DATA SHEET

Versa Secure SD-NIC

Background

Compute platforms in data centers, enterprise offices or in remote sites have been using Ethernet NICs for network connectivity ever since Ethernet was invented. Over time, Ethernet NICs have gone through major performance improvements with faster interfaces and copper to optical transitions. Today's Ethernet NIC interfaces range from 1 Gbps to over 200 Gbps speeds and beyond.

On the functionality front, Ethernet NICs have been enhanced to run a variety of stateless network services, including QoS, ACLs, Ethernet frame fields rewriting (ie: DSCP or TOS fields), policers, shapers, and certain network functions. These functions, running within the Ethernet NIC itself, allow offloading of most of these functions from CPUs, opening more compute cycles. Additional benefits of these functions running on Ethernet chips includes line rate performance, low latency, shaping and QoS accuracy.

While evolutionary enhancements have happened on Ethernet NICs, revolutionary approaches are also being researched by Ethernet chip vendors. NPU and NIC vendors are investigating innovative ways to provide software defined pipeline capabilities within Ethernet chips to offer higher value offload solutions to their compute and networking customers.

This transformative approach got inspired by Software Defined Networking (SDN). Using SDN, network operators could define sequences of software delivered functions and then implement them in the exact order and detail that they specified in a software defined path. This approach triggered major transformations in the way networking and security solutions were architected and deployed. Today Software Defined WAN (SD-WAN), Secure Services Edge (SSE), Secure Access Services Edge (SASE) and Software Defined LAN (SD-LAN) products and solutions are available and commonly used or requested in the market.

SDN inspired thoughts by certain Ethernet chip vendors gave birth to a new generation of programmable NPUs and NICs based on the P4 language. P4 stands for "Programming Protocol-independent Packet Processors." It's a language that defines the behavior of packet forwarding on network devices. This includes tasks like parsing, processing, and generating responses to received packets based on a variety of fields and conditions. With traditional NPUs or ASICs, NICs had fixed functions that could not be modified, now with P4 and programmable NPUs, network operators can customize and adapt the behavior of their hardware to meet specific needs, or introduce new services implemented in NPU or NIC hardware without replacing it. P4 programmability gives them flexibility in how chips process packets, enabling rapid adaptation to changing network requirements or the introduction of new protocols. This level of programmability has wide-ranging applications, enabling advanced features like inline telemetry, traffic engineering, IPSEC crypto termination and more. P4 is available today on select Smart NICs.

While P4 raised the bar of programmability in terms of task sophistication, task order and flexibility, it does not cover most of L4-7 based security needs of compute operators. Advanced security functionality such as Zero Trust Network Access (ZTNA), fingerprinting, security posture assessment, SSL-TLS proxy, application identification, and malware or vulnerability scanning all use more complex state machines which are not supported by today's ASIC-based Smart NICs. In the absence of these advanced functions within Smart NICs, compute operators must continue using external security appliances or security VMs within their compute platforms to bridge that gap.

The Need

Enterprise operators are looking for natively integrated, inline, comprehensive security functions for their compute platforms. These compute platforms may be in data centers, enterprise offices or in remote sites depending on the use-case and applications. Regardless of where they are deployed, in today's world, compute is considered as a critical infrastructure, and loss of valuable data or interruption of services due to malicious actors can result in major problems for Enterprises. Operators are aware of this risk and therefore they typically architect compute solutions with a perimeter-based security approach.

As we look at these deployments closer, we see two distinct sets of deployment scenarios or use cases, each with their own requirements:

1. Virtualized multi-tenant data centers.
2. Compute devices deployed in untrusted or 3rd party environments.

Virtualized multi-tenant data center challenges

In a virtualized multi-tenant data center, the Enterprise operator may not be able to control the VMs or containers deployed within it. As a result, these virtualized workloads should be treated as untrusted entities on the data center network. Given this perspective on the trust posture of virtualized workloads, multi-tenant data centers should require the use of a ZTNA solution.

Today's data centers or enterprise LAN deployments are typically protected in two ways:

1. **Data-Center WAN Edge based security** - WAN Edge-based dedicated firewall appliances focus on securing compute against threats coming from the WAN.
2. **Security VMs on virtualized compute infrastructure** - virtualized firewalls running on the compute infrastructure focus on securing compute platforms against threats coming from virtualized workloads.

In a multi-tenant data center environment, the problem is exacerbated further. Each tenant needs to be separated and protected from each other. VLAN and/or VXLAN VNID based traffic separation are used to isolate the traffic of each tenant, but there is no natively built security that exists in virtualization stacks, hence physical or virtual firewalls are used to bridge that gap.

There are some challenges with the virtualized security approach. While security VMs (ie: firewall VMs) can provide NGFW, IDS/IPS, and UTM functions, they take valuable compute resources away from the server. In addition, they require complicated traffic forwarding paths within virtualized environments, with U-turns and other hair-pinned traffic forwarding paths. They can also potentially become bottlenecks for all traffic on the server.

Alternatively, security functions for workloads of tenants can be provided by dedicated firewall appliances. Such traditional dedicated firewall appliances would be connected to Ethernet switching layers within data centers. This approach creates similar challenges in terms of complexity of traffic steering across layers of devices, and network device interfaces serving trusted (post firewall) and untrusted (pre-firewall) traffic zones intertwined across layers of devices, servers and storage systems. In many cases, it may not be obvious which part of the network is trusted or untrusted as traffic may be served by intermediate workloads or services. Furthermore, hardware centric firewall appliances cannot be coupled together with workloads in a distributed way and they can end up being performance bottlenecks within the datacenter. All of this translates to complexity and cost.

Virtualized multi-tenant data center requirements

Enterprise datacenter operators need seamlessly integrated, comprehensive security including ZTNA and micro-segmentation functions. As performance requirements increase, separate siloed solutions only add to complexity. Market research shows that there is significant security risk in multi-tenant data centers from compromised or malicious tenant VMs or other workloads that can spread laterally across the compute platform. Hence, the ideal multi-tenant data center solution must provide a Zero Trust security approach that can prove effective against internally originated attacks or exploit attempts, which usually go undetected while using today's security perimeter-based approaches focusing on WAN.

Untrusted compute environment challenges

For enterprise compute appliances deployed outside of enterprise sites, for example in untrusted or 3rd party environments, additional security requirements need to be satisfied. These include:

- the ability to find “home” for control and management,
- automated provisioning for ease of deployment in foreign environments, and
- use of encrypted, encrypted tunnels to provide data and application confidentiality.

Today, these requirements are typically satisfied by shipping external firewall or secure SD-WAN appliances together with compute appliances, adding significant cost and complexity to these deployments.

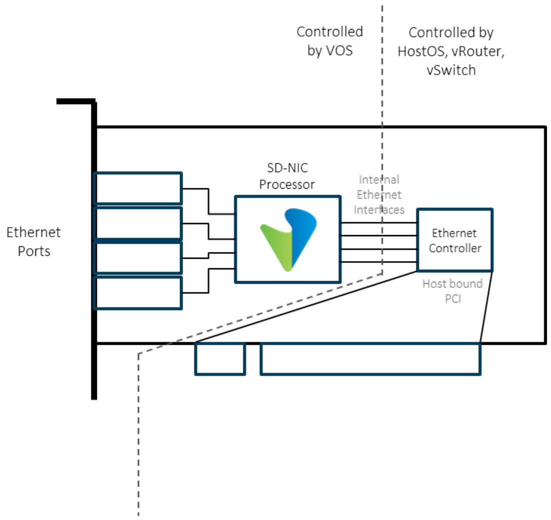
Untrusted compute environment requirements

Enterprises are looking for a reduced footprint, so opportunities to consolidate functionality at the device or NIC level are needed. One potential approach is to deliver natively integrated security functions that are located within the compute appliance itself. This approach would also allow Enterprise to provide all included compute solutions in a single integrated appliance that can potentially be sealed for physical integrity check.

The Versa Solution

Versa Secure SD-NIC solution is a VOS (Versa Operating System) powered intelligent NIC that utilizes the combination of a built-in x86 based multicore processor and Smart NIC ASIC located in one PCI card. The Versa Secure SD-NIC then combines the x86 processor and Smart NIC ASIC to provide the best of both worlds; x86 running VOS with its full comprehensive security and networking functionality (including all its stateful services), and the smart NIC ASIC providing high performance networking as an attached PCI device. This combination addresses the unmet needs of Enterprise operators by providing L2, L3 and full set of stateful L4-7 functions without the limitations of other smart NICs. This is an alternative way to deploy VOS within the compute, in a truly inline and transparent way.

High level diagram of Versa SD-NIC is as follows:



Versa Secure SD-NIC solution is a distributed solution. One or more SD-NIC can be placed in each compute appliance to provide a distributed and highly scalable L2, L3, L4-7 set of functions delivered from within each compute platform. SD-NIC based on VOS is then the Data Plane for all L2-L3, L4-L7 functions.

While the Data Plane is distributed, Management and Control Planes are centralized to provide ease of centralized control and visibility using a single pane of glass. The centralized Control Plane function facilitates exchange of reachability information and sets up network paths while also influencing traffic forwarding decisions to achieve desired outcomes for our customers. The centralized Management Plane administers Zero Trust Provisioning (ZTP), auto-provisioning all Versa Secure SD-NICs while providing a true single pane of glass to manage the entire SD-NIC lifecycle. The Versa management platform provides capabilities from a centralized console to manage configurations of the entire network including topology definitions, policy definitions, L2-L3 and L4-L7 functions, security posture and other features.

Today, Versa uses this same architecture and approach in SD-WAN, SSE and SD-LAN deployments. Now with VOS being deployed on a Smart-NIC, the Versa Secure SD-NIC solution can offer the same architecture, using the same proven software and its natively built-in capabilities directly within compute platforms.

Versa's Secure SD-NIC solution is based on open standards and protocols for ease of deployment, operations and debugging reasons. With an open, highly scalable and resilient SDN approach Versa aims to maximize uptime, eliminate single points of failure, reduce proprietary solutions, eliminate operational complexities and transform data center and enterprise compute connectivity and security in innovative ways.

Seamless Integration of Versa Secure SD-NIC with SDN and SD-LAN for Data Centers and Enterprise LAN

The Versa Secure SD-LAN solution is based on running intelligence on the edges of the LAN, while keeping the core of the LAN (LAN transport layers) simple. This approach allows Versa customers to identify, assess, authenticate, place, control by policy and secure both network attached devices and users based on their profile, security posture, and class. Customers can manage their traffic under policy control from the edge of the LAN and onwards into the network. Versa's focus on making the LAN edge intelligent while keeping transport simple also allows customers to insert and deploy Versa Secure SD-LAN with ease, while retaining their investment on aggregation or core Ethernet switches. Now with Versa Secure SD-LAN, these same capabilities are brought into data-center servers or Enterprise LAN attached compute devices, pulling the intelligent edge even closer to workloads and applications.

Versa Secure SD-LAN and Versa Secure SD-NIC solutions are based on the same standards-based technologies that enable our customers to form a multi-vendor solution. Standards based encapsulations, control plane options and protocols are used to ensure multi-vendor interoperability and successful deployments in datacenters with other vendor SDN and SD-LAN solutions. See the feature-set sections below for more information.

Rich set of L2 and L3 Features

Versa Networks solutions come with a heritage of carrier class routing and networking features. VOS's set of Layer-2 and Layer-3 features include:

- Comprehensive Layer-2 features: Including Bridge-domains, virtual switches for multi-tenancy, xSTP, VLANs, VLAN manipulations, VLAN access/trunk mode, DHCP snooping, LLDP, IRB for integrated routing and bridging to allow multi-tenant seamless integration to L2 networks.
- Comprehensive Layer-3 features: DHCP client/server/relay, VRFs, Static NAT, carrier class routing protocols: OSPFv2/3, RIP-v2, BGP/MP-BGP, IGMP v2/v3, PIM SM/SSM, Auto/Boot-strap RP, BFD, IPv6 extensions of routing protocols to allow seamless integration to L3 networks.
- Rich set of platform features: LAG, rich set of QoS features (priority queuing, WRR, WRED and more), Shapers, Policers, ACLs, ZTP options, auto-provisioning, VRRP, Flow mirroring, Flow reporting, uCPE to host 3rd party VMs.
- Overlay based connectivity options: VXLAN, GRE, MP-BGP EVPN, MP-BGP L3VPN, IKEv2 IPSEC to connect to datacenter or Enterprise LAN overlay networks.
- Network Access Control (NAC) capabilities: 802.1X single/multiple supplicants, RADIUS back-end, Certificate based and MAC bypass list-based authentication.

Such a rich set of L2, L3, platform level capabilities have been developed to meet a variety of the needs of our customers and to fulfill their deployment and interop requirements. These features and capabilities are available on Versa Secure SD-LAN and Versa Secure SD-NIC.

Natively Built-in Security; User and Application Intelligence

Versa Secure SD-LAN and Versa Secure SD-NIC solutions run VOS natively with its comprehensive security stack. The Versa security stack can be summarized as follows:

- Stateful Firewall, CGNAT with ALS support, DOS Protection
- DNS Proxy, DNS Feeds and Filtering
- Application, User, Device policy-based traffic control
- IoT Security
- Unified Threat Management capabilities including NG-IPS, TLS Proxy, ATP and Malware Protection
- Inline Cloud Access Security Broker (CASB), Inline Data Loss Prevention (DLP)

Single Policy Language and Single Policy Engine for the Whole Network

Versa's single, unified policy language is used also on Versa Secure SD-NIC solution. Security, routing, ZTNA, user or device, and/or application policies can be defined once and then applied across each or all SD-NICs as well as the rest of the network, including Switching, WAN Edge or SSE. Use of Versa's proven unified policy language and policy functions for Secure SD-NIC provides a major benefit and consistency to enterprises.

A compute device and its workloads using Versa Secure SD-NIC solution will be admitted to the network by VOS based Versa SD-NIC using user, device-id, application, security policies, security posture, or other combination of factors. Under the administration of these policies, the SD-NIC carrying compute device and its workloads will be allowed to communicate with destinations on the LAN or on the WAN using tunnel overlay or underlay protocol and encapsulation options. If the workload moves to another part of the network, policies will follow the device, applying consistent solutions irrespective of the location where the user and device connect from.

Natively Built-in ZTNA and Micro-Segmentation

Versa's market leading ZTNA on-premises capabilities provide secure connectivity and a next generation software defined perimeter solution for local users and devices connecting to Enterprise LAN networks. Versa's on-premises ZTNA functions are delivered inline, closest to the network attached device, user, or workload, to provide comprehensive detection, identification, classification, and control capabilities.

In virtualized multi-tenant data centers, Enterprise operators may not be able to control VMs and containers. As a result, these workloads should be treated as untrusted entities on the data center network. This requires use of ZTNA solutions within data centers.

Versa's natively built-in ZTNA capabilities are now available within each compute appliance thanks to the Versa Secure SD-NIC solution. Close proximity on the compute appliance allows identification of workloads, assessment of security posture, identification of apps, and implementation of policy-based network control and security functions on the entry point to the network. If deemed necessary, due to dynamically assessed security posture of the workload or the compute environment, traffic can be examined fully inline before it hits the rest of the datacenter network, via built-in L4-7 security functions. Traffic can be managed based on security, network access, application policies. The outcome of such access control, security check and policy implementations may be to drop, forward, log, or place traffic into specific micro-segments of the network. The traffic then can be sent to its destination(s) preferably using SD-LAN overlays in independent ways from underlying network infrastructure. Such functions implemented inline closest to the workloads provide the most comprehensive ZTNA coverage for Enterprise operators.

Another cutting-edge feature of Versa Secure SD-LAN and Versa Secure SD-NIC is its ability to micro-segment client device traffic based on device type, security posture, user, group, and other variables. Versa's powerful policy engine allows our customers to define their own policy rules and map them to different micro segments to fine granular separation of traffic types from each other.

VOS supports different segmentation options such as VLAN, VXLANs and SGT tags to implement micro-segmentation. SGT tag based micro-segmentation is the preferred choice as it allows dynamic assignment of SGT tag values to subsets of traffic based on changing security posture of devices and users w/out changing assigned VLAN, VXLAN IDs or IP subnets. Devices that degrade in security posture over time (ie: AV engine gets disabled on a corporate laptop that runs Versa Client App) will automatically get mapped to restricted access class, identifiable with its SGT tag value, and if desired, network-based security functions such as NGFW and UTM can be applied to it. Once the security posture of the device recovers, then it can regain its access privileges dynamically.

Propagation of SGT tags across Versa Secure SD-LAN and Versa Secure SD-NIC solutions allow consistent policy and traffic management decisions to be implemented across the network within the datacenter or across datacenters, providing a network level secure, and comprehensive ZTNA solution regardless of where traffic gets originated from and where it is destined to.

Versa Secure SD-NIC to Provide Secure Deployments in Untrusted or 3rd Party Environments

Versa Secure SD-NIC also empowers deployment of sensitive compute systems or applications in untrusted or unknown 3rd party network environments. Such environments may include deployments of a sealed enterprise compute and its sensitive applications on an enterprise environment (ie: financial services applications, market news servers) or various compute based specialized solutions (ATMs, Mobile cell tower compute systems), tactical deployments and others.

Thanks to the PCI form factor of the Versa Secure SD-NIC, one can pre-install the SD-NIC in the compute system, seal the whole appliance and ship it to wherever it needs to go. That will remove the need to deploy external routers, firewalls or SD-WAN appliances, eliminating the need for additional devices as well as eliminating the potential for malicious actors to connect or tap into exposed network ports. This all-in-one compute solution with its VOS based SD-NIC will provide all security, connectivity and policy-based traffic management functions from within the compute system, making deployments fast, easy, and secure.

Versa Secure SD-NIC's natively built-in SD-WAN capabilities would provide zero touch provisioning (ZTP) for ease of deployment, centralized management, and auto-provisioning capabilities. Without this ZTP capability, one would need a working network connection to call out to centralized controllers for this to happen. A typical remote compute deployment model would involve SD-WAN based secure encrypted connections across such environments connecting compute to datacenters or other desired points of destination using fully secured and encrypted SD-WAN tunnels.

Versa's SD-WAN capabilities extend far beyond standard IKE based IPSEC VPNs. Versa SD-WAN provides support for:

- Secret never being put to wire and entirely control plane administered encrypted overlay formation.
- Flexibility in key sizes and encryption algorithms, approved by FIPS certification.
- Support for multiple network paths, dynamic effective throughput measurement and appropriate traffic prioritization and management capabilities across multiple paths
- LTE, 5G, satellite network optimized SD-WAN tunnels, including so-called tunnel-less SD-WAN, adaptive probing.
- Full stack of TCP Optimization, FEC, Packet Striping, Packet Cloning to assure best user and application experience.
- L2, L3 (IPv4 and IPv6) connections over SD-WAN tunnels
- IPv4, IPv6 based underlays.
- Flexible topology and controller placement options
- Traffic Engineering, first packet-based traffic identification, DPI based packet identification, URL based traffic classification and management.

- Policy based traffic control and management.

These market-leading SD-WAN capabilities will provide the best user and application experience for our customers with Versa SD-NIC.

With the use of a natively integrated security stack, ZTNA, micro-segmentation, and other capabilities, applications and workloads tdeployed in remote locations can be secured further. Such capabilities apply to baremetal servers as well as to virtualized servers with virtualized workloads, as explained in the sections above.

Such proven expansive capabilities of Versa Secure SD-WAN now being delivered as part of the Versa Secure SD-NIC solution makes the Versa solution an unmatched and pioneering solution in the market.

Big-Data based Analytics and Predictive Analysis

Integrated with Versa Secure SD-NIC is Versa's cloud delivered AI/ML driven Analytics, Observability and Prediction Engine.

Versa's conversational language assistant, Verbo, delivers context sensitive, intent based, troubleshooting in an easy-to-use interface for administrators not well-versed with Versa technology. The solution auto-corrects the responses and provides an automated workflow-based troubleshooting experience.

AI/ML driven Big Data Analytics provides near real-time visibility and historical reporting of the entire network. The Analytics system consumes telemetry data from the network and provides insights into the user, application and network performance and errors. The Observability platform provides actionable insight into the errors. Alarm correlation allows the NOC team to focus on resolving fundamental problems in the network and avoids distractions.

AI/ML driven prediction engine provides advanced insights into events and alarms before they occur allowing administrators precious time to prevent or minimize the impact of the occurrence. This includes ability to predict device performance issues, bandwidth and utilization of individual ports or appliances, application, and user performance impacts.

AI driven Secure SD-NIC allows for automated operation, workflow driven troubleshooting and insights to minimize the mean time to resolution (MTTR).

Genuine Multi-Tenancy

As with the rest of Versa solutions, Versa Secure SD-NIC supports genuine multi-tenancy across all layers of the solution, at the Data Plane, Management Plane, Control Plane and Analytics.

Versa's carrier class multi-tenancy allows multiple tenants to share common infrastructure while each tenant can operate independent of each other including separate L2-L3, L4-7 functions, topologies, users and RBAC definitions. Each device that is running VOS natively can be configured to support multiple tenants, providing unmatched M&A consolidation, shared network workspace infrastructure deployment, separated critical network infrastructure for compliance and/or business continuity and criticality purposes.

Versa's multi-tenant Secure SD-NIC setup is managed by a parent tenant which is able to see and manage all tenants, while each sub-tenant will be able to see and manage only their resources. All the multi-tenancy capabilities available in Versa Secure SD-WAN, Versa Secure SD-LAN and Versa SSE solutions are available on Versa SD-NIC. For more information on Versa's market leading multi-tenancy capabilities please visit Versa's website or speak to your Versa representative.

Versa Secure SD-NIC Platform Options

Versa Secure SD-NIC solution is powered by Versa SD-NIC, a PCI based card that consists of multicore x86 processor coupled with smart NIC ASIC.

Versa SD-NIC comes so far in two flavors, CSN530 and CSN550, providing different price-performance and thermal-power combination options to our customers. In the future, additional Versa SD-NIC SKUs will be available

Versa SD-NIC Characteristics:

- Comes pre-installed with VOS, ready for ZTP.
- Full height, half-length size
- Offered in two flavors: CSN1500 and CSN1100
  - CSN550: 1x QSFP28 interface which can be split to 4x 25/10GE interfaces.
  - CSN530: 2x SFP28 interfaces
- Host facing high speed interface consists of one E810 facing host, controlled by host OS.
- Both complexes connected to each other with Built-in hardware based crypto acceleration.
- Management Ethernet – 1x 1GE port
- Management console – 1x USB3.0
- TPM2.0 and Secure Boot support
- Powered from PCI connector and additional 8-pin Aux Power connector ASIC.

Versa Secure SD-NIC Licensing Overview

The Versa Secure SD-NIC is licensed on a per use-case basis. Here are available licenses and relevant use-cases supported on Versa Secure SD-NIC:

- Versa Secure SD-WAN license based – to support deployments in remote, untrusted locations.
- Versa Secure SD-LAN license based – to support deployments in Enterprise LANs, datacenters.
- Versa NGFW, UTM license based – to support deployments in Enterprise LANs, datacenters with firewall features.
- Versa Pro-Net license based – to support deployments in Enterprise environments with router and L2 features.

Other relevant add-on licenses would also apply.

For more details on Versa Secure SD-NIC licensing or to receive a demonstration, please visit *https://www.versa-networks.com/products/sd-nic* or a Versa sales representative.