Grundsätze beim Aufbau von Verbindungen im ViPNet Netzwerk

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 04 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 die wichtigsten Grundlagen des Routing und der Verarbeitung des Traffics in ViPNet Netzwerken beschrieben, die es erlauben, abgesicherte Verbindungen zwischen den ViPNet Netzwerkknoten unabhängig von der Zugangsart zum Netzwerk bereitzustellen.

Es wird angenommen, dass sich der Leser vor Studium dieses Dokuments mit dem Dokument „Die Technologie von ViPNet. Allgemeine Informationen" vertraut gemacht hat.

Dieses Dokument bietet keine Informationen zur Netzwerkadministration, Schlüsselstruktur, zu den Grundlagen der Trafficfilterung oder zur Vorgehensweise beim Aufbau der Infrastruktur für die Erstellung digitaler Signaturen.

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.

Funktionen eines Coordinators im privaten ViPNet Netzwerk

Der VPN-Server im geschützten Netzwerk wird als Coordinator bezeichnet.

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 (s. Tunnel auf S. 23)) 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. 23), das in der Anwendungsschicht arbeitet. Das MFTP-Modul empfängt Transportdateien (s. Datei (Transportdatei) auf S. 20) 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 (s. Öffentliche IP-Adresse auf S. 22) 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.

Besonderheiten der Traffic-Umleitung in einem auf Basis der ViPNet Technologie aufgebauten VPN Netzwerk

Moderne VPN-Systeme mit klassischer Technologie sind hauptsächlich dazu bestimmt, sichere Verbindungen lokaler Netzwerke über das Internet aufzubauen und den Remotezugang zu Objekten in diesen Netzwerken bereitzustellen. Bei weitem nicht alle Systeme können jedoch dazu verwendet werden, eine abgesicherte Umgebung innerhalb einer heterogenen Netzwerkstruktur zu schaffen und den Aufbau von Verbindungen unmittelbar zwischen Datensender und -empfänger zu gewährleisten.

Die Hauptaufgabe eines VPN-Netzwerks, das mit Hilfe der Technologie von ViPNet aufgebaut wurde, besteht darin, den Schutz des Traffics zu gewährleisten und den Zugang zu Computern und anderen Netzwerkgeräten im Zuge des Datenaustauschs in jenen Netzwerksegmenten sicherzustellen, in denen es erforderlich ist. Es spielt dabei keine Rolle, wo sich diese Netzwerkgeräte befinden – im Internet, im Firmennetzwerk oder in einem Netzwerksegment (auf S. 21).

Wenn zwei Computer, auf denen ViPNet Software installiert ist (Netzwerkknoten: Clients und Coordinatoren), über das ViPNet Netzwerk miteinander kommunizieren, wird die Ver- und

Entschlüsselung des Traffics unmittelbar auf diesen Computern durchgeführt. Auf diese Weise kann der Traffic dazwischen nicht abgefangen werden. Dieser Vorzug wird durch die Verwendung eines speziellen Protokolls für das dynamische Routing des VPN-Traffics sowie durch Einsatz von ViPNet Coordinatoren (s. Coordinator (ViPNet Coordinator) auf S. 20) im Netzwerk gewährleistet.

Neben der Sicherstellung der Interaktion vom Typ „Punkt-zu-Punkt" kann der Coordinator auch die Standardfunktionen eines VPN-Gateways übernehmen: den Traffic ungeschützter Computer und Geräte, die sich hinter dem Coordinator im lokalen Netzwerk befinden, zu anderen Coordinatoren oder Remoteclients tunneln. Im Unterschied zu anderen VPN-Systemen:

- spielt es keine Rolle, auf welchem VPN-Gateway (Coordinator) der Client registriert ist;
- sind keine zusätzlichen Einstellungen erforderlich;
- besteht die Möglichkeit zur automatischen Bereitstellung einer abgesicherten Verbindung jeder beliebigen Anwendung auf dem Computer zu jedem anderen ViPNet Netzwerkknoten.

Grundsätze der Interaktion von Knoten im ViPNet Netzwerk

Wie aus den obigen Darlegungen folgt, können mit Hilfe der ViPNet Technologie VPN-Netzwerke in jedem verteilten IP-Netzwerk beliebiger Struktur aufgebaut werden. Diese Struktur kann globale, regionale und lokale Computernetzwerke vereinigen und die Rechner lokaler, mobiler und entfernter Benutzer einschließen. Lokale Netzwerke können dabei unterschiedliche dedizierte Netzwerksegmente umfassen – sowohl drahtgebundene als auch drahtlose.

Netzwerkknoten (Clients und Coordinatoren) können sich in jedem Teilbereich eines solchen Netzwerks befinden und über private IP-Adressen verfügen, die nicht untereinander abgestimmt sind und welche nicht in globalen oder regionalen Netzwerken geroutet werden können. Die Clients und Coordinatoren haben dabei die Möglichkeit, zueinander erlaubte (sanktionierte) geschützte Verbindungen der Art „peer-to-peer" für beliebige Netzwerkanwendungen aufzubauen.

Ein VPN-Netzwerk auf Basis der ViPNet Technologie kann als anpassungsfähig bezeichnet werden. Die Netzwerkknoten registrieren automatisch Informationen über die Zugangsparameter für andere Knoten und leiten diese Daten über das Netzwerk weiter. Bei Änderungen der Parameter sowohl des physikalischen als auch des virtuellen Netzwerks passt sich das ViPNet Netzwerk selbständig an diese Änderungen an. Es gewährleistet einen transparenten Schutz des Traffics bei der Weiterleitung von Nachrichten vom Sender zum Empfänger, unabhängig davon, wer der Initiator der entsprechenden Verbindung war.

Auf jedem ViPNet Netzwerkknoten wird Client- oder Coordinator-Software installiert, die für die Verschlüsselung des Traffics durch Sitzungsschlüssel sorgt (dabei wird jedes IP-Paket mit einem einmaligen, abgeleiteten Schlüssel verschlüsselt, siehe das Dokument „ViPNet Technologie. Allgemeine Informationen"). Jedes IP-Paket wird für das nachfolgende Routing des Traffics auf den Coordinatoren

mit eindeutigen Bezeichnern (ID) des Senders und des Empfängers ausgestattet. Diese Bezeichner werden nicht verschlüsselt, sondern durch Message Authentication Codes (MAC) geschützt.

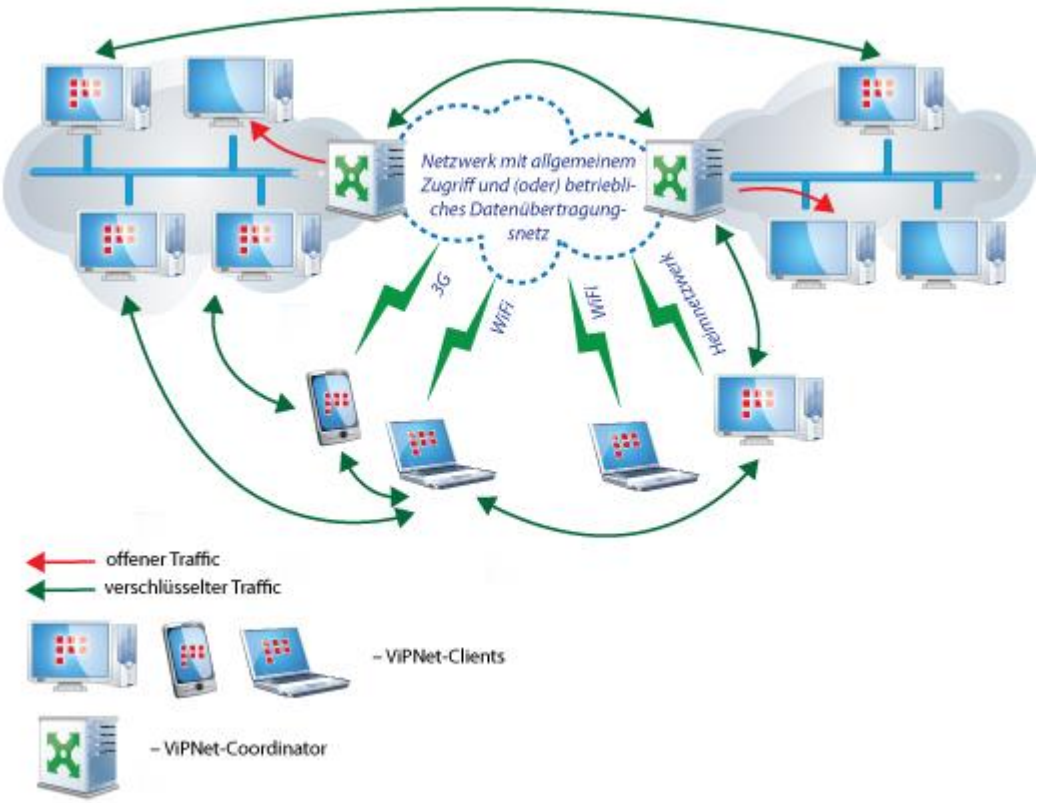

Abbildung 1. Netzwerk auf Basis der ViPNet-Technologie

Informationen über ViPNet Knoten, über ihre Zugangsparameter und aktuelle Aktivitäten erhält jeder Client von seinem Coordinator, der für den betroffenen Client die Funktionen eines IP-Adressenservers (s. IP-Adressenserver auf S. 21) erfüllt. Coordinatoren gewährleisten die Zustellung dieser Daten an andere Knoten.

Jeder Coordinator bekommt Informationen über andere Netzwerkknoten von den Coordinatoren, mit denen er verbunden ist.

Das Herstellen der Verbindungen zwischen den Clientknoten wird folgendermaßen durchgeführt:

- Vor dem Aufbauen der Verbindung zu einem anderen Knoten bestimmt der Client zunächst den Zugangskanal zu seinem Verbindungsserver. Wenn der Client dabei feststellt, dass er über ein NAT-Gerät verbunden wird, dann hält er den Verbindungskanal aufrecht, indem er regelmäßig IP-Pakete an den Coordinator sendet. Das Intervall für den Versand der IP-Pakete an den Verbindungsserver beträgt standardmäßig 25 Sekunden. Dieser Zeitraum ist im Regelfall ausreichend, um mit den meisten NAT-Geräten zu arbeiten. Bei Bedarf kann das Intervall (Timeout) auch geändert werden.
- Nachdem die Verbindung zwischen dem Client und seinem Verbindungsserver hergestellt wird, beginnt der Client, die Verbindung zu einem anderen Knoten herzustellen. Er beginnt, Test-IP-Pakete an den entfernten Knoten über seinen Verbindungsserver zu übermitteln. Der Client übermittelt Test-IP-Pakete gleichzeitig an den Verbindungsserver des entfernten Knotens und direkt an den entfernten Knoten.

- Wenn die Testpakete vom Remoteknoten erfolgreich empfangen wurden, dann wird diese Verbindung vom Remoteknoten registriert. Der Remoteknoten beginnt, Antwortpakete direkt an den Client zu senden. Nach dem Empfang dieser Antwortpakete des Remoteknotens beginnt der Client ebenfalls, alle folgenden IP-Pakete direkt an den Remoteknoten zu übermitteln.

  Wenn die Testpakete nur den Verbindungsserver des Remoteknotens erreicht haben, dann registriert der Verbindungsserver die erfolgte Verbindung und leitet die Antwortpakete des Remoteknotens direkt an den Client weiter.

  Das heißt, mit dem entfernten Knoten wird eine direkte Verbindung oder eine Verbindung über einen Verbindungsserver aufgebaut. Kommt der Rückverkehr von IP-Daten vom entfernten Knoten oder vom seinem Verbindungserver nicht, erfolgt die Verbindung des Clients mit dem entfernten Knoten nach wie vor über seinen Verbindungsserver.

Abbildung 2. Kommunikation der Netzwerkknoten

Auf diese Weise versuchen die Knoten, eine Verbindung unter Verwendung der kürzesten Route ohne Verwendung der Coordinatoren herzustellen, wodurch die Geschwindigkeit beim Austausch des verschlüsselten IP-Traffic erhöht wird.

Hinweis. Die nachfolgend aufgeführte Reihenfolge der Schritte zum Herstellen der Verbindung kann nur dann angewendet werden, wenn auf allen betroffenen Knoten die Software ViPNet der Version 4.2.x oder höher verwendet wird.

Zusätzlich gibt es die folgenden Besonderheiten beim Aufbau von Verbindungen im Netzwerk:

- Wenn sich die Knoten (sowohl Clients als auch Coordinatoren) in einem gerouteten Netzwerk befinden, dann werden die Verbindungen zwischen den Clients in Übereinstimmung mit den vorgegebenen Routen über die Netzwerkgateways hergestellt (und nicht über die Coordinatoren).
- Wenn sich der Remoteknoten, zu dem die Verbindung hergestellt werden soll, nicht hinter einem NAT-Gerät befindet, dann wird vom System sofort gemerkt, dass eine direkte Verbindung möglich ist. Bei nachfolgenden Verbindungen werden keine Testpakete mehr versendet, der IP-Traffic wird sofort direkt an den Remoteknoten weitergeleitet (vorausgesetzt, der Standort des Remoteknotens hat sich nicht geändert).

- Wenn sich die Clients, zwischen denen eine Verbindung aufgebaut wird, hinter Geräten mit dynamischem NAT befinden, dann können die Clients ebenfalls eine direkte Verbindung zueinander herstellen. Dies ist deswegen möglich, weil die Informationen zu den IP-Adressen und Ports, die für den Zugang zu anderen Knoten über NAT-Geräte verwendet werden können, von den Verbindungsservern an die Clients weitergeleitet werden. Diese Daten werden von den Coordinatoren anhand der empfangenen Clientpakete ermittelt.

  Wenn die Clients über diese Daten verfügen, dann können sie Testpakete unter Verwendung der ermittelten IP-Adressen und Ports aneinander senden. Falls die Testpakete zumindest von einer Seite erfolgreich empfangen werden, wird der gesamte IP-Traffic von nun an direkt zwischen den Clients weitergeleitet. D. h. die Technologie der direkten Verbindung wird dann angewendet, wenn zumindest ein NAT-Gerät beim Versand von IP-Paketen seines Clients an unterschiedliche IP-Adressen immer den gleichen dedizierten Port für den Client bereitstellt.

  Eine direkte Verbindung zwischen zwei Clients ist dann nicht möglich, wenn die NAT-Geräte beider Clients beim Versand von IP-Paketen an unterschiedliche IP-Adressen jedes Mal einen zufälligen Port dafür zur Verfügung stellen. Auf diese Art funktioniert die sogenannte symmetrische NAT. In diesem Fall wird die Verbindung zwischen den beiden Clients über einen der Verbindungsserver hergestellt.
- Die Möglichkeit einer direkten Verbindung zu einem Remoteknoten, der sich hinter einem Gerät mit dynamischem NAT befindet, bleibt standardmäßig während einer Zeitspanne von 75 Sekunden (drei Timeouts oder Sendeintervalle der IP-Pakete) ab dem Zeitpunkt der Unterbrechung der letzten Verbindung erhalten.
- Wenn sich der Client hinter einem Gerät mit statischem NAT befindet, dann sollte der korrekte Port für die Kapselung der UDP-Pakete in den Einstellungen des Clients angegeben werden. Anderenfalls ändert sich der Port fortwährend, wodurch eine Verbindung des Clients zu den anderen Knoten verhindert wird.

Verbindungsprotokolle im privaten Netzwerk

ViPNet Netzwerkknoten können in Netzwerken beliebigen Typs untergebracht werden, solange diese das IP-Protokoll unterstützen. Die Art der Anbindung an das Netzwerk kann unterschiedlich sein: Ethernet-Netzwerk, PPPoE über eine XDSL-Verbindung, PPP über eine Dial-up- oder ISDN-Verbindung, Mobilfunknetze GPRS oder UMTS, Wi-Fi-Einrichtungen, MPLS- oder VLAN-Netze. ViPNet Software unterstützt eine Vielzahl an Protokollen der Datensicherungsschicht (Data Link Layer). Zum Herstellen von geschützten Verbindungen zwischen den Netzwerkknoten werden IP-Protokolle dreier Typen (IP/241, UDP und TCP) verwendet. Die Pakete beliebiger anderer IP-Protokolle werden in diese Protokolle verpackt.

Für die Kommunikation der ViPNet-Netzwerkknoten untereinander wird das Protokoll IP/241 (auf S. 22) verwendet, falls sich diese Knoten im gleichen Segment des lokalen Netzwerks befinden und über

Broadcast-Адресса erreichbar sind. Dieses Protokoll ist effizienter, da es keinen UDP-Header (8 Bytes) verwendet. Das Originalpaket wird nach der Verschlüsselung in ein Paket des IP-Protokolls 241 verpackt.

Abbildung 3. Zwischen den Netzwerkknoten befindet sich keine Firewall

Wenn sich die ViPNet Knoten in unterschiedlichen Netzwerksegmenten befinden, dann wird automatisch das Protokoll UDP verwendet, das es den IP-Paketen ermöglicht, solche Firewalls zu passieren. Das Originalpaket wird nach der Verschlüsselung in ein UDP-Paket verpackt.

Abbildung 4. Die Netzwerkknoten werden über eine Firewall miteinander verbunden

Wenn entlang der Route eines IP-Pakets ein NAT-Gerät vorkommt, dann sollten dynamische oder statische NAT-Regeln auf diesem Gerät konfiguriert werden, die den Austausch von UDP-Traffic mit ViPNet Netzwerkknoten erlauben. Beim Konfigurieren von statischen Regeln sollte der UDP-Kapselungsport angegeben werden. Standardmäßig wird der Port 55777 verwendet, bei Bedarf kann aber ein anderer Port angegeben werden. Wenn die Pakete direkt über den Coordinator geleitet werden, dann ist die Portnummer der Knoten, die sich hinter dem Coordinator befinden, nicht von Bedeutung. Nachdem die Pakete den Coordinator durchlaufen haben, werden diesen Paketen die IP-Adressen der entsprechenden Coordinator-Netzwerkadapter zugewiesen (d. h. es wird Netzwerkadressenübersetzung durchgeführt).

Es kommt vor, dass die Kommunikation der geschützten Knoten über das UDP-Protokoll nicht möglich und die Übermittlung der UDP-Pakete vom Provider verboten ist. Beispiel: Remoteverbindungen zum ViPNet Netzwerk aus einem Internetcafe, Hotel oder aus anderen öffentlichen Plätzen. In diesem Fall kann der gesamte IP-Traffic über einen TCP-Tunnel geleitet werden. Dieser TCP-Tunnel kann auf dem Verbindungsserver des Knotens, der als Initiator der Verbindung auftritt, eingerichtet werden. Bei der Konfiguration des TCP-Tunnels auf dem Verbindungsserver (auf S. 23) sollte ein Port angegeben werden. Standardmäßig wird der Port 443 verwendet.

Abbildung 5. Die Netzwerkknoten werden über eine Firewall miteinander verbunden

Auf dem Verbindungsserver werden die empfangenen TCP-Pakete in UDP-Pakete umgewandelt und an den Zielknoten weitergeleitet über das UDP-Protokoll.

Knoten an das ViPNet Netzwerk anbinden

Dank des Protokolls für das dynamische Routing des VPN-Traffic, das in ViPNet Netzwerken eingesetzt wird, sind für die schnelle Anbindung eines neuen Knotens an das VPN-Netzwerk minimale Einstellungen erforderlich. Zum Hinzufügen eines neuen Knotens in die bestehende Netzwerkstruktur sollten Sie:

- einen neuen Knoten im Programm ViPNet Network Manager anlegen,
- für den neuen Knoten zulässige Verbindungen zu anderen ViPNet Knoten definieren,
- die Zugangsadresse zum Coordinator oder den DNS-Namen des Coordinators, auf welchem der neue Knoten registriert ist, sowie die Art der Verbindung zum ViPNet Netzwerk definieren.

Das Herstellen einer Verbindung auf einem Client erfolgt über einen Verbindungsserver (auf S. 23). Informationen über andere Knoten, deren Zugangsparameter und den Status bekommen sie von ihrem IP-Adressen Server. Standardmäßig agiert der IP-Adressenserver (auf S. 21) auch als Verbindungsserver, Sie können das aber bei Bedarf ändern und einen andren Coordinator als Verbindungsserver auswählen. Die Verbindungsparameter bekommen die Clients automatisch ebenso von ihrem Verbindungsserver.

Um die Aufgaben des Verbindungsservers zu erfüllen, tauschen die Coordinatoren die Informationen über andere ViPNet Netzwerkknoten unter einander aus. Um die Verfügbarkeit der Coordinatoren für Clients und andere Coordinatoren zu gewährleisten, ist es wichtig, die richtige Art seiner Verbindung mit dem externen Netzwerk auszuwählen:

- Wenn der Coordinator über eine IP-Adresse im Internet verfügt, dann kann der Verbindungstyp **Ohne Firewall** verwendet werden.
- Wenn der Coordinator sich in einem lokalen Netz befindet, an dessen Grenze ein anderer Coordinator vorhanden ist, sollte der Firewall-Typ **Coordinator** verwendet werden.
- Wenn dem Coordinator keine öffentliche IP-Adresse zugeteilt ist und er mit dem externen Netzwerk über ein Gerät kommuniziert, auf dem die statische IP-Adressenübersetzung konfiguriert werden kann, sollte man der Verbindungstyp **Mit statischem NAT** auswählen.
- Wenn der Coordinator mit dem externen Netzwerk über ein Gerät verbunden wird, auf dem nur dynamische und keine statische IP-Adressenübersetzung möglich ist, verwenden Sie der Verbindungstyp **Mit dynamischem NAT**. In diesem Fall sollte im Netzwerk zumindest ein Coordinator – eine Art Hauptcoordinator – installiert sein, der über offenen Zugang zu diesem Gerät verfügt (d. h. der Verbindungstyp des Coordinators zum Netzwerk sollte entweder **Ohne Firewall** oder **Mit statischem NAT** sein).

Bei den Netzwerkknoten mit der ViPNet Client Windows Software spielt die Art der Verbindung mit dem externen Netzwerk keine Rolle. Sie verbinden sich mit den anderen Knoten automatisch nach den kürzesten verfügbaren Kommunikationswegen. Zum Herstellen einer Verbindung greifen sie auf Verbindungsserver zu.

Hinweis. Im ViPNet Network Manager ist die Art der Verbindung über eine Firewall für einen Client immer noch auswählbar, was die Kompatibilität des Programms mit der Software ViPNet Client 4.1 und deren früheren Versionen gewährleistet.

Bei mobilen Geräten ist es sinnvoll, der Verbindungstyp **Mit dynamischem NAT** zu verwenden. Dieser Verbindungstyp erlaubt es dem Benutzer, sich zum ViPNet Netzwerk sowohl von seinem lokalen Netzwerk als auch von Zuhause oder aus dem Hotel aus zu verbinden, ohne dass die Einstellungen jedes Mal zusätzlich angepasst werden müssten.

In einzelnen Fällen kann es passieren, dass der Verbindungstyp für den mobilen Client geändert werden muss. Zum Beispiel, wenn der mobile Benutzer aus seinem lokalen Netzwerk, in welchem sich sein Coordinator befindet, in das lokale Netzwerk einer Filiale seiner Firma oder in ein Partnernetzwerk, zu welchem Verbindungen erlaubt sind und welches von einem Coordinator geschützt wird, übersiedelt. In diesem Fall sollte auf dem mobilen Client der Verbindungstyp **Coordinator** gewählt und der Coordinator des neuen Netzwerks angegeben werden. Damit die Einstellungen nicht jedes Mal beim Wechseln zu einem anderen Netzwerk geändert werden müssen, können auf dem mobilen Client mehrere voreingestellte Konfigurationen angelegt werden, zum Beispiel „ViPNet VPN in Berlin" oder „ViPNet VPN in Düsseldorf". Beim Eintreffen in der jeweiligen Filiale muss der Benutzer lediglich die richtige Konfiguration auswählen und kann anschließend seine Arbeit ungehindert fortsetzen.

Aber nichtdestotrotz sind die Verbindungsarten nicht an bestimmte Verwendungsszenarien gebunden. Beim Definieren des Verbindungstyps auf einem stationären Netzwerkknoten sollten folgende Verbindungseigenschaften beachtet werden:

- Die Verbindungstypen **Ohne Firewall** und **Coordinator** unterscheiden sich aus technologischer Sicht von den beiden anderen Typen dadurch, dass Daten über Zugangsmöglichkeiten zum betroffenen Knoten auf Remoteknoten anders registriert werden.

  Bei den beiden ersten Verbindungstypen wird die Registrierung auf Basis von kryptografisch geschützten Systeminformationen durchgeführt, die zusammen mit dem eingetroffenen VPN-Paket weitergeleitet wird. Bei Verbindungstyp **Mit statischem NAT** und **Mit dynamischem NAT** werden die Zugangsinformationen anhand der IP-Adresse und des Ports des VPN-Paketabsenders registriert. Diese Daten werden offen übertragen. Dies hat keine Auswirkungen auf die Sicherheit der Verbindungen. Nichtsdestotrotz sind die Verbindungstypen **Ohne Firewall** und **Coordinator** widerstandsfähiger gegenüber Störungsversuchen durch mögliche Attacken, die auf Änderungen der IP-Adresse oder des Ports des Paketabsenders abzielen. Ungeachtet einer solchen Substitution werden Antwortpakete während der Verbindung immer an die Adresse und den Port weitergeleitet, die im Rumpf des VPN-Pakets enthalten sind und nicht geändert werden können.

  Angesichts dieser Überlegungen scheint es angemessen, für den Coordinator den Verbindungstyp **Ohne Firewall** zu verwenden, wenn es eine externe IP-Adresse (s. Externe IP-Adressen auf S. 21) gibt, über die der Coordinator aus dem Internet angesprochen werden kann (ob statisch oder dynamisch (s. Dynamische IP-Adresse auf S. 20) vergeben). Wenn es keine solche IP-Adresse gibt oder wenn es sich um einen anderen Fall handelt, können bei Bedarf auch die restlichen, nicht weniger sicheren Verbindungstypen verwendet werden.

- Wenn innerhalb des ViPNet Firmennetzwerks geschützte Segmente (s. Netzwerksegment auf S. 21)geschaffen werden, die über einen Zugang zum externen Netzwerk verfügen sollen, oder wenn

die Notwendigkeit besteht, den VPN-Traffic über eine bestimmte Route weiterleiten zu lassen, dann können die Coordinatoren in einer Kette aufgestellt werden (Kaskadenschema), wobei der Verbindungstyp **Coordinator** verwendet werden sollte. Dann gelangt der Traffic aus einem inneren Segment ohne weitere Routing-Einstellungen in das externe Netzwerk. Der Traffic wird von einem Coordinator zum nächsten weitergeleitet und bleibt für andere Teilnehmer des Firmennetzwerks, in welchem sich das betroffene geschützte Segment befindet, unzugänglich. Die Kaskadenlänge unterliegt dabei keinen Einschränkungen.

Anbindung ohne Verwendung einer Firewall

Dieser Verbindungstyp wird normalerweise auf dem Coordinator verwendet, falls der Coordinator über eine externe IP-Adresse verfügt. Dabei muss diese Adresse nicht unbedingt statisch (s. Statische IP-Adresse auf S. 22) sein, die IP-Adresse kann auch dynamisch (s. Dynamische IP-Adresse auf S. 20) sein. In diesem Fall sollte die Technologie „Dynamisches DNS" verwendet werden. Im Programm ViPNet Network Manager muss dabei die Adresse des gegebenen Coordinators in Form eines DNS-Namens definiert werden.

Die Netzwerkknoten, die diesen Verbindungstyp verwenden, verbinden sich miteinander stets direkt über das Protokoll IP/241 (auf S. 22). Hierbei wird der verschlüsselte Traffic dieser Clients zu Coordinatoren sowie zu Clients, die einen Coordinator als Firewall verwenden, immer in UDP-Pakete verpackt.

Es wird davon abgeraten, diesen Verbindungstyp auf Clients zu verwenden, da es zu Problemen beim Knotenzugang aus externen Netzwerken führen kann.

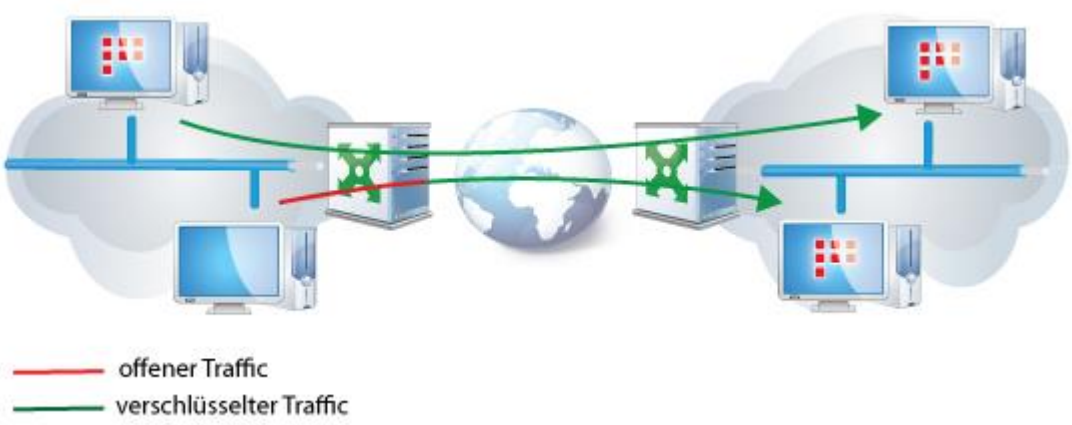

Abbildung 6. Coordinator führt die Tunnelung und die Adressumsetzung für Verbindungen durch

Der Coordinator routet die VPN-Pakete anderer Netzwerkknoten in Übereinstimmung mit den Bezeichnern der Empfängerknoten und leitet sie über das Netzwerk weiter. Den VPN-Paketen wird dabei die IP-Adresse des Netzwerkadapters (und Ports) des Coordinators zugewiesen.

Wenn der Coordinator die Funktion eines tunnelnden Servers (VPN-Gateways (s. Tunnelnder Coordinator auf S. 23)) erfüllt, dann wird der offene Traffic einer vordefinierten Computergruppe im lokalen Netzwerk (im Allgemeinen der Datenverkehr beliebiger IP-Geräte: IP-Telefone, Webkameras und andere) vom Netzwerkadapter des Coordinators empfangen, verschlüsselt und in VPN-Pakete verpackt. Anschließend werden diese Pakete an andere Coordinatoren für die eventuelle Weitergabe an dort getunnelte Geräte

oder Clients geleitet. Den VPN-Paketen wird dabei die IP-Adresse des Netzwerkadapters (und Ports) des Coordinators zugewiesen.

Anbindung über Coordinator

Wenn an der Grenze des lokalen Netzwerks (s. Grenze des lokalen Netzwerkes auf S. 21) ein ViPNet Coordinator als Gateway aufgestellt ist, dann wird es empfohlen, diesen Coordinator als Firewall für die Clients des lokalen Netzwerks zu konfigurieren. In diesem Fall wird der gesamte verschlüsselte Traffic zwischen diesem Client und den Knoten des externen Netzwerks über den Coordinator geleitet. Der Coordinator übernimmt auf diese Weise die Rolle eines Routers für verschlüsselte Pakete, mit eingebauter Funktion der Adressenübersetzung.

Das automatische Routing der verschlüsselten IP-Pakete auf dem Coordinator wird vom ViPNet Treiber durchgeführt. Die Routingtabellen (s. Routingtabelle auf S. 22) des TCP/IP-Stacks, die im Betriebsystem definiert sind, werden dazu nicht verwendet. Das standardmäßig verwendete Gateway und die im TCP/IP-Stack definierten Routen werden nach der Installation von ViPNet Software nicht modifiziert. Das Routing von nicht verschlüsselten IP-Paketen bleibt dadurch unverändert.

Auf den Clients kann im Programm ViPNet Client als Firewall der Coordinator ausgewählt werden, der nicht bereits als IP-Adressenserver für den gegebenen Client auftritt.

Diese Möglichkeit kann für einen mobilen ViPNet Benutzer, der sich in einem anderen ViPNet Netzwerk befindet, von Nutzen sein. Damit der mobile Benutzer auf das ViPNet Netzwerk zugreifen kann, genügt es, als Firewall den Coordinator auszuwählen, der im jeweiligen lokalen Netzwerk installiert ist.

Zusätzlich wird ein Backup der Coordinatoren im Netzwerk sichergestellt. An der Grenze des lokalen Netzwerks kann ein weiterer Coordinator installiert werden. Wenn der vordefinierte Coordinator nicht verfügbar ist, kann ein anderer Coordinator aus der Liste ausgewählt werden, und die Arbeit kann fortgesetzt werden.

Segment des lokalen Netzwerks schützen

Wenn der Datenverkehr eines bestimmten Segments des lokalen Netzwerks geschützt werden soll, und sich an der Grenze des Netzwerks bereits ein ViPNet Coordinator befindet, der die Funktionen einer Firewall für die ViPNet Clients dieses lokalen Netzwerks erfüllt, dann kann an der Grenze des betroffenen Segments ein zweiter ViPNet Coordinator aufgestellt werden, hinter dem sich ebenfalls Clients befinden können.

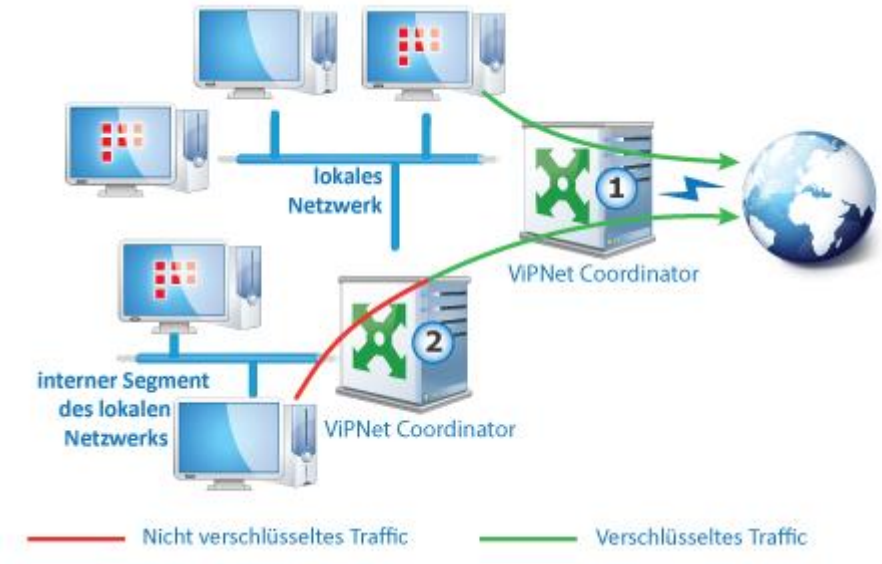

Abbildung 7. Verwendung des Coordinators als eine Firewall

Dabei sollte Coordinator 1 (s. Abbildung oben) als Firewall für Coordinator 2 definiert werden. Zwischen den beiden Coordinatoren sollten sich keine Geräte befinden, die Adressumsetzung (NAT) durchführen.

Diese Aufstellung der Coordinatoren wird als Kaskade bezeichnet. Die Anzahl der Kaskaden ist nicht beschränkt. Dadurch wird für die Coordinatoren das automatische Routing des verschlüsselten Traffics aus dem internen Netzwerksegment sowohl in das lokale als auch in das globale Netzwerk sichergestellt.

Verbindungstyp „Mit dynamischem NAT“

Wenn der Traffic mehrerer Knoten des lokalen Netzwerks geschützt werden soll, und das lokale Netzwerk dabei Verbindungen zum externen Netzwerk über ein Gerät herstellt, das zwar die Adressumsetzung (NAT) durchführt, auf welchem die Einstellung statischer NAT-Regeln aber nur schwer möglich ist, dann wird empfohlen, im lokalen Netzwerk vor dem NAT-Gerät einen ViPNet Coordinator aufzustellen und auf diesem Coordinator den Verbindungstyp mit dynamischer Adressenübersetzung zu konfigurieren. In diesem Fall sollte für alle ViPNet Clients des lokalen Netzwerks die Datenweiterleitung über den Coordinator konfiguriert werden. Bei getunnelten Geräten sollte beim Einstellen des Standardgateways die interne IP-Adresse des Coordinators (s. Interne IP-Adressen auf S. 21) angegeben werden.

Damit ein Knoten, für welchen der Verbindungstyp mit dynamischer Adressenübersetzung ausgewählt wurde, mit externen Knoten über ein NAT-Gerät kommunizieren kann, sollte im externen Netzwerk ein Coordinator zur Verfügung stehen, der über eine öffentliche IP-Adresse (auf S. 22) erreichbar ist (ohne Firewall oder über Firewall mit statischem NAT). Wenn einen mobilen Client über Firewall mit dynamischem NAT funktioniert und sich gleichzeitig im lokalen Netzwerk eines solchen Coordinators befindet, dann wird die die Verbindung des Clients wird nach den gleichen Regeln durchgeführt, die bei Verbindungen über den Coordinator anzuwenden sind.

Abbildung 8. Verbindung über eine Firewall mit dynamischem NAT

Der Verbindungstyp mit dynamischem NAT stellt einen universellen Typ dar un kann in verschiedenen Situationen verwendet werden. Die Hauptaufgabe dieser Lösung besteht jedoch darin, eine sichere zweiseitige Verbindung zu geschützten Knoten zu gewährleisten, die über eine Firewall oder ein NAT-Gerät mit dem externen Netzwerk kommunizieren, auf dem das Einstellen der statischen NAT-Regeln unmöglich oder nur schwer möglich ist (auch dann, wenn fehlende Benutzerrechte der Grund dafür sind). Diese Situation kann typischerweise dann auftreten, wenn einfachste NAT-Netzwerkgeräte wie zum Beispiel DSL-Modems oder WLAN-Basisstationen eingesetzt werden, oder wenn ein gemeinsamer Zugang zum Internet (ICS — Internet Connection Sharing, Internetverbindungsfreigabe) im Betriebssystem Windows verwendet wird. Des Weiteren ist es schwierig, die Konfiguration von NAT-Regeln auf Firewalls vorzunehmen, die bei einem Provider eingerichtet sind (bei Heimnetzwerken, GPRS-Netzen, 3G, 4G, bei öffentlichen Wi-Fi-Netzwerken und anderen Netzwerken, bei denen der Provider eine private IP-Adresse zur Verfügung stellt).

Alle NAT-Geräte gewährleisten standardmäßig die Weiterleitung des UDP-Traffics dank der automatischen Definition sogenannter dynamischer NAT-Regeln für den eingehenden Traffic. Diese Regeln werden anhand der Parameter von ausgehenden, vom NAT-Gerät durchgelassenen IP-Paketen erstellt.

Ein Beispiel: mehrere ausgehende IP-Pakete gleichen Typs passieren das NAT-Gerät. Für diese Pakete wird auf dem NAT-Gerät eine dynamische Regel erstellt. Alle eingehenden Pakete, deren Parameter den Werten dieser dynamischen Regel entsprechen, werden innerhalb einer gewissen Zeitspanne (timeout) nach dem Durchgang des letzten ausgehenden Pakets vom NAT-Gerät durchgelassen. Nach Ablauf dieses Zeitintervalls wird die dynamische Regel gelöscht, und das NAT-Gerät beginnt, die eingehenden Pakete wieder zu blockieren.

Dies bedeutet, dass eine externe Quelle keine Verbindungen zu einem Netzwerkknoten initiieren kann, der sich hinter einem solchen NAT-Gerät befindet. Der interne Knoten muss von Zeit zu Zeit ausgehende Pakete an den externen Knoten weiterleiten, um die dynamische Regel im aktiven Zustand zu halten. Standardmäßig beträgt der Zeitabstand zwischen den Sendevorgängen 25 Sekunden. Dadurch kann jeder externe ViPNet Knoten jederzeit IP-Pakete über den Coordinator der eingehenden Verbindungen an den Netzwerkknoten senden, der sich hinter dem NAT-Gerät befindet. Dabei werden die ausgehenden Antwortpakete des Netzwerkknotens vorbei am eigenen Coordinator für eingehende Verbindungen

immer direkt an den externen Knoten weitergeleitet (wenn der externe ViPNet Knoten keine Firewall mit dynamischem NAT verwendet). Nach Erhalt des ersten Pakets fängt der externe Knoten (falls er keine Firewall mit dynamischem NAT verwendet) ebenfalls an, den gesamten Traffic direkt an den Netzwerkknoten hinter dem NAT-Gerät weiterzuleiten. Auf diese Weise entsteht ein direkter UDP-Datenaustausch zwischen zwei ViPNet Knoten.

Diese Technologie ermöglicht es, einen permanenten Zugang zu ViPNet Knoten zu gewährleisten, die über NAT-Geräte kommunizieren (da die dynamischen Regeln auf den NAT-Geräten dabei nicht gelöscht werden). Außerdem wird eine hohe Geschwindigkeit beim Austausch von verschlüsselten Daten gewährleistet, da der Traffic nur bei der Initialisierung über die Coordinatoren der eingehenden Verbindungen geleitet wird. Der nachfolgende Datenaustausch erfolgt direkt zwischen den Knoten (Abbildung oben). Es muss berücksichtigt werden, dass der ausgehende Traffic eines Netzwerkknotens, der eine Firewall mit dynamischem NAT verwendet, an einen anderen Knoten immer über den Coordinator der eingehenden Verbindungen des anderen Knotens weitergeleitet wird.

Verbindungstyp „Mit statischem NAT“

Wenn an der Grenze des lokalen Netzwerks (s. Grenze des lokalen Netzwerkes auf S. 21) zum externen Netzwerk eine Firewall aufgestellt ist, die die Übersetzung von Netzwerkadressen (NAT) durchführt und auf welcher statische Regeln der Adressenübersetzung definiert werden können, dann sollte zwischen dieser Firewall und den Knoten des lokalen Netzwerks ein Coordinator eingerichtet werden. Auf dem Coordinator sollten in diesem Fall die Parameter der Verbindungen über eine Firewall mit statischem NAT konfiguriert sein. Für die Clients des lokalen Netzwerks sollte der gegebene Coordinator als Verbindungsserver verwendet werden.

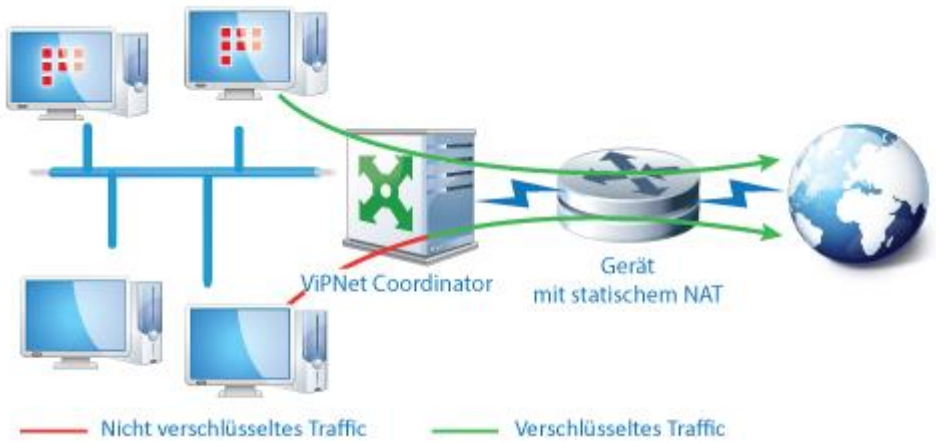

Abbildung 9. Verbindung des Coordinators über eine Firewall mit statischem NAT

Für ordnungsgemäße Verbindungen über eine Firewall mit statischem NAT sollte die IP-Adresse der verwendeten Firewall in den Betriebssystemeinstellungen des Netzwerkknotens als Standardgateway definiert werden. Auf der Firewall selbst sollten folgende statische Regeln der Adressumsetzung konfiguriert werden:

- ausgehende UDP-Pakete mit Adressen und Ports von Netzwerkknoten, die sich hinter der Firewall befinden, durchlassen.

- eingehende UDP-Pakete mit einem Zielport, der in den Einstellungen der Clients als Port der UDP-Kapselung definiert ist, durchlassen und umleiten;

Achtung! Wenn mehrere Netzwerkknoten ein und dieselbe Firewall mit statischer Adressumsetzung benutzen, sollte für jeden Netzwerkknoten eine eigene UDP-Kapselungsportnummer definiert werden. Falls ein und dieselbe Portnummer von mehreren Netzwerkknoten verwendet wird, können Konflikte auftreten.

Virtuelle IP-Adressen

Bei Verbindungen entfernter Benutzer zu Objekten im lokalen Netzwerk oder beim Sicherstellen der Interaktion lokaler Netzwerke unter Verwendung der VPN-Technologie stellt sich die Frage der richtigen Verteilung von IP-Adressen. Die Verteilung von Adressen sollte so vorgenommen werden, dass mögliche Konflikte von vornherein ausgeschlossen sind: auf einem gegebenen Knoten sollten die IP-Adressen aller entfernter Knoten unterschiedlich sein.

In klassischen VPN-Systemen wird diese Aufgabe beim Verbinden lokaler Netzwerke ausschließlich durch Koordination der Adressbereiche der lokalen Netzwerke untereinander gelöst. Beim Bereitstellen eines Remotezugangs unter Verwendung unterschiedlicher VPN-Technologien wird auf dem Clientcomputer normalerweise ein virtueller Adapter erstellt, der beim Herstellen einer Verbindung zum VPN-Gateway eine IP-Adresse erhält. Damit mehrere VPN-Verbindungen zu mehreren VPN-Gateways hergestellt werden können, um den Zugang zu unterschiedlichen lokalen Netzwerken einzurichten, müssen mehrere virtuelle Adapter erstellt werden.

Diese Lösungen weisen eine Reihe von Nachteilen auf:

- Es ist nicht immer möglich, die Verteilung von Adressen in unterschiedlichen lokalen Netzwerken gegenseitig abzustimmen.

  Bei zentralisierter Zuordnung von Adressen an virtuelle Adapter bleibt auf dem VPN-Gateway die Wahrscheinlichkeit eines Konflikts mit dem Subnetzwerk, in welchem sich der Computer des Benutzers physikalisch befindet, erhalten. In einem solchen Fall bleibt das Netzwerk funktionsunfähig. Beim Herstellen von Verbindungen zu unterschiedlichen Gateways ist es ebenfalls schwierig, Konfliktsituationen zu vermeiden.

  In den angeführten Fällen werden die Adressen aus dem Bereich privater IP-Adressen vergeben, was mit hoher Wahrscheinlichkeit zu einer Überschneidung von IP-Adressbereichen führen kann.

- Auf den Clients werden ausschließlich jene Daten verschlüsselt, die zum virtuellen Adapter gelangen. Die Verwaltung der Verschlüsselung wird auf eine sehr unsichere Weise organisiert: durch Konfiguration von Routingtabellen im TCP/IP-Stack (s. Routingtabelle auf S. 22).

In ViPNet Technologie wird eine prinzipiell andere Methode zur Vermeidung von Konfliktsituationen beim Herstellen von VPN-Verbindungen verwendet.

Die Vermeidung von Konflikten wird durch Einsatz virtueller IP-Adressen erzielt. Auf jedem ViPNet Netzwerkknoten wird jedem Remoteknoten und jeder getunnelten IP-Adresse entfernter Coordinatoren eine eigene virtuelle IP-Adresse zugeordnet, die auf dem gegebenen Computer einmalig ist. Virtuelle IP-Adressen werden nicht anhand von IP-Adressen, sondern anhand von eindeutigen Bezeichnern (ID) der Netzwerkknoten zugewiesen. Für jeden Knoten wird genau die Menge an virtuellen IP-Adressen zugeteilt, die der Anzahl reeller Adressen (s. Reelle IP-Adresse auf S. 22) dieses Knotens zum gegebenen Zeitpunkt entspricht. Die jeder getunnelten statischen reellen IP-Adresse des Coordinators zugeordnete virtuelle IP-Adresse existiert, solange es die tatsächliche reelle IP-Adresse gibt. Jedem Bereich getunnelter reeller IP-Adressen wird ein Bereich virtueller Adressen zugewiesen. Der virtuelle IP-Adressbereich existiert, solange es den entsprechenden Bereich reeller getunnelter IP-Adressen des Coordinators gibt.

Beim Auftreten von Konfliktsituationen im Zuge der Interaktion mit Remotecomputern zwingt der ViPNet Treiber die Anwendungen auf dem Computer dazu, die zugeteilten virtuellen IP-Adressen zu verwenden. Dadurch bestehen keine Einschränkungen bei der Struktur von Adressen in unterschiedlichen Subnetzen, IP-Adressen müssen nicht mehr aufeinander abgestimmt werden, die Wahrscheinlichkeit von Konflikten wird bei jedem entfernten Benutzer ausgeschlossen.

Darüber hinaus müssen auf dem Client keine virtuellen Adapter mehr erstellt werden. Die Parameter des TCP/IP-Stacks haben keinen Einfluss mehr auf die Vorgänge der Verschlüsselung. Der ViPNet Treiber fängt den gesamten Traffic ab, deswegen wird jedes IP-Paket verschlüsselt. Die Schlüssel für die Verschlüsselung werden vom ViPNet Treiber aufgrund erhaltener Daten über die IP-Adressen aller Empfänger festgelegt. Dementsprechend wird die Verschlüsselung des Traffics in jede Richtung ohne jegliche vorhergehende Konfiguration des Computers automatisch durchgeführt. Das Routing des Traffics für virtuelle IP-Adressen wird ebenfalls innerhalb des ViPNet Treibers in Übereinstimmung mit der IP-Adresse des zum Empfänger nächstgelegenen Zugangsknotens ausgeführt.

Glossar

C

Coordinator (ViPNet Coordinator)

Netzwerkknoten mit installierter ViPNet Coordinator Software.

D

Datei (Transportdatei)

Dienstinformation, die innerhalb des ViPNet Netzwerkes verwendet wird und durch das MFTP-Modul übermittelt wird.

Dynamische IP-Adresse

IP-Adresse, die dem Computer von einem DHCP-Server zugewiesen wird.

Dynamisches NAT

Diese Technologie ermöglicht eine dynamische Zuweisung von externen Adressen an die Netzwerkknoten aus dem lokalen Netzwerk, wenn diese Verbindungen mit externen Netzwerkknoten aufbauen. Die Netzwerkknoten des externen Netzwerkes können keine Verbindungen zu den Netzwerkknoten des lokalen Netzwerkes initiieren, wenn deren externe Adressen dynamisch zugewiesen werden.

E

Externe IP-Adressen

Die Adressen eines externen Netzwerkes.

G

Grenze des lokalen Netzwerkes

Ein abstrakter Begriff, der einen Übergang von einem LAN in ein WAN oder in ein anderes LAN symbolisiert.

H

Hinter dem Coordinator (der Netzwerkknoten hinter dem Coordinator)

Der Netzwerkknoten, der den Coordinator als Gateway für die verschlüsselten Verbindungen verwendet: alle verschlüsselten IP-Pakete werden von diesem Computer ausschließlich über den Coordinator an die externen Netzwerke versendet.

I

Interne IP-Adressen

Die Adressen eines lokalen Netzwerkes.

IP-Adressenserver

Eine der Funktionen des ViPNet Coordinators. Ermöglicht die Registrierung und Vermittlung der Anschlussinformationen der Netzwerkknoten („online, „offline und Art des Internetanschlusses).

N

Netzwerksegment

Ein Netzwerksegment ist ein Teil eines größeren, zusammenhängenden Netzwerkes, das logisch und/oder physisch vom Rest des Netzwerkes getrennt ist.

O

Öffentliche IP-Adresse

Eine IP-Adresse des Computers, die in den öffentlichen (globalen) Netzwerken (z.B. Internet) eingesetzt werden kann.

P

Protokoll IP/241

Ein speziell für ViPNet entwickeltes IP-Protokoll mit der Protokollnummer 241.

R

Reelle IP-Adresse

IP-Adresse, die dem Netzwerkadapter im LAN oder Internet zugewiesen ist.

Routingtabelle

Eine Routingtabelle ist eine elektronische Tabelle in einem Netzwerkgerät, typischerweise einem Computer oder einem Router. Mit Hilfe dieser Einträge kann das Netzwerkgerät entscheiden, über welche seiner Schnittstellen ein zu versendendes Datenpaket jeweils geschickt werden muss.

S

Statische IP-Adresse

Feste IP-Adresse, die einem Netzwerkobjekt zugewiesen ist.

Statisches NAT

Network Address Translation (NAT) ist in Computernetzen der Sammelbegriff für Verfahren, die automatisiert Adressinformationen in Datenpaketen durch andere ersetzen, um verschiedene Netze zu verbinden. Daher kommen sie typischerweise auf Routern zum Einsatz. Beim statischen NAT wird einen

feste Verbindung zwischen der externen IP-Adresse oder dem Port des internen Netzwerkknotens und der IP-Adresse oder dem Port in die sie übersetzt wird hergestellt.

T

Transportmodul (MFTP)

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

Tunnel

Eine gesicherte Verbindung zwischen einzelnen Netzwerkknoten.

Tunnelnder Coordinator

Eine der Funktionen des Coordinators, die im Programm ViPNet Network Manager (in ViPNet VPN-Netzwerke) oder ViPNet Network Control Center (in ViPNet Netzwerke basierte auf der Software ViPNet Administrator) aktiviert wird: der Coordinator tunnelt den IP-Traffic von oder zu den Netzwerkobjekten, die über keine ViPNet Client bzw. Coordinator Software verfügen. Dabei bleibt der IP-Traffic nur auf der Streke zwischen dem getunnelten Netzwerkobjekt und dem Coordinator unverschlüsselt.

V

Verbindungsserver

Eine Funktion des Coordinators, die die Verbindungen zwischen den Clients auch dann sicherstellt, wenn sich die Clients in unterschiedlichen Subnetzen befinden und keine direkten Verbindungen zueinander herstellen können. Für jeden Client kann ein eigener Verbindungsserver ausgewählt werden. Standardmäßig wird der IP-Adressenserver als Verbindungsserver des Clients festgelegt.

Virtuelle IP-Adresse

Die virtuelle IP-Adresse wird auf einem ViPNet Netzwerkknoten für die Gegenstelle generiert und ist an die ID-Nummer der Gegenstelle gebunden. Die Verwendung der virtuellen IP-Adressen ermöglicht es, IP-Adressen-Überschneidungskonflikte zu vermeiden und die reelle Topologie des Netzwerkes zu kaschieren.