WHITE PAPER

A Four Step Approach to Improve Security Threat Response

Network Security Has Changed

Modernization of government security infrastructure initiatives (like Executive Order 13,800 and the NIST Framework for Improving Critical Infrastructure Cybersecurity) create a larger need for data visibility within the network. This is for one simple reason—you cannot defend against what you cannot see. When it comes to threat response, network visibility is security. To accomplish this goal, government agencies need to create a visibility architecture and then integrate that visibility architecture with their security architecture. Once this is complete, organizations can create a proper threat response to protect their mission critical infrastructure.

You cannot defend against what you cannot see. When it comes to threat response, network visibility is security.

It is important to be able to identify threats, but also to have the ability to pivot and mitigate once an attack or breach is recognized. This is implemented through a combination of tools that deliver intrusion prevention, suspicious data inspection, improved data analysis, and automation of component actions.

There are four actions you need to take to strengthen network security. These actions will accelerate security data acquisition and reduce manual processes, resulting in a more agile security response. These actions are:

- Maximize intrusion prevention by updating perimeter threat detection technology
- Enhance real-time inspection of suspicious data
- Simplify the data capture and analysis process
- Automate responses to remove time delays in manual processes

KEYSIGHT TECHNOLOGIES

Updating Intrusion Prevention Techniques

An important weapon in effective security architectures is the ability to prescreen data at an organization's perimeter. This is where an inline threat intelligence gateway can be extremely beneficial. The gateway inspects data at the network ingress to determine if it is coming from a known bad IP address. These bad data packets can be automatically eliminated before they can penetrate into the network and cause any harm. If the threat intelligence gateway's access list is updated on a daily basis, then these appliances can provide a formidable defense against the onslaught of malicious traffic that is being generated.

By eliminating even thirty percent of unwanted traffic, threat intelligence could save companies some 7,000 hours per year, or the equivalent of 150 weeks in professional time. This can mean a savings of $300,000 per year.

Even with firewalls, IPSs, and a wide array of security tools in place, businesses still miss clues and suffer major breaches every day. Why? Because the sheer volume of alerts being generated places a huge processing drain on the security team, as well as the infrastructure itself. This translates into wasted time and money as well as an increased risk of falling victim to an attack.

Threat intelligence gateways have been proven to reduce false positive security alerts. By pre-filtering known bad IP addresses and traffic from untrusted countries, you can stop unwanted traffic from ever reaching the firewall. Blocking large volumes of traffic based on IP address, location, and bad behavior enhances your security architecture performance, and reduces your team's "alert fatigue."

Reducing the amount of time spent investigating false positive alerts also creates clear cost savings. A 2015 Ponemon Institute report states that security teams at large enterprises waste more than 20,000 hours per year chasing false-positive alerts[1]. By eliminating even thirty percent of unwanted traffic, threat intelligence could save companies some 7,000 hours per year, or the equivalent of 150 weeks in professional time. This can mean a savings of $300,000 per year[2].

Additional cost savings can be recognized by using automatic system updates within the threat intelligence gateways to eliminate the need for manual updates of known bad IP addresses in firewalls. One of the drawbacks of a firewall-only approach is that updates to the Internet Protocol (IP) address access lists are typically manual processes. By adding a threat prevention gateway, which uses automated updates for known bad IP addresses, you can significantly minimize both incoming and outgoing traffic to bad actors. This saves hours of configuration time over a firewall-only approach.

Data egressing the network can also be inspected by threat intelligence gateways. Should malware exist within the network and try to exfiltrate data or communicate with

1 The Cost of Malware Containment 2015, Ponemon Institute. January 26, 2015.

2 The Definitive Guide to Visibility Use Cases, Keysight Technologies. December 2017.

a known bad IP address, that IP traffic is eliminated at the threat intelligence gateway before any data can leave the network. This offers another layer of security.

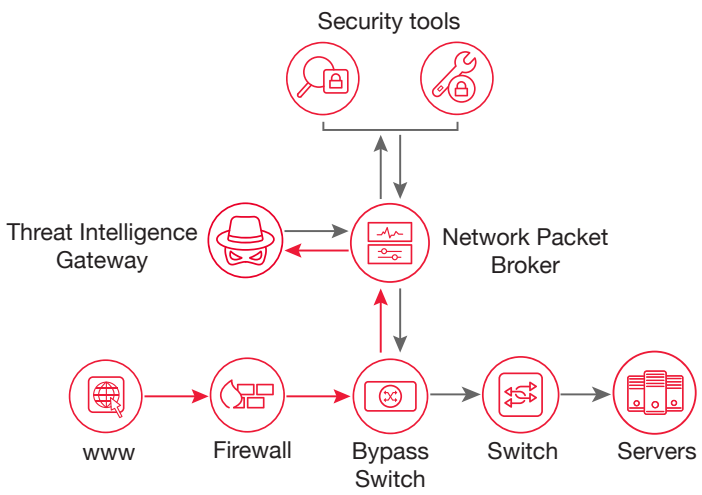

Figure 1. Deployment of a threat intelligence gateway.

As of 2017, over 50% of network attacks are now hidden in SSL encrypted traffic.

To thwart this new threat, encrypted data can be decrypted at the edge of the network to allow data inspection tools to see potentially hidden malware.

Enhancing Data Inspection

A second set of actions to consider is to focus on enhancing the inspection of suspicious data entering your agency's network. There are two common techniques for this:

- Deployment of SSL/TLS decryption capability
- Deployment of inline security inspection tools

Most enterprise applications are now encrypted using the secure sockets layer (SSL) standard, or its updated version called transport layer security (TLS), to thwart security attacks and hackers. Unfortunately, bad actors have adapted to the new security defenses and are using encrypted data to their advantage. These bad actors are able to hide malware within encrypted data streams and use of this attack mechanism is growing rapidly. As of 2017, 50% of network attacks are now hidden in SSL encrypted traffic according to a Computer Weekly article[3].

To thwart this new threat, encrypted data can be decrypted at the edge of the network allowing data inspection tools to see hidden malware. Without decryption, the only options to manage encrypted traffic are to eliminate the traffic at the edge (reducing risk but disrupting business communications), or allow the traffic to transit uninspected, operating on the assumption that the data is safe (which increases security risk).

If decrypted, data can be fed to the security architecture for complete inspection. In the case of inline deployed security tools, decrypted data can be fed to intrusion prevention

3 "Encryption hiding malware in half of cyber attacks," Computer Weekly, Aug. 30, 2016.

system (IPS), next generation firewall (NGFW), web application firewall (WAF), and data loss prevention (DLP) tools for inspection. Suspicious data can go through multiple analysis stages and security threats can then either be halted in real-time or diverted to a sandbox for further analysis.

It should be noted that decrypted data can also be used by out-of-band tools like intrusion detection system (IDS), DLP, and/or a security information and event management (SIEM) to maximize network security defenses. At this point, however, the data has already entered the network so the risk to the organization for this methodology is much higher than using inline security tools.

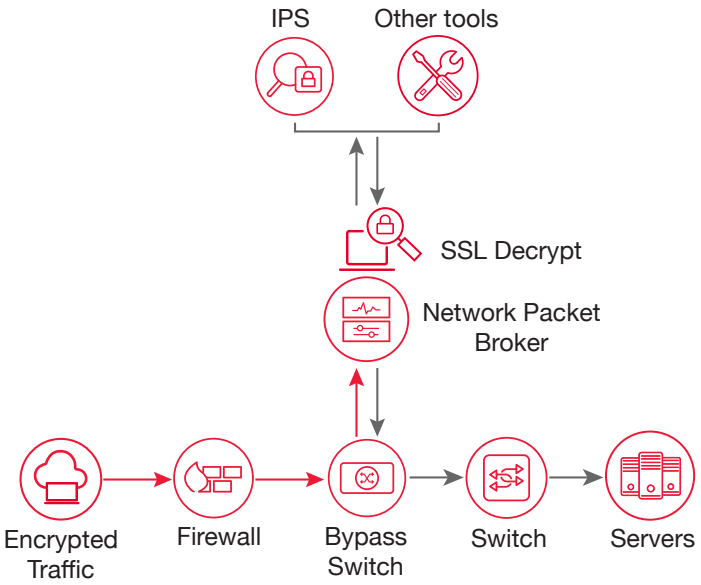

Figure 2. Example configuration of inline SSL/TLS decryption.

Filtering means only the "right" information is sent to the tools and data can be segmented out so that only certain pieces of information go to specific tools. A network packet broker (NPB) is a specialized filtering device that make this objective easy.

Simplifying The Monitoring Data Capture and Analysis Process

Another important activity is to improve monitoring data capture and analysis processes. Inefficient capture and analysis results in higher costs, slower response times, and higher risk that an attack or breach will go undetected for a longer period of time.

Four recommendations to improve data capture and analysis processes include:

- Deploy filtering to deliver the right data to the right tool for faster analysis/resolution
- Capture the right data, which is often a combination of data types (e.g. packet data and flow data)
- Deploy application intelligence that can help recognize indicators of compromise
- Incorporate feature rich dash boards (such as those from Splunk and Plixer) for improved data analysis

Monitoring data is often collected at multiple points within the network and from multiple types of devices (test access point (tap), switched port analyzer (SPAN), bypass switch, etc.). Since the data coming in from these devices is often unfiltered or minimally filtered, at least some of the data will need to be filtered before being sent on to the appropriate monitoring tool. Filtering means only the "right" information is sent to the tools and data can be segmented out so that only certain pieces of information go to specific tools. A network packet broker (NPB) is a specialized filtering device that make this objective easy. It also performs aggregation, load balancing, and packet manipulation.

Other NPB functions, such as deduplication, packet slicing, time stamping, data masking, etc., can be applied to the data to condition it. These features make the monitoring tools more efficient – which means they can process more data than without the packet broker. For instance, if SPAN ports are used, then they often create a lot of duplicate data because of the way the data capture is performed. If you are also looking at data from multiple network segments, then you will typically see duplicate data being sent to the monitoring tools. It is common to see 40% (or more) of duplicate monitoring data within a network.

Some tools can perform deduplication as well. The issue with the tool doing this is that you are now spending tool CPU resources and time to perform this function. This slows down the processing capability and might even necessitate buying another tool to handle the extra load. Since tools are often expensive, this can become a costly choice. A packet broker is usually a more cost-effective alternative.

Application intelligence lets the packet broker perform true signature-based application identification and filtering. This gives you much more control over exactly what you want to monitor.

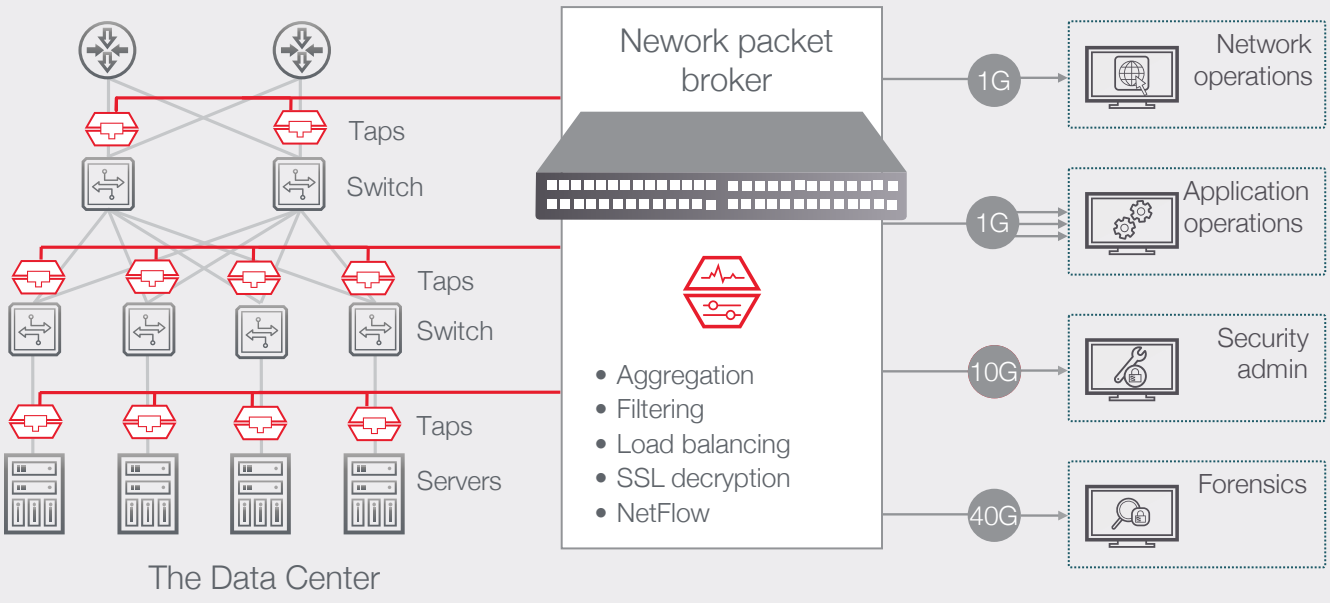

Figure 3. Visibility architecture example based upon a network packet broker.

Some NPB vendors provide a more advanced level of intelligence within their packet brokers. For instance, application intelligence lets the packet broker perform true signature-based application identification and filtering. This gives you much more control over exactly what you want to monitor. For instance, maybe you only want to see Facebook data or do not want to analyze Netflix data. That data is easily identified in the filtering process by isolating on the application type.

In addition, the application intelligence gateway can generate NetFlow data and additional metadata (such as geolocation, user browser type, user device type, etc.). NetFlow and metadata can be used in analysis tools to create very detailed contextual insights, and to further optimize analysis resources. Data masking, regular expression (Regex) searching, and packet capture (PCAP) capabilities are also provided to help analyze specific data natively within that solution or by third-party tools.

One of the fundamental use cases for application intelligence is to recognize indicators of compromise (IOC). The main purpose of investigating IOC is so that you can discover and remediate breaches faster. Security breaches almost always leave behind some indication of the intrusion, whether it is malware, suspicious activity, some sign of other exploit, or the IP addresses of the malware controller.

To thwart security attacks and exfiltration of data, you need the ability to detect application signatures and monitor your network so that you know what is, and what is not, happening on your network. This allows you to see rogue applications running on your network along with visible footprints that hackers leave as they travel through your systems and networks. The key is to look at a macroscopic, or application view, of the network for IOC.

For instance, suppose there is a foreign actor in Eastern Europe (or other area of the world) that has gained access to your network. Using application data and geolocation information, you would easily be able to see that someone in Eastern Europe is transferring files off of the network from an FTP server in Dallas, Texas back to an address in Eastern Europe. Is this an issue? It depends upon whether you have authorized users in that location or not. With application intelligence enhanced IOC, you now know that the activity is happening. The rest is up to you.

Lastly, an easy to use user interface will help tremendously. When creating and modifying filters, a graphical user interface (GUI) reduces a significant amount of time over command line and menu driven interfaces. In addition, a well-designed dashboard provides the optimum ability to view pertinent application and flow data. Without the right dashboard, key pieces of information could be hidden, allowing for attacks to succeed and breaches to continue longer than should have.

Automation means packet brokers can initiate functions (e.g., apply filters, add connections to more tools, etc.) in response to external commands. This data center automation is akin to software defined network (SDN) capabilities, which allow a switch/controller to make real-time adjustments in response to events or problems within the data network.

Automation of component responses dramatically improves monitoring response times

When responding to security threats, time is obviously of essence. Component automation is a very powerful way of removing time delays associated with manual processes.

One of the most powerful, but often overlooked, features for data center automation is automating the network packet broker. In this case, automation means packet brokers can initiate functions (e.g., apply filters, add connections to more tools, etc.) in response to external commands. This data center automation is akin to software defined network (SDN) capabilities, which allow a switch/controller to make real-time adjustments in response to events or problems within the data network. However, the source of the command doesn't have to be an SDN controller. It could be a network management system (NMS), provisioning system, or some other management tool in your network.

Automation of network monitoring allows you to align your tools with dynamic network changes to increase operational efficiencies and create an adaptive monitoring environment.

Conclusion

Government agencies are under constant attack. In addition to the loss of state secrets and personally identifiable information (PII) that may be lost, any breach that occurs is a high-profile event. A solid security architecture with modern defenses is required.

As part of this initiative, there are four actions that will strengthen network security by speeding data acquisition and reducing manual processes: focusing on intrusion prevention, suspicious data inspection, improved data analysis, and automation of component actions. In addition, a strategy that integrates a visibility architecture with the security architecture is required. Network visibility is integral to network security. With this complete approach, you have the capabilities to create a proper threat response and protect your mission critical infrastructure.

Keysight network visibility solutions are a powerful way to optimize your network monitoring architecture and strengthen your network security. The Vision ONE and Net Tool Optimizer have achieved FIPS 140-2 validation and Common Criteria Certification – both help address the new Executive Order and NIST Cybersecurity Framework.

For more information on network monitoring solutions, visit www.keysight.com/solutions/network-visibility.

A strategy that integrates a visibility architecture with the security architecture is required. Network visibility is integral to network security. Once this is complete, you have the capabilities to create a proper threat response and protect your mission critical infrastructure.

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