

Level1 router IPSec VPN vs. FreesWan

Level1 router is applicable to FBR-1407, FBR-1409TX, FBR-1417TX,
WBR-2401, WBR-3403TX, WBR-3404TX and WBR-3402

192.168.0.x---LevelOne VPN router---Linux with FreesWan---192.168.111.x

LevelOne Router LAN IP :192.168.0.1 WAN IP :192.168.123.104

Linux FreesWan internal IP:192.168.111.1 external IP:192.168.123.103

LevelOne router status:

The screenshot shows the LevelOne router web management interface in Microsoft Internet Explorer. The browser address bar shows <http://192.168.0.254/>. The page title is "BroadbandRouter" and the navigation menu includes Status, Wizard, Basic Setting, Forwarding Rules, Security Setting, Advanced Setting, and Toolbox. The "Status" page is active, displaying "System Status" information.

Item	WAN Status	Sidenote
IP Address	192.168.123.104	Static IP
Subnet Mask	255.255.255.0	
Gateway	192.168.122.103	
Domain Name Server	192.168.123.103, 168.95.1.1	

Item	Peripheral Status	Sidenote
Printer(USB)	Not ready	

Statistics of WAN	Inbound	Outbound
Octets	0	8220
Unicast Packets	0	0
Non-unicast Packets	0	0

Current Time: Tuesday, June 01, 2004 12:04:56 AM
Device Time: Tuesday, June 01, 2004 12:04:57 AM

Buttons: View Log..., Clients List..., Help, Refresh

1. enabled VPN and set Max.number of tunnel.
2. enter Tunnel name and press “More” button.

WBR3404TX Broadband Router Web Management - Microsoft Internet Explorer

Address: http://192.168.0.254/

level one BroadbandRouter

Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox Logout

Security Settings

- Packet Filters
- Domain Filters
- URL Blocking
- MAC Control
- VPN
- Miscellaneous

VPN Settings

Item	Setting
VPN	<input checked="" type="checkbox"/> Enable
Max. number of tunnels	2

ID	Tunnel Name	Method
1	ike-with-Freeswan	IKE More
2		IKE More
3		IKE More
4		IKE More
5		IKE More

Current Time: Tuesday, June 01, 2004 12:05:35 AM

<< Previous Next >> Save Undo Dynamic VPN Settings... Help

3. Set the VPN setting as follow picture.

WBR3404TX Broadband Router Web Management - Microsoft Internet Explorer

Address: http://192.168.0.254/

level one BroadbandRouter

Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox Logout

Security Settings

- Packet Filters
- Domain Filters
- URL Blocking
- MAC Control
- VPN
- Miscellaneous

VPN Settings - Tunnel 1 - IKE

Item	Setting
Tunnel Name	ike-with-Freeswan
Local Subnet	192.168.0.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.111.0
Remote Netmask	255.255.255.0
Remote Gateway	192.168.123.102
Preshare Key	freeswan
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

Current Time: Tuesday, June 01, 2004 12:06:03 AM

Save Undo Back Help No change!

4. Set the IKE Proposal as below.

The screenshot shows the 'VPN Settings - Tunnel 1 - Set IKE Proposal' configuration page. The interface includes a sidebar with navigation options: Packet Filters, Domain Filters, URL Blocking, MAC Control, VPN, and Miscellaneous. The main content area features a table of IKE proposals and a 'Remove' button for the selected proposal.

ID	Proposal Name	DH Group	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	G2-3DES-MD5	Group 2	3DES	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	0	Sec.

Current Time: Tuesday, June 01, 2004 12:06:34 AM

5. set IPSec Proposal as below.

The screenshot shows the 'VPN Settings - Tunnel 1 - Set IPSec Proposal' configuration page. The interface includes a sidebar with navigation options: Packet Filters, Domain Filters, URL Blocking, MAC Control, VPN, and Miscellaneous. The main content area features a table of IPSec proposals and a 'Remove' button for the selected proposal.

ID	Proposal Name	DH Group	Encap. protocol	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	G2-ESP-3DES-MD5	Group 2	ESP	3DES	MD5	28800	Sec.
2		None	ESP	3DES	None	0	Sec.
3		None	ESP	3DES	None	0	Sec.
4		None	ESP	3DES	None	0	Sec.
5		None	ESP	3DES	None	0	Sec.
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.

Current Time: Tuesday, June 01, 2004 12:07:05 AM

Configuration for Freeswan as below:

```
#####  
#####
```

```
/etc/ipsec.conf
```

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file
```

```
# More elaborate and more varied sample configurations can be found  
# in FreeS/WAN's doc/examples file, and in the HTML documentation.
```

```
# basic configuration
```

```
config setup
```

```
    # THIS SETTING MUST BE CORRECT or almost nothing will work;
```

```
    # %defaultroute is okay for most simple cases.
```

```
    interfaces=%defaultroute
```

```
    # Debug-logging controls: "none" for (almost) none, "all" for lots.
```

```
    klipsdebug=none
```

```
    plutodebug=none
```

```
    # Use auto= parameters in conn descriptions to control startup actions.
```

```
    plutoload=%search
```

```
    plutostart=%search
```

```
    # Close down old connection when new one using same ID shows up.
```

```
    uniqueids=yes
```

```
# defaults for subsequent connection descriptions
```

```
# (these defaults will soon go away)
```

```
conn %default
```

```
    keyingtries=0
```

```
    disablearrivalcheck=no
```

```
    #authby=rsasig
```

```
    #authby=secret
```

```
    #leftrsasigkey=%dnsondemand
```

```
    #rightrsasigkey=%dnsondemand
```

```
conn ike-with-DDC3404TX-esp-3des-md5
```

```
left=192.168.123.104
leftsubnet=192.168.0.0/24
leftnexthop=192.168.123.103
right=192.168.123.102
rightsubnet=192.168.111.0/24
rightnexthop=192.168.123.103
authby=secret
pfs=yes
auto=add
```

```
#####
#####
```

```
[root@earth]# ipsec auto --up ike-with-DDC3404TX-esp-3des-md5
104 "ike-with-DDC3404TX-esp-3des-md5" #1: STATE_MAIN_I1: initiate
106 "ike-with-DDC3404TX-esp-3des-md5" #1: STATE_MAIN_I2: sent MI2,
expecting MR2
108 "ike-with-DDC3404TX-esp-3des-md5" #1: STATE_MAIN_I3: sent MI3,
expecting MR3
004 "ike-with-DDC3404TX-esp-3des-md5" #1: STATE_MAIN_I4: ISAKMP SA
established
117 "ike-with-DDC3404TX-esp-3des-md5" #2: STATE_QUICK_I1: initiate
004 "ike-with-DDC3404TX-esp-3des-md5" #2: STATE_QUICK_I2: sent QI2, IPsec
SA established
```

```
#####
#####
```

Please edit "ipsec.secrets: file of freeswan for Pre-share Key setting as same as LevelOne router.

```
# This file holds shared secrets or RSA private keys for inter-Pluto
# authentication.  See ipsec_pluto(8) manpage, and HTML documentation.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.  Suitable public keys, for ipsec.conf, DNS,
# or configuration of other implementations, can be extracted convenientl
# with "ipsec showhostkey".
: RSA (
  # RSA 2192 bits  earth2  Tue Apr 22 03:01:58 2003
  # for signatures only, UNSAFE FOR ENCRYPTION
  #pubkey=OsAQOQYFyL6gOQOrVKQh4wRUNFIOuHqMRfnwQ3VO3YHr2w68p/Ww/1yO9:
  #IN KEY Ox4200 4 1 AQOQYFyL6gOQOrVKQh4wRUNFIOuHqMRfnwQ3VO3YHr2w68!
  # (Ox4200 = auth-only host-level, 4 = IPSec, 1 = RSA)
  Modulus: Ox90605c8bea0d10d2b54a421e30454345234b87a8c45f9f043754ed:
  PublicExponent: Ox03
  # everything after this point is secret
  PrivateExponent: Ox18100f6ca7022d78738c605a5d60e08b85e1ebf1760fef:
  Prime1: Oxda0205f08edff2af1720a8ca2da924bd0d6caab6ef0ee92cdb8ca43:
  Prime2: Oxa9896b7eeb75f10b99b25c1d7ff0181f900fa3ac836d4ca8b8e6e3d:
  Exponent1: Ox9156aea05f3ff71f64c07086c91b6dd35e4871cf4a09f0c8925d:
  Exponent2: Ox710647a9f24ea0b26676e813aaa010150ab517c8579e331b25ef:
  Coefficient: Ox9aa051508f71f1582c86e27e332bbca0078c19b879153d2db9!
)

#%any 192.168.123.102 : PSK "12345678"

: RSA /etc/ipsec.d/private/myKey.pem "freeswan"
  Router WAN IP      FreesWan ext. IP      Preshare KEY
# do not change t... of that ")"
192.168.123.104 192.168.123.103: PSK "freeswan"
```