TheGreenBow IPSec VPN Client

Konfigurationsbeispiel

Watchguard Firebox X Edge e-Series

WebSite: http://www.thegreenbow.de
Kontakt: support@thegreenbow.de

Configuration Guide written by:

Autor:	Anastassios Stafilidis
Firma:	ASCS GmbH, Ihr IT-Partner, www.ascs.de

Inhalt

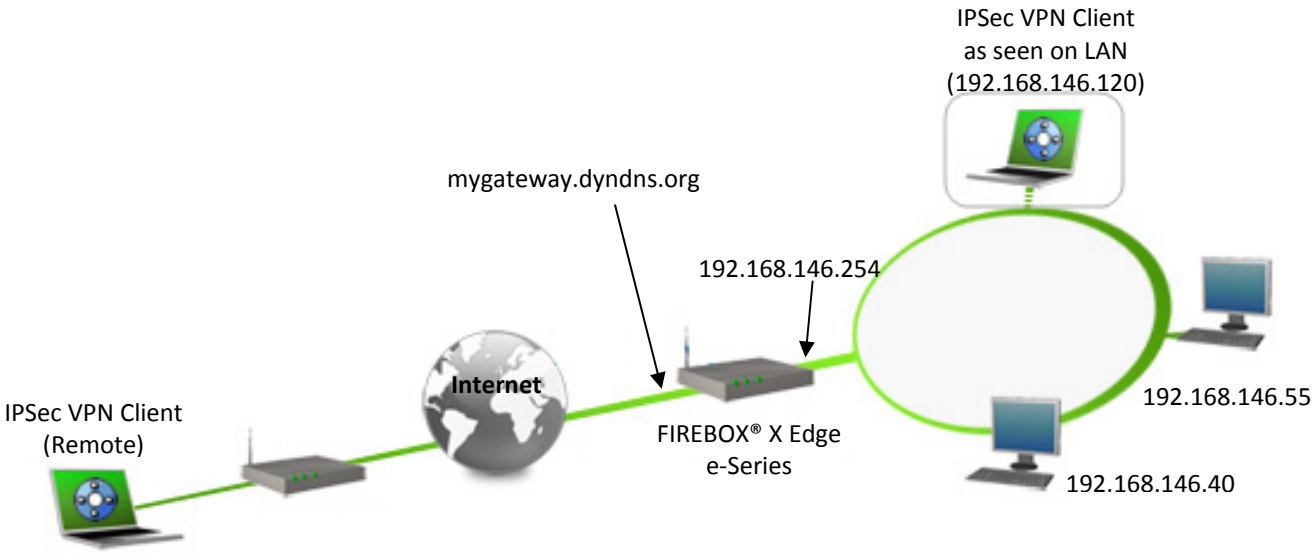
1 Einleitung

1.1 Ziel der Anleitung

Dieses Konfigurationsbeispiel beschreibt eine mögliche Konfiguration des TheGreenBow IPSec VPN Client, um einen IPSec Tunnel zu einem WatchGuard Firebox® X Edge e-Series und dem dahinter liegenden Firmen- oder Heimnetzwerk aufbauen zu können.

1.2 VPN Netzwerktopologie

Dieses Beispiel zeigt, wie wir den TheGreenBow IPSec Client in das lokale Netzwerk hinter der WatchGuard Firebox® X Edge e-Series verbinden. Der Rechner mit dem VPN Client ist mit dem Internet über DSL oder einem Firmennetzwerk verbunden. Die hier aufgeführten IP Adressen und Ranges dienen nur als Beispiel.



1.3 WatchGuard Firebox® X Edge e-Series Einschränkungen

Uns sind keine Einschränkungen bekannt. Die Firmwareversion wird auf der Hauptübersichtsseite der Benutzeroberfläche (unter „Device Information“) angezeigt. Mehr Informationen finden Sie unter http://www.watchguard.de.

1.4 WatchGuard Firebox® X Edge e-Series Security Appliance VPN Gateway

Unseren Test haben wir mit einer WatchGuard Firebox® X55e mit der Firmware Version 11.2.3.B267784 (Fireware XTM OS) durchgeführt.

1.5 WatchGuard Firebox® X Edge e-Series Security Appliance Produktinformationen

Alle Produktinformationen, Handbücher, FAQ und Hilfestellung zu Ihrer WatchGuard Firebox® X Edge e-Series Appliance finden Sie auf den Watchguard Webseiten: http://www.watchguard.de.

Watchguard Produktseite	http://www.watchguard.com/international/de/products/index.asp?t=main
Watchguard Handbuch	http://www.watchguard.com/help/documentation/edge.asp
Watchguard FAQ/Hilfe	http://www.watchguard.com/help/documentation/xtm.asp

2 WatchGuard Firebox® X Edge e-Series VPN Konfiguration

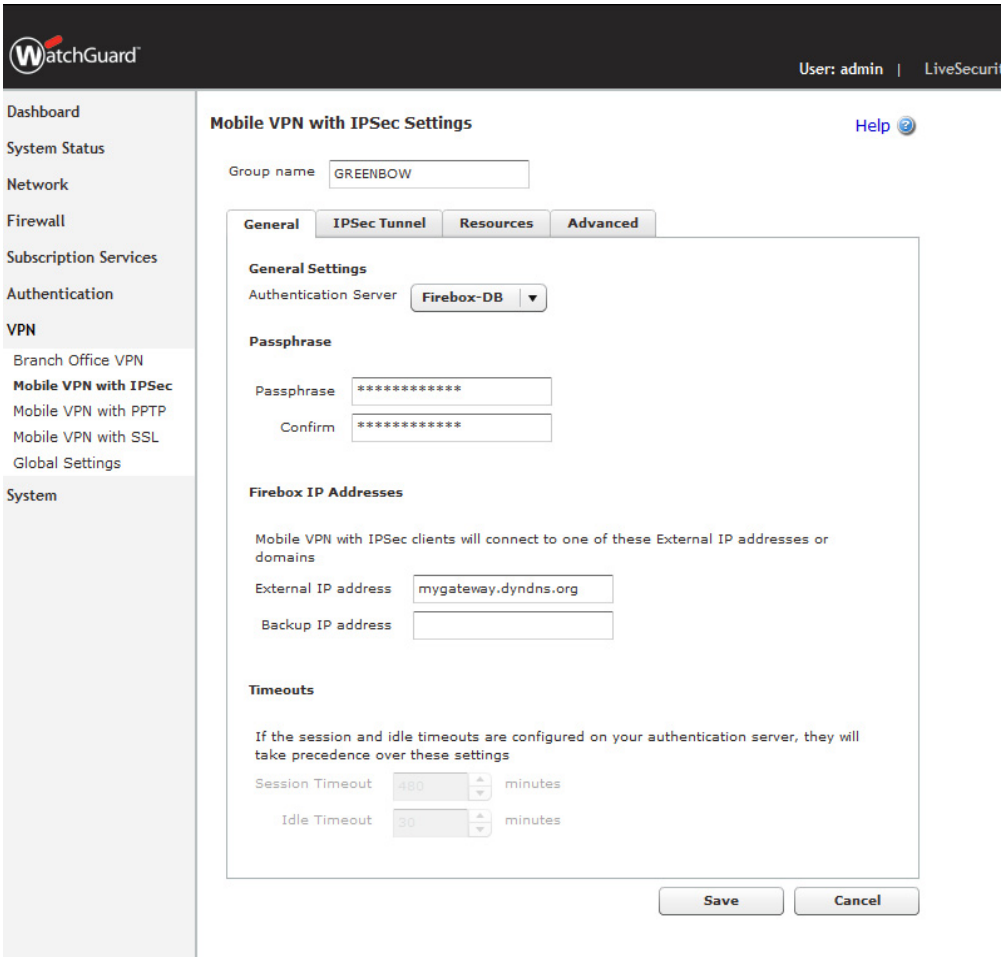
Dieses Kapitel beschreibt die Konfiguration der WatchGuard Firebox® X Edge e-Series.

2.1 Vorbereitungen

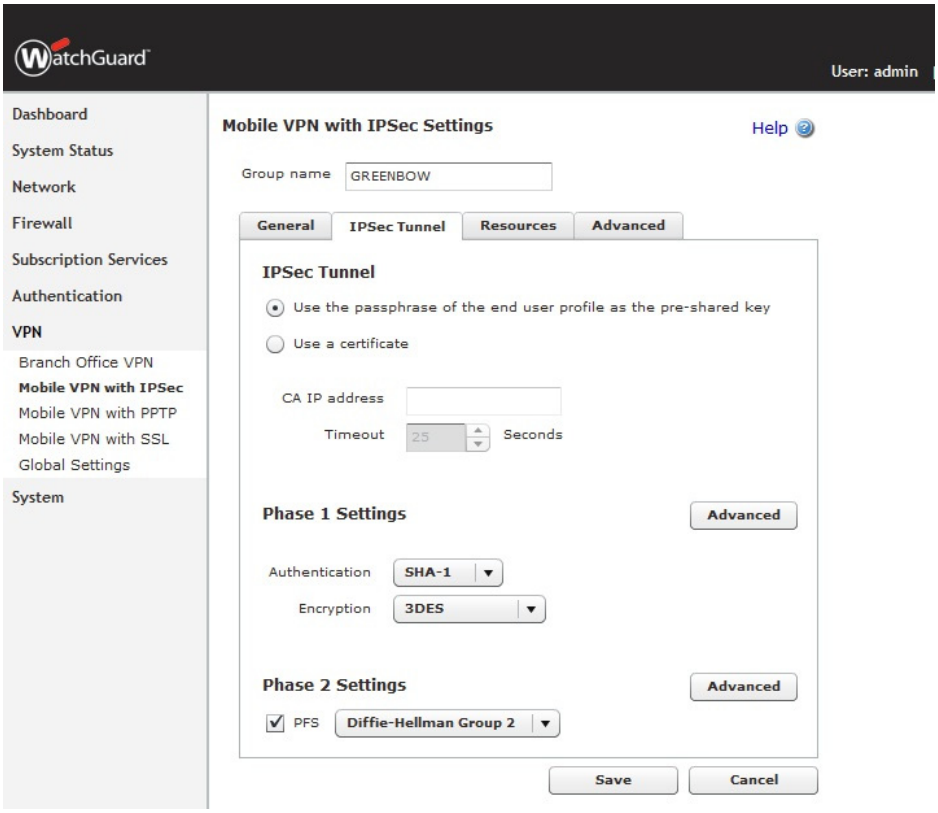
Damit Ihre WatchGuard Firebox® X Edge e-Series über einen Namen aus dem Internet erreichbar ist, sollten Sie einen dynamischen DNS Dienst konfigurieren. Weitere Hilfe zur Einrichtung finden Sie in Ihrem WatchGuard Firebox® X Edge e-Series Handbuch oder unter http://www.watchguard.de.

2.2 Einstellungen in der WatchGuard Firebox® X Edge e-Series

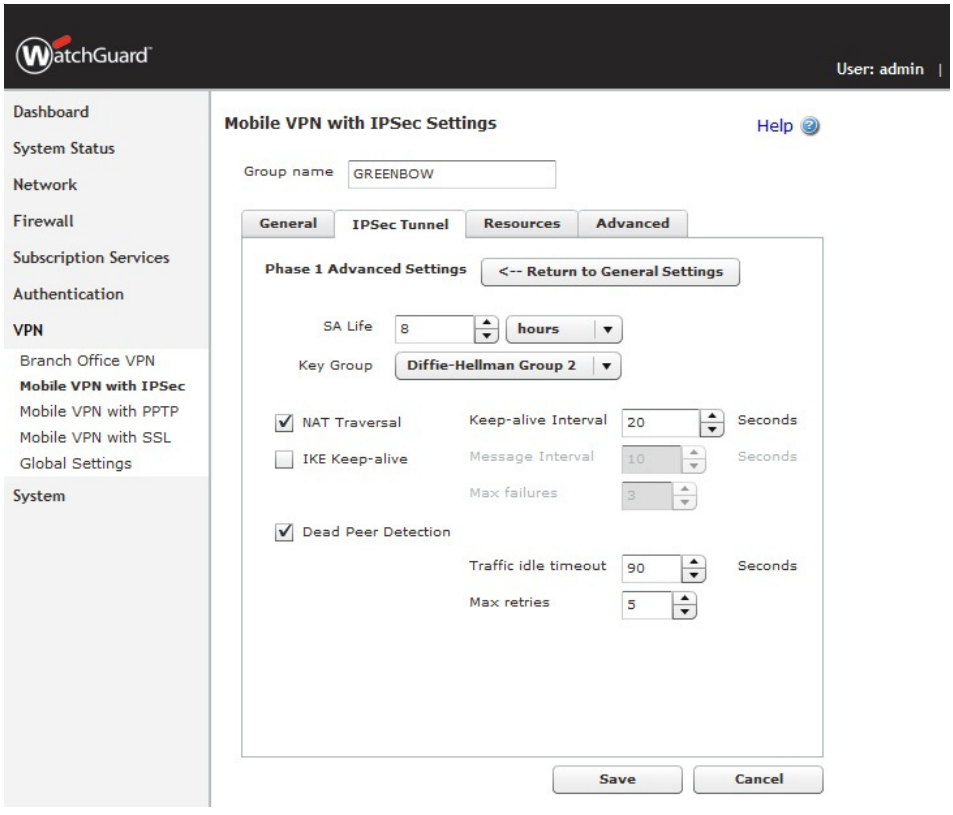
Wählen Sie in der Administrationsoberfläche den Menüpunkt „**VPN**“. Wählen Sie nun im linken Menü „**Mobile VPN with IPSec**“ aus. Geben Sie einen „Group Name“ (in unserem Beispiel „GREENBOW“) ein. Geben Sie im Reiter „General“ unter „Passphrase“ den Preshared Key und unter „Firebox IP Addresses“ > „External IP address“ die externe IP Adresse des Routers oder den dyndns-Namen (in unserem Beispiel mygateway.dyndns.org) ein.



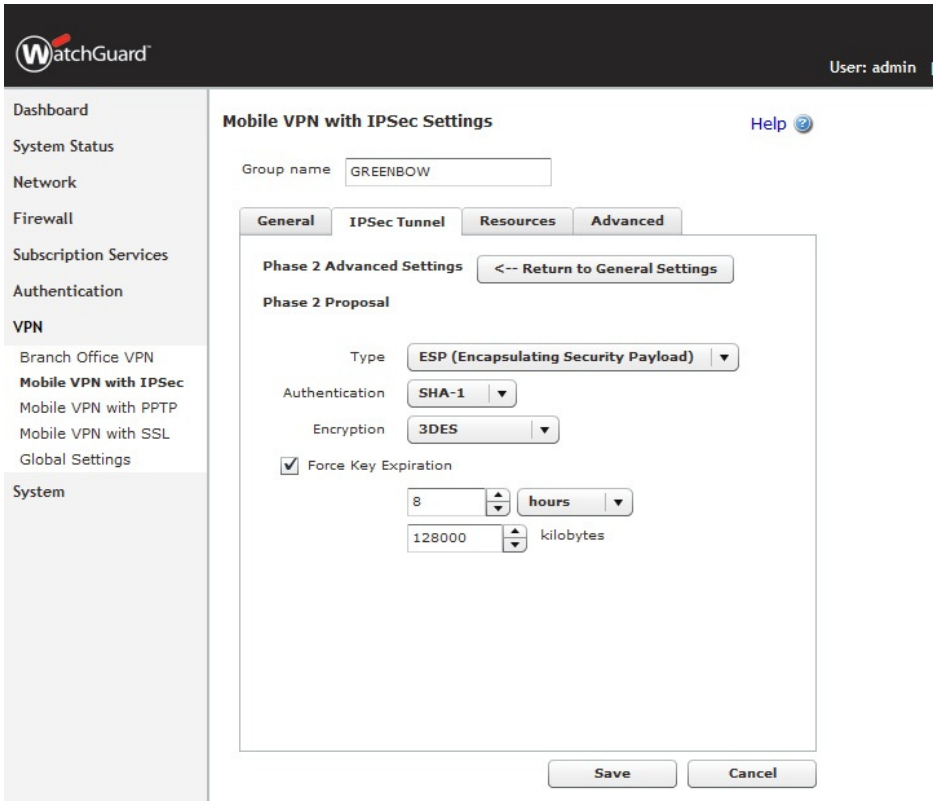
Im Reiter IPSec Tunnel den „Use the passphrase of the end user profile as the pre-shared key“ belassen und Phase 1 wie Phase 2 Einstellungen vornehmen (siehe Beispielbilder).



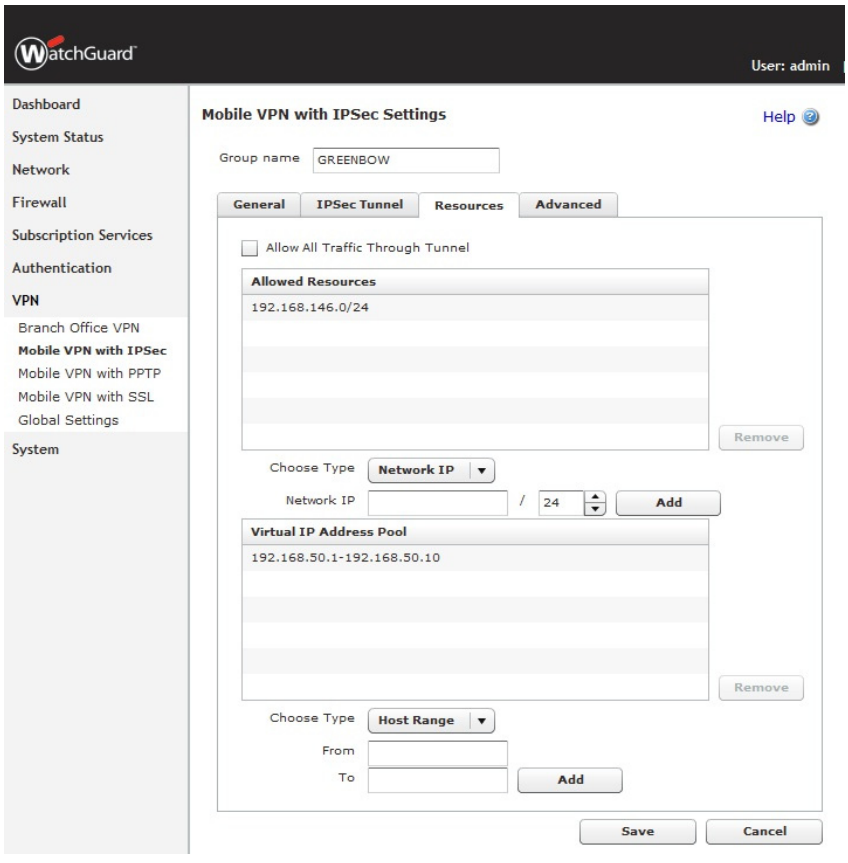
Phase 1 erweiterte Einstellungen



Phase 2 erweiterte Einstellungen

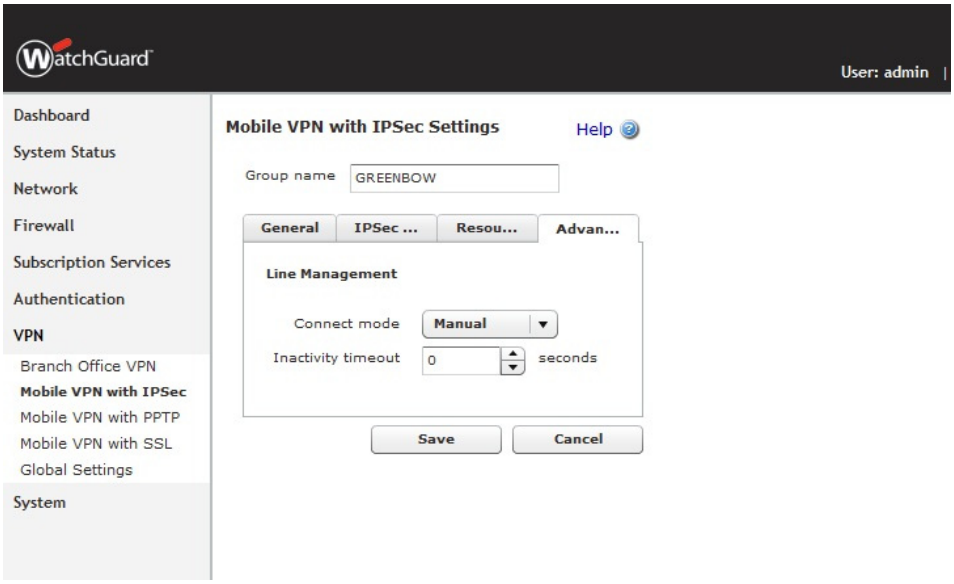


Im Reiter „Resources“ unter „Allowed Resources“ das Subnetz / die Subnetze eingeben an dem/an denen die externe Benutzer zugreifen dürfen (in unserem Beispiel das komplette 192.168.146.0/24 Subnetz). Wenn „Allow All Traffic Through Tunnel“ aktiviert wird, erfolgt der Zugriff ins Internet durch den VPN Tunnel.



Unter „Virtual IP Address Pool“ muss eine oder mehrere IP Adressen (nicht vom eigenen Subnet) definiert werden (in unserem Bespiel die IP-Adressen 192.168.50.1 bis 192.168.50.10). Diese werden später als „VPN Client Adresse“ im Greenbow VPN Client verwendet.

Im Reiter „Advanced“ bleibt alles unverändert

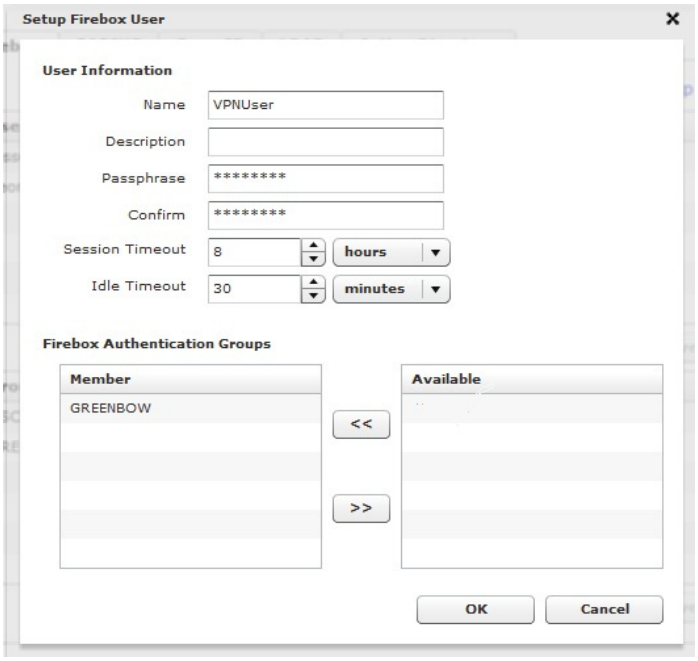


Mit „Save“ die gerade vorgenommene Einstellungen speichern. Ein Blick unter „Firewall“ > „Mobile VPN Policies“ bestätigt dass für die Gruppe „GREENBOW“ Firewall Regeln für die VPN Verbindung(en) erstellt wurden. Unter „Firewall“ > „Firewall Policies“ sind keine zusätzliche Firewall Regeln zu erstellen.

Voraussetzung für die VPN Verbindung ist das Vorhandensein mindestens eines Firefox Benutzers. Dieser kann ein lokaler Benutzer (in unserem Beispiel „VPNUser“ aus der Firebox-DB) oder ein Benutzer aus dem Active Directory eines vorhandenen Domain Servers sein.

Wählen Sie in der Administrationsoberfläche den Menüpunkt „**VPN**“. Wählen Sie nun im linken Menü „**Authentication**“ aus. Klicken Sie auf „Servers“ und im Reiter „Firebox“ unter „Users“ auf „Add…“ um einen neuen lokalen Benutzer anzulegen.

Im Fenster „Setup Firebox User“ den Namen des VPN Benutzers, optional eine kurze Beschreibung und das Passwort für die Authentifizierung für die VPN Einwahl eingeben. Aus den verfügbaren Gruppen die GREENBOW Gruppe auswählen und mit den Pfeilen nach links den Benutzer „VPNUser“ als Mitglied der GREENBOW Gruppe einfügen. Den Vorgang mit „OK“ bestätigen.

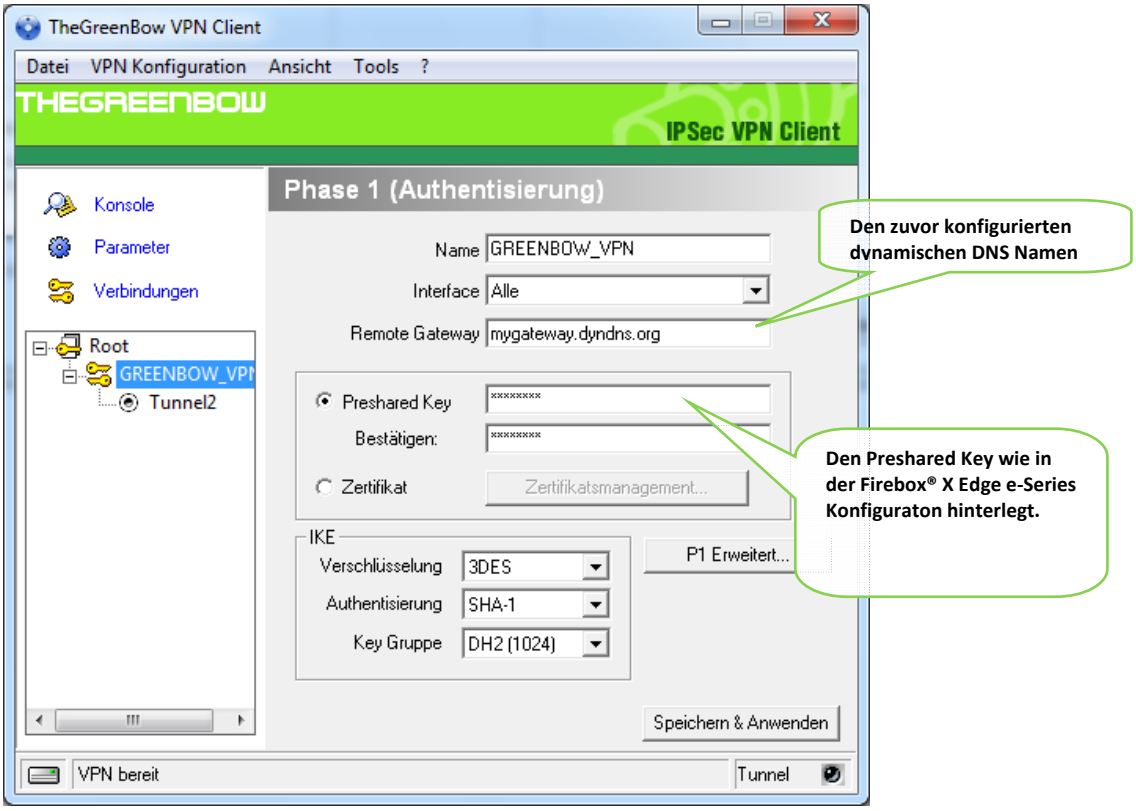


3 TheGreenBow IPSec VPN Client Konfiguration

Dieses Kapitel beschreibt die Konfigurationseinstellungen des TheGreenBow IPSec VPN Client.

Die aktuellste Version des TheGreenBow IPSec VPN Client finden Sie auf der TheGreenBow Webseite: http://www.thegreenbow.de/vpn_down.html.

3.1 VPN Client Phase 1 (IKE) Konfiguration



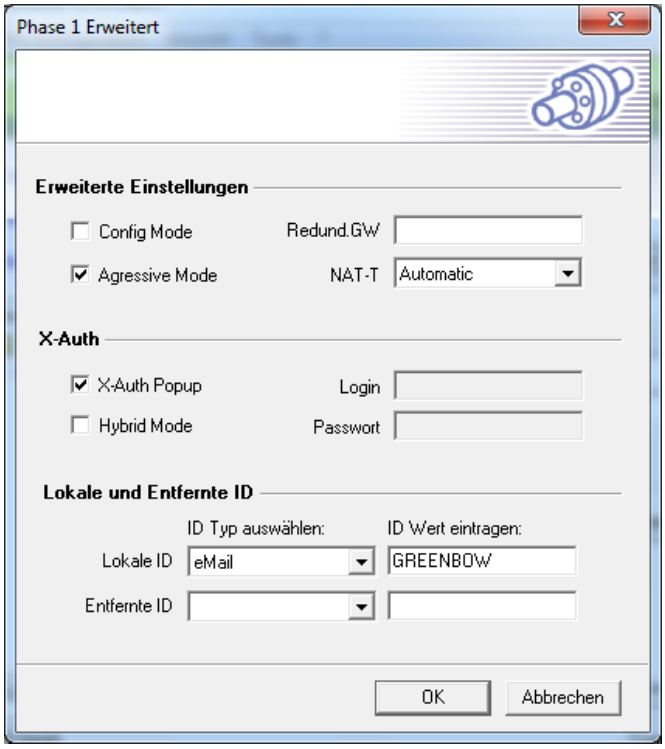
Phase 1 Konfiguration

Zur Benutzerauthentisierung verwenden wir in diesem Beispiel die Methode per Preshared Key und X-Auth. Weitere Möglichkeiten der Authentisierung wie z.B. durch Token, Zertifikate usw. entnehmen Sie bitte Ihrer WatchGuard Firebox® X Edge e-Series Dokumentation.

Geben Sie einen eindeutigen Namen für die VPN Verbindung (in unserem Beispiel „GREENBOW_VPN). „Interface“ kann auf „Alle“ bleiben. Im „Remote Gateway“ den dynamischen DNS Namen (in unserem Beispiel „mygateway.dyndns.org“) oder die externe IP Adresse der WatchGuard Firebox® eingeben. Setzen Sie nun unter „IKE“ die in der WatchGuard Firebox® X Edge e-Series definierten Werte ein.

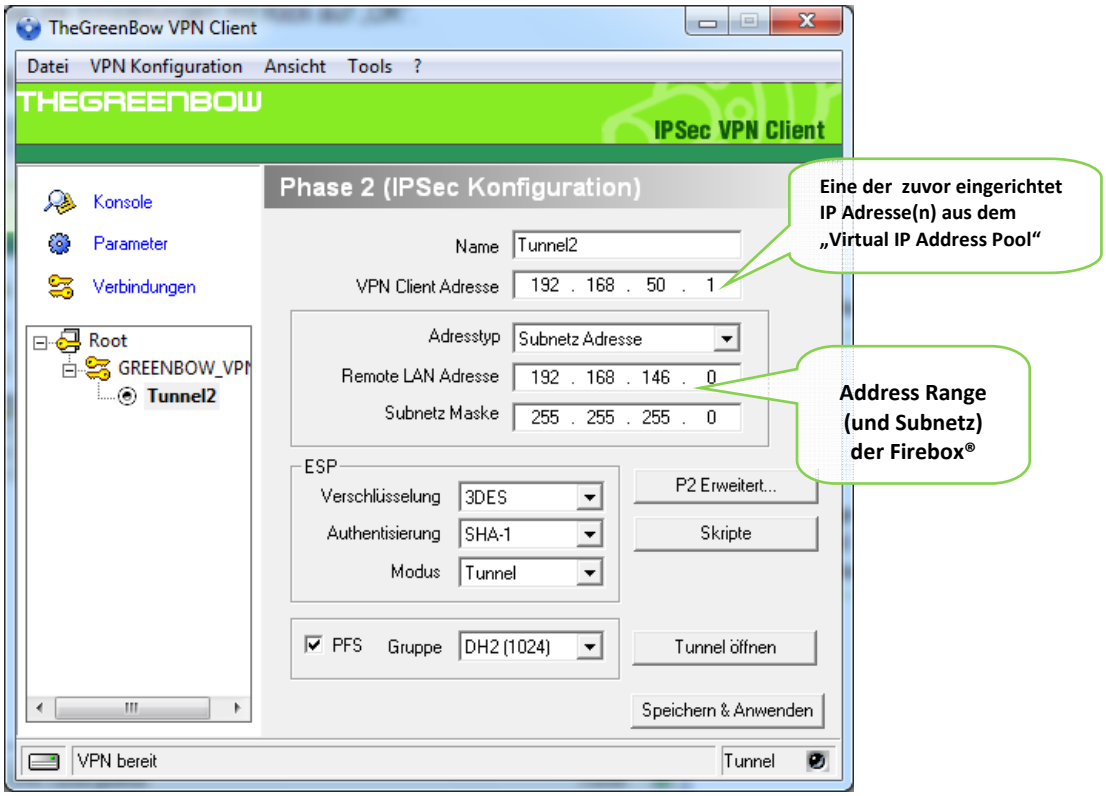
3.2 Phase 1 – Erweiterte Einstellungen

Klicken Sie „P1 Erweitert“ um in die erweiterten Konfigurationseinstellungen der Phase 1 zu gelangen.



Aktivieren Sie die Option “Aggressive Mode”. Aktivieren Sie ebenfalls die Option „X-Auth Popup“ damit sich der aus unserem Beispiel angelegter Benutzer „VPNUser“ anmelden kann. Setzen Sie nun die lokale und entfernte ID für denVPN Client. Wählen Sie hier als ID Typ „eMail“ (Lokale ID) und tragen Sie unter ID Wert „GREENBOW“ (die angelegte VPN Gruppe) ein. Die entfernte ID bleibt leer. Bestätigen Sie die Einstellungen mit Klick auf „OK“.

3.3 VPN Client Phase 2 (IPSec) Konfiguration



Phase 2 Konfiguration

Klicken Sie “Speichern & Anwenden” um alle Konfigurationseinstellungen zu sichern.

3.4 IPSec VPN Tunnel öffnen

1. Klicken Sie auf "**Tunnel öffnen**", das VPN Icon im Systemtray färbt sich grün, sobald der Tunnel etabliert ist.

2. Über den Menüpunkt "**Verbindungen**" können Sie den Status der konfigurierten VPN Tunnel einsehen.

3. Über den Menüpunkt "**Konsole**" haben Sie Einsicht in die Logdatei. Hier wird alle Kommunikation über das IPSec Protokoll zwischen Client und Gateway angezeigt.

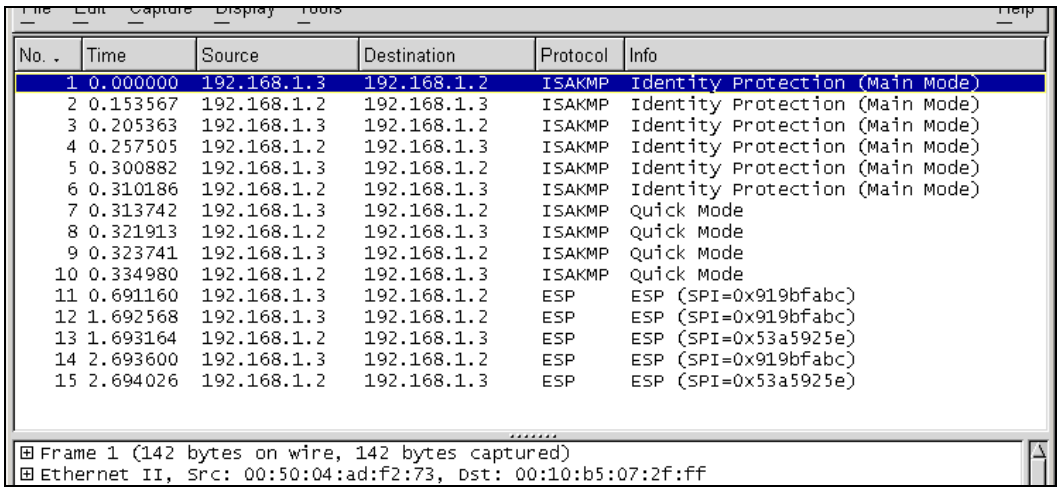
```
20100526 161354 Default (SA GREENBOW-P1) RECV Transaction Mode  [HASH] [ATTRIBUTE]
20100526 161404 Default (SA GREENBOW-P1) SEND Transaction Mode  [HASH] [ATTRIBUTE]
20100526 161406 Default (SA GREENBOW-P1) RECV Transaction Mode  [HASH] [ATTRIBUTE]
20100526 161406 Default (SA GREENBOW-P1) SEND Transaction Mode  [HASH] [ATTRIBUTE]
20100526 161406 Default (SA GREENBOW-Tunnel1-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20100526 161406 Default (SA GREENBOW-Tunnel1-P2) RECV phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID] [NOTIFY]
20100526 161406 Default (SA GREENBOW-Tunnel1-P2) SEND phase 2 Quick Mode  [HASH]
20100526 161524 Default (SA GREENBOW-P1) SEND Informational  [HASH] [NOTIFY] type DPD_R_U_THERE
20100526 161525 Default (SA GREENBOW-P1) RECV Informational  [HASH] [NOTIFY] type DPD_R_U_THERE_ACK
```

4 Fehlerbehebung

IPSec VPN Tunnel reagieren äußerst sensibel. Ein falscher oder fehlender Parameter kann einen erfolgreichen Tunnelaufbau verhindern. Hier einige Werkzeuge und Informationen zur Fehlerbehebung.

4.1 Eine gute Netzwerkanalyse: Wireshark

Wireshark ist eine freie Software (Freeware), mit der Sie Netzwerkpakete und Netzwerkverkehr analysieren können. Sie zeigt und protokolliert alle IP oder TCP Pakete an, die von der Netzwerkkarte empfangen werden. Die Software erhalten sie auf der Webseite http://www.wireshark.org. Sie kann zur Analyse der Protokollkommunikation zwischen 2 Geräten verwendet werden. Hilfe zur Installation und Verwendung vom Wireshark finden Sie hier: http://www.wireshark.org/docs/



5 VPN IPSec Troubleshooting

5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA])

```
114920 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
114920 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [NOTIFY]
114920 Default exchange_run: exchange_validate failed
114920 Default dropped message from 195.100.205.114 port 500 due to notification
type PAYLOAD_MALFORMED
114920 Default SEND Informational  [NOTIFY] with PAYLOAD_MALFORMED error
```

Der Fehler « PAYLOAD MALFORMED » indiziert, dass die Einstellungen der Phase 1 im Client und Gateway nicht übereinstimmen. Prüfen Sie bitte die Verschlüsselungsalgorithmen auf beiden Seiten.

5.2 « INVALID COOKIE » error

```
115933 Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
115933 Default dropped message from 195.100.205.114 port 500 due to notification
type INVALID_COOKIE
115933 Default SEND Informational  [NOTIFY] with INVALID_COOKIE error
```

Der Fehler « INVALID COOKIE » bedeutet, dass einer der Endpunkte (Client oder Gateway) eine Security Association (SA) verwendet, die nicht mehr aktiv oder gültig ist. Setzen Sie in diesem Fall bitte die VPN Verbindung auf beiden Seiten zurück.

5.3 « no keystate » error

```
115315 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115319 Default ipsec_get_keystate: no keystate in ISAKMP SA 00B57C50
```

Prüfen Sie bitte, dass der PreShared Key korrekt ist und mit dem im VPN Gateway hinterlegtem Schlüssel übereinstimmt. Prüfen Sie auch die erweiterten Einstellungen in der Phase 1. Achten Sie hier bitte genau auf die korrekte Konfiguration der lokalen und entfernten ID's. In den Logdateien des VPN Gateways finden Sie in der Regel detailliertere Informationen, welcher Wert hier konkret als fehlerhaft angemahnt wird.

5.4 « received remote ID other than expected » error

```
120348 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default ike_phase_1_recv_ID: received remote ID other than expected
support@thegreenbow.fr
```

Die Remote ID (Typ und/oder Wert) in den erweiterten Einstellungen der Phase 1 stimmen nicht mit den Einstellungen des VPN Gateway überein.

5.5 « NO PROPOSAL CHOSEN » error

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
115915   Default   (SA   CNXVPN1-CNXVPN1-P2)   SEND   phase   2   Quick   Mode
[SA][KEY][ID][HASH][NONCE]
115915 Default RECV Informational  [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error
115915 Default RECV Informational  [HASH][DEL]
115915 Default CNXVPN1-P1 deleted
```

In diesem Fall stimmen die Verschlüsselungseinstellungen in der Phase 2 nicht mit denen des VPN Gateway überein. Prüfen Sie die Verschlüsselungseinstellungen in der Phase 1, wenn sich der Fehler so darstellt:

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115911 Default RECV Informational  [NOTIFY] with NO_PROPOSAL_CHOSEN error
```

5.6 « INVALID ID INFORMATION » error

```
122623 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
122626   Default   (SA   CNXVPN1-CNXVPN1-P2)   SEND   phase   2   Quick   Mode
[SA][KEY][ID][HASH][NONCE]
122626 Default RECV Informational  [HASH][NOTIFY] with INVALID_ID_INFORMATION error
122626 Default RECV Informational  [HASH][DEL]
122626 Default CNXVPN1-P1 deleted
```

Prüfen Sie bei diesem Fehler die Netzwerkeinstellungen der Phase 2. Diese müssen explizit mit der Konfiguration des VPN Gateways übereinstimmen. Beachten Sie hier besonders die Werte der VPN Client IP und der Netzwerkadresse. Prüfen Sie auch den Typ (Subnetz oder Einzeladresse).

5.7 Ich klicke auf “Tunnel öffnen”, aber nichts passiert.

Prüfen Sie die Logdateien auf beiden Seiten (Client und Gateway). Die IKE Anfragen könnten hier durch eine Firewall blockiert werden. IPSec VPNs verwenden das UDP Ports 500 und 4500, sowie das Protokoll ESP (Protokoll 50).

5.8 Der VPN Tunnel ist aktiv aber ich kann nicht pingen!

Ist der VPN Tunnel etabliert, aber das entfernte Netzwerk lässt sich nicht anpingen, prüfen Sie bitte folgende Optionen und Einstellungen:

- Phase 2 Einstellungen: VPN Client Adresse and Remote LAN Adresse. Üblicherweise darf die VPN Client IP Adresse nicht innerhalb der Range des Subnet hinter dem VPN Gateway liegen.
- Ist der Tunnel geöffnet, werden Pakete mittels des ESP Protokoll übertragen. Dies könnte durch eine Firewall blockiert werden. Prüfen Sie jedes Gerät zwischen VPN Client und VPN Gateway, ob dies der Fall ist.
- Prüfen Sie die Logdateien des VPN Gateway. Auch hier können Firewalleinstellungen die Kommunikation blockieren.

- Prüfen Sie bitte, ob Ihr Zugangsprovider ESP Paketübertragungen unterstützt.

- Prüfen Sie die “Standardgateway” Einstellungen im entfernten Netzwerk. Ein Zielhost im entfernten Netzwerk könnte wohlmöglich die Pings empfangen, jedoch an ein falsches Gateway antworten.
- Möglicherweise können Sie den Zielhost nicht über seinen Namen erreichen. Probieren Sie stattdessen die interne IP Adresse.

- Zur weiteren Analyse empfehlen wir Wireshark (http://www.wireshark.org) um zu prüfen, ob die Pings im entfernten Netzwerk ankommen.

6 Kontakt

News und Updates auf der TheGreenBow Website: http://www.thegreenbow.de/

Technischer Suppoert per E-Mail: support@thegreenbow.de

Vertrieb: sales@thegreenbow.de

Secure, Strong, Simple.

TheGreenBow Security Software