VNC und TELNET sicher anwenden

Diese Dokumentation beschreibt eine Lösung für die abgesicherte Verwendung der Programme VNC (Virtual Network Computing) und dem Terminalprogramm TELNET. Beide Programme haben das Manko, dass die aufgebaute Verbindung nicht gesichert, und damit leicht ausgespäht werden kann. Dieses trifft auf jeden Fall für Telnet, aber auch für die VNC Freeware Version zu. Auch für das Terminalprogramm Telnet gibt es eine gesicherte Version; SSH. Will man die VNC Freeversion einsetzen, und kann oder will man nicht SSH verwenden, dann gibt es die Möglichkeit diese Programme über eine sogenannten SSL Wrapper zu betreiben. Dieses Programm, in Form des Open Source Produktes Stunnel (für Unix und Windows), ermöglicht den frei wählbaren Aufbau von TCP Verbindungen innerhalb von SSL (Secure Socket Layer). Auch andere ungesicherte Protokolle, wie POP3, IMAP, LDAP usw., könnten eine solche Verbindung nutzen.

Eine gesicherte Verbindung ist besonders wichtig, wenn man eine Remoteverbindung über das Internet herstellen möchte. Es ist nicht ratsam solche Verbindungen unverschlüsselt zu betreiben. Aber auch innhalb eines Unternehmensnetzes kann die Verschlüsselung der Verbindung sinnvoll und ratsam sein. Dieses trifft eigentlich immer dann zu, wenn kritische Informationen übertragen werden, die ein Angreifer dazu ausnutzen könnte, um weitergehende Schäden anzurichten.

Produkte wie Stunnel beinhalten ein gewisses Risko, wenn es einem Anwender möglich ist mit seinem PC System direkt, ob mit oder ohne Proxy Server, eine Verbindung ins Internet herstellen kann. Da Verbindungen mit Stunnel über jeden beliebigen Port hergestellt werden könne, braucht die Firewall nicht speziell für Stunnel geöffnet werden. Stunnel kann mühelos die bereits geöffneten Ports 80 und 443 für HTTP und HTTPS Verkehr nutzen. Damit ist u. U. ungewollter, verschlüsselter Datenverkehr durch die Firewall hindurch möglich.

Nachfolgend beschreibe ich verschiedene Musterlösungen für unterschiedlichen Umgebungen für VNC und Telnet. Hierfür wurden folgende Umgebung und Software eingesetzt:

- Windows XP und Windows 2000 Systeme
- VNC Server und Viewer 4.1.2, aber auch 4.1.1
- Universall SSL Wrapper Stunnel 4.16
- Jana Proxy Server 2.4.8.51

Für die Test werden max. 3 System benötigt. Ein System wird als VNC/Stunnel Client eingesetz, von dem aus die Verbindung aufgebaut wird. Das 2. System wird als VNC/Stunnel Server benutzt. Das dritte System findet nur Verwendung, wenn ein Proxy Server dazwischengeschaltet wird.

Folgende Konfigurationen habe ich getestet:

- Gesicherte VNC Verbindung zwischen 2 Windows Systemen im Intranet
- Gesicherte VNC Verbindung via Proxy Server zwischen 2 Windows Systemen im Intranet
- Gesicherte TELNET Verbindung via Proxy Server zwischen 2 Windows Systemen im Intranet
- Gesicherte VNC Verbindung zwischen 2 Windows Systemen über das Internet
- Gesicherte VNC Verbindung via Proxy Server zwischen 2 Windows Systemen über das Internet

Für eventuell auftretende Schäden beim Nachstellen der o. a. Musterlösungen übernehme ich keine Gewähr. Ich habe die Tests nach besten Wissen und Gewissen durchgeführt. Im Zusammenhang mit den Tests aufgetretene Probleme habe ich im Anschluss an die Testbeschreibungen aufgeführt.

Inhalt

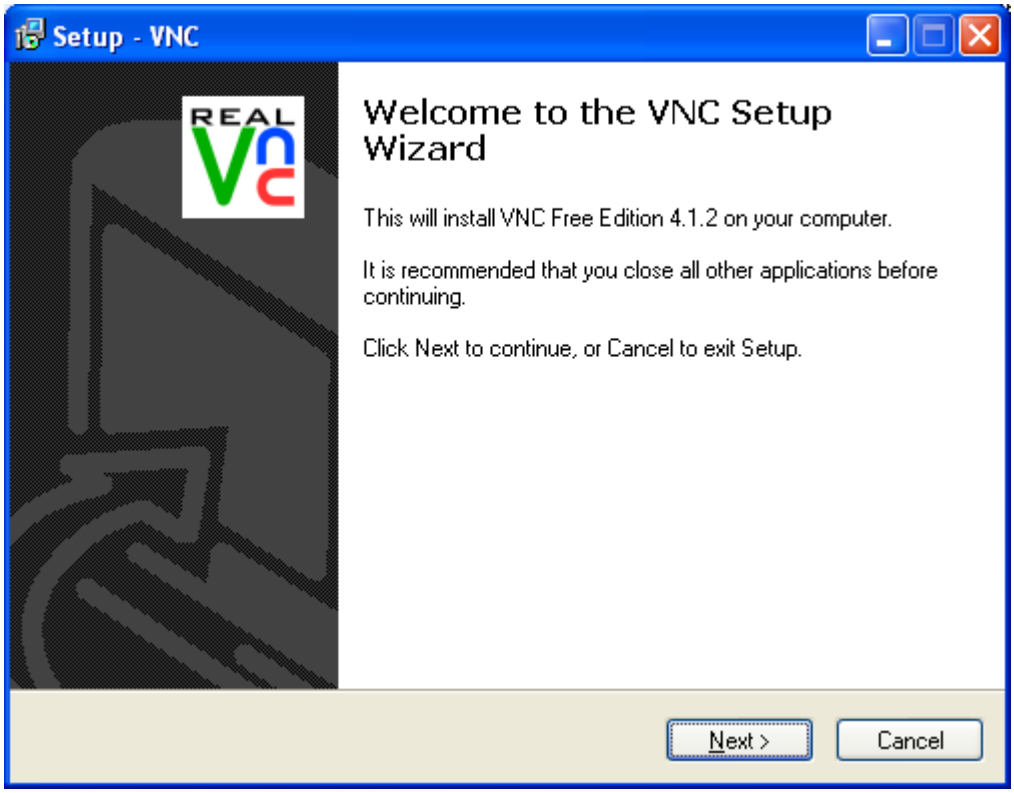
1. Vorbereitungen

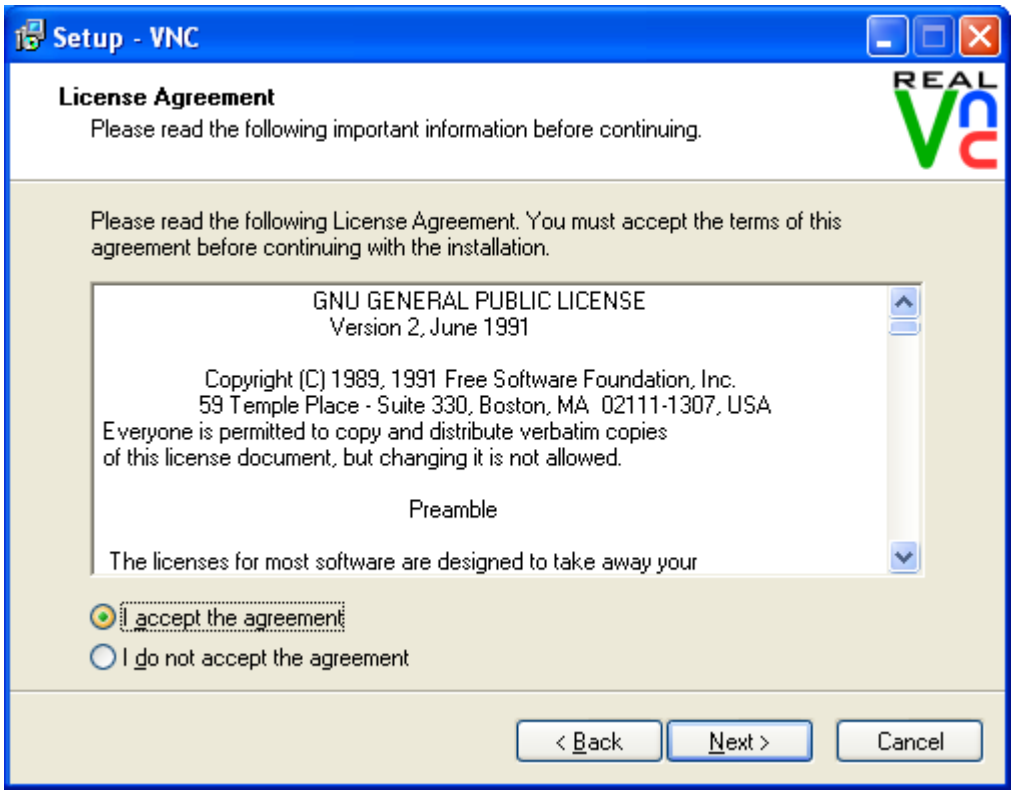
Zur Vorbereitung ist die entsprechende Software auf den Systemen zu installieren. Für die Musterlösung wurden folgende Namen verwendet:

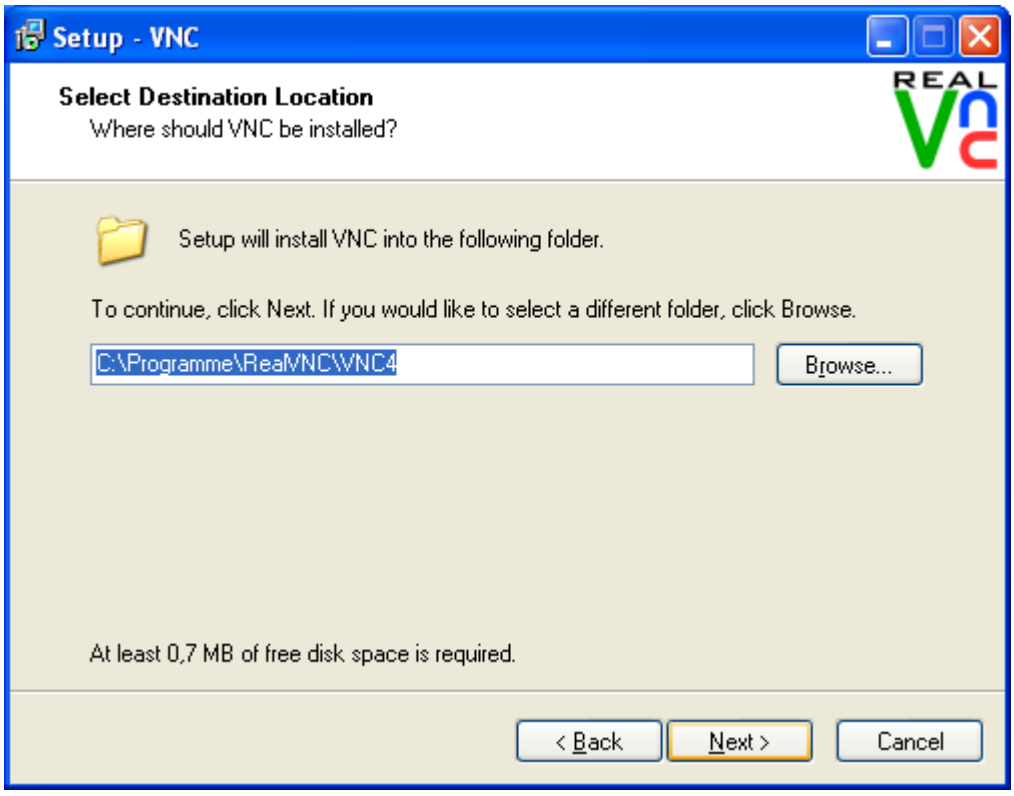
- clientpc für den Client
- serverpc für den Server
- proxypc für den Proxy Server

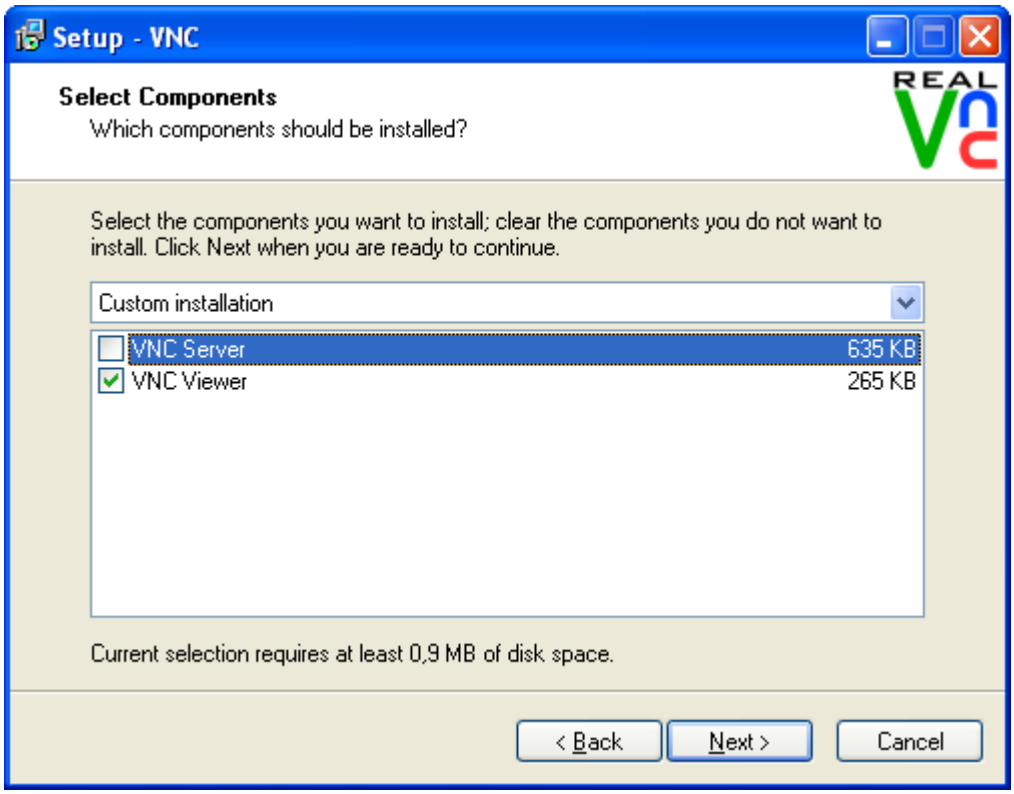
VNC Viewer Installation auf dem Client PC

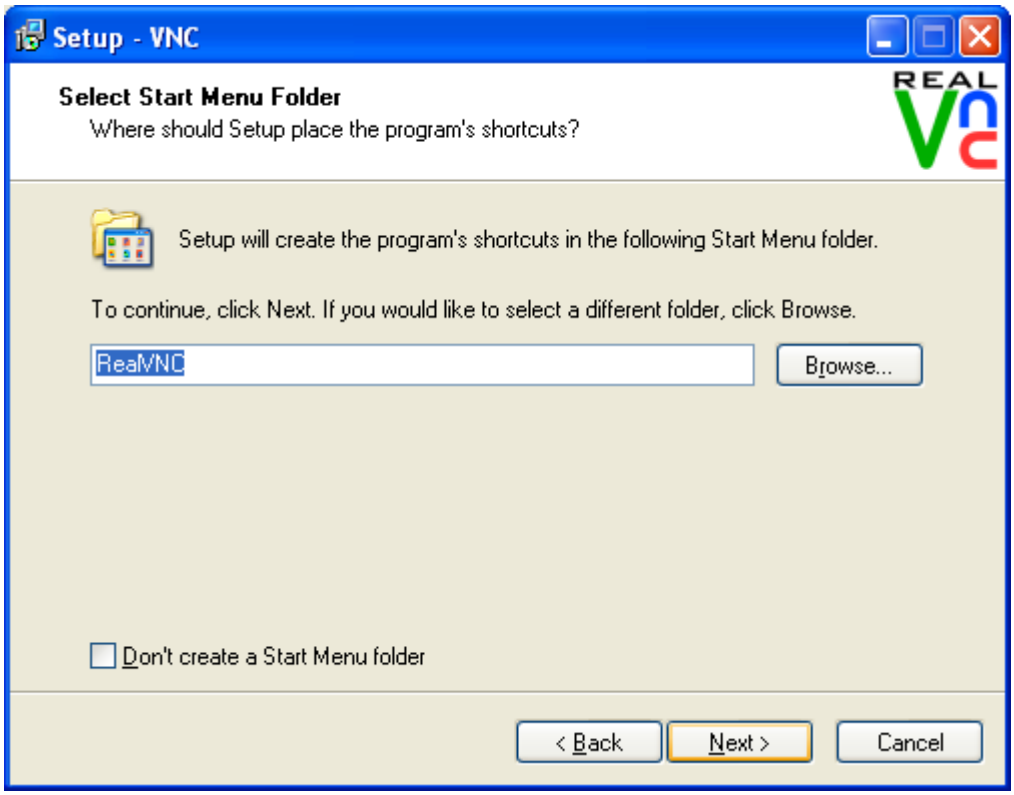
Installiert wird die Real VNC Version 4.1.2. Nach der Installation steht ein Icon „VNC Viewer 4“ auf dem Desktop zur Verfügung. Über diesen Viewer wird dann die Verbindung zum Remotesystem hergestellt. Die Installation erfolgt durch den Aufruf der *vnc-4_1_2-x86_win32.exe*.

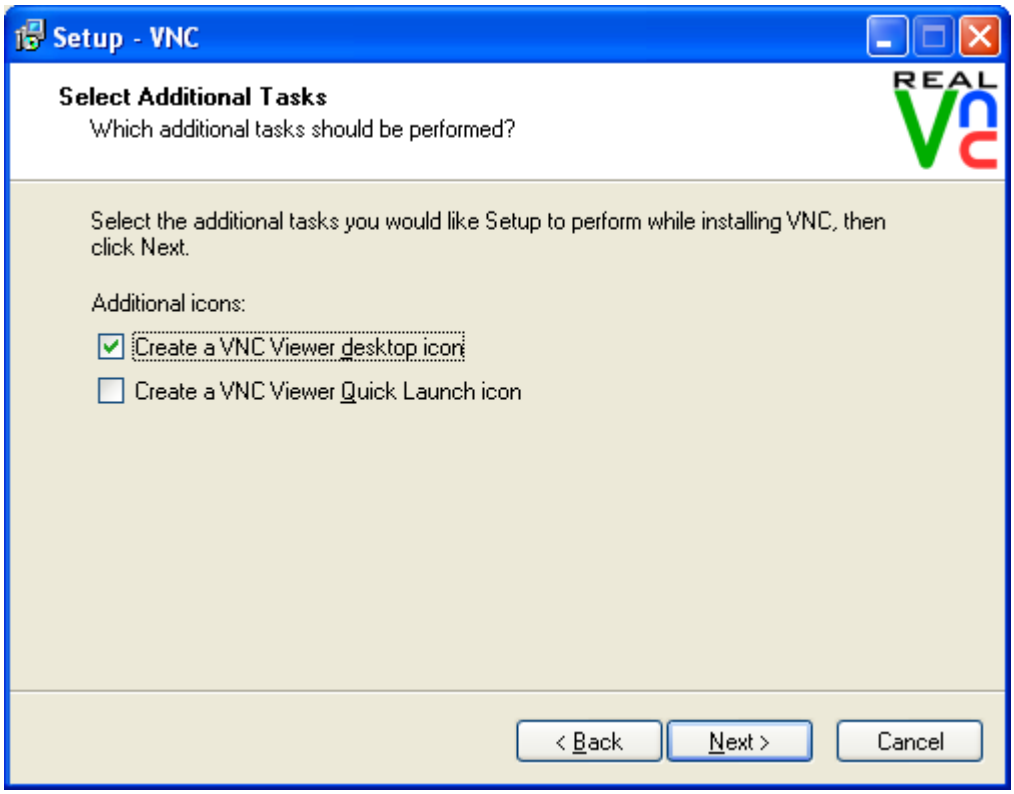


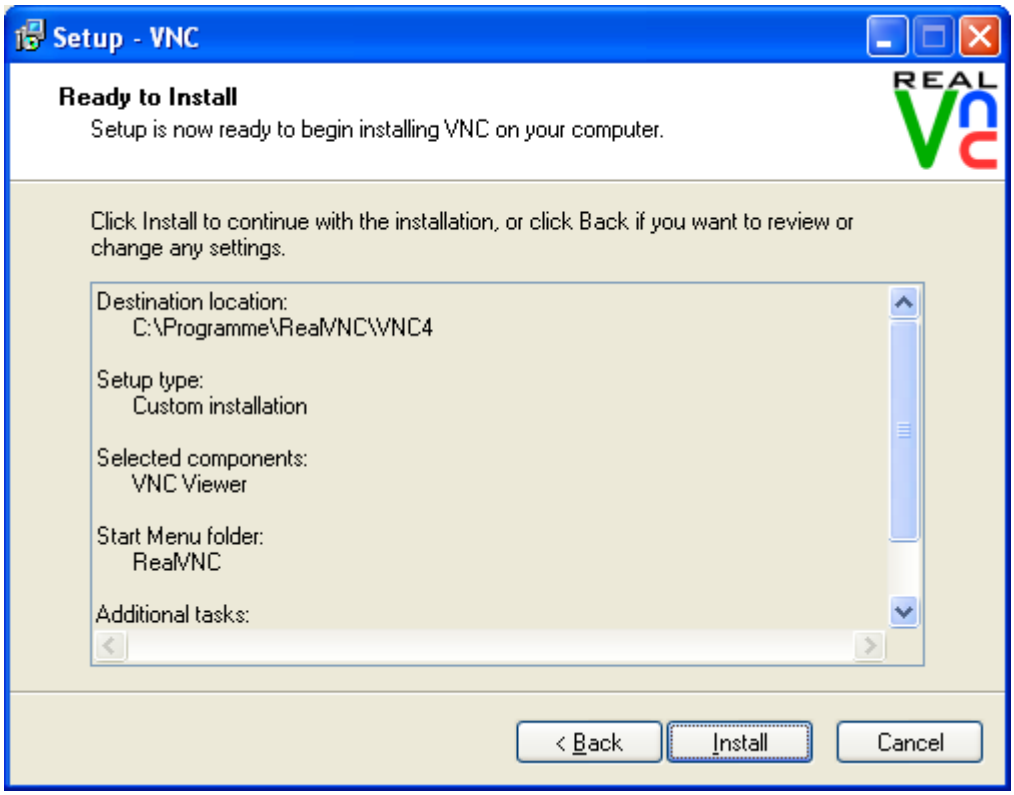

Setup - VNC
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place - Suite 330, Boston, MA 02111-1307, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
Preamble
The licenses for most software are designed to take away your
I accept the agreement
I do not accept the agreement
< Back
Next >
Cancel

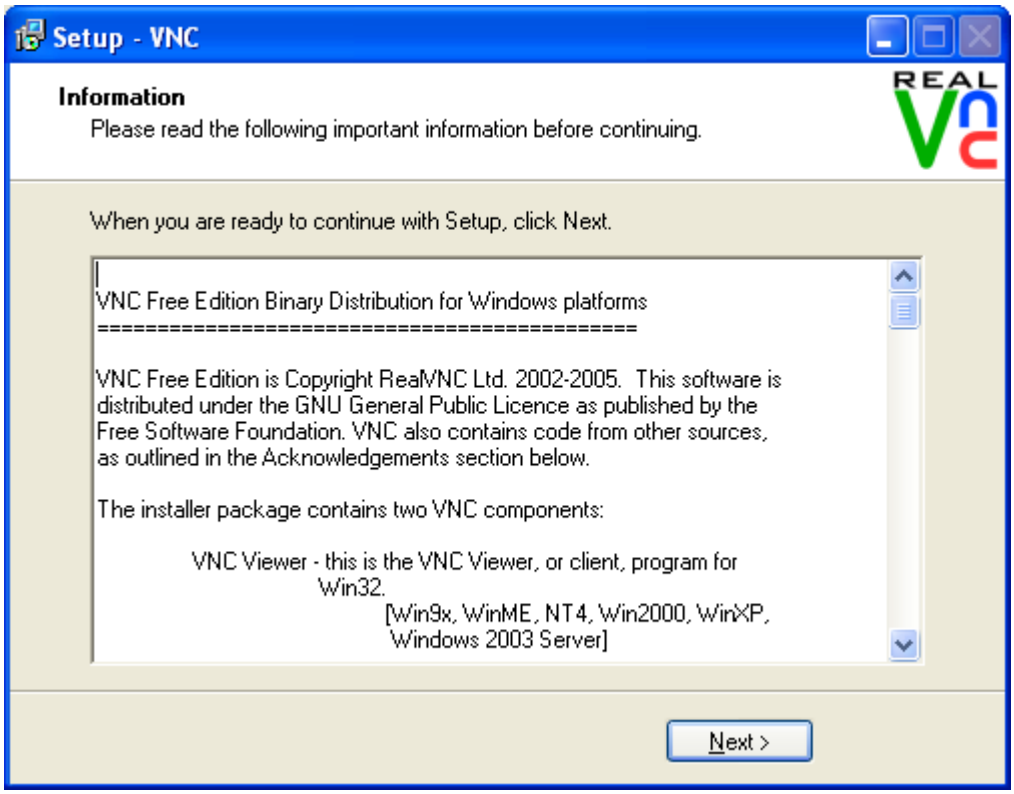

Setup - VNC
Select Destination Location
Where should VNC be installed?
Setup will install VNC into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Programme\RealVNC\VNC4
Browse...
At least 0,7 MB of free disk space is required.
< Back
Next >
Cancel

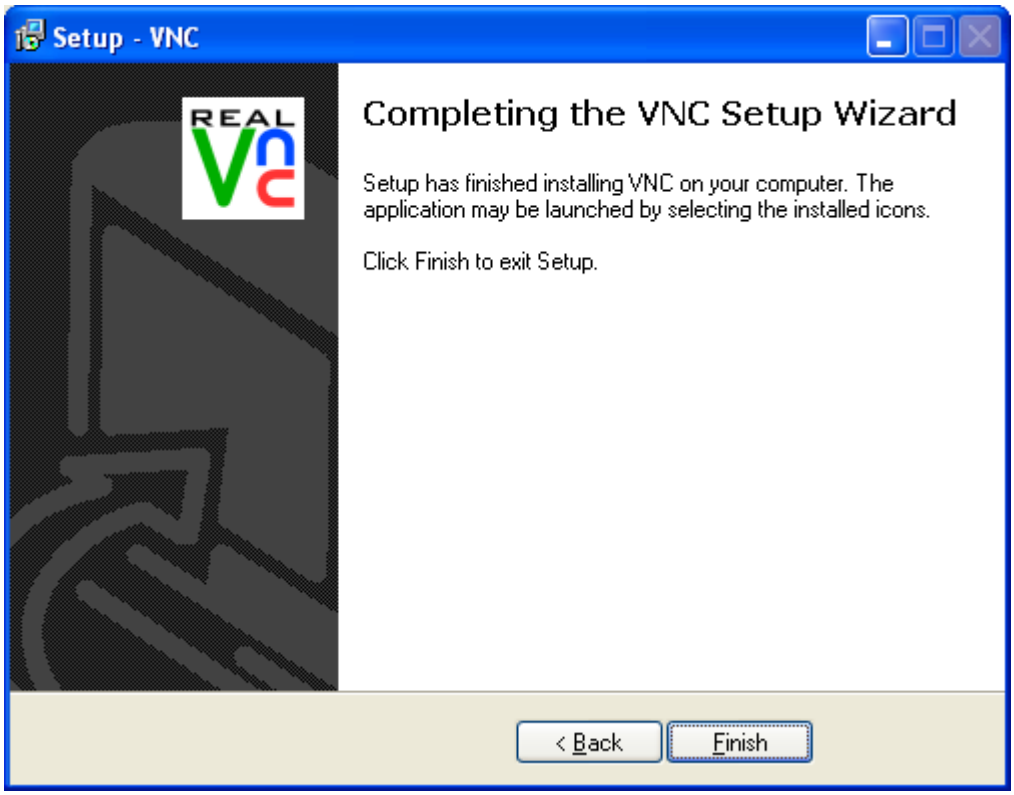

Setup - VNC
Select Components
Which components should be installed?
REAL VNC
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.
Custom installation
VNC Server 635 KB
VNC Viewer 265 KB
Current selection requires at least 0,9 MB of disk space.
< Back
Next >
Cancel


Setup - VNC
Select Start Menu Folder
Where should Setup place the program's shortcuts?
REAL VNC
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
RealVNC
Browse...
Don't create a Start Menu folder
< Back
Next >
Cancel


Setup - VNC
Select Additional Tasks
Which additional tasks should be performed?
REAL VNC
Select the additional tasks you would like Setup to perform while installing VNC, then click Next.
Additional icons:
Create a VNC Viewer desktop icon
Create a VNC Viewer Quick Launch icon
< Back
Next >
Cancel


Setup - VNC
Ready to Install
Setup is now ready to begin installing VNC on your computer.
REAL VNC
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Programme\RealVNC\VNC4
Setup type:
Custom installation
Selected components:
VNC Viewer
Start Menu folder:
RealVNC
Additional tasks:
< Back
Install
Cancel

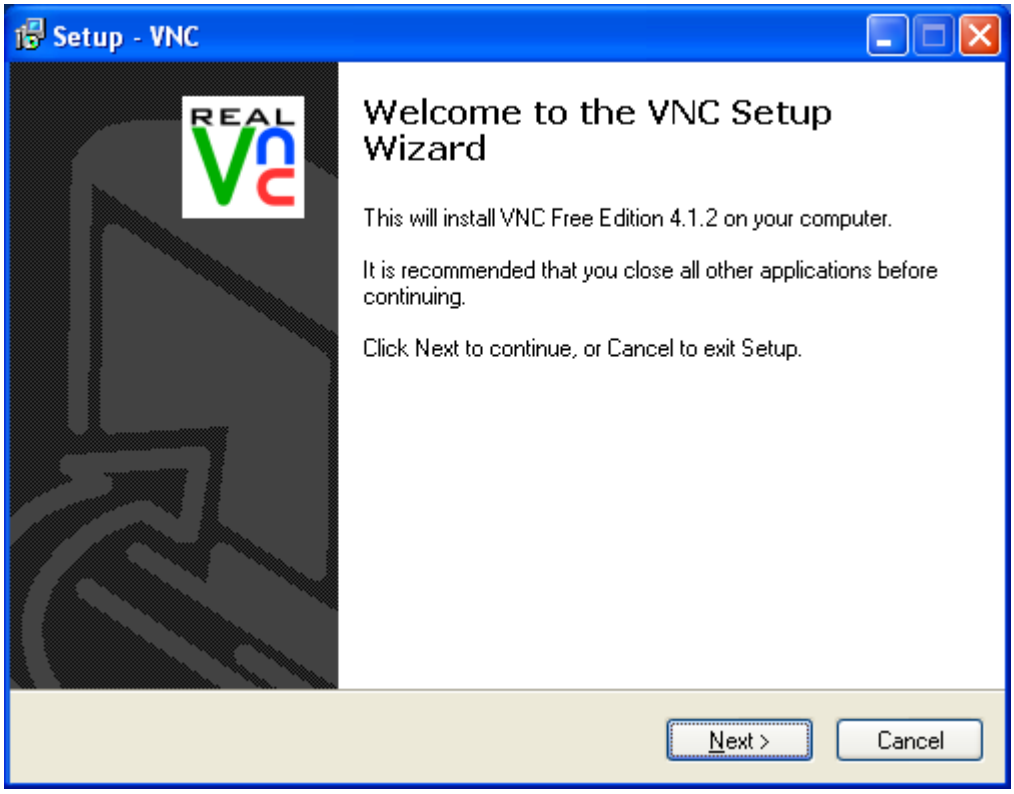


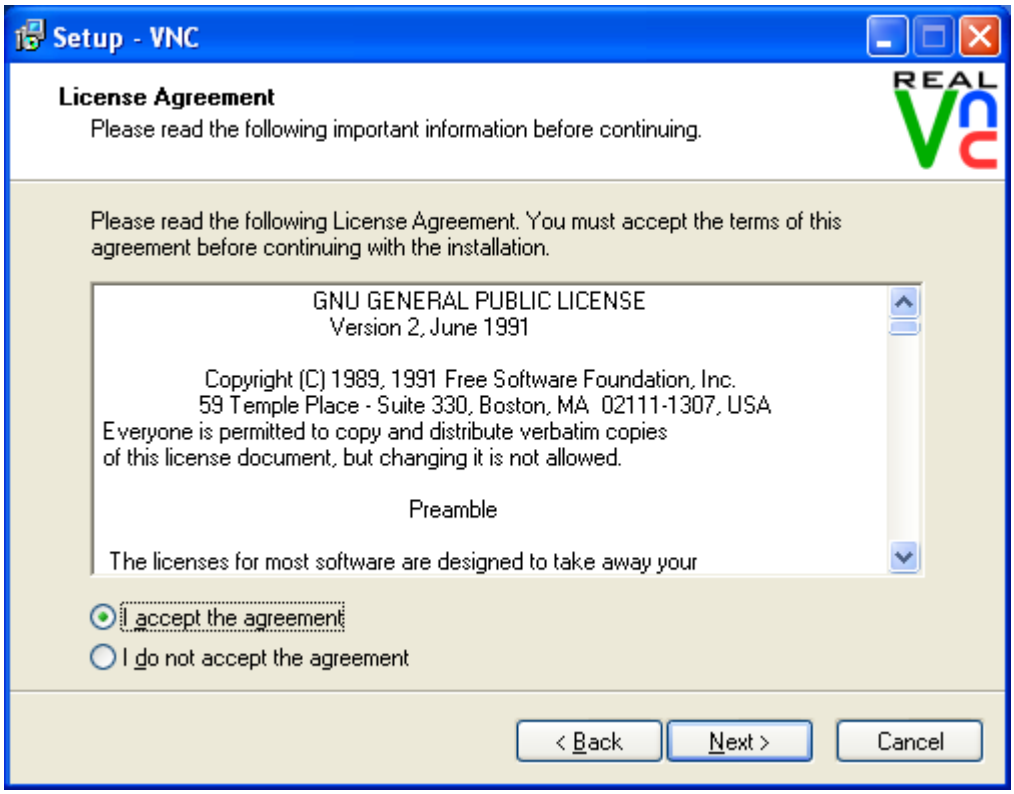


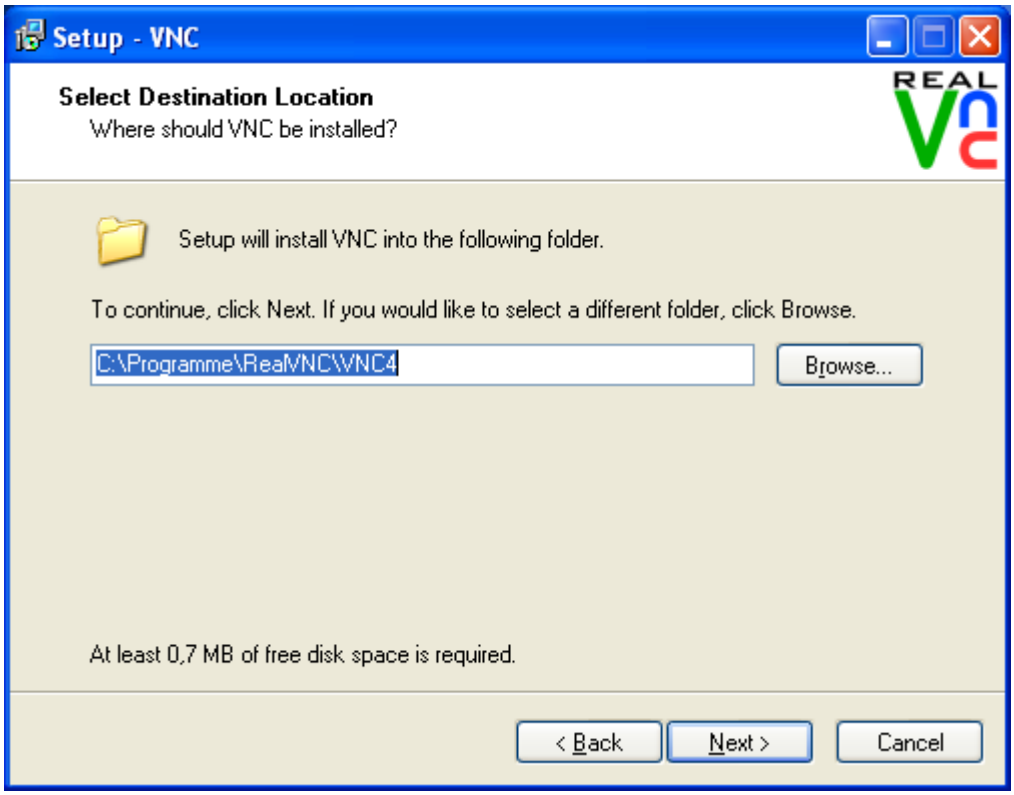
Durch den Klick auf den „Finish“ Button ist die Installation der VNC Client Komponente abgeschlossen.

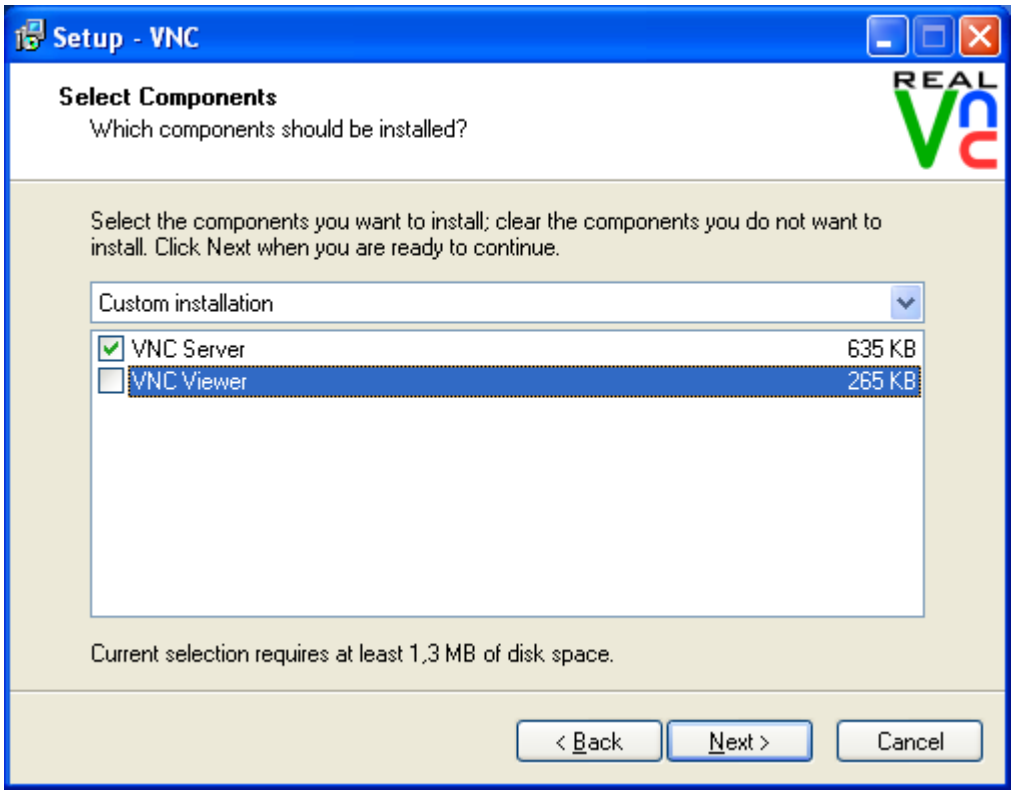
VNC Server Installation auf dem Server PC

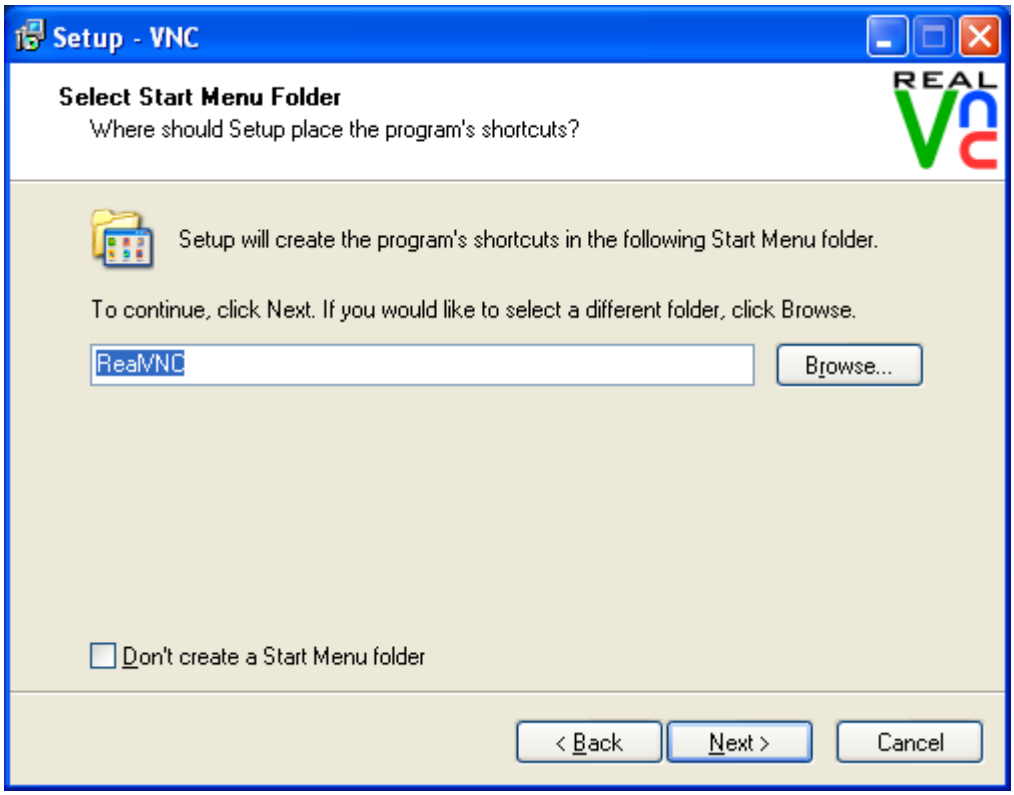
Installiert wird die Real VNC Version 4.1.2. Bei der Installation wird darauf verzichtet die Komponente als Dienst zu installieren. Um später eine Verbindung aufbauen zu können, muß der VNC Server im User Mode gestartet werden. Die Installation erfolgt durch den Aufruf von *vnc-4_1_2-x86_win32.exe*.

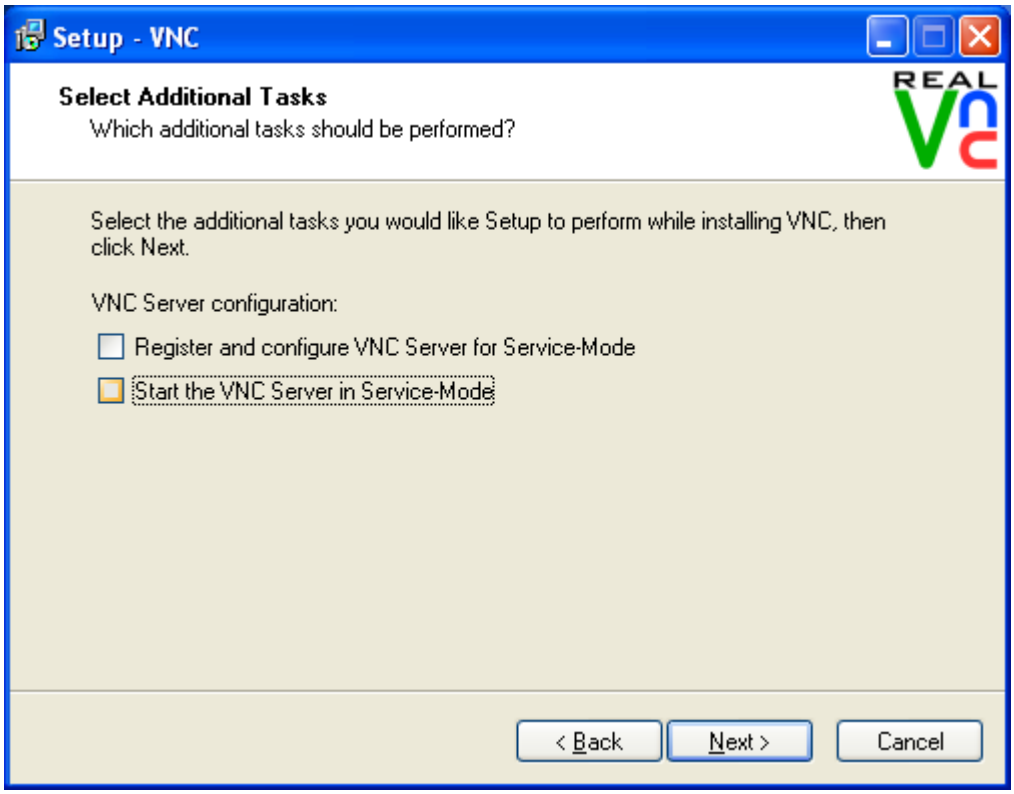


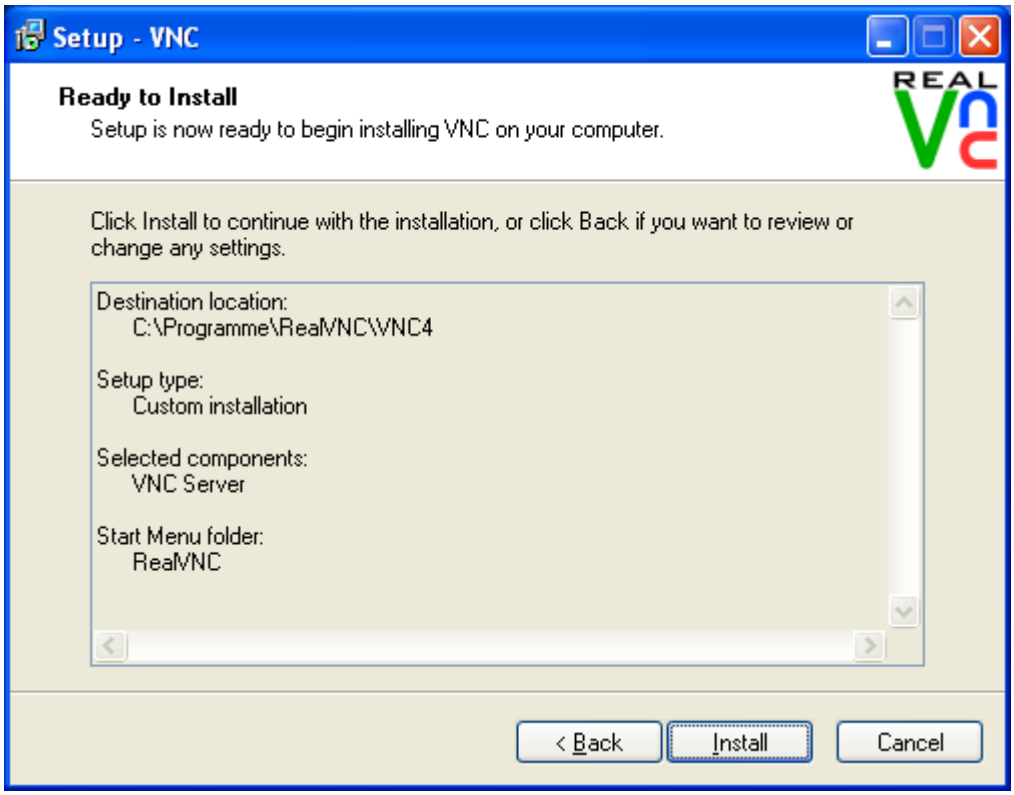

Setup - VNC
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place - Suite 330, Boston, MA 02111-1307, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
Preamble
The licenses for most software are designed to take away your
I accept the agreement
I do not accept the agreement
< Back
Next >
Cancel

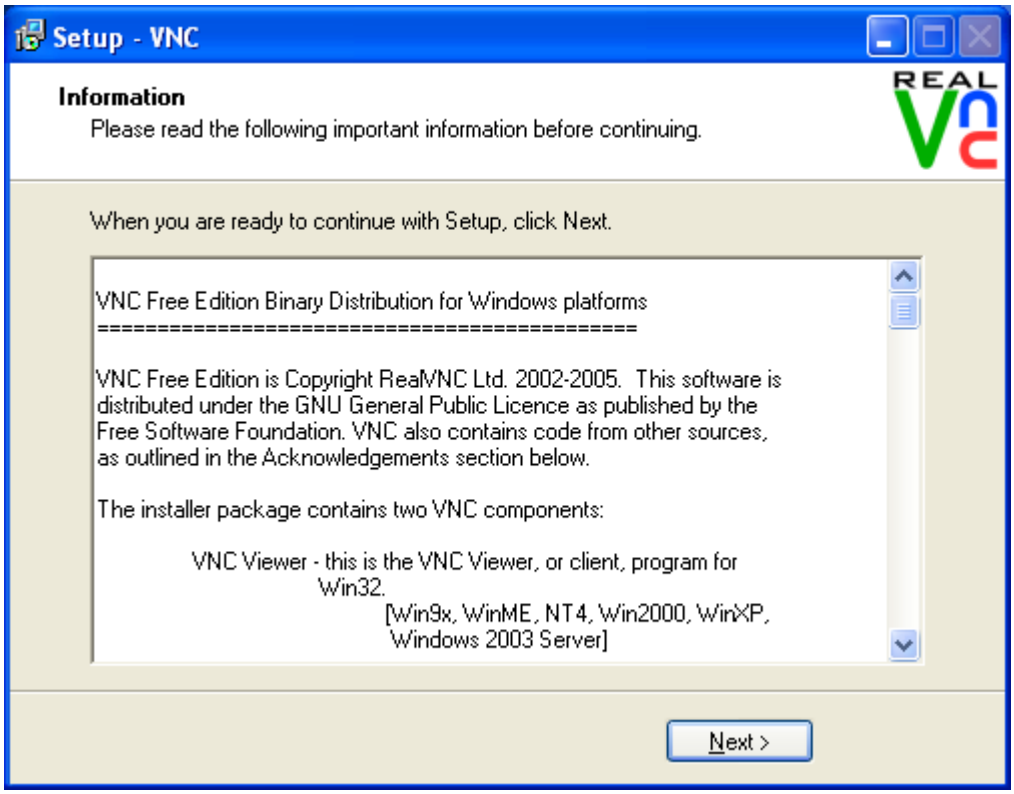

Setup - VNC
Select Destination Location
Where should VNC be installed?
Setup will install VNC into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Programme\RealVNC\VNC4
Browse...
At least 0,7 MB of free disk space is required.
< Back
Next >
Cancel

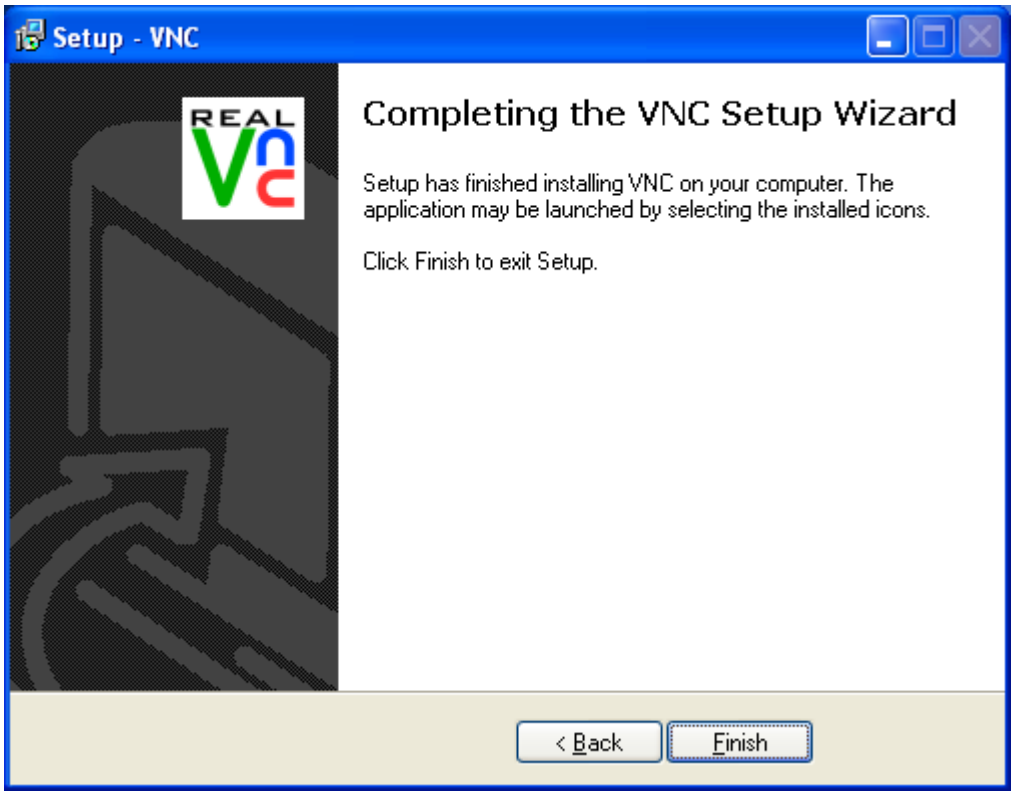

Setup - VNC
Select Components
Which components should be installed?
REAL VNC
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.
Custom installation
VNC Server 635 KB
VNC Viewer 265 KB
Current selection requires at least 1,3 MB of disk space.
< Back
Next >
Cancel


Setup - VNC
Select Start Menu Folder
Where should Setup place the program's shortcuts?
REAL VNC
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
RealVNC
Browse...
Don't create a Start Menu folder
< Back
Next >
Cancel


Setup - VNC
Select Additional Tasks
Which additional tasks should be performed?
REAL VNC
Select the additional tasks you would like Setup to perform while installing VNC, then click Next.
VNC Server configuration:
Register and configure VNC Server for Service-Mode
Start the VNC Server in Service-Mode
< Back
Next >
Cancel


Setup - VNC
Ready to Install
Setup is now ready to begin installing VNC on your computer.
REAL VNC
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Programme\RealVNC\VNC4
Setup type:
Custom installation
Selected components:
VNC Server
Start Menu folder:
RealVNC
< Back
Install
Cancel



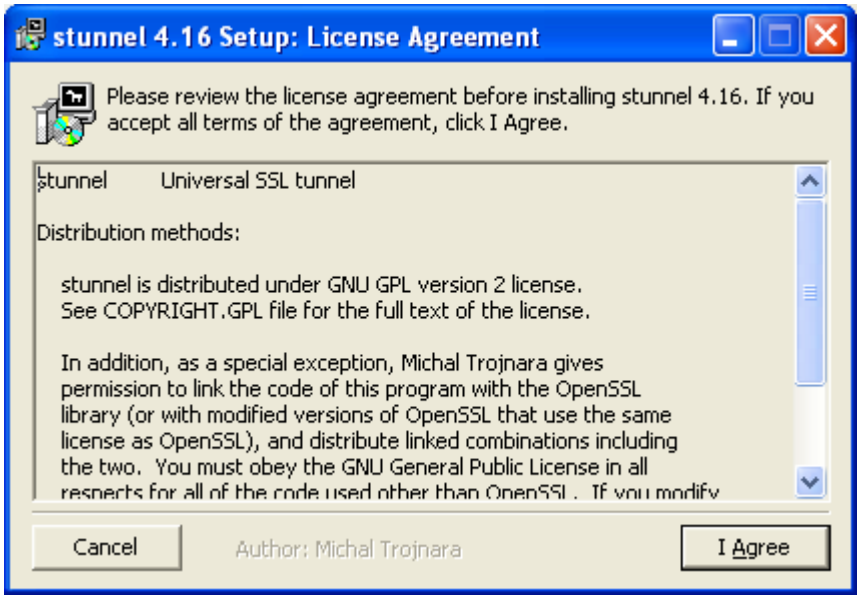


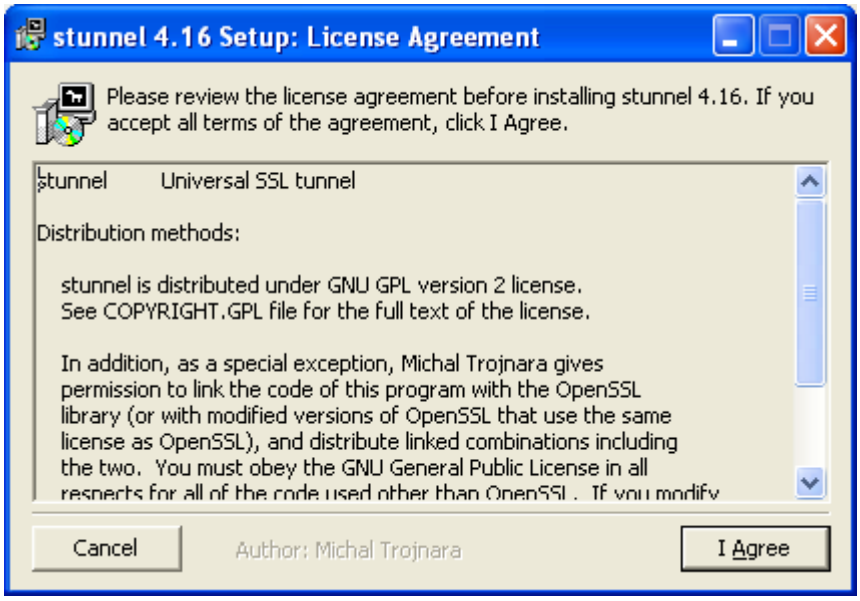
Durch den Klick auf den Button „Finish“ ist die Installation der VNC Server Komponente abgeschlossen.

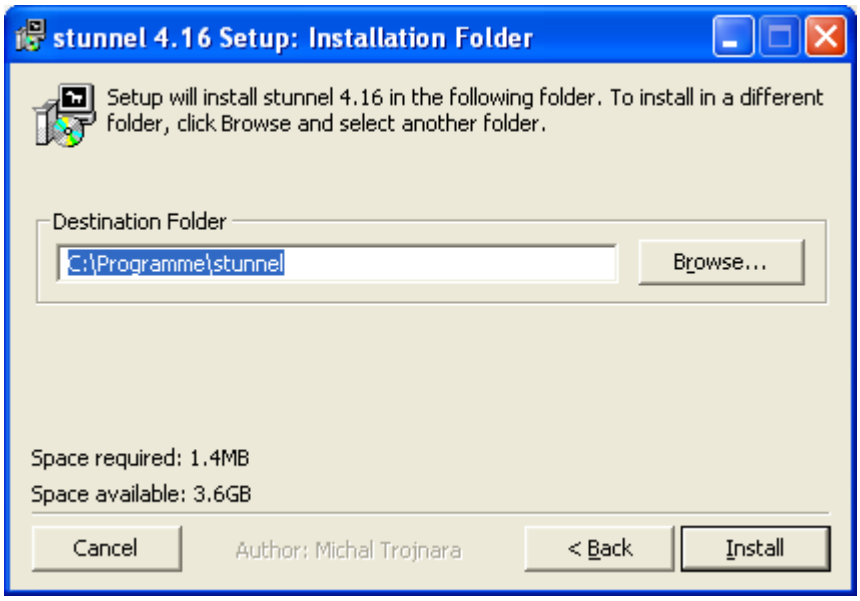
Stunnel Installation auf Client- und Server PC

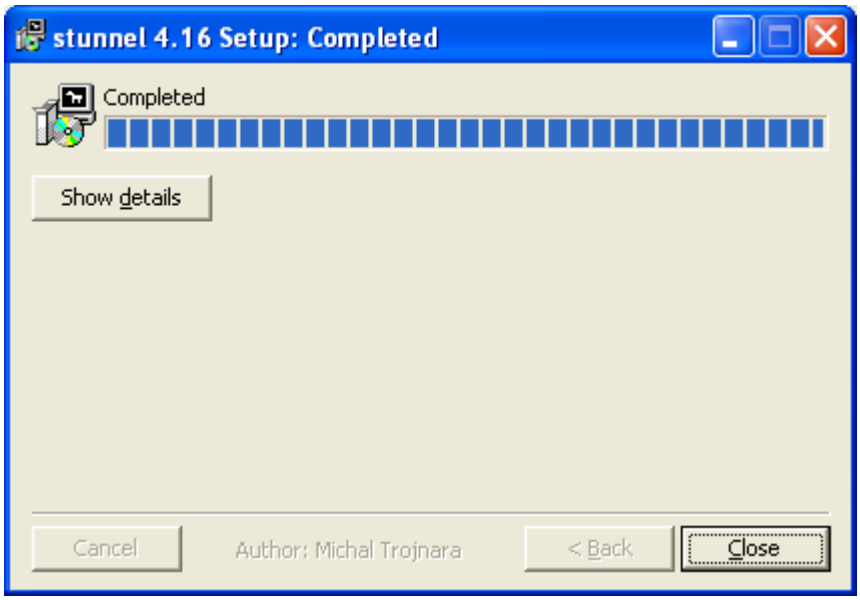
Um eine sicherer Verbindung zwischen Client und Server herstellen zu können, ist die Installation des SSL Wrappers „Stunnel“ erforderlich. In diesem Test wurde die aktuelle Version 4.16 verwendet. Die Installation auf dem Client und Server PC unterscheidet sich letztendlich in der Konfiguration. Auch bei dieser Installation wird darauf verzichtet die Software als Dienst zu installieren. Vor dem Aufbau eine VNC oder Telnet Verbindung muß zunächst die Stunnel Anwendung auf Client und Server aktiv sein.

Die Installation wird durch den Aufruf von *stunnel-4.16-installer.exe* gestartet.





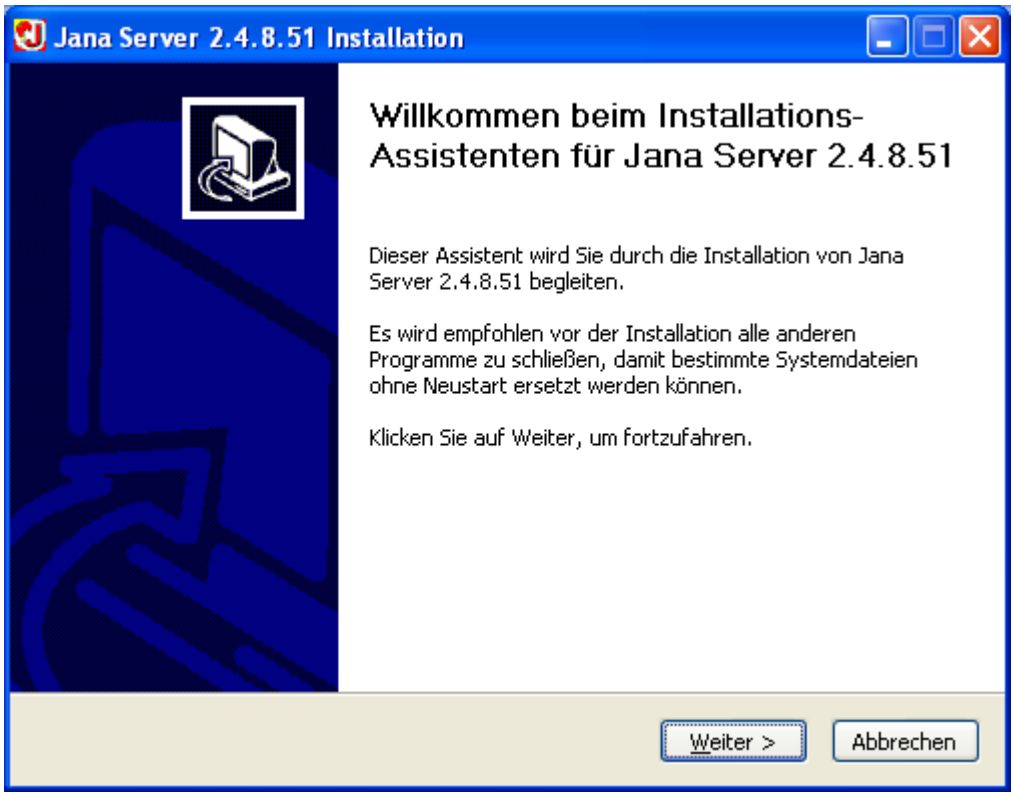


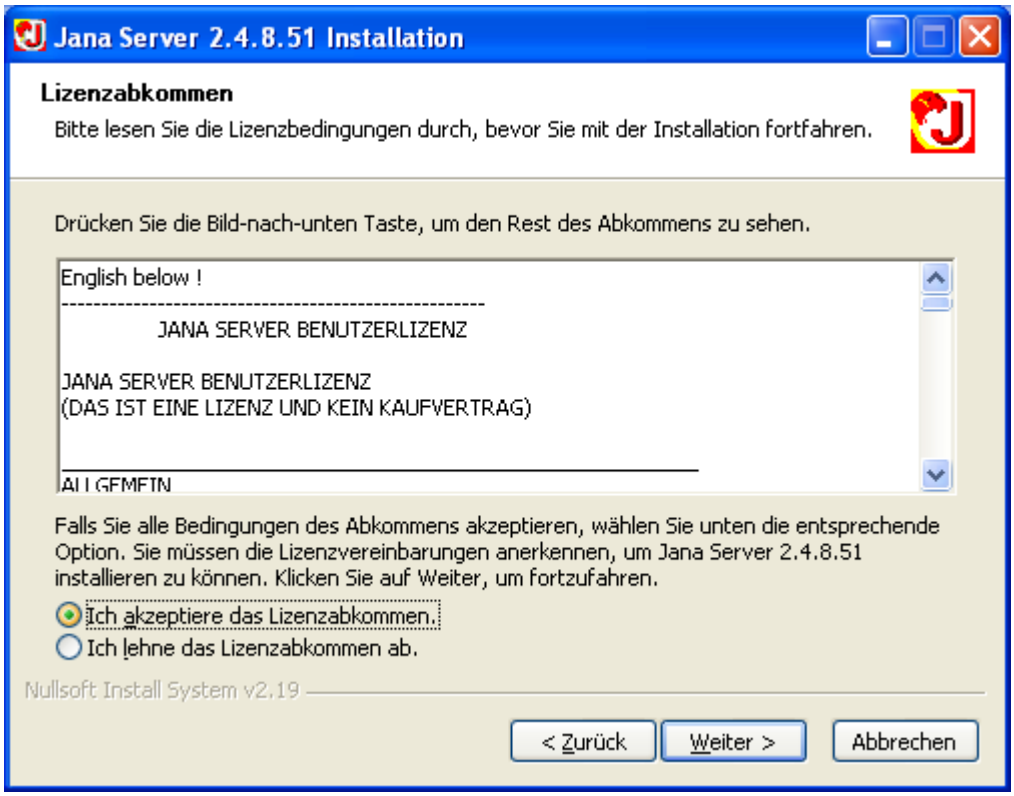


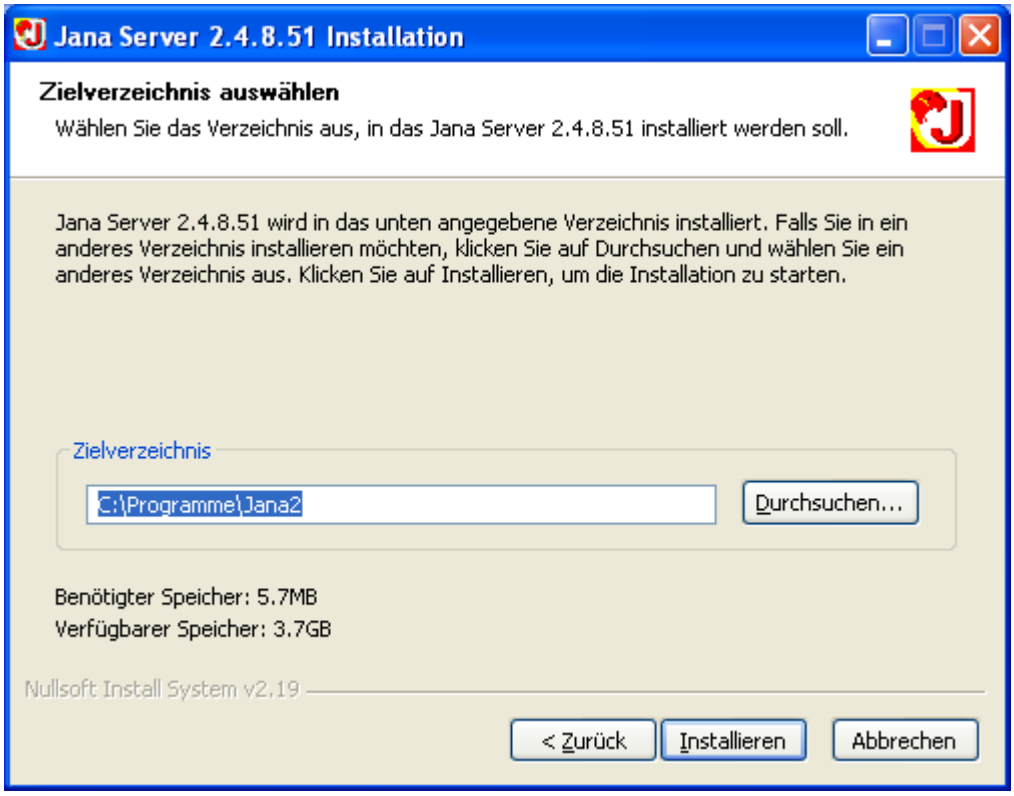
Durch den Klick auf den „Close“ Button ist die Installation abgeschlossen.

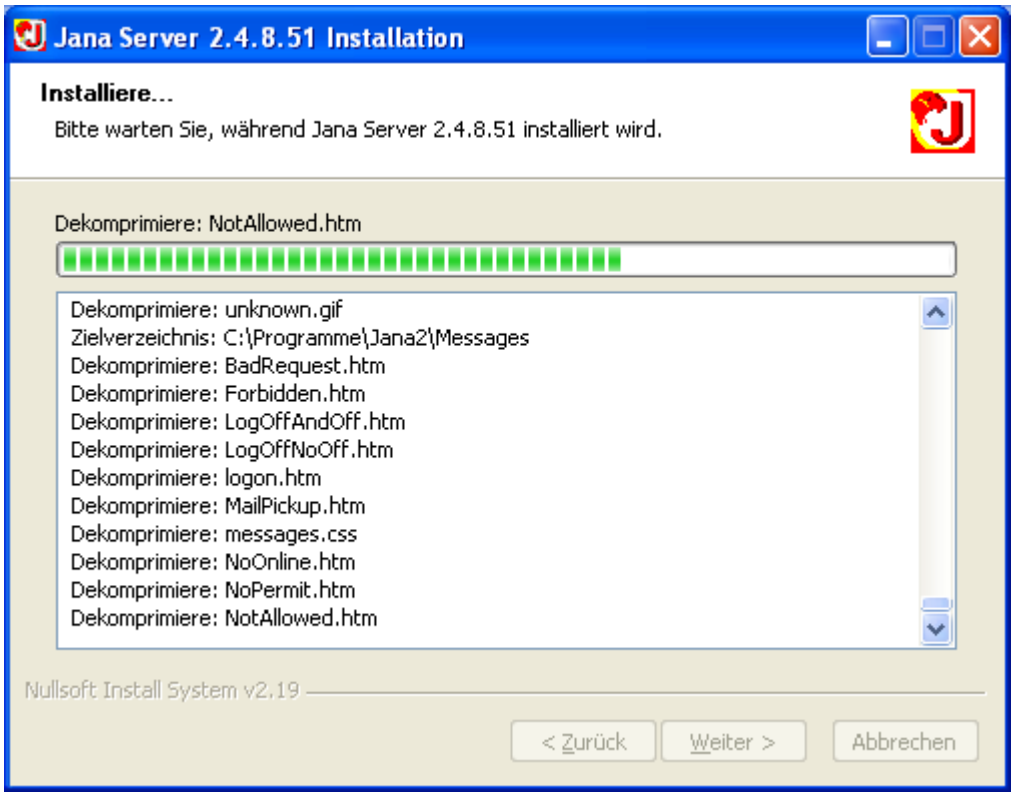
Jana Proxy Server Installation auf dem Proxy PC

Für den VNC Verbindungsaufbau über eine Proxy Server muß auf dem dritten PC, dem Proxy PC, der Jana Server installiert werden. Bei dieser Software handelt es sich um eine frei verfügbare Proxy Server Variante auf Windows Basis. Installiert wurde die Jana Server Version 2.4.8.51. Die Installation wird durch den Aufruf der Programmdatei *JanaSetup.exe* gestartet.




Jana Server 2.4.8.51 Installation
Lizenzabkommen
Bitte lesen Sie die Lizenzbedingungen durch, bevor Sie mit der Installation fortfahren.
Drücken Sie die Bild-nach-unten Taste, um den Rest des Abkommens zu sehen.
English below !
JANA SERVER BENUTZERLIZENZ
JANA SERVER BENUTZERLIZENZ
(DAS IST EINE LIZENZ UND KEIN KAUFVERTRAG)
ALLGEMEIN
Falls Sie alle Bedingungen des Abkommens akzeptieren, wählen Sie unten die entsprechende Option. Sie müssen die Lizenzvereinbarungen anerkennen, um Jana Server 2.4.8.51 installieren zu können. Klicken Sie auf Weiter, um fortzufahren.
Ich akzeptiere das Lizenzabkommen.
Ich lehne das Lizenzabkommen ab.
Nullsoft Install System v2.19
< Zurück
Weiter >
Abbrechen


Jana Server 2.4.8.51 Installation
Zielverzeichnis auswählen
Wählen Sie das Verzeichnis aus, in das Jana Server 2.4.8.51 installiert werden soll.
Jana Server 2.4.8.51 wird in das unten angegebene Verzeichnis installiert. Falls Sie in ein anderes Verzeichnis installieren möchten, klicken Sie auf Durchsuchen und wählen Sie ein anderes Verzeichnis aus. Klicken Sie auf Installieren, um die Installation zu starten.
Zielverzeichnis
C:\Programme\Jana2
Durchsuchen...
Benötigter Speicher: 5.7MB
Verfügbarer Speicher: 3.7GB
Nullsoft Install System v2.19
< Zurück
Installieren
Abbrechen



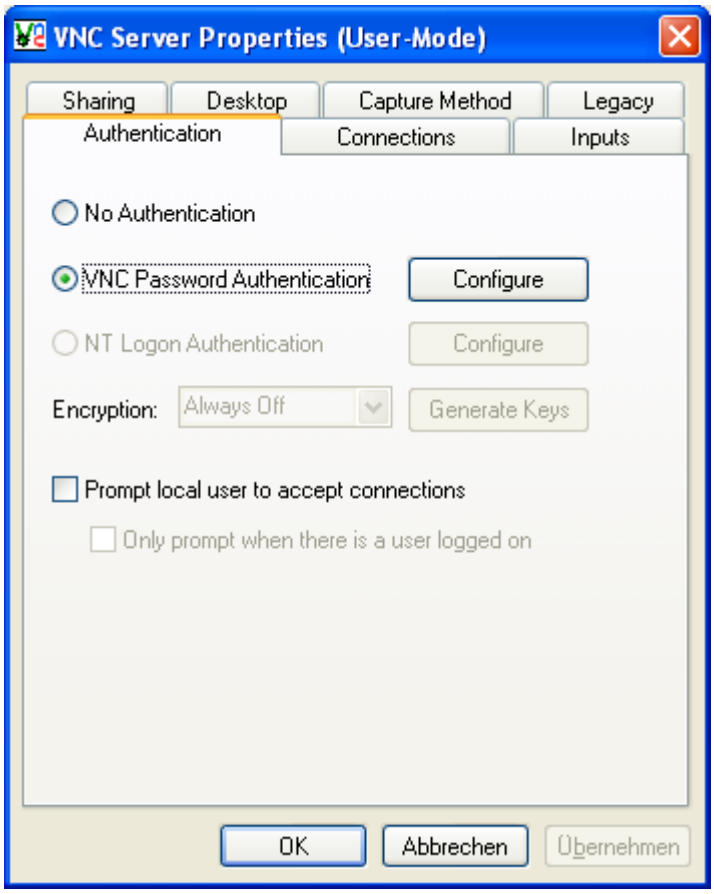
Nach dem Klick auf den Button „Fertig stellen“ ist die Installation des Jana Servers abgeschlossen. Dieser wird standardmäßig als Dienst instllaiert. Im System Tray wird das Symbol des Proxy Servers angezeigt.

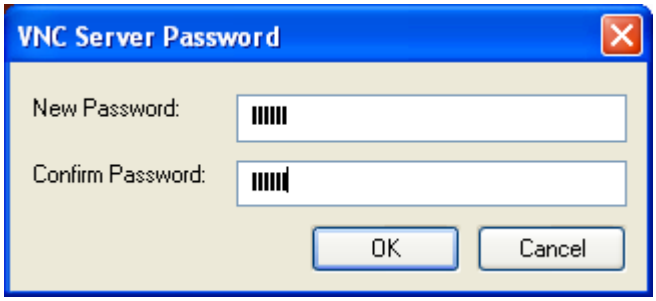
2. Konfiguration der installierten Software

Nachdem nun die Installationarbeiten abgeschlossen sind, müssen die Systeme noch entsprechend konfiguriert werden. Für die Musterlösungen gehen wird von folgenden Überlegungen aus:

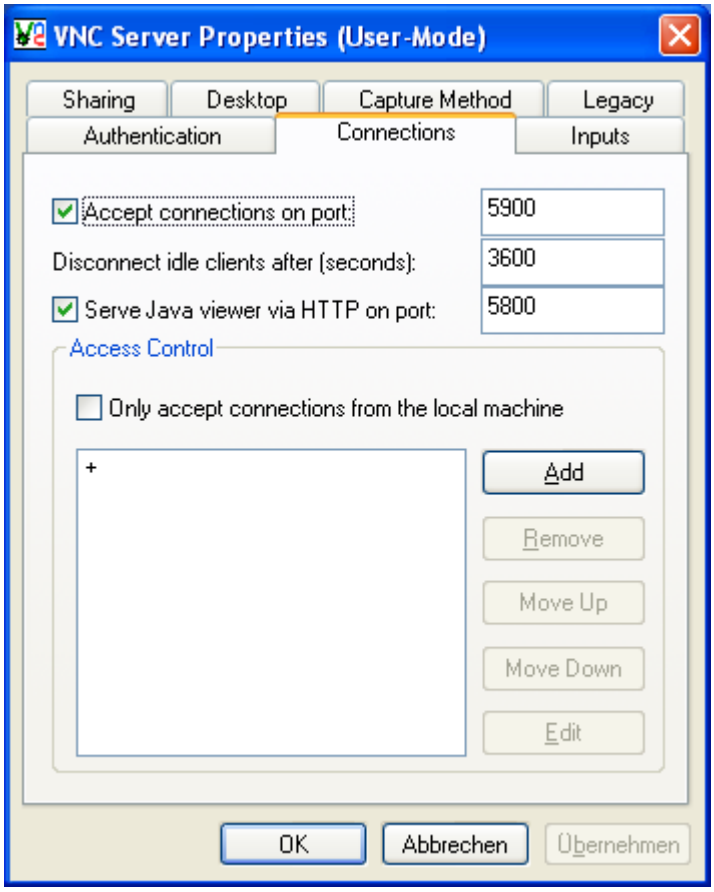
- für die VNC Verbindung wird der Standardport 5900 verwendet
- für die Telnet Verbindung wird wird der Standardport 23 verwendet
- die gesicherte Stunnel Verbindung wird über den Port 443 aufgebaut.
- der Proxy Server wird über den Port 3128 angesprochen.

Bei den Musterlösungen wird keine eigenes Zertifikat für den Aufbau des SSL Tunnels verwendet. Auch die Konfiguration des VNC Server bleibt rudimentär. Auf dem Client PC ist für die VNC Software keine Konfiguration erforderlich. Bei der Konfiguration des VNC Servers über die Eigenschaften (Properties) ist folgendes einzustellen, bzw. zu überprüfen.





Es ist ein Kennwort für den Verbindungsaufbau einzugeben. Wird später der VNC Viewer gestartet, dann wird genau dieses Kennwort abgefragt, um eine Verbindung aufzubauen.



Für die Musterlösung ist auf der Seite „Connectios“ eigentlich nichts einzutragen. Es ist sicherzustellen, dass der Port 5900 für „Accept connections on port“ eingestellt und die Option aktiv ist. Die Verbindung über den Java Viewer auf Port 5800 wird nicht benötigt und könnte auch deaktiviert werden.

Nach der Konfiguration der VNC Software muß nun noch der Stunnel konfiguriert werden. Nach der Installation steht auf Client und Server im Stunnel Programmverzeichnis eine Konfigurationsdatei mit dem Namen *stunnel.conf* zur Verfügung.Diese muß je nach Verwendung (Client oder Server) angepasst werden. Für die Musterlösungen sind nur wenige Konfigurationsänderungen in der Datei erforderlich.

Auf der Clientseite sind folgende Anpassungen notwendig:

Einstellung des Client Modus:

```
; Use it for client mode
client = yes
```

In der Service-Level Section sind alle nicht benötogten Verbindungen auf Kommentar zu setzen:

```
; Service-level configuration

;[pop3s]
;accept  = 995
;connect = 110

;[imaps]
;accept  = 993
;connect = 143
```

```
;[ssmtp]
;accept  = 465
;connect = 25
```

Weitere Anpassungen für die Clientseite sind speziell für die aufzubauende Verbindung und werden in den jeweiligen Kapiteln beschreiben.

Auf der Serverseite sind nachfolgende Anpassungen in der Konfigurationsdatei *stunnel.conf* durchzuführen:

In der Service-Level Section sind alle nicht benötogten Verbindungen auf Kommentar zu setzen:

```
; Service-level configuration

;[pop3s]
;accept  = 995
;connect = 110

;[imaps]
;accept  = 993
;connect = 143

;[ssmtp]
;accept  = 465
;connect = 25
```

Weitere Anpassungen für die Serverseite sind abhängig davon, ob es sich um eine VNC oder um eine Telnet Verbindung handelt. Die entsprechenden Einstellungen werden in den jeweiligen Kapiteln behandelt. Die Einstellungen auf der Serverseite sind unabhängig davon, ob die Verbindung über eine Proxy Server geführt wird oder nicht.

Für die Test über eine Proxy Server muß nun noch der Jana Server konfiguriert werden, damit dieser dann als Proxy für die VNC und Telnet Verbindungen genutzt werden kann. Das Symbol des Jana Servers im System Tray mit der rechten Maustaste anklicken und „Einstellungen“ wählen. Es wird nun die Administration des Server im Browser aufgerufen. Alternativ kann man im Browser auch

http://127.0.0.1:2506/jana-admin/index.shtml

aufrufen. Auf der nun angezeigten Seite „Jana Server Konfiguration“ den Button „Administrator“ anklicken. In der neu angezeigten Seite in der Navigation unter Konfiguration die Option „Grundeinstellungen“ selektieren.

Nun erscheint eine neue Seite und im Navigationsmenü unter „Grundeinstellungen“ ist die Auswahl „IP Adressen“ auszuwählen. Unter „Festlegen der IP Adressen“ ist in dem Feld „IP Adressen“ zu der dort bereits eingetragenen Adresse 127.0.0.1, mit einem Komma getrennt, noch die IP Adresse des Proxy Servers, z. B. 192.168.1.1, einzutragen. Danach den Button „Übernehmen“ anklicken.

Im unteren Teil „Funktionszuordnung für die Netzwerkarte(n)“ erscheint nun eine Spalte mit der soeben eingegebenen IP Adresse. Hier ist nun der Haken für diese IP Adresse in der Zeile „Http- / Ftp-Proxy“ zu setzen und anschliessend unten auf der Seite den Button „Übernehmen“ anklicken. Danach ist der Jana Server neu zu starten. Das kann man erreichen, in dem man oben auf der Seite den Button „Server neu starten“ anklickt.

Nun bleibt noch zu überprüfen, ob unter „Grundeinstellungen“ und „Ports“ die Standardeinstellung 3128 für den Http- /Ftp-Proxy aktiv ist. Will man sicher sein, dass der Proxy Server auch funktioniert, dann sollte man seinen Browser auf dem Client PC so konfigurieren, dass man den Proxy Server mit dem Port 3128 einstellt. Kann man nun weiterhin surfen, und wird in der Jana Server Administration unter „Server Info“ und „Logdateien“ ein „Proxy.log“ angezeigt, dann ist der Proxy Server aktiv. In der Logdatei kann man den Verbindungsaufbau vom Browser nachvollziehen.

WICHTIG: Die beschriebenen Konfigurationsschritte für den Proxy Server haben nicht den Anspruch einer vollständigen Konfiguration des Jana Servers. Es wurden nur die Schritte beschrieben, die erforderlich sind, damit der Proxy Server für die Musterlösungen verwendet werden kann.

Damit sind nun alle Konfigurationsschritte abgeschlossen, die für alle nachfolgenden Musterlösungen notwendig sind. Die weiteren Einstellungen werden in den einzelnen Kapiteln beschrieben. Ausgangspunkt für alle Musterlösungen ist aber die bis hierher beschriebene Konfiguration.

3. Gesicherte VNC Verbindung zwischen 2 Windows Systemen im Intranet

In diesem Kapitel wird beschrieben, wie ich eine SSL geschützte VNC Verbindung im lokalen Netz zwischen Client und Server herstellen kann. Die zuvor beschriebene Konfiguration der Stunnel Konfigurationsdatei stunnel.conf muß auf der Clientseite um folgende Anweisungen in der Service-Level Section erweitert werden:

```
[vnc]
accept = 5900
connect = serverpc:443
```

Für „serverpc“ muss der Hostname oder die IP Adresse des Remotesystems eingetragen werden. Danach kann man das Programm „stunnel.exe“ starten. Im System Tray erscheint ein Symbol. Über das Kontextmenü (rechte Maustaste) kann man das Protokoll auf dem Bildschirm anzeigen lassen.

Im Gegensatz zur Konfiguration auf dem Client PC ist die Konfiguration für Stunnel auf dem Server PC immer gleich. Egal ob direkt oder via Proxy Server die Verbindung aufgebaut wird. Wichtig ist nur, dass der gleiche Port (hier 443) auf Client und Server Seite verwendet wird. Die zusätzlichen Einstellungen in der Service-Level Section auf dem Server PC in der stunnel.conf sieht folgendermaßen aus:

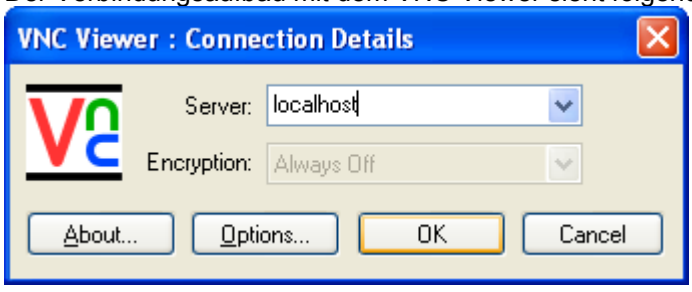
```
[vnc]
accept = 443
connect = 5900
```

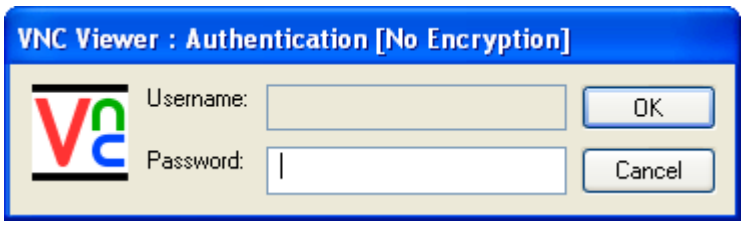
Danach kann auch auf dem Server PC das Programm stunnel.exe gestartet werden. Über das Symbol im System Tray kann auch hier die Protokolldatei angezeigt werden. Man sieht hier nach dem Start mehr Einträge als auf der Client Seite. Z. B. sieht man, dann ein Zertifikat geladen wird. Dieses ist für den Aufbau einer sicheren Verbindung zwischen Client und Server erforderlich.

Was bewirken nun die Einträge in den beiden Stunnel Konfigurationsdateien?

Auf dem Client PC (localhost) horcht das Programm Stunnel auf dem Port 5900. Wird hierüber eine Verbindung aufgebaut, dann baut Stunnel seinerseits eine Verbindung zu dem angegebenen „serverpc“ auf dem angegebenen Port „443“ eine Verbindung auf. Diese Verbindung wird über SSL verschlüsselt. Damit das auch funktioniert, muß das Programm Stunnel auf dem Server PC (serverpc) auf dem Port 443 horchen. Werden nun Daten über den SSL Tunnel geschickt, dann leitet das Stunnel Programm auf dem Server PC die Daten an den Port 5900 weiter. Auf diesem Port horcht der VNC Server, sofern dieser gestartet ist.

Der Verbindungsaufbau mit dem VNC Viewer sieht folgendermaßen aus:





Nachdem das Kennwort eingegeben worden ist, wird die VNC Session gestartet. In den Stunnel Protokolldateien, insbesonders auf dem Server PC, kann man sehr schön sehen, wie eine verschlüsselte Verbindung aufgebaut wird.

Würde man nun einen Netzwerksniffer, wie Ethereal, einsetzen, dann könnte man sehen, dass die übertragenen Pakete verschlüsselt sind.

4. Gesicherte VNC Verbindung via Proxy Server zwischen 2 Windows Systemen im Intranet

Als nächstes wiederholen wir den o. b. Verbindungsaufbau zwischen 2 Windows Systemen im internen Netz. Jedoch wird die VNC Session nicht direkt aufgebaut, sondern über einen Proxy Server. Man kann zurecht nach dem Sinn einer solchen Verbindung fragen. Aber hierbei handelt es sich ja um eine Musterlösung die beschreibt, wie eine solche Verbindung zu konfigurieren ist. Und dabei ist völlig unerheblich, ob es sich um eine Verbindung im internen Netz oder, wie wir später noch sehen werden, über das Internet handelt.

Auf dem Client PC ist die Konfigurationsdatei folendermaßen in der Service-Level Section anzupassen:

```
[vnc]
accept = 5900
connect = proxypc:3128
protocol = connect
protocolHost = serverpc:443
```

Hat man die im vorherigen Kapitel beschriebene Musterlösung getestet, dann ist eine Konfiguration auf Serverseite nicht mehr erforderlich. Ist das nicht der Fall, dann muß auf dem Server PC die stunnel.conf wie folgt ergänzt werden:

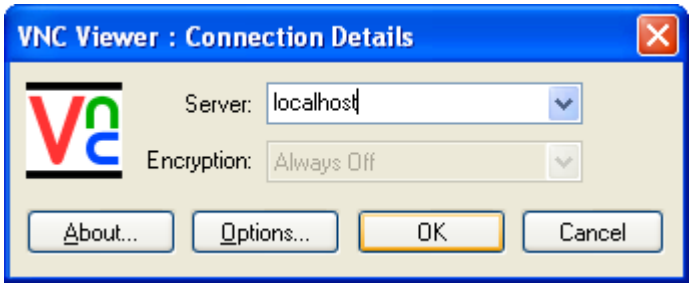
```
[vnc]
accept = 443
connect = 5900
```

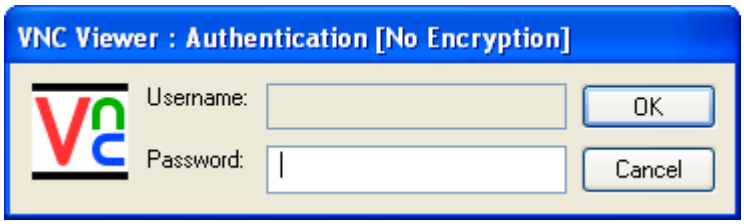
Anschliessend kann das Stunnel Programm auf Client- und Serverseite gestartet werden, bzw. beendet und neu gestartet werden, sofern es bereits aktiv war. Dieses ist erforderlich, damit die neuen Konfigurationsdaten eingelesen werden.

Was bewirken nun die Einträge in den beiden Stunnel Konfigurationsdateien?

Auf dem Client PC (localhost) horcht das Programm Stunnel auf dem Port 5900. Wird hierüber eine Verbindung aufgebaut, dann baut Stunnel seinerseits eine Verbindung zu dem angegebenen „proxypc“ auf dem angegebenen Port „3128“ eine Verbindung auf. Die weiteren Anweisungen „protocol“ und „protocolHost“ sind für den Proxy Server bestimmt, der nun ein „CONNECT“ zu dem angegebenen „serverpc“ auf Port 443 herstellen soll. Diese so hergestellte Verbindung wird über SSL verschlüsselt. Damit das auch funktioniert, muß das Programm Stunnel auf dem Server PC (serverpc) auf dem Port 443 horchen. Werden nun Daten über den SSL Tunnel geschickt, dann leitet das Stunnel Programm auf dem Server PC die Daten an den Port 5900 weiter. Auf diesem Port horcht der VNC Server, sofern dieser gestartet ist.

Der Verbindungsaufbau mit dem VNC Viewer sieht folgendermaßen aus:





Nachdem das Kennwort eingegeben worden ist, wird die VNC Session gestartet. In den Stunnel Protokolldateien, insbesonders auf dem Server PC, kann man sehr schön sehen, wie eine verschlüsselte Verbindung aufgebaut wird. Aber man kann auch sehen, dass die Verbindung nicht direkt vom Client kommt, sondern vom Proxy Server. Im Proxy Log des Proxy PC findet man ein „CONNECT“ Eintrag zum Server PC.

Würde man nun einen Netzwerksniffer, wie Ethereal, einsetzen, dann könnte man sehen, dass die übertragenen Pakete verschlüsselt sind.

5. Gesicherte TELNET Verbindung via Proxy Server zwischen 2 Windows Systemen im Intranet

Zusätzlich zu den beschriebenen Musterlösungen, die sich hauptsächlich mit VNC beschäftigen, möchte ich hier einen Weg aufzeigen, wie man auch eine Telnet Session über eine SSL Verbindung betreiben kann. In dieser Musterlösung wird der Weg über eine Proxy Server beschreiben. In Anlehnung an die Lösung für VNC ohne einen dazwischengeschalteten Proxy kann man problemlos auf die dort beschriebenen Art und Weise auch eine Telnet Verbindung aufbauen.

Als Voraussetzung für einen erfolgreichen Test muss der Telnet Server auf dem Server PC gestartet werden. Es werden hier keine besonderen Einstellungen, wie z. B. Benutzerdefinitionen. Aufzeigen möchte ich lediglich den Weg dahin. Zumal man sicher nicht unbedingt den von Windows mitgelieferten Telnetserver einsetzen wird.

Warum überhaupt eine Telnet Verbindung?

Man kann die hier beschriebenen Musterlösungen auch auf UNIX oder Linux Systeme übertragen. Auch für diese Betriebssysteme gibt es Stunnel. Oft gibt es standardmäßig nur einen Telnet Zugang zu solchen Systemen, nicht aber eine Möglihckeit mit SSH sich auf einen solchen Server zu verbinden. Für diese Fälle könnte man eine gesicherte Verbindung via Stunnel einrichten.

Auf dem Client PC ist die Konfigurationsdatei folendermaßen in der Service-Level Section anzupassen:

```
[telnet]
accept = 23
connect = proxypc:3128
protocol = connect
protocolHost = serverpc:443
```

Auf dem Server PC muss man die stunnel.conf wie folgt anpassen:

```
[telnet]
accept = 443
connect = 23
```

Anschliessend kann das Stunnel Programm auf Client- und Serverseite gestartet werden, bzw. beendet und neu gestartet werden, sofern es bereits aktiv war. Dieses ist erforderlich, damit die neuen Konfigurationsdaten eingelesen werden.

Was bewirken nun die Einträge in den beiden Stunnel Konfigurationsdateien?

Auf dem Client PC (localhost) horcht das Programm Stunnel auf dem Port 23. Wird hierüber eine Verbindung aufgebaut, dann baut Stunnel seinerseits eine Verbindung zu dem angegebenen „proxypc“ auf dem angegebenen Port „3128“ eine Verbindung auf. Die weiteren Anweisungen „protocol“ und „protocolHost“ sind für den Proxy Server bestimmt, der nun ein „CONNECT“ zu dem angegebenen „serverpc“ auf Port 443 herstellen soll. Diese so hergestellte Verbindung wird über SSL verschlüsselt. Damit das auch funktioniert, muß das Programm Stunnel auf dem Server PC (serverpc) auf dem Port 443 horchen. Werden nun Daten über den SSL Tunnel geschickt, dann leitet das Stunnel Programm auf dem Server PC die Daten an den Port 23 weiter. Auf diesem Port horcht der Telnet Server, sofern dieser gestartet ist.

Der Verbindungsaufbau für eine Telnet Verbindung sieht in eine DOS Eingabeaufforderung auf dem Client PC folgendermaßen aus:

```
telnet localhost
```

In den Stunnel Protokolldateien, insbesonders auf dem Server PC, kann man sehr schön sehen, wie eine verschlüsselte Verbindung aufgebaut wird. Aber man kann auch sehen, dass die Verbindung nicht direkt

vom Client kommt, sondern vom Proxy Server. Im Proxy Log des Proxy PC findet man ein „CONNECT“ Eintrag zum Server PC.

Würde man nun einen Netzwerksniffer, wie Ethereal, einsetzen, dann könnte man sehen, dass die übertragenen Pakete verschlüsselt sind.

6. Gesicherte VNC Verbindung zwischen 2 Windows Systemen über das Internet

In diesem Kapitel kehren wir nun zurück zu unseren VNC Verbindungen. Nachfolgend beschreibe ich den Weg, wie man aus dem internen Netz heraus eine VNC Session zu einem VNC Server via Internet aufbaut. Dabei muß man daran denken, dass ein PC System im Internet in den meisten Fällen keine feste IP Adresse hat. Das hat zur Folge, dass man zunächst über „ipconfig“ auf dem Server PC die aktuell gültige IP Adresse ermitteln muß, um diese dann in der stunnel.conf einzutragen. Möglich ist in solchen Fällen auch die Eingabe eines vollqualifizierten Hostnamen, sofern der PC im Internet sich bein einem Dienst, wie z. B. DynDNS, registriert hat. Denn dann braucht man nicht jedes Mal die IP Adresse zu ermitteln.

Die Konfiguration der stunnel.conf n der Service-Level Section auf dem Client PC muß folgendermaßen aussehen, damit eine Verbindung zu dem Server PC im Internet zustande kommt:

```
[vnc-int]
accept = 5900
connect = serverpc:443
```

Für „serverpc“ muss der Hostname oder die IP Adresse des Remotesystems eingetragen werden. Danach kann man das Programm „stunnel.exe“ starten. Im System Tray erscheint ein Symbol. Über das Kontextmenü (rechte Maustaste) kann man das Protokoll auf dem Bildschirm anzeigen lassen.

Im Gegensatz zur Konfiguration auf dem Client PC ist die Konfiguration für Stunnel auf dem Server PC immer gleich. Egal ob direkt oder via Proxy Server die Verbindung aufgebaut wird. Wichtig ist nur, dass der gleiche Port (hier 443) auf Client und Server Seite verwendet wird. Die zusätzlichen Einstellungen in der Service-Level Section auf dem Server PC in der stunnel.conf sieht folgendermaßen aus:

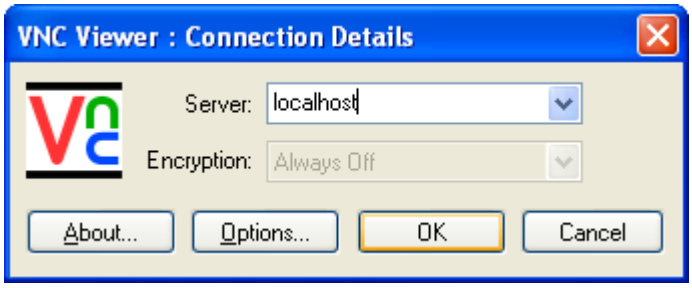
```
[vnc-int]
accept = 443
connect = 5900
```

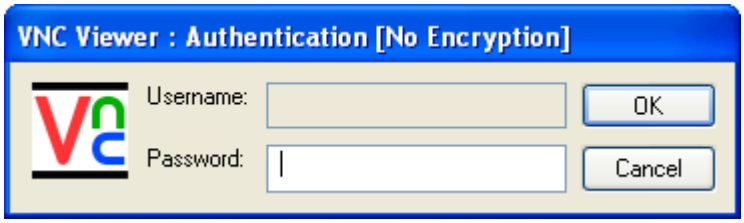
Danach kann auch auf dem Server PC das Programm stunnel.exe gestartet werden. Über das Symbol im System Tray kann auch hier die Protokolldatei angezeigt werden. Man sieht hier nach dem Start mehr Einträge als auf der Client Seite. Z. B. sieht man, dann ein Zertifikat geladen wird. Dieses ist für den Aufbau einer sicheren Verbindung zwischen Client und Server erforderlich.

Was bewirken nun die Einträge in den beiden Stunnel Konfigurationsdateien?

Auf dem Client PC (localhost) horcht das Programm Stunnel auf dem Port 5900. Wird hierüber eine Verbindung aufgebaut, dann baut Stunnel seinerseits eine Verbindung zu dem angegebenen „serverpc“ auf dem angegebenen Port „443“ eine Verbindung auf. Diese Verbindung wird über SSL verschlüsselt. Damit das auch funktioniert, muß das Programm Stunnel auf dem Server PC (serverpc) auf dem Port 443 horchen. Werden nun Daten über den SSL Tunnel geschickt, dann leitet das Stunnel Programm auf dem Server PC die Daten an den Port 5900 weiter. Auf diesem Port horcht der VNC Server, sofern dieser gestartet ist.

Der Verbindungsaufbau mit dem VNC Viewer sieht folgendermaßen aus:





Nachdem das Kennwort eingegeben worden ist, wird die VNC Session gestartet. In den Stunnel Protokolldateien, insbesonders auf dem Server PC, kann man sehr schön sehen, wie eine verschlüsselte Verbindung aufgebaut wird.

Würde man nun einen Netzwerksniffer, wie Ethereal, einsetzen, dann könnte man sehen, dass die übertragenen Pakete verschlüsselt sind.

7. Gesicherte VNC Verbindung via Proxy Server zwischen 2 Windows Systemen über das Internet

Die letzte vorgestellte Musterlösung kommt der Realität sehr nahe. In den meisten Fällen wird eine Verbindung von einem PC im internen Netz in das Internet über einen Proxy Server geführt. Die nachfolgende Musterlösung unterscheidet sich nur unwesentlich von der Lösung via Proxy Server im internen Netz. Aber auch hier gilt das schon in der letzte Musterlösung gesagte. Man muß daran denken, dass ein PC System im Internet in den meisten Fällen keine feste IP Adresse hat. Das hat zur Folge, dass man zunächst über „ipconfig“ auf dem Server PC die aktuell gültige IP Adresse ermitteln muß, um diese dann in der stunnel.conf einzutragen. Möglich ist in solchen Fällen auch die Eingabe eines vollqualifizierten Hostnamen, sofern der PC im Internet sich bein einem Dienst, wie z. B. DynDNS, registriert hat. Denn dann braucht man nicht jedes Mal die IP Adresse zu ermitteln.

Die Konfiguration der stunnel.conf n der Service-Level Section auf dem Client PC muß folgendermaßen aussehen, damit eine Verbindung zu dem Server PC im Internet zustande kommt:

```
[vnc-int]
accept = 5900
connect = proxypc:3128
protocol = connect
protocolHost = serverpc:443
```

Die Konfiguration für den Server PC im Internet unterscheidet sich nicht von der für eine Verbindung ohne Proxy Server und sieht wir folgt aus:

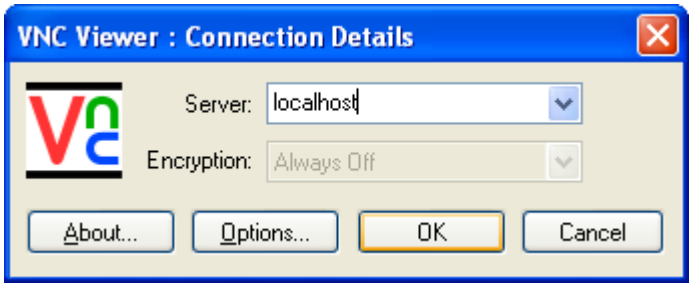
```
[vnc-int]
accept = 443
connect = 5900
```

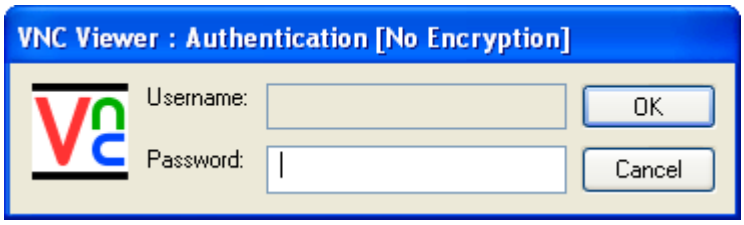
Anschliessend kann das Stunnel Programm auf Client- und Serverseite gestartet werden, bzw. beendet und neu gestartet werden, sofern es bereits aktiv war. Dieses ist erforderlich, damit die neuen Konfigurationsdaten eingelesen werden.

Was bewirken nun die Einträge in den beiden Stunnel Konfigurationsdateien?

Auf dem Client PC (localhost) horcht das Programm Stunnel auf dem Port 5900. Wird hierüber eine Verbindung aufgebaut, dann baut Stunnel seinerseits eine Verbindung zu dem angegebenen „proxypc“ auf dem angegebenen Port „3128“ eine Verbindung auf. Die weiteren Anweisungen „protocol“ und „protocolHost“ sind für den Proxy Server bestimmt, der nun ein „CONNECT“ zu dem angegebenen „serverpc“ auf Port 443 herstellen soll. Diese so hergestellte Verbindung wird über SSL verschlüsselt. Damit das auch funktioniert, muß das Programm Stunnel auf dem Server PC (serverpc) auf dem Port 443 horchen. Werden nun Daten über den SSL Tunnel geschickt, dann leitet das Stunnel Programm auf dem Server PC die Daten an den Port 5900 weiter. Auf diesem Port horcht der VNC Server, sofern dieser gestartet ist.

Der Verbindungsaufbau mit dem VNC Viewer sieht folgendermaßen aus:





Nachdem das Kennwort eingegeben worden ist, wird die VNC Session gestartet. In den Stunnel Protokolldateien, insbesonders auf dem Server PC, kann man sehr schön sehen, wie eine verschlüsselte Verbindung aufgebaut wird. Aber man kann auch sehen, dass die Verbindung nicht direkt vom Client kommt, sondern vom Proxy Server. Im Proxy Log des Proxy PC findet man ein „CONNECT“ Eintrag zum Server PC.

Würde man nun einen Netzwerksniffer, wie Ethereal, einsetzen, dann könnte man sehen, dass die übertragenen Pakete verschlüsselt sind.

Nun wird der eine oder andere zu Recht bemerken, dass in Unternehmen wohl selten ein Jana Proxy Server für den Zugang zum Internet eingesetzt wird. Ich habe die Verbindung auch über eine **Squid Proxy** getestet und diese ebenfalls ohne weiteres herstellen können. Am **Squid Proxy** mussten dafür keinerlei Anpassungen durchgeführt werden.

8. Bekannte Probleme in Zusammenhang mit den Musterlösungen

Einsatz des Checkpoint SecuRemote Client

Ich konnte feststellen, dass eine VNC Verbindung auf einem PC System mit installiertem SecuRemote Client nicht möglich war, wenn diese mit Desktop Security installiert worden ist.

Man kann auf die Desktop Security meiner Meinung nach verzichten, wenn man parallel noch eine Personal Firewall auf dem System installiert hat. Denn der Schutz ist dann doppelt, bzw. es kommt zu sogenannten „unpredictible results“, weil Freigaben in der Firewall u. U. nicht ziehen, weil sie über die Desktop Security zusätzlich noch geblockt sind. Da man aber keine Konfigurationsmöglichkeit für den SecuRemote Client hat, sollte man auf diese doppelte Sicherheit unter den genannten Umständen verzichten.

9. Anmerkungen zu Verwendung des Programmes Stunnel

Das Programm Stunnel ist eine elegante Möglichkeit ungesicherten Datenverkehr über das SSL Protokoll zu tunneln. Dieses beschränkt sich nicht nur auf die in dieser Dokumentation beschriebenen Verbindungen. Im Grunde kann man alle denkbaren TCP Verbindungen über Stunnel kapseln. Es gibt aber eine Ausnahme. Das FTP Protokoll kann nicht über Stunnel geführt werden, da FTP mit 2 Ports (20 u. 21) arbeitet. Aber für FTP gibt es mittlerweile genügend andere Lösungen um einen verschlüsselten Datenverkehr durchführen zu können.

Dennoch sollte man mögliche Riskiken beim Einsatz von Stunnel bedenken. Ermöglicht man Anwendern im internen Netz den direkten Zugang zum Internet, ob mit oder ohne Proxy Server, dann hat dieser Anwender durchaus die Möglichkeit das Produkt einzusetzen, um so ggf. die Restriktionen der eingesetzten Firewall zu umgehen. Da über die Firewall in den meisten Fällen die Ports 80 und 443 freigeschaltet hat, kann man genau diese Ports dazu nutzen, um eine Verbindung zu einem Server im Internet aufzubauen. Was immer auf dem anderen Ende steht. Der über diesen Tunnel geführte Verbindung ist verschlüsselt, und der Datenverkehr kann von Scannern nicht mehr geprüft werden.

Denkbar ist z. B., dass ein Proxy Server am anderen Ende des Tunnels wiederum Webseiten zur Verfügung stellt, die über den URL Blocker eines Unternehmens verboten sind. Aber auch andere, nicht gewollte Verbindungen könnten so aufgebaut werden.

Deshalb kann ich nur empfehlen keinem Anwender mit seinem lokalen PC den Zugang zum Internet zu ermöglichen. Der Zugang sollte nur über ein Terminalserver möglich sein. Damit gibt man der Administration die Kontrolle über die Programme und Systeme, die Sessions ins Internet aufbauen können. Und dann kann man auch über den Einsatz von Stunnel für besondere Anforderungen (z. B. VNC) nachdenken.

Bevor man jedoch Stunnel einsetzt, sollte man in der Lage sein Zertifikate auszustellen. Ein produktiver Betrieb mit dem von Stunnel in der Datei *stunnel.pem* mitgelieferten Zertifikat ist nicht ratsam.

Während ein Verbindungsaufbau im Intranet so recht einfach zu handhaben ist, weil man die Systeme über einen festen Hostnamen mit Hilfe eines Domain Name Servers erreicht, stellt sich der Aufbau einer Verbindung über das Internet etwas schwieriger da. Wie schon erwähnt, haben PCs im Internet meistens keine feste IP Adresse. Dadurch muß die Konfigurationsdatei stunnel.conf vor der Verwendung für eine Remote Verbindung via VNC immer angepasst und Stunnel neu gestartet werden.

Läuft Stunnel auf der Clientseite als Dienst, dann kann man diesen unter Angabe einer Konfigurationsdatei neu starten. Unproblematisch ist die Serverseite von Stunnel. Für eine VNC Verbindung ist diese immer identisch konfiguriert.

Denkbar ist auch, dass sich Dial In Clients über eine DynDNS Software bei einem dynamischen DNS Dienst (z. B. DynDNS) nach der Einwahl ins Internet anmelden. So wäre der betreffende PC immer unter dem gleichen vollqualifizierten Hostnamen im Internet erreichbar.

Befindet sich der Server PC (= VNC Server) hinter einem Router in einem lokalen Netzwerksegement, dann gilt im Grunde das gleiche, als wenn der PC direkt im Internet angemeldet ist. Allerdings ist es für den Anwender an genau diesem PC schwieriger die IP Adresse zu ermitteln, mit der der Router im Internet eingewählt ist. Auch hier bietet sich die Verwendung von DynDNS für den Router an. Viele Router unterstützen diese Funktion. Wichtig ist auch, dass auf dem Router der Zugang zu dem Stunnel Port (in den Musterlösungen ist das Port 443) zu den internen PC Systemen freigeschaltet ist.

10. Linkliste

Nachfolgend aufgeführte Links sind für diese Dokumentation hilfreich:

Webseite des Stunnel Programmes
http://www.stunnel.org

Webseite des VNC Programmes
http://www.realvnc.com

Webseite des Jana Server Programmes
http://www.janaserver.de/start.php?lang=de

Webseite zum Netzwerksniffer Ethereal
http://www.ethereal.com/

OppenSSL Webseite
http://www.openssl.org/

DynDNS Webseite
http://www.dyndns.com/

Impressum

Diese Dokumentation wurde erstellt von

Peter Neugebauer
Kiebitzgrund 50

D-49477 Ibbenbüren

mailto: kontakt@neugebauer-ibb.de

Version: 1.0
Datum: 05.11.2006

Für Hinweise über eventuelle Fehler in dieser Dokumentation an die o. a. Mailadresse wäre ich sehr dankbar.