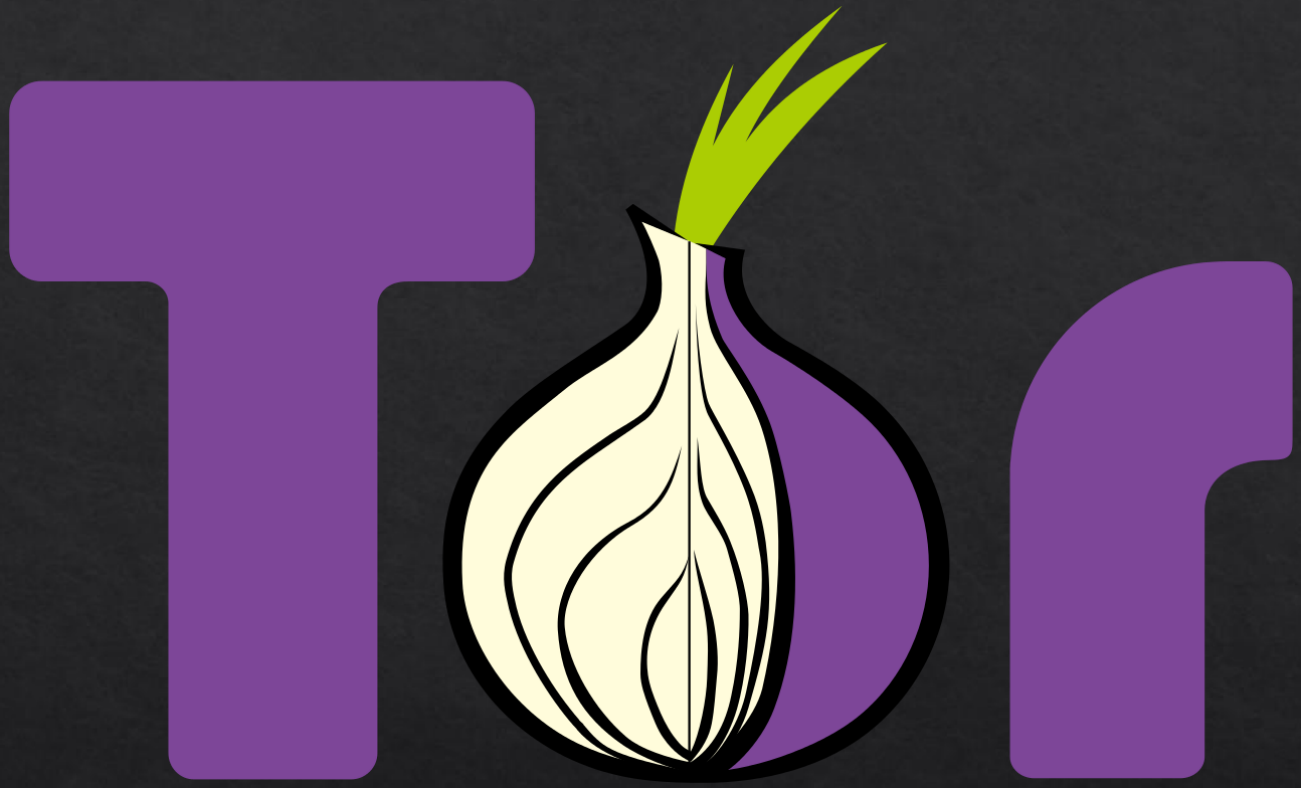
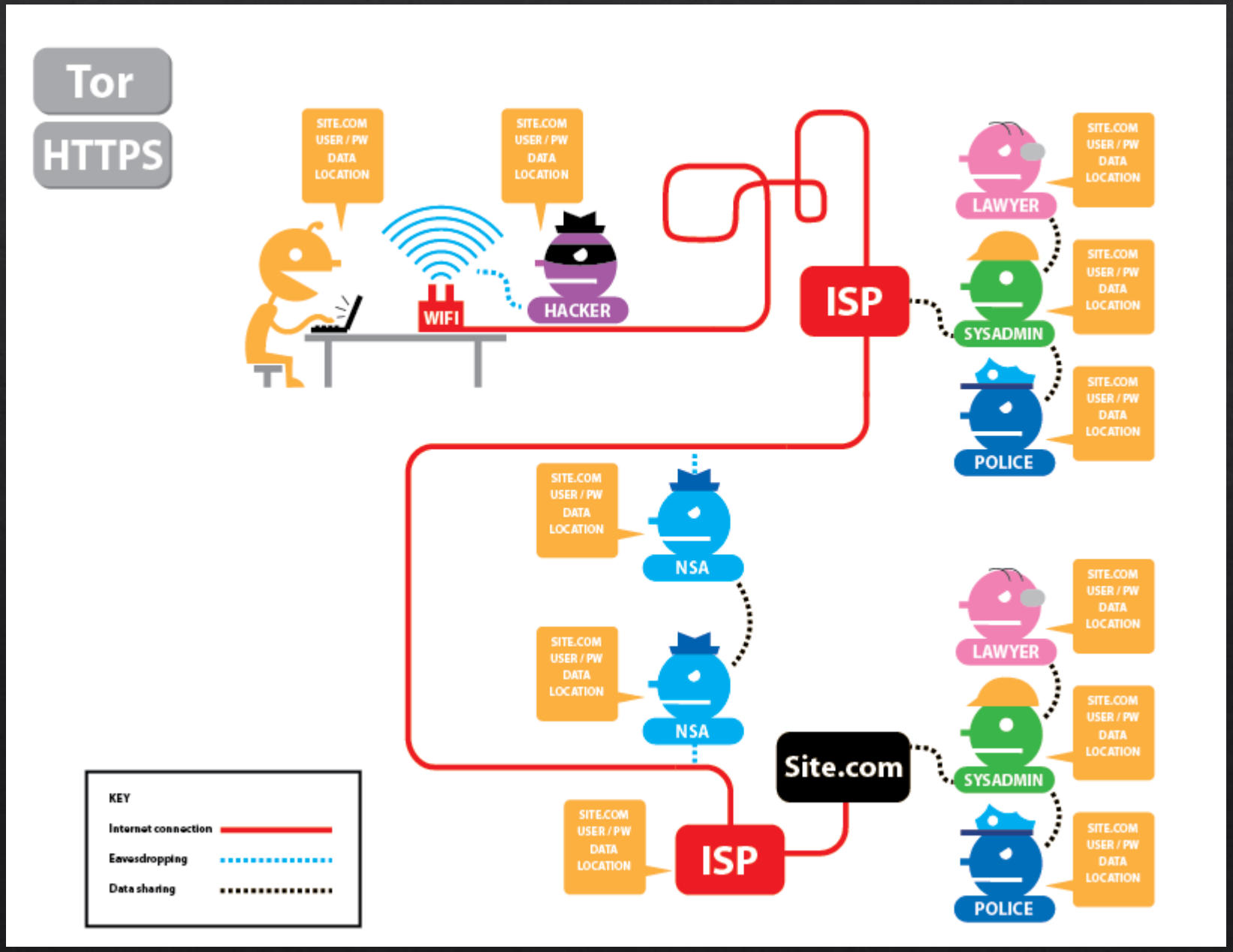
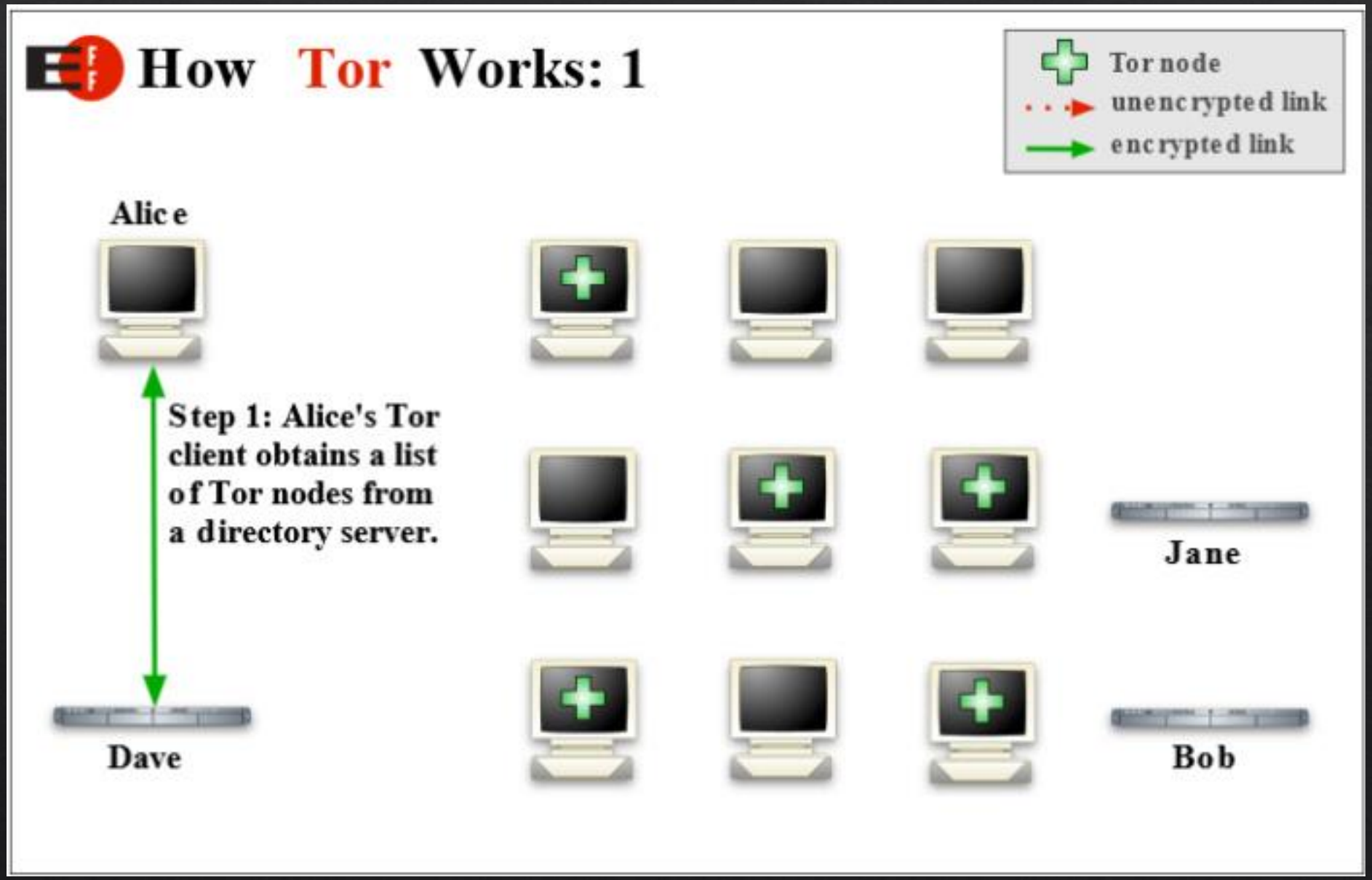

Tor

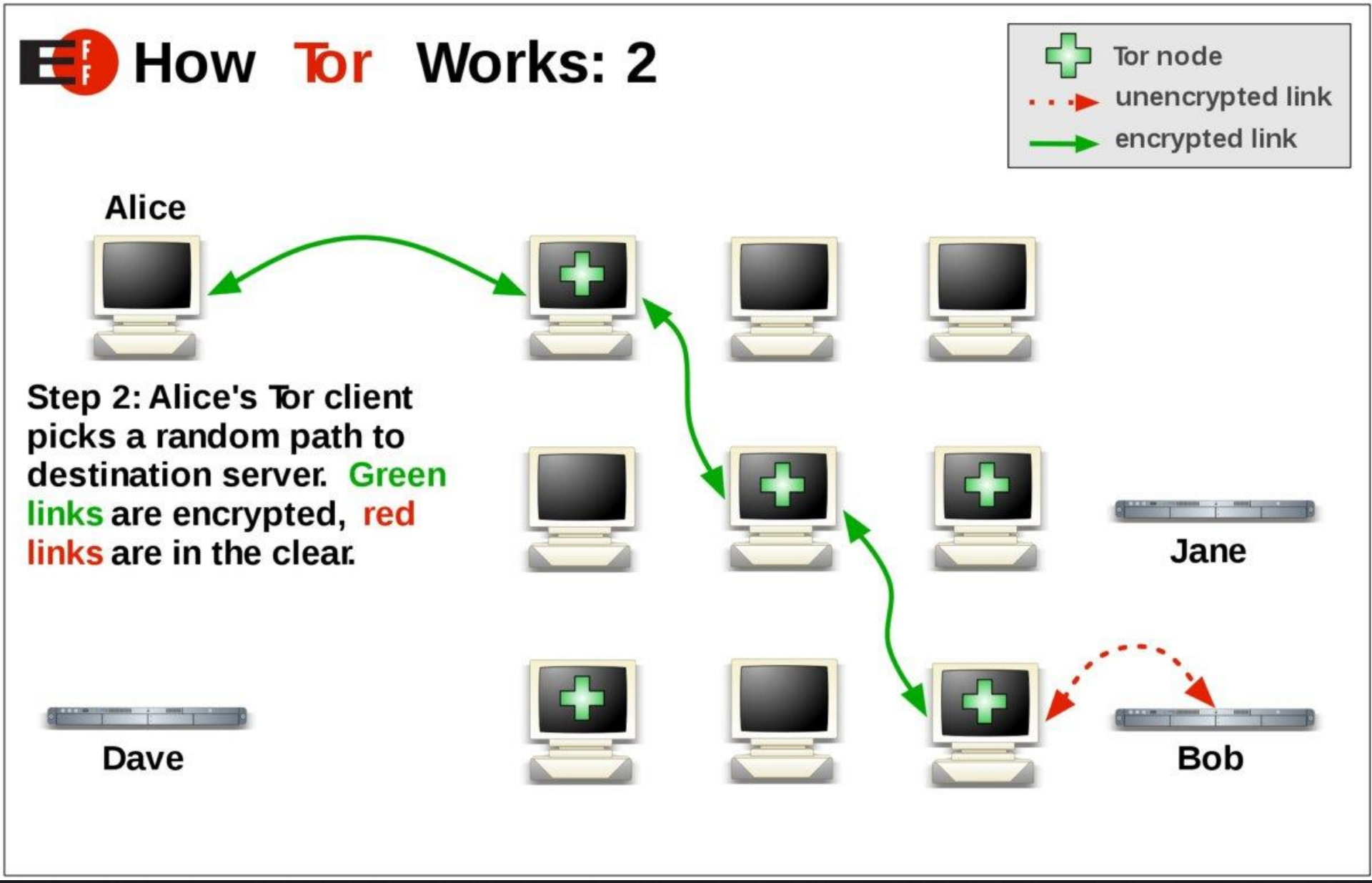
Tor Network: how Works?



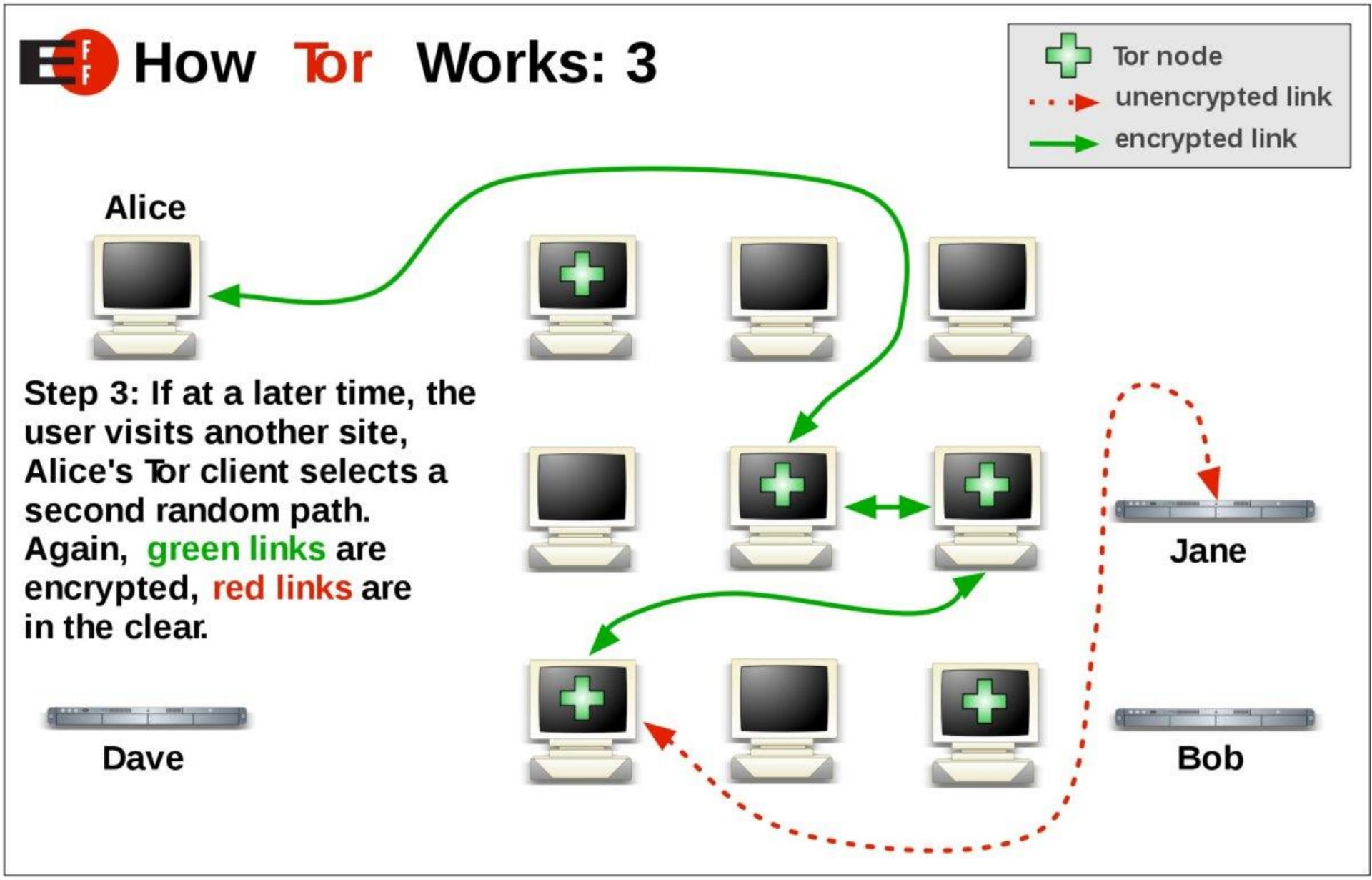
Tor Network: how Works?



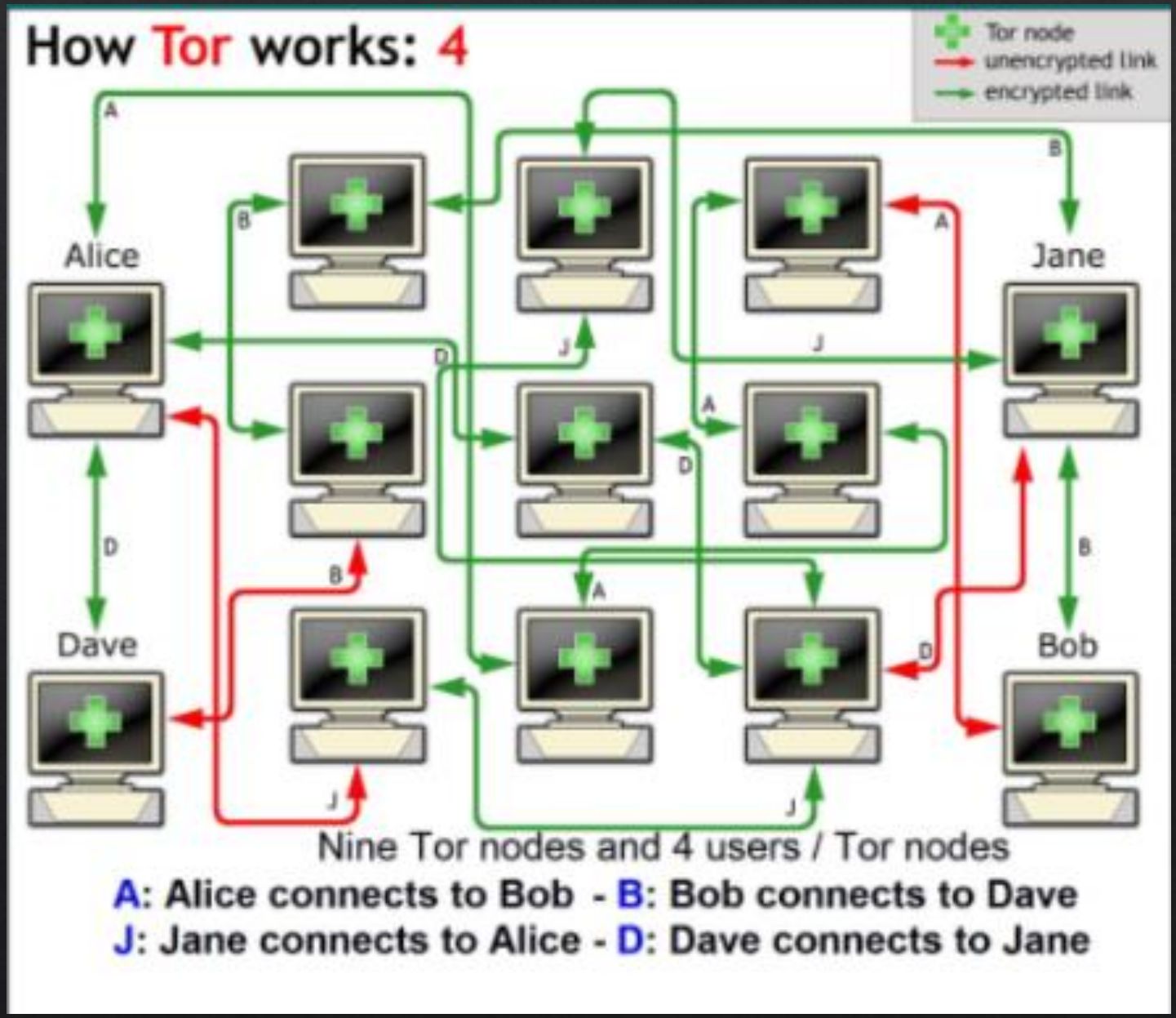
Tor Network: how Works?



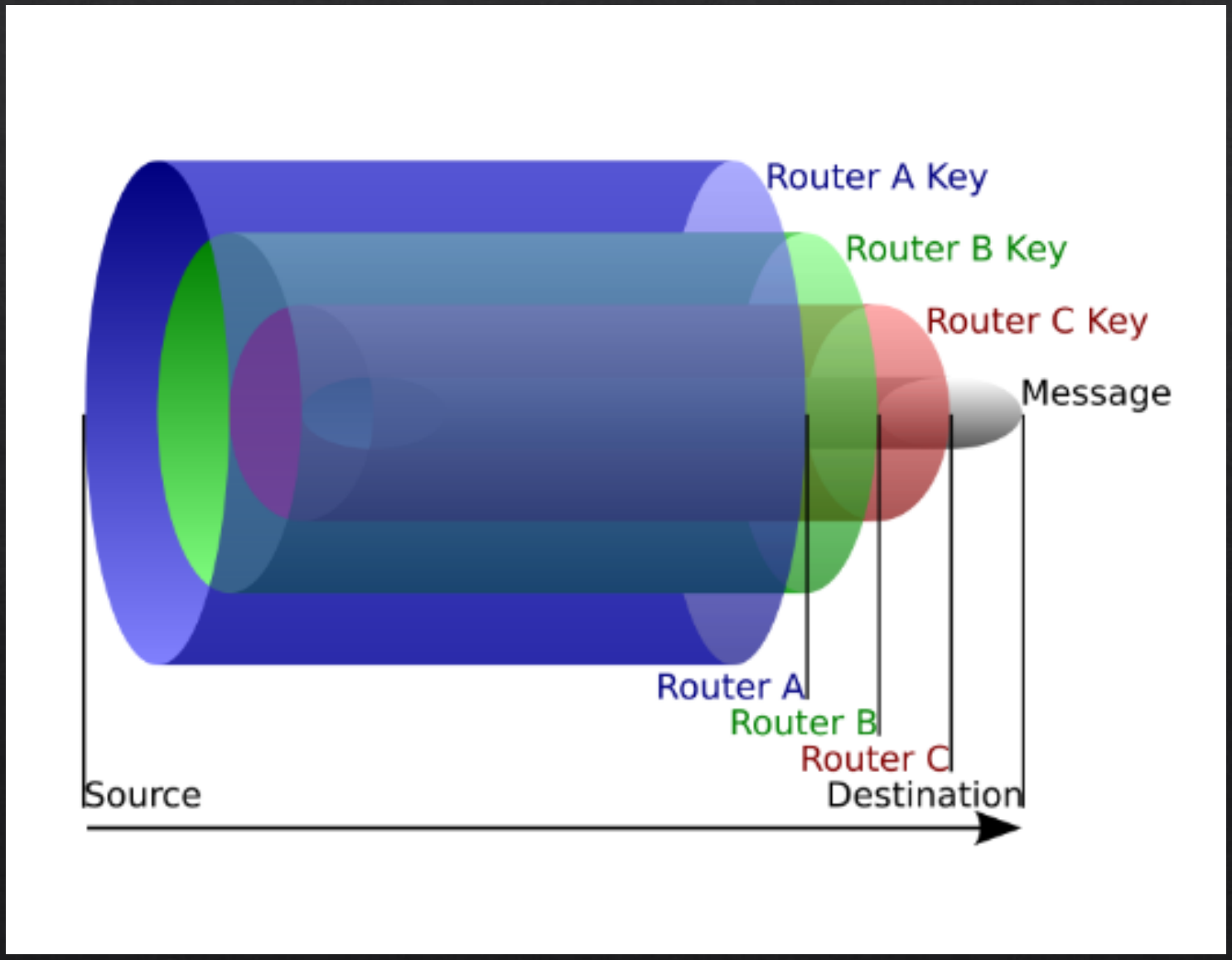
Tor Network: how Works?



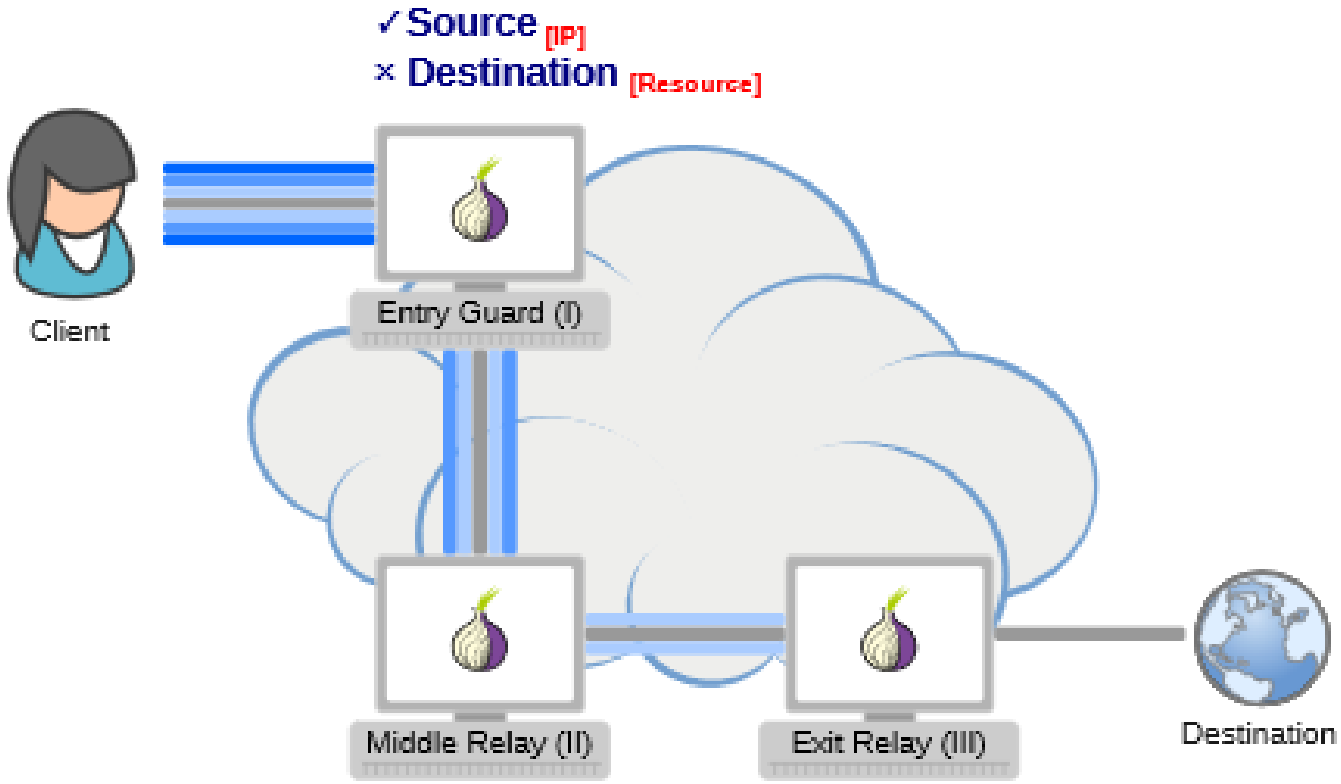
Tor Network: how Works?



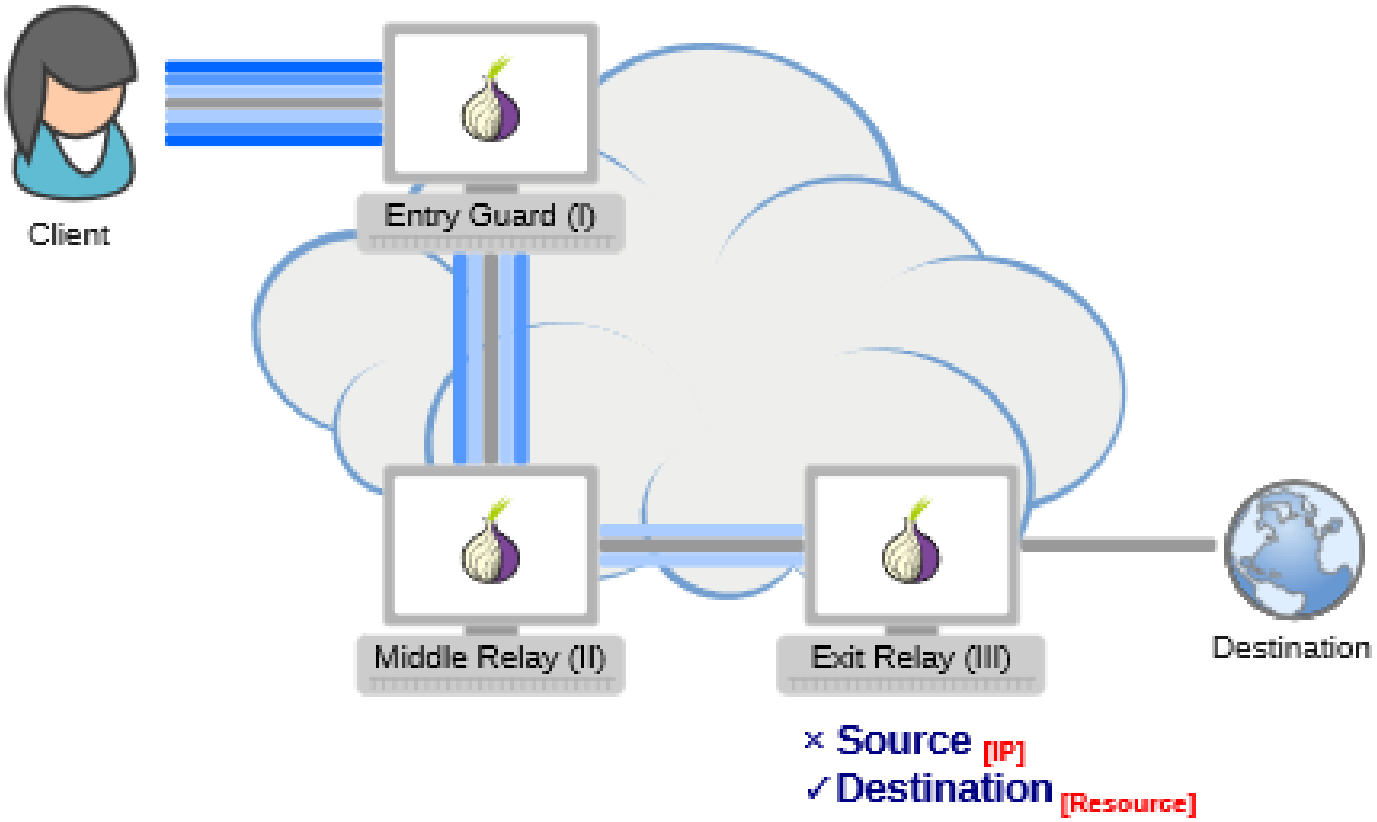
Tor Network: how Works?



Tor Network: how Works?



Tor Network: how Works?



Hidden Service Protocol

Hidden Service Protocol

- O HSP na prática esconde ip do servidor com o objetivo de impedir o rastreamento e possíveis hacks.
- Mas como manter o serviço disponível a um host cliente escondendo o ip?

Hidden Service Protocol

1- Cliente pede acesso ao servidor.

2- Cliente e servidor combinam um ponto de encontro para estabelecer uma conexão.

3- Nenhum dos 2 realmente sabe qual rota o outro usou até o ponto de encontro.

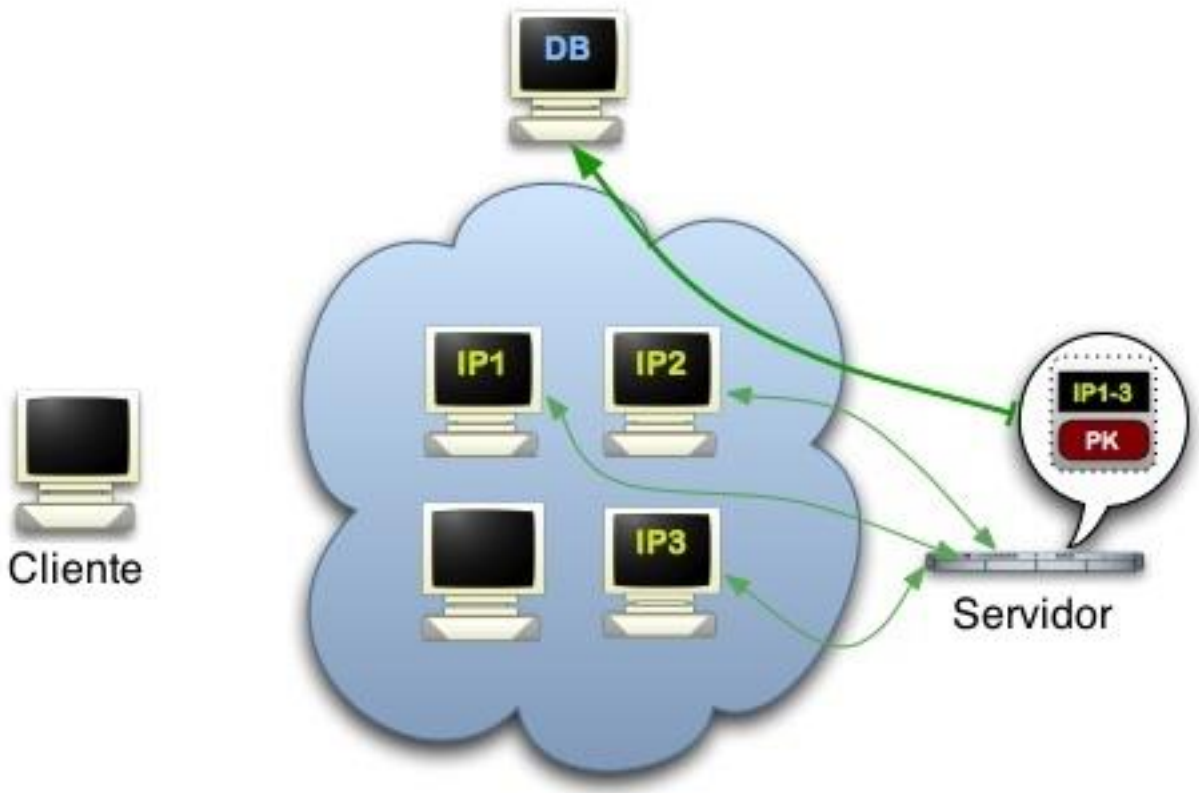
Hidden Service Protocol

Mas como é possível pedir acesso ao servidor sem saber a rota até ele?

Um Hidden Service precisa antes de tudo se anunciar na rede Tor. Ele escolhe aleatoriamente 3 relays, cria rotas até eles, e pede para serem pontos de entrada. Esses pontos de entrada apenas informam a chave pública de criptografia para o acesso ao servidor não informando o ip.

Hidden Service Protocol

Servidor envia chave privada para hashtable da rede tor e anuncia três pontos de entrada na rede.



Hidden Service Protocol

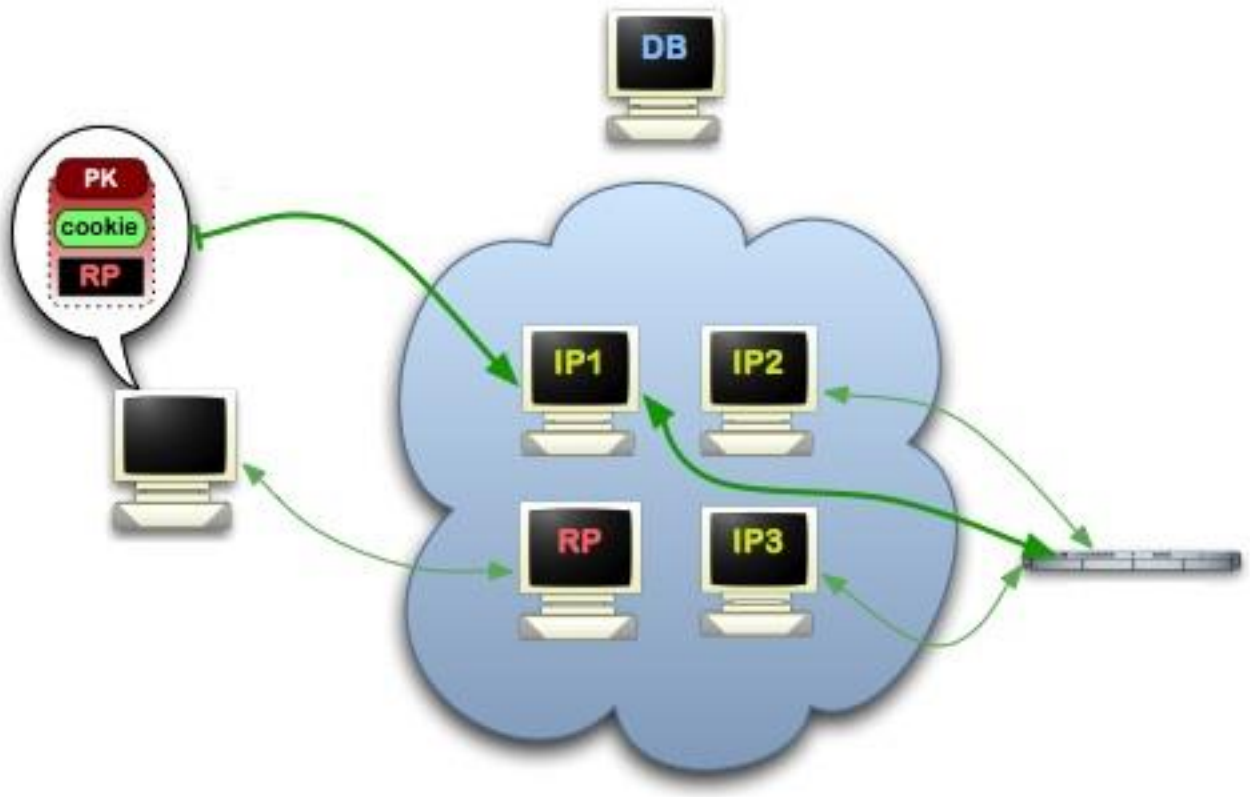
- Hidden Service constrói um “descritor de serviços ocultos” que contém a descrição dos pontos de entrada e a chave pública e faz o upload para uma hashtable distribuída pela rede TOR.
- O descritor será encontrado na hashtable distribuída pela rede, pelo host que tiver o endereço do servidor.
- Exemplo: batatas.onion

Hidden Service Protocol

- Após ser feito o download do descritor o host cliente então já sabe os pontos de entrada do servidor e tem a chave pública de criptografia para estabelecer a conexão.
- O cliente então escolhe um relay aleatório para ser o ponto de encontro entre cliente e servidor.
- Então o cliente manda uma mensagem para um ponto de entrada do servidor, pedindo para ser entregue para o hidden service.

Hidden Service Protocol

Cliente envia mensagem através de um dos 3 relays anunciados pelo servidor comunicando o ponto de encontro que será utilizado a seguir.



Hidden Service Protocol

- O servidor descriptografa a mensagem e encontra a informação sobre o ponto de encontro. Então é criado um circuito até o ponto de encontro.

- É importante que o hidden service mantenha os mesmo 3 pontos de entrada configurados inicialmente para evitar um ataque via relay contaminado caso caia um dos relays.

Hidden Service Protocol

- Por fim o ponto de entrada informa o cliente que o servidor estabeleceu uma conexão com sucesso.
- A partir daí cliente e servidor usam seus circuitos de entrada para trocarem mensagens através do ponto de encontro.

Hidden Service Protocol

Cliente e servidor se comunicando através do ponto de encontro.