

Dokumentation für den IPCop-VPN Zugang mit Mac OS X

[Mirco Schmidt](#)

7. Januar 2006

Inhaltsverzeichnis

1. Mac OS X als Roadwarrior	5
1.1. Voraussetzungen	5
1.2. Konfiguration des IPCop VPN Server's	5
1.3. Vorbereiten der Client-Verbindung	8
1.3.1. Vorbereiten der Zertifikate	8
1.3.2. Importieren der Zertifikate	9
1.4. Einrichten der Client-Verbindung	14
1.4.1. IPSecuritas Einstellungen	17
1.4.2. DynDNS	19
A. Abkürzungen und Begriffe	I
A.1. Abkürzungen	I
A.2. Begriffe	II

Abbildungsverzeichnis

1.1. VPN Verbindung hinzufügen	5
1.2. VPN Verbindungstyp definieren	6
1.3. VPN Verbindungsnamen definieren	6
1.4. VPN Zertifikat erstellen	7
1.5. VPN Verbindung hinzugefügt	7
1.6. VPN Verbindungs Zertifikat herunterladen	8
1.7. VPN Server Host Zertifikat herunterladen	8
1.8. Verbindungszertifikat konvertieren	9
1.9. IPSecuritas Cert-Manager öffnen	9
1.10. IPSecuritas Cert-Manager	10
1.11. IPSecuritas Cert-Manager Host Zertifikat importieren	10
1.12. IPSecuritas Cert-Manager Host Zertifikat auswählen	11
1.13. IPSecuritas Cert-Manager mit Host Zertifikat	11
1.14. IPSecuritas Cert-Manager Verbindung Zertifikat importieren	12
1.15. IPSecuritas Cert-Manager Verbindung Zertifikat wählen	12
1.16. IPSecuritas Cert-Manager Verbindung Zertifikat importieren	13
1.17. IPSecuritas Cert-Manager Verbindung Zertifikat importieren	13
1.18. IPSecuritas neue Verbindung erstellen	14
1.19. IPSecuritas Verbindung Setup - General	14
1.20. IPSecuritas Verbindung Setup - Phase 1	15
1.21. IPSecuritas Verbindung Setup - Phase 2	15
1.22. IPSecuritas Verbindung Setup - Id/Auth	16
1.23. IPSecuritas Verbindung Setup - Options	17
1.24. IPSecuritas Hauptfenster	17
1.25. IPSecuritas Optionen	18
1.26. IPSecuritas Optionen angepaßt	18

Tabellenverzeichnis

A.1. Erklärung der Abkürzungen	I
A.2. Erklärung der Begriffe	II

1. Mac OS X als Roadwarrior

Bevor ich beginne möchte ich dem Autor der englischen Vorlage für diese Dokumentation meinen Respekt aussprechen. Ohne seine Vorarbeit hätte ich dieses Dokument nicht so schnell realisieren können.

<http://www.taupehat.com/vpn/index.html>

1.1. Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein, um diese Dokumentation erfolgreich nachvollziehen zu können.

- IPCop Linux Router in Version 1.4.10
- Mac OS X Tiger in Version 10.4.3
- IPSecuritas von <http://www.lobotomo.com/products/IPSecuritas/index.html>

1.2. Konfiguration des IPCop VPN Server's

<https://your.ipcop.ip.adress:445>

Am Webinterface des VPN Server's anmelden und in der Menüleiste auf VPNs klicken. Unter der Verbindungsübersicht auf Hinzufügen klicken.



Abbildung 1.1.: VPN Verbindung hinzufügen

Jetzt wird der Verbindungstyp definiert, in unserem Fall bleibt die Std. Einstellung Host-zu-Netz erhalten

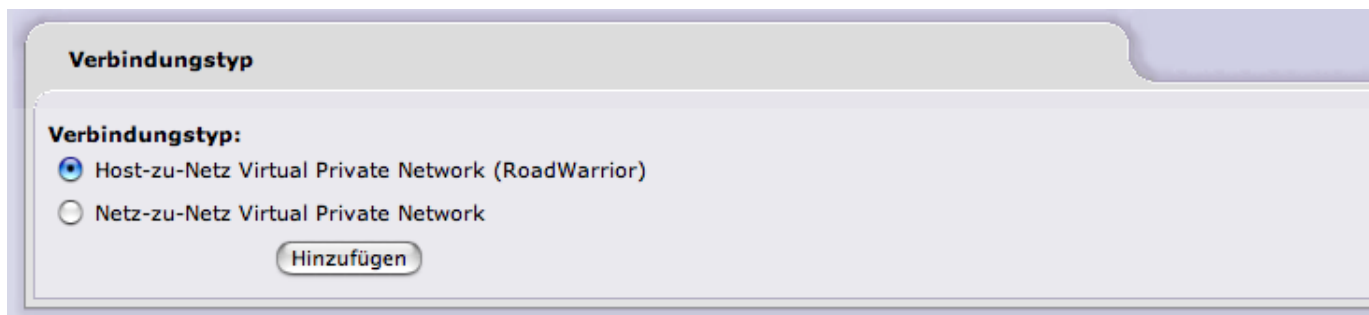


Abbildung 1.2.: VPN Verbindungstyp definieren

Im nächsten Schritt gilt es einen Namen für die neue VPN Verbindung zu vergeben

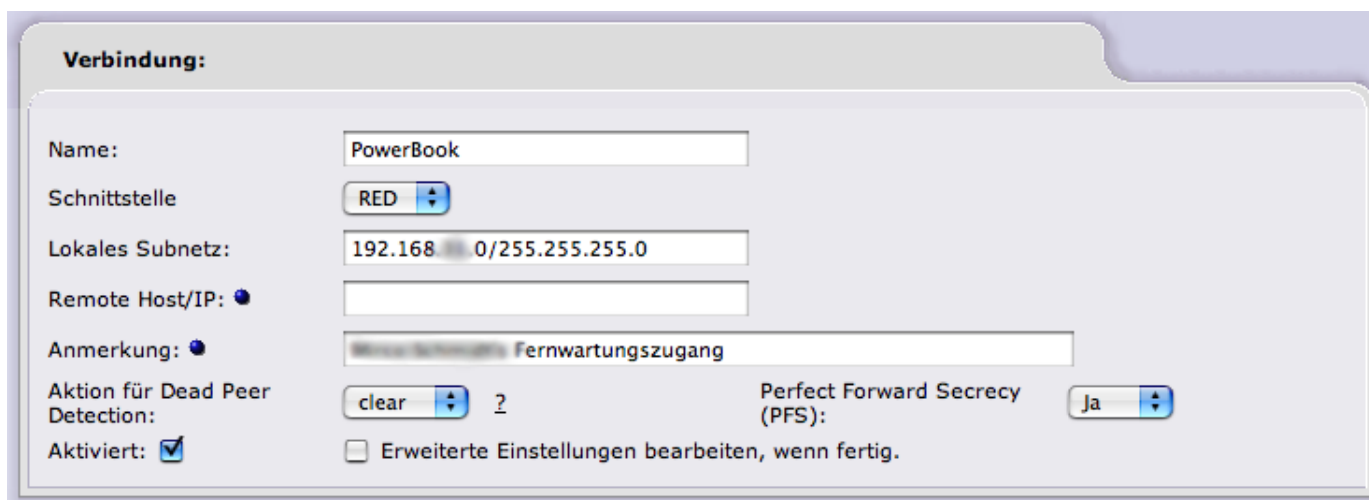


Abbildung 1.3.: VPN Verbindungsnamen definieren

Nun geht es an das erstellen des Zertifikat's

Authentifizierung:

Verwenden Sie einen Pre-Shared Schlüssel:

Eine Zertifikatsanfrage hochladen: Keine Datei ausgewählt

Erzeuge ein Zertifikat:

Voller Name oder System Hostname des Benutzers:

E-mail Adresse des Benutzers:

Abteilung des Benutzers:

Name der Organisation:

Stadt:

Bundesstat oder Provinz:

Land:

PKCS12 Datei-Passwort:

PKCS12 Datei-Passwort: (Bestätigung)

Abbildung 1.4.: VPN Zertifikat erstellen

Jetzt nur noch speichern anklicken und auf der neugeladenen Übersichtsseite die gemachten Einstellungen nochmals kontrollieren.

Verbindungsstatus und -kontrolle:

Name	Typ	Gemeinsamer Name	Anmerkung	Status	Aktion
[blurred]	Host (Zertifikat)	[blurred]	Fernwartungszugang	BEENDET	[Info] [Neustart] [Herunterladen] [Aktivieren] [Deaktivieren] [Bearbeiten] [Löschen]
[blurred]	Netz (Zertifikat)	[blurred]	VPN zur Familie	OFFEN	[Info] [Neustart] [Herunterladen] [Aktivieren] [Deaktivieren] [Bearbeiten] [Löschen]
[blurred]	Netz (Zertifikat)	[blurred]	VPN zu [blurred]	OFFEN	[Info] [Neustart] [Herunterladen] [Aktivieren] [Deaktivieren] [Bearbeiten] [Löschen]

Legende:
 Aktiviert (klicken, um zu deaktivieren)
 Deaktiviert (klicken, um zu aktivieren)

Zertifikat anzeigen

Zertifikate herunterladen

Abbildung 1.5.: VPN Verbindung hinzugefügt

1.3. Vorbereiten der Client-Verbindung

Als erstes gilt es die nötigen Zertifikate vom VPN Server herunterzuladen



Abbildung 1.6.: VPN Verbindungs Zertifikat herunterladen



Abbildung 1.7.: VPN Server Host Zertifikat herunterladen

Zum Herunterladen der Zertifikate einfach auf das Diskettensymbol in der jeweiligen Zeile klicken. Die Zertifikate am besten in einem eigens angelegten Ordner speichern.

1.3.1. Vorbereiten der Zertifikate

Jetzt gilt es die Zertifikate so vorzubereiten dass sie sich im nächsten Schritt in IPSecuritas importieren lassen. Dazu wird zuerst das Zertifikat der VPN Verbindung im Beispiel also PowerBook.p12 mit openssl in zwei einzel Dateien zerteilt.

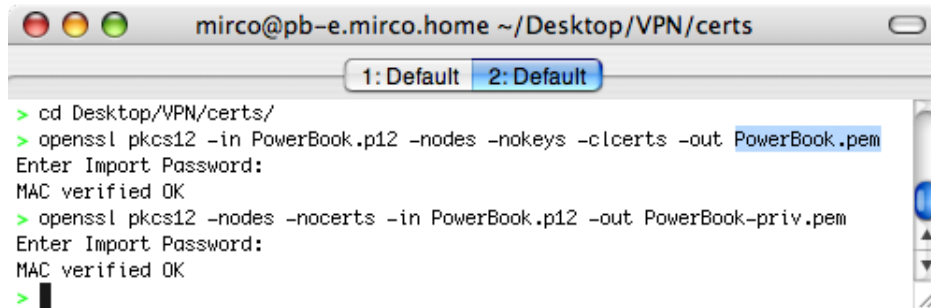
Wichtiger Sicherheitshinweis!

Die aus diesen Aktionen resultierenden Dateien sind unverschlüsselt, und damit ein großes Risiko für die Integrität des Netzwerks. Diese Dateien sollten auf keinen Fall folgende Behandlungen erfahren:

- Versand via E-Mail
- versand via Post auf Diskette, CD, oder sonstigen Datenträgern
- Veröffentlichung auf einer Website
- Sonstige Veröffentlichungsformen

Diese Dateien sollten im Idealfall direkt nach erstellen der VPN Verbindung mit IPSecuritas wieder gelöscht werden, im Bedarfsfall sind sie ja schnell aus den verschlüsselten Originalen erstellt.

Für den nächsten Schritt brauchen wir den Unix Unterbau des Mac, also ein Terminal öffnen und durch Eingabe von "cd Pfad/zum/Zertifikat" in das Verzeichnis mit den Zertifikaten wechseln.



```
mirco@pb-e.mirco.home ~/Desktop/VPN/certs
1: Default 2: Default
> cd Desktop/VPN/certs/
> openssl pkcs12 -in PowerBook.p12 -nodes -nokeys -clcerts -out PowerBook.pem
Enter Import Password:
MAC verified OK
> openssl pkcs12 -nodes -nocerts -in PowerBook.p12 -out PowerBook-priv.pem
Enter Import Password:
MAC verified OK
> █
```

Abbildung 1.8.: Verbindungszertifikat konvertieren

Für diejenigen die lieber kopieren, statt abzuschreiben hier die beiden "openssl" Befehle:

- "openssl pkcs12 -in PowerBook.p12 -nodes -nokeys -clcerts -out PowerBook.pem"
- "openssl pkcs12 -nodes -nocerts -in PowerBook.p12 -out PowerBook-priv.pem"

Wobei hier natürlich der Dateiname den eigenen Gegebenheiten anzupassen ist.

1.3.2. Importieren der Zertifikate

Falls IPSecuritas noch nicht gestartet so ist das nun nachzuholen. Dann im Menü "File" auf "Cert Manager" klicken

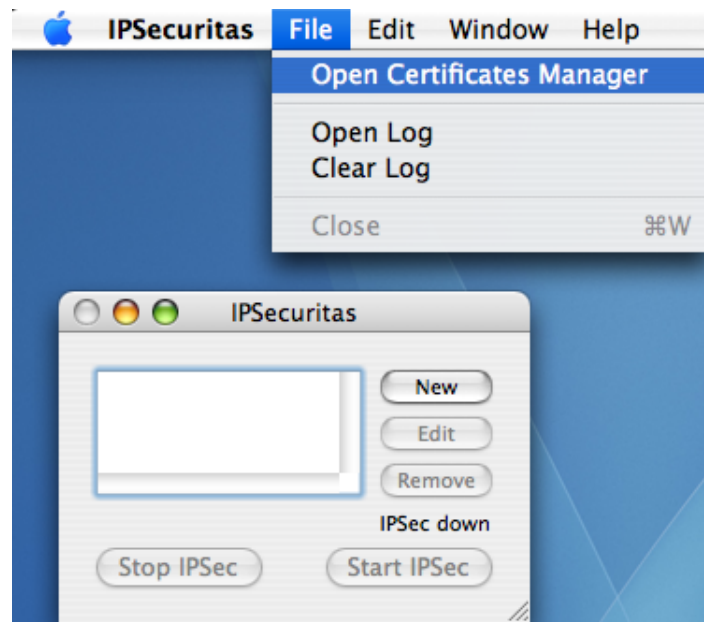


Abbildung 1.9.: IPSecuritas Cert-Manager öffnen

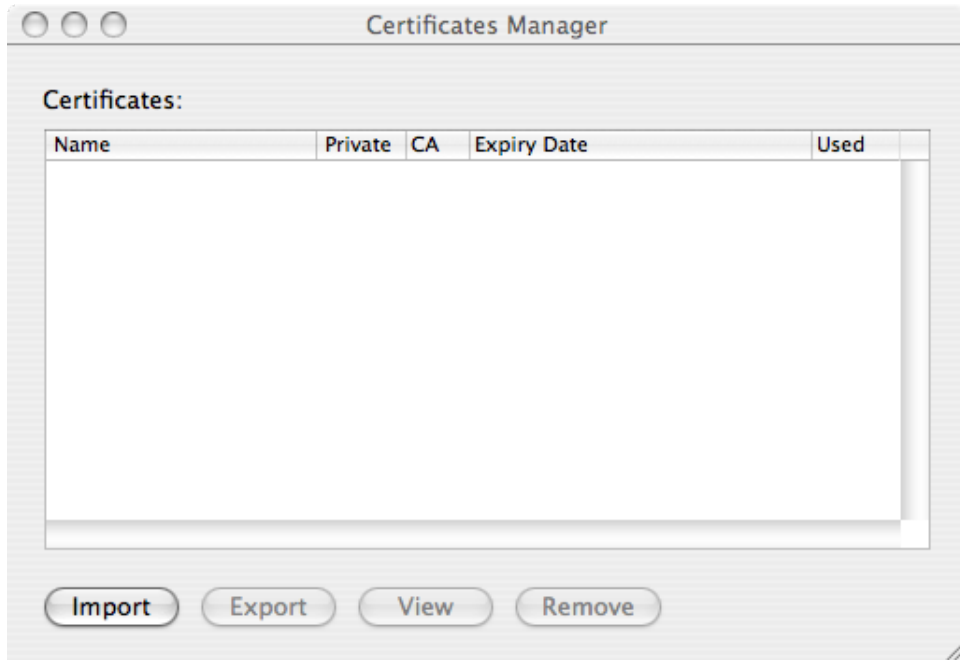


Abbildung 1.10.: IPSecuritas Cert-Manager

Im Fenster des Zertifikat Manager unten links auf "Import" klicken.



Abbildung 1.11.: IPSecuritas Cert-Manager Host Zertifikat importieren

Hier sollte ein aussagekräftiger Name vergeben werden

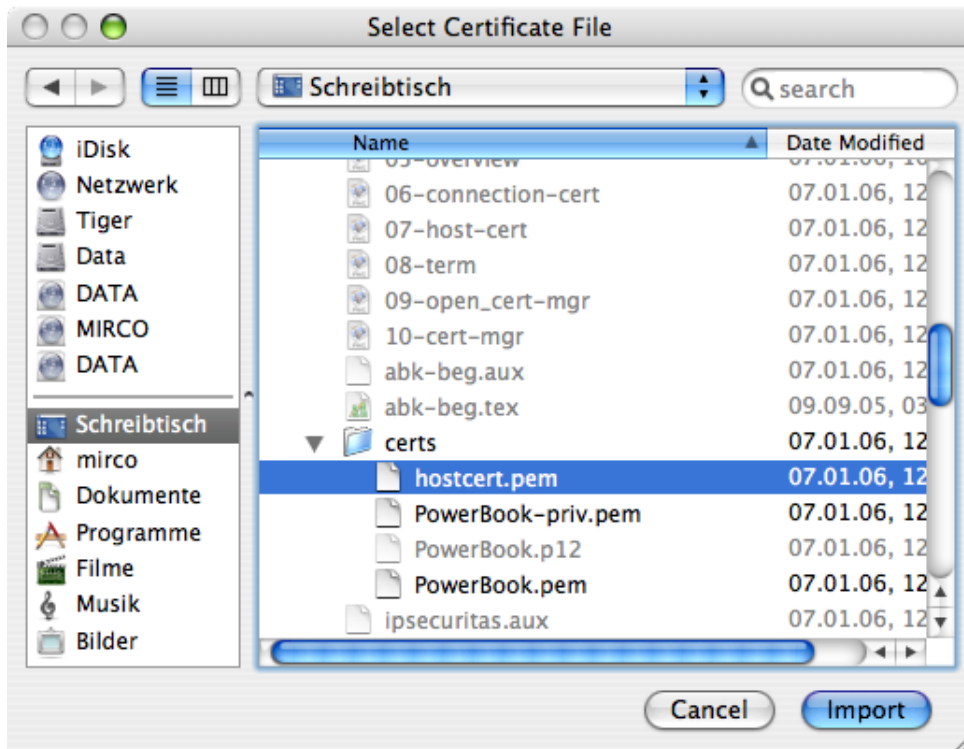


Abbildung 1.12.: IPSecuritas Cert-Manager Host Zertifikat auswählen

Nun die weiter oben heruntergeladene Datei hostcert.pem auswählen.

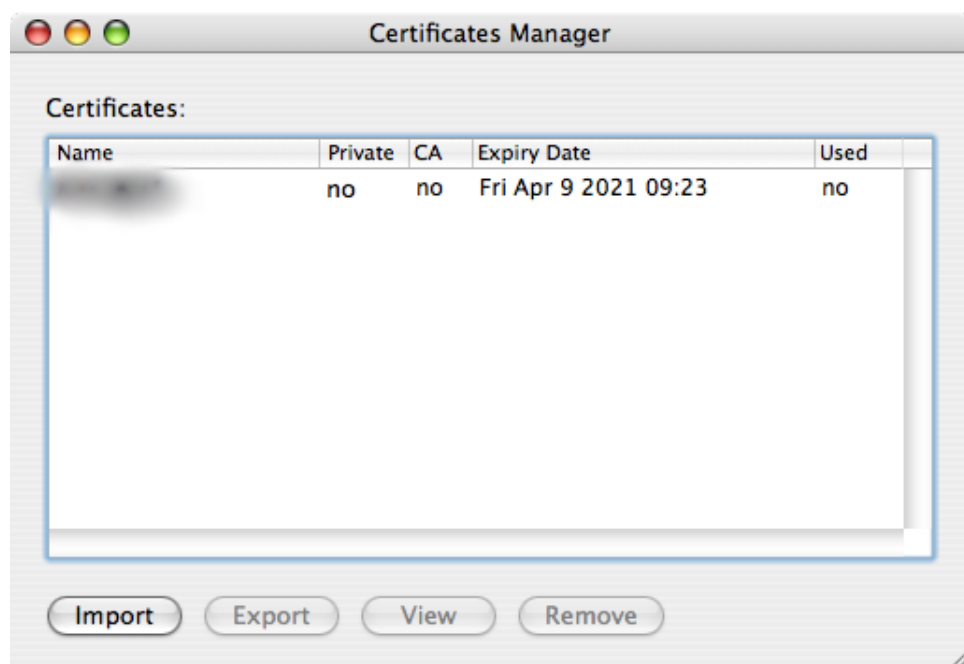


Abbildung 1.13.: IPSecuritas Cert-Manager mit Host Zertifikat

Im Cert-Manager ist nun das importierte Host Zertifikat zu sehen, im nächsten Schritt erneut auf "Import" klicken.



Abbildung 1.14.: IPsecuritas Cert-Manager Verbindung Zertifikat importieren

Auch hier ist wieder ein aussagekräftiger Name zu vergeben.

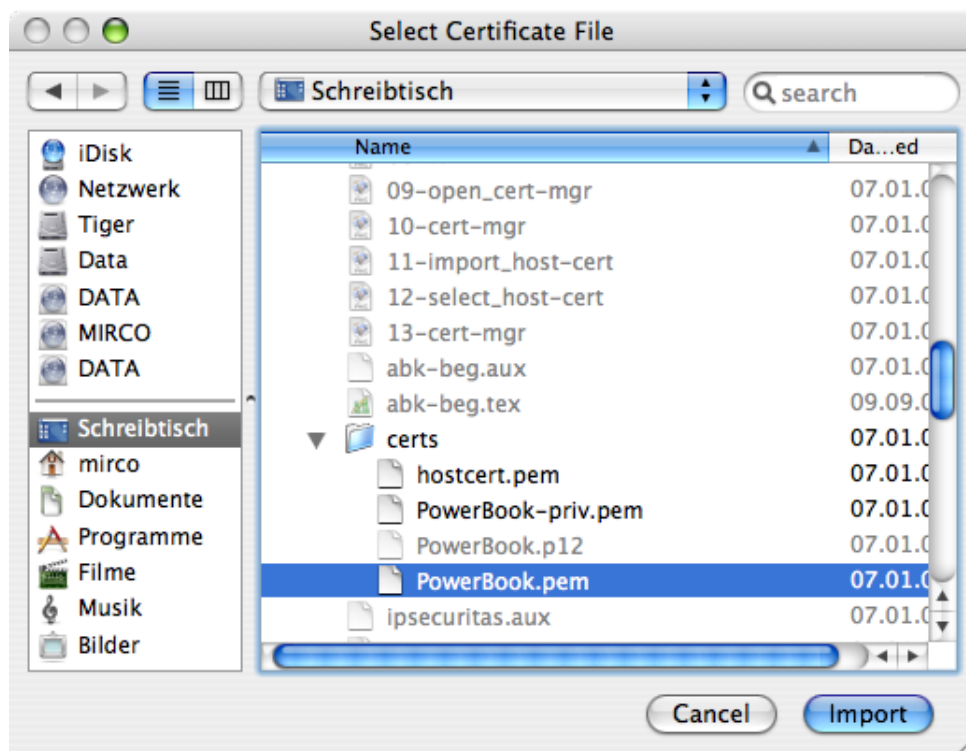


Abbildung 1.15.: IPsecuritas Cert-Manager Verbindung Zertifikat wählen

Hier ist die Datei zu wählen, welche aus dem ersten der beiden oben erwähnten "openssl" Aufrufe resultierte.

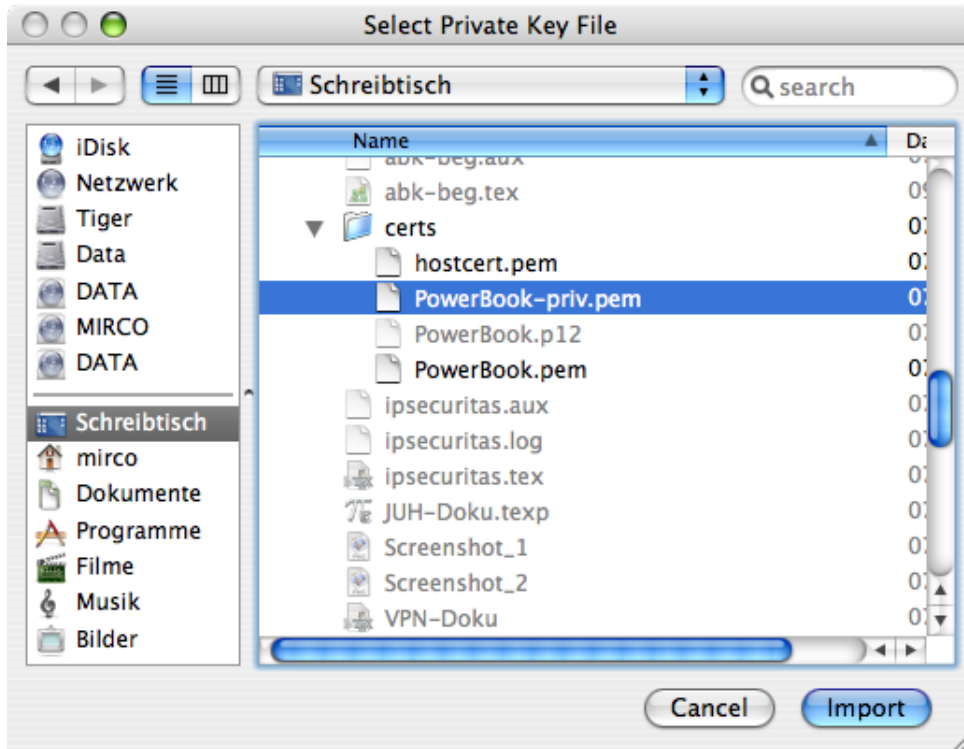


Abbildung 1.16.: IPSecuritas Cert-Manager Verbindung Zertifikat importieren

Und zum Schluß noch das Resultat des zweiten "openssl" Aufrufs.

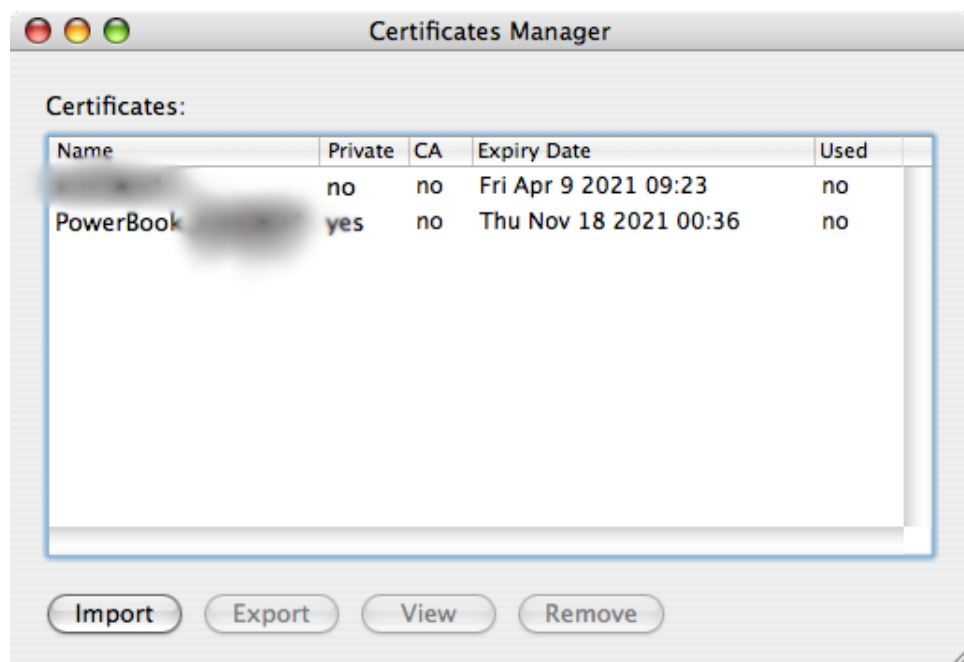


Abbildung 1.17.: IPSecuritas Cert-Manager Verbindung Zertifikat importieren

Das Zertifikat ist importiert die beiden mit "openssl" erzeugten *.pem Dateien können und sollten gelöscht werden.

1.4. Einrichten der Client-Verbindung

Zur Einrichtung einer neuen VPN Verbindung im Hauptfenster von IPSecuritas auf "New" klicken.

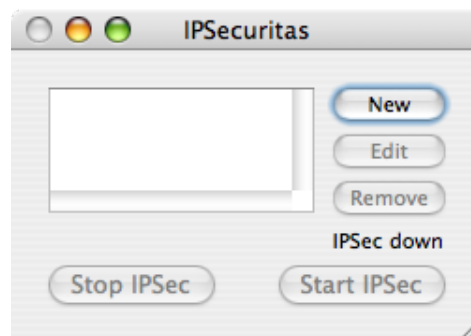


Abbildung 1.18.: IPSecuritas neue Verbindung erstellen

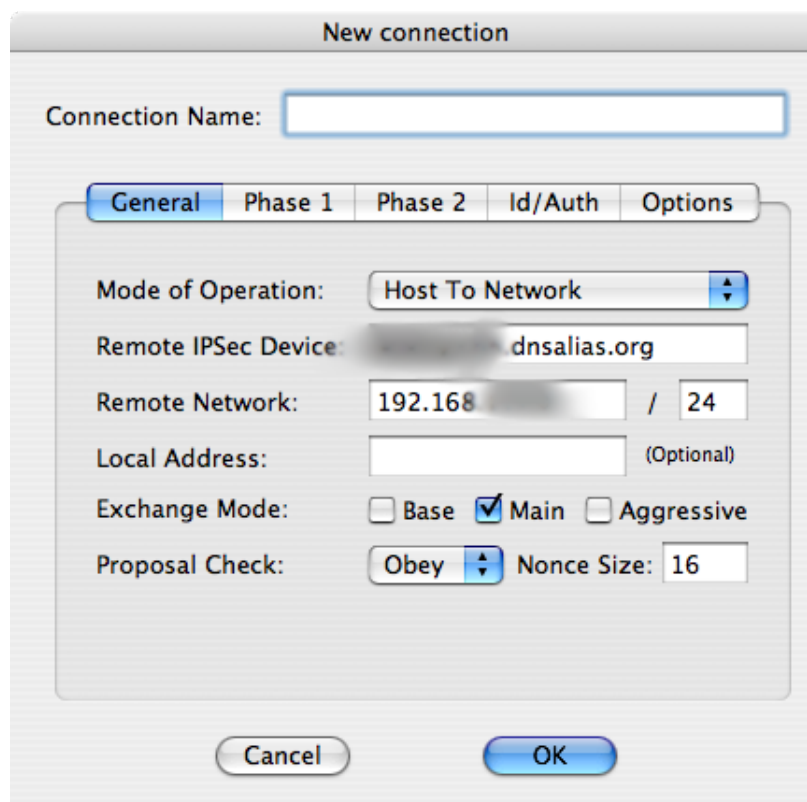


Abbildung 1.19.: IPSecuritas Verbindung Setup - General

Hier ist wieder ein eindeutiger Name für die Verbindung zu vergeben. Ebenso ist sehr genau darauf zu achten, dass alle Felder so wie in den Bildern vorgesehen eingerichtet werden. Da sonst die VPN-Verbindung nicht zustande kommen wird.

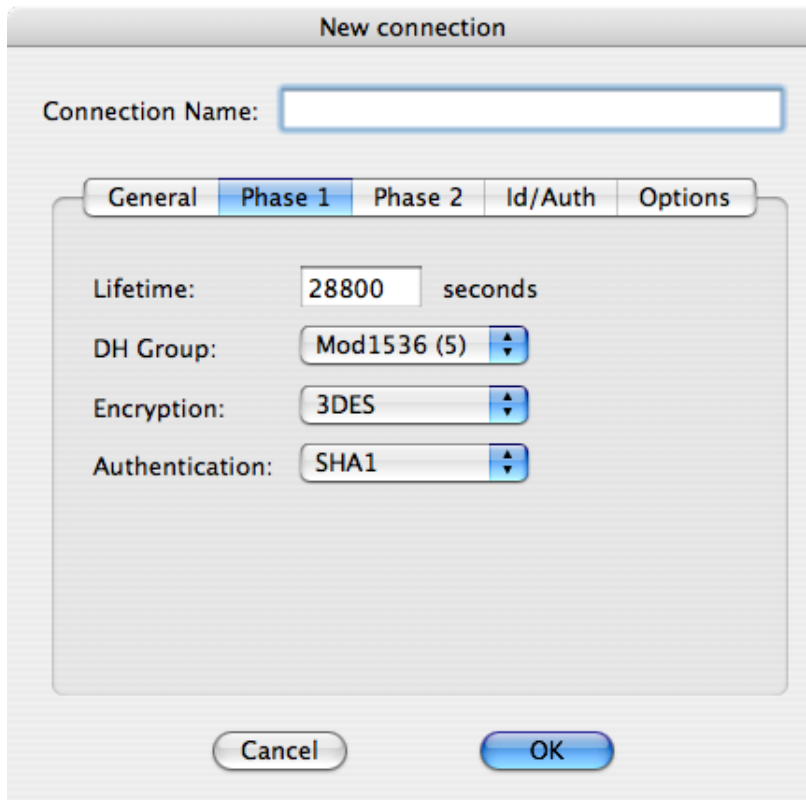


Abbildung 1.20.: IPSecuritas Verbindung Setup - Phase 1

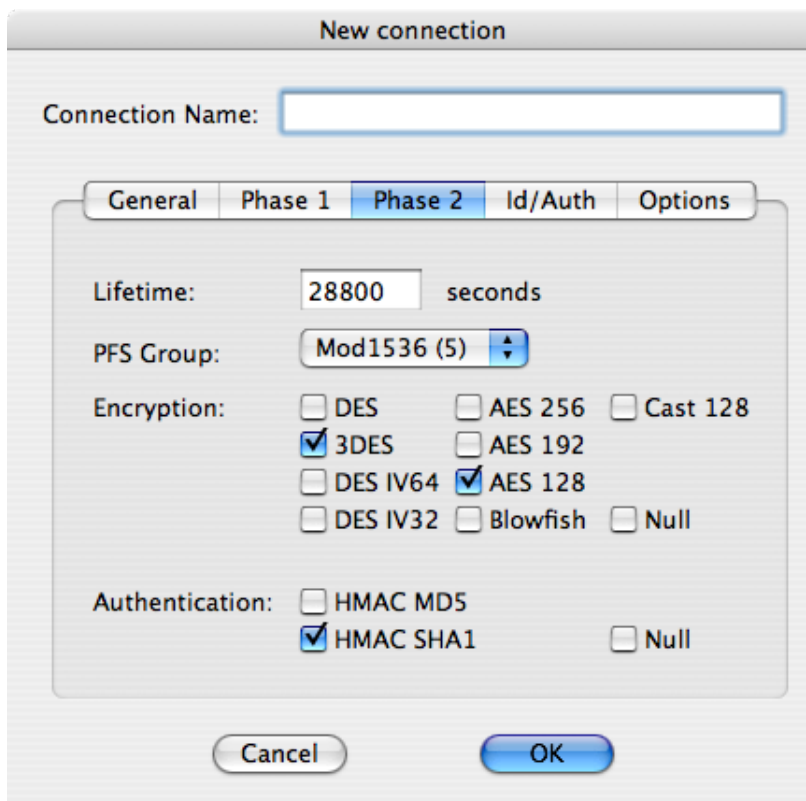


Abbildung 1.21.: IPSecuritas Verbindung Setup - Phase 2

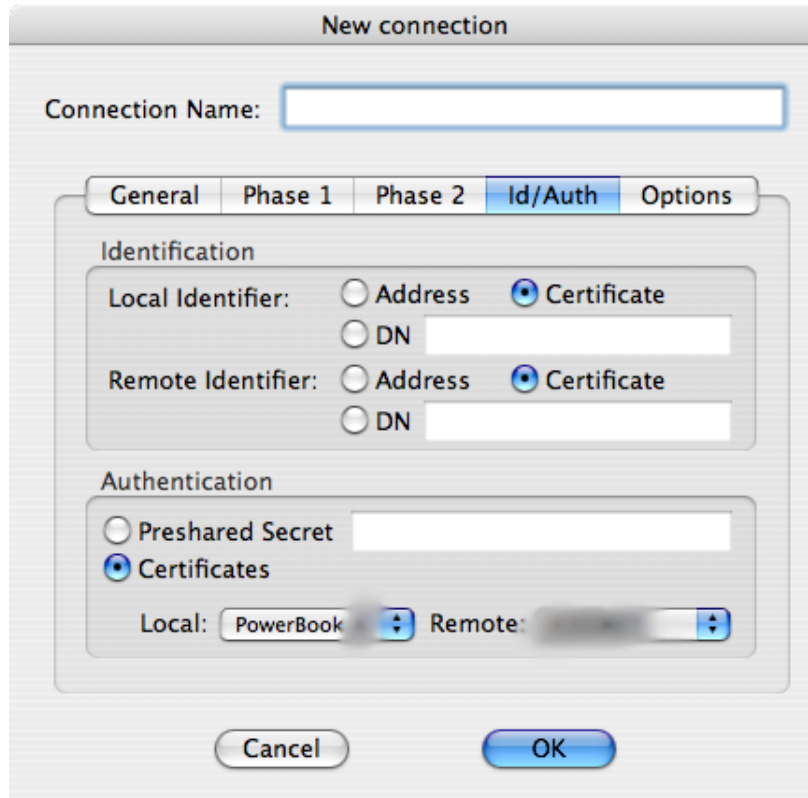


Abbildung 1.22.: IPSecuritas Verbindung Setup - Id/Auth

Diese Stelle ist verwirrend, denn hier muss erst im unteren Teil des Fensters, der Knopf "Certificates" angeklickt werden. Dann das entsprechende "Local" und "Remote" Zertifikat in den Klappmenü's wählen und zum Schluß im oberen Teil des Fenster's hinter "Local Identifier:" und "Remote Identifier:" den Knopf "Certificate" anklicken.

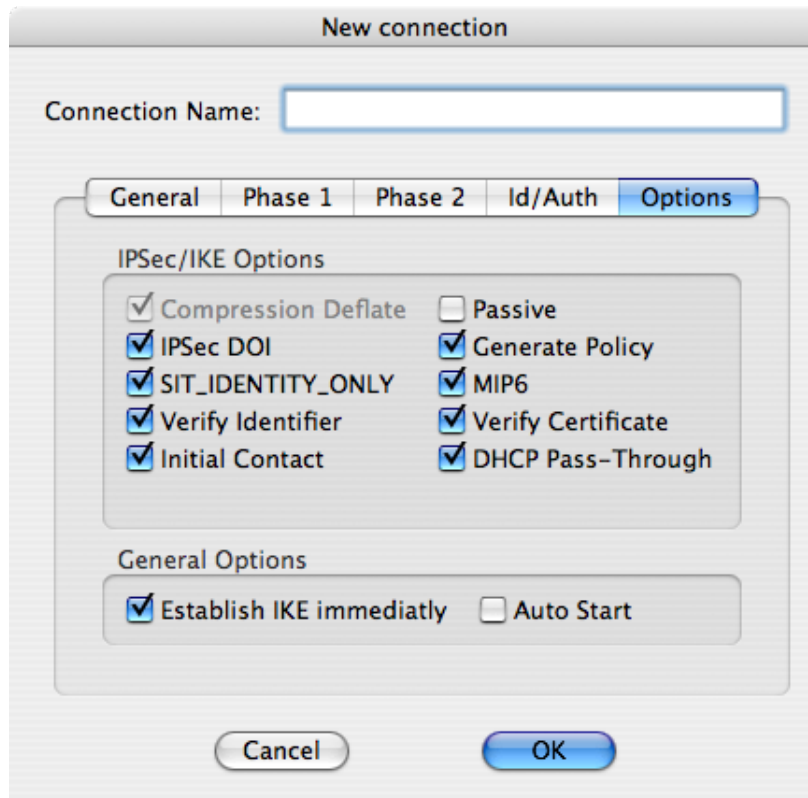


Abbildung 1.23.: IPsecuritas Verbindung Setup - Options

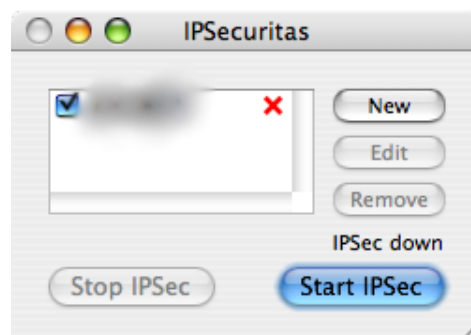


Abbildung 1.24.: IPsecuritas Hauptfenster

Nun kann man durch klicken auf "Start IPsec" die VPN Verbindung herstellen.

1.4.1. IPsecuritas Einstellungen

Noch zu erwähnen bleibt der Optionen Dialog von IPsecuritas, hier läßt sich ein DNS Server für die aktive VPN Verbindung einstellen.

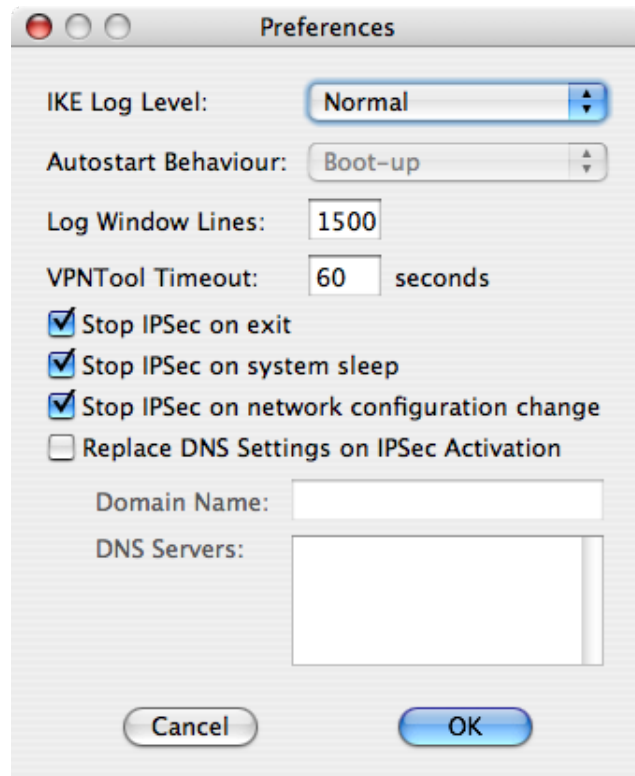


Abbildung 1.25.: IPsec-Optionen

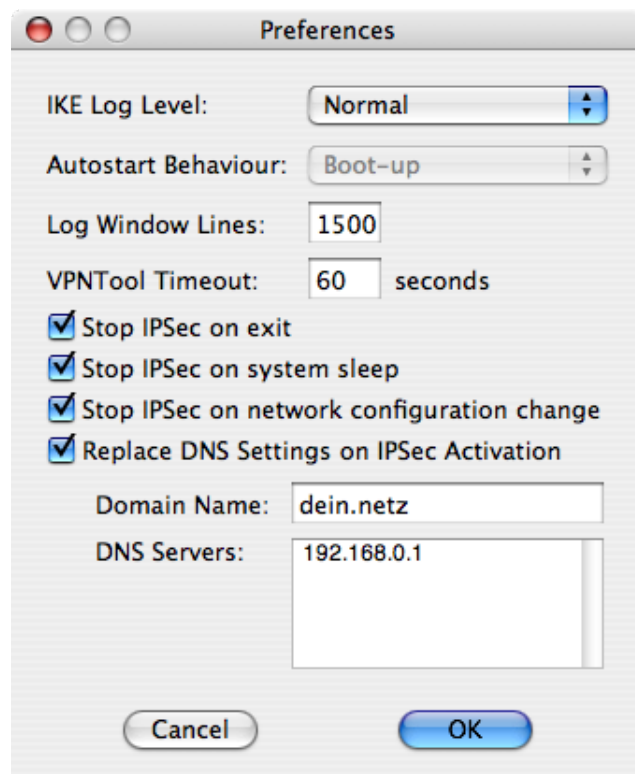


Abbildung 1.26.: IPsec-Optionen angepasst

1.4.2. DynDNS

DynDNS.org ist ein DNS Provider der dynamisch ausgegebenen IP-Adressen einen Hostnamen der Form meinPC.dyndns.org zuordnet.

Wer noch keinen DynDNS Client für den Mac hat dem kann ich den offiziellen DynDNS.org Client von <http://www.dyndns.com/support/clients/mac.html> nur empfehlen, zu dem es übrigens auch ein Dashboard Widget gibt.

A. Abkürzungen und Begriffe

A.1. Abkürzungen

Tabelle A.1.: Erklärung der Abkürzungen

Abk.	Beschreibung
CPU	C entral P rocessing U nit Hauptprozessor
CTI	C omputer T elephony of I ntegration Verbindung von PC und Telefon
DHCP	D ynamic H ost of C onfiguration P rotocol
DNS	D omain N ame S ervice Namensauflösung zu TCP/IP Adressen
FTP	F ile T ransfer P rotocol
HTTP	H yper T ext T ransfer P rotocol
HTTPS	H yper T ext T ransfer P rotocol S ecure
ILO	I ntegrated L ights O ut Ein kleiner Zusatzcomputer, mit dem man einen Server fernsteuern kann auch wenn dieser hängt
IMAP	I nternet M essage A ccess P rotocol
IP	I nternet P rotocol das Netzwerkprotokoll
PC	P ersonal C omputer
POP3	P ost O ffice P rotocol Version 3
RAID	R edundant A rray of I ndependent D isks sichere Datenspeicherung
RAM	R andom A ccess M emory Arbeitsspeicher
RPC	R emote P rocedure C all
RDP	R emote D esktop P rotocol Windows Terminalserver Protokoll
SMB	S erver M essage B lock Protokoll Das Protokoll für Windowsdateifreigaben
SMTP	S imple M ail T ransfer P rotocol
TCP	T ransmission C ontrol P rotocol siehe IP
VNC	V irtual N etwork C omputing Das Protokoll für Desktopfreigaben ähnlich RDP

Fortsetzung auf der nächsten Seite

Abk.	Beschreibung
VoIP	Voice over Internet Protocol
VPN	Virtual Privat Network
WSUS	Windows Server Update Services

A.2. Begriffe

Tabelle A.2.: Erklärung der Begriffe

Begriff	Beschreibung
Backup	Die Datensicherung auf Band oder anderen geeigneten Medien zwecks Schutz vor Datenverlust durch Hardwareausfälle
Hardware	Elektronische Bauteile des PC
Server	Ein Server ist ein leistungsstarker PC, der mit spezieller Hardware für den Dauerbetrieb ausgestattet ist. Der Zweck eines Servers ist die ununterbrochene Verfügbarkeit der auf dem Server bereitgestellten Dienste. Ein Server ist ein reiner Dienstleister.
Roadwarrior	Ein Computer der vom Internet aus, per VPN Zugriff auf das Firmennetzwerk hat