## **D-Link VPN-IPSEC Test Aufbau**



Konfigurationsbeispiel für einen 804-HV:

Konfiguration der IPSEC Einstellungen für das Gateway:

	Advanced	Tools	Status	Hel
VPN Settings				
	ltem		Setting	
VPN		🗹 Enable 🛛 🗲	2	
NetBIOS broad	cast	🗹 Enable		
Max. number of	tunnels	6 🗕 🗲	3	
ID	Tunnel Name		Method	
1			KE 💌 More	
2			IKE  More	
3			IKE  More	
4			IKE  More	
			The second secon	

- -
- -
- Wählen Sie unter "Home" VPN aus (Punkt 1) Aktivieren Sie das VPN Feature (Punkt 2) Wählen Sie die Anzahl der gleichzeitigen VPN Tunnel z. B "10" (Punkt 3) Bestätigen Sie die Änderungen mit dem Apply Button \_
- \_

Konfiguration eines Dialup-Tunnels:

Home	Advanced	Tools	Status	Hel
VPN Settings	3			
	ltem	-	Setting	
VPN		🗹 Enable		
NetBIOS broa	dcast	🗹 Enable		
Max. number o	oftunnels	6		
ID	Tunnel Name		Method	
1			IKE 💽 More	
2			IKE 💌 More	
3			IKE  More	
4			IKE  More	1
-			IKE More	1

Klicken Sie auf "Dynamic VPN Settings"

\_

works for People			D Broadb	<b>I-80</b> 4 and VI	HV PN Rot	uter	
1	Home	Advanced	Tools	St	atus		lelp
	VPN Settings -	Dynamic VPN Tun	nel				
		tem		Se	tting		
	Tunnel Name		dialup	-	141	1	
L	Dynamic VPN		🗹 Enable	-		2	
	Local Subnet		192.168.1.0	-	i i i i i i i i i i i i i i i i i i i	3	
	Local Netmask		255.255.255.0	-		4	
	Preshare Key		****		<b>—</b>	5	
	IKE Proposal ind	ex	Select IKE Propos	al			
	IPSec Proposal i	ndex	Select IPSec Prop	osal			
				<b>G</b> Back	Apply	3 Cancel	C) Help

- Geben Sie dem Tunnel einen beliebigen Namen (Punkt 1)
- Der Name wird verwendet um mehrere Tunnel zu unterscheiden
- Aktiveren Sie die Dialup-Tunnel (Punkt 2)
- Tragen Sie Ihr lokales Subnetz ein. Sofern wir der Zeichnung folgen wollen sollte hier "192.168.2.0" eingetragen werden. Diese Information ist für das Gateway wichtig, da es später zwischen dem lokalen und Remote-Netzwerk vermitteln muss.



Bei D-Link IPSec Gateways wird zwischen diesen beiden Netzen immer unter Verwendung von NAT vermittelt. Sofern Sie also später einen Clienten verwenden, der die Zuweisung von virtuellen Ips ermöglicht, sollten Sie diese Eigenschaft unbedingt bedenken.

- Als nächsten tragen Sie eine Class C (255.255.255.0) Netzmaske ein (Punkt 4)
- Definieren Sie einen gemeinsamen Schlüssel, der später bei der Konfiguration der Clients bekannt sein muss. (Punkt 5)
- Bestätigen Sie diese Eingaben mit dem Apply Button (Schritt 6)

ks for People		DI Broadba	-804HV and VPN Rout	er
Home	Advanced	Tools	Status	Help
VPN Settings	- Dynamic VPN Tun	nel	Patting	
Tunnel Name	nem	dialun	Setung	
Dynamic VPN		Enable		
Local Subnet		192.168.1.0		
Local Netmask	ł	255.255.255.0		
Preshare Key		*****		
IKE Proposal in	ndex	Select IKE Proposa		
IPSec Proposa	l index	Select IPSec Propo	sal	
				0 0
			Back Apply (	ancel Helr
			back Apply C	ancer neu

## IKE Proposal Definition:

Hom	e Advanced	Tools	Status	Hel
VPN Settin	igs - Dynamic VPN Tun	nel - Set IKE Pro	iposal	
IVE Drange	ltem .		Setting	
IKE Propus	armuex	- Empty -		
			move	
ID Propos	Name DH Goup En	cryptialgorithm Au	uth a gorithm Life im	ne Life Time I
1 1	Group 2 💌	DES 💌	MD5 💽 28800	Sec.
2	Group 1 💌	3DES 💌	SHA1 💌 0	Sec.
3	Group 1 💌	3DES 💌	SHA1 💌 0	Sec.
4	Group 1 💌	3DES 💌	SHA1 💌 0	Sec.
5	Group 1 💌	3DES 💌	SHA1 💌 0	Sec.
6	Group 1 💌	3DES 💌	SHA1 💌 0	Sec.
7	Group 1 💌	3DES 💌	SHA1 💌 0	Sec.
8	Group 1 💌	3DES 💌	SHA1 💌 0	Sec.
9	Group 1 💌	3DES 💌	SHA1 💌 0	Sec.
10	Group 1 💌	3DES -	SHA1 V	Sec.

## Erklärungen:

Auf dieser Seite sehen Sie 10 Zeilen mit Konfigurationsparametern. Jede einzelne Zeile ermöglicht eine Verbindung, wenn der Client die gleichen Parameter verwendet. Mehrere Zeilen müssen Sie also nur dann verwenden, wenn Sie den Clients zum Beispiel unterschiedliche Verschlüsselungen anbieten möchten. Tragen Sie bitte auf Ihrer Seite die oben dargestellten Werte ein. Ich empfehle aber die Verwendung von 3DES oder AES sofern Ihr Client diese Verfahren unterstützt. Die oben gezeigte Konfiguration ist so gewählt, dass diese in Kombination mit fast jedem Client funktioniert, aber kein Sicherheitsoptimum darstellt. Eine sichere Empfehlung wäre Group 5, 3DES oder AES zur Verschlüsselung und SHA1 als Authentifizierungs-Algorithmus.

Nachdem Sie Einstellungen angepasst haben, wählen Sie unten die Proposal ID 1 aus der Drop-Down Liste aus und klicken auf "Add to".

Jetzt sollte eine "1" im IKE Proposal Index erscheinen.

Bestätigen Sie alle Eingaben mit "apply".

## IPSEC Proposal Definition:

ks for People			DI Broadba	-804HV and VPN Route	er
	Home	Advanced	Tools	Status	Help
	VPN Settings -	Dynamic VPN Tur	inel		
		ltem		Setting	
	Tunnel Name		dialup		
	Dynamic VPN		🗹 Enable		
	Local Subnet		192.168.1.0		
	Local Netmask		255.255.255.0		
	Preshare Key		*****		
	IKE Proposal ind	dex	Select IKE Proposa	al	
	IPSec Proposal	index	Select IPSec Propo	 psal	•:
			-		-
				🥥 💟 🤇	2 😈
				Back Apply Ca	ncel Help

Klicken Sie auf den Button "Select IPSec Proposal"

Suliding Networks for People			DI Broadba	-804HV and VPN Route	r
	Home	Advanced	Tools	Status	Help
	VPN Settings -	Dynamic VPN Tunne	- Set IPSEC F	<sup>o</sup> roposal Setting	
the on	IPSec Proposal	index	Empty - 🔺 <	Hier soll eine "2"	te anschließend erscheinen
Wizard	Tragen Si	e diese Werte ein	Ren	nove	
	ID Proposal Name	DH youp Enca	Encry	Auth Life	Life <b>ti</b> me Unit
WAN	1 2	Group 2 💌 ESP	DES -	MD5 3600	Sec. 💌
	2	None 💌 ESP	JOES -	None 💌 0	Sec. 💌
LAN	3	None 💌 ESP	- 3DES -	None 💌 0	Sec. 💌
DUICE	4	None 💌 ESP	- 3DES -	None 💌 0	Sec. 💌
DHCP	5	None 💌 ESP	▼ 3DES ▼	None 💌 0	Sec. 💌
VPN	6	None 💌 ESP	▼ 3DES ▼	None 💌 0	Sec. 💌
	7	None 💌 ESP	- 3DES -	None 💌 0	Sec. 💌
	8	None 💌 ESP	- 3DES -	None 💌 0	Sec. 💌
	9	None 💌 ESP	- 3DES -	None 💌 0	Sec. 💌
	10	None 💌 ESP	▼ 3DES ▼	None 🔽 0	Sec. 💌
		Proposal ID 1	▼ Add	to Proposal index	

Hier wurde , wie schon für die IKE Proposals beschrieben, eine möglichst kompatible Konfiguration verwendet. Benutzen Sie auch hier 3DES oder AES, sofern die Clients diese Algorithmen unterstützen.

Zunächst übernehmen Sie bitte die Einstellungen aus der oben gezeigten Darstellung. Anschließend wählen Sie die Proposal ID "1" aus und drücken auf den Button "Add to". In dem IPSec Proposal Index sollte nun eine "2" erscheinen. Bestätigen Sie alle Einstellungen mit dem Apply Button.

Die IPSec Gateway Konfiguration ist damit abgeschlossen.

Außerdem sollten Sie überprüfen ob Ihre PPPOE Einstellungen richtig eingegeben wurden, und ob das Gateway eine Verbindung zum Internet aufgebaut hat. In diesem Zusammenhang sollten Sie sich die IP notieren oder aber Dyndns konfigurieren. Beispiel-Konfiguration für einen IPSEC Client (Forticlient)

- Wichtig: Verwenden Sie auf Ihrem OS immer nur einen IPSEC Client
- Öffnen Sie nach der Installation den FortiClient und klicken Sie auf "VPN"
- Anschließen erstellen Sie eine neue VPN Verbindung indem Sie auf den Button "Add" klicken

FortiClient					
FER	RTINET			FortiC	ient
General	Connections Monitor	My Certificates (	CA Certificates CRL	<u>\</u>	0
<b>*</b>	Name	Gateway	Authentication	Status	
Logs	Test Connec	tAdd	Edit Delete	e Rename	

- Geben Sie der Verbindung einen beliebigen Namen. Dieser dient nur der Identifikation.
- Als Remote Gateway IP geben Sie bitte die WAN oder Internet IP des 804HV ein, oder verwenden Sie bei anderen Clients die DynDNS Adresse.
- Das Remote Netzwerk muss auch dem Client bekannt sein, da auch dieser zwischen Remote und lokalem Netzwerk vermitteln muss. In unserem Beispiel habe wir ein 192.168.2.0 C-Netz verwendet. Geben Sie hier unbedingt ein Netz und keine einzelne IP ein.
- Als "Authentication Method" wählen Sie Preshared Key aus und geben anschließend den Key, den Sie bei der 804Hv Konfiguration definiert haben ein.
- Als nächstes klicken Sie auf "Advanced" um die IKE und IPSEC Proposals zu konfigurieren.

New Connection		×
Connection Name	804 HV Dial UP	
Remote Gateway	217 . 167 . 80 . 98	
Remote Network	192 . 168 . 2 . 0	
1	255 . 255 . 255 . 0	
Authentication Method	Preshared Key	
Preshared Key	*****	
Advanced	OK Cancel	

IKE	Main mode; DH G DES-MD5;	Group: 5	
	Key life: 28800s;	Nat-T: ON, Frequency 5	is; DPD: ON;
PSec	DES-MD5; DH Group: 5 Keylife: Seconds :	: 1800s ; Replay Detectio	on: ON; PFS: ON;
	Legacy	Default	Config
dvanc	ed		
dvanc Acc	ed uire virtual IP addre		Config
dvanc Acc ext	ed uire virtual IP addre ended Authenticatio		Config Config
dvanc Acc ext	ed juire virtual IP addre ended Authenticatio Network	<u> </u>	Config Config
dvanc Acc ext emote	ed juire virtual IP addre ended Authenticatio Network	issi m Mask	Config Config Add
dvanc Acc ext emote IP 192.1	ed uire virtual IP addre ended Authenticatio Network 58.2.0	m Mask 255.255.255.0	Config Config Config Add Edit

- Klicken Sie auf Config um die IPSec und IKE Einstellungen zu verändern.

Encryption       Authentication       Add         DES       MD5       Delete       DH Group         Delete all       Delete all       Key Life       28800         Local ID       Local ID       Local ID         Proposals       DH Group       O 1 ○ 2 ○         Encryption       Authentication       Add         DES       MD5       Delete all         Encryption       Authentication       Add         DES       MD5       Delete all         Delete all       Seconds       KB         Seconds       3600	roposals	14		Mode
DES MD5 Delete all Delete all Delete all Control Control C	Encryption	Authentication	Add	Main Aggressive
ec Proposals Encryption Authentication Add DES MD5 Delete all Delete all Delete all Delete all Delete all Delete all C 1 C 2 C Key Life Delete all C 1 C 2 C Key Life Seconds KB Seconds 3600	DES	MD5	Delete	
ec Proposals Encryption Authentication Add DES MD5 Delete all Delete all Seconds 3600			Delete all	
ec Proposals Encryption Authentication Add DES MD5 Delete Delete all Delete all Seconds 3600	1	T I		Key Life 28800
ec Proposals Encryption Authentication Add DES MD5 Delete all Delete all Seconds 3600				Local ID
ec Proposals Encryption Authentication Add DES MD5 Delete all Delete all Seconds 3600			-//	T
Construction     Add       Encryption     Authentication       DES     MD5       Delete       Delete all       Seconds       Seconds       3600				-
Encryption       Authentication       Add       O 1       O 2       O         DES       MD5       Delete       Key Life       Image: Construction       <	roposals —			- DH Group
DES MD5 Delete Delete all Seconds 3600	Encryption	Authentication	Add	01 02 05
Delete all Seconds ⊂ KB	DES	MD5	Delete	- Key Life
Seconds 3600		<b>A</b>	Delete all	Seconds
		Т	Delete di	Seconds 3600
KD 1 CTOD		ň,		KR I From
KBytes 5120		2	-111 op	KBytes J5120
anceo a duons	Seplay Detect	tion PES	Nat Traversal k	Ceenalive Frequency
Replay Detection V PES Nat Traversal Keepalive Frequency 5		Alive V Dead Peor	Detection	seeparity requeries 15
Replay Detection IP PFS IN Nat Traversal Keepalive Frequency 5	Andrah An Kasa	Alive 🔽 Deau Feel	Delection	

- Stellen Sie alle Parameter, wie oben dargestellt ein. Sofern Sie sich für 3DES oder AES entschieden haben müssen Sie diese Parameter natürlich ändern.
- NAT-Traversal sollten Sie ausschalten, das es zu Konflikten kommen kann wenn dieses Feature verwendet wird. Grundsätzlich setzt man NAT-T nur ein, wenn das Ziel Gateway hinter einem NAT-Gateway betrieben wird.
- Außerdem sollten Sie immer den "Main-Mode" verwenden.
- Die Dead Peer Detection ist nicht unbedingt notwendig, sorgt aber für einen erneuten Verbindungsaufbau, wenn der Tunnel zusammenbricht.
- Replay Detection: Bei einer Replayattacke werden aufgezeichnete Pakete einer vorher stattgefundenen legalen Verbindung mit dem anzugreifenden System spaeter selektiv von dem Angreifer zum System geschickt (Replay), um bestimmte Reaktionen des Systems hervorzurufen (beispielsweise um eine Authentifizierung zu erreichen). Replayattacken werden für gewöhnlich durch die Vergabe von Sequenznummern in den Paketen oder durch Timestamps verhindert.
- Anschließend schließen Sie den Dialog mit dem "OK" Button.

Advanced	Settings		×				
- Policy	Main mode; DH G DES-MD5; Key life: 28800s;	roup: 2 DPD: ON;					
IPSec	Sec DES-MD5; DH Group: 2 Keylife: Seconds : 3600s ; Replay Detection: ON; PFS: ON;						
	Legacy	Default Confi	<u>a</u>				
Advance	ed juire virtual IP addres	35	Config				
	Config						
Remote	Network	Maak	Add				
192.10	\$8.2.0	255.255.255.0	Edit				
	OK	Cancel					

- Schließen Sie auch diesen Dialog, sofern Sie keine virtuelle IP verwenden möchten.

Konfiguration einer virtuellen IP Adresse:

Advanced	Settings	×
– Policy –		_
IKE	Main mode; DH Group; 2 DES-MD5; Key life: 28800s; DPD: ON;	
IPSec	DES-MD5; DH Group: 2 Keylife: Seconds : 3600s ; Replay Detection: ON; PFS: ON;	
	Legacy Default Config	
Advanc	ed	- I
🔽 Acc	quire virtual IP address Config	
🗖 eXt	ended Authentication Config	
Remote	Network	
IP	Mask Add	
192.10	68.2.0 255.255.255.0 Edit	
	Delete	
	OK Cancel	

Setzen Sie den "Acquire IP Address" Haken und klicken Sie auf den dazugehörigen Config Button

Vi	rtual IP Acquisitio	n							x
	Options								
	O Dynamic Host	Configura	ation F	, lo	tocol	(DF	HCP) (	over IPSec	
	Manually Set								
	- Manual VIP								
	IP	10 .	10		10	•	1		
	Subnet Mask	255 .	255	•	255		0		
	DNS Server	0.	0		0		0		
	WINS Server	0.	0		0		0		
		ЭК			Ca	anc	el		

- Sofern Sie kein virtuelle IP verwenden , kann ein Client aus dem Remote Netzwerk Ihren Rechner unter der IP Adresse <u>aus Ihrem lokalen Netzwerk</u> erreichen.
- Wie schon beschrieben dürfen Sie hier auf keinen Fall eine IP aus dem Remote Netzwerk verwenden, da D-Link Geräte zwangsweise NAT verwenden um die Netzwerke zu verbinden. Diese Art der Übersetzung wird als IN oder Outbound NAT bezeichnet. Wenn Sie Sich nun meine Beispielkonfiguration ansehen werden Sie feststellen, dass ich ein Netz frei gewählt habe. Die Kommunikation ist aber wegen der NAT Übersetzung möglich. Grundsätzlich empfehle ich die Verwendung von virtuellen Ips nicht. DHCP über IPSec ist leider nur möglich wenn ein IPSec Gateway die Deaktivierung von In-/Outbound NAT zulässt.
- Schließen Sie alle Dialoge mit dem "OK" Button.

	1			
Cor	nections Monitor	My Certificates	CA Certificates CRL	
N.	ame	Gateway	Authentication Statu	s
. 80	4 HV Dial UP	217.85.171.228	Preshared Key Dowr	n
	Tost Course	ict Add	Edit Delete	Rename

Klicken Sie auf Connect um die Verbindung zu testen.

\_

IKE Negotiation	×
Sep 6 14:49:4: Initiator: sent 217.85.171.228 main mode message #1 (OK) Sep 6 14:49:4: Initiator: sent 217.85.171.228 main mode message #2 (OK) Sep 6 14:49:4: Responder: sent 217.85.171.228 main mode message #3 (DK) Sep 6 14:49:5: Initiator: parsed 217.85.171.228 main mode message #3 (DONE) Sep 6 14:49:5: Initiator: sent 217.85.171.228 quick mode message #1 (OK) Sep 6 14:49:9: Initiator: parsed 217.85.171.228 xauth mode message #0 (OK) Sep 6 14:49:9: Initiator: parsed 217.85.171.228 wauth mode message #0 (OK) Sep 6 14:49:9: Initiator: parsed 217.85.171.228 quick mode message #0 (OK) Sep 6 14:49:10: Initiator: sent 217.85.171.228 quick mode message #0 (OK) Sep 6 14:49:10: Initiator: sent 217.85.171.228 quick mode message #2 (DONE) Negotiation succeeded!	
ОК	

- Diese Status Screen sollte auch bei Ihnen erscheinen. Die beiden xauth Zeilen fehlen bei Ihnen, da es sich um ein erweitertes Feature zur User Authentifizierung handelt.
- Sofern die letzte Zeile "Negotiation succeeded" erscheint haben Sie Ihre Verbindung erfolgreich konfiguriert.

TINET			FortiC
PN			
Connections Monito	or My Certificates	CA Certificates CRL	
Name	Gateway	Authentication	Status
804 HV Dial UP	217.85.171.228	Preshared Key	Up: (3598)
Test Discor	nnect Add	EditDelet	e Rename
Test Discor	nnect Add	Edit Delet	e Rename
Test Discor	nnect Add	Edit Delet	e Rename

- Sie sehen unter "Status", dass der Client von 3600 abwärts zählt. Diese Zahl entspricht der IPSec Lifetime. Sofern diese Zeit abgelaufen ist, wird ein Schlüsselwechsel initiiert.
- Sie können jetzt einen Ping-Test durchführen. Die VPN Konfiguration ist damit abgeschlossen.