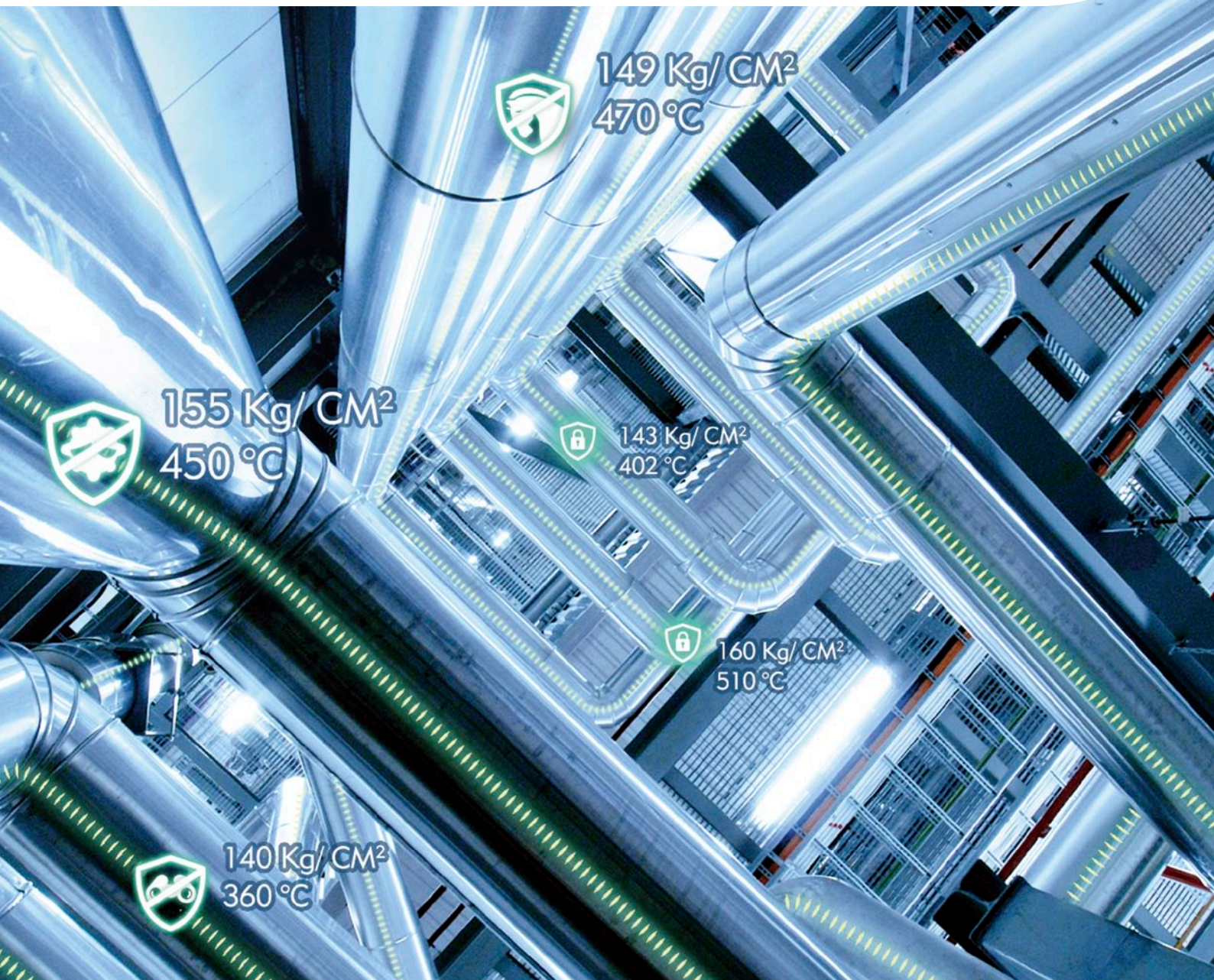
NEXCOM
The Intelligent Systems

White Paper

IDS/IPS Mitigate Cyber Risks in Industrial Networks



Information security used to be concerns for enterprises network as it poses little threat to industrial machines and assets due to their inability to internet access or intranet structures. However, with the trend of IP communication and Internet of Things (IoT), cyber threats intensify, thus making information security controls unignorable issues.

With Industry 4.0, smart factories, and industrial IoT, assets and machines are shifting from closed to open IP communication networks. "With the demands for remote monitor and preventive maintenance, manufacturers link industrial networks with internet, increasing information security risks. Healthcare industries, for instance, should keep data security and patient privacy in mind when pursuing telemedicine advancements. Many industries start paying attention to information security and installing industry firewalls to secure remote access and intercept suspicious data exchanges," said Hadwin Liu, Chief Architect of NEXCOM Network and Communication Solutions Business Group.

Smart IDS/IPS Analytics Complement with Firewalls

Firewalls have been developed over twenty years. They rely on IP or MAC addresses to determine if packets should be allowed or blocked based on the blacklist. Familiar with the mechanism, malicious users keep trying new ways to disguise malware as legitimate packets to bypass firewalls. To complement this, firewall logs must be further examined and analyzed to patch security vulnerabilities.

By integrating advanced intrusion defense systems (IDS) and intrusion prevention systems (IPS), information security products leverage smart control and correlation engine to automatically filter malicious packets that are difficult for firewalls to identify. With industrial protocols and behavior-based pattern matching, they can block suspicious connections from accessing industrial networks and endpoint assets at the bottom layer of the network.

Distributed Architecture for Risk Control and Containment

Enterprise networks adopt central security measures at exit points, which act as gateways for the internal and external data. However, main protection targets in industrial networks are machinery and assets so that network security products should be scattered at exit points of each subdomain in industrial networks for close protection. When malware-infected machinery in one subdomain tries to infect machinery in other domains, once detected, IDS/IPS will drop data packets, cut off connections, and restrict access to the infected subdomain, preventing infection from spreading into the whole networks.

A manufacturer executive revealed that some power trips or malfunctions seemed to have reasonable explanations but chances are that malware infection was the root cause for the incidents. To manufacturers seeing high uptime and efficiency as of great importance, virus- or malware-caused malfunction may lead to as light as short production and productivity interruptions or as critical as production scrap, materials losses, and prolonged lead times.

NEXCOM's industry firewalls combine VPN, firewall, and IDS/IPS as integrated defense to combat various security threats in industrial networks. "Our IDS/IPS engine has rich signature database. Through measures such as log analysis and security incident and event management (SIEM), it detects abnormal programs or codes hiding in normal data packets. While industrial machines adopt dynamic IP address, VPN helps headquarters remotely monitor production," said Liu.

As industries strive to lift management and operational efficiency with IP migration and network connectivity, the security issue should be taken seriously. Shielding industrial networks from virus and malware relies on integrated defense with VPN, firewalls, and IDS/IPS which protects endpoint assets at the bottom layer from risks interrupting operation and from hackers stealing intellectual property and confidential data.

Founded in 1992, NEXCOM integrates its capabilities and operates six global businesses, which are Multi-Media Solutions, Mobile Computing Solutions, IoT Automation Solutions, Network and Communication Solutions, Intelligent Digital Security, and Medical and Healthcare Informatics. NEXCOM serves its customers worldwide through its subsidiaries in five major industrial countries. Under the IoT megatrend, NEXCOM expands its offerings with solutions in emerging applications including IoT, robot, connected cars, Industry 4.0, and industrial security.

www.nexcom.com

© 2015 NEXCOM International Co., Ltd. All Rights Reserved. Published in September 2015