

Sicherer Remote Desktop über DSL, Dynamic IP, Ssh, Remmina

David Kastrup

19. März 2016

Das Problem

- ▶ Linuxkenner hilft Linuxnutzer

Das Problem

- ▶ Linuxkenner hilft Linuxnutzer
- ▶ Nach Anfangsinstallation räumliche Trennung

Das Problem

- ▶ Linuxkenner hilft Linuxnutzer
- ▶ Nach Anfangsinstallation räumliche Trennung
- ▶ Verbindung über Telefon

Das Problem

- ▶ Linuxkenner hilft Linuxnutzer
- ▶ Nach Anfangsinstallation räumliche Trennung
- ▶ Verbindung über Telefon
- ▶ „Ich habe nichts gemacht“

Das Problem

- ▶ Linuxkenner hilft Linuxnutzer
- ▶ Nach Anfangsinstallation räumliche Trennung
- ▶ Verbindung über Telefon
- ▶ „Ich habe nichts gemacht“
- ▶ Verbindungsmöglichkeit über DSL/Internet

Das Problem

- ▶ Linuxkenner hilft Linuxnutzer
- ▶ Nach Anfangsinstallation räumliche Trennung
- ▶ Verbindung über Telefon
- ▶ „Ich habe nichts gemacht“
- ▶ Verbindungsmöglichkeit über DSL/Internet
- ▶ Kernengpaß für Konfiguration: DSL-Modem beim Nutzer

Beteiligte Technologien

`ssh/sshd` Authentifizierung/Sichere Übertragung von eigenem Account auf Heimlaptop zu eigenem Account auf Fremdrechner

Beteiligte Technologien

`ssh/sshd` Authentifizierung/Sichere Übertragung von eigenem Account auf Heimlaptop zu eigenem Account auf Fremdrechner

`DynDNS` Identifizierung im Internet

Beteiligte Technologien

`ssh/sshd` Authentifizierung/Sichere Übertragung von eigenem Account auf Heimlaptop zu eigenem Account auf Fremdrechner

`DynDNS` Identifizierung im Internet

`NAT` Durchleiten von Ports

Beteiligte Technologien

- `ssh/sshd` Authentifizierung/Sichere Übertragung von eigenem Account auf Heimlaptop zu eigenem Account auf Fremdrechner
- `DynDNS` Identifizierung im Internet
- `NAT` Durchleiten von Ports
- `Firewall` Absicherung nach außen

Beteiligte Technologien

ssh/sshd Authentifizierung/Sichere Übertragung von eigenem Account auf Heimlaptop zu eigenem Account auf Fremdrechner

DynDNS Identifizierung im Internet

NAT Durchleiten von Ports

Firewall Absicherung nach außen

Remmina Bildschirmanzeige auf Heimlaptop nach Tunneln durch Ssh-Verbindung

Beteiligte Technologien

ssh/sshd Authentifizierung/Sichere Übertragung von eigenem Account auf Heimlaptop zu eigenem Account auf Fremdrechner

DynDNS Identifizierung im Internet

NAT Durchleiten von Ports

Firewall Absicherung nach außen

Remmina Bildschirmanzeige auf Heimlaptop nach Tunneln durch Ssh-Verbindung

VNC Übertragung des Bildschirminhalts von Fremduser auf Fremdrechner zu eigenem Account auf Fremdrechner

Vorbereitung daheim

Am eigenen Laptop.

- ▶ `sudo apt-get install openssh-client`

Vorbereitung daheim

Am eigenen Laptop.

- ▶ `sudo apt-get install openssh-client`
- ▶ `ssh-keygen -t rsa` als Benutzer aufrufen, falls noch nicht geschehen

Vorbereitung daheim

Am eigenen Laptop.

- ▶ `sudo apt-get install openssh-client`
- ▶ `ssh-keygen -t rsa` als Benutzer aufrufen, falls noch nicht geschehen
- ▶ `~/.ssh/id_rsa.pub` auf USB-Stick kopieren

Vorbereitung daheim

Am eigenen Laptop.

- ▶ `sudo apt-get install openssh-client`
- ▶ `ssh-keygen -t rsa` als Benutzer aufrufen, falls noch nicht geschehen
- ▶ `~/.ssh/id_rsa.pub` auf USB-Stick kopieren
- ▶ `sudo apt-get install remmina`

Vorbereitung daheim

Am eigenen Laptop.

- ▶ `sudo apt-get install openssh-client`
- ▶ `ssh-keygen -t rsa` als Benutzer aufrufen, falls noch nicht geschehen
- ▶ `~/.ssh/id_rsa.pub` auf USB-Stick kopieren
- ▶ `sudo apt-get install remmina`
- ▶ Anmelden bei DynDNS-Anbieter (z.B.: selfhost.de)

Vorbereitung daheim

Am eigenen Laptop.

- ▶ `sudo apt-get install openssh-client`
- ▶ `ssh-keygen -t rsa` als Benutzer aufrufen, falls noch nicht geschehen
- ▶ `~/.ssh/id_rsa.pub` auf USB-Stick kopieren
- ▶ `sudo apt-get install remmina`
- ▶ Anmelden bei DynDNS-Anbieter (z.B.: `selfhost.de`)
- ▶ DynDNS-ID und Hostnamen einrichten

Vorbereitung daheim

Am eigenen Laptop.

- ▶ `sudo apt-get install openssh-client`
- ▶ `ssh-keygen -t rsa` als Benutzer aufrufen, falls noch nicht geschehen
- ▶ `~/.ssh/id_rsa.pub` auf USB-Stick kopieren
- ▶ `sudo apt-get install remmina`
- ▶ Anmelden bei DynDNS-Anbieter (z.B.: `selfhost.de`)
- ▶ DynDNS-ID und Hostnamen einrichten
- ▶ Zugangsdaten abschreiben

Zugangsdaten DynDNS-Service

<i>DYN-DNS Accounts</i>					
Aliasname (ID)	Aktuelle IP	Letztes Update	Updates	LOGIN	Löschen
hans (35 [REDACTED])	78.5 [REDACTED]	18.03.2016 02:24:06	1	Details	X
standard (24 [REDACTED])	80.14 [REDACTED]	02.03.2016 08:53:14	3	Details	X

Neuen DYN-DNS Account anlegen ✓

Zugangsdaten DynDNS-Service

DYN Account hans (ID: 35 [REDACTED]) Aktion: modifi	
Zugangsdaten Updateclient	
Benutzername:	35 [REDACTED]
Password:	[REDACTED]
Hostname:	[REDACTED].selfhost.eu
manuelle Update URL erstellen	
<input checked="" type="radio"/> Authentifizierung per GET-Parameter Hilfe	
<input type="radio"/> Authentifizierung per HTTP (Basic Authentication) Hilfe	
gewünschte Update IP	<input type="text" value="[REDACTED]"/> (Vorgabe: IP vom Browser)
Optionen	<input type="checkbox"/> Textausgabe (Ausgabe mit OK/Error Text) <input type="checkbox"/> Hostliste (Ausgabe der Hostliste) <input type="checkbox"/> Aufruf zur Ausgabe von dyndns.org Return Codes [Hilfe] <input type="checkbox"/> Remoteliste (Ausgabe der aktiven IP Checker) <input type="checkbox"/> HTTP Status des Apache verwenden
[Informationen zur API Schnittstelle]	
URL erstellen	

Arbeiten vor Ort: dyndns im Router

- ▶ Expertenmodus?

Arbeiten vor Ort: dyndns im Router

- ▶ Expertenmodus?
- ▶ DynDNS-Anbieter, DynDNS-Hostname, DynDNS-ID (nicht Account-ID!), DynDNS-Paßwort (nicht Account-Paßwort!)

Arbeiten vor Ort: dyndns im Router

- ▶ Expertenmodus?
- ▶ DynDNS-Anbieter, DynDNS-Hostname, DynDNS-ID (nicht Account-ID!), DynDNS-Paßwort (nicht Account-Paßwort!)

Erleben, was verbindet.

T

Speedport W 723V

Startseite

Assistent

Schritt für Schritt

Konfiguration

Sicherheit

Netzwerk

Telefonie

Status

Übersicht

Details

Verwaltung

Hilfsmittel

Laden & Sichern

Beenden & Logout

Netzwerk / Dynamisches DNS

Dynamisches DNS

Aus Ein

Anbieter für Dynamisches DNS

Anbieter-Auswahl: Selfhost.de

Zugangsdaten für Selfhost.de

Domänenname:

Benutzername:

Kennwort:

Kennwort wiederholen:

Informationen

Dynamisches DNS

Über den Dynamischen DNS-Dienst können Sie Ihrem Router einen individuellen, festen Domännennamen im Internet zuweisen, auch wenn er keine feste IPv4-Adresse hat. Der feste (statische) Namen der Domäne wird dabei an eine dynamische IPv4-Adresse gebunden.

Um diesen Dienst nutzen zu können, benötigen Sie ein vom Anbieter des Dynamischen DNS-Dienstes eingerichtetes Konto, ein Passwort und Ihren statischen Domännennamen.

Arbeiten vor Ort: NAT im Router

- ▶ Expertenmodus? Freigaben? Portfilter?

Arbeiten vor Ort: NAT im Router

- ▶ Expertenmodus? Freigaben? Portfilter?
- ▶ Für gewählten Rechner: Port 22 (ssh) durchschalten

Arbeiten vor Ort: NAT im Router

- ▶ Expertenmodus? Freigaben? Portfilter?
- ▶ Für gewählten Rechner: Port 22 (ssh) durchschalten

Erleben, was verbindet.

T

Speedport W 723V

- Startseite
- Assistent
 - Schritt für Schritt
- Konfiguration
 - Sicherheit
 - Netzwerk**
 - Telefonie
- Status
 - Übersicht
 - Details
- Verwaltung
 - Hilfsmittel
 - Laden & Sichern
- Beenden & Logout

Netzwerk / NAT & Portregeln / Portregel

Regel-Definition

Portregel aktivieren:

Bezeichnung:

Art der Regel:

Betroffenes Gerät

Gültig für Gerät:

Weitergeleitete Ports / Portbereiche - Öffentlich & Private Client

TCP-Portbereich(e):

UDP-Portbereich(e):

Informationen

Portregel bearbeiten

Hier können Sie eine bereits angelegte Regel bearbeiten. Dabei kann die 'Art der Regel' nicht geändert werden.

↻ 🔍 🔄

Arbeiten vor Ort: ssh

Laptop und USB-Stick oder anderes Speichermedium mitbringen.

- ▶ Eigenen Benutzeraccount anlegen (am einfachsten mit demselben Nutzernamen wie daheim).

Arbeiten vor Ort: ssh

Laptop und USB-Stick oder anderes Speichermedium mitbringen.

- ▶ Eigenen Benutzeraccount anlegen (am einfachsten mit demselben Nutzernamen wie daheim).
- ▶ `sudo apt-get install openssh-server`

Arbeiten vor Ort: ssh

Laptop und USB-Stick oder anderes Speichermedium mitbringen.

- ▶ Eigenen Benutzeraccount anlegen (am einfachsten mit demselben Nutzernamen wie daheim).
- ▶ `sudo apt-get install openssh-server`
- ▶ Kopiere `~/.ssh/id_rsa.pub` vom eigenen Laptop (über USB-Stick) auf `~/.ssh/authorized_keys` unter meinem Benutzeraccount auf Zielsystem

Arbeiten vor Ort: ssh

Laptop und USB-Stick oder anderes Speichermedium mitbringen.

- ▶ Eigenen Benutzeraccount anlegen (am einfachsten mit demselben Nutzernamen wie daheim).
- ▶ `sudo apt-get install openssh-server`
- ▶ Kopiere `~/.ssh/id_rsa.pub` vom eigenen Laptop (über USB-Stick) auf `~/.ssh/authorized_keys` unter meinem Benutzeraccount auf Zielsystem
- ▶ In `/etc/ssh/sshd_config`: `PasswordAuthentication no`

Arbeiten vor Ort: ssh

Laptop und USB-Stick oder anderes Speichermedium mitbringen.

- ▶ Eigenen Benutzeraccount anlegen (am einfachsten mit demselben Nutzernamen wie daheim).
- ▶ `sudo apt-get install openssh-server`
- ▶ Kopiere `~/.ssh/id_rsa.pub` vom eigenen Laptop (über USB-Stick) auf `~/.ssh/authorized_keys` unter meinem Benutzeraccount auf Zielsystem
- ▶ In `/etc/ssh/sshd_config`: `PasswordAuthentication no`
- ▶ Eigener Laptop ins Internet, Shell öffnen und

Arbeiten vor Ort: ssh

Laptop und USB-Stick oder anderes Speichermedium mitbringen.

- ▶ Eigenen Benutzeraccount anlegen (am einfachsten mit demselben Nutzernamen wie daheim).
- ▶ `sudo apt-get install openssh-server`
- ▶ Kopiere `~/.ssh/id_rsa.pub` vom eigenen Laptop (über USB-Stick) auf `~/.ssh/authorized_keys` unter meinem Benutzeraccount auf Zielsystem
- ▶ In `/etc/ssh/sshd_config`: `PasswordAuthentication no`
- ▶ Eigener Laptop ins Internet, Shell öffnen und
- ▶ `ssh user@dyndns.name`

Arbeiten vor Ort: Screensharing

Jetzt muß der Betreute sich einloggen.

- ▶ `sudo apt-get install vnc4server`

Arbeiten vor Ort: Screensharing

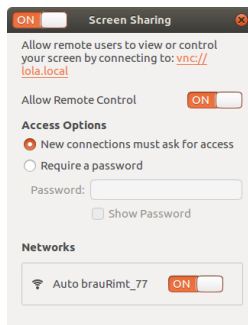
Jetzt muß der Betreute sich einloggen.

- ▶ `sudo apt-get install vnc4server`
- ▶ Einstellungen/Sharing: Sharing des Bildschirms erlauben

Arbeiten vor Ort: Screensharing

Jetzt muß der Betreute sich einloggen.

- ▶ `sudo apt-get install vnc4server`
- ▶ Einstellungen/Sharing: Sharing des Bildschirms erlauben



Remmina Connection Editor

Auf Eigenlaptop:

Remote Desktop Preference

Profile

Name: Hans

Group: [Empty]

Protocol: VNC - Virtual Network Computing

Basic Advanced SSH

Server: [Redacted] selfhost.eu

Repeater: [Empty]

User name: dak

Password: [Empty]

Color depth: 256 colors

Quality: Medium

Show remote cursor View only

Disable clipboard sync Disable encryption

Disable server input

Save Cancel Connect Default

Remote Desktop Preference

Profile

Name: Hans

Group: [Empty]

Protocol: VNC - Virtual Network Computing

Basic Advanced SSH

Enable SSH tunnel Tunnel via loopback address

Same server at port 22

Custom: [Empty]

Character set: [Empty]

SSH Authentication

User name: dak

Identity file: (None)

Password

Public key (automatic)

Save Cancel Connect Default

Problembehebung

Meist Telefonhilfe, teilweise mit technisch begabteren Personen

- ▶ DSL-Modem defekt oder verstellt: Screendumps aller Modemeinstellungen helfen bei Neukonfigurierung nach Austausch

Problembhebung

Meist Telefonhilfe, teilweise mit technisch begabteren Personen

- ▶ DSL-Modem defekt oder verstellt: Screendumps aller Modemeinstellungen helfen bei Neukonfigurierung nach Austausch
- ▶ Rechner defekt: Festplatte in neuen Rechner. Etwaige Windowspartitionen verweigern danach die Weiterarbeit.

Problembehebung

Meist Telefonhilfe, teilweise mit technisch begabteren Personen

- ▶ DSL-Modem defekt oder verstellt: Screendumps aller Modemeinstellungen helfen bei Neukonfigurierung nach Austausch
- ▶ Rechner defekt: Festplatte in neuen Rechner. Etwaige Windowspartitionen verweigern danach die Weiterarbeit.
- ▶ Achtung: MAC-gebundene Identifizierung des Rechners kann nach Wechsel fehlschlagen! Software-Spoofing der MAC-Adresse h"ilfe, ist bei Rechnerupgrade mit zwei Rechnern und gleichem System aber "u"berst problematisch.

Problembehebung

Meist Telefonhilfe, teilweise mit technisch begabteren Personen

- ▶ DSL-Modem defekt oder verstellt: Screendumps aller Modemeinstellungen helfen bei Neukonfigurierung nach Austausch
- ▶ Rechner defekt: Festplatte in neuen Rechner. Etwaige Windowspartitionen verweigern danach die Weiterarbeit.
- ▶ Achtung: MAC-gebundene Identifizierung des Rechners kann nach Wechsel fehlschlagen! Software-Spoofing der MAC-Adresse h"ilfe, ist bei Rechnerupgrade mit zwei Rechnern und gleichem System aber "u"berst problematisch.
- ▶ Eigene & lokale Pa"sw"orter: Aufschreiben, mitnehmen. Wozu?

Problembehebung

Meist Telefonhilfe, teilweise mit technisch begabteren Personen

- ▶ DSL-Modem defekt oder verstellt: Screendumps aller Modemeinstellungen helfen bei Neukonfigurierung nach Austausch
- ▶ Rechner defekt: Festplatte in neuen Rechner. Etwaige Windowspartitionen verweigern danach die Weiterarbeit.
- ▶ Achtung: MAC-gebundene Identifizierung des Rechners kann nach Wechsel fehlschlagen! Software-Spoofing der MAC-Adresse h"ilfe, ist bei Rechnerupgrade mit zwei Rechnern und gleichem System aber "u"berst problematisch.
- ▶ Eigene & lokale Pa"sw"orter: Aufschreiben, mitnehmen. Wozu?
- ▶ N"otig f"ur sudo, u.U. n"otig f"ur Modemzugriff

Problembehebung

Meist Telefonhilfe, teilweise mit technisch begabteren Personen

- ▶ DSL-Modem defekt oder verstellt: Screendumps aller Modemeinstellungen helfen bei Neukonfigurierung nach Austausch
- ▶ Rechner defekt: Festplatte in neuen Rechner. Etwaige Windowspartitionen verweigern danach die Weiterarbeit.
- ▶ Achtung: MAC-gebundene Identifizierung des Rechners kann nach Wechsel fehlschlagen! Software-Spoofing der MAC-Adresse hölfe, ist bei Rechnerupgrade mit zwei Rechnern und gleichem System aber äußerst problematisch.
- ▶ Eigene & lokale Paßwörter: Aufschreiben, mitnehmen. Wozu?
- ▶ Nötig für sudo, u.U. nötig für Modemzugriff
- ▶ Administrations-Paßwörter: Aufschreiben/Dokumentieren, in Hefter vor Ort lassen. Wozu?

Problembehebung

Meist Telefonhilfe, teilweise mit technisch begabteren Personen

- ▶ DSL-Modem defekt oder verstellt: Screendumps aller Modemeinstellungen helfen bei Neukonfigurierung nach Austausch
- ▶ Rechner defekt: Festplatte in neuen Rechner. Etwaige Windowspartitionen verweigern danach die Weiterarbeit.
- ▶ Achtung: MAC-gebundene Identifizierung des Rechners kann nach Wechsel fehlschlagen! Software-Spoofing der MAC-Adresse hölfe, ist bei Rechnerupgrade mit zwei Rechnern und gleichem System aber äußerst problematisch.
- ▶ Eigene & lokale Paßwörter: Aufschreiben, mitnehmen. Wozu?
- ▶ Nötig für sudo, u.U. nötig für Modemzugriff
- ▶ Administrations-Paßwörter: Aufschreiben/Dokumentieren, in Hefter vor Ort lassen. Wozu?
- ▶ Nützlich für potentielle andere Helfer. Wer Computer stiehlt, ist nicht an Accountdaten interessiert.