NETWORK BOX
NEXT
GENERATION
MANAGED SECURITY

www.network-box.com

In the Boxing Ring

MAY 2025

Network Box Technical News

from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the May 2025 edition of In the **Boxing Ring**

This month, we are talking about **Strengthening Network Security: Best Practices for Administrators**. The Network Box Best Practices distills over two decades of experience in protecting our customers' networks into a set of guidelines. While ultimately, the customer decides their policies, they can significantly reduce their exposure to cyber threats by implementing these best practices. On pages 2 to 3, we discuss this in greater detail and highlight the top three critical security measures that every network administrator must prioritize.

On page 4, we highlight the enhancements and fixes for Network Box 5 and our cloud services that will be released in this quarter's Patch Tuesday.

In other news, Network Box is proud to announce that it won GOLD at the **2025 Asia-Pacific Stevie Awards** in the ***Innovation in Cybersecurity Solutions*** category. In addition, Network Box Hong Kong was at **InnoEX 2025**, which took place at the HK Convention and Exhibition Centre.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
May 2025

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://x.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:

Page 2 to 3
Strengthening Network Security: Best Practices for Administrators

In our featured article, we focus on the top three Network Box Best Practices recommendations for strengthening network security: *Remote Administrative Access*, *Effective Policy Control*, and *Network Segmentation*. Every security incident we have been called in to assist with in recent years has, at its root cause, a violation of at least one of these.

Page 4
Network Box 5 Features

The features and fixes to be released in this month's Patch Tuesday for Network Box 5 and our cloud services.

Page 5
Network Box Highlights:

- **Network Box wins Gold at the 2025 Asia-Pacific Stevie Awards**
- **Network Box Hong Kong**
  □ InnoEX 2025

STRENGTHENING NETWORK SECURITY: Best Practices for Administrators

Based on the experience gained from over two decades of delivering Managed Security Services, investigating security incidents, and working with our customers to protect their networks, the Network Box Best Practices distill this experience down to a simple set of guidelines. Security Engineers refer to these Best Practices when designing defense systems for networks under management, when processing policy change requests, and during periodic configuration reviews.

https://network-box.com/best-practices

We recommend that all customers adhere to these. While ultimately, the customer decides the policy — we strive to inform, warn, and point out when policies conflict and open up networks to common attack vectors and unnecessary risk.

This month, we focus on the top three critical security measures that every network administrator must prioritize: remote administrative access, effective policy control, and network segmentation. Every security incident we have been called in to assist with in recent years has, at its root cause, a violation of at least one of these three.

Remote Administrative Access:
Close the open doors

Allowing remote administrative access to be open to the Internet is akin to leaving the front door of a secure facility unlocked. When services such as Secure Shell (SSH), Remote Desktop Protocol (RDP), or Virtual Network Computing (VNC) are exposed to the public Internet, they become easy targets for cybercriminals looking to exploit weaknesses.

Attackers commonly use brute-force attacks, credential stuffing, and exploits for unpatched software to gain entry. More commonly, leaving remote administrative access open leaves you completely reliant on passwords — effectively at the mercy of a single user making a single simple mistake (by using a weak password) or the exploit of an unpatched vulnerability.

To mitigate these risks, administrators must implement strict access controls. Secure (Virtual Private Networks) VPNs or (Software-Defined Wide Area Network) SD-WAN solutions should be the only permitted gateways for remote access, ensuring that only authorized personnel can connect. Multi-factor authentication (MFA) adds an extra layer of security by requiring more than just a password for entry. Additionally, administrators should set effective firewall policies to block remote administrative access from all but explicitly allowed IP addresses, ensuring access is limited to known locations. Finally, unused remote access services should be completely disabled to remove unnecessary exposure.

Effective Policy Control:
Enforcing security at every level

Weak security policies or inconsistent enforcement can create gaps that attackers can easily exploit. Poor password hygiene, excessive privileges, or failure to log administrative actions are common oversights that can lead to breaches. For example, using default credentials such as **admin/admin** can allow attackers instant access to critical systems.

Organizations must take proactive steps to implement and enforce strong security policies. Password complexity requirements should be mandated, forcing administrators to use strong, unique, regularly updated passwords. Role-Based Access Control (RBAC) ensures that users only have the permissions necessary for their duties, reducing the risk of overprivileged accounts becoming attack vectors. Regular security audits help identify policy weaknesses, allowing administrators to adjust controls accordingly. Furthermore, logging and monitoring access attempts enable teams to detect suspicious activity before an incident occurs.

Network Segmentation:
Containing threats before they spread

A flat network architecture, where all devices communicate freely, creates an ideal environment for attackers. Once an adversary gains access to the network, lateral movement becomes effortless, allowing them to reach sensitive systems without much resistance. A lack of segmentation can turn minor security incidents into full-scale breaches.

Proper network segmentation mitigates these risks by isolating critical resources from general users. Using Virtual Local Area Networks (VLANs) and firewalls to define strict communication policies ensures that only necessary interactions between network zones are permitted. Administrators should regularly review inter-segment traffic rules, ensuring that unnecessary connectivity is removed.

> **Organizations can significantly reduce their exposure to cyber threats by implementing these best practices. Security is not a one-time effort but an ongoing process that requires vigilance, adaptation, and continuous improvement. Network administrators play a critical role in safeguarding digital assets, and by applying these principles, they can fortify their defenses and protect their networks from ever-evolving threats.**
>
> **Using our regular external view scans and policy reviews, Network Box strives to inform, warn, and point out when policies conflict and open networks to common attack vectors and unnecessary risk. But ultimately, you, the customer, decides the policy.**

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 6th May 2025, 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

May 2025

This quarter, for Network Box 5, these include:

- Performance enhancements on map display, and switch to new base map provider.
- Improvements to layout of VPN Session report.
- Improvements to IPSEC NAT-T stability.
- Additional support for Server Side Events in HTTP proxies.
- Enhanced supprot for AUTH SASL authentication in POP3 mail.
- Fix to event correlation alert emails.

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.

NEXT
GENERATION
MANAGED SECURITY

www.network-box.com

Network Box HIGHLIGHTS

Network Box wins Gold at the 2025 Asia-Pacific Stevie Awards

Network Box was named the winner of a GOLD Stevie® Award in the ***Innovation in Cybersecurity Solutions*** category in the 12th annual Asia-Pacific Stevie Awards. This accolade reflects our unwavering commitment to pioneering advanced cybersecurity technologies and reinforces Network Box's position as an industry innovator.

Network Box is honored to be recognized alongside esteemed global organizations such as IBM, Tata Consultancy Services, Cisco Systems, and Singtel in a highly competitive field.

> "We are truly honoured to receive this Gold Stevie Award alongside some of the world's most respected innovators. This prestigious recognition is a testament to our team's relentless commitment and inspires us to drive the evolution of cybersecurity solutions continuously."
>
> **Michael Gazeley**
> Managing Director, Network Box

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

Network Box Hong Kong InnoEX 2025

Network Box Hong Kong was at **InnoEX 2025**, which took place at the HK Convention and Exhibition Centre. During the four-day expo, visitors were introduced to Network Box's award-winning security technologies and managed services. Additionally, Managing Director Michael Gazeley gave a talk to **The Hang Seng University of Hong Kong**, discussing emerging cybersecurity challenges and strategies in the AI era.