Cybersecurity

Secure VPN

gigas

To securely and efficiently connect your company's network with your Cloud Datacenter at Gigas.

This new service replaces the traditional VPN solution with a virtual Next-Generation Firewall (NGFW) FortiGate, offering superior performance, security, and flexibility. Through a secure Internet tunnel, a robust connection is established between the client's infrastructure and the private network at Gigas, ensuring data integrity and confidentiality.

KEY FEATURES

- ✓ **High Performance and Scalability:** High bandwidth performance that scales according to the chosen virtual VPN model.
- ✓ **Multiple Tunnel Types:**
  - IPsec VPN (Site-to-Site): The industry standard for securely connecting networks. Ideal for permanently interconnecting offices with Gigas cloud.
  - SSL-VPN (Remote Access): Provides secure access for remote users (teleworking) via a web portal, without the need to configure complex routers on the user side.
- ✓ **Maximum Compatibility (Interoperability):**
  - Thanks to standards compliance, FortiGate guarantees IPsec tunnel creation with devices from almost any manufacturer (Cisco, Palo Alto, Check Point, Juniper, etc.).
  - Support for the most robust protocols and standards: IKE v1 and v2, AES (up to 256 bits), SHA-2, authentication with pre-shared keys (PSK) or digital certificates.
- ✓ **Complete Perimeter Security:** More than a VPN, as it incorporates IP and port filtering with NAT and PAT.
- ✓ **SD-WAN Capabilities:** Optimises traffic routing across multiple Internet connections, improving resilience and user experience.
- ✓ **Unlimited Bandwidth:** Traffic generated through the VPN does not consume the bandwidth of your Cloud Datacenter subscription.
- ✓ **Automated Management and Provisioning:** Real-time deployment and simplified management from the Gigas control panel.

Flexible Models for Every Need

Choose the plan that best fits your performance and scalability requirements. All models include the ability to support both 'LAN to LAN' and 'LAN to Client' tunnels. Additionally, the bundles include computing resources (vCores, RAM, and Storage) and the FortiCare Premium package.

- ✓ **VPN 1v:** For small and medium-sized businesses with fewer than 100 employees and moderate bandwidth requirements.
- ✓ **VPN 2v:** For growing businesses with higher traffic volumes, up to 200 users, and wanting to use advanced security features without impacting performance.
- ✓ **VPN 4v:** For large corporations with up to 400 users, complex networks, and critical applications that demand maximum performance, high availability, and comprehensive security inspection.

CONNECTION SCENARIOS

The client's network topology is transparent to Gigas, only a fixed public IP and a device to establish the tunnel are required.

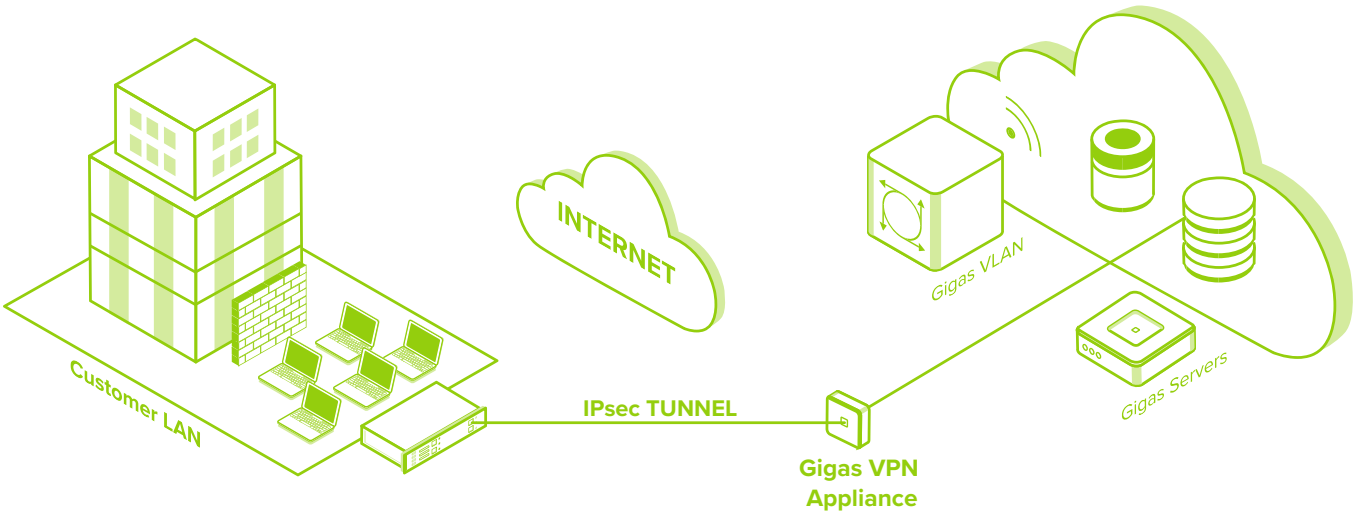
Scenario 1: Network-to-Network Connection
(Lan to Lan)

This scenario is designed to securely and permanently connect the local (LAN) network of an office or company with the Cloud Datacenter at Gigas. The connection is established through a secure IPsec tunnel, which is the industry standard for robustly interconnecting networks over the Internet.

How does it work?
In this topology, our virtual appliance, located in Gigas' infrastructure, acts as the endpoint of the VPN tunnel. The tunnel originates from the main firewall or router device already present in the client's network. This model is ideal, as the client's network topology is transparent to Gigas; only a fixed public IP and a device on the client side capable of creating IPsec tunnels are required.

Main Advantages:

- ✓ **Maximum Compatibility:** Thanks to the use of standard protocols such as IPsec, IKE v1/v2, and AES, Gigas' solution guarantees interoperability and the creation of tunnels with equipment from virtually any other manufacturer, such as Cisco, Palo Alto, or Check Point.
- ✓ **Transparent Integration:** The solution integrates seamlessly with the client's existing network infrastructure, connecting VLANs and applying the necessary routing rules.
- ✓ **Simplified Management:** The client manages their side of the connection, while Gigas manages the virtual appliance, which is automatically provisioned and can be administered from the Gigas control panel.



Scenario 2: Client-to-Network Connection
(Client to Lan / Remote access)

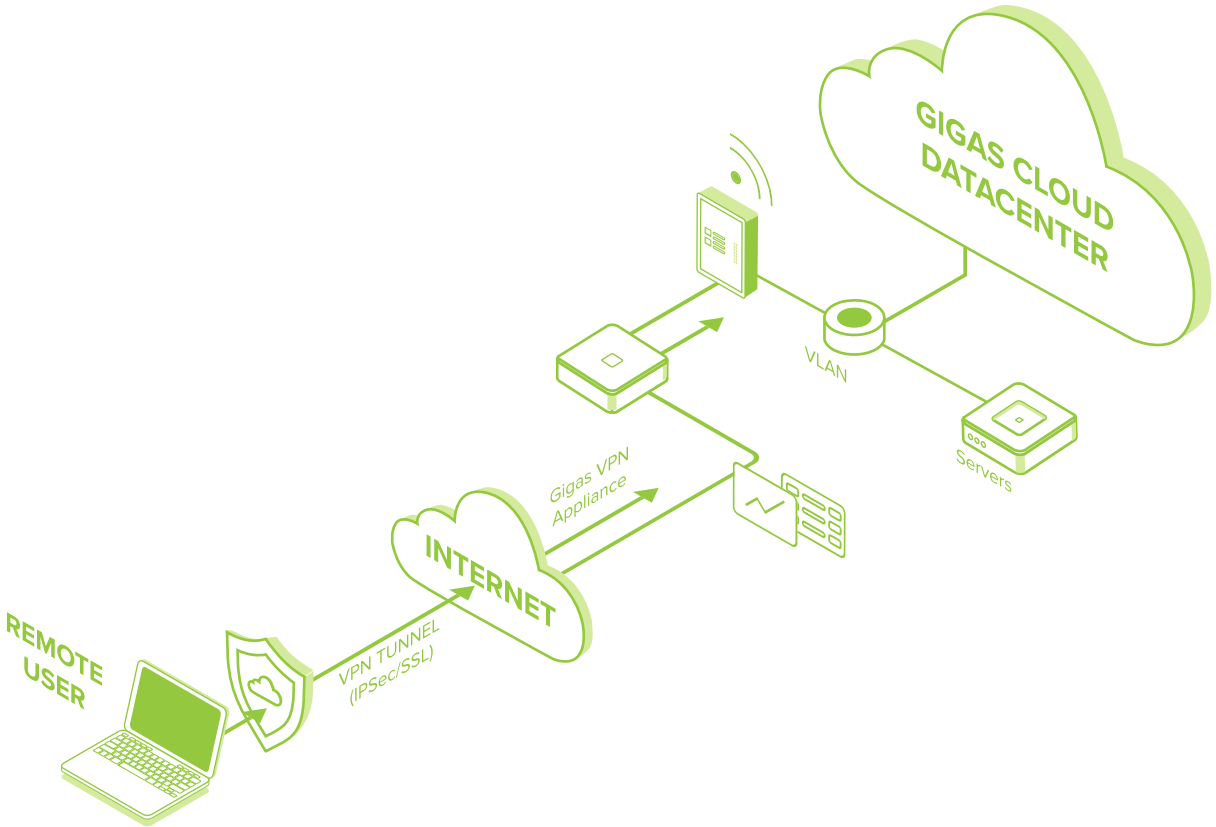
This model is designed to provide secure access to the corporate network at Gigas for individual users located outside the office, such as remote workers or mobile employees. FortiGate technology offers great flexibility by enabling two types of secure tunnels for this purpose, centrally managed by the virtual appliance at Gigas. Both modes can use the FortiClient software for a unified user experience.

Remote Connection Modes:

- ✓ **SSL-VPN:** This is a highly flexible option, ideal for users who need connectivity from multiple locations and networks (hotels, public networks, etc.
  - **Web Portal Mode:** Allows quick, clientless access to corporate web applications and specific resources via a simple web browser. No dedicated software installation is required on the user's device.
  - **Tunnel Mode:** Uses FortiClient software to create an encrypted tunnel. Its main advantage is that it uses TCP port 443 (the same as HTTPS web traffic), which ensures connectivity even in networks with restrictive security policies that block other VPN ports.

- ✓ **IPsec-VPN:** This mode also uses the FortiClient software to establish the connection. It is renowned for its high performance and robustness, creating a tunnel that securely integrates the user's device into the company's network as if it were physically in the office. It is the preferred option for users who require full, high-performance access to all network resources, not just web services. The solution supports the most robust protocols and standards, such as IKEv1/v2 and AES-256 encryption, ensuring maximum security.

Regardless of the chosen method, the virtual appliance at Gigas centralises authentication and traffic management, allowing granular security policies to be applied for each user and ensuring controlled and protected access to the company's critical data and applications.



VPN SOLUTION CAPACITY

Advanced VPN	vCores	GB RAM	Associated Pack
VPN 1v	1	4	Forticare Premium
VPN 2v	2	8	Forticare Premium
VPN 4v	4	16	Forticare Premium

Performance Metrics

The virtualised VPN platform from Gigas offers defined and scalable performance.

Processing capacity is not limited to bandwidth, but is measured by the ability to handle a high volume of concurrent sessions and to perform traffic inspection (NGFW) without creating bottlenecks.

The following matrix details the key performance indicators for each model, allowing you to select the exact capacity your business needs. The number of simultaneous users may vary depending on usage intensity, but the session and SSL-VPN user metrics are an excellent guide to understanding the capacity of each solution.

Performance Metric	VPN 1v	VPN 2v	VPN 4v
Firewall Performance (maximum)	12 Gbps*	15 Gbps*	28 Gbps*
NGFW Performance	850 Mbps*	1.5 Gbps*	2.5 Gbps*
VPN IPsec Performance	1 Gbps*	1.5 Gbps*	3 Gbps*
VPN SSL Performance	800 Mbps	830 Mbps	2 Gbps*
Concurrent TCP Sessions	1.0 millions	2.6 millions	4.3 millions
New Sessions/second	85.000	100.000	125.000
Concurrent SSL-VPN Users	1.000**	2.000**	4.500**
Site-to-Site IPsec Tunnels	2.000**	2.000**	2.000**
Client VPN Tunnels (maximum)	6.000**	12.000**	20.000**

* The Gigas VPN service is delivered with a bandwidth ranging from 100 to 500 Mbps depending on the geographical region of the CDC. To obtain the maximum values shown in the table, please check with Gigas the bandwidth of the bundle assigned in each CDC and the available options for contracting additional capacity for the solution.
** Refers to the maximum number of VPN clients (FortiClient) that can have a tunnel configuration on the firewall. These values are reference figures provided by the manufacturer and may vary depending on the type of applications and the workload the appliance is subjected to.