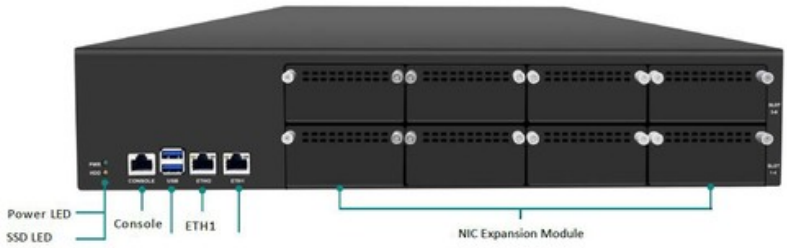
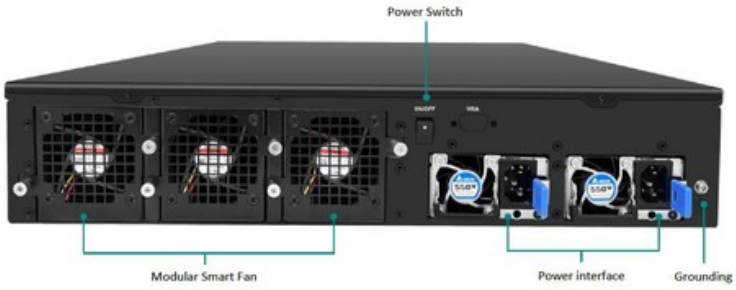
SimgeNet Mühendislik

SIMGENET FIREWALL SECURITY PLATFORM

Datacenter Series — SMG818V5-FW

Product Datasheet





1. Product Description

The Simgenet Firewall Security Platform — SMG818V5 Datacenter Series is a fully modular, high-capacity firewall security platform engineered for datacenter, service provider, and large enterprise networks requiring high bandwidth, high concurrency, and 24/7 uninterrupted operation.

2. Positioning & Target Use Cases

- Datacenter edge security (north–south traffic inspection)
- Datacenter internal network segmentation (east–west traffic)
- Service provider (ISP) edge and aggregation points
- Large enterprise backbone and core network security
- 100G aggregation and segmentation scenarios

Not targeted for: Small office, campus, or SMB environments. Not intended as a datacenter core firewall performing continuous full-bandwidth DPI.

3. Design Philosophy

The SMG818V5-FW Datacenter Series does not target continuous full-bandwidth deep packet inspection. Instead, it provides a **policy-based, selective security architecture** that integrates into layered and hybrid datacenter security designs.

This approach is consistent with modern datacenter security best practices, where traffic inspection is applied selectively based on security zones, policy requirements, and risk assessment.

4. Hardware Platform

Specification	Detail
Chassis	19-inch 2U Rackmount
Architecture	x86_64
Chipset	Intel® C741
CPU	Intel® Xeon® Gold 5418Y — 24 Core / 48 Thread, 2.0 GHz (Turbo ~3.8 GHz), 45 MB L3, TDP 185W
Memory (RAM)	Up to 64 GB DDR5 ECC
Storage	Up to 1 TB NVMe SSD
Expansion Slots	8 × PCIe x8 (modular NIC slots)
Operating System	OPNsense Business Edition (commercially licensed)

5. CPU Performance Scope & Limitations

The Intel Xeon Gold 5418Y processor is selected for 100G aggregation and east–west segmentation scenarios. Designed operational bandwidth:

- 100G aggregation / transit traffic
- Datacenter east–west network segmentation
- High number of VLANs / VRFs / security zones
- Policy-based stateful firewall
- Selective IPS (targeted, not full-bandwidth)
- Sustained 40–60% CPU utilization under mixed workload

Not targeted: Continuous 100G full-bandwidth IPS, 100G SSL/TLS inspection, full DPI architectures.

6. Modular Network Interfaces

The SMG818V5-FW Datacenter Series supports the following field-replaceable modular NIC cards:

Model	Controller	Interfaces	Bypass	PCIe Bus
SMG 3500PF-4SFP-M	Intel® I350-AM4	4 × GbE SFP	None	PCIe x8
SMG 3501BP-4T-M	Intel® I350-AM4	4 × GbE RJ45	2 (Gen3)	PCIe x8
SMG 1001PF-8SFP-M	Intel® I350-AM4	8 × GbE SFP	None	PCIe x8
SMG 3500BP-8T-M	Intel® I350-AM4	8 × GbE RJ45	4 (Gen3)	PCIe x8
SMG 5991PF-2SFP+-M	Intel® 82599ES	2 × 10G SFP+	None	PCIe x8
SMG 7100PF-4SFP+-M	Intel® XL710 BM1	4 × 10G SFP+	None	PCIe x8
SMG 7100PF-2QSFP+-M	Intel® XL710 BM2	2 × 40G QSFP+	None	PCIe x8
SMG 8100PF-2QSF28-M	Intel® E810	2 × 100G QSFP28	None	PCIe x8

Note: *40G and 100G NIC modules are designed for the datacenter edge and east–west segmentation scenarios targeted by the SMG818V5 platform.*

7. 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

Environmental & Hardware Specifications

- Operating Temperature: -20°C ~ +60°C
- EMC: EN 61000-4 Level 3

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.

8. Summary

- Datacenter-focused Firewall Security Platform
- Optimized for 100G aggregation and east–west segmentation
- Single CPU model — clean, sustainable architecture
- Fully modular NIC ecosystem (1G / 10G / 40G / 100G)
- OPNsense Business Edition — commercially licensed, LINCE-certified
- Complementary positioning — not competing with, but supplementing branded firewalls