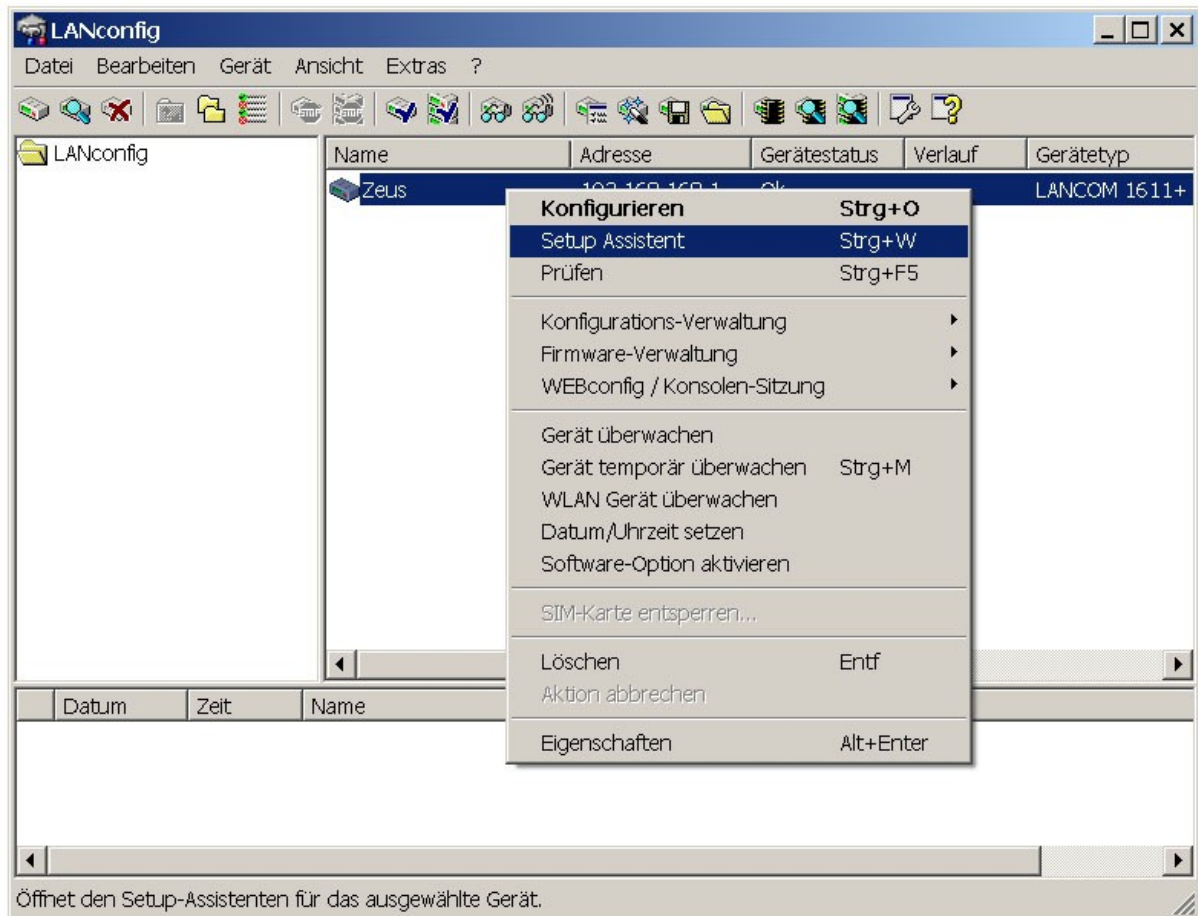
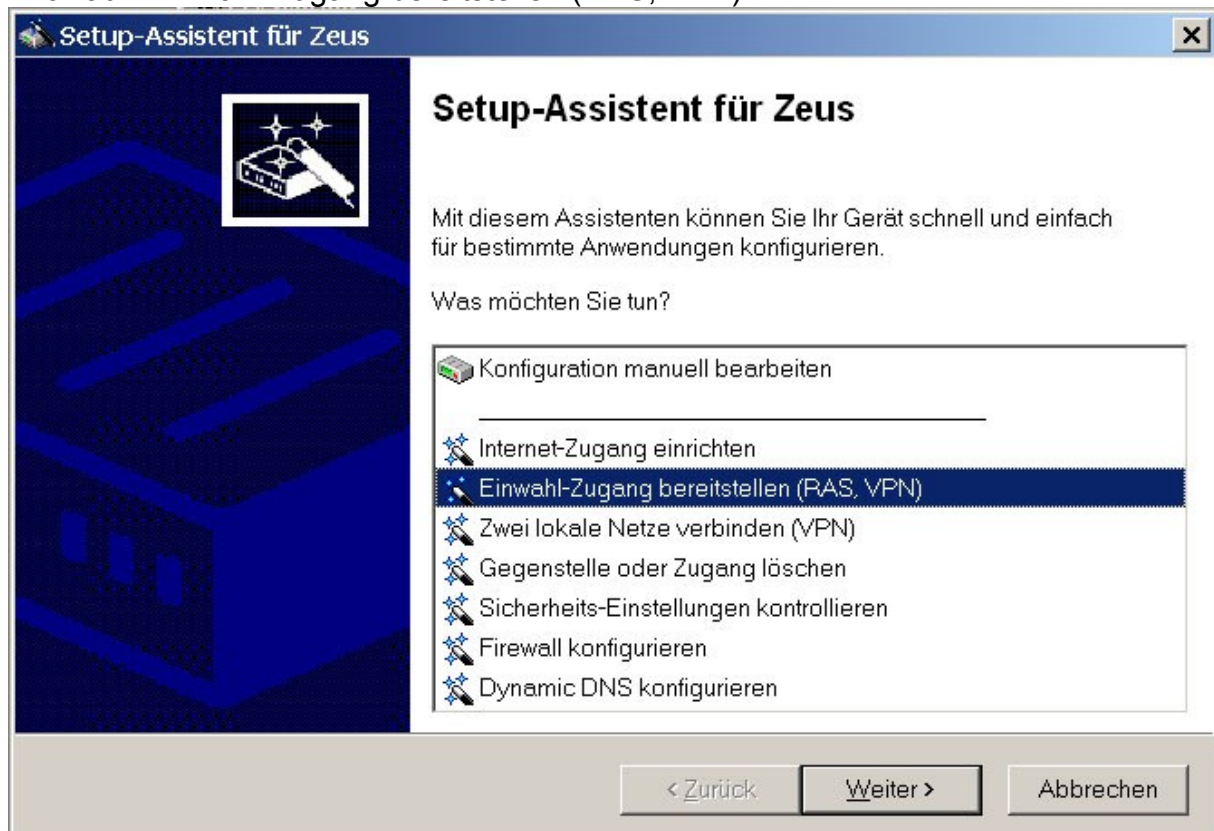


Lancom 1611+ VPN Konfiguration für Shrew VPN-Client

LANconfig öffnen, Router markieren und mit rechter Maustaste den Setup Assistenten anwählen...



Klick auf "Einwahl-Zugang bereitstellen (RAS, VPN)"



"VPN-Verbindung über das Internet" wählen...

Setup-Assistent für Zeus

Einwahl-Zugang bereitstellen (RAS, VPN)
Welche Art von Einwahlzugang möchten Sie bereitstellen?

Dieser Assistent hilft Ihnen bei der Einrichtung eines Einwahlzugangs (Remote-Access-Service, kurz RAS). Damit können Sie beispielsweise einem Mitarbeiter die Möglichkeit geben, sich von außen in Ihr Firmennetz einzuwählen.

Mit Ausnahme der direkten ISDN-Einwahl wird der Einwahlzugang über VPN (Virtual Private Network) hergestellt. So wird sichergestellt, dass Ihre Daten von Dritten nicht mitgelesen werden können, auch wenn die Übertragung über das Internet stattfindet.

Es sind in Abhängigkeit vom Zugangsweg unterschiedliche Einstellungen vorzunehmen.

Welche Art von Einwahlzugang möchten Sie bereitstellen:

VPN-Verbindung über das Internet

Direkte ISDN-Einwahl (ohne VPN)

< Zurück Weiter > Abbrechen

"VPN-Client mit benutzerdefinierten Parametern" wählen...

Setup-Assistent für Zeus

Einwahl-Zugang bereitstellen (RAS, VPN)
Wählen Sie den VPN-Client für diese Verbindung


In Abhängigkeit vom verwendeten VPN-Client werden einige Informationen benötigt.


Welcher VPN-Client soll verwendet werden:

VPN-Client mit benutzerdefinierten Parametern

LANCOM Advanced-VPN-Client

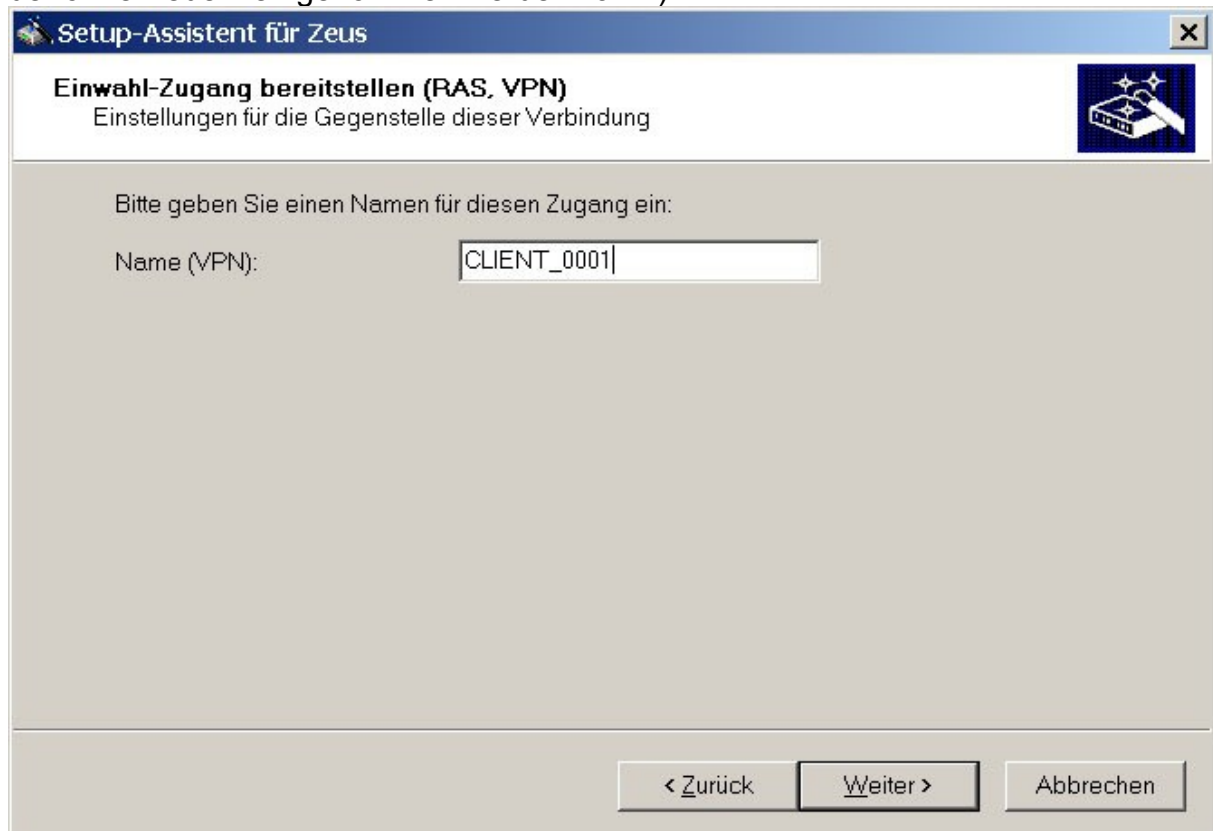
Beschleunigen Sie das Konfigurieren mit 1-Click-VPN

 Beim 1-Click-VPN für den LANCOM Advanced-VPN-Client wird Ihnen ein eindeutiger Name für die Verbindung vorgeschlagen. Alle Schlüssel werden automatisch und per Zufall erzeugt. Darüber hinaus kann der Assistent die meisten Einstellungen für den VPN-Einwahlzugang aus den Geräte-Einstellungen ableiten.

 Für den LANCOM Advanced-VPN-Client wird Ihnen später angeboten, eine Import-Datei mit den Zugangsdaten zu erzeugen

< Zurück Weiter > Abbrechen

Den VPN-Client benennen... (zu sehen ist der Default-Eintrag des Lancom-Wizards, der ohne Bedenken genommen werden kann.)



Setup-Assistent für Zeus

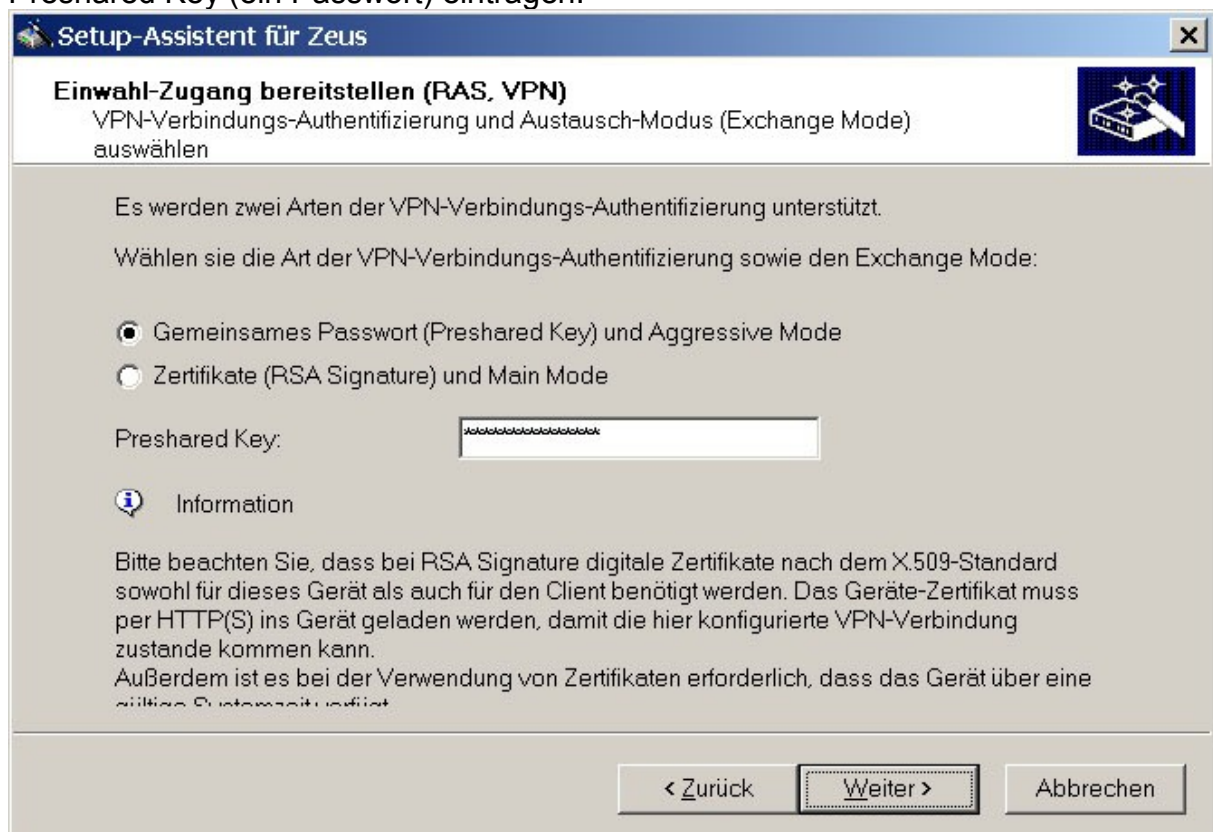
Einwahl-Zugang bereitstellen (RAS, VPN)
Einstellungen für die Gegenstelle dieser Verbindung

Bitte geben Sie einen Namen für diesen Zugang ein:

Name (VPN):

< Zurück Weiter > Abbrechen

Für die Authentifizierung die Variante mit "Preshared Key" wählen **UND** einen Preshared Key (ein Passwort) eintragen.



Setup-Assistent für Zeus


Einwahl-Zugang bereitstellen (RAS, VPN)
VPN-Verbindungs-Authentifizierung und Austausch-Modus (Exchange Mode) auswählen

Es werden zwei Arten der VPN-Verbindungs-Authentifizierung unterstützt.

Wählen sie die Art der VPN-Verbindungs-Authentifizierung sowie den Exchange Mode:

Gemeinsames Passwort (Preshared Key) und Aggressive Mode
 Zertifikate (RSA Signature) und Main Mode

Preshared Key:

 Information

Bitte beachten Sie, dass bei RSA Signature digitale Zertifikate nach dem X.509-Standard sowohl für dieses Gerät als auch für den Client benötigt werden. Das Geräte-Zertifikat muss per HTTP(S) ins Gerät geladen werden, damit die hier konfigurierte VPN-Verbindung zustande kommen kann.
Außerdem ist es bei der Verwendung von Zertifikaten erforderlich, dass das Gerät über eine gültige Systemzeit verfügt.

< Zurück Weiter > Abbrechen

Den eingetragenen Preshared Key nach dem Klick auf Weiter nochmals zur Bestätigung eintragen.

Setup-Assistent für Zeus

Einwahl-Zugang bereitstellen (RAS, VPN)
VPN-Verbindungs-Authentifizierung und Austausch-Modus (Exchange Mode) auswählen

Es werden zwei Arten der VPN-Verbindungs-Authentifizierung unterstützt.
Wählen sie die Art der VPN-Verbindungs-Authentifizierung sowie den Exchange Mode:

Gemein
 Zertifikat
 Preshared Key

Inform

Eingabe bestätigen

Bitte wiederholen Sie die folgende Eingabe:

Preshared Key

OK
Abbrechen

Bitte beachten Sie, dass bei RSA Signature digitale Zertifikate nach dem X.509-Standard sowohl für dieses Gerät als auch für den Client benötigt werden. Das Geräte-Zertifikat muss per HTTP(S) ins Gerät geladen werden, damit die hier konfigurierte VPN-Verbindung zustande kommen kann. Außerdem ist es bei der Verwendung von Zertifikaten erforderlich, dass das Gerät über eine gültige Systemzeit verfügt.

< Zurück Weiter > Abbrechen

Für die IKE-Parameter die Default-Einstellung belassen. (Sollte hier aus vorherigen Fehl-Versuchen kein IKE-PRESH-KEY mehr existieren, so sind die Proposals im Lancom zu prüfen. In dem Fall bietet der Wizard den IKE-PRESH-KEY nicht mehr an.)

Setup-Assistent für Zeus

Einwahl-Zugang bereitstellen (RAS, VPN)
Standard-IKE-Parameter für alle ankommenden Aggressive-Mode-Verbindungen

Es sind bereits folgende Standard-IKE-Parameter für alle ankommenden Aggressive-Mode-Verbindungen definiert:

Standard-IKE-Proposal-Liste: IKE_PRESH_KEY
Standard-IKE-Gruppe: 2

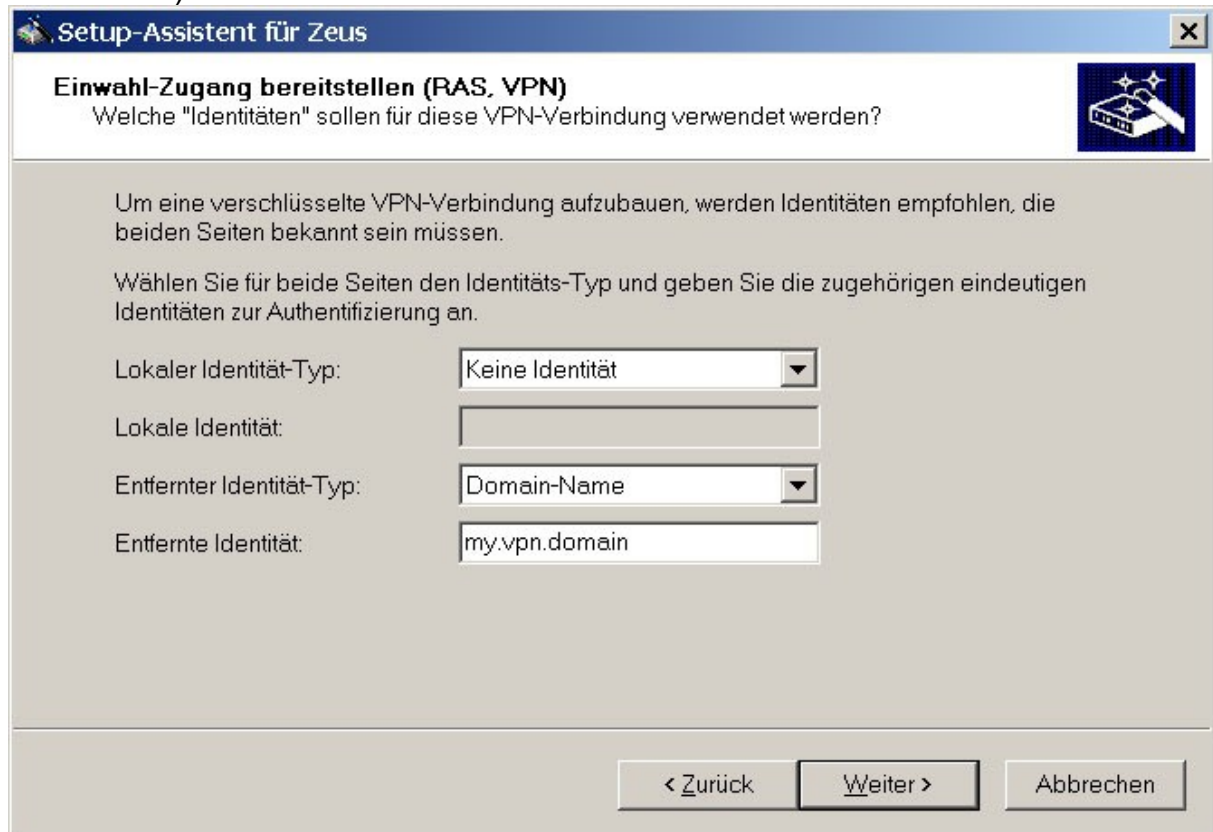
Da diese Einstellungen von allen Verbindungen gemeinsam genutzt werden, wird empfohlen, diese nicht zu verändern.

Standard-IKE-Parameter verändern (betrifft alle ankommenden Aggressive-Mode-Verbindungen).

Achtung: Bitte bedenken Sie, dass durch eine Änderung in diesen Einstellungen vorhandene Verbindungen unbrauchbar werden können!

< Zurück Weiter > Abbrechen

Nun müssen die Identitäten konfiguriert werden... (im Beispiel ist eine einfache Konfiguration zu sehen, die später mit dem Shrew-VPN-Client problemlos funktioniert.)



Setup-Assistent für Zeus

Einwahl-Zugang bereitstellen (RAS, VPN)
Welche "Identitäten" sollen für diese VPN-Verbindung verwendet werden?

Um eine verschlüsselte VPN-Verbindung aufzubauen, werden Identitäten empfohlen, die beiden Seiten bekannt sein müssen.

Wählen Sie für beide Seiten den Identitäts-Typ und geben Sie die zugehörigen eindeutigen Identitäten zur Authentifizierung an.

Lokaler Identität-Typ: Keine Identität

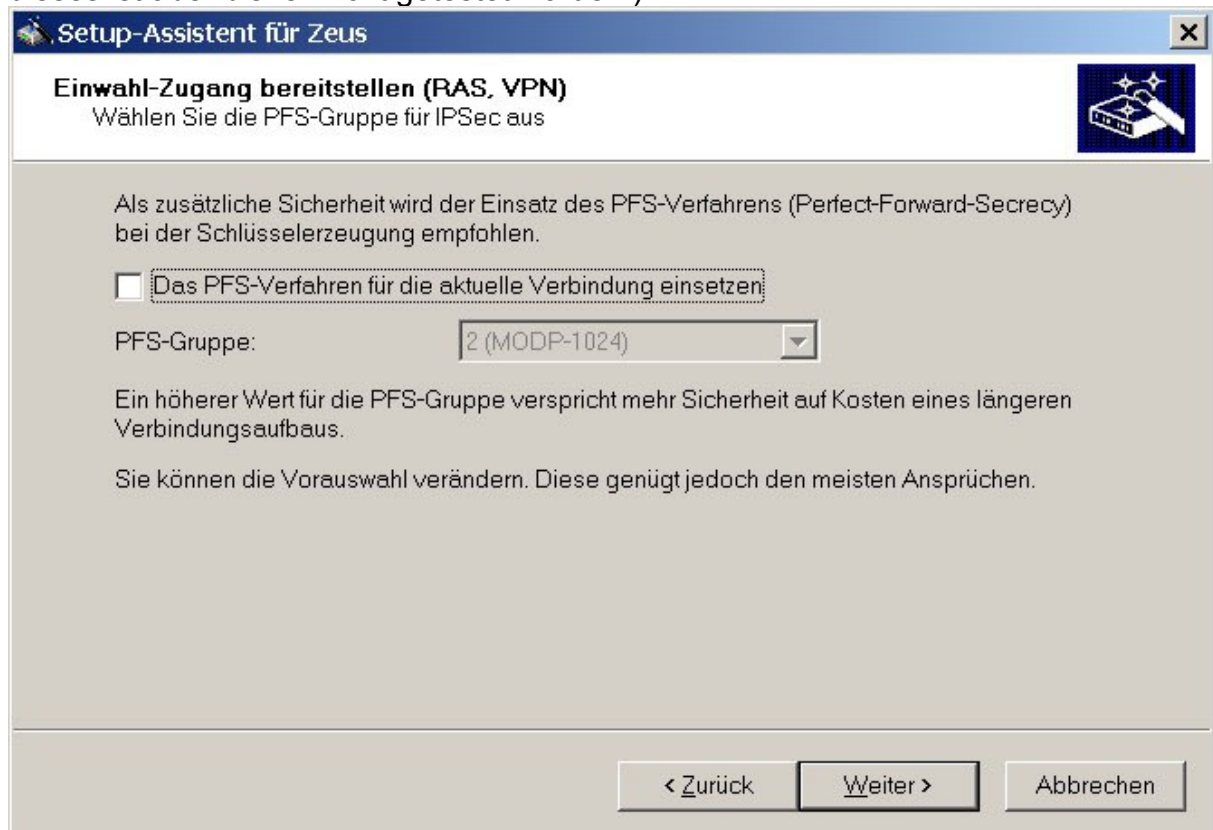
Lokale Identität:

Entfernter Identität-Typ: Domain-Name

Entfernte Identität: my.vpn.domain

< Zurück Weiter > Abbrechen

Das PFS-Verfahren deaktivieren... (möglicherweise funktioniert es auch hiermit, dieses ist aber bisher nicht getestet worden.)



Setup-Assistent für Zeus

Einwahl-Zugang bereitstellen (RAS, VPN)
Wählen Sie die PFS-Gruppe für IPSec aus

Als zusätzliche Sicherheit wird der Einsatz des PFS-Verfahrens (Perfect-Forward-Secrecy) bei der Schlüsselerzeugung empfohlen.

Das PFS-Verfahren für die aktuelle Verbindung einsetzen

PFS-Gruppe: 2 (MODP-1024)

Ein höherer Wert für die PFS-Gruppe verspricht mehr Sicherheit auf Kosten eines längeren Verbindungsaufbaus.

Sie können die Vorauswahl verändern. Diese genügt jedoch den meisten Ansprüchen.

< Zurück Weiter > Abbrechen

Nun die Verschlüsselungsverfahren auswählen... (zu sehen sind die Default-Einträge des Lancom-Wizards, die ohne Bedenken genommen werden können.)

Setup-Assistent für Zeus

Einwahl-Zugang bereitstellen (RAS, VPN)

Welche IPSec-ESP-Verschlüsselungs- und -Authentifizierungs-Verfahren sollen dem Client erlaubt werden

Das Gerät unterstützt zur Datenübertragung (IPSec) mit ESP verschiedene Verschlüsselungs- und Authentifizierungs-Verfahren.

Welche Verschlüsselungs-Verfahren sollen dem Client erlaubt werden (mind. eines)?

AES (128bit)

Blowfish (128bit)

3DES (168bit)

DES (56bit)

Welche Authentifizierungs-Verfahren sollen dem Client erlaubt werden (mind. eines)?

HMAC-MD5-96

HMAC-SHA1-96

< Zurück Weiter > Abbrechen

Kein zusätzliches Authentifizierungsprotokoll aktivieren...

Setup-Assistent für Zeus

Einwahl-Zugang bereitstellen (RAS, VPN)

Welche IPSec-AH-Authentifizierungs-Verfahren sollen dem Client erlaubt werden?

Zusätzlich kann das Gerät ein weiteres Authentifizierungs-Protokoll (Authentication Header, kurz AH) für IPSec verwenden.

Achtung: Dieses Verfahren funktioniert nicht, wenn der Client sich hinter einer maskierten Verbindung befindet (NAT/PAT)!

Welche AH-Authentifizierungs-Verfahren sollen dem Client erlaubt werden?

Authentifizierung: Kein AH

Außerdem stehen verschiedene IPCOMP-Kompressionsverfahren zur Verfügung:


Kompression: Kein IPCOMP

Sie können die Vorauswahl verändern. Diese genügt jedoch den meisten Ansprüchen.

< Zurück Weiter > Abbrechen

Nun für den VPN-Client eine IP-Adresse im Adressraum des RouterLANs wählen...


Setup-Assistent für Zeus X

Einwahl-Zugang bereitstellen (RAS, VPN)
Einstellungen für das TCP/IP-Protokoll 

Bitte geben Sie eine eindeutige IP-Adresse (Virtuelle IP) ein, die in Ihrem VPN-Client konfiguriert sein muss. Geben Sie eine freie Adresse aus dem Adressbereich Ihres Netzes ein.

Dies ist das Intranet-Netzwerk zu dem Ihr Gerät gehört:


IP-Netz:	192.168.168.0
Netzmaske:	255.255.255.0
Erlaubte Adressen:	192.168.168.1 - 192.168.168.254
IP-Adresse:	<input type="text" value="192.168.168.150"/>

 Information

Auf die Eingabe einer IP-Adresse kann verzichtet werden, wenn der benutzte VPN-Client den Config-Mode unterstützt. Dies ist für den LANCOM-Advanced-VPN-Client der Fall.

Dann die Adressräume definieren, die der VPN-Client erreichen können soll...

Setup-Assistent für Zeus X

Einwahl-Zugang bereitstellen (RAS, VPN)
Einstellungen für das TCP/IP-Protokoll 


Der VPN-Client kann alle IP-Adressen über die VPN-Verbindung erreichen (Standard), oder Sie schränken die erlaubten IP-Adressen auf ein bestimmtes Netzwerk ein.

Welche IP-Adressen sollen vom VPN-Client erreicht werden können:

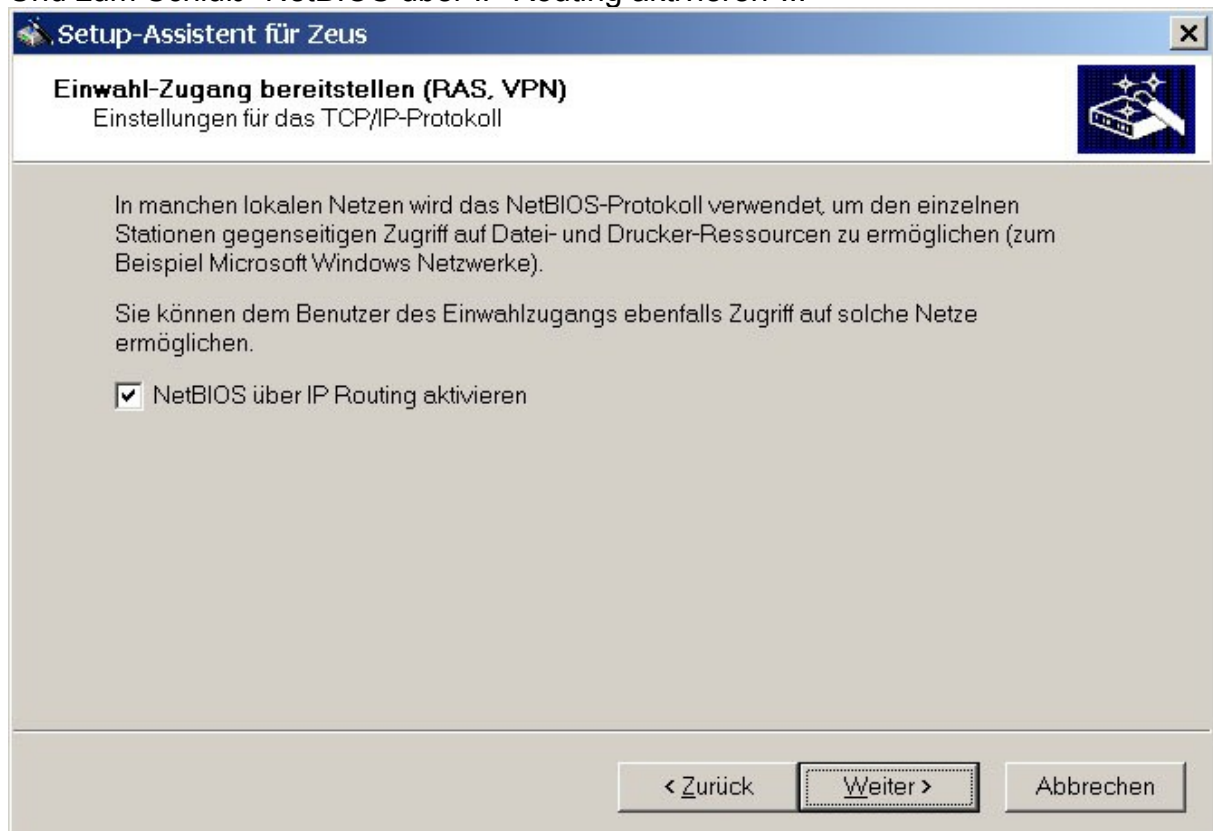
Folgendes IP-Netzwerk soll vom VPN-Client erreicht werden können:

IP-Netz:	<input type="text" value="192.168.168.0"/>
Netzmaske:	<input type="text" value="255.255.255.0"/>

Bitte beachten Sie, dass dieses IP-Netzwerk auch im VPN-Client konfiguriert werden muss, damit eine VPN-Verbindung zustande kommen kann.

 Weitere Netzwerke und Netzwerkbeziehungen oder Übertragungseigenschaften können in der zugehörigen neu erzeugten Regel der Firewall ergänzt werden

Und zum Schluß "NetBIOS über IP Routing aktivieren"...



Fertig!

