VPN Overview

The **NYC Mesh Virtual Private Network (VPN)** is a system that enables a computer that is physically disconnected from the rest of the NYC Mesh network (e.g., because it is too distant from existing nodes) to access the network. Put another way, it extends the NYC Mesh network to computers that are not physically part of the mesh. This is used for a number of different purposes, including to provide access to intra-mesh services, ease new node installations, bootstrap new neighborhoods, and more.

A **VPN (virtual private networking)** is a *virtual* network, creating a tunnel, or express route, across another network, such as the internet. Within the tunnel the network has no knowledge of the outside network, making it appear as if the entire network is seamless and directly connected. The outside network also has no knowledge of the inside network, making it a safe way to traverse dangerous or unknown networks.

VPN Infrastructure

NYC Mesh maintains some common VPN infrastructure for use by mesh members.

Please feel free to use the VPNs. However, please note that NYC Mesh is not a commercial VPN provider or reseller, nor are we trying to achieve an Internet-based darknet. The VPN service is subject to change and/or breakage at any time. Do not rely on NYC Mesh's VPN service as your primary or critical VPN provider. Also, as with all NYC Mesh resources, do not abuse the VPN service or the access it provides.

When might you use a VPN

We run a VPN service for a variety of reasons. You might want to use the NYC Mesh VPN to:

- **tie distant neighborhoods together.** For instance, if a distant part of the mesh is too far away from the other nodes to make a reliable physical connection, you can use the VPN to (logically) tie the mesh back together and make intra-mesh services available over the public Internet to the physically separated part of the NYC Mesh network. This isn't required, of course; the distant portion of the mesh can have its own connection to the Internet (an exit node) and maintain itself locally, but without a VPN connection it won't be able to access the rest of the mesh.

- **connect your laptop to NYC Mesh over the public Internet.** For example, if you are working in a coffee shop but need access to the mesh in order to conduct tests or develop and maintain mesh-specific features, you can connect to the mesh via the VPN. As another example, you can masquerade to Web sites and public Internet services as a NYC Mesh user, so that you can see the Internet from NYC Mesh's "point of view."
- **configure networking equipment during an NYC Mesh installation.** An installation may involve connecting to another node to configure it, which can be difficult to accomplish without already being on the mesh. By using a VPN connection, an install team member can temporary become part of the mesh prior to the completion of the physical installation.

VPN types and endpoints

Each supernode provides a few VPN options, depending on the supernode's locally available hardware. You may connect to any or all of the supernodes and, in some cases, depending on your hardware, you can even connect to multiple supernodes simultaneously. For the documented currently available endpoints, see § endpoints, below.

Choosing a VPN endpoint

Although you can generally use whatever endpoint you wish, you should consider a combination of factors for the best experience using the NYC Mesh VPN service. These considerations include:

- VPN software support on your computer.
- VPN protocol support provided by the NYC Mesh VPN endpoint.
- Your goal in connecting via the VPN; do you intend to connect a single device (laptop, phone, home router, etc.), or will you do meshing?

Based on these decisions, you will need to choose a different protocol and setup procedure. If your computer does not support any of the VPN protocols our endpoints do, you may need to connect using a different laptop.

Endpoint types

The NYC Mesh VPN service currently offers VPN connectivity using the following protocols. Each page will list endpoints available for that protocol.

L2TP/IPsec

L2TP/IPSec is a common general-purpose VPN protocol that work with most platforms. For example, computers running Windows, macOS, iPhones, and Android devices all support this type of VPN out-of-the-box. This type of VPN is a little bit oldschool, in that it is typically found in enterprise corporate environments, which is part of what makes it so ubiquitous.
For this reason, we have decided to provide and endpoint of this protocol.

For configuration instructions, please see our L2TP/IPsec page.

WireGuard

WireGuard is a modern type of VPN that was originally developed for Linux. There are now versions of the WireGuard VPN software available for recent Windows, macOS, iPhone, and Android devices as well; however, some older versions of those platforms may not support Wireguard. WireGuard is also typically fast, but is a bit more challenging to set up.

Other VPN types

At this time, we have not set up other VPN types, but we would like to in our spare-time. Other VPN protocols we are considering include: OpenVPN, and VTrunkD.

Revision #7
Created 9 December 2023 04:39:51 by Willard Nilges
Updated 9 August 2024 02:36:23 by Lydon Thorpe