Anybus®
BY HMS NETWORKS



Anybus Defender Compact

Industrial Firewall for NAT and Network Segmentation

hms-networks.com/industrial-network-security



INDUSTRIAL CYBERSECURITY

What does your OT network need to survive?

Operational Technology networks were never designed for the threats they face today. Built for reliability and uptime, they were connected to the wider world before security was an afterthought - let alone a priority. Now, with manufacturing, utilities and critical infrastructure firmly in the sights of cyber attackers, the question is no longer whether your OT network needs protecting. It is how you do it without disrupting the production it runs on.

The Anybus Defender Compact was built to answer that question. It is a compact industrial firewall that puts security where it matters most - between the threats outside and the machines that keep your business running.



KEY FEATURES

Under the microscope

Learning Mode for Auto Rule Setup
Monitors traffic and automatically builds security rules.

Industrial-Grade Firewall
Protects your network with IP, port, MAC and protocol-based filtering.

Secure Project Handling
Encrypted, password-protected configurations linked to each device.

Easy Configuration via PC Tool
Set up and managed like a PLC using an intuitive software.

Compact DIN-Rail Design
Space-saving metal housing with industrial-grade durability (IP30).

NAT & Bridge Mode Support
Flexible deployment in new or existing network environments.

Click HERE to find out more >

HOW IT WORKS

A firewall that speaks your language

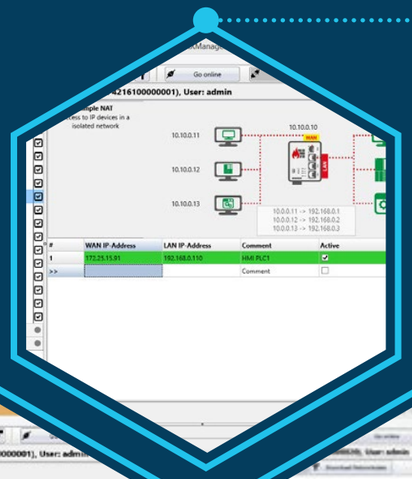
The Anybus Defender Compact is configured using the **Anybus Defender Compact Manager** - a Windows-based tool designed from the ground up for OT engineers, not network security specialists. It feels like configuring a PLC. If your team can commission automation hardware, they can deploy this firewall. It operates in two modes depending on what your installation requires.

In **Bridge mode**, it sits transparently between segments of your existing network, applying firewall rules without requiring any changes to the IP addresses of the devices it protects. There is no reconfiguration, no downtime, no disruption to the machines behind it.

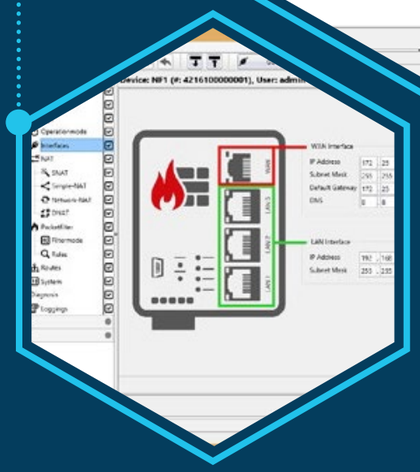
In **NAT mode**, it creates an isolated private network behind a single WAN address - giving you the ability to connect machines with overlapping IP addresses to the same factory network simultaneously, route traffic securely, and expose only exactly what you choose to expose.

Designed for OT teams
The configuration tool is built to resemble PLC programming software - familiar to automation engineers, with no command-line complexity or IT expertise required.

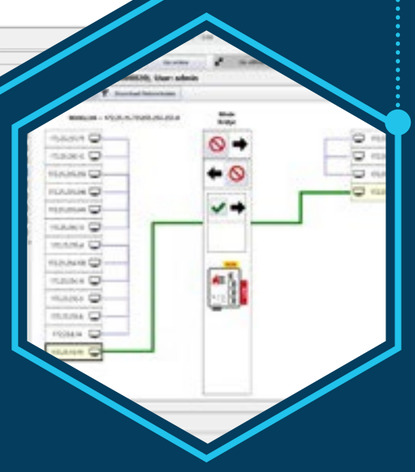
Familiar Workflow for Automation Users



User-friendly Graphical User Interface



Smart Learning Mode



SECURITY ARCHITECTURE

Why security by design is critical

There is a significant difference between a firewall that has had security added to it and one that was built with security as its foundation. The Anybus Defender Compact was designed from the first line of code with the specific threat landscape of OT environments in mind.

Every project file is encrypted and uniquely paired to the device using an RSA key. A configuration pulled from one unit cannot simply be loaded onto another - eliminating one of the most common vectors for industrial network compromise. Secure Boot ensures the device only runs verified, signed firmware. There is no embedded web interface to exploit. Access to the device itself is governed by a 3+2 tiered user access model.

This is not security as a feature. It is security as an architecture. And it matters, because when an OT network is breached, the consequences are not just data loss. They are production shutdowns, safety incidents and reputational damage that can take years to recover from.

Why the governance model matters

- ☑ Secure Boot - device only runs verified, signed firmware
- ☑ No embedded web interface - a common and easily exploited attack surface, removed entirely
- ☑ RSA-paired project files - configurations are encrypted and device-specific
- ☑ 3+2 tiered user access - granular control over who can see and change what
- ☑ Four network access levels - from read-only monitoring to full administration

70% of OT-related incidents are traced back to the IT environment, which means the biggest risk often isn't a "direct hit" on the plant floor - it's lateral movement from IT into OT through shared services, remote access paths, or insufficient separation.

In practice, this is why clear IT/OT zoning and network segmentation (to control and limit pathways) is one of the highest-impact first steps for reducing OT cyber risk.*

*dragos.com

USE CASES

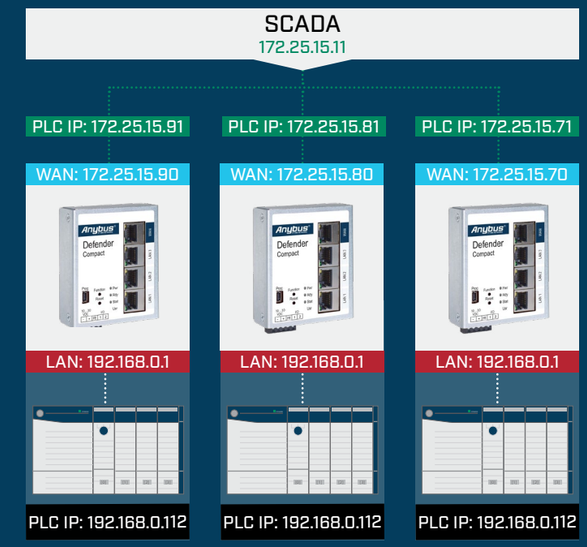
How we're helping customers secure their networks

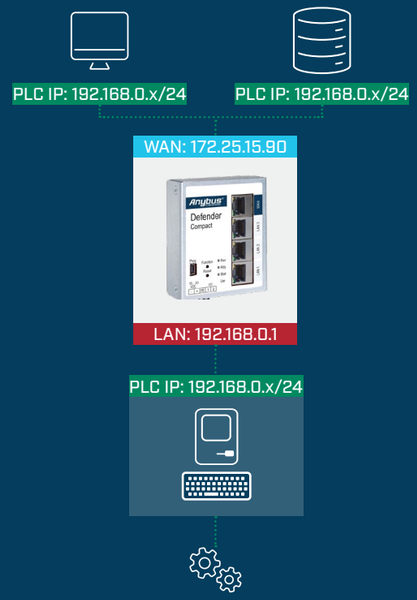
MACHINE BUILDER / SYSTEM INTEGRATOR

Connecting machines that share the same IP address (NAT 1:1)

The challenge: A manufacturer operates a production line made up of cells from three different machine builders. Every cell shipped from the factory uses the same default PLC IP address. Connecting them to a shared OT network creates immediate conflicts - the SCADA system cannot distinguish between them.

The solution: One Anybus Defender Compact is deployed at each machine cell. Using NAT 1:1, a unique virtual WAN IP is assigned to each PLC without touching the PLC configuration. The SCADA system communicates with each machine via its unique address. No changes to field devices. No downtime. No conflicts.





OT NETWORK MANAGER / PLANT ENGINEER

Protecting legacy equipment that cannont be patched (Brigde Mode / Rules)

The challenge: A food processing plant runs CNC equipment that is central to production but cannot be taken offline for software updates. The machines run end-of-life operating systems and are exposed on the factory's flat network - reachable from any connected device.

The solution: The Anybus Defender Compact is placed in front of each legacy cell in bridge mode. IP, port and protocol rules are applied to limit inbound and outbound traffic to exactly what the machine requires. The machines remain untouched. Their exposure is reduced to near zero. Production continues uninterrupted.



SPECIFICATION

Built for industrial environment

The Anybus Defender Compact is housed in a compact metal enclosure rated IP30, designed for DIN-rail mounting in standard control cabinets.

It is engineered to operate reliably across the full temperature range of an industrial setting - from deep-freeze food production to high-temperature process environments.

Specification	Detail
Article number	ABD1004-NATFW
Dimensions (L x W x H)	38.5 × 69 × 92.6 mm / 1.51 × 2.72 × 3.65 in
Weight	235 g / 8.29 oz
Housing	Metal enclosure — IP30 rating (all ports populated)
Mounting	DIN rail — EN50022, 35 × 7.5 and 35 × 15
Operating temperature	-40 to 75°C / -40 to 167°F
Humidity	Non-condensing, 0–95%
Power input	10–30V DC
Power consumption	Max 250 mA @ 24V DC
Network interfaces	1× WAN + 3× LAN — 10/100 BASE-T(X) RJ45
Operating modes	Bridge mode / Gateway (NAT/Routing) mode
NAT modes	1:1 NAT, SimpleNAT, NetworkNAT, SNAT, Port Forwarding (DNAT)
Firewall filtering	IP, port, protocol, MAC — WAN->LAN and LAN->WAN — Black/White listing
Leaning mode	Live traffic capture converted to filter rules
Access control	Four user access levels + 3+2 tiered admin model
Services	NTP Client, Syslog Client
Configuration	Anybus Defender Compact Manager (Windows) or CLI via SSH
Certificates	CE, UL (E482663)

CE c UL us LISTED PROG. CNTLR. E482663



Work with HMS Networks. The number one choice for Industrial Communication and IIoT

HMS Networks - Contact

HMS Networks is represented all over the world.
Find your nearest contact here:

www.hms-networks.com/contact-us

Scan the QR code
to explore Anybus
Defender Compact:

Anybus® are registered trademarks of HMS Industrial Networks AB, Sweden, USA, Germany and other countries. Other marks and words belong to their respective companies.
All other product or service names mentioned in this document are trademarks of their respective companies.
© HMS Industrial Networks - All rights reserved - HMS reserves the right to make modifications without prior notice.