Fat IPsec VPN Tunnels on a Budget

Unleashing 6WIND's Virtual Security Gateway

White Paper

6WIND

Virtualized Networking Software

www.6wind.com

Table of Content

Notices & Disclaimers: Performance benchmarks vary by configuration and other factors. Performance results are based on the testing environment described in the testbed description section.

1. Introduction

There are many use cases that require high-throughput – around 10 Gbps per link or more – authenticated and encrypted exchange of privileged consumer or corporate data between sites. Examples of such use cases are: general-purpose datacentre (DC) interconnects, data aggregation from distributed locations at centralized storage sites organized in a hub-spoke topology and real-time data synchronization across a (meshed) network. The common approach to address aforementioned use cases is to deploy a Virtual Private Network (VPN) onto each applicable site, secured by IPsec authentication and encryption algorithms.

Traditionally, the IPsec VPN tunnels are implemented on purpose-built proprietary silicon-based security gateway (SecGW) hardware, sourced from a reputable vendor.

This approach comes with its own pros and cons. In this White Paper, we propose an alternative, leveraging the performance and efficiency of 6WIND's virtual security gateway (vSecGW) to deliver performance on par with purpose-built systems, but without the associated cost and hardware vendor lock-in.

[1] Application-Specific Integrated Circuits.

2. Challenges with traditional hardware based solutions

A hardware-based SecGW sourced from a reputable vendor can be expected to deliver the IPsec throughput and number of concurrent IPsec sessions stated in its brochure.

The natural weakness of such HW-centric, “black box” solutions does not reside in their efficiency or performance, but in the fact that they are monolithic and inherently inflexible. The hardware and firmware are inseparable, and the hardware is proprietary, containing proprietary silicon (ASICs[1]) and a proprietary HW architecture. That creates an inseverable HW-SW dependency: a vendor lock-in, which is great for the vendor, and less so for the buyer.

Moreover, the performance of a typical monolithic network edge SecGW solution – in terms of maximum IPsec throughput and number of concurrent IPsec sessions – is pre-determined at the drawing board, being a function of proprietary silicon, and mostly not scalable at all, or to a very limited degree (number of concurrent IPsec sessions only). The user will therefore tend to over-dimension the SecGW, and thus over-invest, rather than risk facing a near-term capacity crunch.

Clearly, overinvesting is not a great way to pare down cost per bps, and the pressure to lower “cost per bit” is tremendous in the communications service provider industry in order to keep business sustainable in times of stable or declining ARPU[2].

If on the other side the IPsec throughput or the number of concurrent sessions exceed the capabilities of the monolithic solution, the security gateway will have to be replaced by a more potent model; a “forklift upgrade”. Unless by chance it can be redeployed elsewhere in the network, it will have to be sold at a low price on the second-hand market or scrapped and depreciated. That’s the cost of having no or limited scaling flexibility.

[2] Average Revenue Per User – typically on a monthly basis.

3. How 6WIND’s vSecGW addresses the customer challenge

There’s good news though, and it comes in the shape of 6WIND’s vSecGW software. Our vSecGW addresses the efficiency, performance and scaling weaknesses of hardware solutions, while steering clear of proprietary hardware, vendor lock-in, lack of a cloud deployment perspective and problematic vertical and horizontal scalability issues burdening proprietary HW-centric SecGW approaches.

vSecGW features a highly optimized data plane, our prime asset that can, on the latest-generation general-purpose CPUs digest 7 Gbps of IPsec IMIX traffic per (v)CPU core without HW-acceleration in any form or shape. We have proven[3] that by combining multiple CPU cores, real-life IPsec traffic throughputs of at least 100 Gbps full-duplex (200 Gbps aggregate) are feasible on just one single instance of the latest x86-based servers. Figure 1 shows what can be achieved in terms of IPsec throughput with different traffic patterns (including IMIX[4] and IMIX2[5]) and different numbers of allocated CPU[6] cores.

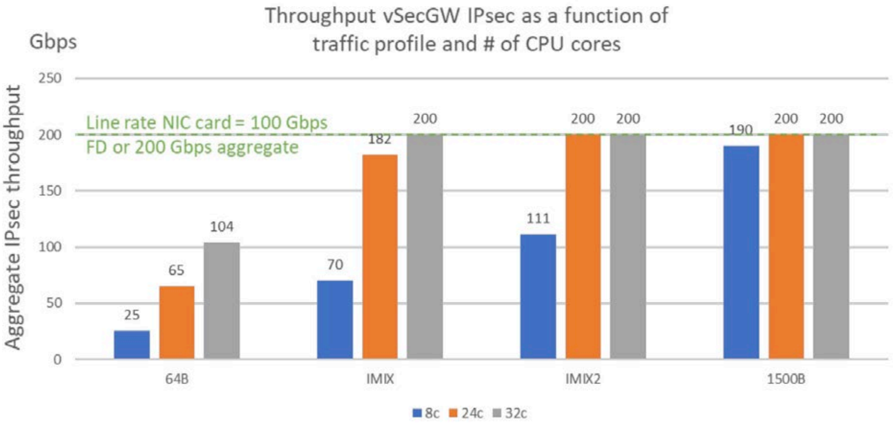

Figure 1: vSecGW IPsec aggregate throughput (upstream + downstream) as a function of different packet size distributions and as a function of different numbers of allocated CPU cores.

This high level of performance rivals the performance level of special-purpose HW-centric solutions, without the aforementioned strings attached. By tiering CPU cores in the data plane, with a limited number of load-sharing cores, each taking care of load sharing across multiple worker cores, elephant streams or “fat” IPsec streams carrying n x 7 Gbps are at your fingertips.

[3] 6WIND’s White Paper titled: “6WIND Proves the 5G Virtual Security Gateway Concept”

[4] Internet MIX with frame distribution: 64B (58,3%), 590B (33.3%), 1514B (8.3%), averaging 350B.

[5] A “pseudo-IMIX” with a customer-specific 5G New Radio frame distribution: 64B (8%), 127B (36%), 255B (11%), 511B (4%), 1024B (2%), 1539 (39%), averaging 700B.

[6] The CPU used is a Dual Intel Xeon Gold 6348 @2.6 GHz, comprising 2 x 28 cores. We did not allocate more than 32 cores in total.

It has to be noted that 6WIND's vSecGW doesn't depend on the latest and greatest in terms of hardware or CPU architecture to achieve broadly usable IPsec throughputs, in the range of 10 Gbps, a value well-suited for most applications. vSecGW will run happily and efficiently on omnipresent older-generation x86 and ARM CPUs, like for example the Intel Atom® C3000 product family (Denverton). This fact greatly enhances its applicability and its deployability to datacenters, public, private or hybrid clouds anywhere in the world.

Moreover, it shall be mentioned that vSecGW provides, if required, for a High Availability (HA), carrier-grade security gateway solution, based upon stateful synchronization between 1+1 redundant instances of the vSecGW, as outlined in Figure 2. The stateful synchronization or hot standby setup ensures a fast (within 300 ms) and revertive switchover between the two instances, without notable traffic interruption, and thereby – provided that it's implemented on mutually independent hardware instances – it caters for extremely high availability. Therefore, the highest Quality of Experience (QoE) will be guaranteed.

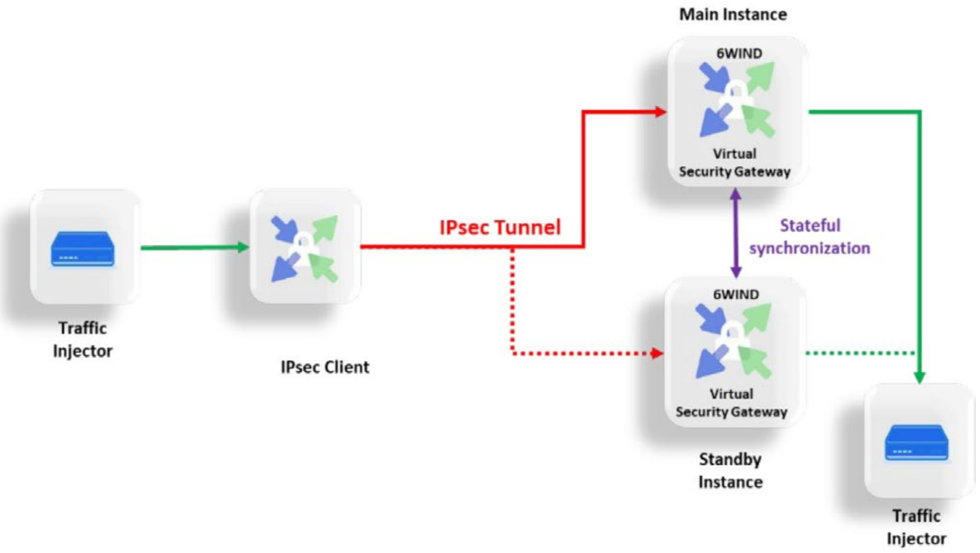

Figure 2: carrier-grade redundancy of our vSecGW solution through stateful synchronization.

Lastly, our vSecGW solution can do way more than just instantiating "fat" IPsec VPN tunnels. Being part of our Virtual Service Router (VSR) software suite, the software can be tailored to each use case's specific requirements. Just a few examples of attributes that can be helpful are:

- Support for VRF[7]s to for instance separate the external from the internal networks,
- Support for the following routing protocols: BGP, OSPF, IS-IS and more,
- Support for basic filtering (firewalling) for security purposes,
- A NETCONF based CLI, which greatly aids configuration management,
- A free KPI / telemetry dashboard capability, using the Telegraf product to export router KPIs to an external time series database (InfluxDB). Grafana then reads the DB and graphically represents the KPIs.
- Pre-boot execution environment (PXE), or bootloader installation capability. It provides a user-friendly hands-off means for installing the VSR on new bare metal servers, picking an installation server through the Network Interface Card.

[7] Virtual Routing and Forwarding.

4. Conclusions

6WIND's vSecGW features a highly optimized data path on ubiquitous x86 and ARM-CPU-based COTS servers, which puts its IPsec VPN performance cheek-to-cheek with dedicated and proprietary SecGW platforms, while avoiding vendor lock-in and the associated costs, risks and vertical & horizontal scalability limitations for its users. vSecGW can readily be deployed as a cloud-native instance, including on 3rd party infrastructure, enabling practically infinite and "organic" horizontal scaling.

This industry-leading efficiency and performance level enables our vSecGW, running on the latest COTS-server HW, to challenge purpose-built security gateways of reputable hardware vendors, and then beat them in terms of price / performance ratio. Yet vSecGW doesn't require the latest in hardware to perform: it delivers meaningful capabilities in the order of 10 Gbps of IPsec throughput on older servers and CPU designs.

vSecGW furthermore supports carrier-grade availability thanks to 1+1 system redundancy with stateful synchronization and it supports elephant streams or "fat" IPsec VPNs carrying tens of Gbps of traffic.