# Security (outdated)

## Security

The goal of this document is to provide the most useful information for anyone interested in the security of the network. If there is missing information that would help understand and improve our network, please reach out to contact@nycmesh.net or join our slack.

> We are actively looking for ways to improve the security, resiliancy, and ease-of-use of the network to help the widest range of use cases. If you have ideas on how to improve anything, please join our slack

Our current threat landscape is most concerned with in-mesh security - once traffic is routed over an IXP, provider gateway, or peer, its equivalent to what people are used to.

In mesh threats include:

- DoS by announcement of bogus routes
- MiTM attacks on SSL servers using letsencrypt (should be alleviated by multiroute verification if we interconnect in more places)
- Visibility of *who* you talk to when using unencrypted HTTP, DNS queries, SNI, etc for someone along the route chain

## Data

- We do not keep logs of anything in-mesh. However anyone along the route chain could view unencrypted data or metadata (just like any ISP can).
- The organizers of nyc mesh can see a spreadsheet of signup information volunteered by participants on the join nycmesh page (name, email, phone, address all but email are optional)
- We create a map using map-nodes, from the above spreadsheet

## Wifi

A typical home install creates two wireless networks - one open 802.11 access point (with a captive portal), and one WPA2 encrypted upstream gateway. You can change the open access point to be encrypted if you wish.

# DNS

The default setup routes `.mesh` tld DNS requests to 10.10.10.10, which is anycast. Multiple people are running our knot-dns setup available on github (including supernode 1 at 10.10.10.11), but a malicious actor that is closer could take advantage of this.

---

Revision #3
Created 9 December 2023 04:40:00 by Willard Nilges
Updated 16 December 2023 04:52:48 by Andy