SimgeNet Mühendislik

# SIMGENET FIREWALL SECURITY PLATFORM

## Modular Edge & Internal Network Firewall Platform

SMG104-EDGE | SMG104-EDGE PLUS | SMG104-EDGE MAX

*Product Datasheet*

## 1. Product Description

The Simgenet Firewall Security Platform — SMG104-EDGE Series is a server-class, modular firewall platform built for hotels, factories, campuses, large enterprise internal networks, and critical infrastructure requiring 24/7 uninterrupted operation with high port density and flexible network interfaces.

The platform is positioned not as a direct replacement for branded firewalls, but as a **complementary, cost-effective security layer** for internal network security, corporate edge, and aggregation scenarios.

## 2. Positioning & Target Use Cases

- Large-scale hotel networks
- Factory and industrial facility networks
- Campus and site networks
- Enterprise internal network segmentation (VLAN / zone-based)
- Corporate edge and aggregation points
- Critical infrastructure substation security gateways (35/10kV, 110/35kV)
- Projects where branded firewall licensing costs exceed technical requirements

**Not targeted for:** Small office / SOHO environments. Not intended for datacenter core firewall roles.

## 3. Design Philosophy

The SMG104-EDGE Series does not adopt the “all-in-one firewall” approach. It is designed as a **purpose-built component within a properly architected security infrastructure**, delivering high bandwidth and stability without excessive licensing costs. This approach is fully compatible with hybrid security and layered architectures widely used in modern networks.

## 4. Product Family

The SMG104-EDGE Series is offered in three capacity tiers on the same chassis, CPU architecture, and modular NIC ecosystem:

| Model | RAM | Storage | 40G Support | PCIe Slots |
|---|---|---|---|---|
| **SMG104-EDGE** | 16 GB DDR4 ECC | SATA / CF | — | 4 × PCIe x8 |
| **SMG104-EDGE PLUS** | 32 GB DDR4 ECC | SATA / CF | **Supported** | 4 × PCIe x8 |
| **SMG104-EDGE MAX** | 64 GB DDR4 ECC | SATA / CF | **Supported** | 4 × PCIe x8 |

## 5. Hardware Platform

| Specification | Detail |
|---|---|
| **Chassis** | 19-inch 1U Rackmount |
| **Architecture** | x86, DDR4 |
| **Chipset** | Intel® C236 |
| **CPU** | Intel® Xeon® E3-1230 v5 — 4 Core / 8 Thread, 3.4–3.8 GHz, TDP 80W, ECC support |
| **Memory (RAM)** | 16 / 32 / 64 GB DDR4 ECC (model dependent) |
| **Storage** | 2 × SATA 3.0 (2.5” / 3.5”) + 1 × CF Interface |
| **Expansion Slots** | 4 × PCIe x8 (modular NIC slots) |
| **Operating System** | OPNsense Business Edition (commercially licensed) |

## 6. Physical & Environmental Specifications

| Parameter | Value |
|---|---|
| **Power Supply** | 1 × 220 VAC, 250W Single PSU |
| **Dimensions (W×D×H)** | 430 mm × 550 mm × 44.5 mm |
| **Weight** | Net 20 kg |
| **Operating Temperature** | -20°C ~ +60°C |
| **EMC** | EN 61000-4 Level 3 |
| **Storage Temperature** | -20°C – 75°C |
| **Humidity** | 5% – 95% (non-condensing) |
| **Front Panel I/O** | 2 × USB 2.0, 2 × RJ45 GbE, 1 × COM Port, Power/HDD LEDs |

## 7. Modular Network Interfaces

The SMG104-EDGE Series supports the following field-replaceable modular NIC cards. Module selection is configured per customer requirements.

| Model | Controller | Speed | Media | Ports | Notes |
|---|---|---|---|---|---|
| **SMG 7103PF-2QSFP+** | Intel XL710 | 40G | Fiber | 2 × QSFP+ | PLUS/MAX only |
| **SMG 7103PF-4SFP+** | Intel XL710 | 10G | Fiber | 4 × SFP+ | |
| **SMG 7103PF-2SFP+** | Intel XL710 | 10G | Fiber | 2 × SFP+ | |
| **SMG 5993PF-2SFP+** | Intel 82599 | 10G | Fiber | 2 × SFP+ | |

| | | | | | |
|---|---|---|---|---|---|
| **SMG 3503PF-4SFP** | Intel I350 | 1G | Fiber | 4 × SFP | |
| **SMG 3503PT-4T** | Intel I350 | 1G | Copper | 4 × RJ45 | |
| **SMG 3503PT-8T** | Intel I350 | 1G | Copper | 8 × RJ45 | |
| **SMG 3503PT-4T4S** | Intel I350 | 1G | Copper+Fiber | 4×RJ45+4×SFP | |
| **SMG 3503BP-4T** | Intel I350 | 1G | Copper (Bypass) | 4 × RJ45 | |
| **SMG 3503BP-8T** | Intel I350 | 1G | Copper (Bypass) | 8 × RJ45 | |

***Note:*** *40G QSFP+ modules are supported only on SMG104-EDGE PLUS and SMG104-EDGE MAX models.*

## 8. Supported Software Features (OPNsense Business Edition)

The Simgenet Firewall Security Platform supports all core and advanced network security features provided by the OPNsense operating system. Software capabilities are **hardware-model independent**; the hardware determines the concurrent capacity and performance level of these features.

| Category | Supported Features |
|---|---|
| **Stateful Firewall** | Layer 3 / Layer 4 stateful packet inspection, zone-based security, IPv4/IPv6 |
| **Firewall Aliases** | Simplified rule management using aliases for IP addresses, networks, ports, MACs, GeoIP and BGP ASN |
| **Time-based Firewall Rules** | Schedule-based firewall rules — active only during specified times or schedules |
| **NAT** | Source NAT, Destination NAT, Port NAT, 1:1 NAT, NPt (IPv6 prefix translation) |
| **ACL / Packet Filter Rules** | Granular Access Control Lists — rule-based packet filtering with per-rule logging and counters |
| **Anti-DDoS** | DDoS protection using SYN cookies, rate limiting and connection limits |
| **Bogon Network Blocking** | Blocks traffic from bogon (unallocated or private) IP address spaces |
| **GeoIP Filtering** | Country-based traffic blocking using MaxMind GeoLite2 databases |
| **Granular State Table Control** | Control over state table size, rule bases limitations, connections per second, timeout and state type options |
| **Traffic Normalization** | Protects internal machines against inconsistencies in Internet protocols and implementations |
| **Packet Capture & Analysis** | Captures and analyzes network traffic at the packet level for troubleshooting and security analysis |
| **IDS / IPS (Suricata)** | Network-based intrusion detection and prevention using Suricata engine — inline or passive mode |
| **ICS Protocol Awareness** | Application-layer protocol analysis for Modbus TCP, DNP3 and EtherNet/IP — ICS/SCADA visibility |
| **SCADA/ICS Threat Detection** | Proofpoint ET Pro ruleset integration — SCADA/ICS attack, exploit and protocol anomaly detection signatures |
| **IPsec VPN** | IKEv1/IKEv2, route-based VTI, site-to-site and remote access — strongSwan engine |
| **OpenVPN** | SSL/TLS VPN — site-to-site, road warrior, easy client export with QR code |
| **WireGuard VPN** | Modern, high-performance VPN protocol with easy QR code-based client configuration |
| **Additional VPN Options** | OpenConnect, Stunnel, Tinc, ZeroTier (via plugins) — SDWAN/commercial VPN compatibility |
| **L2TP VPN** | Layer 2 Tunneling Protocol for legacy VPN client compatibility |
| **Multi-Factor Authentication** | TOTP-based 2FA with Google Authenticator and hardware token support for VPN and GUI login |
| **Web Application Firewall** | Protects web services against injection attacks — provides encryption for traffic to and from external world |
| **Web Proxy (Squid)** | Transparent and explicit caching proxy — HTTP/HTTPS content filtering and access control |
| **URL Filtering** | Controls access to websites based on URLs, domains and categories using blacklists |
| **SSL/TLS Inspection** | Decrypts and inspects SSL/TLS traffic using Squid proxy with SSL bumping capabilities |
| **DNS Filtering & Security** | DNS-based threat protection using DNS over TLS (DoT) — blocking malicious domains |
| **ICAP Support** | External content adaptation services integration for advanced filtering (via plugin) |

| | |
|---|---|
| **Antivirus Integration** | Web traffic antivirus scanning via ClamAV proxy integration (via plugin) |
| **Let's Encrypt (ACME)** | Automated SSL/TLS certificate issuance and renewal for secure web access |
| **Static Routing** | Manual route configuration — control traffic paths through the network |
| **Dynamic Routing (FRR)** | OSPF, BGP, IS-IS, LDP, PIM and RIP via FRRouting plugin — full dynamic routing suite |
| **Policy-Based Routing** | Routes traffic based on defined policies and criteria (source routing) |
| **VLAN / Segmentation** | IEEE 802.1Q VLAN — up to 4096 VLANs per interface, QinQ 802.1ad stacking supported |
| **VXLAN** | Virtual eXtensible Local Area Network — overlay network support |
| **Bridging** | Layer-2 bridge with (Rapid) Spanning Tree Protocol (RSTP/RTP) support |
| **GIF/GRE Tunneling** | Generic Routing Encapsulation and Generic Tunnel Interfaces for point-to-point links |
| **Virtual IP Configuration** | Add extra addresses to already defined interfaces using virtual IPs (CARP, IP Alias, Proxy ARP) |
| **IPv6 Dual-Stack** | Full IPv4 + IPv6 dual-stack addressing and routing support |
| **Link Aggregation (LAGG)** | Combines multiple network interfaces for increased bandwidth and redundancy |
| **Traffic Shaping / QoS** | Bandwidth management, priority queuing and scheduling for traffic prioritization |
| **Multi-WAN / Gateway Groups** | Balances outbound traffic across multiple WAN connections — failover and load balancing |
| **Gateway Quality Monitoring** | Real-time gateway monitoring with RTT, RTTd and packet loss metrics |
| **DHCP Server / Relay** | DHCPv4/v6 server and relay — ISC/Kea DHCP engine for IP address management |
| **DNS Server (Unbound / Dnsmasq)** | DNS resolution services — Unbound recursive resolver + Dnsmasq forwarder, DNS over TLS (DoT) |
| **NTP Server** | Built-in NTP server for network time synchronization across infrastructure |
| **Dynamic DNS (DynDNS)** | Keeps VPN endpoints reachable with dynamic IP addresses by updating DNS records automatically |
| **SNMP v1/v2c/v3** | Simple Network Management Protocol for monitoring and health management of network equipment |
| **CARP Failover** | Common Address Redundancy Protocol — active/passive or active/active failover |
| **pfsync State Synchronization** | Synchronizes firewall states between clustered firewalls for seamless failover |
| **High Availability Config Sync** | Synchronizes configuration between primary and secondary firewalls in HA setup |
| **Load Balancing** | Distributes incoming traffic across multiple servers — relay and Web Application Firewall options (via plugin) |
| **Local User & Group Management** | Manages users and groups locally for authentication and access control |
| **RADIUS / LDAP / Active Directory** | Centralized identity management — integrates with RADIUS servers and LDAP/AD directories |
| **Captive Portal** | Web-based user authentication portal before granting network access |
| **Certificate Management** | SSL/TLS certificate management — includes CA, trust manager and Certificate Revocation Lists (CRL) |
| **Single Sign-On (SSO)** | Limited SSO capabilities through integration with directory services |
| **Web-based Management GUI** | Modern web interface with role-based access control and customizable dashboard |
| **CLI / Console Access** | FreeBSD shell + OPNsense console — serial and SSH access for advanced management |
| **REST API** | Full REST API with ACL support for automation and integration with external tools |
| **Central Management (OPNCentral)** | Multi-site firewall management, firmware control and monitoring from a central point |
| **NetFlow / IPFIX** | Flexible NetFlow Analyzer with drill-down and export — flow-based traffic analysis |
| **Syslog** | Local and remote syslog — supports UDP, TCP and encrypted TLS transport over IPv4/IPv6 |
| **Live Traffic Monitoring** | Streaming live traffic graph with egress and ingress per-interface bandwidth and Top Talkers overview |
| **System Health Monitoring** | Detailed system performance graphs — CPU, memory, disk I/O and network throughput over time |
| **Monit Service Monitoring** | Monitors services and system resources, sends alerts based on defined conditions |
| **Firmware Management** | Automatic updates and easy firmware management via web interface or console |
| **Backup & Restore** | Configuration backup/restore — supports local, Google Drive, Git and NextCloud storage |
| **Configuration History** | Tracks configuration changes — view and revert to previous configurations |
| **Snapshots** | Space-efficient full system snapshot for quick rollback |
| **LLDP** | Link Layer Discovery Protocol for network topology discovery (via os-lldpd plugin) |
| **Plugin Architecture** | Modular and extensible plugin system — 70+ community and commercial plugins available |

### Performance & Usage Note

All supported software features are available on every Simgenet Firewall Security Platform model. However, the concurrent utilization and performance level of these features depends on the hardware model, processor capacity, and system resources. Scenarios requiring continuous full-bandwidth deep packet inspection (IPS / SSL inspection) are outside the product's target scope and are addressed through architectural design choices.

## 9. Summary

- Designed for enterprise internal network and edge security
- Server-class hardware built for 24/7 uninterrupted operation
- Scalable modular NIC ecosystem: 1G / 10G / 40G
- Three capacity tiers on a unified platform architecture
- OPNsense Business Edition — commercially licensed, LINCE-certified
- Complementary positioning — cost-effective security without excessive licensing
- Clean, defensible, and sustainable product architecture