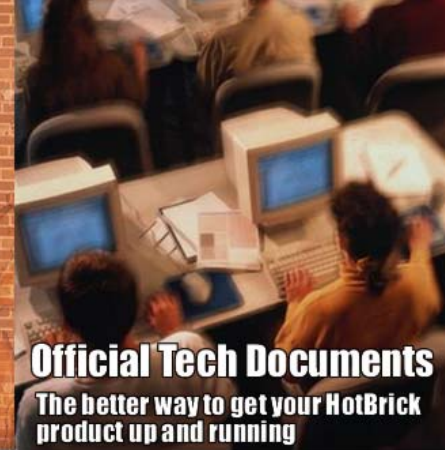


HotBrick
Don't Get Hacked. Get HotBrick.



Official Tech Documents
The better way to get your HotBrick product up and running

HotBrick VPN Client Troubleshooting

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

EUROPE
Generatorstraat 26
Hengelo (Ov), 7556 RC
Amsterdam - Netherlands
www.hotbrick.nl
support@hotbrick.nl

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

Table of contents

1	Introduction	0
2	Tools in case of trouble	0
2.1	A good network analyser: ethereal	0
3	VPN IPSec Troubleshooting	0
3.1	« PAYLOAD MALFORMED » error (wrong Phase 1 [SA])	0
3.2	« INVALID COOKIE » error	0
3.3	« no keystate » error	0
3.4	« received remote ID other than expected » error	0
3.5	« NO PROPOSAL CHOSEN » error	0
3.6	« INVALID ID INFORMATION » error	0
3.7	No response for phase 1 requests	0
3.8	SEND, RECV and that is all !	0
3.9	No response to phase 2 requests	0
3.10	I clicked on "Open tunnel", but nothing happens.	0
3.11	The VPN tunnel is up but I can't ping !	0
4	Contacts	0

1 Introduction

The goal of this document is to help IT Managers, system administrators or users facing VPN configuration issues of their IPSec VPN network. All information concerning VPN connection state, VPN trace or VPN Logs can be found in the "Console" Window of HotBrick VPN Client.

2 Tools in case of trouble

Configuring an IPSec VPN tunnel can be a hard task. One missing parameter can prevent a VPN connection from being established. Some tools are available to find source of troubles during a VPN establishment.

2.1 A good network analyser: ethereal

Ethereal is a free software that can be used for packet and traffic analysis. It shows IP or TCP packets received on a network card. This tool is available on website <http://www.ethereal.com/>. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation.

3 VPN IPSec Troubleshooting

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

```
114915 Default sysdep_app_open: Init Connection for : Cnx\Cnx-P2 Cnx-remote-addr
114915 Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
114915 Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
114920 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA] [VID]
114920 Default (SA Cnx-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 notifica-
tion type PAYLOAD_MALFORMED
114920 Default SEND Informational [NOTIFY] with PAYLOAD_MALFORMED error
```

If you have an « PAYLOAD MALFORMED » error you might have a wrong Phase 1 [SA], check if the encryption algorithms are the same on each side of the VPN tunnel.

3.2 « 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 notifica-
tion type INVALID_COOKIE
115933 Default SEND Informational [NOTIFY] with INVALID_COKIE error
```

If you have an « INVALID COOKIE » error, it means that one of the endpoint is using a SA that is no more in use. Reset the VPN connection on each side.

3.3 « no keystate » error

```
115305 Default sysdep_app_open: Init Connection for : Cnx\Cnx-P2 Cnx-remote-addr
115305 Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
115305 Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
```

USA

7243 NW 54th Street
Miami, FL 33166
www.hotbrick.com
support@hotbrick.com

EUROPE

Generatorstraat 26
Hengelo (Ov), 7556 RC Amsterdam
Netherlands
www.hotbrick.nl

BRAZIL

Francisco Tramontano, 100
05686-010 – São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

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

If you have an « no keystate » error, check if the preshared key is correct or if the local ID is correct (see

« Advanced » button). You should have more information in the remote endpoint logs.

3.4 « received remote ID other than expected » error

```
120343 Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
120343 Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
120343 Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
120348 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA] [VID]
120349 Default (SA Cnx-P1) RECV phase 1 Main Mode [SA] [VID]
120349 Default (SA Cnx-P1) SEND phase 1 Main Mode [KEY] [NONCE]
120351 Default (SA Cnx-P1) RECV phase 1 Main Mode [KEY] [NONCE]
120351 Default (SA Cnx-P1) SEND phase 1 Main Mode [ID] [HASH] [NOTIFY]
120351 Default (SA Cnx-P1) RECV phase 1 Main Mode [ID] [HASH] [NOTIFY]
120351 Default ike_phase_1_rcv_ID: received remote ID other than expected support@hotbrick.com
```

The " Remote ID " value (see " Advanced " Button) does not match what the remote endpoint is expected.

3.5 « NO PROPOSAL CHOSEN » error

```
115905 Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
115905 Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
115905 Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
115911 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA] [VID]
115913 Default (SA Cnx-P1) RECV phase 1 Main Mode [SA] [VID]
115913 Default (SA Cnx-P1) SEND phase 1 Main Mode [KEY] [NONCE]
115915 Default (SA Cnx-P1) RECV phase 1 Main Mode [KEY] [NONCE]
115915 Default (SA Cnx-P1) SEND phase 1 Main Mode [ID] [HASH] [NOTIFY]
115915 Default (SA Cnx-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 Cnx-Cnx-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 Cnx-P1 deleted
```

If you have an « NO PROPOSAL CHOSEN » error, check that the « Phase 2 » encryption algorithms are the same on each side of the VPN Tunnel.

Check « Phase 1 » algorithms if you have this:

```
115905 Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
115905 Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
115905 Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
115911 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA] [VID]
115911 Default RECV Informational [NOTIFY] with NO_PROPOSAL_CHOSEN error
```

3.6 « INVALID ID INFORMATION » error

```
122609 Default sysdep_app_open: Init Connection for : CnxCnx-P2 Cnx-remote-addr
122609 Default sysdep_app_open: IPV4_SUBNET Network 192.168.3.1
122609 Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
122623 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA] [VID]
122625 Default (SA Cnx-P1) RECV phase 1 Main Mode [SA] [VID]
122625 Default (SA Cnx-P1) SEND phase 1 Main Mode [KEY] [NONCE]
122626 Default (SA Cnx-P1) RECV phase 1 Main Mode [KEY] [NONCE]
122626 Default (SA Cnx-P1) SEND phase 1 Main Mode [ID] [HASH] [NOTIFY]
122626 Default (SA Cnx-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 Cnx-Cnx-P2) SEND phase 2 Quick Mode [SA] [KEY] [ID] [HASH] [NONCE]
122626 Default RECV Informational [HASH] [NOTIFY] with INVALID_ID_INFORMATION er-
ror
122626 Default RECV Informational [HASH] [DEL]
122626 Default Cnx-P1 deleted
```

If you have an « INVALID ID INFORMATION » error, check if « Phase 2 » ID (local address and network address) is correct and match what is expected by the remote endpoint.

Check also ID type ("Subnet address" and "Single address"). If network mask is not check, you are using a IPV4_ADDR type (and not a IPV4_SUBNET type).

Check in your VPN Router SA monitor if a previous SA is still alive.

3.7 No response for phase 1 requests

```
114920 Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA]
[KEY_EXCH]
[NONCE] [ID] [VID]
114920 Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA]
[KEY_EXCH]
[NONCE] [ID] [VID]
114920 Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA]
[KEY_EXCH]
[NONCE] [ID] [VID]
114920 Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA]
[KEY_EXCH]
[NONCE] [ID] [VID]
```

If the remote gateway does not answer, there must be wrong parameters. Check the algorithms are the same on each side of the VPN tunnel. Check also phase 1 IDs (in "Advanced" window).

3.8 SEND, RECV and that is all !

```
115315 Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA]
[KEY_EXCH]
[NONCE] [ID] [VID]
115317 Default (SA CnxVpn1-P1) RECV phase 1 Aggressive Mode [HASH] [SA]
[KEY_EXCH]
[NONCE] [ID] [VID]
```

Check if the preshared key is correct. Maybe two VPN tunnels are configured on your VPN Router.

3.9 No response to phase 2 requests

```
120348 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA]
[NONCE]
[ID] [ID]
120349 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA]
[NONCE]
[ID] [ID]
120351 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA]
[NONCE]
[ID] [ID]
120351 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA]
[NONCE]
[ID] [ID]
```

Check algorithms and phase 2 identities ("Local address" and "Network address"). Some settings must mismatch between the VPN and the VPN gateway.

3.10 I clicked on "Open tunnel", but nothing happens.

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPSec Client uses UDP port 500 and protocol ESP (protocol 50).

3.11 The VPN tunnel is up but I can't ping !

If the VPN tunnel is up, but you still cannot ping the remote LAN, here are a few guidelines:

- ? Check Phase 2 settings: VPN Client address and Remote LAN address. Usually, VPN Client IP address should not belong to the remote LAN subnet
- ? Once VPN tunnel is up, packets are sent with ESP protocol. This protocol can be blocked by firewall. Check that every device between the client and the VPN server does accept ESP
- ? Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- ? Check your ISP support ESP
- ? If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Ethereal for example). You will have an indication that encryption works.
- ? Check the "default gateway" value in VPN Server LAN. A target on your remote LAN can receive pings but does not answer because there is a no "Default gateway" setting.
- ? You cannot access to the computers in the LAN by their name. You must specify their IP address inside the LAN.
- ? We recommend you to install ethereal (<http://www.ethereal.com>) on one of your target computer. You can check that your pings arrive inside the LAN.

4 Contacts

News and updates on HotBrick web site : <http://www.hotbrick.com>

Technical support by email at support@hotbrick.com