

Roadwarrior (Host zu Netz) – Anleitung für ZERINA 0.9.0b – 0.9.4b

Diese Anleitung führt Euch Schritt für Schritt durch die Konfiguration des OpenVPN-Addons "ZERINA" für den IPCop, mit welcher ihr eine sogenannte "Roadwarrior"-Verbindung, also einer Host-zu-Netz-Verbindung, von einem Client-Rechner zur IPCop-Firewall erstellen könnt, um auf das hinter der Firewall liegende Netz zugreifen zu können.. In dieser Anleitung verwenden wir als Client einen Rechner mit Windows-XP Betriebssystem.

Bevor wir starten noch einige wichtige Hinweise:

Diese Anleitung beinhaltet keinerlei Gewährleistung bzw. Garantie, die Nutzung erfolgt daher auf eigenes Risiko!

Bitte beachte das ZERINA immer weiterentwickelt wird und einige Schritte bzw. Grafiken von der eingesetzten ZERINA-Version abweichen können.

Desweiteren gehe ich davon aus, dass ihr das "Zerina"-Addon bereits im IPCop installiert habt, sowie das "OpenVPN 2.1_rc15" unter Windows installiert wurde. Die Links zu den Seiten wo die entsprechende Software herunter geladen werden kann findet ihr im Abschnitt "1. Schritt: Start".

VPN und Zertifikate sind ein sehr komplexes Thema und beinhalten mehr Punkte/Bereiche als diese einfache Anleitung beinhaltet. Benötigt ihr weitere Informationen zu diesem Thema, so informiert euch bitte auf den entsprechend dafür zuständigen Internet-Seiten.

Inhalt:

- 1. Schritt:** Start
- 2. Schritt:** Globale Einstellungen
- 3. Schritt:** Root/Host-Zertifikate
- 4. Schritt:** Client-Zertifikate
- 5. Schritt:** OpenVPN-Server Start
- 6. Schritt:** Verbindung vom Client zum Server

1. Schritt - Start

Benötigte Software: [IPCop](#), [ZERINA-Addon für IPCop](#), [OpenVPN für Windows](#)

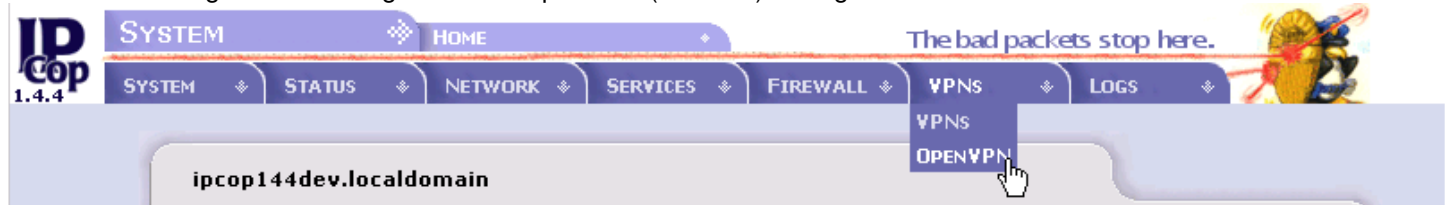
Wir gehen von nachfolgender Situation aus:

IPCop **ROTES** Netz: 192.168.181.2

IPCop **GRÜNES** Netz: 10.10.10.1

Unser Windows-XP Rechner ist über DSL mit dem Internet verbunden.

Als erstes benötigen wir den Zugriff auf die OpenVPN (ZERINA)-Konfigurationsseite:



Die Startseite des OpenVPN (ZERINA)-Addons im IPCop öffnet sich und zeigt zwei Bereiche an:

Global settings

Current OpenVPN Server Status: **STOPPED** ①

OpenVPN on RED

OpenVPN on BLUE

OpenVPN on ORANGE

Local VPN Hostname/IP: OpenVPN Subnet(e.g. 10.0.10.0/255.255.255.0)

OpenVPN device:

Protocol: Destination port:

MTU Size:

LZO-Compression: Encryption:

Certificate Authorities: ②

Name	Subject	Action
Root Certificate:	Not present	
Host Certificate:	Not present	

CA Name:

① **Global settings** > Diese konfigurieren wir als erstes.

② **Certificate Authorities** > Zu diesem Abschnitt kommen wir in Schritt 2.

2. Schritt – Globale Einstellungen

The screenshot shows the 'Global settings' window for OpenVPN. At the top, it says 'Current OpenVPN Server Status: STOPPED'. Below this are three checkboxes: 'OpenVPN on RED' (checked), 'OpenVPN on BLUE' (unchecked), and 'OpenVPN on ORANGE' (unchecked). There are three input fields: 'Local VPN Hostname/IP' (containing '192.168.181.2'), 'OpenVPN Subnet(e.g. 10.0.10.0/255.255.255.0)' (containing '10.10.10.0/255.255.255.0'), and 'OpenVPN device' (set to 'TUN'). The 'Protocol' is set to 'UDP', 'Destination port' is '1194', 'MTU Size' is '1400', and 'LZO-Compression' is checked. The 'Encryption' is set to 'BF-CBC'. At the bottom, there are buttons for 'Save', 'Advanced', 'Start OpenVPN Server', and 'Restart OpenVPN Server'. Red circles with numbers 1 through 12 highlight specific elements: 1 (checkbox 1), 2 (checkbox 2), 3 (checkbox 3), 4 (hostname field), 5 (subnet field), 6 (device dropdown), 7 (protocol dropdown), 8 (port field), 9 (mtu field), 10 (checkbox 10), 11 (encryption dropdown), and 12 (save button).

Nr.	Feldname	Beschreibung	Wert
1	OpenVPN on RED	Hier aktiviert man den OpenVPN-Server im Roten Netz des IPCops	Ausgewählt
2	OpenVPN on BLUE	Hier aktiviert man den OpenVPN-Server im Blauen Netz des IPCops Dieses Feld ist nur sichtbar bei aktivem Blauen Netz!	Nicht ausgewählt
3	OpenVPN on ORANGE	Hier aktiviert man den OpenVPN-Server im Orangen Netz des IPCops Dieses Feld ist nur sichtbar bei aktivem Orangen Netz!	Nicht ausgewählt
4	Local VPN Hostname/IP	Hier wird die IP oder der Hostname eingetragen unter welcher der IPCop im roten Netz erreichbar ist. Dies ist im Normalfall die öffentliche IP über die der IPCop aus dem Internet erreichbar ist. Wenn ihr keine statische IP-Adresse habt, könnt ihr hier auch eine sog. Dynamische Domain eintragen (Bsp.: meine-domain.dyndns.net)	192.168.181.2
5	OpenVPN Subnet	OpenVPN benötigt ein eigenes virtuelles Subnetz, dieses Subnetz darf nirgendwo anders im IPCop verwendet werden! Ebenfalls darf dieses Subnetz nicht im Netzwerk des Clients genutzt werden!	10.0.10.0/255.255.255.0
6	OpenVPN device	Hier das gewünschte Interface auswählen (derzeit wird nur TUN unterstützt , später ist hier noch eine Bridge-Option geplant)	TUN
7	Protocol	Hier kann man zwischen TCP und UDP auswählen, wobei UDP die schnellere Variante ist.	UDP
8	Destination port	Hier kann ein Port gesetzt werden, auf dem der OpenVPN-Server lauscht. Dieser Port darf nirgendwo anders im IPCop vergeben werden, bzw. auch nicht forwardet sein.	1194
9	MTU Size	Der Default MTU-Wert beträgt 1400. OpenVPN fügt wie andere VPN Protokolle auch, einen Header zu jedem Paket hinzu, daher setze diesen Wert so, das keine unnötige IP-Fragmente entstehen.	1400
10	LZO-Cempression	Diese Option aktiviert/deaktiviert die LZO-Kompression. Standardwert ist aktiviert.	Ausgewählt
11	Encryption	Hier kann die Verschlüsselungsart gewählt werden, abhängig davon wie paranoid ihr seid :). Standardeinstellung ist BF-CBC	BF-CBC
12	Save	Wenn alle Einstellungen vorgenommen wurden, wird die Konfiguration durch drücken auf diesen Speicher-Button gespeichert.	

Nachdem die globalen Einstellungen gespeichert wurden sollte der Abschnitt **"Global Settings"** so aussehen:

3. Schritt – Root/Host - Zertifikate

Beim Einrichten des OpenVPN (ZERINA)-Addons sind noch keine Zertifikate vorhanden. Beachtet bitte, dass das OpenVPN (ZERINA)-Addon seine eigene PKI nutzt, wir dachten das es besser wäre separate PKI zu nutzen als die Standard IPCop VPN PKI.

Die erste Version von OpenVPN (ZERINA) verhielt sich wie die IPCop vpnmain.cgi, wo alle erzeugten Zertifikate dieselbe Seriennummer erhielten, dies wurde jetzt geändert.

Um nun Verbindungen zu akzeptieren/autentifizieren brauchen wir als nächstes ein Root- und ein Host-Zertifikat.

Nr.	Feldname	Beschreibung	Wert
1	Generate Root/Host Certificates	Diesen Button drücken um den Prozess zu starten, welcher die Zertifikate generiert.	Draufdrücken
2	CA Name	Hier kann der CA-Name vergeben werden (wird in diesem Howto nicht benötigt).	Nichts
3	Durchsuchen	Hier kann man vorhande Zertifikate auf der lokalen Festplatte suchen (wird in diesem Howto nicht benötigt).	Nichts
4	Upload CA Certificate	Hier können Zertifikate die auf der lokalen Festplatte ausgewählt worden hochgeladen werden (wird in diesem Howto nicht benötigt).	Nichts

Nachdem ihr auf den "Generate Root/Host Certificates"-Button gedrückt habt wird euch eine neue Seite angezeigt.

Root/Host-Zertifikate erstellen:

Generate Root/Host Certificates:

Organization Name: ①
 IPCop's Hostname: ②
 Your E-mail Address: ③
 Your Department: ④
 City: ⑤
 State or Province: ⑥
 Country: ⑦
 ⑧

This field may be blank.
WARNING: Generating the root and host certificates may take a long time. It can take up to several minutes on older hardware. Please be patient.

Upload PKCS12 file: ⑨
 PKCS12 File Password: ⑩
 ⑪

This field may be blank.

Nr.	Feldname	Beschreibung	Wert
①	Organization Name	Hier den Namen eurer Organisation eingeben	myorg
②	IPCop's Hostname	Dieses Feld wird automatisch mit der IP vom roten Netz des IPCops gefüllt.	192.168.181.2
③	Your E-mail Address	Hier könnt ihr eine Kontakt eMail-Adresse angeben (nicht zwingend notwendig)	myemail@myhost.com
④	Your Department	Hier könnt ihr den Namen eurer Abteilung angeben (nicht zwingend notwendig)	mydepartment
⑤	City	Hier könnt ihr die Stadt angeben (nicht zwingend notwendig)	hamburg
⑥	State or Province	Hier könnt ihr ein Bundesland angeben (nicht zwingend notwendig)	hamburg
⑦	Country	Hier wird der Staat ausgewählt (Bsp.: Germany)	Germany
⑧	Generate Root/Host Certificates	Sind die notwendigen Angaben der Punkte 1-3, sowie Punkt 7 gemacht worden, so klickt auf diesen Button um den Prozess zum erstellen der Zertifikate zu starten.	Draufklicken
⑨	Durchsuchen	Diese Funktion ist optional, entweder ihr generiert ein neues Zertifikat oder ihr ladet ein bereits vorhandenes Zertifikat hoch. Wenn ihr ein bereits vorhandenes Zertifikat nutzen wollt, so wählt hier den Ort aus wo das Zertifikat liegt und ladet es dann hoch, das Zertifikat muss PKCS12-Format vorliegen.	Nichts machen
⑩	PKCS12 File Password	Hier kann ein Passwort für die PKCS12-Datei vergeben werden (nicht zwingend notwendig).	Nichts angeben
⑪	Upload PKCS12 File	Hier kann eine vorhande PKCS12-Datei hochgeladen werden. Dieser Button ist nur in Verbindung mit dem „Durchsuchen“-Button nutzbar!	Nichts machen

Nachdem alle Angaben gemacht wurden, sollte der Bereich so aussehen:

Generate Root/Host Certificates:

Organization Name:
 IPCop's Hostname:
 Your E-mail Address:
 Your Department:
 City:
 State or Province:
 Country:

This field may be blank.
WARNING: Generating the root and host certificates may take a long time. It can take up to several minutes on older hardware. Please be patient.

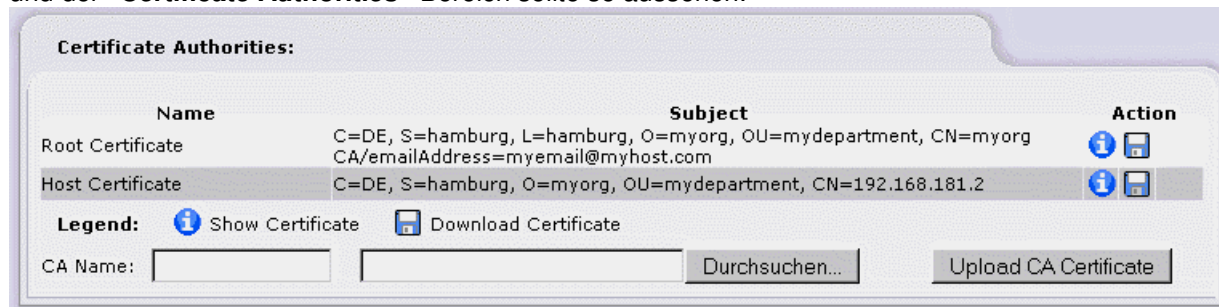
Upload PKCS12 file:
 PKCS12 File Password:

This field may be blank.

Jetzt klicken wir auf den „**Generate Root/Host Certificates**“-Button.

Je nach eurer Hardware kann dieser Prozess eine sehr lange Zeit dauern, da auch eine sogenannte dh-Datei (Diffie Hellman) generiert wird, welche der OpenVPN (ZERINA)-Server benötigt. **Während dieser Zeit bitte keine Aktion tätigen!**

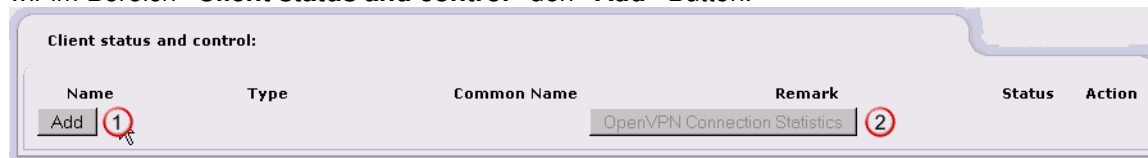
Nachdem (hoffentlich) erfolgreichen Generierungs-Prozess öffnet sich automatisch die OpenVPN (ZERINA) Hauptseite und der "**Certificate Authorities**"-Bereich sollte so aussehen:



4. Schritt – Client-Zertifikate

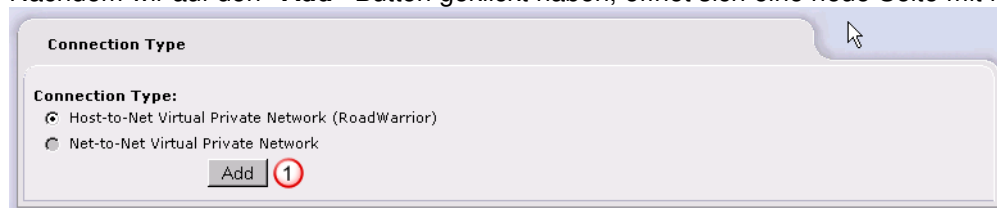
Als nächstes benötigen wir nun ein Client-Zertifikat. Hierzu gibt es mehrere Möglichkeiten, jedoch wählen wir die einfachste Möglichkeit aus.

Wir gehen nun zurück zur OpenVPN (ZERINA) Hauptseite, da wir einen neuen Client hinzufügen wollen. Hierzu klicken wir im Bereich "**Client status and control**" den "**Add**"-Button.



Nr.	Feldname	Beschreibung	Wert
1	Add-Button	Durch klicken auf diesen Button fügen wir einen neuen Client hinzu.	Draufdrücken
2	OpenVPN Connection Statistics	Hier kann man eine Statistik über OpenVPN-Verbindungen abrufen.	Nichts

Nachdem wir auf den "**Add**"-Button geklickt haben, öffnet sich eine neue Seite mit folgendem Bereich:



Nr.	Feldname	Beschreibung	Wert
1	Add-Button	Durch klicken auf diesen Button fügen wir einen neuen Verbindungstyp laut Auswahl hinzu	Draufdrücken

Als Verbindungstyp kann derzeit nur die Roadwarrior-Methode ausgewählt werden (Host-zu-Netz).

Nach einem Klick auf den Add-Button hier, kommt man auf eine weitere Seite mit zwei Bereichen "**Connection**" und "**Authentication**".

Als erstes widmen wir uns dem Bereich "**Connections**":



Nr.	Feldname	Beschreibung	Wert
1	Name	Hier gibt man einen Namen für die neue Verbindung an.	client1
2	Remark	Hier könnt ihr wahlweise noch eine Bemerkung zur Verbindung angeben, um sie später z.b. besser zu identifizieren zu können, wenn ihr mal viele Clients eingerichtet habt.	This is client 1
3	Enabled	Hier könnt ihr die Verbindung aktivieren, bzw. deaktivieren.	Ausgewählt

Als nächstes widmen wir uns dem zweiten Abschnitt "Authentication":

Nr.	Feldname	Beschreibung	Wert
1	Upload Section	Hier kann man entweder ein Zertifikat oder eine Zertifikats-Anfrage hochladen. Dieser Abschnitt wird aber in diesem Howto nicht behandelt.	Nichts
2	Generate Certificate Section	In diesem Abschnitt machen wir unsere Angaben zur Erstellung eines neuen Zertifikates.	
3	User's Full Name or System Hostname	Hier wird der Name des Zertifikates angegeben	client1
4	User's E-mail Address	Hier wird die Kontakt eMail-Adresse des Users/Client angegeben (nicht zwingend notwendig).	client1@myhost.com
5	User's Department	Hier wird die Abteilung des Users/Clients eingetragen (nicht zwingend notwendig).	mydepartment
6	Organization Name	Hier wird der Name der Organisation des Users/Clients eingetragen (nicht zwingend notwendig).	myorg
7	City	Hier kann man die Stadt des Users/Clients eintragen (nicht zwingend notwendig).	hamburg
8	State or Province	Hier wird das Bundesland des Users/Clients eingetragen (nicht zwingend notwendig).	hamburg
9	Country	Hier wählt man den Staat des Users/Clients aus	Germany
10	PKCS12 File Password	In diesen beiden Feldern gibt man das Passwort an mit dem die PKCS12-Datei verschlüsselt wird (mind. 6 Zeichen)	123456
11	Save/Cancel	Buttons um den neuen Client anzulegen (Save) oder das Anlegen des neuen Clients abubrechen (Cancel)	Draufklicken

Nachdem wir alle notwendigen Felder ausgefüllt haben sollte beide Abschnitte so aussehen:

The screenshot shows a web-based configuration form for an OpenVPN client. It is divided into two main sections: 'Connection' and 'Authentication'.
Connection section:
- Name: client1
- Remark: This is client1
- Enabled: checked
Authentication section:
- Radio buttons for 'Upload a certificate request', 'Upload a certificate', and 'Generate a certificate'. 'Generate a certificate' is selected.
- Fields for: User's Full Name or System Hostname (client1), User's E-mail Address (client1@myhost.com), User's Department (mydepartment), Organization Name (myorg), City (hamburg), State or Province (hamburg), Country (Germany), PKCS12 File Password (two fields with masked characters).
- Buttons: Save, Cancel.

Nun klicken wir nur noch auf den **"Save"**-Button um die Daten zu speichern und den Client anzulegen. Danach sollte sich wieder die OpenVPN (ZERINA) Hauptseite öffnen und uns im Bereich **"Client status and control"** den neu angelegten Client anzeigen:

The screenshot shows the 'Client status and control' page. It features a table with the following columns: Name, Type, Common Name, Remark, Status, and Action.
- Name: client1
- Type: Host (Certificate)
- Common Name: client1
- Remark: This is client1
- Status: CLOSED
- Action: A set of icons including a blue circle with a plus sign, a document icon, a checkmark, a pencil, and a trash can.
- Legend: Includes checkboxes for 'Enabled (click to disable)' (checked) and 'Disabled (click to enable)'.
- Buttons: Add, OpenVPN Connection Statistics.

Nun können wir das Client-Paket herunterladen indem wir auf das erste der sechs Aktions-Symbole rechts aussen klicken:

This screenshot is identical to the previous one, but a mouse cursor is hovering over the first icon in the 'Action' column. A tooltip box is visible, containing the text 'Download Client package (zip)'.

Nach dem Anklicken des Symbols öffnet sich ein Dialogfenster zum downloaden des Client-Paketes:

The screenshot shows a Firefox download dialog box titled 'Öffnen von client1-TO-IPCop.zip'.
- Text: 'Sie möchten folgende Datei herunterladen:'
- File name: client1-TO-IPCop.zip
- Type: WinRAR ZIP archive
- Source: https://192.168.181.2:445
- Question: 'Wie soll Firefox mit dieser Datei verfahren?'
- Options: 'Öffnen mit WinRAR (Standard)', 'Auf Diskette/Festplatte speichern' (selected), 'Für Dateien dieses Typs immer diese Aktion ausführen' (unchecked).
- Buttons: OK, Abbrechen.

Speichert das Client-Paket nun ab und kopiert es auf den Client-Rechner auf dem ihr zuvor das **"OpenVPN 2.1_rc15"**-Paket installiert habt. In das entsprechende Verzeichnis (Bsp.: C:\Programme\OpenVPN\config)

5. Schritt – OpenVPN-Server Start

Nachdem alle vorhergehende Schritte korrekt durchgeführt wurden sind wir nun soweit den OpenVPN-Server (ZERINA) zu starten. Hierzu klickt ihr einfach nur auf der OpenVPN (ZERINA) Hauptseite auf den **"Start OpenVPN Server"**-Button.

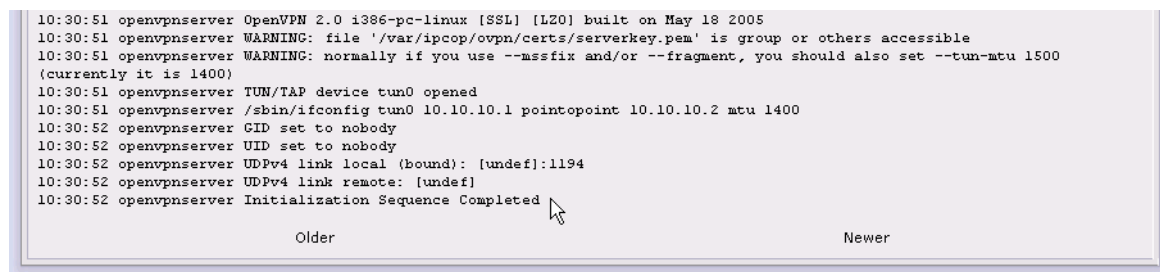
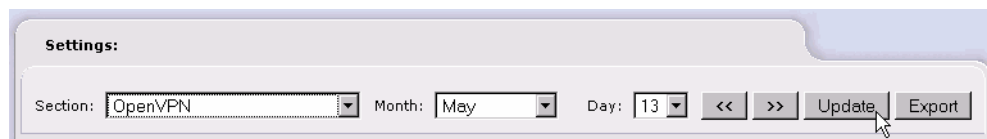
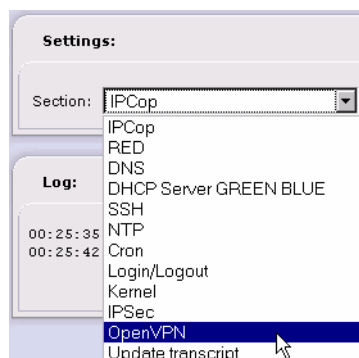
Start OpenVPN Server

Nach dieser Aktion ändert sich der Serverstatus wie folgt:

Current OpenVPN
Server Status: **RUNNING**

Mit in dem OpenVPN (ZERINA)-Addon ist eine erweiterte Version der logs.dat, welche es euch erlaubt die OpenVPN-Server Log-Nachrichten anzusehen.

Um diese OpenVPN-Server Log-Nachrichten anzusehen folgt einfach der Schritte anhand der nächsten Bilder:

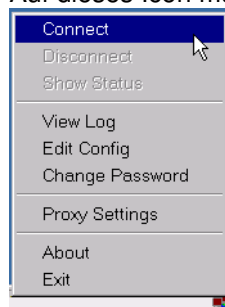


Wichtig ist hierbei das in der letzten Zeile **"Initialization Sequence Completed"** steht. Dies bedeutet bei jedem Start des OpenVPN (ZERINA) - Servers, das der Server läuft und bereit ist neue Verbindungen zu akzeptieren.

6. Schritt - Verbindung vom Client zum Server

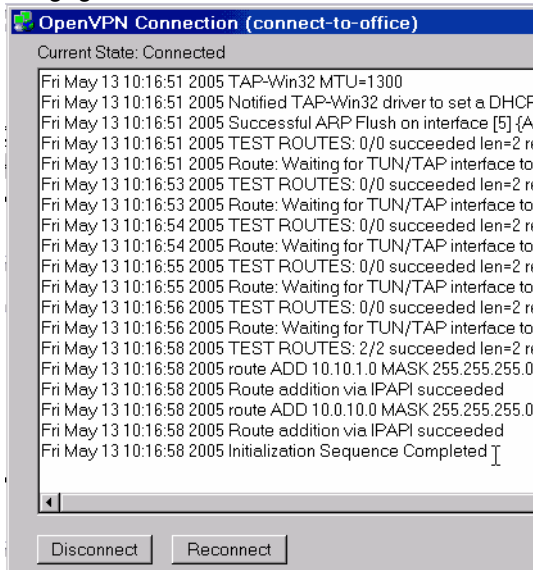
Zurück auf dem Client-Rechner, starten wir die OpenVPN GUI (falls dies noch nicht geschehen ist). Es erscheint nach dem Start ein neues Icon im Tray unten rechts, welches wie ein Netzwerk-Icon aussieht, aber stattdessen zwei dunkelrote Monitore hat.

Auf dieses Icon macht ihr nun einen Rechtsklick mit der Maus, danach wird euch ein Kontextmenü angezeigt wie folgt:

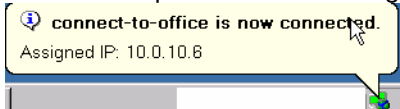


In diesem Kontextmenü klickt ihr nun auf **"Connect"**, danach öffnet sich ein neues Fenster welches ein weiteres kleineres Fenster öffnet wo ihr nach dem Passwort für die Client-PKCS12 Datei gefragt werdet. Hier gebt ihr das, beim Erstellen des Client im OpenVPN (ZERINA)-Server, vergebene Passwort ein und klickt auf **"OK"**.

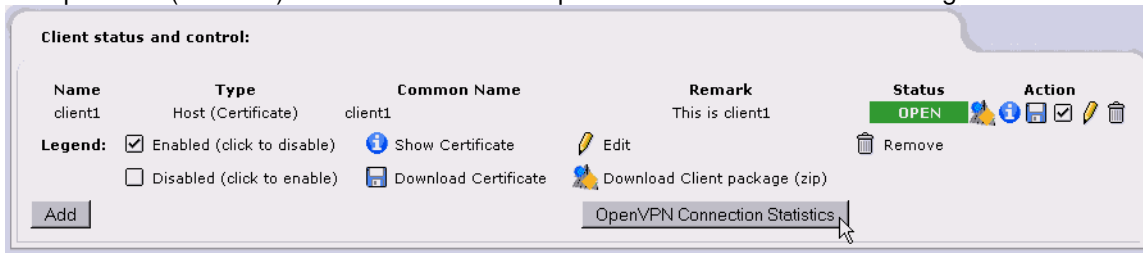
Wurde das korrekte Passwort angegeben, so werden in dem ersten Fenster einige Statusmeldungen erscheinen, welche Informationen über den Aufbau der OpenVPN-Verbindung anzeigen. Ebenfalls werden hier auch Fehlermeldungen ausgegeben, sollte es zu Fehlern beim Aufbau der Verbindung, sowie während der Verbindung kommen.



Wurde die OpenVPN-Verbindung erfolgreich aufgebaut, so wird euch eine sog. Ballon-Nachricht darüber informieren:



Im OpenVPN (ZERINA) - Server auf dem IPCop können wir nun den Verbindungsstatus des Clients sehen:



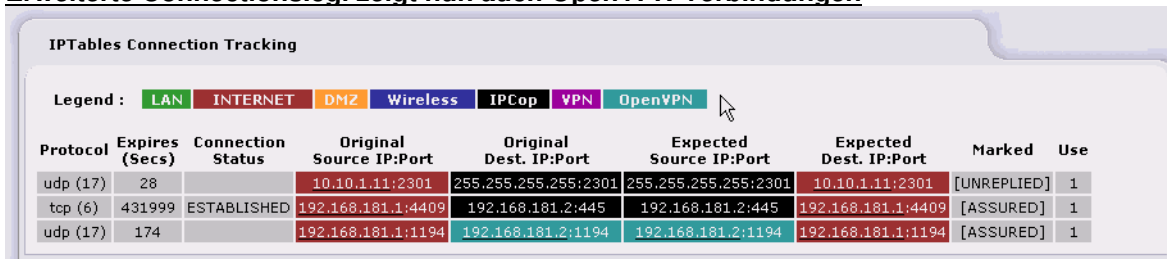
An dieser Stelle endet dieses Howto/ diese Anleitung.

Nachfolgend noch einige Bilder über Funktionen die in OpenVPN (ZERINA) enthalten sind:

OpenVPN Verbindungs-Statistiken



Erweiterte Connections.cgi zeigt nun auch OpenVPN-Verbindungen



Erweiterte Proxy.cgi mit Support für Proxy-Support für OpenVPN

Web proxy:

Enabled on Green :	<input type="checkbox"/>	Upstream proxy (host:port): ●	<input type="text"/>
Transparent on Green :	<input type="checkbox"/>	Upstream username: ●	<input type="text"/>
		Upstream password: ●	<input type="text"/>
		Proxy Port:	<input type="text" value="800"/>
Enabled on OpenVPN :	<input type="checkbox"/>		
Transparent on OpenVPN :	<input type="checkbox"/>		
Log Enabled:	<input type="checkbox"/>		

Hinweise vom Autor

Diese Anleitung beinhaltet keinerlei Gewährleistung bzw. Garantie, die Nutzung erfolgt daher auf eigenes Risiko!

Diese Anleitung ist im Grunde eine Übersetzung des Howtos von Ufuk Altinkaynak mit einer kleinen Änderung. In Ufuk's Howto wird das Tool „OpenVPN-GUI“ als Standalone-Tool verlinkt/angesprochen, ich habe in dieser Anleitung jedoch Bezug auf das Tool "OpenVPN 2.1_rc15" genommen, welches den OpenVPN-Client und Die OpenVPN-Gui zusammenfasst und aktueller ist als das Standalone-Tool OpenVPN-GUI.

13.05.2009 Steffen Haase