



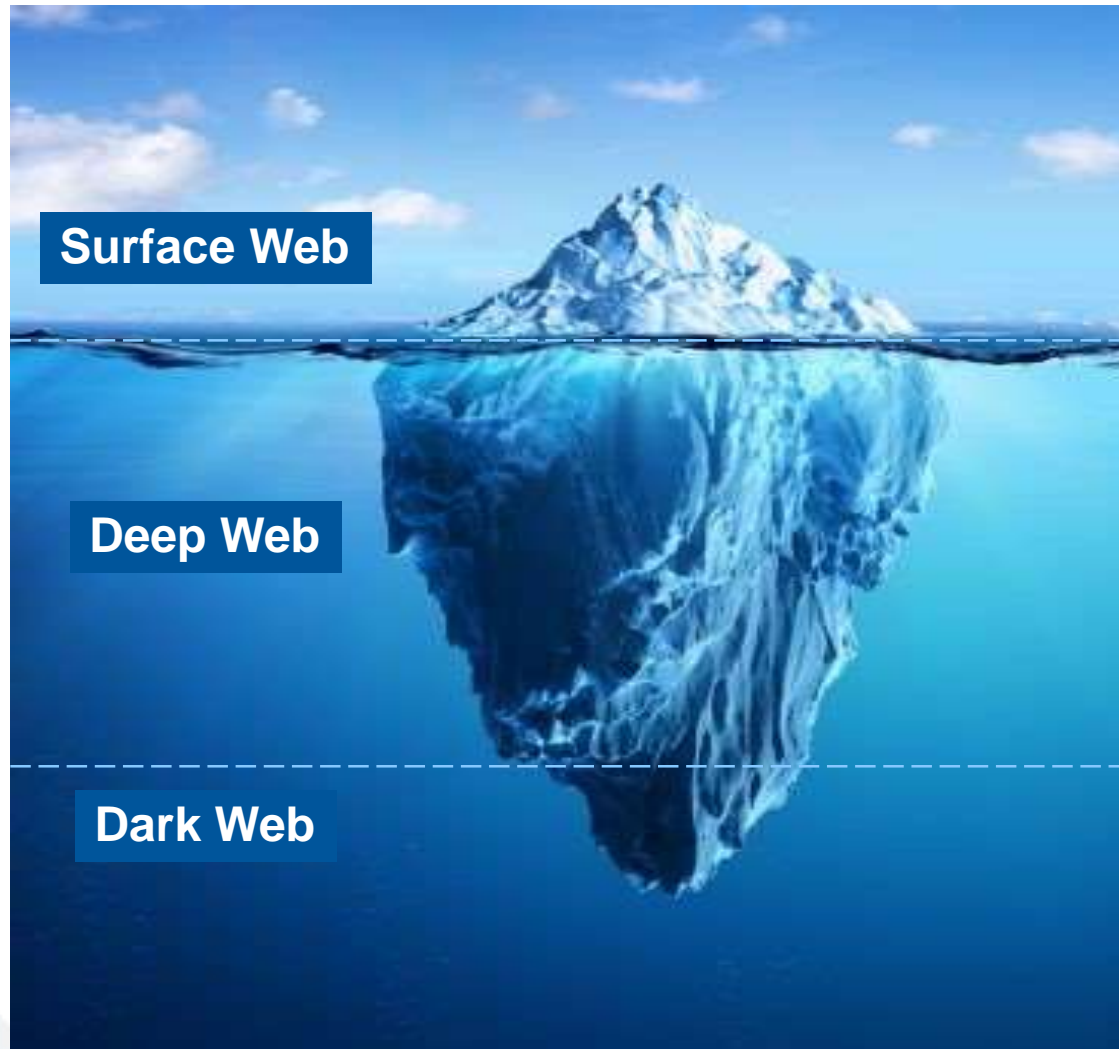
# Illuminating the Dark Web

Simon Bryden  
Consulting Systems Engineer, EMEA

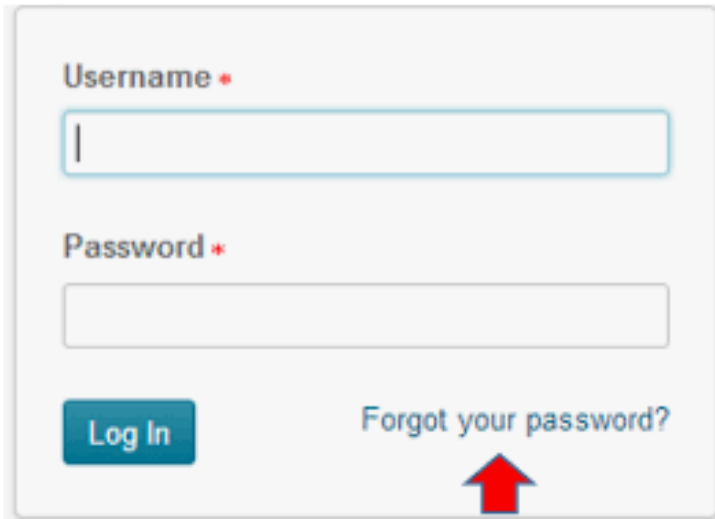
# Illuminating the Dark Web

- ▶ **Introduction to the dark web**
- ▶ **The Onion Router and Hidden Services**
- ▶ **Dark Web Takedowns**
- ▶ **Protecting yourself from the dark web**

# “The iceberg”



# Deep Web characteristics



Username \*

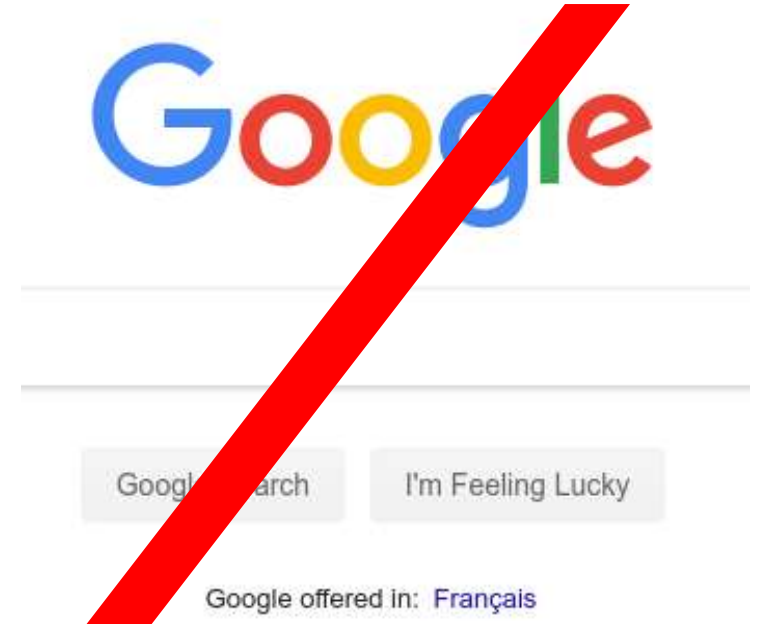
Password \*

[Log In](#) [Forgot your password?](#)

Protected by authentication layer or paywall



Not linked from any other pages

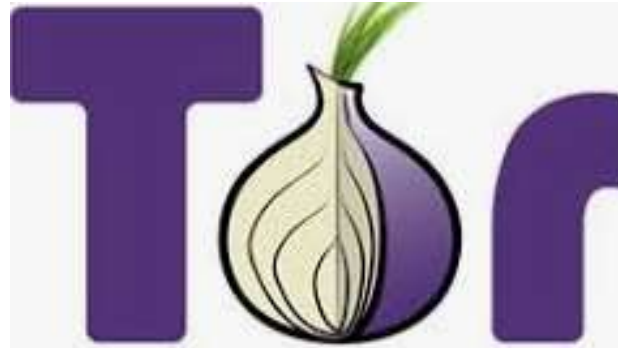


Not referenced by search engines

# Dark Web characteristics



Anonymous



Special access software



Associated with illegal activities

# What can be found on the Dark Web?



Illegal content



Illegal marketplaces



Cybercrime services



Cryptocurrency services



# SLAYERS HITMEN

## SLAYERS ASSASSINATION AND LIFE RUINING SERVICES



*Slayers are a group of hitmen from all over the world. We take jobs from different parts of the world .*

*Our hitmen are always willing to travel to locations where slayers are non existent.*

*We are extremely professional in our dealings and try our best to keep to contractual terms.*

*As well as assassinations we also offer life ruining services like cripplings, acid attacks, setups and many other services listed in our price list.*

*we currently have 48 hitmen on call therefore we would assign you the available and most convenient hitmen according to your location*

*we dont accept unrealistic hits*

*PRICES LISTED BELOW MAY DIFFER SLIGHTLY ACCORDING TO OPERATIONAL LOGISTICS*

### ASSSINATIONS

guns	\$15,000
knife	\$22,000
poison	\$40,000
painless poison	\$42,000
death torture	\$50,000

### LIFE RUINING

acid attack	\$4,000
facial scar	\$3,000
crippling	\$10,000
blindning	\$11,000
castration	\$30,000

### OTHERS

torture	\$20,000
rape	\$2,000
beatings	\$2,000
scare	\$1,000
the price for setup and framings differ according to intentions	



## Facebook 500 Followers - The easy way to get famous

Does your friend has more followers then you? have you ever posted a photo and got a small amount of Likes, while your friend ...

Sold by **optiman** - 0 sold since August 04, 2018

Vendor Level 1

Trust level 1

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

default - 1 day - USD + 0.00

Purchase price: **USD 25.00**

Qty:

 Buy Now

 Buy Now

 Buy Now

Queue

0.006370 BTC / 0.428082 LTC / 0.475647 XMR





## Counterfeit \$20 USD notes-High Quality-Full Escrow! minimum order is 5

To my good customers who know me, Thank you! and I LOVE you! I will never let you down. Look at my feedback people! You ca...

Sold by **swimnotes** - 393 sold since March 03, 2018 **Vendor Level 5** **Trust level 4**

	Features		Features
Product Class	Physical Package	Origin Country	United States
Quantity Left	Unlimited	Ships to	United States
Ends In	Never	Payment	Escrow

	Bulk Discounts	Price	
Bulk Discount	From qty 50 to 99	USD 4.49	0.00114338 BTC
Bulk Discount	From qty 100 to 249	USD 3.99	0.00101605 BTC
Bulk Discount	From qty 250 to 1000	USD 3.84	0.00097785 BTC

FREE 512 days USPS - 12 days - USD + 0.00 / order

Purchase price: **USD 5.39**

Qty:

**Buy Now**

**Queue**

0.001373 BTC

# Legal dark web services



Journalism



Legal markets



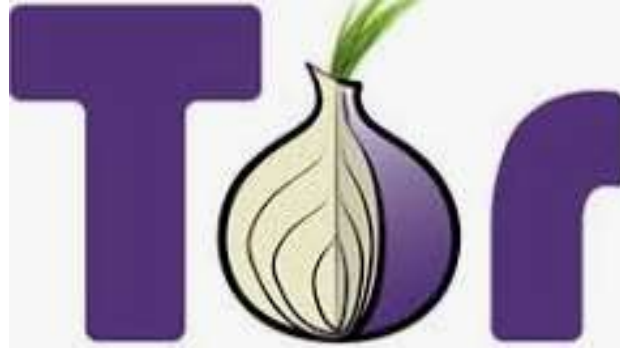
Social Media



Repressed minorities

# The Onion Router

# What is Tor?



- Based on technology developed by the US Naval Research Laboratory in 1990s
- Designed to protect US intelligence communications online
- Tor project launched in 2002, first public release in 2004
- The Tor Project Inc. launched in 2006 as a non-profit organisation

# How much Anonymity does Tor Provide?

Tor can provide two levels of anonymity:

## **Anonymous access to surface web services**

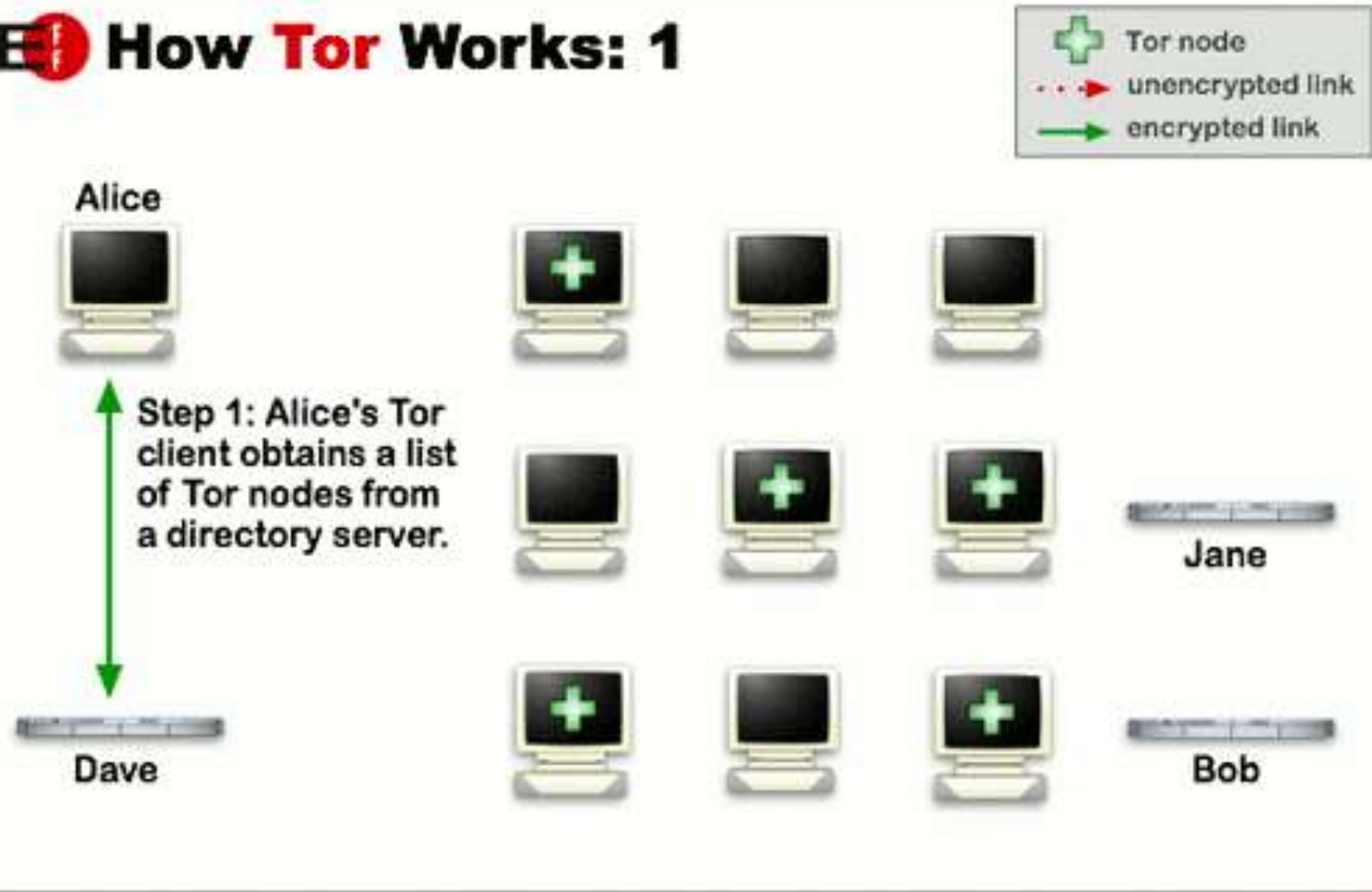
- The Tor network provides an anonymous access through the Tor network.
- The Tor network “exit node” connects to the surface web server

## **Anonymous access to hidden services**

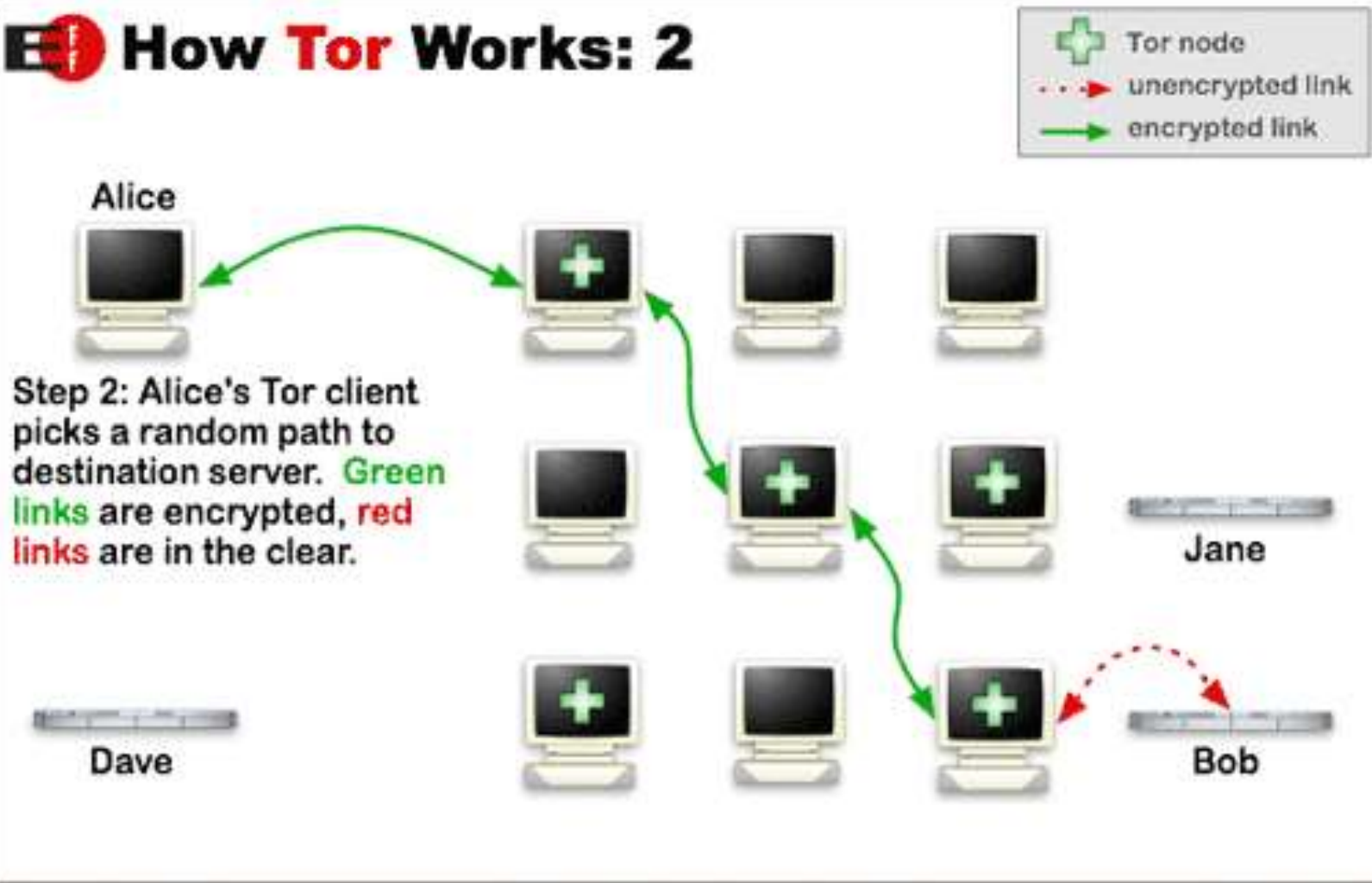
- The Tor network provides complete end-to-end anonymity
- Hides the identity of both client and server



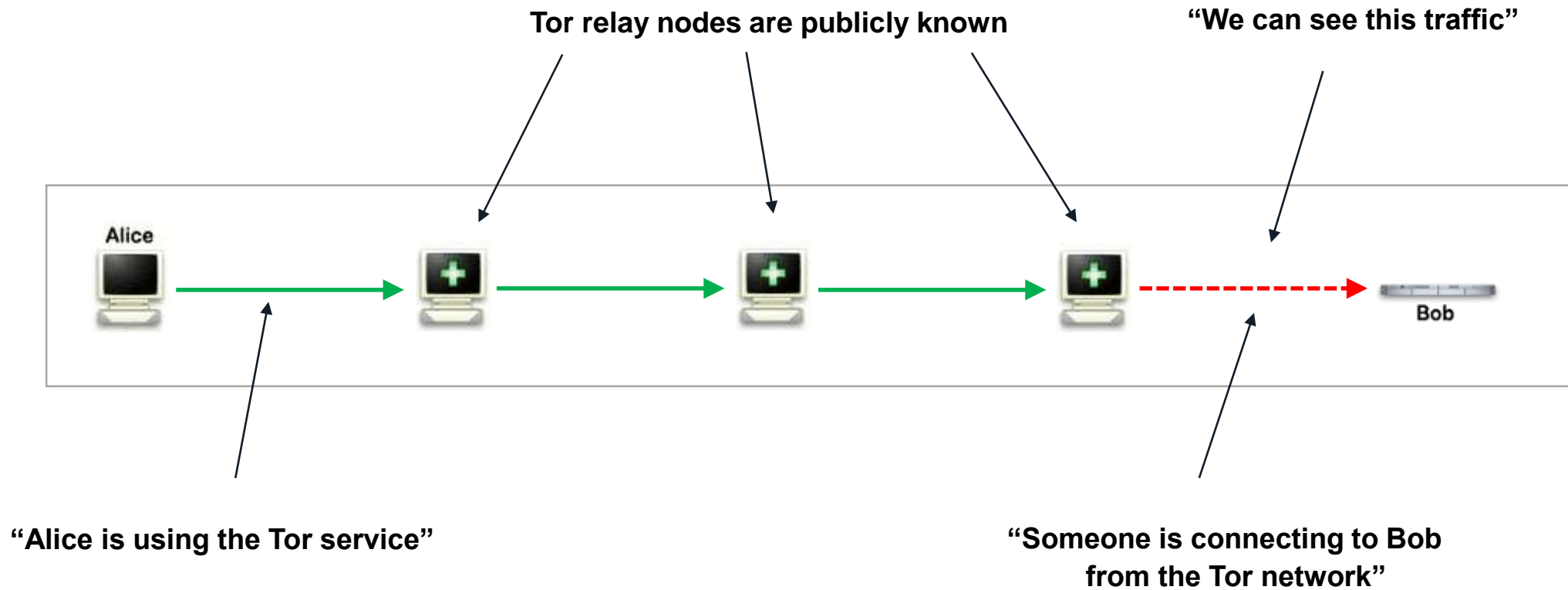
## How Tor Works: 1



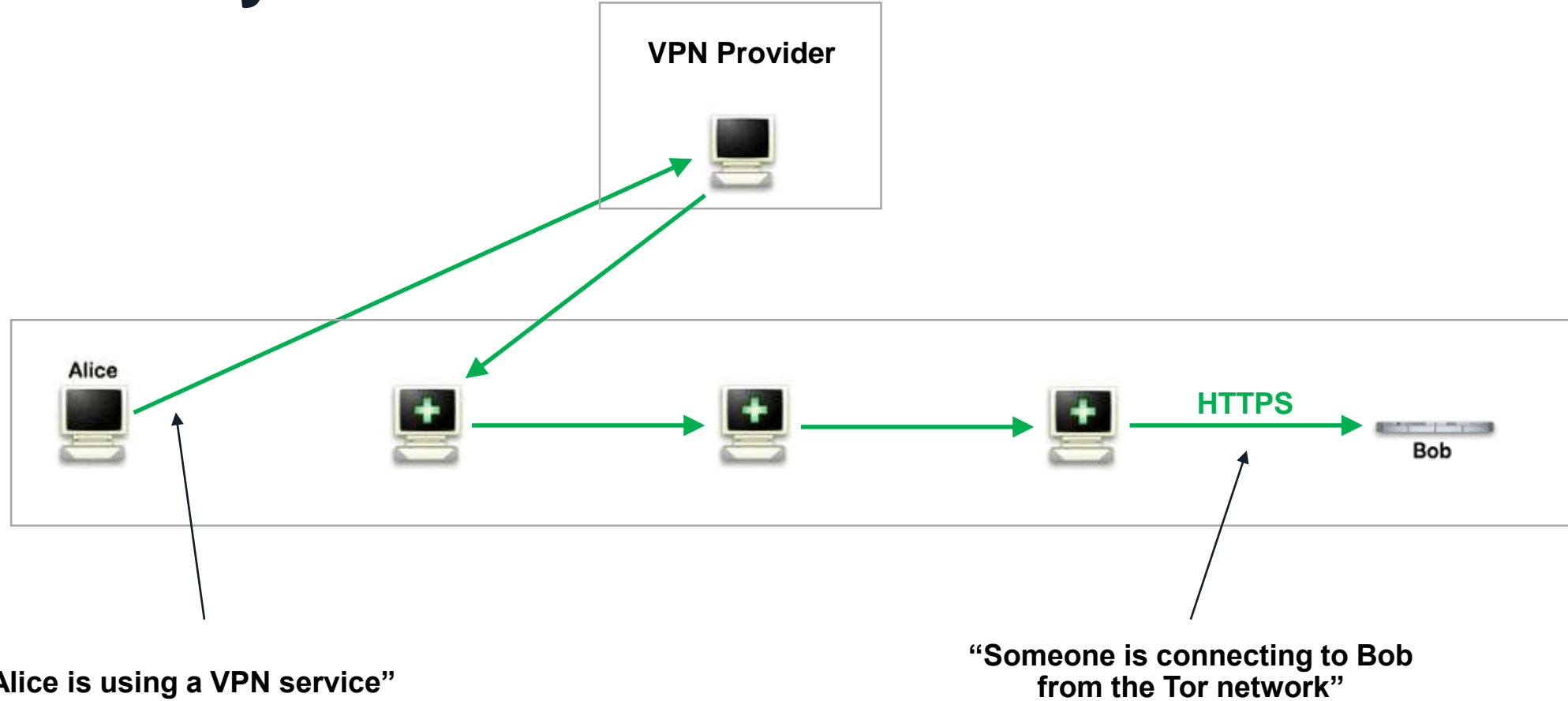
## How Tor Works: 2



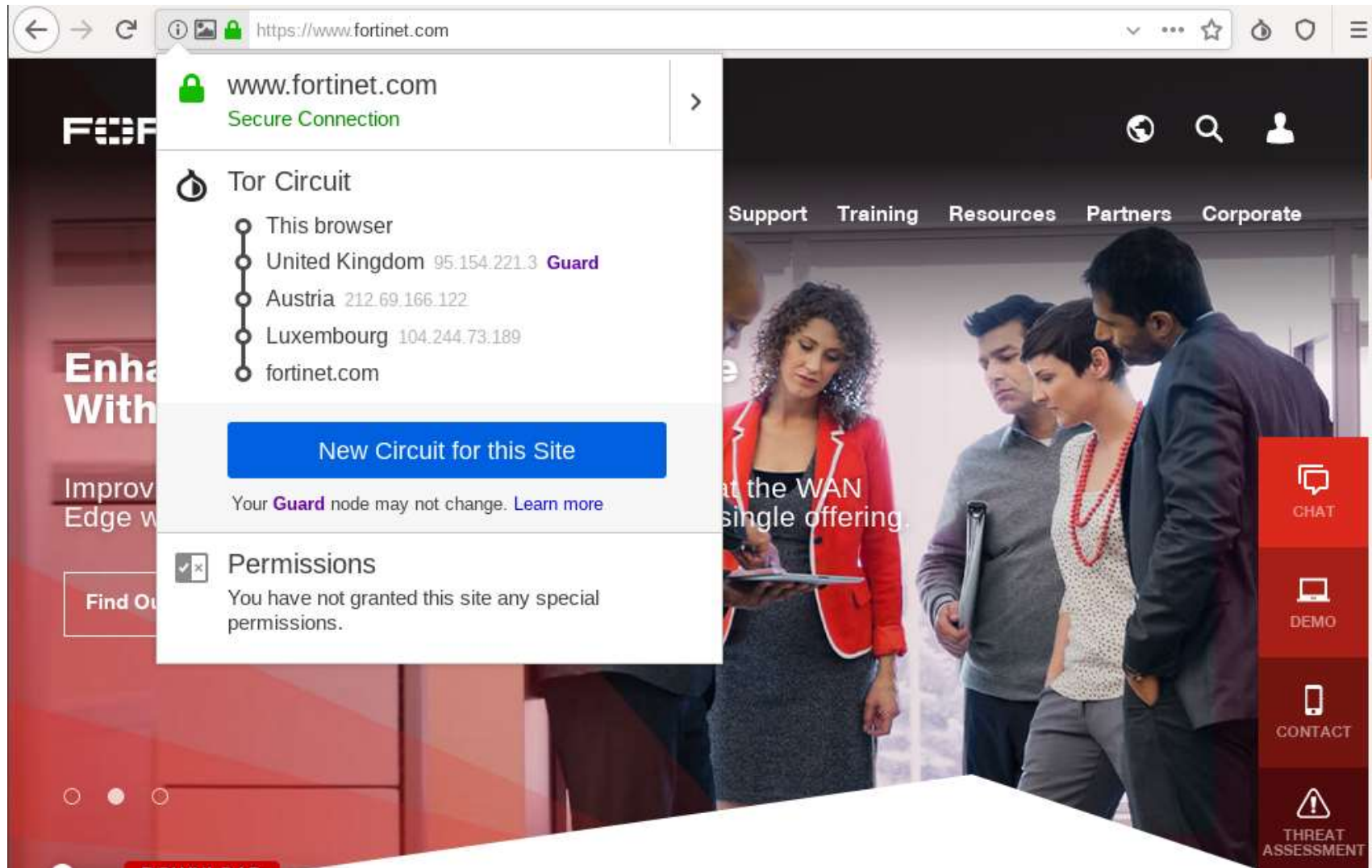
# How Anonymous?



# How Anonymous?



# Tor Browser





# Who Owns the Tor Nodes?

Volunteers.



Often universities and other institutions

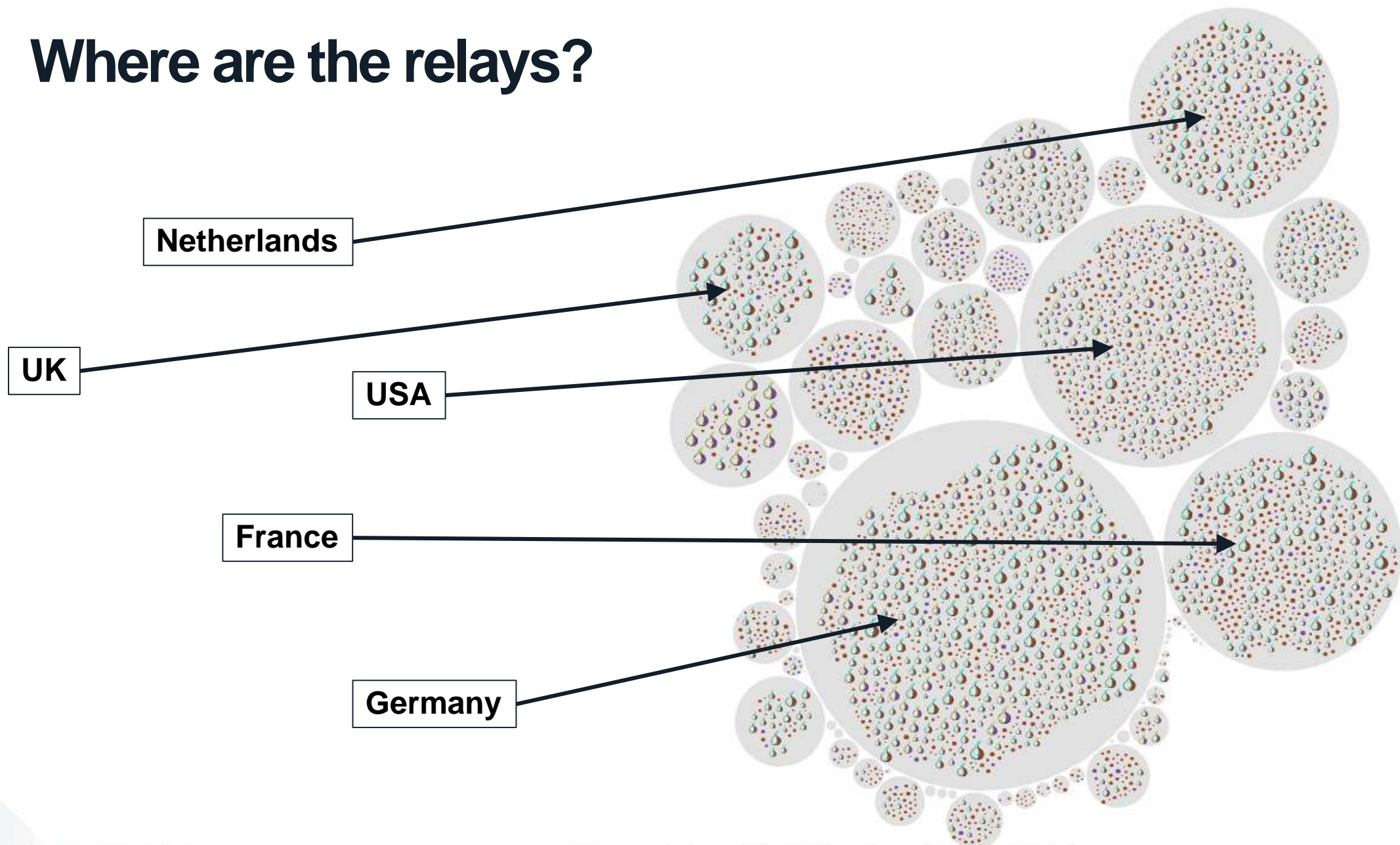
Most people host Relay or Guard (Entry) nodes

Nodes cannot become guards unless they are stable, and have at least 2Mbytes/s bandwidth

Running an Exit node opens up the potential of receiving abuse complaints

Exit nodes are often blocked by providers or website owners

# Where are the relays?

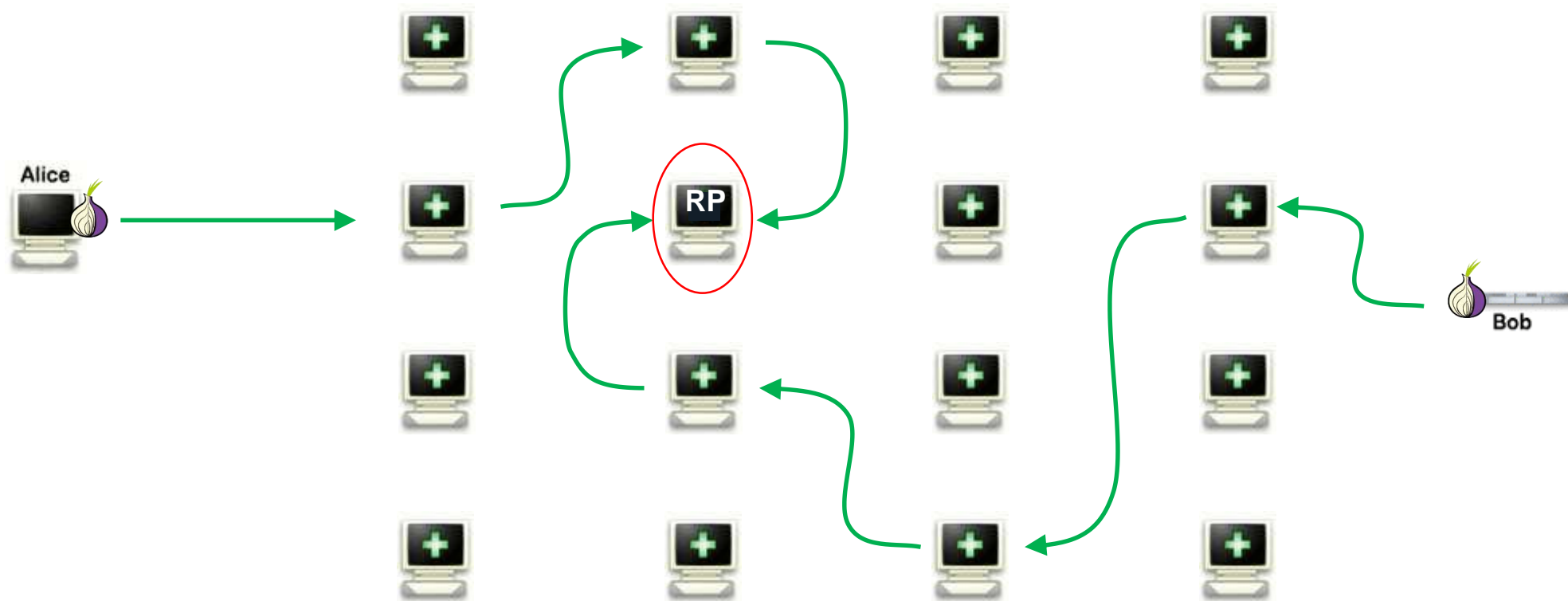


# Tor Hidden Services

# Tor Hidden Services

- Hidden services provide anonymity for the server
- Servers are identified by an onion address such as 4nrvt5xpejyo27zf.onion
- These are not resolved by DNS, rather by the Tor network itself
- Most importantly:
  - There is no link between server name and server address

# Tor Hidden Service Operation





# Browsing Hidden Sites

The screenshot shows a web browser interface. On the left, a Facebook sidebar is partially visible with the text "Connect world a". In the center, a Tor Circuit overlay is displayed, showing a secure connection to Facebook, Inc. and a list of nodes in the circuit: This browser, United Kingdom (95.154.221.3, Guard), Slovakia (212.89.225.242), Germany (217.79.184.72), and three Relay nodes, ending at facebookcorewwi.onion. Below the circuit list is a blue button "New Circuit for this Site" and a note: "Your Guard node may not change. Learn more". At the bottom of the overlay is a "Permissions" section with a checkmark icon and the text: "You have not granted this site any special permissions." On the right, the Facebook sign-up page is visible, featuring a blue header with "Email or Phone" and "Password" input fields, a "Log In" button, and a "Forgot account?" link. The main content area is titled "Sign Up" with the text "It's quick and easy." Below this are input fields for "First name", "Last name", "Mobile number or email", and "New password". There is also a "Birthday" section with dropdowns for month (Aug), day (28), and year (1994), and a "Gender" section with radio buttons for "Female", "Male", and "Custom". At the bottom of the sign-up form is a green "Sign Up" button. A small disclaimer at the bottom of the sign-up form states: "By clicking Sign Up, you agree to our Terms, Data Policy and Cookies Policy. You may receive SMS Notifications from us and can opt out any time."

# **Dark Web Take-Down**

# Perfect anonymity is **Difficult**

- It's more than just Tor!
- Payment methods
- Delivery of goods
- All other system tools and applications must be anonymized
- Ancillary communications (forgotten passwords, tech support)
- Web services platforms (Wordpress, Joomla etc. are full of vulnerabilities)

# Freedom Hosting

In 2013, the FBI managed to infiltrate “Freedom Hosting”, a hosting operation serving child pornography sites

It inserted an exploit kit which targeted a vulnerability in Firefox 17 (used in Tor browser)

This resulted in the download of a file which would report back the identity of the user

Resulted in the arrests of the owner, and many of the consumers



## Silk Road

The Silk Road marketplace was reportedly identified through a non-anonymized captcha

# Welcome To Video

Child sex abuse marketplace

More than 8 terabytes of data

Used bitcoin – 7,300 recorded transactions from more than 1 million user addresses

UK National Crime Agency used BitCoin transaction analysis to identify users

Arrests of 337 users made in 38 countries

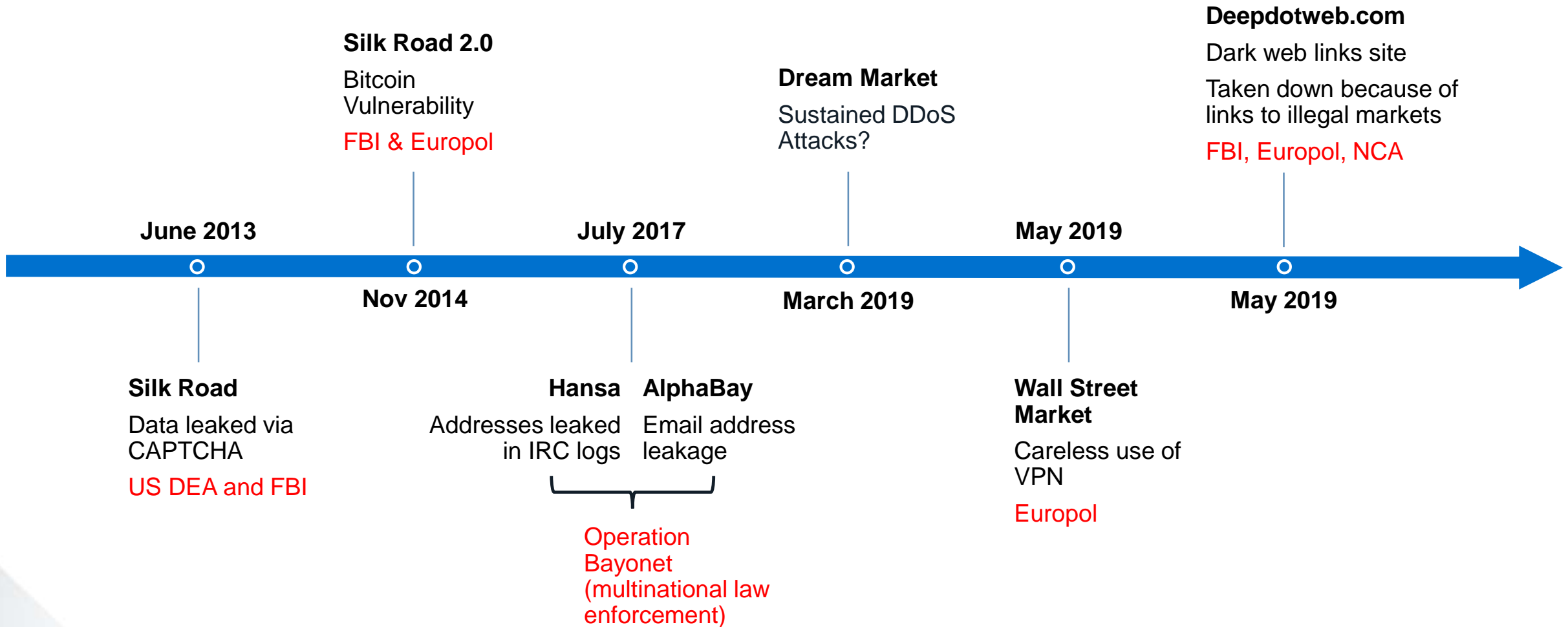
23 abused children identified and rescued

Abusers found, not by using offensive hacking, but by simply tracing bitcoin transactions



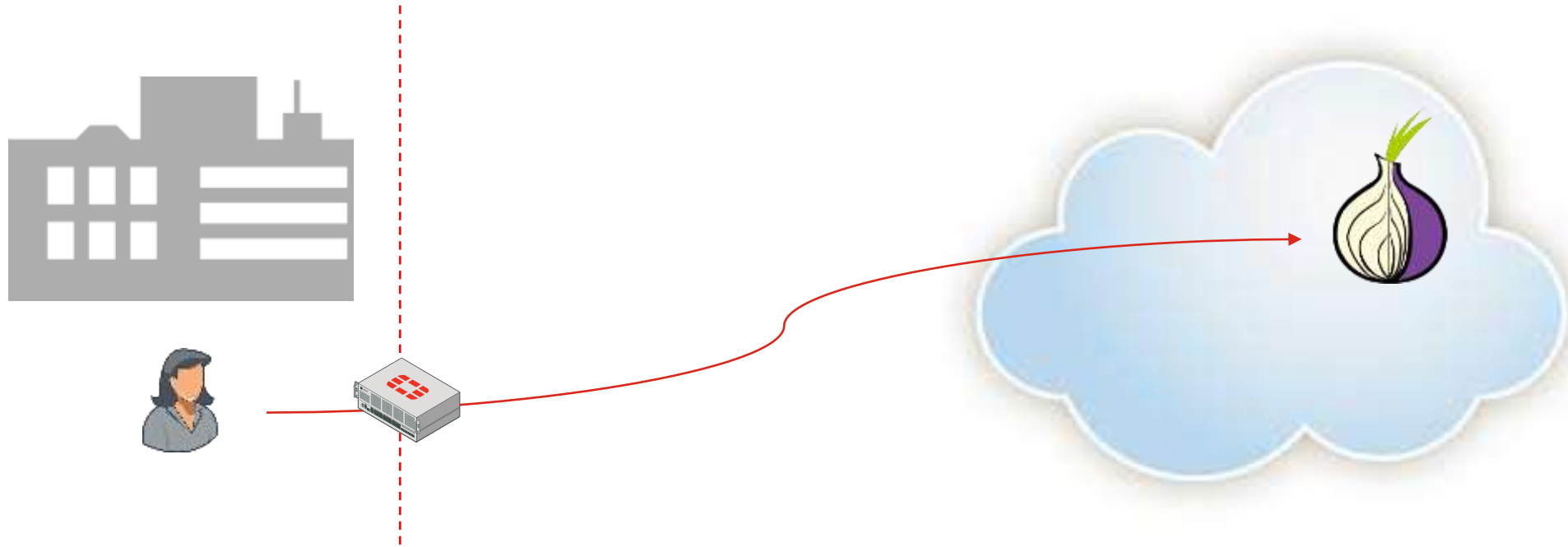


# Dark Web Markets

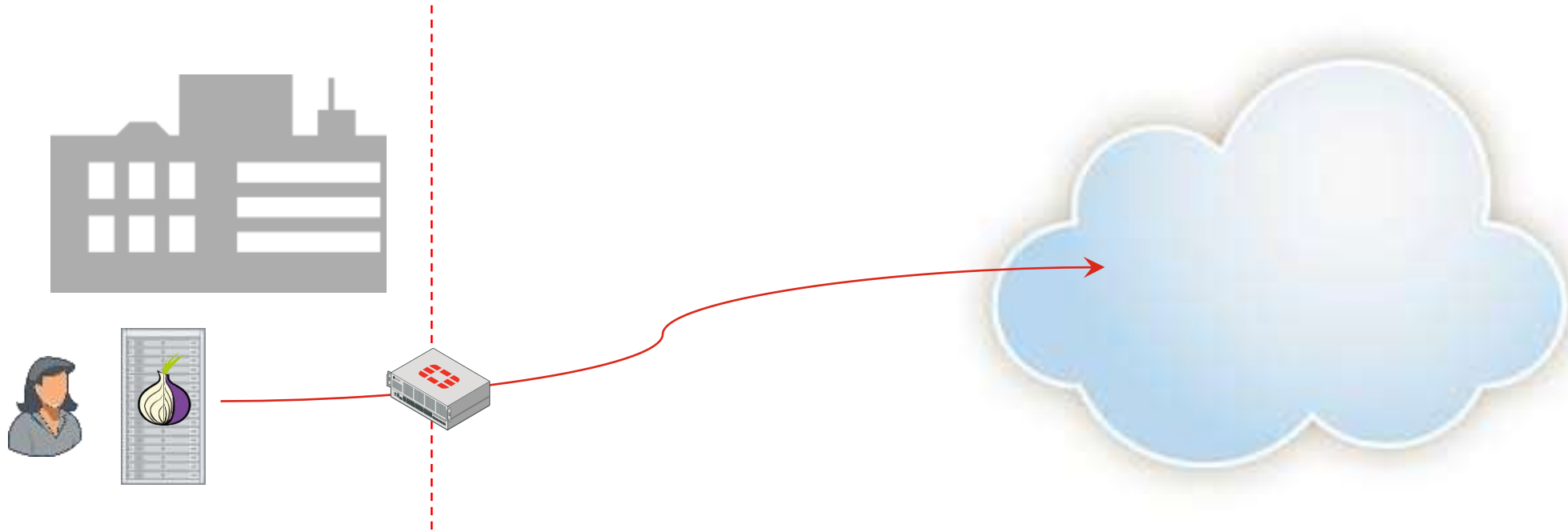


# **Detection and Protection**

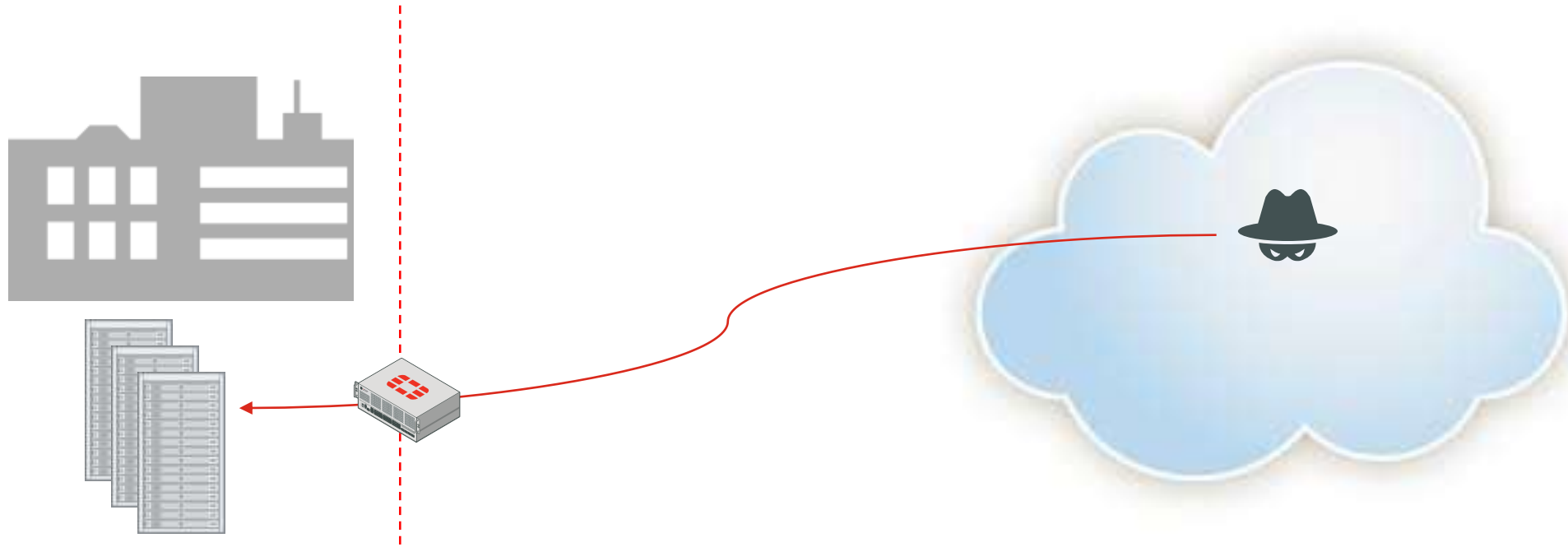
# Case 1: Employees access dark web sites



## Case 2: Employees hosting dark web sites



# Case 3: Anonymous external reconnaissance



# Tor Detection by Relay Addresses

Several sites provide the list in convenient form:

<https://check.torproject.org/exit-addresses> (exit nodes only)

<https://www.dan.me.uk/tornodes> (exit only, or all relays)

<http://blutmagie.de> (exit only, or all relays)

Security vendors often have automatically-updated node lists built in to their solutions.



# Detection by Protocol

Good news: It is possible to detect the Tor protocol

Not so good news: Tor provides explicit means to avoid being detected

Fortinet has built-in application detection of Tor, I2P, FreeNet, and others, as well as popular proxy applications such as Psiphon and Ultrasurf.

Tor does makes it possible to use *private relay nodes* and *personalized transport protocols* which can make detection close to impossible.

However, in practice, there are many associated difficulties with these techniques.

# Key Takeaways

- Dark web is more about the technology than the content
- Much of the content is legal and legitimate
- Tor is by far the most popular access technology
- It is very difficult to make a site 100% anonymous
- The dark web can present a risk to legitimate users and companies
- Simple security measures can deter all but the most determined attackers



**Come and see us at stand 14**