How Traffic Filtering Works using IP Geolocation

Posted on May 20, 2019

The cyber threat landscape changes daily. These days, it’s the real people that are launching spam attacks and other malicious activities against networks. Traditional security measures that have previously been effective against various forms of attack are no longer adequate. With the growing number of sophisticated attacks, new security measures are needed.

How is Network Traffic Managed?

Traffic management, sometimes called traffic filtering, refers to the use of network traffic attributes to grant or deny access to your network. It also involves the use of the source country attribute to grant or deny specific IP addresses access to your network in what's called geo IP filtering.

How is IP Geological Filtering Used for Traffic Management?

The first line of defense in any network is the firewalls which monitor the data received and sent on their assigned network. To verify the traffic is legitimate, they analyze any flagged transmissions to see if access is to be denied or granted. The firewall will use a lot of criteria when filtering out traffic that is suspesious.

A more popular solution along the filtering is blocking traffic from specific countries. The most popular firewalls have the ability to filter out IP addresses from specific countries. Many web servers like Apache and IIS can also do that. Any country that ends up blacklisted by using such filtering will see their traffic denied to the given network. You won't be able to send data to them either.

IP Geolocation API, for example, provides a geolocation tool for IP addresses to identify users from any country of origin. Their service helps you detect risky accounts and behaviors from a given location.

How is IP Geological Filtering Used to Combat Malicious Traffic?

If a pattern reveals that a series of attacks is coming from the same country or countries, blocking all traffic to and from those countries would seem to be the quickest and easiest solution. How practical is that? Not very.

Rejecting traffic from entire countries could interfere with the genuine need to interact with lawful systems or servers there. It's one of the reasons people have been hesitant about traffic management with an IP geolocation.

It should also be understood that the attacker may not be in the country where the traffic is coming from. It could be that they are running data packets through systems that have been compromised in the identified countries. Using open proxies to multiply his threats, the attacker can make it look like the traffic is coming from a number of places in order to protect himself and hide his patterns. It's also meant to try to slide past the security measures in place.

With the advances in threat security, like IP Geolocation API, an additional layer of screening is added to traffic going both ways.

So how does IP geolocation-based traffic management help filter traffic that's malicious? Security applications like IP Geolocation API can help you handle malicious traffic in a variety of ways. And it can do way more than just filter traffic.

- **Detect Fraud:** Using the API, you can match visitor geolocation IP data with customer data you already have to catch fraud and identity theft attempts.
- **Identify Malicious Activity:** Detects questionable activity and specifies the country where it comes from.
- **Insights for Marketing:** Using the geolocation data provides truly invaluable insights about those visiting your website, allowing you to find new opportunities or patterns you can use to enhance your online marketing efforts

.

- **Strengthen Indicators of Compromise:** Data from the API can strengthen indicators of compromise (IoCs) within a strong threat intelligence platforms and security information and event management (SIEM) systems.

A Powerful Tool in the Battle Against Cyber Threats

Cyber attack and malicious traffic are increasing, but we have more advanced ways to identify where it's coming from by using geolocation. In using powerful geo-specific filtering methods, you gain far better control of your network. You'll be better able to remove a lot of undesirable traffic from your network. You'll also be able to keep traffic from being directed beyond your network for improved security.