



viprinet®

# Never be offline again.

Multichannel VPN Router™

Multichannel VPN Hub™

- Suited for every connection scenario
- Real bonding of more than six WAN connections
- Modular design provides flexibility
- Hot-plug modems for various access media
- Outage risk distribution to multiple media and ISPs
- Data encryption with highest security standards
- Enables ultra-mobile, portable, and stationary connections



# The Network Revolution

## We are Viprinet

Since 2006, Viprinet has been manufacturing innovative network components. Viprinet is the inventor of a patented technology which really aggregates bandwidths of different wide area network connections. Today, 35 employees develop, produce and sell Viprinet products from Bingen am Rhein into the whole world. Viprinet is profitable and grows fast, financed by its own revenues. Sustainability is a pivotal topic in the corporate philosophy and appears in the length of the product life cycles, in the production which only uses regenerative energy, and in the low energy consumption of Viprinet devices. All products of Viprinet are “Made in Germany” and fulfill the highest standards concerning security and confidentiality.

## Connectivity newly defined

With its unrivaled VPN tunnel technique, Viprinet allows for an entirely new kind of connection for stationary as well as for mobile sites – highly available, fast and cost-effective. The congenial Viprinet principle provides reliability and increased data transfer rates.

## Real bonding of more than 6 WAN links

The Multichannel VPN Router is the core of the Viprinet technology. With this device, several broadband lines can be combined into a single, highly available joint line. Unlike load balancing, which can only distribute load to several WAN links, real bonding of all connections available is realized here.

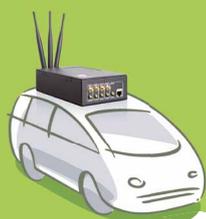
Viprinet can combine all different types of access media, for instance, ADSL, SDSL, 3G/UMTS/HSPA+, or 4G/LTE. The LAN sees these connections as one single line providing the accumulated up- and downstream of the different links – even for single downloads.

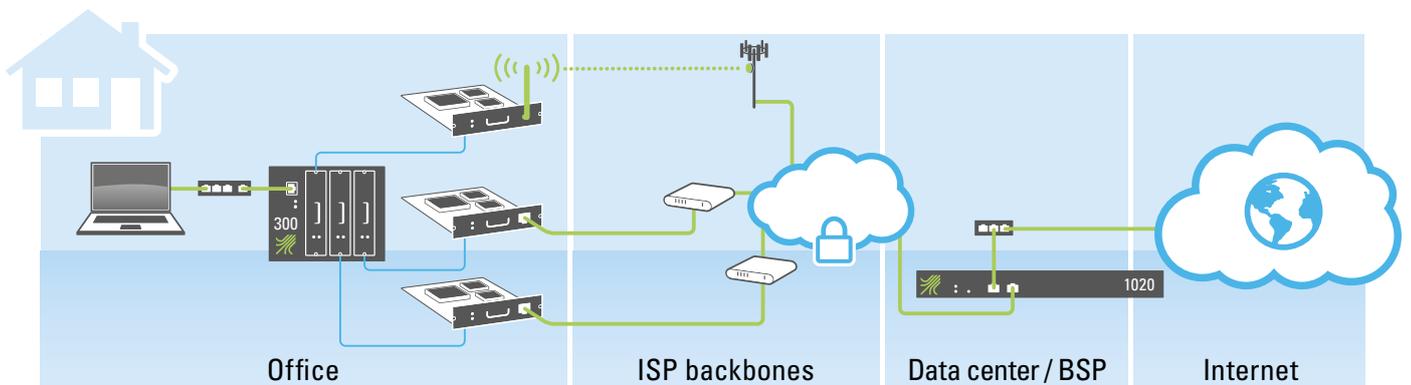
## The remote station principle

Viprinet uses an exceptional VPN tunnel technique with a star topology for secure and fast site, facility and vehicle connectivity. For this purpose, the integration of two different devices is needed:

A Multichannel VPN Router establishes an encrypted VPN tunnel to a single central remote station, the Multichannel VPN Hub, via each Internet line available. These VPN tunnels are then bundled into one tunnel through which the data is transferred.

The Multichannel VPN Hub is usually located in a highly reliable data center and acts as an exchange: Data targeted at another company site will be forwarded through the respective VPN tunnel; data targeted at the public Internet will be decrypted and forwarded to its destination. The VPN Hub provides secure and quick communication between different Multichannel VPN Routers but it also serves as pivotal exchange point between the encrypted VPN and the public Internet.





The data stream from the LAN is encrypted by the Multichannel VPN Router and distributed onto the Internet connections (here: 2x DSL, 1x 3G/UMTS). The encrypted and fragmented data passes the networks of the utilized ISPs and reaches the Multichannel VPN Hub in the data center, which in turn decrypts the data stream and reassembles it correctly. Afterwards, the data stream is forwarded to its actual destination on the Internet. The same goes for the opposite direction: Here, the Hub encrypts the data stream, while the VPN Router decrypts it.

## Bonding Service Provider

Viprinet Bonding Service Providers (BSP) have been established for all those without data center space of their own and/or unwilling to be concerned with bonding. According to the scope of supply negotiated, they provide their customers with Hub capacities or a dedicated Hub and guarantee for the correct termination of the Multichannel VPN Routers on the respective Hub in the data center.

Depending on the demand, the BSPs supply their customers with public IP addresses routed from the data center via VPN tunnels to the respective sites. As an option, the BSPs offer firewall services and other applications that depend on customers' requirements and budgets.

## User-defined combination of access media & ISPs

This principle provides a previously unrivaled flexibility in the network access choice. Users and companies no longer need to be bound to a specific carrier but can freely compose a network design that fits their needs.

Instead of costly dedicated lines hosted by a single provider, they now can utilize cost effective consumer offers like ADSL. This also means security of investment: The Multichannel VPN Router's modular setup allows the smooth integration of future access technologies.



# The Network Revolution

## Company connection newly defined

According to a study of Infonetics Research, medium-sized companies (100 to 1000 employees) lose 3.6 % of their turnover on average each year by downtimes during which the companies' IT sections lie idle. Depending on the branch of business, these downtimes cost a lot of money because communications and production drop out, and employees as well as customers are unable to access information. Mostly, these indirect costs of site-to-site VPN links are underestimated drastically.

Hourly costs (in US\$) for downtimes sorted by branches:	
Retail	69,000
Home shopping	89,000
Media (pay per view)	90,000
Logistics	113,000
Online ticket reservation	150,000
Credit card processing	2,600,000
Broker	6,400,000
Average	336,000

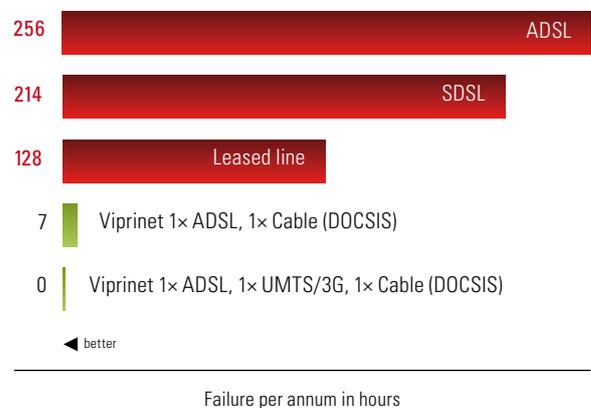
Source: Ponemon Institute 2012, *How much does downtime really cost*

The main focus when planning a company network must thus be the reliability of the concept. Solutions based on the combination of SDSL and IPsec are not very efficient in this regard, since they fail 5–7 days a year on average. The considerably higher priced MPLS offers are not much better – a connection breakdown of several days must be reckoned.

## Reliability by risk distribution

The Multichannel VPN Router's well-trying bonding technique considerably minimizes the outage risk.

By combining several different lines, single line failures do not cause a connection loss inside the bonded tunnel. Only the available total bandwidth decreases by the rate of the link that dropped out; once the link is re-established, the total bandwidth increases automatically. By combining different access ISPs and media types accordingly, a highly available connection can be created. If, for instance, 3G/4G technology is also factored into the bonding, even a total breakdown of all wired links, e.g. during civil engineering works, can be compensated.



## Statistic security instead of ISP promises

With a Viprinet based network solution, money cannot only be saved by a drastic reduction of outage times. Business ISPs are forced to invest considerable time and effort to be able to reach availabilities of over 97% with their offers. For customers, service personnel and technology must be at hand day and night to be able to fix failed lines. Corresponding "Service Level Agreements" (SLAs) make the whole thing more expensive for the ISPs and thus for the customers as well.



With a Viprinet-based linking solution, this effort is not necessary at all: Instead of costly business offers, low priced standard offers geared to the consumer market like ADSL and 3G/UMTS are used. By bonding and risk distribution using the Viprinet technology, it is absolutely sufficient that each Internet link is available only 97% per annum – it is only important that these access lines independent from each other typically do not break down at the same time. Thus, the reliability of the Internet connection increases exponentially with the number of different media bonded by a Viprinet Router.

### Example calculation for a site-to-site company VPN

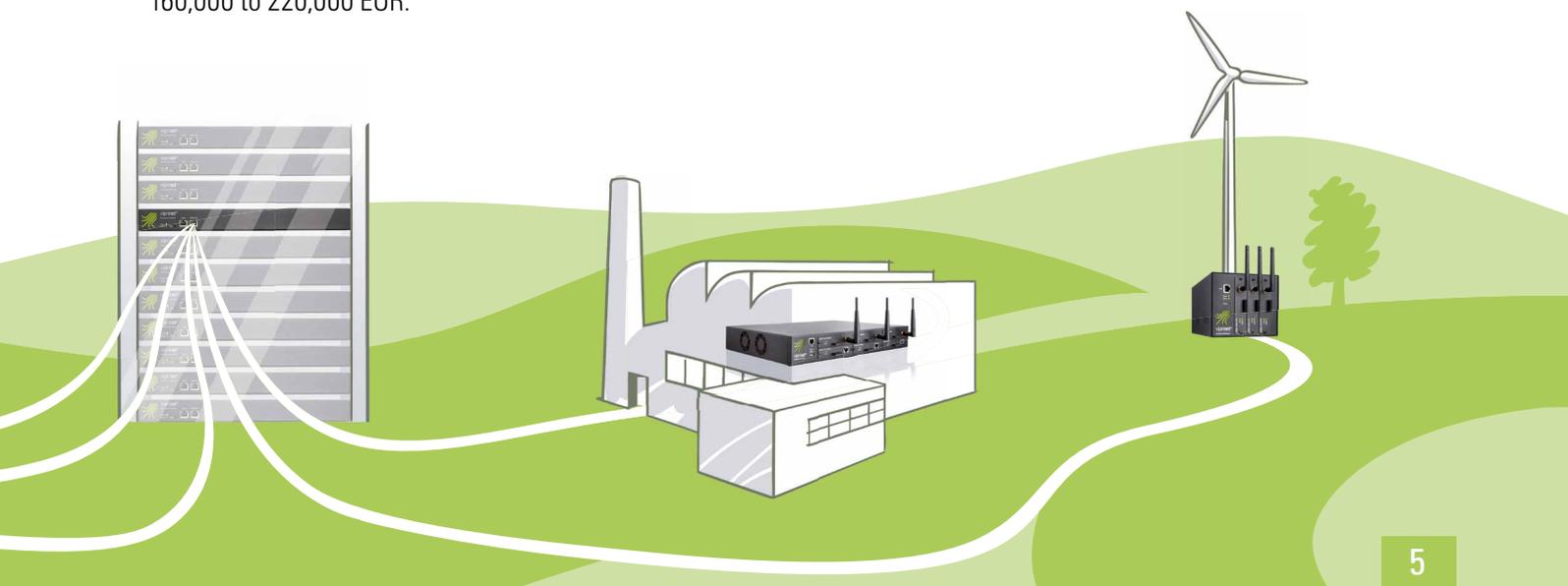
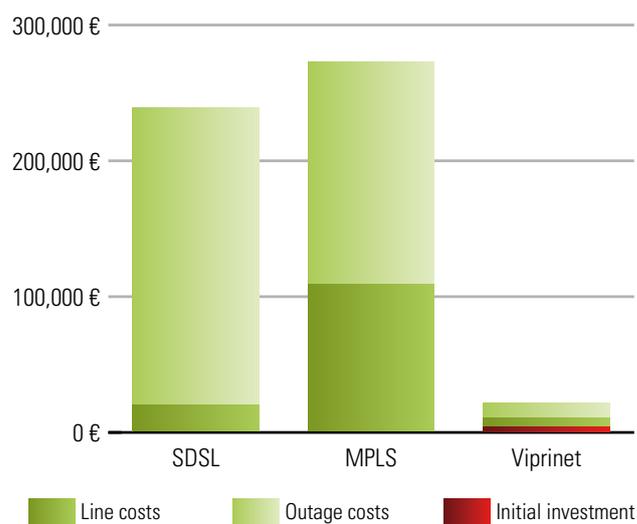
The costs for a site-to-site VPN mostly consist of two components: the actual acquisition and operation costs as well as the risk of financial loss by company standstills caused by connection outages. The graphic shows a company connecting three sites using a bandwidth of ca. 4 MBit/s via VPN with each other.

Here, the cost of financial loss for one day of connection breakdown has been set fairly low at 10,000 EUR. For the common kinds of VPN connections, SDSL and MPLS, service level agreements have been taken into account, which guarantee an availability of 98% (SDSL) respectively 98.5% (MPLS) per year.

98% availability sounds good, but means that a line outage of 5 days per year has to be tolerated. For 36 months, the risk of financial loss of both SDSL and MPLS is about 160,000 to 220,000 EUR.

The Viprinet solution reaches an availability of 99.9% by risk distribution, causing a risk of financial loss of only about 16,000 EUR. In addition, the costs for the Internet lines are lower.

As a result, a reliable connection from Viprinet is not only superior to other VPN solutions by pure operating costs, but shows its enormous possible savings especially in an overall view of the costs including outage times. In comparison to solutions based on SDSL/IPSec and MPLS, possible savings of a Viprinet solution result in about 90%.



# The Network Revolution

## Security against interception

According to various studies, every second company's communication is intercepted. The German Technical Control Board amounts the annual economic damage in 2012 to 4.2 billion EUR for Germany only; other studies start from 50 billion EUR, with a growing tendency. The motivation of criminal gangs and foreign secret agencies alike ranges from classic theft of company secrets over massive abuse of confidential customer data (e.g. credit card data) up to blackmailing.

Like classic burglars, attackers from external data networks always search for the line of least resistance. The most comfortable way today is an attack on the Internet routers being used: All company data traffic travels through over this central device and can thus be easily intercepted. Especially economic Chinese router products often supplied by Internet providers and widely available on the market feature security holes that allow "taking over" the device remotely. Sometimes, these leaks have been known for years and still haven't been eliminated.

In regards to secret agencies, it's general knowledge since the NSA scandal that our communications infrastructure is intercepted extensively, with direct access to the respective networks. Network providers' assertions that their networks can be used for secure company communication are thus reckless. It has to be assumed that especially MPLS networks are wiretapped extensively.

So, since network providers can no longer be trusted, it's time to take IT security and connection encryption into one's own hands. Especially the encryption keys of a company's Internet connection ought to stay with the respective company only.

However, there is another problem: Since quite some time, IT security experts and politicians alike have been assuming that big Chinese manufacturers secretly code back doors for the Chinese government into their products on purpose – one of the largest manufacturers equipping many network providers in Europe is also suspected to be under direct control of Chinese secret agencies.

In western countries, though, things aren't much better. For instance, everyone knows by now that US American router manufacturers can be compelled by law to install back doors into their products. Although such back doors may be intended for legitimate interests like criminal prosecution a back door still is only a door, and doors don't ask who is knocking. Here, it must be feared that the respective surveillance ports may be abused by third parties.

Or, to put it in a nutshell: By trying to unlawfully gain access to data of companies and citizens, the most diverse interest groups have made IT security a topic which ought to be prioritized.

## Viprinet products guarantee security

For all these problems, Viprinet products are an adequate solution. The basic idea of Viprinet Multichannel VPN Routers was from the start that a single network provider's assertions regarding bandwidth availability, stability, and reliability cannot be trusted – rather, any risks regarding an Internet connection should be distributed onto several different media and network providers.

This principle of bonded usage increases security tremendously. All data packets sent via a Viprinet router are first chopped up for being transmitted over several data links, and then encrypted separately for each link.

For that reason, no single carrier network ever transports a complete payload stream. Even if someone were able to break the packets' encryption on the fly, they would only decode data fragments. In order to steal useful information, all packets in all different provider networks would have to be intercepted and correctly attributed to a specific data stream. According to all accounts, no one has of yet been able to do that.

The encryption methods used in Viprinet routers fulfill the highest industrial standards and steer clear of all known attack scenarios. For instance, Viprinet encryption always consists of a mixture of hardware and software solutions that are purchased from neutral suppliers and combined with proprietary development. For that reason, even attacks from supplier side are impossible.

In addition, all Viprinet products are developed and produced in Germany. Thus, Viprinet is in complete control over its production chain, as opposed to other manufacturers. Furthermore, Viprinet is in no danger of being compelled to install back doors and, at the same time, hide that fact from their customers. The company's management staff personally guarantees that Viprinet does not, and never will, maintain business relations with secret agencies.

So, IT security and protection against industrial espionage is all about the right technology, a secure supply chain, and a trustworthy manufacturer. Viprinet guarantees all that.

## Secure site-to-site connection in the field

The functional principle of Viprinet technology is as simple as efficient: Between a Viprinet Multichannel VPN Router on-site and a Multichannel VPN Hub in a specially secured

### Security Features:

- AES 256 Bit CBC
- 2048-bit RSA key with SHA256 certificates
- TLS 1.2
- Diffie-Hellman key exchange with elliptic curves (Perfect Forward Secrecy)
- VPN Hub public key fingerprinting
- All internal services protected with ACLs

and certified data center, a secure VPN tunnel per transmission medium used is established in every direction.

All communication between the different sites is then processed within these VPN tunnels – that way, an end-to-end system is created that cannot be accessed from the outside. Viprinet can also be used in cross-border communication, e.g. when integrating branch offices abroad into a company's network infrastructure, and German IP addresses have to be used at foreign sites.

Besides the well-known advantages of higher bandwidth and almost 100% reliability, companies connecting their different branch offices with Viprinet have the security that no outsiders can ever set eyes on their business documents.

This way, companies can also establish secure communication with their suppliers – they only have to use a Viprinet Multichannel VPN Router terminating at the same Multichannel VPN Hub that processes the company communication. It is possible to precisely fine-tune who is able to access which data streams. Also, companies are free to decide whether suppliers are integrated in the communication permanently or for a limited period of time only.

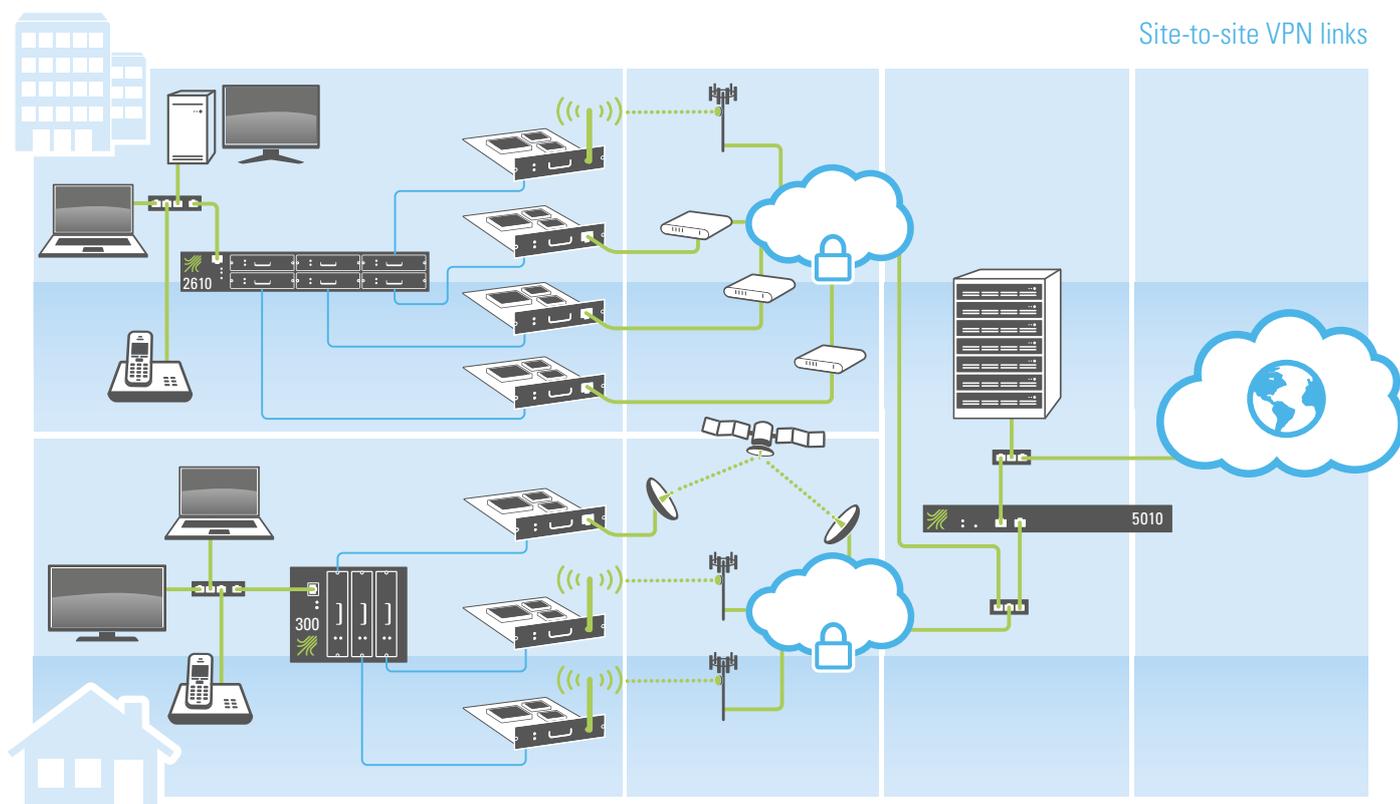
# Fields of Use

## Manifold applications

Due to its flexibility, the Viprinet technology can be employed in a great number of application scenarios. In contrast to competing solutions, Viprinet offers three main benefits: high bandwidths, extraordinary availability, and access from any location. Thus, competitive consumer offers can be upgraded to professional business connections, perfectly catered to the requirements on site. Whether mobile or stationary: Everyone dependent on a fast and secure Internet connection will find Viprinet to be the perfect solution.

## Site-to-site VPN links

Connecting company sites at home and abroad and, at the same time, integrating road warriors, home offices, frequently varying places of operation or sites in insufficiently connected regions are often realized by solutions like MPLS or common leased lines. These are expensive inflexible and do not warrant reliability. Here, well-tried Viprinet technology provides relief by bonding several Internet connections.



*The headquarter is connected to the Internet via a Multichannel VPN Router 2610 bonding three DSL links with an additional 3G/UMTS link. The router establishes an encrypted VPN tunnel to a Multichannel VPN Hub 5010 in a data center. There, a server rack has been installed, in which the company's central applications are running.*

*The branch office is connected via a Multichannel VPN Router 300. Due to lack of DSL availability, 1x Satellite and 2x 3G/UMTS are bonded here. The Router 300 establishes its VPN tunnel to the same VPN Hub as the headquarter.*

*Thus, communication between both sites is always done using the central VPN Hub and is encrypted the whole way. The same applies to the access to the server infrastructure in the data center. Internet access for both sites is also handled by the VPN Hub.*

## Video Streaming

Whether live coverage, event broadcasting or surveillance: Viprinet bonding technology provides a reliable and fast Internet connection at any place for each of these tasks. For this field of application, Viprinet has devised a special kind of bonding. For this kind of application, ready-to-use solutions covering the whole area of video streaming are offered by Viprinet technology partners.

## eHealth

Telemedicine and telemonitoring require high bandwidth and the highest reliability. One field of application is communication between doctor or nursing staff in hospitals and their patients with chronic diseases at home. Viprinet routers are designed especially for the respective application. They bond wired and wireless Internet connections in any combination to a reliable leased line, and thus allow for secure assessment and monitoring of patients.

## Vehicles

The connection of vehicles requires high flexibility due to the vehicles moving and the connection needing to be rebuilt from radio cell to radio cell. In addition, permanent switchovers between different mobile phone standards (GPRS, 3G/UMTS, 4G/LTE) must be mastered.

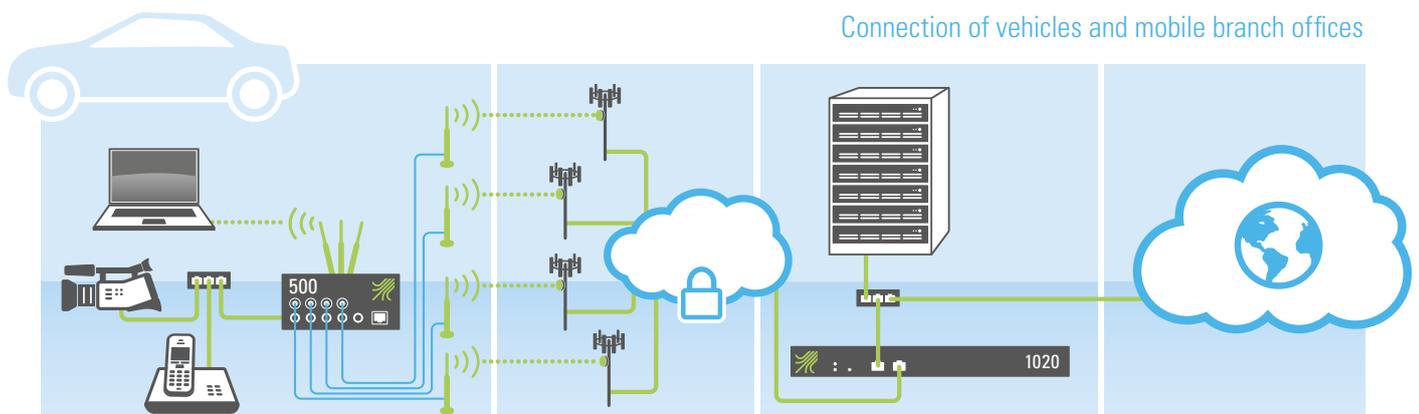
With a vehicle router especially designed for these requirements, Viprinet offers the right solution for uninterrupted Internet connectivity.

## Public sector

Connecting police and emergency vehicles as well as fire trucks to VPNs requires the highest reliability and bandwidth. Viprinet enables usage scenarios that have previously been impossible, e.g. mobile traffic surveillance, e-health applications in ambulance cars and central coordination of rescue squads. The encrypted VPN tunnels satisfy the highest security requirements.

## Ships and oil platforms

With Viprinet, even the most difficult connection scenarios in the maritime and off-shore area can be realized, as in regions without mobile reception or when frequently crossing borders. For instance, highly reliable broadband connections by Viprinet are already applied on oil platforms in order to reduce the use of expensive satellite links to emergencies; also, they are applied on river cruise ships where they enable a seamless Internet connection even when frequently crossing borders.



*The vehicle is equipped with a Multichannel VPN Router 500 providing WLAN which offers easy and comfortable Internet access within the vehicle. Fixed devices however are connected to the router via LAN. The router uses 4 wireless connections to establish a VPN tunnel to the Multichannel VPN Hub 1020 located in the data center. From here, traffic is forwarded to the Internet without encryption.*

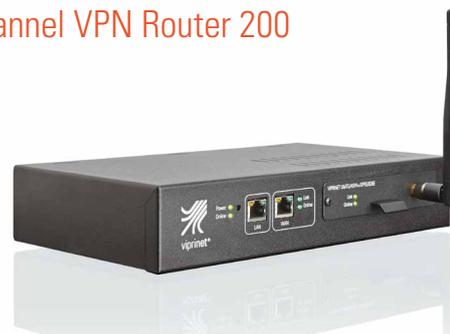
# Product Overview

## Suitable solutions for all requirements

There are five variants of Multichannel VPN Routers: the standard device for bonding up to six connections (Model 1610), the enterprise version with higher performance and additional management features (Model 2610), the desktop version for bundling up to three lines for use in smaller businesses, or in home offices (Model 300), the ultra-mobile variants for use in vehicles (Series 500 and 51X), and the entry level model (Model 200). With their interchangeable module system, most Multichannel VPN Routers are designed for "hot plugging", thus lines and modems can be added or substituted during operation, without loss of connectivity. In contrast, robust designed Multichannel VPN Router model series 500 and 51X contain built-in modems, since uninterrupted operation can only be guaranteed without movable parts, due to the harsh usage conditions.

By individually combining the different routers with one of the Multichannel VPN Hub models 1020 (standard performance), 2020 (enterprise version) and 5010 (ISP variant), a scalable solution for any kind of connectivity can be set up.

## Multichannel VPN Router 200



The Multichannel VPN Router 200 was designed especially for use in home offices and while travelling. With this device, an existing Internet connection can be bonded with another one.

By adding free unused upload capacities in mobile phone networks to a slow DSL connection with 300 KBit/s upstream, a symmetric link with a speed of several megabits in the upstream direction can be established, e.g. for video conferencing.

The device comes with an integrated WiFi Access Point with 2.4 or 5 GHz (Dual Band) and passive cooling; it is thus extremely energy-efficient, and completely noiseless. Thanks to its module slot, model 200 can be easily upgraded to future technologies.

## Technical Specifications

Model	200	300	500
Enclosure Format	Desktop	Desktop	Portable
Dimensions (WxHxD)	273 x 53 x 160 mm	147 x 130 x 177 mm	115 x 55 x 195 mm
Weight (ca.)	1 kg	1 kg	1.5 kg
Power rating	12 VDC, 2 A max	12 VDC, 4 A max	7–33 VDC, 2 A max
Power supply	External power supply, 100–240 VAC, 50–60 Hz	External power supply, 100–240 VAC, 50–60Hz	External power supply, 100–240 VAC, 50–60 Hz
Coolers: Number / Regulation / Control	0 / - / -	0 / - / -	0 / - / -
LAN interface	GBit Ethernet	Fast Ethernet	GBit Ethernet
WAN	1 module slot, 1x Gbit Eth	3 module slots	4x UMTS/HSPA+, 1x GBit Eth
WLAN access point	2.4 & 5 GHz Dual Band	-	2.4 & 5 GHz Dual Band
Maximum power consumption	24 Watt	48 Watt	15 Watt
Typical power consumption	10 Watt	20 Watt	10 Watt
SNMP basic / extended	✓ / ★	✓ / ★	✓ / ★
Bonding capacity MBit/s	35	50	35
Recommended number of users in LAN	5	25	10

## Multichannel VPN Router 300



The Multichannel VPN Router 300 is the perfect solution to connect small offices to the Internet or a corporate VPN via up to three Internet connections. Thanks to its three module slots, the device is suited for all current and future broadband technologies, and can be utilized very flexibly.

As the Multichannel VPN Router 300 has been designed for the highest possible degree of energy efficiency, it is passively cooled without fans and thus operates completely silent. That way, the router may well be used directly at workstations. Power is provided using an external AC adapter (IEC plug 100–240V, 50–60Hz), allowing international deployment without any problems.

## Multichannel VPN Router 500



This router makes high bandwidths and reliable data connection available for ultra-mobile usage scenarios: Four integrated UMTS/HSPA+/EDGE modules guarantee optimal utilization of all available cellular mobile bandwidths. This router model is able to handle a broad spectrum of mobile phone frequencies used worldwide, and can thus be deployed internationally. SIM cards may be changed during operation.

The device stands out due to its robust and power saving layout – it has been designed without any moving parts, so it is able to easily withstand vibrations. The integrated WiFi access point works with 2.4 or 5 GHz (Dual Band).

In combination with a MultiAMP Combiner 400, the device only needs one car antenna for all four antenna outputs.

51X	1610	2610
Portable	19" 1.5 U	19" 1.5 U
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
External power supply, 100–240 VAC, 50–60 Hz	Integrated IEC socket	Integrated IEC socket
0 / - / -	2 / ✓ / -	2 / ✓ / -
Gbit Ethernet	Gbit Ethernet	Gbit Ethernet
4x LTE/DC-HSPA+, 1x Gbit Eth	6 module slots	6 module slots
2.4 & 5 GHz Dual Band	-	-
15 Watt	70 Watt	75 Watt
10 Watt	40 Watt	45 Watt
✓ / ★	✓ / ★	✓ / ✓
35	125	200
10	50	250

★ optional

# Product Overview

## Multichannel VPN Router 51X



The model series 51X was also designed for ultra-mobile usage scenarios, but comes with more complex inner workings. Here, four integrated LTE/DC-HSPA+/EDGE/GPS modems ensure the best possible bandwidth from all available mobile phone connections.

Furthermore, this device enables efficient geo-tracking by its GPS functionality – ideal for vehicle fleet management. The integrated WiFi access point with 2.4 or 5 GHz (Dual Band) provides all the available bandwidth for any number of users.

When it comes to the fourth generation of mobile phone networks, different frequencies are used in different countries. For that reason, Viprinet has developed different models in this router series that have been designed for specific regions. So, model 510 was designed to cover European frequencies; model 511 aims at covering US American frequencies; for Canada, model 512 was developed; and last but not least, model 513 was designed for Australia.

## Multichannel VPN Router 1610



This 19"-sized router allows bonding up to six different WAN lines into a single, high-performance virtual link. Whether it is used for site link even in remote areas at home or abroad, for integrating home offices or road warriors into the company VPN, or for establishing a reliable and fast Internet link in rural areas: The Multichannel VPN Router 1610 offers ideal bonding capacities for setting up company networks of different sizes. The router is particularly robust and persistent.

## Multichannel VPN Router 2610

The Multichannel VPN Router 1610's big brother has higher performance and enhanced management features. The device bundles up to six different WAN lines into a single, high-performance virtual link. Extended bonding capacity of up to 200 MBit/s provides long-term security of investment for companies.

## Technical Specifications

Model	1020	2020	5010
Enclosure Format	19" 1 U	19" 1 U	19" 1 U
Dimensions (WxHxD)	435 x 44 x 235 mm	435 x 44 x 235 mm	435 x 44 x 410 mm
Weight (ca.)	3.3 kg	3.3 kg	7.3 kg
Power rating	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz	100–240 VAC, 47–63 Hz
Power supply	Integrated IEC socket	Integrated IEC socket	2x Integrated IEC socket
Coolers: Number / Regulation / Control	2 / ✓ / ✓	2 / ✓ / ✓	2 / ✓ / ✓
LAN interface	Gbit Ethernet	Gbit Ethernet	Gbit Ethernet
WAN	Gbit Ethernet	Gbit Ethernet	Gbit Ethernet
Maximum power consumption	30 Watt	40 Watt	110 Watt
Typical power consumption	25 Watt	35 Watt	90 Watt
SNMP basic / extended	✓ / ★	✓ / ✓	✓ / ✓
Redundancy system	★	✓	✓
Bonding capacity MBit/s	200	400	2000
Maximum number of sites	25	50	250

★ optional

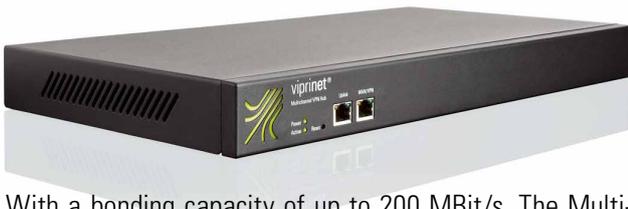
The router is especially suited for setting up large company networks. The Multichannel VPN Router 2610 is equipped with additional management features facilitating large network maintenance.

## Multichannel VPN Hub

In addition to the Multichannel VPN Router, a remote device is needed for establishing a Viprinet network: the Multichannel VPN Hub. Here, the data sent through the VPN tunnel by the local router is being reassembled and decrypted, before it gets forwarded to its original destination on the Internet. With only one height unit and a typical power consumption of less than 100 Watts, the device is specifically designed for cost-effective operation in data centers.

The use of high-quality parts and the integrated smart redundancy system make the Multichannel VPN Hub a particularly durable low maintenance device. The Multichannel VPN Hub is available in three versions to be combined freely with all other Viprinet devices. This provides more flexibility and ideal configuration for company networks.

## Multichannel VPN Hub 1020



With a bonding capacity of up to 200 MBit/s, The Multichannel VPN Hub 1020 was especially designed to be used for smaller or medium-sized company networks. This model is able to cover about ten company sites; when utilizing slow connections at the respective sites (e.g. 3G bonding), it can provide highly reliable broadband Internet even for up to 15 branch offices.

## Multichannel VPN Hub 2020

This Hub model was designed for large bonding capacities in the enterprise sector. Particularly big companies that want to connect a great number of sites will find the Multichannel VPN Hub 2020 with its bonding capacity of up to 400 MBit/s the ideal option. It allows for termination of numerous Multichannel VPN Routers on one single Hub. The novel redundancy system is especially noteworthy.

It guarantees the highest reliability in maintaining the remote station. In addition to those Hubs in productive use, one or more backup (hot spare) Hubs can be operated that – in case of a Hub malfunction – will take over all functions of the defective device with the least possible delay.

## Multichannel VPN Hub 5010



With a bonding capacity of 2 GBit/s, the Multichannel VPN Hub 5010 is the most powerful device in the Viprinet product range. It has been designed especially for the needs of Business ISPs that want to create their own differentiating connectivity products with Viprinet for their customers. In addition to the Hub Redundancy System, applications especially for ISPs like Hub Tunnel Segmentation have been implemented in this device. The Multichannel VPN Hub 5010 perfectly supports ISP business models as it can handle every kind of customer characteristics. Additional functions like Extended SNMP Monitoring with its own Management Information Base, or a separate Traffic Accounting server provide everything necessary for deployment in large data centers.

# Modules & Accessories

## Hot Plug Modules

Viprinet's Hot Plug Modules allow for flexible equipment of Multichannel VPN Routers. Hot plugging here means that modules may be added or replaced during operation, without any interruption to running data transfers from clients inside the LAN. The modular layout allows equipping the existing hardware with the most up-to-date technologies. That way, Viprinet routers are, for example, able to function with the next mobile phone generations without any problems. For all current access technologies, a distinct module is available.

Currently, the following Hot Plug Modules are available:

- ADSL 2+ (Annex A or Annex B)
- VDSL 2 / ADSL2+
- VDSL 2 / ADSL2+ Bonding (for two lines)
- LTE / UMTS / DC-HSPA+ / GPRS / EDGE (in different regional variants and with / without GPS receiver)
- LTE / CDMA / EV-DO (USA)
- UMTS / HSPA+ / GPRS / EDGE
- CDMA 450 (in different regional variants for Northern and Eastern Europe)
- 802.11 b/g/n WiFi Client
- Gigabit Ethernet

With the Gigabit Ethernet module, all kinds of external modems or line routers, e.g. for SDSL links, leased lines, satellite radio or microwave relay, can be integrated into the bonded tunnel. Further modules are constantly developed.



## Antenna technology – Always on „Receive“

The reception quality of mobile radio signals depends on the distance to the next radio cell, on the properties of a building, on the length of antenna cables, and on whether the mobile radio device is moving. In such scenarios, external antennas or installation on buildings and vehicles bring clear advantages. Thus, Viprinet offers a range of powerful antenna solutions.

## MultiAMP Combiner



The MultiAMP Combiner increases the quality of sending and receiving 3G/UMTS mobile radio signals. The device is interconnected between a maximum of four UMTS/HSPA+ modules in Viprinet Multichannel VPN Routers and one mobile radio antenna, and is able to compensate for distances of up to 25m between router and antenna without any signal loss.

In addition, the device concentrates mobile radio signals onto one antenna output, so the entire installation requires one antenna only. The MultiAMP Combiner increases signal strength in buildings as well as in vehicles, especially when greater distances between router and antenna have to be compensated for, or when conditions for sending and receiving are difficult.

## LTE / UMTS MIMO Dual Omni Panel Antenna



This antenna's MIMO (Multiple Input Multiple Output) technology as well as two ultra-wideband receivers amplify the whole frequency range of 4G and 3G signals within all frequency bands used in the EU with a gain of 2 times 2.5 dBi. The antenna is suitable for simple wall or pole mounting, and the casing is weatherproof. The antenna can be connected to one LTE or two UMTS/HSPA+ modules from Viprinet.

## 3G/UMTS Directional Panel Antenna



3G/UMTS signals are often poor in buildings. Here, this outdoor antenna helps. In its weather-resistant and stable housing, an ultra-wideband receiver is installed which gains up to 11 dBi. The antenna is suitable for simple wall or pole mounting; it must be directed at the transmission tower of the respective mobile service provider employed.

## 3G/UMTS Mini Window Antenna



This antenna is self-adhesive and can be attached to the inside of a window, and gains up to 2 dBi. The 3 m cable allows sufficient flexibility for choosing the location of the router.

## LTE / UMTS Car Antenna



This omni-directional antenna for fixed installation on the roof of a vehicle is ideal for mobile 4G/LTE or 3G/UMTS applications. With a gain of up to 5 dBi, it enables signal reception even in areas where no mobile phone signal can be received without an external antenna. Please note that to receive 4G/LTE signals, two antennas are necessary.

## Cable Extension

High-quality, low-loss CS 29 coaxial cable for indoor and outdoor installation. The cable is available in lengths of 5m and 10m, the connectors are SMA (female) and SMA (male). For 4G/LTE, the cable extension is also available as a twin cable.

# Enterprise Features

## Software Licenses

Besides many routers for all requirements of different sites, Viprinet also offers a range of optionally purchasable features, so-called “software licenses”, which are very important especially for large enterprises or special needs. This way, Viprinet covers quite a number of mission-critical applications. Here, the focus lies on sophisticated solutions for high availability and redundancy of complete infrastructures, no matter whether they are installed in a data center or at important sites.

As an example, these solutions enable more detailed network monitoring using SNMP, installation of additional hubs as failover devices, enhanced data transmission over delicate connections, or advanced network administration. The following software licenses are available:

## VPN Client



Viprinet’s VPN Client enables bonding two Internet connections without any further hardware, e.g. one Wi-Fi link and one 3G mobile phone connection. At the same time, an SSL-encrypted VPN tunnel is established. The user interface can be easily operated, and gives an extensive overview over the utilization and performance of the connections bonded.

The administration of the VPN Clients is handled by a Multichannel VPN Hub. Configuration options allow defining whether all data traffic or only data traffic with destination in certain networks should be bonded.

Licenses can be purchased for 1, 10, or 50 users. License administration is managed centrally on the Hub used for login. Additional licenses for more users can be added to the VPN Hub at any time during operation. Currently, the VPN Client is available for the operating systems Microsoft Windows 2000/XP/Vista/7/8 and Mac OS X. Installation requires administrator rights; the subsequent use, however, is also possible with limited user rights.

## Streaming Optimization

The standard bonding method of a Viprinet router is designed so that all data reaches its target without packet loss, with as high bandwidths and low latencies as possible. For applications like telephony or audio and video streams however, the complete transmission of all data is more important. With Streaming Optimization, two new bonding methods are unlocked within the router which allow better control and adjustment of repeated transmission of lost packets:

With the “Lossy Bonding” mode, it can be controlled how much delay may occur, and when packet loss has to be accepted instead. By that, video or audio data is transmitted at minimum latency.

In “Bonding Diversity” mode, data packets are duplicated and transmitted simultaneously through multiple channels at the same time. Thus, latency, jitter and packet loss are minimized, although packet loss is not allowed.

## Node Stacking

Viprinet's Node Stacking enables coupling several Multichannel VPN Routers to one virtual super router managing the bandwidth of all coupled devices' WAN connections. The Node Stacking network is controlled by a fixed router: the master. If the master itself fails, another Multichannel VPN Router takes over its role within only a few seconds. If a slave fails, only bandwidth decreases.

Altogether, with the Viprinet software licenses for Node Stacking and Hub Redundancy in connection with the use of various WAN media (wired/wireless, different technologies, different providers), an Internet link with a maximum annual availability of over 99.9% can be formed. The coupled routers can be devices from different series; the respectively strongest device in the network should be configured as the master.

## Hub Redundancy System

In addition to the productively used Multichannel VPN Hubs, users can install one or more Hubs in the data center running as a "Hot Spare", i.e. in standby mode. In the event of a productive Hub failing, the "Hot Spare" device automatically takes over the complete identity of the failed Hub. A defective Hub therefore means only a connection interruption of seconds for affected customers using the Hub Redundancy System.

## Hub Tunnel Segmentation

When different users of a Viprinet tunnel with private subnets use one and the same Hub in a data center, IP address conflicts become likely. The same problem can also occur in normal site-to-site links within a company.

The solution to this problem is the Hub Tunnel Segmentation which separates tunnel segments logically from each other as if they were physically apart, much like VLANs do.

## Traffic Accounting

The Viprinet Traffic Accounting System gathers data sent from Multichannel VPN Hubs. By that, data volumes can be analyzed. For ISPs, this system is useful for the accounting of traffic volumes of rental customers; for larger companies, it may be used for evaluation of data volumes of individual branch offices.

A convenient, web-based administration tool provides all functions for management and evaluation of data traffic. It is also possible to set thresholds and limits per customer. If these are exceeded, the customer will be alerted by email. The Traffic Accounting System is delivered in PHP source code. One site license is valid for all Hubs in one data center.

## Extended SNMP Monitoring

Users monitoring and controlling their network via SNMP can use standards-compliant monitoring for all Viprinet devices. Extended SNMP Monitoring provides additional important details based on the Viprinet MIB (Management Information Base). It includes information about the router, its status, the status of the system fan, the network interfaces, as well as the configured tunnel and tunnel channels.

# Service & Trainings

## Guarantee and warranty

Besides the legal warranty of 12 months for commercial customers, Viprinet offers an additional optional manufacturer's guarantee for all Multichannel VPN Routers and Hubs. Up to six months after the purchase date, this guarantee can be extended to three years by buying the respective license. In case a device with manufacturer's guarantee becomes defect, Viprinet will generally repair this device free of charge within the guarantee period.

## User support

Viprinet offers users email and telephonic support for all Viprinet products. Email support here means first-level support on general technical questions that is free of cost, e.g. when experiencing problems with the initial configuration of Multichannel VPN Routers or Hubs, or with the integra-

tion of a newly purchased module into an existing network. In general, this kind of support is also given by Viprinet distributors.

Viprinet telephonic consultation goes beyond first-level support services, and is administered when individual installations are to be discussed or maintained, or when the Viprinet support team needs to access an installation remotely. Telephonic support given by a Viprinet employee is liable for costs, and can be purchased in form of a license for a remote assistance quota.

Also, Viprinet technicians can be booked for consultation on installations on-site. Experience has shown that this is often connected to trainings for those employees that will manage the Viprinet infrastructure in the future.



## Trainings

In order to raise users' awareness of the manifold configuration possibilities of Multichannel VPN Routers and Hubs, Viprinet offers trainings. These take place at Viprinet headquarters in Bingen am Rhein, Germany, and generally last two days.

Participation in these trainings is recommended especially for users that either want to sell Viprinet technology themselves, or operating larger Viprinet infrastructures. Viprinet trainings are free of charge; the registration fee is refunded as credit on the later placement of an order.

In addition, Viprinet offers free marketing webinars. These online video conferences are designed as advanced product consultations, and mainly aim at interested customers. However, it is possible to book Viprinet employees for technical trainings and consultations outside of Bingen for a small fee. This can be a reasonable alternative especially when several employees of a company have to be trained in working with Viprinet technology.

## Additional services

The Viprinet bonding principle is further developed continuously in order to always be up-to-date. Nevertheless, not all technological possibilities are adapted into Viprinet products out of economic reasons. In case a project needs features that are not already implemented in the standard Viprinet products, Viprinet offers individual programming. In a non-binding one-on-one interview, Viprinet technicians will happily figure out whether the desired changes can be realized and which costs they might generate.

## Consulting

Since Viprinet is very aware of the complexity of its technology, the company provides support for its customers in many ways. So, Viprinet technicians will be happy to take over the analysis of existing network infrastructures, evaluation of optimization possibilities, as well as planning and concrete implementation of a Viprinet infrastructure on demand. Also, Viprinet will gladly accompany customers that wish to migrate a network installation as solution partner. Viprinet technicians have years and years of experience in implementing even extraordinary projects, and therefore are able to deploy their knowledge in every new task with profitable success.

## Turn-key solutions

Together with its customers, the worldwide network of Viprinet implementation partners has been able to master quite a large number of exciting projects. For instance, Scandinavian distributor Sharecon has been able to incorporate their eHealth solution Viewcare firmly into the Danish health system. Also, English Viprinet distributor Wired Broadcast was very creative, and developed the Mediaport: a mobile video broadcasting system based on Viprinet. By now, the Mediaport is used frequently by various broadcasting companies, but also in the area of insurance for damage surveys.



Viprinet Europe GmbH  
Gaustr. 22-32  
55411 Bingen am Rhein  
Germany

Phone +49 (0)6721 4 90 30-0  
Fax +49 (0)6721 4 90 30-109  
E-Mail [info@viprinet.com](mailto:info@viprinet.com)  
Web [www.viprinet.com](http://www.viprinet.com)

Received from your Viprinet partner: