SAFEcore 1000

Engineered for flexibility. Built for the future.

In a world where security and performance can no longer be trade-offs, Sitehop's SAFEcore 1000 delivers both–without compromise. Designed for organisations that demand ultra-low latency encryption at massive scale, this high-performance platform redefines secure aggregation for data centres, telecoms, and critical national infrastructure. Powered by Sitehop's proprietary FPGA architecture, SAFEcore enables real-time, crypto-agile security that keeps pace with today's demands–and tomorrow's threats.

Platform Overview

The Sitehop SAFEcore 1000 platform, combined with high-performance SAFEblade 1000 modules, delivers unprecedented power density and ultra-low latency encryption for next-generation secure network aggregation. Designed for the most demanding environments–ranging from financial institutions to telecommunications backbones, this modular, crypto-agile system ensures maximum throughput with robust, future-proof cryptographic protection.

Each 1U SAFEframe chassis houses two independent SAFEblades, with hot-swappable power supplies, field-replaceable fans, and a dedicated management interface that integrates seamlessly with Sitehop SAFEnms, Sitehop's centralised management and auditing solution. This enables streamlined deployment, monitoring, and policy enforcement across distributed environments.

Every SAFEblade includes a single WAN and LAN interface supporting one of multiple high-speed encryption licenses. Customers can deploy SAFEencrypt licenses to enable 10G or 100G IPsec aggregation, delivering the world's lowest encryption latency. For environments requiring quantum-resilient security, SAFEpqc licenses leverage the ML-KEM post-quantum cryptographic algorithm to secure IPsec key exchange without compromising on performance.

Ideal for data centre aggregation, multi-domain secure communications, and cloud-edge connectivity, the SAFEcore platform is the foundation for organisations demanding both performance and long-term cryptographic agility.

PQC transition

Sitehop offers a seamless solution for upgrading legacy cryptography to the latest Post-Quantum Cryptography (PQC) standards.

Cryptographic agility

Cryptographic standards are advancing faster than ever. Unlike ASICs, FPGAs provide unmatched flexibility, allowing your system to adapt to new threats and stay ahead.

10x less power

Reduce your carbon footprint with energy-efficient hardware that uses up to 10 times less power than software-only solutions.

Sub-microsecond latency

Secure your data with latency measured in microseconds, highly deterministic encryption delivering unmatched speed and reliability for mission-critical operations.

Unyielding Protection

Hardware-Enforced Security delivers trusted, resilient systems that are immune to the vulnerabilities and exploits commonly used to compromise software-based VPNs.

sitehop.com

sitehop

info@sitehop.com

SAFEcore 1000

Simple to Deploy. Effortless to Manage.

SAFEcore is designed with ease-of-use at its core–enabling seamless integration into complex, mission-critical environments:

Centralised management

SAFEcore integrates fully with Sitehop SAFEnms, a secure, centralised platform that simplifies deployment, monitoring, auditing, and policy updates across distributed networks.

Zero-touch provisioning

SAFEblades are managed centrally via SAFEnms, making even large-scale deployments fast and efficient.

Modular and serviceable

Field-replaceable fans, hot-swappable power supplies, and easily configurable SAFEblades reduce operational overhead and downtime.

Flexible network topologies

Works in point-to-point, mesh, or hub-and-spoke deployments across multi-domain environments, supporting both aggregation and edge security.

From data centre aggregation to rugged operational tech environments, SAFEcore enables enterprise-grade security without complexity.

sitehop.com

FPGA-based security and crypto agility for next-generation networks.

High-performance security with FPGA technology

Field Programmable Gate Arrays (FPGAs) provide a dynamic and adaptable approach to network security, offering significant advantages over fixed-function hardware solutions like Application-Specific Integrated Circuits (ASICs). Unlike ASICs, which require extensive development cycles and cannot be modified post-production, FPGAs are fully reprogrammable. This capability enables rapid deployment of updated cryptographic protocols, ensuring that security infrastructure remains resilient against emerging threats without requiring costly hardware replacements.

The importance of crypto agility in the age of quantum computing

The advent of quantum computing poses a significant risk to current cryptographic standards, as quantum algorithms have the potential to break widely used encryption methods. As Post-Quantum Cryptography (PQC) standards continue to evolve to counteract these risks, organizations must remain adaptable to avoid vulnerabilities. Crypto agility–the ability to seamlessly adopt and transition to new cryptographic algorithms–is critical for ensuring long-term data protection.

FPGAs inherently support crypto agility by allowing real-time reconfiguration, enabling security teams to implement PQC algorithms and other emerging encryption methods without service interruptions. This flexibility not only safeguards sensitive information but also translates into cost savings by eliminating the need for frequent hardware replacements as cryptographic standards evolve.

Sitehop's FPGA-based security approach

Sitehop leverages FPGA technology to deliver robust, high-performance encryption solutions with minimal impact on network performance. By integrating FPGAs into security appliances, Sitehop ensures:

Future-proof network security

With the increasing risks posed by quantum computing and the rapid evolution of PQC standards, organizations must adopt security solutions that can evolve alongside these challenges. Sitehop's FPGA-based architecture provides an agile, scalable, and energy-efficient foundation for securing mission-critical networks, ensuring that businesses remain protected in a rapidly changing digital landscape while reducing long-term security costs.

sitehop

info@sitehop.com

SAFEcore 1000

SAFEblade Encryption Licenses

The SAFEblade platform supports a range of flexible, high-performance encryption licenses to meet diverse operational and security requirements. Each license is tied to a specific cryptographic capability and throughput profile, enabling customers to tailor their deployment to both current and future needs.

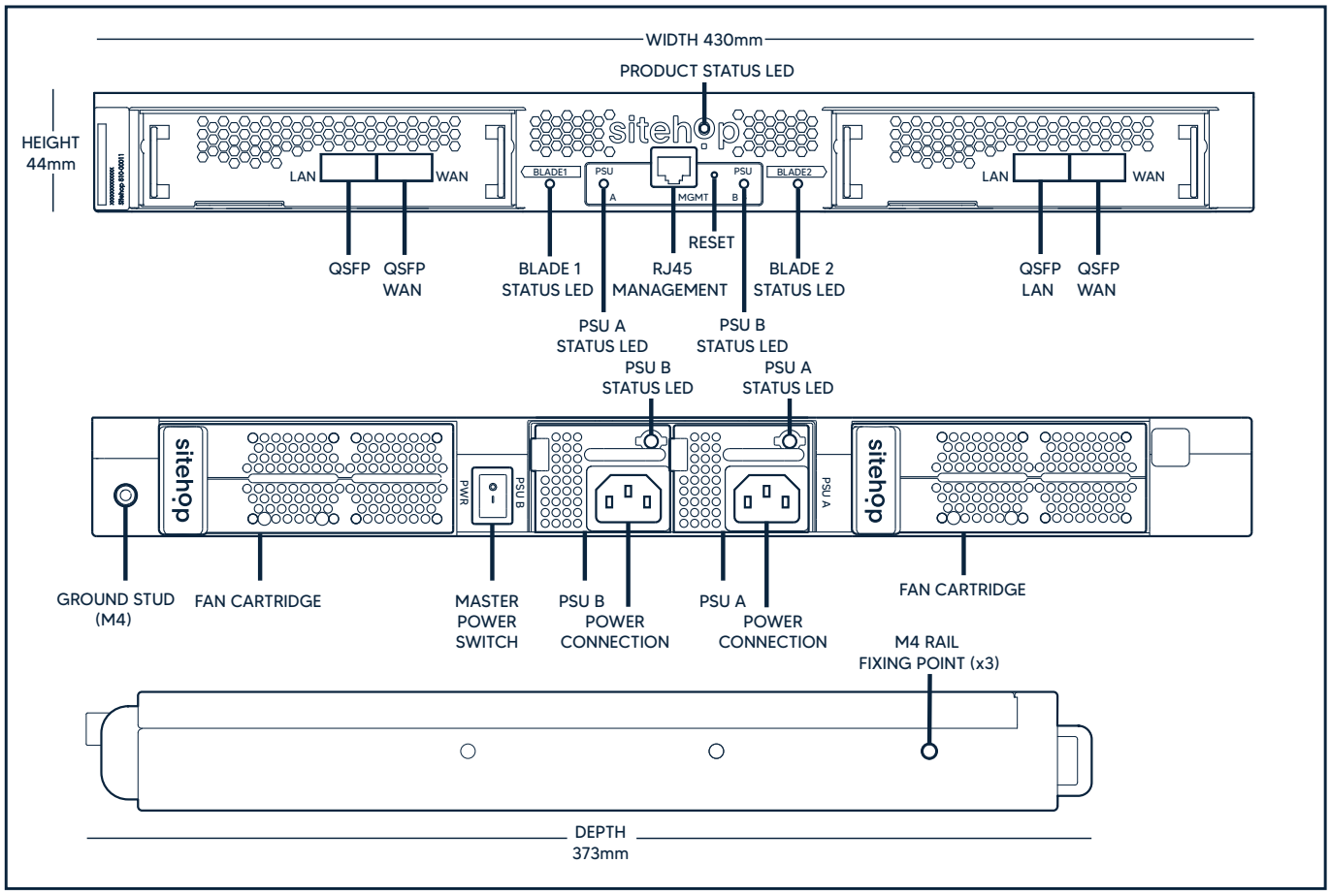
	SAFEencrypt10	SAFEencrypt100	SAFEpqc10	SAFEpqc100
Support SAFEblade 1000	•	•	•	•
IPsec aggregation	•	•	•	•
10G throughput	•		•	
100G throughput		•		•
PQC (ML-KEM) Key Exchange			•	•
RFC9370 Hybrid key exchange			•	•

The SAFEblade architecture ensures that each blade can independently host and enforce its own license, allowing service providers and enterprise customers to deploy mixed workloads within a single SAFEcore chassis.

sitehop

info@sitehop.com

SAFEcore 1000



Interfaces and modules

Device	Interface	Type	Value
SAFEcore 1000	Management interface	type	RJ45
		data rate	1Gbps/100Mbs/10Mbps
SAFEblade1000 unit 1	WAN interface	type	QSFP28
		data rate	100 Gbit/s
	LAN interface	type	QSFP28
		data rate	100 Gbit/s
SAFEblade1000 unit 2	WAN interface	type	QSFP28
		data rate	100 Gbit/s
	LAN interface	type	QSFP28
		data rate	100 Gbit/s

sitehop

info@sitehop.com

SAFEcore 1000

System Performance and Capacity

Mangement	SAFEencrypt 100	SAFEencrypt 10	SAFEpqc 100	SAFEpqc 10
Latency IPv4 64B 1/2 RTT @ 40% (µs)	1.68	3.36	1.68	3.36
Latency IPv4 9000B 1/2 RTT @ 40% (µs)	4	8	4.00	8
Latency IPv4 IMIX 1/2 RTT @ 70% (µs)	2.18	4.36	2.18	4.36
Latency IPv6 IMIX 1/2 RTT @ 70% (µs)	1.91	3.82	1.91	3.82
Number of IPsec Connections	4000	400	4000	400
Number of PQC IPsec Connections	-	-	4000	400
IKE-v2 standards	RFC 6071		RFC 6071 / RFC 9370	
IPsec mode	Tunnel mode			
Post Quantum Crypto Key Exchange	-	-	ML-KEM (RFC9370)	
ESP Cryptography	AES256-GCM			
Certificates Supported	ECDSA - (secp256r1, secp384r1, secp521r1) / RSA (bit length 4096/6144/7680/8192)			
Diffe Helman Groups	Diffe-Helman Group (3072/4096/6144/8192)			
VPN - IPv4	Policy - Based / Route - Based			
VPN - IPv6	Route Based			
Local Management	Local Device GUI			
Local Monitoring	Local Device GUI / SNMPv3			
Remote Configuration/Monitoring	Sitehop SAFEnms			
Secure Remote Update	Yes			
Crypto Agility	Yes			

sitehop

info@sitehop.com

SAFEcore 1000

PSU input (dual inputs) - AC	Supply voltage	min.	110 V
		max.	250 V
	Supply Frequency	min.	40 Hz
		max.	65 Hz
	External power draw*	max.	190 W
	Input connection (per module)	IEC 60320 C14	
PSU input (dual inputs) - DC	Supply voltage	min.	-36 V
		max.	-72 V
	Supply Frequency	min.	40 Hz
		max.	65 Hz
	External power draw*	max.	190 W
	Input connection (per module)	Screw terminal for blade or ring connector. 3 terminals +, -, GND	
Fan	Hot Swappable		

Operating temperature	0 to +40 Deg C	
Storage temperature	-40 to +70 Deg C	
Operating Humidity (non-condensing)	10 - 90	%
Storage Humidity (non-condensing)	< 95	%
Operating Altitude (above sea level)	3048	m
	10000	ft
Operating Altitude (above sea level)	12000	m
	40000	ft
Compliance	CE, CB	

Security without compromise

The SAFEcore 1000 isn't just a platform–it's a strategic investment in the future of secure, high-performance networking. Whether you're protecting financial transactions, securing critical infrastructure, or building quantum-ready cloud connectivity, SAFEcore empowers you to move fast, stay secure, and adapt without limits.

Take the Next Step

Ready to accelerate your security strategy?
Contact Sitehop today to speak with a solutions expert, schedule a demo, or learn how SAFEcore can transform your network edge-to-core.

Engineered for Speed. Built for the Future.