

# Reference Design Accelerates Critical Networking and Security Functions

The Intel® NetSec Accelerator Reference Design is a blueprint to commercialize an Intel architecture-based PCIe add-in card for supporting processor intensive workloads. The card features all of the functionality of a server with the capability to support full orchestration and management capabilities and is ideal for security workloads such as IPsec, SSL/TLS, firewall, SASE, analytics, and inferencing. This reference design can help improve performance, scale, and efficiency for customers from edge to cloud.



As the transformation toward cloudification continues, trends in edge computing and the increase of employees working from home/anywhere are making enterprise environments more distributed than ever before. Traditional perimeter-focused security models and fixed deployment models no longer apply. Monolithic applications have been replaced by chains of containerized microservices that traverse on-premises and cloud infrastructure, decoupled from the underlying hardware; workloads need to be deployed where they are needed. These dynamic, software-defined environments require new approaches to apply security functions at the per-workload, per-user, and per-device level.

The secure access service edge (SASE) model meets these new distributed security requirements by converging software-defined security and wide-area network (WAN) functions into a cloud-delivered set of services. The virtualized or containerized services enhance efficiency with centralized orchestration and reduce equipment costs by using cloud infrastructure based on commercial off the shelf (COTS) servers in place of legacy, single-purpose hardware.

Most SASE solutions are fully integrated stacks of network and security functions, with licensing models based on enabling specific components. SASE vendors make massive investments to evaluate, obtain, and integrate them. SASE software functions require performance and stability in a server that shares multiple compute intensive workloads and multiple tenants. Integrating a performant solution of software-defined WAN (SD-WAN) together with a security stack that includes NGFW, ZTNA, CASB, SWG, DLP, and more is particularly challenging.

The Intel NetSec Accelerator Reference Design offers an alternative approach to SASE function isolation that can dramatically reduce the infrastructure footprint for network and security workloads. It provides users the full functionality of a server on a PCIe card, including an Intel Atom® processor, Intel Ethernet E810 Network Adapter, and substantial onboard DDR4 memory.

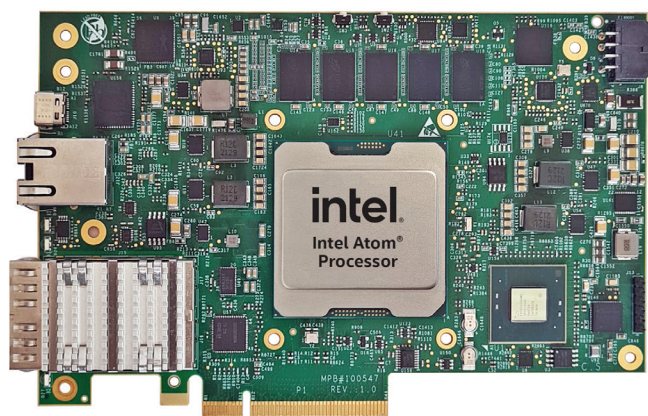


Figure 1. Intel® NetSec Accelerator Reference Design.

## Expanded Processing Horsepower for Security Workloads

The Intel NetSec Accelerator Reference Design can handle the compute capacity of network and security appliances, providing one or more separate physical execution environments. The accelerator supplements the server's primary processor with dedicated acceleration hardware for network and security functions.

Instruction set compatibility and a shared driver architecture between the main CPU and the accelerator CPU helps make the overall solution seamless using standards-based Intel architecture. The consistency of programming models enables platform commonality between the Intel Atom® processor on the accelerator and Intel® Xeon® Scalable processors or Intel® Xeon® D processors in the host machine.

*The Intel Atom processor at the heart  
of the Intel NetSec Accelerator  
Reference Design enables inline IPsec.*

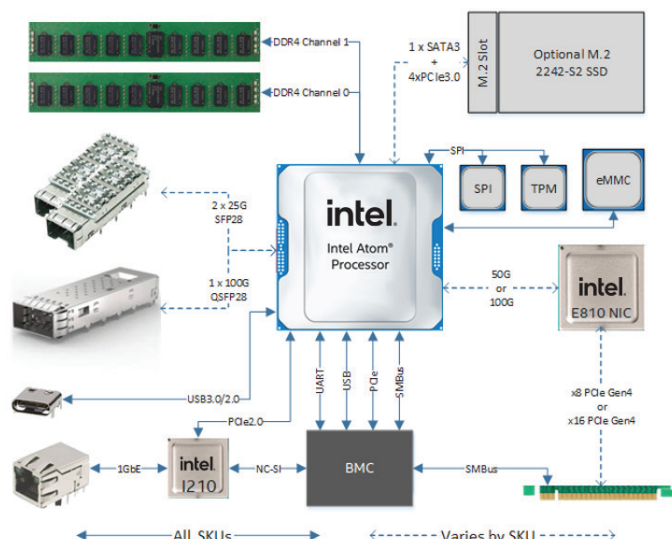


Figure 2. Expanded component view.

The autonomous compute resource isolates data and operations from the rest of the system, helping architects overcome incompatibilities among software components from multiple vendors. The addition of hardware resources based on the reference design enables dramatic gains in solution capability and density. It also provides flexible capacity on demand for Day 2 upgradeability of in-place solutions.

Original equipment manufacturers (OEMs) and original design manufacturers (ODMs), working with network and security solutions providers, can take advantage of the reference design to bring network security accelerators to market more quickly. Intel is working with a number of partners to develop products, making a choice of technology vendors available to systems vendors, solutions integrators, and end customers.

## Reference Design Hardware Specifications

The reference design includes two variations, which are differentiated by processor (and core count), as well as I/O and networking resources.

	8-Core Reference Design	16-Core Reference Design
CPU	Intel Atom® P5721 processor	Intel Atom® P5742 processor
Form Factor	Full height, Half length	
External Ports	2x 25GbE SFP28	1x 100GbE QSFP28
Power Consumption	~50 to 90 watts	70 to 115 watts
Memory Capacity	Up to 32 GB @ 2933 MT/s	
Host Interface	x8 PCIe Gen4	x16 PCIe Gen4
Storage Capacity	Up to 256 GB eMMC	
Throughput Target (Bi-directional Acceleration)	25 Gbps	50 Gbps
Throughput Target (Uni-directional Acceleration)	50 Gbps	100 Gbps

## SASE Acceleration Use Case

Enterprises use WAN and security services through SASE points of presence (POPs) that are geographically dispersed to be in relative proximity to user endpoints and on-prem, edge, and cloud services. POPs act as access gateways that meet service level objectives for latency and throughput in a secure manner. Distributed delivery of cloud-native security services avoids the need to backhaul WAN traffic to centralized locations to apply security policies. This fundamental shift in topology provides substantial bandwidth cost savings while also improving the user experience by cutting out the transfer latency associated with backhaul. A cluster of POP servers hosts any or all of the primary SASE components in real time, for all user network traffic:

- **Next-Generation Firewall (NGFW)** combines traditional firewall functionality with complementary services such as deep packet inspection, intrusion protection, and threat intelligence.
- **Software-Defined WAN (SD-WAN)** dynamically self-optimizes to connect users to applications, centrally directing traffic across any combination of transport services, such as MPLS, 4G/5G, and cable broadband.
- **Zero Trust Network Access (ZTNA)** provides seamless remote access to resources and applications while granting the least privilege possible, regarding all entities as untrusted for all other purposes.
- **Secure Web Gateway (SWG)** filters user-initiated traffic to detect and remove malware and other unwanted software, helping enforce corporate security standards and maintain compliance.

- **Data Loss Prevention (DLP)** monitors outgoing user traffic to identify sensitive information and prevent unauthorized egress, whether malicious or otherwise.

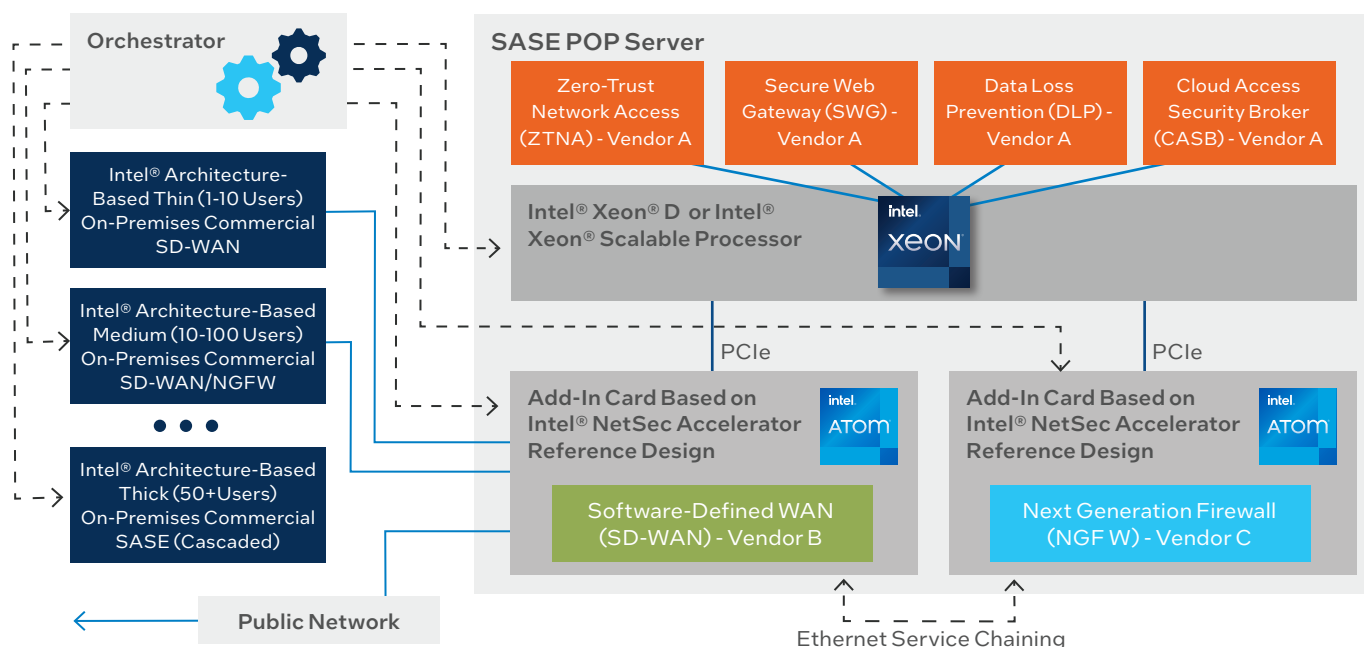
- **Cloud Access Security Broker (CASB)** is an enforcement point between users and cloud services that applies policies such as authentication, encryption, and logging.

A well-designed and constructed SASE ensures delivery of these services with fidelity across locations and endpoint types, such as worker laptops, IoT sensors/actuators, and mobile devices. Quality of service is dependent on the ability to provide adequate POP reach, including both the number of locations and the capacity for each to deliver services. SASE vendors optimize POP servers for the most cost/capacity efficiency.

## SASE POP Server Provisioning

In addition to Intel Xeon Scalable processors, Intel Xeon D processors are designed specifically for provisioning dense compute at the network edge, making them a popular choice as the foundation for SASE POP servers. The platform provides energy-efficient performance, hardware-based security and acceleration technologies, and advanced integrated Intel Ethernet connectivity.

Solution architects can expand the service capacity of Intel Xeon Scalable processors and Intel Xeon D-based POP servers with the addition of one or more accelerators based on the reference design. For example, a two-socket POP server based on 20-core Intel Xeon D processors would have a total of 40 cores. Deploying two 16-core accelerator cards in the system makes an additional 32 Intel Atom processor cores available, for an 80 percent increase in core count without increasing the server footprint. Each accelerator can run a separate SASE service, with its own set of compute, memory, and I/O resources; providing further parallelization of the workload to improve deterministic performance.



**Figure 3.** SASE Architecture enabled by Intel NetSec Accelerator Reference Design.

## Accelerator Connection Topology

An accelerator card based on the Intel NetSec Accelerator Reference Design may be connected directly to the external public network, enabling certain SASE functions to be accomplished independently of the main Intel Xeon Scalable processor or Intel Xeon D processor. This connectivity also makes it possible for the card to provide inline capabilities that independently push inbound data to the appropriate compute resource, for increased efficiency. Ethernet-based service chaining can interconnect services directly between accelerators, combining capacity or functionality, as in the example shown of delivering SD-WAN and security stack together as a single service from two distinct accelerators. The built-in switching capability of the Intel Atom processor facilitates resource sharing to improve efficiency, with load balancing between ports without involvement from the Intel cores running on the Intel NetSec Accelerator Reference Design solution.

For some implementations, an accelerator based on the Intel NetSec Accelerator Reference Design may not be connected to the outside world. For example, it may use service chaining to deliver services through another accelerator that is on the public network or provide functionality such as a sandboxing application for deep packet inspection that does not require external connectivity.

## Potential for SASE Acceleration in Real World Deployments

The SASE acceleration use case demonstrates some representative usage patterns for devices based on the reference design in SASE POP servers:

- **Increased density and infrastructure efficiency** based on deploying added compute capacity with one or more accelerators with the full range of server-on-a-card resources.
- **Multi-vendor integration**, instantiated by the SASE POP server providing unified services based on solutions that would otherwise be incompatible on a single system.
- **Advanced traffic control** using the integrated network switch in the Intel Atom processor to direct inbound data appropriately, independent of the main processor.
- **Service chaining and delivery** of distributed SASE services using multiple accelerators in a single SASE POP server.

By expanding the hardware and making it more capable, these factors help lower cost of operation by reducing the total number of servers required to accomplish a given performance goal.

## Building Blocks for Accelerated Networking and Security

The reference design provides an independent, functional compute node that delivers server-class performance and reliability within a conservative power envelope. It provides integrated Ethernet switching and inline cryptography for IPsec, as well as look-aside operation, which is appropriate for asynchronous bulk encryption workloads.

### Intel Atom processor—High Performance per Watt and Inline IPsec

The foundation of the Intel NetSec Accelerator Reference Design is the Intel Atom processor, which provides high throughput for security and networking workloads in an energy-efficient SoC form factor. The highly integrated device incorporates Intel Ethernet, a network switch, and hardware accelerators into the SoC package, which provides low-latency operation and drives significant advantages in reduced equipment cost, space/server requirements, and energy consumption.

- **Network Acceleration Complex (NAC)** provides high-performance Ethernet I/O and switching. The integrated eight-port Ethernet switch provides the basis for a sophisticated 100 GbE or 200 GbE packet processing pipeline that is fully programmable using Intel-provided APIs. The processor's switching capacity provides advanced traffic management using built-in packet classifiers, with full load balancing between ports.
- **Integrated Intel® QuickAssist Technology (Intel QAT) Gen3** accelerates symmetric and asymmetric encryption, driving up to 100 Gbps of throughput. The Intel QAT hardware communicates directly with the onboard Ethernet controller to decide which packets to process and which to pass to the processor, using the platform's integrated switch. By shortening the data path, this capability enables inline IPsec.

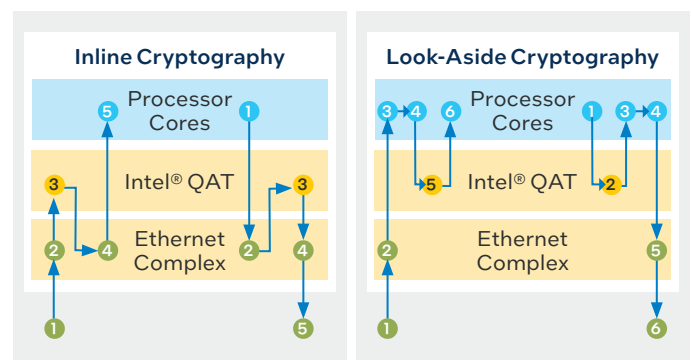


Figure 4. Enabling inline IPsec.

## Intel Ethernet Network Adapter E810—Advanced Networking for Security Functions

The reference design includes an Intel Ethernet Network Adapter E810. The adapter provides throughput of up to 100 Gbps that takes advantage of sophisticated packet processing, traffic shaping, and intelligent acceleration to improve performance. It uses the same high-quality, open-source drivers as the host machine's network adapters, assisting in smooth solution integration. Additional technology features support the intelligent networking built into the reference design:

- **Dynamic Device Personalization (DDP)** enables administrators to establish multiple profiles for different traffic types, specifying packet-handling parameters and optimizations for each. Traffic prioritization based on DDP can be configured dynamically at runtime to enhance flexibility and agility.
- **Application Device Queues (ADQ)** provide the mechanism for individual applications to proactively reserve one or multiple dedicated Ethernet hardware queues. ADQ helps ensure deterministic performance for critical data flows.

## Conclusion

The Intel NetSec Accelerator Reference Design is a highly efficient blueprint for delivering all the functionality of an independent server in a PCIe form factor for effective slot-in integration into security appliances and edge platforms. It provides a separate physical compute environment within the server chassis.

The addition of resources including system memory in the reference design enables the accelerator device to run independently of the main server platform. The accelerator runs security services independently to expand server capacity, including support for multi-vendor software stacks that would otherwise not be compatible on a single system. This capability may help end customers reduce TCO by supporting more services per host.

The pre-validated reference design streamlines the development of new security appliances by OEMs and ODMs, working with network and security solutions providers. It enhances platform flexibility and reduces design-in requirements for those solution developers, helping them bring new security products to market more quickly and cost-effectively.

To learn more about Intel Atom processors, go to:

[www.intel.com/atom](http://www.intel.com/atom)

Solution provided by:



Performance varies by use, configuration and other factors. Learn more at [www.Intel.com/PerformanceIndex](http://www.Intel.com/PerformanceIndex)

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

Code names are used by Intel to identify products, technologies, or services that are in development and not publicly available. These are not "commercial" names and not intended to function as trademarks.

Any forecasts of goods and services needed for Intel's operations are provided for discussion purposes only. Intel will have no liability to make any purchase in connection with forecasts published in this document.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

0522/HD/MESH/349364-001US