In the Boxing Ring JUN 2024

Network Box Technical News

from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the June 2024 edition of In the **Boxing Ring**

This month, we are talking about **SSL/TLS** Inspection. It is estimated that 85% of traffic on the Internet is encrypted (with a large portion of that SSL/TLS encrypted), and approximately 70% of malware campaigns use some form of encryption. However, if you do not decrypt all that traffic for inspection and policy enforcement, it may pose a considerable security risk. To address this issue, Network Box provides various levels of inspection and policy enforcement for SSL/TLS traffic. On pages 2 to 3, we discuss these in greater detail.

On page 4, we highlight the set of enhancements and fixes to be released in this month's Patch Tuesday for Network Box 5 and our cloud services.

In other news, Network Box is proud to announce that the company has won three **Cybersecurity Excellence Awards** from *Cybersecurity Insiders*. Additionally, Network Box Hong Kong held a cybersecurity seminar in partnership with *FUJIFILM Business Innovation HK*. And in this month's Technology Focus, we are spotlighting **Network Box SOC Services**. Did you know that when you subscribe to Network Box, you get SOC services at no extra cost?

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
June 2024

Stay Connected

You can contact us here at Network Box HQ by email: **nbhq@network-box.com**, or drop by our office next time you are in town. You can also keep in touch with several social networks:

https://twitter.com/networkbox

https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse

https://www.linkedin.com/company/network-box-corporation-limited/

https://www.youtube.com/user/NetworkBox

In this month's issue:

SSL/TLS INSPECTION

It is estimated that 85% of traffic on the Internet is encrypted - with a large portion of that SSL/TLS encrypted. 99% of browsing time on Google Chrome is spent on HTTPS websites, and 95% of websites on Google use HTTPS. Approximately 70% of malware campaigns use some form of encryption.

Not decrypting all that traffic for inspection and policy enforcement may obviously be a huge security issue, but we must all recognize the complexities of decrypting (man-in-the-middle style) all SSL/TLS traffic.

To address this, Network Box provides various levels of inspection and policy enforcement for SSL/TLS traffic, and this article presents these options in some detail.

Protocol Enforcement

With so much encrypted traffic passing outbound on standard ports such as TCP/443 (https), TCP/993 (imap4s), TCP/955 (pop3s), etc., it is not unusual for malware to attempt evasion by connecting outbound on these ports. Network Box can monitor traffic on these ports and inspect such traffic to ensure it is actually SSL/TLS encrypted. If not, a policy rule can be configured to block and alert appropriately. However, some common applications (such as WhatsApp and others) also attempt to use these standard ports but don't use SSL/TLS protocol - so care needs to be taken when enforcing such a policy.

SSL/TLS Server Name Indication (SNI) Categorization

For many years, the SSL/TLS client handshake has included an option called SNI (Server Name Indication), which is almost universally used nowadays. Very few applications (mostly custom, old, or obsolete) don't provide this option. The SNI includes the server's name to be connected to (and is essential as the server can then use it to provide the appropriate connection and certificate if the server is hosting multiple different SSL/TLS services on the same IP address or port). If SSL inspection is enabled, Network Box can see these SNI hints and categorize those server names in the same way that a website is categorized. Then, policy rules and further decoding can be controlled based on either the server name or category of that server rather than simply on the IP address. This is extremely useful, simple to enable, and has minimal impact on the network.

SSL/TLS Offload

In the case that web servers are being protected (i.e., our servers, not client browsers), SSL/TLS offload is an option. In this configuration, the SSL/TLS certificate for the protected servers is placed on the Network Box device performing the protection (usually WAF+). In this way, Network Box can terminate the SSL/TLS connection, decrypt the traffic, inspect, scan, and apply policy. The resulting acceptable traffic can be passed on to the web server as HTTP or re-encrypted as HTTPS.

SSL/TLS Man-In-The-Middle

The final, most comprehensive, but most intrusive approach is total SSL/TLS Man-in-the-Middle decryption - used to protect web or mail clients from malicious servers or content on the Internet. The core problems with this approach are **(a)** the SSL/TLS protocol is fundamentally designed to protect against such technology, and **(b)** some client applications (not typically web browsers, but apps running on mobile phones) use certificate pinning technology to try to stop this technology.

There is really only one way to implement such an approach. The approach is to firstly create a certificate authority on the Network Box itself, and to install that certificate authority certificate as trusted in the web browsers and operating systems of all the workstations to be protected. Then, when a client browser accesses an HTTPS website, the Network Box unit can retrieve the remote certificate, validate it, check if it is acceptable to policy, and if so, then re-sign the certificate using the Network Box certificate authority. In this way, the traffic from the web client to the Network Box is decrypted on the unit, inspected, scanned, policy control applied, and if acceptable, re-encrypted to be sent to the remote website. Traffic coming back from the remote website is handled similarly.

The issues with this approach can be summarized as:

- Some mobile phone apps use certificate pinning to specifically restrict which certificate authorities they will accept. Network Box can bypass these apps (using SNI or other policy-based approaches), but it is not ideal and can be troublesome.
- To be protected, the Network Box Certificate Authority certificate needs to be installed on all workstations. While automated tools exist to help with this, it can be onerous.

The advantage is that this provides the most comprehensive and effective protection of SSL/TLS traffic. It even goes beyond what is available in the client workstations by providing centralized policy control over acceptable policies and sites. The SSL/TLS policy can be moved from the workstation (where users typically click 'yes' to bypass protection and get to what they want) to the gateway (where centralized policy as to what is acceptable can be applied).

Conclusions

So, which of these four approaches is the best? The answer, of course, is that "it depends." There will always be a trade-off between convenience and security; this is just another one of those cases. We can, however, provide some overall guidance and suggestions:

- **Protocol Enforcement** is typically not required but recommended for more secure networks with sensitive data. For example, enabling this on DMZ networks containing mostly servers is very easy and has little impact on normal day-to-day operation, but it is extremely useful in detecting and preventing data exfiltration.
- **SSL/TLS SNI Categorization** is simple to implement, has almost no drawbacks, and should generally be enabled. Even if no policy rules are defined, enabling it improves the logging of SSL/TLS traffic events (enabling logging of not just IP addresses but also protocol details and remote server names).
- **SSL/TLS Offload** should be enabled for all web servers protected by WAF+ and for other DMZ servers (such as SMTP, IMAP4, POP3, etc.) providing SSL/TLS-protected services. Again, this is simple to implement and allows for scanning and policy enforcement with few drawbacks.
- Recognizing the difficulty in the initial deployment of **SSL/TLS Man-in-the-Middle** decryption, we generally recommend this be deployed to LAN and DMZ segments containing Linux, OSX, and Windows workstations and servers only. It is not typically required to be deployed to WIFI networks containing mobile phones (due to the issues surrounding certificate pinning, custom apps, etc., and the relatively low risk to such hardened devices).

We hope the information in this article is helpful for you - both in explaining the technology and deciding how best to use it within your networks. As usual, please feel free to talk to your local regional Network Box SOC for further advice and assistance.

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 4th June 2024, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next seven days.

Network Box 5 Features
June 2024

This month, for Network Box 5, these include:

- Improvements to event correlation in IDS/IPS.
- Whitelist HTML SCRIPTs commonly used by Microsoft Azure (no longer mark such scripts as executable when attached to email messages).
- Improvements to updating of IP addresses in host ACLs.
- Enhancements to regional SOC IP address ranges, to support SOC expansion in Taiwan and Philippine regions.

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

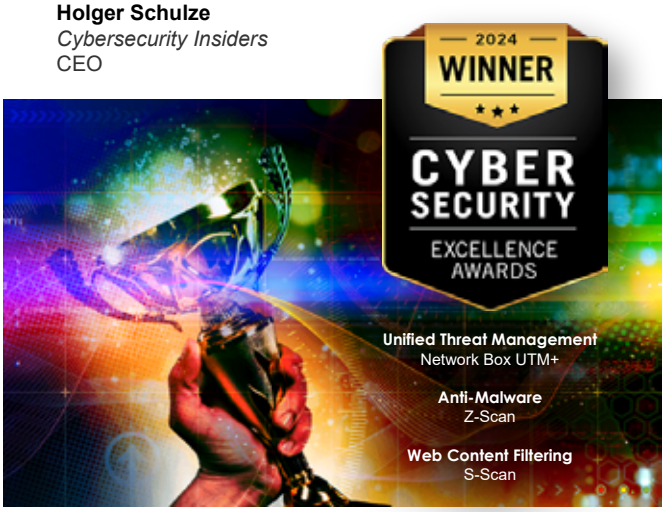
Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.

Network Box HIGHLIGHTS

Cybersecurity Excellence Awards 2024

Network Box is proud to announce that the company won three *Cybersecurity Insiders'* **2024 Cybersecurity Excellence Awards** in the categories of Unified Threat Management, Anti-Malware, and Web Content Filtering.

> *"Network Box's remarkable achievement is a testament to their unwavering commitment to the core principles of excellence, innovation, and leadership in cybersecurity."*
>
> **Holger Schulze**
> *Cybersecurity Insiders*
> CEO



LINK: https://network-box.com/awards

Network Box Hong Kong Cybersecurity Seminar

In partnership with FUJIFILM Business Innovation HK, Network Box Hong Kong held a cybersecurity seminar for SMEs. The key issue covered at the event was *Why hackers target small companies*.

Network Box Technology Focus

Did you know...

When you subscribe to Network Box, you get SOC services at no extra cost?

Listed below are some of the key features of the Network Box SOC and the services it provides:

- 24x7x365 Monitoring and Support
- Global Threat Intelligence
- Real-Time Security Updates
- Live Response and Support
- Hardware Monitoring and Backups
- Centralized Logging and Management

and more...

For more details about Network Box SOC services, please visit:
https://network-box.com/securityresponse-soc

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Kevin Hla
Production Support

Network Box HQ
Network Box USA
Contributors

Subscription

Network Box Corporation
nbhq@network-box.com
or via mail at:

Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong.

Tel: +852 2736-2083
Fax: +852 2736-2778

www.network-box.com

Copyright © 2024 Network Box Corporation Ltd.