SOLUTION BRIEF

NPB Automation Dramatically Improves Security and Monitoring Response Times

Deployment Scenario: Inline & Out-of-Band Visibility

In the past, static programming for data filtering to security and monitoring tools has been a good practice. Unfortunately, with the myriad of changing security threats and the need for maximum network uptime, IT personnel cannot accept the time limitations of that process anymore. Data captures and analysis must happen as close to real-time as possible. Automating workflows to create an adaptive monitoring environment is the only way to address the new needs.

Automation of network monitoring allows you to align your security and monitoring tools with dynamic network changes to increase operational efficiencies. This creates an adaptive monitoring environment. The automation capability does this by creating a tight integration between a network controller device (like a Security Information and Event Management (SIEM)) and a network packet broker (NPB).

Solution Components:

- Keysight Network Packet Brokers
- Security Tools
- Monitoring Tools

Benefits

- Respond to security
- Improve MTTR objectives with a faster response to problems
- Reduce costs by integrating monitoring activities with orchestration systems
- Simplify element management by integrating monitoring equipment with system managers

KEYSIGHT TECHNOLOGIES

Solution Overview

This network visibility solution allows you to:

- Improve operations by integrating a SIEM with an NPB to pass specific data to specific security tools for further analysis
- Implement NPBs that can automatically respond to network incidents with actions in near real-time
- Use REST interfaces to allow commands from a network management system (NMS), SIEM, policy controller, or orchestration system to be understood by an NPM for security incidents, network incidents, or equipment changes

There are typically three main groups within IT that need adaptive monitoring (or automation of monitoring functions)—the network security group, the IT operations group, and the network monitoring group.

What is Adaptive Monitoring?

There are typically three main groups within IT that need adaptive monitoring (or automation of monitoring functions)—the network security group, the IT operations group, and the network monitoring group. The main driver for the security group is a faster, real-time response to security threats while the main driver for the operations group is achieving operational efficiency to reduce manual processes and the delays/errors that those processes introduce. For the tools group, the main driver is to increase the monitoring capability for the whole network because most IT departments usually do not have enough money to provision multiple sets of tools across the whole network.

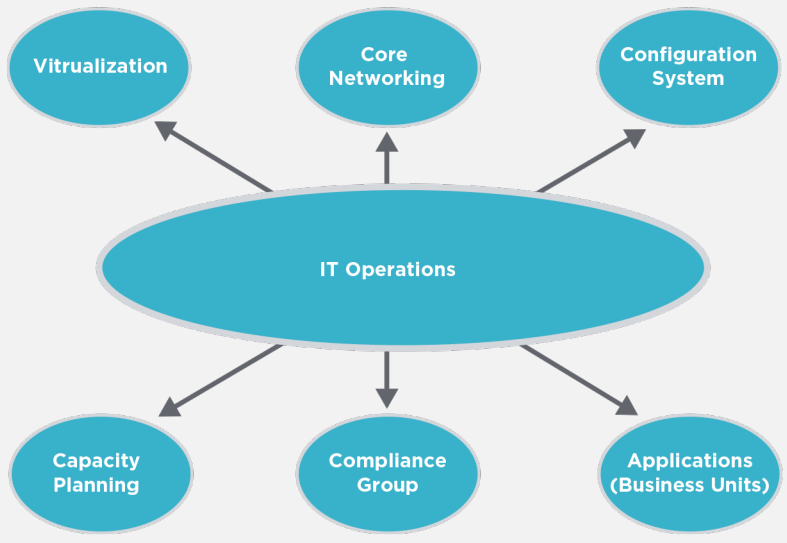

Figure 1. IT Operations Group

This solution allows an automated data center controller to send commands to an NPB to initiate various functions. This automation is akin to software-defined networking (SDN). However, the source of the command does not have to be an SDN controller. It could be an NMS, data center provisioning system like operational system support (OSS) or an orchestration system, a SIEM tool, or another management tool on your network. The adaptive monitoring function can be triggered in response to internal events (based upon some filter parameter or event monitoring parameter) or external events (such as Simple Network Management Protocol (SNMP) traps, SNMP polls, Syslog, NMS events, SIEM events, or other software tool that supports a RESTful interface).

Dynamically changing security threats mean that what an enterprise needs to monitor is constantly changing. In addition, increasing network speeds makes it impractical to perform deep packet inspection on all traffic.

SIEM Integrations Automate Threat Detection and Mitigation

Dynamically changing security threats mean that what an enterprise needs to monitor is constantly changing. In addition, increasing network speeds make it impractical to perform deep packet inspection on all traffic. The security tools only have time to look at relevant data, not all of the data. Hence, an NPB is needed to filter out non-essential information. A typical use case is for a SIEM to analyze data to detect any anomalies. SIEMs use log data to provide a wide view of the network and have powerful correlation capabilities. However, SIEMs themselves do not have packet-level visibility to analyze anomalies in detail.

Once the SIEM finds an anomaly, it can send a command through a REST interface to an NPB. Incident remediation can begin the instant an anomaly occurs because the security tools and engineers have all the information they need. This type of solution speeds up root cause analysis, eliminates time consuming manual steps, and simplifies compliance. Keysight's SIEM integration allows customers to leverage their investments in SIEM and packet based tools to dynamically adjust what they monitor and protect.

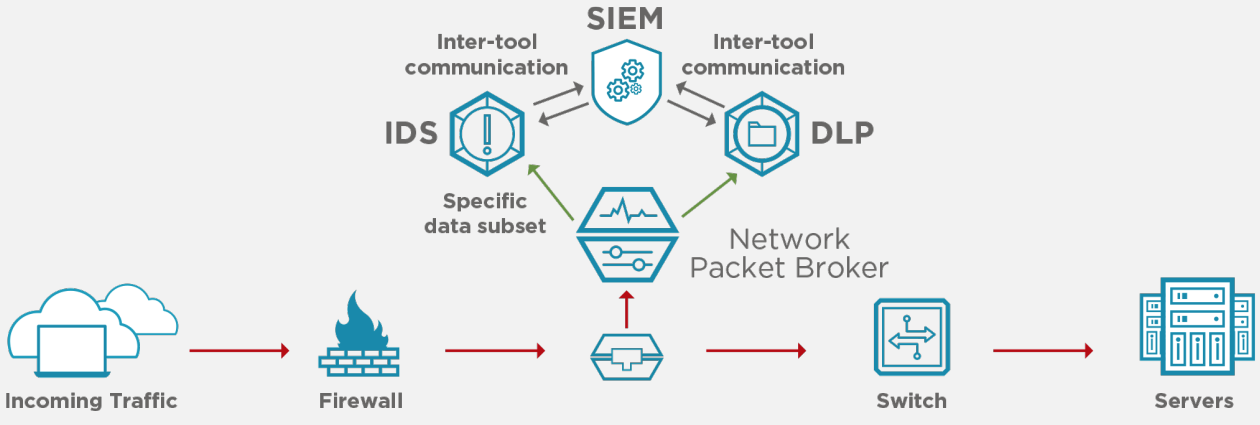

Figure 2. Integration between an NPB and a SIEM

Implement Automation to Reduce Time to Resolution

Reducing the time that it takes to resolve network problems is an important for any organization. Reducing this time is directly dependent upon determining the problem. In fact, according to ZK Research, 85% of mean time to repair (MTTR) is due to just trying to figure out what the problem is. Automated workflows can help in this area to speed up root cause analysis.

Automation of packet captures is an important tool for problem diagnosis. Most IT departments usually do not have enough money to provision multiple sets of tools across the whole network. By automating packet captures and tool filtering based upon network events, critical diagnosis information can be captured to speed along the problem resolution process. The previously existing delay time to recreate an event and start a manual packet capture has been eliminated. This is especially true for spurious/intermittent anomalies.

With the automated packets captures comes reduced operational costs and increased ease of use. This is because the staff doesn't have to spend time constantly writing and rewriting static filter rules. In addition, there is a reduction of errors that are typically associated with manual programming.

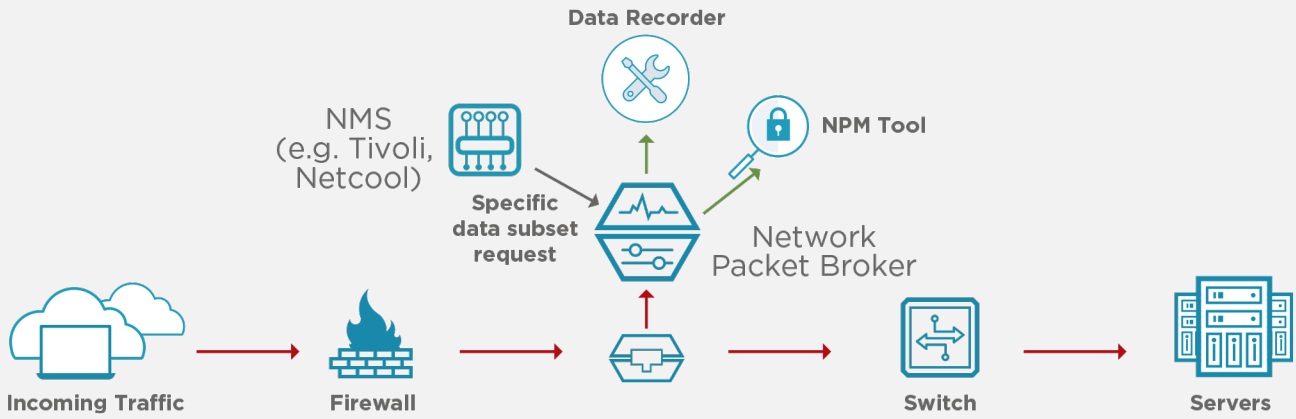

Figure 3. Integration between an NPB and an NMS

According to ZK Research, 85% of mean time to repair (MTTR) is due to just trying to figure out what the problem is. Automated workflows can help in this area to speed up root cause analysis.

Summary

Automation of network monitoring equipment, particularly NPBs, has a powerful capability to improve network threat protection, security event analysis, and network impairment remediation. Outdated manual processes are automated to speed up incident detection and mitigation. This also has the effect of lowering OPEX and CAPEX costs for security events, troubleshooting, and user/equipment orchestration.

Visibility Architecture Solution from Keysight

Keysight's network visibility solution involves using NPBs in conjunction with taps.
Learn more about Keysight's Network Packet Brokers and Visibility Architecture Technology.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES