Utilizing Virtual Network Taps to Increase Visibility into Virtualized Control System Networks

Nikolas Upanavage
Bechtel NS&E
ICS Cybersecurity Technical Center
naupanav@bechtel.com

Patrick Orr
Bechtel NS&E
ICS Cybersecurity Technical Center
pjorr1@bechtel.com

ABSTRACT

Situational awareness is a popular topic in safety and quality messages and practice at Bechtel. Being cognizant of your surroundings and the activities taking place can make a dramatic difference when faced with an unsafe situation. Network visibility provides situational awareness in an Industrial Control System (ICS). Securing a process control network without understanding the flow of network traffic, and who is communicating on the network, is like providing physical security to a facility without using cameras. Many projects tend to use physical passive network taps to forward network traffic to endpoint tools used to monitor and detect malicious behavior.

Using physical network taps is a great first step in achieving the goal of ICS network visibility. However, as more ICS vendors incorporate virtual machines into their designs, an additional layer of tapping is required. Virtual taps augment a network tapping design by facilitating views of network traffic between virtual machines. The Bechtel ICS Cybersecurity Technical Center has implemented virtual taps on the Distributed Control System (DCS) in the laboratory. This paper will describe the process taken to setup and configure the taps, and how to forward the tapped data to appropriate tools for analysis.

Augmenting physical network taps with virtual network taps enhances visibility of a live ICS network, and allows for greater flexibility in securing the architecture. Virtualized tapping will provide a huge benefit to future Bechtel projects and position the company as a lead integrator with regards to cybersecurity capabilities in design.

INTRODUCTION

As demonstrated with the TRITON attack on Triconex Safety Instrumented System (SIS) controllers [1], attacks against ICS are increasing in complexity and severity and they show no signs of diminishing. Believed to be nation state sponsored [2], the attackers intended to reprogram a SIS controller which conservatively leads to the assumption that physical harm was an objective. As with many attacks, the actors surveyed the target network from within to gain intel and plan their attack. The time an adversary is covertly on a network is often referred to as dwell time. For context, the median dwell time in 2017 in the Americas was 99 days [3].

To gain the ability to detect and defeat attack such as TRITION, having visibility into an ICS network is necessary. The potential for more severe and disruptive attacks increases the longer an adversary is on a network. Adding to this, ICS suppliers are incorporating virtualization in their designs, which adds to the complexity of the networks. Physical network taps are not able to fully capture the communication between virtual machines.

Through the partnership between Information Technology (IT) and Engineering, virtual network taps were researched

as a potential enhancement, which could be utilized on future projects that contain virtualized environments, or a mix of physical and virtual devices, to increase network monitoring capabilities. This paper will go through the process of implementing the virtual taps and the immediate benefits observed over the use of only physical taps.

ICS VIRTUALIZATION AND CURRENT SIEM IMPLEMENTATION

The use of virtualization in ICS designs has increased over time, and is likely to continue to expand in the future [4]. Virtualization is the process of emulating a physical computer or system. A virtualized computer is most commonly referred to as a virtual machine (VM).

Software called a hypervisor is used to deploy and manage VMs and is classified as type-1 or type-2. Type-1 is often referred to as a bare-metal hypervisor because it is installed directly to a physical machine with no operating system (OS). Type-2 hypervisors are an application installed on a main OS. In each case, several different types of OSes can be installed on a hypervisor which allows for great flexibility in an overall system's design. The laboratory Schneider system utilizes Microsoft's hypervisor known as Hyper-V and allows multiple operator and engineering workstations as well as servers to operate on the same physical host.

The use of VMs brings many benefits to a control system. The number of physical machines required for a system is reduced because several VMs can be deployed on a single physical host. This leads to a reduction of power needs, physical space, physical hardware and thus greatly reduces cost. Provisioning VMs can be simplified using templates or other automated tools to reduce the time it takes to deploy resources. Hardware upgrades for a single physical host typically takes less time to implement than multiple physical hosts and cost less. Resource sharing is also another major benefit. In a virtualized environment, resources can be shared more effectively and allocated to VMs who need it the most.

Despite the listed benefits discussed above, there could be drawbacks if careful system planning is not considered. For example, if the system is designed without redundancy, a server issue could affect all VMs installed on the server which would not be the case if the VMs were separate physical devices. From a cybersecurity perspective, if a hypervisor is compromised, all VMs residing on the affected node are also vulnerable to security threats.

The Technical Center DCS contains a mix of physical and virtual devices. There are two host servers that contain eight virtual machines each. The VMs are used for various purposes such as an antivirus server, a domain controller, virtual operator and engineering workstations, etc. With such a large use of VMs, the existing physical network tap installation was not able to provide visibility into the communication between each VM.

Figure 1 is a diagram depicting the physical network tap installation at the laboratory before virtual network taps were deployed. For last year's Technology Fair, the authors from the Bechtel ICS Cybersecurity Technical Center described a Network Security Monitoring (NSM) solution using physical taps and a Security Information Event Manager (SIEM). This solution used a strategically placed physical tap to gain enough visibility to detect an attack against a Programmable Logic Controls (PLC) on the network.

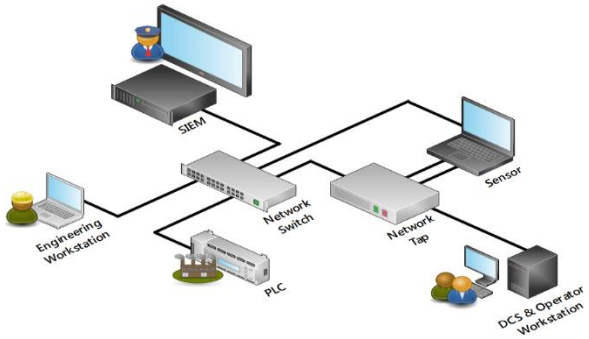

Figure 1. Network Diagram Including Physical Tap

The physical tapping solution was an important first step. Figure 2 shows the Technical Center's laboratory network when only physical taps are in use. This and other selected figures are also shown enlarged for clarity in Appendix 1. The diagram in Figure 2 was generated using a free program called GRASS MARLIN. By forwarding the tapped network traffic to a virtual machine running GRASS MARLIN, the program can provide a live logical view of the tapped network, and show which devices or nodes are communicating. The varying colors shown in Figure 2 represent the different subnets on the laboratory network. The lines connecting nodes represent communication pathways between devices.

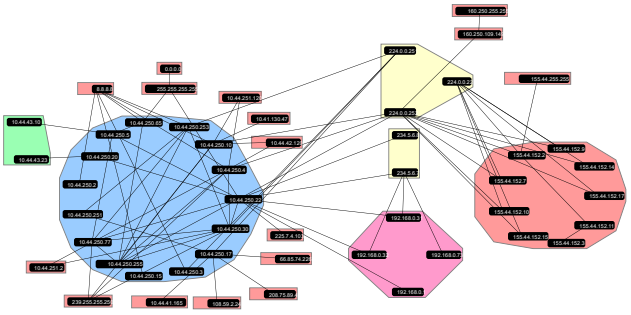

Figure 2. Logical Network View (Physical Taps Only)

TAPPING A DCS THAT INCLUDES VIRTUALIZATION

There are several methods available to tap VM network traffic, and the option used at the Technical Center is a product from IXIA called Cloudlens vTap. The software consists of two main components, the Cloudlens Manager and vTap modules. Both components are virtual machines that are installed on a host server. However, the Cloudlens Manager is only required to be installed on one host, if there is more than one host in the network. The Cloudlens Manager is used to configure and deploy the virtual taps on the host servers on the network.

In the Technical Center DCS network, there are two physical host servers. The installation process for the Cloudlens Manager and vTap modules is described in sufficient detail in the documentation provided by IXIA. However, the major steps taken to setup and configure the taps are described in this section as a high-level overview of the process to aide engineers who may not have IT experience.

There are three major steps to install the Cloudlens Manager on a Hyper-V host. Download the installation files and PowerShell scripts from IXIA, run the PowerShell scripts on the host, and finally run the installer for the Cloudlens Manager VM. Once the Cloudlens Manager is installed on a host server, the web interface can be accessed to configure and deploy the virtual taps.

The web interface provides a portal to the features needed to install and use the taps. Before any taps can be used, it is critical to enter the license information for the taps. A license is required for the virtual taps to capture network data. An offline license option is available for use in systems that have no internet connection, such as the system in the Bechtel ICS Cybersecurity Technical Center laboratory or a typical ICS network on a project. Once the license is configured, the taps are ready to be deployed.

For the Technical Center DCS network, taps were deployed on both our primary and secondary host servers. The process to deploy the taps starts in the web interface. The Cloudlens Manager then creates a virtual machine tap for each virtual network switch on each host. In the DCS network, there are three virtual network switches which leads to the creation of six virtual taps across the two host servers. Once the taps are created, the Cloudlens Manager virtual machine must be accessed to configure each tap. Figure 3 shows the command line interface (CLI) to configure a tap. After all configuration information is entered, the web interface must be configured to capture network communication.

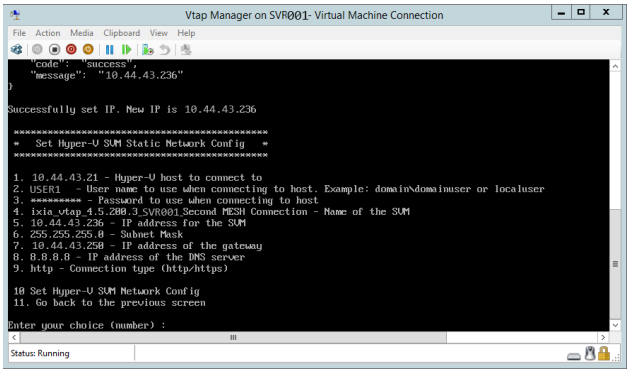

Figure 3. Cloudlens Manager CLI

The Policy tab in the Cloudlens Manager web interface is where capture and forward policies are created. Forward policies are required to allow the taps to send data to endpoint network monitoring tools. Capture policies allow the tapped data to be filtered as needed, to allow for control over what data is desired to be seen. In addition to the software configuration, some hardware changes are recommended by IXIA.

An available network interface card (NIC) port is recommended to be used on the host with the Cloudlens Manager. The port is connected to an endpoint tool to allow the forwarded network traffic to reach its destination. If no spare NIC port is available, the network traffic can be configured to use the existing virtual switch connection.

There are several options for filtering the network activity captured from the taps. Inbound, outbound or all network traffic can be selected, as well as capturing all packets or matching a specific IP, port number, or communication protocol. In the laboratory configuration, several filter options were tested. To provide the most visibility in the GRASS MARLIN tool, a capture policy looking at all packets both inbound and outbound was created.

VIEWING YOUR NETWORK

As discussed above, GRASS MARLIN is a powerful tool that provides valuable information about a network. The most obvious benefit is the logical view of the network. Figure 4 shows the logical view of the ICS Technical Center laboratory network, including the DCS network utilizing virtual taps. Compared to the earlier view which only employed physical taps, the number of nodes and communication pathways visible is noticeably greater. The green and red subnet groups in Figure 4, when compared to Figure 2, are most noticeably enhanced. These two subnets contain the VM communication.

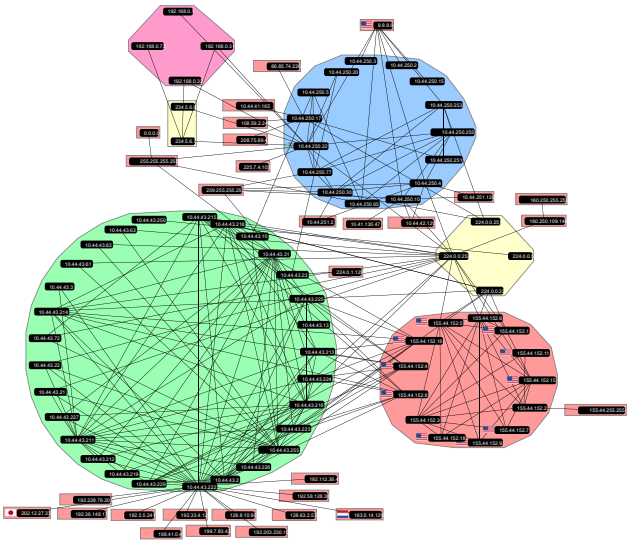

Figure 4. Logical Network View (Physical & Virtual Taps)

Another benefit of GRASS MARLIN is that the tool is passive. By utilizing the tapped data, and further, by forwarding the data outside of the laboratory DCS network, there is no observable impact to running processes. This type of tapping and monitoring configuration would be very beneficial to a facility containing an ICS. Although GRASS MARLIN only provides monitoring capabilities, future work tying it into Intrusion Detection (IDS) or Intrusion Prevention Systems (IPS) could increase a site's Cybersecurity posture well ahead of a typical adversary's capabilities.

While GRASS MARLIN is a passive tool, this paper has shown it is also capable of displaying a live logical network view. Any device communicating on the network will be displayed, and the details of the communication can be viewed.

By right clicking on any node in the logical view, many options are available to view the communications. Selecting "Watch Connections" will show the selected node, and just the other nodes it communicates with. "View Frames" displays a graph and table of all communications to and from the node. The table rows are time stamped, and include a PCAP file that can be opened in Wireshark to show more details of the communication. Figures 5, 6, and 7 display examples of each option.

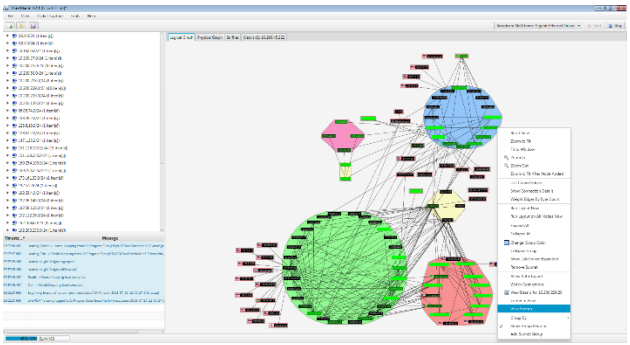

Figure 5. Live Logical View with Drop Down Options

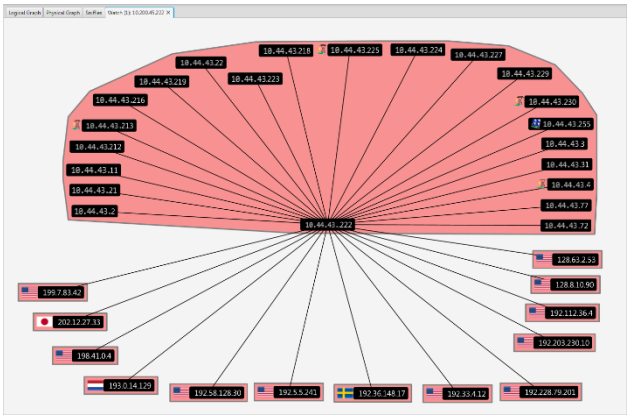

Figure 6. Watch Connections Option

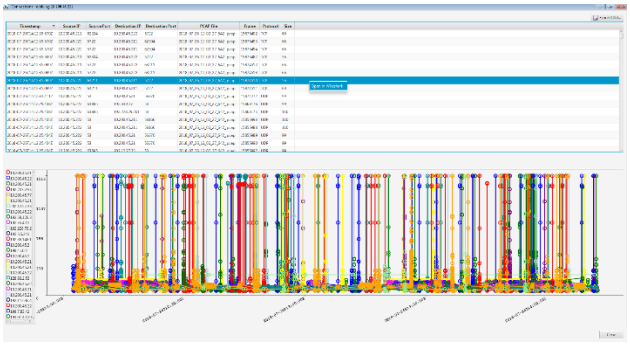

Figure 7. View Frames Option

Lastly, on the right side of the program, a list of subnets discovered are displayed. This can be seen in Figure 5. Each subnet can be expanded to show all IP addresses. Drilling down more will show each IP address that the selected IP address is communicating with. "View Frames" and "View Details" are also available in this list view.

CONCLUSION

As demonstrated above, network activity configured to be forwarded to a VM on our laboratory network containing GRASS MARLIN provided a much more detailed logical network view using virtual taps. The benefits of the increased visibility are numerous. In the simplest case of using GRASS MARLIN, situational awareness is greatly increased. With this tool, an operator can view active communication on the tapped network and investigate suspicious nodes. PCAP files generated can be audited on a predetermined schedule to look for any anomalous activity.

Another benefit of a live logical view, is seeing real time data flows. The real-time data can allow an organization to become smarter about their network. By reviewing the logical view, an unexpected communication link may be discovered. The link may be due to a node not being completely hardened. The connection information can then lead to the device being examined for additional hardening potential, which will increase the security of the network.

Tapping a network and using a tool like GRASS MARLIN is an important step in the process of gaining complete network visibility and securing a network. However, there are many opportunities to continue to strengthen the security posture of an ICS network.

NEXT STEPS

With the laboratory network utilizing physical and virtual taps, a large amount of data is being forwarded to a dedicated monitoring VM. Data on an ICS network can be transferred over many different communication protocols, which are typically DCS vendor dependent. Because the communication is often not strictly TCP/IP, many IT tools used can't utilize the data in a meaningful way.

To overcome the protocol issue, parsers will need to be developed. A parser is program that takes the raw bits from a communication data stream and groups the data into a useable format. Once the data is parsed, the information can be used in network monitoring tools to detect suspicious activity, rather than just for monitoring.

This paper, and much of the Cybersecurity work in the ICS industry is focused on the network layer of a system. In the future, detection will be further down the communication stack to be monitoring field device traffic. This level of monitoring will require the use of serial taps since the communication between these types of devices and a PLC or DCS is not over TCP/IP.

The path forward for utilizing serial taps will be similar to the next steps for virtual taps. The communication at the device level will have to be parsed for use in monitoring tools and for analysis/detection. In the end, the more visibility into a network, the more Bechtel can provide value to customers who may be struggling to stay ahead of malicious actors looking to compromise their networks.

ACRONYMS

CLI	Command Line Interface
DCS	Distribution Control System
ICS	Industrial Control System
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
NIC	Network Interface Card
NSM	Network Security Monitoring
PLC	Programmable Logic Controller
SIEM	Security Information Event Manager

REFERENCES

[1] Johnson, Blake, et al. "Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure.", *Threat Research Blog*, 14 Dec. 2017, www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.

[2] Miller, Steve, and Evan Reese. "A Totally Tubular Treatise on TRITON and TriStation.", *Threat Research Blog*, 7 June 2018, www.fireeye.com/blog/threat-research/2018/06/totally-tubular-treatise-on-triton-and-tristation.html.

[3] FireEye, Inc., M-Trends 2018, accessed July 26, 2018, https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf\

[4] Young, Barry. "Recent Trends Shape Future of Distributed Control Systems", 22 Dec. 2012, https://www.automationworld.com/article/technologies/dcs/recent-trends-shape-future-distributed-control-systems

APPENDIX 1: Enlarged Figures

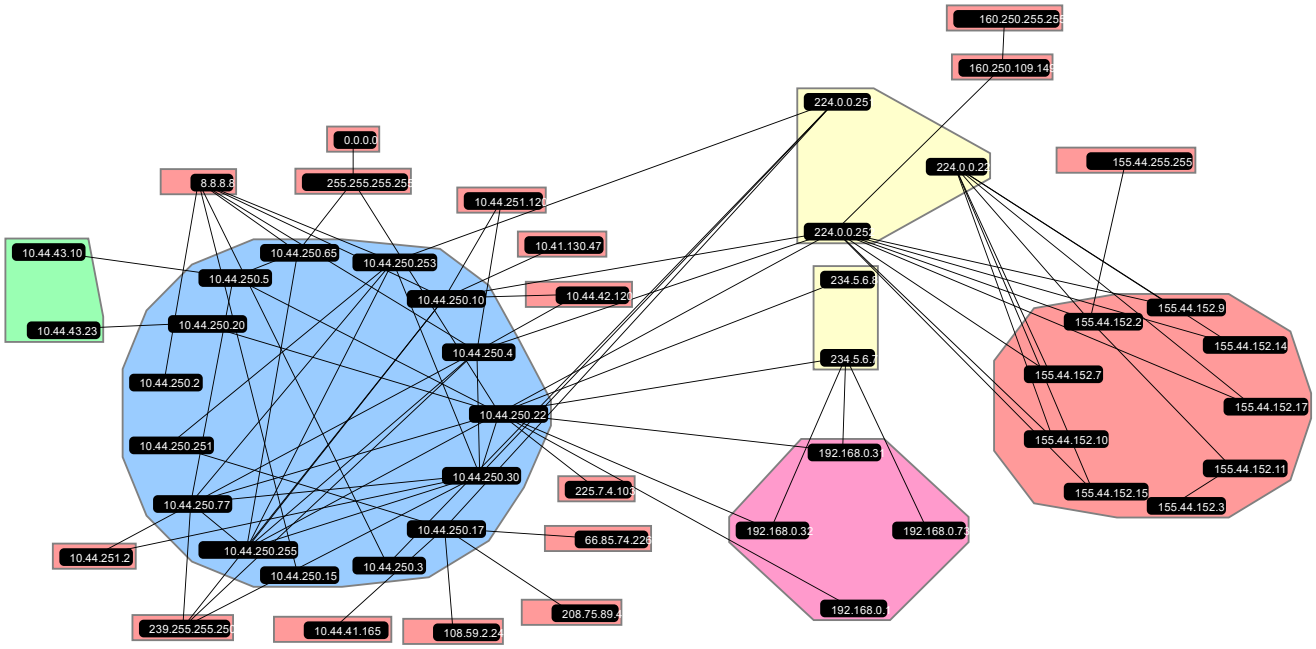

Figure 2. Logical Network View (Physical Taps Only)

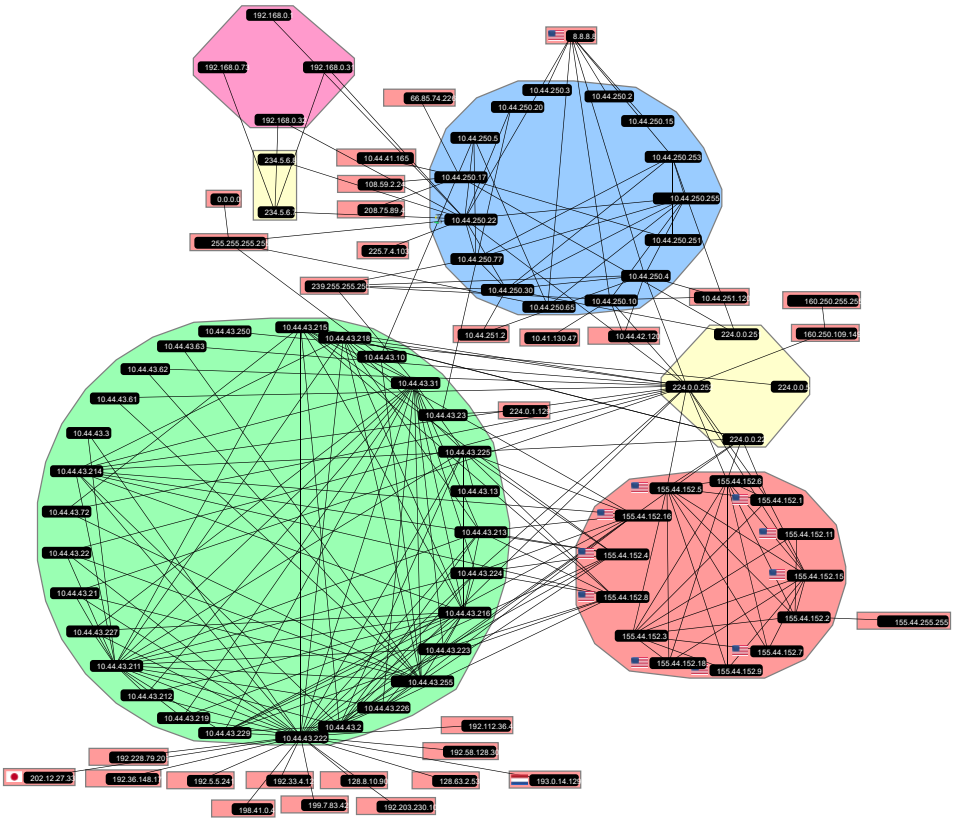

Figure 4. Logical Network View (Physical & Virtual Taps)

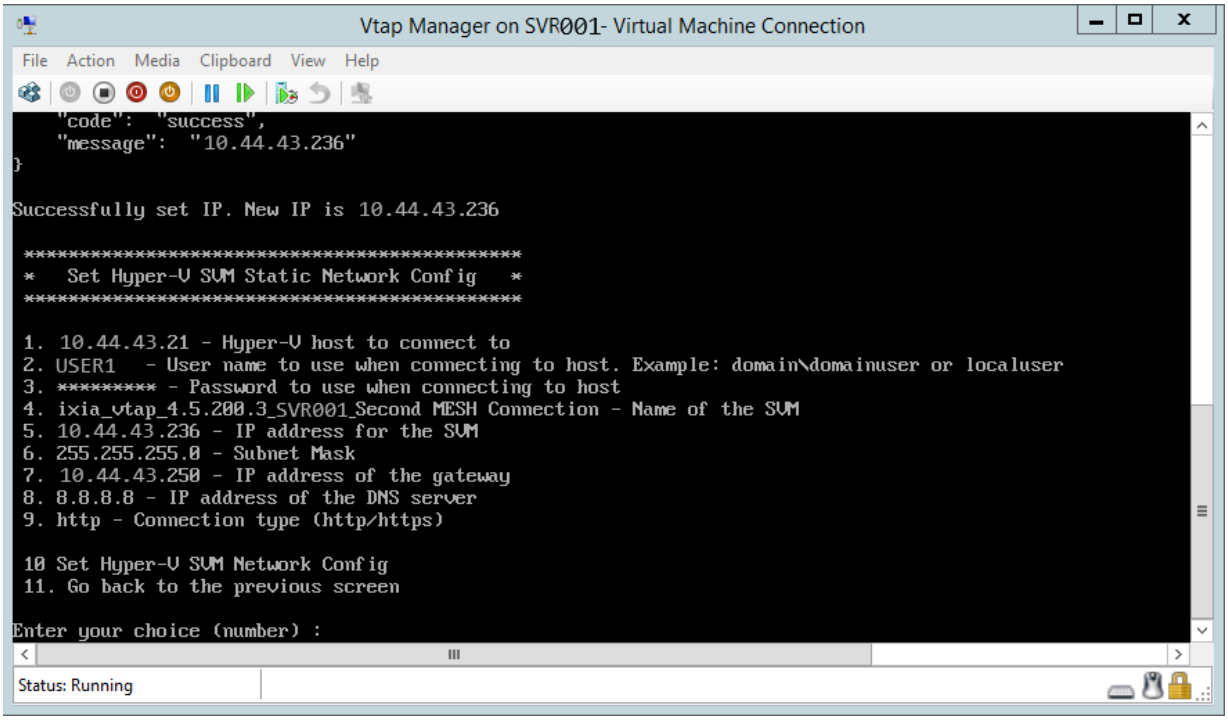

Figure 3. Cloudlens Manager CLI

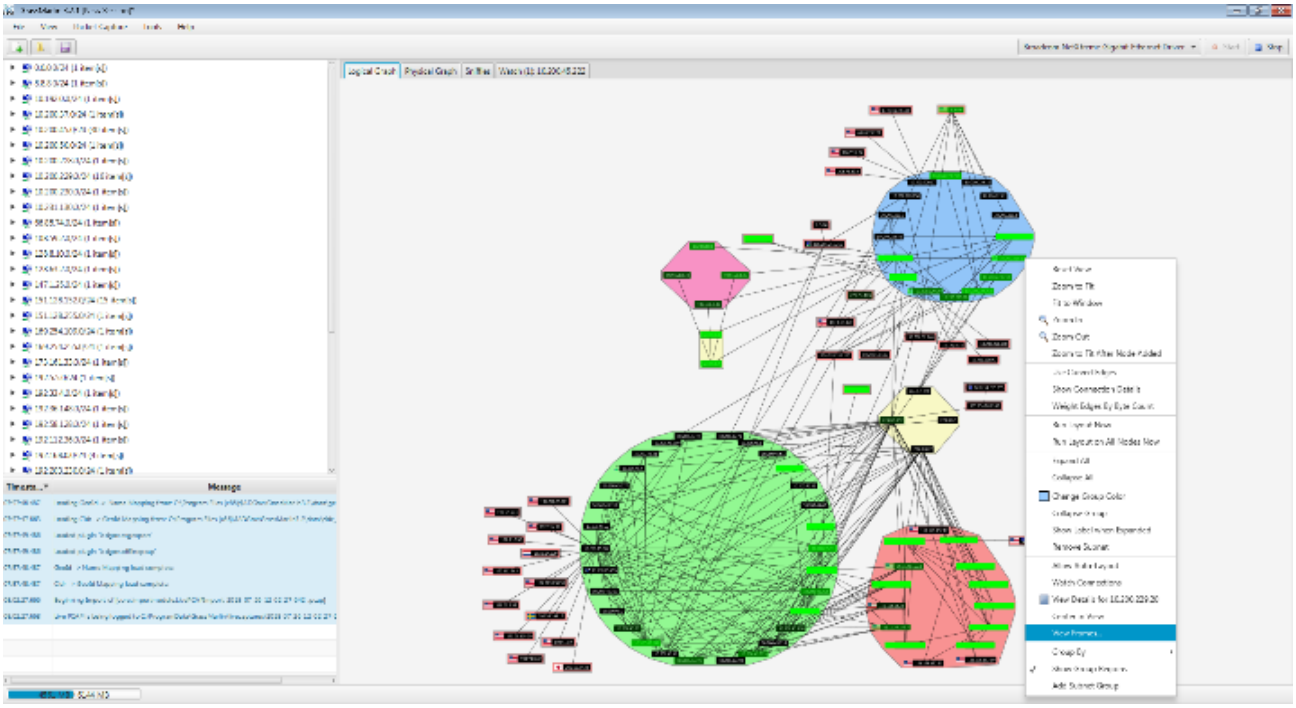

Figure 5. Live Logical View with Drop Down Options

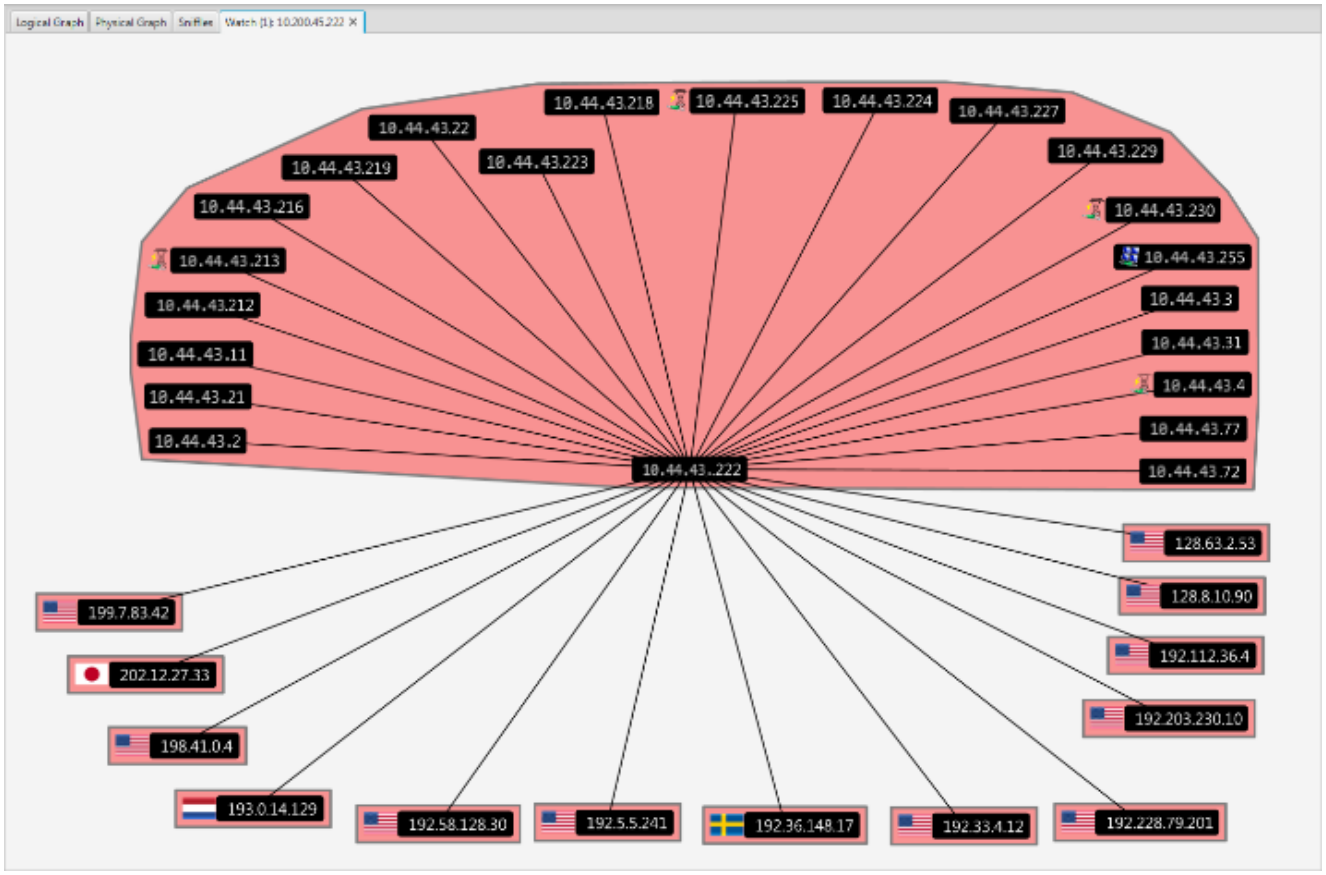

Figure 6. Watch Connections Option

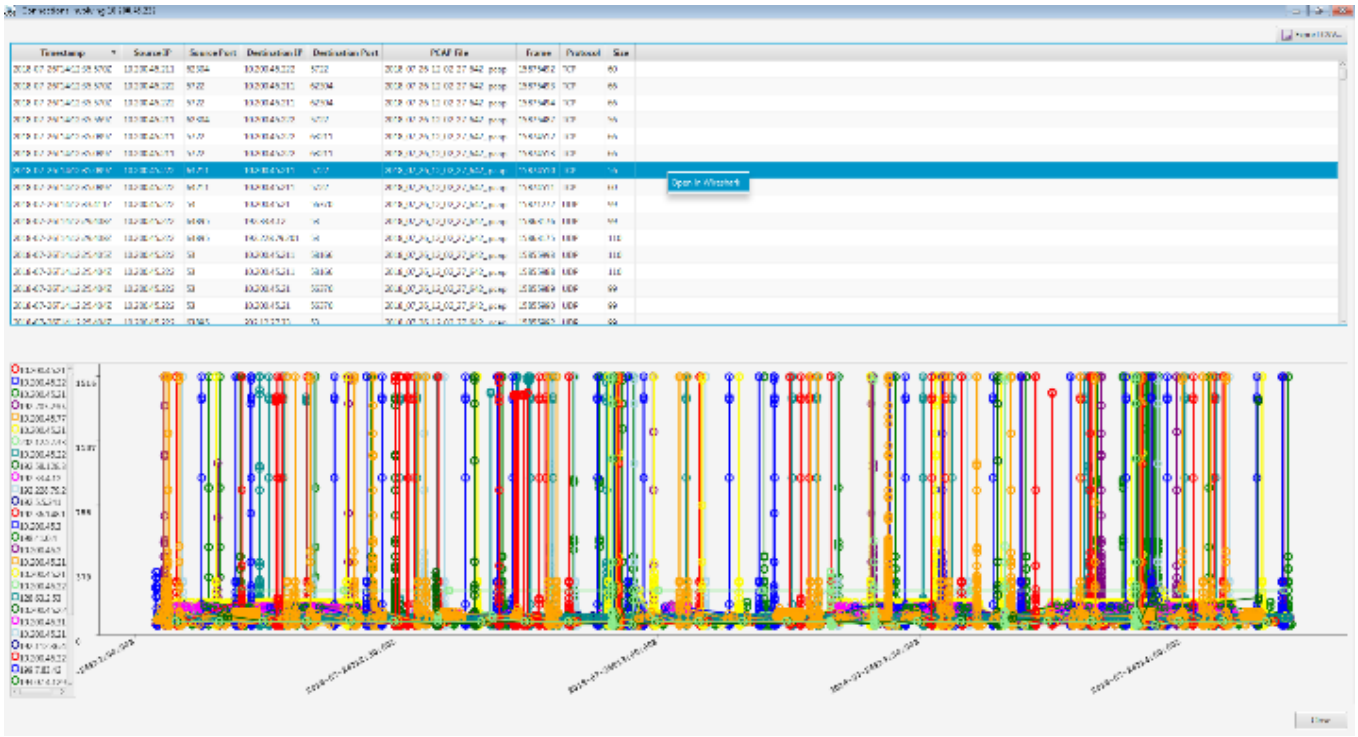

Figure 7. View Frames Option