



viprinet®

Never be offline again.

Multichannel VPN Router™

- Bundles up to 3-6 WAN Modules
- May be used as Access- and VPN-Router
- Hotplug modems for ADSL, UMTS, ISDN and others
- Arbitrary combinations of line types & ISPs
- Real bonding of all line bandwidths
- VPNs using 256Bit SSL/AES per channel



The product at a glance

Real bundling of up to six WAN links

The Multichannel VPN Router lets you bundle up to six broadband lines into a single high available connection. Unlike existing load balancing technologies our router is the first to enable real bundling of arbitrary types of lines. For example, you can combine four ADSL lines from different providers with a synchronous SDSL line and an EDGE/UMTS wireless connection. The LAN sees these connections as one single line providing the accumulated up- and downstream of the different lines even for single downloads.

Arbitrary combinations of line types and ISPs

This technology enables a previously unattainable flexibility in selecting Internet access packages. You are no longer bound to a specific carrier – instead you can flexibly select lines suitable for your requirements, replacing expensive leased lines with low-cost consumer products like ADSL.

Fail-safe risk distribution

The Multichannel VPN Router's novel bundling technique provides you with a new dimension in fail-safe connectivity: single lines going down never cause connection aborts. Instead only the total available bandwidth gets reduced by the faulting line's throughput. The available bandwidth automatically increases as soon as the line goes back up again.

By combining different access providers and media types you get a highly available connection – the outage risk gets distributed and thereby minimized significantly.



Up to six integrated hot pluggable line modems

For portable or fixed use

Up to six internal modem cards for different access types can be plugged into the Multichannel VPN Router 1600. With its 19" form factor, it may either be mounted into a rack or used in a desktop environment.

With the Multichannel VPN Router 300, a compact desktop variant of the product is available, featuring three hot-plug slots compatible to those of the 1600 model. This router is ideally suited for small or home offices. Portable usage of the device makes stable broadband available rapidly even when used at frequently changing locations.

Both router models are hotplug-enabled – lines and modems can be added, exchanged or removed during operation without interrupting connections. Ethernet modules let you easily integrate line types for which an internal modem module is not yet available.



Range of use

Connect company branches with VPNs

The Multichannel VPN Router is the ideal base for building a powerful VPN network between office branches. The router establishes a VPN tunnel to a central "VPN Hub" via a Internet line bundle custom-tailored for each branch's requirements. This virtual bundled link is then used for communicating with other branches and the Internet. More information on this use case is available on pages 4 and 5.

Fast and fail-safe Internet connectivity

By linking it with a peer located at an Internet backbone (e.g. at an ISP or in a data center), the Multichannel VPN Router can be used to provide a single company office with a high-bandwidth, high-available Internet connection. By bundling several lines into one, the Multichannel VPN Router is especially useful for areas where broadband

connectivity is scarce or only low bandwidth lines are available. Using multiple bundled UMTS/3G links, stable broadband connectivity becomes available for mobile applications. More Information on how the Multichannel VPN Router may be used to increase the usable bandwidth is available on pages 6 and 7.

Cost-benefit ratio

WAN integration based on the Multichannel VPN Routers finally enables fast and safe VPN connectivity even for small to mid-sized businesses. Compared to leased lines or MPLS-based services running costs may be cut drastically. Not being bound to a single ISP also enables shorter line contract terms, providing the option to upgrade line capacities at any later time. And finally the lowered risk of total connectivity outages helps reduce the costs attached to IT downtimes. With purchase prices starting below 2,400 Euro (net) for a router equipped with a typical mixture of modules, expenditures are to amortize quickly.

Technical specifications - Multichannel VPN Router 1600 / 300

The Multichannel VPN Router is equipped with a fixed Fast Ethernet LAN jack. When used as a VPN Node this port is used to connect to a LAN switch. When the router is used as a VPN Hub (for example inside the head office or a data center), it forwards traffic between both the various encrypted VPN site links and the unencrypted Internet. The Router is fitted with multiple slots for hotplug modem modules. Modem types can be freely mixed and matched. An Ethernet module can be used to connect external modems, e.g. for SDSL or leased lines, for usage in the bundled link.

| Model: | 1600 | 300 |
|------------------------------|--------------------------|--|
| Format: | 19" enclosure, 1,5 HU | Desktop enclosure |
| Dimensions: | WxHxD 440 x 65 x 325 mm | WxHxD 147 x 130 x 177mm |
| Weight: | ca. 4,7 kg | ca. 1 kg |
| Power rating: | 90-265 VAC, 47-63 Hz | 12V, 4A max |
| Power supply: | Integrated IEC socket | External AC/DC adapter 90-265 VAC, 47-63Hz |
| Cooling: | Redundant case fans | Passive (Ambient temperature 0-40°C) |
| Maximum power consumption: | 78 Watt | 50 Watt |
| CPU clock speed: | 1 GHz | 500 Mhz |
| Hardware traffic encryption: | AES 256 Bit | AES 256 Bit |
| RAM: | 512 MB | 256 MB |
| LAN-Port: | Fast Ethernet 100 MBit/s | Fast Ethernet 100 MBit/s Auto-MDIX |
| Module slots: | 6 | 3 |
| VPN/Routing bandwidth: | 100 MBit/s | 75 MBit/s |

Supported features (excerpt):

- Quality of service / traffic shaping (per WAN module / VPN tunnel)
- NAT and port forwarding
- Monitoring (graphical and remote-syslog)
- Unlimited number of VPN tunnels and VPN client connections (SSL/AES)
- Rule-based routing
- Traffic accounting via external SQL server
- Web administration frontend that supports multiple organizations

Connecting company branches with VPNs

Introduction

Today, company structures distributed across several locations are almost the rule rather than the exception, caused by frequent expansion, location change and outsourcing of departments. Changes in society also influence the flow of communication inside a company – experts working from home offices are commonplace in many industry sectors. Also cooperation with external customers, partners and supplier gets closer and closer.

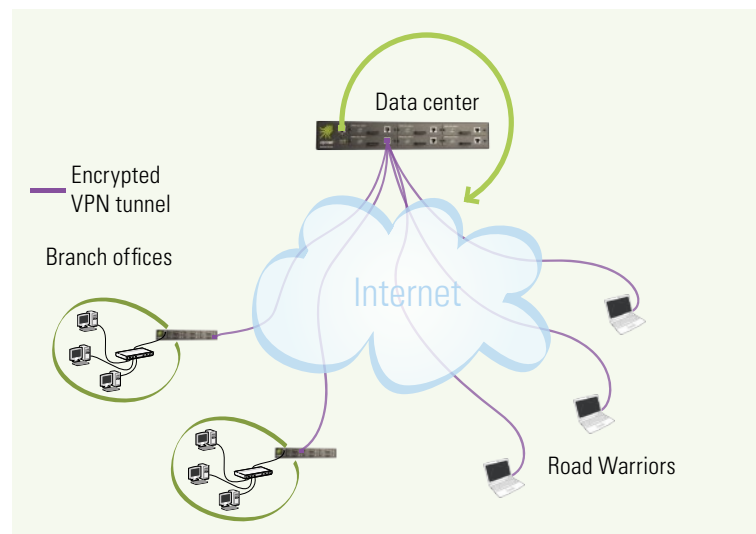
Therefore, a continually growing number of business processes is connected to electronic data exchange between different locations. It is often not apparent at first glance how much a company's success here depends on reliable communication paths – until they fail for the first time and take operations down with them.

Virtual private networks (VPNs) are the answer to the demands of the interconnected business world. They allow consolidating all distributed activities into a single secure network isolated towards the outside. The data is transported across public wide area networks (WANs) – for example, the Internet.

The Viprinet technology, implemented in the Multichannel VPN Router for the first time, demonstrates a unique way to deploy such an Internet-based VPN with extreme reliability at a highly economic cost. Secure and reliable inter-site networking becomes affordable for businesses of all sizes for the first time.

An overview of VPN technologies

MPLS is a technology often used as an alternative to classical leased lines that provide an actual physical connection between two locations. Data traffic between two peers is routed along fixed paths inside a MPLS's line provider. This is mostly a cost saving effort compared to leased lines – many disadvantages known from leased lines remain. First and foremost is the dependency on the network and choice of products of a single provider – the operator of the MPLS net. Furthermore there are not many access technologies available, and they are not sufficiently fail-safe on their own, making additional backup lines necessary. Also, without additional measures

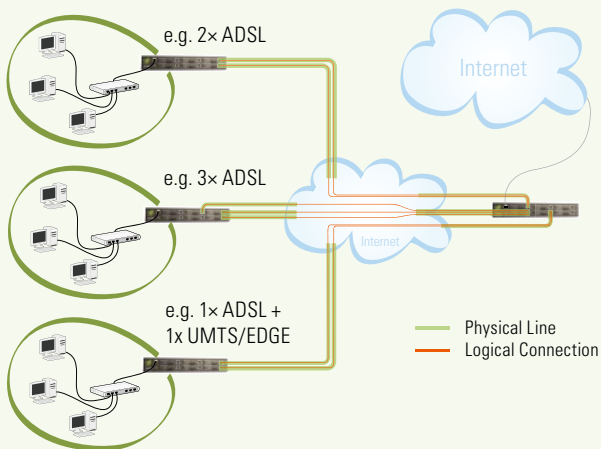


the data transferred using MPLS is unencrypted – paying only lip service to the “P” in VPN. IPSec on the other hand is a VPN standard independent of the line type used. It is a special version of the common Internet protocol (IP). IPSec is pretty widespread nowadays, however the protocol is complex and prone to failure. IPSec alone is not a VPN solution, because it does not define communication paths. This means that once the decision for IPSec has been made, the problem of physically connecting sites remains to be addressed – expensive leased line providers are required to get adequate availability. Therefore high costs and contract durations sneak “through the back door” with IPSec. Another disadvantage: IPSec packets are clearly visible in Internet traffic – in some networks (e.g. UMTS/EDGE) the providers even block IPSec traffic.

Viprinet – the new independence

Business VPN solutions offered by network carriers are bound to the carrier's infrastructure, making them inflexible and not available at every site. Letting the provider operate those dedicated networks is expensive, too.

The consumer market for Internet access technologies paints a vastly different picture: Competing local, regional and national providers offer cheap and fast Internet connections using locally available access technologies (DSL, UMTS/EDGE, ISDN, WLAN, packet radio...). However, these products do not meet the requirements for a robust VPN connection – the reliability of the individual access technologies is insufficient.



This is where Viprinet comes in: Your VPN network's reliability does not depend on the physical line provider anymore. Instead the failure risk gets distributed across several lines that would be unreliable on their own – and thereby radically minimized. By using different access methods downtime gets reduced exponentially with the number of lines, and you achieve a total availability that would be impossible to attain using conventional technology.

Forget about special lines, providers or access technologies suitable for VPN technology. Just use the best locally available access methods for each site, selected according to the site's requirements. Using our Multichannel VPN Router you can freely mix and match Internet access solutions to deploy a secure, private company network. Your VPN always stays cost-effective and flexibly adapts to changing demands.

What makes Viprinet special: Several potentially different Internet access technologies can be combined at a single site. Unused backup lines simply don't exist here: The router bundles all currently available links to connect the site with the VPN. When a single line goes down during operation no connection gets aborted, just the total available bandwidth decreases. This works because the Multichannel VPN Router, as the heart of your VPN, builds up a VPN tunnel over each line using the industry standard SSL (with 256 bit AES encryption) and then bundles these connections into one single tunnel through which your data flows.

The concept "security by obscurity" is frowned upon, and rightfully so – but it does not cause any harm to make data traffic invisible to potential attackers after it has been encrypted using open and proven standards against eavesdropping. This is the case with Viprinet technology, as far as even possible: The data gets distributed across several lines and thereby provider backbones, with separate encryption for each line. By using SSL it is hard to distinguish the traffic from other TCP/IP packets – unlike IPSec. A nightmare for every attacker: encrypted, incomplete, hard-to-detect data.

Network Topologies

A site-to-site network using Viprinet is usually implemented using a star topology. A Multichannel VPN Router working as "VPN node" is equipped with the modems required for the line types present and deployed in each branch. It then uses all available lines to connect to the "VPN hub", a central router located at a data center. When the company headquarters is directly connected to a Internet backbone the VPN hub can be placed there, otherwise it should be put inside a high-availability, high-security colocation site. The VPN hub routes data between the various encrypted tunnels established with the VPN nodes. It also acts as a gateway to the Internet for packets leaving or entering the VPN, making it a ideal place for enforcing a central firewall policy.

Field staff and home offices can easily be integrated into the network using secure authentication with the VPN Client software available for Windows, Linux and Mac OS X.

The Multichannel VPN Router – the heart of your VPN solution

The Multichannel VPN Router with its ability to use up to six local access lines in a bundle is the ideal base for a flexible VPN solution that can always adapt to changing requirements.

A company network requires strategies, goals and solid planning as well. Here you can rely on Viprinet's numerous affiliates. We would love to work with you to ensure optimal support for your VPN project. Contact us!

Fast and fail-safe Internet connectivity

Introduction

In many industry sectors a fast and reliable Internet connection is nowadays a resource critical for day-to-day business. Network usage patterns are as various as the requirements for the access method – voice over IP telephony needs low-latency connections, streaming video and file transfers require large bandwidth, and many business-critical processes demand the highest availability rate achievable with the respective access method.

This multitude of growing and continually changing requirements currently gets a cold reception by a small and inflexible range of products for business Internet connectivity. Cheap consumer solutions like one single ADSL line are rarely sufficient: A common availability rate of 97% per year, equivalent to over 250 hours of yearly downtime, disqualifies them as a viable solution in the business world.

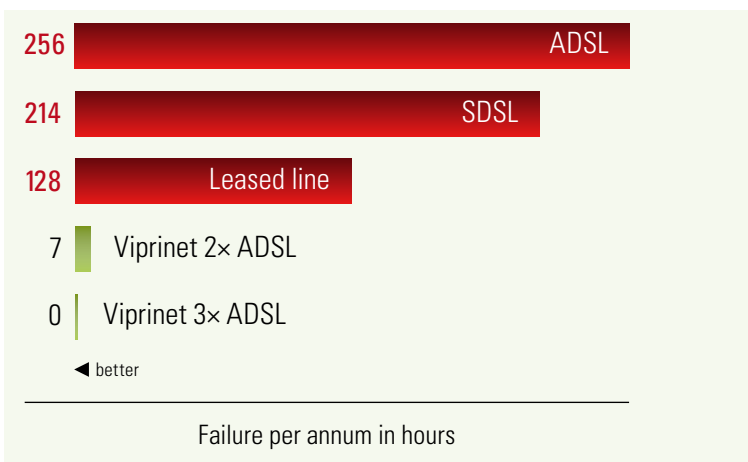
Access products aimed at companies used to be based on dedicated leased lines which could achieve acceptable availability rates in combination with a backup line. The running costs for that solution remain prohibitive, however: Lack of competition leads to prices often more than an order of magnitude above consumer products with comparable bandwidth.

The middle ground is covered by SDSL-based business products with a typical up- and downstream rate of 2 MBit/s. Their uptime availability rate of 98% though is hardly better than ADSL consumer lines in terms of reliability. Usually backup lines are employed here as well, causing additional costs.

But what if an application needs more than 2 MBit/s upstream capacity? Or in addition to that 30 MBit/s downstream is required? What about business critical applications, where every outage leads to unacceptable standstill in operations? Or branch offices without any DSL products available to them?

The solution: Bundling several broadband lines

The Viprinet Multichannel VPN Router enables you to use up to six Internet access lines in a bundled form. The novel bundling technology developed by Viprinet can combine arbitrary access products. All connected lines appear together towards the LAN as one “fat pipe”. Single lines going down only cause a reduction in available bandwidth. By distributing the failure risk across several access providers, a total availability of over 99.99% can easily be achieved.



Using the Multichannel VPN Router even the most demanding requirements for business Internet connectivity can be met. ADSL and SDSL products can be mixed and matched according to up- and downstream bandwidth needs. If downtime needs to be as low as possible, high-availability network connectivity can be achieved by combining different Internet providers and access methods. For example, DSL-based lines can be combined with UMTS connections – even when DSL equipment in the switching center should malfunction, the network stays up via UMTS. At sites where DSL is not available, several UMTS connections can be bundled as an alternative – this is also an ideal broadband access solution where location changes frequently (expositions, broadcast vans).

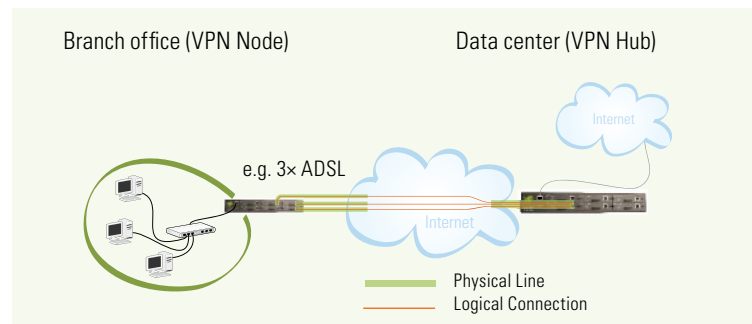
Practical realization

The access lines connected to the Multichannel VPN Router are not directly utilized for data transmissions. Instead an encrypted VPN tunnel to a peer (the so-called “VPN Hub”) located at an Internet backbone is established for each currently available line. These encrypted tunnels are then internally bundled by the router and appear towards the LAN as one single line. The VPN Hub then decrypts and correctly reassembles the data streams and forwards them to their original destination in the Internet.

This technology not only makes it possible for one single download to use all lines simultaneously, the router can also retransmit packets lost due to a failing line using the remaining lines. This way, lines going down do not cause any connection aborts – even 24h disconnects common with ADSL lines cannot be noticed anymore.

IP addresses provided by the physical line providers do not get used in the LAN anymore – they are completely transparent and shielded. Instead an arbitrary number of IP networks can be routed from the VPN Hub to the respective site. This way, many services that need to be publicly available (e.g. mail servers or tele-work software) can be run inside the company network. This also makes the local site independent of provider IP address assignments, so you do not depend on long contract periods and can always use the most economic Internet lines available.

In order for the Multichannel VPN Router bundling technology to provide offices with a flexible, fast and reliable Internet connection, it needs a peer in the form of another Multichannel VPN Router with a reliable and secure connection to an Internet backbone. Companies from e.g. the IT industry that already have space in a data center at their disposal can operate this peer under their own authority. The VPN Hub is simply mounted in a rack alongside existing server hardware.



Another alternative is to rent a peer – a service offered by Viprinet, its affiliates and others. Here the VPN Hub is deployed directly at an Internet backbone in a data center complying with the strictest standards for monitoring and physical security. The customer can still freely choose which lines to use at their site.

Even though the requirement of a peer does pose a certain initial overhead, the advantages prevail in practice. The way is also paved for future network expansions: One single VPN Hub can simultaneously serve many branch offices and field workers, and a fully-fledged VPN spanning across further branches including some offices is only a small step away. Further information on the extended possibilities when using the VPN Router for site interconnection is available in our solution overview “VPN branch interconnection”.

We would love to work with you and our partners to deliver you custom-tailored network connectivity. Contact us!



Viprinet GmbH
Mainzer Str. 43
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
Web www.viprinet.com

Received from your Viprinet partner: