In the Boxing Ring

Network Box Technical News
from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the September 2018 edition of In the Boxing Ring

This month, in the first of a series of articles about the upcoming Network Box Security Incident and Event Management Plus (NBSIEM+) system, we talk in detail about Retrieving Log Events and how they may be sent into the NBSIEM+ system.

The goal here is to integrate all the security logs and incidents into one centralized system, to provide an overview of the entire network, and to be able to apply Integrated Security Intelligence, Digital Forensics, and Security Incident Management; all delivered as cloud based and/or on-premises solutions.

On page 4, we highlight the features and fixes to be released in this month’s patch Tuesday for Network Box 5.

Finally, we are pleased to announce that Network Box won the Best Managed Security Services Provider at the e-brand 2018 Awards. In addition, Network Box Germany hosted a partner day with Server Eye, and Network Box held Security Seminar for Guardforce. Furthermore, Network Box Malaysia was at the Asia Cybersecurity Exchange to discuss Security for IoT.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
September 2018

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 us by several social networks:

- https://twitter.com/networkbox
- https://www.facebook.com/networkbox
- https://www.linkedin.com/company/network-box-corporation-limited/
- https://plus.google.com/u/0/107446804085109324633

Page 2 to 3
NBSIEM+ Logging Options
This month, we are releasing the NBSIEM+ Logging Option to all Network Box 5 appliances globally, as part of our September 2018 Patch Tuesday release cycle. This will allow us to expand the pre-release availability of NBSIEM+; allowing more Network Box appliances, and other network devices, to submit event logs. On page 2 to 3 we discuss this in further detail, and highlight the different options to submit event logs to NBSIEM+.

Page 4
Network Box 5 Features
The features and fixes to be released in this month’s patch Tuesday for Network Box 5.

Page 5
Network Box Highlights:
- e-brand Awards 2018 Best Managed Security Service Provider
- Network Box Hong Kong Guardforce Security Seminar
- Network Box Malaysia Asia Cybersecurity Exchange
- Network Box Germany Server Eye - Partner Day
In a series of articles about the upcoming Network Box Security Incident and Event Management Plus (NBSIEM+) system to be released later this year, this month we talk in more detail about retrieving log events and how they may be sent into the NBSIEM+ system.

Event logs may be generated by many different sorts of equipment, in many different formats. Some examples include:

- **Windows servers**
  (windows event logs)
- **Switches, firewalls, and network equipment**
  (syslog events)
- **Network Box UTM+ appliances**
  (nbsyslog and/or syslog events)

Whatever the source, when sending in these events to NBSIEM+, we need to ensure three core principles are adhered to:

1. **Server authentication**
   The client sending in the events must authenticate the server to ensure that there is no Man-in-the-Middle (MITM) attack, and that the server is who it says it is. This is to protect against the sensitive data in the events being intercepted.

2. **Client authentication**
   When NBSIEM+ receives the events, it must authenticate the client, to ensure there is no MITM attack and the client is who he says he is. This is to protect against spoofing of event data.

3. **Channel protection**
   The communication channel itself used to transmit logs must be protected against interception, tampering, replay, and other sorts of attacks. This is to protect against eavesdropping and/or tampering of the events in transit.

The SSL/TLS protocol, coupled with client and server certificate authentication as well as high strength encryption, is well suited to meet these requirements, and works well for this purpose. Network Box NBSIEM+ standardizes on the use of this SSL/TLS, authenticated with client and server certificates, as its fundamental secure transport layer.

The simple syslog protocol, using UDP/514, doesn’t come anywhere close to meeting these requirements. But unfortunately, the majority of simple networking equipment offers little in the configurability of managing event log data, and most simply offer the option to enter an IP address of a syslog server to send events to over UDP/514.
Whatever the source, when sending in these events to NBSIEM+, we need to ensure three core principles are adhered to:

1. **Server authentication**
The client sending in the events must authenticate the server to ensure that there is no Man-in-the-Middle (MITM) attack, and that the server is who it says it is. This is to protect against the sensitive data in the events being intercepted.

2. **Client authentication**
When NBSIEM+ receives the events, it must authenticate the client, to ensure there is no MITM attack and the client is who he says he is. This is to protect against spoofing of event data.

3. **Channel protection**
The communication channel itself used to transmit logs must be protected against interception, tampering, replay, and other sorts of attacks. This is to protect against eavesdropping and/or tampering of the events in transit.

The SSL/TLS protocol, coupled with client and server certificate authentication as well as high strength encryption, is well suited to meet these requirements, and works well for this purpose. Network Box NBSIEM+ standardizes on the use of this SSL/TLS, authenticated with client and server certificates, as it’s fundamental secure transport layer.

The simple syslog protocol, using UDP/514, doesn’t come anywhere close to meeting these requirements. But unfortunately, the majority of simple networking equipment offers little in the configurability of managing event log data, and most simply offer the option to enter an IP address of a syslog server to send events to over UDP/514.

Within NBSIEM+, all events (no matter their source) are unified into the same security event format for further processing, incident correlation and response.

This month, Network Box is releasing this functionality to all Network Box 5 appliances globally, as part of our September 2018 Patch Tuesday release cycle. This will allow us to expand the pre-release availability of NBSIEM+; allowing more Network Box appliances, and other network devices, to submit event logs.
Network Box 5

On Tuesday, 4th September 2018, 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 14 days.

Network Box 5 Features

September 2018

This month, for Network Box 5, these include:

- Improvements to URL categorisation
- Improvements to logging for GSB URL categorisation engine
- Improvements to GMS status message for anti-malware scanning engines
- Enhanced support for TLS handshake negotiations
- Improved memory consumption in TLS/SSL certificate validation
- Support for ‘100-continue’ status messages in HTTP protocol
- General improvements to display of international encodings in email records
- Provide an option for a GMS self-check in proxy service
- Introduction of the NBSIEM+ logging option

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 e-brand Awards 2018

Network Box won the Best Managed Security Service Provider Award 2018, at the e-brand Awards. Network Box Managing Director, Michael Gazeley, collected the award on behalf of the company at the awards ceremony that took place at the Grand Ballroom of the Hyatt Regency. Many of the world's top brands were in attendance, including: Amazon Web Services, Fortinet, Trend Micro, ASUS, Fuji Xerox, Pioneer, Cannon, LG, Microsoft, Shell, Alibaba Cloud, Huawei, and HGC.

Network Box Hong Kong Guardforce - Security Seminar

Guardforce was at Network Box, to discuss some of the latest Network Box 5.5 cybersecurity capabilities, which have been leveraged to augment GRID (Guardforce Real-time Insured Defence), the new cyber-insurance backed managed cyber-security service, being offered to Guardforce’s customers worldwide.

Network Box Malaysia Asia Cybersecurity Exchange

Network Box Malaysia was at the Asia Cybersecurity Exchange, to discuss the current IT and cybersecurity landscape in Malaysia. The theme of the event was ‘Security for IoT,’ focusing on the Security Management Standard, and challenges for IoTs.

Network Box Germany Server Eye - Partner Day

Network Box Germany hosted a partner day, with ‘Server-Eye,’ Germany’s experts in IT monitoring software.