Gemeinsame Verwendung von ViPNet VPN und Cisco IP-Telefonie

Anhang zum ViPNet VPN Benutzerhandbuch

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: 00121-06 90 02 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 4
Vorteile der Einrichtung eines ViPNet Netzwerks 4
Anforderungen an die Netzwerkstruktur 6
Allgemeine Hinweise 6
Konfiguration der Coordinatoren 7
Konfiguration der Clients 9
Konfiguration getunnelter Knoten 10
    Wenn sich geschützte und getunnelte Knoten im gleichen Netzwerksegment befinden 10
Konfiguration von Remoteclients 13
    Notebook des Remotebenutzers konfigurieren 13
    Desktopcomputer des Remotebenutzers konfigurieren 14
Überprüfung der Funktionalität der IP-Telefonie 15

Über dieses Dokument

Dieses Handbuch wendet sich an Netzwerkadministratoren, welche Cisco IP-Telefonie in einem ViPNet Netzwerk einrichten und konfigurieren.

Für die Installation von ViPNet VPN bedarf es keiner tiefgehenden Kenntnisse der Netzwerktechnologien. Ein gewisses Grundwissen über die Arbeit mit Netzwerken kann jedoch hilfreich sein.

Vorteile der Einrichtung eines ViPNet Netzwerks

Zum Schutz des Traffics der Cisco IP-Telefonie kann innerhalb der Organisation ein virtuelles privates ViPNet Netzwerk eingerichtet werden. Neben dem Schutz des Traffics hilft die ViPNet Technologie dabei, den Konfigurationsaufwand bei der Sicherstellung von Verbindungen zu Cisco-Remotebenutzern, Zweigniederlassungen und Partnerorganisationen zu minimieren und die Konfiguration des Firmennetzwerks zu vereinfachen.

Die Einrichtung eines privaten ViPNet Netzwerks bringt folgende Vorteile:

- Bei Übertragung über externe Netzwerke wird der VoIP-Traffic („voice over IP", IP-Telefonie) verschlüsselt.
- Innerhalb des Firmennetzwerks kann der VoIP-Traffic verschlüsselt oder offen übertragen werden.
- Festnetzbenutzer (PSTN – public switched telephone network) können problemlos mit Benutzern der IP-Telefonie kommunizieren, die im Büro oder per Fernzugriff arbeiten.

Hinweis. Beachten Sie, dass, wenn ein Remotebenutzer auf einem ungeschützten Rechner arbeitet, die Sicherheit der VoIP-PSTN Verbindung nicht garantiert werden kann.

- Remotebenutzer, die Verbindungen zum Internet mit Hilfe unterschiedlicher Zugriffspunkte herstellen, können für jede Verbindung eine eigene Konfiguration des Programms ViPNet Monitor erstellen. Dadurch können zusätzliche Einstellungen vermieden werden, und der Benutzer kann bei jeder Verbindung Anrufe aus dem Programm Cisco IP Communicator (CIPC) tätigen.
- Dank der Verwendung virtueller IP-Adressen behält ein Remotebenutzer beim Wechsel des Standorts seine sichtbare IP-Adresse. Dazu müssen keine Änderungen in den Einstellungen von Cisco CallManager vorgenommen werden.
- Die Verwendung virtueller IP-Adressen hilft, IP-Adressenkonflikte bei Verbindungen zu Knoten in anderen lokalen Netzwerken zu vermeiden.
- Die Kapselung aller Arten des geschützten Traffics in das einheitliche UDP-Paketformat hilft, die Konfiguration von Firewalls erheblich zu vereinfachen.

Das nachfolgende Schema zeigt das Beispiel einer Netzwerktopologie, in der abgesicherte IP-Telefonie von Cisco verwendet wird.

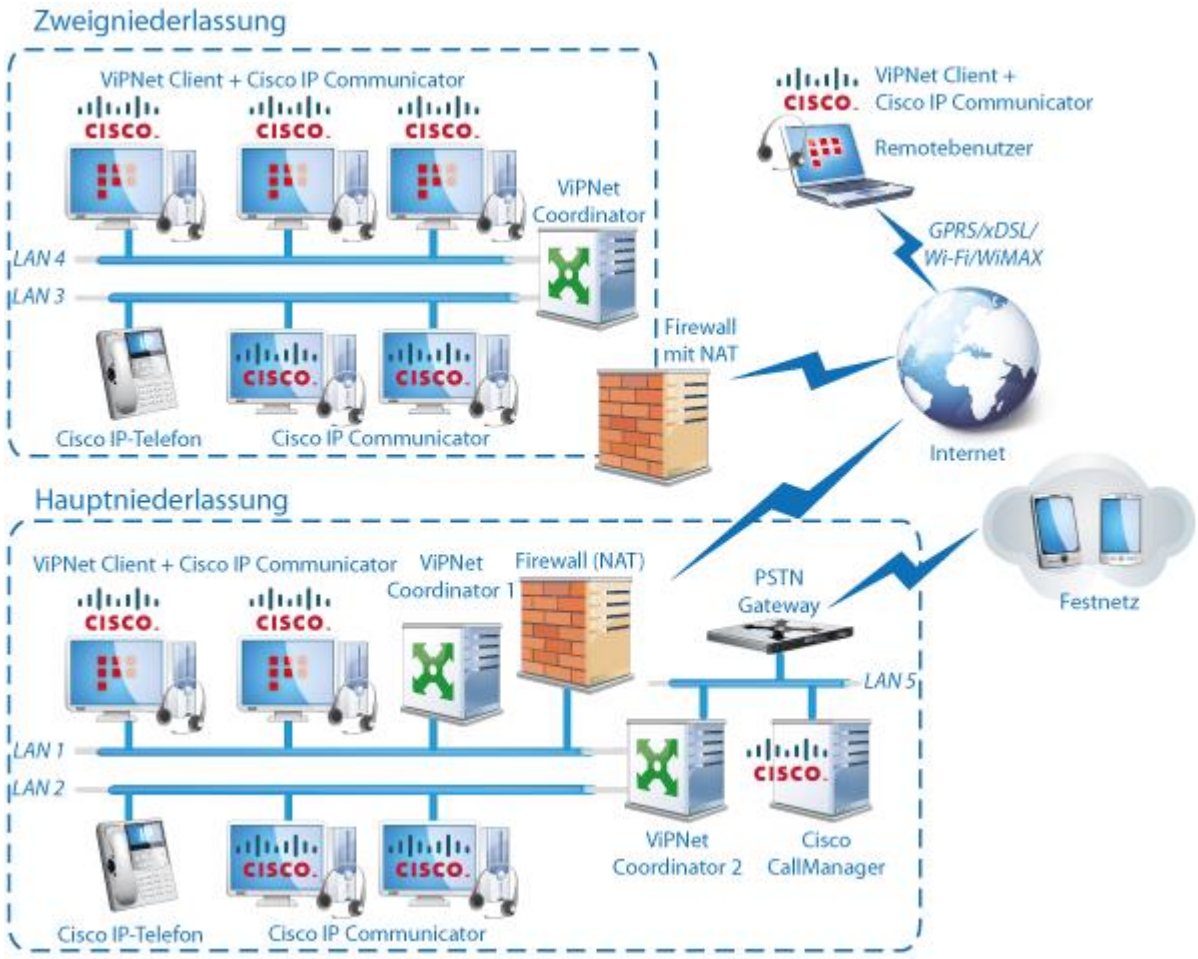

Abbildung 1. Schutz der IP-Telefonie von Cisco mit Hilfe von ViPNet OFFICE

Nehmen wir an, eine Organisation besteht aus einer Hauptniederlassung und zwei Zweigniederlassungen. Die Computer und Netzwerkgeräte, die sich in der Hauptniederlassung und in den Filialen befinden, können in zwei Typen unterteilt werden:

- ViPNet Netzwerkknoten mit Cisco-Software: Computer, auf denen die Programme ViPNet Client und Cisco IP Communicator installiert sind. Im Folgenden werden wir diese Rechner als ViPNet Netzwerkknoten bezeichnen.
- Offene Knoten: Computer, auf denen die Software Cisco IP Communicator, jedoch nicht ViPNet Client installiert ist; IP-Telefongeräte von Cisco; Server, auf denen die Software Cisco CallManager installiert ist. Im Folgenden werden wir diese Geräte als getunnelte Knoten bezeichnen.

Achtung! Aus Sicherheitsgründen sollten geschützte ViPNet Netzwerkknoten und getunnelte Knoten in unterschiedlichen Netzwerksegmenten untergebracht werden.

Wenn dies nicht möglich ist, sollten für den Schutz des Traffics innerhalb des lokalen Netzwerks zusätzliche Einstellungen vorgenommen werden (s. Wenn sich geschützte und getunnelte Knoten im gleichen Netzwerksegment befinden auf S. 10).

Remotebenutzer, die auf Notebooks mit installierter ViPNet Client- und Cisco IP Communicator-Software arbeiten, verbinden sich zum ViPNet Netzwerk über das Internet.

Das lokale Netzwerk der Hauptniederlassung ist über ein PSTN-Gateway mit dem Festnetz verbunden.

Das PSTN-Gateway und der Server Cisco CallManager befinden sich in einem separaten Netzwerksegment der Hauptniederlassung (LAN 5 in der Abbildung).

Anforderungen an die Netzwerkstruktur

Damit die Cisco IP-Telefonie effektiv geschützt werden kann, sollten folgende Bedingungen erfüllt sein:

1 Damit die Cisco IP-Telefonie effektiv geschützt werden kann, sollten folgende Bedingungen erfüllt sein:

- PSTN-Gateway, IP-Telefone von Cisco und Computer, auf denen Cisco IP Communicator, jedoch nicht ViPNet Client installiert ist, sollten vom Coordinator der eigenen Niederlassung getunnelt werden;
- der Server Cisco CallManager sollte sich hinter einem eigenen Coordinator (Coordinator 2) befinden (s. Abbildung 1 auf S. 5) und über eine eindeutige IP-Adresse verfügen.

Hinweis. Wenn im Netzwerk mehrere Cisco CallManager-Server installiert sind, und jedem Server unterschiedliche Benutzergruppen zugeordnet sind, ist es empfehlenswert, sich an den technischen Support der Infotecs GmbH zu wenden, um weitere Konfigurationsempfehlungen einzuholen.

---

2 Auf allen Computern mit installiertem Cisco IP Communicator sollte auch die Software ViPNet Client installiert sein (anderenfalls sollten diese Computer vom Coordinator der eigenen Niederlassung getunnelt werden, siehe Punkt **1**).

3 Auf allen Remotecomputern sollte die Software Cisco IP Communicator und ViPNet Client installiert sein.

Allgemeine Hinweise

Beim Einrichten und Konfigurieren des ViPNet Netzwerks sollte in jeder Niederlassung die folgende Reihenfolge der Konfigurationsschritte eingehalten werden:

1 Installieren Sie die Software ViPNet Coordinator und konfigurieren die Tunnelung offener Computer und Geräte, die am IP-Telefoniesystem teilnehmen sollen (s. Konfiguration der Coordinatoren auf S. 7).

Hinweis. Mehr über die Installation der ViPNet Coordinator Software lesen Sie in Kapitel 2 des Dokuments „ViPNet VPN. Benutzerhandbuch“ im Abschnitt „Installation von ViPNet Coordinator auf ViPNet Netzwerkserver“.

2 Installieren und konfigurieren Sie die ViPNet Client Software auf einzelnen PCs mit Cisco IP Communicator (s. Konfiguration der Clients auf S. 9). Wenn auf einigen PCs die Installation von ViPNet Client nicht möglich oder nicht erwünscht ist, sollten diese PCs getunnelt werden, siehe Punkt **3**.

Hinweis. Ausführliche Anleitungen zur Installation der Software ViPNet Client finden Sie im Dokument „ViPNet VPN. Benutzerhandbuch“, Kapitel 2, Abschnitt „Einrichtung der Benutzerarbeitsplätze im ViPNet Netzwerk“.

Die Konfiguration der Software ViPNet Client wird im Administratormodus durchgeführt.

3 Konfigurieren Sie alle getunnelten Knoten, die am IP-Telefoniesystem teilnehmen sollen (s. Konfiguration getunnelter Knoten auf S. 10). Auf den getunnelten Knoten sollte keine ViPNet Software installiert werden.

4 Installieren und konfigurieren Sie die Software ViPNet Client Software auf allen Remotecomputern, auf denen Cisco IP Communicator installiert ist (s. Konfiguration von Remoteclients auf S. 13).

5 Führen Sie Testanrufe von den Clients im Büro, von getunnelten Knoten und von Remotecomputern durch (s. Überprüfung der Funktionalität der IP-Telefonie auf S. 15).

Konfiguration der Coordinatoren

Führen Sie die folgenden Schritte durch, um den Coordinator zu konfigurieren:

1 Definieren Sie im Programm ViPNet Network Manager die Zugriffsparameter für den Coordinator (s. Dokument „ViPNet VPN. Benutzerhandbuch“, Kapitel 5, Abschnitt „Konfiguration der Coordinatoren“).

2 Geben Sie im Programm ViPNet Network Manager die IP-Adressen offener Knoten, die am IP-Telefoniesystem teilnehmen sollen, als getunnelte IP-Adressen an (s. Dokument „ViPNet VPN. Benutzerhandbuch“, Kapitel 5, Abschnitt „Tunnelung“).

3 Definieren Sie auf der Firewall, die sich an der Grenze des lokalen Netzwerks befindet, Routingregeln für den Traffic.

4 Führen Sie auf dem Coordinator die folgenden Netzwerkeinstellungen durch:

- Wenn der Coordinator über eine Firewall mit dem Internet verbunden ist, geben Sie die Firewall-Parameter an (s. Dokument „ViPNet VPN. Benutzerhandbuch“, Kapitel 5, Abschnitt „Firewall des Coordinators“).
- Wenn der Coordinators über einen Netzwerkadapter direkt mit dem Internet verbunden ist, geben Sie für diesen Netzwerkadapter das Gateway des Internet-Anbieters als Standardgateway

an. Definieren Sie für alle anderen Netzwerke, mit denen der Coordinator verbunden ist, statische Routen, sodass die IP-Pakete für diese Netzwerke an die jeweiligen Gateways geleitet werden.

5 Definieren Sie im Programm ViPNet Coordinator Monitor auf dem Coordinator 2 (s. Abbildung 1 auf S. 5) in der Hauptniederlassung einen Transitfilter, um die Verbindungen zwischen den getunnelten Knoten, die sich hinter unterschiedlichen Netzwerkadaptern befinden, sicherzustellen. Dazu:

Hinweis. Im betrachteten Beispiel (s. Abbildung 1 auf S. 5) sollte einen Transitfilter konfiguriert werden, um das Subnetz LAN 2, in dem sich offene Computer mit installierter Cisco IP Communicator-Software und Cisco IP-Telefongeräte befinden, mit dem Subnetz LAN 5, in dem sich der Server Cisco CallManager und das PSTN-Gateway befinden, zu verbinden.

- Wählen Sie in der Panel-Ansicht den Bereich **Netzwerkfilter** > **Transit-Filter des offenen Netzwerk**.
- Klicken Sie auf **Erstellen**.
- Legen Sie im eingeblendeten Fenster im Bereich **Allgemeine Optionen** den Namen und das Verhalten des Filters (Traffic erlauben) fest.
- Klicken Sie im Bereich Quellen auf Hinzufügen und wählen **IP-Adresse oder Adressbereich**.

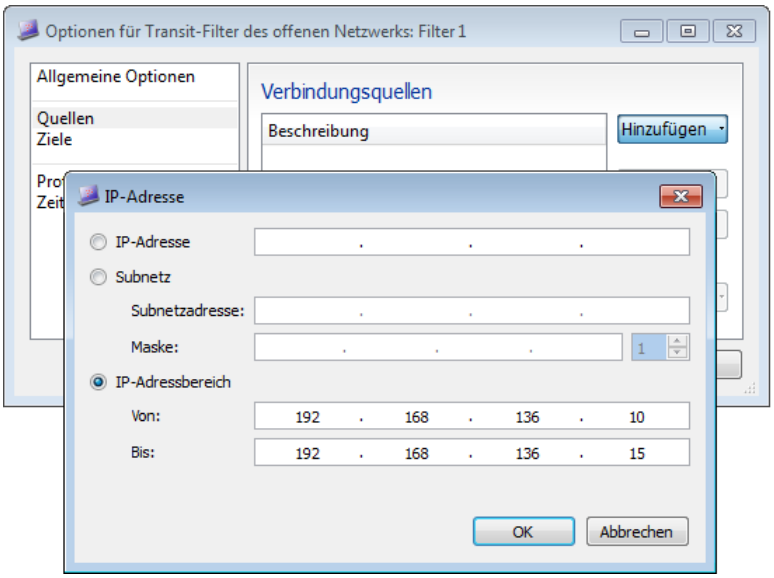

Abbildung 2. Transitfilter erstellen

- Wählen Sie **IP-Adressbereich** im Fenster **IP-Adresse** und geben die Anfangs- und die End-IP-Adresse aus dem IP-Adressenbereich getunnelter Knoten im Subnetz LAN 2 an. Klicken Sie auf **OK**.
- Geben Sie im Bereich **Ziele** die IP-Adressen getunnelter Knoten des Subnetzes LAN 5 an (Cisco CallManager-Server und PSTN-Gateway).

6 Wenn in den lokalen Netzwerken der Hauptniederlassung und der Zweigniederlassungen die gleichen IP-Adressen verwendet werden, dann führen Sie im Programm ViPNet Coordinator Monitor

für alle Coordinatoren, die im Bereich **Privates Netzwerk** aufgelistet sind, die folgenden Schritte durch, um IP-Adressenkonflikte zu vermeiden:

- Doppelklicken Sie im Bereich **Privates Netzwerk** auf einen der Coordinatoren. Es wird das Fenster **Netzwerkknoten-Eigenschaften** geöffnet.
- Öffnen Sie die Registerkarten **Tunnel** und aktivieren das Kontrollkästchen **Virtuelle IP-Adresse verwenden** (standardmäßig deaktiviert).

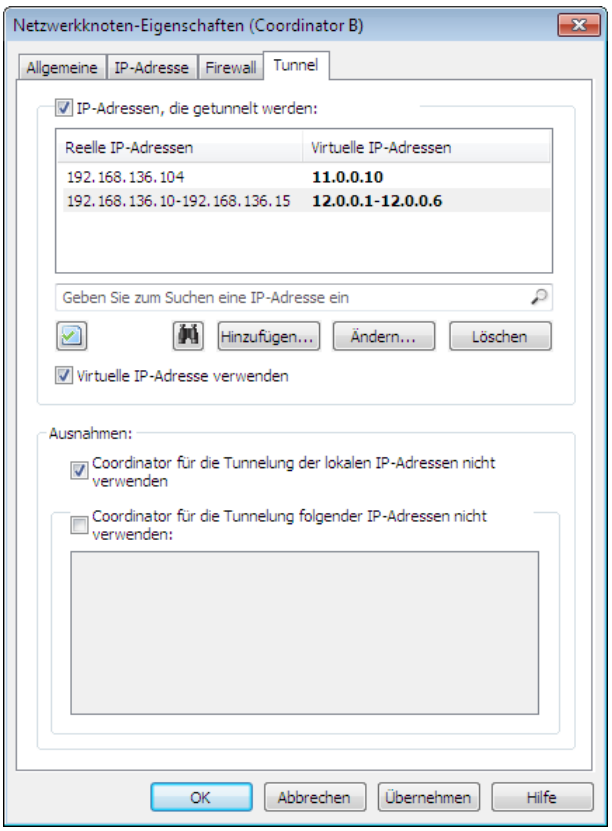

Abbildung 3. Virtuelle IP-Adressen verwenden

Konfiguration der Clients

Führen Sie auf jedem Client in der Haupt- oder Zweigniederlassung die folgenden Einstellungen durch:

1. Melden Sie sich im Programm ViPNet Client Monitor als Administrator an.
2. Zum Vermeiden von IP-Adressenkonflikten führen Sie für jeden Coordinator im Bereich **Privates Netzwerk** die folgenden Einstellungen durch:
   - Doppelklicken Sie im Bereich **Privates Netzwerk** auf einen der Coordinatoren. Es wird das Fenster **Netzwerkknoten-Eigenschaften** geöffnet.
   - Öffnen Sie die Registerkarte **Tunnel** (s. Abbildung 3 auf S. 9) und aktivieren das Kontrollkätschen **Virtuelle IP-Adresse verwenden** (standardmäßig deaktiviert).

Konfiguration getunnelter Knoten

Achtung! Aus Sicherheitsgründen sollten geschützte ViPNet Netzwerkknoten und getunnelte Knoten in unterschiedlichen Netzwerksegmenten untergebracht werden.

Wenn dies nicht möglich ist, sollten für den Schutz des Traffics innerhalb des lokalen Netzwerks zusätzliche Einstellungen vorgenommen werden (s. Wenn sich geschützte und getunnelte Knoten im gleichen Netzwerksegment befinden auf S. 10).

Führen Sie folgende Schritte durch, um die getunnelten Knoten zu konfigurieren:

1 Legen Sie in jedem lokalen Netzwerk auf allen getunnelten Knoten (mit Ausnahme des Cisco CallManager-Servers und des PSTN-Gateways) die IP-Adresse des Coordinators, der sich in diesem lokalen Netzwerk befindet, als Standardgateway fest. Wenn der Coordinator nicht als Standardgateway eingesetzt werden kann, gehen Sie zu Schritt **2** über.

Hinweis. Wenn sich die getunnelten Knoten im gleichen Subnetz befinden, erfolgt der Datenaustausch direkt ohne Beteiligung des Coordinators.

2 Führen Sie in der Hauptniederlassung die Einstellungen für das Subnetz, in dem sich der Cisco CallManager-Server und das PSTN-Gateway befinden, durch.

Der Coordinator kann nicht als Standardgateway für den Cisco CallManager-Server eingesetzt werden, da für Verbindungen zum Festnetz das PSTN-Gateway als Standardgateway definiert werden muss.

Um dieses Problem zu lösen, sollte auf dem Cisco CallManager-Server eine statische Route konfiguriert werden, die den Traffic zwischen dem Cisco CallManager-Server und dem Netzwerk der Hauptniederlassung über den Coordinator umleitet.

Wenn sich geschützte und getunnelte Knoten im gleichen Netzwerksegment befinden

Standardmäßig werden Verbindungen von Clients zu getunnelten Knoten im gleichen Netzwerksegment direkt aufgebaut. Damit der Zugriff auf die getunnelten Knoten kontrolliert werden kann, können die Clients so konfiguriert werden, dass sie Verbindungen zu getunnelten Knoten über den Coordinator aufbauen. Dazu:

1 Führen Sie auf jedem Client, der sich im gegebenen Netzwerksegment befindet, im Programm ViPNet Monitor die folgenden Schritte durch:

- Wählen Sie in der Navigationsleiste den Bereich **Privates Netzwerk**.
- Doppelklicken Sie im Bereich **Privates Netzwerk** auf den tunnelenden Coordinator dieses Subnetzes. Es wird das Fenster **Netzwerkknoten-Eigenschaften** geöffnet.

- Deaktivieren Sie auf der Registerkarte **Tunnel** in Gruppe **Ausnahmen** das Kontrollkästchen **Coordinator für die Tunnelung der lokalen IP-Adressen nicht verwenden** (standardmäßig aktiviert).

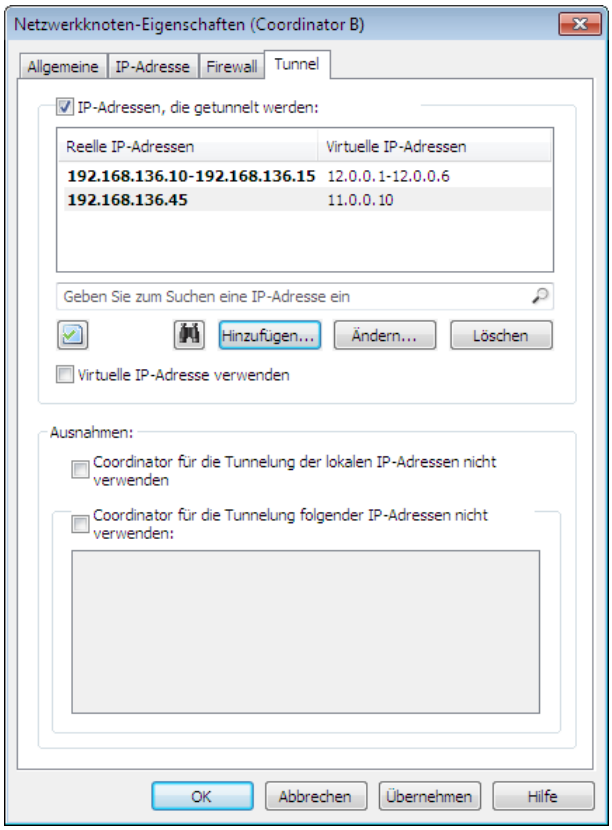

Abbildung 4. Subnetz mit geschützten und getunnelten Knoten konfigurieren

- Wenn der Datenaustausch zwischen dem gegebenen Client und einem bestimmten getunnelten Knoten direkt erfolgen soll, dann führen Sie die folgenden Schritte durch:
  - Aktivieren Sie in Gruppe **Ausnahmen** das Kontrollkästchen **Coordinator für die Tunnelung folgender IP-Adressen nicht verwenden**.

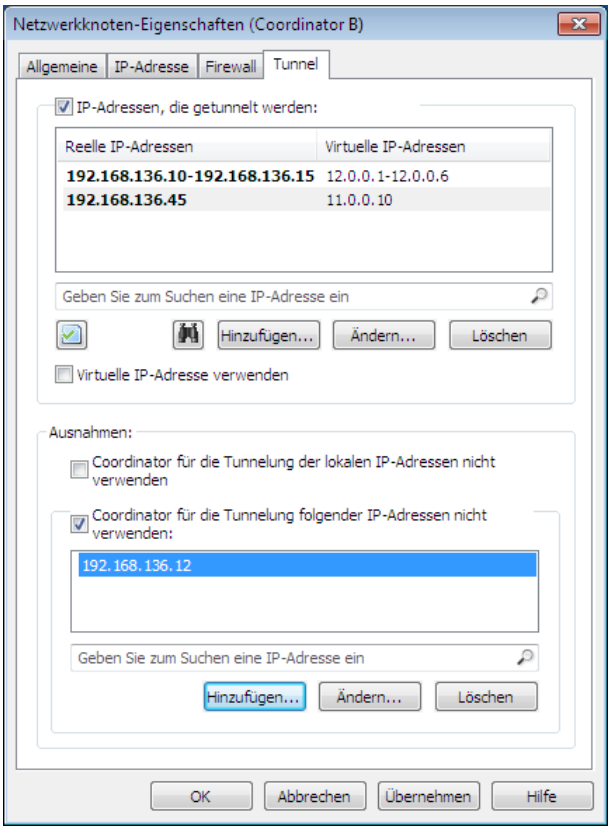

Abbildung 5. Definieren der IP-Adressen, die getunnelt nicht werden

- Klicken Sie auf **Hinzufügen**. Das Fenster **IP-Adresse oder Bereich hinzufügen** öffnet sich.

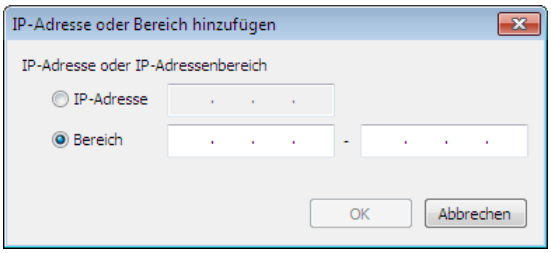

Abbildung 6. IP-Adresse eingeben

- Wählen Sie im Fenster **IP-Adresse oder Bereich hinzufügen** die Option **Bereich** und dann geben die Anfangs- und die End-IP-Adresse aus dem IP-Adressenbereich, der nicht getunnelt werden soll, an. Klicken Sie auf **OK**.

o Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

2 Definieren Sie auf jedem getunnelten Knoten eine statische Route, damit der Datenaustausch zwischen diesem Knoten und den Clients über den Coordinator geleitet wird.

3 Definieren Sie auf jedem Client eine statische Route, damit der Datenaustausch zwischen diesem Client und den getunnelten Knoten über den Coordinator geleitet wird.

Konfiguration von Remoteclients

Die Remotebenutzer können auf einem Notebook oder auf einem Desktopcomputer arbeiten.

Notebook des Remotebenutzers konfigurieren

Ein Remotebenutzer, der mit einem Notebook arbeitet, verbindet sich an unterschiedlichen Standorten zum Internet und verwendet dazu unterschiedliche Verbindungstypen. Damit ViPNet Software nicht bei jeder Verbindung zum geschützten Netzwerk neu konfiguriert werden muss, ist es empfehlenswert, mehrere Konfigurationen des Programms ViPNet Monitor für unterschiedliche Verbindungstypen anzulegen. Für den Zugang zum ViPNet Netzwerk wird es genügen, eine passende Konfiguration auszuwählen.

Zum Anlegen einer neuen Konfiguration:

1 Melden Sie sich in Programm ViPNet Client Monitor als Administrator an.

2 Klicken Sie im Hauptfenster von ViPNet Client in der Navigationsleiste mit der rechten Maustaste auf den Bereich **Konfigurationen** und wählen im Kontextmenü den Punkt **Konfiguration erstellen**.

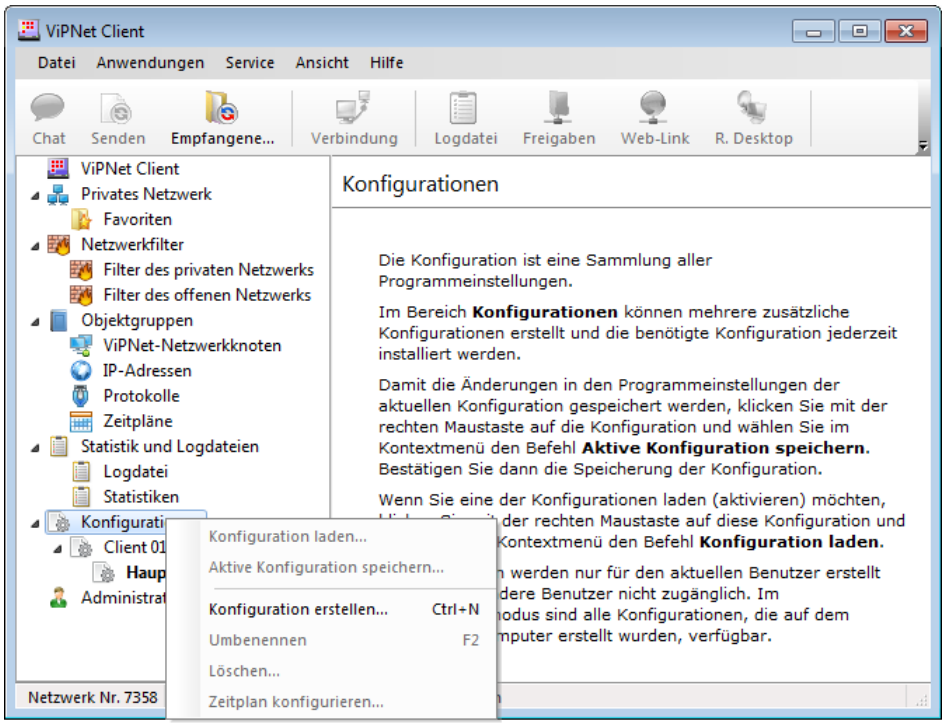

Abbildung 7. Neue Konfiguration erstellen

In der Liste der Konfigurationen wird der Order „Neue Konfiguration" eingeblendet. Die aktuellen Programmeinstellungen werden automatisch in der neuen Konfiguration gespeichert.

3 Es wird empfohlen, die neu angelegte Konfiguration umzubenennen, damit sie leichter in der Liste gefunden werden kann. Wählen Sie dazu die gewünschte Konfiguration aus und drücken die Taste

F2 oder klicken mit der rechten Maustaste auf die Konfiguration und wählen im Kontextmenü den Punkt **Umbenennen**.

4 Zum Speichern der Konfiguration klicken Sie in der Navigationsleiste mit der rechten Maustaste auf **Konfigurationen** und wählen im Kontextmenü den Eintrag **Aktuelle Konfiguration speichern**.

Es wird empfohlen, die folgenden Konfigurationen anzulegen und zu speichern:

- Erstellen Sie eine Konfiguration mit den Einstellungen für die Arbeit im lokalen Netzwerk der Niederlassung. Diese Einstellungen stimmen mit den Einstellungen der Clients, die in der Niederlassung arbeiten, überein (s. Konfiguration der Clients auf S. 9).
- Erstellen Sie eine Konfiguration für Verbindungen zum ViPNet Netzwerk über das Internet, falls außerhalb der Niederlassung gearbeitet wird.

Zum Vermeiden von IP-Adressenkonflikten können in jeder Konfiguration zusätzlich die folgenden Schritte durchgeführt werden:

1 Wählen Sie im Hauptfenster des Programms ViPNet Client in der Navigationsleiste den Bereich **Privates Netzwerk**.

2 Doppelklicken Sie im Bereich **Privates Netzwerk** auf Ihren Coordinator. Das Fenster **Netzwerknoten-Eigenschaften** wird geöffnet.

3 Aktivieren Sie im Fenster **Netzwerkknoten-Eigenschaften** auf der Registerkarte **Tunnel** (s. Abbildung 3 auf S. 9) das Kontrollkätschen **Virtuelle IP-Adressen verwenden** (standardmäßig deaktiviert).

Desktopcomputer des Remotebenutzers konfigurieren

Ein Remotebenutzer, der auf einem Desktopcomputer arbeitet, verbindet sich zum ViPNet Netzwerk über das Internet. Sein Standort ändert sich dabei nicht. Zum Konfigurieren eines Desktopcomputers führen Sie die folgenden Schritte durch:

1 Melden Sie sich in Programm ViPNet Client Monitor als Administrator an.

2 Zum Vermeiden von IP-Adressenkonflikten:

   - Wählen Sie im Hauptfenster des Programms ViPNet Client Monitor in der Navigationsleiste den Bereich **Privates Netzwerk**.
   - Doppelklicken Sie im Bereich **Privates Netzwerk** auf Ihren Coordinator. Das Fenster **Netzwerkknoten-Eigenschaften** wird geöffnet.
   - Aktivieren Sie im Fenster **Netzwerkknoten-Eigenschaften** auf die Registerkarte **Tunnel** (s. Abbildung 3 auf S. 9) das Kontrollkätschen **Virtuelle IP-Adresse verwenden** (standardmäßig deaktiviert).

Überprüfung der Funktionalität der IP-Telefonie

Nach erfolgter Installation des ViPNet Firmennetzwerks, nach der Konfiguration von Coordinatoren, Clients und getunnelten Knoten sollte sichergestellt werden, dass das Cisco IP-Telefoniesystem ordnungsgemäß funktioniert. Führen Sie dazu die folgenden Schritte durch:

1. Stellen Sie sicher, dass Cisco-Geräte und -Software korrekt installiert und konfiguriert sind.
2. Überprüfen Sie die Verbindung zwischen den Clients und ihren Coordinatoren sowie zwischen den verschiedenen Coordinatoren.
3. Falls keine Verbindung aufgebaut werden konnte, stellen Sie sicher, dass die IP-Adressen aller ViPNet Netzwerkknoten richtig definiert sind und dass alle Netzwerkknoten über korrekte Verbindungseinstellungen verfügen.
4. Überprüfen Sie mit Hilfe des Befehls ping, ob die getunnelten Knoten von Clients und anderen getunnelten Knoten, die sich im lokalen Netzwerk einer anderen Niederlassung befinden, angesprochen werden können.

   Falls keine Verbindungen zu getunnelten Knoten aufgebaut werden können, stellen Sie sicher, dass auf den Coordinatoren die Tunnelung eingestellt ist und auf den getunnelten Knoten die Standardgateways und die statischen Routen richtig konfiguriert sind.
5. Führen Sie Testanrufe von Clients in den Niederlassungen, von getunnelten Knoten und von Remotecomputern durch.

   Wenn alle Einstellungen ordnungsgemäß durchgeführt wurden, steht nun das firmeninterne IP-Telefoniesystem von Cisco für den Einsatz zur Verfügung.