WHITE PAPER

4D Visibility

Network Visibility as an Organizational Strategy

Looking at Network Visibility as an Organizational Strategy

What is network visibility? What is a visibility strategy? Who is responsible for visibility strategy? Why is visibility important beyond the IT department? When should organizations start developing a visibility strategy? What are the consequences if a comprehensive visibility strategy is not pursued? How can organizations benefit by considering four dimensions in visibility strategy?

These are some of the questions that will be discussed in this paper. The four dimensions to consider include technical, financial, political and legal. Developing sound practices around these dimensions is not only the purview of IT staff. It is a strategic focus that requires attention and commitment throughout the organization.

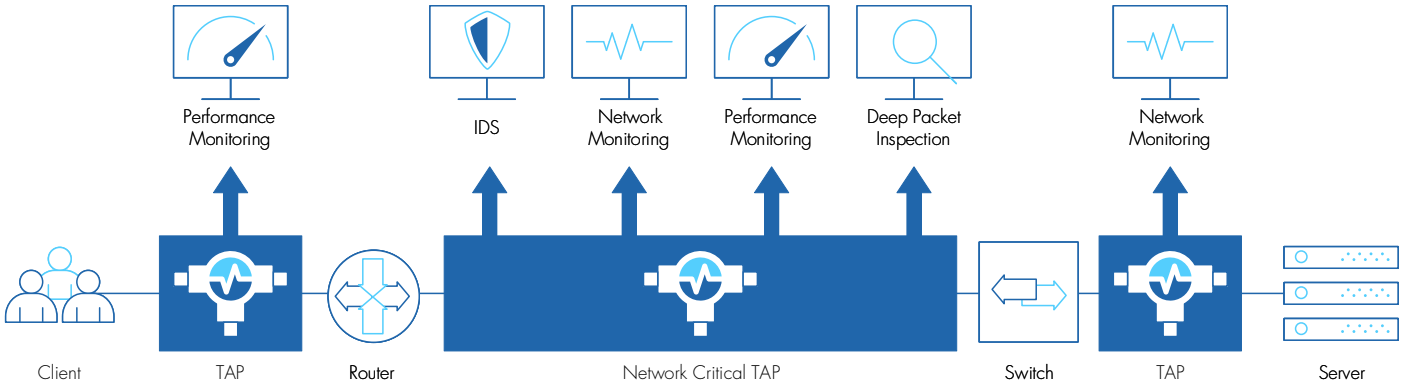
What is Network Visibility?

Network visibility is enabling network administrators to capture and see network traffic and applications that are traveling across Wide Area and Local Area network links. Once captured, traffic can be mapped to various tools for analytics, performance enhancement and security. There are many specialized tools to perform these functions that all must be connected to network links in order to provide traffic data to tools. This connectivity is the foundation of visibility and can be managed in one of three ways:

1. Direct connection is where the tools are connected directly to live links. This allows the tool to directly see and manipulate traffic. It becomes an integral part of the network and will be able to analyze data, block data and send packets back into the network. The primary limitation of direct in-line connection is potential network disruption if the tool should go off line due to a power disruption, maintenance or any other reason. If the tool goes down, the link goes down. If you have multiple tools on a link, the probability for disruption increases accordingly. There are also financial considerations with this method. In target networks, it can be financially stressful to deploy multiple network tools on every link.

2. Port mirroring is using specialized switch/router ports that will duplicate all traffic and send it to a specialized port where a tool is connected. This allows network tools to see all the traffic passing in both directions through the switch. There are limitations to using this process. First, there are a limited number of mirror ports on switches and routers. This can limit the number of tools to be connected. Potential for flawed traffic analysis can also be an issue. Port mirroring does not always pass every packet. Not having 100% of the information needed to make an informed decision can lead to false conclusions. Further, port mirroring can not manipulate traffic, disrupt traffic or send any new packets into the network. Therefore, port mirroring is not useful for real time security solutions where the tools actually block or isolate malicious traffic.

Network Critical
The Window to your Network™



3. Network TAPs are stand-alone tools that connect in-line to network links. They are independent to the switch and are installed in-line between switches and routers or firewalls. A TAP passes all the traffic it sees in both directions directly into the network and also makes a mirror copy of the traffic to output to network tools. TAPs are available in varying port configurations to accommodate small business all the way up to multi-site global networks. Also, because TAPs are independent of the the network equipment, they can be configured to allow network tools to manipulate and inject packets into the live network. So, for security applications, TAPs can connect tools that have the capability to predict, detect and prevent malicious attacks. TAPs also include fail-safe technology that keeps network traffic flowing even in the event of a power failure. Other features such as port mapping and filtering allow the flexibility to distribute tools economically throughout the network by aggregating traffic from multiple links to a single tool. This practice allows more efficient utilization of tools, lowers the probability of link outages and saves on CAPEX for new equipment purchases. For more complex networks, TAPs are often connected to Packet Brokers which provide more ports and higher level features such as load balancing and packet manipulation. Combining TAPs and Packet Brokers in large networks allows organizations to connect multiple tools efficiently to links and take full advantage of specialized tools for security, analysis, performance and protection.

Developing a Visibility Strategy

Developing a visibility strategy is similar to constructing a building. Start with the foundation and work your way up. The foundation of a visibility strategy is, of course, the visibility. First, all the traffic passing through the network needs to be seen, visible. Because TAPs are independent of network switches and see all the data passing through the links, the focus here will be on TAPs as the foundational piece. Once the TAPs are inserted into network links, all the traffic in both directions on those links will become available. To review from the section above, inserting TAPs will not impact network availability or reliability. So TAPs become the visibility foundation.

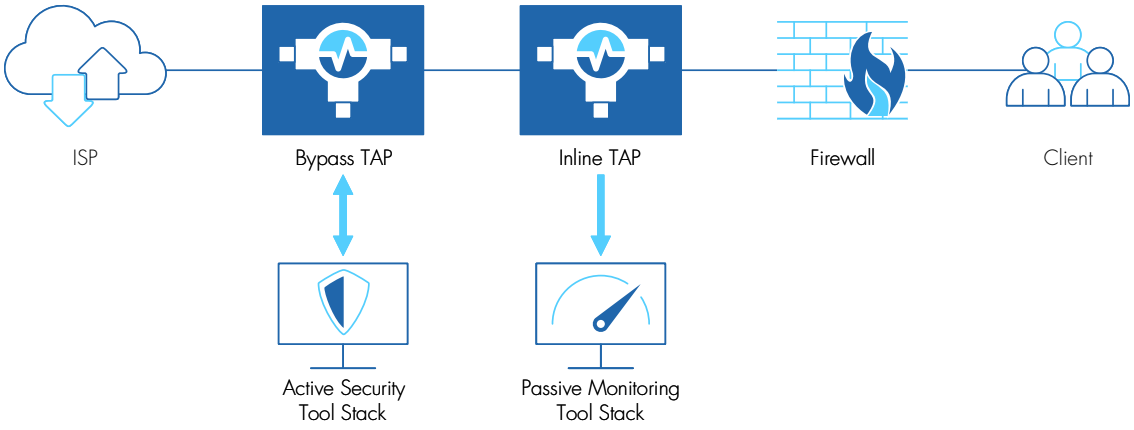
This bottom-up plan sounds obvious, but often times, the plan starts at the top floor of the building. The higher level applications provided by the network tools are often top of mind for the network architects and planners. The tools are budgeted and purchased with little thought of how those tools will be connected to the network. When this happens, networks tend to evolve along a rabbit trail with one purchase correcting or enhancing an operation from a previous purchase. The tools are all working but, perhaps, not as efficiently or cost effectively as possible.

It is important to start with the end result in mind, but also to look at how the network ecosystem will be affected by the changes. Monitoring is one of the base functions for network management. This allows the manager to see what is going on and look for potential bottlenecks and areas for traffic improvement. Often, for example, a problem thought to be bandwidth, is actually application performance. There are special tools to help identify and resolve these issues. Network protection and information security are also critical issues. Threats are not only persistent but are constantly changing. It is easy to see that managing and securing networks requires some planning and a blueprint prior to picking out specific tools.

Planning TAP connectivity to links is a great foundational starting point. TAPs can have multiple ports and will not cause delay or disruption to the network. Not all ports need to be in use upon deployment. Therefore, with a TAP foundation, the framing of your visibility strategy becomes much easier. Once the ports are in place, the traffic monitoring tools can provide important data from which other decisions can be made. Knowing that connectivity, monitoring and efficient traffic distribution to potential tools are in place, other aspects of the plan can be built. Adding performance, application, compliance and security tools will require less time and cause minimal network disruption.

Technical Dimension

Network design, management, monitoring, performance and security are highly technical and fall in the Information Technology group. Determining what visibility platform is utilized and what tools are needed requires deep technical expertise. However, what is often not solicited, is input from other departments in the organization. In fact, sometimes, there are divisions within the IT department about who controls various sub-sets of network operations such as switching,



security and applications. The scope, scale and functionality of this strategy will impact the entire organization, not just the controlling IT functions. More about this in the Political section.

This example will highlight the flexibility of a TAP based visibility architecture and the broad organizational reach of the tools that are attached. The following diagram is a live TAP based visibility architecture for a large department of the United States Federal Government.

As shown the diagram above, there are two stacks of tools. (Note that some of the brand names in the diagram may have changed due to industry merger and acquisition activity.

Passive Stack - A mirror copy of network traffic is sent to the tools for analysis. The tools are not impacting live traffic or sending any packets back into the network. SiLK is a sensor allowing for rapid access and analysis of network traffic data. Cisco LANCOPE provides flow based network security analytics across the extended network and cloud. RSA Netwitness Decoder is a log management and monitoring solution.

Active Stack - In this configuration, live network traffic passes through the TAP, directly into the active tool and back into the network in real time. This allows the tool to analyze the traffic, manipulate packets, stop suspicious packets and take immediate action on the link to block malicious traffic. Cisco Sourcefire is an active Firewall and Intrusion Prevention System (IPS/NGFW) that can identify and block malicious traffic. Symantic Bluecoat SSL Proxy is a web gateway device that scans internet traffic for security threats, authenticates users, and manage encrypted traffic. The TAP in the active stack has unique by-pass technology that sends a heartbeat to the active tool. If the tool goes off line for any reason, the TAP can by-pass the tool keeping live network traffic flowing. When the heartbeat returns, traffic automatically returns to normal operation flowing through the tool.

Managing and protecting network infrastructure and information requires focus. Each of these devices specializes on a very tight functional range. The example above is by no means a complete list of network monitoring, management and security tool options. There are many purpose built tools for applications such as Data Loss Protection (DLP), Customer Experience Management (CEM), and Identity Access Management (IAM). A simple web search will turn up a wide variety of devices that can be added to these links based on specific threats or required analysis. Having a multiple port TAP foundation allows tools to easily and safely be added, repurposed or changed depending on the immediate needs of the network.

There is a logical step by step flow when developing a visibility strategy; access, capture, analyze, secure and remediate if necessary. Ideally, if the right strategy and tools are in place along with other organizational influences to be discussed later, the remediation step will hopefully not be required. However, as is often said, plan for the best but prepare for the worst.

Financial Dimension

It is easy to rationalize a soft budget for visibility. Many organizations feel comfortable as long as a firewall is inlace and a probe is connected to a switch mirror port. The minimal architecture provides some intrusion protection and allows the network manager to analyze network traffic when needed. As long as no one complains, why complicate things? The simple answer is that being prepared and protected for advanced threats is less expensive than trying to repair the damage after an attack or breach. No one pays much attention to IT when everything is working fine. However when things go wrong, they can go very wrong.

Being hit by a malicious attack that cripples the infrastructure can shut down a business. When the Amazon web site crashed, it cost the company $1,000,000 per minute of down time. According to a 2019 IBM Data Breach report, the global average direct cost of a data breach is US$3.9 Million. The United States is the most expensive country for a company to experience a breach at an average cost of US$8.19 Million. Health Care is the most expensive industry when hit by a breach at an average cost to the company of US$6.45 Million. The average number of records stolen is over 25,000. That is a lot of customers who will loose trust in the brand and perhaps sue for damages.

These averages do not apply to all breaches. Some are more, some are less, but it is easy to see that investing time, effort and money in a robust visibility strategy and strong defense can actually demonstrate a great return on investment. The problem is that spending on defense prior to an attack can be hard to justify. The web news, however, is full of companies like Amazon and Equifax that help quantify the potential return from full visibility and strong defense strategy. There are other intangibles such as loss of consumer trust, bad press, loss of market share and brand damage that also figure into the financial justification.

Further, there are financial efficiencies built into higher end smart TAPs. A few cost saving feature advantages include:

Aggregation - Traffic from different links can be combined and output to an attached tool. This ensures that the tools are being utilized to their full potential and helps cut down on the quantity of tools that need to be purchased.

Load Balancing - Incoming traffic from high speed ports (10G, 25G, 40G, 100G) can be evenly distributed among a number of lower speed tools. This allows legacy tools to continue to be utilized even as networks transition to higher speed links.

Political Dimension

Organizational politics vary widely from company to company. Generally, smaller organizations have managers performing a broad scope of duties. Larger organizations, by contrast, have what are typically called functional silos. In large networks, for example, switches might be managed by a different group than that responsible for security. Another group manages infrastructure, another for applications, another for operating systems and so on.

When developing visibility strategy there may be many stakeholders involved in just the IT portion of the plan. For example, when using a switch mirror port for visibility, the group responsible for the switch will "own" the devices connected to the switch. If an analytic tool and a security tool are connected to two mirror ports on a switch, which group controls the application? Which group is responsible when the either or both devices goes down? Which budget is charged for the switch port, the analytic device and the security device? In short, who pays for what and who's throat gets choked when things go wrong?

This is not to say that multiple silos can not work together as a team. Using an independent TAP as the foundation of the visibility strategy simplifies management across demarcation lines. The TAPs touch the switch and they also touch the connected tools. This allows each functional silo to manage its own purview with out impinging on or impacting other groups. It is simple to parse budget and responsibility according to function.

Another political component of 4D visibility strategy is managing non-IT organizations. The entire organization is impacted by the success or failure of the network. Managing and protecting the network goes well beyond the IT department. When things go right, no one outside IT notices. When things go wrong, the pain is often felt throughout the organization.

All users of the network, from Accounting to Engineering to Production to Sales have a responsibility to safely manage their access to corporate network resources. When attacks succeed, perhaps because someone unfamiliar with phishing tactics clicks a link, it is the IT department who answers for lost information or infrastructure damage. Non-IT personnel network usage training is helpful but not fool proof. The physical protection against malicious attacks on all fronts must be in place in addition to continual training throughout the organization.

> "Organizations are failing at early breach detection, with more than 92% of breaches undetected by the breached organization."
>
> - Gartner

83%

Malicious Cryptomining attacks have increased 83% to over 5 million attacks in 2018.*

42 Million

There were over 42 million internet malware threats in 2018.**

Finally, there is a component of job security for network managers who are proactively protecting their organization's resources and information.

Legal Dimension

IT managers are being required to adhere to a wide variety of new laws and regulations that are related to network security, access to information and protection of personal privacy. Regulations such as HIPPA, GDPR, FISMA, CALEA and others require various protections for network users both inside and outside the organization. Stiff penalties and fines can be levied for non-compliance.

The other component of protecting the legal dimension is liability. Beyond regulatory compliance, unauthorized distribution and malicious use of information that is entrusted to the organization by a user can create a very expensive liability. People entrust very personal and private information to organizations through web sites ever day. Social Security numbers, credit card numbers, bank account numbers are often entered into web sites for making purchases, verifying personal identity or other reasons. When this information finds its way into the wrong hands, it can be devastating to the individual both personally and financially. Organizations that do not adequately protect that private data can be vulnerable to large financial penalties.

Remediation expenses after an attack may be only a small part of a much greater cost after a successful network attack. There can be fines from regulatory bodies, legal costs, and potentially, large punitive awards to third parties damaged by the unauthorized release of their personal information. Returning to normal operations after an attack can be very expensive, time consuming and painful. Strong proactive defensive tactics are generally a preferred option allowing the organization to stay out of legal jeopardy.

Without a broad visibility strategy, it is impossible for organizations to comply with these regulations. Networks must have architectures and tools in place to protect information received from customers and other visitors to the company web site. They must have the tools in place to identify malicious traffic and block attacks. They must have tools in place that block confidential information from being directed to unauthorized devices. They must have tools that protect the network infrastructure from damaging malware. These specialized tools must cover all links in both incoming and outgoing directions. All this must be in place while making the customer facing network available and open to the world.

Summary

Visibility is the foundational piece to a larger strategy of network and organizational protection against malicious attacks. Good visibility strategy is critical to day to day analytics and management for efficient operation of the network. While there are many specialized tools required to understand and protect network traffic, they can be deployed efficiently with the proper foundation.

Network management touches all parts of the organization and beyond. Customers and employees depend on the network every day. Often the reach is global. Liability, therefore, can also extend beyond international boundaries. Addressing technical, financial, political and legal dimensions in the early planning stages allows organizations to efficiently build and manage a robust network infrastructure with strong defenses. The benefits include productive internal use of network resources, maintaining the trust of external users, defending against malicious threats and protecting the integrity of the company and brand.

*Symantec Security Report 2019.
**2019 Kaspersky Labs Security Report.