



Virtual SecGW

Key features

- ▶ **16 Mpps per CPU core**
(Forwarding rate)
- ▶ **18 Gbps per CPU core**
(Over 200G per single instance)
- ▶ **100,000 tunnels**
(VPN IPsec tunnels)
- ▶ **1,000 tunnel/s**
(Establishment rate)

Benefits

- ▶ End-to-End encryption and secure VPN IPsec tunnels
- ▶ Centralized certificate-based security
- ▶ Support for physical and virtual deployments (NFV)
- ▶ High scalability (100k+ sessions per instance) and High availability
- ▶ Optimized network performance and efficiency with reduced operational costs and complexity

Virtual Security Gateway (vSecGW)

The 6WIND VSR can be used as a Virtualized Security Gateway (vSecGW) that provides comprehensive, highly scalable and network-integrated Layer 3 IPsec-based VPN connectivity.

The vSecGW functionality can be applied to any type of network traffic in fixed, wireless and converged environments.

The 6WIND vSecGW covers different deployment use cases including:

- ▶ Mobile Security Gateway
- ▶ Remote Access IPsec VPN Concentrator
- ▶ Secure multi-cloud access
- ▶ Site-to-site and network-to-network encrypted IP security

Network operators benefit from superior deployment flexibility, a rich feature set, carrier-grade performance, high availability and enhanced support tools, enabling quick deployment and operationalization of a flexible and powerful IPsec feature set in cloud and hybrid environments.

“ 6WIND Virtual IPsec vRouters are a **drop-in replacement for Brocade vRouters with an added bonus of high performance IPsec VPN functionality.** 6WIND’s price/performance combo make it a contender for any vRouter, firewall and secure VPN project. ”

Chris Konger, Senior Network Engineer

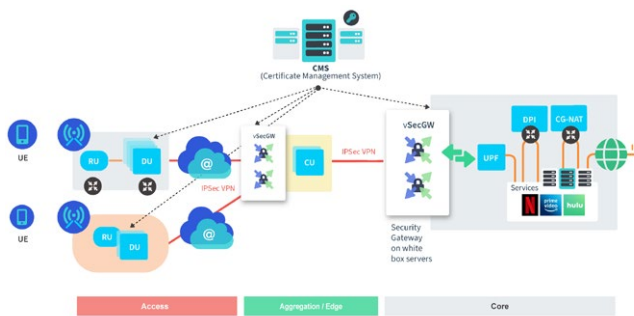
SOVRN

The 6WIND vSecGW can be deployed in different use cases, delivering high performance, scalability, resiliency and end-to-end security benefits for each one.

The following sections describe the most relevant deployment use cases for CSP and Enterprise networks.

Mobile Security Gateway

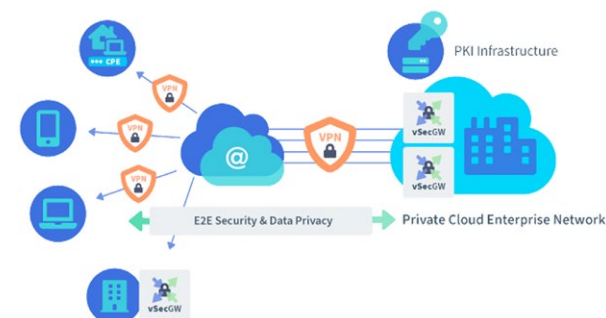
Communication Service Providers can leverage the 6WIND vSecGW to deliver end-to-end encryption and secure IPsec VPN tunnels. The vSecGW can be deployed in a 4G network to secure S1 traffic and terminate VPN tunnels initiated at eNodeBs and small cells. The vSecGW can also be deployed in 5G networks to secure the CU to DU or the CU to core network connectivity.



The 6WIND's vSecGW can use a centralized certificate management to install the required security certificates.

Remote Access IPsec VPN

The Remote Access IPsec VPN service addresses CSP and enterprise use cases and offers scalable VPN connectivity to securely connect remote workers and branch offices to the enterprise private network. VSR software provides encryption and interoperability capabilities allowing aggregation of VPN connections issued by any native VPN client solution including Windows, iOS, Android and Linux.



Furthermore, the solution comes with high availability capabilities, for a secure and reliable connectivity service, and delivers highly scalable performance not only on the throughput but also on the number of simultaneous VPN connections.

Secure Multi-Cloud Access

The secure multi-cloud access service allows enterprise customers to securely extend their private networks to the public cloud and thus to leverage cloud hosted services, assets and applications without compromising their data confidentiality and integrity. The solution offers consistent data protection across cloud providers.



Site-to-site and Network-to-network Encrypted IP security

The 6WIND VSR solution provides highly scalable DMVPN capabilities that allows small, mid-scale and large enterprises to securely create site-to-site, network-to-network or light SD-WAN networks over agnostic transport access such as Fiber, Radio Transmission, LTE, and 5G.

Specification

IP Networking:

- ▶ IPv4 and IPv6
- ▶ IPv6 auto-configuration
- ▶ Multi-tenancy (VRF)
- ▶ IPv4 and IPv6 tunneling
- ▶ IPv4 and IPv6 filtering
- ▶ Network address translation
- ▶ Multi-cast

Routing:

- ▶ BGP4, BGP4+
- ▶ BGP RPKI
- ▶ OSPFv2, OSPFv3
- ▶ RIPv1, RIPv2, RIPng
- ▶ Static routes & path monitoring
- ▶ BGP multi-path (ECMP)
- ▶ Policy base routing (PBR)
- ▶ MPLS
- ▶ BGP L3VPN
- ▶ BFD
- ▶ NHRP
- ▶ VXLAN EVPN

Quality of Service:

- ▶ Rate limiting per Interface
- ▶ Rate limiting per VRF
- ▶ Class-based QoS
- ▶ Classification:
 - ToS/IP/DSCP/CoS
- ▶ Shaping and policing
- ▶ Scheduling:
 - PQ, PB-DWRR

Management / Monitoring:

- ▶ SSHv2
- ▶ CLI
- ▶ NETCONF / YANG
- ▶ SNMP
- ▶ KPIs / telemetry (YANG -based)
- ▶ RBAC with AAA
- ▶ Syslog
- ▶ 802.1ab LLDP
- ▶ sFlow

L2 and Encapsulations:

- ▶ GRE, mGRE
- ▶ VLAN (802.1Q, QinQ)
- ▶ VXLAN
- ▶ LAG (802.3ad, LACP)
- ▶ Ethernet bridge

IP Services:

- ▶ DHCP server / client / relay
- ▶ DNS client / proxy
- ▶ NTP

Security:

- ▶ ACLs (stateless & stateful)
- ▶ uRPF
- ▶ CP protection
- ▶ BGP FlowSpec (IPv4, IPv6)

VPN IPsec:

IKE v1/v2 pre-shared keys or X509 certificates

- ▶ MOBIKE
- ▶ Encryptions:
 - 3DES, AES-CBC/GCM (128, 192, 256)
- ▶ Hash:
 - MD-5, SHA-1, SHA-2 (256, 384, 512) AES-XCBC (128)
- ▶ Key management:
 - RSA, DH MODP groups 1 (768 bits), 2 (1024 bits), 5 (1536 bits) and 14 (2048 bits), DH PFS
- ▶ EAP/Radius, EAP-MSCHAPv2
- ▶ Extended sequence numbers (ESN), large anti-replay windows
- ▶ High performance (AES-NI, QAT)
- ▶ Tunnel, transport or BEET mode
- ▶ Static and dynamic VTI
- ▶ Dynamic multi-point VPN
- ▶ OpenVPN

CG-NAT support:

- ▶ NAT44, NAT64
- ▶ Static NAT
- ▶ Port Assignment
 - Deterministic
 - Random or Parity
 - Port Block Allocation (PBA) or detailed logging per session
 - Per user/CPE session limiter
- ▶ Mapping and filtering
 - Endpoint-independent mapping and filtering
 - Address and port dependent mapping and filtering
- ▶ Hairpinning
- ▶ IP Pool Management
 - Dynamic IP pool resizing
 - Paired pooling
- ▶ Logging
 - Port batching
 - Advanced logging features
 - Syslog
- ▶ ALG Support
 - ICMP, FTP, TFTP, RTSP, PPTP, SIP, H323, DNS over UDP

High Availability:

- ▶ IKE/IPsec synchronization
- ▶ VRRPv2 (IPv4/IPv6)
- ▶ VRRPv3 (IPv6)

System Requirements

Processor:

- ▶ Single or multi-sockets Intel® Xeon® and Atom® processor

CPU/vCPU cores:

- ▶ 2 minimum (one for control, one for data plane)

Memory:

- ▶ 2GB minimum

NICs:

- ▶ Intel: 1G, 10G, 40G, 100G
- ▶ Mellanox: 10G, 25G, 40G, 50G, 100G: CX4, CX5, CX6*
- ▶ Broadcom NetExtreme E-Series

I/O virtualization:

- ▶ virtIO (Linux KVM)
- ▶ SR-IOV
- ▶ PCI passthrough
- ▶ VMXNET3 (VMware ESXi)
- ▶ ENA

Supported Hypervisors

- ▶ KVM (RH, Ubuntu, CentOS)
- ▶ VMware ESXi (6.5+),
- ▶ Microsoft Hyper-V

Public Clouds Support

- ▶ Amazon Web Services
- ▶ Microsoft Azure
- ▶ Google Cloud Platform

Deployments

- ▶ Bare metal, virtual machines, containers (Kubernetes/docker)
- ▶ Installation: PXE, USB, ISO, QCOW2, OVA
- ▶ Update / rollback support
- ▶ Provisioning: cloud-init, Ansible, ZTP
- ▶ Licensing: Online licensing system for feature and capacity enablement