White Paper

Universal Customer Premises Equipment

NEXCOM and Enea Test Open Source flexiWAN SD-WAN and pfSense Firewall

Companies team with Intel, flexiWAN, and pfSense to test enterprise edge/uCPE systems with Intel Atom® processor or Intel® Xeon® D processor; results[1] show up to 200 Mbps WAN speed for small-to-medium-sized branch offices.

The growth in cloud computing has significantly changed the networking needs of small- and medium-sized branch offices. Once content to leverage multiprotocol label switching (MPLS) connections to access email, databases, and other resources from corporate data centers, enterprise users now need additional connection types, such as broadband access and 4G/5G wireless, to address their need for higher data rates and diverse traffic patterns. Branch office workers use cloud-based email services, edge cloud based communications systems, and more. Companies are moving to software-defined WAN (SD-WAN) solutions for branch offices because these solutions enable both MPLS and more secure IP-based connectivity.

SD-WAN solutions are virtualized and run on Intel® architecture-based servers. SD-WAN solutions come from many vendors, but are also available in robust open source virtual network functions (VNFs) that will perform well in branch office settings with fewer than 10 users and up to several hundred users. Open source software is typically less expensive because the cost structure of open source companies usually requires less investment in sales, but IT managers have questions about how well these solutions perform. The benchmark test results[1] in this paper demonstrate that these solutions can deliver the performance needed for offices with up to several hundred employees.

An ideal open source solution features the ability to use the same software stack on hardware with multiple cost points. This can allow for a lower-cost server to reduce the cost for smaller branch offices, with the same functionality being deployed in a higher-performance system for larger offices that have higher data volumes.

Intel® Network Builders ecosystem partner NEXCOM teamed up with NFV infrastructure software company Enea to develop a test to show SD-WAN throughput for a low-cost server based on an eight-core Intel Atom® processor and a higher-capacity server based on a 14-core Intel® Xeon® D-2177 processor. The companies selected flexiWAN's open source SD-WAN software to provide the routing functionality. Recognizing the importance of network security at all branch offices, the companies added an open source firewall from pfSense to the test to determine its impact on data throughput.

Table of Contents

Branch Office SD-WAN Configurations

Two servers were used in the tests, each with different capacity and cost. The NEXCOM TCA 5170B uCPE server is a 1U rackmount form factor based on a 14-core Intel Xeon D-2177NT processor. It is designed for high performance virtualized and non-virtualized (bare metal) services at small branch offices and small-to-medium-sized businesses.

Intel Xeon D-2100 processors bring the architectural innovations of the Intel Xeon Scalable platform to a system-on-a-chip (SoC) processor for lower-power, high-density solutions, integrating essential network, security, and acceleration capabilities. For uCPE workloads like the ones in this test, the Intel Xeon D-2100 processors support Intel® Advanced Vector Extensions 512 (Intel® AVX-512) and Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI).

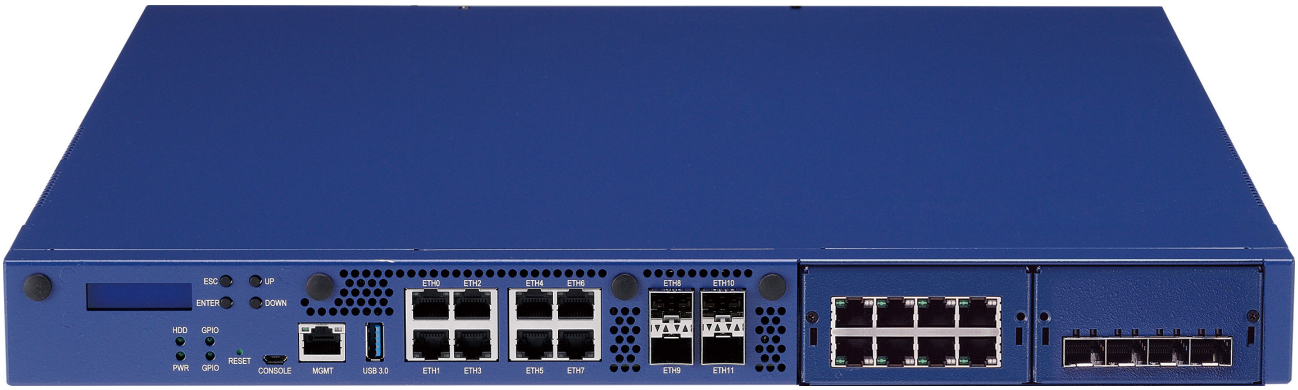

Figure 1. NEXCOM TCA 5170B

The server is a verified Intel® Select Solution for uCPE, which means it is optimized for uCPE applications.

The NEXCOM TCA 5170B comes with eight 1 GbE ports and four SFP+ ports for 10 GbE connections. Via built-in M.2 connections, the TCA 5170B provides LTE and Wi-Fi wireless connections. It also supports PCIe x16 or x8 SFP interfaces for backbone LAN connections up to 100 GbE.

When needed for heavy encryption workloads, the TCA 5170B can utilize built-in Intel® QuickAssist Technology (Intel® QAT), which accelerates encryption/decryption so as to free up the CPU for other tasks. The TCA 5170B supports the Intelligent Platform Management Interface (IPMI 2.0) for system monitoring by third-party software.

The other server used in the test was NEXCOM's DTA 1160, which is a desktop appliance featuring an eight-core Intel Atom C3758 processor. This CPU is designed for a variety of light scale-out workloads that require very low power, high density, and high I/O integration, including on-premises uCPE featuring routing, switching, data security, dynamic web serving, and more. The Intel Atom C3000 processor is Intel's third-generation system-on-a-chip based CPU manufactured on Intel's optimized 14 nm process technology.

This desktop uCPE supports up to 64 GB of DDR4-2400 RAM and has two 10 GbE SFP+ ports and six 1 G RJ45 ports. For storage, the uCPE supports a 2.5" internal SSD that is optional, one SAA connector, or one M.2 SSD socket supporting either SATA or NVMe drives.

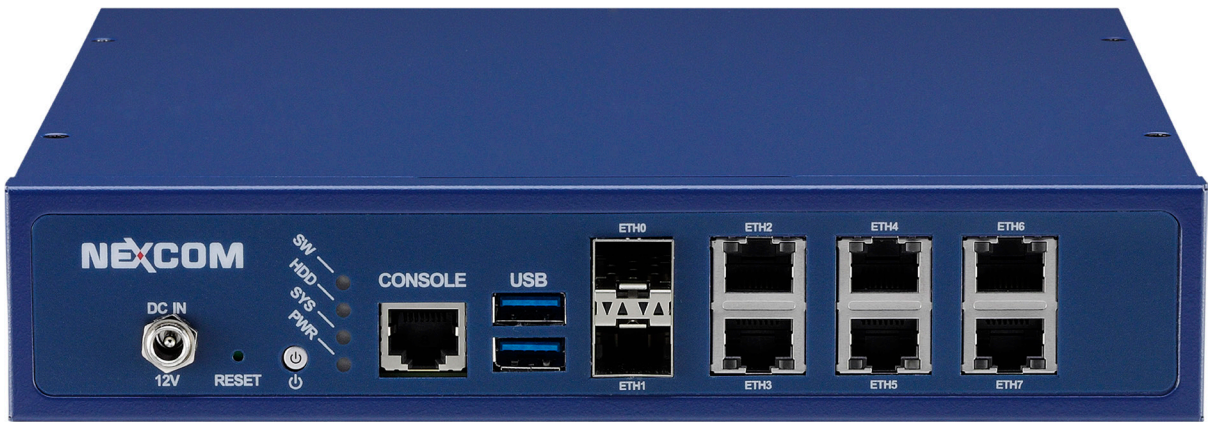

Figure 2. NEXCOM DTA 1160

Enea NFV Access

Enea has designed the Enea NFV Access as virtualization infrastructure platform for uCPE deployment (see Figure 3). It features a small footprint with a complete feature set for both virtual network functions (VNFs) or containerized network functions (CNFs). Some key functions include system management, virtualization and containerization layer, virtual switching, data path acceleration, and security.

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.

Figure 3. Block diagram of demonstration setup including Enea NFV Access Platform as the provider of all network functions virtualization infrastructure (NFVI)

flexiWAN SD-WAN

flexiWAN is an open source VNF that supports SD-WAN routing of data flows as well as network management, orchestration, and automated deployment capabilities. flexiWAN slices SD-WAN to horizontal layers that include a networking infrastructure layer and an application framework. Through an SDK, networking applications can be dynamically loaded to the flexiEdge router or flexiManage central cloud management. This allows CommSPs or enterprises to modify the core SD-WAN functionality, add or expand features to optimize traffic flows, or provide unique data security features.

Figure 4 shows the software components of the flexiWAN solution, including the 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.

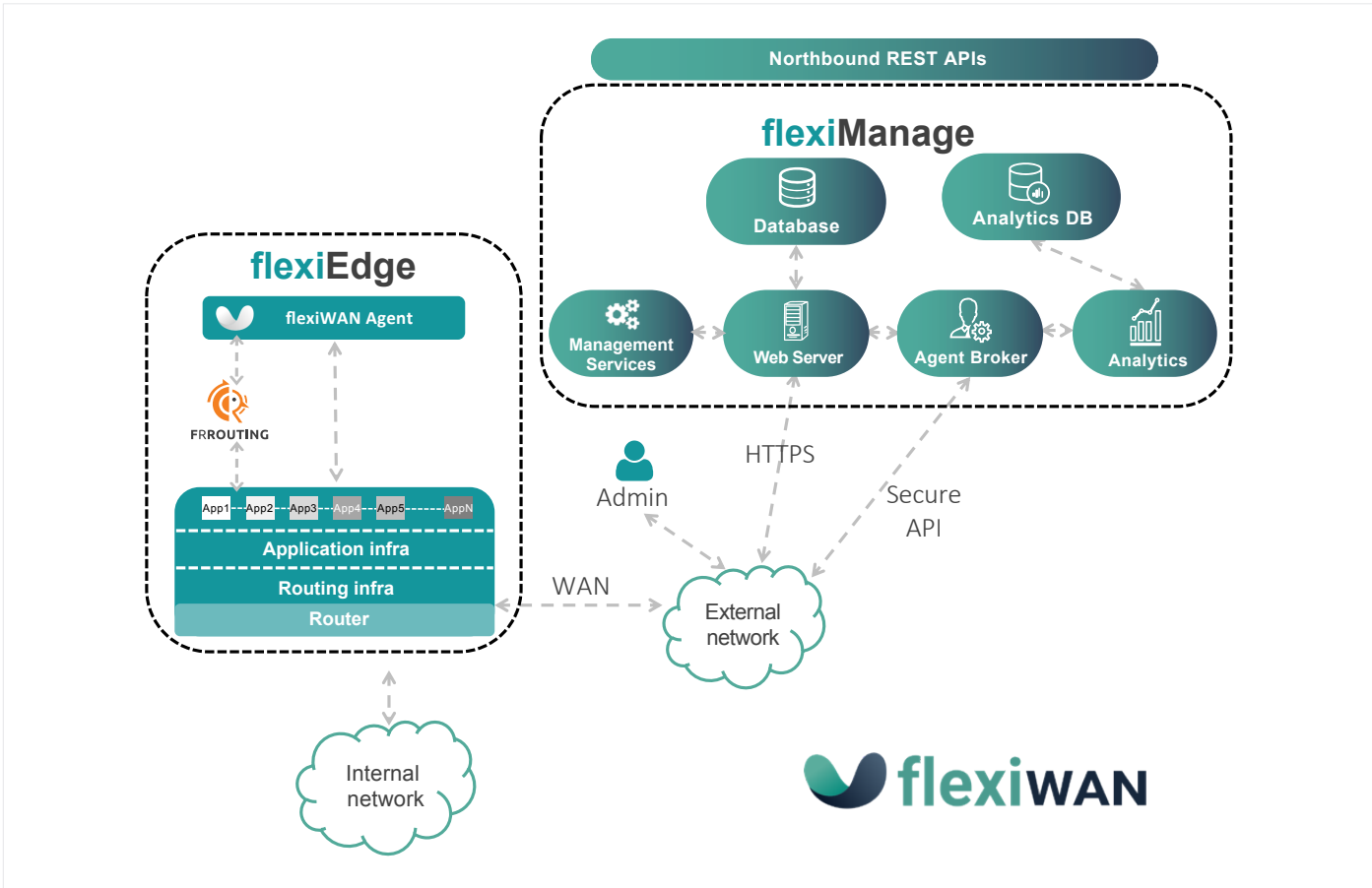

Figure 4. flexiWAN SD-WAN architecture, including the flexiEdge and flexiManage software

pfSense Open Source Virtual Firewall

pfSense is an open source dedicated firewall/router that is functionally competitive with proprietary commercial firewalls. It can be configured as a stateful packet filtering firewall, a LAN or WAN router, VPN appliance, DHCP server, DNS server, or can be configured for other applications and special purpose appliances. pfSense is entirely managed via a web interface and is upgradeable via a package system designed to allow end user expandability without adding additional code that can result in security vulnerabilities to the base distribution.

pfSense security appliance features include the following:

- Stateful packet filtering firewall or pure router
- Routing policy per gateway and per-rule for multiple WAN, failover, load balancing
- Transparent layer 2 firewall
- Support for IPV6, NAT, BGP
- Captive portal with MAC filtering, RADIUS support, etc.
- VPN supporting IPsec, OpenVPN, PPTP
- Dynamic DNS client
- DHCP server and relay functions
- PPPoE server
- Reporting and monitoring features with real-time information
- IoT gateway/security endpoint
- Network tap
- IPMI/BMC firewall

Performance Test Configuration

The tests[1] were designed to measure HTTP/HTTPS throughput and also the number of connections that each NEXCOM server was able to sustain. Both NEXCOM servers had the same software configuration that included dedicating four cores to Enea NFV Access and two cores each to flexiWAN and pfSense. This software stack used up all eight cores available in the Intel Atom processor-based DTA 1160 server, which is targeted at smaller branch offices. The Intel Xeon D processor-powered TCA 5170B has 14 cores, so it can run the entire secure SD-WAN software stack and have compute available for other services. In both tests, the flexiWAN VNF was allocated a single CPU core.

The traffic flow was set up to simulate HTTP web traffic similar to a branch office user clicking on a website or web-enabled cloud service. GET commands for data were configured for a set number of data file sizes ranging from 1 KB to 37 KB. Traffic was generated by increasing the desired throughput over a span of 60 seconds until errors occurred. Performance measurements were based on application layer (L7) analysis—rather than IP / MAC layer (L2/L3) benchmarks—in order to best emulate the user experience.

The data flow for the test is shown by the red line in Figure 5. Packets were generated by a TRex Advance Stateful Feature Sets (ASTF) traffic generator connected to the DUT via a 10 GbE network connection. Once at the server, the packets were processed by the pfSense firewall, which created routes inside the default routing table and applied rules for passing IPv4 traffic. The firewall then forwarded the packet to flexiWAN for routing through an IPsec tunnel across a simulated 10 Gbps WAN connection to be terminated by the flexiWAN instance in DUT 2 and then counted by the TRex ASTF.

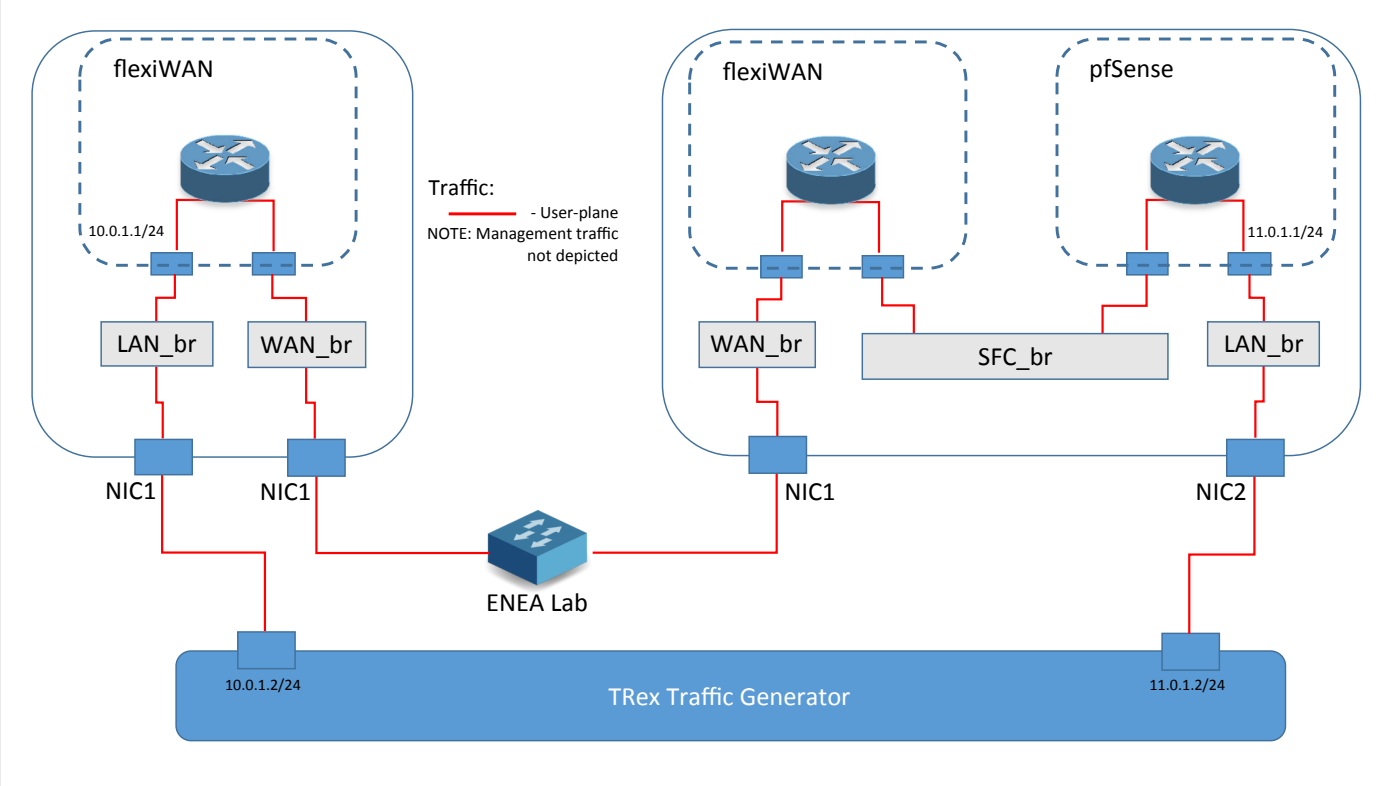

Figure 5. Service chain for test of SD-WAN and firewall services

Both NEXCOM servers were used as the DUT (Figure 5 right hand side) to show the performance difference, while DUT 2 (Figure 5 left hand side) was a FWA3050 CAR-5040 server powered by an 8-core Intel Xeon D-2145NT processor and didn't influence the performance of the DUT.

The tests measured HTTP/HTTPS throughput in megabits per second. Table 1 shows the HTTP results for the DTA-1160.

GET RESPONSE	THROUGHPUT (MBPS)	CONNECTIONS PER SECOND
1 KB	144	8,000
4.5 KB	196	4,000
10 KB	255	2,500
19 KB	305	1,700
37 KB	300	900

Table 1. DTA 1160 HTTP performance

The HTTP results show that even with the smallest data file size, the SD-WAN system can deliver more than 100 Mbps of WAN throughput, which meets the needs of most small branch offices.

Performance of the pfSense firewall is shown as connections per second—a measurement of how quickly the firewall can evaluate a data request against a firewall policy and then set up a connection. Using a rule of thumb of an average of three connections per user, the performance of the DTA-1160 supports up to 300 users at the largest GET file size.

GET RESPONSE	THROUGHPUT (MBPS)	CONNECTIONS PER SECOND
1 KB	215	4,000
4.5 KB	207	2,400
10 KB	278	2,000
19 KB	298	1,400
36 KB	315	870

Table 2. DTA 1160 HTTPS performance

Table 2 shows performance of HTTPS traffic on the DTA-1160. Although the GET sizes were different (all GET sizes were determined by the TRex ASTF), performance was slightly better with equivalent GET file sizes. The full impact of the HTTPS encryption/decryption was felt in the connections per user, which were halved at the 1 KB file size and dropped 3.4% at the 36 KB file size. The performance, though, is still adequate to support about 300 users using the industry rule of thumb.

Table 3 shows the same HTTP measurements for the Intel Xeon D processor-based TCA 5170B:

GET RESPONSE	THROUGHPUT (MBPS)	CONNECTIONS PER SECOND
1 KB	190	10,500
4.5 KB	290	5,900
10 KB	352	3,500
19 KB	322	3,500
37 KB	340	950

Table 3. TCA 5170B HTTP performance

The more powerful processor adds significant throughput for the 1 KB GET compared to the DTA 1160 and provides significant improvement in CPS. These performance indicators show that the TCA 5170B can meet the needs of larger offices. Same is true for HTTPS performance levels, which are shown in Table 4.

GET RESPONSE	THROUGHPUT (MBPS)	CONNECTIONS PER SECOND
1 KB	295	5,500
4.5 KB	215	2,500
10 KB	330	2,400
19 KB	310	1,450
36 KB	340	1,000

Table 4. TCA 5170B HTTPS performance

These results demonstrate that the DTA 1160 and TCA 5170B are market-ready solutions that support the throughput and CPS performance needed for small branch offices with up to 300 employees. And while these test results are focused on performance, the solutions are pre-integrated and tested for easy deployment and configuration.

Conclusion

Open source SD-WAN and firewall services are a very cost effective way to build out a branch office network. NEXCOM provides these capabilities pre-integrated on its Intel architecture-based servers, making it no more work to deploy than commercially provided alternatives. With Enea NFV Access, orchestration and life cycle management can be done remotely, simplifying deployment and administration of the largest networks.

With the Intel Atom processor-based DTA 1160 and the Intel Xeon D processor-based TCA 5170B, NEXCOM has provided solutions at two price points that should economically serve small- and medium-sized offices. These results demonstrate that the DTA 1160 and TCA 5170B are market-ready solutions that support the throughput and CPS performance needed for small branch offices with up to 300 employees. The flexibility and performance of these solutions are combined with future-ready flexibility, which allows IT staff to utilize the same infrastructure for other services in the future if desired.

For More Information

Enea and NEXCOM are members of the Intel® Network Builders ecosystem

Enea NFV Access

NEXCOM homepage

NEXCOM TCA 5170B

NEXCOM DTA 1160

flexiWAN

pfSense

0121/DO/H09/PDF ♻ Please Recycle 345785-001US