Simgenet Firewall Security Platform

Simgenet Modular Edge & Internal Network Firewall Platform

Ürün Tanımı

Simgenet Firewall Security Platform, oteller, fabrikalar, kampüsler ve büyük kurumsal iç network yapıları için geliştirilmiş, 7/24 kesintisiz çalışmaya uygun, sunucu sınıfı donanım mimarisi üzerine inşa edilmiş, yüksek port yoğunluğu ve modüler ağ arayüzü sunan bir Firewall Security Platformudur.

Platform, klasik marka firewall çözümlerinin doğrudan alternatifi olarak değil; iç network güvenliği, kurumsal edge ve aggregation senaryoları için tamamlayıcı ve maliyet-etkin bir güvenlik katmanı olarak konumlandırılmıştır.

Konumlandırma ve Hedef Kullanım

- Büyük ölçekli otel ağları
- Fabrika ve endüstriyel tesisler
- Kampüs ve yerleşke ağları
- Kurumsal iç network segmentasyonu (VLAN / zone bazlı)
- Kurumsal edge ve aggregation noktaları
- Marka firewall lisans maliyetlerinin teknik ihtiyacın önüne geçtiği projeler

Küçük ofis / SOHO ortamları hedeflenmez.

Datacenter core firewall rolü hedeflenmez.

Tasarım Felsefesi

- “Her şeyi tek başına yapan firewall” yaklaşımını benimsemez
- Doğru mimarinin bir parçası olarak konumlandırılır
- Yüksek bant genişliği ve stabiliteyi, gereksiz lisans maliyetleri olmadan sunar

Bu yaklaşım, modern ağlarda yaygın olarak kullanılan hibrit güvenlik ve katmanlı mimarilerle tam uyumludur.

Ürün Ailesi

Simgenet Firewall Security Platform, aynı donanım platformu üzerinde farklı kapasite seviyeleriyle sunulur:

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

Tüm modeller aynı şasi, aynı CPU mimarisi ve aynı modüler ağ kartı ekosistemi üzerine kuruludur. Farklar; RAM, disk kapasitesi ve 40G yetkilendirmesi ile belirlenir.

Donanım Platformu

- Şasi: 1U Rackmount
- Mimari: x86, DDR4
- Chipset: Intel® C236
- İşletim Sistemi: OPNsense Community Edition
  Simgenet Firewall Security Platform, OPNsense Community Edition ile sunulur.
  Kullanıcılar, ihtiyaç duymaları halinde OPNsense ticari abonelik modeline bağımsız olarak geçiş yapabilir.

İşlemci (CPU)

- Intel® Xeon® E3-1230 v5
- 4 Core / 8 Thread
- 3.4 – 3.8 GHz
- 80 W TDP
- ECC bellek desteği

Bu seçim, platformun uzun süreli yüksek yük altında stabil çalışmasını hedefler.

Bellek (RAM)

- SMG104-EDGE: 16 GB DDR4 ECC
- SMG104-EDGE PLUS: 32 GB DDR4 ECC
- SMG104-EDGE MAX: 64 GB DDR4 ECC

Depolama

- 2 × SATA 3.0 (2.5” / 3.5”)
- 1 × CF Interface
- Disk konfigürasyonu: Tek disk veya çift disk (mirror – log güvenliği)

Uzun süreli log saklama için harici syslog / SIEM entegrasyonu önerilir.

Güç ve Fiziksel Özellikler

- Güç Kaynağı: 1 × 220 VAC, 250 W Single PSU
- Boyut: 430 mm (W) × 550 mm (D) × 44.5 mm (H)
- Ağırlık: Net 20 kg
- Çalışma Sıcaklığı: -20℃ ~ +60℃
- EMC: EN 61000-4 Level 3
- Depolama Sıcaklığı: -20℃ ~ 75℃
- Depolama Nem: %5 ~ %95 (yoğuşmasız)

Ön Panel Arayüzleri

- 2 × USB 2.0

- 2 × RJ45 Gigabit Ethernet
- 1 × COM Port
- Power LED / HDD LED

Genişleme Yuvaları

4 × PCIe x8

Modüler Network Arayüzleri (Seçimlik)

Simgenet Firewall Security Platform, aşağıdaki seçilebilir ağ modülleri ile yapılandırılabilir. Modül seçimi, müşteri ihtiyacına göre yapılır.

Module Type	Controller	Link Speed	Media Type	IO Ports
SMG 7103PF-2QSFP+	Intel XL710	40G	Fiber	2 x QSFP+
SMG 7103PF-4SFP+	Intel XL710	10G	Fiber	4 x SFP+
SMG 7103PF-2SFP+	Intel XL710	10G	Fiber	2 x SFP+
SMG 5993PF-2SFP+	Intel 82599	10G	Fiber	2 x SFP+
SMG 3503PF-4SFP	Intel I350	1G	Fiber	4 x SFP
SMG 3503PT-4T	Intel I350	1G	Copper	4 x RJ45
SMG 3503PT-8T	Intel I350	1G	Copper	8 x RJ45
SMG 3503PT-4T4S	Intel I350	1G	Copper + Fiber	4 x RJ45 + 4 x SFP
SMG 3503BP-4T	Intel I350	1G	Copper (Bypass)	4 x RJ45
SMG 3503BP-8T	Intel I350	1G	Copper (Bypass)	8 x RJ45

Not: 40G QSFP+ modülleri yalnızca SMG104-EDGE PLUS ve SMG104-EDGE MAX modellerinde desteklenir.

Özet

- Kurumsal iç network ve edge güvenliği için tasarlanmıştır
- 7/24 çalışmaya uygun sunucu sınıfı donanım
- 1G / 10G / 40G ölçeklenebilir modüler ağ yapısı
- Markalarla rekabet etmeyen, tamamlayıcı konumlandırma
- Kurumsal, sade ve savunulabilir ürün mimarisi

Desteklenen Yazılım Özellikleri (OPNsense)

- Simgenet Firewall Security Platform, **OPNsense yazılımının sunduğu tüm temel ve gelişmiş ağ güvenliği protokollerini destekler**.

Desteklenen yazılım özellikleri **donanım modelinden bağımsızdır**; donanım farkı, bu özelliklerin **eşzamanlı kullanım kapasitesini ve performans seviyesini** belirler.

Başlıca desteklenen protokoller ve özellikler:

- **Stateful Firewall** — IPv4/IPv6 durum tabanlı paket denetleme, bölge tabanlı güvenlik
- **Firewall Aliases** — IP, ağ, port, MAC, GeoIP ve BGP ASN alias tabanlı kural yönetimi
- **Time-based Firewall Rules** — zamanlama tabanlı güvenlik duvarı kuralları
- **NAT** — Source NAT, Destination NAT, Port NAT, 1:1 NAT, NPt (IPv6)
- **ACL / Packet Filter Rules** — kural bazlı paket filtreleme, loglama ve sayaçlar
- **Anti-DDoS** — SYN cookies, hız sınırlama, bağlantı limitleri
- **Bogon Network Blocking** — bogon IP adres alanlarından gelen trafiği engelleme
- **GeoIP Filtering** — MaxMind GeoLite2 ile ülke bazlı trafik engelleme
- **Granular State Table Control** — durum tablosu boyutu, bağlantı/saniye, zaman aşımı kontrolü
- **Traffic Normalization** — protokol tutarsızlıklarına karşı koruma
- **Packet Capture & Analysis** — paket seviyesinde ağ trafiği yakalama ve analiz
- **IDS / IPS (Suricata)** — ağ tabanlı saldırı tespit ve önleme, inline veya pasif mod
- **ICS Protocol Awareness** — Modbus TCP, DNP3, EtherNet/IP uygulama katmanı analizi
- **SCADA/ICS Threat Detection** — Proofpoint ET Pro kural seti ile endüstriyel saldırı tespiti
- **IPsec VPN** — IKEv1/IKEv2, rota tabanlı VTI, siteler arası ve uzaktan erişim (strongSwan)
- **OpenVPN** — SSL/TLS VPN, siteler arası, gezici kullanıcı, QR kodlu istemci dışa aktarma
- **WireGuard VPN** — modern, yüksek performanslı VPN protokolü, QR kodu ile yapılandırma
- **Ek VPN Seçenekleri** — OpenConnect, Stunnel, Tinc, ZeroTier (plugin ile)
- **L2TP VPN** — eski VPN istemci uyumluluğu için Katman 2 Tünelleme Protokolü
- **Multi-Factor Authentication** — VPN ve GUI için TOTP tabanlı 2FA, Google Authenticator, hardware token
- **Web Application Firewall** — web servislerini injection saldırılarına karşı koruma
- **Web Proxy (Squid)** — transparent ve explicit önbellekleme proxy, HTTP/HTTPS filtreleme
- **URL Filtering** — URL, domain ve kategorilere göre erişim kontrolü (plugin ile)
- **SSL/TLS Inspection** — Squid proxy ile SSL bumping, şifreli trafik denetleme
- **DNS Filtering & Security** — DNS over TLS (DoT) ile DNS tabanlı tehdit koruması
- **ICAP Support** — harici içerik uyarlama servisleri entegrasyonu (plugin ile)
- **Antivirus Integration** — ClamAV proxy entegrasyonu ile web trafiği antivirüs taraması (plugin ile)
- **Let's Encrypt (ACME)** — otomatik SSL/TLS sertifika düzenleme ve yenileme
- **Static Routing** — manuel rota yapılandırması
- **Dynamic Routing (FRR)** — OSPF, BGP, IS-IS, LDP, PIM, RIP (FRRouting plugin ile)
- **Policy-Based Routing** — politika ve kriterlere göre trafik yönlendirme (kaynak yönlendirme)
- **VLAN / Segmentation** — IEEE 802.1Q (arayüz başına 4096 VLAN), QinQ 802.1ad
- **VXLAN** — Virtual eXtensible Local Area Network, overlay ağ desteği
- **Bridging** — Katman 2 köprüleme, (Rapid) Spanning Tree Protocol (RSTP/RTP)
- **GIF/GRE Tunneling** — noktadan noktaya bağlantılar için GRE ve GIF tünel arayüzleri
- **Virtual IP Configuration** — CARP, IP Alias, Proxy ARP ile sanal IP tanımlama
- **IPv6 Dual-Stack** — tam IPv4 + IPv6 çift yığın adresleme ve yönlendirme
- **Link Aggregation (LAGG)** — bant genişliği artırma ve yedeklilik için arayüz birleştirme
- **Traffic Shaping / QoS** — bant genişliği yönetimi, öncelik kuyruğu, trafik önceliklendirme
- **Multi-WAN / Gateway Groups** — birden fazla WAN bağlantısı üzerinde yük devretme ve dengeleme
- **Gateway Quality Monitoring** — RTT, RTTd ve paket kaybı metrikleri ile ağ geçidi izleme
- **DHCP Server / Relay** — DHCPv4/v6 sunucu ve aktarıcı (ISC/Kea DHCP motoru)
- **DNS Server (Unbound / Dnsmasq)** — recursive resolver + forwarder, DNS over TLS (DoT)
- **NTP Server** — altyapı genelinde ağ zaman senkronizasyonu (yerleşik ntpd)

- **Dynamic DNS (DynDNS)** — dinamik IP adreslerinde DNS kayıtlarını otomatik güncelleme
- **SNMP v1/v2c/v3** — ağ ekipmanı izleme ve durum yönetimi protokolü
- **CARP Failover** — aktif/pasif veya aktif/aktif yük devretme
- **pfsync State Synchronization** — kümelenmiş güvenlik duvarları arasında durum senkronizasyonu
- **High Availability Config Sync** — birincil ve ikincil cihazlar arasında yapılandırma senkronizasyonu
- **Load Balancing** — gelen trafiği birden fazla sunucuya dağıtma (plugin ile)
- **Local User & Group Management** — yerel kullanıcı ve grup yönetimi
- **RADIUS / LDAP / Active Directory** — merkezi kimlik yönetimi entegrasyonu
- **Captive Portal** — ağ erişimi öncesi web tabanlı kullanıcı kimlik doğrulama
- **Certificate Management** — SSL/TLS sertifika yönetimi, CA ve CRL
- **Single Sign-On (SSO)** — dizin servisleri ile SSO desteği
- **Web-based Management GUI** — rol tabanlı erişim kontrolü ve özelleştirilebilir pano
- **CLI / Console Access** — FreeBSD shell + OPNsense konsolu, seri ve SSH erişimi
- **REST API** — ACL destekli tam REST API, otomasyon ve harici araç entegrasyonu
- **Central Management (OPNCentral)** — merkezi çoklu site yönetimi, firmware kontrolü
- **NetFlow / IPFIX** — akış tabanlı trafik analizi, detaylı raporlama
- **Syslog** — IPv4/IPv6 üzerinden UDP, TCP ve şifreli TLS aktarım destekli yerel/uzak syslog
- **Live Traffic Monitoring** — arayüz başına canlı trafik grafiği ve Top Talkers görünümü
- **System Health Monitoring** — CPU, bellek, disk I/O, ağ çıktısı performans grafikleri
- **Monit Service Monitoring** — hizmet ve kaynak izleme, koşullu uyarı gönderimi
- **Firmware Management** — web arayüzü veya konsol üzerinden otomatik güncelleme
- **Backup & Restore** — yerel, Google Drive, Git ve NextCloud destekli yedekleme/geri yükleme
- **Configuration History** — yapılandırma değişiklik takibi, önceki versiyonlara geri dönme
- **Snapshots** — hızlı geri alma için disk tasarruflu tam sistem anlık görüntüsü
- **LLDP** — ağ topolojisi keşfi (os-lldpd plugin ile)
- **Plugin Architecture** — 70+ topluluk ve ticari plugin ile modüler genişletilebilirlik

Performans ve Kullanım Notu

- Desteklenen yazılım özellikleri tüm Simgenet Firewall Security Platform modellerinde mevcuttur. Ancak bu özelliklerin **aynı anda ve hangi performans seviyesinde kullanılabileceği**, donanım modeli, işlemci kapasitesi ve sistem kaynaklarına bağlıdır.

Tam bant genişliğinde sürekli derin paket inceleme (IPS / SSL inspection) gerektiren senaryolar, ürünün hedef kullanım kapsamı dışında değerlendirilir ve mimari tercihlere bağlı olarak ele alınır.