

ViPNet: 10 Pro-Argumente

TECHNISCH

- ■ ■ ■ **ViPNet** konzentriert sich nicht nur auf die „Client-to-Server“, sondern vielmehr auf die „**Client-to-Client**“ **Verbindungen**. Da bei den meisten VPN-Lösungen nur „Server-to-Server“ oder „Client-to-Server“ Verbindungen möglich sind, gibt es auf dem IT-Markt kaum Systeme, die einen Schutz auch für lokale Netze bieten, d.h. den inneren Bereich, der oft als Bedrohungsquelle unterschätzt wird.
- ■ ■ ■ Die einzigartige, seit Jahren erprobte **ViPNet**-Technologie, ermöglicht **VPN-Verbindungen über Firewalls** und **Proxy** mit NAT und NAPT. Diese Eigenschaft ist besonders für den mobilen Benutzer von Bedeutung, der sich aus unterschiedlichen Netzwerkumgebungen über das Internet an das eigene VPN-Netzwerk anschliessen muss und einen möglichst einfachen Installationsprozess erfordert.
- ■ ■ ■ **ViPNet** verwendet eine **256-Bit Datenverschlüsselung**, basierend auf einem proprietären System des symmetrischen und asymmetrischen Schlüsselaustausches. Das schließt einerseits die bekannten Schwachstellen eines Systems mit öffentlichen Schlüsseln aus, andererseits bietet es 100% Vertraulichkeit der Kommunikation zwischen zwei VPN-Benutzer.
- ■ ■ ■ Jedes **ViPNet**-Modul, das eine geschützte Verbindung aufbaut, verfügt über eine integrierte **Firewall und IDS**. Dadurch werden nicht nur vertrauliche Daten auf dem Rechner geschützt, sondern auch Angriffe auf die Schlüssel und das Kryptomodul abgewehrt.
- ■ ■ ■ Um Unabhängigkeit von der bestehenden Netzwerkstruktur zu gewährleisten und eine IP-Adressenüberschneidung bei verschiedenen Standorten zu vermeiden, verwendet **ViPNet**-Lösung eine proprietäre Technologie von **virtuellen IP-Adressen**.

Im Gegensatz zu allen anderen klassischen VPN-Lösungen bietet **ViPNet** eine Reihe von integrierten **Kommunikationsanwendungen** wie [Business Mail], [File Exchange], [Secure Chat/Instant Messaging], die innerhalb des aufgebauten virtuellen Netzwerkes einen gesicherten, hochverschlüsselten und **spam-freien** Informationsaustausch ermöglichen.

Zusätzliche **Sicherheitsmechanismen**, wie digitale Signatur, Programmkontrolle, Internetschleuse, WatchDog oder der Schutz während des Bootvorganges machen aus dem klassischen VPN-Client eine Bastion, die Ihre vertraulichen Daten schützt und Hacker- und Virenangriffe abwehrt, sowohl von außen als auch von innen.

Leichte Konfiguration, **benutzerfreundliches Interface**, das teilweise auch in die Windows-Oberfläche integriert ist, macht die tägliche Arbeit mit dem VPN komfortabel und verständlich.

Da **ViPNet** eine reine **Software-Lösung** ist, besteht bei dem Aufbau des VPN kein Bedarf an zusätzlicher Hardware oder Restrukturierung des bestehenden Netzwerkes, was seinerseits zu keinen zusätzlichen Kosten und Arbeitsunterbrechungen führt.

Flexible Preisgestaltung in Verbindung mit der Möglichkeit, **ViPNet**-Software auf spezifische Kundenanforderungen anzupassen.

KAUFMÄNNISCH