SOLUTION BRIEF

Universal Customer Premises Equipment
Software Defined WAN (SD-WAN)

Enea, Intel Showcase Firewall-Protected Open Source SD-WAN

Pioneering reference solution combines open source SD-WAN and firewall software on an Intel® architecture-powered uCPE using Enea NFV Access for virtualization.

Software defined wide area network (SD-WAN) services have become vitally important for enterprises, allowing them to re-configure their branch office networks to take advantage of cloud-based services. With SD-WAN, branch offices can use legacy WANs to access corporate resources and can have more secure access to cloud-based applications across broadband internet services.

The availability of open source SD-WAN software takes advantage of the rapid innovation and lower cost of open source options when compared to commercial offerings.

In a reference solution showcased at the SDN NFV World Congress 2019, a coalition of companies led by Enea AB and Intel demonstrated how a robust open source SD-WAN system by flexiWAN could be developed and deployed by communications service providers (CommSPs) or enterprises. As universal customer premises equipment (uCPE)-based SD-WANs are deployed globally, service providers are looking for solutions that are more affordable, yet customizable while offering scale and robustness. Solutions such as the one detailed in this brief allow service providers to take SD-WAN into new price-sensitive markets while leveraging their existing infrastructure.

Reference Solution Description

SD-WAN services disrupted the WAN connectivity market, and the availability of open source SD-WAN software is equally disruptive as it provides a customizable solution and changes the price point of these services when compared to a solution using a commercial SD-WAN.

In this reference solution, an Intel® architecture-based uCPE from Lanner with Enea NFV Access virtualization platform was configured with flexiWAN open source SD-WAN software and an open source firewall using pfSense software. Two different white box uCPE configurations were used—each with different processor resources, RAM, and hard disk options in order to demonstrate the functionality and scalability of the overall solution.

The reference solution components included the following hardware and software:

Enea NFV Access
Enea NFV Access is a complete virtualization platform with a small footprint that is designed for uCPE deployment. In the demo, for example, Enea NFV Access needs only one core and less than 1.5 Gbps of RAM after creating the bridges but before deploying any VNFs. This light footprint leaves the remaining resources available for the applications.

The software supports both network functions virtualization (NFV) virtual network functions (VNFs) or containerized VNFs. Figure 1 shows a block diagram of the platform including its system management, virtualization/containerization layer, virtual switching, data path acceleration, and security.

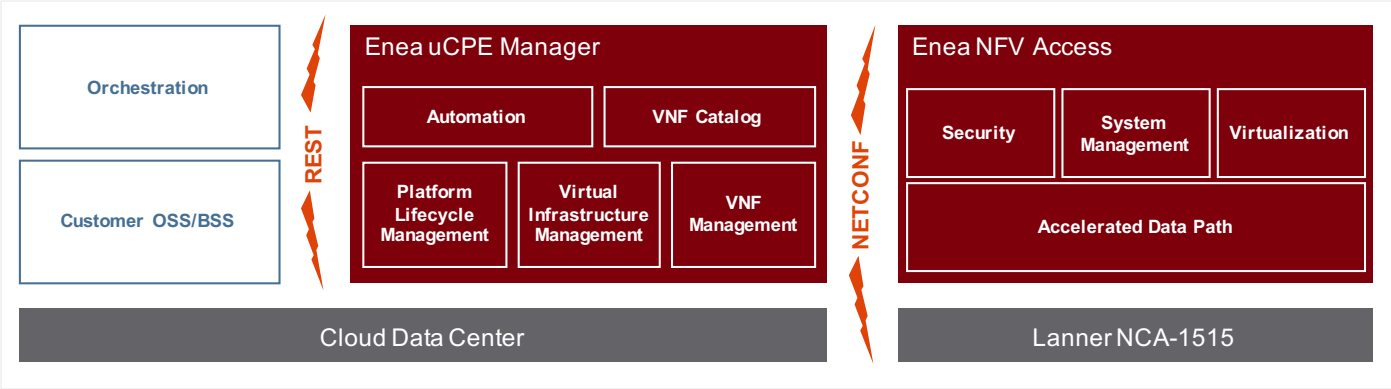

Figure 1. Enea NFV Access block diagram.[1]

The universal design of Enea NFV Access supports all VNFs, can work with any orchestrator, and can utilize all Intel architecture server CPUs. Remote VNF deployment is simplified using the onboarding wizard, which orchestrates the resources required to install the software.

Management of both uCPEs and VNFs is an important component of an SD-WAN solution. Enea NFV Access includes the Enea uCPE Manager, a virtualized infrastructure manager (VIM) and VNF manager that manages the uCPE and the lifecycle of the VNFs using NETCONF/YANG. The Enea uCPE Manager provides remote management for small and large network sizes. The uCPE Manager also integrates with third-party orchestrators using REST APIs and can utilize multi-VIM orchestrators for integration with OpenStack or VMware.

NETCONF/YANG makes it possible for the management components to take up far less resources on the uCPE compared with OpenStack and other management frameworks. This is an important part of reducing the footprint to allow cost-efficient white box hardware.

flexiWAN SD-WAN

flexiWAN is an open source VNF that supports SD-WAN routing of data flows either on legacy WANs, broadband services, or 4G/5G wireless connections. flexiWAN also has network management, orchestration, and automated deployment capabilities.

Integration points have been built into flexiWAN so that CommSPs or enterprises can modify the core SD-WAN functionality to add or expand features to optimize traffic flows or provide unique data security features.

As seen in Figure 2, the flexiWAN solution comprises flexiEdge software that runs on a uCPE in a branch office and provides routing and SD-WAN services. flexiEdge can also be installed in the cloud for cloud-to-enterprise connectivity or service delivery by CommSPs. The centralized flexiManage software manages all of the flexiEdge instances and provides configuration, provisioning, software upgrade, and orchestration of flexiEdge devices and applications.

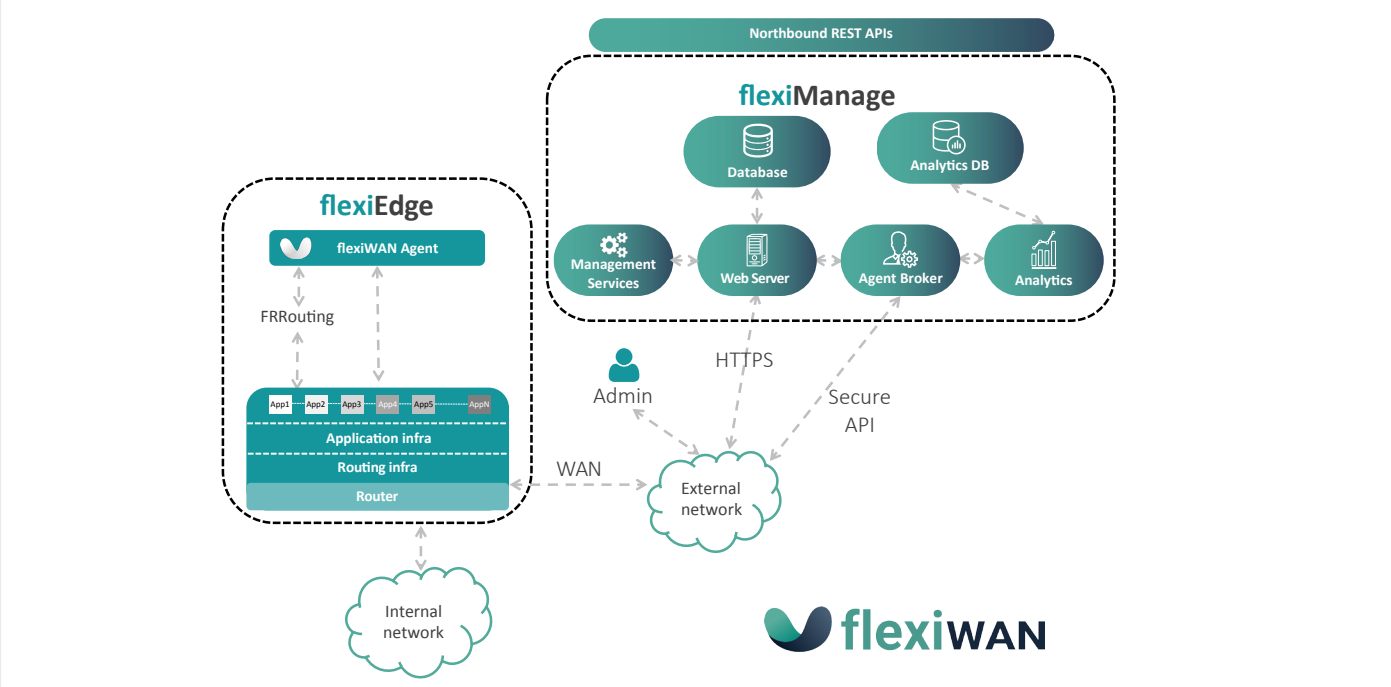

Figure 2. flexiWAN SD-WAN architecture including the flexiEdge and flexiManage software.[2]

pfSense Firewall
For firewall security, the demo featured the free and open source pfSense, which can operate as a stateful packet filtering firewall or as an IP router for LAN or WAN applications. Other pfSense features include:

- Routing policy per gateway and per-rule for failover and load balancing
- Transparent layer 2 firewall
- Support for IPv6, network address translation (NAT), BGP routing
- Captive portal with MAC filtering, RADIUS support
- IPsec, OpenVPN, and L2TP VPNs
- Dynamic DNS client
- Reporting and monitoring features with real-time information

For the reference solution, the software was configured as a firewall.

Lanner NCA-1515 uCPEs
The white box uCPEs used in the reference solution are from the Lanner NCA-1515 series of networking servers—purpose-built for branch office and access deployments. Lanner has designed these servers to be future ready for additional VNFs. The reference solution was built to demonstrate both the minimum and ideal configurations.

The Lanner NCA-1515B server was selected to show the minimum configuration necessary for a cost-effective solution that would host just the secure SD-WAN. The NCA-1515B is based on the four-core 2.2 GHz Intel Atom® C3558 processor. The NCA-1515B has a 64 GB SSD and 8 GB of RAM. The ideal uCPE configuration was represented by the NCA-1515A, which uses the eight-core 2.2 GHz Intel Atom C3758 processor with 128 GB SSD and 16 GB of RAM.

While not used in the demonstration, both CPUs feature Intel® QuickAssist Technology (Intel® QAT) that can be activated for applications that need accelerated encryption and decryption, which improves the performance of data security applications. Lanner also incorporates Intel-developed open source technologies that can improve VNF performance. These include the Data Plane Development Kit, a set of data plane libraries for fast packet processing, and single root input/output virtualization (SR-IOV), which provides a direct connection between a VNF and a PCI Express resource such as a network interface.

Putting It All Together

Figure 3 is a block diagram of the systems used in the reference solution. The reference solution mimicked a connection between two branch offices with data traffic flowing between the LAN and the WAN, with Enea NFV Access creating a service chain that helps ensure that all data passes through the firewall before being processed by the SD-WAN. The service chain is based on DPDK accelerated Open vSwitch for very high VNF-to-VNF throughput.

The reference solution also highlights a secure zero touch provisioning (ZTP) connection over NETCONF (RFC 8071) and in-band management using the WAN connection for management for easy deployment.

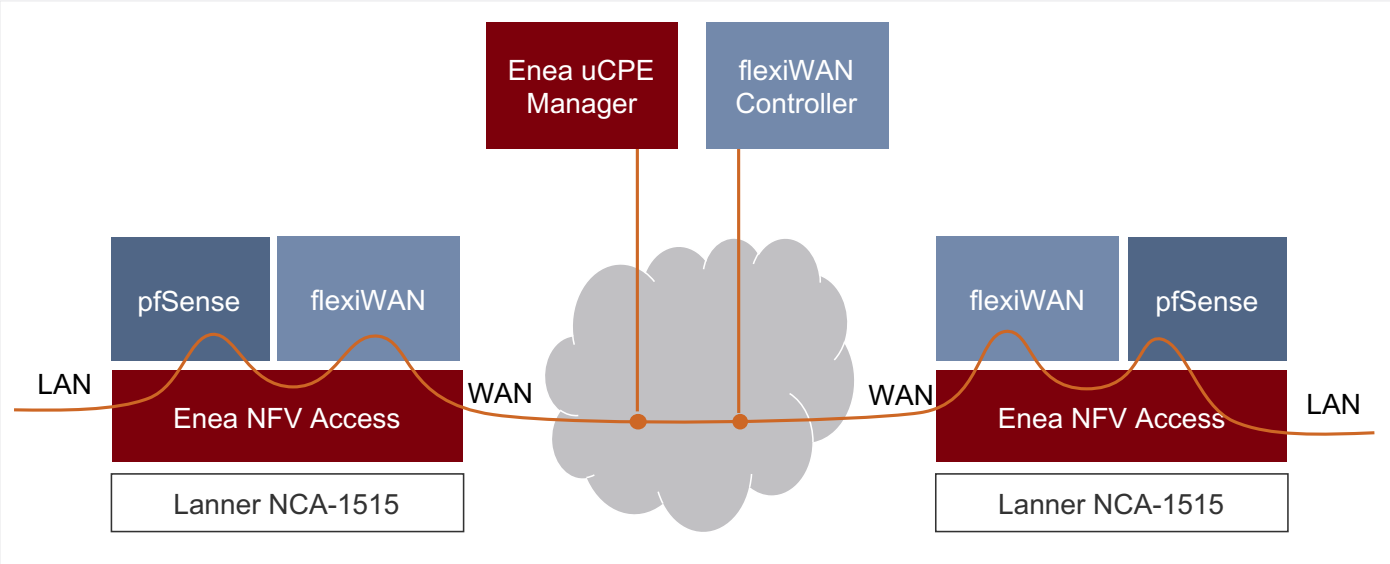

Figure 3. Reference solution system block diagram.

Figure 4 shows the scalability of the minimum and ideal uCPE configurations. With only four cores, the Lanner NCA-1515B can support only the firewall, SD-WAN, and virtualization layer software. This server is a good option for applications that are cost-competitive and it still has remaining RAM and SSD capacity for these services.

The use of NETCONF/YANG makes it possible for the management components to take up far less resources on the uCPE compared with other management frameworks. This is an important part of reducing the footprint to allow cost-efficient white box hardware.

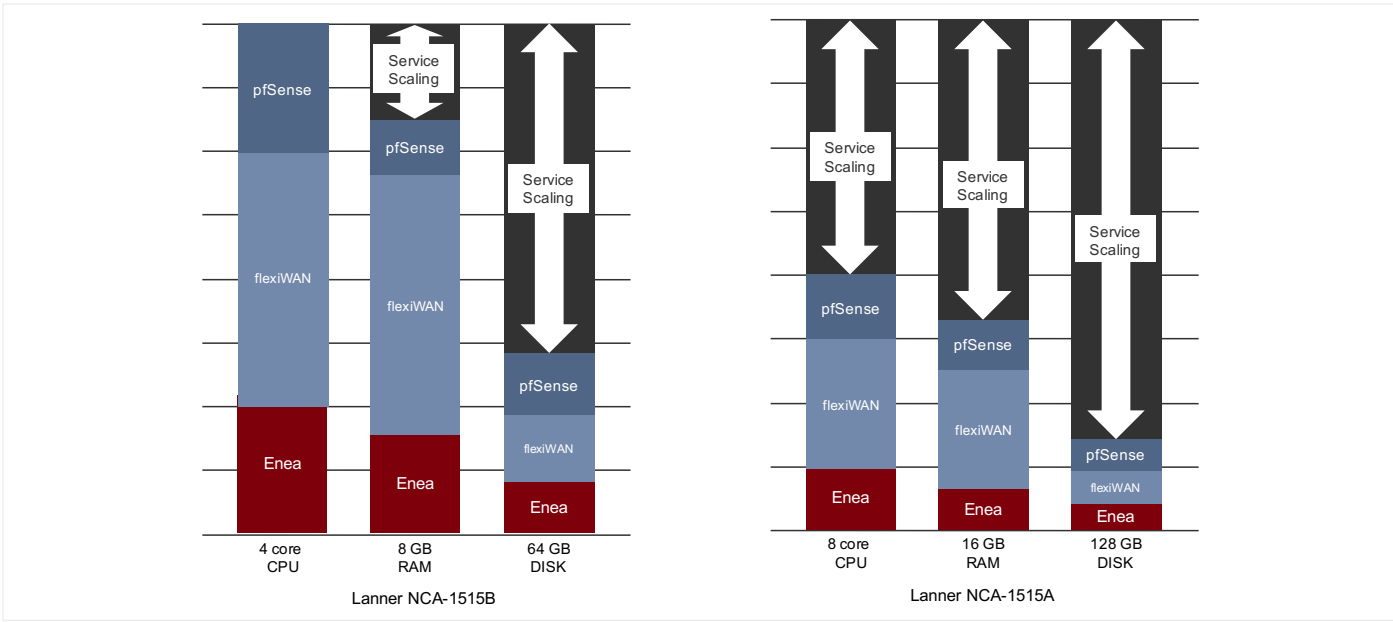

Figure 4. Comparison of resources available on two Lanner uCPE platforms for scaling the open-source, firewall-protected SD-WAN application.

The configuration based on the Lanner NCA-1515A is the ideal configuration of the service deployment as the eight cores can easily accommodate the reference solution's VNFs with four unused cores for other VNFs or to expand the cores assigned to the SD-WAN or firewall to help improve performance. This platform has a significant amount of RAM and disk space expandability.

Conclusion

The reference solution showcases two deployment modes for an open source firewall-protected SD-WAN solution. The reduced cost and customization potential of the open source solution is enhanced by Enea NFV Access, which provides virtualization using minimal uCPE resources. The solution showed this using a four-core uCPE as a minimal configuration to deliver the ultimate value service. The same small footprint provides value in a more powerful uCPE because it can support the secure SD-WAN with capacity for additional services.

For More Information

Enea and Lanner are members of the Intel® Network Builders Ecosystem: networkbuilders.intel.com

The Intel Atom® processor family: www.intel.com/atom

Enea NFV Access: www.enea.com/products/nfv-virtualization-platforms/enea-nfv-access

Lanner NCA-1515 Products: www.lannerinc.com/products/network-appliances/x86-desktop-network-appliances/nca-1515

pfSense: www.pfsense.org

flexiWAN: flexiwan.com

[1] Figures 1, 3, and 4 provided courtesy of Enea.

[2] Figure provided courtesy of flexiWAN.