Protecting Sensitive Data During Monitoring

Over the last two decades, governments around the world have passed legislation regulating the flow of personal information across the network. In 1996, the United State of America (USA) introduced the Health Insurance Portability and Accountability Act (HIPAA), followed by the Payment Card Industry Data Security Standard (PCI-DSS) in 2004 – both of which are in force today.

In 2016, the USA and European Union (EU) introduced the EU–US Privacy Shield, also currently in effect. That same year, the EU introduced the General Data Protection Regulation (GDPR), which will be enforced starting May 2018. The purpose of these regulations is to protect individual privacy and other sensitive data given that so much of our personal information is in electronic form, stored in servers, and transmitted across networks.

Network monitoring also must comply with these standards. NETSCOUT® monitoring and security solutions, in particular its nGenius® Packet Flow System (PFS) products, help ensure that a customer's visibility network complies with these regulations, whether in localized datacenters, within the cloud, or in a hybrid network.

Necessary Features for Visibility Network Compliance

GDPR, HIPAA, and PCI-DSS define the types of personal data that may be collected and recorded, as well as where this data can be sent. To ensure compliance, networking and security teams need to understand which countries' data will be traversing the network, what paths the data will take, where the data will be stored, and all the locations that will have monitoring tools and security applications deployed. Once this is understood, the company will need a visibility network (such as a NETSCOUT unified packet plane) that supports selectively removing or masking out data within packets and obfuscating monitoring traffic as it is backhauled from remote sites to central monitoring locations.

Masking and Slicing

These regulations mean that anything from IP addresses to credit card information will need to be hidden or removed from packets that are to be used in monitoring and/or recording of network traffic.

Figure 1: The NETSCOUT unified packet plane powered by PFOS (Packet Flow Operating System) logically separates the network from the monitoring systems.

The NETSCOUT PFS portfolio supports conditional masking and/or slicing of certain packet types and at specific locations with the packets.

- Packet masking is the act of writing user-defined data over existing data in the packet, effectively hiding the data that was originally in the packet, at a specified starting point in the packet.
- Packet slicing is the act of removing all data from a packet, starting at a specified point in the packet. This has the added benefit of reducing the size of the packet and hence the amount of traffic to be forwarded to the monitoring and security tools. Slicing may be preferable to masking if there are numerous elements of sensitive data scattered throughout a packet.

With the NETSCOUT solution, there is no limit as to where the masking or slicing occurs in each packet.

These capabilities are available on the advanced hardware chassis modules on the nGenius 2200 series packet flow switch and nGenius 4200 series packet flow switch products, on the advanced line cards of the nGenius 6000 series packet flow switch product, and the nGenius Packet Flow eXtender (PFX) series product as well.

Encrypted Forwarding

Unfortunately, when backhauling traffic from remote to central monitoring sites using unsecure methods, the traffic is visible to bad actors. Most tunneling protocols, such as GRE or L2TP, are either UDP or natively IP based, and they do not have any built in method for encrypting the traffic . This makes the tunneled monitoring traffic vulnerable to snooping. These tunneling methods also use a best-effort delivery mechanism, which results in packets not arriving, and have no message transfer unit (MTU) size awareness across the network, which results in packet fragmentation, or worse, packet truncation. Fragmentation places more processing load on the monitoring and security applications to reassemble the fragmented packets to be able to properly analyze them. Truncation makes the packets potentially worthless due to the truncated data simply being lost without any control or selectivity.

NETSCOUT nGenius 2200 series packet flow switch supports a high-throughput encrypted TCP-based tunneling capability, referred to as vStack over TCP/IP. This not only encrypts the tunneled traffic ensuring all monitoring traffic remains obfuscated while being tunneled, but it also provides a guaranteed delivery mechanism as well as negotiated MTU to prevent fragmentation or truncation from occurring.

Conclusion

Ensuring your visibility network complies with GDPR, HIPAA, and PCI-DSS requires knowing your company, its network, and the monitoring and security needs.

Responsibility lies with the operators of the visibility network, as well as the monitoring and security applications, to ensure data is protected by design and by default, covering the data control, forwarding, and processing functions. Being educated in data protection and privacy is critical.

NETSCOUT is ready to partner with you to help identify the needs of your monitoring and security infrastructure, and its nGenius solutions provide the tools to enable you to successfully comply with modern regulations.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us-2/

PFSAN_007-1700 07/2017