# The IP Address as Identity is Lazy Security

Lori MacVittie, 2018-16-08

It’s also largely ineffective

The Internet works largely because of DNS. The ability to match a site with an IP address – needed to route requests and responses across the Internet – is what ultimately makes the Internet usable. The majority of users are likely blissfully unaware of IP addressing in the first place. Because cheese.com is just far easier to remember.

But this association – of a singular identity with an IP address – is now so tightly ingrained in our heads that we tend to apply it to other areas of technology. Even when it’s utterly ineffective.

Like security.

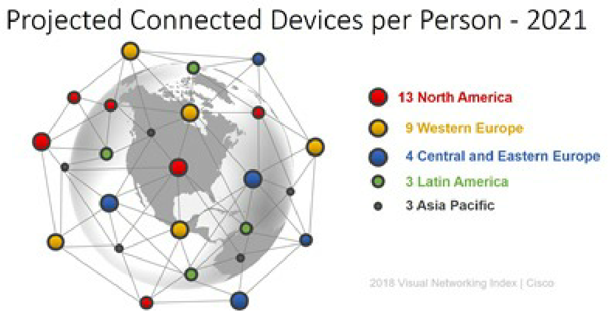
Back in the day, IP addresses were fairly fixed things. Routes were flexible, IP addresses for the most part stayed where they were assigned. Today, however, IP addresses are like candy. They’re handed out and traded with greater frequency than SPAM hits my inbox.

Cloud commodified the network. IP addresses are mine only as long as the resource it was assigned to is in service. Mobile, too, has played a role in turning IP addresses into virtually meaningless octets. A quick search will yield a variety of technical dramas in which a legitimate business running an app in a public cloud has been blocked automatically by blacklists because the previous assignee of that IP address used it improperly.

Add in the modern, connected home with its growing number of Internet-reliant gadgets and there is absolutely no value in matching IP addresses to any individual thing or person.

Traditional security that relies on IP addresses – usually through blacklisting and blocking – fails in the face of this flexibility.

So it’s not surprising when a report pops up noting that the ability to IP-shifting habits of bad bots makes it difficult to identity and block them. Particularly those bots who’ve attached themselves to a mobile device.



Using IP addresses as the basis for identifying anything – devices, bots, users – is lazy. It’s the simplest piece of data to extract, yes, but it’s also the least trustable.

This is not new. The information security industry has been preaching for several years now that traditional, signature-based techniques are not going to protect us any more. That’s because they’re based on the premise that bad actors are recognizable; that we know what they look like. While that’s true, it’s only true for yesterday’s attacks. It doesn’t really help us with tomorrow’s attack, because we have no idea what that’s going to look like.

Combined with the increased use of end-to-end encryption by everything – including malware – traditional security options are left guessing as to whether any given interaction is legitimate or malicious. Rendered blind by encryption, signature-based solutions become little more than bumps in the wire. Without the ability to inspect traffic, security on the wire is a dying breed of technology at which bots sneer as they pass by on their way to make a home amongst your resources.

It takes minimal effort to use IP addresses alone to identify endpoints. When paired with information like the user-agent from an HTTP header (which is user input and itself inherently untrustable) there are barely measurable improvements in success. With the processing power available to us today there is no reason we cannot take a few microseconds to extract from connections and interaction a broader array of characteristics from which we can deduce if not identity, then at least intent.

Using IP addresses or signatures alone isn't enough to protect apps and networks from infiltration. Behavioral analysis, challenge-response, and deep inspection will need to be used together to effectively weed out the bad from the good.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | wwww.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com