



Creating a Tor Service

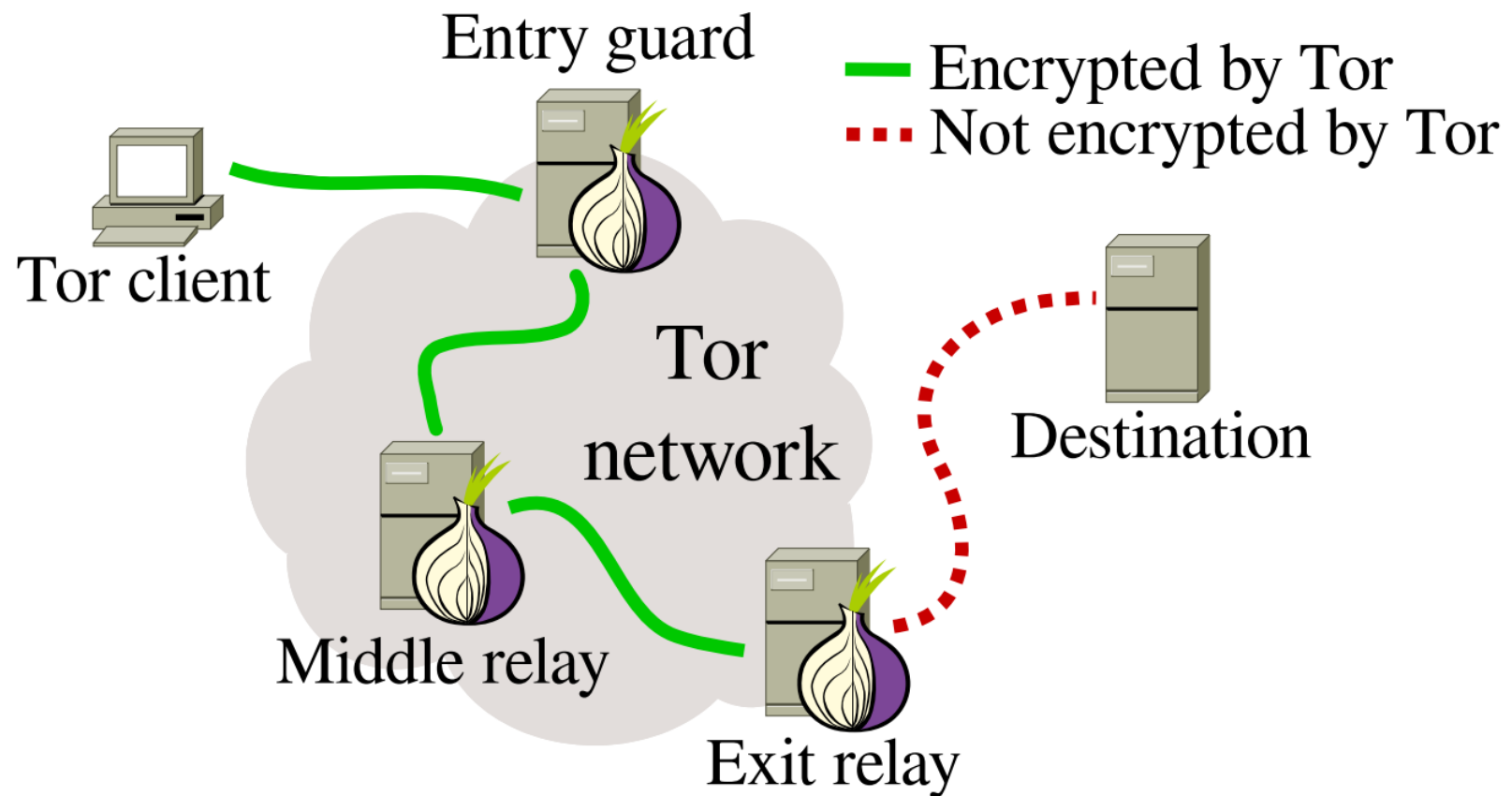
Rubén Calvo Villazán



Index

- How does Tor work between servers?
- How having a hidden service works?
- Installation
- Making our site secure

Choosing the path



Creating a hidden service

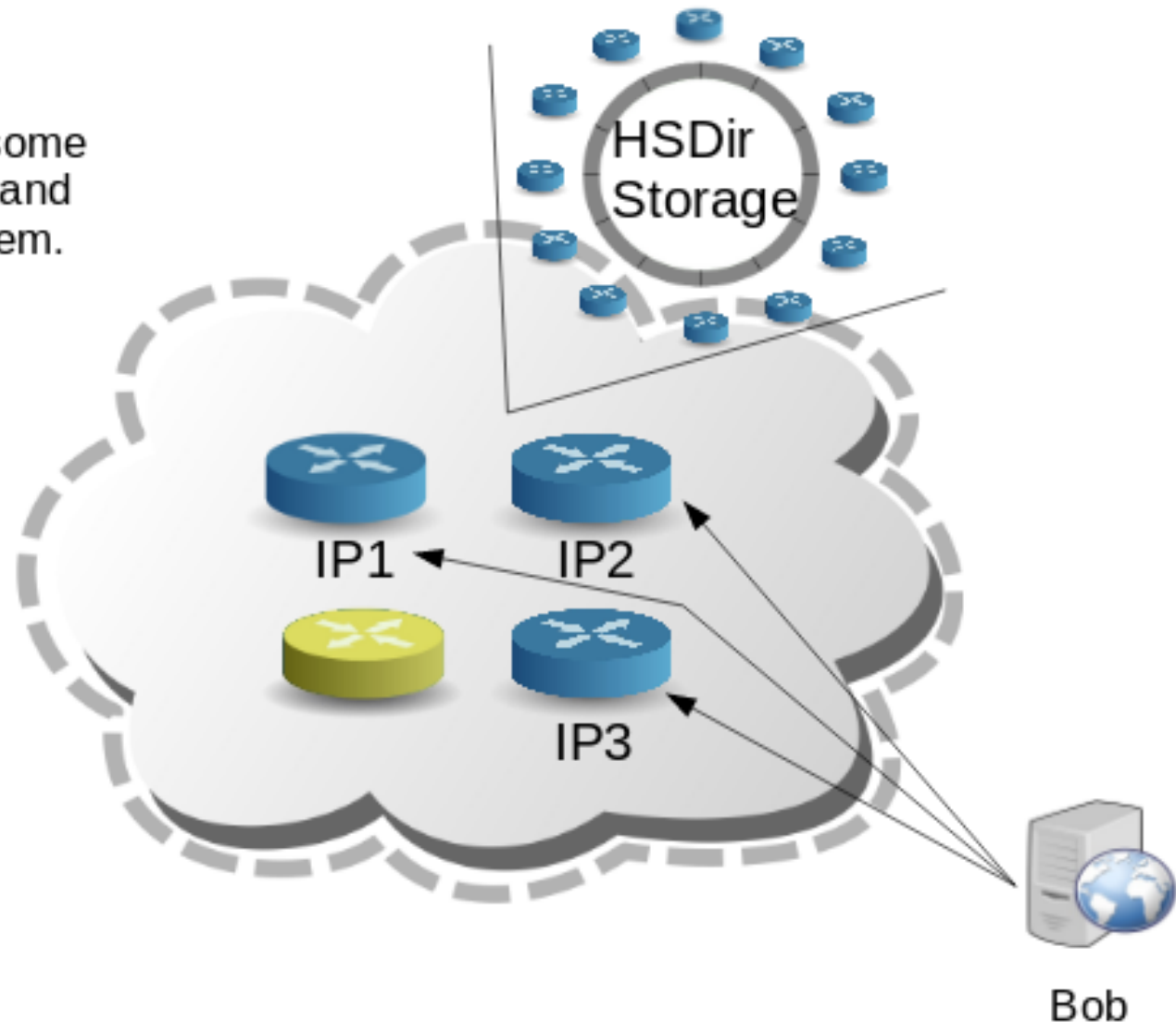


Creating a hidden service

Step1: Bob picks some introduction points and builds circuits to them.



Alice

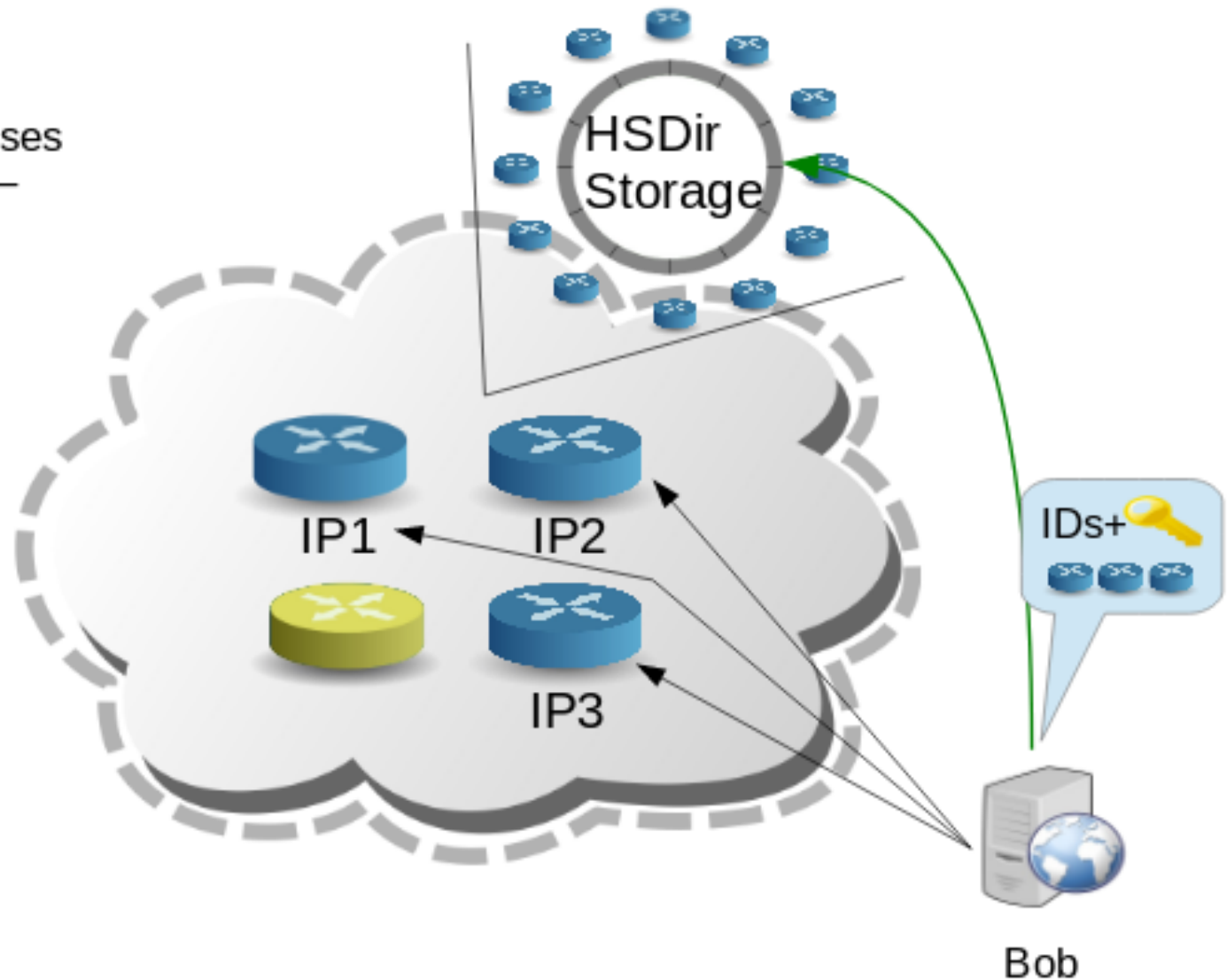


Creating a hidden service

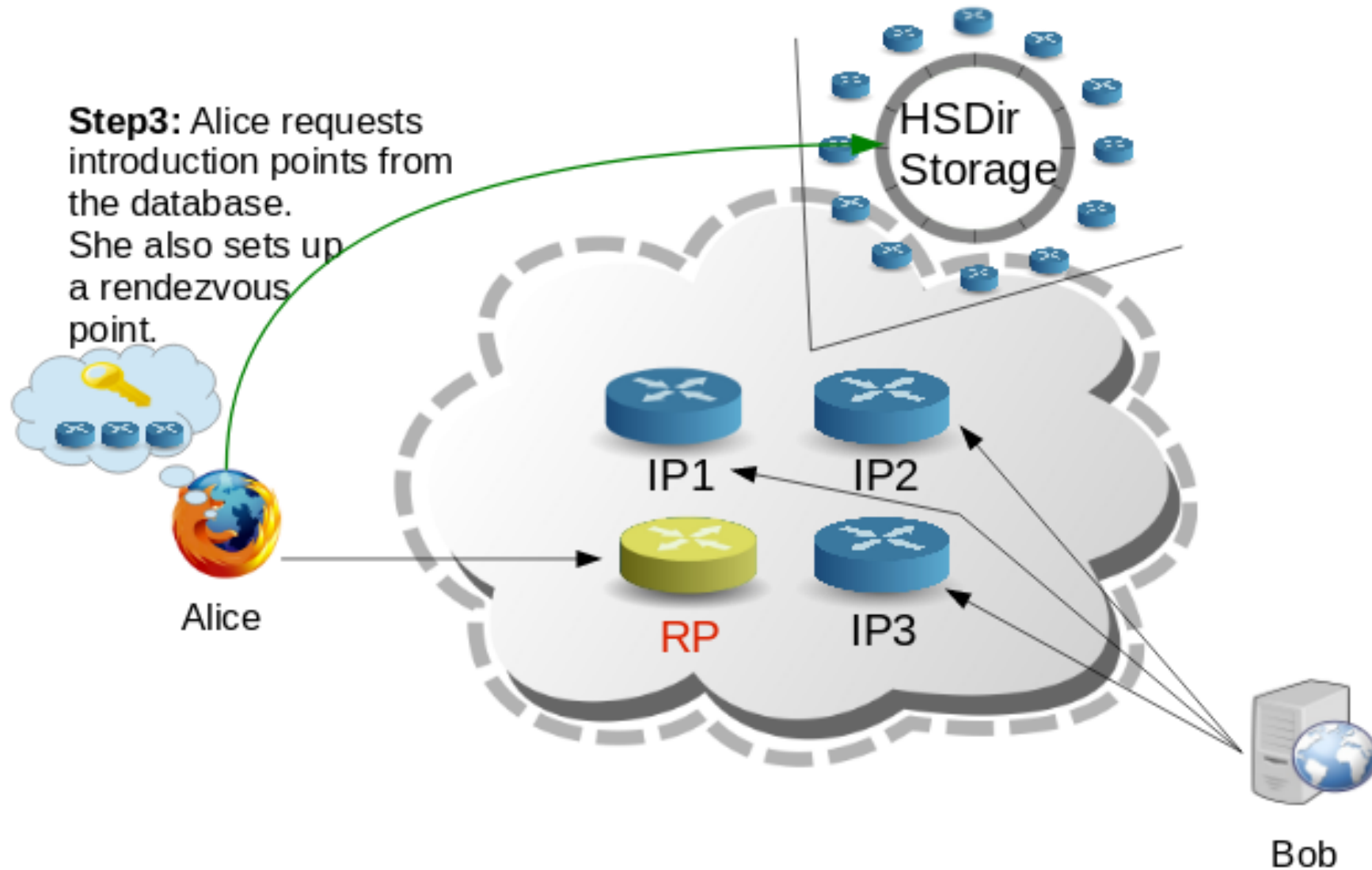
Step2: Bob advertises his hidden service – `<z>.onion` – at the database.



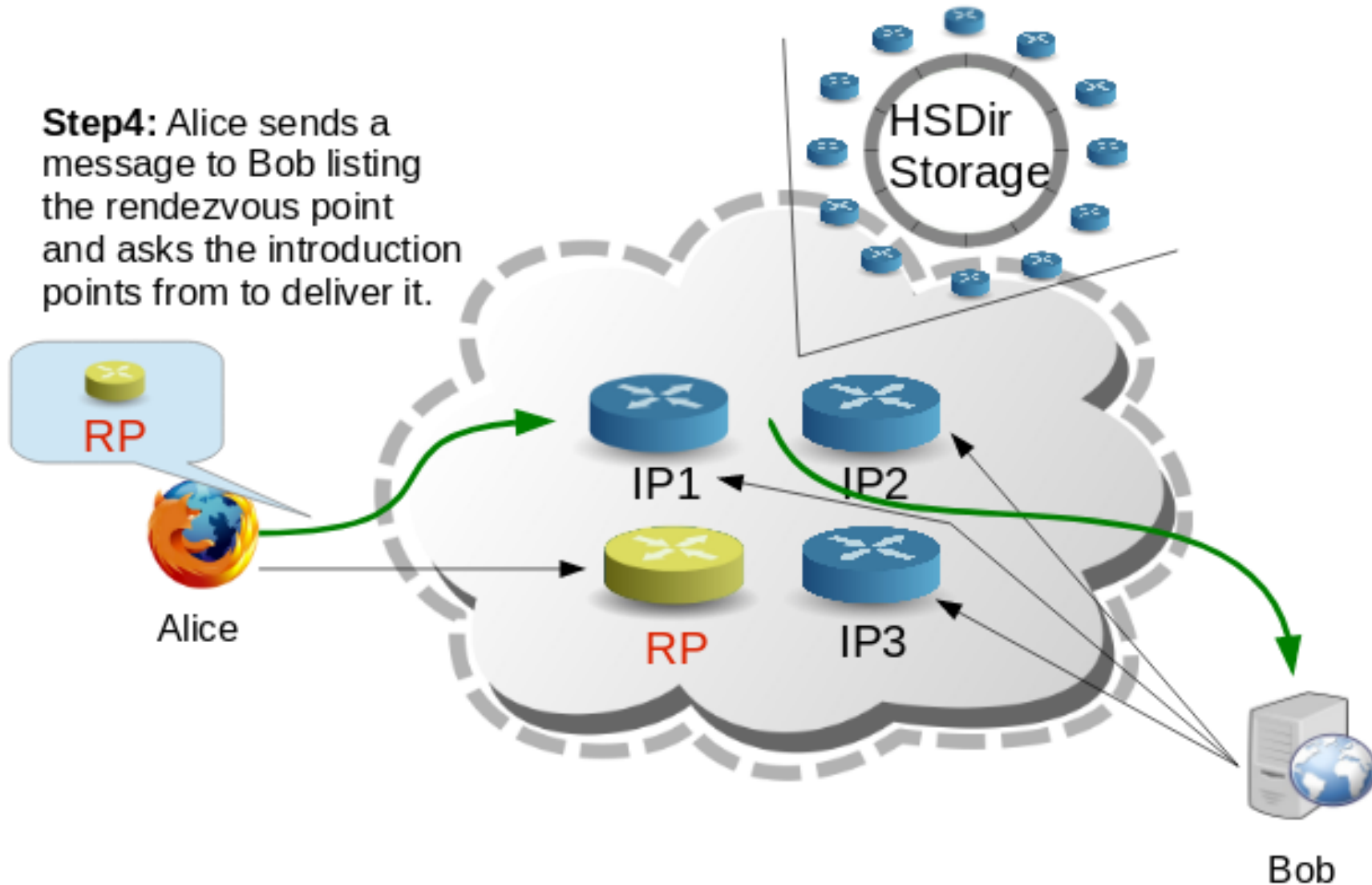
Alice



Creating a hidden service

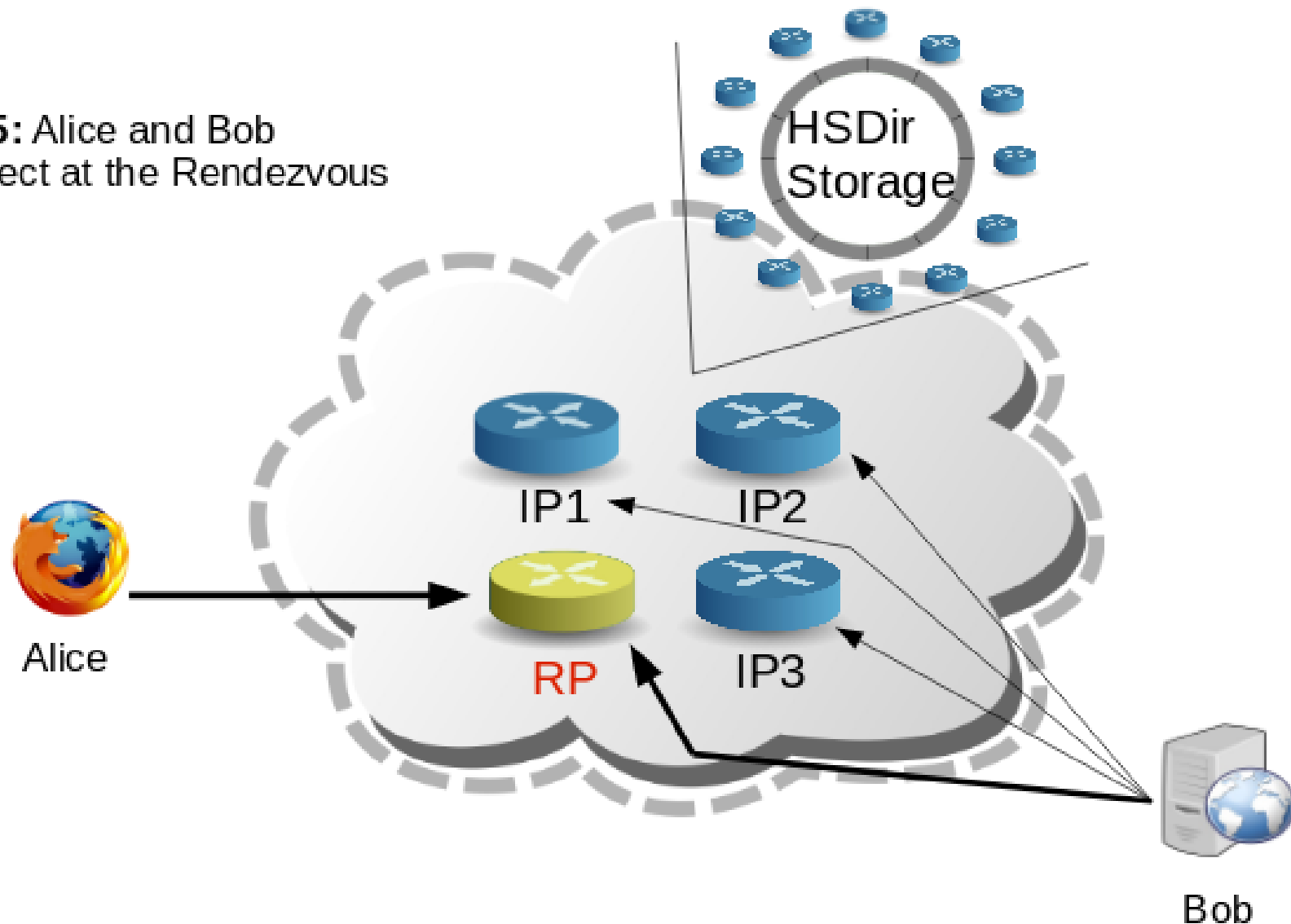


Creating a hidden service



Creating a hidden service

Step5: Alice and Bob
Connect at the Rendezvous
point



Installation



Installation - Nginx

1. Install Nginx

```
root@valkyrie:~# apt-get install nginx
```

2. Current configuration backup

```
root@valkyrie:~# cp /etc/nginx/sites-available/default  
/etc/nginx/sites-available/default.old
```

3. New configuration from scratch

```
root@valkyrie:~# rm /etc/nginx/sites-available/default  
root@valkyrie:~# vim /etc/nginx/sites-available/default
```

Installation - Nginx

```
server {  
    listen 127.0.0.1:8080 default_server;  
    server_name localhost;  
    root /usr/share/nginx/html;  
    index index.html;  
    location / {  
        allow 127.0.0.1;  
        deny all;  
    }  
}
```

Installation - Tor

```
root@valkyrie:~# lsb_release -a
No LSB modules are available.
Distributor ID: Kali
Description:    Kali GNU/Linux Rolling
Release:       kali-rolling
Codename:      kali-rolling
```

I run Debian stable (stretch) ▾ and want Tor ▾ version

stable ▾

Installation - Tor

1. Install from apt

```
root@valkyrie:~# vim /etc/apt/sources.list
```

```
deb https://deb.torproject.org/torproject.org stretch main  
deb-src https://deb.torproject.org/torproject.org stretch main
```

Installation - Tor

2. Exchange keys

```
root@valkyrie:~# gpg --keyserver keys.gnupg.net --recv A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89
gpg: keybox '/root/.gnupg/pubring.kbx' created
gpg: key EE8CBC9E886DDD89: 1 duplicate signature removed
gpg: key EE8CBC9E886DDD89: 78 signatures not checked due to missing keys
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key EE8CBC9E886DDD89: public key "deb.torproject.org archive signing key" imported
gpg: no ultimately trusted keys found
gpg: Total number processed: 1
gpg:             imported: 1
root@valkyrie:~# gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo apt-key add -
OK
```

Installation - Tor

3. Install (obviously)

```
root@valkyrie:~# apt install tor deb.torproject.org-keyring
```

4. Also install the .tar

Installation - Tor

```
root@valkyrie:~# vim /etc/tor/torrc
```

```
##### This section is just for location-hidden services ###  
  
## Once you have configured a hidden service, you can look at the  
## contents of the file ".../hidden_service/hostname" for the address  
## to tell people.  
##  
## HiddenServicePort x y:z says to redirect requests on port x to the  
## address y:z.  
  
HiddenServiceDir /var/lib/tor/hidden_service/  
HiddenServicePort 80 127.0.0.1:8080  
  
#HiddenServiceDir /var/lib/tor/other_hidden_service/  
#HiddenServicePort 80 127.0.0.1:80  
#HiddenServicePort 22 127.0.0.1:22
```

5. Restart

```
root@valkyrie:~# service nginx restart
```

```
root@valkyrie:~# service tor restart
```

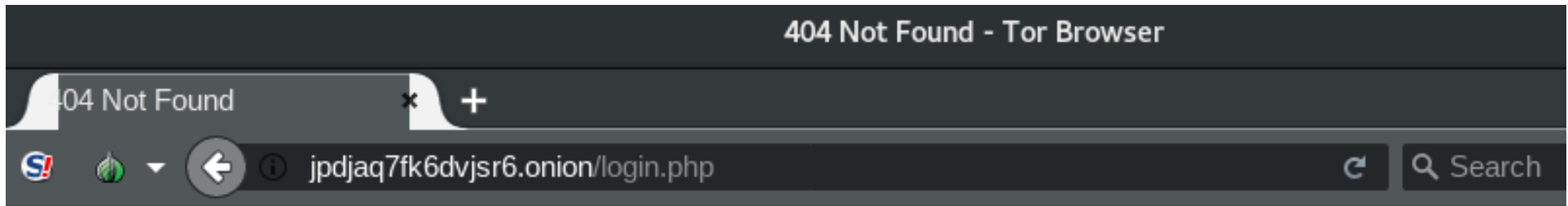
6. Surprise

```
root@valkyrie:~# vim /var/lib/tor/hidden_service/  
hostname      private_key  
root@valkyrie:~# cat /var/lib/tor/hidden_service/hostname  
jpdjaq7fk6dvjsr6.onion
```

Making our site secure



Making our site secure



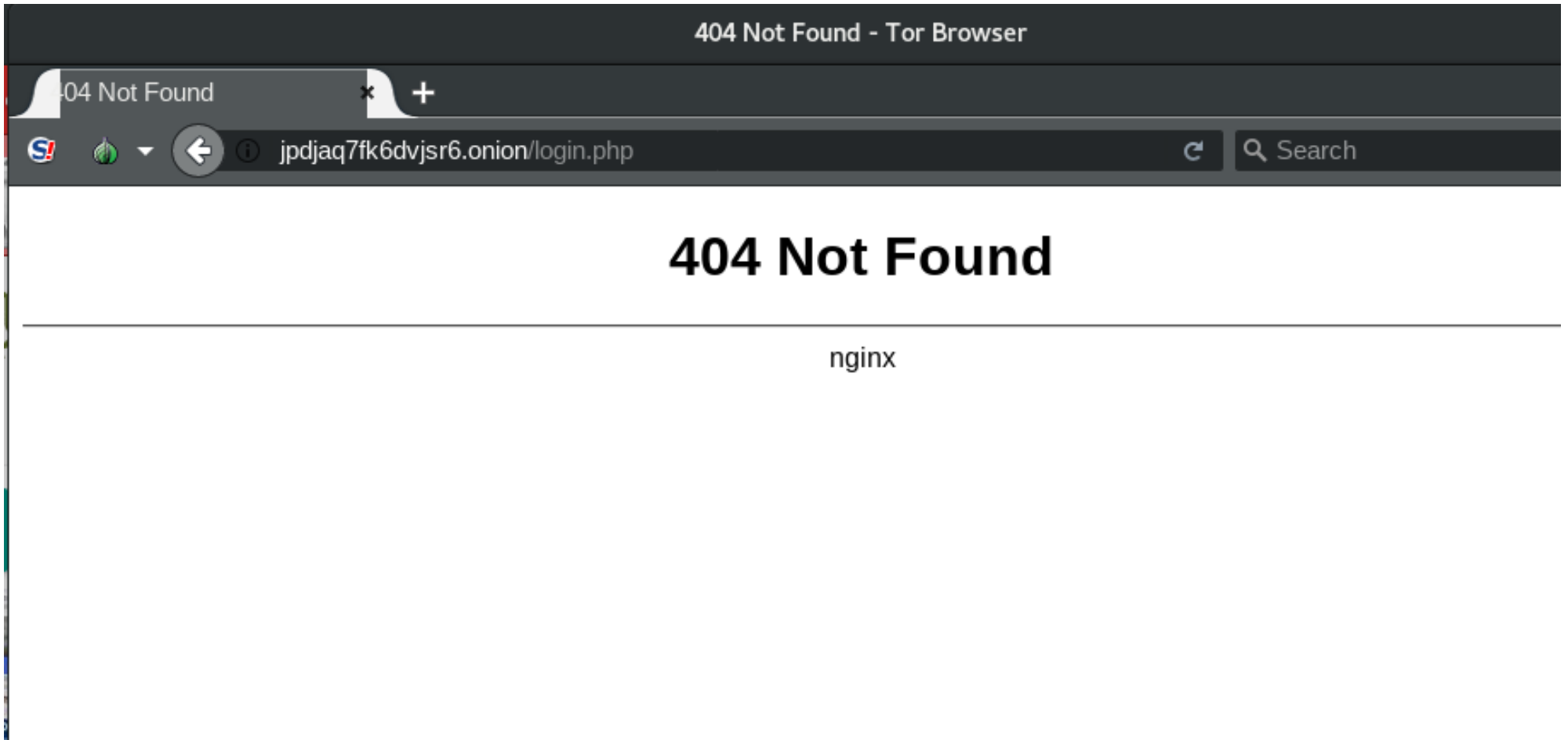
404 Not Found

nginx/1.13.12

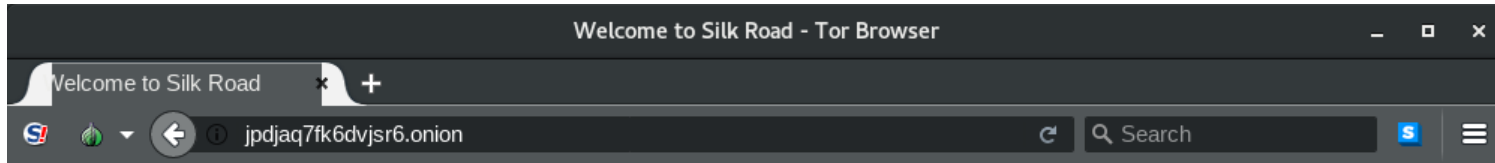
Making our site secure

```
server {  
    listen 127.0.0.1:8080 default_server;  
    server_name localhost;  
    root /usr/share/nginx/html;  
    index index.html index.html;  
    server_tokens off;  
    location / {  
        allow 127.0.0.1;  
        deny all;  
    }  
}
```

Making our site secure



Making our site secure



Welcome to Silk Road



Anonymous Market Place

Making our site secure


1. Create new password

```
root@valkyrie:~# perl -le 'print crypt("admin1", "1xzcq")'  
1xlpf6ZgGiVU
```

```
root@valkyrie:~# cat .htpasswd  
admin1:1xlpf6ZgGiVU
```


Making our site secure

Authentication Required



http://jpdjaq7fk6dvjsr6.onion is requesting your username and password. The site says:
"Administrator Login"

User Name:

Password:

Cancel

OK

Making our site secure

```
root@valkyrie:~# cat /etc/nginx/sites-enabled/default

server {
    listen 127.0.0.1:8080 default_server;
    server_name localhost;
    root /usr/share/nginx/html;
    access_log /var/log/nginx/localhost.access.log;
    error_log /var/log/nginx/localhost.error.log;
    index index.html index.html;
    server_tokens off;
    auth_basic "Administrator Login";
    auth_basic_user_file /root/.htpasswd;
    location / {
        allow 127.0.0.1;
        deny all;
    }
}
```

Welcome to Silk Road



End



THIS HIDDEN SITE HAS BEEN SEIZED

**by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York**

