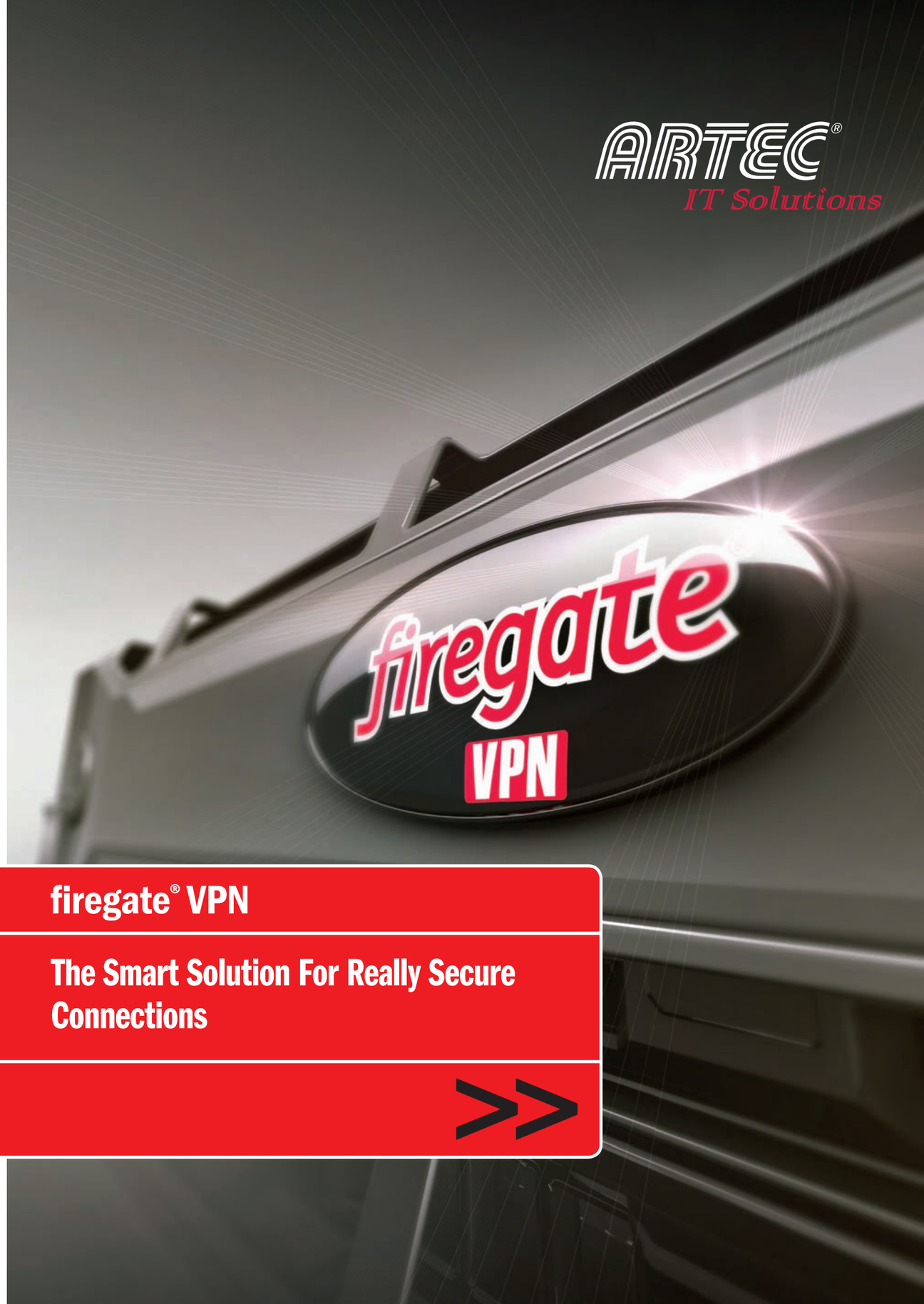
ARTEC Cloud Solutions
MADE IN GERMANY

Good to Know: 100 % Made in Germany
firegate® VPN was especially developed for highly secure connections in cloud projects. In this context the security of data is of central importance for companies and organizations. EMA® Cloud Services by ARTEC are built and operated in Germany. Development, data storage, maintenance, and support are all fully handled in Germany to ensure that your data never leaves German borders.

- All products and technologies are developed in Germany under the control of ARTEC and are free of third-party technologies.
- Your data is optimally protected under German privacy regulations.
- ARTEC is a solid and privately owned company without investors that influence business operations. The company's headquarter is in Karben near Frankfurt am Main, Germany.
- ARTEC's service level agreements (SLA) are in accordance with German law.
- The jurisdiction for all contractual and legal matters is in Germany.
- ARTEC's customer service operates from Germany and all support agents speak fluent German and English.

Advantages of firegate® VPN

- ✓ Connects locations with each other using secure encryption
- ✓ Ensures secure access to hosted data and applications
- ✓ Optimized for monitoring and full managed service of remote systems
- ✓ Little to no need for administration (set and forget)
- ✓ No complex credential management required
- ✓ Preconfigured delivery to get you started right away
- ✓ Works with every router and standard Internet connection
- ✓ Includes specialized data compression algorithms that deliver high performance and throughput
- ✓ Uses Trusted Computing technologies to detect and prevent tampering reliably
- ✓ Saves time and costs with its appliance-based design
- ✓ Tailored for use with ARTEC's EMA® and VSTOR® solutions



AMERICA
ARTEC IT Solutions USA
1600 Parkwood Circle
Atlanta, Georgia 30339, USA
Phone: +1 - 855 - 462 - 7832
Fax: +1 - 678 - 666 - 5153
E-mail: info@artec-it.com
Internet: http://www.artec-it.com

EMEA
ARTEC IT Solutions AG
Robert-Bosch-Str. 38
61184 Karben, Germany
Phone: +49 - 6039 - 9154 - 0
Fax: +49 - 6039 - 9154 - 54
E-mail: info@artec-it.de
Internet: http://www.artec-it.de

ASIA PACIFIC
ARTEC IT Solutions AP
#1003 U-Top Tech Valley, 7, Beobwon-ro 6-gil, Songpa-gu, Seoul 05855, Korea
Phone: +82 - 2 - 515 - 3349
Fax: +82 - 2 - 6008 - 3403
E-mail: info-ap@artec-it.com
Internet: http://www.artec-it.com

Turning Data Into Information

ARTEC® IT Solutions

firegate® VPN

The Smart Solution For Really Secure Connections

firegate® VPN – For Really Secure Connections

firegate® VPN was developed for the secure, encrypted connection of individual sites and systems for cloud projects. This allows corporations and organizations to ensure high-security access to hosted data and applications.

The firegate® VPN concept by ARTEC is based on a hardware-secured, point-to-point VPN that allows it to achieve a totally new level of security. This applies especially in comparison to conventional VPNs, which in terms of their structure are a combination of hardware and software and are not always entirely successful.

firegate® VPN establishes a dedicated connection between two appliances: a source network (e.g. company network) and a target network (e.g. cloud service provider). In this way, the tasks involved in establishing a secure connection and the access control are strictly separated from each other, and the multitude of connections of individual terminals to the VPN is replaced by a single, high-security connection. The firegate® VPN appliances take on the tasks of access control for all the nodes and clients connected to the source and target networks.

The firegate® VPN technology is based on trusted computing as a foundation for the mutual detection and verification of trustworthy communication partners. In the appliances, trusted computing, as a hardware-based security platform, is responsible for protecting all the critical data in the appliances and in addition also protects the appliance from all forms of tampering. This architecture leads to the decisive advantages of firegate® VPN in the relevant application scenarios.

Basic Application Scenarios

In the corporate environment, firegate® VPN is predestined for two basic application scenarios.

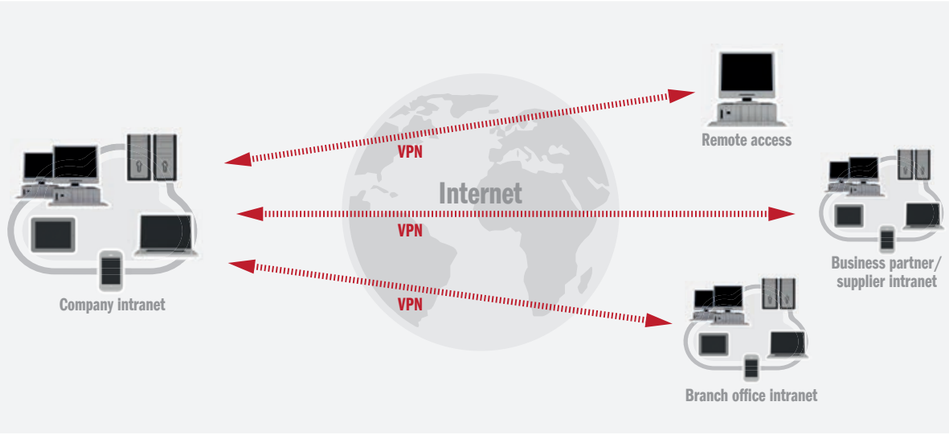
Client Access to the Cloud

The firegate® VPN appliance allows any number of terminals in the company network secure access to the cloud-based services. What is important here is that the clients do not have to be administered by or even be known to the cloud service provider, but can be handled locally in a manner that is easy and flexible. From the perspective of the cloud, there is only one single, secure connection to the company network per customer, which represents a provisional separation of tasks.

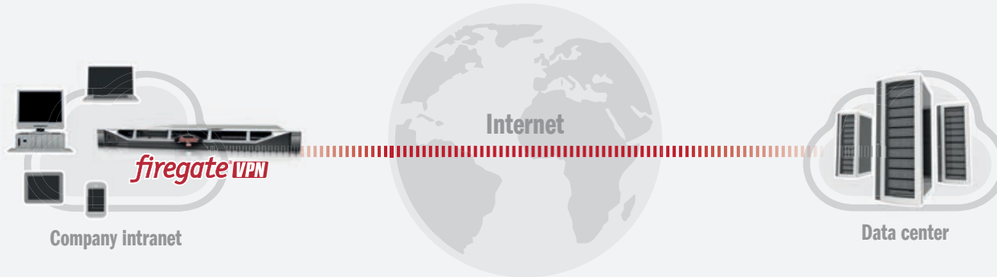
Service Access to the Company Network

Conversely, firegate® VPN can also facilitate secure access to a company network for an external service provider. Here, the appliance is delivered by the service provider and provided with the necessary access permissions on the customer's premises for the server and clients to be connected in the company network. During the installation, customers can be assured that the configuration of the appliance gives the service provider only the permissions that are absolutely necessary. In this way, a wide range of application scenarios, such as remote monitoring and maintenance or an externally hosted archive, can be implemented securely.

ARTEC customers are already using firegate® VPN extensively to secure their Enterprise Managed Archive® (EMA®) solutions in both scenarios mentioned. On the one hand, firegate® VPN provides secure maintenance access for ARTEC to the EMA® appliance on the customer's premises. On the other hand, occasionally an externally hosted EMA® archive must also establish connections back to the company network for tasks like the synchronization of folder structures and file servers or the return of archived data. Here as well, firegate® VPN ensures a high-security connection.



firegate® VPN



Easy Initial Startup

Initial startup of a firegate® VPN appliance is designed to be very easy for the customer. After customers have provided an IP address, gateway, subnet mask and DNS server for access, and certain information on their infrastructure, the appliance is preconfigured by ARTEC. After delivery, customers can transfer access permissions to the appliance as needed so that, for example, the ARTEC archiving service can access all the necessary data sources for synchronization, which does not require any sensitive information to be transferred to ARTEC.

Zero-Configuration Connection

Every firegate® VPN appliance is delivered uniquely and unalterably "engraved" with its trusted remote terminal, which is able to connect to the target network at any time and from anywhere – assumed there is an Internet connection. All necessary data and settings are already present in the appliance and secured by trusted computing in the hardware. This eliminates many steps to configure specifics such as server addresses, communication ports, authentication methods and protocols, and, in particular, also the generation of keys for secure communication.

Easy Integration of Terminals

Instead of configuring the VPN access into individual clients, firegate® VPN allows central administration of the access control for all terminals. They can obtain access to the VPN using any authentication methods desired.

Hardware-Based Security Thanks to Trusted Computing

On the one hand, trusted computing protects all the sensitive data of the firegate® VPN appliance against unauthorized change and readout. On the other hand – and even more importantly – trusted computing also provides methods that can be used to test the appliances from a distance. In this way, every time a connection is established, trusted computing ensures that the hardware and software of the remote terminal have not been changed. These properties are bound to the identity of every appliance, which is also hardware secured. This makes authentication using the firegate® VPN a high-security process.