FlowTraq

KEEP YOUR NETWORK HEALTHY:

FIVE NETWORK VITAL SIGNS TO MONITOR

Vital signs are measurements of the body's most basic functions. The main vital signs routinely monitored by healthcare providers include body temperature, heart rate, respiration rate, and blood pressure. The first step in diagnosing an illness is to check for changes in your vital signs. What's most interesting about vital signs is often not their specific value, but the change in value over time for a given patient. If vital signs such as blood pressure or temperature rise, it's a reliable indicator that further testing may be needed to find the root cause of an impending illness.

The same is true of your enterprise network. There are a number of vital signs that you should monitor, and you need to know what changes to watch for. Here are five key network vital signs you should be monitoring.

1. NEW CLIENTS AND SERVERS

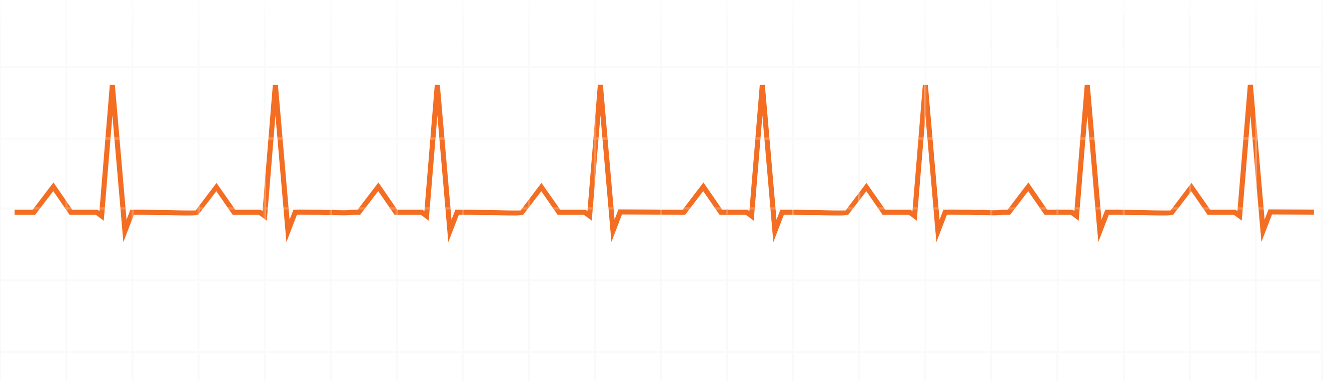
What to look for: There are lots of servers and clients on your network — and new ones being legitimately added as part of regular business operations. New rogue servers on the network and unexpected clients communicating with those servers could be a sign that something is wrong.

Diagnosis: A new, unknown file server on your network could be a sign that someone is trying to exfiltrate information. A new SubSeven/Back Orifice/SVN server could indicate a backdoor used by a hacker. A new Web server could mean illegal file sharing.

2. SCANS

What to look for: Unusual or increased scanning behavior on the network could indicate that your systems have been compromised and you need to find and stop the perpetrators fast.

Diagnosis: Scanning for open and available services is a common reconnaissance technique used by hackers who have found a way to infiltrate your network. Worms often resort to random scanning to find other systems to spread to.



3. BLACKLISTED COMMUNICATIONS

What to look for: There are a number of hosts that are known to be botnet or malware distribution channels. Any communication within your network to those bad or suspicious hosts likely spells trouble.

Diagnosis: A communication with a known bad host could mean that malware is being downloaded or even that the attacker has already found a way into the network and is establishing additional control and exploits.

4. VOLUME-BASED ACTIVITY

What to look for: There's a high volume of traffic flowing through your network pipes on a continuous basis. Unusual increases in network traffic and connections could represent an amplification, SYN flood, smurf/fraggle, slowloris, Christmas tree, LAND, IP/TCP NULL, or other attack.

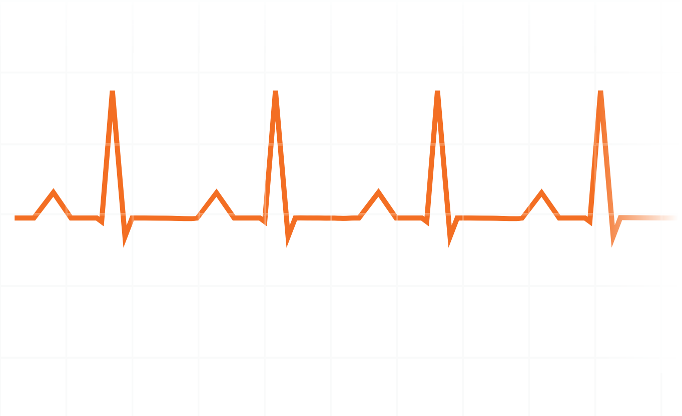
Diagnosis: These types of traffic patterns signal a potential in-progress DDoS attack that could take down your systems, so you need to be able to detect, classify, and mitigate them fast.

5. DATA EXFILTRATION

What to look for: Data is routinely accessed and transferred out of your network. Unusually high volumes of data leaving the borders of the network — especially sensitive data such as customer/employee personal information, credit card data, or intellectual property — need to be investigated immediately.

Diagnosis: This could be a sign that someone is stealing data. There has been **a data exfiltration epidemic** of late. And when, as is too often the case, organizations discover that they have been hemorrhaging sensitive data for years, the financial and reputational fallout can be devastating.

New clients and servers, scans, external communications, and data transfer are all routine events on high-volume enterprise networks. The fact that they are happening isn't a sign of a problem, just like having a temperature or a heart rate doesn't mean you are sick — it's just part of your body's function. But when those activities change in volume or pattern, much like an elevated temperature or irregular heartbeat, it's a sign that there could be something wrong. Your network's vital signs are an early warning system, and monitoring them allows you to quickly identify and address changes so you can keep your network healthy.



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 USA
Phone +1 (603) 727-4477 | Email info@flowtraq.com