NETWORK BOX | NEXT GENERATION MANAGED SECURITY

network-box.com

In the Boxing Ring AUG 2021

Network Box Technical News

from Mark Webb-Johnson
Chief Technology Officer, Network Box

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

This month, we are talking about one of our core systems - **Network Box Intrusion Detection and Prevention (IDP)**. Network Box has multiple Intrusion Detection and Prevention systems working together in combination with the core routing and firewall functions to provide a highly flexible and modular approach to the problem of securing network traffic. The system offers four modes of operation to balance protection level (and latency) with performance. On pages 2 to 4, we outline how the system works and highlight its key features.

Also this month, we highlight the key features of the **Network Box SD-WAN**, available to all Network Box customers. We have been providing SD-WAN for decades now, and services are available for on-premises Network Box devices, virtual cloud, and multi-tenanted SaaS services. And in this month's media coverage, Network Box was featured in **Hong Kong Lawyer**, published by the Law Society of Hong Kong.

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

In this month's issue:

Stay Connected

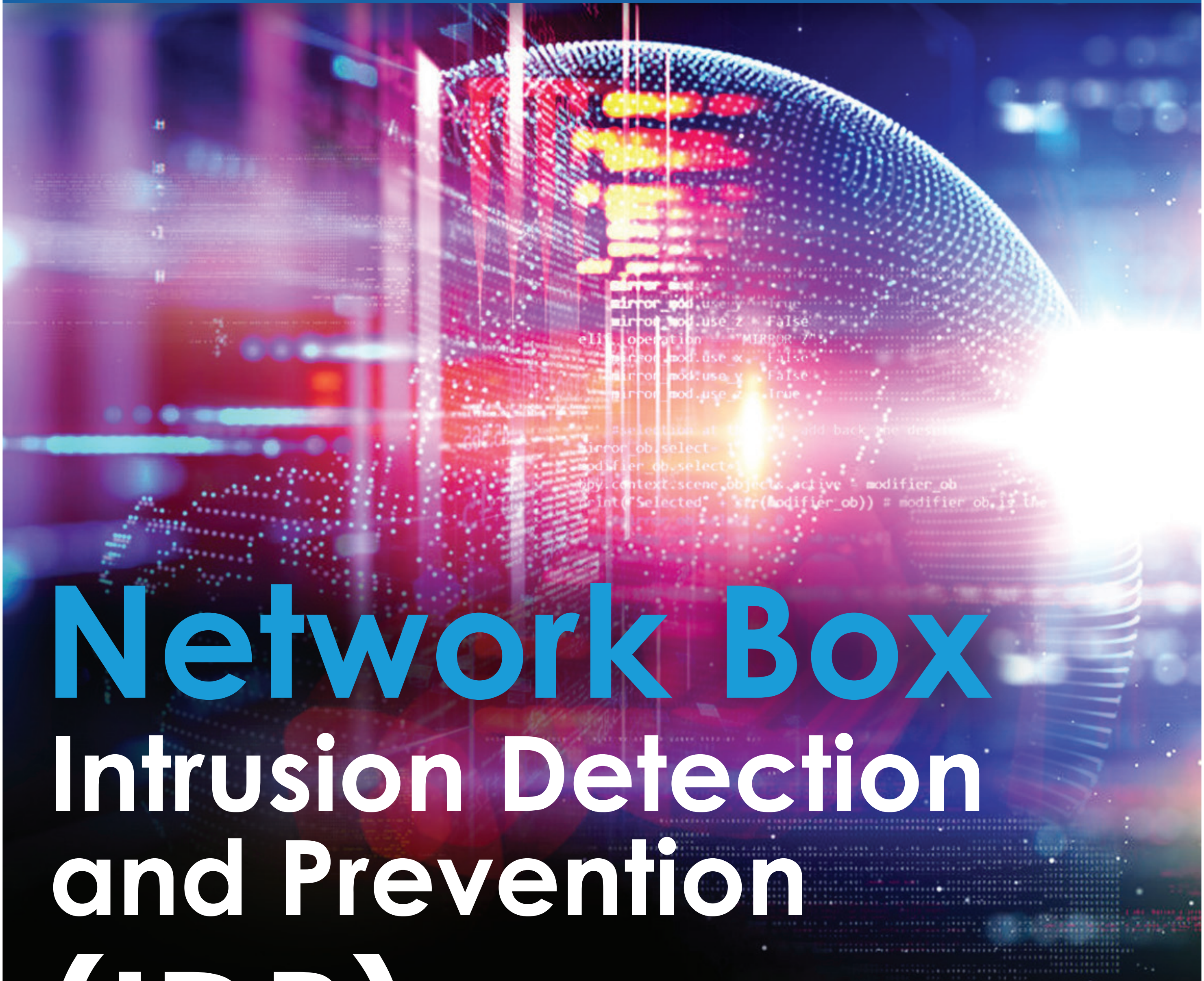
You can contact us here at Network Box HQ by email: **nbhq@network-box.com**, or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

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



Network Box Intrusion Detection and Prevention (IDP)

The first in an ongoing series of Network Box technology deep dives, in this article, we will be talking about the Network Box Intrusion and Detection system.

Network Box has multiple Intrusion Detection and Prevention (IDP) systems working together in combination with the core routing and firewall functions to provide a highly flexible and modular approach to the problem of securing network traffic.

Wikipedia defined Intrusion Detection as, "the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource," and then goes on to say that "when Intrusion Detection takes a preventive measure without direct human intervention, then it becomes an Intrusion Prevention System."

Modes of Operation

Network Box provides four modes of Intrusion Detection and Prevention. In passive and active IDS modes, the engine is run separately from the network traffic stream to minimize the performance impact and offer options to limit the visibility of the monitoring on the network. The inline IPS modes allow the engine to run inline with the traffic stream and offer zero-latency response to attacks.

Intrusion Detection (passive and active IDS) and Intrusion Prevention (IPS) systems have their places in network security. An industry first, the Network Box system combines the four approaches into a single unified platform. It allows the technology and tools to be best applied on an individual device basis.

Frontline IPS

An extremely light-weight, high-speed service, offering zero-latency protection, inline with the data-stream, against network worms, exploits, and other such attacks. It operates in conjunction with the firewall at the individual packet level (after fragment re-assembly). The front-line IPS adds packet content inspection, rate limiting, and traffic analysis to the base firewall capabilities.

Network Box IDP

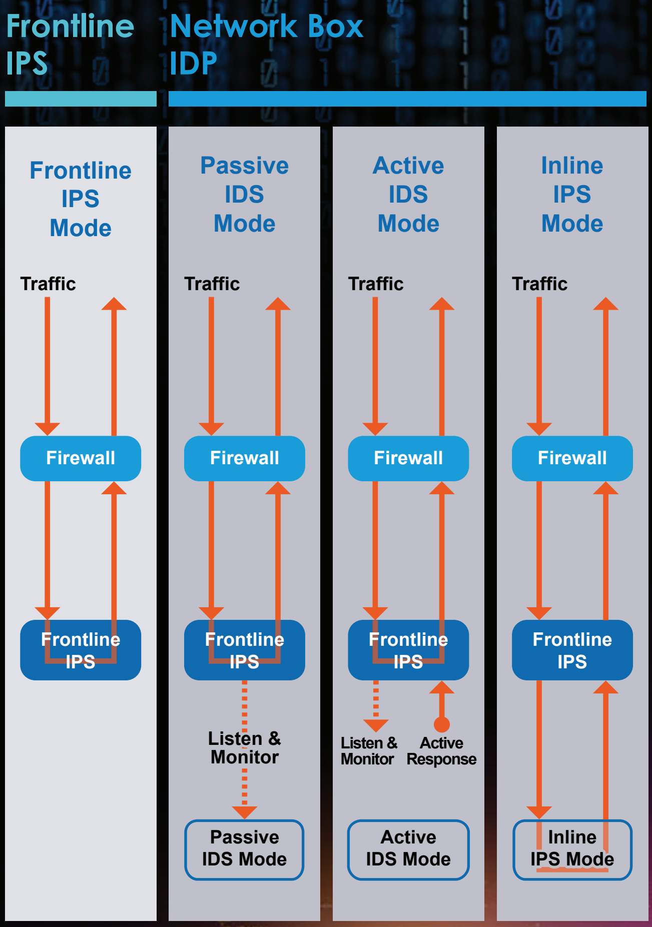
With full stream and protocol disassembly, able to operate in promiscuous mode (with a switch tap port or hub). IP-less if required, and in one of three modes:

Passive IDS - alerting and logging of traffic, side-by-side with the data stream. Useful for policy enforcement and more aggressive rules.

Active IDS - alerting and logging of traffic, side-by-side with the data stream. Has the ability to actively teardown connections once malicious traffic has been identified.

Inline IPS - alerting and logging of traffic, inline with the data stream. Tightly coupled to the firewall, it can drop traffic before the remote system even sees it.

Modes can be combined to suit customer requirements, allowing deployment of the highest possible protection levels, given monetary and performance constraints.



Security Architecture

Network Box employs a layered security architecture. Traffic passing between network interfaces passes through the five layers of Network Box protection.

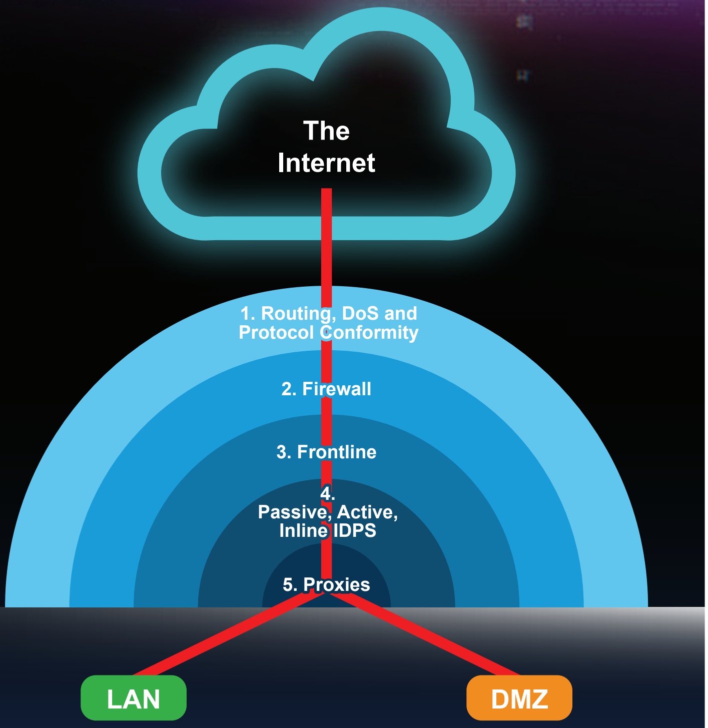
1. The first protection layer provides basic routing, denial-of-service protection, and protocol conformity. This layer is handled closest to the hardware and protects against routing, protocol obfuscation, and load-orientated attacks.

2. The second protection layer is the firewall. At this layer, traffic that does not conform to firewall policies is blocked.

3. The third protection layer is the Front-line IPS system. This offers extremely light-weight, zero-latency protection against worms, exploits, and other such attacks.

4. The fourth protection layer is the Network Box IDP system. This offers passive IDS, active IDS, and inline IPS protection using sophisticated rules and protocol/stream decoding engines.

5. The fifth protection layer consists of a set of Protected Services Proxies for specific protocols, such as POP3, IMAP4, SMTP, HTTP, and FTP. These provide application-layer protection against malware, spam, protocol enforcement, and policy violations.


The Internet
1. Routing, DoS and Protocol Conformity
2. Firewall
3. Frontline
4. Passive, Active, Inline IDPS
5. Proxies
LAN
DMZ

Network-Based Intrusion Detection and Prevention

Being a gateway device, the Network Box system is ideally placed to apply Intrusion Detection and Prevention at the gateway (where malicious traffic passes into or out of the network). The Network Box system offers a highly specialized hardware + software platform to analyze, detect, block, and report security-related events.

The Network Box Intrusion Detection and Prevention system takes traffic from the network and passes it through the following enforcement/analysis capabilities:

- **Fragment re-assembly**
  Operating at the IP level, fragment re-assembly is performed at the router level of the Network Box system (prior to applying higher-level firewall and IDS/IPS rules). The Network Box can detect and respond to IP fragmentation attacks at this very low level.

- **IP anomaly detection/response**
  Also operating at the IP level, this module can detect anomalies in the IP protocol itself and respond appropriately.

- **Scan detection/response**
  The scan detection and response module analyses network traffic looking for scanning behavior. It can respond to such scanning activity in a pseudo-random manner, obfuscating the firewall's deterministic behavior and providing an active response.

- **Protocol anomaly detection/response**
  Protocol analyzers provide for protocol-based anomaly detection and response. Many protocols are supported (including HTTP, FTP, SMTP, etc.); and specific application-level servers (e.g., Apache, Microsoft IIS web servers).

- **Rate limiting**
  The rate limiting features allow rules to be tuned based on the number of connections/packets/streams of a specified type from a single source to a single destination, used for denial-of-service protection, rule limiting, and general anomaly detection.

- **Stream re-assembly and anomaly detection/response**
  Groups packets into individual streams and allows higher-level modules to operate against the streams (including stream direction such as client request or server-response).

- **Protocol analysis**
  The protocol analyzers can decode application-layer protocols (such as HTTP, FTP, SMTP, etc.) and test the different parts of the protocol for abnormal behavior.

- **Packet/Stream pattern recognition and anomaly detection/response**
  The core signature base of the Intrusion Detection and Prevention System. The pattern recognition module applies signatures of known malicious attacks (and unknown behavior/vulnerability exploits) against the protocol stream, looking for matches.

Protection Signatures

At its foundation, the Network Box IDP system integrates security, logging, and management frameworks. This allows us to leverage industry-standard format signatures and heuristics and gives us a powerful rules language and extensive stream and protocol decoders.

Signatures for the Network Box IDP engines can be created on a global, Security Operations Centre, and per-customer basis. An on-the-box system takes the signatures and configurations to produce a live configuration on a per-box basis. Network Box currently has over 29,000 Intrusion Detection and Prevention signatures.

Logging is integrated into our NOC stats/reporting/monitoring systems, periodic reporting, and the admin portal.

> **Engines, such as the Network Box IDP, offer powerful rules languages and extensive stream and protocol decoders. Good news, but with a performance impact. The solution is to provide the four modes of operation to balance protection level (and latency) with performance. We can configure different interfaces to operate in different modes (for example, active IDS for LAN policy enforcement and inline IPS for NET). Or, we can simply operate with one mode for all traffic.**

Network Box HIGHLIGHTS

The Network Box SD-WAN optimizes network traffic, and allows organizations to easily connect between head office and branch offices, data centres, cloud services/applications; regardless of network environment and connection type.

Network Box provides SD-WAN services and operates SD-WAN networks using our secure Network Box 5 platform. With full support for Internet, leased lines, and Multi-Protocol Label Switching (MPLS) circuits, Network Box can build an SD-WAN optimized for each customer's requirements. Solutions are dynamic and scriptable, supporting complex business logic. By integrating commodity Internet links rather than expensive leased lines or MPLS circuits, Network Box can help drive down costs and provide a fast, optimized network experience.

Provides QoS and Security Technologies: Traffic Prioritisation, Traffic Shaping, Traffic Policing; with UTM+ services.

Supports various network connection types and configurations: MPLS, Lease Line, Broadband, Hub-and-spoke; Mesh, Hybrid combinations, etc.

Centralized administration of the SD-WAN, including configuration, link status monitoring, alerting, and reporting.

For more details:
https://www.network-box.com/sites/default/files/files/NetworkBox_SD-WAN.pdf

Media Coverage & Security Headlines

BBC

SolarWinds: Top US prosecutors hit by suspected Russian hack

LINK: https://bbc.in/2TMU5Eq

BBC

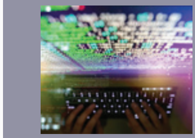
British man arrested in Spain over Twitter hack

LINK: https://bbc.in/3fhoimA

BBC

Major websites hit by global outage

LINK: https://bit.ly/3x7xuAV



The Guardian

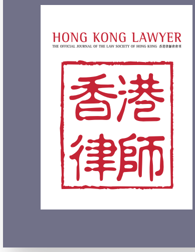
Latest ransomware attack appears to hit hundreds of American businesses

LINK: https://bit.ly/3fndq6J

The Hacker News

Apple Releases Urgent 0-Day Bug Patch for Mac, iPhone and iPad Devices

LINK: https://bit.ly/3j5NLk4



The Law Society of Hong Kong | Hong Kong Lawyer

If the Law Matters, If Justice Matters, Then Cyber-security, Matters.

LINK: https://bit.ly/3yiM60J

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