IP Copper™

Network and Data Security Solutions

PANORAMIC FORENSICS

A new concept in network monitoring

INFORMATION SECURITY: ELUSIVE GOAL, INVALUABLE PROCESS

Network and data security is a process, rather than a destination. While it is admirable to keep security as a conceptual goal, it would be a mistake to succumb to the illusion of actually having achieved it. Information security as a reachable destination or goal is an illusion, a mirage that recedes into the distance, despite the steps taken achieve it. True security is a balanced combination of personnel, technology, planning and process.

Network security is a moving target. Successful implementation of personnel guidelines, technology and processes rely on a reasoned valuation of the organizations assets and planning informed by actionable data, i.e., operational information on the exact workings and activities of a network. The first step towards securing a network is knowledge of the network's activity. The concept of panoramic forensics provides a comprehensive and effective framework for gathering network information at both the entryways into the network and within the network itself, that is, both internet and intranet.

PANORAMIC FORENSICS

Panoramic forensics can be likened to video surveillance. Most video surveillance systems incorporate multiple cameras covering multiple areas of the subject premises; likewise, panoramic forensics involves placing network monitoring and recording equipment at various network points to monitor activity between network segments and at the network's points of entry. With today's threat environment and the evolution of advanced persistent threats (APTs), monitoring and recording the activity only at the network perimeter no longer suffices.

Different network segments may not require the same levels of monitoring or same permanency of the recorded data. For a high value asset, such as a server that houses customer records or intellectual property, the historical record should span a longer amount of time (perhaps with the recorded data retained permanently) than for a lesser value asset. Network activity recording and monitoring at an entry-point into the network should be continuous and long-term, as stolen data is most likely to leave and secret commands to any compromised equipment to come in through a network's connections to outside.

Recording and monitoring the various segments of a network achieves unprecedented visibility into network activity from multiple, overlapping vantage points. Should an APT gain a foothold in one network segment, with the internal visibility made possible by panoramic forensics, its scope and attempts to spread beyond the original affected network segment to a more high-value asset could be detected by its intranet activity, even if the APT was overlooked when it initially entered the network and infected the original network segment.

With the overlapping nature of panoramic network surveillance, the data on one recording device serves to authenticate and corroborate the data captured on another device. Should a legal action or prosecution become necessary, the multiple recorded instances of a breach, theft or other compromise strengthen the forensic evidence.

The steps for setting up a system for panoramic forensics are:

1. Identify assets and vulnerabilities.
2. Install monitoring equipment for both assets, of a class or cost commensurate with their value, and vulnerabilities, of a class or cost commensurate with their likelihood of exploitation.
3. Implement a plan to regularly review the recorded data captured by the monitoring equipment.
4. Create a process for investigating and addressing any discovered anomalies or suspicious activity.
5. Periodically revisit the security-monitoring plan to adjust for changes in assets, vulnerabilities and network topology.

Panoramic forensics, like any network forensics implementation is not a static, one-time solution to checkmark off the list and forget. The most effective network managers approach panoramic forensics as a process, to be modified as the network changes and threats to the network evolve.

SPAN vs. Pass-through

Whether it is best to place a packet capture appliance in a SPAN or pass-through configuration depends on the activity targeted for recording. To simply capture the flow between two points on the network, setting up the appliance as a pass-through device is easy and effective (and does not require a router or switch with SPAN/mirror ports).

In a different situation, in which a workgroup connects to the rest of the network via a router, it may be advantageous to capture both the activity within the workgroup and the activity between the workgroup and the rest of the network. A packet capture appliance placed on the SPAN port of the workgroup's router would capture and record both the transmissions between the workgroup and the rest of the network and the network activity between workgroup members themselves. This set-up is also helpful for matching up the activity of local workgroup DHCP addresses with the transmissions sent out to the rest of the network (since the individual workgroup members' internal DHCP assignments would be masked by the workgroup router's DHCP assignment on the larger network). The ability to match up the communications from a workgroup to the

larger network with the individual workgroup computer that originated the transmission helps ascertain which specific computer sent a particular communication.

Equipment for Panoramic Forensics

Network recording, commonly known as packet capture, comes in a variety of "flavors", ranging from software to hardware, from short-term to long-term, and from complicated to simple. For a network security process incorporating panoramic forensics, the best and most effective packet capture is accomplished using packet capture appliances that are compact and easy to install, requiring no changes in network topology to implement. The goal of network forensics is not to re-do the network or disrupt its netflow in order to make the equipment work, but to be able to install monitoring equipment wherever needed and at will, without distorting the network.

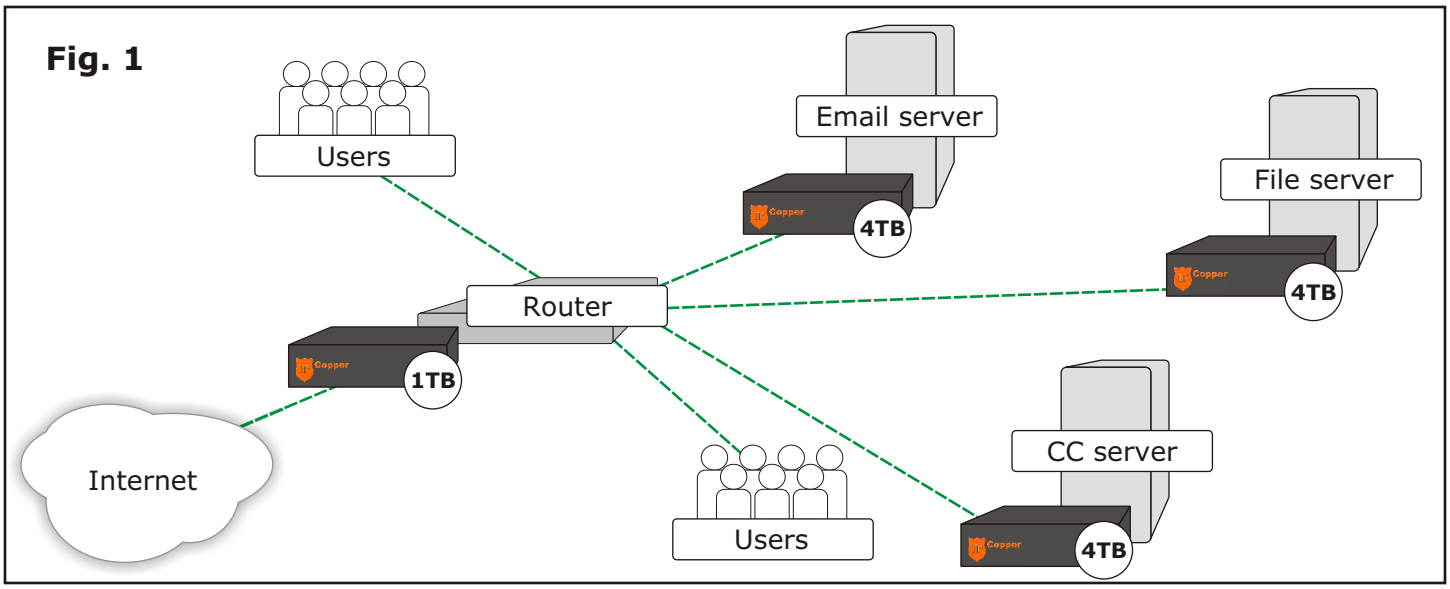
Two other considerations when choosing a network packet capture appliances are storage capacity and whether the data is retained permanently and cannot be deleted or overwritten, or whether the oldest data is overwritten with the newest once the appliance reaches capacity. The answers to these questions depend on the volume of network activity and what is being monitored. In some cases it may be sufficient to retain only the most recent one or two terabytes of data, while in other cases it would be prudent to permanently record and store all activity, with no possibility for it to be overwritten.

One last consideration is format. Your packet capture appliances should be capable of exporting data in a format such as PCAP, which is compatible with a large variety of security tools and analysis programs.

Sample Panoramic Forensics Implementation

In one sample implementation of panoramic forensics (fig. 1), an organization with one internet connection and three assets (e.g., an email server, a file server and a credit card processing server) deploys one packet capture appliance that retains data permanently at the point of connection to the public internet and one appliance that retains only the most recent 4 TB of data in front of each of the three assets. In this fashion, the organization has a permanent record of all activity that comes in and goes out via the internet connection, while also individually monitoring their three network assets.

In another implementation (fig. 2), an organization with multiple incoming internet connections and a large number of network segments (for different workgroups or departments) deploys one packet capture appliance that retains data permanently on the SPAN port of the router through which all internet connections run and one appliance

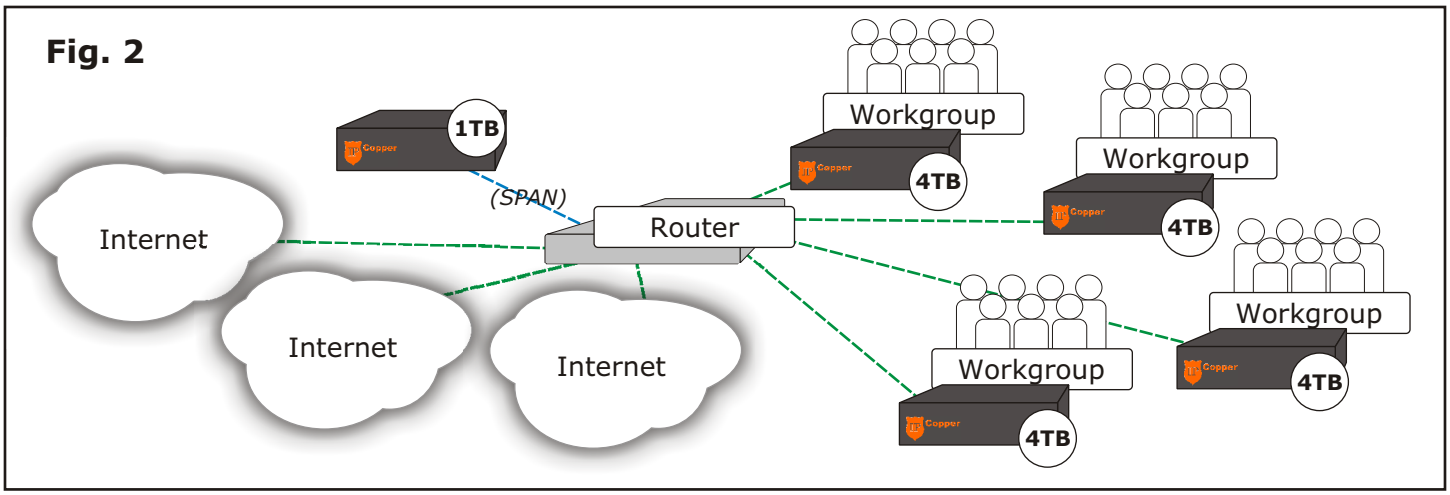


that retains only the most recent 4 TB of data between each network segment and the rest of the network. This organization also has a permanent record of all activity that traverses the internet connections along with records of the most recent activity between the various network segments. An alternate configuration for this organization, in which the packet capture appliance is used as a pass-through device, is shown in fig. 3.

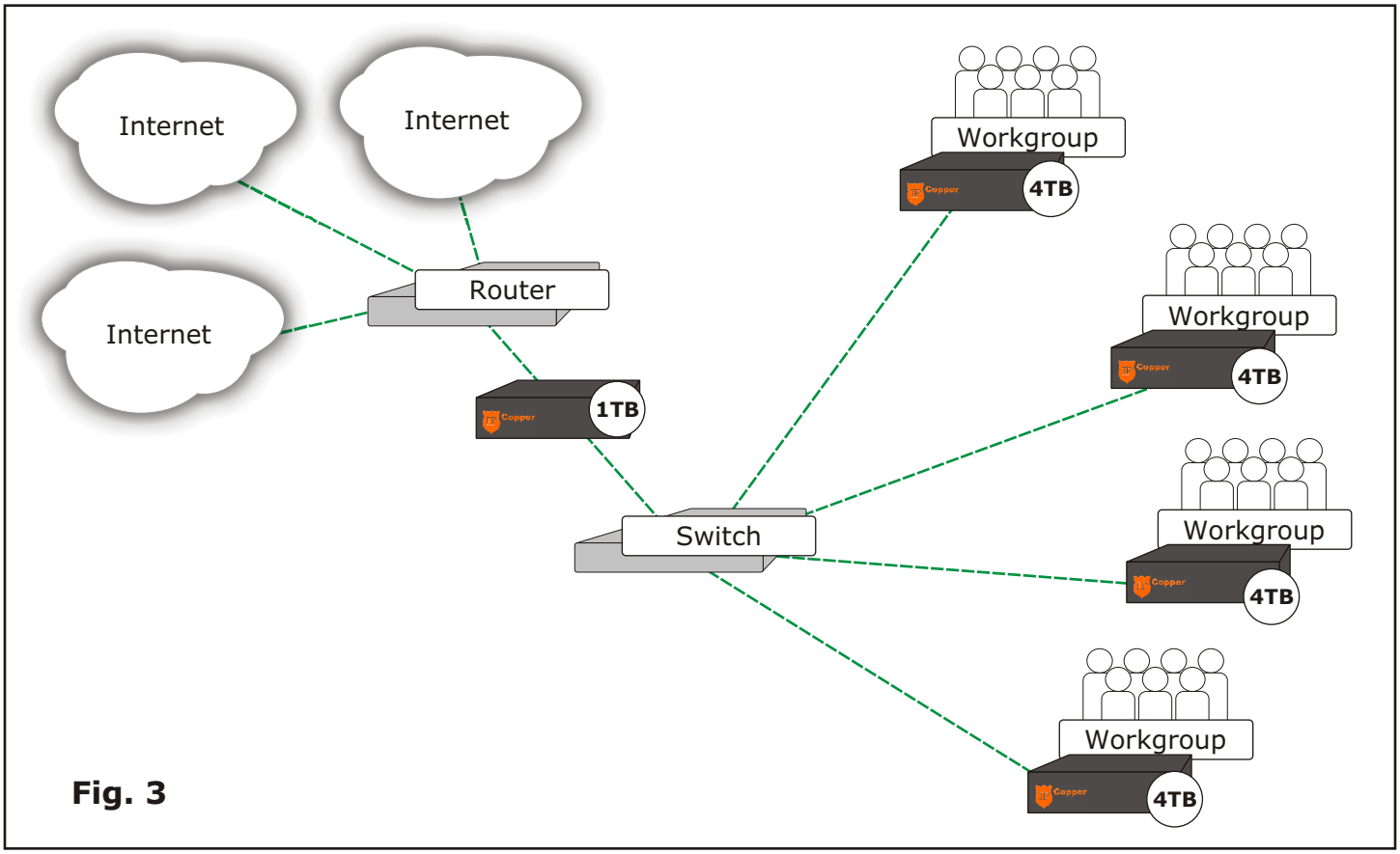
In both implementations, the organizations have several points on their networks from which to detect suspicious activity. The appliances at the internet connection(s) monitor the "gates," while the other appliances placed around the network monitor the intranet, capturing any suspicious activity within the network that may be due to insider error or malfeasance or due to compromised or infected equipment attempting to spread from one network segment to another.

INFORMATION AND VISIBILITY ARE THE KEY TO DEFENDING AGAINST NEXT GENERATION THREATS

IT security personnel live with an ever-evolving threat landscape. Every year the types of threats become ever more varied and ever more numerous. The current next generation threats are complex and multi-dimensional: persistent, zero-day, multi-vector, ever-evolving and port independent. And the worst of these are the ones that network administrators, IT security experts, and firewall and AV vendors do not know about. Tackling the threats presented by today's threat environment (and tomorrow's) involves a comprehensive and flexible security framework built upon situational awareness. Network situational awareness can only be achieved through knowledge of the network's activity, both internet and intranet. Implementing a comprehensive



In Fig. 2, the packet capture appliance that records the activity in and out of the internet connections is connected via the SPAN port on the router. In the diagram below, the packet capture appliance that records the activity in and out of the internet connections is located in between the router (to which the internet connections connect) and the switch that connects to the individual network segments. In both configurations, the packet capture appliances capture and record essentially the same information.



IP Copper™ Packet capture appliances

panoramic forensic structure throughout a network provides the information leading to situational awareness, threat detection, intelligent incident response and effective prevention techniques.

Best of Class Network Forensic Technologies

Effective network forensics requires personnel, technology and process. While a variety of tools and skills exist to analyze network information, those cannot work effectively without best of class data gathering tools. The 100% packet capture rate, historical activity record, gigabit speeds and stealthy profile of IPCopper USC Series network forensic solutions provide the informational foundation for comprehensive forensic analysis, threat assessment and detection.

Network forensics from IPCopper, Inc. illuminates past and present network traffic, giving a full timeline of network activity from the moment it starts recording. Find any data transmission or IP packet in its entirety, including packet headers and payloads – this comprehensive record enables network administrators and investigators to understand the full scope and impact of any network event, as well as reconstruct the event as it progressed from start to finish, not the least of which is determining which, if any, data was compromised.

IPCopper USC Series Network Forensics Appliances

The IPCopper USC Series of network forensics appliances capture, record and make visible all data that traverse them. Based on a proprietary operating system, the series currently includes 1 TB, 2 TB and 4 TB models that can sustain full packet capture at speeds up to 1 Gbps. IPCopper USC forensic appliances are hardware packet capture solutions, designed to be deployed anywhere on a network without affecting network topology, speed or flow. Regardless of where placed on the network, either inline or on a switch's SPAN port, IPCopper USC appliances unobtrusively record network activity, without affecting the network or the packets. Utilizing neither an IP nor MAC address, electronic invisibility hides the IPCopper USC's present from remote or local snoopers, while 20,000 bit encryption provides an extra, robust layer of security for your recorded data.

One of the newest IPCopper packet capture appliances is the USC1030, a truly forensic class appliance. The information captured and recorded to its 1 TB memory cannot be deleted nor overwritten, ensuring the integrity of the captured data. If needed, the data captured and recorded by the USC1030 can be tested and authenticated by our lab. Additional security features include a sealed, tamperproof 12-gauge metal case and the electronic invisibility featured in all IPCopper packet capture appliances.

Dedicated Packet Capture, Immediate Accessibility

IPCopper packet capture appliances are specifically designed to deliver uninterrupted and unaltered network packet capture for network forensics. The appliances automatically capture, encrypt and store all data packets that cross the network, even at speeds of 1 Gbps. Basically, IPCopper appliances take the network data packets, encrypt, timestamp, sequence and then record them to memory in exactly the same order and composition as received.

Once captured and recorded, a packet or stream of packets may be immediately downloaded and reviewed, without affecting the appliance's continued operations or impacting network performance. IPCopper USC appliances export data into the widely-used PCAP format, compatible with a large number of network forensic analysis and other network security tools.

PUTTING NETWORK FORENSICS IN PERSPECTIVE

The goal of any network forensics framework, and panoramic forensics in particular, is to accurately and unobtrusively collect and retain all network activity. With a record of network activity taken from various network points, network security administrators can develop network intelligence, that is, actionable information with which to determine network performance, evaluate network vulnerabilities and improve network security processes. In addition, having a complete, unaltered and unfiltered record of network activity is invaluable for conducting effective, thorough and quick incident response and for investigating the scope and timeline of a breach or other network anomaly.

In today's network and internet environments, IT security administrators and network managers must look to the network future with an eye informed by an accurate rendering of the network past. A prepared network not only keeps appropriate defenses in place against intrusions, but also implements appropriate information gathering tools. Even with the best equipment, breaches happen and the only solution is to continuously monitor and record network activity. In the event post-network incident analysis becomes necessary, a panoramic forensic solution using continuous, 100% packet capture guarantees that you will have the information you need to discover, investigate and mitigate.

ABOUT IPCOPPER, INC.

IPCopper, Inc's line of high-speed network packet capture appliances offer long-term, reliable, continuous packet capture for standard and panoramic forensics applications. IPCopper packet capture appliances include 1 TB, 2 TB and 4 TB models that capture, encrypt and record 100% of your network activity at speeds up to 1 Gbps, with upcoming 10 Gbps models and 8 TB and 12 TB models under development. The data is accessible in PCAP format for use with any network security, compliance, analysis or other network management applications and equipment. All IPCopper packet capture appliances are designed and manufactured in the USA.

IPCopper, Inc. is headquartered in Portland, Oregon. For more information on IPCopper products, please visit http://www.ipcopper.com.

Contact Us

IPCopper, Inc
707 SW Washington St #1410
Portland, OR 97205

phone: 503-290-0110
fax: 503-290-0111
email: sales@ipcopper.com