VyOS Networks

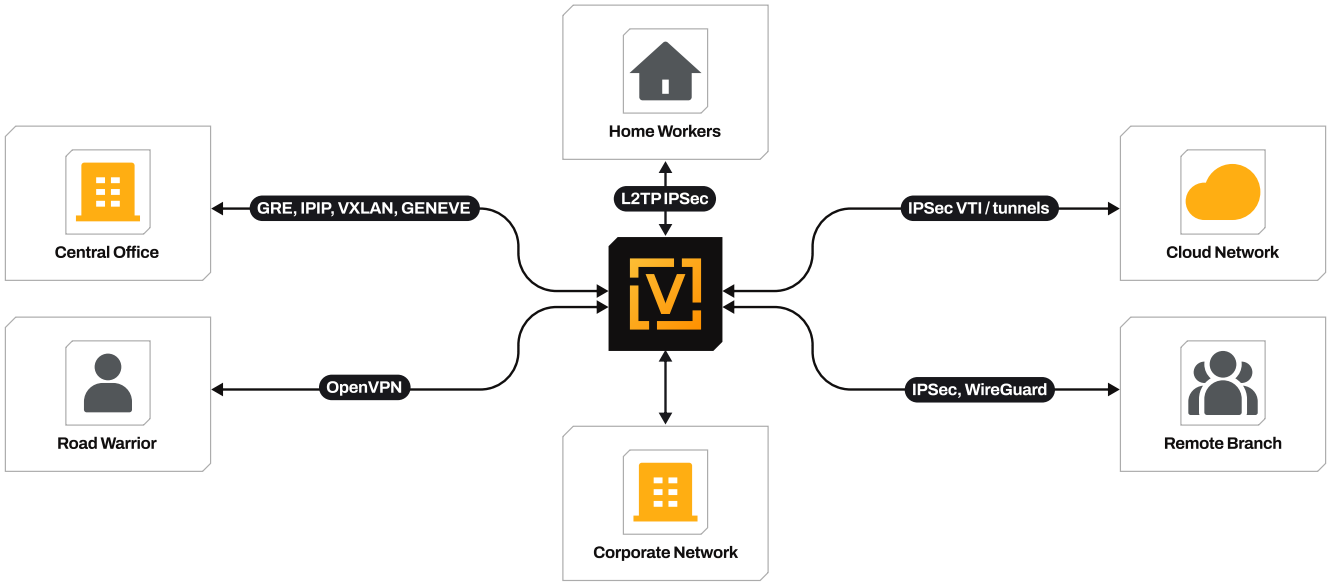
SOLUTION BRIEF

VYOS VPN GATEWAY

Why Your Business Needs a VPN Gateway – A Smarter Way to Connect and Protect

As enterprises accelerate their digital transformation, securely connecting users, offices, and cloud environments becomes critical. A **VPN Gateway** is the cornerstone of a secure, scalable, and high-performance network architecture that enables your business to thrive in a distributed world.

A **VPN Gateway** acts as a secure entry point into your network, allowing encrypted connections from remote users, branch offices, or partner networks. It ensures that all data traveling to and from your corporate environment is protected from unauthorized access, interception, or tampering.



Why Your Company Should Use a VPN Gateway:

- **Secure connectivity** between on-premises networks and cloud environments (e.g., Azure, AWS, GCP).
- **Trusted access** for remote employees, partners, and third-party vendors to corporate internal services
- **End-to-end encryption** of data across the public internet.
- **Efficient site-to-site communication** for global branch networks.
- **Centralized security enforcement** and traffic inspection at the network edge.

Whether you're enabling hybrid work, integrating cloud applications, or connecting global locations, a VPN Gateway offers the secure foundation your business needs to scale with confidence.

Essential Features of a VPN Gateway Solution:

- **Support for multiple VPN protocols** like IPsec/IKEv2, SSL/TLS, OpenVPN, and WireGuard.
- **High throughput and low latency** to support demanding workloads.
- **Scalability and auto-scaling** to handle dynamic user and traffic growth.
- **Redundancy and failover** for high availability and disaster recovery.
- **Strong authentication mechanisms** including multi-factor authentication (MFA)
- **Granular access control policies** based on user roles, IP ranges, or device posture.
- **Logging, monitoring, and analytics** for visibility, compliance, and troubleshooting.

Leading Technologies and Protocols Used:

- **IPsec/IKEv2** – the industry standard for secure site-to-site and remote access VPNs.
- **SSL VPN** – ideal for clientless or browser-based access.
- **OpenVPN & WireGuard** – flexible, modern protocols favored for remote user access.
- **Cloud-native VPN gateways** – such as **Azure VPN Gateway, AWS VPN, Google Cloud VPN**, enabling seamless hybrid cloud connectivity.

A VPN Gateway is more than a security layer—it's a business enabler. It empowers your workforce, connects your infrastructure, and protects your data wherever it travels. In today's cloud-first, hybrid-work world, choosing the right VPN Gateway isn't just smart—it's strategic.

Key Points – VyOS VPN Capabilities and Protocols

OpenVPN is ideal for end-user VPNs with VyOS:

- Easy to use and stable.
- Compatible with mobile phones, tablets, and laptops.
- Uses single-file client/server configuration profiles.

WireGuard:

- High-performance, user-friendly VPN.
- Widely adopted in cloud environments.
- Offers strong encryption and fast connectivity.

VyOS supports multiple tunneling protocols for network-to-network VPNs:

- GRE, IPIP, VXLAN, GENEVE.
- For encryption: IPSec (VTI or tunnel) and WireGuard are fully supported.
- L2TP/IPSec is recommended for networks with custom encryption needs.
- SSTP is an alternative when traditional VPN protocols are blocked or restricted.

OpenConnect:

- Provides SSL VPN compatibility with third-party vendors.
- Uses standard protocols: HTTP, TLS, DTLS.
- Supports advanced authentication: RADIUS, 2FA, etc.
- Bridges on-premise and cloud environments securely.

DMVPN (Dynamic Multipoint VPN):

- Allows VPNs between multiple sites without static configurations on all devices.

VPN Connectivity

Security on All Devices

Due to the increased amount of devices connected to corporate networks followed by the implementation of “bring your own device” policies, businesses are concerned about providing secure access to their systems for their remote workers.

IP Whitelisting

The option to determine which hosts that are allowed to access the network and the ability to assign static IP addresses to automatically trusted sources of traffic can be crucial to a secure network.

Cloud Agnostic Integration

Protection of sensitive data from a single interface becomes a priority for businesses as a consequence of integrating their VPNs into cloud-based platforms and services.

Precise User Segmentation

In order to properly monitor the access and usage of a corporate network, a granular policy-based permission system is necessary, which is beyond the capabilities of traditional VPNs.

Why VyOS?

- Save costs for your traveling workforce and stay safe in untrusted environments.
- Increased productivity and accelerated encryption performance, scalable to high connections counts.
- Better return on investment than a regular WAN for sensitive data.
- Security and privacy while keeping control over the traffic flow.
- Scalability with multiple protocols and platforms.
- Extended geographic presence across the world.
- Simple configuration of network services.

sales@vyos.io
vyos.io