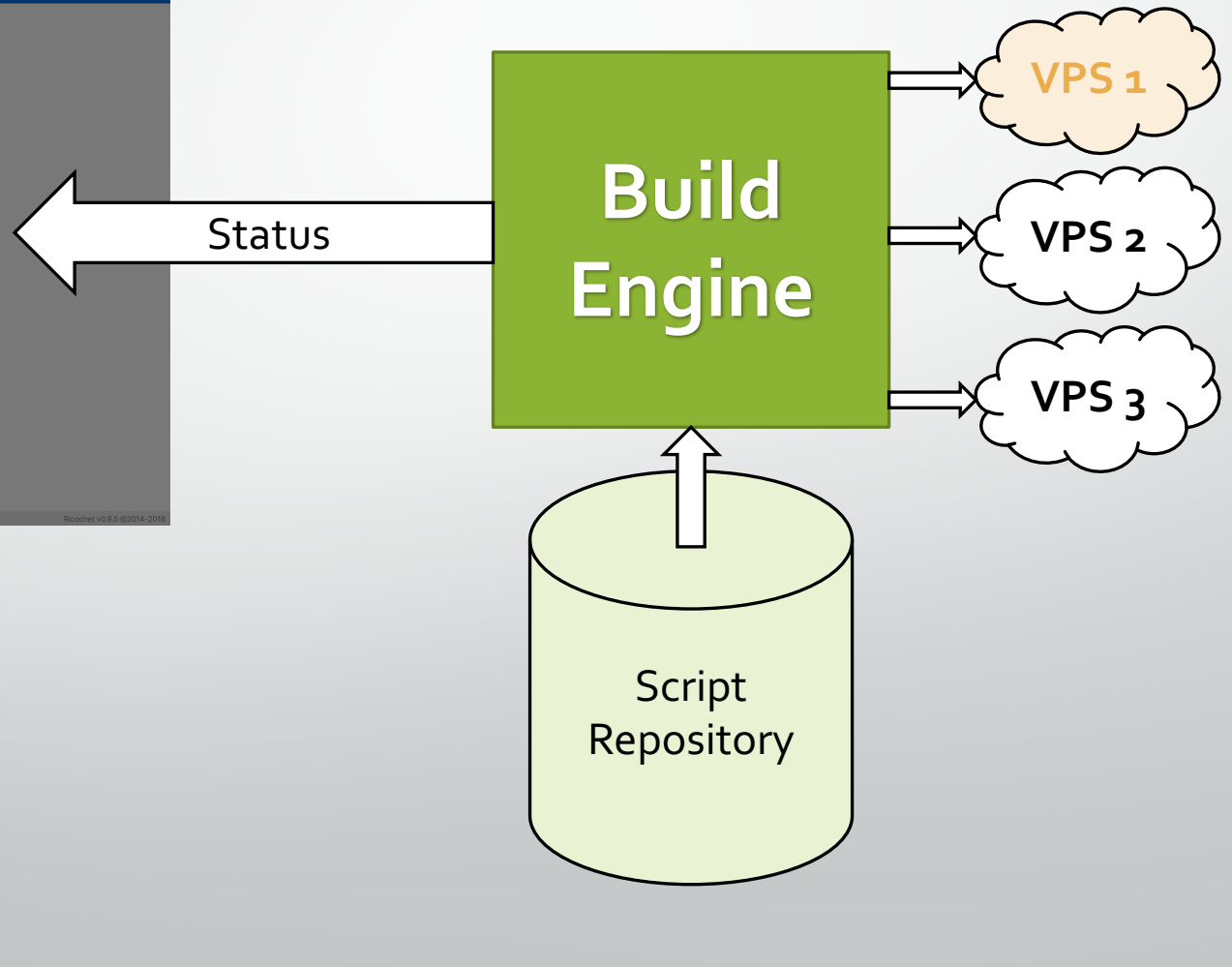

Build Engine
JSON Build Request

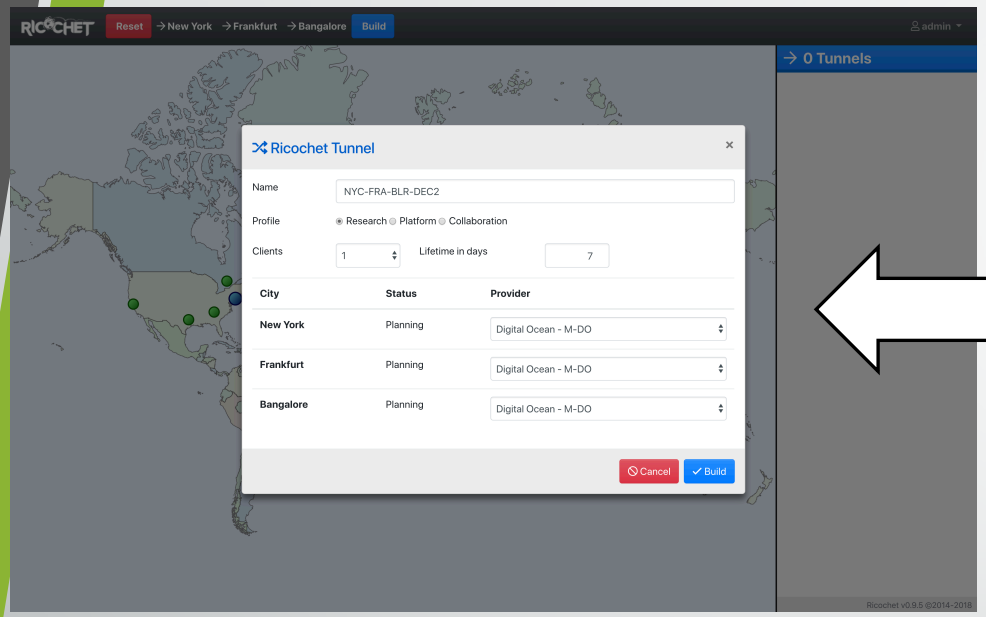

Script Repository

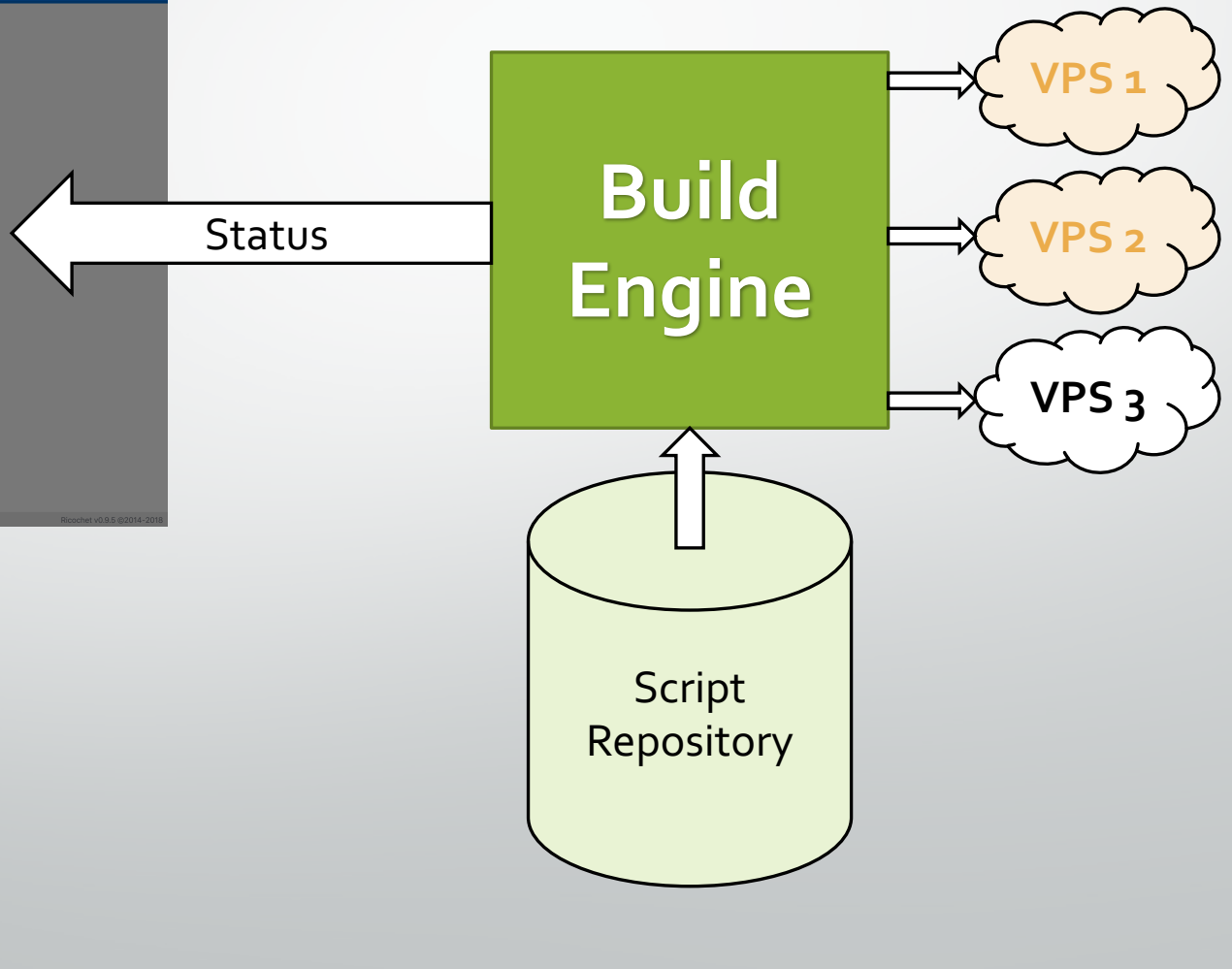

RICOCHET
Reset
New York
Frankfurt
Bangalore
Build
admin
0 Tunnels
Ricochet Tunnel
Name
NYC-FRA-BLR-DEC2
Profile
Research
Platform
Collaboration
Clients
1
Lifetime in days
7
City
Status
Provider
New York
Planning
Digital Ocean - M-DO
Frankfurt
Planning
Digital Ocean - M-DO
Bangalore
Planning
Digital Ocean - M-DO
Cancel
Build
Ricochet v0.9.5 ©2014-2018

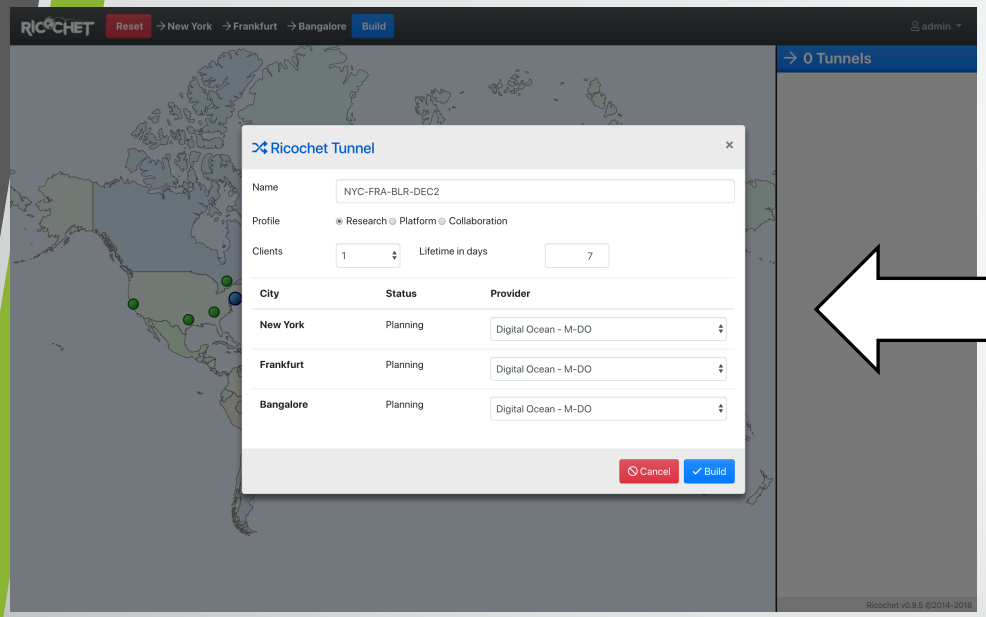

Status
Build Engine
VPS 1
VPS 2
VPS 3
Script Repository

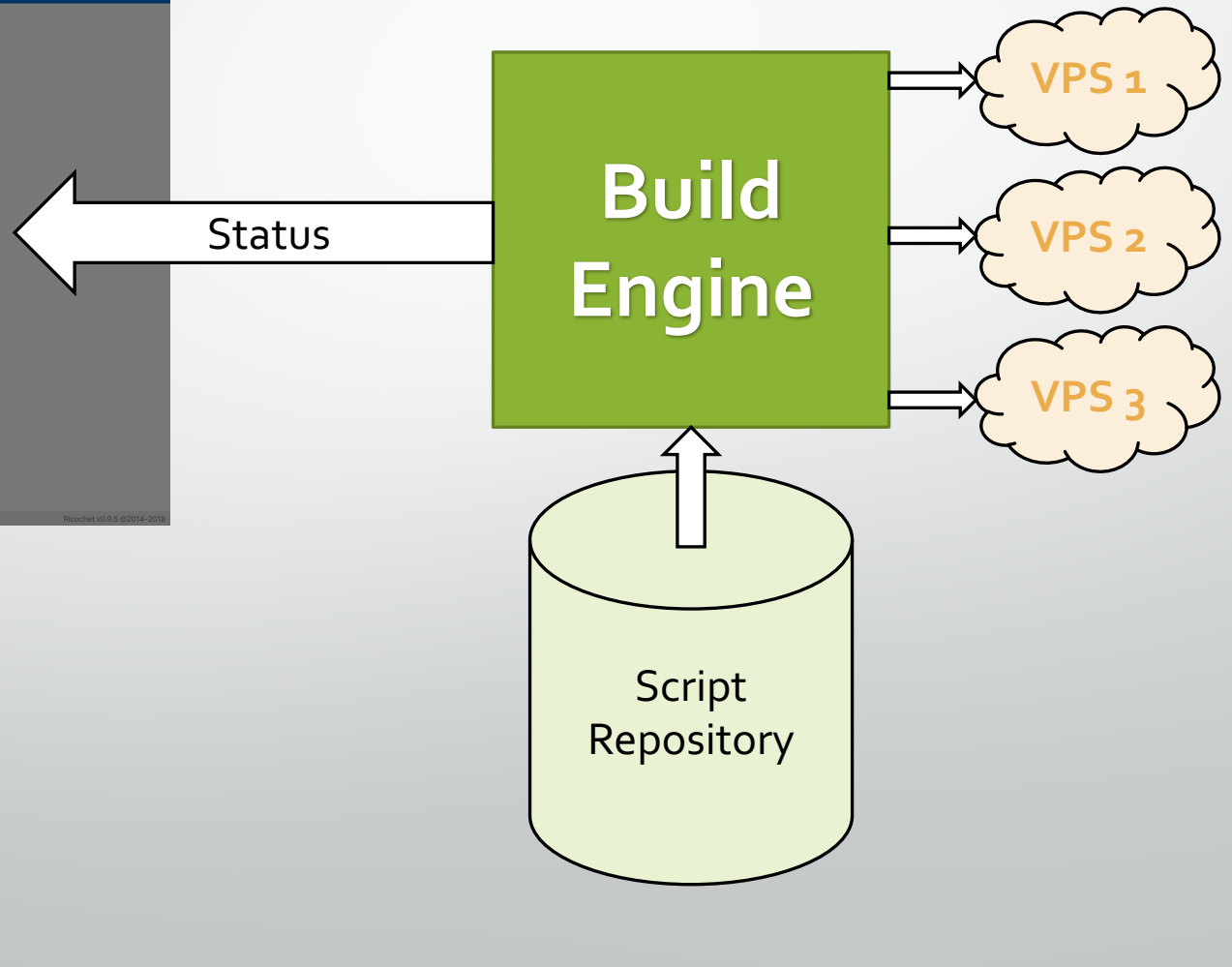

RICOCHET
Reset
New York
Frankfurt
Bangalore
Build
admin
0 Tunnels
Ricochet Tunnel
Name
NYC-FRA-BLR-DEC2
Profile
Research
Platform
Collaboration
Clients
1
Lifetime in days
7
City
Status
Provider
New York
Planning
Digital Ocean - M-DO
Frankfurt
Planning
Digital Ocean - M-DO
Bangalore
Planning
Digital Ocean - M-DO
Cancel
Build
Ricochet v0.9.5 ©2014-2018

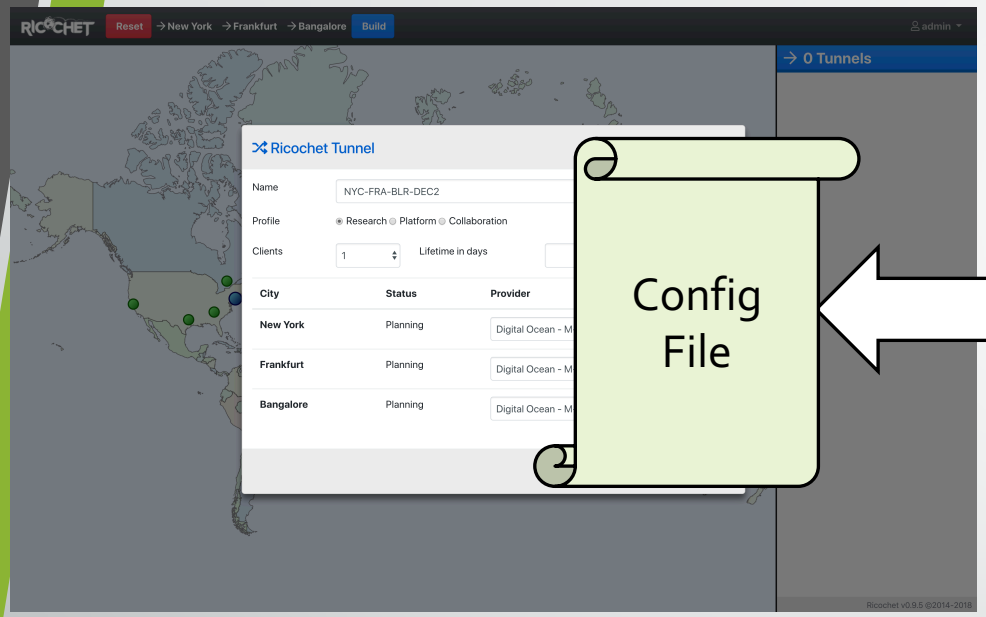

Status
Build Engine
VPS 1
VPS 2
VPS 3
Script Repository


RICOCHET
Reset
New York
Frankfurt
Bangalore
Build
admin
0 Tunnels
Ricochet Tunnel
Name
NYC-FRA-BLR-DEC2
Profile
Research
Platform
Collaboration
Clients
1
Lifetime in days
7
City
Status
Provider
New York
Planning
Digital Ocean - M-DO
Frankfurt
Planning
Digital Ocean - M-DO
Bangalore
Planning
Digital Ocean - M-DO
Cancel
Build
Ricochet v0.9.5 ©2014-2018


Status
Build Engine
VPS 1
VPS 2
VPS 3
Script Repository


RICOCHET
Reset
New York
Frankfurt
Bangalore
Build
admin
0 Tunnels
Ricochet Tunnel
Name
NYC-FRA-BLR-DEC2
Profile
Research
Platform
Collaboration
Clients
1
Lifetime in days
7
City
Status
Provider
New York
Planning
Digital Ocean - M-DO
Frankfurt
Planning
Digital Ocean - M-DO
Bangalore
Planning
Digital Ocean - M-DO
Cancel
Build
Ricochet v0.9.5 ©2014-2018


Status
Build Engine
VPS 1
VPS 2
VPS 3
Script Repository



Config File

Success

Build Engine

VPS 1

VPS 2

VPS 3

Script Repository

DOWNRANGE TECHNOLOGIES

Feature Backlog

1. Additional VPS Provider Support
   - Azure and Google
2. Support for "owned" hardware

   e.g. We support node deployment to on-prem or customer hardware
3. Different Build Techniques
   1. Engine builds X; X builds A, B, C, Server destroys X
   2. Engine Builds A, A Builds B, B Builds C
4. Improve IDS feature-set
5. Integrate more communications services: Real-time Video
6. Expose VPS costing to the user
7. Implement more aggressive active countermeasures

Deployment Strategies

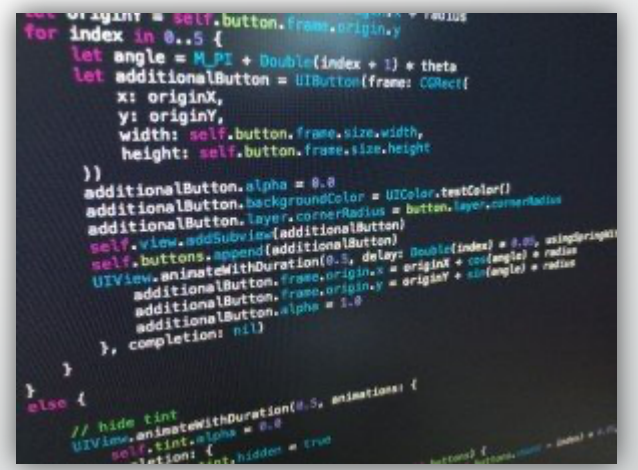
- On Premise: behind your firewall
  - Requires a Linux server
  - Supports Docker
- At customer site: As an virtual or hardware-based appliance
- In the Cloud
  - Adequately locked down
  - Uses nginx to manage TLS connections

DOWNRANGE TECHNOLOGIES

DOWNRANGE TECHNOLOGIES

Demo Artifacts

- Source Code
- User Manual
- Admin Guide



Questions?

Joe Yeglic, joe@downrange.tech