1 Problem

This paper talks about VPN Gate - relay system to **achieve blocking resistance** from Government censorship. To implement VPN Gate, Author used VPN Gate server, VPN Gate list server(GLS), VPN Gate client. Author highlighted 2 key techniques **Innocent IP mixing, Collaborative Spy detection**. Along with these techniques, changing IP addresses of Servers also contributed to success of VPN Gate. Distributing server lists to users and then sharing a partial fraction of entire list helped. Status monitoring, port assignment to servers behind NAT, recording packet logs were used to prevent abuse from users. In the end, statistics were discussed.

2 Contributions

Author conducted various analysis experiments and implemented VPN Gate, most successful relay system with 464,000 active users. The 2 key techniques to mix vital IP addresses to server list and many volunteers combine together to form a spy improved the usage of VPN Gate against GFW, Censorship authority of China. Many features such as changing IP's, recording packet logs, Distributed Hash Table(DHT) to return different partial server list, daily mirror URL mail service, status monitoring made this relay system a hit. The system is setup in such a way that a PC can be a volunteer at times and can be a client in other cases. **Cat-and-mouse game** with GFW authority to improve the scalability of VPN Gate lead to discharge of all blocked servers.

3 Conclusions & Support

We need a volunteer server to provide access to prohibited websites. For this, A volunteer registers itself in GLS. If volunteer is behind the NAT box, VPN Gate server opens a port using **Universal Plug and Play(UPnP)/UDP hole punching**. To prevent the discovery of all VPN servers by GFW authority, GLS returns subset of the list. The censorship authority, GFW used python automated program to scan, add, block the IP addresses in the blocking list. In Innocent IP mixing, Innocent IP addresses(DNS root servers, ANS, TLD etc) are mixed in the server list. Upon accessing innocent IP, user gets *connection error*. The second technique, collaborative spy detection is used to detect probing activities performed by censorship authorities, gets the IP address of the source and blocks it(drops packets) when a request is made(censorship authority). GLS also aggregates the logs, this helps in identifying spies(incomplete, tiny calls). While distributing the lists to the user, GLS uses **key space hopping, Indirect server list transfer protocol**. VPN Gate server digitally signs the server list to prevent modification by intermediate server. The **daily mirror URL service** emails the latest URL list to subscribers on a daily basis. **Status monitoring** feature enables the users to choose a good VPN server which has low-delay, high bandwidth internet connection, **Modified GUI** lists the active VPN servers. Unlike Tor, VPN gate cannot be used as an anonymizer. The packet logs(header+payload) are recorded and prevent the VPN Gate from taking any abuse from users. VPN server generates temporary ZIP file for each request to achieve blocking resistance. According to statistics, Korea ranks first in total data transfer with comparatively less number of VPN connections because of high-speed home internet lines(no packet loss). Having large number of VPN connections, Thailand did not yield large data transfer, Low speed internet in these areas caused a huge packet loss. Therefore, many factors on the client side influenced the data transfer rate.

4 Likes & Dislikes

Detailed analysis of VPN Gate performance, active users, active servers made the project progress from **30%** reachable to **78%** reachable by integrating the system with modern, innovative approaches. A volunteer running a VPN server has the access to alter the decapsulated packets of the users is a problem which is yet to resolve. VPN server might use up the entire bandwidth.