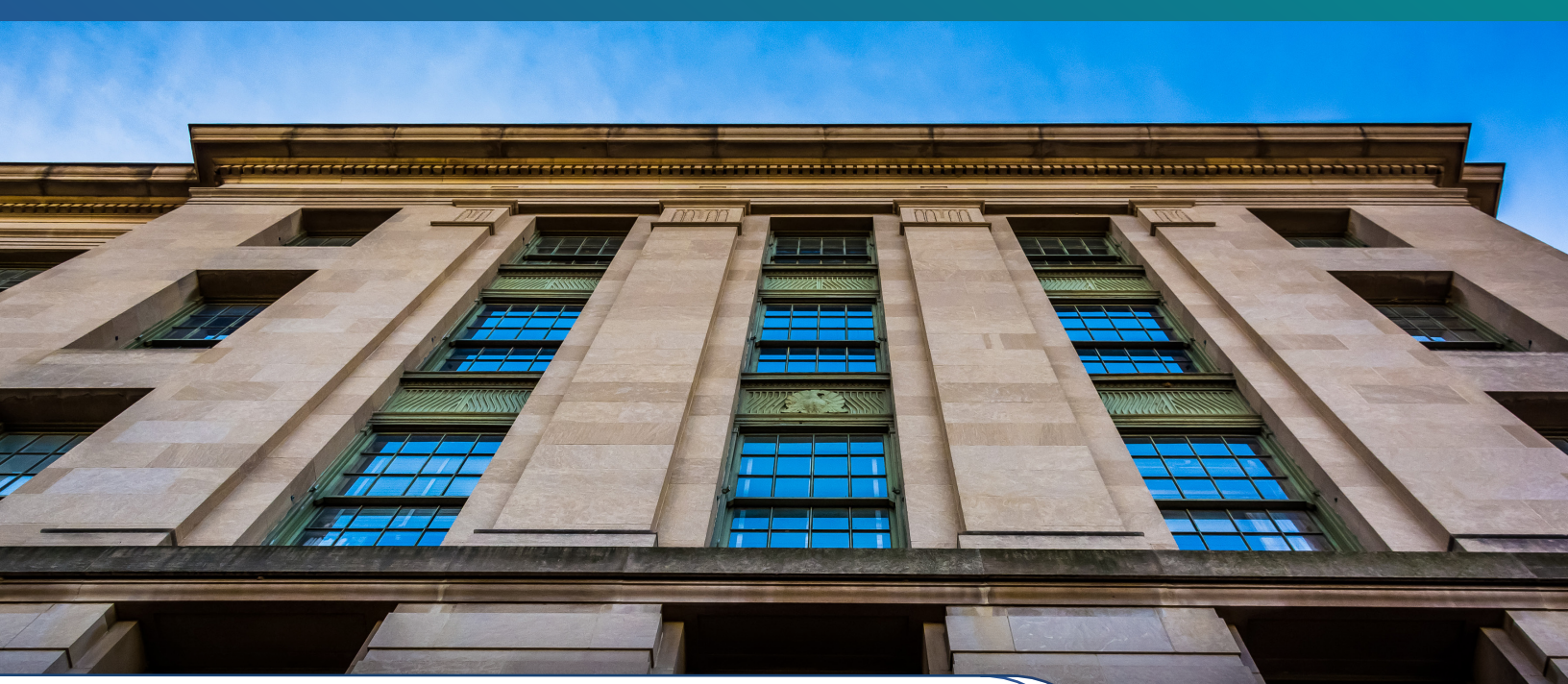

WHITE PAPER

Government IT: A Four-Step Approach to Improve Network Security

Ransomware's success and profitability have dramatically increased the number of cyberattacks on government entities worldwide. The resources and assets that federal, state, and local agencies control are often sensitive, critical to the functioning of society, and marked by security vulnerabilities. Internationally, cyberattacks have become the preferred weapon of geopolitics.[1] SecuLore, which tracks reported security attacks, found a 164% increase in monthly incidents at the state and local levels over the two years ending August 2019.[2]

The Security Perimeter Has Changed

Modernization of government technology infrastructure has expanded the network perimeter and increased the attack surface for government entities. Potential points of entry to a network include Internet of Things devices, Wi-Fi-enabled mobile devices, cloud applications, and remote offices. To protect this expanded attack surface, security managers must understand the context of the traffic flowing within their networks and be prepared to act as soon as they have identified malicious or anomalous behavior.

1 O'Neill, Patrick Howell. "Hackers will be the weapon of choice for governments in 2020." MIT Technology Review, January 2, 2020. https://www.technologyreview.com/s/614974/hackers-will-be-the-weapon-of-choice-for-governments-in-2020.

2 Miller, Ben. "Hackers Are Hitting Government More, but That's Nothing New." Government Technology, September 23, 2019. https://www.govtech.com/data/Hackers-Are-Hitting-Government-More-but-Thats-Nothing-New.html.

KEYSIGHT TECHNOLOGIES

Cybersecurity requires total network visibility for one simple reason: you cannot defend against what you cannot see. When it comes to threat response, network visibility is the foundation of security. To practice defensive security, government agencies need to deploy a visibility platform and integrate it with their security architectures. Once agencies achieve total visibility, they can activate a proper threat response to protect their mission-critical infrastructure.

Government IT can take four actions to strengthen network security:

- maximize intrusion prevention
- enhance real-time inspection of suspicious traffic
- simplify data capture and analysis
- automate and accelerate threat response

This paper examines each action in more detail.

1. Maximize Intrusion Prevention

The first important action is prescreening data at the network perimeter. The perimeter is where an inline **threat intelligence gateway** can be beneficial. The gateway inspects data at the ingress point to see if it is coming from a known-bad IP address, then automatically eliminates traffic from these addresses before it can pass into the network and cause harm. If the gateway receives updated intelligence daily, these appliances provide a formidable defense against the onslaught of malicious traffic.

Even with firewalls, intrusion protection systems, and other security tools in place, organizations still suffer major breaches every day. Why? Because the sheer volume of alerts places a huge burden on the security team and the infrastructure itself. This translates into wasted time and resources, as well as an increased risk of falling victim to an attack. Another advantage of threat intelligence gateways is that they reduce false-positive alerts, so staff can focus on true threats. This focus is particularly important as there is a massive shortage of cybersecurity professionals worldwide.[3]

Intelligent gateways offer nearly unlimited capacity for maintaining blacklist and whitelist addresses, which makes them superior to a firewall-only approach. You can also configure gateways for automatic daily updates from an approved intelligence feed, eliminating the need for manual maintenance.

A threat intelligence gateway also can inspect data egressing the network. Should malware inside the network try to exfiltrate data or communicate with a known-bad IP address, the gateway will eliminate that traffic before any data can leave the network. This process offers another layer of security.

3 Muncaster, Phil. "Cybersecurity Skills Shortage Tops Four Million." Infosecurity, November 7, 2019. https://www.infosecurity-magazine.com/news/cybersecurity-skills-shortage-tops.

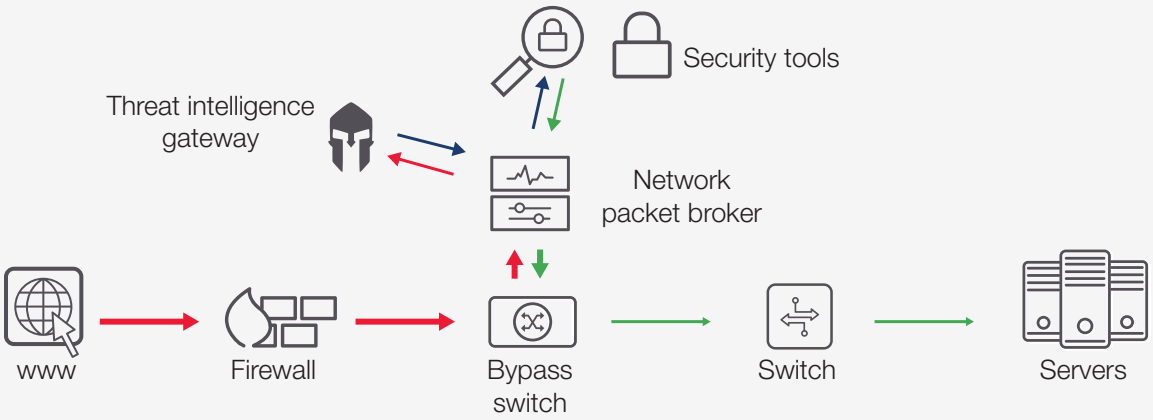

Figure 1. Deployment of a threat intelligence gateway

2. Enhance Real-Time Inspection

A second critical security action is to enhance the inspection of suspicious data entering your network. There are two common techniques for this:

- deployment of Secure Sockets Layer (SSL) or Transport Layer Security (TLS) decryption capability
- deployment of inline security inspection tools

Most enterprise applications employ encryption using the SSL standard or the updated version called TLS to thwart security attacks and hackers. Unfortunately, bad actors have adapted to the new security defenses and are using encryption to their advantage. Hackers can hide malware within encrypted data streams. Use of this attack mechanism is growing rapidly. The latest available data, taken from the Fortinet *Quarterly Threat Landscape Report* for Q3 2018, estimated that 72% of all network traffic uses SSL encryption.[4]

To thwart this technique, decrypt encrypted traffic at the edge of the network to allow data-inspection tools to see hidden malware. Without decryption, the only option for security managers is to allow encrypted packets to flow into the network uninspected, which dramatically increases the risk of attack.

Security solutions, even sophisticated ones, are designed to process plaintext, not encrypted messages. Some solutions include onboard decryption, but this function uses up valuable processing cycles and can seriously degrade tool performance. Many security teams choose to decrypt using a separate device. If they use a network packet broker (NPB) with decryption functionality, they can run the process once and send

4 *Q3 2018 Quarterly Threat Landscape Report*. Fortinet. November 2018. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2018.pdf. Subsequent reports did not update this statistic.

plaintext traffic to multiple inline security tools, such as intrusion prevention systems, next-generation firewalls, and web application firewalls, for inspection. Once an inline tool identifies a suspicious packet, it can drop the packet in real time or divert it to a sandbox for further analysis.

Out-of-band tools, such as intrusion detection systems, data loss prevention (DLP) tools, and security information and event management (SIEM) systems, also require decrypted data. At this point, however, the data has already entered the network, so the risk to the organization from this methodology is much higher than it is from using inline security tools.

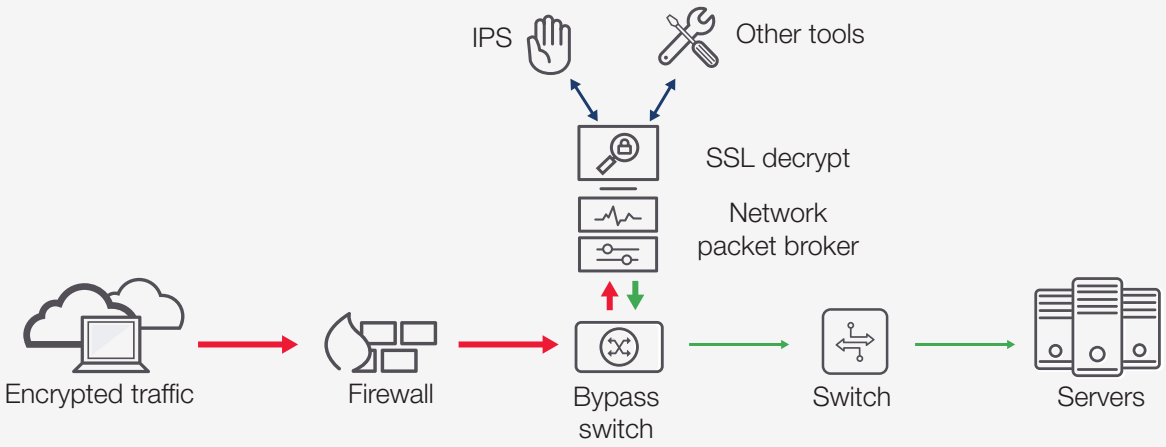

Figure 2. Example configuration of inline SSL / TLS decryption

3. Simplify Data Capture and Analysis

Another important security practice is to increase the efficiency and accuracy of data capture and security analysis. Inefficiency can result in higher costs, slower response times, and increased risk that an attack or breach will go undetected by the organization for a longer period.

Here are four recommendations to simplify data capture and analysis:

- Capture the right data, which is often a combination of packet and flow data.
- Use packet filtering to zero in on the specific data needed.
- Leverage application intelligence to recognize indicators of compromise.
- Display results on feature-rich dashboards to increase understanding.

Organizations collect packet data at multiple points in their networks. Packets then need to be aggregated, sorted, and delivered to the appropriate security monitoring tools. An NPB, which performs at high speed and automatically, according to preset rules, can easily execute these actions. An NPB can also load balance the processing workload between multiple devices and control the sequential flow of data from one tool to another. See below for other key functions.

Flow data

Some security analysis tools use both packet and flow data to identify anomalous behavior. If this applies to your environment, you will want an NPB that also can provide your security tools with flow data such as NetFlow.

Packet deduplication

Typically, you would capture network packets using physical and virtual network taps, cloud-native taps, switched port analyzers, and bypass switches. Depending on the placement of these devices and the redundancy built into your network, you could end up collecting many duplicate packets. Forty percent or more of packets commonly are duplicates. To avoid wasting processing cycles on your monitoring tools, you should eliminate redundant packets using your NPB before forwarding the traffic to tools for security inspection and analysis. Since security tools are often expensive, you may be able to justify the purchase of your NPB by reducing your tool capacity requirements.

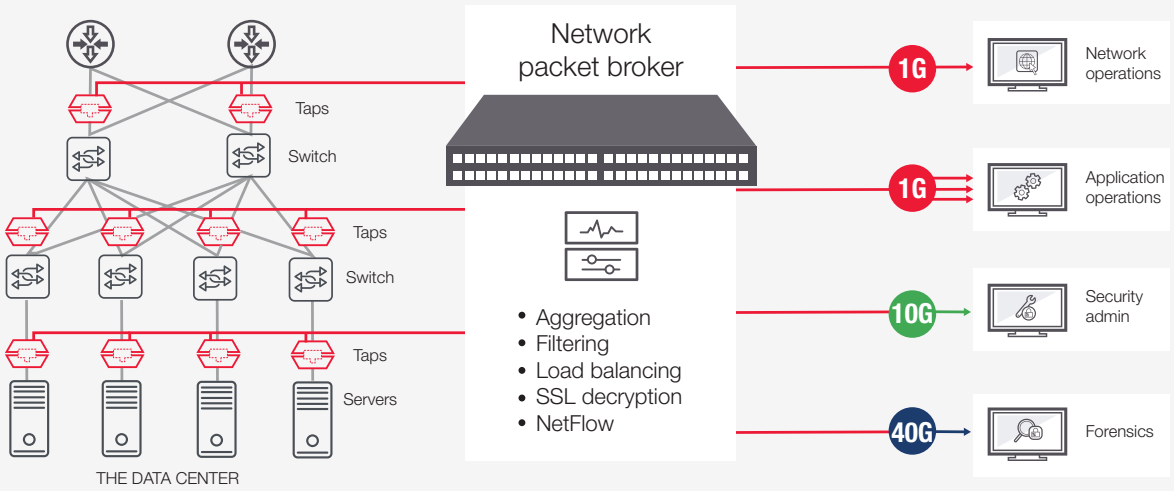

Figure 3. Visibility architecture example based on an NPB

Application intelligence

Some NPBs can understand contextual information associated with a packet — a capability referred to as *application intelligence*. This feature allows the NPB to identify the application associated with the packet, as well as details such as the geolocation, type of networked device, and operating system. Having this information gives you much more control over the data you want to monitor. For instance, maybe you want to exclude Netflix packets from inline security inspection. An NPB with application intelligence can easily identify that data.

Application intelligence also helps your security team recognize indicators of compromise, so it can discover and remediate breaches faster. Security attacks almost always leave behind some indication of the intrusion, whether it is malware, unusual activity, a sign of another exploit, or the IP addresses of the malware controller. For example, application intelligence tells you if a large amount of data flows to a country where you do not do business.

Easy-to-use interface

Security analysts can spend a lot of time creating and modifying data filters or configuring data delivery to new monitoring tools. An easy-to-use NPB with a drag-and-drop graphical user interface will help analysts work more efficiently and make fewer errors. In addition, a well-designed dashboard helps analysts quickly understand pertinent information and take corrective action.

4. Automate and Accelerate Threat Response

When you need to respond to a security threat, time is of the essence. Orchestration and automation are powerful ways of reducing delays associated with manual processes. Examples include

- network packet brokers with RESTful interfaces to SIEMs or DLPs
- serial data chaining of inline security tools
- automated updates of threat intelligence gateways

Automating the NPB

One of the most powerful, but often overlooked, scenarios for security automation is the NPB. In this use case, analysts can program the NPB to execute a function such as aggregating traffic for certain applications or sending traffic to an additional security tool in response to an external command. The command can come from a network management system (NMS), provisioning system, SIEM, or other management tool in your network.

Automated security monitoring allows you to respond instantly to dynamic network conditions and increase operational efficiencies. Internal and external events can trigger automation. Internal events include a filter parameter or event monitoring parameter. External events include Simple Network Management Protocol traps, Syslog, NMS events, or SIEM events.

For example, if your SIEM identifies a problem, it can tell your NPB to start a specific packet capture or initiate the forensic recorder. In this way, incident remediation can begin the instant an anomaly occurs. The automation speeds up root-cause analysis, eliminates time-consuming manual steps, and simplifies compliance.

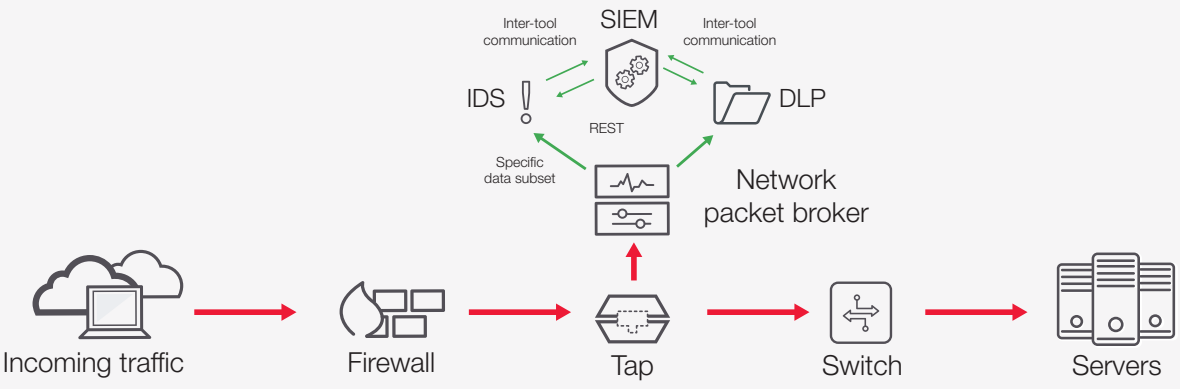

Figure 4. Automation example using an NPB connected to a SIEM

Serial tool chaining

Another powerful use for automation is the movement of data packets serially through a chain of security solutions. This lets you send suspect data identified by one tool for further inspection by another tool. Packets without anomalies move into the network quickly to maintain maximum response time. An NPB is also the enabler for this functionality. A well-designed NPB can support complex service chaining with many rules in parallel, serial, or a combination.

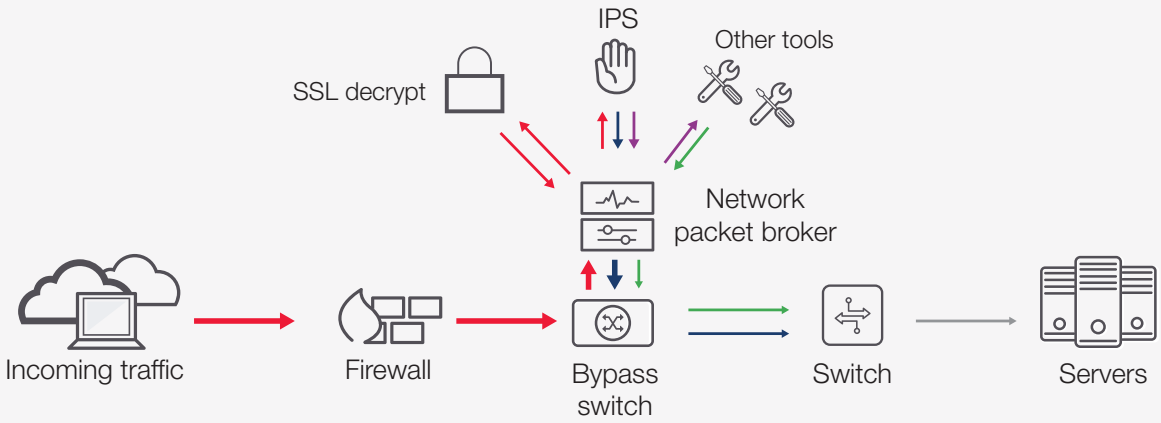

Figure 5. A tool chaining example based on an NPB

Intelligence updates

As mentioned earlier, you can use a threat intelligence gateway to prevent the exfiltration of data to blacklisted sites. Entities generally subscribe to a threat intelligence feed and use it to keep the site list updated. You can configure some gateways to receive automatic daily intelligence updates and maintain the site list. This practice reduces false positives and the effort required to maintain functionality.

Conclusion

Government agencies are under constant threat of cyberattack. The potential disruption of public services, exorbitant ransom, and loss or exposure of sensitive data are serious concerns for federal, state, and local entities alike. In addition, breaches can be high-profile events that undermine the confidence of citizens and business partners. Responding to these threats requires a solid security architecture with modern defenses.

The foundation of strong network security is total network visibility. The security architecture you deploy on top of your visibility platform should have robust strategies to maximize intrusion prevention, enhance real-time inspection of suspicious traffic, simplify data capture and analysis, and automate threat response. With this two-pronged approach, you will have the capability to initiate a proper threat response and protect your mission-critical infrastructure.

Learn about Ixia's network visibility and security solutions for government at: https://www.ixiacom.com/solutions/segments/government-solutions.

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