HowTo – IPSec mit XAuth

Damit auch Endgeräte mit Google's Android Betriebssystem oder die Apple-Produktpalette (iPad, iPhone, MacBook) eine IPSec-Verbindung mit TDT-Geräten herstellen können, muss dazu an den TDT-Geräten eine IPSec-Verbindung mit XAUTH konfiguriert werden.

Dieses HowTo beschreibt beispielhaft die dazu notwendingen Schritte.

1 Router Konfiguration

1.1 Anlegen einer IPSec Konfiguration

Der TDT-Router stellt die sog. »linke« Seite, den VPN-Server eines VPN-Netzwerkes dar. Folgende Konfigurationsparameter sind auf einem TDT-Gerät nötig, damit (mobile) Endgeräte eine VPN-Verbindung zu diesem initiieren können:

Parameter	Wert	
Global Settings		
Action on Startup	Load/Add	
Connection Type	Tunnel	
Enable Dead Peer Detection	Yes	
DPD Action on Timeout	Clear	
Phase1(ISAKMP) Settings		
ISAKMP Method	Main Mode	
Our/Left IP-Address	z.B. %ppp3 Dieser Wert muss dem Interface entsprechen, über das die VPN-Verbindung aufgebaut werden soll.	
Peer/Right IP-Address	%any	
Authentication Method	Pre-Shared-Keys	
Our/Left ID	Our/Left IP	
Peer/Right ID	Peer/Right IP	
Pre-Shared-Key / Confirm Pre-Shared-Key	IHRGEHEIMERPRESHAREDKEY	
XAuth Server	Yes	
MODECFG-Server	Yes	
XAuth Username	USERNAME	
XAuth Password (Assigned) / Confirm XAuth Password (Assigned)	PASSWORT	
IKE Algorithmus	**Encryption**	aes128
	Authentication	sha1
	MODP-Group	KEINE
IKE Lifetime	1h	

Parameter	Wert	
Phase2 Settings		
Local Subnet	192.168.0.0/24	
Local Source IP	192.168.0.50	
Remote Subnet	192.168.100.0/24	
Encapsulating Security Payload (ESP)	**Encryption**	aes128
	Authentication	sha1
	PFS-Group	KEINE

1.2 Zugriff für VPN-Clients auf das lokale Netzwerk

> Hinweis
> ➢ Damit nun die per VPN angebundenen (mobilen) Endgeräte auch Zugriff auf das lokale Netzwerk erhalten, muss dazu noch eine Firewall-Regel hinzugefügt werden.

Zum anpassen dieser Einstellung sind nur wenige Schritte nötig. Navigieren Sie dazu nach ***Networking > Linux Firewall*** und wechseln Sie zur Tabelle ***Network address translation (nat)***. Fügen Sie beim Abschnitt ***Packets after routing (POSTROUTING)*** eine neue Regel hinzu. Für diese Regel wählen Sie folgende Optionen:

Action to take	Comment	Outgoing Interface
Masquerade	NAT for xAuth Clients	***Equals*** -> ***eth1***

Nachdem Sie diese Regel erfolgreich hinzugefügt haben, muss diese mit einem Klick auf den Button ***[Apply Configuration]*** übernommen werden.

1.3 Konfiguration abschließen

Um die Konfiguration abzuschließen ist es nötig die durchgeführten Änderungen dauerhaft zu speichern. Dazu wechselt man auf die Seite ***Permanent Save*** und drückt auf ***Save Config***.

> Achtung!
> ➢ Wird dieser Schritt nicht ausgeführt, gehen die Einstellungen bei einem Router-Neustart verloren.

2 Mobile Device

2.1 Android 4.0

Die IPSec-Verbindung wurde mit der aktuellen Version von Android getestet.

Öffnen Sie die Systemeinstellungen. Unter ***Drahtlos & Netzwerke*** wählen Sie den Menüpunkt ***mehr*** aus. Im darauf erscheinenden Menü wählen Sie ***VPN*** aus. Durch berühren des Menüpunktes ***VPN hinzufügen*** können Sie die Einstellungen der neuen VPN-Verbindung editieren. Verwenden Sie dabei folgende Einstellungen:

Parameter	Wert
Name	Name der Verbindung
Typ	IPSec Xauth PSK
Serveradresse	IP / DNS-Name der Gegenstelle
Vorinstallierter IPSec-Schlüssel	IHRGEHEIMERPRESHAREDKEY

Wenn Sie nun die Verbindung starten, werden Sie nach einem Benutzernamen und einem dazugehörigen Passwort gefragt. Verwenden Sie dazu die bei ***XAuth Username*** und ***XAuth Password*** definierten Werte.

Ein Schlüsselsymbol in der Menüleiste signalisiert nun, dass die Verbindung erfolgreich hergestellt werden konnte.

2.2 Apple iOS 5

Die IPSec-Verbindung wurde mit einem iPad der ersten Generation und der Software Version 5.1.1 getestet.

Navigieren Sie in den Einstellungen zu ***Allgemein > Netzwerk > VPN > VPN hinzufügen***

Wählen Sie folgende Werte im Konfigurationsmenü:

Parameter	Wert
Art der Verbindung	IPSec
Beschreibung	Bezeichnung der Verbindung
Server	IP / DNS-Name der Gegenstelle
Account	Xauth Username
Kennwort	Xauth Password
Shared Secret	IHRGEHEIMERPRESHAREDKEY

In der Menüleiste signalisiert das Symbol ***VPN*** den erfolgreichen Verbindungsaufbau.

Weitere Informationen zu IPSec Einstellungen in iOS wie z.B. unterstützte Verschlüsselungsarten, können dem offiziellen **iPhone OS Enterprise Deployment Guide** im Kapitel **Cisco VPN Server Configuration** (ab Seite 67) entommen werden.

http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf (Second Edition, for Version 3.2 or later, Stand 11.06.2012)

3 Verschlüsselungsarten

Die folgenden Verschlüsselungsarten werden sowohl von Android als auch von Apple iOS unterstützt. Sie wurden erfolgreich mit unseren Geräten getestet.

AES 128 - AES 192 - AES 256