



## TheGreenBow IPSec VPN Client

### Konfigurationsbeispiel

## Watchguard Firebox X Edge e-Series

WebSite: <http://www.thegreenbow.de>

Kontakt: [support@thegreenbow.de](mailto:support@thegreenbow.de)

Configuration Guide written by:

Autor: Anastassios Stafilidis

Firma: ASCS GmbH, Ihr IT-Partner, [www.ascs.de](http://www.ascs.de)

## Inhalt

1	Einleitung .....	3
1.1	Ziel der Anleitung .....	3
1.2	VPN Netzwerktopologie .....	3
1.3	WatchGuard Firebox® X Edge e-Series Einschränkungen.....	3
1.4	WatchGuard Firebox® X Edge e-Series Security Appliance VPN Gateway .....	3
1.5	WatchGuard Firebox® X Edge e-Series Security Appliance Produktinformationen.....	3
2	WatchGuard Firebox® X Edge e-Series VPN Konfiguration.....	4
2.1	Vorbereitungen .....	4
2.2	Einstellungen in der WatchGuard Firebox® X Edge e-Series.....	4
3	TheGreenBow IPSec VPN Client Konfiguration.....	9
3.1	VPN Client Phase 1 (IKE) Konfiguration .....	9
3.2	Phase 1 – Erweiterte Einstellungen .....	10
3.3	VPN Client Phase 2 (IPSec) Konfiguration .....	11
3.4	IPSec VPN Tunnel öffnen .....	11
4	Fehlerbehebung.....	12
4.1	Eine gute Netzwerkanalyse: Wireshark .....	12
5	VPN IPSec Troubleshooting .....	13
5.1	« PAYLOAD MALFORMED » error (wrong Phase 1 [SA]).....	13
5.2	« INVALID COOKIE » error.....	13
5.3	« no keystate » error .....	13
5.4	« received remote ID other than expected » error.....	13
5.5	« NO PROPOSAL CHOSEN » error .....	14
5.6	« INVALID ID INFORMATION » error .....	14
5.7	Ich klicke auf “Tunnel öffnen”, aber nichts passiert .....	14
5.8	Der VPN Tunnel ist aktiv aber ich kann nicht pingen! .....	14
6	Kontakt.....	16

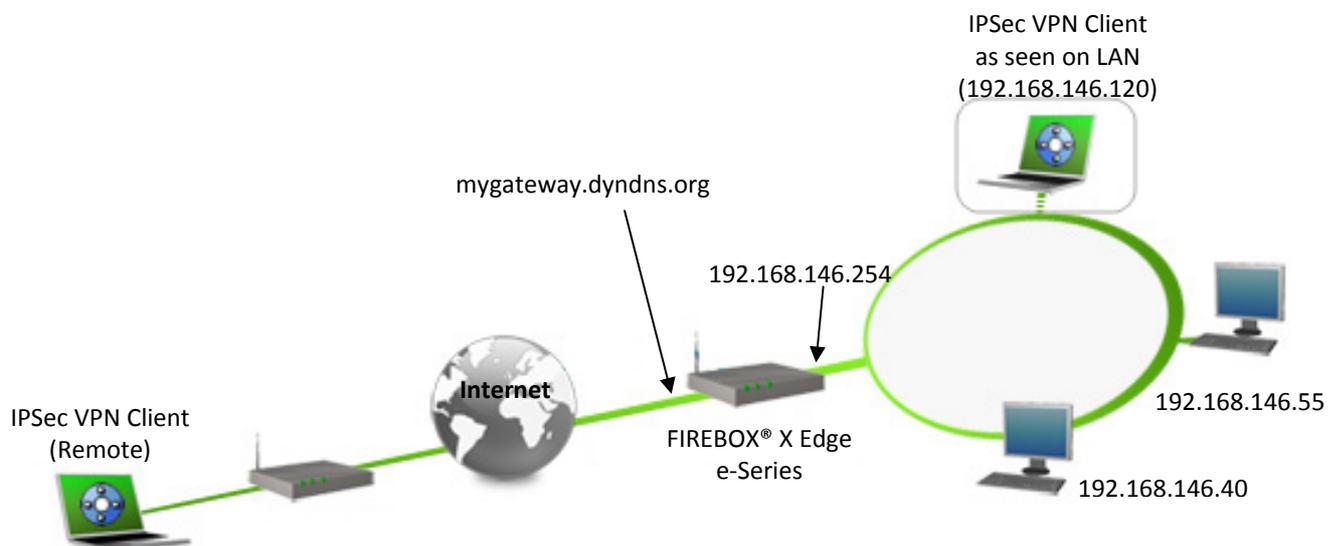
## 1 Einleitung

### 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	<a href="http://www.watchguard.com/international/de/products/index.asp?t=main">http://www.watchguard.com/international/de/products/index.asp?t=main</a>
Watchguard Handbuch	<a href="http://www.watchguard.com/help/documentation/edge.asp">http://www.watchguard.com/help/documentation/edge.asp</a>
Watchguard FAQ/Hilfe	<a href="http://www.watchguard.com/help/documentation/xtm.asp">http://www.watchguard.com/help/documentation/xtm.asp</a>

## 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.

The screenshot displays the WatchGuard web interface for configuring Mobile VPN with IPSec. The left sidebar shows the navigation menu with 'VPN' > 'Mobile VPN with IPSec' selected. The main content area is titled 'Mobile VPN with IPSec Settings' and includes a 'Help' link. The configuration is organized into tabs: 'General', 'IPSec Tunnel', 'Resources', and 'Advanced'. The 'General' tab is active and contains the following settings:

- Group name:** GREENBOW
- General Settings:**
  - Authentication Server:** Firebox-DB
  - Passphrase:** [Redacted]
  - Confirm:** [Redacted]
- Firebox IP Addresses:**
  - External IP address:** mygateway.dyndns.org
  - Backup IP address:** [Empty]
- Timeouts:**
  - Session Timeout:** 480 minutes
  - Idle Timeout:** 30 minutes

At the bottom right, there are 'Save' and 'Cancel' buttons.

Doc.Ref	tgvpn-cg-watchgard-firebox-edge-de
Doc.version	1.0 – mei 2010
VPN version	4.65

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).

The screenshot shows the 'Mobile VPN with IPSec Settings' configuration page in the WatchGuard web interface. The 'General' tab is selected. The 'IPSec Tunnel' section has the radio button 'Use the passphrase of the end user profile as the pre-shared key' selected. Below it, the 'CA IP address' field is empty and the 'Timeout' is set to 25 seconds. The 'Phase 1 Settings' section shows 'Authentication' set to SHA-1 and 'Encryption' set to 3DES. The 'Phase 2 Settings' section has 'PFS' checked and 'Diffie-Hellman Group 2' selected. 'Save' and 'Cancel' buttons are at the bottom.

Phase 1 erweiterte Einstellungen

The screenshot shows the 'Phase 1 Advanced Settings' sub-page. A '<-- Return to General Settings' button is at the top left. The 'SA Life' is set to 8 hours. The 'Key Group' is 'Diffie-Hellman Group 2'. Under 'NAT Traversal', the 'Keep-alive Interval' is 20 seconds, 'Message Interval' is 10 seconds, and 'Max failures' is 3. Under 'Dead Peer Detection', it is checked with a 'Traffic idle timeout' of 90 seconds and 'Max retries' of 5. 'Save' and 'Cancel' buttons are at the bottom.

## Phase 2 erweiterte Einstellungen

The screenshot shows the 'Mobile VPN with IPsec Settings' configuration page in the WatchGuard web interface. The 'Phase 2 Advanced Settings' tab is active. The 'Group name' is set to 'GREENBOW'. Under 'Phase 2 Proposal', the 'Type' is 'ESP (Encapsulating Security Payload)', 'Authentication' is 'SHA-1', and 'Encryption' is '3DES'. The 'Force Key Expiration' checkbox is checked, with a value of '8' hours and '128000' kilobytes.

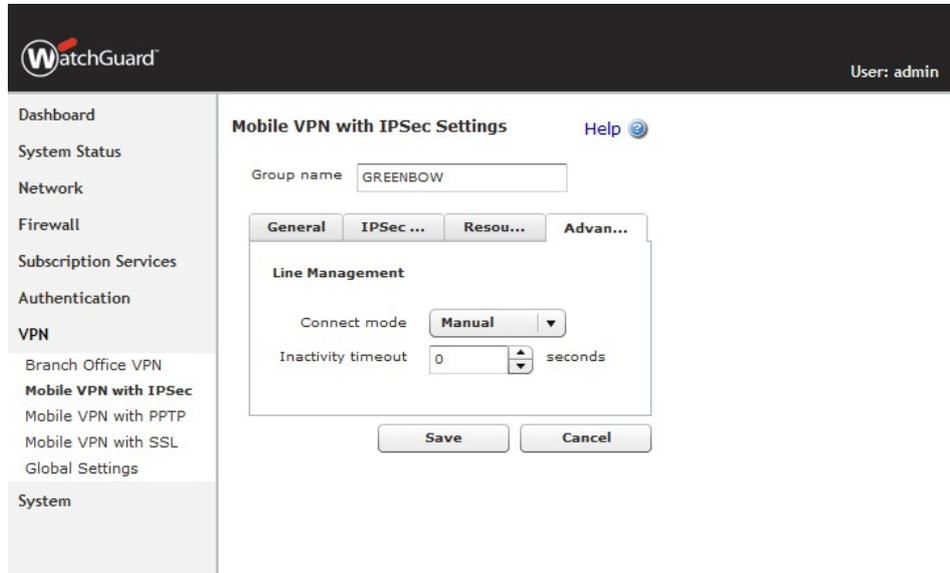
Im Reiter „Resources“ unter „Allowed Resources“ das Subnetz / die Subnetze eingeben an dem/an denen die externe Benutzer zugreifen dürfen (in unserem Beispiel das komplette 192.168.146.0/24 Subnetz). Wenn „Allow All Traffic Through Tunnel“ aktiviert wird, erfolgt der Zugriff ins Internet durch den VPN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

The screenshot shows the 'Resources' tab of the 'Mobile VPN with IPsec Settings' configuration page. The 'Allow All Traffic Through Tunnel' checkbox is unchecked. Under 'Allowed Resources', the network '192.168.146.0/24' is listed. Below this, there are fields to 'Choose Type' (set to 'Network IP'), 'Network IP' (with a dropdown for '24'), and an 'Add' button. Under 'Virtual IP Address Pool', the range '192.168.50.1-192.168.50.10' is listed. Below this, there are fields to 'Choose Type' (set to 'Host Range'), 'From', 'To', and an 'Add' button.

Doc.Ref	tgbvpn-cg-watchgard-firebox-edge-de
Doc.version	1.0 – mei 2010
VPN version	4.65

Unter „Virtual IP Address Pool“ muss eine oder mehrere IP Adressen (nicht vom eigenen Subnet) definiert werden (in unserem Beispiel 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.

Doc.Ref	tgbvpn-cg-watchgard-firebox-edge-de
Doc.version	1.0 – mei 2010
VPN version	4.65

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.

**Setup Firebox User**

**User Information**

Name: VPNUser

Description:

Passphrase: \*\*\*\*\*

Confirm: \*\*\*\*\*

Session Timeout: 8 hours

Idle Timeout: 30 minutes

**Firebox Authentication Groups**

**Member**

- GREENBOW

**Available**

<< >>

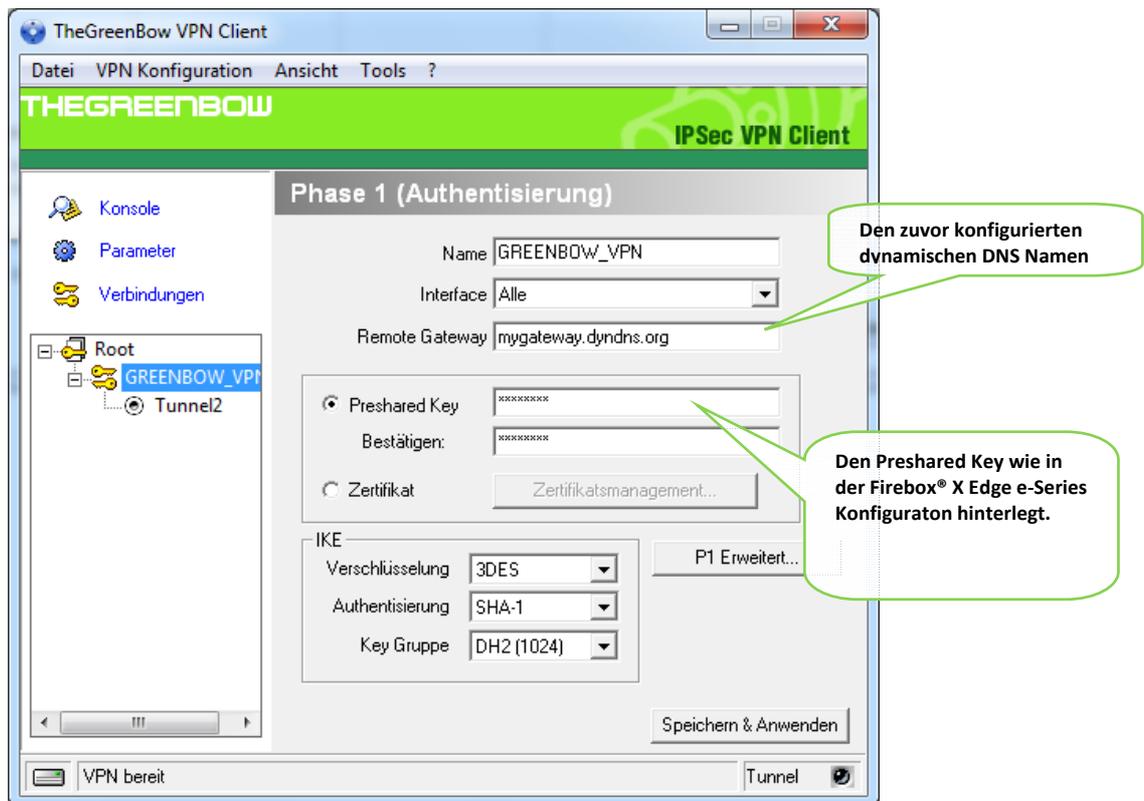
OK Cancel

### 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](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.

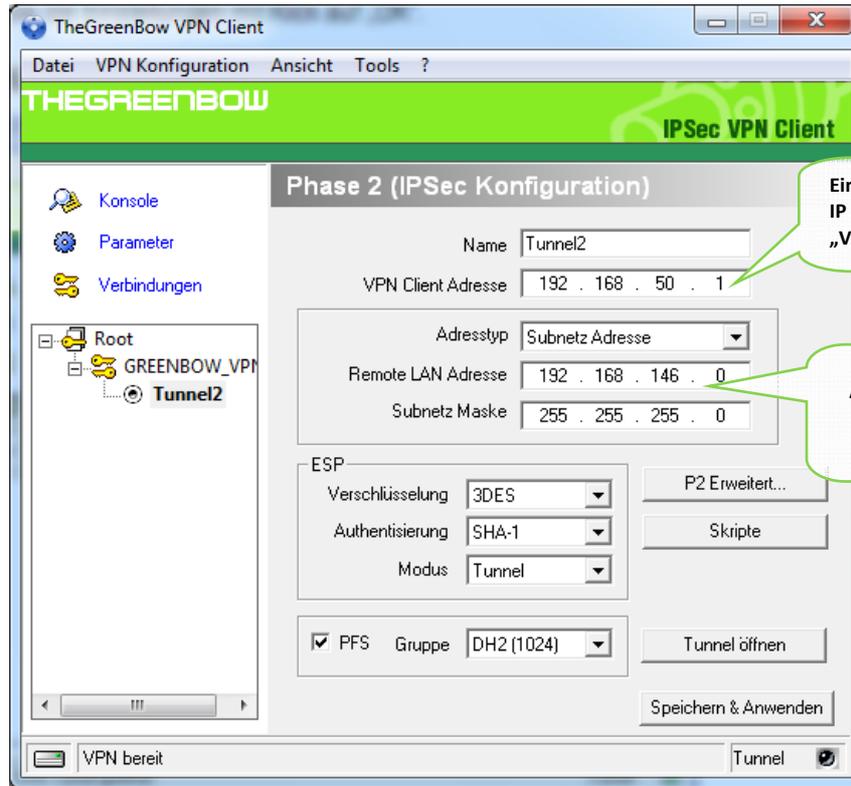
Geben Sie einen eindeutigen Namen für die VPN Verbindung (in unserem Beispiel „GREENBOW\_VPN“). „Interface“ kann auf „Alle“ bleiben. Im „Remote Gateway“ den dynamischen DNS Namen (in unserem Beispiel „mygateway.dyndns.org“) oder die externe IP Adresse der WatchGuard Firebox® eingeben. Setzen Sie nun 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



Eine der zuvor eingerichtet IP Adresse(n) aus dem „Virtual IP Address Pool“

Address Range (und Subnetz) der Firebox®

#### 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/>

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
2	0.153567	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
3	0.205363	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
4	0.257505	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
5	0.300882	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
6	0.310186	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
7	0.313742	192.168.1.3	192.168.1.2	ISAKMP	Quick Mode
8	0.321913	192.168.1.2	192.168.1.3	ISAKMP	Quick Mode
9	0.323741	192.168.1.3	192.168.1.2	ISAKMP	Quick Mode
10	0.334980	192.168.1.2	192.168.1.3	ISAKMP	Quick Mode
11	0.691160	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x919bfabc)
12	1.692568	192.168.1.2	192.168.1.3	ESP	ESP (SPI=0x919bfabc)
13	1.693164	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x53a5925e)
14	2.693600	192.168.1.2	192.168.1.3	ESP	ESP (SPI=0x919bfabc)
15	2.694026	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x53a5925e)

Frame 1 (142 bytes on wire, 142 bytes captured)  
 Ethernet II, Src: 00:50:04:ad:f2:73, Dst: 00:10:b5:07:2f:ff

## 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 Firewallinstellungen die Kommunikation blockieren.

Doc.Ref	tgbvpn-cg-watchgard-firebox-edge-de
Doc.version	1.0 – mei 2010
VPN version	4.65

- 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.

<b>THEGREENBOW</b>	Doc.Ref	tgbvpn-cg-watchgard-firebox-edge-de
	Doc.version	1.0 – mei 2010
	VPN version	4.65

## 6 Kontakt

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

Technischer Support per E-Mail: [support@thegreenbow.de](mailto:support@thegreenbow.de)

Vertrieb: [sales@thegreenbow.de](mailto:sales@thegreenbow.de)

**Secure, Strong, Simple.**

TheGreenBow Security Software