SANS

A SANS Whitepaper

Network Architecture with Security in Mind

Written by **Matt Bromiley**

October 2018

Sponsored by:

Gigamon

Executive Summary

It's time to face a hard truth: Modern enterprise networks can be extremely—sometimes painfully—complex to manage and defend. Even worse, these behemoths may be constructed of legacy hardware that can barely keep up with the demands of a modern workforce. Network speeds to 100Gbps, unfettered access to cloud applications and end-to-end encryption are just some of today's requirements. When you add in mobile and IoT devices, the complexity grows exponentially.

As the hunger for bandwidth and the number of devices continue to increase, there's another area where users are becoming increasingly demanding: the security of the networks they connect to. However, as networks and the need for security expand, many organizations struggle with protecting their users.

We need a new approach that provides visibility to data flowing across various infrastructures to ensure that the right traffic is sent to the right security tools. This approach should also enable security operations and network operations teams to collaborate and improve the security posture of the organization.

In this paper, we will examine:

- Common security pain points for networks with legacy architecture
- How today's users are forcing organizations to consider security and include it in their network architecture
- How a lack of security can affect network availability and performance
- How to bridge the NetOps and SecOps divide

We will discuss how efficient and security-minded network routing and security tool utilization can shorten detection and response times. We'll also examine two case studies where legacy devices, inefficient networks and cumbersome security setups can result in extremely slow detection and response times, significantly heightening the severity of incidents.

We hope this paper will inspire you to reassess the current state of your network and security infrastructure to enable collaboration between your SecOps and NetOps teams and improve your security posture. Let's begin!

Living in Yesterday's Networks

Unfortunately, many organizations deal with a common set of issues when it comes to incorporating network security monitoring into their security programs. These pain points are often caused by legacy networking devices and appliances that still perform their original functions but were not designed or implemented with security in mind. Furthermore, organizations that have grown through mergers, acquisitions and increased sales may have data centers or network architectures that look at best like complicated spaghetti diagrams. Let's examine some of the problems today's enterprises are seeing in yesterday's networks (see Figure 1).

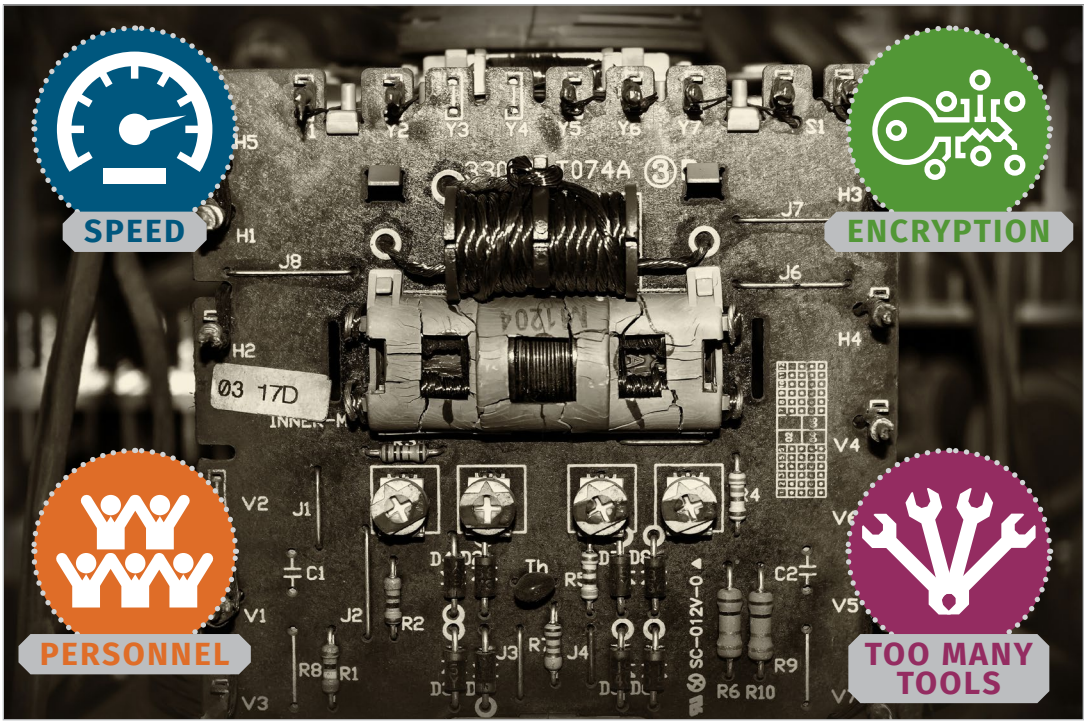

Figure 1. Common Pain Points of Yesterday's Networks

Speed

The largest impact legacy devices have on networks is the inability to handle throughput equal to what organizations need to operate. In early enterprise network design, it was enough to have a single line providing high bandwidth to a single ingress/egress point. Gone are those days! Users now want high bandwidth at every corner of the office, and their applications are structured accordingly.

If your organization is attempting to push new packets over old hardware, you're going to encounter significant routing issues just to get traffic out the door. Further complicating the issue, when you try to layer an element of security over an already-constrained network, you can expect packet loss and decreased visibility to be common problems.

Modern in-memory applications, such as browsers and chat applications, sometimes require network connectivity just to get started. When multiplied by a few hundred or thousands of employees simultaneously, it takes only one or two applications to bog down a network.

Encryption

The internet has seen significant growth in the amount of encrypted traffic over the past several years. From the explosion of mobile apps and third-party services to the ease with which developers can obtain certificates, encryption is here to stay and will continue growing. In its most recent transparency report, Google indicates that 83% to 93% of traffic it observes is encrypted, but statistics differ greatly between desktop and mobile devices.[1] Unfortunately, this use of encryption poses a unique problem for organizations, which at one time were able to view and analyze all their traffic.

Now, let's be clear on one thing: *The inspection of encrypted traffic is up to your organization and your legal department. Act responsibly!* Certain regulations, such as GDPR, HIPAA and PCI DSS, may dictate whether you can or cannot inspect decrypted traffic.

The inspection of encrypted traffic is up to your organization and your legal department. Act responsibly!

Too Many Tools

Last, we must consider what corporate growth has done to network architecture and how that has affected security teams. As organizations grow through mergers and acquisitions, SecOps is often forced to work with a plethora of tools, dashboards and analysis platforms, some of which may be completely different and incompatible, causing frustration and inefficiencies. Rather than directing traffic to the appropriate places for ingestion and analysis, and routing it with security monitoring in mind, organizations simply place another aggregator over traffic of interest and forward everything to a SIEM.

[1] "HTTPS Encryption on the Web," Google, 2018, https://transparencyreport.google.com/https/overview?hl=en

This approach has resulted in SIEMs becoming bloated to the point of being unusable and additional analysis points analysts must manage. Such situations have led to too many alerts—also known as analyst fatigue—and too much overhead for teams to successfully detect and respond to threats. We'll examine a situation highlighting the impact of too many tools in one of the case studies below.

Inefficient tools and bogged-down personnel can upend best practices and business policies. While your team may be trying to implement the most efficient processes possible, ineffective network architecture can stand in the way.

Personnel

All the pain points discussed thus far, while enough of a burden individually, are often experienced simultaneously. The confluence of these issues typically causes a loss of network visibility, an inability to effectively secure data and frustrated users who must bend to the network's capabilities instead of working efficiently.

Unwieldly networks also result in unnecessary personnel costs. Network engineers, who have expertise in ensuring optimal traffic routes and implementing security measures, often get bogged down troubleshooting network complications. Meanwhile, security analysts and engineers end up wasting time navigating the unnecessary complexities of a Frankenstein network rather than working to defend data and keep out attackers. Time that should be spent protecting, enhancing and securing the network is instead spent on troubleshooting visibility—and these time-consuming activities are creating windows that attackers are taking advantage of.

Building with Security in Mind

The windows that are being left open by inefficient, security-last networks are creating significant opportunities for attackers to enter and move around undetected. It's time to move security to the focus of network design, thereby making attackers' lives more difficult. Whether your organization is starting new or starting over, the considerations in Figure 2 and described in this section are designed to move security to the forefront of the network architecture discussion.

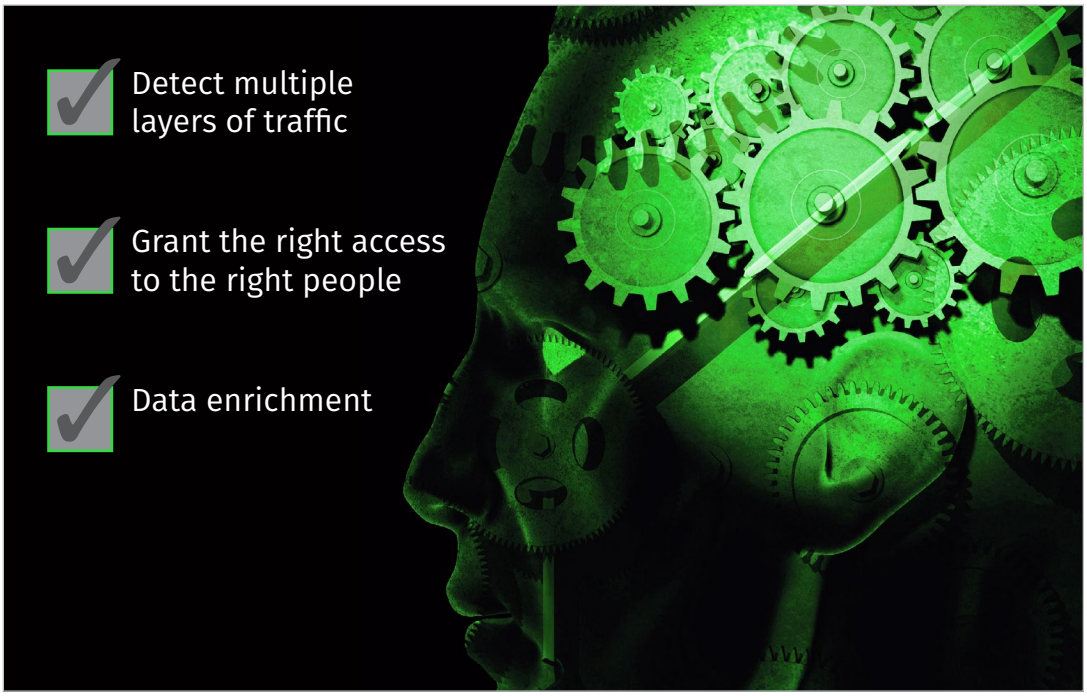

Figure 2. Checklist of Capabilities Needed to Make Security the Focus of Network Design

Traffic from All Angles

As your organization grows in complexity, you will likely acquire more data centers, more ingress and egress points, and more endpoints. You'll see some operations move to the cloud, some move to virtual servers, and some stay on physical servers. Like a shell game, anything can be moved around at any point in time. It can be daunting to figure out who's coming from where.

To understand your various traffic sources, you must ensure visibility. Too often, organizations are caught dealing with vulnerabilities and breaches that are outside of their monitoring scope—the recent breach of a large credit monitoring organization comes to mind.[2] And the worst time to discover lack of visibility is when you need it most. While your organization's growth can be a quick way to increase the size of your network, it can also be a quick way to introduce greater loss of visibility.

For security teams to be most effective, they should be able to detect threats at multiple layers of traffic. Don't limit visibility to the point where the perimeter and internal traffic look the same–it makes your team's job harder!

The Right Data to the Right Tools

After traffic is correctly routed, ensuring the right tools are getting visibility is key. Organizations need to answer multiple questions simultaneously: Can the team detect threats, ignore the "noise" of the organization and ensure that protected data is truly protected? You need to filter out, filter in, protect, decrypt, and encrypt! Consider these points to get the right data to the right tools:

- The security team likely has specific needs; filter out unnecessary traffic before it gets to your security tools. Do you really need to be monitoring 2TB of Netflix traffic daily?[3]
- Does the network engineering team need access to IDS and IPS logs? They are likely monitoring uptime, throughput and utilization.
- Business practices may dictate that protected data stays encrypted, whereas other data can be decrypted per employment agreements. Things such as GDPR may further complicate encryption/decryption matters—security-minded network routing can ensure that data is handled correctly and legally.

The Right Access to the Right People

Having access to the right data is also crucial for effective network security monitoring. Remember, different groups within the organization need access to different data. The network engineers, for example, may need only metadata to determine uptime, traffic spikes and troubleshooting. The security team, on the other hand, should have access to metadata and full content, where applicable (see the disclaimer on encrypted traffic above). Efficient network routing, via a network packet broker (NPB), for example, can ensure the *right* traffic is being sent to the *right* people.

---

[2] "Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach," Report to Congressional Requesters, U.S. Government Accountability Office, www.gao.gov/assets/700/694158.pdf

[3] Of course, if your goal is finding people watching Netflix at work, then DNS can work just fine here!

Retention periods are also of concern when it comes to ensuring the right people can access the right (and necessary) data. Network engineers may need data for only days at a time, whereas the security or compliance teams may think in months or years. Logically, it doesn't make sense for these teams to be pulling everything off the same tap—they have different needs, and excess traffic can effectively waste the organization's resources.

Enriching Data

We've largely summed up the concepts of efficiently directing, collecting and providing access to enterprise network traffic. Remember, the goal here is to view network infrastructure with security in mind. While steps can certainly be taken to collect and route traffic that may be disparate within your networks, security teams will benefit most from traffic enrichment.

Seek out security tools that can not only handle the needs of a large, complex network, but also enrich data. Your security team will experience shorter detection, correlation and monitoring times, which may be the difference between detecting and preventing a breach earlier versus later.

Note that traffic enrichment can be done post-flow by third-party tools and API lookups, but this is yet another step in the monitoring, detection and prevention cycle that analysts currently either have to do manually or automate and maintain. As such, seek out NPBs that not only can handle the needs of a large, complex network, but also have built-in data enrichment capabilities. Security teams expect modern networks to be able to simultaneously enrich and route network data, saving an additional step of correlation.

NPBs should be able to go beyond simple network flow data and provide protocol-aware metadata, including URLs, status codes and the like. The coupling and enrichment of DNS query and response data are among the more useful benefits of using a network security device. Having access to DNS data within the environment may be a valuable network monitoring detection and analysis technique, yet it is frequently ignored or dropped. With the right data included and enriched, your security teams will experience shorter detection and correlation times, enabling it to detect a breach before it's too late.

Utilize your modern NPB, become protocol-aware and enrich your traffic on the fly. Let your network devices do the heavy lifting so your security team can focus on detecting and responding to threats.

Security-First Networking in Action

Given the network security architecture concerns and recommendations outlined above, it's time to put the concepts in action. Let's examine two case studies where security and networking working together can help organizations successfully defend and respond to threats.

The Case of the Cross-Eyed Analyst

Angela is the top security analyst at 4343 Lumber Corp., a global conglomerate that manages nearly 100,000 endpoints and 80 egress points. 4343 has a history of acquiring smaller companies and incorporating them into its global network with very little testing or integration planning—and business has been booming, meaning there's an increased urgency to get stuff done on the patched-together corporate network. Due to a **lack of**

security planning, Angela relies on approximately 15 different dashboards to get access to the minimum level of information she needs to efficiently monitor 4343's operations.

At 5:30 p.m. on a Friday, Angela receives a call from Darlene in the security operations center that a subsidiary in the northeastern U.S. is under attack. It takes Angela **approximately 8 minutes** to sort through all the applications and dashboards needed to view network data related to the event. While that doesn't seem like a long time, it's long enough for the attackers to gain entry, enumerate the domain and move laterally to the domain controller, which is housed in a data center on the West Coast. **Angela needs another two dashboards to view that traffic, too.**

The case described above is typical at large organizations that have grown without security considerations. Unfortunately, as traffic links are "connected," the security team is forced to incorporate whatever mechanism was being used for monitoring prior to an acquisition—if there was one. Network traffic is not efficiently distributed through the security team's monitoring and detection mechanisms, but the team is still charged with securing the additional traffic. Even worse, the fastest an analyst can respond is still too slow for a skilled, determined attacker. **The human reaction process is handicapped, meaning it can be only so fast.**

The solution to Angela's problem is twofold, at a minimum. First, 4343 could do with some efficient network packet routing, using a device such as a NPB. Efficient routing and traffic deduplication would not only ensure that packets get to the right place, but also that Angela and her team get pervasive network visibility from one location, instead of more than a dozen. Packet routing would allow them to implement stronger network security monitoring because they can monitor and detect a single high-speed link.

With a single source of network visibility, Angela's team could develop strong filtering, detection and analysis techniques, and truly implement effective network defenses. It could begin to enrich traffic for investigative purposes, and handle application-specific traffic as well as physical, virtual and cloud traffic. Strong network security monitoring involves that and more, with the goal of having real-time, high-fidelity network data that can be used to detect, track and prevent threats within seconds instead of minutes. Furthermore, having an historical record of the metadata (or full packet capture) of the attack and the network activity would let Angela and her team "turn back the clock" and correctly scope the entire incident, instead of just a small piece.

The second part to Angela's solution is to ensure that the security team is at the table for discussions of how a new network joins the old network upon corporate growth or restructuring. Too often, these steps are taken without the security team's involvement. In a new network-with-security approach, the security team would first consider how it will wrap monitoring and detection around the new traffic and connect networks when they are ready to defend. While this may require a significant change in organizational structure, it is a critical step that should be considered by executives and operations teams.

The Case of the Packet Strapped to a Tortoise

It's 8:57 a.m. on a Monday. Elliot, an incident response analyst at MC² Corp., has just arrived for work. He sets down his bag and almost-empty coffee, logs into his workstation, and begins parsing his Inbox. His email sometimes takes a while to load because the security team was provided a "bolt-on" office with a 10Mbps line, which was the only port available on the legacy switch at the time. Elliot's morning email includes a few low-level security alerts, and he would like to follow up on each just to be sure.

Elliot opens his browser, logs into a few dashboards and kicks off queries for network data related to his tasks. He could use NetFlow to answer most of his questions, but he's not allowed access to aggregate flow data from one of the subnets of interest—the subnet that houses the engineering R&D. He goes to refill his coffee, as he knows it's going to be at least 25 minutes before the data he requested is returned.

This situation is unfortunately one that SANS incident responders have seen all too often. At best, **security was an afterthought (a.k.a. security-last) for Elliot's organization and was added on to meet a compliance requirement** instead of to help protect the organization. Unlike Angela, who has visibility but in too many places, Elliot doesn't even have access to the data he needs to successfully complete his job. It's not hard to imagine how dire of a situation this can be when the security team has no visibility into the most crucial part of the organization.

The first issue Elliot's organization must overcome is moving security to the forefront of the discussion. Past decisions have allowed the company's most crucial network—the engineering R&D—to remain unmonitored. The danger this decision presents if an attacker were to successfully compromise that subnet is considerable, as engineering R&D likely is working on building the future products of the organization. One potential approach, again via efficient network packet routing, is to correctly filter, tag and enrich packet data. The security team can also wrap stricter detection mechanisms around crucial subnets such as this one.

The second issue Elliot faces is access to the right data. After effective packet routing measures are in place, the team can ensure that traffic is being viewed by the correct people and only the correct people. By employing a security-conscious mindset, the needs of securing the network are considered at every packet turn.

At MC², correct packet handling can serve multiple groups, not just the security team. For example, network engineers may need only metadata and, as such, receive only what they need at their consoles. Elliot's team, on the other hand, may need to collect packet capture data from the engineering subnet and NetFlow or metadata from the payment network. Efficient packet routing can ensure that departments are viewing only what they need to view, thus streamlining the security of the organization.

Conclusion

Have enterprise networks changed? You'd better believe it. Networks have grown in complexity and speed, and many organizations are struggling to keep up with their security tools. Unfortunately, without visibility into the various infrastructures organizations are working with today, security tools are unable to detect and prevent threats to the organization.

If your organization is suffering from a lack of security-focused networking and can't keep up with monitoring and detecting attackers within your network, we recommend analyzing what the root cause of the problem may be. Is it a lack of a coordinated effort between networking and security teams, or the larger issue of security as an afterthought? If so, can the network be revamped?

Perhaps the networking and security teams need to get in a room and sort out network traffic visibility for the benefit of the organization. If you already have traffic access in place but it's not being used correctly, then make that shift sooner rather than later. If you need to purchase new devices or rearchitect, those are clearly more complex solutions that may require new devices, more time and more investment. If your organization needs to start at square one, start small: Drop in security-optimized network devices such as an NPB and build out monitoring and data flows segment by segment. **Ensure your networking and security teams are involved in the whole process—they will both benefit immensely, and your organization will end up with an improved security posture.**

Sometimes, it's as simple as getting network visibility into your entire infrastructure and providing the right traffic to the right tools. Other times, it's a realization that security has always been an afterthought instead of a conversation leader. It's time to enable your security and networking teams to collaborate and protect your business, your customers and your networks.

About the Author

Matt Bromiley is a SANS Digital Forensics and Incident Response instructor, teaching Advanced Digital Forensics, Incident Response, and Threat Hunting (FOR508) and Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response (FOR572), and a GIAC Advisory Board member. He is also a principal incident response consultant at a major incident response and forensic analysis company, combining experience in digital forensics, incident response/triage and log analytics. His skills include disk, database, memory and network forensics, as well as network security monitoring. Matt has worked with clients of all types and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor: