

Defender 6024

Industrial Security Appliance



The Anybus Defender is an advanced industrial security appliance engineered to provide unparalleled protection for operational technology (OT) networks. Featuring a robust combination of NAT, Routing, Deep Packet Inspection (DPI), and VPN Server and Client functionalities, it serves as a cornerstone for safeguarding critical infrastructure against a myriad of cyber threats.

Key use cases:

- **OT/IT Segregation:** Enforce strict policies for domain separation.
- **Address Conflict Avoidance:** Manage IP addresses efficiently thorough implementation of Network Address Translation (NAT) and routing scenarios.
- **Deep Packet Inspection:** Ensure security of industrial protocols.
- **IEC62443 Compliance:** Implement security zones and conduits according to industry standards for precise machine isolation.
- **Secure Plant-to-Plant OT Connections:** Establish encrypted links between facilities using WireGuard®, OpenSSL, and IPsec Virtual Private Network (VPN) protocols.

Advanced Router and Firewall

1x WAN and 3x LAN Gigabit Ethernet ports plus 2 SFP ports for fibre optic connectivity in a Rugged Fan-less IP50 construction for tough environments. Configurable in transparent bridge mode or NAT/Routing mode. Full IPv4 and IPv6 compatible includes DHCP Server, Relay, PPPoE, IGMP Proxy and support for RIPv1 & v2, BGPv4 routing protocols. Supports Rules/policy scheduling and Application and URL whitelisting.



3 License options

The Anybus Defender comes pre-configured with one of 3 licensed options to meet your use-cases:

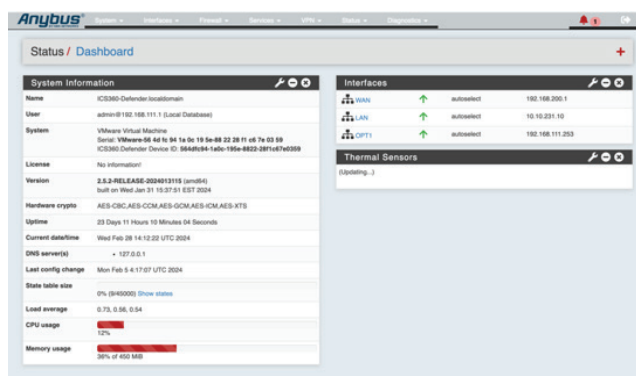
- **NAT/FW:** for network segmentation and translation
- **DPI/FW:** + Virtual Patching of legacy devices and granular Access Control with policy management of industrial protocol transactions
- **PRO/FW:** + Advanced VPN (WireGuard, OpenSSL & IPsec), Traffic shaping and routing functions & high availability capability



Graphical User Interface (GUI)

Configuration via on board Web interface with use-case wizards for easy configuration. Create rules effortlessly with One-Click Easy Rule creation directly from firewall logs, alongside Floating Rules applicable across all interfaces. Benefit from rich debug and traffic diagnostics capabilities, complemented by an integrated Restful API for seamless integration with higher-level systems. Additionally, gain access to CLI SSH/Console for maintenance tasks.

Optional: Central Anybus Cybersecurity Console for management of a group of Defenders.



Product selection

| Article nr: | Description: |
|---------------|--|
| ABD6024-NATFW | Industrial Security Appliance - DIN Rail - 2x1Gbit SFP + 4x1Gbit RJ45NAT/FW Perpetual License inc. 3Y support |
| ABD6024-DPIFW | Industrial Security Appliance - DIN Rail - 2x1Gbit SFP + 4x1Gbit RJ45 - DPI/FW Perpetual License inc. 3Y support |
| ABD6024-PROFW | Industrial Security Appliance - DIN Rail - 2x1Gbit SFP + 4x1Gbit RJ45 - PRO/FW Perpetual License inc. 3Y support |

Defender 6024

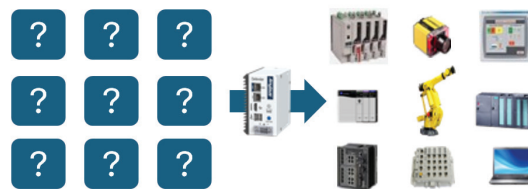
Rich Network Security Controls



Anybus Defenders uphold a Deny by Default policy, ensuring that all network communication traffic is prohibited unless explicitly permitted by the system in both inbound and outbound directions. Simplified NAT Configuration facilitates the setup for single or multiple IP addresses, subnets, or transparent layer 2 firewalling, capable of bridging interfaces and filtering traffic. Enjoy seamless high-throughput Deep Packet Inspection (DPI) for common industrial protocols, supported by an intuitive user interface equipped with auto-learn capabilities to minimize manual rule creation. Integrated of Snort and Suricata, the Defenders offer robust Intrusion Protection capabilities, allowing for virtual patching scenarios. Monitoring and reporting functionalities include Arp and bandwidth monitoring accessible through API. Standard features encompass email reports, syslog integration, and integration with Telegram Messenger as well as Pushover Notifications, while optional NetFlow integration provides additional integration options.

Asset Discovery & Inventory

The platform incorporates a specialized network asset identification scanner meticulously tailored for OT/ICS devices, offering comprehensive visibility into connected assets. Utilizing a range of industrial-specific protocols and methodologies, it seamlessly discovers, queries, and identifies assets within the network. Extracted information includes crucial details such as make, type, software version, patch level, and serial number, accompanied by an accuracy score for reliability assessment. Accessible through the intuitive Web GUI or centrally propagated to the optional Central Anybus Cybersecurity Console, this information empowers users with actionable insights for enhanced network management and security.



| Features License Type | NAT/FW | DPI/FW | PRO/FW |
|---|--------|--------|--------|
| Simple NAT Wizard, 1:1, 1:∞ | ✓ | ✓ | ✓ |
| Stateful Firewall | ✓ | ✓ | ✓ |
| Transparent/Bridge Mode | ✓ | ✓ | ✓ |
| Certificate Management | ✓ | ✓ | ✓ |
| Central Anybus Cybersecurity Console Support | ✓ | ✓ | ✓ |
| Asset Discovery & Inventory | ✓ | ✓ | ✓ |
| Email, Syslog, Telegram Messenger and Pushover Notifications | ✓ | ✓ | ✓ |
| Remote Client VPN | | ✓ | ✓ |
| RADIUS, LDAP/AD Authentication | | ✓ | ✓ |
| Industrial Protocol DPI with traffic analyser to learn traffic and allow easy config (Ethernet/IP CIP & Modbus) | | ✓ | ✓ |
| Virtual Patching through IPS (Snort, Suricata) | | ✓ | ✓ |
| WireGuard*, OpenSSL & IPsec VPN | | ✓ | ✓ |
| DHCP Server & DHCP Forwarding | | ✓ | ✓ |
| Rules/Policy Scheduler (by date/time/duration) | | ✓ | ✓ |
| Captive Portal | | | ✓ |
| RIPv1 & v2, BGPv4 routing protocols | | | ✓ |
| Load Balancing, Multi-WAN | | | ✓ |
| Traffic Shaping | | | ✓ |
| High Availability Redundancy | | | ✓ |

Defender 6024

General

| | |
|----------------------------|--|
| Dimensions with connectors | 140,4 x 69,6 x 179,7 mm / 5,53 x 2,74 x 7,07 inch |
| Weight | 1270 gr, 2.8 lbs |
| IP rating | IP50 construction |
| Housing material | Metal enclosure |
| Mounting | DIN rail according to EN50022 |
| Operating temperature | 0°-50°C 32°-122°F |
| Humidity | Non-Condensing 0%- 85% |
| Configuration | Via Web interface locally or optional Anybus Cybersecurity Console capable of managing several Defenders simultaneously. CLI SSH/Console access for maintenance tasks. |
| Certification | CE, 2011/65/EU (RoHS) |

Power

| | |
|---------------------|---|
| Input voltage | 24V DC Power Entry |
| Current consumption | Max 1100 mA @ 24 Volts, 26,4 Watts (based on maximum ratings) |

Network interfaces

| | |
|-----|---|
| WAN | One (1) RJ45 Gigabit Ethernet |
| LAN | Tree (3) RJ45 Gigabit Ethernet ports Two (2) SFP ports providing the choice of 1Gig LC Fibre (multi-mode or single-mode) or additional RJ45 Gigabit Ethernet ports |

**LAN ports are individually configurable and can be reconfigured as a 2nd WAN port for appropriate use-cases.*

Software Specifications

| | |
|----------------------------|---------------------------------------|
| Operating Modes | Bridge / Gateway mode |
| Choice of security license | NAT/FW, DPI/FW, PRO/FW |
| License type | Perpetual |
| Warranty | 3 years support and warranty included |

