SignWall

DATASHEET

SignWall Network Security Appliances

S · M · L · XL

SignWall combines a stateful firewall, threat protection, IPsec VPN, SD-WAN, dynamic routing, an advanced built-in captive portal and signed log retention compliant with Turkish Law No. 5651 in a single appliance. With domain single sign-on, internet access is managed by user and group name. All four hardware models run the same software.

01 Three capabilities that stand out

Advanced captive portal, built in

Guest and staff internet access is managed by the appliance's own portal: SMS verification, sponsor approval, authentication against LDAP/AD or an external database, a multilingual interface and hotel PMS integration. No separate portal server or cloud service required.

Signed log retention for Law No. 5651

Traffic and access logs are retained on a dedicated log disk (256 GB – 2 TB) inside the appliance, signed and timestamped by KAMU SM. Personal data is masked; logs are searchable through a local index and can be exported.

User-based internet control through SSO

The domain single sign-on agent binds the user signed in to Active Directory to their IP address. Security policies, quotas, web filtering and reports work with user and AD group names instead of IP addresses.

02 Highlights

- Advanced captive portal built in — SMS, sponsor approval, LDAP/AD, hotel PMS, multilingual portal
- Domain single sign-on (SSO) for internet control by user and AD group
- IPsec VPN (IKEv1/IKEv2, IPv4/IPv6) and SignClient, the managed endpoint client
- Signed log retention with KAMU SM timestamps, compliant with Law No. 5651, plus log search
- SignGuard threat protection — IPS/IDS, application control, web and DNS filtering, GeoIP, IP reputation
- SD-WAN, BGP/OSPF/RIP, multicast routing and up to 32 virtual firewalls

SignWall S

Small office / branch

4 × 2.5GbE



SignWall M

Mid-size branch

8 × 2.5GbE



SignWall L

Campus / regional hub

4 × GbE + 2 × 10G SFP+



SignWall XL

HQ / data-center edge

6 × 2.5GbE + 2 × 10GbE + 2 × 10G SFP+



03 Model summary

	S	M	L	XL
Target deployment	Small office / branch	Mid-size branch	Campus / regional hub	Headquarters / data-center edge
Network interfaces	4 × 2.5GbE	8 × 2.5GbE	4 × GbE + 2 × 10G SFP+	6 × 2.5GbE + 2 × 10GbE + 2 × 10G SFP+
Firewall throughput	4.5 Gbps	7.5 Gbps	18 Gbps	40 Gbps
IPS throughput	0.9 Gbps	1.4 Gbps	3.5 Gbps	7.5 Gbps
Threat protection throughput	500 Mbps	800 Mbps	1.9 Gbps	4.1 Gbps
Concurrent sessions	3 million	6 million	12.5 million	25 million
Memory / log disk	8 GB / 256 GB	16 GB / 512 GB	32 GB / 1 TB	64 GB / 2 TB

04 Hardware specifications

	S	M	L	XL
Processor	Intel Core i3-5005U	Intel Core i3-10110U	Intel Core i3-N305	Intel Core Ultra 5 125H
Cores / threads	2 / 4	2 / 4	8 / 8	14 (4P + 8E + 2LP-E) / 18
Memory	8 GB DDR3	16 GB DDR4	32 GB	64 GB
System disk	64 GB 2.5" SATA	64 GB 2.5" SATA	64 GB	64 GB
Application / log disk	256 GB mSATA	512 GB mSATA	1 TB	2 TB
2.5GbE RJ45	4 (Intel I225-V / I226-V)	8 (Intel I225-V / I226-V)	—	6
1GbE RJ45	—	—	4	—
10GbE RJ45	—	—	—	2
10G SFP+	—	—	2	2
USB	2 × USB 3.0, 2 × USB 2.0	4 × USB 3.0	2 × USB 3.0, 2 × USB 2.0	3 × USB 3.0, 4 × USB 2.0, 1 × USB-C 3.0
Console	1 × RS-232 (DB9)	1 × RS-232 (RJ-45)	1 × RS-232 (RJ-45)	1 × RS-232 (RJ-45)
Power supply	Single	Single	Single	Single (dual PSU optional)
Form factor	Desktop, fanless	Desktop, fanless	1U rack mount	1U rack mount
Processor TDP	15 W	15 W	15 W	28 W

Network ports are named port1 … portN in the web interface and the CLI; numbering is fixed at installation. Logs and application data are kept on a disk separate from the system disk.

05 System performance

Throughput, session and packet figures for the four models. The enterprise mix is an HTTP/HTTPS-weighted blended traffic profile.

	S	M	L	XL
Firewall throughput (1518 / 512 / 64 byte UDP)	4.5 / 1.5 / 0.2 Gbps	7.5 / 2.5 / 0.3 Gbps	18 / 6 / 0.8 Gbps	40 / 13 / 1.7 Gbps
Packet rate (64 byte)	0.39 Mpps	0.63 Mpps	1.5 Mpps	3.3 Mpps
New sessions per second (TCP)	35,000	60,000	150,000	320,000
Concurrent sessions (TCP)	3 million	6 million	12.5 million	25 million
IPS throughput (enterprise mix)	0.9 Gbps	1.4 Gbps	3.5 Gbps	7.5 Gbps
NGFW throughput (IPS + application control)	650 Mbps	1 Gbps	2.5 Gbps	5.3 Gbps
Application control throughput (HTTP 64K)	1.2 Gbps	1.9 Gbps	4.8 Gbps	10 Gbps
Threat protection throughput (IPS + app control + web filtering)	500 Mbps	800 Mbps	1.9 Gbps	4.1 Gbps
IPsec VPN throughput (512 byte, AES-GCM)	550 Mbps	900 Mbps	2.1 Gbps	4.7 Gbps
New flows per second (IPS enabled)	2,300	3,700	9,000	19,600

All figures are maximum values; actual results vary with configuration, traffic mix and the security features in use.

06 System capacities (all models)

Virtual firewalls	Up to 32 (in addition to the main firewall)
High availability	Active-passive cluster; VRRP
IPsec tunnel types	Site-to-site, remote access (dial-up)
IKE versions	IKEv1, IKEv2 (including MOBIKE)
IP versions	IPv4 / IPv6 dual stack (firewall, NAT, VPN, routing)
Administrator two-factor authentication	Yes (TOTP)
VPN two-factor authentication	TOTP and SMS
Captive portal authentication	SMS, sponsor approval, LDAP/AD, RADIUS, external database, hotel PMS
Log retention	Dedicated on-appliance log disk: 256 GB / 512 GB / 1 TB / 2 TB
User sources	Local, LDAP/AD (nested groups), RADIUS, domain single sign-on agent
Syslog forwarding formats	CEF, RFC 5424; UDP / TCP / TLS
Built-in alert rules	22
Interface languages	Turkish, English

07 Features

Firewall

- Stateful, zone-based policies; per-rule traffic counters and a policy test tool
- Identity-based rules: local users, LDAP/AD groups, RADIUS, domain single sign-on
- SNAT, DNAT/VIP (1:1, secondary IP), DNAT bound to a security policy
- Local-in policies for traffic to the appliance, trusted management sources
- Session timeout management (global and per port), session helpers (ALG)
- Virtual firewalls (up to 32) and inter-virtual-firewall links

User identity, SSO and internet control

- Domain single sign-on agent: the user signed in to Active Directory is matched to their IP address
- User sources: local users, LDAP/AD (nested groups), RADIUS, external database
- Policies, quotas, web filtering and application control applied per user and per AD group
- Visibility by user name instead of IP in logs, reports and live monitoring views
- Schedules for access by hour and day; per-user concurrent session and quota limits
- Two-factor authentication for portal and VPN (TOTP, SMS), attempt limits and user quarantine

Threat protection · SignGuard

- IPS/IDS with signature-based detection and blocking
- Application control by application and category
- Web filtering via cloud rating service, blocking of unrated sites, custom block pages
- DNS filtering and enforced safe search
- Geolocation (GeoIP), IP reputation and internet services database
- Anti-spam, file reputation and national threat list (USOM) integration
- DoS/DDoS protection: threshold policies, SYN proxy, source quarantine, RTBH and Flowspec

VPN

- IPsec site-to-site and remote access; IKEv1/IKEv2, IPv4/IPv6, NAT traversal, MOBIKE
- Pre-shared key, certificates (IKEv2), XAUTH, RADIUS over IKEv2 (MSCHAPv2)
- Ordered user sources per tunnel and concurrent connection limits
- Two-factor authentication (TOTP, SMS), attempt limits and user quarantine

07 Features · 2

SignClient endpoint client · Windows, macOS

- Central enrollment and client policy; device groups
- Posture checks: disk encryption, OS firewall, antivirus/EDR, minimum client version
- Always-on tunnel and fail-close when the tunnel is down
- Tamper protection (uninstall password, signed settings) and tamper alerts
- Remote actions: disconnect, quarantine, isolation, diagnostics bundle, process termination
- Hardware and software inventory, endpoint DNS/web filtering and application control

Networking and routing

- Static routing, policy-based routing (PBR)
- BGP, OSPF, RIP; BFD, graceful restart, route reflector
- Multicast: IGMP/MLD, IGMP proxy, PIM-SM/DM, SSM, BSR (IPv4/IPv6)
- SD-WAN: link profiles, health monitoring, load-balancing algorithms
- VLAN, VXLAN, LACP, LLDP, loopback, GRE
- DHCP server, DNS server, dynamic DNS client, traffic shaping and quotas

Guest access and built-in captive portal

- The captive portal / hotspot runs inside the appliance; no separate portal server or cloud service
- Authentication methods: SMS verification, sponsor approval, LDAP/AD, RADIUS, external database
- Hotel PMS integration; sign-in by room and surname, access limited to the length of stay
- Multilingual portal, a sign-in page customizable to your brand, and terms-of-use text
- Guest identity records, session management, session duration and quota limits
- Device identification (DHCP, MAC vendor, mDNS, SSDP, user agent)

Logging, Law No. 5651 compliance and monitoring

- Log signing compliant with Turkish Law No. 5651, with KAMU SM timestamping
- Logs are kept on a log disk separate from the system disk: 256 GB, 512 GB, 1 TB or 2 TB by model
- Local log index and log search; query results can be exported
- Privacy-focused data handling: personal data masked in logs
- Syslog forwarding (24 log types; CEF, RFC 5424; UDP / TCP / TLS), NetFlow export
- SNMP (v2c, v3) with private MIB; SIEM-style alert rules (22 built-in), email and SMS notifications
- Customizable dashboard, live monitoring views, per-module diagnostics commands
- SignMesh: secure pairing and central visibility with SignLogger products

Management

- Web interface (Turkish/English) and CLI with a hierarchical configuration tree
- Candidate configuration, commit and rollback to earlier revisions
- Role-based access control, administrator two-factor authentication, remote administrator identity
- Certificate management: built-in CA, CSR, import as PEM/DER/PKCS#7/PKCS#12
- Signed A/B firmware updates with automatic rollback on failure, update from USB
- Configuration backup, full backup to a Windows share, factory reset

08 Licensing and subscriptions

SCOPE	INCLUDES	LICENSE
Base	Firewall, NAT, static routing, SD-WAN, site-to-site IPsec VPN, virtual firewalls	No license required
Product license	Remote-access IPsec VPN, SignClient management and security checks, captive portal, 5651 log signing, dynamic routing, VRRP, BFD, GRE, VXLAN, DDNS, DoS protection	Product license
SignGuard threat protection	IPS/IDS, application control, web filtering, DNS filtering, GeoIP / IP reputation, anti-spam, file reputation	Product license + signature and rating updates
Updates	Firmware and signature packages	Valid license

09 Ordering information

PRODUCT	DESCRIPTION
SignWall S	4 × 2.5GbE, 8 GB RAM, 64 GB system + 256 GB log disk, fanless desktop chassis
SignWall M	8 × 2.5GbE, 16 GB RAM, 64 GB system + 512 GB log disk, fanless desktop chassis
SignWall L	4 × GbE + 2 × 10G SFP+, 32 GB RAM, 64 GB system + 1 TB log disk, 1U rack
SignWall XL	6 × 2.5GbE + 2 × 10GbE + 2 × 10G SFP+, 64 GB RAM, 64 GB system + 2 TB log disk, 1U rack
Dual power supply (XL)	Optional second power supply for XL
License / subscription	1, 3 and 5-year options

Contact our sales team for order codes and current pricing.

Sysnet

ADDRESS

Esas Kurtköy Aeropark Kat: 5
Yenişehir Mah. Osmanlı Bulvarı No: 11/A 28
34912 Pendik / İstanbul / Türkiye

PHONE

+90 216 706 36 40

E-MAIL

bilgi@signwall.com.tr
signwall.com.tr
sysnet.com.tr