Installed a lot of excellent cyber protection devices but still got hacked from outside or from inside?

Your trusted IT guy intentionally or by mistake allowed access to your sensitive data to your competitors?

Suffering from unauthorized documents copying?

Need to ensure your sensitive traffic reaches your destination directly at a very predictable exact time?

Need to redirect the traffic to additional destination(s), modify or just drop?

Embedded Solutions
Network Applications

Industrial BitNetSentry (iBNS)

Protects your data and your assets. Save your time with BitNetSentry based on and converted from military patented technology.

About Us

Embedded Solutions was established in 2002. The company operates in two modes: 1) In standard mode, the company provides time and mission-critical communication solutions as well as tactical systems. Its technology deals with unstable end-to-end connectivity, strict prioritization requirements, traffic, and protocol restrictions. 2) In stealth mode, Embedded Solutions has developed the BitNetSentry (BNS) communication security device.

Contact Us

Europe and the middle east:
emea@embedded-solutions.co.il

Asia Pacific:
apac@embedded-solutions.co.il

North America and Canada:
usa@embedded-solutions.co.il

North and South Africa:
africa@embedded-solutions.co.il

How It Works?

Transparent network entity

iBNS is a palm-size network device that may be connected at any network.
iBNS has neither network address nor data link address.
BNS inserts negligible latency to the traffic.

Seamless bit-level protection

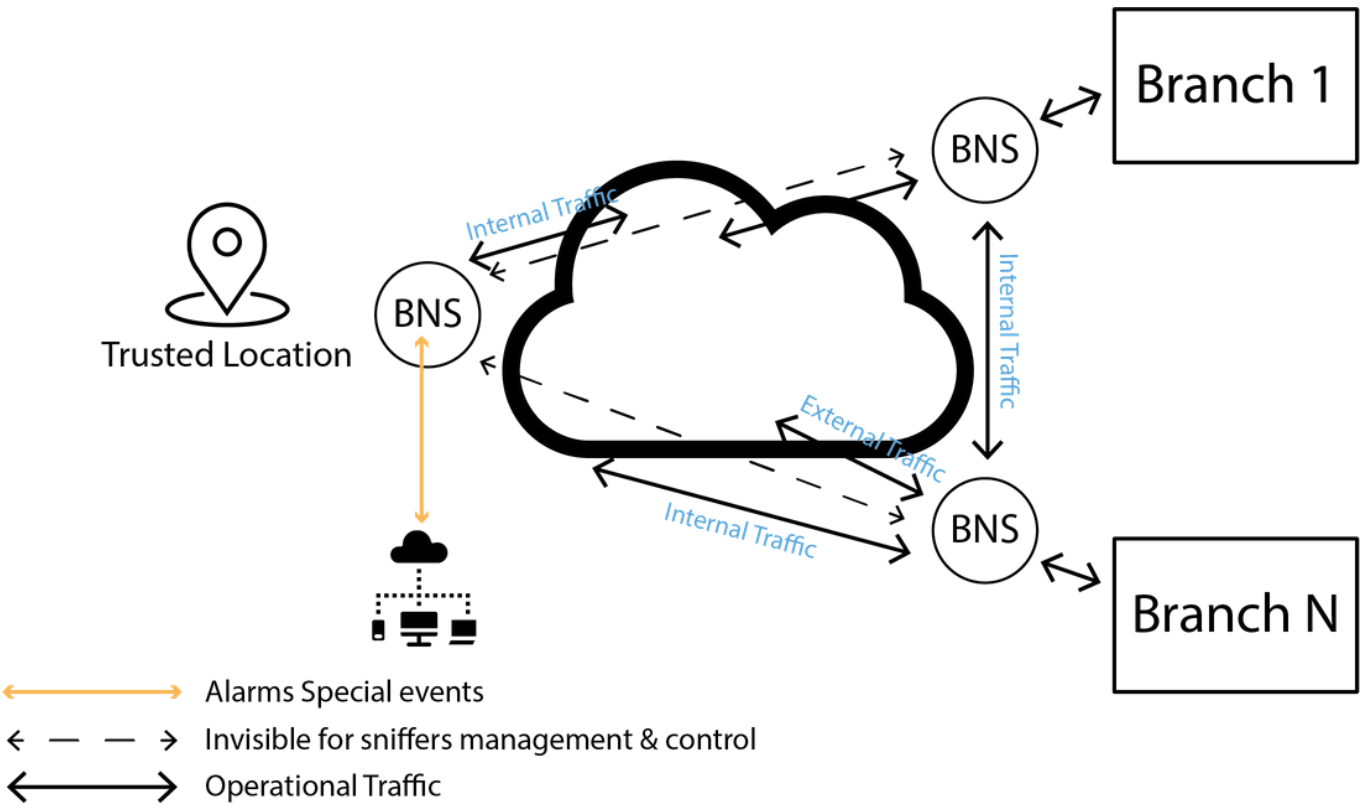
iBNS is not a standard application-level protection. It sits at the lowest level of the network, bringing several key advantages such as independence of the high- level protocols, transparency, and the ability to work also with encrypted data. Our low-level inspection method can tag and monitor network activity without penetrating or decrypting the data, ensuring client privacy. Both data rate (Mb/sec) and network behavior remain unaffected by the system

Seamless traffic modification

Seamless traffic modification BNS allows a seamless modification of any part of the traffic, context or address. Modification of the address part of the traffic will result in the redirection to other destination(s) or sending on behalf of another source (s) thus overriding some of the network devices restrictions.

Seamless and instant integration

Seamless and instant integration BNS can be easily and seamlessly integrated into the existing architecture. No downtime required for the deployment.



Examples of Use Cases

Industrial Espionage

Case Description:
Attempts of an Insider (IT administrator) to provide access to the company's database from outside (competitor's home).

Main Challenge:
IT administrator has all the needed authorization to get access to any data of the company. Therefore, he easily can set a VPN from the hidden location to the database. Moreover, he can also easily define the source address of the request to the data access as a correct address of the company. That is why the VPN would be fully legal, correct, and will pass all firewall checking.

iBNS Benefits:

iBNS seamlessly applies fingerprints (which constantly change, according to a unique mathematical model with variable parameters) to the traffic. The fingerprints are actually some bits long. The entire procedure has zero-latency and is fully invisible to other network entities. Access to the database is allowed only via the BNS box(es). If the traffic comes from an illegal location (even with correct protocol parameters and source addresses), it will be dropped, and its location will be reported as required.

Real-Time redirection of certain kinds of traffic to different destinations

Case Description:
Selection and sorting of real-time data traffic, coming from the same sources to the same destinations. The customer (VOD and interactive games service provider) has to provide different services, different priorities, and different bandwidth to the same consumer, according to a billing code embodied into the traffic.

Main Challenge:
All services are provided in a hard real-time. 1 millisecond delay in the data delivery is considered huge. That is why the context-aware traffic management is totally unacceptable.

iBNS Benefits:
iBNS manages the traffic at the bit level. The required billing code and other customer's criteria for the traffic selection are configured as bit patterns. It allows a zero latency for traffic handling.





Specification

Name	Industrial_BitNetSentry (iBNS)
Model	**Description**
iBNS-BS02	iBNS base station 2 ports
iBNS-BS04	iBNS base station 4 ports: 2 operational, 2 management (optional)
iBNS-RS02	iBNS remote station 2 ports
SW version	ES00X.2.1.2x
Interfaces	
Display Interface	HDMI 1920 x 1200 @ 60Hz (optional)
LAN	2 - 4 x GbE LAN ports subject to iBNS model
Serial	1x Serial communication port, RS232 (optional)
	MIL-SRD 1553 muxbus (optional)
SSD	mSATA SSD 120GB and optional Micro-SD slot support SD/SDHC/SDXC cards
Special I/O	1x micro SIM slot (optional)
Encryption	
Advanced Encryption Standard (AES)	Encryption data traffic per selected channel/s according to AES 256 bit standard (optional)
Operating Conditions	
Input Voltage	Unregulated 10 – 15VDC input, external AC/DC adopter
Power Consumption	5W – 15W
Operating Temperature	-40°C to 70°C
Relative Humidity	10% to 90% (operation), 5% to 95% (storage)
MTTF	> 100,000 hours
Enclosure	
Material	Die Cast Aluminum
Cooling	Passive Cooling Fanless Design
Dimensions	16cm x 16cm x 2.5cm
Weight	660gr
Warranty	3 years (option 5 years)

*iBNS comprehensive functions are confidential. Thus, disclosing additional information is subject to management approval, including signing an NDA.

**Product specification is subject to changes without notice.