



HARDWARE PLATFORM MADE IN TÜRKİYE

FIREWALL SECURITY PLATFORM

Firewall

**Not a brand license,
the right hardware.**

Server-class, modular-port firewall hardware for hotels, factories, campuses, enterprise internal networks and the data-centre edge. The hardware platform is Simgenet's; on it runs an open-source firewall operating system delivered with its free edition, with an optional move to the licensed edition — software licensing and software support belong to the software vendor.

1G–100G

MODULAR PORTS

1U · 2U

TWO CHASSIS
FAMILIES

Bypass

CARD PORT
OPTION

**–20 to
+60 °C**

INDUSTRIAL
TEMPERATURE



Datacenter Series · 2U modular chassis, 8 expansion slots



01

CORPORATE

We Build the Hardware, We Are Open About the Software

Simgenet Mühendislik is a Turkish engineering company delivering industrial networking and critical-infrastructure communication systems. In the Firewall Security Platform **Simgenet's part is the hardware platform**: chassis, processor and memory selection, modular network cards, bypass, industrial temperature and EMC, installation and hardware support.

2000

FOUNDED

500+

PROJECTS DELIVERED

30+

COUNTRIES SERVED

100+

PRODUCTS

■ Hardware — Simgenet

- Server-class x86 chassis: 1U (SMG104-EDGE family) and 2U (SMG818 Datacenter Series)
- Modular network-card ecosystem: 1G copper/fiber, 10G, 40G, 100G; **bypass cards**
- Industrial temperature -20 to +60 °C, EN 61000-4 Level 3 EMC, CE / LVD / RoHS
- Installation, commissioning, hardware warranty and on-site support

■ Software — third-party firewall operating system

- Open-source **OPNsense**; the appliance ships with the **free Community edition**
- If the customer wishes, they move to the **commercial Business subscription** independently, with the software vendor
- Software licensing, updates and software support **belong to the software vendor**; Simgenet does not develop or own this software
- Simgenet configures the platform with this software and verifies hardware compatibility

No confusion. Simgenet's SMGOS, SVP, GNSS, NAC, storage and IP-PBX software is developed entirely in house; **the Firewall is not on that list**. The Firewall Security Platform is a hardware product; firewall functions belong to the third-party operating system running on it. We state this distinction explicitly at proposal and specification stage.

Our Mission

To deliver innovative, reliable and sustainable technology solutions for industrial networking and critical-infrastructure communication, safeguarding our customers' business continuity.

Our Vision

To become Türkiye's most trusted and innovative network-infrastructure technology partner and a globally recognized brand.



02

PLATFORM

What Is the Firewall Security Platform?

A **server-class, modular-port firewall hardware platform built for 24/7 operation**, for projects where the license cost of a branded firewall outweighs the technical need. Positioned for enterprise internal-network segmentation, enterprise edge and aggregation points and the data-centre edge — not as a direct replacement for the classic branded firewall but as **the complementary, cost-effective layer of a layered architecture**.

■ The right hardware

Server-class processor, ECC memory, mirrored-disk log safety, industrial temperature and EMC; port layout is defined per project by cards, and the line stays up with a bypass card.

■ Open, up-to-date software

A widely used, actively developed open-source firewall operating system: stateful firewall, IDS/IPS, VPN, proxy, routing, high availability and more than 70 plug-ins.

■ License flexibility

Start with the free edition; if a commercial subscription is needed the customer deals directly with the software vendor. The hardware investment is independent of the software decision.

Design Philosophy

- No claim of "the firewall that does everything alone"; a part of the right architecture
- Policy-based and selective security: IPS and deep packet inspection on targeted traffic
- High bandwidth and stability without unnecessary license cost
- Full fit with hybrid and layered security architectures
- Single-processor model: simple, sustainable, long-lived hardware
- External syslog / SIEM integration recommended for long-term log retention

■ Intended use

- Large hotel networks, factories and industrial facilities, campus networks
- Enterprise internal-network segmentation (VLAN / zone based), enterprise edge and aggregation
- Critical-infrastructure and substation security gateway (ICS protocol awareness)
- Data-centre edge (north-south) and internal (east-west) segmentation; ISP edge/aggregation; 100G aggregation

■ Not intended for

- Small office / SOHO environments
- The data-centre core firewall role
- Architectures requiring continuous IPS, SSL/TLS inspection or full DPI at full 100G bandwidth

Why this approach. In many enterprise and industrial projects the firewall's real job is segmentation, VPN and policy enforcement; a brand license multiplies the price of that job. Simgenet builds the right hardware, configures it with open software and supports the hardware — the customer makes the license decision.



03

HARDWARE

Models and Modular Port Architecture

Two chassis families, the same modular card ecosystem. The port count is not fixed: **slots × installed cards**. With bypass cards the line stays up even if the firewall goes down.



SMG104-EDGE · EDGE PLUS · EDGE MAX — Modular Edge and Internal Network

- 1U 19" rackmount; server-class 4-core / 8-thread processor, ECC memory
- Memory 16 / 32 / 64 GB DDR4 ECC (EDGE / PLUS / MAX); 40G entitlement on MAX
- 2× SATA (single or mirrored disk — log safety) + CF; 4× PCIe x8 slots; 2× on-board GbE, 2× USB, console
- 1× 220 V AC 250 W; 430 × 550 × 44.5 mm; -20 to +60 °C

■ Card catalogue — 1U EDGE family

- **1G:** 4× SFP · 4× RJ45 · 8× RJ45 · 4× RJ45 + 4× SFP
- **10G:** 2× SFP+ · 4× SFP+
- **40G:** 2× QSFP+ (EDGE MAX)
- A different card in every slot; e.g. 4 slots × 8×1G = 32 copper ports

■ Bypass — the line is never cut

On bypass copper cards, if the appliance powers off or the software stops, the port pairs are physically connected to each other; the critical line stays up even through a firewall failure. A prerequisite for in-line deployment in power and production networks.



SMG818 Datacenter Series — Data-Centre and ISP Edge

- 2U 19" rackmount; 24-core / 48-thread server processor, 45 MB L3
- 8× PCIe slots; designed for 100G aggregation and east-west segmentation
- Many VLANs / VRFs / zones; policy-based firewall; selective IPS; sustained 40–60 % processor band
- -20 to +60 °C; EN 61000-4 Level 3

■ Card catalogue — 2U Datacenter Series

- **1G:** 4× SFP · 8× SFP · 4× RJ45 **bypass (2 pairs)** · 8× RJ45 **bypass (4 pairs)**
- **10G:** 2× SFP+ · 4× SFP+
- **40G:** 2× QSFP+ · **100G:** 2× QSFP28
- Up to 8 slots × 2×100G; 40G/100G cards for the data-centre edge and east-west segmentation

■ EMC and compliance (both families)

- EN 55035 immunity: ESD ±4/±8 kV · RF 10 V/m · EFT ±2/±1 kV · surge ±2/±1 kV · conducted RF 10 V · magnetic 30 A/m · voltage dips
- CE (2014/30/EU EMC, 2014/35/EU LVD) · LVD IEC/EN 62368-1 · RoHS 2011/65/EU
- Storage -20 to +75 °C, 5–95 % humidity (non-condensing)



04

SOFTWARE CAPABILITIES

Firewall, IDS/IPS and Content Security

The functions below are capabilities of the **open-source firewall operating system** on the platform; they are offered by version and plug-in, and licensing and support belong to the software vendor. Simgenet verifies the hardware's compatibility and performance with these functions.

■ Stateful firewall

- IPv4/IPv6 stateful packet inspection, zone-based security
- Rule aliases: IP, network, port, MAC, GeoIP, BGP ASN; schedule-based rules
- NAT: source, destination, port, 1:1, NPT (IPv6)
- Rule-based packet filtering, logging and counters; packet capture and analysis

■ Attack and abuse protection

- Anti-DDoS: SYN cookies, rate limiting, connection limits
- Bogon blocking; country-based (GeoIP) traffic blocking
- State-table control: size, connections/s, timeouts
- Traffic normalization — protection against protocol inconsistencies

■ IDS / IPS and industrial protocol awareness

- Network-based intrusion detection and prevention — in-line or passive mode
- **ICS protocol awareness:** Modbus TCP, DNP3, EtherNet/IP application-layer analysis
- SCADA/ICS attack and anomaly rule sets (commercial rule subscription option)
- Deep packet inspection and L7 application control (plug-in)

■ Web and content security

- Web application firewall — against injection attacks
- Transparent / explicit caching web proxy; HTTP/HTTPS filtering; SSL/TLS inspection
- URL, domain and category-based access control (plug-in); antivirus scanning (plug-in)
- DNS filtering (DNS over TLS); automatic SSL/TLS certificate issuance and renewal

For the substation and the factory. ICS protocol awareness and SCADA rule sets enable the in-line security-gateway role at the IT/OT boundary; with a bypass card the line is never cut. IEC 61850/62351 robustness and OT security vectors are measured at installation with Simgenet SVP.



05

SOFTWARE CAPABILITIES

VPN, Identity, Routing and High Availability

■ VPN and remote access

- **IPsec** — IKEv1/IKEv2, route-based VTI, site-to-site and remote access
- **OpenVPN** — SSL/TLS VPN, site-to-site and road warrior; client export with QR code
- **WireGuard** — modern, high-performance VPN; configuration by QR code
- Further VPN types by plug-in; L2TP · **Multi-factor authentication** (MFA)

■ Identity and access control

- Local user and group management; **RADIUS / LDAP / AD** central identity integration
- Captive portal — web-based authentication before network access
- Certificate management: SSL/TLS certificates, CA and CRL
- Single sign-on (SSO) with directory services

■ Routing and networking

- Static and dynamic routing: OSPF, BGP, IS-IS, LDP, PIM, RIP (plug-in); policy-based routing
- VLAN 802.1Q (4096/interface), QinQ 802.1ad, VXLAN overlay, layer-2 bridging (RSTP)
- GRE/GIF tunnels; virtual IPs (CARP, IP alias, proxy ARP); full IPv4/IPv6 dual stack; LAGG
- Traffic shaping / QoS; multi-WAN (failover and balancing); gateway monitoring (RTT, loss)

■ High availability and network services

- **CARP** active/passive or active/active failover; **state synchronization**; configuration sync
- Server load balancing (plug-in)
- DHCPv4/v6 server and relay; DNS server (recursive + forwarder, DNS over TLS); NTP server; dynamic DNS
- SNMP v1/v2c/v3

■ Management and monitoring

- Web interface: role-based access, customizable dashboard; console and SSH; **REST API** (ACL-backed)
- Central multi-site management and firmware control (plug-in)
- NetFlow / IPFIX flow analysis; live traffic graph and top talkers; system health graphs; service monitoring and conditional alerts
- Syslog: UDP/TCP/TLS, local and remote; LLDP topology discovery

■ Backup and version management

- Automatic updates from web/console
- Backup and restore: local and cloud/repository targets
- Configuration history: change tracking, rollback to a previous version
- Full system snapshot and fast rollback; extensible with 70+ plug-ins



06

USE

Scenarios and Positioning

■ Hotel, campus, estate

VLAN/zone segmentation with high port density, guest access with captive portal, multi-WAN, QoS; direct floor connections with copper cards. SMG104-EDGE / PLUS.

■ Factory and industrial facility

In-line security gateway at the IT/OT boundary: ICS-aware IDS/IPS, uninterrupted line with a bypass card, industrial temperature; together with SMG-SW switches and the NAC Server. SMG104-EDGE MAX.

■ Enterprise edge and aggregation

Site-to-site IPsec/WireGuard, remote-access VPN and MFA, dynamic routing, 1+1 redundancy with CARP; the enterprise edge without a brand license. SMG104-EDGE PLUS / MAX.

■ Data-centre and ISP edge

100G aggregation, east-west segmentation, many VLANs/VRFs/zones, policy-based firewall and selective IPS; 2U chassis, 8 slots, 100G cards. SMG818 Datacenter Series.

Model Positioning

SMG104-EDGE

Internal network and edge — 1U, 16 GB, 1G/10G cards

EDGE PLUS / MAX

Enterprise edge, facility — 32 / 64 GB, 40G on MAX

SMG818 DC

Data-centre edge, ISP — 2U, 8 slots, 100G

With the Simgenet ecosystem. The firewall hardware is deployed from one source with SMG-SW switches, the Simgenet NAC Server (802.1X/AAA), the GNSS Server (time) and the SVP test platform; segmentation and OT security acceptance is delivered with an SVP report.

About software support. Installation and configuration are done by Simgenet; the operating system's licensing, updates and software-level support are the responsibility of the software vendor. Paid components such as the commercial subscription, SCADA rule sets and the DPI plug-in are procured directly by the customer.



07

SPECIFICATIONS

Hardware Platform

FEATURE	SMG104-EDGE	SMG104-EDGE PLUS	SMG104-EDGE MAX	SMG818 DATACENTER
Form factor	1U 19" rackmount	1U 19" rackmount	1U 19" rackmount	2U 19" rackmount
Processor	Server-class 4 cores / 8 threads, 3.4–3.8 GHz, ECC			Server-class 24 cores / 48 threads, 2.0 GHz (turbo ~3.8), 45 MB L3
Memory	16 GB DDR4 ECC	32 GB DDR4 ECC	64 GB DDR4 ECC	Per project
Storage	2× SATA 3.0 (single or mirrored disk) + CF			Per project
Expansion	4× PCIe x8			8× PCIe
Cards	1G: 4×SFP · 4×/8×RJ45 · 4×RJ45+4×SFP · 10G: 2×/4×SFP+		+ 40G: 2× QSFP+	1G: 4×/8×SFP · 4×/8×RJ45 bypass · 10G: 2×/4×SFP+ · 40G: 2×QSFP+ · 100G: 2×QSFP28
On-board	2× RJ45 GbE, 2× USB 2.0, 1× console			Console / management
Power	1× 220 V AC, 250 W			Per project
Size / weight	430 × 550 × 44.5 mm · 20 kg			2U
Operating temperature	–20 to +60 °C · storage –20 to +75 °C, 5–95 % humidity (non-condensing)			
EMC / compliance	EN 61000-4 Level 3 · EN 55035 immunity · CE (2014/30/EU, 2014/35/EU) · IEC/EN 62368-1 · RoHS 2011/65/EU			
Intended use	Hotel, factory, campus, enterprise internal network and edge; critical-infrastructure security gateway			Data-centre edge and internal network, ISP edge/aggregation, 100G aggregation

SOFTWARE (THIRD PARTY)	DESCRIPTION
Operating system	OPNsense — open-source firewall operating system; the appliance ships with the free Community edition; the customer moves to the commercial Business subscription independently, with the software vendor
License and support	Software licensing, updates and software support belong to the software vendor; Simgenet provides the hardware platform, installation, configuration and hardware support
Capability summary	Stateful firewall, NAT, anti-DDoS, GeoIP · IDS/IPS (ICS-aware), DPI (plug-in) · web proxy / WAF / URL / DNS filtering · IPsec, OpenVPN, WireGuard, MFA, captive portal · RADIUS/LDAP/AD, SSO · OSPF/BGP/IS-IS, VLAN/VXLAN, multi-WAN, QoS · CARP HA, state sync · web/API/NetFlow/syslog · backup, snapshots, 70+ plug-ins



Why Simgenet Firewall Security Platform

The right hardware at the right price

Server-class processor, ECC memory, mirrored disk, modular 1G–100G ports, industrial temperature — without a brand license.

The line is never cut

With bypass cards the port pairs stay connected even if the firewall stops; for in-line OT deployment.

Open software, your license decision

Delivered with the free edition; the customer moves to a commercial subscription on their own. Software support with the vendor, hardware support with Simgenet.

Part of the ecosystem

Deployed from one source with SMG-SW switches, NAC Server, GNSS Server and SVP; acceptance delivered with an SVP report.

GET IN TOUCH

Address

Kartal / İstanbul, Türkiye

Phone

+90 555 600 4506

E-mail · Web

info@simgenet.net · simgenet.net

Simgenet Mühendislik Enerji San. ve Tic. Ltd. Şti.

Product Brochure · SMG-UB-FW-EN · Rev. 2 · © 2026

Hardware Made in Türkiye