Product Brief

Distributed Services Platform for the Enterprise

NETWORKING, SECURITY AND STORAGE SERVICES AT CLOUD-SCALE

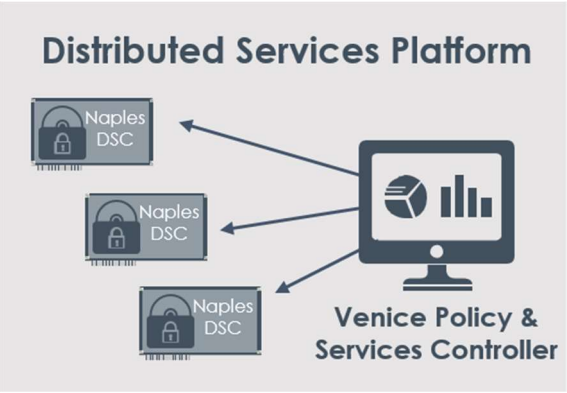
The massive expansion in the number and diversity of applications, as well as an explosion in the amount of data being generated and transported through enterprise data centers, has pushed the architectural limits of modern IT infrastructure. Traditional "scale-up" approaches – where networking services are embedded into top-of-rack switches, or networking and security appliances – are no longer able to keep up, suffering from either performance, agility or scale limitations as policy tables bloat and the number of active flows reaches into the millions. The limitations and expense of this centralized resource model have led data center architects to limit the core network infrastructure functions to simply transporting IP traffic with as little latency and jitter as possible.

Just as compute and storage systems are adopting a "scale out" approach, so too the networking and security elements of the data center must adopt a *Scale-out Services Architecture* and these functions need to find a new home in this model. The ideal place to instantiate these services is the server edge (the border between the server and the network) where services such as firewall, encryption, tunneling and VPN termination can be delivered in a scalable manner. In fact, each server edge is tightly coupled to a single server and needs to be aware only of the policies related to that server and its users. This approach naturally scales – as more services capabilities come along when new servers are added.

Pensando's "**Distributed Services Platform**" (**DSP**) delivers a powerful suite of software-defined services at the compute edge. Easily installed in standard servers, the Pensando **DSP** solution provides high-performance scalable networking, security and storage functions, eliminating an assortment of discrete appliances throughout the data center and dramatically simplifying IT operations while providing unmatched telemetry, I/O visibility and troubleshooting insights.

PENSANDO DISTRIBUTED SERVICES PLATFORM

Built on custom, fully programmable silicon and positioned at the server edge, Naples™ Distributed Services Cards (**DSC**) bring software-defined services adjacent to the workloads where policy enforcement and visibility are most effective.



The Pensando Venice™ Policy and Services Controller manages all aspects of the deployed edge services, including lifecycle and health monitoring of Naples DSCs. Resources can be automatically provisioned and new software-defined services deployed from a single pane of glass. Venice handles seamless distribution of ACLs and stateful firewall policies, network configuration settings, encryption keys, etc. to active Naples services nodes to consistently manage network performance while ensuring policy compliance. Comprehensive telemetry features enable full data center visibility and rapid troubleshooting of problems.

HIGHLIGHTS

BENEFITS

- Improve security posture through distributed network protection and east-west security
- Maximize server CPU availability by offloading networking and security functions at wire speed
- Eliminate complexity and latency associated with "tromboning" through multiple appliances
- Simplify configuration and policy management for large scale deployments
- Achieve deep visibility into network behavior with 'Always-On' telemetry
- Solution works seamlessly with virtualized, bare metal and containerized workloads
- OS version agnostic

FEATURES

- Integrated security, networking and storage functions in a single device
- Incorporates both data plane and control plane, eliminating host agents
- Isolated domain of security enforcement
- NVMe storage virtualization with NVMe-oF
- Scale: 100s of thousands of Firewall rules, >1M routes
- Centralized management system securely manages policy and offers full network visibility

SOFTWARE-DEFINED INFRASTRUCTURE SERVICES (SDIS™)

Server-based network services extend the intelligence and resilience of network devices to the server, greatly simplifying the network operational model. A flattened architecture with infrastructure services such as routing, traffic shaping, load balancing, security and telemetry deployed at every server has lower latency and – with an automated central management system – can be easier to reconfigure and manage than legacy approaches using multi-vendor appliances for services functions.

The network and services layer are decoupled, so network decisions can be made independently of the security architecture – policies remain the same regardless of the underlying transport mechanism.

UNIFIED MANAGEMENT

Managing security at Cloud-scale requires a new way of thinking about both management and security. Pensando's **Venice**™ Policy and Services Controller leverages an intent-based model of delivering network and security policy to Naples nodes for services implementation at the edge. With an intent-based model, IT administrators are assured of consistent policy and reliable network configuration throughout a multi-tenant domain supporting thousands of nodes. Naples services nodes incorporate gRPC and RESTful management APIs for managing and monitoring of all device capabilities.

Designed for high-availability and fault-tolerance, the Venice system is distributed and redundant. All communications between Venice and the edge services nodes are encrypted and authenticated.

The Pensando DSP solution can integrate smoothly with existing Central Management infrastructure, either communicating with Venice via its "northbound" APIs, or by connecting directly to the Naples devices via gRPC / REST APIs.

USE CASES

- Distributed stateful firewall at the server edge
- Routing, Segment Routing, MPLS, BGP
- SDN and Virtual Networking with underlay/overlay encapsulations (VXLAN, etc.)
- Deep network and security visibility and telemetry
- East-West encryption within the data center
- Network load balancing, including TCP/TLS termination
- Storage virtualization functions including NVMe-oF

SERVICES PACKAGES PORTFOLIO

Tailored services packages ensure that the specific needs of your data center are met. Additional capabilities can be deployed in the field through Venice using secure over-the-network (OTN) software updates.

The baseline Naples product delivers comprehensive network I/O functionality with leading edge network offloads, then one or more of the available software subscription packages include:

Advanced Networking – Switching/Routing, Segment Routing, L3/L4 Load Balancing, overlay networking, VXLAN, NAT, ERSPAN, rich

packet telemetry and streaming NetFlow

Advanced Security – Stateful L4 firewall with ALGs and URL filtering, Micro-Segmentation, packet-based attack protection, VPN termination (IPsec), TLS/DTLS encryption, TLS Proxy

Enhanced Storage – NVMe virtualization, NVMe-oF with RDMA or TCP transport, data-at-rest encryption, data compression, deduplication acceleration

ENHANCED DATA CENTER SECURITY

Customers are increasingly reporting that north of 80% of all data center traffic is East West. The security landscape is evolving, with pervasive threats emerging from inside the data center that render perimeter based solutions ineffective. Enterprises have begun to adopt distributed host based security services, however these have serious limitations given that security policy is executed in software adjacent to the OS attack surface.

Isolation of network, security and storage services from the server CPU brings several benefits:

Significantly enhanced security	Strict host isolation enforced by HardGap™ technology protects Naples from compromise in the presence of attacks on the server
Doesn't require host- based agents	No disturbance to existing server configuration or applications
Single point of enforcement	All server traffic traverses the Naples Services Node, where policy is consistently applied
Free-up host CPU resources	Compute-intensive security functions offloaded to domain-specific hardware

ALWAYS-ON TELEMETRY AND DEEP VISIBILITY

Naples brings sophisticated Telemetry at the edge, providing real time observability and insights for network and storage, without affecting application performance. It can correlate packets and perform message level inferences. Always-on telemetry enables proactive end to end troubleshooting and problem reporting.

Native tools in Venice enable the infrastructure to automatically report potential issues such as unusual behavior from a compromised workload based on firewall statistics (policy drops, known attack vectors, probing multiple ports), bandwidth usage patterns, connection duration (short-lived vs. long-lived), number of connections established, rate of incoming/outgoing connections, number of inbound vs. outbound connections, data content (incongruent data patterns within applications), and other criteria.

With its hardware-accelerated telemetry engines, Naples supports proactive testing and probing without compromising latency or impacting server CPU resources.

These powerful visibility tools give IT administrators the ability to:

- Vastly improve Time-To-Repair across the entire infrastructure
- Automate problem detection AND remediation
- Proactively monitor and manage systemic health

COMPREHENSIVE AUDIT and COMPLIANCE

Explicit "zero trust" policy enforcement and optional data encryption capability complies with best-practices requirements in regulated industries.

Firewall, Syslog and Audit logs can be exported to industry-standard SIEM software like Splunk, and are compatible with 3rd party analysis plugins. Venice supports 6-month retention on all audit logs with flexible archiving options.

INDUSTRY-LEADING PLATFORM

Pensando's custom-designed Capri™ P4 Programmable Processor powers the Naples DSC, enabling wire-speed performance and enhanced security through isolated policy enforcement. The data plane and control plane are fully software-defined and supported with hardware accelerators. Up to 8 GBytes of on-chip High Bandwidth Memory (HBM) provides the low-latency and flow-table capacity for true cloud-scale deployments.

DEPLOYMENT OPTIONS

Naples™ Distributed Services Card (DSC)

Naples DSC-25

- Installs in Server, delivers Ethernet I/O and software-defined networking, security & storage services
- Naples DSC-25: 2-port 10/25G Services Card
  - PCIe Gen3 8-lane
  - 2x SFP-28 connectors
  - 1x RJ45 100M/1G management port
- 50Gb/s networking and services throughput

Power: 20W typical

Naples DSC-100

- High-performance card; delivers high-speed connectivity to the applications as well as sophisticated networking, security & storage services
- Naples DSC-100: 2-port 100G Services Card
  - PCIe Gen3/4 16-lane
  - 2x QSFP28 connectors supporting DAC and fiber
  - 2x RJ45 100M/1G management ports
- 100Gb/s networking and services throughput

Power: 27-36W typical

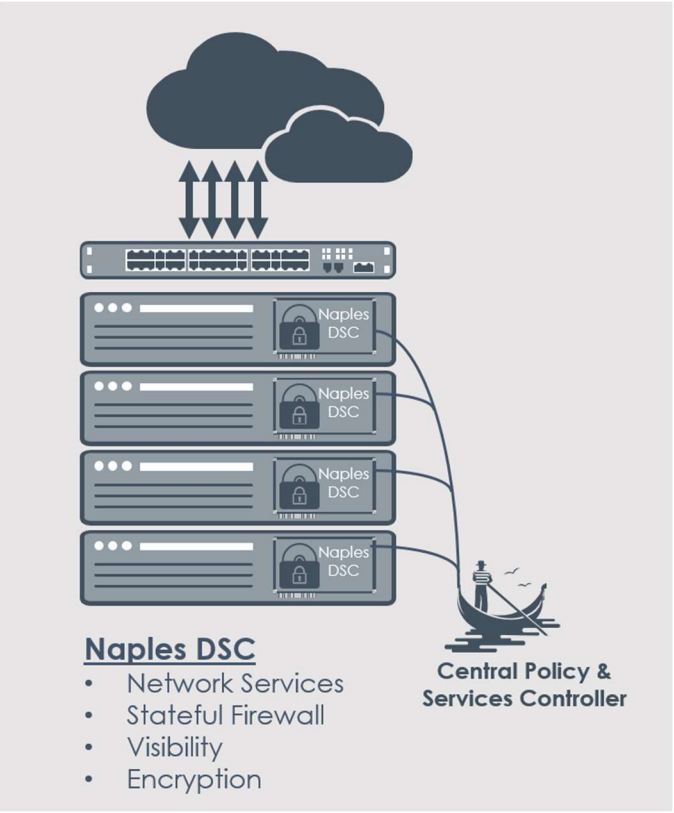
Venice™ Policy and Services Controller

- Microservices-based, fault-tolerant management infrastructure, supporting large-scale data centers
- Policy and network services configuration centrally managed from Venice GUI or via REST API
- Collect events, logs and metrics from DSCs
- Powerful troubleshooting tools
- Intent-based object model
- Integrates with VMware vCenter® policy manager
- Deployed as a VM or native Kubernetes microservices
- Clustered instances with High Availability (quorum) features
- Federation of multiple Venice domains for large-scale deployments

DEPLOYMENT CONFIGURATION

Naples DSCs are installed into standard servers to provide advanced services as well as high speed network I/O ports. **Venice** manages the DSC devices over the network, in-band or out-of-band.

Distributed Services Cards Deployed in Servers



PERFORMANCE

Naples delivers 100G wire-speed services to the server, including chained services e.g. L4 stateful firewall + IPSec encryption + Load Balancing.

Performance Metric	Naples DSC-100
L4 Stateful Firewall throughput	100Gb/s
L4 Load Balancer throughput	100Gb/s
Encryption throughput	100Gb/s (AES-GCM-256, @ 256B pkts)
NVMe-oF/TCP IOPS	3M, 100Gb/s @ 4KB transactions
Packet rate	40 Mpps
Avg Latency	3µs
Avg Jitter	40ns

SCALE

The Distributed Services Card can be software defined into multiple configurations to support immense scale for the largest data centers, one of which is detailed below:

Scale Metric	Naples DSC-100
Route Tables (LPM)	1M IPv4 and 1M IPv6 2M total
Firewall Rules	100,000 per node
Overlay Mappings	128k Local Mappings
	1M Remote Mappings
	1M SIP to TEP Mappings
NAT Mapping Tables	512k
Policers	4K

ABOUT PENSANDO SYSTEMS

Founded in 2017, Pensando Systems is pioneering distributed computing designed for the New Edge, powering software-defined cloud, compute, networking, storage and security services to transforms existing architectures into the secure, ultra-fast environments demanded by next generation applications. The Pensando platform, a first of its kind, was developed in collaboration with the world's largest cloud, enterprise, storage, and telecommunications leaders and is supported by partnerships with HPE, NetApp, Oracle, IBM, Equinix, and multiple Fortune 500 customers.

For more information, please visit www.pensando.io