White Paper

Network Security Requirements Changing Rapidly, Market Success Relies on Hardware Expertise

www.nexcom.com

According to International Data Corp. (IDC), in 2020 there will be approximately 1.9 billion computers, 2.6 billion smart phones, 2 billion consumer electronics and 25 billion of embedded and intelligent systems. The number of which is larger than the other three combined. It is apparent that the growth potential of Internet of Things (IoT) is monumental; therefore, in the emerging connected world, ensuring secure network connections will become an important issue.

In 2012, a nuclear power plant in southern Iran was brought to an unexpected halt after a malware attack. Despite the fact that the problem was immediately contained, the threat alerted other nations about the importance of network security. The need for network security exists not only in enterprise data centers. It also exists in telecom data center, machine to machine (M2M) network, industrial applications and small office/home office (SOHO) network. Any device with network connectivity could become a potential entry point for cyber attack and must be protected as well.

Under these premises, the design of the next generation network security platforms must reflect the trend of "Internet everywhere" in addition to focusing on network traffic generated by data access. The platforms must go into telecom data center on account of surging mobile network traffic. They also have to give thorough thought to different network environments including ZigBee, Wi-Fi and industrial network using EtherCAT protocol to ensure security for M2M and industrial networks.

"As applications expand, the amount of network traffic will increase substantially. The existing infrastructure and the underlying platform alone will not suffice to monitor and control the increased traffic. Changes will be required to adapt," said Hadwin Liu, director of product management, NEXCOM Network and Communication Solutions Business Unit.

Step into the New Era of High-Tech Integration

High bandwidth and high-speed packet processing are key to accommodating the increased network traffic, explained Liu. Network security platforms must be dedicated appliances which integrate network processor units (NPU) and switching capabilities for efficient packet processing in contrast to conventional platforms which are computers assembled with add-on cards.

More specifically, next generation network security platforms must equip intelligent NPU capable of implementing security policies to filter packets, inspect packet header for errors, skip and forward the ones with the same header information immediately to avoid repeated inspections. Offloading packet processing from computing cores to a dedicated NPU can increase throughput for network security platforms.

Network security platforms require high throughput capacity because of multimedia packet overhead. In addition, the amount of data generated by M2M is far beyond imagination and beyond the capability of existing infrastructures.

New Evolution of Customized Machines

On the other hand, to allow network security platforms to be used in different application environments and to handle different levels of network traffic, it is essential that the platforms are highly compatible with a variety of network security software to simplify integration for customers. In addition, the platform must comply with standards. For example, NEBS Level 3 certification is the key to ensuring customer success in telecommunication application while EN50155 certification is required by railway application. Liu adds, as industrial control is shifting towards M2M communication, incorporating rugged designs such as wide operating temperatures, water and dust proof, shock and vibration resistance into the platform are also a necessity.

Network security platforms are moving towards a more specialized and custom design to adapt to the changing environment and traffic volume in the future. Beyond unique exterior design, increasing multi-core performance and technology integration, it is far more important to design solutions tailored to specific application needs.

In 2013, NEXCOM, for example, has released new network security hardware aimed at different application needs of the telecommunication, industrial control and high-throughput industries. For telecommunications, NEXCOM provides NEBS Level 3 certified Advanced Telecommunications Computing Architecture (ATCA) blade servers and rackmount servers; for industrial controls, it offers EN50155 certified transportation computers and platforms with DIN-rail mounts for factory environments. As for high-throughput solutions, NEXCOM can design customized solution according to the customers' needs using different central processor units, NPUs and network switch chips.

About NEXCOM

Founded in 1992, NEXCOM has five business units which focus on vertical markets across industrial computer, in-vehicle computer, multimedia, network and communication, and intelligent digital security industries. NEXCOM serves its customers worldwide through its subsidiaries in seven major industrial countries. NEXCOM gains stronghold in vertical markets with its industry-leading products including the rugged fanless computer NISE series, the in-vehicle computer VTC series, the network and security appliance NSA series and the digital signage player NDiS series. www.nexcom.com