SPEEDMATTERS

Application Brief

Powering the New Generation of IPsec Gateways

Mobile Internet traffic is growing exponentially and subscribers increasingly expect advanced services on mobile platforms. Service Providers are migrating their networks to the all-IP Long Term Evolution (LTE) standard. At the same time, many operators are implementing wireless offload schemes to route traffic over the Internet in order to provide increased coverage for subscribers while reducing the overall load on the wireless network. In this scenario, user traffic from WiFi access points, picocells and femtocells is connected to the core network via public Internet connections. This potentially exposes the core network to a wide variety of Internet-based attacks.

Internet attacks continue to increase risks for data centers as well. Cloud Providers offering data center virtualization solutions must secure connections across their virtual networks. And Enterprise Providers who make network equipment for large enterprises must deliver high performance solutions to secure connections across distributed data centers.

Internet Protocol Security (IPsec) and Internet Key Exchange (IKE) are protocols that exist in IPsec Gateways to secure IP communications by authenticating and encrypting IP packets. Service, Cloud and Enterprise Providers must deploy IPsec Gateways as a critical layer of protection, while providing the performance and flexibility necessary to support an increasing number of diverse access points, the growth in mobile traffic bandwidth, and the shift from physical to virtual infrastructure.

6WINDGate™ packet processing software solves networking performance bottlenecks to enable high performance physical and virtual IPsec Gateways on generic hardware platforms, thus reducing time to market and providing competitive advantage.

Since the first shipment of 6WINDGate™ software in 2007, 6WIND has been selected by many Service Providers and Network Vendors for their security gateway equipment to unlock hidden infrastructure performance for commercial off-the-shelf (COTS) hardware.

IPsec Gateway Use Cases

- Application Delivery Controllers
- Server Load Balancers
- Firewalls
- Security Gateways
- Routers
- vCPE

Fastest IPsec Performance Leveraging Multi-vendor Hardware Crypto

Over 190 Gbps of encrypted traffic

Turbo Boost Linux

Requirements Increase for the New Generation of IPsec Gateways

To meet evolving security requirements, new generation IPsec Gateways must include the following:

- Use of cost-effective generic hardware platforms and commercial or open source Linux distributions
- Benefit from high performance Ethernet NICs (10G and 40G) as well as dedicated crypto acceleration (software crypto, built-in or external hardware crypto-engines)
- High performance packet processing software for key network security features such as IPsec and IKE using minimal processor resources to remove performance bottlenecks at all levels and sustain high network throughput of encrypted traffic
- Availability of a large number of protocols such as Layer 2 encapsulation, IPv6, routing, virtual routing, firewall, NAT, QoS and more to easily integrate the IPsec Gateway into a complete networking infrastructure
- Flexible and extensible software architecture to develop physical IPsec Gateways and prepare the shift to virtual IPsec Gateways based on commercial or open source virtualization environments
- Open architecture to reuse in-house or third party application software

6WINDGate's High Performance IPsec Solution on Generic Hardware

6WINDGate is high performance Layer 2 – 4 packet processing software for market leading processors including Cavium, Broadcom, Intel and EZchip/Tilera. 6WINDGate networking software uses the services of the processor vendor's Software Development Kit (SDKs). On Intel platforms, 6WINDGate sits on top of Data Plane Development Kit (DPDK) extended by 6WIND to support multi-vendor NICs as well as software and hardware crypto-acceleration.

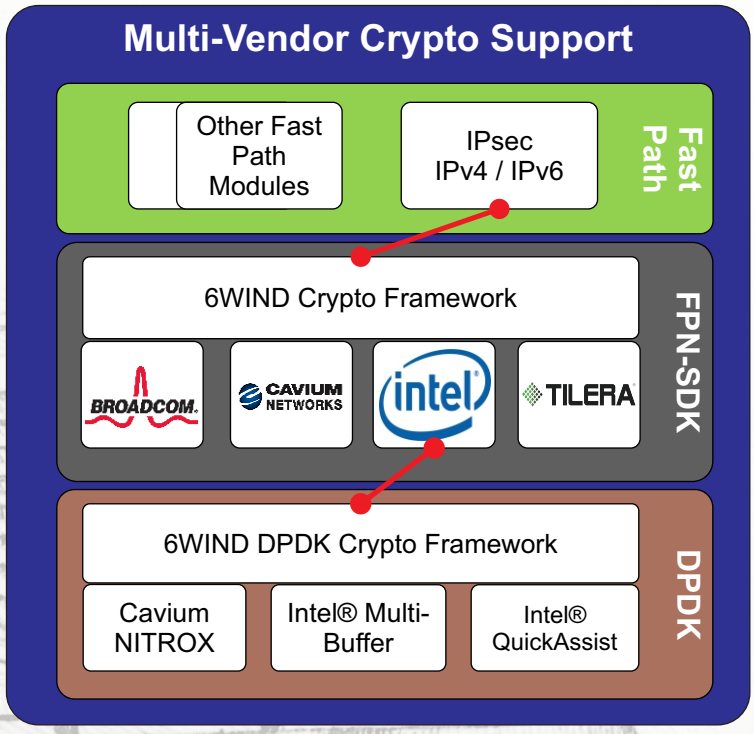
Based on a fast path architecture, 6WINDGate transparently accelerates Linux network environments to provide 10x network performance improvements compared to standard software architectures. 6WINDGate is compatible with commercial and open source Linux distributions and does not require any modification of the Linux kernel.

Beyond data plane protocols, 6WIND also provides control plane protocols including routing, virtual routing, IKE, VRRP and high availability capabilities. All these protocols are pre-integrated with 6WINDGate's high performance fast path to reduce time-to-market.

6WINDGate transparently reuses standard APIs such as Netlink between userland and the kernel so that legacy control plane applications running on a standard Linux network stack can be reused without any modification on 6WINDGate's accelerated data plane. In-house or third-party control plane protocols can therefore be easily integrated on top of 6WINDGate.

6WINDGate provides the most comprehensive portfolio of protocols on the market to develop high performance and cost-effective IPsec Gateways including:

- High performance IPsec stack to sustain more than 190 Gbps of encrypted traffic over several tens of thousands of IPsec tunnels on a single Intel server with low-latency
- Support for software and hardware crypto-acceleration as well as external hardware crypto-engines on Intel, Cavium, Broadcom and EZchip/Tilera architectures
- High-capacity IKE control plane able to manage several tens of thousands of IKE sessions on a single server
- High capacity for encapsulation protocols such as VLAN, PPP, L2TP, GRE and more
- High performance and scalable IPv4 and IPv6 forwarding supporting 10 million packets per core on Intel platforms with virtual routing support for a large number of instances
- High performance and capacity firewall and NAT



Extensions for Virtualized Environments

NFV (Network Functions Virtualization) is a major trend in the telecom industry that can be applied to IPsec Gateways. Instead of developing dedicated equipment, a generic virtualized platform embeds an IPsec Gateway function (vIPsec Gateway) as a software appliance running in a Virtual Machine (VM) with other virtual security functions on a single server.

6WINDGate's architecture extends to provide the same performance improvement and feature set for an IPsec Gateway function running in a VM.

However, virtualized architectures add many software processing layers between the network interface and the workload running in a VM that cause significant networking performance penalties. It is an increasing challenge for workloads such as vIPsec Gateways that must individually process a very large amount of traffic. NFV Infrastructure (NFVI) is a critical software component to provide the different workloads with the required bandwidth.

6WINDGate has been extended to provide an open and high-performance NFVI platform designed around a software switch. Based on its fast path architecture, 6WINDGate transparently accelerates the selected software switch to provide extreme bandwidth and low-latency to Virtual Networking Functions (VNF). As an example, 6WINDGate Open vSwitch (OVS) acceleration provides over 10x performance improvements without any modification to OVS or its management. 6WINDGate's extensions for virtualized environments provide a transparent and progressive path for virtualization of IPsec gateways.