Understanding NetFlow Monitoring, Security, and Forensics

By: Dr. Vincent Berk and Dr. John Murphy

Table of Contents

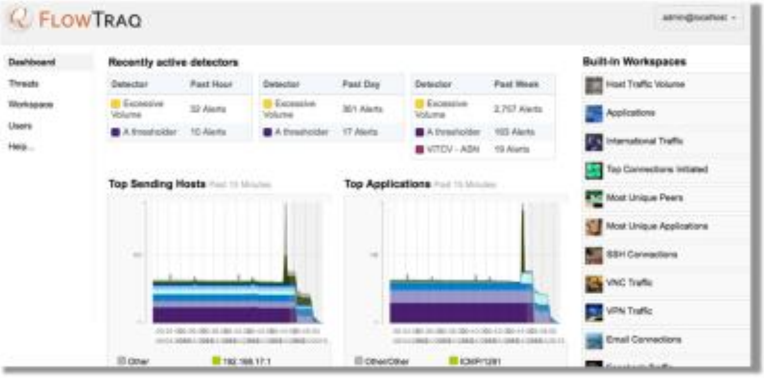
"If you can't measure something, you can't understand it. If you can't understand it, you can't control it. If you can't control it, you can't improve it."

~ James Harrington

1. Introduction to NetFlow

NetFlow represents the conversations that make your business work: emails, web requests, VoIP calls, file transfers, and all the low-level back-and-forth that makes a network a network. Among these conversations are also attacks: spam, scanning, malware, data exfiltrations, and other potential threats.

Cisco, the inventors of NetFlow, describe it as a phone bill for your network[2]: a listing of all the conversations that take place on your network, whether hours-long or milliseconds-long. Unlike an ordinary phone bill with hundreds of conversations, however, there are not hundreds of conversations but there are thousands or millions of conversations at any one time. These conversations are the ebb and flow of data and control of a modern computer network, embodying the business processes that your network is supporting. The size of the conversation does not matter: a single-kilobyte communication can be as important to the operation of your network as a multi-gigabyte download.



Recently active detectors

Detector	Past Hour
Excessive Volume	32 Alerts
A thresholder	10 Alerts

Detector	Past Day
Excessive Volume	301 Alerts
A thresholder	17 Alerts

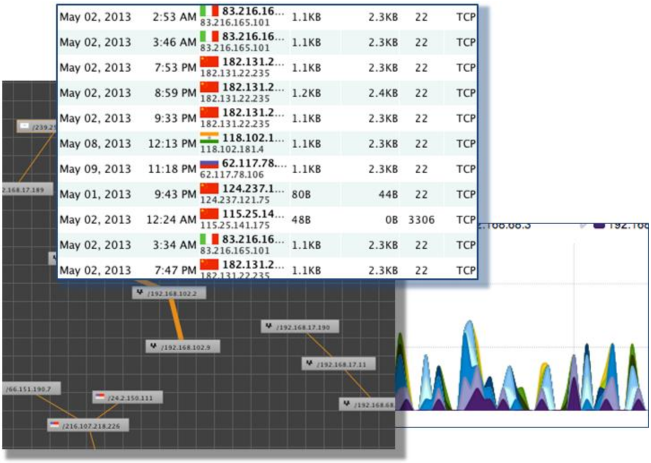
Detector	Past Week
Excessive Volume	2,757 Alerts
A thresholder	103 Alerts
VITDV - ASN	19 Alerts

[2] "CISCO IOS NETFLOW AND SECURITY", Internet Technologies Division, Feb 2005

A properly-deployed NetFlow solution gives you excellent visibility into your network, providing the best available balance between scope and depth. NetFlow by itself gives you an excellent view, but combined with the proper analytical tools it gives you unparalleled control over your network. Products like FlowTraq can help analyze bottlenecks, identify security threats to your organization, and allow in-depth audits of past traffic.

2. Network Auditing and Accurate Billing

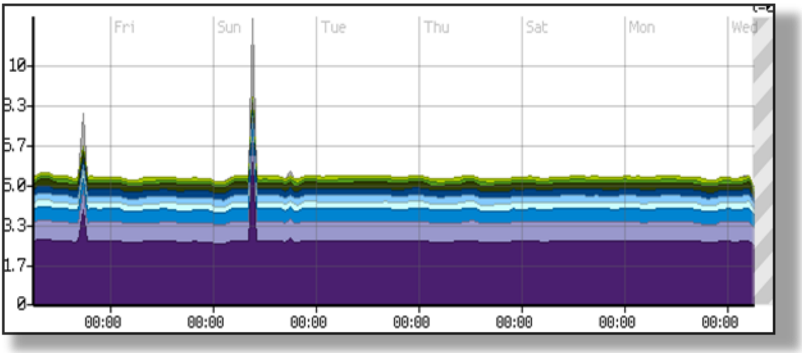
Different networks have different record-keeping requirements. If you handle medical records you are required to show HIPAA compliance. If you handle credit card details you must maintain PCI compliance. In all cases you are required to track the flow of data to and from the systems that process this vital information, showing all accesses, even the smallest.



May 02, 2013	2:53 AM	83.216.16... 83.216.165.101	1.1KB	2.3KB	22	TCP
May 02, 2013	3:46 AM	83.216.16... 83.216.165.101	1.1KB	2.3KB	22	TCP
May 02, 2013	7:53 PM	182.131.2... 182.131.22.235	1.1KB	2.3KB	22	TCP
May 02, 2013	8:59 PM	182.131.2... 182.131.22.235	1.2KB	2.4KB	22	TCP
May 02, 2013	9:33 PM	182.131.2... 182.131.22.235	1.1KB	2.3KB	22	TCP
May 08, 2013	12:13 PM	118.102.1... 118.102.181.4	1.1KB	2.3KB	22	TCP
May 09, 2013	11:18 PM	62.117.78.... 62.117.78.106	1.1KB	2.3KB	22	TCP
May 01, 2013	9:43 PM	124.237.1... 124.237.121.75	80B	44B	22	TCP
May 02, 2013	12:24 AM	115.25.14... 115.25.141.175	48B	0B	3306	TCP
May 02, 2013	3:34 AM	83.216.16... 83.216.165.101	1.1KB	2.3KB	22	TCP
May 02, 2013	7:47 PM	182.131.2... 182.131.22.235	1.1KB	2.3KB	22	TCP

If you monetize your network by hosting networked services, you will need to track bandwidth use accurately to determine usage-billing. Relying on 95th percentile billing can be risky: it can be gamed, and you can miss spikes in traffic that degrade performance to other customers.

Clear and readable reports form the backbone of your audit trail or billing service. FlowTraq is unique in that it collects and stores flow data without aggregating, allowing fine-grained control over user access.



Multi-tenancy is at the core of the FlowTraq system. Individual end-users can be restricted to access only the traffic relevant to them. FlowTraq allows arbitrary virtual compartmentalization of a data store without limiting analysis capability.

3. Scalable Deployment: From Micro to Mega

Whether your network comprises a small office or a global network of office buildings, your NetFlow solution should scale to fit you.

Big Data? Big Benefit

The more you know about your network, the better prepared you'll be for the decisions you'll need to make:

- Is your web service suffering a denial of service attack? Are all of your backups made on time, every time?

- That foreign IP address that is currently trying a brute-force attack against a system in your Chicago network: has it contacted any of your other networks today? (Last week? Last year?) Are they trying blindly, or did they perform any reconnaissance first?

- Can you reduce load on your Boston servers by moving functionality to San Francisco, or do they experience peaks at the same time?

Big networks, multi-site networks, and datacenters are challenging to secure and manage. Designed from the ground up to deal with large data volumes, FlowTraq can be distributed over a cluster to achieve scalable access to flow analysis, without enforcing a central bottleneck.

Lean and Mean? Why Pay More?

If your needs are modest, hardware-based NetFlow solutions can be a bitter pill to swallow: tens of thousands of dollars for a rack-mounted unit capable of ten times your required capacity. FlowTraq Cloud offers all the benefits of an enterprise NetFlow solution, while charging only for true usage. FlowTraq’s Cloud service collects network flows to a secure cloud platform. No need to manage physical servers. No need for extra staff. No need to pay a penny too much, even as network needs expand.

4. Insight into Virtual Networks, Virtual Machines, and Mobile Devices

A modern computer network encompasses a wide variety of Internet-capable devices, not all of them physical, joining and leaving your network in almost no time at all. The network infrastructure itself can change drastically with just a few keystrokes, without moving even a single wire of your physical infrastructure. NetFlow keeps pace with these changes and more.

Virtual Networks

The ability to rapidly deploy virtual networks and virtual hosts has been a game-changer for many companies, allowing unprecedented flexibility. NetFlow deployment is fast enough to keep pace: the minute your virtual network goes live, so does your NetFlow export. FlowTraq can quickly drill down into the traffic that matters, view and report on it, filter it, set up alerts, and profile its behavior with FlowTraq NBI. See at a glance the flow and balance of traffic between VLANs, and watch for spikes or failures–or set FlowTraq to alert at threshold breaches and anomalies.

Mobile Devices

Cisco's 2013 Annual Security Report saw the number of exploits targeted at Android mobile devices increase rapidly. Though still a small portion of the overall network traffic, a monitoring plan that does not take these devices into account risks being taken unaware.

Mobile devices are particularly difficult to monitor because they move rapidly from network to network, are not easy to instrument, and do not have easily accessible log files. NetFlow provides a convenient and robust means of monitoring these devices when they associate with your wireless networks. By using FlowTraq's MAC address support you can track mobile devices as they move from network to network, profile their behavior, and pick up on anomalies.

5. Network Forecasting and Planning

Networks grow. Whether your site is getting more popular, your team is expanding, your partners start preferring video conferences to voice calls, or the size of the average web page is increasing; the only certainty is that you will need more bandwidth. But where?

Long-term NetFlow trends can tell you where resources are most likely to be needed most urgently. They can tell you which traffic is dominating your network and, at a glance, show you the rates at which it's increasing. This makes it easy to spot potential bottlenecks and strategically plan for expansion.

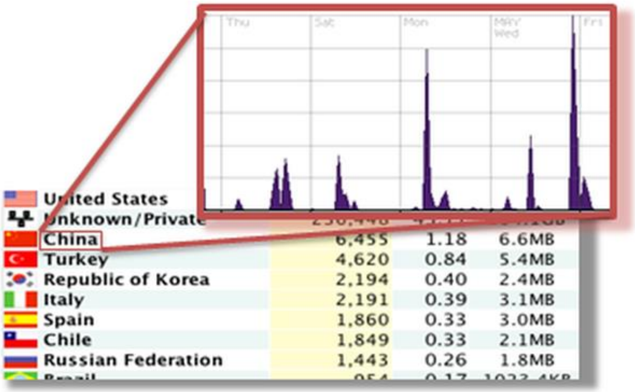
> "When you can measure what you are speaking about, and express it in numbers, you know something about it. When you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely in your thoughts advanced to a stage of science."
>
> *~William Thomson, Lord Kelvin*

You may even be able to optimize bandwidth without spending a dime. FlowTraq provides pair-wise statistics for IP addresses, Autonomous Systems, VLANs, and Interfaces. In some cases bandwidth can be improved by reorganizing your network so that high-volume pairs are routed more efficiently.

6. Data Exfiltration

In today's digital world data is at the core of your company. In order to operate you must collect, store, and protect your data from exposure. Your ultimate challenge is to avoid your most *toxic data* from leaving your network.

There are many places in your computer systems where hackers, rootkits, and viruses can hide away. There is no guarantee you will ever find them. Computer systems are getting ever bigger and more complex, making it easier and easier for them to hide. The ultimate bastion of defense against data exfiltrations is the network: once data is on the move, FlowTraq will record it.



United States	[illegible]	[illegible]	[illegible]
Unknown/Private	[illegible]	[illegible]	[illegible]
China	6,455	1.18	6.6MB
Turkey	4,620	0.84	5.4MB
Republic of Korea	2,194	0.40	2.4MB
Italy	2,191	0.39	3.1MB
Spain	1,860	0.33	3.0MB
Chile	1,849	0.33	2.1MB
Russian Federation	1,443	0.26	1.8MB
Brazil	954	0.17	1023.4KB

Whether a large bulky upload, or a slow trickle over a long time, FlowTraq makes it easy to track how much data leaves your network and where it's going. FlowTraq provides extensive behavioral profiling, complex filtering, and many other tools to pinpoint potential exfiltrations and help you put a quick end to them.

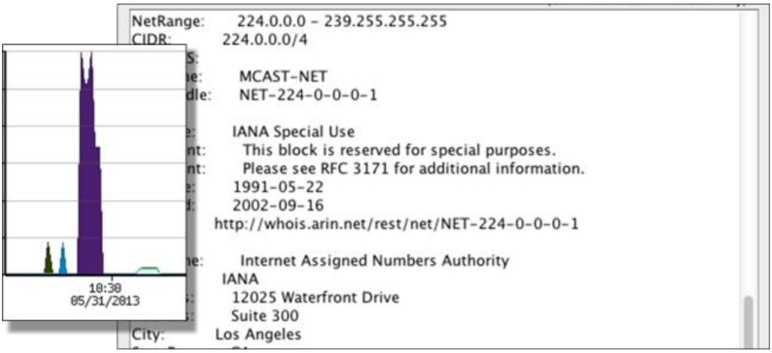
7. Full History Attack Investigation

The malware detection industry is smart and fast. But it's not instantaneous. Oftentimes a new attack can run undetected for months (or in the case of Flame, years).

Toxic Data (n) That information owned or managed by your company, the leak of which will indelibly tarnish your reputation: credit card numbers, medical records, financial records, personnel files, etc.

Typically, infectious malware contacts dials home by contacting their Command and Control server early in the infection and then stay quiet. Once your virus scanners and IDS signatures are updated you will be watching fresh traffic. You will not, however, expose existing cases. FlowTraq catches command-and-control communications, which are often quite small and overlooked by traditional Aggregating NetFlow Products. FlowTraq was designed to give the insight needed to find the nastiest lingering threats.

A full-fidelity NetFlow search is therefore critical to finding these lurking infections. Even long after the initial infection, FlowTraq can still find the original conversations. Once an initial C&C connection is identified, the spread can be tracked through the network to determine exactly which systems are affected and require cleaning.



```
NetRange:     224.0.0.0 - 239.255.255.255
CIDR:       224.0.0.0/4
           S:
           e:      MCAST-NET
           dle:    NET-224-0-0-0-1

           e:     IANA Special Use
           nt:     This block is reserved for special purposes.
           nt:     Please see RFC 3171 for additional information.
           e:     1991-05-22
           d:     2002-09-16
                http://whois.arin.net/rest/net/NET-224-0-0-0-1

           e:      Internet Assigned Numbers Authority
                IANA
           s:     12025 Waterfront Drive
           s:     Suite 300
City:           Los Angeles
```

Were you targeted by the Chinese military for spear-phishing? L at: *www.flowtraq.com/spear-phishing*

8. Detection and Remediation

Denial of service (DDoS) attacks overwhelm a network or service with a flood of fake requests. The goal is to make it harder, and even impossible, for legitimate customers or users to connect to and use your service.

Hostile actors often use large botnets – a network of compromised systems under their control--to pummel a target. Frequently they make use of third-party servers as multipliers and to shield themselves from scrutiny. FlowTraq's sophisticated NBI tools are designed to help you determine the best mitigation strategy for DDoS attacks.

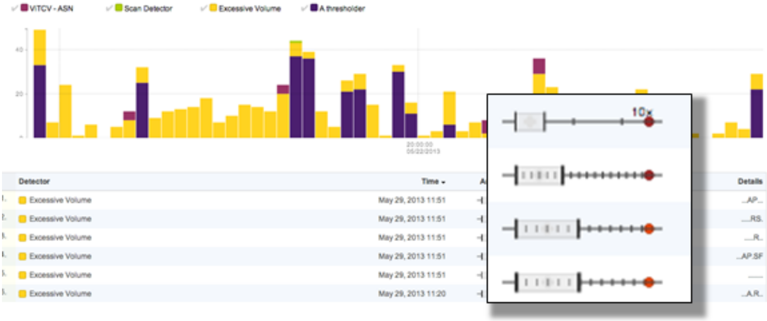
The flip side of this coin is also an issue: is your network participating in a denial of service attack against someone else? Is your equipment part of a malicious botnet? Compromised hosts can be discovered by using FlowTraq's Behavioral Fingerprint Generator, which uses machine learning techniques to track computer systems' behavior over time and determine when new behavior patterns are out of the ordinary.

9. Network Behavioral Intelligence

The security guard or receptionist in your building knows the habits of people who work there. They know delivery schedules and the usual drivers. They know which doors are usually kept closed. They know this even though things change over time. There's a difference between what's *usual* and what's *unexpected*. Recognizing the *unexpected* has saved employers from theft, arson, and other losses on countless occasions.

Protecting a computer network from data theft and data leakage requires the same knowledge of the usual and expected so you can spot the unusual and unexpected. Computers and mobile devices have very predictable patterns of behavior. For instance, Web servers serve predictable amounts of content, and email volumes vary predictably by time of day. Deviations from the norm can indicate DDoS attacks, worms, viruses, and data exfiltrations.FlowTraq uses NetFlow to expose these behaviors in the millions of connections that are made in a computer network.

By using powerful Network Behavioral Intelligence technology to automatically learn what is usual and expected in large volumes of traffic, FlowTraq is your always-aware, always-learning network security guard.



	Detector	Time ▾	A	Details
1.	Excessive Volume	May 29, 2013 11:51		...AP...
2.	Excessive Volume	May 29, 2013 11:51		...RS.
3.	Excessive Volume	May 29, 2013 11:51		...R..
4.	Excessive Volume	May 29, 2013 11:51		..AP.SF
5.	Excessive Volume	May 29, 2013 11:51		....
6.	Excessive Volume	May 29, 2013 11:20		..A.R..

Threats are managed through an innovative ‘Anomaly Index’ that shows you at a glance how unusual the behavior is, and how confident FlowTraq is about the anomaly. This allows you to quickly prioritize alerts and focus your time where it is most needed.

10. Summary

These are only some of the benefits of NetFlow and FlowTraq for your company’s security, mission, and bottom line. Give it a try, free and completely unrestricted, and see for yourself just how much better your network can work for you.

Related Resources

More articles online – www.flowtraq.com/whitepapers

Watch FlowTraq in Action - www.flowtraq.com/demo

Online Tutorials - www.flowtraq.com/tutorials

Free 14-Day FlowTraq Trial - www.flowtraq.com/trial

About the Authors

Dr. Vincent Berk, CEO of ProQSys, has 15 years of IT security and network management experience, and is the designer of the FlowTraq system. He is a member of the ACM, the IEEE.

✉ vberk@flowtraq.com

in linkedin.com/in/vincentberk

t @flowtraq

Dr. John Murphy, ProQSys Network Security Researcher, contributes his expertise of network security, attack graphs, insider threat detection, and malware analysis to the development of FlowTraq. He is a member of the ACM and IEEE.

✉ jmurphy@flowtraq.com

in linkedin.com/pub/john-murphy/8/a35/754

Thank you for taking the time to read this reference. I hope this information presented is valuable to you now and continues to be a handy reference tool going forward.

Let us know what you think. We would love to hear and discuss your thoughts and opinions. You can always visit www.flowtraq.com for more information, or contact us directly.

About FlowTraq

FlowTraq, by ProQSys, is network security software that uses full-fidelity network flow records to provide unified security, monitoring, and forensics.

Its behavioral analytics and alerting helps IT administrators identify and investigate data leaks, compromises, spammers, botnets, worms, and DDoS attacks in high-volume networks. FlowTraq monitors network performance and bandwidth consumption, catalogs applications in use, and detects problematic changes in network activity.

Designed to complement and improve existing network security operations, it can be deployed stand-alone or in a cluster, enabling it to offer its forensically accurate analytics at any bandwidth level.

Please visit www.flowtraq.com for more information.

All other company and product names may be trademarks of their respective holders. While every effort is made to ensure the information given is accurate, ProQSys does not accept liability for any errors which may arise. Specifications and other information in this document may be subject to change without notice.