DATASHEET

NSFOCUS

Magic Flow

INTEGRATED NETWORK GOVERNANCE PLATFORM

KEY BENEFITS

Quick and easy deployment

Global analytics and visibility

Optimize network resources

Advanced threat identification

Outstanding threat traceability

Scale security with business growth

Complete service provider ready solution

Lowest total cost of ownership (TCO)

KEY FEATURES

Flexible network domain definition: IP, IP segment, AS number, AS path, BGP community, router interface, etc.

Traffic direction analysis

Application traffic analysis: business analysis, content analysis, CDN analysis, ICP analysis

BGP routing hijack and BGP routing oscillation detection

Low false positives, high performance

Easy to integrate and cohabitate

Efficient and intelligent protection from the botnet-based attacks wit

OVERVIEW

As a result of the rapid advancement of information technology (IT), 5G, cloud services, and the Internet of Things (IoT) have been widely applied in the organizations. However, it has also led to a significant growth of cyber-attack incidents often with disastrous and grievous consequences.

Organizations have already large amounts of funds into their IT infrastructure and security. But the continuously growing network complexity and constantly evolving threats continue to find ways to get through. Therefore, it is necessary to get insight into the network threats and adopt the corresponding security policy to guarantee business services run normally continuously, stably, and correctly.

The NSFOCUS Magic Flow (MF) Integrated Network Governance Platform delivers the broadest and most high-fidelity behavioral-based network analysis capabilities, paired with the integration of monitoring visibility, traceability, and threat intelligence.

NETWORK ANALYSIS

The core value of MF is that it can pinpoint malicious behavior that might be an early indicator of a larger security incident. Using a combination of behavioral modeling, machine learning, and threat intelligence, MF can process massive network flow to identify traffic directions, traffic components, and hotspot encrypted traffic, as well as to detect threats in large networks, providing all-around network-wide traffic analysis and handling capabilities for customers.

ATTACK DETECTION

The MF also provides a DDoS attack detection capability with centralized management according to the NSFOCUS Network Traffic Analyzer (NTA). It supports more than twenty-seven types of DDoS attacks identification. And the baseline self-learning function will provide a suitable threshold to satisfied different business network environment. And the flow detection support both of inbound and outbound traffic, even the encrypted data analysis to help customers gain advanced insight of their business services.

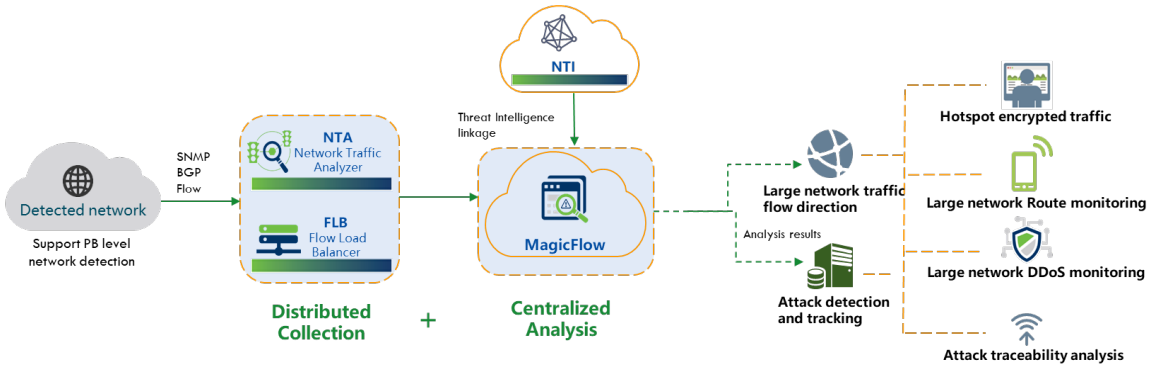
BUSINESS VISIBILITY

The MF offers visibility of large network traffic and popular applications. Based on the more than 4 billion+ threat intelligence library accumulated by NSFOCUS Threat Intelligence (NTI), it could directly analyze the encrypted network traffic of large networks environment and provide multi-dimensional monitoring and reporting. This viewpoint and capability allow

network administrator to understand how each application is performing over time, in context of everything else that is going on across the network environment.

THREAT TRACEABILITY

The MF provides real-time tracing function for each incoming network flow with GEO, organization, DNS, IP reputation and threat intelligence details. According to real-time attack situation monitoring and historical attack events tracing function, customers can proactively identify emerging threat vectors that provide the opportunity to create innovative, holistic, and positive mitigation and prevention polices to deal with the future network threats.



HOST CONFIGURATIONS REQUIREMENTS

Host	
Item	**Recommended Configuration**
CPU	At least 32 logical cores (2.6 GHz or above)
Memory	128 GB ECC DDR4
Hard Disk	2 x 500 GB SSD: RAID 1 configuration recommended 8–24 x 4 TB HDD (> 7200 RPM): RAID 0 or no-RAID configuration (such as Hadoop or Kafka) recommended * The server's disk drives cannot be configured as RAID 5 or LVM. *When the server's disk drives are in RAID 0, a separate group must be configured for each disk drive. *You must carefully check the status of disk drives and RAID. An error in RAID may cause MF to work improperly.
CD Drive	Built-in CD drive
Network interface card (NIC)	1 x 1000M management NIC and n x 1000M working NIC One additional 1000M NIC recommended for every 1 million flows/s, or directly using a 10G NIC
RAID card	RAID card with read/write cache, such as PERC H710p
Power Supply	Hot pluggable redundant power supply (1+1 redundancy), 1100 W
Operating system	64-bit OS only: CentOS 7.4 or later Recommended OS: CentOS 7.4 *Before installation, make sure that the host has only a new OS available, without unnecessary software; otherwise, MF installation would fail. *During OS installation, you should select Software Development Workstation; otherwise, MF installation would fail because of no dependency library.
Dependency library	The following libraries should be installed: Cyrus-sasl Cyrus-sasl-plain Libxml2 Libxslt Fontconfig Python 2.7 Java 1.8 or later

PERFORMANCE

Item	Single Deployment	Cluster Deployment
Concurrent Users	10	10*N
Analysis Capability	60k flow/s (enable threat traceability) 120k flow/s	Up to 1000K flow/s
Number of connected ports	40k	40k*N
Number of connected routers	25	128
Number of connected ports form single router	8192	8192*N
Number of configurable networks	200	4096
Number of supported IP addresses	3 million IP addresses per 30 seconds with 80 million total amounts	3 million IP addresses per 30 seconds with 80 million total amounts
Number of supported protocols	142	142
Number of matrix analysis creation	200	200*N