IPCOP Version 1.4.10 VPN von Blau auf Grün mit Zerina und OpenVPN

Grundsätzliches

Dieses Tutorial setzt eine Funktionierente Grundkonfiguration wie in dem Tutorial zur Installation des IPcop voraus (www.ipcop.org). Die IP-Adressen müssen an der lokalen Systemkonfiguration angepasst werden.

Vorbereitung

1. Grundkonfiguration des IPcop erfolgreich durchgeführt.

- Einwahl ins Internet Möglich / Ping auf z.B www.heise.de
- 2. Blaue Netzwerkkarte installiert und konfiguriert.

- Eine Internetverbindung über WLAN ist möglich / Ping auf z.B

VVVV	<u>/ v v . i</u>	lers	<u>se.</u>	Je	

Geräte auf Blau			l	
Hostname	Quell-IP-Adresse	MAC-Adresse	Anmerkung	Aktion
x20.localdomain	192.168.1.2	00	Tobias	🗹 🦉 🗍

3. Download der zu Benötigten Komponenten.

- PuttY (Telnet und SSH Client) http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

- WinSCP (SFTP und SCP Client) http://winscp.net/eng/download.php

- Zerina OpenVPN Erweiterung für IPCOP <u>http://www.zerina.de/downloads/</u>

- OpenVPN GUI für Windows http://openvpn.se/download.html



Installation von Zerina auf IPCOP

 Sitzung gespeicherte Sitzunger Umgebung Verzeichnisse SSH Einstellungen 	Sitzung		D
	192.168.0.1		Portnummer
			222 🗔
	<u>B</u> enutzername	<u>K</u> ennwort	
	root	•••••	
	Protokoll		
	C <u>s</u> ftp ⊙ sft	P (notfalls SCP)	C SCP
			arbe auswäh
Expertenmodus			aibe a <u>u</u> swai

1. WinSCP Starten und Verbindung zu IPCOP herstellen

2. Im / root Verzeichnis des IPCOPS ein neues Verzeichnis openvpn erstellen (rechte Maustate – Neu – Verzeichnis)

🍢 / - root@IPCOP - WinSCP				
Datei Befehle Markierung Sitzu	ng <u>A</u> nsicht <u>H</u> ilfe	e		
Adresse 🗀 /				💽 💽
		r 🖉 🖂 🖟	a 🔤 🛃 💼	9
🔹 🖃 - 💽 🎲 - 隆 Sta	andard	• • 5	•	
 ✓ / <root></root> ✓ bin ✓ boot ✓ dev ✓ etc ✓ home ✓ lib ✓ lost+found ✓ mnt ✓ openvpn ✓ proc ✓ root ✓ sbin ✓ sbin ✓ war 	bin boot dev bot bot bot bot bot bot bot bot bot bot			
0 B von 32.768 KB in 0 von 16	4.518 B	335 B	SFTP (v3)	0:01:33



3. ZERINA0.9.3bInstaller.tar.gz ins Verzeichnis openvpn Kopieren

Kopiere				? ×
Kopiere Datei ZERINA0.9	.3blinstaller.tar.gz' nach Ei	ntferntes Verzeicł	nnis	
/openvpn/*.*				-
🔲 Im Hintergrund übertrag	gen (In die Übertragungs <u>l</u> i	ste aufnehm		
Profile	<u>M</u> ehr>>	Kopiere	Abbrechen	Hilfe

WinSCP kann	jetzt	Beendet	werden.
-------------	-------	---------	---------

4. Mit PuttY die Verbindung zum IPCOP herstellen

Session	Basic options for your PuTTY s	ession
Logging Terminal Keyboard Bell Features Window	Specify your connection by host name or Host <u>Name (or IP address)</u> [192.168.0]1 Protocol: <u>© R</u> aw <u>© I</u> elnet <u>©</u> Rlogin	IP address Port 222 © <u>S</u> SH
Appearance Behaviour Translation Selection Colours	Load, save or delete a stored session Saved Sessions IPCOP	
- Connection	IPCOP	
- Data Proxu		Save
- Telnet - Rlogin		<u>D</u> elete
- Kex - Auth - X11	Close <u>w</u> indow on exit: C Always C Never © Only on	clean exit



5. Mit Benutzer root und root/Passwort am IPCOP anmelden

- mit cd / ins root Verzeichnis Wechseln
- mit cd openvpn ins openvpn Verzeichnis wechseln
- über tar xzvf ZERINA0.9.3blnstaller.tar.gz die Datei entpacken



- mit ./install Zerina Installieren

```
🚰 192.168.0.1 - PuTTY
                                                                   - 🗆 X
misc/header.old
misc/header
misc/rc.firewall.local.start
misc/rc.local.zerina
OKI
3. Backing up files for easy uninstall .. OK!
4. Installing new files .... OK!
... OK!
5. Adding entrys .....
ZERINA Installer finished
   * You can now access OpenVPN via the IPCop web gui.
   * WARNING: This package is NOT an official IPCop addon. It hasn't b
een
     approved or reviewed by the IPCop development team. It comes with
 NO
     warranty or guarantee, so use it at your own risk.
   * WARNING: You have to create your own certificates for OpenVPN!
   * For support try: www.openvpn-forum.de
   * howto : http://home.arcor.de/u.altinkaynak
root@ipcop:/openvpn #
```



6.Bugfix über WinSCP einspielen

- mit WinSCP auf IPCOP Connecten
- bugfix Downloaden http://www.zerina.de/wp-content/openvpnctrl.tar
- Datei in /usr/local/bin Kopieren.



- mit PuttY auf IPCOP Verbinden und als root anmelden
- cd / ins /root Verzeichnis wechseln

Folgende Schritte ausführen:

- tar xvf openvpnctrl.tar -C /usr/local/bin
- chown root.nobody /usr/local/bin/openvpnctrl
- chmod 4750 /usr/local/bin/openvpnctrl
- IPCOP neu Starten



Konfiguration von OpenVPN im WebInterface

1. Durch Aktualisieren des WebInterface ist der neue Menüeintrag OPENVPN im Register VPNs zu sehen.

VPNs 🚸	OPEN¥PN +	The bad packets stop here.	
SYSTEM + STATUS +	NETZWERK * DIENSTE *	FIREWALL * VPNS * LOGS *	B
		VPNs	
Globale Einstellungen		OPENVPN	2
OpenVDN Server Status			
OpenVPN server status:			
OpenVPN auf RLAU			
Lokaler VPN Hostname/IP:		OpenVPN Subnetz (z.B. 10.0.10.0/255.255.2	:55.0) 10.202.29.0/255.255.255.0
OpenVPN Gerät	TUN 💌		
Protokoll		Ziel-Port:	1194
MTU Size:	1400		
LZO-Kompression:		Verschlüsselung:	BF-CBC
No. 1	A.I		-

- 2. Konfiguration der einzelnen Punkte
 - Aktivieren von "OpenVPN auf Blau"

- Lokaler VPN Hostname/IP

(Hier wird die IP Adresse ROTEN Interfaces oder die Statische IP-Adresse des WAN's eingetragen)

- OpenVPN Subnetz (Vorgeschlagene IP-Adresse übernehmen)

- OpenVPN Gerät = TUN
- Protokoll = UTP
- MTU Size = 1400
- LZO-Kompresion = Aktivieren
- Ziel Port = 1194
- Verschlüsselung = BF-CBC



3. Erzeugen eines Root-Host Zertifikates

Erzeuge koot/Host Zertifikate:		
Name der Organisation:	MS Solutions	
IPCop's Hostname:		
Ihre E-mail Adresse: 鱼	t.goehl@ms-solutions-it.de	
Ihre Abteilung: 鱼	IT	
Stadt: 鱼	Untersteinach	
Bundesstat oder Provinz: 鱼	Bayern	
Land:	Germany	
	Erzeuge Root/Host Zertifikate	

- 4. Einrichten eines Zertifikates für eine Roardwarrior Verbindung
 - im IPCOP Interface bei "Client Status und Kontrolle auf Hinzufügen Klicken



- Verbindungstyp: Host-zu-Netz Virtual Private Network (RoadWarrior)
- Die Geforderten Daten eintragen und Speichern

Verbindung:		
Name: Anmerkung: • Aktiviert: 🗹	MS MS-Soluti	ions
Authentifizierung:		
 C Eine Zertifikatsanfra C Ein Zertifikat hochla 	ge hochladen den:	n: Durchsuchen
 Erzeuge ein Zertifika Voller Name oder Sy Hostaname des Ben 	at: (stem utzers:	Tobias
E-mail Adresse des Abteilung des Benut	Benutzers: 🌢 zers: 🍳	tobias.goehl@t-online.de
Name der Organisat	ion: 鱼	MS Solutions
Bundesstat oder Pro	vinz: 🌢	Bayern
Land: PKCS12 Datei-Passy	vort:	Germany
PKCS12 Datei-Passv (Bestätigung)	vort:	XARARA
	Sp	eichem Abbrechen



- über Symbol 🦄 Client Paket herunterladen und auf Festplatte Speichern

5. Unter Globale – Einstellungen OpenVPN Server Starten

- Bleibt der Status auf Angehalten stehen müssen die Logs im IPCOP Webinterface überprüft werden. Logs – System Logdateien – Abschnitt OpenVPN.

- İst dieser Eintrag zu erkennen "Options error: Unrecognized option or missing parameter(s) in /var/ipcop/ovpn/se rver.conf:29: verb (2.0.5)"

Ist Folgendes zu auszuführen:

- in der OpenVPN Konfiguration auf Advanced Server Options wechseln

- Ohne einen Eintrag vorzunehmen auf Speichern Klicken.

- OpenVPN Server Starten, die Anzeige sollte im Status jetzt auf "Läuft" Stehen.



Installation von OpenVPN auf WindowsXP/2000 Client

- openvpn-2.0.7-gui-1.0.3-install.exe Starten und Installationsanweisungen Folgen.

- Client Paket in das OpenVPN Verzeichnis / config entpacken.



- VPN Verbindung Herstellen

MS-TO-IPCop
Tobias-TO-IPCop
Proxy Settings
0bout
About

- Zerifikat PW eingeben
- ist Folgende Meldung im Status-Log zu sehen:

Thu Apr 20 13:59:28 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expected peer address: 192.168.200.166:1194 (allow this incoming source address/port by removing --remote or adding --float)



OpenVPN Connection (MS-TO-IPCop)	
Current State: Connecting	
Thu Apr 20 14:00:22 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:23 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:25 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:27 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:27 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:27 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:28 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:30 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:30 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:30 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:33 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:33 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:33 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:33 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:33 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:33 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:37 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:37 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:37 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:37 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:39 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:39 2006 TCP/UDP: Incoming packet rejected from 192.168.2.1:1194[2], expe Thu Apr 20 14:00:39 2006 TCP/UDP: Incoming packet rejected from 19	icted peer a icted peer a
Disconnect Reconnect	Hide

Muss die Client-Konfig Datei angepasst werden, diese ist im Openvpn Installations- Pfad im Config Verzeichnis zu finden. In meinen Fall die Datei MS-TO-IPCop.ovpn mit Notepad öffnen.

In der letzten Zeile ein -float einfügen und Datei Speichern.

- VPN Verbindung Herstellen.

- Bei einer erfolgreichen VPN Verbindung sollte die Anzeige auf Grün Springen und Folgendes angezeigt werden.



In der Client-Log Datei sollte außerdem Folgende Meldung erscheinen. Thu Apr 20 14:04:32 2006 Initialization Sequence Completed

Zugriff auf Grünes Netzwerk sollte jetzt Bei Richtiger Konfiguration Möglich sein.

