WHITE PAPER

Regulatory Compliance

and Other Networking Challenges

A top concern of corporate IT departments today is how to maintain compliance with evolving regulatory initiatives. To maintain compliance, organizations need to establish greater visibility into the data that flows through their networks, where it goes, and how to control it. They can achieve this by creating a visibility architecture, which is end-to-end infrastructure that delivers network, application, and security visibility. This visibility allows you to optimize your network data capture, data privacy, and compliance verification techniques.

Deployment of data masking, network monitoring, regular expression (regex) searching, packet trimming, and lawful intercept enables organizations to better comply with local and international regulations.

This paper outlines how to use network visibility to meet compliance initiatives, including the following:

- enhancing regulatory compliance with data masking
- discovering rogue IT on your network
- searching for and capturing specific data with application intelligence
- eliminating sensitive data propagation with packet trimming
- performing lawful intercept data captures
- enforcing IT network security and compliance policies
- documenting security policies for regulatory compliance

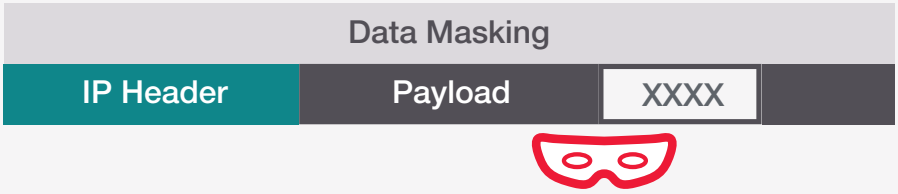
KEYSIGHT TECHNOLOGIES

Enhance Regulatory Compliance with Data Masking

Summary

- Data masking protects sensitive regulatory compliance information
- Data masking is one of the top five most commonly used network packet broker (NPB) features.
- NPBs can mask monitoring data and forward it to specific analysis tools for inspection.

Deployment scenario: Out-of-band visibility architecture



Solution overview

Regulatory compliance is a concern for enterprises. Just when you think you have the network set up correctly, some company business decision adds products and applications to (or removes them from) the network. This can cause new compliance issues. For instance, recent regulations typically demand the protection of personally identifiable data, whether at rest, in motion, or in use.

A common way to secure this data in monitoring solutions is to mask it to protect it as the data passes downstream to other tools. Using real-time packet data analysis and replacing data with a fixed-field value before forwarding it to security and monitoring tools is possible. This is one of the top features of a packet broker.

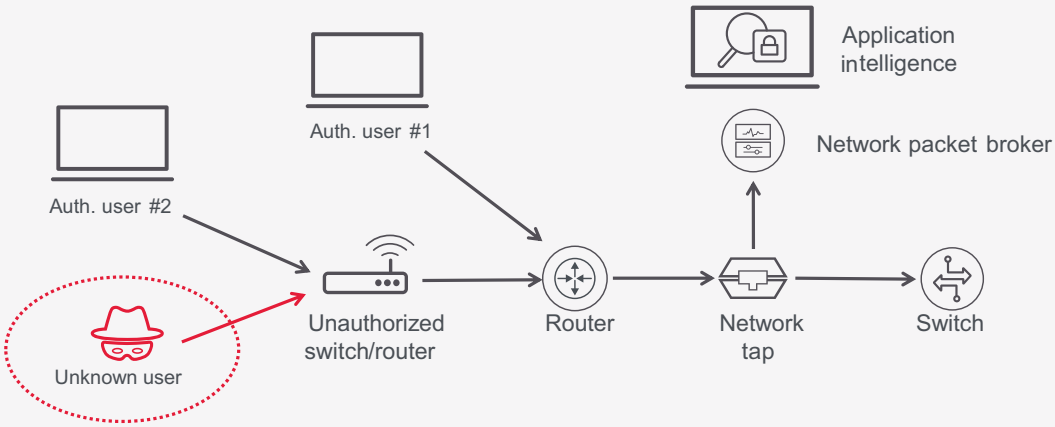
Masked data is still useful. For instance, for credit card data, you would mask only the first 12 digits and leave the last four unmasked. This would allow tools to search the data for use of specific credit card numbers. Maybe you leave the first digit unmasked, as well. This allows your tools to perform searches to categorize the types of credit cards in use — American Express, Visa, Mastercard, Discover, and so on. The level of masking is user-determinable.

Discover Rogue IT on Your Network

Summary

- Deploy an NPB with application intelligence to discover unauthorized activity.
- Identify user equipment and device types added to the network.
- Detect signatures of applications not authorized for the network.
- Protect against unauthorized use of network resources.

Deployment scenario: Out-of-band visibility architecture



Solution overview

Rogue IT is when users add their own equipment and applications to the network. This includes portable Ethernet switches, Wi-Fi access points (such as a Wi-Fi hotspot from an iPhone), and off-network data storage (like Dropbox), or any other additions to the network. These examples should (as a best practice) be violations of company security policies, because they introduce potential vulnerabilities. IT rarely knows anything about these devices, especially as they can appear sporadically, like Wi-Fi hotspots.

To thwart these compliance and liability threats, you need to be able to monitor your network and detect application signatures, so you know what is and what is not happening on your network. This lets you see rogue applications running on the network, along with visible footprints that hackers leave behind as they travel through your systems and networks. Application intelligence can expose hidden applications, geolocation of users, browser types in use, and device types on the network.

As an example, an employee might deploy an insecure hotspot that a hacker can use for criminal activity. The hacker could sit in a van on a public street outside the office and use the hotspot to gain access to the internet through the corporate routers. Once on the internet, the hacker can conduct all sorts of cybercrime (illegal trading,

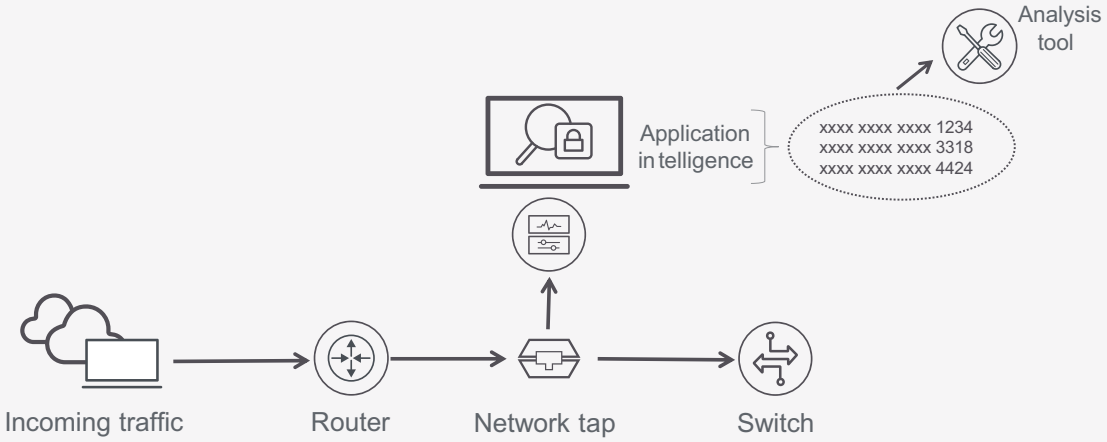
identity theft, cyber espionage, communication with terrorist organizations, child pornography, and hacktivism for political, social, or religious reasons). Law enforcement agencies can trace those crimes back to that business (and that hotspot). This could create issues for both the company and the employee who installed the hotspot. In the end, this behavior could cost both the business and the (possibly soon-to-be-former) employee lots of time, energy, money, and aggravation.

Search for and Capture Specific Data with Application Intelligence

Summary

- Use an NPB with application intelligence to perform granular regex data searches.
- Forward specific data to monitoring tools for further analysis.
- Lower your capex for security and monitoring tools.

Deployment scenario: Out-of-band visibility architecture



Solution overview

Regex searching is another application intelligence capability that lets you search monitoring data. Once the specific information or type of information that matches the search criteria is found, that data can be passed to a security analysis tool (for example, data loss prevention [DLP]) for processing. This search capability helps your tools to be more effective as they have less data to sift through.

Specifically, regex allows you to perform granular searches for data such as credit card numbers, phone numbers, Social Security numbers, emails from certain IP addresses, names, phrases, and specific numbers. By using an NPB with application intelligence to perform the data searches, CPU resources on more expensive monitoring tools can focus on other tasks. This increases the efficiency of the monitoring tools and potentially

lowers your capex costs as you may be able to purchase fewer tools but still accomplish your goals.

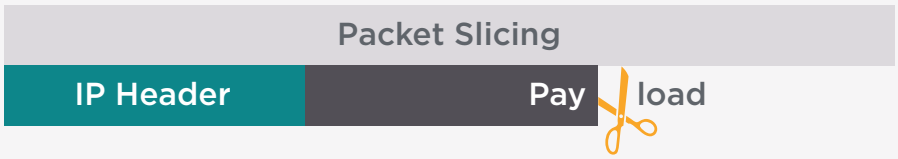
As an example, an NPB with application intelligence can capture credit card data and send it to a purpose-built tool that analyzes the number using the Luhn checksum algorithm. All valid credit card numbers adhere to the Luhn algorithm, a special formula that sums all the digits to come up with a multiple of 10, if the number is valid. If a credit card number fails the test, it is immediately flagged as fraud. Finding fraud more quickly reduces the chance of financial harm. Luhn checksum analysis algorithms are available for other systems, such as Canadian and Greek social security numbers.

Packet Trimming Eliminates Sensitive Data Propagation

Summary

- Use an NPB to remove credit card data, phone numbers, Social Security information, and other sensitive information.
- Data removal reduces the load on the tools by reducing packet size, which frees up long-term storage of unneeded payload information.
- Packet slicing can significantly reduce monitoring data traffic payloads.

Deployment scenario: Out-of-band visibility architecture



Solution overview

Packet trimming (payload stripping) removes the payload data from the packet, leaving only essential envelope information, before sending the packet to monitoring tools. The amount of packet trimming is user-definable (for example, all or just part of the payload).

This feature allows the tool to be more efficient and analyze incoming data faster. Some monitoring tools do not require packet payload information. In that case, removing payload data allows more data to pass across the link from the network monitoring switch to the monitoring tool. As a result, the monitoring tool can process a greater amount of network data.

Another benefit of packet slicing is that once the payload is removed, the sensitive personally identifiable information is gone as well. This technique protects personal data while letting the monitoring data pass downstream to monitoring tools without the worry of a regulatory compliance infraction.

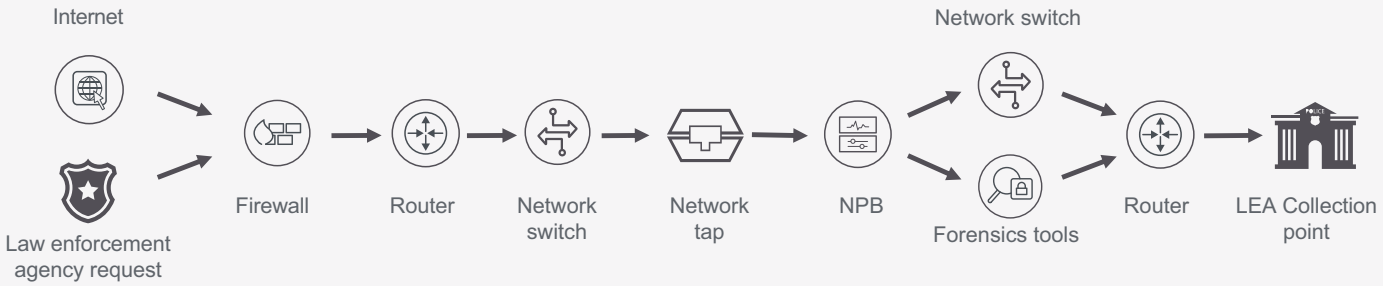
There is a trade-off though. You cannot search the payload data once it has been removed, as it is gone forever. If that is a concern, you should take the data masking approach. Otherwise, you can use this approach.

Perform Lawful Intercept Data Captures

Summary

- Lawful intercept requests for carriers and ISPs.
- An NPB can segment the information sought in a warrant.
- Only relevant pieces of data pass to the law enforcement agency.

Deployment scenario: Out-of-band visibility architecture



Solution overview

The ability to support a lawful data intercept order is becoming increasingly important for service providers. This has also become a new challenge for enterprises. Legally mandated access to communications is expanding as many nations pass laws requiring access to all types of user information, including voice, video, data, and location information. It does not stop there, because the requirements and application of laws vary by country and state.

The US Communications Assistance for Law Enforcement Act (CALEA) applies to more than the public switched telephone network (PSTN) and wireless carriers. Lawful intercept orders are issued to internet service providers (ISPs) as well. Entities with user communication content can overlap in the big data era. This content includes voice communications, video, instant messaging, facsimile, internet connections, digital pictures, text messages, data downloads, and file transfers. A law enforcement agency can request one or more of these content streams under a lawful intercept order. Depending on the number of user communication services an entity provides, it can get very complicated to comply with lawful intercept requests.

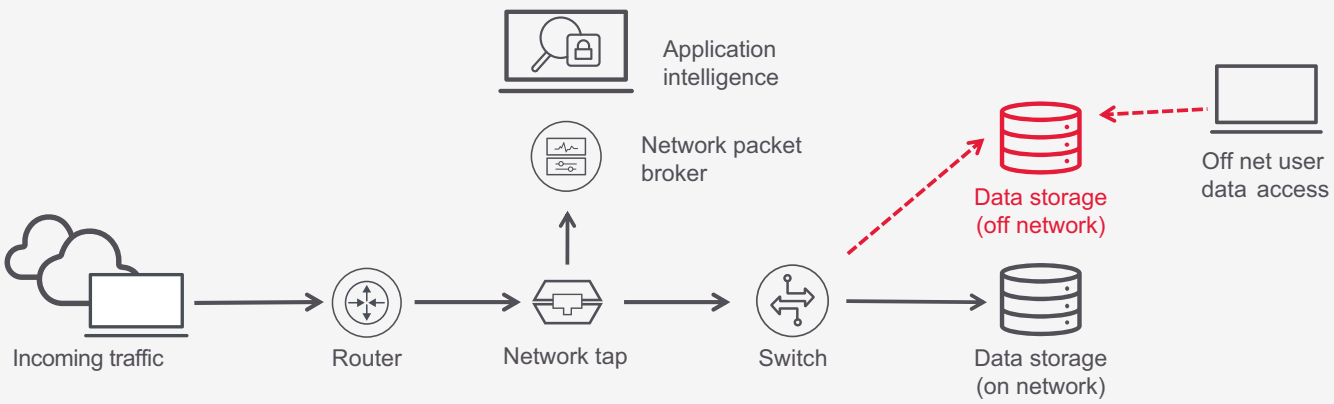
The next issue is how to capture the information. A filtering device can help you capture, filter, aggregate, and segment the necessary data. An NPB can deduplicate data, create detailed rules to segment data packets, aggregate the required data, and send it downstream to the appropriate collection point for the law enforcement agency. NPBs can process data at line rates and eliminate concerns of tainted evidence. The filtering device should be firmware-based, and not a SPAN device. Without an NPB, lawful intercept will be an expensive and painful activity as you try to separate relevant and nonrelevant packet data using other devices.

Enforce IT Network Security and Compliance Policies

Summary

- Use an NPB with application intelligence to validate IT policies.
- Monitor use of unsanctioned storage apps, such as Dropbox.
- Understand if employees are using non-company-standard email services and downloading files through web-based email that bypasses virus inspection.
- Reduce company risk with a defined policy and enforcement method

Deployment scenario: Out-of-band visibility architecture



Solution overview

A fundamental concern for IT is to enforce security and regulatory compliance of network policies. In several cases, they may honestly not know what is happening on the network. This issue has been top of mind for enterprises for several years. How can they reduce corporate risk? Part of the solution is policy-related, but they also need to show due diligence in enforcing policy.

One solution is to use context-aware data processing to monitor the use of cloud applications. For instance, application monitoring lets you know whether employees are using services such as Dropbox to transfer company files and bypass your security policies. People using those services may continue to have access to work-related files even after they leave the company, since IT cannot restrict privileges to off-network storage devices.

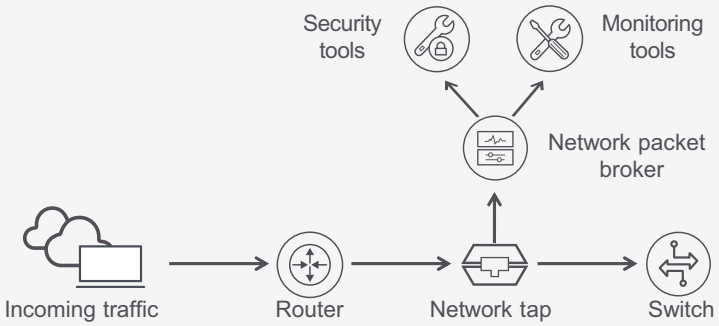
Another example is where employees may be using other, non-company standard email services (such as web-based email) to access and download files. This use case usually involves accessing media that do not go through antivirus or anti-malware inspection. Uninspected file downloads can pose a security threat to the corporate network. These practices could introduce ransomware or create security holes that might allow hackers into the network. Application intelligence helps expose whether specific policy violations are happening on the network.

Document Security Policies for Regulatory Compliance

Summary

- Create empirical data to validate that network policies and procedures are working correctly.
- Properly document data at rest, in use, and in motion for regulatory compliance.

Deployment scenario: Out-of-band visibility architecture



Solution overview

Regulatory compliance requires companies to secure their network data at rest, in use, and in motion. Companies must document their plans and procedures in writing and capture the necessary data. However, you also need to document the validation of these policies. Validation is straightforward, and a visibility architecture helps you accomplish it.

The process starts with capturing the data for both inline and out-of-band data monitoring architectures using taps, virtual taps, and bypass switches. Captured data should pass through a packet broker. The packet broker provides data segmentation to send the right data to the right type of security tools (such as a firewall, next-generation firewall (NGFW), intrusion prevention or detection system (IPS and IDS), DLP, or security information and event management tool [SIEM]) and monitoring tools (such as network and application performance management (such as network and application performance management, proactive monitoring, analyzers, log analysis, and packet captures). The NPB can provide granular segmentation to ensure that tools in use are working correctly. It can apply application intelligence to metadata to illuminate even more information about network policies and procedures.

A visibility architecture allows you to verify who and what are on your network, create a dependencies profile, create an IP address to a MAC table, apply application intelligence to monitoring data, and capture and deliver granular data. It also validates (with empirical data) that the network policies and procedures put in place to protect network data are working correctly.

Conclusion

A strong regulatory compliance strategy requires visibility into network data. This is especially true regarding the EU's General Data Protection Regulation (GDPR), which mandates strengthening network security and preventing data loss. One of the most important parts of a regulatory compliance plan is the network architecture, the foundation upon which your policies and procedures are built upon.

A visibility architecture should allow for data access, data manipulation, and monitoring and compliance. Devices such as NPBs let you mask sensitive data, perform packet slicing, implement lawful intercept, and discover rogue IT. Purpose-built compliance solutions benefit from NPB-filtered data to perform activities better and allow IT to more easily demonstrate regulatory compliance.

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