White Paper

Server-Based IPsec for Cloud & Telecom Providers

Prepared by

Gabriel Brown
Senior Analyst, Heavy Reading
www.heavyreading.com

on behalf of

www.6wind.com

www.hpe.com

March 2016

IPsec & the "Network Cloud"

IPsec is an important security technology for virtually all communications service providers. It is used to create secure tunnels between trusted endpoints for a wide variety of applications, from high-throughput data center interconnects to enterprise VPN, mobile backhaul and per-user services with high session setup rates. In larger networks and more demanding applications, IPsec is typically supported on specialist gateways optimized for packet processing and hardware-based encryption. Software-only solutions typically serve smaller-scale use cases where performance density is less critical.

There is now an opportunity to create competitive IPsec gateway products on general purpose x86 servers using software from independent vendors. These deployments can scale according to the required number of processor cores, making it possible to efficiently address very high-performance applications in large, sophisticated networks, as well as to optimize for a smaller-scale use cases. The aim is to take advantage of high-volume server economics – and ultimately the "service agility" associated with network functions virtualization (NFV) – to offer IPsec gateway solutions at substantially lower cost than today's specialist hardware products.

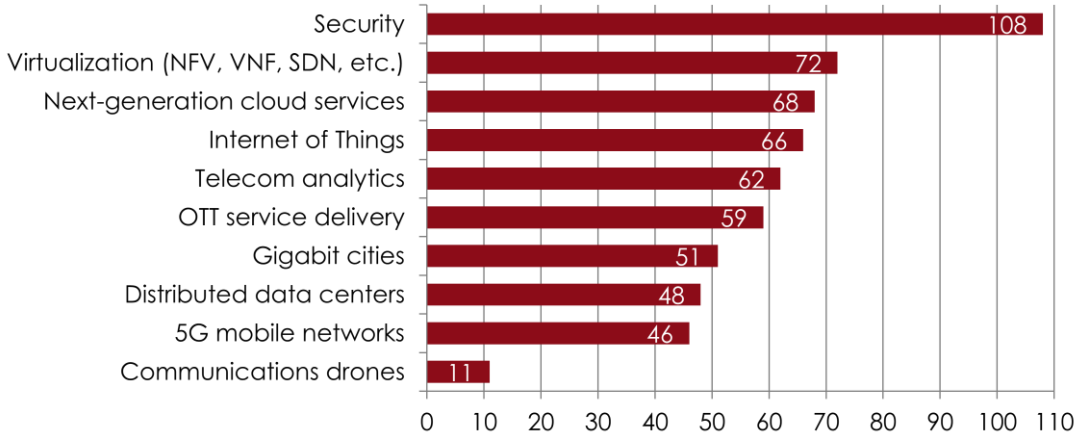
This white paper discusses emerging use cases for server-based IPsec gateways and highlights recent test data that shows 144 Gbit/s of throughput is possible on Hewlett Packard Enterprise (HPE) ProLiant DL580 four-socket Gen8 and Gen9 servers running Intel Xeon Processors, 6WIND Turbo IPsec deployed in virtual machines (VMs) and 6WIND Virtual Accelerator software in the hypervisor.

Security Is the Long Pole in the Tent

Security has always been important to service providers. The IP-era introduced many new concerns that the industry is, arguably, still coming to terms with. In recent years, as more services move to IP and the cloud, the profile of security and its importance to business operations has risen dramatically. This is shown in **Figure 1**.

Figure 1: Importance of Security to Network Service Providers

How important are each of the following to the telecom industry over the next five years? (chart shows responses ranked "essential")



Source: Heavy Reading survey of 144 service provider respondents, November 2014

Figure 1 shows the results of a survey of telecom and cloud providers carried out by Heavy Reading in 2014. In this survey, respondents identified security as one of the most important issues in the networking industry over the next five years. This is, in some ways, surprising given that security is generally more associated with cost and the other options listed in the question are mostly on the revenue side.

One explanation for this is that operators now see security as essential to yielding the full benefit from digital services. Simply put, without secure, trusted networks, the opportunities presented by cloud services will not be fully realized, and many services may not be viable at all. It was in this context, in 2013, that the CEO and chairman of AT&T, Randall Stephenson, described security as "the long pole in the tent" when it comes to capturing revenue from connected devices and the cloud.

Role of IPsec in the Network Cloud

Although an old technology (in Internet terms), IPsec is important to modern network and cloud services: It is one of the primary method to secure enterprise connections to the cloud, for example. It must, however, evolve to meet new networking and computing models. There are two key aspects to this:

Cloud Economics & COTS Hardware

Economics demand that service providers have a low cost of production to enable them to design services that are "price elastic" and applicable to a wide range of customers and use cases.

The classic model of specialist IPsec gateway platforms, each with its own hardware optimizations, training, management, etc., is now facing challenges. Within the limited budget service providers have to work with, the price/performance ratio is coming under pressure as alternatives based on industry standard servers start to look more attractive, with a new cost model driven by high-volume server economics and Linux-based networking software that is portable by the service provider.

A first step in the transition to general-purpose x86 servers is to deploy IPsec on bare metal, where the performance of IPsec on Linux is now within range of that achieved by specialist, router-based IPsec gateways. With software accelerators, it is also attractive to move directly to deploy in VMs.

Encryption & Virtualization

Running IPsec as a virtual network function (VNF) in VMs gives the operator greater operational flexibility, including the ability to scale up for high-performance use cases or scale down for smaller deployments. There are challenges on the management and operations side to IPsec deployed as a VNF; however, VM environments are maturing, and this is now a realistic option for deployment in live production networks.

Taking a more expansive view from virtualization to "cloudification," it is not yet clear how the future virtual network architecture will incorporate IPsec. One potential step is to embed IPsec in the virtual switching layer to secure inter-VM communications. This would probably require software-based, data-plane accelerators to reduce the CPU resources necessary for packet processing and encryption. Ultimately, security must be inherent to the network cloud architecture. It cannot be an additional cost, deployed as an overlay to existing IP networks, as is the case with classic IPsec, but should be embedded in the virtual network environment.

Use Cases for Server-Based IPsec

There is a very broad range of use cases for IPsec in telecom and cloud provider networks. This section covers selected use cases for IPsec on commercial-off-the-shelf (COTS) servers in scenarios where the requirement is for a lower cost, but functionally equivalent, solution than is traditionally available. These use cases can scale from small-scale to very high-performance requirements.

Data Center Interconnect

In this scenario, a cloud service provider needs to interconnect processing and storage clusters at different locations. Typically, it would lease IP services from a third-party network provider, using Internet transport or MPLS VPN. Where cheaper Internet transport is used, the payload must be secured using an IPsec VPN. And in cases where the payload is sensitive, such as protected media content (e.g., films or TV shows), even managed IP transit services (non-Internet) and MPLS VPNs may require additional IPsec security.

In this scenario, the IPsec gateway must be very high-performance because cloud providers are moving lots of data quickly between locations. Some high-level performance requirements are:

- **Throughput:** Very high throughput (multiple Gbit/s) for generally large packet sizes; predictable flows at (normally) predictable times
- **Session Scalability:** A small number of highly available connections needed; scale throughput up/down according workload timing
- **Setup Rate:** Relatively static configuration, although ability to move connections between cloud locations is important

These use cases can be met by hardware-based products from established vendors, particularly if physical locations are relatively static. The challenge is to do it cost effectively. As shown later in this paper, it is now possible to provide 144 Gbit/s IPsec throughput on an HPE ProLiant DL580 4U rack server running "fast path" acceleration software. This dramatically changes the economics and makes it possible to scale to very high speed IPsec VPNs needed to support the most demanding data center interconnect services over leased transport. Cloud service providers are organizations that are capable of running IPsec VPNs on COTS hardware and do not require some of the features and after-market support offered by traditional "big iron" vendors. This makes them well suited to virtual IPsec.

Enterprise WAN & Cloud Services

Enterprise IPsec VPNs are a very common way to connect office and cloud locations in a way that is substantially cheaper than MPLS VPN equivalents and is often "good enough" performance-wise. The opportunity is for network service providers to use server-based IPsec Gateways to connect enterprises to cloud services.

The client side connections (at the enterprise premises) are relatively modest from a throughput perspective (100 Mbit/s to 1 Gbit/s), and show the need to be able to scale IPsec down to just a single VM or processor. On the other side of the link, the aggregation node will require much higher throughput, as multiple locations and customers are combined, driving a need to scale up. Some high-level performance requirements are:

- **Throughput:** Low to medium on the client-side; very high throughput (Gbit/s) on the network gateway side; fairly bursty traffic
- **Session Scalability:** Medium; requires support for multiple enterprise customers (and multiple sites per customer)
- **Setup Rate:** Relatively static configuration, although ability to on-board new customers and locations is important

Like the enterprises and cloud providers they are connecting, network service providers want lower cost; hence, virtual IPsec on COTS is attractive. One challenge for COTS solutions in this market is the need for customer support. Service providers typically buy IPsec gateways from the same vendors that provide their routers and other WAN equipment and benefit from the associated after-market technical support.

Mobile Networks & IPsec

There are some interesting emerging use cases for IPsec in the mobile network that demand low-cost solutions and are, therefore, good candidates for COTS deployments. Two of the leading opportunities are:

- **IPsec Gateways for Small Cells.** Small cell backhaul links are often over untrusted broadband access networks and secured with IPsec. This deployment model depends on low cost per link and can tolerate slightly lower reliability than traditional mobile backhaul.
- **IPsec Gateways for Carrier WiFi**. Service providers use IPsec between the WiFi network controller and the operators' network gateway to secure payload and control-plane data. Carrier WiFi is "IT-oriented" and operators, therefore, are already comfortable with COTS products.

Summary of Use Cases

Figure 2 summarizes a range of emerging use cases for IPsec in data center and telecom operator networks. In each example, the relative performance requirements in terms of throughput, number of simultaneous IPsec tunnels and tunnel setup/teardown rate are shown.

Figure 2: IPsec Use-Case Summary

Use Case	Throughput	No. of Tunnels	Setup Rate
Data center connect	Very high	Low	Low
Enterprise WAN/cloud	Medium	Medium	Low
Small cell gateway	Medium	High	Low to medium
Carrier WiFi aggregation	Medium to high	Medium to high	Low to medium
Mobile backhaul	High	Medium to high	Low

Operators, in some markets, make extensive use of IPsec to secure 4G backhaul over third-party transport services, but due to extreme reliability and specific operational requirements, this use case is probably not suitable for COTS servers today.

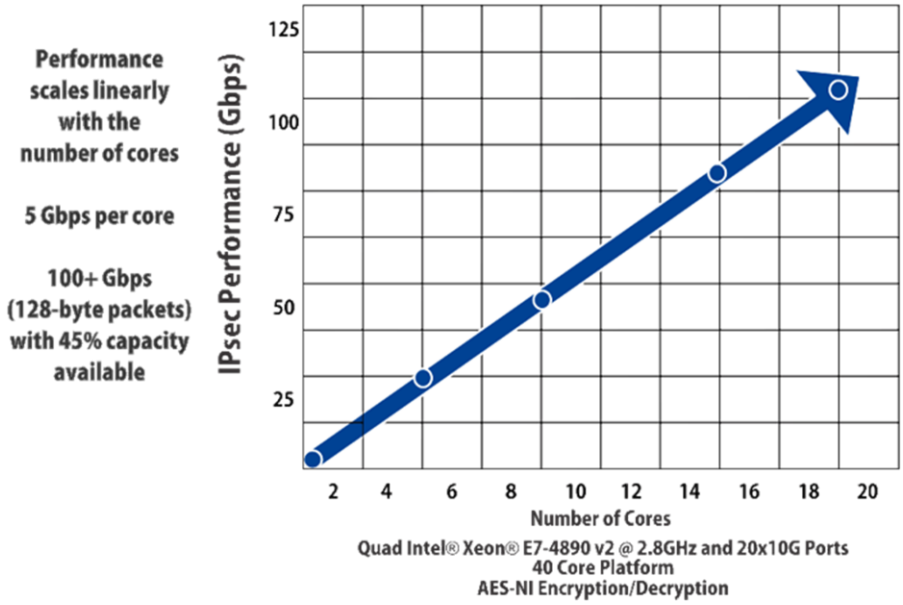
IPsec Performance on General-Purpose Servers

Server volume shipments and performance per CPU have increased dramatically over the past few years, driving a radically better price/performance ratio. These basic economic factors are driving the move to general-purpose x86 server hardware available off the shelf.

Why COTS Servers?

Massive improvement in performance makes high-performance packet processing and encryption functions achievable on x86 servers. Some very high-performance Layer 3 networking functions, such as edge and core routers, will still require specialist hardware, but general-purpose x86 hardware is now good enough for many applications. As **Figure 3** shows, IPsec performance scales linearly with the number of CPU cores when used in combination with "fast path" networking software. This will make it very difficult to resist the cost advantage of COTS, especially given that server performance continues to improve.

Figure 3: IPsec Performance on x86 Processors



Source: 6WIND on Intel reference platform

The intent is to continue to optimize performance per CPU to maximize packet processing performance to support NFV infrastructures. There are many technologies available to help achieve this, including network interface cards (NICs) for packet processing offload on the hardware side, and optimizations – such as DPDK, SR-IOV, and hypervisor and vSwitch enhancements – on the software side. For applications with an optimized "fast-path" architecture, software accelerators can massively improve packet processing performance without the need for hardware offload or SR-IOV. The major challenge is to improve server performance for networking applications without compromising the "off-the-shelf" nature of the platform with specific build requirements.

IPsec Performance Test Results

To demonstrate the suitability of IPsec on COTS servers for small, medium and large networks, HPE and 6WIND cooperated on a test program over the winter of 2016 to benchmark the performance of 6WIND software on HPE ProLiant Servers. Heavy Reading was not involved with the test and is not able to verify the results independently. However, we have had an opportunity to review detailed test report and to interview the product managers and testing personnel. We believe the test was conducted in good faith.

Benchmark Performance Results

The benchmark tests measured performance using HTTP traffic over IPsec. The intent was to determine the maximum stable performance at reasonable CPU resource levels. The HTTP traffic model is designed by test vendor Spirent to imitate a real-world scenario and provides a more reliable indicator of actual performance than simple "bit-blaster" performance tests.

Two server devices were placed under test: an HPE ProLiant Gen8 with 60 cores, used mainly for decryption, and a Gen9 with 72 cores, used mainly for encryption. Both servers were running the 6WIND Turbo IPsec software in VMs and 6WIND Virtual Accelerator software in the hypervisor. **In the test, HPE and 6WIND were able to show 144 Gbit/s of application traffic (AES-256) sustained at 75 percent of CPU utilization.** The results are detailed in **Figure 4**.

Figure 4: Performance Test Results

System Components	HPE ProLiant DL580 Gen8 Server	HPE ProLiant DL580 Gen9 Server	Notes
Processor	Intel Xeon CPU E7-4890 v2 @ 2.80 GHz	Intel Xeon CPU E7-8890 v3 @ 2.50 GHz	4 sockets per system
Cores per system	60	72	
VM information	Turbo IPsec	Turbo IPsec	1 VM per socket, 4 VMs per system
Total cores for all (4) VMs	34	34	32 fastpath; 2 control
Total Virtual Accelerator cores	24	24	Part of hypervisor
Unused cores per system	2	14	Available for more VMs, performance
IPsec HTTP total bandwidth	144 Gbit/s	144 Gbit/s	IPsec uses AES-256 HMAC-MD5
CPU utilization	Turbo IPsec: 90% Virtual Accelerator: 70%	Turbo IPsec VM: 75% Virtual Accelerator: 55%	Nginx @ 100% utilization
IPsec HTTP BW/VM	144/32 = 4.5 Gbit/s	4.5 Gbit/s	32 cores in fastpath

Source: 6WIND

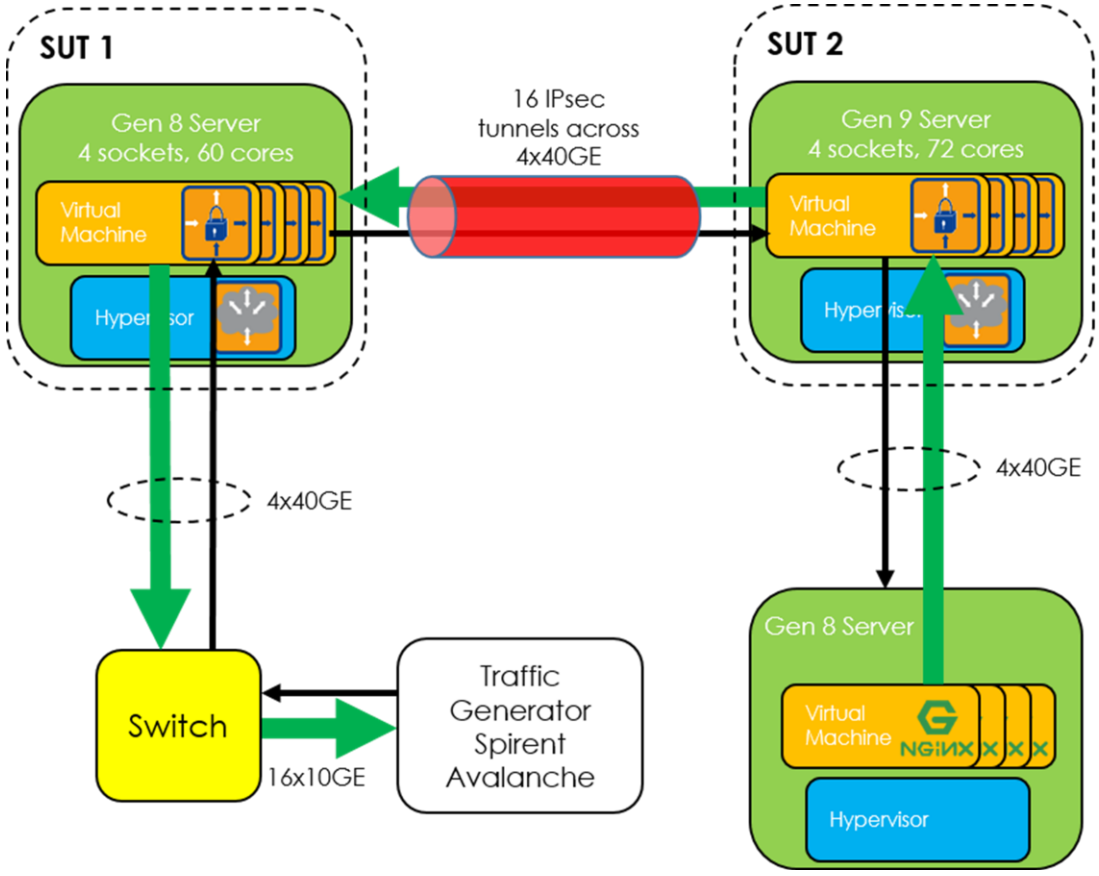
Note that the upper limit on performance was determined by the Nginx Web server, running at 100 percent utilization. The Gen9 server in particular could otherwise have achieved greater performance based on the CPU utilization rate. The full test used all four server sockets to achieve maximum performance, but the same tests were also run on a single, double and triple sockets, and demonstrated linear scalability from low to high performance.

Test Bed Setup & System Components Under Test

The test setup is shown in **Figure 5** below. It includes the traffic generator provided by Spirent, the Gen9 server, the Gen8 server and the Nginx Web server software (also running on an HPE ProLiant server). The Spirent Avalanche was set up to simulate 12,000 users distributed across four 40 Gigabit Ethernet links, each generating 10,000 file download requests to the target Nginx Web servers.

Note that both servers perform encryption and decryption, but that the majority of the traffic is in the downlink from the Nginx Web servers to the Spirent traffic generator (144 Gbit/s of clear traffic was seen in the test). In the uplink, the traffic generator sent an aggregate of 5 Gbit/s of clear traffic requests to the Web servers.

Figure 5: Logical Test Bed Setup



Source: 6WIND

The two systems under test were both four-socket, 4 RU HPE ProLiant devices: the DL580 Gen9 and Gen8 running the 6WIND Turbo IPsec software (34 cores) and 6WIND Virtual Accelerator in the hypervisor (24 cores). The rest of the system components under test are as follows:

- **HPE ProLiant DL580 Gen9 Server:** Four Intel Xeon E7-8890 v3 @ 2.50 GHz with 18 cores each (a total of 72 cores in the platform) and eight Mellanox 40 Gigabit Ethernet NICs.
- **HPE ProLiant DL580 Gen8 Server:** Four Intel Xeon E7-4890 v2 @ 2.80 GHz E7-8890 with 15 cores each (a total of 60 cores in the platform) and eight Mellanox 40 Gigabit Ethernet NICs.
- **6WIND Turbo IPsec** software for bare metal and VM deployments.
- **6WIND Virtual Accelerator** software for hypervisor scaling.
- **CentOS KVM hypervisor** as a host for the software.

Conclusion

In conclusion, it is now possible to run IPsec gateways as a VNF on general-purpose x86 servers at a range of performance levels from small-scale deployments to large, high-performance cloud applications.

This puts software-based IPsec in direct competition with classic, specialist hardware-based IPsec equipment and provides a potentially compelling system cost. The overall cost of ownership naturally also includes items like operations and management, technical support and training, and software upgrade costs, and is out of scope for this paper.