**Intro to Outbound Firewall Bypassing**

**In order to get through a firewall, you have to pretend to be something that is allowed through the firewall**

* You can’t just force it; you’ve got to work with it

Most common way is to send an encrypted tunnel through an allowed port, like 80, 443 or 53, and to the final destination

* This is basically just hijacking an open port and sending your encrypted traffic through it

If you were sending your encrypted traffic through a certain port, **you would want your DNS resolutions to happen on the same port** so that you’re not doing local DNS resolutions and the network can see what you’re doing

**Proxies**

Weak form of local censorship evasion

Works if adversary isn’t using serious checks

**SSH Tunnelling / Dynamic Port Forwarding**

Encrypted SSH tunnel through an allowed port, out to the SSH server and then to the destination

Will have to change the port on the SSH server from 22 to an open port on the firewall e.g., 80 or 443

DPI by the adversary will allow them to know that it’s SSH traffic and can block it

Querying the port on the SSH server will show them that it’s an SSH server

Web traffic fingerprinting can also potentially give away where you are visiting even if traffic is encrypted

SSH can’t go through HTTP proxies

**OpenVPN Tunnels**

Potentially get though firewall

Change port on OpenVPN server form 1194 UDP to an open port on the firewall

UDP 53 is the best for speed if its open, especially since OpenVPN uses UDP

Better to use TCP however if you’re trying to look like regular traffic

DPI will show that this is a VPN

Querying server will show that it’s a VPN server

God for hiding real location for things like Netflix censorship

* Good when known VPNs are blocked because you can use your own server and if it does ever get blocked, you can just up a new one v quickly

**JonDoNym**

Low profile, less likely to be blocked by places like Netflix

Obvious to DPI that you are not using HTTPS if you are going through the 443 port

Similar SSH and OpenVPN in terms of getting out the network

* Will not work with HTTP and HTTPS proxies as it is not genuine HTTP/S traffic

**Pushing traffic through a firewall using an encrypted tunnel to the destination will only work if the firewall doesn’t use DPI**

Encrypted traffic will look different to what you’re pretending to be in terms of timing, size, direction etc.

Probing can also be used where they query the ports on the server you’re connecting to, to determine that it’s a proxy

* Isn’t common, but can happen – Great Firewall of China

**Tor**

Using Obfs or programmable transports to disguise the traffic to get through a firewall to get to the guard relay

Meek uses CDNs and delivery networks which if they were blocked, would block access to many other sites causing problems for users

* So isn’t often blocked

Some transports evade ip based blocks rather than content-based blocks which will all circumvent casual DPI but will be highlighted on closer inspection

Provides best protection for local censorship but it isn’t fool proof