Praktische Anleitung zu Konfiguration von IPSEC Verbindungen

mittels FreeS/WAN und PGPnet

-Screenshots-

Torsten Höfler

 $\label{eq:linear} htor@informatik.tu-chemnitz.de\\ hoefler@delta.de$

Inhaltsverzeichnis

1	Konfiguration eines PGPnet Clients (Windows) - Screenshots 3										
	1.1	PGPn	et Version 6.5.8	3							
		1.1.1	Erzeugen der Schlüssel	3							
		1.1.2	Vorhandene Schlüssel in PGPnet importieren	14							
		1.1.3	Konfigurieren von PGPnet	19							
		1.1.4	Hinzufügen einer neuen Verbindung	24							
	1.2	PGPn	et Version 7.0.3	28							
		1.2.1	Vorhandene Schlüssel in PGPnet importieren	28							
		1.2.2	Konfigurieren von PGPnet	34							
		1.2.3	Hinzufügen einer neuen Verbindung	39							

1 Konfiguration eines PGPnet Clients (Windows) - Screenshots

- 1.1 PGPnet Version 6.5.8
- 1.1.1 Erzeugen der Schlüssel

PGPkeys										
<u>File Edit View Keys Server Groups Help</u>)									
🥱 🗶 🏹 😵 🔍 😤 🌺 🖆 🛙										
Keys	Validity Trust	Size	Description							
•			F							

Abbildung 1: neuen Schlüssel erzeugen - 1

PGPkeys, nachdem alle vorhandenen Schlüssel gelöscht wurden.



Abbildung 2: neuen Schlüssel erzeugen - 2

Erzeugen eines neuen Schlüssels - Startlogo

Key Generation Wizard	×
PGP	What name and email address should be associated with this key pair? By listing your name and email address here, you let your correspondents know that the key they are using belongs to you. Eull name: freeswan Email address: freeswan
	< <u>Z</u> urück <u>W</u> eiter > Abbrechen Hilfe

Abbildung 3: neuen Schlüssel erzeugen - 3

Eingabe der Identifikationsdaten für den neuen Schlüssel, anhand des hier vergebenen Namens wird später der FreeS/WAN Key extrahiert.

Key Generation Wizard		×
	What type of key would you like to generate? If you don't know, it's recommended that you generate a Diffie-Hellman/DSS key pair. RSA is the "old-style" PGP key. Most new users of PGP will be expecting a Diffie-Hellman/DSS key. If you'd like more information on the differences between the two key types, press the Help button, below.	
PGP	Key Pair Type C <u>D</u> iffie-Hellman/DSS C <u>B</u> SA	
	< <u>Z</u> urück <u>W</u> eiter> Abbrechen Hilfe	

Abbildung 4: neuen Schlüssel erzeugen - 4

 RSA Verschlüsselung wählen.

Key Generation Wizard		X
-	How large a key pair do you wish to generate? As a rule, larger keys are more secure, but slower.	
	Key Pair Size	1
	1024 bits	
	C 1536 bits	
	C 2048 bits	
DCD	C <u>C</u> ustom (1024 - 2048 bits)	
	2048	
	< <u>Z</u> urück <u>Weiter</u> Abbrechen Hilfe	

Abbildung 5: neuen Schlüssel erzeugen - 5

 $1024~\mathrm{Bit}~\mathrm{RSA}$

Key Generation Wizard		×
	You can set your key pair to automatically expire within a certain amount of time. When your key pair expires, you will no longer be able to use it for encrypting or signing. However, it will still decrypt and verify. Once you generate your key pair, you will not be able to change its expiration setting. Key Expiration Key pair never expires Key pair <u>expires</u> on 22.08.02	
	< <u>Z</u> urück <u>W</u> eiter > Abbrechen Hilfe	

Abbildung 6: neuen Schlüssel erzeugen - 6

Gültigkeit des Schlüsselpaares (zu Testzwecken läuft es nie ab)

Key Generation Wizard		×
	Your private key will be protected by a parthat you do not write this passphrase dow Your passphrase should be at least 8 char contain non-alphabetic characters. Passphrase: Passphrase Quality : •••••	assphrase. It is important on. aracters long and should I Hide Typing
	< <u>Z</u> urück <u>W</u> eiter> Abbr	echen Hilfe

Abbildung 7: neuen Schlüssel erzeugen - 7

Persönliches Kennwort (Mantra).

Key Generation Wizard		×
	PGP is now generating your new key pair. On a slow machine, this could take several minutes. Please be patient.	
PGP	Complete	
	< <u>Zurück</u> Weiter> Abbrechen Hilfe	

Abbildung 8: neuen Schlüssel erzeugen - 8

Generierung des neuen Schlüssels abgeschlossen

Key Generation Wizard	×
PGP	If you have an Internet connection, we suggest that you send your new public key to the server. This will make it easy for your correspondents to get your key and communicate with you securely. If you don't have an Internet connection, or are not connected right now, leave "Send my key to the root server now" unchecked. You can send your key later from within PGPkeys.
	< Zurück Weiter > Abbrechen Hilfe

Abbildung 9: neuen Schlüssel erzeugen - 9

Schlüssel nicht an Root-Server schicken, wenn keine eindeutige Identifikation möglich ist!

Key Generation Wizard	×
8	Congratulations! You have just generated a PGP key pair!
LN O	You will now be able to receive secure messages and sign documents.
The second secon	If you wish to send your key to the server at a later date, simply right click on it in PGPkeys, and use the "Send to" menu item.
PGP	Click Finish below to add your new key to your keyring!
	< <u>∠</u> urück <u>Fertig stellen</u> Abbrechen Hilfe

Abbildung 10: neuen Schlüssel erzeugen - 10

Schlüssel in keyring speichern



Abbildung 11: neuen Schlüssel erzeugen - 11

Ansicht des neu erzeugten Schlüssels in PGPkeys



Abbildung 12: neuen Schlüssel erzeugen - 12

Die Dateien pubring.pkr und secring.pkr im Keyring-Verzeichnis

¦ ₽ P	GPk	eys											_ □	X
<u>F</u> ile	<u>E</u> dit	⊻iew	<u>K</u> eys	<u>S</u> erver	<u>G</u> roups	<u>H</u> elp								
Key	S X	& ©	Si Sa <u>A</u> c Di Ra Ra	gn at as Defa table sable a <u>v</u> oke averi <u>f</u> y Sij	ault Key gnatures	Ctrl+S Ctrl+D	۲	dity	Trus	t 🚺	Size	Descrip	tion	_
			<u>N</u> e Sł	ew Key hare S <u>p</u> lit		Ctrl+N								
			l <u>m</u>	port		Ctrl+M								
			Εž	port		Ctrl+E								
┛			Pr	operties .		Ctrl+I						 J		▶
														1.

1.1.2 Vorhandene Schlüssel in PGPnet importieren

Abbildung 13: Schlüssel importieren - 1

Menüpunkt Schlüssel importieren.

ę	💡 PG Pke	hz											- 🗆 🗵
	<u>F</u> ile <u>E</u> dit	⊻iew	<u>K</u> eys	<u>S</u> erver	<u>G</u> roups	<u>H</u> elp							
L	Select Fil	e Con	taining	j Key							3	2 ×	
	Suchen in:	6	🛛 pgpn	iet			•	٤	2	č *		=	cription
	🕅 pubrini	a okr					_	_		_	_	-	v public key
		g.piki niekr											rID
I	- Second	- SIG											v exportable sig
	Dateiname	e la	ectina	skr					1 Г	Öß	nen	1	
	Datolijane	~ s	eenny.	51/1						OĨI	ICH .	1	▶
	Dateityp:	F	Keyring	Files (*.pl	kr; *.skr; *.	pgp; *.p	ubkr; .) 🔻	1	Abbre	chen		
-												1	

Abbildung 14: Schlüssel importieren - 2

Schlüssel wählen (Keyring Files)



Abbildung 15: Schlüssel importieren - 3

Öffentlichen Schlüssel von freeswan signieren, und als "trusted" definieren

PGP Sign Key	? ×					
By signing the selected user ID(s), you are certifying based on your own direct first-hand knowledge that the key(s) and attached user ID(s) actually belong to the identified user(s).						
Before signing, make sure the key(s) were giv fingerprint with the owner.	ven to you in a secure manner by the owner or you have verified the					
Key/User Name	Fingerprint					
📧 freeswan <freeswan></freeswan>	5566 83FC 7868 2976 977F A556 8BC0 A379					
	`					
Allow signature to be exported. Othe	rs may rely upon your signature.					
More Choices	<u> </u>					

Abbildung 16: Schlüssel importieren - 4

Dialog zum signieren des Schlüssels

Second Se				_ 🗆 ×
<u>File E</u> dit <u>V</u> iew <u>K</u> eys <u>S</u> erver <u>G</u> roups	<u>H</u> elp			
🥱 🛪 📽 🔍 🛫 😤 🖆	¥ 🔳			
Keys	Validity	Trust	Size	Description
🛨 🖙 freeswan <freeswan></freeswan>	0	10 (D)	1024	RSA public key
🕀 🍖 pgpnet <pgpnet></pgpnet>		V////	1024	RSA key pair
<				

Abbildung 17: Schlüssel importieren - 5

Ansicht der komplett importierten Schlüssel

1.1.3 Konfigurieren von PGPnet



Abbildung 18: Optionen anpassen - 1

Konfiguration von PGPnet (Taskleistensymbol)

PGPnet	
Status Status Log Hosts Options	Address Subnet Authentication SA
PGPnet C 0 <u>n</u> ⊙ <u>0</u> ff	E <u>dit</u> <u>B</u> emove <u>A</u> dd <u>C</u> onnect
status : Off	0 active SAs

Abbildung 19: Optionen anpassen - 2

Menüpunkt Optionen

Options ?	×
General Authentication Advanced	
User Interface	
Expert Mode	
Security	
Allow communications with unconfigured hosts	
Require secure communications with all hosts	
Require valid authentication key	
Cache passphrases between logins	
Expiration	
Setup Keys (IKE) Primary Keys (IPSEC)	
✓ Duration : 0d, 01h, 00m + ✓ Duration : 0d, 01h, 00m +	
Megabytes: 5 🚽 Megabytes: 1024 🚽	
OK Abbrechen Hilfe	

Abbildung 20: Optionen anpassen - 3

Menüpunkt "General"

Options	? ×
General Authentication Advanced	
- PGPnet Keyring Files	
Public :	
d:\programme\pgp\PGP Keyrings\pubring.pkr	Browse
Private :	
d:\programme\pgp\PGP Keyrings\secring.skr	Bro <u>w</u> se
	Use Mu PGP Keuring Files
- PGP Authentication	
😤 pgpnet <pgpnet></pgpnet>	Select K <u>e</u> y
	Clear <u>K</u> ey
	OK Abbrechen Hilfe

Abbildung 21: Optionen anpassen - 4

Menüpunkt "Authentication"

Op	tions					? ×		
G	ieneral Au	Ithentication	Advanced					
	- Allowed F	emote Propo	osals					
		Ciphers :	CAST	✓ IripleDES	□ <u>N</u> one			
		Hashes :	☑ S <u>H</u> A-1	✓ MD5	∏ N <u>o</u> ne			
	Diffie	Hellman :	🗹 <u>1</u> 024 bits	☐ 1 <u>5</u> 36 bits				
	Con	npression :	□ <u>L</u> ZS	🔲 De <u>f</u> late				
	- Proposals							
	IKE	Authentical RSA Signat RSA Signat	tion Hash ture MD5 ture SHA	Cipher TripleDES TripleDES	DH 1024 bits 1024 bits	New		
						<u>E</u> dit		
	IPSEC	AH	ESP	IPPCP		<u>R</u> emove		
		None	MD5, TripleDE9	6 None S None		Move <u>U</u> p		
		None	SHA, HIPIEDES			Mo <u>v</u> e Down		
	Perfect Forward Secrecy : 1024 bits							
	Defa <u>u</u> lt	Settings						
				OK	Abbrec	hen Hilfe		

Abbildung 22: Optionen anpassen - 5

 $Men \ddot{u} punkt \ , Advanced``$

1.1.4 Hinzufügen einer neuen Verbindung

🕰 PGPnet				_ 🗆 ×
<u>F</u> ile <u>V</u> iew <u>H</u> elp				
Stat <u>u</u> s Log Hos <u>t</u> s				
Name	Address	Subnet	Authentication	SA
PGPnet-				
⊙ 0 <u>n</u> ○ <u>0</u> ff	E <u>d</u> it	<u>R</u> emove	Add	Connect
status : Un; user logged off	U active SAs			11.

Abbildung 23: Neue Verbindung anlegen - 1

Hinzufügen eines neuen IPSEC-Servers

Host/Gateway	×
<u>N</u> ame : apollo IP Address : 10 . 1 . 40 . 1 <u>D</u> NS Lookup	
Secure Host	
Shared Secret Configuration	
Identity Type : IP Address	
[dentity: 10 . 1 . 40 . 17	
Remote Authentication O Any <u>v</u> alid key O <u>P</u> GP Key	
G freeswan <freeswan> ▲</freeswan>	
<u> </u>	

Abbildung 24: Neue Verbindung anlegen - 2

Generelle Einstellungen

ee Ek	PGPnet				
	e <u>v</u> iew <u>H</u> eip				
		Address	Subast	Authentication	
		10.1.40.1	Subnet		
					- 8
					- 8
	DCDust				
		E <u>d</u> it	<u>R</u> emove	Add	Disconnect
stat	us : On; user logged on	1 active SAs			//_

Abbildung 25: Neue Verbindung anlegen - 3

Verbindung aktivieren (Connect)

ee Fik	PGPnet					
	e <u>v</u> iew <u>n</u> eip					
		*				1
	Destination	Protocol	Encryption	Authentication	Expires	Max. Data
	∰ 10.1.40.1	ESP	TripleDES	HMAC MD5	22.08.01 12:26:45	
[PGPnet				Sav	/ <u>e</u> <u>R</u> emove
stat	us : On; user logged	on	1 active	e SAs		

Abbildung 26: Neue Verbindung anlegen - 4

Verbindung hergestellt

1.2 PGPnet Version 7.0.3

1.2.1 Vorhandene Schlüssel in PGPnet importieren

<mark>₿</mark> ₽	GPke	eys											_	
<u>F</u> ile	<u>E</u> dit	⊻iew	<u>K</u> eys	<u>S</u> erver	<u>G</u> roups	<u>H</u> elp								
С Кеул	X :	4 %	Si Se <u>A</u> c Er Di Re Re	gn Ig as Defa Id Iable sable syoke sverify Sij	ault Key gnatures	Ctrl+S Ctrl+D	F	dity	Tru	ust	Size	Desc	ription	
			<u>N</u> e SP	ew Key rare S <u>p</u> lit.		Ctrl+N								
			l <u>m</u> E <u>x</u>	port port		Ctrl+M Ctrl+E								
╘			P <u>r</u>	operties		Ctrl+l								

Abbildung 27: Schlüssel importieren - 1

Schlüssel importieren

B File	Select File	Containing Key	?×□×
- <u>-</u>	<u>S</u> uchen in:	🔁 pgpnet 💽 🔝	
Ke	Pubring		pn
	, Datei <u>n</u> ame:	secring	[]
•	Da <u>t</u> eityp:	Keyring Files (*.pkr; *.skr; *.pgp; *.pubkr;)	Abbrechen

Abbildung 28: Schlüssel importieren - 2

Keyring File auswählen

pgpnet <pgpnel< th=""><th>Þ</th><th>? ×</th></pgpnel<>	Þ	? ×
General Subki	eys	
<u>I</u> D:	0x0380CF0B	
<u>T</u> ype:	RSA Legacy	
<u>S</u> ize:	1024	
<u>C</u> reated:	21.08.01	
<u>E</u> xpires:	Never	
Cip <u>h</u> er:	IDEA	
<u> </u>	Enabled	Change <u>P</u> assphrase B A15C 49B5 BE25 50D6
– Trust Model– Invalid	Valid	I Hexadecimal Untrusted Trusted
I <u>M</u> I <u>m</u> plicit T	rust	
		Schließen Hilfe

Abbildung 29: Schlüssel importieren - 3

Optionen (Key Properties) - (incl. Hexadezimalem Fingerprint)



Abbildung 30: Schlüssel importieren - 4

FreeS/WAN Public Key signieren

PGP Sign Key	?×				
By signing the selected user ID(s), you are certifying based on your own direct first-hand knowledge that the key(s) and attached user ID(s) actually belong to the identified user(s). Before signing, make sure the key(s) were given to you in a secure manner by the owner or you have verified the fingerprint with the owner.					
Key/User Name	Fingerprint				
Freeswan <freeswan></freeswan>	5566 83FC 7868 2976 977F A556 8BC0 A379				
☐ Allow signature to be exported. Other	rs may rely upon your signature.				
More Choices	<u> </u>				

Abbildung 31: Schlüssel importieren - 5

Bestätigung der Unterzeichnung

F PGPkeys			
<u>File E</u> dit <u>V</u> iew <u>K</u> eys <u>S</u> erver <u>G</u> roups <u>H</u> el	P		
🤏 🛪 🔌 🔍 🛫 🎭 🧏 🖆 I			
Keys	Validity Trust	Size	Description
🛨 🖙 freeswan <freeswan></freeswan>)	1024	RSA legacy public
🕀 🕎 pgpnet <pgpnet></pgpnet>	🍖 🛛 🖉	1024	RSA legacy key pa
			•

Abbildung 32: Schlüssel importieren - 6

Konfigurierte Schlüssel

1.2.2 Konfigurieren von PGPnet



Abbildung 33: Optionen anpassen - 1

VPN wählen (Tray-Icon)

📲 PGPnet		
File View Help Status ✓ VPN	Intruders	PGPNET 🛈
Intruders Log Options Ctrl+T	Address Subnet	Authentication SA
	Properties <u>R</u> em	rove Add Connect
status: On	0 active SAs	

Abbildung 34: Optionen anpassen - 2

Optionen

GP Options	? ×				
General VPN	Files Email HotKeys Servers CA Advanced VPN Authentication VPN Advanced				
VPN	VPN PGPnet uses standard IP Security and Internet Key Exchange protocols to communicate securely with other devices over the Internet. Enable VPN connections				
- Dynamic VF	Dynamic VPN When communicating with unconfigured hosts, you can choose to attempt secure communications automatically, allow secure communications, or require them.				
- Automatic K	ey Renewal				
Ö	Setup Keys (IKE) Primary Keys (IPsec)				
	✓ Duration: 0d, 01h, 00m → ✓ Duration: 0d, 01h, 00m →				
	Megabytes: 1024				
	OK Abbrechen Hilfe				

Abbildung 35: Optionen anpassen - 3

Optionen - "VPN"

PGP Options
General Files Email HotKeys Servers CA Advanced VPN VPN Authentication VPN Advanced Image: California and Californi and California and Californi and California and Calif
PGP Authentication
Pgpnet <pgpnet> Select Key</pgpnet>
Clear <u>K</u> ey
Remote Authentication
Normally, you will want to require a valid authentication key or certificate from configured hosts.
Require valid remote authentication from configured hosts
Unconfigured hosts may have no prior trust relationship with you. Allowing them to connect with an invalid key or certificate provides encryption of traffic which would otherwise be in the clear.
Require valid remote authentication from <u>unconfigured hosts</u>
OK Abbrechen Hilfe

Abbildung 36: Optionen anpassen - 4

Optionen - "VPN Authentication"

PGP Options					<u>? ×</u>	
General VPN	Files	Email VPN A	HotKeys Suthentication	Servers	CA Advanced VPN Advanced	
Diffie	Ciphers: Hashes: Hellman:	□ <u>CAST</u> □ <u>CAST</u> □ S <u>H</u> A-1 □ <u>1</u> 024 bits	 ✓ <u>I</u>ripleDES ✓ <u>M</u>D5 ✓ 1<u>5</u>36 bits 	∏ <u>N</u> one ∏ N <u>o</u> ne		
Cor — Proposals	mpression:	<u>⊢</u> <u>L</u> ZS	☐ De <u>f</u> late			
IKE	Authentica RSA Signa RSA Signa	tion Hash ture SHA ture MD5	Cipher TripleDES TripleDES	DH 1024 1024	Ne <u>w</u>	
IPsec AH ESP IPPCP Bemove None SHA, TripleDES None MD5, TripleDES None Move Up Move Dov				<u>H</u> emove Move <u>Up</u> Ma <u>v</u> e Dawn		
Perfect Forward Secrecy: 1024						
Defa <u>u</u> lt Settings						
			0	< At	brechen Hilfe	

Abbildung 37: Optionen anpassen - 5

Optionen - "VPN Advanced"

1.2.3 Hinzufügen einer neuen Verbindung

🕰 PGPnet				- D ×
<u>F</u> ile Vie <u>w</u> <u>H</u> elp				
≪ Status 👜 ⊻PN 💕 Intr	uders		PGP	
Name	Address	Subnet	Authentication	SA
	Properties	<u>H</u> emove	<u>Add</u>	Connect
status: On	0 active SAs			

Abbildung 38: Neue Verbindung anlegen - 1

PGPnet Grundfenster

Host ? 🗙
<u>N</u> ame: apollo
IP Address: 10 . 1 . 40 . 1 DNS Lookup
Secure Host
Connection Options Connect automatically Require manual connection Username: Authentication Type :
Shared Secret Set S <u>h</u> ared Passphrase
Remote Authentication
C Any valid <u>k</u> ey C PGP Key
Ger freeswan < freeswan>
Use <u>W</u> izard <u>D</u> K <u>C</u> ancel

Abbildung 39: Neue Verbindung anlegen - 2

Neue Verbindung anlegen (Expert Mode)

File View Help				
≪ Status 📴 ⊻PN 💕 Intr	uders 🗐 🗐 Log 🛛 🗎		PGP	'NET 💛
Name	Address	Subnet	Authentication	SA
apollo	10.1.40.1			
	Properties	<u>R</u> emove	Add	Disconnect

Abbildung 40: Neue Verbindung anlegen - 3

Verbindung herstellen (Connect)

8	PGPnet					
 	,					
	✔ Status 🛛 🗗 YF	PN 🔊 🔊 İnţi	ruders o	Elog		
	Destination	Protocol End	ryption	Authentication	Expires	Sent / Rovd
	₽ 10.1.40.1	ESP Trip	leDES	HMAC SHA	24.08.01 11:32:10	805 KB / 57.0 KB
	I					
					Properties	Sav <u>e</u> <u>R</u> emove
st	atus: On		1 active	SAs		

Abbildung 41: Neue Verbindung anlegen - 4

Verbindung hergestellt (Status)