In the Boxing Ring OCTOBER 2021

Network Box Technical News

from Mark Webb-Johnson

Chief Technology Officer, Network Box

Welcome to the October 2021 edition of In the **Boxing Ring**

This month, we are talking about the **Network Box Email Protection**. While it can no longer claim the top position for distribution of malware, emails remain a highly popular vector for both targeted attacks (such as spear phishing, ransomware, and advanced persistent threats) as well as general mass phishing and spam campaigns. On pages 2 to 4, we discuss the flow of emails and how Network Box technologies are used to detect and block malicious or unwanted messages.

On page 5, we highlight the features and fixes to be released in this quarter's Patch Tuesday for Network Box 5.

Also this month, we are pleased to announce the latest revision to the Network Box **UTM-5Q.** In this month's media coverage, Network Box was featured in the **Harbour Times.** Furthermore, in this month's global security headlines, numerous security vulnerabilities were found in Cisco, Fortinet, and wearable fitness tracking products.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
October 2021

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.facebook.com/networkboxresponse

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

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

In this month's issue:

Network Box Email Protection

While it can no longer claim the #1 position for distribution of malware, emails remain a highly popular vector for both targeted attacks (such as spear phishing, ransomware, and advanced persistent threats) as well as general mass phishing and spam campaigns. With the proliferation of "rich text" communications, email clients continue to be targeted, and the applications launched when an attachment is opened, with Microsoft Office being the #1 target.The good news is that email is not so time-critical and lends itself well to the in-depth thorough scans that Network Box technology does so well.

In this article, we will be looking at the flow of emails and how Network Box technology is used to detect and block malicious or unwanted messages.

The Flow of Email Scanning

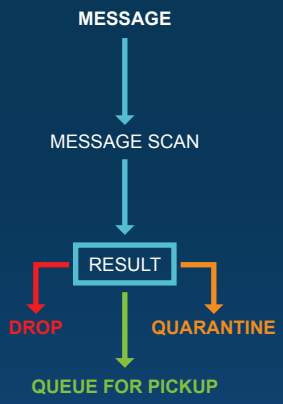
There are restrictions inherent in different email protocols, which lead to diverse capabilities in how the Network Box email scanners treat them:

POP3 / IMAP4 Mail

Messages delivered using the POP3 or IMAP4 protocols only contain a message body with no envelope and can only be filtered. Quarantine is not possible due to protocol restrictions. Such messages are passed through the message scanner and either accepted or filtered. Filtered emails are replaced with an alert message or marked to indicate they are not acceptable.

SMTP Mail

SMTP email has both an envelope and a message body, and can be quarantined. As such, as the message envelope is received (at the DATA stage of the smtp email transaction) it is passed through an envelope pre-scan and reception of the email message itself is only permitted if this pre-scan is accepted. The full message body is then received and passed through the message scanner.



The Network Box Email Envelope Scanner

The Network Box email Envelope Scanner operates at the envelope level, containing just message sender, recipients, source IP address, and some protocol information. As it operates before reception of the actual message, a block at the envelope scan stage can result in significant bandwidth and workload capacity savings.

The system works by scanning the envelope using a variety of engines to determine acceptability. The result of this scan can be one of:

- **Defer** – the message is temporarily deferred, and an instruction is sent to the sender to try to re-send the message at a later time.
- **Reject** – the message is permanently rejected, and an instruction is sent to the sender never to send this same message again.
- **Discard** – the message sender is informed that the message has been accepted, but the message itself is discarded without delivery.
- **Accept** – the envelope is acceptable, and the client should continue to send the entire message for further scanning by the Network Box email message scanner.

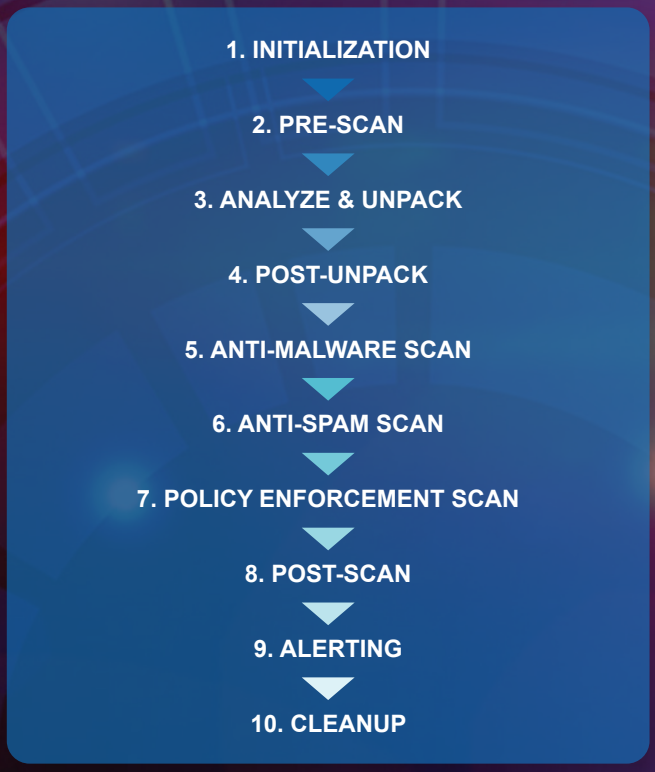
Optionally, the Network Box Email Envelope Scanner can be connected to customer systems for recipient address verification and the Network Box IDP/Firewall system for directory harvest attack protection, and temporary blacklisting of malicious source IP addresses.

The Network Box Email Message Scanner

The Network Box Internet Threat Protection system can comprehensively scan emails for company policy conformance, viruses, intrusions, and spam. Let's examine the flow of email through the scanner:

1. **Initialization** – preparation for the scan
2. **Pre-Scan** – cleanup and selection of scanning system
3. **Analyze & Unpack** – loop until message completely unpacked and analyzed
   - **Analyze** – analysis of email message and embedded content sections
   - **Unpack** – unpacking of message structures and attached archive files)
   - At the analyze and unpack stage, the Network Box unit handles the extraction of text and images from PDF and office document formats. Metadata regarding email sections and attachments are also derived during these stages.
4. **Post-Unpack** – cleanup of unpacking system
5. **Anti-Malware Scan** – searching for viruses, by heuristics and signatures
   - **Pre-Anti-Malware** – preparation of anti-malware engines
   - **Anti-Malware Scan on the Message** – scan message body and headers
   - **Anti-Malware Scan on Files** – scan attach files
   - **Anti-Malware Scan Content** – scan attached content
   - **Post-Anti-Malware** – cleanup for anti-malware engines
6. **Anti-Spam Scan** – searching for spam by multiple engines and methods
   - **Pre-Anti-Spam** – preparation of anti-spam engines
   - **Anti-Spam Scan on the Message** – scan message body and headers
   - **Anti-Spam Scan on Files** – scan attach files
   - **Anti-Spam Scan on Content** – scan attached content
   - **Post-Anti-Spam** – cleanup for anti-spam engines
7. **Policy Enforcement Scan** – enforcement of company policy
   - **Pre-Policy** – preparation of policy enforcement engines
   - **Policy Scan on the Message** – scan message body and headers
   - **Policy Scan on Files** – scan attach files
   - **Policy Scan on Content** – scan attached content
   - **Post-Policy** – cleanup for policy engines
8. **Post-Scan** – cleanup for all engines
9. **Alerting** – raising alerts
   - **Pre-Alert** – preparation for alerting
   - **Alert** – issuing of alert messages
   - **Policy Scan on Content** – scan attached content
   - **Post-Alert** – cleanup for alert engines
10. **Cleanup** – final cleanup, reporting, and logging

Stage 5 of the scan provides for the anti-malware engines to hook into the scanning system and help decide if a message is a malware or not.



The Network Box Email Scanning System

Currently, the Network Box email scanning system consists of 21 engines and more than 17 million signatures.

1. The "env_scan_rbl" engine examines a large number of real-time blacklists for senders or source IPs known to distribute spam, phishing, malware, or other such messages. This is an extremely quick check performed at the envelope scanning stage.
2. The "env_scan_spf" engine examines messages at the envelope stage to ensure they conform to published Sender Policy Framework (SPF) policies.
3. The "env_scan_verify" engine examines message sender and recipients at the envelope stage and checks to ensure both are valid.
4. The "msg_analysis_encrypted" engine examines message content looking for encrypted text or attachments. It can then categorize these for later policy enforcement.
5. The "msg_analysis_executable" engine examines messages looking for executable bodies or attachments. It can then categorize these for later policy enforcement.
6. The "msg_analysis_extension" engine examines attachments, determining file extensions (including attempts to obfuscate these). It then categorizes these for later policy enforcement.
7. The "msg_analysis_content" engine examines the actual content of the attachments, not simply the filename, to determine the file type. It then categorizes these for later policy enforcement.

8. The "msg_analysis_macros" engine examines attachments, looking for macros or other scripting technology used by applications such as Microsoft Office. These are a form of executable code that are categorized for later policy enforcement.
9. The "msg_scan_badheader" engine examines the message structure looking for obfuscation of protocol violations attempting to bypass/avoid scanning. Once discovered, these are categorized for later policy enforcement.
10. Similar to SPF, the "msg_scan_dkim" engine examines messages and enforces DKIM policies.
11. The "msg_scan_dnsrbl" and "msg_scan_rbl" engine operates at the message scanning stage, able to perform real-time blacklist checks on the Received-By headers of the message and blocks known malicious/unwanted senders and source IPs.
12. The "msg_scan_multext" engine looks for common extension obfuscation with attachments using multiple extensions to bypass/avoid scanning.
13. The "msg_scan_newdomain" engine examines domains found inside the envelope, message, or attachments to determine the age of the domains found. New domains created very recently are categorized for later policy enforcement.
14. The "msg_scan_policy" engine enforces user-defined policy rules on the messages.
15. The "msg_scan_razor" engine performs fuzzy-match lookups of the message against a clearinghouse of known malicious/unwanted messages.
16. The "msg_scan_rules" engine performs detailed analysis of the message, its headers, structure, and attachments, looking for malicious activity. In particular, these rules are designed to identify SPAM, PORN, DLP, HOAX, MALWARE, PHISHING, and other undesirable content.
17. The "msg_scan_sendermatch" engine implements custom rules to enforce relationships between the "From" header and envelope "MAIL FROM" sender of the message. These can be used to detect spear-phishing and other such forms of attack.
18. The "msg_scan_signatures" engine implements signature-based matching of known malicious attachments and email sections. It compares hashes, headers, and other such aspects. This is an extremely fast way of detecting and blocking non-polymorphic malicious code. Various techniques are used to bypass signature obfuscation techniques used by common viruses.
19. The "msg_scan_zscan" engine obtains samples from over 250,000 virtual honey traps and releases its own signatures to protect against zero-day threats 4,200 faster than traditional anti-virus systems.
20. The "scan_kaspersky8" anti-virus engine is used to run the Kaspersky AVP anti-virus scanner against the entire message (using Kaspersky unpackers as an extra layer of defense) as well as individual attachments.
21. The "scan_bitdefender" anti-virus engine is used to run the BitDefender anti-virus scanner against the entire message (using BitDefender unpackers as an extra layer of defense) as well as individual attachments.

Network Box Security Response is constantly expanding this list of engines, and the added protection PUSHed out to Network Boxes, globally, in real-time. Both engines and signatures can be updated using the Network Box DynaCode technology.

Scanning Configuration

The Network Box email system is highly configurable. Individual engines can be enabled/disabled based on tests, including:

1. The direction of the message (inbound or outbound)
2. Whether the message is being filtered (e.g., POP3, IMAP4)
3. Whether the message is redirectable (e.g., SMTP)
4. Globally (i.e., for everything)
5. Based on the content of message headers
6. Based on the proxy handling the message (e.g., SMTP, POP3)
7. Based on a single recipient of the message
8. Based on a recipient being one of the recipients of the message
9. Based on the sender of the messages
10. Based on the sender IP address

The engines classify the email messages, so that customized policy rules can be configured to handle appropriately: defer, accept, reject, or discard.

The Network Box email scanning solution is the most comprehensive and effective gateway email protection solution in the market today. It provides 21 scanning engines, supporting over 700 encoding and packing formats, combining several different techniques, and is backed by a database of over 17 million signatures. It provides true defense-in-depth in a single managed gateway appliance.

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 5th October 2021, 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
2021Q4

This quarter, for Network Box 5, these include:

- Enhancements and improvements to SOC systems for device maintenance
- Add support for M-395i 2021 model
- Improvements and updates to IPv4 and IPv6 geolocation
- Support for long city names, and international characters, in IPv4 and IPv6 geolocation
- Enhanced support for new ACL rule verdicts, to enable policy rule subroutine support
- Introduce support for subroutines in mail spam policy rules
- Support new nb_event_id unified field for Network Box NBSIEM+ events
- Obsolete old expired DST X3 root trusted certificate (no longer used by Let's Encrypt)
- Introduce the ability to set eMail addresses in mail server transport policies
- Add cloud transport support to mail server module
- Yearly renewal of admin and user portal SSL certificates
- Minor change to wording 'IDS Blocks' to 'IDS Alerts' in KPI report for IDS
- Remove unused 'user' section in KPI report on IPSec connections
- Other minor enhancements and improvements to KPI reporting

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

Network Box
UTM-5Q Hardware Upgrade

Network Box is pleased to announce our latest revision to the UTM-5Q hardware unit for small offices, home offices, branch offices, or other smaller sites that require comprehensive UTM+ protection.

Features	Details
Processor	64bit, 2.24GHz, 4 physical cores
RAM	8GB, 1600MHz DDR3
Storage	1 x 256GB mSATA SSD
Networking	4 x 1Gb RJ45
Power Supply	60w (external)
Chassis	Desktop SFF Fanless
I/O Interface	1 x reset button 1 x RJ-45 Management Console 1 x USB 3.0
Physical Dimensions	115mm(w) x 39mm(h) x 107.5 mm(d)
Weight	0.5kg
Approvals/ Compliance	CE Class B, FCC Class B, RoHS

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 © 2021 Network Box Corporation Ltd.

Media Coverage & Security Headlines

Harbour Times
Latest data breach attacks Hong Kong hospitals: What happened and what to do?
LINK: https://bit.ly/3iuHGOq

Threat Post
Critical Cisco Bugs Allow Code Execution on Wireless, SD-WAN
LINK: https://bit.ly/3mjeMlO

Bleeping Computer
Hackers leak passwords for 500,000 Fortinet VPN accounts
LINK: https://bit.ly/2ZYrxuB

The Register
Microsoft fixes flaw that could leak data between users of Azure container services
LINK: https://bit.ly/3owkIKW

ZDNet
Over 60 million wearable, fitness tracking records exposed via unsecured database
LINK: https://zd.net/2WC8vIW

CRN
Ransomware gang claims it used Accenture data to breach airport: report
LINK: https://bit.ly/3D3teF4