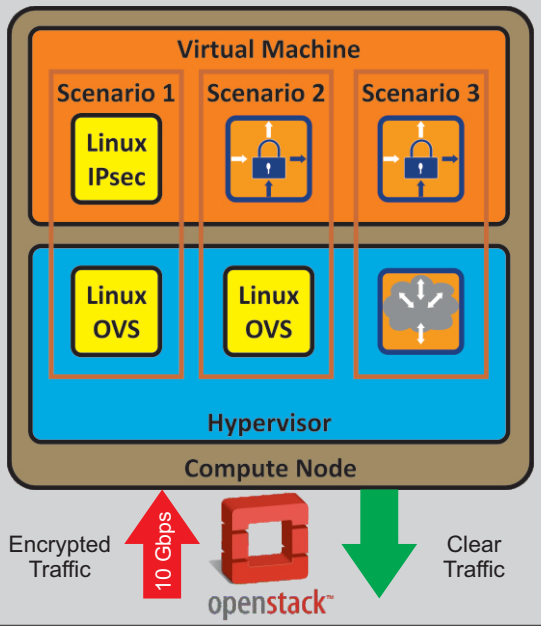
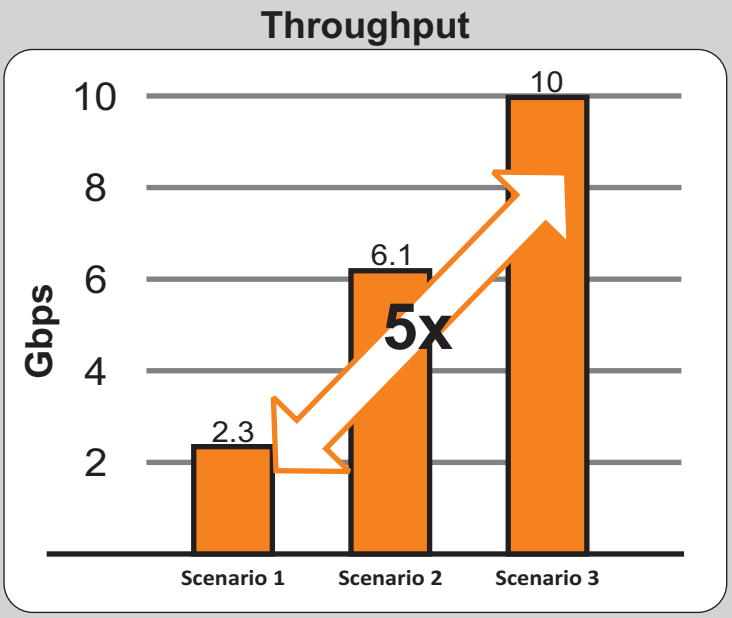
Turbo IPsec and Virtual Accelerator

Scalable Virtual IPsec Aggregation For Remote Users





- **Leverage virtual IPsec applications on COTS servers and break the dependence on expensive, proprietary hardware**
- **Optimize resource utilization to increase throughput and scale services**
- **Bare metal performance in a virtual IPsec Gateway**

IPsec Technology for Remote Users

IPsec is a necessary security technology for Network Operators as it is used to create secure, high speed communication tunnels between trusted endpoints across the internet and WAN. Examples include remote engineers accessing a company's intellectual property, remote medical technicians or doctors accessing a medical imaging storage facility or an account manager downloading the latest company pricelist from the intranet. Since the internet is inherently insecure, an IPsec VPN is a critical solution. Each user's device now has an IPsec client that generates its own secure tunnel that terminates at the IPsec aggregator, effectively extending the private (cloud) network to the user's device.

The IPsec aggregator must support hundreds if not thousands of IPsec tunnels and at the same time must not be the bottleneck in the access path.

Whether a user uploads or downloads large files, manipulates databases or browses private webpages, the IPsec aggregator must provide the required throughput.

High Performance Software Alternative

Legacy IPsec aggregator solutions include expensive, purpose-built hardware. Today, virtual appliances in an OpenStack-enabled virtual infrastructure provide cost-effective, scalable, and flexible alternatives on commercial-off-the-shelf (COTS) servers.

6WIND Turbo IPsec™ Aggregation Solution

6WIND Turbo IPsec is a software appliance designed for bare metal or virtual machine (VM) deployments on COTS servers. Multiple virtual Turbo IPsec appliances can reside in VMs in a virtual infrastructure environment on the same server providing independent, high performance, cost-effective IPsec aggregation solutions.

However, just like any VM, maximum Turbo IPsec throughput is hindered by a well-known bottleneck in the hypervisor that affects forwarding performance.

Two well-known solutions that increase VM performance are PCI passthrough and SR-IOV. By design these technologies bypass the hypervisor and its rich networking features; therefore, the performance benefit

breaks virtualization. 6WIND Virtual Accelerator is hypervisor scaling software that can be combined with 6WIND Turbo IPsec to increase VM performance without breaking virtualization.

6WIND Virtual Accelerator™ and Turbo IPsec

6WIND Virtual Accelerator provides performance for NFV by accelerating KVM-based hypervisors to increase throughput for VMs. It is a packet switching software solution that transparently and efficiently increases hypervisor performance by a factor of 10. Any VM with any operating system leveraging standard Virtio can benefit from the performance boost.

Combining 6WIND Turbo IPsec and Virtual Accelerator results in bare metal-like performance while preserving the virtual environment. Virtual Accelerator co-exists with Linux bridge or Open vSwitch (OVS) with no changes to Linux or OpenStack management and monitoring tools.

IPsec Benchmarks: 6WIND Turbo IPsec and Virtual Accelerator vs. Linux

6WIND conducted benchmark testing in an OpenStack virtual infrastructure configuration to provide a comparison of different IPsec software deployments. The test includes a traffic generator (transmitter/receiver) connected via two 10GE links to the system under test. The traffic generator transmitted encrypted packets and received un-encrypted (in-the-clear) packets. A total of 5,000 tunnels were created and 10 Gbps of encrypted traffic (2 Mbps/tunnel) was transmitted. The system under test is a COTS server with a single 12 core CPU (E5-2680 v3).

Getting the highest throughput with Linux hypervisors is not an easy task. As cores are shared between the hypervisor and the VM, it is hard to determine the bottleneck location. If the VM does not have enough vCPUs, the bottleneck will be the VM. Conversely, too many vCPUs moves the bottleneck to the virtual switch of the hypervisor. Our testing methodology maximizes throughput with the optimal number of vCPUs assigned to the VM.

Conclusion

6WIND's Turbo IPsec virtual appliance has the performance and scalability to support large scale IPsec VPNs. Turbo IPsec triples the performance of a Linux IPsec application without breaking virtualization. Add 6WIND Virtual Accelerator to the hypervisor for 5x performance. As an added benefit, Virtual Accelerator maximizes performance while optimizing resource utilization. Testing shows 6WIND Turbo IPsec with Virtual Accelerator can process a full 10 Gigabit Ethernet traffic stream comprised of 5000 IPsec tunnels with a total of three cores to Turbo IPsec and two cores to Virtual Accelerator. The remaining eight spare cores can be used by other VMs or they can be used to increase performance.

IPsec Test Results Summary

	Scenario 1	Scenario 2	Scenario 3
Throughput (Gbps) (% of linerate)	2.3 23% linerate	6.1 61% linerate	10 100% linerate
Packet Size (B)	IMIX	IMIX	IMIX
Maximum Number of Cores to VMs	4	4	3
Number of Linux vSwitch or Virtual Accelerator Cores	8	8	2
Spare Cores (12 cores in the system)	None	None	8

Scenario 1 (baseline): Linux Ubuntu VM with Linux CentOS hypervisor with Open vSwitch

Scenario 2: 6WIND Turbo IPsec with Linux CentOS hypervisor with Open vSwitch

Scenario 3: 6WIND Turbo IPsec with Linux CentOS hypervisor with Open vSwitch and 6WIND Virtual Accelerator

www.6WIND.com