Solution Brief

NetFlow-based DDoS Detection

Fast, Accurate and Reliable DDoS Attack Detection is Key for Effective Incident Mitigation and Overall Network Security

This solution brings new cyber defense capabilities to businesses by providing early detection of DDoS attacks before network devices and servers targeted by DDoS are incapacitated.

The Challenge

DDoS attacks are notoriously difficult to detect on a timely basis and defend against. Traditional perimeter-based technologies such as firewalls and intrusion detection systems (IDSs) do not provide comprehensive DDoS protection. Solutions positioned inline must be deployed at each endpoint, and are vulnerable in case of a volumetric attack. Typically, solutions require systems to run in "learning" mode, passively monitoring traffic patterns to understand normal behavior and establish a baseline profile. The baseline is later used to detect anomalous network activity, which could be a DDoS attack. This approach takes a long time to implement and any change in the infrastructure makes the baseline obsolete, and results in False Positives.

The Solution

In contrast to common systems, NetFlow Logic's solution is based on flow information analysis. It is not susceptible to volumetric flood attacks, and does not rely on baseline data collection, which may take days or weeks to establish. Instead, NetFlow Logic's DDoS Detector App uses an innovative approach that makes it operational in 15 to 20 minutes after deployment. Changes in the infrastructure do not require any restart or modification of DDoS Detector, as it immediately adjusts to the new network configuration.

DDoS Detector is based on advanced statistical and machine learning methods and consists of several components, each analyzing network metadata from a different perspective. Results of the analysis are combined and a final event reporting or alerting decision is made. The result of this "collective mind" approach is a reduction in False Positives without compromising the rapid detection of a possible attack.

Solution Advantages

- **Rapid Detection** – other solutions usually provide rapid detection in the case of a volumetric attack, but can take hours to detect a DDoS attack of another type. Early Warning DDoS Detector App from NetFlow Logic can identify possible DDoS attack almost immediately. In some cases, the App can even predict an attack as it is about to happen. DDoS Detector can detect anomalous traffic within 30 seconds of its appearance, even when the attack is low and slow.

- **Reduction of False Positives** – majority of alerts in common solutions are a result of a False Positive. These typically occur due to network configuration changes, or other baseline behavior changes and harmless usage spikes. Advanced analytics engine used by DDoS Detector can reduce False Positive alerting by 90%, enabling your administrative staff to focus on real threats to your networks and infrastructure.

- **Broad Spectrum Threat Detection** – DDoS Detector App offers the widest coverage against many types of network availability threats. The App is not dependent on any specific threat signature or attack pattern. It uses analytical and machine learning capabilities to detect new threats and anomalies as they appear. It can adapt to constantly evolving attack techniques without any human intervention.

Solution Benefits

- **Protection continuity** – Changes in your network infrastructure do not require any changes in configuration of DDoS Detector App, ensuring that your threat detection system is always current.

- **Increased Attack Resilience –** Early stage attack detection allows rapid mitigation before targeted network devices and servers are incapacitated. Mitigation cost and effort are a fraction of the cost and effort of business interruption and recovery.

- **Cost Effective and Easy to Deploy** – The solution is 100% software based and requires minimal efforts and expense to deploy and use. It can be integrated with your existing SIEM system to accelerate return on investment of your existing security infrastructure, and lets you focus on your primary business goals.

Learn More About Our NetFlow-based Solution

If you would like more information about our core flow processing product NetFlow Optimizer or any specific NetFlow-based solution please visit our website www.netflowlogic.com or contact us via email info@netflowlogic.com.

System Requirements

Hardware/Virtual Appliance

16GB RAM, 8 Cores CPU, 20 GB disk space.

Virtual Appliance

VMware ESXi 5.x and above

Operating System

Linux CentOS 5.5, 6.5, 7 – Debian 6 – RHEL 5.5, 6.5, 7 – SUSE ES 11 (kernel 2.6+ 64-bit)
Windows Server 2008 R2, 2012, and 2012 R2 (64-bit)
