ARTEC Cloud-Lösungen™
MADE IN GERMANY

Gut zu wissen: 100 % Made in Germany
firegate® VPN wurde gezielt für die hochsichere Anbindung bei Cloud-Projekten entwickelt. In diesem Kontext ist die Sicherheit der Daten für Unternehmen und Organisationen von zentraler Bedeutung. Mit den EMA® Cloud-Services von ARTEC setzen Sie dabei ganz konsequent auf Cloud-Lösungen »**Made in Germany**«: Von der Entwicklung über die Datenspeicherung bis hin zu kontinuierlicher Betreuung und Support. Sämtliche Daten bleiben zu jedem Zeitpunkt in deutschen Händen.

- Alle Produkte und Technologien werden in Deutschland unter der Kontrolle von ARTEC entwickelt und sind frei von Technologien von Drittanbietern.
- Ihre Daten sind nach deutschen Datenschutzrichtlinien optimal geschützt.
- ARTEC ist ein solides, in Deutschland gegründetes Privatunternehmen mit Hauptsitz in Karben bei Frankfurt am Main, welches völlig unabhängig von Investoren-Einflüssen agiert.
- ARTEC schließt mit seinen Cloud-Service-Kunden Verträge mit Service Level Agreements (SLA) nach deutschem Recht.
- Der Gerichtsstand für alle vertraglichen und juristischen Angelegenheiten liegt in Deutschland.
- ARTEC stellt für Kundenanfragen einen lokal ansässigen, deutschsprachigen Service und Support zur Verfügung.

Die Vorteile von firegate® VPN

- ✓ Verbindet Standorte verschlüsselt miteinander
- ✓ Gewährleistet sicheren Zugang zu gehosteten Daten und Applikationen
- ✓ Eignet sich optimal zum Monitoring sowie für Full Managed Services für Remote-Systeme
- ✓ Geringer Administrationsaufwand
- ✓ Keine aufwendige Verwaltung von Anmeldeinformationen
- ✓ Vorkonfigurierte Auslieferung
- ✓ Betrieb an jedem standardmäßigen Router oder DSL-Anschluss möglich
- ✓ Hohe Performance durch spezielle Daten-Kompression
- ✓ Durch Trusted Computing garantiert keine Manipulationsmöglichkeiten
- ✓ Zeit- und kosteneffektive Box-Lösung
- ✓ Optimal auf die Zusammenarbeit mit den ARTEC-Lösungen EMA® und VSTOR® abgestimmt

AMERICA
ARTEC IT Solutions USA
1600 Parkwood Circle
Atlanta, Georgia 30339, USA
Telefon: +1 - 855 - 462 - 7832
Telefax: +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
Telefon: +49 - 6039 - 9154 - 0
Telefax: +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
Telefon: +82 - 2 - 515 - 3349
Telefax: +82 - 2 - 6008 - 3403
E-Mail: info-ap@artec-it.com
Internet: http://www.artec-it.com

Turning Data Into Information

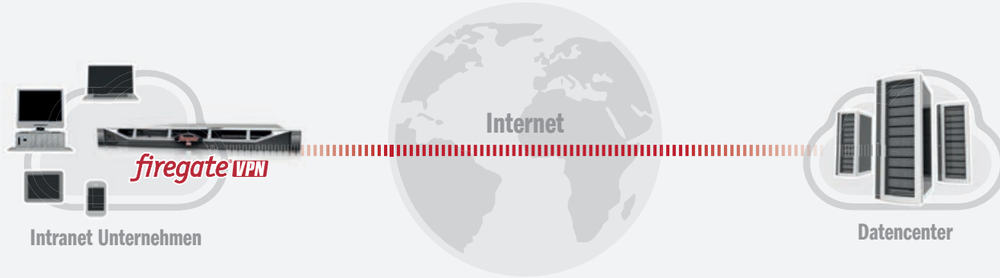
firegate® VPN

ARTEC® IT Solutions

Die clevere Lösung für wirklich sichere Verbindungen

>>

firegate® VPN



firegate® VPN – Für wirklich sichere Verbindungen

firegate® VPN wurde für die sichere, verschlüsselte Anbindung von einzelnen Standorten und Systemen bei Cloud-Projekten entwickelt. Unternehmen und Organisationen sind damit in der Lage, einen hochsicheren Zugang zu gehosteten Daten und Applikationen zu gewährleisten.

Das firegate® VPN-Konzept von ARTEC basiert auf einem hardwaregesicherten Punkt-zu-Punkt-VPN und erreicht somit ein völlig neues Sicherheitsniveau. Dies gilt insbesondere im Gegensatz zu herkömmlichen VPNs, die aktuell hinsichtlich des Aufbaus eine mehr oder weniger gelungene Kombination aus Hardware und Software bilden.

firegate® VPN baut grundsätzlich eine fest zugeordnete Verbindung zwischen zwei Appliances auf: einem Quellnetzwerk – etwa einem Unternehmensnetz – und einem Zielnetzwerk – zum Beispiel einem Cloud-Dienstleister. Dadurch werden die Aufgaben des Aufbaus einer gesicherten Verbindung und der Zugangskontrolle sauber voneinander getrennt und die Vielzahl der Verbindungen einzelner Endgeräte in das VPN durch eine einzige, hochsichere Verbindung ersetzt. Für alle angeschlossenen Knoten und Clients im Quell- und Zielnetzwerk übernehmen die firegate® VPN-Appliances die Aufgaben der Zugangs- und Zugriffskontrolle.

Die Technologie von firegate® VPN basiert wesentlich auf Trusted Computing als Grundlage für die gegenseitige Erkennung und Überprüfung vertrauenswürdiger Kommunikationspartner. Trusted Computing sorgt in den Appliances dabei als hardwarebasierte Sicherheitsplattform für den Schutz aller kritischen Daten und sichert die Appliances zudem gegen jede Form der Manipulation. Dieser Aufbau führt zu den entscheidenden Vorteilen von firegate® VPN in den entsprechend relevanten Anwendungs-Szenarien.

Grundlegende Anwendungsszenarien

Im Unternehmensumfeld ist firegate® VPN für zwei grundlegende Anwendungs-Szenarien prädestiniert.

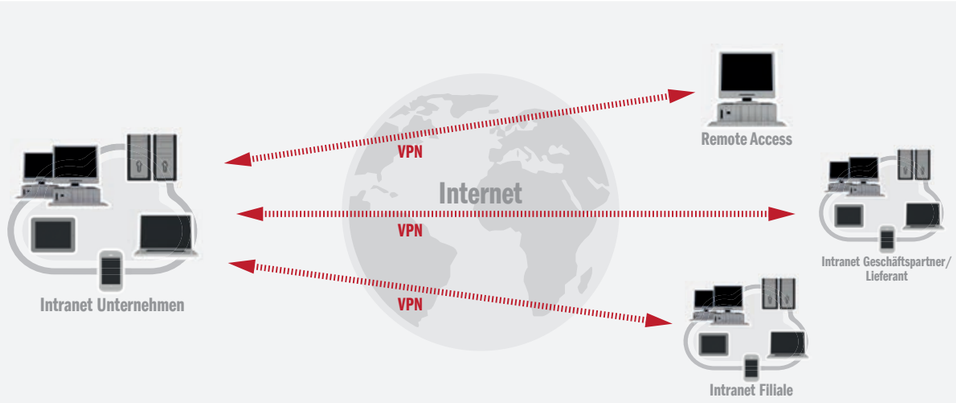
Client-Zugang zur Cloud

Hierbei ermöglicht die firegate® VPN-Appliance im Unternehmensnetzwerk einer beliebigen Anzahl von Endgeräten den sicheren Zugang zu cloud-basierten Diensten. Entscheidend dabei ist, dass die Administration der Clients nicht beim Cloud-Dienstleister durchgeführt oder gar mit diesem verhandelt werden muss, sondern einfach und flexibel lokal gehandhabt werden kann. Aus Sicht der Cloud besteht pro Kunde nur eine einzige, sichere Verbindung zum Firmennetz, was einer provisorischen Arbeitsteilung entspricht.

Servicezugang zum Firmennetz

Umgekehrt kann firegate® VPN auch den sicheren Zugang zu einem Firmennetz für einen externen Dienstleister ermöglichen. Dabei wird die Appliance vom Dienstleister ausgeliefert und vor Ort beim Kunden mit den nötigen Zugangsrechten für die anzuschließenden Server und Clients im Firmennetz versehen. So können sich Kunden während der Installation überzeugen, dass die Konfiguration der Appliance dem Dienstleister nur die unbedingt nötigen Rechte einräumt. Auf diese Weise lassen sich vielfältige Anwendungsszenarien wie etwa Remote-Überwachung und -wartung oder ein extern gehostetes Archiv sicher realisieren.

ARTEC-Kunden verwenden firegate® VPN bereits intensiv zur Sicherung ihrer EMA®- und VSTOR®-Lösungen in beiden genannten Szenarien. Einerseits realisiert firegate® VPN einen sicheren Wartungszugang für ARTEC zu der beim Kunden befindlichen EMA®-Appliance. Andererseits muss ein extern gehostetes EMA®-Archiv für Aufgaben wie die Synchronisierung von Ordnerstrukturen und Fileservern oder das Rückspielen von archivierten Daten gelegentlich auch Verbindungen zurück ins Firmennetz ausführen. Auch hier sorgt firegate® VPN für eine hochsichere Verbindung.



Einfache Inbetriebnahme

Die Inbetriebnahme einer firegate® VPN-Appliance gestaltet sich für Kunden denkbar einfach. Nachdem Kunden IP-Adresse, Gateway, Subnetzmaske sowie DNS-Server zum Zugang und einige Informationen über ihre Infrastruktur zur Verfügung gestellt haben, wird die Appliance von ARTEC vorkonfiguriert. Nach der Auslieferung können Kunden je nach Bedarf Zugriffsrechte auf die Appliance übertragen, so dass zum Beispiel der Archivierungsdienst von ARTEC auf alle nötigen Datenquellen zur Synchronisierung zugreifen kann, wofür keine sensiblen Informationen an ARTEC übertragen werden müssen.

Konfigurationsloser Verbindungsaufbau

Jede firegate® VPN-Appliance ist bei der Auslieferung eindeutig und unveränderbar auf ihre vertrauenswürdige Gegenstelle „geprägt“, die sie – eine bestehende Internetverbindung vorausgesetzt – jederzeit auffinden kann. Alle notwendigen Daten und Einstellungen sind in der Appliance bereits vorhanden und hardwareseitig mit Trusted Computing gesichert. Dadurch entfallen viele Schritte der Konfiguration von zum Beispiel Serveradressen, Kommunikations-Ports, Authentifizierungsmethoden und Protokollen und insbesondere auch die Erzeugung von Schlüsseln für die sichere Kommunikation.

Leichte Einbindung von Endgeräten

Statt auf den einzelnen Clients den VPN-Zugang zu konfigurieren, erlaubt firegate® VPN die zentrale Administration der Zugriffskontrolle aller Endgeräte. Diese können über frei wählbare Autorisierungsmethoden Zugang zum VPN erhalten.

Hardwarebasierte Sicherheit durch Trusted Computing

Trusted Computing sichert zum einen alle sensitiven Daten der firegate® VPN-Appliance gegen unberechtigte Veränderung und Auslesen. Zum anderen – und noch wichtiger – stellt Trusted Computing aber auch die Methoden bereit, mit denen sich die Appliances aus der Ferne überprüfen lassen. So ist bei jedem Verbindungsaufbau sichergestellt, dass Hard- und Software der Gegenstelle nicht verändert wurden. Diese Eigenschaften sind an die – ebenfalls hardwaregesicherte – Identität jeder Appliance gebunden. Damit wird die Authentifizierung bei firegate® VPN zu einem hochsicheren Vorgang.