Powered By
ATOMNIA
Connection Protection Detection

SASE SNIPER – Brief Technical Spec

SASE SNIPER is OMNIA's cloud-based, deviceless SD-WAN and ZTNA remote-access solution. It replaces legacy VPN models with multi-link, always-on, zero-trust connectivity for remote, hybrid and mobile workers, supported by integrated Check Point cloud security.

Area	Technical specification
Platform role	Cloud-based OMNIA remote-access component, designed to provide secure access to corporate applications, data, cloud and SaaS resources for remote, hybrid and mobile teams.
Deviceless deployment	Delivered through a lightweight downloadable client on a user's Windows or MAC OS laptop; no physical CPE is required for remote staff. Onboarding is initiated through an email invitation with an application download link and instructions.
Zero Trust access	Verifies every user, device and session before granting access. Full ZTNA provides application-level access control rather than network-wide VPN access. Multi-factor authentication is supported on the SD-WAN side.
Cloud security	Integrated Check Point CloudGuard firewall and cloud security engine. Provides firewall, DLP, IPS, application control, IPsec VPN capabilities, antivirus, anti-bot, anti-spam and URL filtering.
Encrypted-traffic inspection	SSL/TLS traffic inspection with traffic forwarding and SNI support enables deep inspection of encrypted traffic. Optional SandBlast adds Threat Extraction and Threat Emulation for zero-day attacks.
Security efficacy	Advertised vendor test figures state a 100% block rate, 100% malware prevention, 100% exploit resistance and 0% false positives.

Area	Technical specification
Encryption	ChaCha-based encryption support within the SD-WAN fabric.
Multi-link connectivity	Uses multiple connectivity types simultaneously, including Wi-Fi, 4G and broadband, for greater resilience. The SD-WAN head-end can also use multiple connectivity types, including LTE.
Path selection and failover	Best-path selection is applied per session. Sub-second failover automatically switches to backup paths during outages, while forward error correction mitigates packet loss, jitter and delay on unstable home or public networks.
Connection policy	Individual application connections can be defined as Enabled, Backup or Disabled within SASE SNIPER policy.
Management and visibility	A single pane of glass provides unified security management, policy enforcement and reporting across public, private and hybrid clouds and on-premises networks. It also monitors SD-WAN head-end performance and user activity.
Logging and compliance	Traffic logging provides visibility into user-access patterns and internet usage for compliance and troubleshooting. Detailed logs and security policies across users and locations support audits.
Scalability	Scales as user numbers and locations change without additional hardware.

Remote-Access Model

SASE SNIPER combines networking and security in one cloud service. It automatically routes traffic over the best available path, delivering secure, robust connectivity back to corporate environments or directly to the internet and cloud as appropriate.

The solution is designed to reduce the hardware, maintenance and IT overhead associated with VPN concentrators while providing consistent security and performance regardless of user location.

VPN Limitations Addressed

- Replaces all-or-nothing network access with application-level ZTNA controls.
- Avoids reliance on a single connection and fixed endpoint by using multiple connectivity options and automatic failover.
- Reduces the latency, bottlenecks and poor user experience caused by backhauling cloud-application traffic through VPN concentrators.
- Removes the need for physical remote-access CPE and supports users working from any location and network.