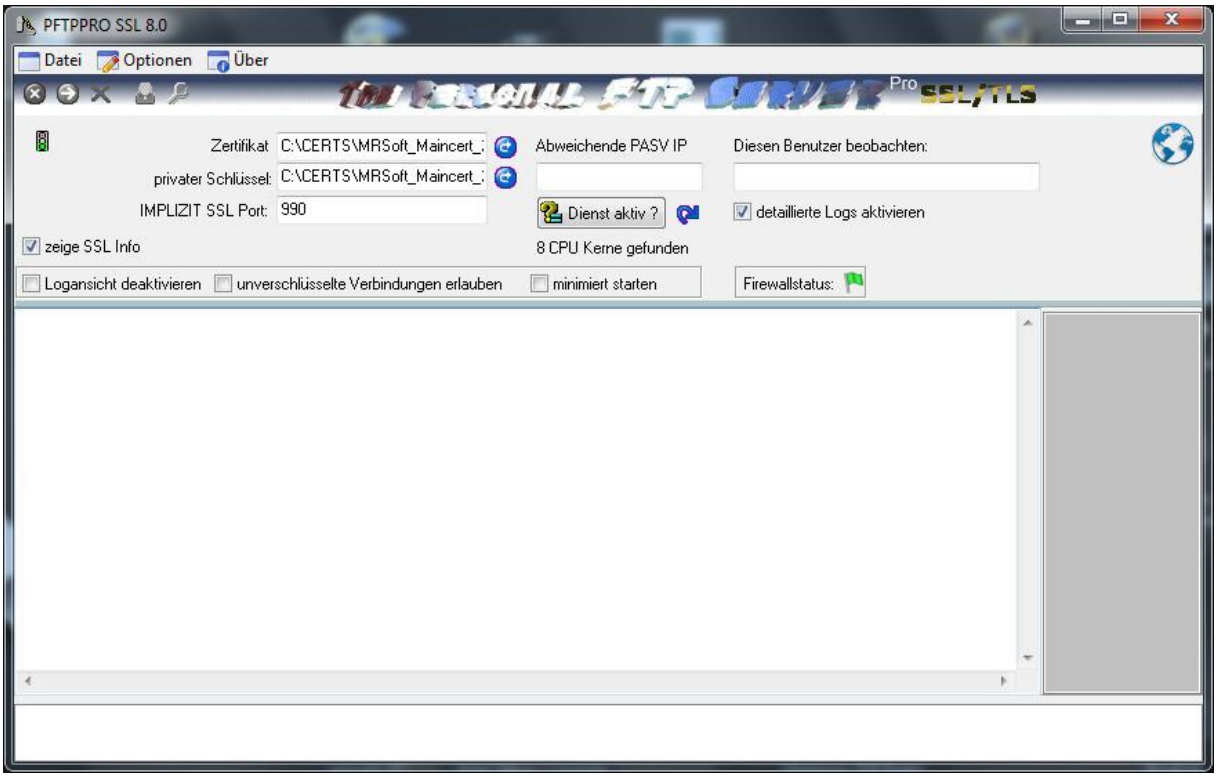
The Personal FTP Server Professional SSL

EINFACH SICHER BEWÄHRT



Installieren->Starten->Zertifikat erstellen->Benutzer anlegen-> Fertig

Nie war der Weg zu Ihrem persönlichen verschlüsselten Server so einfach.

1.0 Hinweise

Der Personal FTP Server SSL macht aus Ihrem PC einen vollwertigen FTPS-Server. Das bedeutet, das andere in Ihrem Netzwerk (Internet,Intranet) verschlüsselt auf Ihren PC zugreifen können um Dateien oder Ordner zu kopieren, zu löschen, zu speichern oder zu lesen. Das FTP Protokoll ist standardisiert. Es ermöglicht den Zugriff und den Datenaustausch auch mit anderen Betriebssystemen und anderen Computersystemen. Ist der FTP Server gestartet, wartet er im Hintergrund auf Anmeldungen und Anfragen aus dem Netz. Um die Sicherheit zu gewährleisten können Nutzernamen und Passwörter sowie Lese und Schreibrechte vergeben werden.
Dieser FTPS-Server verfügt über eine Schutzfunktion der die einzelnen User Accounts gegen Brute Force Angriffe aus dem Netz sichern soll. Ist die Brute Force Protection (BFP) aktiviert, läßt der Server nur drei falsche Einlogversuche zu. Danach wird die IP Nummer des potentiellen Angreifers für eine gewisse Zeitspanne gesperrt. Dieser Schutz verhindert natürlich nicht das erraten zu einfacher Passwörter, macht aber ein automatisches durchprobieren aller Möglichkeiten unmöglich.

This product includes software developed by the OpenSSL Project
for use in the OpenSSL Toolkit. (http://www.openssl.org/)

* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).

1.1 Gewährleistung

Wir übernehmen keine Gewähr für die Fehlerfreiheit der Software oder der Dokumentation und stehen auch nicht für die Befriedigung von Kundenwünschen ein. Für durch Benutzung unseres Programmes entstehende Schäden oder Folgeschäden übernehmen wir keine Haftung. Insbesondere haften wir nicht für den Verlust von Daten. Unsere Gewährleistung beschränkt sich ausschließlich auf den Ersatz von von uns gelieferten Datenträgern, soweit diese nachweislich fehlerhaft sind. Der Gewährleistungszeitraum hierfür beträgt 30 Tage.

1.2 Urheberrecht

1.3 Nutzungsrecht
Sie sind berechtigt die Software auf einen Computer zu übertragen und Sicherheitskopien anzufertigen. Die Software darf aber nicht von zwei verschiedenen Personen an zwei verschiedenen Orten benutzt werden. Wenn Sie "Updates" des Programms erworben haben, so stellen diese eine untrennbare Einheit mit der ursprünglichen Software dar. (Dies ist erkennbar an der identischen Registrierungsnummer). Die Nutzungsrechte können Sie an eine dritte Person übertragen, sofern Sie das gesamte Paket (Disketten, Dokumentation und Sicherungskopien des ursprünglichen Programms und gegebenenfalls der Updates) an diese dritte Person übergeben. Sie sind dann nicht mehr zur Benutzung der Software berechtigt.
Sollte es sich bei der von Ihnen erworbenen Version dieser Software um eine als solche Gekennzeichnete Freewareversion handeln, so darf diese Software weitergegeben werden, solange keine Änderungen an den Originaldaten vorgenommen werden.
Die in dieser Dokumentation erwähnten Produktbezeichnungen sind z.T. eingetragene Warenzeichen (auch wenn sie nicht so gekennzeichnet sind) und unterliegen als solche den gesetzlichen Bedingungen.

1.4 Hardwarevoraussetzungen
Minimale Hardwarevoraussetzungen:
- x86 kompatibler Prozessor ab 1,0 GHz
- Hauptspeicher mindestens 1 GB
- Maus oder anderes Zeigegerät
- Bildschirm und Bildschirmadapter 800*600 oder besser
- Ausreichend Platz auf einer Festplatte

1.5 Softwarevoraussetzungen
-MS-Windows ab Version Windows 2000/XP/Vista/7/8 oder die entsprechenden Server
-Installiertes TCP/IP Protokoll

1.6 Installation
Starten Sie einfach das beiliegende Setupprogramm.

1.7 Probleme
Das vorliegende Programm wurde umfangreich auf verschiedenen Rechnern getestet. Sollten Sie Probleme mit dem Programm haben, so bitten wir Sie, uns diese schriftlich zu schildern.
Um Ihnen helfen zu können, benötigen wir folgende Angaben:

1) Hardware (Prozessortyp, Hauptspeicher, Grafikkarte, Drucker)
2) Software (MS-Windows-Version)
3) Eine vollständige Beschreibung des aufgetretenen Fehlers und, wenn vorhanden, der Text einer Programmabbruchsmeldung
4) Eine Liste der Schritte, die den Fehler hervorriefen
5) Eine Liste der während des Auftretens des Fehlers im Hintergrund laufenden Programme

Schriftliche Anfragen können nur beantwortet werden, wenn genügend Rückporto beiliegt. Auch wenn Sie keine Probleme haben, sind wir für die Zusendung von Verbesserungsvorschlägen dankbar und werden bemüht sein, diese in kommenden Versionen zu berücksichtigen.

Fragen, Verbesserungsvorschläge und Fehlermeldungen senden Sie bitte an:

Michael Roth Software
Schillerstraße 3
31246 Lahstedt

email: info@michael-roth-software.de

2.0 PFTP PRO Befehlsreferenz

2.1 Datei

2.1.1 Starte Server
Diese Funktion startet den Server und ermöglicht so das Einloggen von Clients.

2.1.2 Stoppe Server
Dieser Menüpunkt sorgt dafür das der Server gestoppt wird. Es können sich nun keine Clients mehr einloggen.

2.1.3 Beenden
Dieser Menüpunkt beendet nicht nur den Server, sondern schließt das gesamte Programm und gibt den belegten Speicher wieder frei. Es kann gewählt werden ob der Serverdienst nach beenden des GUI Teils im Hintergrund weiterlaufen soll oder ob er mit beendet wird.

2.2 Optionen

2.2.1 Lösche Display
Diese Funktion löscht das gesamte Display. Die Logdateien werden von dieser Funktion nicht beeinflußt.

2.2.2 Benutzerverwaltung
Die Auswahl dieses Menüpunktes öffnet die PFTPS Benutzerverwaltung. In der Benutzerverwaltung werden alle User die Zugriff auf den Server haben sollen eingetragen. Die Funktionsweise der Benutzerverwaltung wird unter Punkt 3.1 genauer beschrieben.

2.2.3 Alle Verbindungen trennen
Diese Funktion trennt alle aktiven Verbindungen und alle derzeit aktiven Clients aus dem System.

2.2.4 Aktive User
Die Auswahl dieses Menüpunktes öffnet ein weiteres Fenster, welches Ihnen genaue Informationen über einen Client gibt.

2.2.5 Sprache

2.2.5.1 Deutsch
Schaltet die Sprache bei laufendem Betrieb in die deutsche Fassung.

2.2.6 Erweiterte Optionen
Dieser Menüpunkt führt direkt in den Optionsdialog von PFTPS.
Hier können alle Servereinstellungen vorgenommen werden.

2.3 Über

Diese Menüpunkte öffnet die Informationsfenster von PFTPPRO SSL.
Hier gibt es Informationen zur eingesetzten OpenSSL Version, geben Ihren Lizenzschlüssel ein oder finden weitergehende Informationen auf unseren Webseiten.

3.0 Die Benutzerverwaltung

In diesem Fenster werden alle User eingetragen, die Zugriff auf Ihren Server haben sollen.
Im unteren Teil des Fensters sehen Sie eine Tabelle in der alle Eintragungen vorgenommen werden.

Ich beschreibe nun die Dateneingabe in die Tabelle von der linken zur rechten Seite.

3.1 Username:
Hier werden die Namen der einzelnen User eingetragen.
Z.B.: Michael, Simon, Klaus Bötcher usw. usw.

3.2 Passwort:
In diese Spalte kommt das Passwort für den entsprechenden User.

3.3 Pfad:
In diese Spalte schreiben Sie bitte den Pfad (Ordner, Verzeichnis) zu dem der User Zugriff haben soll. Z.B. C:\tmp\Simon\ oder D:\ oder c:\ usw.
Alle Unterordner in dem Freigabepfad werden grundsätzlich auch freigegeben.
Wenn sie C:\tmp\ freigeben, ist also auch ein Zugriff auf z.B. C:\tmp\test\ möglich.

3.3.1 Pfad 2 bis Pfad 4:

In diesen drei Spalten können Sie zusätzliche Pfade eintragen. Diese Pfade werden zusätzlich zu dem ersten Pfad freigegeben, und Sie werden in den Verzeichnisbaum virtuell eingelinkt . Um die Pfade 2 bis 4 auch sichtbar zu machen, muß unter *Erweiterte Optionen* die Checkbox „Freigegebene Laufwerke im Dateisystem anzeigen“ aktiviert (angekreuzt) sein.

3.4. Rechte:

Hier wird angegeben welche Rechte ein User in dem für Ihn freigegebenen Ordner hat.
Es sind zur Zeit 4 verschiedene Werte möglich.

r für „nur lesen“

w für „nur schreiben“

rw für „lesen und schreiben“ (nur in PFTP PRO und PFTP PRO SSL)

a für „Lesen schreiben und löschen“

Eine Kombination der verschiedenen Werte ist nicht möglich.

In PFTP PRO können verschiedene Rechte der einzelnen Pfade zugeordnet werden.
Z.B. **Pfad 1:** C:\tmp\Simon\ **Rechte P1**: rw
Pfad 2: D:\ **Rechte P2:** r
u.s.w.

3.7 Autoload: (nur in PFTP PRO)

Diese Funktion erlaubt es die Userdaten (PFTPUSERS.dat) stündlich neu in den Speicher zu laden und macht somit eine Fernwartung des Servers möglich. Die geänderten Userdaten einfach in das Verzeichnis übertragen, in dem sich PFTP befindet und nach spätestens einer Stunde werden die Änderungen wirksam.

3.8 Suche nach Username:

Wie es der Name schon sagt, hier kann nach einem User suchen, um z.B. seine Rechte ändern zu können. Der zu suchende Name muß exakt mit dem Usernamen übereinstimmen.
Wildcards wie * oder ? sind nicht möglich (noch nicht).

3.9 Anonymous Login erlaubt:

Anonymous Login bedeutet, das sich jeder auch ohne Passwort in Ihr System einloggen kann. Diese anonymous User melden sich alle mit dem Usernamen anonymous an.
Ist diese Checkbox aktiviert, müssen Sie vorher einen User in der Tabelle anlegen der beispielhaft für alle anonymous User steht.
Sie geben also in die Tabelle unter Usernamen „anonymous“ ein und lassen das Passwort einfach leer. Sie können nun noch die Pfade eingeben die freigegeben werden sollen und stellen die Rechte ein. Ein Ratio ist bei anonymous login’s sinnlos, da es immer mehrere Logins zur gleichen Zeit gibt.

4. Erweiterte Optionen

In dieses Fenster gelangt man auch, wenn man in der Benutzerverwaltung auf „Erweiterte Optionen“ klickt.

4.1 FTP- Optionen

Hier werden die grundlegenden Servereinstellungen vorgenommen.

4.1.1 Brute Force Protection (BFP)

Dieser FTP-Server verfügt über eine Schutzfunktion der die einzelnen User Accounts gegen Brute Force Angriffe aus dem Netz sichern soll. Ist die Brute Force Protection (BFP) aktiviert, läßt der Server nur drei falsche Einlogversuche zu. Danach wird die IP Nummer des potentiellen Angreifers für eine gewisse Zeitspanne gesperrt. Dieser Schutz verhindert natürlich nicht das erraten zu einfacher Passwörter, macht aber ein automatisches durchprobieren aller Möglichkeiten unmöglich.

4.1.2 BFP neu initialisieren

Ein Klick auf diesen Button reinitialisiert die BFP Funktion und gibt alle derzeit durch BFP gesperrten IP’s wieder frei.

4.1.3 kein doppeltes Einloggen zulassen

Diese Funktion verhindert ein doppeltes Einloggen der gleichen IP Nummer und sorgt so für weniger Systemlast. Bitte beachten Sie beim Einsatz dieser Funktion das einige FTP Client’s (auch der IE®) gerne mehrere Verbindungen gleichzeitig herstellen und bei aktiver Sperre eine Fehlermeldung ausgeben.

4.1.4 Ereignisse in Logdatei speichern

Einmal aktiviert legt PFTP Logdateien im Programmordner an und protokolliert alles Systemereignisse mit.

4.1.5 Clients nach XX Minuten ohne Anfrage trennen

Diese Funktion trennen einen Client nach einer bestimmten Zeit ohne Serveranfrage.
Im Hintergrund laufenden Dateidownloads zählen nicht als Anfrage. Stellen Sie den Timeout also nicht zu klein ein. Der Defaultwert ist 10 Minuten. Durch die Funktion werden auch hängende Verbindungen nach der eingegebenen Zeit automatisch getrennt.

4.1.6 Freigegebene Laufwerke im Dateisystem anzeigen

Bei aktivierter Funktion werden die Pfade 2 bis 4 im Dateisystem angezeigt.

4.1.7 direktes LIST zulassen (nur in PFTP PRO)

Mit dieser Funktion wird ein direktes LIST auf Dateien zugelassen.
Standardmäßig ist diese Funktion deaktiviert und sollte auch nur aktiviert werden, wenn man sich absolut sicher ist.

4.1.8 Eigenen Bannertext zulassen (nur in PFTP PRO)

Ist diese Funktion aktiviert, kann man seinen eigenen Begrüßungstext (ca. 100 Zeichen) in das Textfeld eintragen, daß dann beim Einloggen von FTP Clients (z.B. WS-FTP) angezeigt wird. Die Änderungen, werden erst nach einem Serverstopp und erneuten Serverstart wirksam.

4.1.9 Port
Hier hat man die Möglichkeit den FTP Port zu ändern. Standardmäßig ist Port 21 eingetragen. Wenn Sie eine Firewall o.ä. benutzen, schauen Sie nach, welche Porteinstellung Sie vornehmen müssen.

4.1.10 Statische IP (LAN IP) dieses Rechners (nur in PFTP PRO)
In diesem Feld wird die statische (feste) IP Adresse des Rechners eingetragen.
Normalerweise ist die statische IP 127.0.0.1 und braucht auch nicht geändert zu werden.
In einigen Netzwerken kann es allerdings sein, daß die IP Adresse geändert wurde und in diesem Falle kann die dynamische IP nicht mehr korrekt ausgelesen werden.
Um die statische IP herauszubekommen, reicht es PFTP zu starten um die derzeitige IP zu sehen.

4.1.11 maximal gleichzeitige User
Um das System nicht zu überlasten, kann in diesem Feld angegeben werden, wieviel User sich gleichzeitig auf dem Server einloggen dürfen. 0 (Null) bedeutet unbegrenzte Anzahl an Usern.

4.2 Virtuelle Textdatei
Diese virtuelle Datei wird in das Dateisystem eingehängt und angezeigt, wenn das Kontrollkästchen *„Messagedatei in Filesystem anhängen“* aktiviert ist.

4.2.1 Name der Datei
Hier geben Sie den Namen der Datei ohne Dateierweiterung an.
Die Datei bekommt automatisch die Endung ***.txt***

4.2.2 Inhalt der Datei
Hier können Sie einen eigenen Text eingeben. Alles was Sie hier eingeben erscheint später in der Datei.

4.3 Nicht zugelassene Dateien
Hier können Sie verschiedene Dateitypen für den upload auf Ihren Server sperren. Wenn Sie z.B. keine illegalen mp3 Dateien auf Ihrem Server wünschen, geben Sie *.mp3 ein und klicken auf hinzufügen.
Es können nun keine mp3 Dateien mehr upgeloadet werden.

4.4 Execute Software
Hier können Sie einen Ordner festlegen der alle Dateien die in Ihn upgeloadet werden sofort mit dem dazugehörigen Programm startet, wenn das Kontrollkästchen „*Software auf Server ausführen*“ aktiviert ist. PFTP PRO benutzt für das starten der Dateien die Verknüpfungen von Windows®.
Diese Funktion ist mächtig, hat aber auch Gefahren.
Seien Sie mit dieser Funktion vorsichtig. Geben Sie den Executeordner niemals unbekannten Personen frei.

4.6 IP Sperre
Diese Funktion verhindert das Einloggen von allen eingetragenen gesperrten IP Nummern. Wildcards wie * und ? sind nur in PFTP PRO erlaubt.
Z.B. sperrt die Eingabe 127.101.44.* alle 255 IP Nummern, die mit 127.101.44 beginnen.

4.7 IP Begrenzung (nur in PFTP PRO verfügbar)
Diese Funktion beschränkt das Einloggen auf bestimmte IP Adressen. Wildcards wie * und ? sind erlaubt. Die Eingabe von 127.101.44.* erlaubt allen IP Nummern, die mit 127.101.44 beginnen, das Einloggen. Alle anderen werden nicht akzeptiert.

4.8 Ratio
Ein Ratio ist ein Verhältnis, das das Verhältnis von hochgeladenen zu heruntergeladenen Dateien (oder Bytes) beschreibt.
Hier können Sie bestimmen welche Art von Ratios Sie wünschen.
Entweder Dateibasiert (es werden nur die Dateien gezählt) oder Bytebasiert (es werden die Dateigrößen verglichen) oder beides.
Erreicht ein User ein bestimmtes Ratio, kann er ohne einen erneuten Dateiupload keine Dateien mehr von Ihrem Server laden.

4.9.7 Import von Userdaten aus CSV Dateien

PFTP PRO unterstützt den Import von Userdaten aus CSV Dateien, deren Daten durch das ; Zeichen voneinander getrennt sind. Diese Dateien erzeugt z.B. Excel® bei einem entsprechenden Datenexport. So können nun auch umfangreiche Userdaten importiert werden.

6.0 Die TLS/SSL Funktionen

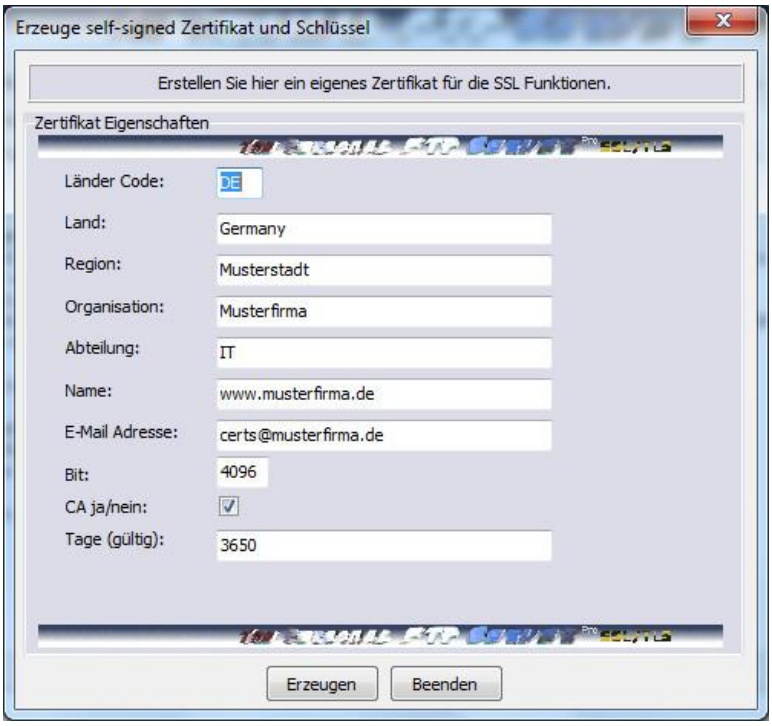
5.0.1 SSL Funktionalität

PFTP PRO SSL nutzt X.509 Zertifikate und private Schlüssel um einen sicheren Datenaustausch mit FTPS fähigen FTP Clients zu ermöglich.
Sowohl das Zertifikat als auch der eigene private Schlüssel werden direkt im Hauptfenster in den entsprechenden Eingabefeldern hinterlegt.

5.0.2 Zertifikat und Schlüssel

PFTPPRO erwartet hier zwei Dateien im PEM Format die einmal das Zertifikat und einmal den privaten Schlüssel enthalten.
Legen Sie diese Dateien unbedingt in geschützten Ordnern ab die NICHT für Dritte freigegeben sind.

5.0.3 Der Zertifikat Assistent



Um die sonst eher komplexen Dinge einer Zertifikaterstellung zu vereinfachen und den nötigen Kauf teurer Zertifikate bei einer Zertifizierungsstelle zu vermeiden nutzt PFTP PRO SSL eigene selbstsignierte Zertifikate.
Ein eigener Assistent unterstützt Sie bei der Erstellung. Sowohl das erstellte Zertifikat als auch der private Schlüssel werden im Anschluss automatisch in die entsprechenden Eingabefelder des Servers übernommen.

Geben Sie hier Ihre persönlichen Daten für Ihren Server ein und achten Sie darauf das die Zahl die sie unter Bit nur 1024, 2048 oder 4096 enthalten darf.
Aus Sicherheitsgründen empfehlen wir 4096 Bit.

6.0 Dies müssen Sie bei der Einrichtung Ihres SSL FTP Servers beachten

6.1 Einrichtung Ihres Routers

In den meisten Fällen sind Sie über einen Router mit dem Internet verbunden. Das bedeutet dass alle Anfragen aus dem Internet von außen immer als erstes an Ihrem Router ankommen. Damit Ihr Router weiß an wen er die Anfragen von außen in Ihrem internen LAN weiterleiten soll müssen Sie einmalig die Ports 21 (FTP Commandport für FTP ES) und Port 990 (FTP Commandport für implizites SSL) in Ihrer Routerfirewall eingehend freigeben sowie an die interne IP weiterleiten auf der PFTP PRO SSL erreichbar ist.

Im FTP Protokoll werden alle Datenübertragungen über weitere Ports (im weiteren Dataports genannt) durchgeführt.
Bei unverschlüsselten FTP Verbindungen werden diese Ports vom Router automatisch freigegeben da diese im Klartext über den Commandport gesendet und in Echtzeit ausgewertet werden.

Bei verschlüsselten FTP(E)S Verbindungen ist dies nicht möglich da diese Daten verschlüsselt übertragen werden und so der Router diese nicht sehen kann.
FTPS Verbindungen laufen daher am einfachsten immer im passive Mode ab (dies ist bei allen FTPS Clients auch die Default Einstellung) in der alle Dataportanfragen vom Client in Richtung Server aufgebaut werden.

Diese Data Ports legt der Server fest.

Bei PFTPPRO 8 SSL werden für den passiven Modus die Ports
16300 bis 21300 genutzt. Bei Bedarf können Sie die PASV Ports in den erweiterten Optionen des Servers auch ändern.
Geben Sie nun in Ihrem Router noch die genannten Ports (16300 bis 21300) in der Firewall frei und leiten Sie diese Ports ebenso weiter wie die Command Ports.

Nun können sich alle FTP(E)S fähigen Clients im Passive Mode voll verschlüsselt von außen mit PFTP PRO 8 SSL verbinden.

PFTP PRO SSL UNTERSTÜTZT CCC (Clear Command Channel)

Wenn Sie eine dynamische Firewall nutzen können CCC fähige Clients auch ohne die Freigabe der Data Ports mit dem Server verbinden.
Dabei werden die anfragen auf dem Command Port unverschlüsselt übertragen und nur die Daten selbst sind verschlüsselt. Der Router kann in diesem Fall also die nötigen Daten wieder selbst lesen und die Freigaben dynamisch durchführen.