Die Technologie von ViPNet

Allgemeine Informationen

infotecs

Ziel und Zweck

Dieses Handbuch beschreibt die Installation und Konfiguration von ViPNet Produkten. Für die neuesten Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere Release Notes lesen – insbesondere, wenn Sie ein Software-Upgrade zu einem höheren Release-Stand durchführen. Die aktuellsten Release Notes sind immer zu finden unter http://www.infotecs.de

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in Ihrem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Der Hersteller haftet nur im Umfang seiner Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und Release Notes für ViPNet Produkte finden Sie unter http://www.infotecs.de. Der Hersteller übernimmt keine Verantwortung für Datenverlust und Schäden, die durch den unsachgemäßen Betrieb des Produkts entstanden sind.

Version: 00121-04 90 05 DEU

Wie Sie Infotecs erreichen

Infotecs GmbH

Oberwallstr. 24

10117 Berlin

Deutschland

Tel.: +49 (0) 30 206 43 66 0

Fax: +49 (0) 30 206 43 66 66

WWW: http://www.infotecs.de

E-Mail: support@infotecs.de

Inhalt

Über dieses Dokument

In diesem Dokument werden erste einführende Informationen über die Technologie von ViPNet präsentiert, ihre Anwendungsgrundlagen und -prinzipien erklärt sowie ihre primären Vorteile hervorgehoben.

Verwendete Konventionen

Weiter unten sind Konventionen aufgeführt, die im gegebenen Dokument zur Kennzeichnung wichtiger Informationen verwendet werden.

Tabelle 1. Symbole, die für Anmerkungen benutzt werden

Symbol	Beschreibung
	**Achtung!** Dieses Symbol weist auf einen Vorgang hin, der für die Daten- oder Systemsicherheit wichtig ist.
	**Hinweis.** Dieses Symbol weist auf einen Vorgang hin, der es Ihnen ermöglicht, Ihre Arbeit mit dem Programm zu optimieren.
	**Tipp.** Dieses Symbol weist auf zusätzliche Informationen hin.

Tabelle 2. Notationen, die zur Kennzeichnung von Informationen im Text verwendet werden

Notation	Beschreibung
Name	Namen von Elementen der Benutzeroberfläche. Beispiele: Fensterüberschriften, Feldnamen, Schaltflächen oder Tasten.
Taste+Taste	Tastenkombinationen. Zum Betätigen von Tastenkombinationen sollte zunächst die erste Taste gedrückt und dann, ohne die erste Taste zu lösen, die zweite Taste gedrückt werden.
Menü > **Untermenü** > **Befehl**	Hierarchische Abfolge von Elementen. Beispiele: Menüeinträge oder Bereiche der Navigationsleiste.
`Code`	Dateinamen, Pfade, Fragmente von Textdateien und Codeabschnitten oder Befehle, die aus der Befehlszeile ausgeführt werden.

Die Technologie von ViPNet

Die Technologie von ViPNet ist darauf ausgerichtet, abgesicherte virtuelle private Netzwerke (Virtual Private Network, VPN) oberhalb bestehender globaler und lokaler Netze einzurichten. Die ViPNet Technologie gewährleistet eine transparente Interaktion der geschützten Computer untereinander, unabhängig von ihrem Standort und der Art der Anbindung an das Netzwerk oder der IP-Adresse. Die Kommunikation kann auf Basis des Schemas „client-to-client“, „client-to-site“ oder „site-to-site“ (VPN-Tunnel) eingerichtet werden.

Der grundsätzliche Unterschied der ViPNet Technologie zur Mehrzahl anderer moderner VPN-Systeme, die hauptsächlich dazu dienen, abgesicherte Verbindungen zwischen lokalen Netzwerken sowie Remote-Zugriffsmöglichkeiten auf Netzwerkobjekte innerhalb dieser Netze bereitzustellen, besteht in der Verfügbarkeit spezieller Protokolle für das dynamische Routing des VPN-Traffics. Diese Protokolle ermöglichen es, einen abgesicherten Datenaustausch nicht nur mit dem VPN-Gateway selbst, der an der

lokalen Netzwerkgrenze installiert ist, sondern auch unmittelbar zwischen den Endempfängern der Daten, auch unter Verwendung eines VPN-Gateways automatisiert sicherzustellen.

Eine wichtige Besonderheit der ViPNet Technologie besteht in der Verwendung der symmetrischen Schlüsselstruktur bei VPN. Als Folge davon müssen keine regelmäßigen Sitzungen zur Authentifizierung der Netzwerkknoten mehr aufgebaut sowie keine Vorgänge zur Herausarbeitung von Schlüsseln durchgeführt werden. Diese Prozesse sind für Systeme mit Verteilung öffentlicher Schlüssel wichtig, beeinträchtigen jedoch den Einsatz von VPN in lokalen Netzen und verringern die Fehlertoleranz von Verbindungssitzungen wegen der Wahrscheinlichkeit einer Störung im Zuge der Synchronisation. Eine komplexe Public-Key-Infrastruktur, die für den sicheren Einsatz asymmetrischer Schlüssel erforderlich ist, muss nicht mehr aufgebaut werden. Im Unterschied zur Mehrzahl der modernen VPN-Systeme, in welchen die Verwendung symmetrischer Schlüssel ebenfalls möglich ist, steht hier ein automatisiertes Administrationssystem für die symmetrischen Schlüssel zur Verfügung.

Die Einrichtung eines abgesicherten Netzwerks erfolgt durch Installation folgender Software auf den Computern und den mobilen Clients:

- ViPNet Network Manager: dient der Steuerung des ViPNet Netzwerks (Anlegen der ViPNet Netzwerkstruktur, Definition von Verbindungstypen der Netzwerkknoten, Erstellung und Aktualisierung von Schlüsselinformationen) und der Organisation von Interaktionen mit anderen ViPNet Netzwerken.
- ViPNet Client: dient der Sicherstellung des Netzwerkschutzes sowie der Anbindung des Rechners, des mobilen Endgeräts oder anderer Knotentypen an das VPN-Netz unabhängig vom Standort ihres Anschlusses an die Netzwerkinfrastruktur. ViPNet Client enthält außerdem eine VPN-integrierte, persönliche Netzwerk-Firewall, die für den Schutz des Knotens sowohl bei offenen Verbindungen als auch innerhalb von VPN-Verbindungen sorgt. Nachfolgend wird ein Computer mit installierter ViPNet Client Software als Client bezeichnet.
- ViPNet Coordinator: erfüllt die Funktionen eines VPN-Gateways bei Anbindung offener Rechner und anderer Netzwerkgeräte an das VPN-Netzwerk, organisiert die Interaktion der Clients des ViPNet Netzwerks untereinander und mit Objekten, die vom ViPNet Coordinator geschützt werden. ViPNet Coordinator enthält ebenfalls eine VPN-integrierte Firewall, die für den Schutz von offenen Objekten, die sich hinter der Firewall befinden, sowohl bei offenen Verbindungen dieser Objekte zu externen Ressourcen als auch innerhalb der vom ViPNet Coordinator aufgebauten VPN-Verbindungen sorgt. Nachfolgend wird ein Computer mit installierter ViPNet Coordinator Software als Coordinator bezeichnet. Der Coordinator wird für gewöhnlich an der Grenze des lokalen Netzwerks oder eines Netzwerksegments installiert.

Ein Coordinator kann die folgenden Funktionen übernehmen:

- **IP-Adressenserver**: der Coordinator stellt den Datenaustausch zwischen den geschützten Netzwerkknoten (Clients und anderen Coordinatoren), die sich innerhalb eines Netzwerks oder in unterschiedlichen ViPNet Netzwerken befinden, automatisiert sicher. Dies ist dadurch möglich, da dazu ein spezielles Protokoll für das dynamische Routing des VPN-Traffics verwendet wird, das zur Verbesserung der Netzwerkkonvergenz beiträgt. Dieses Protokoll gewährleistet das optimale Routing des VPN-Traffics zwischen den Netzwerkknoten in einem ViPNet Netzwerk im Hinblick auf den Verbindungstyp, der für die betroffenen Knoten ausgewählt wurde.
- **VPN-Router**: der Coordinator routet den VPN-Traffic zwischen den VPN-Knoten. Das Routing wird anhand der Netzwerkknoten-Bezeichner durchgeführt, die sich im unverschlüsselten Teil des VPN-

Pakets befinden, der mit Fälschungsschutz versehen ist. Das Routing wird auch anhand von Daten, die beim dynamischen Routing des VPN-Traffics mit Hilfe des speziellen Protokolls gesammelt wurden, durchgeführt. Zur gleichen Zeit wird für den VPN-Traffic die Adressenübersetzung ausgeführt. Alle vom Coordinator empfangenen VPN-Pakete werden unter Verwendung der Coordinator-IP-Adresse an andere Knoten weitergeleitet.

- **VPN-Gateway**: Standardfunktion beim klassischen VPN. Verbindungskanäle (Tunnels) werden geschützt, indem der Traffic zwischen offenen Netzwerkknoten (die sich hinter dem Coordinator befinden) und anderen VPN-Gateways, mobilen Clients und Remoteclients verschlüsselt wird. Diese abgesicherten Verbindungskanäle werden Tunnel genannt. In ViPNet Coordinator ist das VPN-Gateway mit einer Firewall integriert, die geschützte und offene Verbindungen zu Knoten, die von diesem Coordinator getunnelt werden, sowie zum Coordinator selbst kontrolliert. Andere VPN-Gateways (mit möglicher intergrierter Firewall) filtern lediglich den unverschlüsselten Traffic. Im Gegensatz dazu filtert ViPNet Coordinator auch den Traffic einer verschlüsselten Verbindung. Die Filterung des Traffics während einer abgesicherten Verbindung zwischen getunnelten Knoten und dem Coordinator selbst wird anhand der IP-Adressen und Bezeichner der geschützten Knoten durchgeführt.
- **Kommunikationsserver**: der Coordinator sorgt für eine ordnungsgemäße Zustellung von Dienstmeldungen und Aktualisierungen der Adresslisten und Schlüssel vom ViPNet Network Manager an ViPNet Knoten.

  Pakete mit Anwendungs- und Dienstdaten werden mit Hilfe des ViPNet MFTP-Moduls geroutet (s. Transportmodul (MFTP) auf S. 27), das in der Anwendungsschicht arbeitet. Das MFTP-Modul empfängt Transportdateien vom Coordinator und von anderen ViPNet Knoten und leitet diese zum Zielknoten weiter.

  Das Routing der Daten von einem Coordinator zu einem anderen wird über logische Verbindungskanäle durchgeführt, die zwischen den beiden Coordinatoren aufgebaut werden, verwirklicht. Logische Kanäle können nach beliebigen Mustern definiert werden. Wenn es mehrere Routen gibt, wird für die Weiterleitung der Daten der kürzeste Weg ausgewählt. Für die Übermittlung der Daten von einem Netzwerk in ein anderes werden in beiden Netzwerken Gateway-Coordinatoren verwendet. Diese Coordinatoren sind dazu bestimmt, die Interaktion der Netzwerke untereinander sicherzustellen.
- **Firewall**: der Coordinator sorgt für die Filterung offener Transit- sowie lokaler Netzwerkverbindungen anhand von IP-Adresse, Protokoll, Port, Verbindungsrichtung und anderen Parametern in Übereinstimmung mit vordefinierten Regeln durchführt. Zur gleichen Zeit führt der Coordinator die Umsetzung von IP-Adressen (NAT) für den offenen Traffic, der den Coordinator passiert, durch.

  Die Funktion zur Umsetzung von IP-Adressen für den offenen Datenverkehr ermöglicht es, Regeln für statische und dynamische NAT einzustellen. Dadurch werden zwei wichtige Aufgaben gelöst:

  - Verbindung des lokalen Netzwerks zu öffentlichen Objekten im Internet, wenn die Anzahl der Knoten im lokalen Netzwerk die Anzahl der vom Provider bereitgestellten öffentlichen IP-Adressen überschreitet.
  - Zugang zu öffentlichen Servern im lokalen Netzwerk aus dem Internet.

  Daneben ermöglicht diese Funktionalität die Lösung folgender zusätzlicher Aufgaben:

- Sicherstellung des Zugangs geschützter Remoteknoten zu Knoten, die vom betroffenen Coordinator getunnelt werden, unter Verwendung der internen IP-Adresse des Coordinators. Dadurch wird die Routingkonfiguration innerhalb des lokalen Netzwerks vereinfacht.
- Sicherstellung des Zugangs aller geschützten VPN-Knoten, die mit dem betroffenen Coordinator verbunden sind, zu öffentlichen Objekten im Internet unter Verwendung der externen IP-Adresse des Coordinators. Um dies zu ermöglichen, sollte die Tunnelung einiger oder aller Internetadressen (Internet-Tunnelung) konfiguriert werden. Diese Funktionalität kann extrem nützlich sein, wenn ein zentralisierter, abgesicherter Zugang zum Internet für alle geschützten Knoten unabhängig von ihrem Standort organisiert werden soll. Das Netzwerk des lokalen Internetanbieters wird dabei als Transportumgebung für Verbindungen zum Coordinator genutzt, der im Firmennetzwerk installiert ist und den Zugang geschützter Knoten zum Internet gewährleistet.

Es stehen sowohl Windows- als auch Linux-basierte Coordinatoren zur Verfügung. Zusätzlich gibt es die Softwarelösung ViPNet Coordinator HW/VA, die als eingebautes Betriebssystem auf unterschiedlichen Netzwerkgeräten wie zum Beispiel MiniPCs oder Industrie-PCs benutzt werden kann. Für den Aufbau einer hochverfügbaren Lösung auf Basis von ViPNet Coordinator für Windows kann die Software ViPNet Cluster verwendet werden. Für den Aufbau einer hochverfügbaren Lösung auf Basis von ViPNet Coordinator Linux steht das Failover-System ViPNet Failover zur Verfügung.

Grundlegende Eigenschaften

Die ViPNet Technologie verfügt über folgende grundlegende Eigenschaften:

- **Vielseitiges System zur Gewährleistung der Informationssicherheit**
  - Mehrschichtiger Schutz vor Netzwerkattacken sowohl für offene als auch für abgesicherte Verbindungen.
  - Vertraulichkeit, Integrität und Verfügbarkeit der Informationsressourcen bei Benutzung beliebiger Verbindungskanäle.
  - Zentralisierte Verwaltung der Datenschutzmaßnahmen.
- **Umfassende Mechanismen zur Gewährleistung der Netzwerksicherheit**
  - Es besteht die Möglichkeit, vom ViPNet Knoten und von Objekten, die von diesem Knoten getunnelt werden, auf andere ViPNet Knoten und entsprechende getunnelte Objekte zuzugreifen. Der Zugriff erfolgt über eindeutige virtuelle IP-Adressen, die auf jedem ViPNet Knoten automatisch festgesetzt werden.
  - Vollständige Verhüllung der Struktur des geschützten Netzwerks und der übermittelten Daten. Interne IP-Adressen der geschützten Knoten werden zusammen mit dem Rumpf des Originalpakets im verschlüsselten Teil des VPN-Pakets übertragen.
  - Kernel-Level-Treiber für den Schutz von Anwendungen und Betriebssystem (s. Der Kern der ViPNet Technologie: ein Kernel-Level-Treiber auf S. 9).
- **Transparentes Arbeiten in modernen multiservicefähigen Kommunikationsnetzwerken**

- Unterstützung aller gängigen Kommunikationstechnologien: xDSL, Ethernet, WiFi, LTE, GPRS/EDGE/3G und andere.
- Vollständige Kompatibilität zum Protokoll TCP/IP.
- Transparentes Arbeiten unter Verwendung von NAT/PAT sowohl im Client- als auch im Server-Modus, unabhängig vom benutzten NAT/PAT-Typ. Der geschützte Traffic wird in diesem Fall in das gewöhnliche UDP-Protokoll verpackt. Der Port und die Zugangsadresse des Absenderknotens werden automatisch auf allen anderen Knoten registriert oder können (um die Anfälligkeit für Attacken zu senken) fix festgesetzt werden, indem die Parameter im verschlüsselten Systemdatenverkehr des Protokolls für das dynamische Routing von VPN-Paketen mit übertragen werden. Die automatische Unterstützung von DHCP, DNS und anderen Diensten wird auch unter den Bedingungen einer unabhängigen Vergabe virtueller IP-Adressen auf jedem Knoten gewährleistet.
- Operative Verarbeitung des Multimedia-Datenverkehrs, der Video- und IP-Telefoniedaten durch unterschiedliche Netzprotokolle (SIP, SCCP, H323 und andere).

- **Uneingeschränkte Skalierbarkeit und Zuverlässigkeit**
  - Zehntausende von Netzwerkknoten in einem geschützten Netzwerk.
  - Möglichkeit zur willkürlichen Verbindung von Knoten aus unterschiedlichen geschützten ViPNet Netzen.
  - Konfigurationen von Serverprodukten mit Hot-Backup- und Clustering-Modus sind erhältlich.
  - Automatische Suche nach verfügbaren Zugangsadressen zu anderen Knoten, Unterstützung von Metriken bei Existenz mehrerer Zugangsadressen zum Coordinator, Unterstützung der Technologie des dynamischen DNS beim Fehlen einer festen IP-Adresse des Coordinators.
  - Automatisches Wiederherstellen von geschützten Verbindungen bei Unterbrechungen sowie automatischer Aufbau einer geschützten Verbindung beim Starten des Betriebssystems (zum Beispiel nach einem planmäßigen oder außerordentlichen Neustart des Netzwerkknotens).
- **Fortgeschrittene Anwendungsdienste**
  - Sicherer Mailclient mit eingebautem Mechanismus der digitalen Signatur.
  - Sicherer Chat- und Konferenzdienst, Dateiaustauschdienst, Benachrichtigungsdienst über die Erreichbarkeit von Knoten.
  - Unterstützung von Standardschnittstellen für die mögliche Einbindung in die Softwarelösungen des Kunden.
- **Übereinstimmung mit den Zertifizierungsanforderungen von TÜV Rheinland Group**

- Regelmäßige Zertifizierung der Produkte gemäß ihrer Übereinstimmung mit den Anforderungen der Firma TÜV Rheinland Group an die Schutzmaßnahmen für vertrauliche Daten (inklusive personenbezogener Daten).

Der Kern der ViPNet Technologie: ein Kernel-Level-Treiber

Den Kern der ViPNet Software bildet der sogenannte ViPNet Treiber, zu dessen primären Funktionen die Filterung und die Ver-/Entschlüsselung der ein- und ausgehenden IP-Pakete gehört.

Die Position des ViPNet Treibers im OSI-Modell

Der ViPNet Treiber ist zwischen der Sicherungs- und der Vermittlungsschicht des OSI-Modells aktiv und ermöglicht die Verarbeitung der IP-Pakete noch bevor sie vom übergeordneten TCP/IP-Protokollstack verarbeitet und an die Anwendungsschicht übergeben werden. Auf diese Weise schützt der ViPNet Treiber den IP-Traffic aller Anwendungen, ohne dass die Benutzer in ihrer Arbeit beeinträchtigt werden.

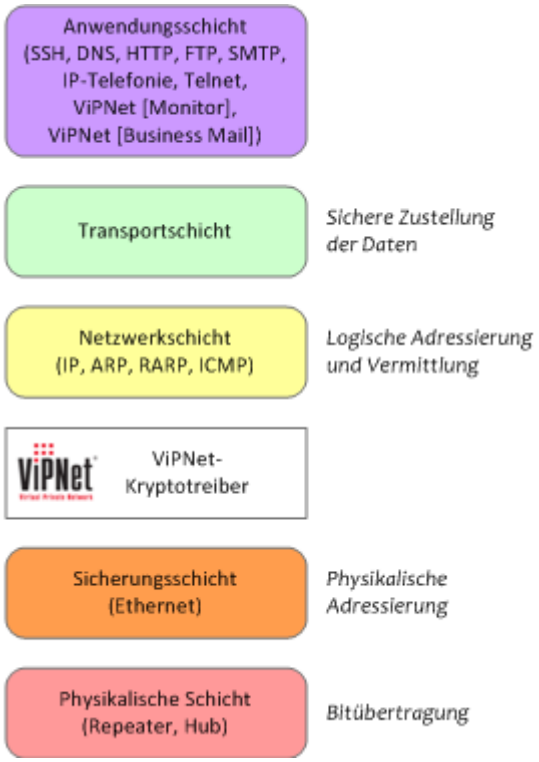

Abbildung 1. ViPNet-Treiber im OSI Modell

Dank dieser Vorgehensweise beeinträchtigt die Einbindung des Treibers nicht die Arbeit anderer Anwendungen und die Einführung der ViPNet Technologie erfordert keine Änderungen an den bestehenden Geschäftsprozessen.

Hinweis. Das oben aufgeführten OSI-Modell wurde folgenderweise vereinfacht:

- Die Transport- und die Sitzungsschicht wurden als Transportschicht zusammengefasst.
- Die Anwendungs- und die Darstellungsschicht wurden als Anwendungsschicht zusammengefasst.

Die nachfolgende Abbildung veranschaulicht die Funktionsweise des ViPNet Treibers bei der Verarbeitung einer Anfrage zum Anzeigen einer Webseite. Die Webseite befindet sich auf einem Web-Server, der auf Computer B läuft.

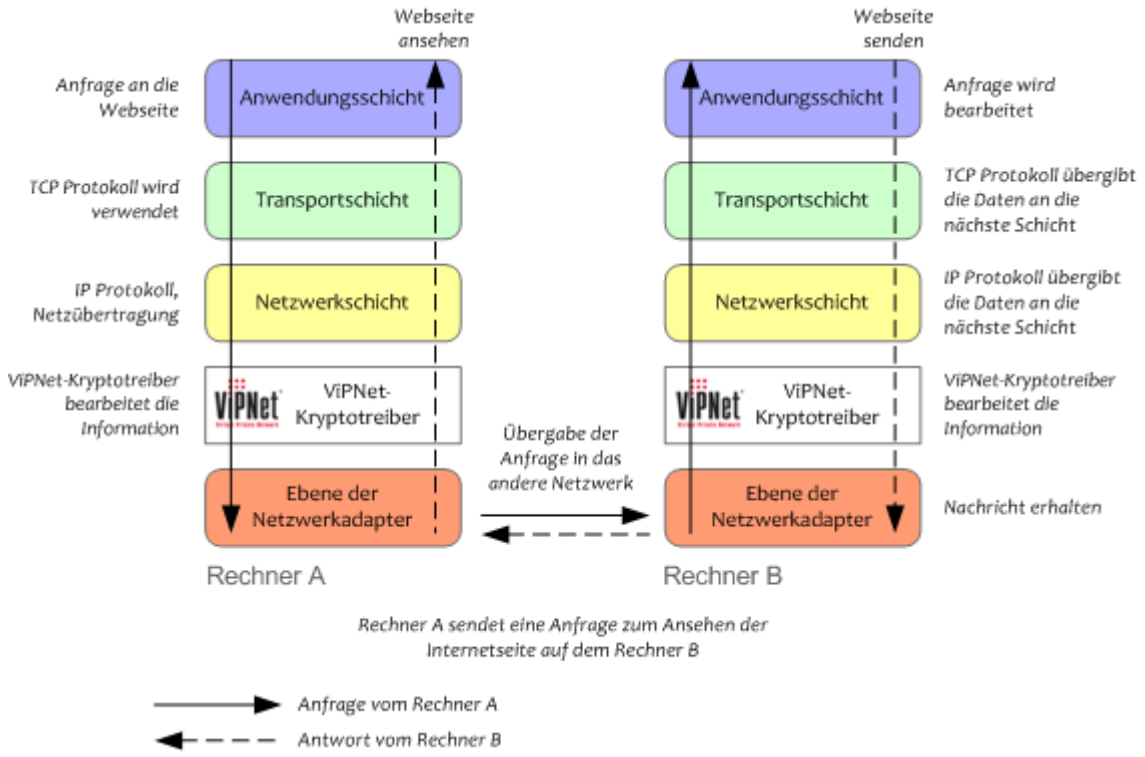

Abbildung 2. Funktionsweise eines TCP/IP-Netzwerks mit ViPNet-Schutz

Netzwerkknoten A sendet an Netzwerkknoten B eine HTTP-Anfrage. Die Anfrage wird an untergeordnete Schichten des TCP/IP-Stacks weitergeleitet. In jeder Schicht werden der Anfrage weitere Dienstinformationen hinzugefügt. Wenn das IP-Paket den ViPNet Treiber auf Computer A erreicht, führt der Treiber die folgenden Aktionen durch:

- wandelt, wenn nötig, die virtuelle Zieladresse in die reelle IP-Adresse des Empfängerknotens um,
- fügt dem Paket eindeutige Kennungen des Quell- und des Zielknotens sowie die Sendezeit hinzu,
- erzeugt einen Message Authentication Code,
- verschlüsselt das Originalpaket und einen Teil der Dienstdaten (ausgenommen eindeutige Bezeichner),
- kapselt das Paket in ein UDP- oder IP/241-Paket ein,
- setzt in diesem Paket als Zugangsadresse und –port die dem aktuellen Knoten bekannten Daten über die näherste Zugangsmöglichkeit zum Empfängerknoten ein.

ViPNet Treiber, der auf dem Computer B läuft, nimmt das IP-Paket entgegen, entschlüsselt es mit Hilfe der eindeutigen Empfängerkennung, entfernt daraus alle Dienstdaten von ViPNet, wandelt, wenn nötig, die reelle IP-Adresse des ursprünglichen Paketabsenders in die virtuelle Adresse des Absenders um. Dann leitet der ViPNet Treiber das Paket entlang des TCP/IP-Stacks an die Anwendungsschicht weiter. Dort wird das Paket entsprechend weiterverarbeitet.

Wenn es entlang des vom IP-Paket passierten Weges Coordinatoren gibt, dann wird auf dem jeweiligen Coordinator ohne vorhergehende Entschlüsselung, nur aufgrund der nicht verschlüsselten eindeutigen Bezeichner in den Paketdaten eine Änderung der Zieladresse und des Zielports des Pakets unter

Berücksichtigung von Informationen über den nähesten Zugangspunkt zum Zielknoten durchgeführt. Das Paket wird im Namen der IP-Adresse der jeweiligen Schnittstelle des Coordinator weitergesendet.

Filterung des Traffics durch den ViPNet Treiber

Jedes ausgehende IP-Paket wird vom ViPNet Treiber folgenderweise verarbeitet:

- Wenn das Paket nicht verschlüsselt werden soll, dann wird es gemäß den Regeln des offenen Netzwerks entweder blockiert oder ins Netzwerk weitergeleitet. Auf dem Coordinator wird dann das Transit-IP-Paket allen erforderlichen Transformationen unterzogen (falls NAT-Einstellungen für den offenen Traffic aktiviert sind).
- Wenn das Paket verschlüsselt werden soll, wird es in Übereinstimmung mit den Regeln des privaten Netzwerks entweder blockiert oder den im letzten Abschnitt aufgeführten Änderungen unterzogen, und anschließend in das Netzwerk weitergeleitet.

Nach Verarbeitung durch den ViPNet Treiber steht das ursprüngliche IP-Paket, das für einen geschützten Knoten bestimmt ist, in verschlüsselter Form zur Verfügung. Es wird ein neues IP-Paket erstellt, das aus dem verschlüsselten Originalpaket, den offenen Kopfdaten mit eindeutigen Bezeichnern sowie aus den versteckten Dienstdaten besteht, die alle durch einen Message Authentication Code geschützt sind. Zusätzlich enthält das IP-Paket die neuen Kopfdaten.

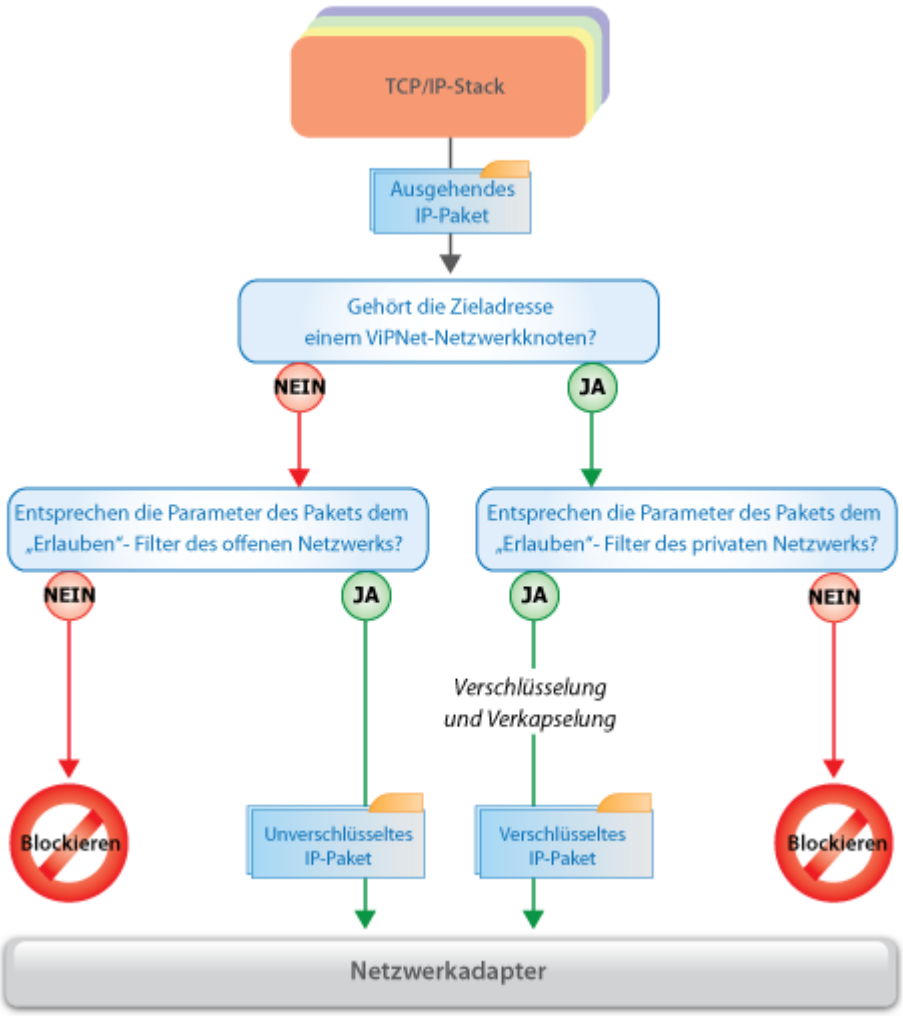

Abbildung 3. Verarbeitung eines ausgehenden Pakets durch den ViPNet-Treiber

Jedes eingehende Paket wird folgendermaßen verarbeitet:

- Wenn das Paket nicht verschlüsselt ist und nicht von einem geschützten Knoten versendet wurde, wird es in Übereinstimmung mit den Filterregeln des offenen Netzwerks blockiert oder durchgelassen. Wenn das Paket von einem geschützten Knoten gesendet wurde, wird es als ein möglicherweise gefälschtes Paket eingestuft und blockiert.
- Wenn das Paket verschlüsselt ist und an den aktuellen Knoten adressiert ist (erkennbar anhand des Bezeichners), wird das Paket entschlüsselt, in Übereinstimmung mit den Filterregeln des privaten Netzwerks blockiert oder Transformationen unterzogen, die bereits weiter oben beschrieben wurden, und anschließend an den TCP/IP-Stack weitergeleitet.
- Wenn am Coordinator ein verschlüsseltes Paket eintrifft, das an einen anderen Knoten adressiert ist (erkennbar an der Id), dann wird dieses Paket nicht entschlüsselt. Die IP-Adressen und Ports des VPN-Pakets werden in Übereinstimmung mit den aktuellen Informationen über den nächstmöglichen Zugangspunkt zum Zielknoten verändert. Das Paket wird über denjenigen Netzwerkadapter des Coordinators an das Netzwerk weitergeleitet, der gemäß den Routingtabellen für die Übermittlung des Pakets an den Zielknoten optimal ist.

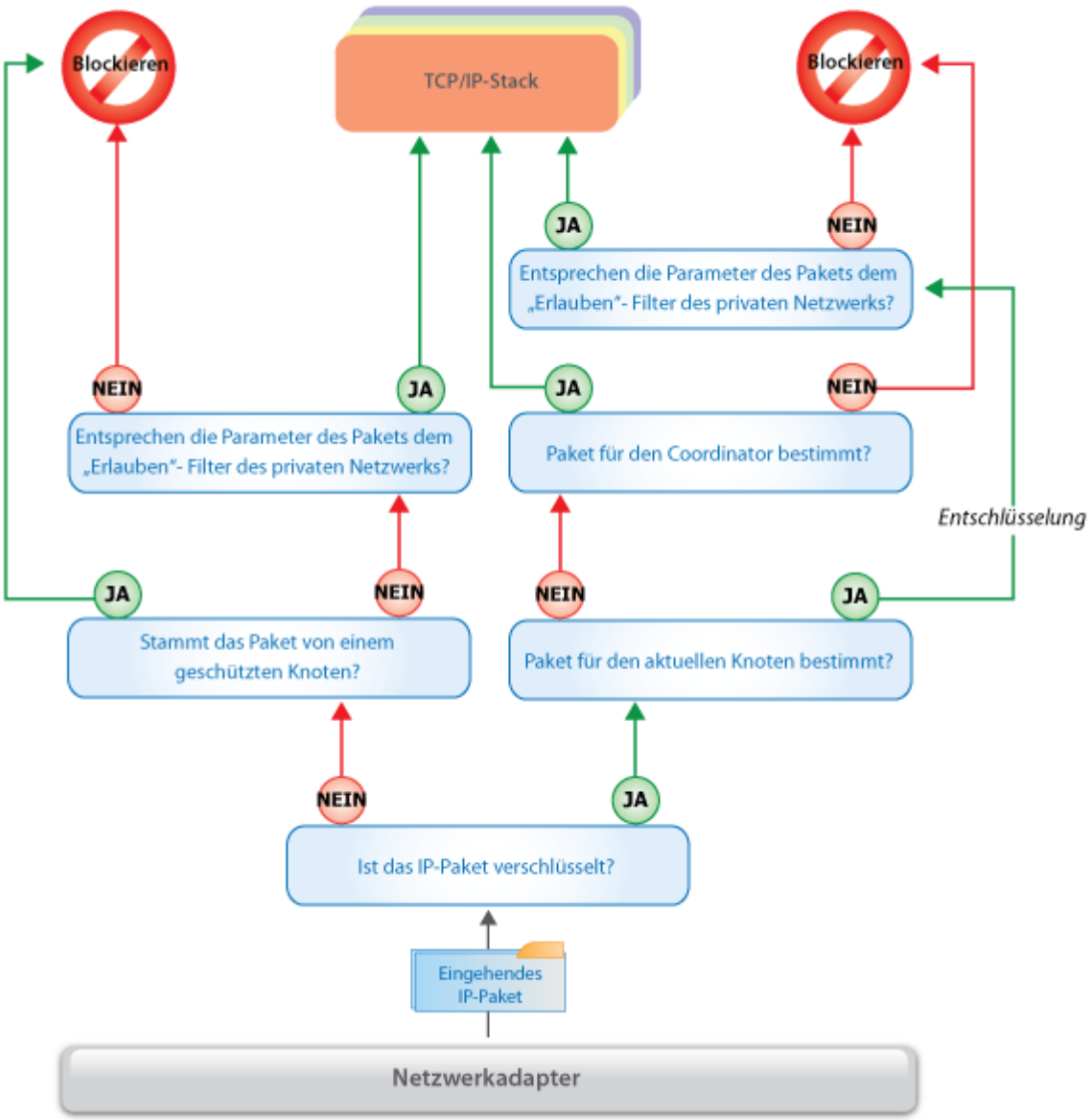

Abbildung 4. Verarbeitung eines eingehenden Pakets durch den ViPNet-Treiber

Das Schlüsselsystem von ViPNet

Die abgesicherte Interaktion von Objekten innerhalb des ViPNet Netzwerks wird mit Hilfe symmetrischer Schlüssel unterschiedlicher Typen gewährleistet.

Schlüssel werden für die Sicherstellung der Interaktion zwischen folgenden Objekten benötigt:

- Netzwerkknoten (Client oder Coordinator) und Netzwerkknoten (Client oder Coordinator);
- Netzwerkknotenbenutzer und Netzwerkknoten mit installierter ViPNet Network Manager Software;

- Netzwerkknoten mit installierter ViPNet Network Manager Software und Netzwerkknoten (Client oder Coordinator).

Schlüssel (s. Symmetrischer Schlüssel auf S. 27) für neue Netzwerkknoten werden zentralisiert im Programm ViPNet Network Manager gebildet und auf eine vertrauliche Art und Weise den Benutzern oder Administratoren der entsprechenden Knoten übergeben. Die Aktualisierung der Schlüssel wird aus dem Programm ViPNet Network Manager über die gleichen abgesicherten Kanäle des VPN-Netzwerks remote durchgeführt.

Die Verteilung der Schlüssel im Netzwerk wird in der Anwendungsschicht unter Verwendung eines speziellen Verfahrens zur automatischen Aktualisierung der Schlüssel unabhängig von der Netzwerkschicht durchgeführt. Dies gewährleistet einen unterbrechungsfreien Betrieb des ViPNet Netzwerks insbesondere in lokalen Netzen.

Symmetrische Schlüssel in ViPNet

Symmetrische Schlüssel werden für die Verschlüsselung von Informationen und für die Kontrolle der Informationsintegrität verwendet.

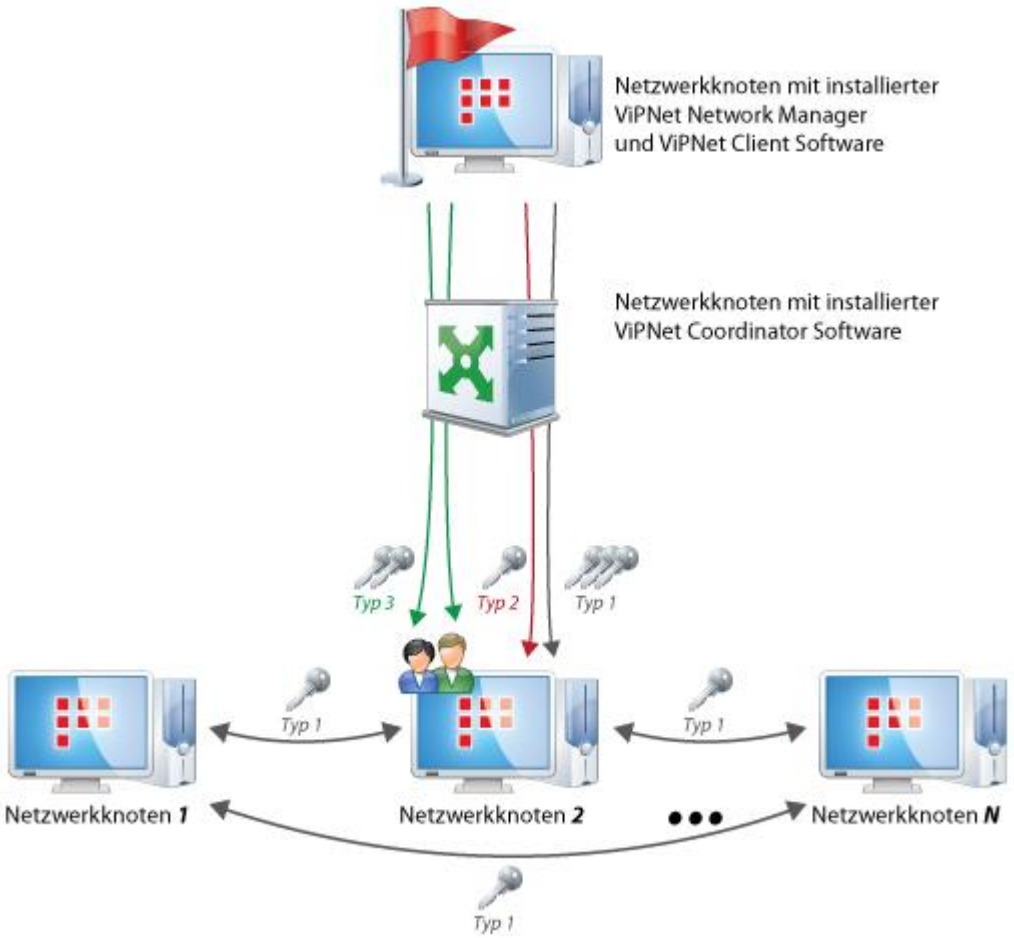

Abbildung 5. Schutz der ViPNet-Netzwerkobjekte mit Hilfe von Schlüsseln unterschiedlicher Typen

In ViPNet Software werden folgende symmetrische Schlüssel eingesetzt (s. Abbildung oben):

- Typ 1. **Austauschschlüssel**: werden für die Verschlüsselung des IP-Traffics zwischen den Knoten auf der Ebene der Netzwerkschicht verwendet. Die Austauschschlüssel selbst werden aber nicht unmittelbar für die Verschlüsselung des Traffics benutzt. Die Verschlüsselung erfolgt mit Hilfe von Schlüsseln, die von Austauschschlüsseln abgeleitet werden und für jedes IP-Paket einmalig sind. Beim planmäßigen Wechsel der Schlüssel, bei Kompromittierung der Netzwerkknoten oder bei Änderungen in der Netzwerkstruktur werden Austauschschlüssel aus dem Programm ViPNet Network Manager zentralisiert an die entsprechenden Netzwerkknoten verteilt. Beim Speichern auf den Netzwerkknoten werden diese Austauschschlüssel unter Verwendung spezieller Schutzschlüssel (Typ 2) chiffriert.
- Typ 2. **Schutzschlüssel für Austauschschlüssel**: werden für die Organisation der Interaktion zwischen dem Netzwerkknoten, auf welchem das Programm ViPNet Network Manager installiert ist, und allen anderen Knoten des ViPNet Netzwerks auf der Anwendungsschicht eingesetzt. Mit Hilfe dieser Schlüssel erfolgt die Verschlüsselung der Austauschschlüssel (Typ 1). Beim Speichern auf den Netzwerkknoten werden diese Schlüssel unter Verwendung spezieller Schutzschlüssel (Typ 3) chiffriert.
- Typ 3. Schutzschlüssel für Schlüssel vom Typ 2 oder **persönliche Schlüssel**: dienen der Abgrenzung des Zugriffs mehrerer Benutzer desselben Netzwerkknotens auf unterschiedliche Daten. Mit Hilfe dieser Schlüssel erfolgt die Verschlüsselung der Schlüssel vom Typ 2 für jeden Netzwerkknotenbenutzer sowie die Verschlüsselung anderer persönlicher Daten, die zum jeweiligen Benutzer gehören. Diese Schlüssel müssen nur dann aus dem Programm ViPNet Network Manager an den konkreten Benutzer eines Netzwerkknotens übergeben werden, wenn die Schlüssel kompromittiert wurden oder ein planmäßiger Wechsel der Schlüssel durchgeführt wird. Private Schlüssel werden mit Hilfe der privaten Ersatzschlüssel chiffriert. Private Schlüssel können sowohl auf einem externen Gerät als auch auf dem Netzwerkknoten aufbewahrt werden. Beim Abspeichern werden private Schlüssel mit dem Kennwortschlüssel des Benutzers chiffriert.

  Kennwortschlüssel: eine Abfolge von Bytes, die durch Berechnung des Werts der Hash-Funktion des Benutzerkennworts gebildet wird. Mit dem Kennwortschlüssel werden die privaten Schlüssel jedes Benutzers chiffriert. Der Kennwortschlüssel kann sowohl zentralisiert im Programm ViPNet Network Manager als auch individuell von einem Benutzer auf dem Netzwerkknoten erstellt werden. Der Kennwortschlüssel wird nach Bedarf erzeugt, temporär verwendet und nicht auf Geräten gespeichert.

  Passwort: eine Abfolge von alphanumerischen Zeichen mit einer Gesamtlänge von 9 bis 32 Bytes. Das Passwort kann sowohl zentralisiert im Programm ViPNet Network Manager als auch individuell von einem Benutzer auf dem Netzwerkknoten angelegt werden. Falls ein externes Gerät verwendet wird, das durch eine PIN geschützt ist, kann statt eines Passworts auch der PIN-Code dieses Gerät eingesetzt werden.

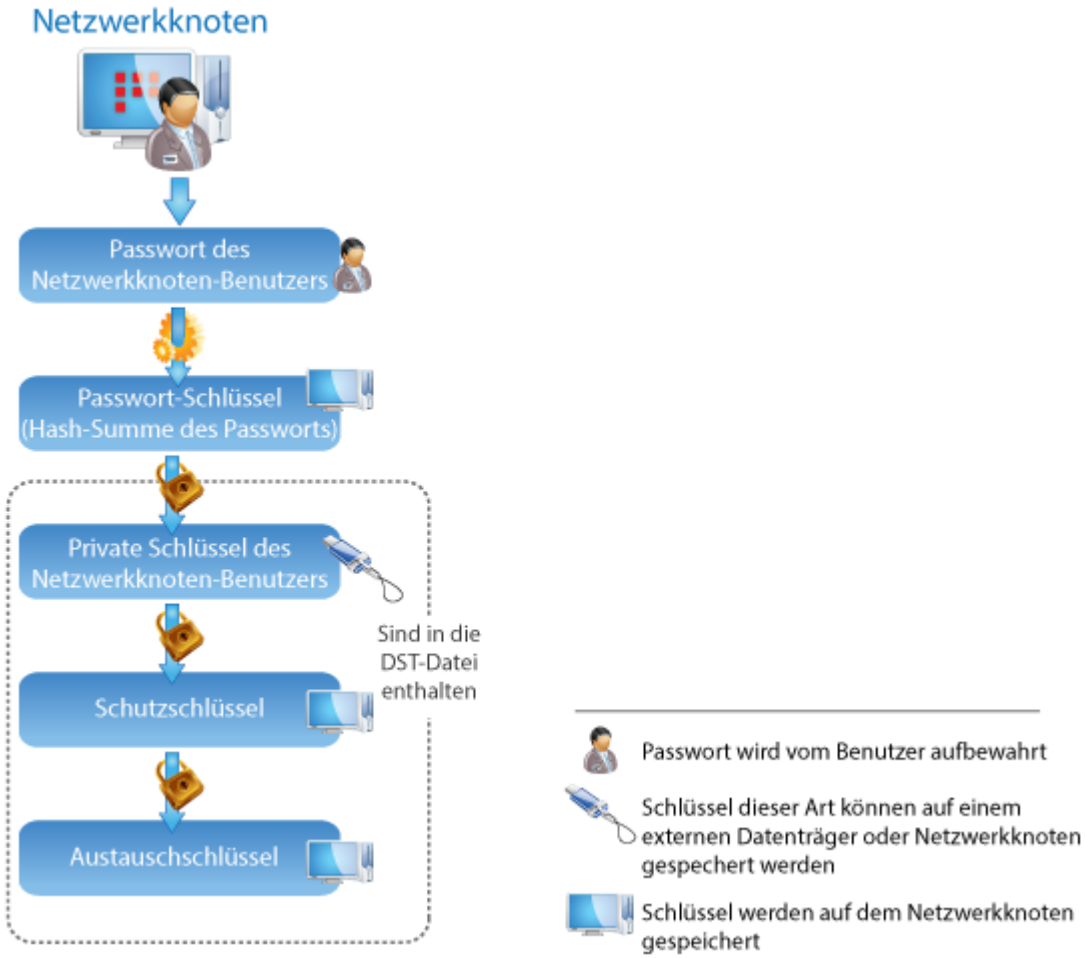

Abbildung 6. Schema der Sicherung symmetrischer Schlüssel in ViPNet

Schlüssel im Programm ViPNet Network Manager generieren

Alle Schlüssel eines separaten ViPNet Netzwerks werden mit Hilfe mehrerer Typen von Masterschlüsseln generiert:

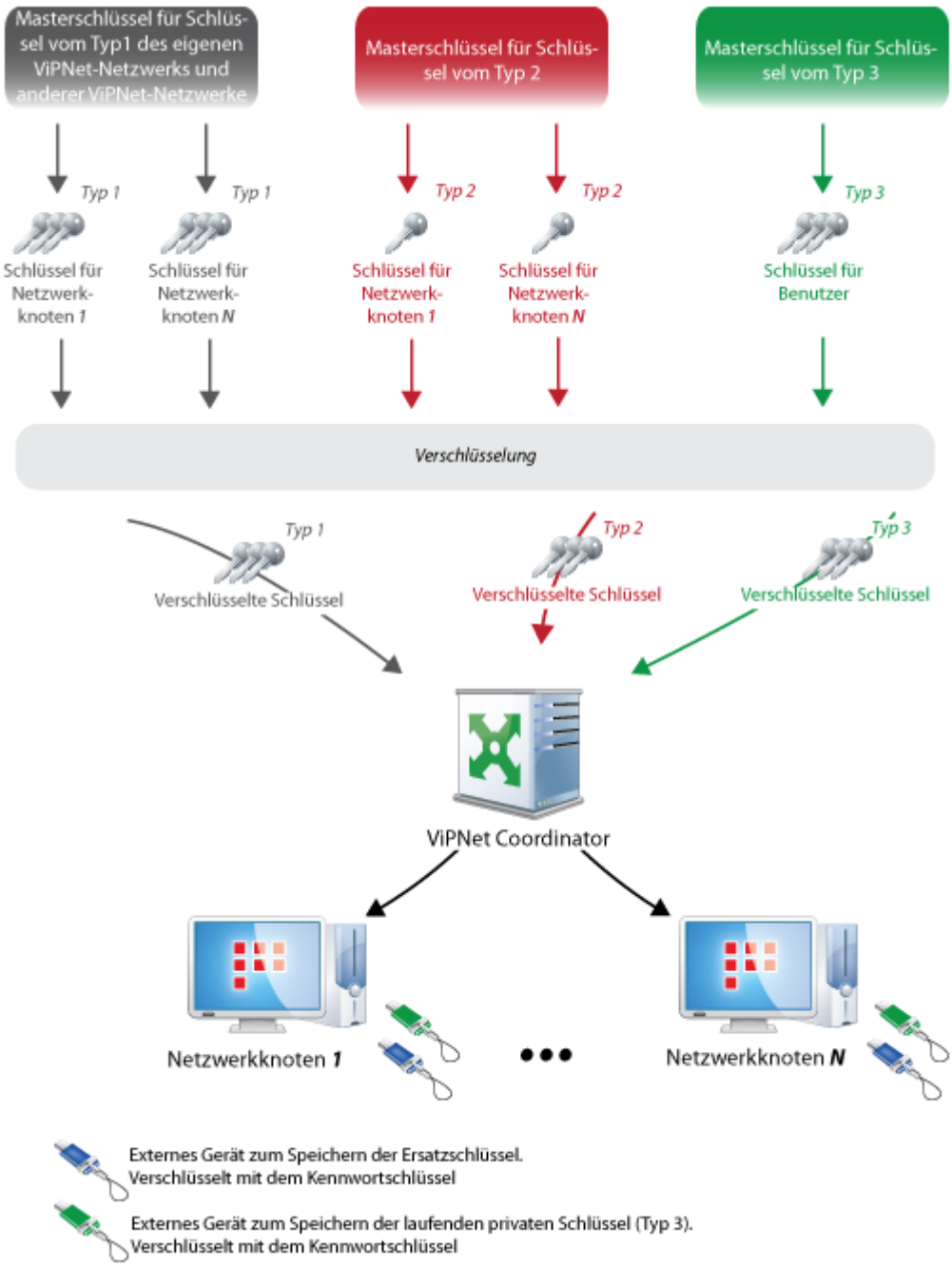

Abbildung 7. Schlüssel unterschiedlicher Typen auf Basis der Masterschlüssel generieren

Beim Generieren der Schlüssel für Verbindungen zu Knoten anderer ViPNet Netzwerke wird der Internetzwerk-Masterschlüssel verwendet. Für jedes ViPNet Netzwerk, das an der Interaktion teilnehmen soll, wird ein separater Internetzwerk-Masterschlüssel benötigt.

Internetzwerk-Masterschlüssel können auf eine der folgenden Arten generiert werden:

- Nach dem Zufallsprinzip in einem der ViPNet Netzwerke. Anschließend wird der Masterschlüssel mit Hilfe des Kennwortschlüssels chiffriert und auf eine sichere Art und Weise an das andere ViPNet Netzwerk weitergeleitet.

- Über das Diffie-Hellman-Protokoll (auf S. 27) durch Austausch signierter öffentlicher Schlüssel zwischen den Administratoren der ViPNet Netzwerke.

Asymmetrische Schlüssel in ViPNet

Asymmetrische Schlüssel (öffentlich und privat) werden in der ViPNet Technologie zum Erzeugen von digitalen Signaturen sowie zum Signieren und Verschlüsseln von Nachrichten in den auf dem Computer installierten Anwendungen (über kryptografische Standardschnittstellen) verwendet. Die Software ViPNet beinhaltet einen Cryptoprovider, der auch von anderen Programmen, wie zum Beispiel MS ViPNet VPN, für die Verschlüsselung von Dateien und Datenblöcken eingesetzt werden kann. Zum Erstellen von Zertifikaten des öffentlichen Schlüssels kann sowohl das Programm ViPNet Network Manager als auch eine externe Zertifizierungsstelle verwendet werden.

Zum Signieren wird ein eigener privater Schlüssel verwendet, während für die Überprüfung der Signaturgültigkeit ein öffentlicher Schlüssel (Zertifikat des Signaturschlüssels) ausreicht, der dem Unterzeichner der Nachricht gehört. Zum Verschlüsseln (Entschlüsseln) werden der öffentliche Schlüssel des Empfängers (Absenders) sowie der eigene private Schlüssel benötigt. Das Zertifikat beinhaltet einen öffentlichen Schlüssel, der durch einen Bevollmächtigten bescheinigt (signiert) ist (zum Beispiel durch den Administrator des ViPNet Netzwerks), sowie Informationen über den Zertifikatsbesitzer, die Gültigkeitsdauer des Zertifikats und weitere Daten.

Der private Schlüssel muss vor anderen Benutzern geheim gehalten werden; es wird empfohlen, für die Speicherung externe Datenträger oder Geräte zu verwenden. Auf der Festplatte wird der private Schlüssel in verschlüsselter Form in einer Datei aufbewahrt, die als Schlüsselcontainer bezeichnet wird. Der Schutzmechanismus für private Signaturschlüssel wird in der nachfolgenden Abbildung dargestellt.

Abbildung 8. Sicherungsverfahren für geheime Signaturschlüssel

Wenn der private Signaturschlüssel auf einem externen Gerät gespeichert ist, bildet der Kennwortschlüssel oder die PIN des Geräts seinen Schutzschlüssel. Wenn der private Signaturschlüssel auf der Festplatte oder in einer Schlüsseldistribution gespeichert ist, stellt der private Schlüssel des ViPNet Benutzers seinen Schutzschlüssel dar.

Verteilung der Schlüssel im ViPNet Netzwerk

Die weiter oben beschriebene mehrstufige symmetrische Schlüsselstruktur ermöglicht es nicht nur, ein skalierbares und zuverlässiges System zur Verteilung symmetrischer Schlüssel einzurichten. Es kann damit auch ein leicht zu verwaltendes, kryptografisch geschütztes System der Zugriffskontrolle für öffentliche Informationsressourcen und für die Informationsressourcen der Benutzer installiert werden.

Die Verteilung symmetrischer Schlüssel ist vollständig automatisiert und erfordert keine weiteren Eingriffe seitens des Benutzers.

Der Netzwerkknoten kann sich unter Einhaltung folgender Bedingungen an das VPN-Netz anschließen:

- Der Knoten und die Knotenbenutzer müssen im Programm ViPNet Network Manager registriert sein.
- Verbindungen dieses Knotens zu anderen Knoten im Netzwerk müssen definiert sein.
- Für den Knoten muss eine Schlüsseldistribution vorliegen, die folgende Daten enthält: Benutzerschlüssel (privater Schlüssel des Benutzers und, wenn nötig, die Signaturschlüssel), Austauschschlüssel für andere Netzwerkknoten, Adresslisten, die für Verbindungen zu anderen Netzwerkknoten erforderlich sind sowie die Registrierungsdatei infotecs.re. Die Schlüsseldistribution wird mit dem Benutzerschlüssel chiffriert, der seinerseits mit dem Kennwortschlüssel verschlüsselt wird.

Nach Erhalt der Schlüsseldistribution kann das ViPNet Programm auf dem Computer installiert werden. Nach Abschluss der Installation kann der Computer gleich an das VPN-Netzwerk angeschlossen werden. Anschließend kann er beginnen, mit anderen Knoten sowohl des eigenen Netzwerks als auch mit Knoten anderer ViPNet Netzwerke, zu denen im Programm ViPNet Network Manager Partnernetzwerk-Verbindungen definiert wurden, zu kommunizieren. Verbindungen zu Knoten anderer ViPNet Netzwerke werden vom Administrator im Programm ViPNet Network Manager aufgrund von gegenseitigen Vereinbarungen mit den Administratoren des Programms ViPNet Network Manager in diesen Netzwerken erstellt.

Falls neue Knoten in die Struktur des bestehenden ViPNet Netzwerks integriert werden sollen, müssen diese Knoten ebenfalls im Programm ViPNet Network Manager registriert werden. Anschließend müssen neue Schlüssel erstellt werden: sowohl für die neuen Knoten des eigenen Netzwerks als auch für jene Knoten des eigenen Netzwerks, die mit den neuen Knoten kommunizieren sollen. Gemeinsam mit den Schlüsselinformationen werden auch die erforderlichen Adresslisten erstellt. Die Schlüsseldistribution wird auf eine vertrauliche Art und Weise an den neuen Knoten übergeben. Vor dem Weiterleiten an einen bereits vorhandenen Netzwerkknoten werden die Schlüsselinformationen mit den Austauschschlüsseln des Programms ViPNet Network Manager und des entsprechenden Knotens verschlüsselt. Anschließend werden die verschlüsselten Schlüsseldaten und Adresslisten über bestehende VPN-Tunnel (über den ViPNet Coordinator oder direkt, falls entsprechende Einstellungen vorgenommen wurden) an den betroffenen Knoten übertragen. Nach Erhalt neuer Schlüssel und Adresslisten aktualisiert der Netzwerkknoten automatisch seine Schlüssel- und Adressdaten. Die gleiche Abfolge an Schritten wird auch beim Löschen eines Knotens aus der bestehenden Netzwerkstruktur oder beim Ändern von

definierten Verbindungen zu anderen Knoten durchgeführt. Beim Löschen von Verbindungen werden nicht mehr benötigte Schlüsselinformationen aus der Schlüsseldatenbank entfernt.

Wenn die Verbindungen eines Knotens zu Knoten in anderen ViPNet Netzwerken verändert werden, dann werden automatisch neue Adresslisten für diese Netzwerke angelegt. Diese Daten werden dann automatisch über bestehende VPN-Verbindungen an das Programm ViPNet Network Manager in den entsprechenden Netzwerken weitergeleitet.

Wenn ein Netzwerkknoten kompromittiert wird, sollte dieser Knoten im Programm ViPNet Network Manager gelöscht und wieder neu erstellt werden. In diesem Fall werden für diesen Knoten andere Schlüsselinformationen angelegt. Anschließend müssen die neuen Schlüsseldistributionen auf eine vertrauliche Art und Weise an die Benutzer des betroffenen Knotens übergeben werden. Zusätzlich müssen Schlüsselupdates an andere Netzwerkknoten versendet werden, damit diese Verbindungen zum neuen Knoten aufbauen können. Alte Schlüsselinformationen des kompromittierten Knotens werden auf allen Netzwerkknoten gelöscht.

Es ist äußerst wichtig, dafür zu sorgen, dass die Schlüsselupdates synchron durchgeführt werden. Dazu kann im Programm ViPNet Network Manager die genaue Absendezeit für die Schlüsselupdates eingestellt werden. Zusätzlich kann dort der Annahmeprozess der Updates auf den einzelnen Knoten überwacht werden. Dank dieser Möglichkeit wird ein unterbrechungsfreier Betrieb des ViPNet Netzwerks auch im Fall von Schlüsselupdates auf allen Netzwerkknoten gewährleistet.

Vorteile der ViPNet Technologie

Zum heutigen Zeitpunkt existieren neben ViPNet eine Mehrzahl anderer Technologien zur Gewährleistung einer sicheren Übermittlung von Daten über öffentliche Netze. Es sollte jedoch auf eine Reihe zusätzlicher funktioneller Konzepte hingewiesen werden, die die ViPNet Technologie aus der Menge der klassischen VPN-Lösungen wie IPsec, OpenVPN, PP2P u. a. hervorheben.

Technologische Vorteile

- **Schutz des Traffics innerhalb des lokalen Netzwerks**

  Klassische VPN-Lösungen. Ursprünglich entwickelte sich die VPN-Technologie als eine Lösung für das Problem der sicheren Datenübertragung über das Internet: es wurde angenommen, dass es innerhalb eines lokalen Netzwerks die Gefahr des Abfangens vertraulicher Daten gar nicht gibt. Dieser Ansatz lässt sich noch immer bei einer Mehrheit der modernen VPN-Lösungen nachverfolgen. Während die Sicherheit bei Verbindungen zwischen den lokalen Netzwerken und beim Remotezugang zu lokalen Netzwerken garantiert wird, schaffen es diese Lösungen nicht, ein anderes Problem zu lösen: eine in sich abgeschlossene Umgebung innerhalb einer heterogenen Netzwerkinfrastruktur aufzubauen und einen sicheren, direkten Datenaustausch zwischen den einzelnen Teilnehmern dieser Umgebung zu gewährleisten.

Da das lokale Netzwerk als vertrauenswürdig gilt, wird der Traffic zwischen dem VPN-Gateway (Einrichtung, die als Zugangspunkt zum VPN-Netzwerk auftritt) und dem Endknoten des lokalen Netzwerks nicht verschlüsselt. Auf diese Weise kann die Vertraulichkeit von Daten nach dem Entschlüsseln auf dem VPN-Gateway auf ihrem Weg durch das Netzwerk nicht garantiert werden. Auf dem Gateway sind alle Daten bereits entschlüsselt und bei potentiellen Abfangversuchen im lokalen Netzwerk vollkommen ungeschützt.

ViPNet. Der VPN-Gateway (Coordinator) tritt gleichzeitig als Router für den VPN-Traffic auf. Der VPN-Gateway führt das Routing von vertraulichen Daten zu den entsprechenden Knoten des VPN-Netzwerks durch, ohne die Daten dabei zu entschlüsseln. Dank dieser Vorgangsweise bleiben die Daten sowohl auf dem Coordinator als auch in allen Segmenten des lokalen Netzwerks entlang der Paketroute vor möglichen Abfangversuchen aller Benutzer (auch der Administratoren) geschützt.

Gleichzeitig kann der Durchgang von Daten durch mehrere Coordinatoren gewährleistet werden (das sogenannte „kaskadierte Einschalten der Coordinatoren"). Auf diese Weise können die Daten über eine bestimmte Route oder in zusätzlich geschützte Segmente des lokalen oder des Firmennetzwerks geleitet werden. Coordinatoren führen das Routing des VPN-Traffics auf Basis von Daten über Zugangspunkte zu VPN-Knoten durch. Diese Daten erhalten sie aus dem Systemdatenverkehr, der mit Hilfe des Protokolls für das dynamische Routing von VPN-Paketen weitergeleitet wird. Dank dieser Vorgangsweise kann die Routenwahl nicht mehr unbefugt beeinflusst werden.

Indem die Funktionalität von traditionellen VPN-Lösungen mit den Möglichkeiten des dynamischen Routings beim VPN-Traffic (unter Verwendung eines speziellen Protokolls) kombiniert wird, erleichtert die ViPNet Technologie den Aufbau von zuverlässig geschützten Netzwerkstrukturen in komplexen, verteilten Systemen. Beliebige Typen von gesicherten Interaktionen können auf eine einfache Weise organisiert werden, auch zwischen unterschiedlichen Organisationen.

- **Flexibilität, Möglichkeit zum Aufbau zahlreicher Formen der gesicherten Interaktion**

  Klassische VPN-Lösungen. Erlauben es, den gesicherten Austausch von vertraulichen Daten meistens in Form von „client-to-site" und „site-to-site" aufzubauen. Der Client-Computer verbindet sich beim Verbindungsaufbau zu einem anderen Client zunächst zum Server, um die primäre Authentifizierung durchzuführen. Der Einsatz anderer Vorgangsweisen und Szenarien ist insoweit eingeschränkt, als Möglichkeiten zum Routing des VPN-Traffics ohne seine vorhergehende Entschlüsselung an der Grenze des lokalen Netzwerks (auf dem VPN-Gateway) fehlen. Verbindungsaufbau in Form von „client-to-client" ist zwar möglich, in der Regel stellen solche Verbindungen „flache" Formen der Interaktion in gerouteten Netzwerken dar, die dazu geschaffen werden, den Zugang zu bestimmten Servern einzuschränken.

Abbildung 9. Aufbau eines VPN-Netzwerks auf Basis der IPSec-Technologie

- **ViPNet.** Dank der Technologie des dynamischen Routings für den IP-Traffic kann neben den Formen „client-to-site" und „site-to-site" auch das Schema „client-to-client" unkompliziert realisiert werden. Andere potentielle Formen ermöglichen entweder eine direkte Weiterleitung des Traffics oder eine Weiterleitung über Coordinatoren, jedoch ohne die Daten dabei zu entschlüsseln. Dadurch können beliebige Richtlinien für die Sicherstellung der Zugriffskontrolle im Rahmen des gesamten geschützten Netzwerks eingeführt werden. Zusätzlich kann die Belastung der VPN-Server verringert werden.

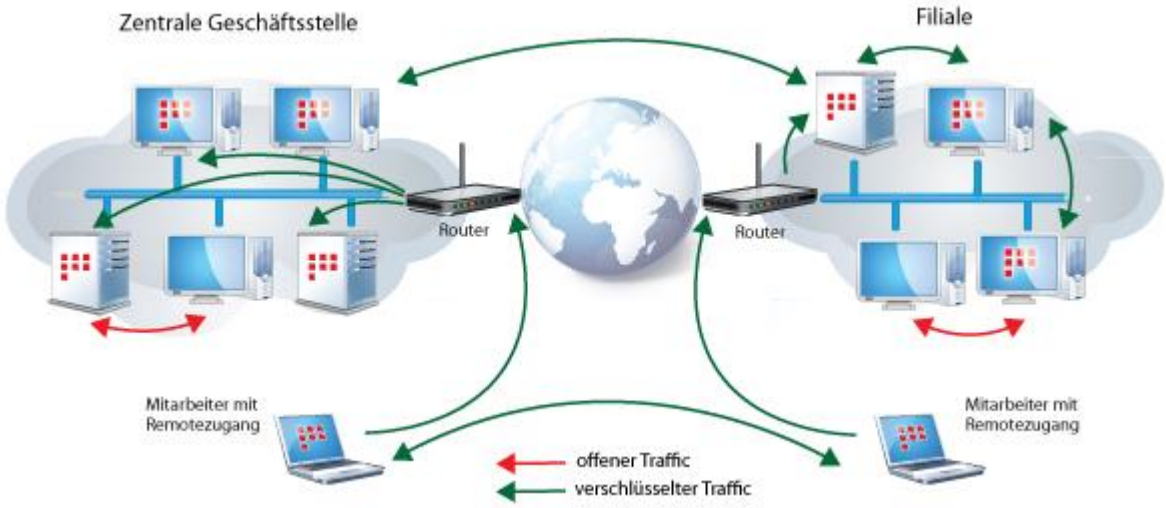

Abbildung 10. Aufbau eines VPN-Netzwerks auf Basis der ViPNet-Technologie

- **Lösung des Problems der Überschneidung von IP-Adressbereichen**

  Klassische VPN-Lösungen. Falls mehrere lokale Netzwerke zusammengeschlossen werden sollen, kann dies zu Problemen der Überschneidung von IP-Adressbereichen führen (zum Beispiel bei Interaktion mit einem Partnernetzwerk, das teilweise die gleichen privaten IP-Adressen verwendet). Dieses Problem kann auch dann auftauchen, wenn ein ferner Benutzer Verbindungen zum Netzwerk aufbaut. In der Technologie von Open VPN wird dieses Problem gelöst, indem auf dem Computer des Remotebenutzers ein virtueller Adapter installiert wird, der die IP-Adresse zentralisiert vom VPN-Gateway bezieht. Diese Lösung besitzt folgende Nachteile:

- Der IP-Adressenkonflikt kann unmittelbar im Netzwerk entstehen, zu welchem sich der Remotebenutzer verbinden will.
- Die Gestaltung von Interaktionen mit Netzwerken, die sich hinter anderen VPN-Gateways befinden, ist relativ komplex.
- Die Organisation der Traffic-Verschlüsselung erfolgt durch seine Umleitung auf den virtuellen Adapter. Die Routingtabelle kann dabei ungehindert lokal modifiziert werden, wobei auch die Verschlüsselung des Traffics für die Tunnelung deaktiviert werden kann.

ViPNet. Die Überschneidung von IP-Adressen wird mit Hilfe der Technologie der virtuellen IP-Adressen verhindert. Für alle Remoteknoten werden auf einem separaten Knoten virtuelle IP-Adressen vergeben, die unabhängig von den reellen IP-Adressen der Knoten sind. Andere geschützte Netzwerkknoten können von diesem Knoten aus über eindeutige virtuelle IP-Adressen angesprochen werden, die dort automatisch angelegt werden. Wenn der Remoteknoten ein Coordinator ist, bleibt er dank der Technologie der virtuellen IP-Adressen von jedem offenen Computer aus, den er tunnelt, ansprechbar. Der getunnelte Rechner kann seinerseits auf andere getunnelte Computer und geschützte Knoten zugreifen.

Die Benachrichtigung der Anwendungen über die virtuellen IP-Adressen der Remoteknoten erfolgt mit Hilfe einer speziellen Verarbeitung des Traffics, der für die Auflösung von Namen für alle gängigen Protokolle und Dienste gebildet wird: DNS, NetBios, Multimediaprotokolle SIP, SCCP, H323, H225, H245 und andere. Im Zuge der Interaktion von Anwendungen mit fernen Computern werden bei Bedarf die IP-Adressen in den ausgehenden IP-Paketen entsprechend umgewandelt (reelle in virtuelle und umgekehrt).

Neben der Lösung des Problems der Überschneidung von IP-Adressbereichen verhindern virtuelle IP-Adressen auch mögliche Fälschungsversuche von IP-Adressen. Zum Zeitpunkt des Empfangs wird das IP-Paket vom ViPNet Treiber nach Substitution der reellen Absenderadresse durch die entsprechende virtuelle IP-Adresse an die jeweilige Anwendung weitergeleitet. Dies passiert nur dann, wenn das Paket mit Hilfe der Absenderschlüssel erfolgreich entschlüsselt werden konnte, d. h. nachdem der Absender eindeutig identifiziert werden konnte. Diese Vorgangsweise gewährleistet den Schutz vor einer absichtlichen Substitution der Absenderadresse aus Fälschungsgründen und ermöglicht eine sichere Abgrenzung des Zugangs zu geschützten Objekten auf Basis von virtuellen IP-Adressen.

- **Arbeit mit offenen Ressourcen im Internet**

Klassische VPN-Lösungen. Auf Remotecomputern wird der Datenaustausch über einen VPN-Kanal üblicherweise mit Hilfe eines virtuellen Adapters realisiert, der IP-Adressen vom VPN-Gateway über das DHCP-Protokoll bezieht. Die Interaktion eines Remotecomputers mit offenen Ressourcen im Internet über die korporative Firewall kann bewerkstelligt werden, indem der gesamte Traffic über einen VPN-Tunnel an das VPN-Gateway der Firma geleitet wird. Dadurch kann die Verarbeitung des offenen Traffics in Übereinstimmung mit den Sicherheitsanforderungen der Organisation erfolgen. Damit dieser Lösungsansatz flexibel verwaltet werden kann, muss jedes Mal die Routingtabelle des Betriebssystems entsprechend angepasst werden (und zwar muss als Standardgateway die mit Hilfe des DHCP-Protokolls erhaltene virtuelle IP-Adresse angegeben werden). Der Schutz einer solchen Form der Interaktion kann sich als mangelhaft erweisen: es kann versucht werden, die Routingtabelle lokal auf die eine oder andere Weise zu modifizieren und den Internet-Traffic direkt über den örtlichen Provider zu leiten. Zusätzlich können dabei die Verschlüsselung des Traffics vor

der Tunnelung und damit die Vertraulichkeit der Daten außer Kraft gesetzt werden (wie weiter oben beschrieben).

ViPNet. Die Technologie basiert darauf, die Umleitung des IP-Traffics ohne Zuhilfenahme virtueller Adapter und ohne Anpassungen der Routingtabelle des Betriebssystems zu bewerkstelligen. Der ViPNet Treiber übernimmt die Verschlüsselung des Traffics in Übereinstimmung mit der Liste registrierter IP-Adressen der geschützten Knoten. Um den Zugang zu offenen Ressourcen über die korporative Firewall sicherzustellen, blockiert der Treiber alle Daten ausgenommen DHCP-Daten für die Verbindungen zum Provider. Der Internet-Traffic selbst wird in den Tunnel des VPN-Gateways umgeleitet.

- **Stabiler Betrieb bei häufigen Änderungen von Verbindungstypen oder bei Zugriffen auf andere VPN-Gateways (falls mobile Geräte eingesetzt werden)**

  Klassiche VPN-Lösungen. Der häufige Wechsel von Basisstationen (zum Beispiel bei 3G-Verbindungen) kann zur Instabilität im Netzwerkbetrieb führen. Nach dem Unterbrechen einer Verbindung muss zum Beispiel die Authentifizierung erneut durchgeführt werden. Falls der Zugang zu einem anderen VPN-Gateway erforderlich wird, müssen Konfigurationsparameter entsprechend angepasst werden. Dadurch kann ein unterbrechungsfreier Betrieb des VPN-Netzwerks nicht mehr garantiert werden.

  ViPNet. Im Falle einer Unterbrechung wird die Verbindung automatisch wiederhergestellt; dabei müssen die Kontodaten des Benutzers nicht erneut eingegeben werden. Falls auf andere Netzwerke zugegriffen werden soll, müssen die Konfigurationsparameter nicht mehr geändert werden. Das Protokoll des dynamischen Routings von VPN-Paketen ermöglicht ein automatisches Routing von Paketen zum benötigten Coordinator.

- **Schlüsselstruktur**

  Klassiche VPN-Lösungen. Bei „client-to-site" Verbindungen ist die Benutzung symmetrischer Schlüssel beim Bereitstellen des Remotezugriffs nur auf Basis eines bestimmten, einzelnen Schlüssels möglich. Bei „site-to-site" Verbindungen können für jedes Paar von Netzwerkknoten unterschiedliche symmetrische Schlüssel erzeugt werden. Es fehlt jedoch ein Mechanismus zur Verteilung der Schlüssel und zur Administration der entsprechenden symmetrischen Schlüsselstruktur. Aus diesem Grund ist die Anwendung symmetrischer Schlüssel in weitläufigen, stark verzweigten geschützten Netzwerken äußerst kompliziert und unsicher.

  ViPNet. Es existiert ein eigenes, einzigartiges automatisiertes System zur Administration der symmetrischen Schlüsselstruktur, das sicherer und zuverlässiger ist als das System der offenen Schlüsselverteilung.

- **Filterung des verschlüsselten IP-Traffics unabhängig von der IP-Adresse des Paketabsenders**

  Klassische VPN-Lösungen. Die Filterung des Traffics erfolgt auf Basis von IP-Adressen der Paketabsender. Dieser Ansatz ist darauf zurückzuführen, dass die Traffic-Filterung in der Regel von der Firewall vorgenommen wird, die unabhängig von VPN ist. Nach Entschlüsselung der IP-Pakete gehen dort aber sämtliche Daten über diese Pakete mit Ausnahme von IP-Adressen der Absender verloren. Die IP-Adresse selbst bleibt jedoch in keinster Weise vor möglichen Substitutionsversuchen seitens möglicher interner Hacker geschützt.

  ViPNet. Die Firewall ist mit VPN integriert. Die Filterung des geschützten Traffics erfolgt zu einem Zeitpunkt, wenn nach der Entschlüsselung des Pakets seine Relation zur Absender-ID noch nicht

verlorengegangen ist. Deswegen werden Filterregeln nicht für IP-Adressen, sondern für Netzwerkknoten definiert. Die IP-Adressen selbst spielen dabei keine Rolle. Diese Vorgangsweise schließt alle möglichen Versuche interner Hacker, die IP-Adresse des Absenders zu substituieren, um die Filter des geschützten Netzwerks zu umgehen, auf eine wirkungsvolle Weise aus.

Kommerzielle Vorteile

- Im Vergleich zu gewöhnlichen VPN-Lösungen stellt ViPNet Software eine Reihe zusätzlicher funktioneller Möglichkeiten für den sicheren Datenaustausch zur Verfügung: eingebaute Dienste für den sofortigen Austausch von Nachrichten (Konferenz- und Chatdienste) und Dateien, ein eigener sicherer Maildienst mit der Möglichkeit zur automatisierten Nachrichtenverarbeitung und Dateiaustausch sowie mit Unterstützung der digitalen Signatur.
- Zusätzliche Möglichkeiten der ViPNet Software im Bereich der Netzwerkkommunikation wie zum Beispiel die Überwachung der Netzwerkaktivitäten von Anwendungen, exakte Regelungen für den Zugang zum Internet, Mechanismen zur Gewährleistung eines Neustarts im Notfall erlauben es, das System vor einer Mehrzahl von Attacken zu schützen und die Kosten für das Sicherheitssystem insgesamt zu senken.
- Die Lösungen von ViPNet sind autark, deswegen müssen keine weiteren Module wie Datenbanken oder spezielle Serverplattformen angeschafft werden. Die Produkte von ViPNet enthalten keine versteckten Kosten: Sie bezahlen nur diejenigen Komponenten, die Sie auch wirklich brauchen.
- Da ViPNet Produkte in Form von integrierten Hard- und Softwarelösungen geliefert werden können, erfordert ihre Installation und Konfiguration keine Anschaffung spezieller Hardware und kann unter Verwendung des vorhandenen Rechnerbestands durchgeführt werden. In der Mehrheit der Fälle muss die Konfiguration der bestehenden Netzwerkausrüstung ebenfalls nicht angepasst werden.
- Flexible Preisgestaltung und die Möglichkeit, Lizenzen für die einzelnen ViPNet Komponenten nur bei Bedarf zu aktivieren, erlauben es uns, eine im Hinblick auf Preis und Leistung optimale Lösung für jeden Kunden zu finden. Sie bezahlen nur das, was Sie zum aktuellen Zeitpunkt wirklich brauchen; den Rest können Sie später jederzeit nachkaufen.

Glossar

A

Austauschschlüssel

Ein symmetrischer Schlüssel, der den Sender und Empfänger verschlüsselter Information bekannt ist.

Siehe: Symmetrischer Schlüssel (auf S. 27).

C

Client (ViPNet Client)

Computer mit installierter ViPNet Client Software.

Coordinator (ViPNet Coordinator)

Netzwerkknoten mit installierter ViPNet Coordinator Software.

D

Diffie-Hellman-Protokoll

Eines der Protokolle mit öffentlicher Schlüsselverteilung, bei welchem zwei Benutzer durch die dynamische Interaktion untereinander einen gemeinsamen geheimen Schlüssel erzeugen können. Es basiert auf dem Austausch offener (nicht verschlüsselter) Nachrichten ohne irgendwelche gemeinsame geheime Information, die im Voraus verteilt wird.

Digitale Signatur

Eine digitale Signatur ist ein kryptografisches Verfahren, bei dem zu einer „Nachricht (d. h. zu beliebigen Daten) eine Zahl (die digitale Signatur) berechnet wird, deren Urheberschaft und Zugehörigkeit zur Nachricht durch jeden geprüft werden können. Digitale Signaturen basieren auf asymmetrischen Kryptosystemen und verwenden folglich ein Schlüsselpaar, das aus einem privaten (geheimen) und einem öffentlichen (nicht geheimen) Schlüssel besteht.

S

Schlüsselcontainer

Datei, in der der private Schlüssel und das zugehörige Zertifikat des öffentlichen Schlüssels gespeichert sind. Beim Bilden einer Anfrage für die Zertifikatsaktualisierung wird der Name des Containers, in dem das neue Schlüsselpaar der Signatur (privater Schlüssel und das Zertifikat) aufbewahrt wird, automatisch vergeben und hat die Form `sgn-<Zufallszahl im Hexadezimalformat>`.

Schlüsselkompromittierung

Man spricht von einer Kompromittierung, wenn durch die verwendeten Schlüssel kein Informationsschutz (Integrität, Vertraulichkeit, Authentizität) mehr sichergestellt werden kann.

Symmetrischer Schlüssel

Eine Bit-Folge bestimmter Länge (dieLänge der AES-Algorithmus beträgt 256 Bit). Wird sowohl für die Verschlüsselung als auch für die Entschlüsselung eingesetzt.

T

Transportmodul (MFTP)

Die Software-Komponente für den Informationsaustausch innerhalb des ViPNet Netzwerkes.

V

ViPNet Network Manager

Verwaltungsmodul aus dem Paket ViPNet VPN, dient zum Erstellen und Verwalten kleiner und mittlerer ViPNet Netzwerke.

ViPNet Netzwerk

Mit Hilfe von ViPNet Software aufgebautes logisches Netzwerk.