Network Security Visibility is the New Bacon for InfoSec Professionals

Like bacon you can never have too much network visibility

Executive Summary

Network visibility is like bacon, there is no such thing as too much. For the InfoSec professional, it is a key ingredient that pulls everything together and helps you make sense of what is going on in the data center and beyond.

The first in a two-part series, this paper discusses how to break away from the resource drain of deploying point security devices. It provides you with a proven way that you can transform a piecemeal mix of security devices to better defend your environment with holistic and unified network security visibility.

This paper is a quick and enjoyable read for the InfoSec professional looking for ways to strengthen their layered security initiatives with integrated security architectures and unified visibility that doesn't break the budget.

Introduction

Every day another IT organization invests in a new security device or system aimed at fortifying their layered security program. For many, justifying the IT expense for new security devices has become a matter of investing in the current best-of-breed solution to defend against the latest threat. Over time, enterprise IT organizations have gathered a variety of firewalls, IDS/IPS, DLP, anti-malware, sandboxes and forensic security solutions to help them defend their environment. These security devices all have different interfaces that can be difficult to master, cumbersome to manage, and can quickly drain you of skilled administrator's time and resources. The "security technology du jour" approach has induced an environment of diminishing returns and has made managing network security challenging. Unfortunately, multiple security devices managed by too few people is the hallmark of today's enterprise security operations.

Right now, security spending among enterprise organizations is hitting some of the highest levels ever. Analysts estimate anywhere from a 7 to 20% uptick in cybersecurity spending this year with overall spending projections are on the top end of $70 Billion for 2015[1]. At the same time, the Fortune 500 has also experienced some of the most damaging security breaches ever reported.

Current threat intelligence is clocking in with estimates showing that the average enterprise environment, typically comprised of 10K employees or more in size, has a file containing sensitive data leaving their network every 36 minutes. New unknown malware is downloaded by employees every 34 seconds and once every minute a bot communicates with its command and control center [2].

These realizations boil down to the fact that piecemeal approaches to layered security spurred by device-by-device deployments has become difficult to manage and less effective at blocking legitimate threats.

It's also clear cybercriminals are well aware that most enterprise organizations operate with significant blind spots in securing their infrastructure and they are continually finding ways to circumvent point security systems. Malware and targeted attacks get more sophisticated by the day and are increasingly being designed to take advantage of silos that point solutions create within your IT environments. Malware can now detect virtual machines (VMs), be timed to detonate at a later date, and can survey your systems to find vulnerabilities in your environment.

This challenging environment is producing a shift in mindset among the InfoSec profession to break away from the endless cycle of reactionary alert-driven practices and point solutions and move towards improving their layered security programs. With this shift in mindset, InfoSec professionals acknowledge;

- Combatting multi-vector threats has become impossible without end-to-end visibility of network traffic
- Bolting on more disparate security solutions without a security architecture isn't working
- Both real-time and post-compromise threat management must be deployed to combat multi-vector threats.

To address these concern and improve upon existing layered security measures, InfoSec professionals are developing new approaches to achieving end-to-end visibility and monitoring all network traffic. At first, this might seem like an extravagant endeavor and asking for the funding can leave you feeling like you just asked for triple bacon on your burger. On the surface, it seems like a gargantuan investment in security tools to extend network visibility across campuses, the data center and branch offices. Not to mention people to manage them. And as it is right now, most InfoSec teams can't hire people fast enough.

Happily, obtaining end-to-end network visibility for security monitoring is now a different story. Except for hiring InfoSec personnel, which may still be challenging for most organizations. But, you don't have to hire an army, have a bake sale or dedicate your entire annual budget to get visibility of your entire network that you need.

Improving Layered Security Defenses – The Options

Layered security is the most widely accepted approach to defending enterprise attack surfaces, and with good reason. It makes sense to combine best-of-breed solutions for next generation firewalls, anti-malware, anti-spam, intrusion detection, intrusion prevention, data loss prevention, and sandboxing. With each layer of deployment, it provides multiple opportunities to defend against an attack. Each style of security analysis and defense compensates for weaknesses in other layers of protection and together they provide best of breed protection.

Traditionally, companies start with perimeter defense and various complementary endpoint security solutions. As discussed, past modus-operandi tends to favor security devices being deployed via a SPAN port per each network segment. The problem with

this approach is that it provides a limited view of the network and it can't scale. The more coverage you need, the more SPAN ports you use and more security devices you need to buy. It's a losing proposition and SPAN ports are best utilized in low-throughput situations that only require passive monitoring.

The promise of layered security breaks down when each layer of protection does not operate with a shared view of the end-to-end network. Fragmented visibility among devices is an outcome of bolting-on new security devices via a SPAN port in a piecemeal fashion across the network. You have probably experienced this yourself and it's frustrating when security systems don't detect the same thing.

To address the problem of getting visibility of your entire network, there are several routes you could take:

1. Invest in herculean efforts to integrate tools, via a SIEM solution to achieve the fabled "single pane of glass" visibility.
2. Move to a single vendor solution, but that would keep most InfoSec professionals up at night or in a perpetually uncomfortable state of mind.
3. Budget for and instrument your network with multiple sets of security devices to get the full-network security coverage.

These obstacles to achieving end-to-end visibility are very real but it's not all bad news. There are better answers to how you can bring your layered security initiatives to the next level of effectiveness and protection without raising the bar on your budget.

Today's *Lean Forward* Approach to Layered Security

The best layered security programs are built with specific support for the incremental addition of security defenses. This could include threat intelligence services, incident response, DLP and or forensic analysis capabilities. Perhaps Lawrence Orans, research director at Gartner, said it best in his Five Styles of Advanced Threat Defense Framework paper, "Today's threats require an updated layered defense model that utilizes "lean forward" technologies at three levels: network, payload (executables, files and Web objects) and endpoint. Combining two or all three layers offers highly effective protection against today's threat environment".

A first step towards making a combination of these *lean forward* security systems effective in a layered security architecture requires that they share a common view of network traffic throughout your organization. Otherwise they quickly become a point solution and can easily detract instead of fortify your overall layered security program.

You can afford this *lean forward* approach to your layered security architecture by giving equal consideration to the underlying infrastructure supporting the selection and deployment of the most-effective threat defense technologies.

When you combine layers of best of breed functionality it is critical that they are deployed on a foundational visibility plane for monitoring and visibility, to improve layered security defenses. This enables you to combine layers of security devices so you

can effectively implement the broadest range of best-of-breed functionality, while also achieving a more integrated approach to defense.

VSS Monitoring calls this the VSS Unified Visibility Plane™ and combined with the VSS vProtector, it enables differing security technologies to see and act upon the same data and network traffic. It is a simple and elegant way for both active and passive security systems to share the same view of network traffic and better deliver on the principles of layered security.

So, how does the Unified Visibility Plane™ work?

Deploying perimeter and endpoint security are typically the starting point for most layered security deployments. As discussed past modus-operandi tends to favor security systems being deployed via a SPAN port to cover each network segment knowing that this may or may not cause a blind spot in your ability to detect malicious traffic.

Figure 1 shows how a layered security approach is effected with a VSS Monitoring Network Packet Broker (NPB).

In this use case, deployment now takes place with the benefit of using a VSS Network Packet Broker (NPB). The NPB is deployed inline where it can receive traffic from various points in the network and deliver the aggregated traffic to multiple security devices.

With a VSS NPB acting as the foundational enabler for your tool deployment, it presents end-to end traffic for real-time analysis so that security devices see and can act on the same traffic. Inline security is then made possible by enabling a security tool chain to inspect traffic, allowing multiple security devices to be chained together. This enables you see the inspection layer as one coherent picture so you can observe and flag the behavior of packet payloads. See Figure 1.

Sidebar

"*Security analytics, equipped with full-packet capture and analysis capabilities, is the top-rated network security technology planned for acquisition in 2015***."** SANS Analytics and Intelligence Survey 2014

With devices sharing the same inspection layer you now have the ability to take a number of different approaches to improve your layered security defenses. One route might include adding sandboxing that can analyze and deliver suspicious files and captured traffic to a cloud based threat intelligence service that can generate a signature for that file/pattern. With that type of capability policies can be deployed among any or all devices connected to the NPB.

Other lean forward security initiatives involve the ability to actively "hunt" for the first signs of a malware infection. In this use case, you might add full packet capture capabilities and a forensics tool. This would allow you to store traffic captures received from endpoints across the network for analysis aimed at finding malicious patterns or unknown malware. Or you could use forensic capabilities to reconstruct and replay the traffic leading to a malware infection or insider threat. In these situations, the ability to collect a sample of data from across the network is critical. Bigger the sample sizes produces better data for analysis.

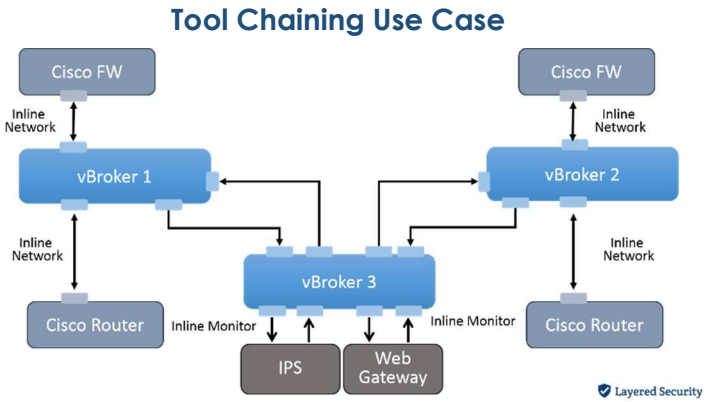

Figure 1. Deploying NPBs provide centralized management and unified visibility in a disruption-free environment. Immediate benefits include;

- *Eliminating onsite trips and midnight maintenance windows in order to make changes, tune or reconfigure your security devices.*
- *Flexibility to deploy any combination of inline or passive security devices with any-to-any traffic mapping between network segments and security devices.*

Layered security begins with the inline deployment of security devices and grows to accommodate the end-to-end collection, processing, and analysis of volumes of security data. With VSS's vProtector, you gain the critical network visibility needed to quickly make sense of activity throughout your environment.

Visibility is critical and if that was all VSS NPBs provided the value proposition wouldn't be so widely recognized. But this is only one facet of the benefit that adding network packet brokers provides. Keep reading to learn more about how you can now do more, even with a smaller staff.

Disruption Free Architecture

Once you have deployed VSS NPBs in your environment, InfoSec personnel can now operate with several advanced capabilities and productivity improvements that are a central part of a solid *lean forward* layered security approach.

The genius behind building a security monitoring and visibility layer with vProtector is that now your security devices are no longer anchored to static links. Your monitoring environment is now decoupled from the network plane. So, the inspection and monitoring of network traffic is no longer tied to physical ports, server location, tool location, or even time. What this means is that you now have an impact and disruption-free architecture. Any one or more of the inline devices can now be taken out for tuning or maintenance without disrupting other inline devices that are in operation or scheduling midnight maintenance windows.

Trigger Policies Improves Response

VSS vProtector trigger policies improve your response to unplanned changes in network conditions or security device states. You can define conditions or events that correspond to actions that you specify when the event occurs. Triggers allow you to plan and set automated responses so you can:

- Replace and upgrade active and passive security devices, without incurring network downtime
- Maintain full visibility, even in instances of changing network conditions
- Automate failover to redundant or standby monitoring devices

Triggers enable you to detect and issue alerts based on port status, utilization, security device health and status of remote NPBs. Trigger policies allow for different user-defined triggers to automate a wide variety of actions, including:

- Implementing mappings to re-distribute balanced flows/sessions as defined by your monitor and bypass settings
- Response with syslog messages, SNMP traps servers, LED alerts or disable/force link down on selected ports

Or you can define required actions by using a combination of several trigger events. vProtector enables full traffic capture for suspect traffic and synchronously delivering a copy of the traffic to a forensic analysis system or to anti-malware tool for deeper investigation and root cause analysis. Leveraging vProtector unique tool chaining features you can identify specific traffic flows and actively redirect these flows to the appropriate security appliances or series of tools each offering a layered approach to network security.

Calculating the Value of Improved Visibility

There is no straightforward way to calculate the ROI of any security investments but there are ways that you can show how investing in a VSS NPBs can save on tool purchases and improve productivity.

There are two ways hard cost savings are realized:

- With vProtector you can extend usage of your existing security devices by regulating the speed at which traffic arrives at the device. Regulating traffic speed enables a security device that can only inspect traffic at 1G or 10G speeds to be usable in a 40G network.
- New investments will not require purchasing multiple devices for full network coverage. By aggregating hundreds of network connections and using advanced filtering to only deliver traffic of interest, you will not have to purchase multiple devices to get full coverage.

Soft costs, the productivity improvements realized by saving time and making your life easier are numerous. The biggest benefits InfoSec teams realize with a VSS layered

security solution is that making changes to your security devices no longer has to happen during off hours. You can reorder your devices or reconfigure the type of traffic each receives in software – without concern over network disruption or being onsite.

Other soft cost savings include:

- Less time spent trying to create usable insights across disparate security devices
- Automated responses based on network and device status
- Create integrated workflows that automatically capture suspect traffic

Conclusion

A VSS NPBs enables you to deploy groups of inline or out-of-band security devices on single or multiple links – without impacting the network. If you need to make changes to the security infrastructure – for example, reordering the devices or reconfiguring the type of traffic each receives – you have complete control, without concern over network downtime. This security monitoring and visibility capability is well-suited to support a wide range of layered security technologies and provide agile InfoSec in the areas of:

- Deploying groups of inline or out-of-band security tools on a single or multiple links – without impacting the network
- Make changes to the security infrastructure – for example, reorder or reconfigure the type of traffic each tool receives – without concern over network disruption or scheduling midnight maintenance windows
- Central management and control over global visibility and the traffic flow to each security tool

Footnotes:

[1] Check Point Software 2015 Security Report

https://www.checkpoint.com/resources/2015securityreport/CheckPoint-2015-SecurityReport.pdf

[2] Gartner Worldwide Information Security Spending August 22, 2014

http://www.gartner.com/newsroom/id/2828722

SANS Analytics and Intelligence Survey 2014

http://www.sans.org/reading-room/whitepapers/analyst/analytics-intelligence-survey-2014-35507

Tackling Attack Detection and Incident Response, Enterprise Strategy Group (ESG), April 2015

http://www.mcafee.com/us/resources/reports/rp-esg-tackling-attack-detection-incident-response.pdf