Versa Secure SD-NIC™ for Data Centers

Security postures of the past relied on the assumption that enterprise and customer data would be under externally-originated threats, so perimeter security measures were enacted to protect data centers from outside attacks. Firewalls were placed around the external access points to the data centers.

In data centers, cloud compute constructs are deployed in traditional baremetal server form or in the form of virtualized cloud infrastructure using VMware, KVM/QEMU, OpenStack and other virtualization software stack options. These compute constructs would servr workloads or applications while generally focusing on high performance and making most use of resources. Whether in baremetal form or in virtualized form of deployment, compute solutions do not offer built-in security. A VM or a workload can be brought in with malicious code which would then be running in the most sensitive area of the Enterprise, the data center. Especially in the case of VMs, there is no way to ensure that the virtual machine does not carry any malicious code. Therefore, all workloads in a data center need to be secured using zero trust principles and appropriate security functions.

Traditional virtualization solutions provide separation at the virtual switch layer using VLAN tags, and either embedded virtual router function or a dedicated router function in VM form is used in order to route between the VLANs. If the solution requires L4-7 security capabilities, then a security application must be instantiated in the form of a virtual machine or externally attached appliance. Both of these models introduce a hairpin effect.

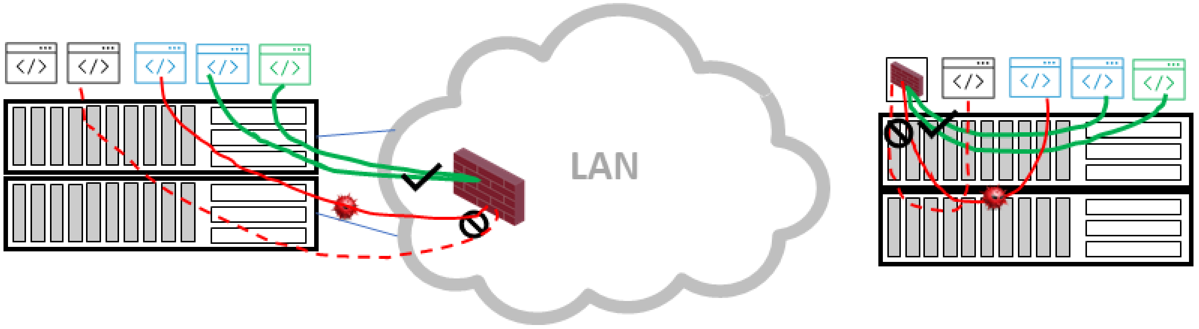

Figure 4 - Virtual Compute Security Hairpin Examples

Figure 4 demonstrates wo examples of security applied to virtual VMs. On the left, the firewall is external to the compute complex and one of the flows is blocked and the other is permitted. On the right, the firewall is a VM inside the compute complex. The figure on the left causes doubling of traffic on the network connections while the one on the right causes doubling of traffic within the virtual switching complex as well as utilizing the shared compute and memory of the compute complex to run security functions. The latter would have to be sized according to the size of traffic that needs to be secured and for several Gbps of traffic that need to be scanned, it can translate to large sized security VMs taking away valuable compute and memory capacities from the virtualized server or compute complex.

Furthermore, in today's world in which attacks and hackers becoming more sophisticated, expectations are raised. A new class of security solutions are required to provide true zero trust network access, detailed cloud access control and data leakage prevention. Traditional data center VM based on data center edge based security solutions do not provide such capabilities.

Versa is the first of its kind to address these challenges. Thanks to a rich set of native connectivity and network / data security functions in VOS, Versa customers can now enjoy fully secured network connectivity and deployments capabilities whether they are connecting to LAN or to WAN or to cloud or working from home. VOS with fully comprehensive connectivity and network, cloud resources, enterprises own data centers or for other deployment scenarios.

Versa's comprehensive network and data security capabilities allow IT and security administrators to define security functions and policies once and apply them on all VOS nodes deployed across the network uniformly.

Versa now offers the same set of comprehensive connectivity and security functions on Versa's Software Defined Network Interface Card (SD-NIC) providing additional deployment options and flexibility for IT and security administrators.

Leveraging Versa's comprehensive networking and security stack, Versa's Software-Defined Network Interface Card (SD-NIC) extends the security perimeter to within compute devices providing ZTNA, network and data security within the cloud infrastructure.

Versa SD-NIC is based on a PCI card, running VOS natively, gets inserted into standard PCI slot(s) inside the server, just like a traditional NIC expansion card. Versa SD-NIC card has a multicore processor on it which runs the Versa Operating System (VOS). With this, now Versa can instantiate a Versa SASE device within the server complex. As seen in Figure 5, the security appliance is now residing inside the server complex.

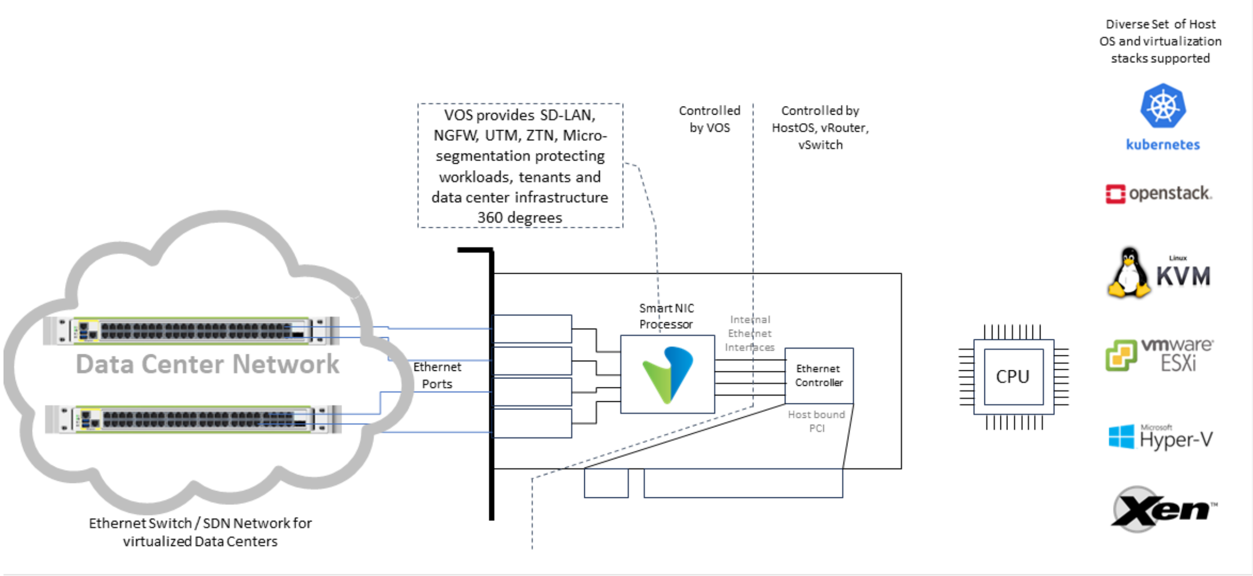
Diverse Set of Host OS and virtualization stacks supported
kubernetes
openstack.
Linux KVM
vmware ESXi
Microsoft Hyper-V
Xen
VOS provides SD-LAN, NGFW, UTM, ZTN, Micro-segmentation protecting workloads, tenants and data center infrastructure 360 degrees
Controlled by VOS
Controlled by HostOS, vRouter, vSwitch
Smart NIC Processor
Internal Ethernet Interfaces
Ethernet Controller
Host bound PCI
Ethernet Ports
CPU
Data Center Network
Ethernet Switch / SDN Network for virtualized Data Centers

Figure 5 - Software-Defined Network Interface Card

By placing the security appliance inside the server, the security posture checks, and network & data security functions get placed in the server complex in the path of the traffic without the need for sending the traffic to outside.

The Versa SD-NIC runs the same software, VoS, as with any other Versa device. Therefore, the SD-NIC has the full set of capabilities of VOS including SD-WAN, SD-LAN, Next-Gen Firewall (NGFW), Unified Threat Management (UTM), Zero-trust Network Access (ZTNA), micro-segmentation, Cloud Access Security Brokerage (CASB), Network based Data Leakage Prevention (DLP) and more. VOS is application-aware which allows for different security postures per application, segment, user, or device.

Among rich of features, we anticipate ZTNA to be utilized to provide access control to/from the network to the compute-based workload or application under strict policy guidance, and based on dynamically assessed security posture. Versa's ZTNA solution assesses the security posture of the guest OS by factoring in variety of parameters including OS details, whether any security package is used within the guest VM, if other security best practices have been implemented or not. VOS's native ZTNA capabilities can be configured in full (forward or reverse) proxy mode to terminate user or server-initiated sessions / flows to scan them using rich set of NGFW, UTM, SWG, ATP functions looking for malware or any other suspicious activity. Furthermore, VOS can be configured to provide detailed access control using built-in inline CASB functions and to scan for data for DLP purposes.

VOS would natively integrate with popular data center SDN stacks to provide VXLAN based overlay connectivity across the data center environment. Lastly, traffic to/from workloads can be micro-segmented based on dynamically assessed security posture, application, user or other parameters. Such rich set of connectivity functions would give ultimate deployment flexibilities in brownfield deployments with no change in host OS or data center software.

As demonstrated by Figure 6, the Versa SD-NIC alleviates the issues of complexity by being natively in the line of communication, eliminating the need for complex traffic forwarding paths and by relieving compute and memory being used for networking and security functions, it opens up more capacity for the workloads. Furthermore, Versa SD-NIC solution reduces the traffic load on the network connection.

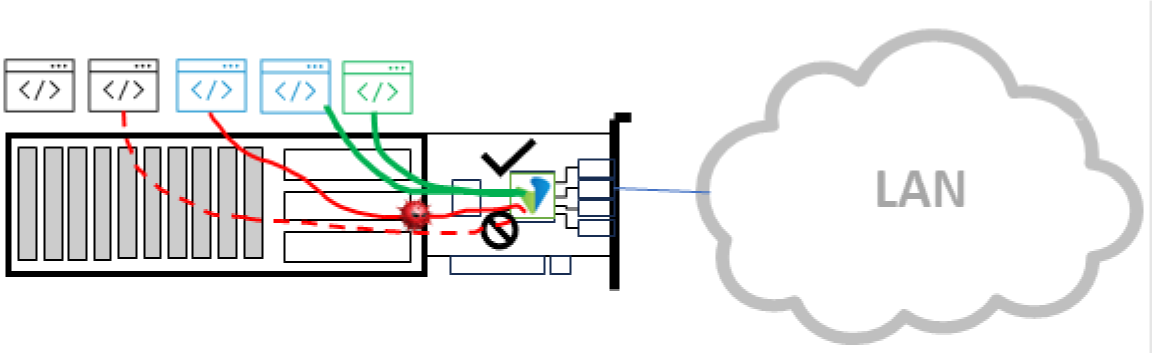

Figure 1 - SD-NIC Security Single Compute Complex

VOS running SD-NIC comes with its dedicated memory and compute. This enables the server to secure traffic in the east west direction between VLANs and workloads without utilizing compute complex resources nor sending the traffic external to the server complex. This figure assumes that all the applications and traffic are contained within a single server. However, modern compute complexes consist of many servers interconnected with virtualization software.

As seen in Figure 7, the Versa SD-NIC can be installed into all the servers, if desired with more than one SD-NIC card, and secures traffic even within the same VLAN if on different physical servers.

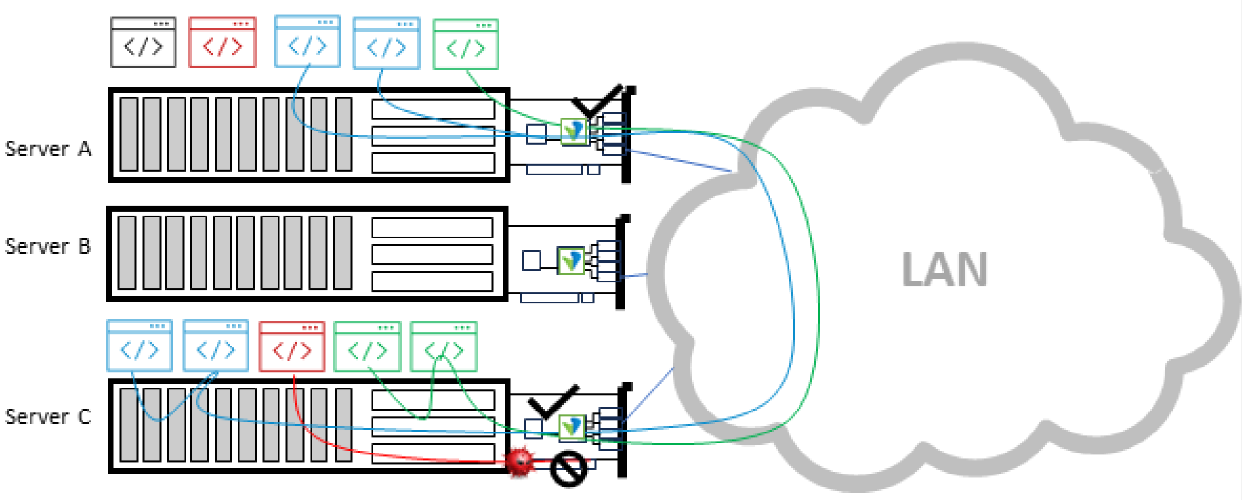

Figure 7: SD-NIC Security (Multiple Compute Complexes)

Notice that the virtual machines in the green and blue segments on server A successfully send traffic to the intended virtual machines in the respective green and blue segments on Server C. In this setup, the traffic is validated at two different points utilizing the SD-NIC, one in server A and the other in server C. However, the virtual machine in the red segment on server C has been stopped from transmitting malware to a virtual machine in the red segment on Server A. This differs from traditional data center design where an authentication/authorization and VM onboarding decision would be made for each VM without any natively built-in ZTNA, network or data security capabilities.

Since the Versa SD-NIC has its own CPU, memory, and storage, this SD-NIC can be installed into hardened devices where a traditional software agent would not be allowed. There is no dependence on the compute software. If the server allows for the PCI card to be installed, then the Versa device can secure the traffic. Additionally, the SD-includes a Trusted Platform Module (TPM) 2.0. This enables the server to recognize the SD-NIC as valid and allows the SD-NIC to securely connect to the enterprise network. Additionally, the SD-NIC can be configured to use the TPM chip of the server to create a secure authentication relationship between the server and the SD-NIC. This would prevent lateral movement of the SD-NIC from one server complex to another.

Furthermore, since the Versa appliance is now installed into the compute device, the design solution no longer requires extra space, power, nor additional cabling requirements. Thus, this reduces the physical footprint needed to support the compute, network, and security devices.

Traditionally, security appliances require one set of management tools and routers and switches require another set of management tools, perhaps even a different management tool set per vendor. Increased set of management tools implies that the security policies need to be configured separately in each of the management tools, and when changes are made to the security policies, this needs to be replicated to all the different management tools. Since the SD-NIC runs VOS natively, the Versa SD-NIC does not require any additional management tools if the customer already deployed Versa solution in any part of their network.

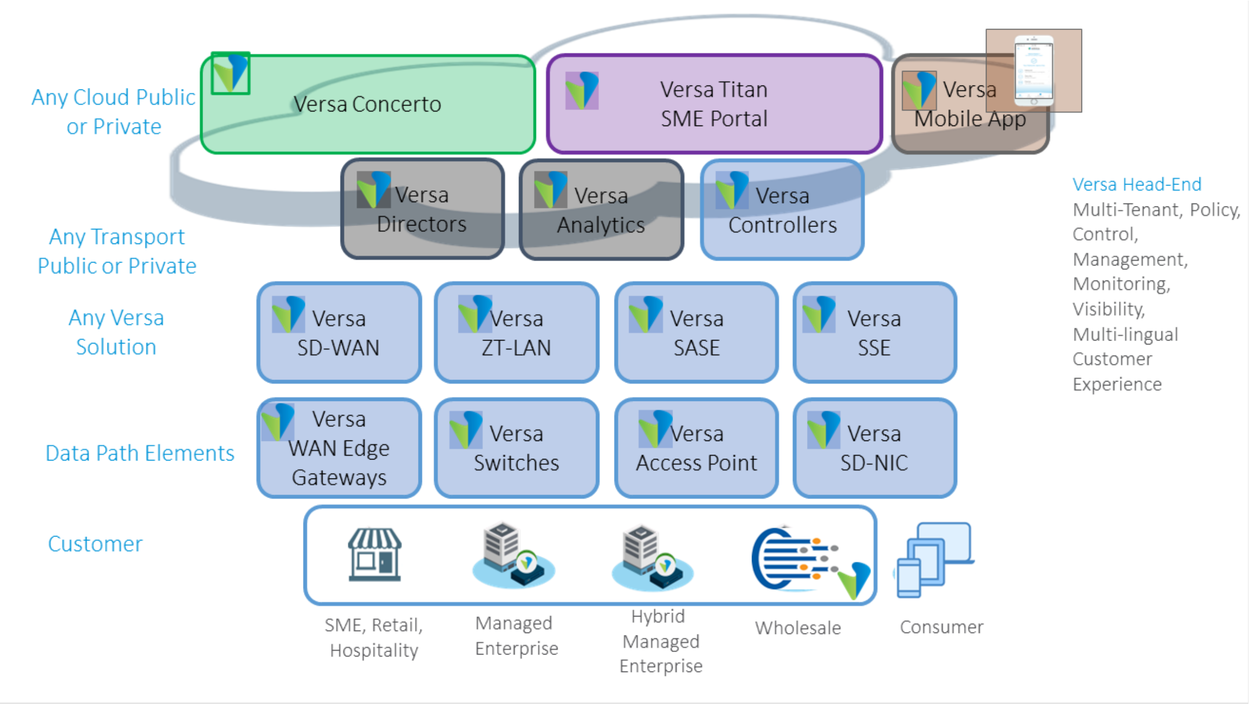

Figure 8 - SD-NIC and Versa Solutions

As seen in Figure 8, the Versa management is centralized and controlled by the Versa Director, Concerto and Controllers. Additionally, the information data store is centralized in the Versa Analytics. This centralized management design allows for security policies to be applied uniformly across VOS instances across the network and on the cloud to deliver SD-WAN, SD-LAN, ZTNA, SASE and SSE. Utilizing the Versa SD-NIC, these security policies extend into the compute server and IOT devices.

The Versa SD-NIC utilizes the same Zero Touch Provisioning (ZTP) mechanisms that any VoS device utilizes. The ZTP process utilizes security mechanisms to assure that the appropriate device connects to the appropriate service before any configuration can be applied to the SD-NIC. The Versa SD-NIC has the capability to perform a Secure Boot. Secure Boot utilizes keys stored in on the SD-NIC to validate that the bootable image is a trusted image and from a trusted source.

The Versa SD-NIC is available in two different configurations today. The first is a 2x25G/10G interface card. This provides for approximately over 10 Gbps throughput with advanced security and micro-segmentation functions enabled, making it suitable for use-cases that do not need as high performance.

The second SKU is a 1x100G which is capable of 4x25G/10G breakout which provides throughput of over several 10s of Gbps of advanced security and micro-segmentation performance.

Our customers can deploy multiples of these cards in each server.

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