viprinet®

Nie wieder offline.

Multichannel VPN Router™
Multichannel VPN Hub™

- Die passende Lösung für jedes Anbindungsszenario
- Echte Bündelung von 6 und mehr Internetzugängen
- Flexibilität durch modularen Aufbau
- Hot-Plug-Modems für alle gängigen Zugangsmedien
- Ausfallsicherheit durch Risikoverteilung
- Datenverschlüsselung nach höchstem Standard
- Ermöglicht ultra-mobile, portable und stationäre Anbindungen

Die Netzwerkrevolution

Wir sind Viprinet

Seit 2006 stellt Viprinet innovative Netzwerkkomponenten her. Viprinet ist Erfinder einer patentierten Technologie, mit der die Bandbreiten unterschiedlicher Wide-Area-Network-Verbindungen tatsächlich aggregiert werden. Derzeit 35 Mitarbeiter entwickeln, produzieren und vertreiben Viprinet-Produkte von Bingen am Rhein aus weltweit. Viprinet ist profitabel und wächst schnell – finanziert aus den eigenen Erträgen. Nachhaltigkeit ist ein zentraler Punkt des Unternehmensleitbildes. Sie ist es in der Entwicklung hinsichtlich der Länge der Lebenszyklen der Produkte, in der Produktion – dort wird ausschließlich Energie aus regenerativen Quellen genutzt – oder im niedrigen Energieverbrauch der Viprinet-Geräte. Alle Produkte von Viprinet sind „Made in Germany“ und erfüllen höchste Standards, was Sicherheit und Vertraulichkeit angeht.

Internetanbindung neu definiert

Mit seinem einzigartigen VPN-Tunnelverfahren ermöglicht Viprinet eine vollkommen neue Art der Anbindung für feste wie mobile Standorte – hochverfügbar, schnell und kosteneffektiv. Das geniale Viprinet-Prinzip bringt Ausfallsicherheit und erhöhte Übertragungsgeschwindigkeit.

Echte Bündelung aller WAN-Links

Herzstück der Viprinet-Technologie ist der Multichannel VPN Router. Hiermit lassen sich mehrere Breitbandzugänge zu einer einzigen hochverfügbaren Gesamtanbindung vereinen. Dabei findet eine echte Bündelung aller verfügbaren Internetzugänge statt und nicht – wie z.B. beim Loadbalancing – lediglich eine Lastverteilung auf mehrere WAN-Links.

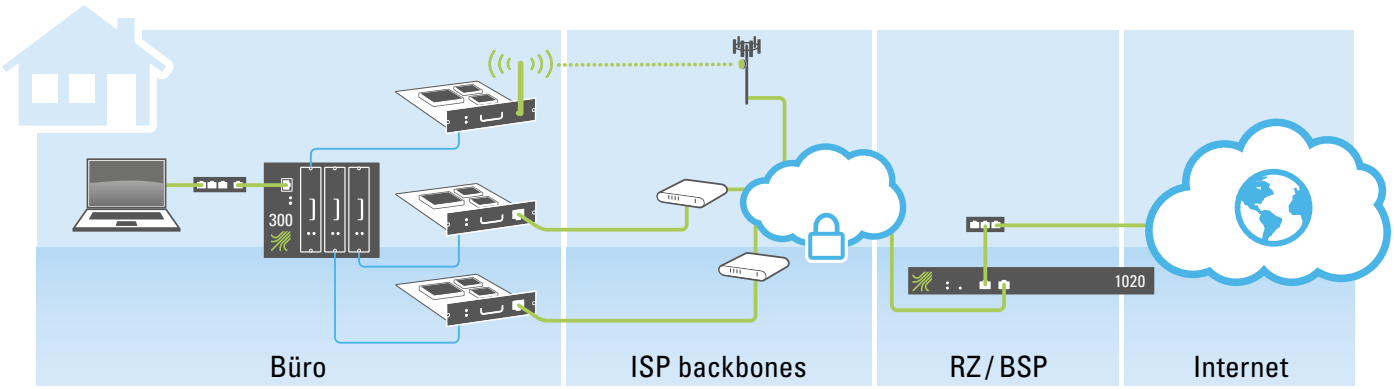
Viprinet kombiniert beliebige Leitungstypen, ob ADSL, SDSL, UMTS/HSPA+ oder LTE und lässt diese zum LAN hin als eine einzige Leitung erscheinen. So steht die Summe der Up- und Downstream-Bandbreiten der Leitungen selbst für einzelne Downloads zur Verfügung.

Das Prinzip Gegenstelle

Für die sichere und schnelle Anbindung von Standorten, Anlagen und Fahrzeugen verwendet Viprinet ein einzigartiges VPN-Tunnelverfahren in Sternstruktur, für das die Einbindung von zwei verschiedenen Geräten notwendig ist:

Jeder angeschlossene Multichannel VPN Router baut über jede der angeschlossenen Leitungen einen verschlüsselten VPN-Tunnel-Kanal zu einer zentralen Gegenstelle, einem Multichannel VPN Hub, auf. Diese VPN-Tunnel-Kanäle werden zu einem Gesamttunnel gebündelt, durch den dann die eigentliche Datenübertragung erfolgt.

Der Multichannel VPN Hub, üblicherweise in einem hochausfallsicheren Rechenzentrum platziert, fungiert als Vermittlungsstelle: Daten mit Ziel in einer anderen Niederlassung werden über den zugehörigen VPN-Tunnel weiter versandt. Daten mit dem Ziel des öffentlichen Internets werden hingegen entschlüsselt und in Richtung des Ziels weitergeleitet. Der VPN Hub sorgt für eine sichere und schnelle Kommunikation der Multichannel VPN Router untereinander, dient aber zugleich auch als zentraler Austauschpunkt zwischen dem verschlüsselten VPN und dem öffentlichen Internet oder dem Unternehmensnetzwerk.



Der Datenstrom vom LAN wird vom Multichannel VPN Router verschlüsselt und auf die Internetanschlüsse (hier: 2x DSL, 1x UMTS) verteilt. Die verschlüsselten Daten passieren aufgeteilt die Netze der verwendeten ISPs und erreichen den Multichannel VPN Hub im Rechenzentrum. Dieser entschlüsselt den Datenstrom und setzt ihn wieder korrekt zusammen. Anschließend wird der Datenstrom zum eigentlichen Ziel im Internet weitergeleitet. Ebenso wird in der Gegenrichtung verfahren – hier übernimmt der VPN Hub die Verschlüsselung, der VPN Router die Entschlüsselung.

Bonding Service Provider

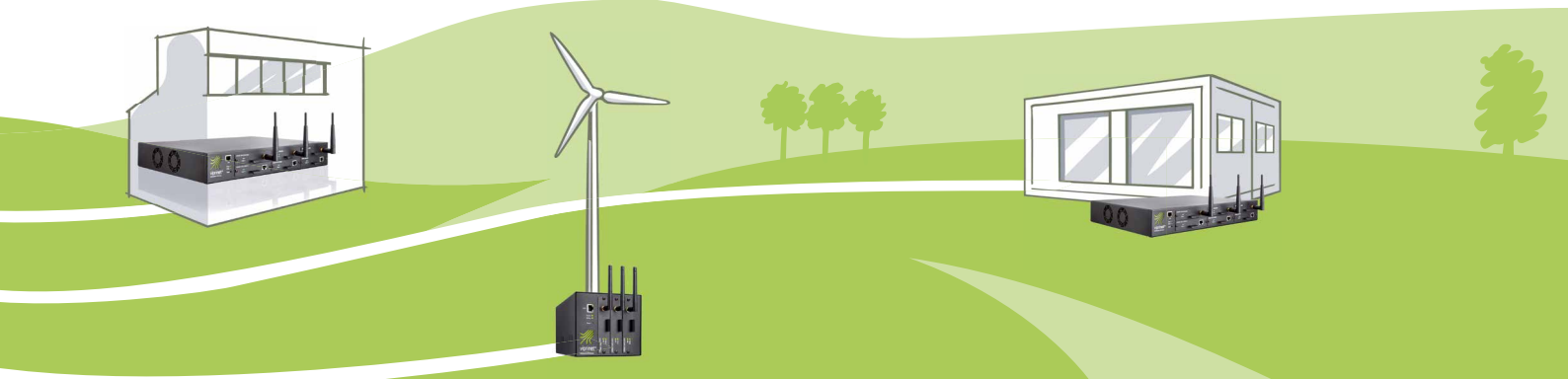
Für alle, die über keine eigene Rechenzentrumsfläche verfügen und/oder sich technisch nicht mit dem Thema Bündelung befassen möchten, gibt es Bonding Service Provider (BSP). Bonding Service Provider stellen ihren Kunden in Rechenzentren je nach vereinbartem Leistungsumfang Kapazität auf einem Hub oder einen dedizierten Hub zur Verfügung. Sie gewährleisten, dass die Multichannel VPN Router ordnungsgemäß auf den gemieteten Hub im Rechenzentrum terminieren.

Je nach Bedarf versorgen die BSP ihre Kunden mit öffentlichen IP-Adressen, die vom Rechenzentrum aus durch die VPN-Tunnel zu den jeweiligen Standorten geroutet werden. Optional bieten die BSP auch zentrale Firewall-Services und ggf. weitere Dienstleistungen an, abhängig von Anforderungen und Budget.

Beliebige Kombination von Leitungstypen & ISPs

Dieses Prinzip ermöglicht eine bisher unerreichte Flexibilität bei der Auswahl von Netzzugängen. Anwender und Unternehmen sind nicht länger an einen bestimmten Carrier gebunden, sondern können sich flexibel ihren Anforderungen entsprechend die passende Leitungskombination zusammenstellen.

Statt teurer Standleitungen eines Einzelanbieters können sie preisgünstige Consumer-Angebote wie ADSL nutzen. Das bedeutet Investitionssicherheit: Durch den modularen Aufbau der Multichannel VPN Router lassen sich auch künftige Zugangstechnologien problemlos integrieren.



Die Netzwerkrevolution

Weniger Ausfälle bedeuten geringere Kosten

Einer Studie von Infonetics Research zufolge verlieren mittlere Unternehmen (100 bis 1000 Angestellte) jährlich durchschnittlich 3,6 % ihrer Umsätze durch Downzeiten, in denen die IT des Unternehmens brachliegt. Diese kosten je nach Branche viel Geld, weil Kommunikation und Produktion ausfallen und Mitarbeiter sowie Kunden keinen Zugriff auf Informationen haben. Diese indirekten Kosten bei einer Standortvernetzung werden meist drastisch unterschätzt.

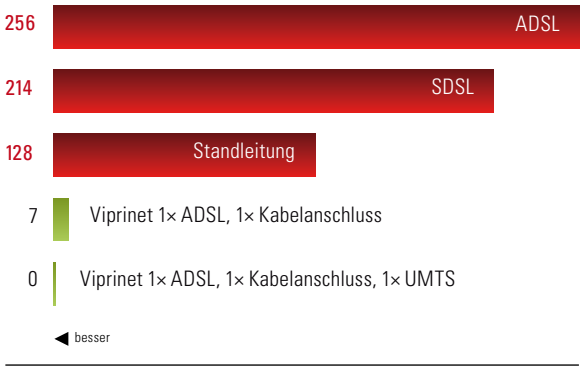
Stündliche Kosten (in US$) für Downzeiten nach Branchen:	
Einzelhandel	69.000
Home-Shopping	89.000
Medien (Pay per View)	90.000
Logistik	113.000
Online-Kartenvorverkauf	150.000
Kreditkartenverarbeitung	2.600.000
Broker	6.400.000
Durchschnittlich	336.000

Quelle: Ponemon Institute 2012, *How much does downtime really cost?*

Das Hauptaugenmerk bei der Planung einer Unternehmensvernetzung muss daher auf die Ausfallsicherheit des Konzepts gelegt werden. Lösungen, die auf SDSL-Angeboten in Kombination mit IPSec-VPNs basieren, sind in dieser Hinsicht nicht sehr effizient, denn sie fallen pro Jahr durchschnittlich für 5–7 Tage aus. Bei den deutlich teureren MPLS-Angeboten ist das nicht viel besser – auch hier muss man mit mehreren Tagen Ausfall im Jahr rechnen.

Ausfallsicherheit durch Risikoverteilung

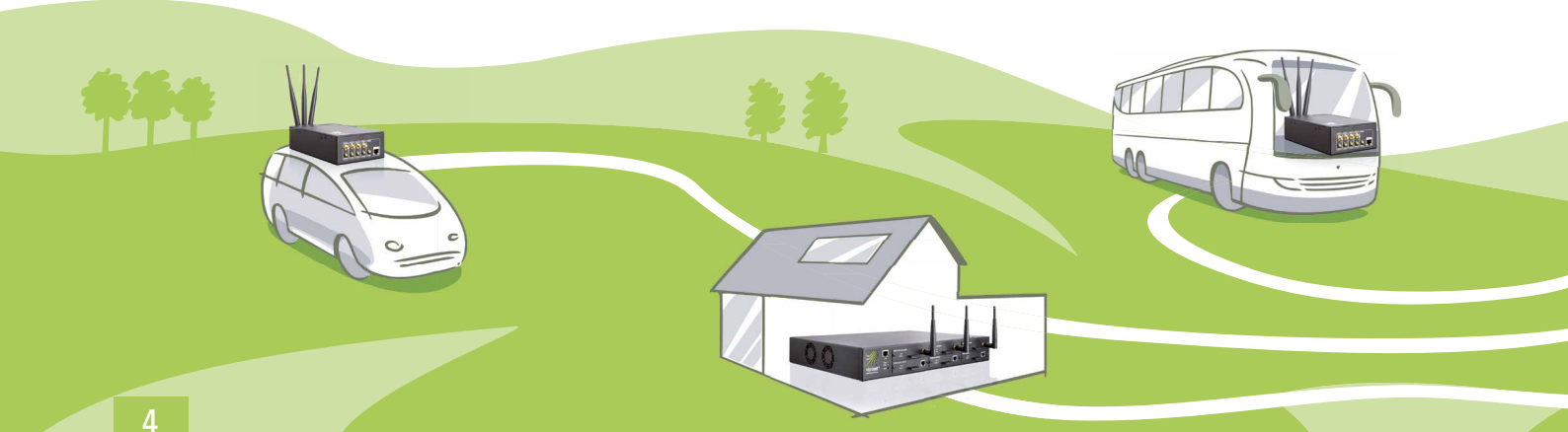
Das bewährte Bündelungsverfahren des Multichannel VPN Routers minimiert das Ausfallrisiko deutlich. Durch die Kombination mehrerer verschiedener Leitungen bewirkt der Ausfall einzelner Leitungen im Bündelungsverbund keinerlei Verbindungsabbrüche. Lediglich die verfügbare Gesamtbandbreite verringert sich um den Anteil der weggefallenen Leitung. Ist die Leitung wieder verfügbar, erhöht sich die Gesamtbandbreite vollautomatisch entsprechend. Durch Kombination verschiedener Zugangs-ISPs bzw. Medientypen lässt sich auf diesem Wege eine hochverfügbare Anbindung schaffen. Bezieht man beispielsweise auch UMTS-/LTE-Technik in den Bündelungsverbund mit ein, kann selbst ein Komplettausfall der kabelgebundenen Anbindungen, z.B. durch Tiefbauarbeiten, abgefangen werden.



Typische Ausfallzeit der Gesamtanbindung
in Stunden pro Jahr

Statistische Sicherheit statt ISP-Versprechen

Nicht nur durch die drastische Reduzierung von Ausfallzeiten lässt sich mit einer Viprinet-basierten Vernetzungslösung Geld sparen. Damit ein Business-ISP mit seinen Angeboten Verfügbarkeiten von über 97% im Jahr erreichen kann, muss dieser einen erheblichen Aufwand betreiben. Für die Kunden müssen rund um die Uhr Servicepersonal und Technik vorhanden sein, um eine ausgefallene Leitung



kurzfristig entstören zu können. Entsprechende „Service Level Agreements“ machen das Ganze für den ISP und damit auch für den Kunden teuer.

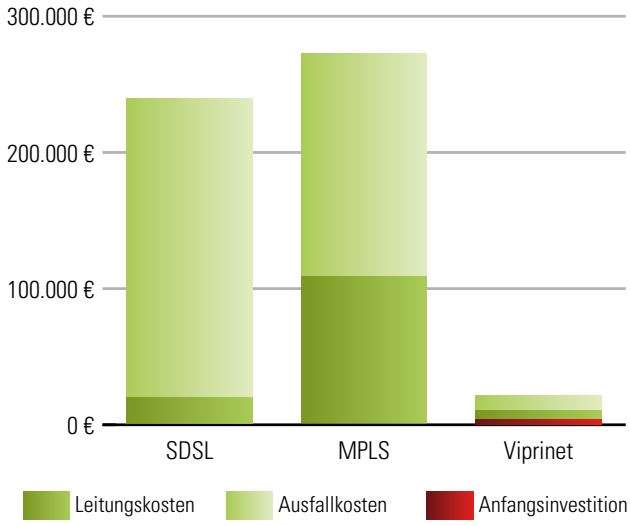
Bei einer Viprinet-basierten Anbindungslösung entfällt dieser Aufwand – statt teurer Businessangebote werden auf den Privatkundenmarkt ausgerichtete günstige Standardangebote wie z.B. ADSL und UMTS verwendet. Durch die Bündelung und Risikoverteilung der Viprinet-Technik reicht es völlig aus, dass die einzelnen Internetzugänge für sich genommen jeweils nur eine Verfügbarkeit von 97% im Jahr haben – entscheidend ist, dass diese voneinander unabhängigen Zugänge typischerweise nicht gleichzeitig ausfallen. Mit der Anzahl der unterschiedlichen Medien, die mit dem Viprinet-Router gebündelt werden, steigt die Ausfallsicherheit daher exponentiell – ganz ohne Zutun der Internetprovider.

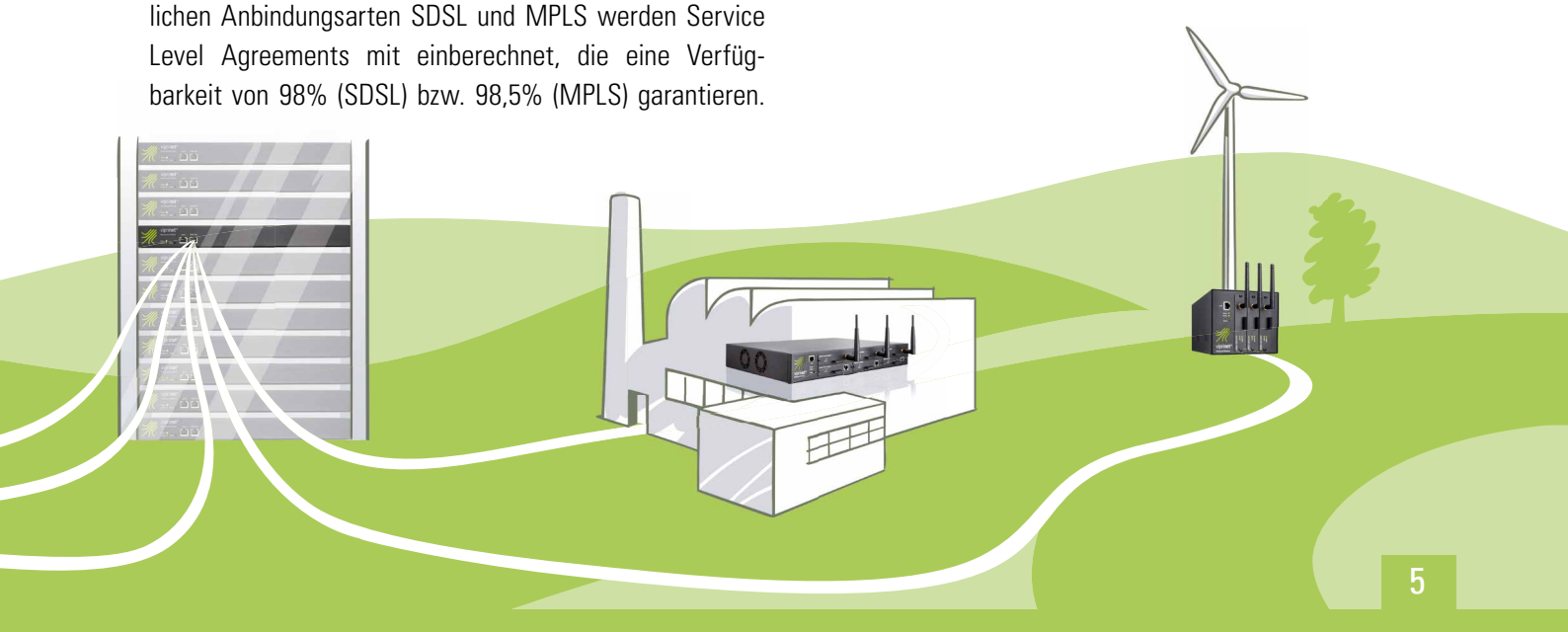
Beispielrechnung Unternehmensvernetzung

Die Kosten für die Anbindung von Standorten bestehen im Wesentlichen aus zwei Komponenten: den eigentlichen Anschaffungs- und Betriebskosten sowie dem einzukalkulierenden Kostenrisiko für Unternehmensstillstände durch Leitungsunterbrechungen. Die Beispielgrafik beschreibt den Fall, dass ein Unternehmen drei Standorte mit einer Bandbreite von ca. 4 MBit/s per VPN miteinander verbindet.

Das Kostenrisiko für einen Tag Leitungsausfall ist hier mit 10.000 Euro recht niedrig angesetzt. Bei den herkömmlichen Anbindungsarten SDSL und MPLS werden Service Level Agreements mit einberechnet, die eine Verfügbarkeit von 98% (SDSL) bzw. 98,5% (MPLS) garantieren. 98% Verfügbarkeit klingt gut, bedeutet allerdings, dass ein Wegfall der Anbindung von bis zu 5 Tagen pro Jahr toleriert werden muss. Auf 36 Monate betrachtet ist dies bei SDSL und MPLS ein Kostenrisiko von 160.000 bis 220.000 Euro. Die Viprinet-Lösung kommt durch ihre Risikoverteilung auf eine Verfügbarkeit von 99,9%, hier fällt daher nur ein Kostenrisiko von rund 16.000 Euro an. Zudem sind die Leitungskosten selbst geringer.

Im Ergebnis ist eine ausfallsichere Anbindung von Viprinet nicht nur bei den reinen Betriebskosten überlegen, sondern zeigt ihr gewaltiges Einsparpotenzial vor allem in der Gesamtbetrachtung der Kosten unter Einbeziehung der Ausfallzeiten. Im Vergleich zu Lösungen basierend auf SDSL/IPSec und MPLS ergibt sich ein Einsparpotenzial von ungefähr 90%.





Die Netzwerkrevolution

Hintergrund Unternehmensspionage

Studien zufolge wird jedes zweite Unternehmen in Deutschland ausgespäht. Der TÜV Süd beziffert den wirtschaftlichen Schaden alleine für Deutschland im Jahr 2012 mit 4,2 Milliarden Euro; andere Studien gehen von bis zu 50 Milliarden Euro aus, Tendenz weiter steigend. Die Motivationen von kriminellen Banden wie ausländischen Geheimdiensten gleichermaßen reicht dabei vom klassischen Diebstahl von Firmengeheimnissen über den massenhaften Missbrauch schutzwürdiger Kundendaten (z.B. Kreditkartendaten) bis hin zu Erpressungen.

Angreifer aus Datennetzen suchen sich wie der klassische Wohnungseinbrecher immer den Weg des geringsten Widerstandes. Der bequemste Weg ist dabei heute meist ein Angriff auf die verwendeten Internet-Router – schließlich läuft über dieses zentrale Gerät aller Datenverkehr des Unternehmens, der sich so bequem abgreifen lässt. Insbesondere preisgünstige Routerprodukte aus China, wie sie von den Netzbetreibern zum Anschluss mitgeliefert werden, weisen dabei teilweise über Jahre einschlägig bekannte Sicherheitslücken auf, mit denen diese Geräte aus der Ferne sehr einfach „übernommen" werden können.

Für den Bereich der Geheimdienste ist es seit den NSA-Skandalen Allgemeinwissen, dass unsere Kommunikationsinfrastruktur nahezu flächendeckend abgehört wird, mit direktem Zugriff auf die entsprechenden Netze. Zusicherungen von Netzbetreibern, dass deren Netze für die sichere Unternehmenskommunikation genutzt werden könnten, sind daher fahrlässig. Man muss davon ausgehen, dass insbesondere MPLS-Netzwerke flächendeckend ausgeforscht werden.

Da man also den Netzbetreibern nicht mehr vertrauen kann, wird es Zeit, die IT-Sicherheit und Anbindungsverschlüsselung in die eigenen Hände zu nehmen. Insbesondere die Verschlüsselungs-Schlüssel dürfen ausschließlich in der Hand des Unternehmens selbst sein.

Nun stellt sich aber ein weiteres Problem: Seit längerem gehen IT-Sicherheitsexperten und zunehmend auch die Politik davon aus, dass große chinesische Hersteller heimlich Hintertüren für den chinesischen Staat in ihre Produkte einbauen – bei einem der größten Hersteller, der auch in Europa viele Netzbetreiber ausstattet, steht zudem zu vermuten, dass dieser unter direkter Kontrolle chinesischer Geheimdienste steht.

Aber auch im Westen sieht es nicht sehr rosig aus. So ist mittlerweile bekannt geworden, dass US-amerikanische Routerhersteller zum Einbau von Hintertüren in ihre Produkte verpflichtet werden können. Solche Hintertüren dienen in erster Linie zwar legitimen Interessen wie Strafverfolgung, aber eine Hintertür ist nun einmal eine Tür, und Türen unterscheiden nicht danach, wer daran klopft. Es steht zu befürchten, dass entsprechende Überwachungsschnittstellen auch von Dritten missbraucht werden.

Anders gesagt: Die Versuche verschiedenster Interessensgruppen, sich widerrechtlich Zugriff auf die Daten von Unternehmen wie Bürgern zu verschaffen, haben die IT-Sicherheit zu einem Thema gemacht, dem sehr hohe Priorität eingeräumt werden muss.

Viprinet-Produkte sorgen für Sicherheit

Für all diese Problemfelder sind die Produkte von Viprinet eine adäquate Lösung. Die Grundidee von Viprinet Multichannel VPN Routern war von Anfang an, dass man Zusicherungen hinsichtlich Bandbreitenverfügbarkeit, Stabilität und Ausfallsicherheit eines einzelnen Netzbetreibers nicht vertrauen kann, sondern stattdessen die Risiken auf mehrere verschiedene Medien und Netzbetreiber streuen sollte.

Dieses Prinzip der gebündelten Nutzung bringt auch einen gewaltigen Sicherheitsgewinn. Alle Datenpakete, die über einen Viprinet-Router transportiert werden, werden zunächst zum Versand über mehrere Datenleitungen „zerhackt" und dann für jede Leitung separat verschlüsselt.

Damit transportiert kein einzelnes Carrier-Netz jemals einen vollständigen Nutzdatenstrom. Selbst wenn jemand in der Lage wäre, die Verschlüsselung der Pakete auf ihrem Transportwege zu knacken, würde er nur Bruchteile der Daten erhalten. Um sinnvolle Informationen stehlen zu können, müssten alle Pakete in den unterschiedlichen Betreibernetzen zugleich abgefangen und zugeordnet werden. Über eine solche Fähigkeit verfügt nach allem, was bekannt ist, derzeit niemand.

Die in den Viprinet-Routern verwendeten Verschlüsselungverfahren erfüllen zudem die alllerhöchsten Industriestandards und umgehen alle bekannten Angriffsszenarien. So bestehen die Verschlüsselungen immer aus einer Mischung von Hardware- und Softwarelösungen, die von neutralen Lieferanten bezogen und mit Eigenentwicklungen kombiniert werden. Damit sind anders als bei anderen Herstellern selbst Angriffe über die Zulieferkette ausgeschlossen.

Zudem werden alle Produkte von Viprinet vollständig in Deutschland entwickelt und produziert. So hat Viprinet seine Produktionskette komplett in seiner Hand. Des Weiteren besteht für Viprinet keine Gefahr, zum Einbau von Hintertüren gezwungen zu werden. Die Geschäftsleitung von Viprinet garantiert persönlich, dass Viprinet keinerlei Geschäftsbeziehungen zu Geheimdiensten pflegt und auch niemals pflegen wird.

IT-Sicherheit und die Absicherung gegen Unternehmensspionage ist also eine Frage der richtigen Technik, einer gesicherten Lieferantenkette und eines vertrauenswürdigen Herstellers. All dies bietet Viprinet.

Sichere Standortvernetzung in der Praxis

Die Funktionsweise der Viprinet-Technologie ist so simpel wie effizient: Zwischen den Viprinet Multichannel VPN Routern an den unterschiedlichen Standorten und dem Multichannel VPN Hub in einem gesondert gesicherten und zertifizierten Rechenzentrum wird pro verwendetem Übertragungsmedium ein sicherer VPN-Tunnel in jede Richtung aufgebaut. Jegliche Kommunikation zwischen den verschiedenen Standorten wird nun innerhalb dieser VPN-Tunnel abgewickelt – auf diese Weise entsteht ein lückenloses System, das von außen nicht erreichbar ist. Viprinet kann dabei auch über Ländergrenzen hinweg eingesetzt werden, um Niederlassungen im Ausland mit einzubinden, und auch in Auslandsniederlassungen deutsche IP-Adressen zu verwenden.

Sicherheits-Features:

- AES 256 Bit CBC
- 2048-bit RSA-Schlüssel mit SHA256-Zertifikaten
- TLS 1.2
- Diffie-Hellman-Schlüsselaustausch mit elliptischen Kurven (Perfect Forward Secrecy)
- VPN Hub Public Key Fingerprinting
- Alle internen Dienste mit ACLs abgesichert

Unternehmen, die ihre verschiedenen Standorte mit Viprinet vernetzen, haben neben den bekannten Vorteilen einer höheren Bandbreite und einer Ausfallsicherheit von fast 100% die Sicherheit, dass kein Außenstehender vertrauliche Datenkommunikation entschlüsseln kann.

Auf diese Weise können Unternehmen auch eine sichere Kommunikation mit ihren Zulieferbetrieben einrichten: Diese müssen nur einen Viprinet Multichannel VPN Router nutzen, der auf den gleichen Multichannel VPN Hub terminiert, über den auch die Unternehmens-Kommunikation abläuft. Wer nun innerhalb dieses privaten Netzes auf welche Datenströme zugreifen kann, kann fein granular konfiguriert werden. Dabei können die Zulieferer dauerhaft oder zeitlich befristet eingebunden werden, ganz nach Bedarf.

Einsatzbereiche

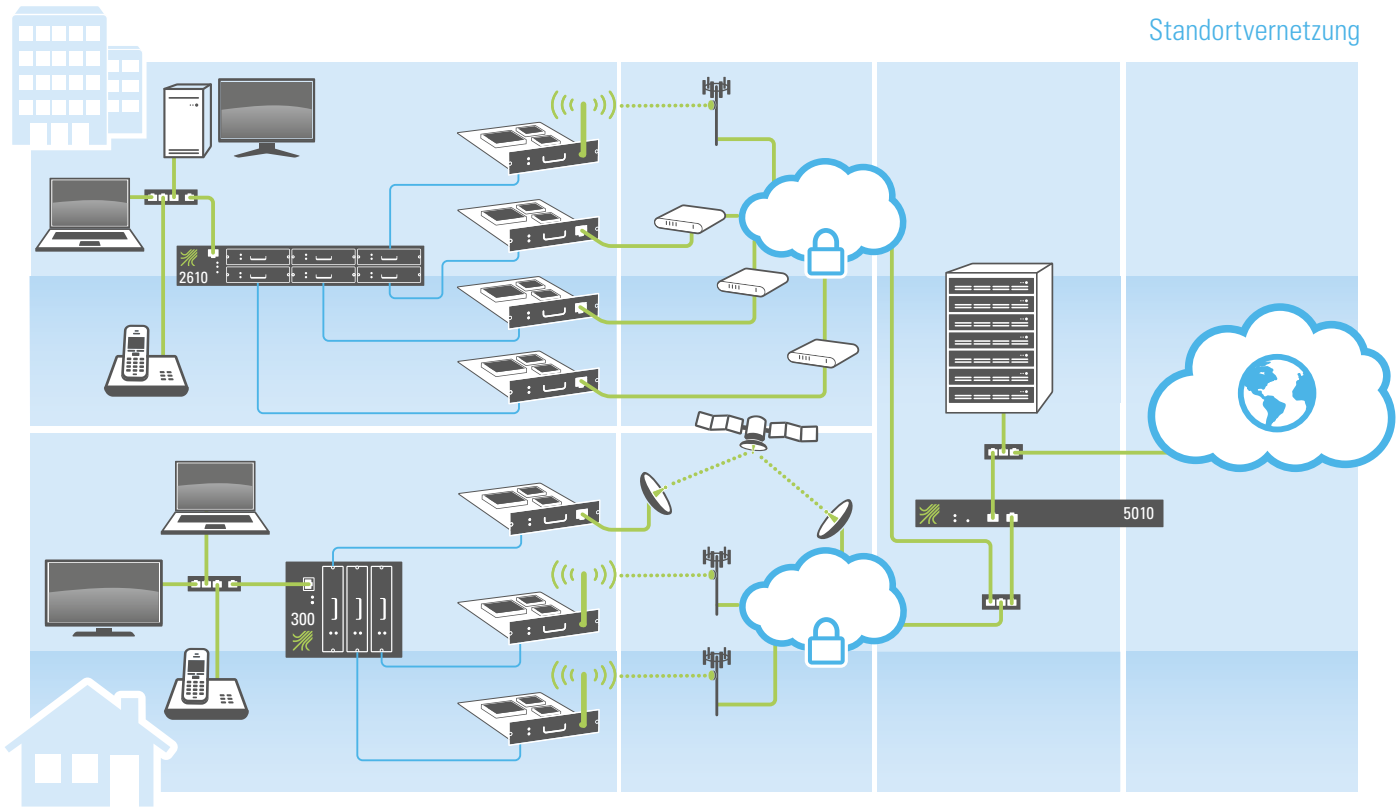
Vielfältige Anwendungsszenarien

Die Viprinet-Technologie lässt sich durch ihre Flexibilität in einer Vielzahl von Szenarien einsetzen. Gegenüber anderen Lösungen zur Unternehmensanbindung bietet Viprinet drei wesentliche Vorteile: hohe Bandbreiten, außergewöhnliche Verfügbarkeit und ortsunabhängigen Zugriff. Preisgünstige Consumer-Angebote lassen sich so zur professionellen Internetanbindung veredeln, perfekt zugeschnitten auf die Anforderungen vor Ort. Ob mobil oder stationär: Wer auf eine schnelle und sichere Internetanbindung angewiesen ist, für den stellt Viprinet die optimale Lösung dar.

Standortanbindungen

Die Vernetzung von Unternehmensstandorten im In- und Ausland und die gleichzeitige Einbindung von Road Warriors, Heimarbeitsplätzen und häufig wechselnden Einsatzorten oder Standorten in schlecht angebundenen Regionen wird oft von Lösungen wie MPLS oder herkömmlichen Standleitungen beherrscht. Dabei sind diese teuer, unflexibel und bieten keine Ausfallsicherheit noch erhöhte Verfügbarkeit. In solchen Fällen schafft die bewährte Viprinet-Technologie durch die Bündelung mehrerer Internetverbindungen Abhilfe.

Standortvernetzung



Das Hauptbüro ist mit einem Multichannel VPN Router 2610 über drei DSL-Anschlüsse angebunden, zusätzlich wird ein UMTS-Zugang mitgebündelt. Der Router baut seinen VPN-Tunnel zu einem Multichannel VPN Hub 5010 im Rechenzentrum auf. Dort befindet sich auch der Server, auf denen die zentralen Applikationen des Unternehmens laufen.

Das Nebenbüro ist mit einem Multichannel VPN Router 300 angebunden. Mangels Verfügbarkeit von DSL wird hier 1x Satellit mit 2x UMTS kombiniert. Der Router baut seinen VPN-Tunnel zum gleichen VPN Hub auf wie das Hauptbüro.

Die Kommunikation zwischen den beiden Standorten wie auch der Zugriff auf die Server im Rechenzentrum läuft immer über den zentralen VPN Hub, und ist über den gesamten Weg verschlüsselt. Auch der Zugang zum Internet läuft für beide Standorte über den VPN Hub.

Video Streaming

Ob Live-Berichterstattung, Eventübertragung oder Überwachung: Die Viprinet-Bündelungstechnologie stellt für diese Aufgaben überall eine ausfallsichere und schnelle Internetverbindung bereit. Viprinet hat für diesen Anwendungsbereich eine spezielle Bündelungsart konzipiert, welche die vorhandene Bandbreite optimal nutzt. Viprinet-Partner bieten hier gebrauchsfertige Video-Streaminglösungen.

eHealth

Telemedizin und Telemonitoring benötigen hohe Bandbreite und höchste Zuverlässigkeit, z.B. bei der Kommunikation zwischen Arzt oder Pflegern in der Klinik und chronisch kranken Patienten in deren Wohnung. Viprinet-Router bündeln Festnetz- und Mobilfunkverbindungen zu einer ausfallsicheren Standleitung und ermöglicht so eine sichere Beurteilung und Überwachung der Patienten.

Fahrzeuge

Die Anbindung von Fahrzeugen erfordert hohe Flexibilität, wenn sich Fahrzeuge bewegen und die Verbindung ständig von Funkzelle zu Funkzelle neu aufgebaut werden muss. Dabei muss der permanente Wechsel zwischen unterschiedlichen Mobilfunkstandards (GPRS, UMTS, LTE) bewältigt werden. Viprinet bietet mit seinem speziell dafür entwickelten Fahrzeugrouter die richtige Lösung für eine unterbrechungsfreie Internetanbindung.

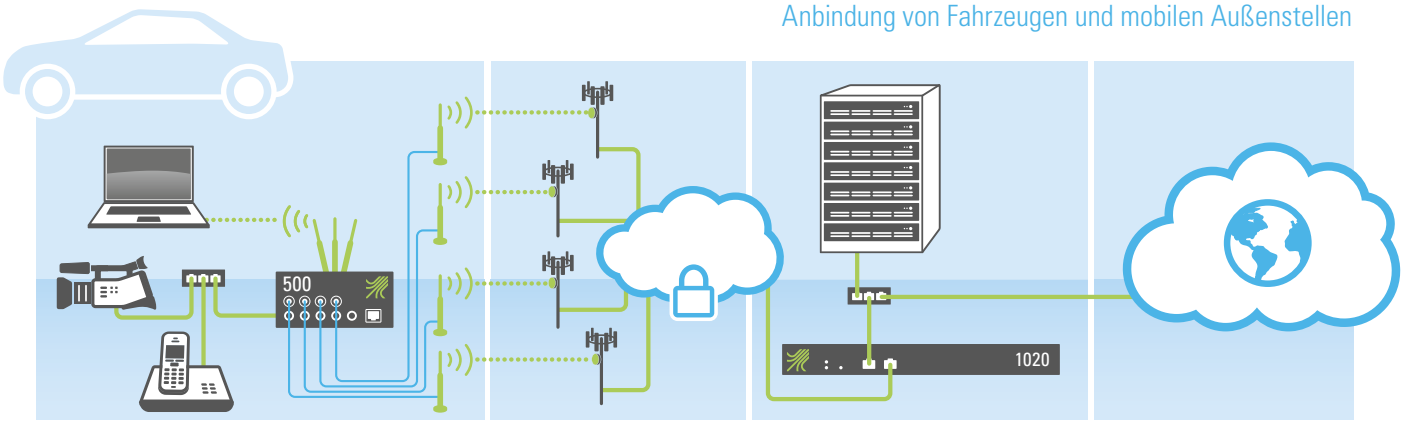
Hoheitliche Aufgaben

Die Anbindung von Polizei-, Feuerwehr- und Krankenwagen durch die bewährte Viprinet-Bündelung mehrerer Internetanbindungen gewährt höchste Ausfallsicherheit und Bandbreite. Beispielanwendungen sind etwa mobile Verkehrsüberwachung, visuell unterstützte Koordination von Vor-Ort-Einsatzkräften sowie die ambulante Behandlung von Patienten durch Spezialisten über Video- und Datenkonferenzen. Die verschlüsselten VPN-Tunnel genügen höchsten Sicherheitsanforderungen.

Schiffe und Bohrinseln

Mit Viprinet können auch schwierigste Anbindungsszenarien im maritimen und Off-Shore-Bereich realisiert werden, z.B. in Gegenden ohne Mobilfunkempfang oder bei häufigen Grenzübertritten. Anwendung finden ausfallsichere Breitbandanbindungen von Viprinet z.B. auf Bohrinseln zur Reduzierung einer teuren Satellitenverbindung auf Notfälle oder auf Flussschiffen für eine nahtlose Internetanbindung bei häufigen Grenzübertritten.

Anbindung von Fahrzeugen und mobilen Außenstellen



Das Fahrzeug wird mit einem Multichannel VPN Router 500 ausgestattet. Dieser bietet ein WLAN an, welches innerhalb des Fahrzeugs z.B. von Laptops genutzt wird. Festinstallierte Geräte sind hingegen per LAN an den Router angebunden. Der Router nutzt 4 Mobilfunkverbindungen. Über diese baut der Router einen VPN-Tunnel zum Multichannel VPN Hub 1020 auf, der sich im Rechenzentrum befindet. Von hier aus wird der Traffic dann unverschlüsselt ins Internet weitergeleitet.

Die Produkte im Überblick

Für jede Anforderung die passende Lösung

Den Multichannel VPN Router gibt es in fünf Varianten: Als Standard-Gerät zur Bündelung von bis zu sechs Zugängen (Modell 1610), als Enterprise-Ausführung (Modell 2610), als Desktop-Version für den Einsatz in kleinen Unternehmen (Modell 300), als ultra-mobile Variante zur Nutzung in Fahrzeugen (Serien 500 und 51X) oder als schlankes Einsteigermodell (Modell 200). Die meisten Multichannel VPN Router sind mit ihrem zueinander kompatiblen Modulsystem als „Hot-Plug" ausgelegt, es können also im laufenden Betrieb ohne Verbindungsunterbrechungen Modems und somit Leitungen hinzufügt, ausgetauscht oder entfernt werden. Die robust ausgelegten Multichannel VPN Routerserien 500/51X hingegen beinhalten fest eingebaute Modems, da durch die harten Einsatzbedingungen nur ohne bewegliche Teile ein störungsfreier Betrieb gewährleistet werden kann.

Durch die beliebige Kombinationsmöglichkeit aller Viprinet Router-Typen mit den Multichannel VPN Hub-Modellen 1020 (Standardperformance), 2020 (Enterprise-Variante) und 5010 (ISP-Version) lässt sich für jede Anbindung die passende Lösung finden – ob es sich nun um einen, 10 oder auch 1.000 Standorte handelt.

Multichannel VPN Router 200

Der Multichannel VPN Router 200 wurde speziell für den Einsatz an Heimarbeitsplätzen und auf Reisen konzipiert. Mit ihm kann ein bestehender Internetzugang mit einem zweiten Anschluss gebündelt werden.

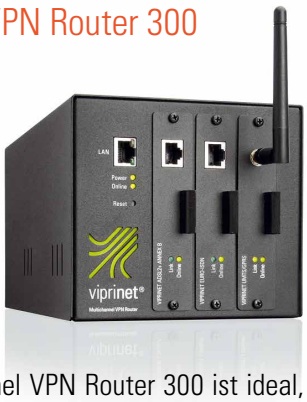
Durch Hinzubündeln freier Upload-Kapazitäten in Mobilfunknetzen wird so z.B. aus einem langsamen DSL-Anschluss mit 300 KBit/s Upstream ein symmetrischer Zugang mit mehreren Megabit im Upstream, wie sie etwa für Videokonferenzen benötigt werden..

Das Gerät hat einen integrierten WLAN Access Point mit 2,4 oder 5 GHz (Dualband) und ist zudem aufgrund passiver Kühlung äußerst energieeffizient und völlig geräuschlos. Durch den Modulslot ist das Modell 200 auch für zukünftige technische Entwicklungen bestens gerüstet.

Technische Daten

Modell	200	300	500
Formfaktor Gehäuse	Desktop	Desktop	Portable
Abmessungen BxHxT	273 x 53 x 160 mm	147 x 130 x 177 mm	115 x 55 x 195 mm
Gewicht (ca.)	1 kg	1 kg	1,5 kg
Stromversorgung	12 VDC, 2 A max	12 VDC, 4 A max	7–33 VDC, 2 A max
Stromanschluss	Netzteil 100-240 VAC, 50-60 Hz	Netzteil 100-240 VAC, 50-60 Hz	Netzteil 100-240 VAC, 50-60 Hz
Lüfteranzahl / -regelung / -überwachung	0 / - / -	0 / - / -	0 / - / -
LAN-Interface	GBit Ethernet	Fast Ethernet	GBit Ethernet
WAN	1 Modulslot, 1x Gbit Eth	3 Modulslots	4x UMTS/HSPA+, 1x GBit Eth
WLAN Access Point	2,4 & 5 GHz Dualband	-	2,4 & 5 GHz Dualband
Leistung Volllast max.	24 Watt	48 Watt	15 Watt
Leistung typisch	10 Watt	20 Watt	10 Watt
SNMP einfach / erweitert	✓ / ★	✓ / ★	✓ / ★
Bonding-Kapazität MBit/s	35	50	35
Empfohlene Anzahl Nutzer im LAN	5	25	10

Multichannel VPN Router 300



Der Multichannel VPN Router 300 ist ideal, um kleine Büros über bis zu drei Internetverbindungen ausfallsicher und breitbandig an das Internet und/oder ein Firmen-VPN anzubinden. Dank seiner drei Modulslots ist er für alle aktuellen und kommenden Breitbandtechnologien gerüstet und höchst flexibel einsetzbar.

Durch konsequente Ausrichtung des Produktes auf niedrigen Energieverbrauch wird der Multichannel VPN Router 300 komplett passiv gekühlt und arbeitet damit geräuschlos. Die Stromversorgung erfolgt über ein externes Steckernetzteil mit einer IEC-Kaltgerätebuchse mit Weitbereichseingang (100–240V, 50–60Hz). So kann dieser Router auch problemlos international eingesetzt werden.

Multichannel VPN Router 500

Dieser Router macht hohe Bandbreiten und ausfallsichere Datenanbindung für den ultra-mobilen Einsatz verfügbar: Vier fest integrierte UMTS/HSPA+/EDGE-Modems garantieren die optimale Ausschöpfung der verfügbaren Mobilfunkbandbreiten. Er beherrscht ein großes Spektrum der weltweit genutzten Mobilfunkfrequenzen und ist dadurch auch länderübergreifend einsetzbar. Die SIM-Karten können im laufenden Betrieb gewechselt werden.

Seine Stärken sind der geringe Energieverbrauch und seine Robustheit. Da er keine beweglichen Teile beinhaltet, machen ihm auch Erschütterungen nichts aus. Der integrierte WLAN Access Point arbeitet mit 2,4 oder 5 GHz (Dualband).

In Kombination mit dem als Zubehör erhältlichen MultiAMP Combiner 400 reicht dem Gerät für alle vier Mobilfunkzugänge zudem eine einzige Fahrzeugantenne aus.

51X	1610	2610
Portable	19" 1,5 HE	19" 1,5 HE
115 x 55 x 195 mm	435 x 66 x 320 mm	435 x 66 x 320 mm
1,3 kg	5,1 kg	5,1 kg
7–33 VDC, 2 A max	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz
Netzteil 100-240 VAC, 50-60 Hz	IEC Kaltgerätebuchse	IEC Kaltgerätebuchse
0 / - / -	2 / ✓ / -	2 / ✓ / -
GBit Ethernet	GBit Ethernet	GBit Ethernet
4xLTE/DC-HSPA+, 1x GBit Eth	6 Modulslots	6 Modulslots
2,4 & 5 GHz Dualband	-	-
15 Watt	70 Watt	75 Watt
10 Watt	40 Watt	45 Watt
✓ / ★	✓ / ★	✓ / ✓
35	125	200
10	50	250

★ optional

Die Produkte im Überblick

Multichannel VPN Router 51X

Die Modellreihe 51X ist ebenso für den ultra-mobilen Einsatz vorgesehen wie das Modell 500, besitzt aber ein komplexeres Innenleben. So sorgen vier fest integrierte LTE/DC-HSPA+/EDGE-Modems für die bestmögliche Bandbreite aus allen verfügbaren Mobilfunktechnologien.

Darüber hinaus ermöglicht dieses Gerät durch die GPS-Funktionalität effizientes Geo-Tracking, wie es etwa für Flotten- oder Fuhrparkmanagement benötigt wird. Der integrierte WLAN Access Point (2,4 oder 5 GHz, Dualband) versorgt beliebige Verbraucher mit ausreichend Bandbreite.

Da für die vierte Generation der Mobilfunknetze unterschiedliche Frequenzen genutzt werden, gibt es in der Serie verschiedene Modelle, die jeweils auf eine Region ausgelegt sind. So deckt das Modell 510 europäische Frequenzen ab, das Modell 511 hingegen US-amerikanische; für Kanada existiert das Modell 512, und für Australien schließlich das Modell 513.

Multichannel VPN Router 1610

Dieser Router im 19"-Format ermöglicht die Bündelung von bis zu sechs beliebigen Internetzugängen unterschiedlicher Anbieter zu einer einzigen virtuellen Standleitung. Dieses Gerät ist die richtige Wahl für Unternehmensstandorte mit bis zu 50 Mitarbeitern. Der Multichannel VPN Router 1610 bietet mit bis zu 125 MBit/s optimale Bündelungskapazitäten für die Einrichtung von Unternehmensnetzwerken kleinerer bis mittlerer Größe. Der Router ist besonders robust und langlebig und bietet eine Vielzahl in der profesionellen Unternehmens-IT unverzichtbarer Features.

Multichannel VPN Router 2610

Der große Bruder des Multichannel VPN Router 1610 mit höherer Performance und erweiterten Management-Features. Das Gerät bündelt bis zu sechs beliebige Internetzugänge unterschiedlicher Anbieter zu einer einzigen virtuellen Standleitung. Die erweiterten Bündelungskapa-

Technische Daten

Modell	1020	2020	5010
Formfaktor Gehäuse	19" 1 HE	19" 1 HE	19" 1 HE
Abmessungen BxHxT	435 x 44 x 235 mm	435 x 44 x 235 mm	435 x 44 x 410 mm
Gewicht (ca.)	3,3 kg	3,3 kg	7,3 kg
Stromversorgung	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz	100–240 VAC, 47–63 Hz
Stromanschluss	IEC Kaltgerätebuchse	IEC Kaltgerätebuchse	2x IEC Kaltgerätebuchse
Lüfteranzahl / -regelung / -überwachung	2 / ✓ / ✓	2 / ✓ / ✓	2 / ✓ / ✓
LAN-Interface	GBit Ethernet	GBit Ethernet	GBit Ethernet
WAN	GBit Ethernet	GBit Ethernet	GBit Ethernet
Leistung Volllast max.	30 Watt	40 Watt	110 Watt
Leistung typisch	25 Watt	35 Watt	90 Watt
SNMP einfach / erweitert	✓ / ★	✓ / ✓	✓ / ✓
Redundanzschaltung	★	✓	✓
Bonding-Kapazität MBit/s	200	400	2000
Maximale Anzahl Standorte	25	50	250

★ optional

zitäten von bis zu 200 MBit/s bieten langfristige Investitionssicherheit für Unternehmen. Der Router eignet sich speziell für die Einrichtung großer Unternehmensnetze und für Standorte mit mehr als 50 Mitarbeitern. Der Multichannel VPN Router 2610 ist mit zusätzlichen Management-Features ausgestattet, mit denen die Verwaltung von großen Netzwerken wesentlich erleichtert wird.

Multichannel VPN Hub

Zur Einrichtung eines Viprinet-Netzwerkes ist neben den Multichannel VPN Routern auch ein Gegenstellen-Gerät notwendig, der Multichannel VPN Hub. Dort werden die vom Router durch den VPN-Tunnel versandten Datenpakete wieder korrekt zusammengesetzt, entschlüsselt und anschließend an die eigentliche Zieladresse im Internet weiter geleitet. Mit nur einer Höheneinheit und einem typischen Stromverbrauch von 25 Watt (Modell 1020) sind die Geräte speziell auf den kostensparenden Betrieb im Rechenzentrum ausgelegt.

Durch die Verwendung hochwertiger Bauteile und die Integration einer intelligenten Redundanzschaltung sind die Multichannel VPN Hubs außerdem besonders wartungsarm und langlebig. Der Multichannel VPN Hub ist in drei Varianten erhältlich, die sich im Hinblick auf ihre Bündelungskapazität voneinander unterscheiden und sich beliebig mit allen anderen Viprinet-Geräten kombinieren lassen. Für Kunden, die keinen eigenen Hub betreiben können, besteht die Möglichkeit, diese Gegenstellenkapazitäten zu mieten. Das bedeutet mehr Flexibilität und optimale Konfiguration für Unternehmensnetzwerke.

Multichannel VPN Hub 1020

Mit einer Bündelungskapazität von bis zu 200 MBit/s ist dieser Hub für die Einrichtung kleiner und mittlerer Unternehmensnetzwerke geeignet. Eine Versorgung von rund zehn, bei Nutzung von langsamen Anbindungen (z.B. UMTS-Bündelung) sogar bis zu 15 Unternehmensstandorten kann hiermit eingerichtet werden.

Multichannel VPN Hub 2020

Dieses Hub-Modell ist für größere Bündelungskapazitäten im Enterprise-Umfeld ausgelegt. Speziell für große Unternehmen mit einer Vielzahl an Standorten stellt der Multichannel VPN Hub 2020 mit seiner Bündelungskapazität von bis zu 400 MBit/s die optimale Variante dar. Denn hiermit kann eine große Zahl von Multichannel VPN Routern auf einem einzigen Hub terminiert werden. Besonders hervorzuheben ist das innovative Redundanzsystem, mit dem höchste Ausfallsicherheit im Gegenstellen-Betrieb gewährleistet werden kann. Hierbei werden zusätzlich zu den produktiv genutzten VPN Hubs einer oder mehrere Backup-Hubs betrieben, die im Fall eines Gerätedefekts mit minimaler Verzögerung die Aufgaben des ausgefallenen Geräts übernehmen können.

Multichannel VPN Hub 5010

Der Multichannel VPN Hub 5010 ist mit einer Bündelungskapazität von 2 GBit/s das leistungsfähigste Gerät im Viprinet-Produktportfolio. Es ist speziell für die Belange von Business ISPs ausgelegt, die mit Viprinet eigene differenzierende Anbindungsprodukte für ihre Kunden schaffen möchten. Neben dem Redundanzsystem sind auch ISP-spezifische Anforderungen wie die Hub-Tunnel-Segmentierung in diesem Gerät implementiert. Der Multichannel VPN Hub 5010 unterstützt das Geschäftsmodell von ISPs in perfekter Art und Weise, da jede Art von Kundenstruktur abgebildet werden kann. Weitere Zusatzfunktionen wie Erweitertes SNMP-Monitoring mit eigener Management Information Base oder ein separater Traffic-Accounting-Server bieten alles für den Einsatz in großen Rechenzentren.

Module & Zubehör

Hot-Plug Module

Die Viprinet Hot-Plug-Module ermöglichen die flexible Bestückung der Multichannel VPN Router. Hot-Plug bedeutet hier, dass die Module im laufenden Betrieb des Routers eingebaut oder gewechselt werden können und ohne Unterbrechung für Verbindungen aus dem LAN mitgenutzt werden. Für jede gängige Zugangsart existiert ein eigener Modultyp. Diese Auswahl wird laufend um neue Techniken ergänzt, daher sind die Multichannel VPN Router zukunftssicher.

Derzeit stehen folgende Modultypen zur Verfügung:

- ADSL 2+ (Annex A oder Annex B)
- VDSL 2 / ADSL2+
- VDSL 2 / ADSL2+ Bonding (für zwei Anschlüsse)
- LTE / UMTS / DC-HSPA+ / GPRS / EDGE (in verschiedenen Ländervarianten und mit / ohne GPS-Empfänger)
- LTE / CDMA / EV-DO (USA)
- UMTS / HSPA+ / GPRS / EDGE
- CDMA 450 (in verschiedenen Ländervarianten für Nord- und Osteuropa)
- 802.11 b/g/n WLAN Client
- Gigabit Ethernet

Mit dem Gigabit Ethernet Modul lassen sich alle Arten von externen Modems oder Leitungsroutern, z.B. für die Einbindung von SDSL-Leitungen, Standleitungen, Satellitenfunk oder Richtfunkstrecken in den Bündelungsverbund integrieren. Weitere Module befinden sich laufend in der Entwicklung.

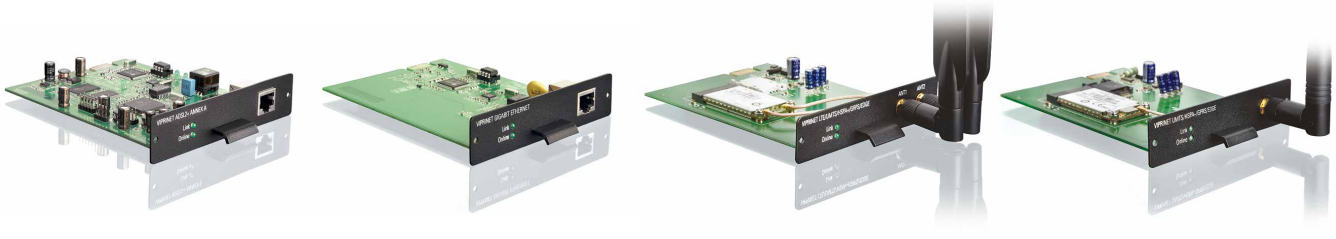
Antennentechnologie – Immer auf Empfang

Je nach Entfernung zur nächsten Funkzelle oder Gebäudebeschaffenheit kann die Empfangsqualität von Mobilfunksignalen an bestimmten Standorten unzureichend sein. Externe Empfangsantennen bringen hier deutliche Vorteile.

Wir bieten Ihnen eine Auswahl verschiedener Antennenlösungen, mit denen sich die meisten Empfangsprobleme schnell und einfach lösen lassen. Dennoch gilt: Je länger das Kabel, desto schlechter die Signalqualität. Versuchen Sie daher stets, das kürzest mögliche Kabel zu verwenden.

MultiAMP Combiner

Der MultiAMP Combiner verbessert die Sende- und Empfangsqualität von UMTS-Mobilfunksignalen. Er wird zwischen maximal vier UMTS/HSPA+-Modulen in Viprinet Multichannel VPN Routern und eine Mobilfunkantenne geschaltet und kann Abstände bis 25m zwischen Router und Antenne verlustfrei überbrücken. Zusätzlich konzentriert er alle verfügbaren Mobilfunk-Signale auf einen Antennenausgang, sodass die Gesamtinstallation lediglich eine Antenne benötigt. Der MultiAMP Combiner steigert die Signalstärke sowohl in Gebäuden als auch in Fahrzeugen, z.B. bei größeren Entfernungen zwischen Router und Antenne oder schwierigen Sende- und Empfangsbedingungen am jeweiligen Einsatzort. Kombiniert mit dem Multichannel VPN Router 500 vereinfacht der MultiAMP Kombiner die Integration der Viprinet-Lösung in Fahrzeuge ganz erheblich.



LTE / UMTS MIMO Dual Omni Panel-Antenne

Die MIMO-Technik („Multiple In Multiple Out“) dieser Antenne sowie zwei Ultrabreitbandempfänger verstärken das gesamte Frequenzspektrum der LTE- und UMTS-Signale in allen in der EU üblichen Frequenzbändern bis zu einem Gewinn von 2 mal 2,5 dBi. Die Wand- oder Mastmontage ist einfach, das Gehäuse wettergeschützt. Die Antenne wird an ein LTE- oder zwei UMTS/HSPA+-Module von Viprinet angeschlossen.

UMTS gerichtete Panel-Antenne

UMTS-Signale sind in Gebäuden häufig schlecht. Dagegen hilft diese Außenantenne. In deren wetterfesten Gehäuse befindet sich ein Ultra-Breitbandempfänger, der einen Gewinn von bis zu 11 dBi erzielt. Die Antenne ist für die Wand- und Mastmontage geeignet und muss auf den Sendemast des jeweiligen Mobilfunkproviders ausgerichtet werden.

UMTS Mini Fensterantenne

Die Antenne kann selbstklebend von innen am Fenster befestigt werden und ermöglicht Gewinne von bis zu 2 dBi. Das drei Meter lange Kabel erlaubt genügend Flexibilität für die Standortwahl des Routers.

LTE / UMTS KFZ-Antenne

Diese Rundstrahlantenne für die feste Fahrzeugmontage ist ideal für mobile LTE- oder UMTS-Anwendungen. Mit einem Gewinn von bis zu 5 dBi ermöglicht sie noch einen Verbindungsaufbau in Gebieten, wo ohne externe Antenne kein Mobilfunksignal mehr empfangen werden kann. Bitte beachten Sie, dass für den Empfang von LTE-Signalen zwei Antennen nötig sind.

Antennenkabelverlängerung

Viprinet bietet zusätzlich zu den beschriebenen ein hochwertiges, verlustarmes CS29-Antennenkabel für die Innen- und Außeninstallation an. Das Kabel ist in den Längen 5m und 10m verfügbar, die Anschlüsse sind SMA (weiblich) und SMA (männlich). Für LTE sind die Verlängerungskabel auch als Doppelkabel erhältlich.

Enterprise-Features

Softwarelizenzen

Viprinet bietet neben zahlreichen Routern für alle Anforderungen unterschiedlicher Standorte auch eine ganze Palette von optional hinzukaufbaren Features, sogenannten „Softwarelizenzen“ an, die insbesondere in großen Unternehmen oder für besondere Anforderungen sehr wichtig sind. Auf diese Weise deckt Viprinet eine Vielzahl von missionskritischen Anwendungen ab. Besonders hervorzuheben sind hier die ausgeklügelten Lösungen für Hochverfügbarkeit und Redundanz der gesamten Technik, egal ob diese im Rechenzentrum oder an wichtigen Standorten verbaut werden. Diese Lösungen ermöglichen zum Beispiel detailliertere Netzwerküberwachung mit Hilfe von SNMP, die Installation zusätzlicher Hubs als Failover-Geräte, eine verbesserte Übertragung von Daten über störungsanfällige Verbindungen oder eine erweiterte Netzwerkadministration. Folgende Softwarelizenzen sind verfügbar:

VPN Client

Der VPN Client ermöglicht die Bündelung von zwei Internetverbindungen wie zum Beispiel WLAN und Mobilfunk ohne weitere Hardware. Gleichzeitig wird ein mit SSL verschlüsselter VPN-Tunnel aufgebaut.

Die Benutzeroberfläche ist einfach bedienbar und gibt Auskunft über die Auslastung und die Leistungsfähigkeit der gebündelten Leitungen. Administriert wird der VPN Client über einen Multichannel VPN Hub. Mit der Konfiguration kann festgelegt werden, ob der gesamte Datenverkehr oder nur der für bestimmte Netze vorgesehene Teil gebündelt wird.

Der VPN-Client kann in Paketen für 1, 10 und 50 User erworben werden. Die Lizenzadministration erfolgt zentral auf dem Hub, der zur Einwahl genutzt wird. Lizenzen für weitere Benutzer können dem Hub jederzeit im laufenden Betrieb hinzugefügt werden. Derzeit ist der VPN Client für die Betriebssysteme Microsoft Windows 2000/XP/Vista/7/8 und für Mac OS X verfügbar. Die Installation erfordert Administratorrechte, die anschließende Nutzung ist hingegen auch mit eingeschränkten Benutzerrechten möglich.

Streaming-Optimierung

Die Standard-Bündelungsverfahren der Viprinet-Router gehen davon aus, dass sämtliche Daten mit möglichst hoher Bandbreite und geringer Latenz ohne Paketverluste zum Ziel kommen sollen. Bei Anwendungen wie Telefonie oder Audio- und Videostreams ist die Minimierung der zeitlichen Verzögerung wichtiger. Mit der Streaming-Optimierung werden im Router zwei neue Bündelungsverfahren freigeschaltet, mit dem sich die erneute Übertragung verlorener Pakete feiner steuern und anpassen lässt:

Mit dem „Lossy Bonding“-Modus lässt sich kontrollieren, wie viel Verzögerung entstehen darf und wann stattdessen Paketverluste in Kauf genommen werden. So läuft eine Video- oder Audioübertragung mit minimaler Latenz.

Im „Bonding Diversity“-Modus werden bei Bedarf Datenpakete dupliziert und über mehrere Kanäle gleichzeitig übertragen. So werden Latenz, Jitter und Paketverluste für die genutzte Anwendung minimiert, obwohl keine Paketverluste toleriert werden.

Node Stacking

Das Node Stacking von Viprinet ermöglicht die Kopplung mehrerer Multichannel VPN Routern zu einem virtuellen Super-Router, der die Bandbreite aller verfügbaren WAN-Verbindungen der gekoppelten Geräte verwaltet. Gesteuert wird der Verbund durch einen festgelegten Router, den Master. Fällt dieser selbst aus, übernimmt ein anderer Multichannel VPN Router innerhalb weniger Sekunden dessen Rolle inklusive IP-Adresse und Konfiguration, bei Ausfall eines Slaves verringert sich nur die Bandbreite.

In Summe kann mit den Viprinet Softwarelizenzen für Node Stacking und Hub-Redundanz, in Verbindung mit der Nutzung unterschiedlicher WAN-Medien (leitungs-/funkbasiert, unterschiedliche Technologien, unterschiedliche Provider) eine Übertragungsstrecke mit maximaler Verfügbarkeit von über 99,9% im Jahr geformt werden. Die gekoppelten Router können Geräte unterschiedlicher Baureihen sein. Das jeweils leistungsfähigste Gerät im Verbund sollte als Master fungieren.

Hub-Redundanzsystem

Zusätzlich zu den produktiv genutzten Multichannel VPN Hubs können Nutzer einen oder mehrere Hubs im Rechenzentrum installieren, die als „Hot Spare", das heißt im Bereitschaftsmodus, laufen. Wenn ein im Produktivbetrieb arbeitender Hub ausfällt, übernimmt das „Hot Spare"-Gerät dessen komplette Identität. Ein Gerätedefekt eines Hubs bedeutet daher für betroffene Kunden mit Hub-Redundanzsystem nur eine Anbindungsunterbrechung im Sekundenbereich.

Hub-Tunnelsegmentierung

Wenn sich verschiedene Nutzer eines Viprinet-Tunnels mit privaten Subnetzen ein und denselben Hub im Rechenzentrum teilen, sind IP-Adresskonflikte wahrscheinlich. Gleiches gilt für normale Standortanbindungen innerhalb eines Unternehmens. Die Lösung dieser Probleme ist die Hub-Tunnelsegmentierung, die wie ein VLAN die Tunnelsegmente logisch so voneinander trennt, als wären sie physikalisch separat.

Traffic-Accounting

Das Viprinet Traffic-Accounting-System sammelt und analysiert Daten, die von Viprinet Multichannel VPN Hubs gesendet werden. Damit lässt sich das Datenaufkommen auf allen Multichannel VPN Routern protokollieren und auswerten. Für ISPs dient dieses System zur Abrechnung des Datenaufkommens bei Mietkunden, für größere Unternehmen kann es zur Auswertung des Datenaufkommens der einzelnen Niederlassungen genutzt werden.

Ein komfortables, webbasiertes Administrationstool stellt alle Funktionen zur Verwaltung und Auswertung zur Verfügung. Es besteht die Möglichkeit, Schwell- und Grenzwerte je Kunde einzupflegen. Werden diese überschritten, wird der Kunde per E-Mail alarmiert. Das Traffic-Accounting-System wird im PHP-Quelltext geliefert, was Anpassungen an eigene Anforderungen ermöglicht. Eine Site-Lizenz genügt dabei für alle Hubs in einem Rechenzentrum.

Erweitertes SNMP-Monitoring

Nutzer, die ihr Netzwerk mit Hilfe von SNMP überwachen und steuern, können ein standard-konformes Monitoring für alle Viprinet-Geräte nutzen. Die Basisfunktionalität zur Abfrage grundlegender Betriebszustände ist bei allen Geräten integriert.

Mit der Softwarelizenz für Erweitertes SNMP-Monitoring können zusätzliche wichtige Detailinformationen abgefragt werden. Dazu hat Viprinet eine eigene MIB (Management Information Base) entwickelt und implementiert. Sie umfasst Informationen zum Router, dessen Status, zum Status der Systemlüfter, der Netzwerkschnittstellen sowie der konfigurierten Tunnel und Tunnelkanäle.

Service & Schulungen

Garantie und Gewährleistung

Neben der gesetzlichen Gewährleistung von 12 Monaten gegenüber gewerblichen Abnehmern bietet Viprinet darüber hinaus eine freiwillige Herstellergarantie für alle Multichannel VPN Router und Hubs. Diese kann bis zu sechs Monate ab Kaufdatum mit einer entsprechenden Lizenz auf drei Jahre erweitert werden. Sollte ein Gerät mit Herstellergarantie defekt werden, repariert Viprinet dieses Gerät innerhalb der Garantiezeit in der Regel kostenfrei.

Anwendersupport

Viprinet bietet Anwendern sowohl E-Mail- als auch Telefonsupport für alle Viprinet-Produkte an. Beim E-Mail-Support handelt es sich um einen kostenfreien First-Level-Support zu grundsätzlichen technischen Fragen, zum Beispiel bei Problemen mit der erstmaligen Einrichtung von Multichannel VPN Routern oder Hubs oder der Integration eines neu erworbenen Moduls in ein bestehendes Netzwerk. In der Regel wird diese Art Support auch vom jeweiligen Distributor eines Landes übernommen.

Von Viprinet geleisteter Telefonsupport geht über First-Level-Supportleistungen hinaus und kommt immer dann zum Einsatz, wenn individuelle Installationen besprochen oder betreut werden sollen, oder wenn ein Fernzugriff des Supportteams auf eine Installation nötig wird. Telefonsupport durch einen Viprinet-Mitarbeiter ist kostenpflichtig und kann in Form einer Lizenz für ein Supportkontingent erworben werden.

Auch können Viprinet-Techniker zur Unterstützung für Vor-Ort-Installationen gebucht werden. Erfahrungsgemäß wird dies häufig mit einer Schulung der Mitarbeiter verbunden, die in Zukunft die Viprinet-Infrastruktur betreuen werden.

Schulungen

Um Anwender für die Vielfalt der Konfigurationsmöglichkeiten von Multichannel VPN Routern und Hubs zu sensibilisieren, bietet Viprinet Schulungen an. Diese finden am Hauptsitz von Viprinet in Bingen am Rhein statt und dauern

in aller Regel zwei Tage. Die Teilnahme an diesen Schulungen wird speziell solchen Anwendern empfohlen, die entweder selbst Viprinet-Technologie verkaufen möchten oder größere Viprinet-Infrastrukturen betreiben. Viprinet-Schulungen sind kostenlos, die Anmeldegebühr wird auf spätere Bestellungen angerechnet.

Des Weiteren bietet Viprinet kostenlose Marketing-Webinare an. Diese Online-Videokonferenzen sind als erweiterte Beratung gedacht und richten sich in erster Linie an interessierte Kunden. Es ist jedoch auch möglich, Viprinet-Mitarbeiter gegen Gebühr für technische Schulungen und Beratungen außerhalb von Bingen zu buchen. Insbesondere, wenn mehrere Mitarbeiter eines Unternehmens im Umgang mit Viprinet-Technologie geschult werden sollen, kann dies eine sinnvolle Alternative sein.

Zusatzleistungen

Das Viprinet-Bündelungsprinzip wird immer wieder weiterentwickelt, um jederzeit auf dem neuesten Stand der Technik zu sein. Dennoch werden aus wirtschaftlichen Gründen nicht alle technologischen Möglichkeiten in die Viprinet-Produkte übernommen. Sollten für ein Projekt Spezifikationen benötigt werden, die standardmäßig nicht implementiert sind, dann sind individuelle Programmierungen möglich. Viprinet-Techniker sind gerne bereit, in einem unverbindlichen Gespräch zu klären, ob die gewünschten Änderungen umsetzbar sind und welche Kosten dabei ungefähr entstehen werden.

Consulting

Viprinet ist sich der Komplexität seiner Technologie sehr wohl bewusst und unterstützt daher seine Kunden auf vielfältige Weise. So übernehmen Viprinet-Techniker auf Anfrage gern die Analyse bestehender Netzwerkinfrastrukturen, die Evaluierung der Optimierungsmöglichkeiten sowie die Planung und konkrete Implementierung einer Viprinet-Infrastruktur. Die Umstellung einer Netzwerkinstallation begleitet Viprinet gerne als Lösungspartner. Viprinet-Techniker haben jahrelange Erfahrung in der Umsetzung selbst außergewöhnlicher Projekte und sind so in der Lage, ihr Wissen bei jeder neuen Aufgabe gewinnbringend einzusetzen.

Schlüsselfertige Lösungen

Das weltweite Netz an Viprinet-Implementierungspartnern hat gemeinsam mit seinen Kunden schon eine Vielzahl an aufregenden Projekten gemeistert. So hat der skandinavische Distributor Sharecon seine eHealth-Lösung Viewcare fest im dänischen Gesundheitssystem verankert. Auch der englische Viprinet-Distributor Wired Broadcast war sehr kreativ und entwickelte den Mediaport, ein auf Viprinet basierendes mobiles Video-Übertragungssystem. Der Mediaport wird mittlerweile von zahlreichen Rundfunkanstalten, aber auch im Versicherungsbereich zur Schadensaufnahme eingesetzt.

viprinet®

Viprinet Europe GmbH
Gaustr. 22–32
D–55411 Bingen am Rhein

Telefon +49 (0)6721 4 90 30-**0**
Fax +49 (0)6721 4 90 30-**109**
E-Mail info@viprinet.com
Web www.viprinet.com

Überreicht durch Ihren Viprinet-Partner:

Layout & Photos: Frauke Bönsch, Illustrations: Andreas Müller & Jörg Pelka