DATASHEET

ATM

Attack Threat Monitoring

OVERVIEW

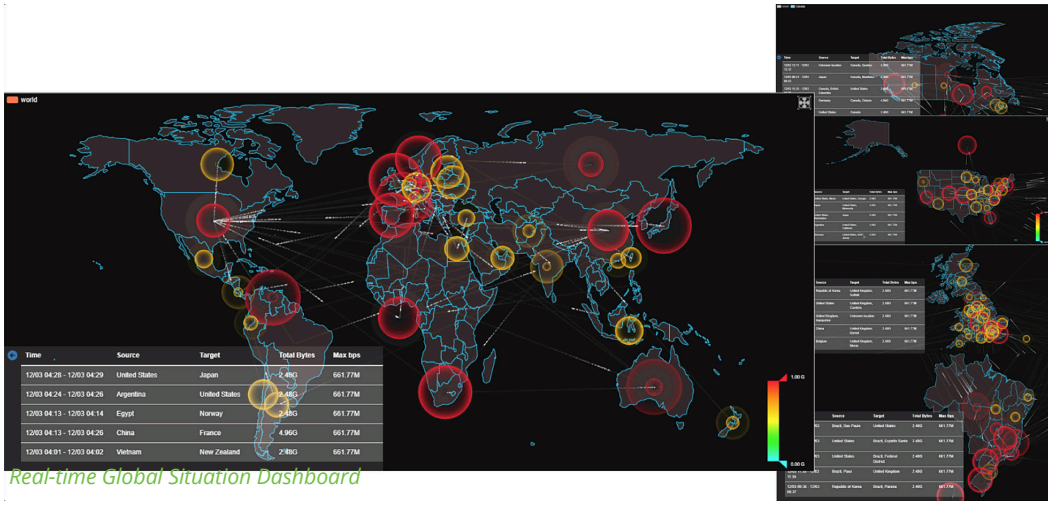
Nearly 50 percent of DDoS attacks observed are under 10Gbps in size, and last less than 30 minutes in duration. These attacks can easily be defended or mitigated by NSFOCUS On-Premises DDoS Defenses. But what do you do when attacks become larger and longer?

DDoS defense always begins with detection first. The most economical and effective way to detect DDoS attack traffic is to monitor flow data (xFlow, iFlow, etc.) coming from border, core, and/or edge routers. Once a DDoS attack is detected the most common way to protect customers is to divert both good and bad traffic for the IP addresses under attack to out-of-path mitigation technology. Once the DDoS traffic is mitigated, legitimate traffic is re-injected back into the network for the entity under attack.

However, a lot of data is generated during a DDoS attack which is difficult to analyze in real time. This makes adjusting your DDoS mitigation strategy difficult when suffering multiple larger attacks over a period of time.

ASSESS THE THREAT FROM A DDOS ATTACKER

Traffic flow analysis is the typical method of developing statistics for a DDoS attack. But the threat assessment from flow analysis alone is superficial and limited. NSFOCUS ATM takes DDoS threat analysis and assessment into the next generation and beyond!



Real-time Global Situation Dashboard

The Global Situation Dashboard delivers real-time awareness of the DDoS situation based on data received from the NSFOCUS Network Traffic Analyzer (NTA) or third-party data flow aggregators. ATM provides drilldown capability into countries from the world map providing a better view of attack sources and targets.

Current and historical DDoS attack data is available to provide better insight into the size and scope of DDoS attacks to the organization.

*To learn more about IP Chain-Gangs, refer to the report "Behavior Analysis of IP Chain-Gangs": https://nsfocusglobal.com/behavior-analysis-ip-chain-gangs/

KEY FEATURES

Real-time contextual awareness of both the local and global DDoS threat landscape

Includes global data from NSFOCUS Cloud services

Automatically relates relevant global data to local events

Integration with award winning NSFOCUS Threat Intelligence

Provides Attacker IP Reputation information in 10 categories

Previous attack history

Automatically identifies attackers into IP Chain-Gangs

Groups related source attackers into IP Chain Gangs

Provides IP Chain Gang Reputation information in 10 categories

Provides previous IP Chain Gang attack history

Reduce O&M costs

Extend the life of ADS license

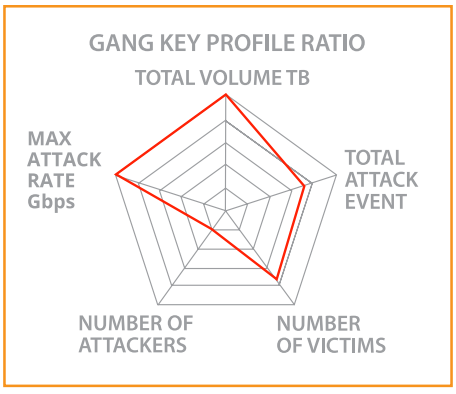
Extend the life of ADS appliances

Integration with NSFOCUS Threat Intelligence (NTI) provides contextual information about attack sources such as their IP reputation in 10 categories, previous attack history, and commonality with other IP addresses in the sources ASN.

TI based contextual analysis

THEY'VE BEEN WORKING ON THE IP CHAIN-GANG!

From NTI, global DDoS data is correlated and mapped to the DDoS data within the local environment. Deep analysis and machine learning then groups attackers into IP Chain-Gangs, attack sources that share common traits including victims. Once IP Chain-Gangs have been identified, behavior profiles are created displaying information on total number of attacks participated in, attack rates & volumes, durations, number of gang members and total number of victims. From these profiles an organization can determine what the level of risk to them is and if they are future potential targets.



REDUCE O&M COSTS

Based on ATM's comprehensive analysis and reporting, organizations can develop strategies for mitigating future DDoS attacks. System ROI can be improved by crowdsourcing NTA data back to the NTI cloud to provide comprehensive DDoS attack blacklists that can extend the life of existing ADS licenses by 9-12 months.

REAL TIME DDOS SITUATIONAL AWARENESS

NSFOCUS Attack Threat Monitoring provides real-time contextual awareness of both the local and global DDoS threat landscape. Identification of IP Chain-Gangs can provide early warning of further DDoS attacks. ATM will provide attack insights for organizations with the smallest internet footprint to multi-national businesses that own IP ranges all over the world

NSFOCUS ATM not only identifies your DDoS risk on the internet, it can reduce O&M costs by increasing ROI by extending the life of ADS licenses and appliances. Reduce your risk, save money using Security that is Smart and Simple.