viprinet®

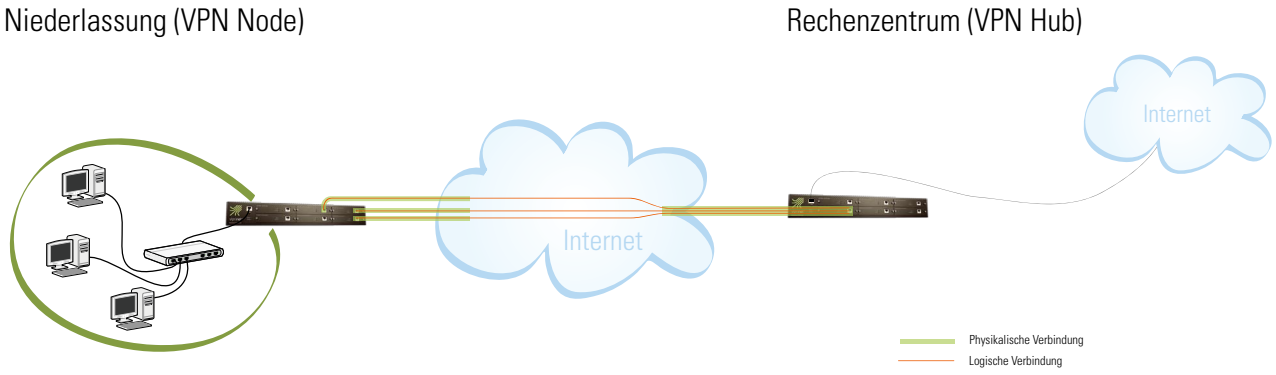
Funktionsweise des Viprinet Multichannel VPN Router™

1. Grundsätzliche Funktionsweise und Vernetzungsstrukturen

Der Multichannel VPN Router verbindet ein lokales Netzwerk über bis zu sechs Breitbandleitungen mit einer VPN-Gegenstelle. Für die verbreitetsten Leitungstypen stehen Modems als Module zur Verfügung, die in das Routergehäuse eingeschoben werden. Derzeit werden Module für ADSL/ADSL2+, Euro-ISDN und Fast Ethernet angeboten. Über das Fast Ethernet Modul lassen sich auch externe Modems (z.B. WLAN, UMTS, SDSL, SHDSL) an das Gerät anbinden. Unterstützt werden hierbei alle Modems, die wahlweise PPPoE oder die Zuweisung einer IP in Richtung Ethernet-Modul per DHCP zulassen.

Der Multichannel VPN Router agiert als Layer 3-Router, er vermittelt also auf IP-Ebene zwischen Netzen an unterschiedlichen Standorten. IP-Datenströme werden dabei über das LAN-Interface aufgenommen, und auf alle aktuell verfügbaren Leitungen/Modemkarten verteilt. Um diese Ströme nach der Übertragung wieder zusammenzusetzen, ist immer eine Viprinet-Gegenstelle erforderlich.

Über jede der physikalischen Internet-Zugangsleitungen wird ein separater, verschlüsselter VPN-Tunnel (SSL-Verfahren mit wählbarerer Verschlüsselungsstufe) zur konfigurierten Gegenstelle über das Internet aufgebaut. Über diese verschlüsselten Tunnel werden dann gebündelt Daten übertragen.



Daraus folgt, dass die verwendete Gegenstelle über alle physikalischen Leitungsprovider gut erreichbar sein sollte. Es bietet sich eine Platzierung der Gegenstelle in einem direkt mit einem Provider-Backbone verbundenen Rechenzentrum oder direkt an einem Austauschknoten eines ISPs an. Alternativ ist der Betrieb der Gegenstelle im Anwendungsfall einer Filialvernetzung in der Firmenzentrale möglich, so diese über eine ausfallsichere und breitbandige Internet-Anbindung verfügen sollte. Ist dies nicht der Fall, oder soll die Zentrale ebenfalls durch einen Viprinet Multichannel VPN Router mit Bündelung angebunden werden, sollte eine Sternstruktur gewählt werden, bei dem die Gegenstelle für alle Filialen und die Zentrale sich wiederum in einem Rechenzentrum an einem Internet-Backbone befindet.

2. Das Gerät

Beim Multichannel VPN Router handelt es sich um ein leistungsfähiges Gerät modularer Bauweise. Das System besteht auf einem 19“ Gehäuse mit 1.5 Höheneinheiten. Es kann als Desktopgerät genutzt werden, über mitgelieferte Winkel ist aber auch eine Montage in einem 19“ Rack problemlos möglich.

Der Router verwendet intern eine mit 1GHz getaktete CPU, die Datenverschlüsselung in Hardware beherrscht. Der Router ist in der Standardausführung mit 256MB RAM ausgestattet, das zum größten Teil zur Paketzwischenspeicherung bei der Kanalbündelung zum Einsatz kommt.

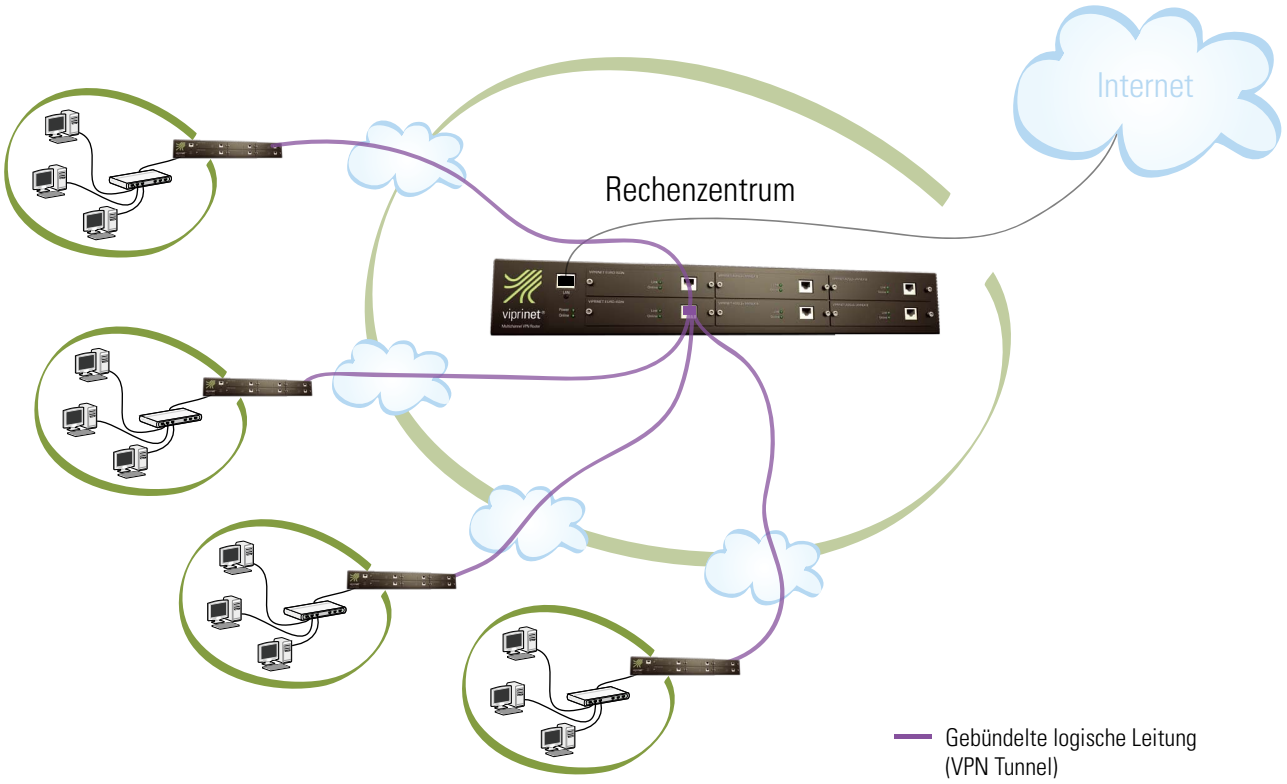
Das Gerät wurde auf Robustheit und Langlebigkeit ausgelegt. Das System ist komplett passiv gekühlt und enthält keine beweglichen Teile. Alle Komponenten sind auf bestmögliche Effizienz ausgelegt. Dadurch sinkt die typische Leistungsaufnahme mit Modul-Vollbestückung auf nur 40 Watt. Das Gerät verfügt über ein robustes internes Netzteil, welches eine Versorgung mit 90-265 VAC, 47-63 Hz unterstützt. Der Anschluss an das Stromnetz erfolgt über eine Kaltgerätebuchse (1).

Über die Fast Ethernet LAN-Buchse (2) wird das Gerät mit dem LAN bzw. einem LAN-Switch verbunden. Die sechs vorhandenen Modul-Einschübe (3) können in beliebiger Kombination und Anzahl mit Viprinet-Modems bestückt werden. An diese Module werden dann direkt die physikalischen Zugangsleitungen (ADSL und ISDN Module) oder externe Modems (Ethernet Modul) angeschlossen (4). Der Minimalausbau des Gerätes ist dabei die Bestückung mit einem Modul, der Maximalausbau sind sechs Module. Eine Aufrüstung kann jederzeit durch den Benutzer selbst vorgenommen werden.

Die Haupt-Statusanzeigen (5) liefern Informationen darüber, ob das Gerät mit Strom versorgt ist und zumindest über eine der physikalischen Leitungen eine Verbindung zur VPN-Gegenstelle besteht (Online-LED). Jedes Modul verfügt zudem über LEDs (6), die den korrekten Anschluss einer Leitung (Link-LED) sowie den Status der VPN-Verbindung über dieser Leitung (Online-LED) anzeigen.

3. Die Gegenstelle (VPN Hub)

Die vom Multichannel VPN Router benötigte Gegenstelle entbündelt die aus den Niederlassungen kommenden Datenströme. Als Gegenstelle dient in der Regel ein weiterer Multichannel VPN Router, der mit einem Fast-Ethernet Modul pro anzubindender Niederlassung bestückt ist. Diese Module werden mit dem Internet-Backbone des Rechenzentrums verbunden. Alle über die von der Filiale über mehrere physikalische Leitungen aufgebauten VPN-Tunnel-Kanäle enden nun auf dem für diese Filiale zuständigen Modul. Die Datenströme werden vom Router wieder zusammengefügt. Liegt das Ziel einer IP-Verbindung in einer anderen Filiale, werden die Daten anschließend über das entsprechende Modul verschlüsselt weiter übertragen. Ist das Ziel der Daten außerhalb des eigenen Gesamtnetzes, werden diese über die LAN-Buchse unverschlüsselt ins Internet ausgegeben. Die LAN-Buchse ist somit wiederum mit dem Internet-Backbone verbunden.



Es ergibt sich, dass für die Ausfallsicherheit und Performance des VPN-Gesamtnetzes dieser sogannte VPN Hub eine zentrale Bedeutung hat. Ihm sollte bei der Planung also besondere Aufmerksamkeit geschenkt werden.

VPN Hub mieten – die bequeme Alternative

Kunden, denen kein geeigneter Standort für einen VPN Hub zur Verfügung steht (wie z.B. Flächen in einem Rechenzentrum), können auf Mietbasis durch die Firma Viprinet in deren Rechenzentrum in Frankfurt am Main einen VPN Hub als zentrale Gegenstelle betreiben lassen.

4. VPN-Clients / Road Warriors

Jeder Multichannel VPN Router ist neben seiner Hauptaufgabe, dem Zusammenschließen von Netzen, in der Lage eine beliebige Anzahl von Einzelverbindungen durch VPN-Clients aufzunehmen. Unter einem VPN-Client versteht man einen einzelnen Rechner, der sich außerhalb aller per VPN verbundenen Netze befindet. Dies kann üblicherweise ein Außendienstmitarbeiter oder Heimarbeitsplatz sein. Über VPN-Clientverbindungen werden solche Einzelarbeitsplätze an den VPN-Verbund angeschlossen. Der VPN-Client bindet sich als virtuelle Netzwerkkarte in das Betriebssystem ein, und verwendet—vergleichbar mit dem Multichannel VPN Router—anschließend dynamisch alle verfügbaren Online-Verbindungen (z.B. UMTS und WLAN). Dies stellt einen erheblichen Fortschritt gegenüber bisherigen VPN-Clientsystemen dar. Der VPN-Client ist als Softwarelösung für die Betriebssysteme Microsoft Windows, Apple MacOS X sowie Linux verfügbar.

5. IP-Routing

Der Multichannel VPN Router arbeitet auf Layer 3 des OSI-Schichtenmodells. Er verknüpft somit IP-Netze an unterschiedlichen Standorten per IP-Routing. Jeder Standort verfügt dabei über ein eigenes Subnetz, in dem der Multichannel VPN Router als Gateway fungiert. Zusätzliche externe VPN-Clients befinden sich ebenfalls jeweils in einem abgetrenntem Subnetz.

Bedingt durch das verwendete Tunnel-Verfahren sind die dynamischen IP-Adressen der verwendeten physikalischen Zugangsleitungen „unsichtbar". Sie finden nur innerhalb des Routers selbst Verwendung. Die zum LANInterface und im LAN selbst verwendeten IP-Adressen sind vollkommen virtualisiert.

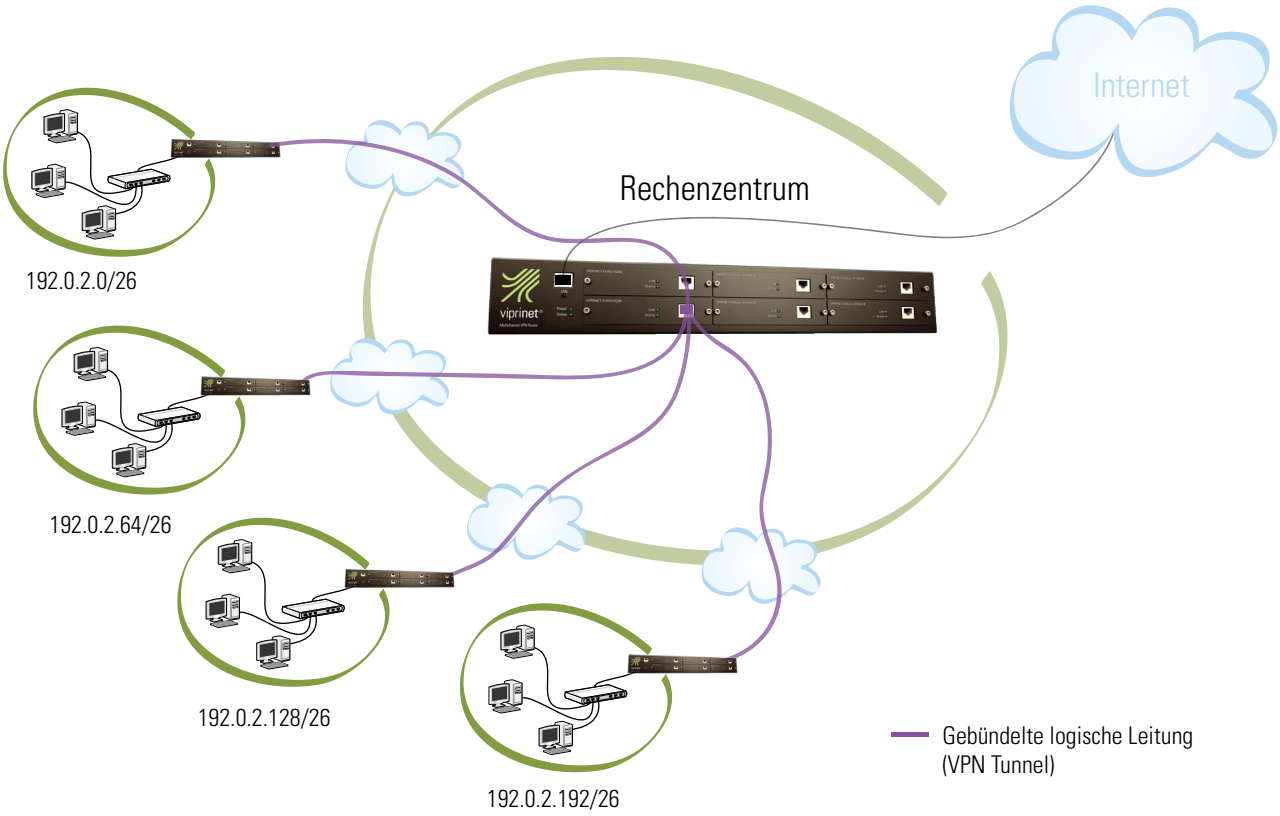
Dieses Verfahren ermöglicht es, beliebige IP-Adressräume für das eigene Netzwerk zu verwenden, ohne Wissen oder Unterstützung der physikalischen Leitungsanbieter. Von der in einem Rechenzentrum befindlichen Gegenstelle (dem VPN Hub) können beliebige dort verfügbare Adressbereiche über die VPN-Verbindung zu den Niederlassungen geroutet werden. In diesen sind somit bei Bedarf von außen erreichbare IP-Adressen in beliebiger Anzahl verfügbar.

Der Viprinet VPN Router beherrscht alternativ auch NAT (Network Adress Translation). In diesem Falle werden in den Niederlassungen private IP-Adressen verwendet. Bei Verbindungen, die über die Gegenstelle das VPN in Richtung Internet verlassen, werden diese dann durch eine öffentliche IP-Adresse ersetzt.

Auch ein Mischbetrieb ist möglich – so lassen sich über einen Multichannel VPN Router mehrere öffentliche wie auch private Netze routen.

Hier eine Beispielkonfiguration mit öffentlichen IP-Adressen, ausgehend von einem öffentlichen Gesamtnetz 192.0.2.0/24 („Class C“ Netz), welches in vier Subnetze aufgeteilt wurde:

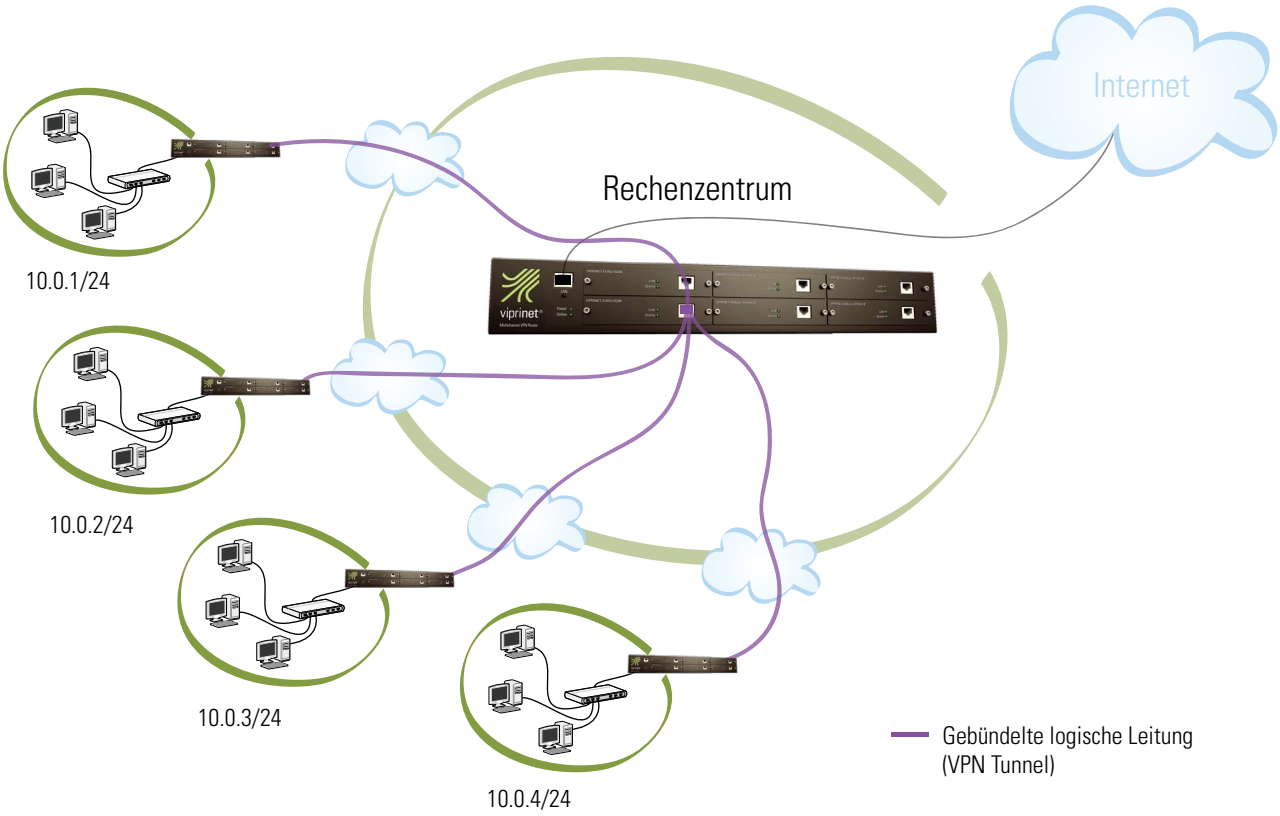
Niederlassung	Subnetz	Gateway (IP des LAN-Ports des Routers)
A	192.0.2.0/26	192.0.2.1
B	192.0.2.64/26	192.0.2.65
C	192.0.2.128/26	192.0.2.129
D	192.0.2.192/26	192.0.2.193



Alle vier Netze erreichen sich jeweils über die sich im Internet-Backbone befindliche Gegenstelle („VPN Hub“). Bei Paketen aus dem Netz A mit Ziel Netz B oder umgekehrt werden diese direkt im Router von VPN Tunnel A auf VPN Tunnel B weitergeleitet. Pakete ins Internet verwenden die öffentliche IPAdresse aus diesem Netz als Quelladresse. Alle vier Netze sind von außen aus dem Internet erreichbar.

Hier nun noch eine Beispielkonfiguration mit privaten IP-Adressen, ausgehend von einem Gesamtnetz 10.0/16, aus welchem vier (von insgesamt 256 möglichen) Subnetze der Größe /24 („Class C“ Netz) verwendet werden:

Niederlassung	Subnetz	Gateway (IP des LAN-Ports des Routers)
A	10.0.1.0/24	10.0.0.1
B	10.0.2.0/24	10.0.2.1
C	10.0.3.0/24	10.0.3.1
D	10.0.4.0/24	10.0.4.1



Alle vier Netze erreichen sich wiederum jeweils über die sich im Internet-Backbone befindliche Gegenstelle – da die Pakete durch einen VPN Tunnel übertragen werden, ist es kein Problem dass die privaten IP-Adressen im Internet nicht gerouted werden können. Bei Paketen aus dem Netz A mit Ziel Netz B oder umgekehrt werden diese direkt im Router von VPN Tunnel A auf VPN Tunnel B weitergeleitet. Pakete ins Internet erhalten per NAT an der Gegenstelle eine neue, öffentliche Quelladresse.

6. Die VPN-Technologie

Über jede der angeschlossenen physikalischen Leitungen wird durch den Backbone des jeweiligen ISPs eine unabhängige Tunnel-Verbindung mit der Viprinet-Gegenstelle aufgebaut. Diese Tunnel-Verbindungen werden dann vom Multichannel VPN Router intern wie eine einzige virtuelle Standleitung behandelt. Die Tunnel-Verbindungen auf den einzelnen Leitungen verwenden das bewährte und geprüfte SSL/TLS Verfahren zur Authentifzierung und Verschlüsselung. Als Verschlüsselungsalgorithmus kommt hierbei die hochsichere AES-Verschlüsselung mit 256 Bit zum Einsatz. Zusätzliche Sicherheit entsteht dadurch, dass durch das Bündelungsverfahren des Routers die Daten auf unterschiedliche VPN-Tunnel verteilt werden. Um die Datenströme zu entschlüsseln ist es erforderlich, die Verschlüsselung jedes einzelnen VPN-Tunnels auf allen physikalischen Leitungen zu brechen.

Das Bündelungsverfahren

Der Multichannel VPN Router verteilt IP-Datenströme (z.B. TCP-Verbindungen) auf die über die physikalischen Leitungen verbundenen VPN-Tunnel. Statt verbreiteten Round-Robin-Lösungen kommt hier ein neuartiges Bündelungsverfahren zum Einsatz.

Dieses bietet die folgenden Eigenschaften:

- Existieren weniger gleichzeitige Datenströme als Leitungen vorhanden sind, verwenden auch Einzelverbindungen zugleich mehrere physikalische Leitungen. Eine einzelne TCP-Verbindung kann also die Bandbreite aller existierenden Leitungen gebündelt vollständig ausnutzen

- Bricht eine der physikalischen Leitungen im Betrieb zusammen, werden keine bestehenden Verbindungen abgebrochen. Bei nicht-gebündelten Verbindungen werden diese auf eine andere, funktionsbereite Leitung übertragen. Bei gebündelten Verbindungen, die sich über mehrere Leitungen spannen, werden die durch den Leitungsausfall verlorengegangenen Datenpakete vollautomatisch über die übrigen noch intakten Leitungen nachgesendet. Dies geschieht routerintern vollkommen transparent für alle Anwendungen.

Quality of Service und Bandbreitenmanagement

Die durch die physikalischen Leitungen in ihrer Summe bereitgestellte Bandbreite wird innerhalb des Multichannel VPN Router zunächst grundsätzlich als Einheit betrachtet. Aus diesen Kapazitäten lassen sich über das integrierte Bandbreitenmanagement Anteile an einzelne Abteilungen oder Dienste einer Niederlassung zuweisen.

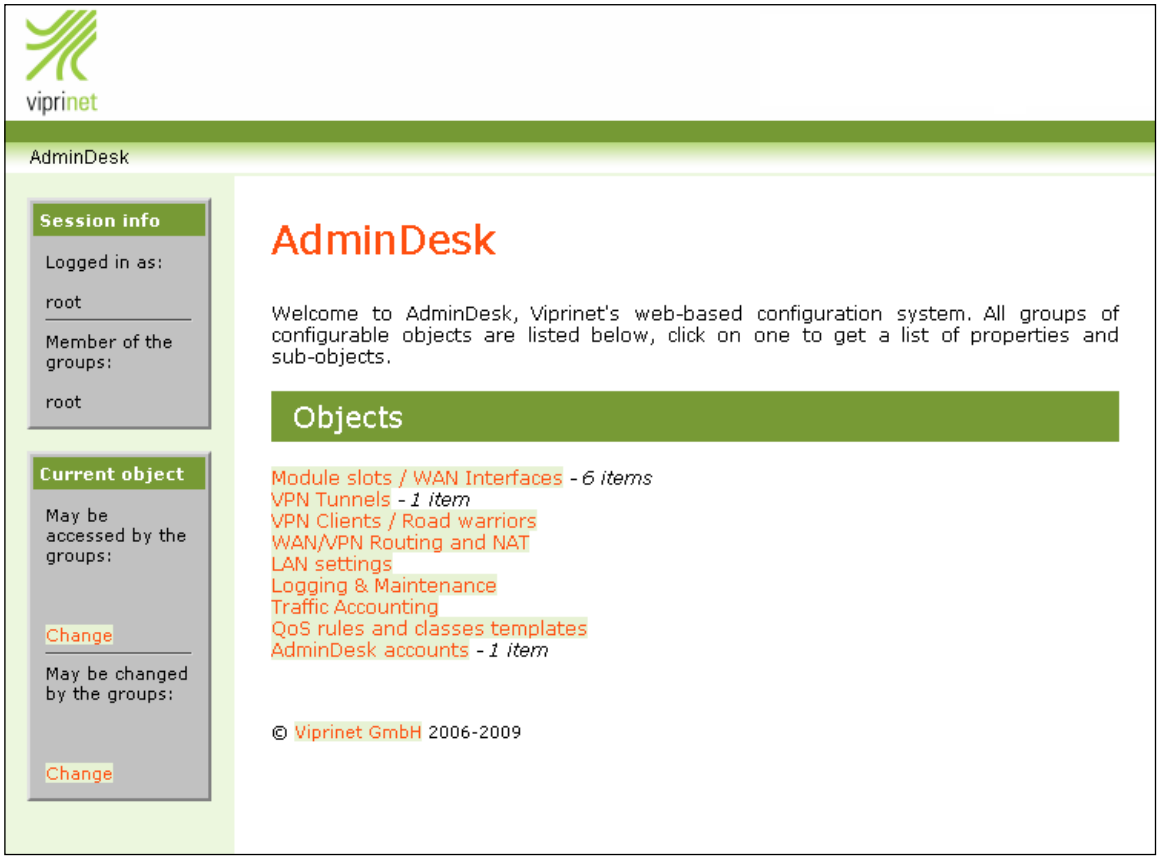
So ist es beispielsweise möglich, bestimmten Diensttypen eine garantierte Mindestbandbreite zuzuweisen, und andere hingegen zu drosseln. Entsprechende Regeln lassen sich auf Basis zahlreicher Datenquellen wie IP-Netzbereich, Portnummern oder Paketeigenschaften festlegen.

Der Multichannel VPN Router stützt sich hierbei auf zweigeteiltes Konzept: Es gibt Trafficklassen, die festlegen wie eine bestimmte Art von Datenströmen behandelt werden soll – so ist es z.B. möglich, für latenzsensitiven Traffic wie Voice-Over-IP-Telefonate den Router automatisch die Leitung mit der aktuell niedrigsten Latenz wählen zu lassen, während normale HTTP-Downloads auf alle Leitungen verteilt werden. Über ein integriertes Regelsystem wird dann festgelegt, nach welchen Kriterien Datenströme in die jeweiligen Trafficklassen sortiert werden.

Diese intuitive Ausführung des Bandbreitenmanagements und QoS ermöglicht eine bequeme Abbildung vorhandener realer Geschäftsprozesse auf die Netzwerkinfrastruktur.

7. Administration, Management und Monitoring

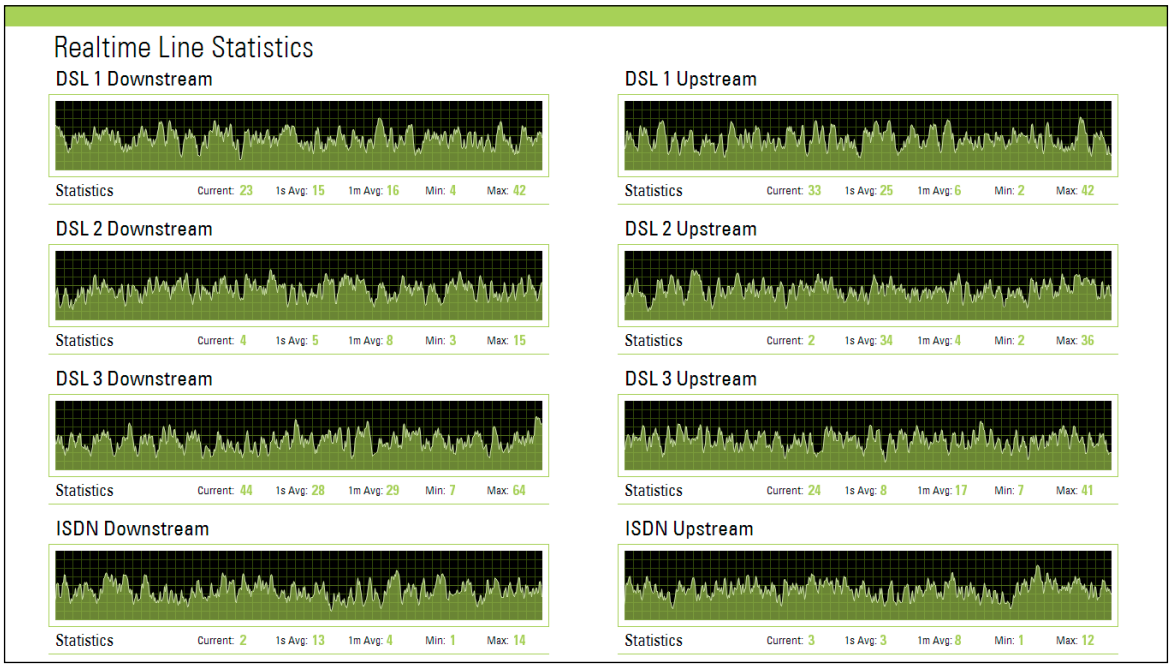
Die Konfiguration des Multichannel VPN Router erfolgt per einfach zu bedienendem und umfassenden Webinterface. Das Administrationssystem ist dabei mandantenfähig – Teilbereiche der Konfigurationsoptionen lassen sich also für Unter-Administratorengruppen freigeben, als nur-lesen markieren und ähnliches. Damit wird es möglich, Teile der Konfiguration (z.B. Bandbreitenmanagement / QoS) den Abteilungen oder Kunden zu überlassen, während die Grundkonfiguration unter der Kontrolle einer zentralen Administration (oder des ISPs) bleibt.



Zur Integration in bestehende Monitoring- und Management-Setups in größeren Netzen unterstützt der Multichannel VPN Router gängige Management-Protokolle wie Syslog und SNMP (in Vorbereitung).

Zur visuellen Auswertung der aktuell vorhandenen Datenströme sowie der Nutzungsquote der verfügbaren Leitungen existiert ein komfortables Monitoringtool, was diese Daten in Echtzeit visuell ansprechend aufbereitet — performanceprobleme lassen sich über diesen Weg ideal diagnostizieren.

Schließlich bietet das System auch umfangreiche Möglichkeiten zum Accounting und zur Abrechnung. So ist der Multichannel VPN Router z.B. in der Lage, Statistiken über das Nutzungsverhalten pro Dienst oder Netzbereich direkt auf einen SQL-Server im Netz zu loggen, was eine bequeme Weiterverarbeitung dieser Daten ermöglicht.



8. Exzellenter Support

Auch dies ist ein wichtiger Punkt – bei Viprinet erhalten Sie umfassenden Kundensupport von qualifizierten Mitarbeitern direkt aus Deutschland. Sollten Sie noch weitere Fragen zu den Möglichkeiten unseres Multichannel VPN Routers und der dazugehörigen Technologie haben, zögern Sie bitte nicht sich an unseren Vertrieb zu wenden. Wir helfen gerne, auch Ihre Unternehmensanbindung zu optimieren.

Kontaktieren Sie uns

Viprinet GmbH
Mainzer Str. 43
55411 Bingen am Rhein

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