VyOS Networks

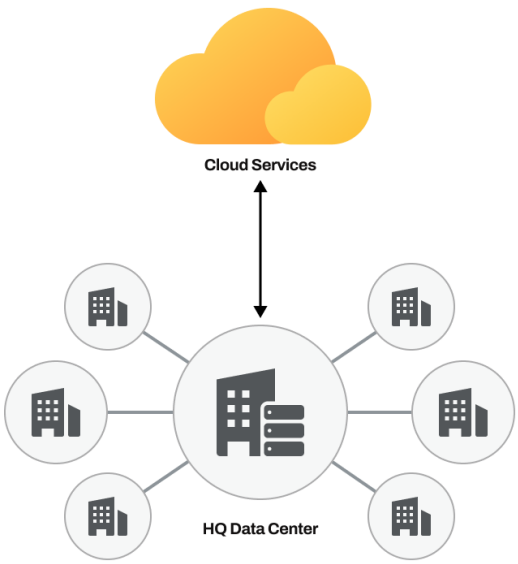
SOLUTION BRIEF

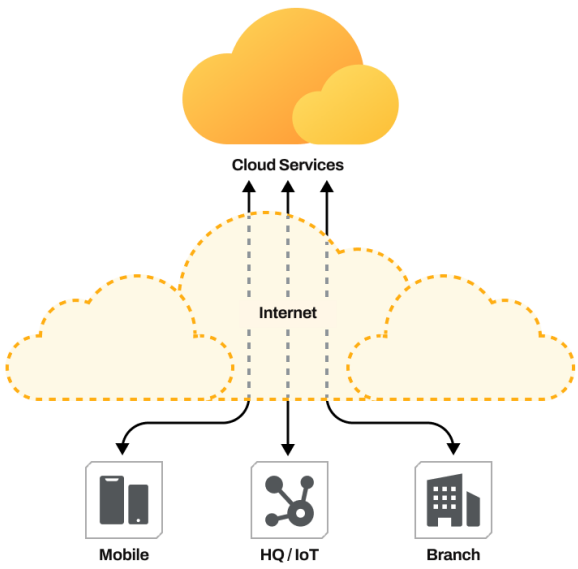
VYOS SECURITY GATEWAY

Why Your Business Needs a Security Gateway – The First Line of Defense

As businesses expand into hybrid, cloud, and distributed environments, safeguarding network traffic and user access has never been more critical. A Security Gateway is the foundation of a resilient cybersecurity strategy, providing centralized control, visibility, and protection against evolving threats.

A Security Gateway acts as the secure border of your network, inspecting, filtering, and enforcing policies on all incoming and outgoing traffic. By combining firewall, VPN, intrusion prevention, and advanced threat intelligence, it ensures that your corporate assets remain protected, whether hosted on-premises, in the cloud, or across branch networks.





Why Your Company Should Use a Security Gateway:

- **Unified protection** against malware, ransomware, and zero-day threats at the network edge.
- **Granular access** control for users, applications, and devices.
- **End-to-end encryption** and secure tunneling for remote employees and partners.
- **Application-aware firewalling** to enforce policies beyond simple IP/port filtering.
- **Integrated intrusion detection and prevention (IDS/IPS)** to block malicious traffic in real time.
- **Centralized visibility and logging** to simplify compliance and auditing.

Whether you're enabling secure remote work, adopting SaaS applications, or connecting multi-cloud environments, a Security Gateway is essential to protect sensitive data and business continuity.

Essential Features of a Security Gateway Solution:

- **IDS/IPS.** Proactive security that identifies and blocks cyber threats instantly.
- **VPN support** for secure site-to-site and remote access (IPsec, SSL, WireGuard, OpenVPN).
- **High availability and failover** to guarantee uptime.
- **Identity-aware security,** with MFA and integration to LDAP/Active Directory/IdPs.
- **Scalable performance** to support enterprise and service provider workloads.
- **Monitoring, analytics, and alerting** for real-time security visibility.

Leading Technologies and Protocols Used:

- **IPsec/IKEv2** – enterprise-grade VPN security.
- **WireGuard & OpenVPN** – modern, lightweight VPNs for remote access.
- **SSL/TLS inspection** – securing web traffic without compromising visibility.
- **IDS/IPS engines** – detecting and mitigating intrusions dynamically.
- **Application Layer Filtering** – managing traffic based on apps, not just ports.
- **Cloud-native security gateways** (Azure Firewall, AWS Network Firewall, GCP Cloud Armor) – extending protection across hybrid and multi-cloud networks.

VyOS Security Gateway Capabilities

VyOS offers a flexible and robust Security Gateway platform that adapts to enterprise and cloud needs:

Stateful firewall

With zone-based policies.

VPN protocols

IPsec, WireGuard, OpenVPN, L2TP/IPsec, SSTP, and OpenConnect.

Dynamic tunneling options

GRE, VXLAN and DMVPN for scalable site interconnects.

Advanced authentication

RADIUS, TACACS+, LDAP, 2FA.

Traffic shaping & QoS

Ensure performance for critical applications.

Unified logging & monitoring

Full visibility into traffic and security events.

In today's cloud-first, mobile, and distributed business environment, a Security Gateway is not just a firewall, it's your organization's shield. It secures your digital ecosystem, enables safe connectivity, and gives you the confidence to scale without compromise.

sales@vyos.io
vyos.io