Traffics Management using IP Geolocation

Network threats are constantly changing. Nowadays, real people are doing the spam attacks and other malicious network activities. The traditional techniques that were developed to fight off network abuse, attacks and spam bots have been deemed inefficient. To tackle the new form of threats you will need to conduct traffics management at both macro and micro level.

What is network traffics management?

Traffics management also called traffic filtering is using the attributes of network traffics to grant or deny access into your network. Using the source country attribute to determine whether a specific IP address should access your network or not is called Geo IP filtering.

How can we use IP geo-location to perform traffics filtering?

Firewalls are the first line of defence against network attacks. Firewalls monitor data being transmitted to and fro a network. They check the data against the flagged transmissions to determine if the data should be granted access or denied. They are many criteria of filtering out data using a firewall. One of the most popular ways is to block traffics from one specific country.

Most firewall devices such as Cisco® come with the ability to filter out IP based on country of origin. Some web servers such as Apache and IIS also come with the IP address filter feature. If the country is blacklisted, then access to your network is denied. It is important to note that when you filter out a specific country, you won't be able to send data to that country as well. IP2Location provides a free web service to produce IP filter list by country. The output format supported are Apache .htaccess, Linux iptables, CIDR, Netmask, Inverse Netmask, IIS web.config and Cisco ACL. Please visit IP2Location Firewall List for more information.

Email can also be attacked with spam. Some email traffics management solutions have the ability to categorize the mail based on country origin. Blocking emails from spam prone countries will significantly reduce or even completely eliminate the presence of spam in your inbox. Spam quarantine applications on the client side will be rendered useless once you can filter all spams on the mail server side.

In conclusion, IP Geo-location traffics filtering may not be a bulletproof solution, it is best utilized to complement other network security measures you have in place. Local or regional based businesses will have the easiest time determining which Geo-locations to filter but even international businesses can apply this technique to some extent as well. At the end of the day, implementing the network filters properly will give you peace of mind knowing that your network is protected from spams and attacks.