ARTEC®
IT Solutions

WHITEPAPER //

Virtual Private Networks – Mächtige Technologie mit Fallstricken

>>

INHALTSVERZEICHNIS

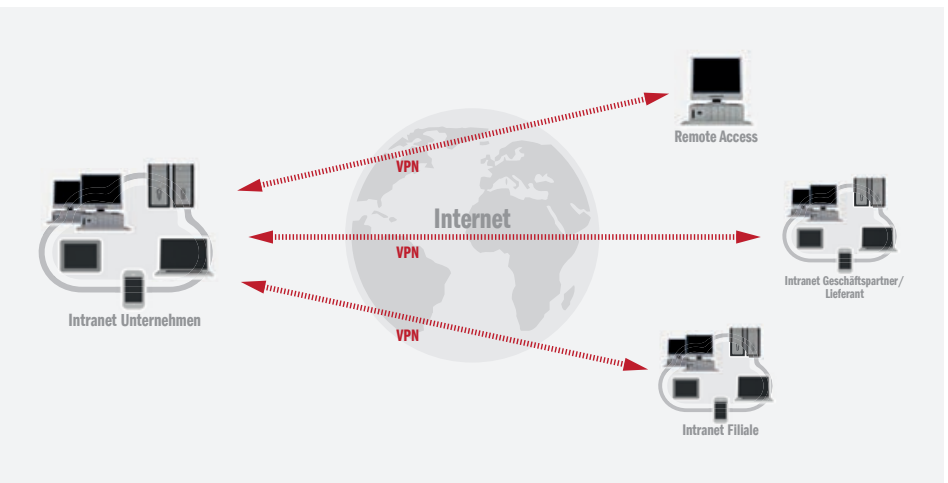
VIRTUAL PRIVATE NETWORKS – MÄCHTIGE TECHNOLOGIE MIT FALLSTRICKEN

Die zunehmende Mobilität von Mitarbeitern in Unternehmen führt dazu, dass bei Kunden und Partnern, also „off-premise“, immer mehr und komplexere Aufgaben erfüllt werden müssen, die teilweise in den Kernbereich des Unternehmens hineinreichen. Es ist daher unerlässlich, dass Mitarbeiter im Außeneinsatz auf Dienste und Daten der Unternehmens-IT zugreifen können. Die Sicherheit der Daten und Anwendungen, auf die durch „fremde“ Netze zugegriffen wird, hat dabei höchste Priorität.

Virtual Private Networks (VPNs) haben sich als wirtschaftliche Lösung für den Fernzugriff auf Unternehmensnetze weitgehend durchgesetzt. Der entscheidende Vorteil von VPNs ist die transparente Nutzung einer allgemein verfügbaren Kommunikations-Infrastruktur – dem Internet – für einen proprietären Zweck: Die Erweiterung des eigenen Firmennetzes außer Haus.

VPNs werden üblicherweise durch den Einsatz von VPN-Gateways abgesichert, also durch logische oder physische Appliances, die als Kommunikationsendpunkt für die extern angeschlossenen Geräte dienen. Das VPN-Gateway erfüllt sicherheitsrelevante Aufgaben wie Verschlüsselung und Authentifizierung sowie die Zugriffskontrolle auf Teilnetze. Über VPN-Gateways lassen sich heute die verschiedensten Endgeräte bzw. „Clients“ in Firmennetze einbinden – vom Laptop über das Smartphone oder Tablet bis hin zu speziellen Geräten wie Kassenscannern.

Neben ihren vielen offensichtlichen Vorteilen haben klassische VPNs aber auch ernstzunehmende Nachteile.



Typische VPN-Architektur

Hoher Kompetenzbedarf für Konfiguration und Administration

Die Verwaltung von VPNs umfasst verschiedene Bereiche: IP-Adressen und ihre Zuweisung, Protokoll-Konfigurationen, Verwaltung von Teilnetzen, Auswahl und Einstellung von Sicherheitstechniken und vieles mehr. Dies erfordert allein aufgrund der vielfältigen Realisierungsmöglichkeiten und zugehörigen Optionen fachlich geschultes Personal und bringt Beratungsbedarf in der Startphase mit sich. Zudem besitzen moderne VPN-Appliances meist sehr viele Features, die sie zu anspruchsvollen und komplexen Produkten machen. Client-seitig muss zudem für die vielen verschiedenen Typen von Endgeräten entsprechend angepasste VPN-Software eingesetzt und gepflegt werden.

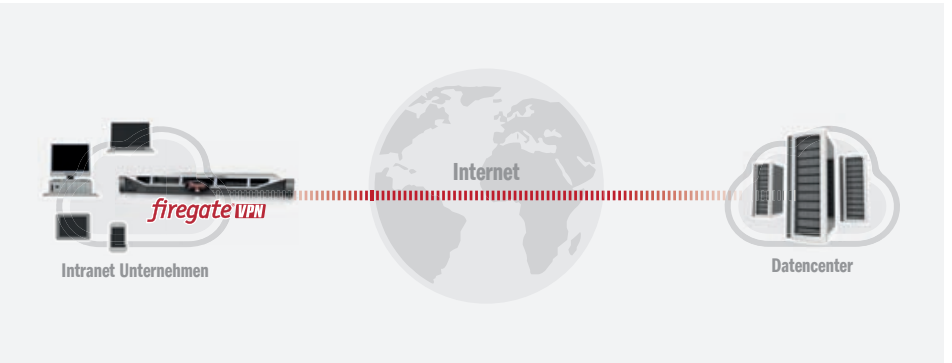
Aufwendige Verwaltung von Anmeldeinformationen

Die Sicherheit von VPNs basiert auf dedizierten Anmeldeinformationen – so genannten „Credentials“ – für Nutzer und Endgeräte. Neben Passwörtern werden hierfür typischerweise digitale kryptographische Zertifikate verwendet. VPN-Lösungen bieten dazu Anbindungen an Nutzerverzeichnisse, wie zum Beispiel LDAP-Server, und eine Public-Key-Infrastruktur. Dennoch bleibt die Verwaltung und hierbei insbesondere das Ausrollen der Credentials auf jedes einzelne Endgerät und für jeden einzelnen Nutzer eine praktische Herausforderung. Häufig sind Administratoren gezwungen, jedes Endgerät vor Ort zu warten, um es in das VPN einzubinden.

Clients als Sicherheitslücken

Noch wesentlicher als die bereits genannten praktischen Probleme von klassischen VPNs ist ein prinzipbedingtes Sicherheitsproblem: Jeder Client, der in falsche Hände gerät – hier sei etwa ein gestohlenes oder verloren gegangenes Laptop oder Smartphone erwähnt – ist ein potenzielles Einfallstor in das VPN. Ein Angriff auf ein Endgerät kann lange unentdeckt oder ungemeldet bleiben. In diesem Zeitraum bleibt der Teil des VPNs, auf den dieser Client Zugriff hat, ungeschützt. Noch prekärer wird das Sicherheitsproblem durch die bereits beschriebene Heterogenität der Endgeräte, die in der Regel völlig unterschiedliche Voraussetzungen in Bezug auf Hard- und Softwaresicherheit haben. Es ist daher empfehlenswert, VPN-Lösungen mit mobilen Clients nicht ohne zusätzliche Sicherheitslösungen für diese Endgeräte zu betreiben – etwa Anwendungen speziell zur Fernkontrolle und -abschaltung, etc.

FIREGATE VPN – DIE PUNKT-ZU-PUNKT VPN-LÖSUNG



Wie beschrieben, stellen herkömmliche VPNs architektonisch eine mehr oder weniger gelungene Kombination aus Hardware (VPN-Gateway-Appliances, Clients) und Software (Server und Client) dar. Im Gegensatz dazu steht das firegate VPN-Konzept des hardwaregesicherten Punkt-zu-Punkt-VPN. Hierbei bauen immer zwei firegate VPN-Appliances zwischen einem Quellnetzwerk – etwa einem Unternehmensnetz – und einem Zielnetzwerk – zum Beispiel einem Cloud-Dienstleister – eine fest zugeordnete Verbindung auf. Dadurch werden die Aufgaben des Aufbaus einer gesicherten Verbindung und der Zugangskontrolle sauber voneinander getrennt und die Vielzahl der Verbindungen einzelner Clients in das VPN durch eine einzige, hochsichere Verbindung ersetzt. Für alle angeschlossenen Knoten und Endgeräte in 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 schützt die Appliance zudem gegen jede Form der Manipulation. Dieser Aufbau führt zu den entscheidenden Vorteilen von firegate VPN in relevanten Anwendungsszenarien.

Konfigurationsloser Verbindungsaufbau

Jede firegate VPN-Appliance ist bei der Auslieferung eindeutig und unveränderbar auf ihre vertrauenswürdige Gegenstelle „geprägt“, die sie jederzeit auffinden kann (bei bestehender Internetverbindung). 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, Kommunikationsports, Authentifizierungsmethoden und Protokollen und insbesondere auch die Erzeugung von Schlüsseln für die sichere Kommunikation.

Einfache 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

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.

Im Unternehmensumfeld ist firegate VPN prädestiniert für zwei grundlegende Anwendungsszenarien:

a) **Client-Zugang zur Cloud**.
   Hierbei ermöglicht die firegate VPN-Appliance im Unternehmensnetz einer beliebigen Anzahl von Endgeräten den sicheren Zugang zu cloudbasierten Diensten. Entscheidend ist hierbei, 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. Dies entspricht einer subsidiären Arbeitsteilung.

b) **Servicezugang zum Firmennetz.**
   Umgekehrt kann firegate VPN 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 kann sich der Kunde während der Installation überzeugen, dass die Konfiguration der Appliance dem Dienstleister nur die unbedingt nötigen Rechte einräumt. Damit lassen sich vielfältige Anwendungsszenarien wie etwa Remote-Überwachung und -wartung oder ein extern gehostetes Archiv sicher realisieren.

ARTEC selbst verwendet firegate VPN intensiv zur Sicherung der EMA® Enterprise Managed Archive®-Lösung in beiden Szenarien. Einerseits realisiert firegate VPN einen sicheren Wartungszugang zu der beim Kunden befindlichen EMA®-Appliance. Andererseits muss ein extern gehostetes EMA®-Archiv für Aufgaben wie Synchronisierung von Ordnerstrukturen und Fileservern oder das Rückspielen von archivierten Daten gelegentlich auch Verbindungen zurück ins Firmennetz ausführen. Auch hier sorgt firegate VPN für die sichere Verbindung.

Das Ausrollen und in Betrieb nehmen einer firegate VPN-Appliance gestaltet sich für den Kunden denkbar einfach. Nachdem der Kunde eine IP-Adresse, Gateway, Subnetzmaske sowie DNS-Server zum Zugang und einige Informationen über seine Infrastruktur zur Verfügung gestellt hat, wird die Appliance von ARTEC vorkonfiguriert. Nach der Auslieferung kann der Kunde je nach Bedarf Zugriffsrechte auf die Appliance übertragen, so dass zum Beispiel der Archivierungsdienst von ARTEC auf alle nötigen Datenquellen zur Synchronisierung zugreifen kann. Vorteilhaft aus Kundensicht ist hierbei, dass für den Zugang keine sensiblen Informationen an ARTEC übertragen werden müssen.

Somit können jetzt einzelne Standorte und Systeme bei Cloud-Projekte nicht nur effizient – sondern auch wirklich hochsicher und verschlüsselt – angebunden werden.

IMPRESSUM

Unternehmensanschrift
ARTEC IT Solutions AG
Robert-Bosch-Str. 38
61184 Karben
Telefon: +49 - 6039 - 9154 - 0
Telefax: +49 - 6039 - 9154 - 54
E-Mail: info@artec-it.de
Internet: http://www.artec-it.de

Geschäftsführung/Vorstand
Jerry J. Artishdad (Vorsitzender)

Geschäftsführung/Aufsichtsrat
Dr. Andreas U. Schmidt (Vorsitzender)

Sitz der Gesellschaft
Karben, Germany, HRB 84834 Frankfurt

Registergericht
Amtsgericht Frankfurt 72133

Umsatzsteuer-Identifikationsnummer
DE 264190542

Inhaltlich Verantwortlicher
Jerry J. Artishdad

Disclaimer

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

ARTEC® IT Solutions

Turning Data Into Information