Laren Metcalf
Director, IP Services

DDoS Attacks are not an IF, but a WHEN. Are you ready?

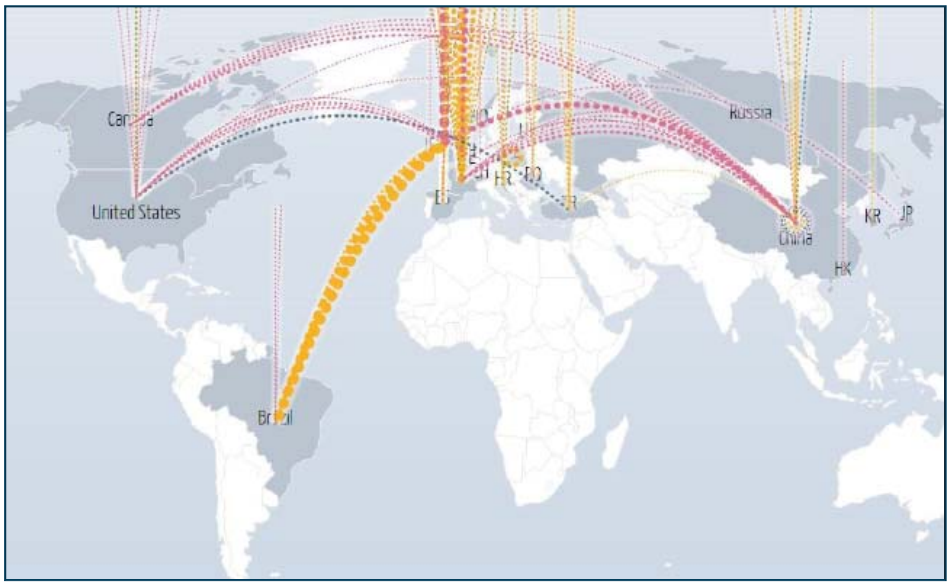
Distributed Denial of Service (DDoS) attacks are now a fact of life for service providers. Every service on the internet has been affected from application providers and cloud services, to internet service providers providing connectivity. Due to the dynamic nature and increased sophistication of the attacks old methods grew ineffective and new techniques had to be deployed.

DDoS attacks are the internet's largest and most sophisticated type of attacks. When they first appeared they were being run from hacked web servers utilizing a portion of their internet bandwidth. Now they have increased in scale and sophistication which has made their advent a turning point in security on the internet.

The magnitude of the attacks are clearly evident if you look at a map of current DDoS attacks www.digitalattackmap.com[1]. This shows multiple streams of network traffic, both locally and around the globe, composed of billions of bytes of traffic. All of it is routed--it's valid traffic—with essential information like a destination and source address. But none of it is usable data. It's simply a stream of empty packets aimed at a target on the internet. Its intent is to overload the target device to the point of either crashing the system or flooding it so it can't process legitimate traffic. This not only affects the targeted system but will take out the entire provider's network costing them downtime and ultimately services and money.

We have security - firewalls, IDS/IPS, malware detect, antivirus...so we are safe, right?

First and foremost, Distributed Denial of Service attacks are the most difficult to defend against. DDoS attacks commonly originate from Bots. Bots are remotely controlled malware that are usually used to connect to other systems, but in this case are programmed to launch the attacks. Botnets are vast numbers of bots. An example of how easy it is for hackers to use botnets in a bot-herding scheme was demonstrated at the Black Hat convention in Las Vegas in 2013. The attack grew to 8 million bots in 18 hours. The bots were imbedded in online ads that could be updated remotely. An article describing the amplification was published in the malware/hacking section on www.networkworld.com [2] .



www.digitalattackmap.com

Attacks of this magnitude require an adaptive device like a next generation firewall or a security appliance utilizing adaptive threat intelligence. Routers can be set up to drop traffic after hitting a maximum threshold, or identify a specific packet as undesirable, but aren't sophisticated enough to adapt to continually changing attacks. The dynamic attack threatscape requires continual updates to ensure current attack types are identified. Firewalls inspect each packet and create a connection table entry for each connection request. As each new request comes in another entry is created in the connection table.

In a DDoS attack there are millions of connection requests coming in that fill the firewalls connection table. If the number of requests coming in exceeds the size of the connection table, the firewall either crashes or slows down to the point where it can't be accessed to analyze the problem. To make matters worse, a firewall may be dealing with an internal network infected with viruses, worms, and trojans, all making requests to allow more traffic in from the outside.

Making sure you have a clean network is the best internal defense. Monitoring your network during normal traffic levels when users are active is the best way to know if your network is clean. Low activity won't have enough real traffic and real users on their devices; high traffic would give abnormally high rates for all monitoring criteria.

The type of security you need is not going to come from the existing security infrastructure you've been using. DDoS attacks can be prevented by a device designed to handle millions of connection requests without allowing them as connection table entries, thus saving system resources. Routers can be used to mitigate the most common DoS/DDoS attacks.

Providers have started to include management information in their BGP route information. This alerts routers to specific BGP areas generating attacks and automatically drop traffic. Routers can also limit the number of connections, drop traffic that resembles an attack that uses a specific protocol or packet size, but the attacks have evolved. Hackers have been able to work around these fortifications by manipulating the packet's size, connection information, and continually changing the attack signature increasing the sophistication of DDoS attacks.

If Firewalls can't block DDoS attacks, what about IDS/IPS devices? Intrusion detection/prevention devices are packet analyzers. They wouldn't be able to keep up with the extreme amount of traffic in a DDoS attack. They look for attack signatures in network packets. The amount of traffic needed to analyze an attack would overwhelm its capability. The best way to mitigate DDoS is at the edge before it hits your border router. Using a device dedicated to identifying DDoS traffic before it gets to the customer router will ensure no packets get through.

DDoS mitigation requires a device capable of very high throughput at the network edge receiving updates 24/7 on new attacks as they are discovered. Utilizing a redundant or failover design would be high cost, provider connections are expensive, but environments where high 99% SLA requirements are required guarantees no loss of service. This model would work for any type of service outage and opens the door for all types of protection. Constant 24 hour updating would minimize zero day attacks due to early detection and immediate response.

The security landscape has become very dynamic. Recent attacks on major retail and financial institutions have broadened awareness and opened up the security field with new products that are just now becoming mainstream. Next generation firewalls expand on the principle of the firewall as a border device but address all facets of security including monitoring of internal resources like dns, windows domains, and behavior anomalies.

All solutions target specific security threats with varying techniques and choosing the platform best suited for you depends on your specific security needs. It is important to continually audit your security practices and update your strategy to adapt to the ever changing threatscape. In the future, complete prevention systems may be developed that incorporate immediate attack response systems that prevent the attacks. Today we identify and limit our attack exposure and try to prevent major losses incurred in the unfortunate event a cyberattack occurs.

Taking a proactive approach to security will prepare you for when an attack occurs. Ensure your business and residential customers can rely on your services. Begin by creating a strategy for operational excellence.

Contact Finley Engineering IP Services, at 952-582-2912 or m.ockenga@fecinc.com for a complimentary discussion to jump start protecting your network from the most complex and debilitating DDoS attacks.

1. www.digitalattackmap.org

2. http://www.networkworld.com/article/2168696/malware-cybercrime/black-hat--how-to-create-a-massive-ddos-botnet-using-cheap-online-ads.html