FLOWTRAQ

YOU HAVE THE DATA YOU NEED TO TIGHTEN UP ENTERPRISE SECURITY — BUT ARE YOU MAKING THE MOST OF IT?

Think of flow data as the "blood" that runs through your network. Like high white blood cell counts, high cholesterol and low platelet counts, flow data has its own set of criteria that indicate potential risks to your network health. These include traffic surges, unrecognizable IP addresses and other network anomalies. Whether you are using NetFlow, jFlow, sFlow or cFlow, you have valuable information that could provide you with visibility to shore up your network security. However, without the right tools to analyze your flow data, there's no way of quickly knowing when your network is at risk and what it's at risk from.

WHAT INFORMATION DOES FLOW DATA PROVIDE?

Flow data provides granular insight into your network that can help you diagnose a potential problem. With the right tools, a network administrator can determine the source and destination of network traffic, prominent peering relationships, and common bottlenecks. Specifically, flow records contain information about:

- **Source IP address:** who is originating the traffic
- **Destination IP address:** who is receiving the traffic
- **Ports:** the application utilizing the traffic
- **Class of service:** the priority of the traffic
- **Device interface:** how the traffic is being used by the network device
- **Tallied packets and bytes:** the amount of traffic
- **And more:** including packet timestamps

Most network operators use the data for performance monitoring and to understand who is using your network resources, what they're using it for, where they're using it, when they're using it, and how they're using it.

HOW DOES FLOW DATA IMPROVE SECURITY?

By analyzing flow data, network and security operations personnel can flag unfamiliar IP addresses (or IP addresses known to host malware), analyze distributed denial of service (DDoS) attacks, identify potential worms and botnets, track unusual data traffic patterns, find non-compliant users, and give you a detailed audit trail of all network activity. Flow analysis can also help you pinpoint unwanted data exfiltrations, identify causes of slowdowns, and spot where attacks or information leaks are coming from.

BOTNET PROTECTION

Once you learn your organization's typical network patterns, you can use your flow data to help detect network anomalies that often indicate botnets, rogue servers, unauthorized clients, or other network threats.

DDOS AND BRUTE FORCE ATTACK DEFENSE

A significant traffic surge can indicate a potential DDoS or brute force attack, two of the most common network threats around. DDoS attacks can make your websites, email, or other applications unavailable to your customers or employees, while a successful brute force attack allows a perpetrator, virus, or worm to penetrate your network with compromised credentials. By regularly analyzing your flow traffic you can recognize these types of malicious threats in real-time so you can immediately react to them and select the appropriate defense.

WORMS, SCANS, AND NETWORK RECONNAISSANCE PREVENTION

Worms propagate through your network by rapidly looking for hosts with common vulnerabilities and exploiting those weaknesses to spread throughout your network. By using flow data, this scanning behavior can be easily identified when several internal systems show the same bad pattern in rapid succession. This is a very common reconnaissance technique used by attackers, and can serve as an early warning for other more malicious attacks to come. Flow data can help you catch and control these incidents before they become a real problem.

DATA EXFILTRATION RECOGNITION

You may already spend time and resources searching for viruses on computers, blocking spam, and tracking down abuse. But it's not only worms and viruses that may be exfiltrating your most sensitive data, it could be anyone within your own walls. However, by monitoring flow data to detect anomalies, you can immediately recognize undesired uploads and data breaches from your network. This allows you to stop a leak before you face millions of dollars of cyber theft damages, lawsuits and public embarrassment, or before your CEO, CSO or CIO lose their jobs due to failed data security practices.

DATA BREACH DEFENSE

To spot potential data leaks or information security breaches, you can analyze network flow records to quickly recognize hosts initiating a connection, receiving data outside of normal thresholds, or exhibiting unexpected network behavior patterns. With the proper tools, flow data analysis can help you keep sensitive information safe from outside intruders and unauthorized insiders.

FINDING THE RIGHT FLOW ANALYSIS TOOL

There are two different types of software tools that collect flow data: aggregators and full-fidelity collectors. Aggregators periodically generate a pre-configured set of reports on the records they've collected and store them temporarily, giving you general insight into network traffic patterns and a sense of how busy your network is. But full-fidelity flow collectors store every flow record in a database, which allows you to filter and view the traffic after the fact and in much more detail than aggregators. If you want to analyze unique traffic patterns, investigate never-before-seen attacks, and prepare your organization for sophisticated network attacks, you will need a full-fidelity flow collector. Full-fidelity collectors allow the skilled analyst to become truly effective at keeping the network safe and secure.

ABOUT FLOWTRAQ

FlowTraq® provides software and services for high-performance network monitoring, analytics, security and forensics to detect a range of network behaviors, including distributed denial of service (DDoS), brute force attacks, botnets, worms, network scans and other network traffic anomalies. To request a free trial of FlowTraq, visit **www.flowtraq.com/trial**.

FLOWTRAQ

16 Cavendish Court, Lebanon, New Hampshire 03766
Phone +1 (603) 727-4477 | Email info@flowtraq.com