Where You Decrypt Network Data Matters

Decryption is a necessary function nowadays. It is estimated that 70% or more of malicious traffic is hiding within encrypted traffic. While there has been a lot of talk about the need for decryption, very little attention has been paid to how and where you should perform the decryption. This is actually an EXTREMELY important consideration because where you decrypt matters. It's similar to a core real-estate mantra – location, location, location. The location of where you purchase property (or in this case - decrypt network traffic for threat detection) is just as important as to what you purchase (or the data you inspect).

The reason why where you decrypt matters is straightforward. This choice of location can affect decryption quality, complexity, and cost. There are two fundamental decryption options for ingress traffic:

1. The first option is to set up your architecture so that each and every one of your security tools decrypts traffic (in a serial fashion) before the tool processes that traffic. Then after each tool inspects the traffic, the traffic is re-encrypted and sent on to the next tool (assuming no threats were found).

2. The second option is to create a hub where the traffic is decrypted once and then each security tool inspects that traffic before it is re-encrypted and set into the network (assuming no threats were found).

Enterprise Management Associates in their 2022 Network Visibility Architecture for the Hybrid, Multi-Cloud Enterprise research report found that 43% of study participants were decrypting traffic on each analysis tool. This means that almost half of the enterprises surveyed chose option 1 above. Option 1 is a less favorable selection than option 2 for the following reasons.

Not All Decryption Capabilities Are The Same

Unfortunately, not all decryption algorithms are the same – some are better, and some are worse. As an example, for any device performing decryption (and encryption) there is a time delay. However, some products process the decryption faster due to CPU, RAM, and data bus choices. There may also be a question as to whether the security tool supports the 30+ decryption algorithms in use by the marketplace. If the tool doesn't support a specific decryption algorithm being used, it skips decryption for those packets and passes them on to the next tool or into the network.

In addition, there is usually a significant performance hit meaning your security tools can create bottle necks. A study by ZK Research found that when decryption is activated, the security tool's performance becomes so impacted that 45% of security engineers ended up turning the feature off. Therefore, it's better to offload the feature to a separate decryption device (like a packet broker) to prevent those performance impacts.

Reduce Complexity – Decrypt Once and Inspect Thoroughly

When option 1 (above) is selected, multiple tools have to be configured to decrypt and re-encrypt traffic. This creates complexity for tool programming. You will need to consider the labor effort, cost to program each tool, and tool programming consistency that is required. For instance, are all tools set for TLS 1.3 or are some at TLS 1.2 and some at SSL 1.0? A related question is are you using man-in-the middle or passive data decryption techniques? If you have more than one tool performing decryption, then you will have to set this configuration up for each and every tool.

Why create unnecessary complexity by having every security tool perform decryption? Instead, you could decrypt one time with a network packet broker and then have the packet broker pass the unencrypted data to one or more security tools for inspection. If the data is safe, the packet broker can then re-encrypt the data and send it on into the network.

Decryption Costs Vary Depending Upon Where You Decrypt

Decryption is often an expensive purchase, especially when you look at recurring license costs. Therefore, you don't want to have to pay for the decryption feature in multiple tools. In addition (depending upon your decryption goals), you will probably find that as the amount of incoming network data increases every year, you will encounter licensing thresholds that require you to pay more fees on each of those tools.

An alternative is to stop inspection of all traffic and just inspect a subset. While this controls your cost, it increases the risk that more security threats will enter your network. However, a lower cost option would be to decrypt the traffic only one time and then re-encrypt once the data has been inspected.

Whether you are looking to reduce costs, meet compliance, or enhance your security posture, Keysight is here to help. We have various network visibility and network security solutions that follow both NIST and CISA guidance.

Reach out to Keysight Technologies and we can show you how to optimize your security solutions.

Learn more at: www.getnetworkvisibility.com

Keysight sponsors GetNetworkVisibility.com, a thought leadership website dedicated to the importance of packet-based visibility to power security, performance and network monitoring tools. For more information, contact us at:

www.getnetworkvisibility.com/contact-us/