anoNet

anoNet is a decentralized friend-to-friend network built using VPNs and software BGP routers. anoNet works by making it difficult to learn the identities of others on the network allowing them to anonymously host IPv4 and IPv6 services. One of the primary goals of anoNet is to protect its participants' rights of speech and expression.

anoNet	
Initial release	2005
Type	Anonymity, Peer-to-peer
Website	http://anonet.org

Motivation

Implementing an anonymous network on a service by service basis has its drawbacks, and it is debatable if such work should be built at the application level. A simpler approach could be to design an IPv4/IPv6 network where its participants enjoyed strong anonymity. Doing so allows the use of any number of applications and services already written and available on the internet at large.

IPv4 networks do not preclude anonymity by design; it is only necessary to decouple the identity of the owner of an IP address from the address itself. Commercial internet connectivity and its need of billing records makes this impossible, but private IPv4 networks do not share that requirement. Assuming that a router administrator on such a metanet knows only information about the adjacent routers, standard routing protocols can take care of finding the proper path for a packet to take to reach its destination. All destinations further than one hop can for most people's threat models be considered anonymous. This is because only your immediate peers know your IP. Anyone not directly connected to you only knows you by an IP in the 21.0.0.0/8 range, and that IP is not necessarily tied to any identifiable information.

anoNet is pseudonymous

Everyone can build a profile of an anoNet IP address: what kind of documents it publishes or requests, in which language, about which countries or towns, etc. If this IP ever publishes a document that can lead to its owner's identity, then all other documents ever published or requested can be tied to this identity. Unlike some other Friend to Friend (F2F) programs, there is no automatic forwarding in anoNet that hides the IP of a node from all nodes that are not directly connected to it.

However, all existing F2F programs can be used inside anoNet, making it harder to detect that someone uses one of these F2F programs (only a VPN connection can be seen from the outside, but traffic analysis remain possible).

Architecture

Since running fiber to distant hosts is prohibitively costly for the volunteer nature of such a network, the network uses off-the-shelf VPN software for both router to router, and router to user links. This offers other advantages as well, such as invulnerability to external eavesdropping and the lack of need for unusual software which might give notice to those interested in who is participating.

To avoid addressing conflict with the internet itself, anoNet initially used the IP range 1.0.0.0/8. This was to avoid conflicting with internal networks such as 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16, as well as assigned Internet ranges. In January 2010 IANA allocated 1.0.0.0/8 to APNIC.[1] In March 2017 anoNet changed the network to use the 21.0.0.0/8 subnetwork, which is assigned to the United States Department of Defense but is not currently in use on the internet.

The network itself is not arranged in any regular, repeating pattern of routers, although redundant (>1) links are desired. This serves to make it more decentralized, reduces choke points, and the use of BGP allows for redundancy.

Suitable VPN choices are available, if not numerous. Any robust IPsec package is acceptable, such as FreeS/WAN or Greenbow. Non-IPsec solutions also exist, such as OpenVPN and SSH tunneling. There is no requirement for a homogeneous network; each link could in fact use a different VPN daemon.

How it works

It is impossible on the Internet to communicate with another host without knowing its IP address. Thus, the anoNet realizes that you will be known to your peer, along with the subnet mask used for communicating with them. A routing protocol, BGP, allows any node to advertise any routes they like, and this seemingly chaotic method is what provides users with anonymity. Once a node advertises a new route, it is hard for anyone else to determine if it is a route to another machine in another country via VPN, or just a dummy interface on that users machine.

It is possible that certain analysis could be used to determine if the subnet was remote (as in another country), or local (as in either a dummy interface, or a machine connected via Ethernet.) These include TCP timestamps, ping times, OS identification, user agents, and traffic analysis. Most of these are mitigable through action on the users' part.

Scaling

There are 65536 ASNs available in BGP v4. Long before anoNet reaches that number of routers the network will have to be split into OSPF clouds, or switched to a completely different routing protocol or alter the BGP protocol to use a 32bit integer for ASNs, like the rest of the Internet will do, since 32-bit AS numbers now are standardised.

There are also only 65536 /24 subnets in the 21.0.0.0/8 subnet. This would be easier to overcome by adding a new unused /8 subnet if there were any.

Security concerns

Since there is no identifiable information tied to a user of anoNet, one might assume that the network would drop into complete chaos. Unlike other anonymous networks, on anoNet if a particular router or user is causing a problem it is easy to block them with a firewall. In the event that they are affecting the entire network, their peers would drop their tunnel.

With the chaotic nature of random addressing, it is not necessary to hide link IP addresses. These are already known. If however, a user wants to run services, or participate in discussions anonymously, they can advertise a new route, and bind their services or clients to the new IP addresses.

See also

- Anonymous P2P
- Crypto-anarchism
- DarkNET Conglomeration
- Darknet
- Freenet
- GNUnet
- I2P
- RetroShare

References

Consideration of User Preference on Internet-based Overlay Network, T Gu, JB Yoo, CY Park - ..., Networking, and Parallel/Distributed Computing, 2008 ..., 2008 - ieeexplore.ieee.org

1. "IANA IPv4 Address Space Registry" (https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.txt) . *iana.org*.

External links

- anoNet wiki (https://web.archive.org/web/20140127020051/http://anonet2.biz/)
- Another informative page (including information on connecting) (http://wiki.ucis.nl/Anonet)