WebSensing

Smart NIC / VIN

Guarantee data integrity and prevent network attacks with WebSensing's **Smart Network Interface Card (Smart NIC).**

The Web Sensing **Smart Network Interface Card (Smart NIC)** acts as an intelligent bridge to the Internet from a corporate LAN. It allows corporations to verify that only legitimate and allowed data – i.e. documents and network traffic – flow through the device; all other data is dropped, thereby guaranteeing data integrity and ensuring the absence of network attacks.

The Smart NIC features a customizable data parsing engine that allows formats specified using industry standard Bison/Yacc grammars, state-of-the-art Hammer combinators (for arbitrary binary data), or manually crafted parsing code.

Options are available that allow the Smart NIC to perform IPSec ESP protocol encapsulation and CAVP certified AES encryption on-the-fly.

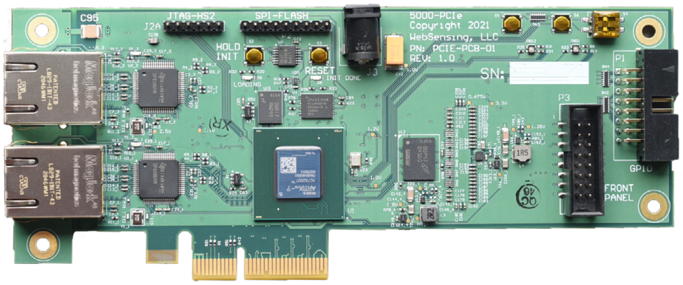
Connections to the Smart NIC can be made via industry standard PCIe and Ethernet interfaces, or optionally, via MIL-STD-1553 and or J1939 interfaces.

When used in matched sets of two or more devices, the Smart NIC provides a network overlay within the Internet called a **Virtual Isolated Network (VIN).** Each VIN connects any group of devices -- computers, laptops, servers and IoT devices -- allowing them to inter-operate while being completely isolated from the rest of the Internet. This effectively creates a "virtual air-gap" around the VIN, precluding malicious intrusions.

Computers or devices can be anywhere in the world, connected to any network, so long as there is a wired Ethernet connection into the Internet.

Since no communication from the VIN to other hosts on the Internet is possible, a VIN is an appropriate location to house valuable data that must be shared within it: intellectual property, industrial manufacturing data, or private personal information.

Web Sensing Smart NIC's are all-hardware devices, containing no vulnerable operating systems or other software. This renders them impervious to software attacks embedded in network traffic.



Form Factor	Card, Desktop or 1U rack-mount
WAN/LAN	Ethernet (10/100/1000)
Protocols	PCIe, Ethernet, MIL-STD-1553, J1939, TCP/IP protocol suite
Encapsulation Protocol	IPSec ESP[1]
Encryption Algorithm	AES[2]
Custom Filtering & Validation	Available
Max Throughput / Latency	1Gbps / 50 micro-seconds
Max Concurrent Sessions	Limited by throughput
Logic	Web Sensing Packet Inspection and AES engines[3]
SNMP[4] Monitoring	Available
Power supply	12vdc/3A
Configuration	Dedicated back-channel

[1] Encapsulating Security Payload
[2] Advanced Encryption Standard
[3] US. Patents: 10,148,761 (Dec 4 2018) and 10,616,344 (Apr 7 2020).
[4] Simple Network Management Protocol