Table of contents

1 Introduction .................................................................................................................................................... 3
  1.1 Goal of this document ............................................................................................................................ 3
  1.2 VPN Network topology ........................................................................................................................... 3
  1.3 Juniper NetScreen 5GT Firewall ............................................................................................................ 3
  1.4 Juniper NetScreen 5GT Firewall product info ........................................................................................ 3
2 Juniper NetScreen 5GT VPN configuration ................................................................................................... 4
  2.1 Create GateWay .................................................................................................................................... 4
  2.2 Set Advanced ......................................................................................................................................... 4
  2.3 Create IKE ............................................................................................................................................. 5
  2.4 Set Advanced ......................................................................................................................................... 5
  2.5 Create VPN policy .................................................................................................................................. 5
3 TheGreenBow IPSec VPN Client configuration ............................................................................................. 7
  3.1 VPN Client Phase 1 (IKE) Configuration ............................................................................................... 7
  3.2 VPN Client Phase 2 (IPSec) Configuration ............................................................................................ 8
  3.3 Open IPSec VPN tunnels ....................................................................................................................... 8
4 Tools in case of trouble .................................................................................................................................. 9
  4.1 A good network analyser: Wireshark ..................................................................................................... 9
5 VPN IPSec Troubleshooting .......................................................................................................................... 10
  5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) .................................................................... 10
  5.2 « INVALID COOKIE » error .................................................................................................................. 10
  5.3 « no keystate » error ............................................................................................................................ 10
  5.4 « received remote ID other than expected » error ................................................................................. 10
  5.5 « NO PROPOSAL CHOSEN » error ....................................................................................................... 11
  5.6 « INVALID ID INFORMATION » error .................................................................................................. 11
  5.7 I clicked on “Open tunnel”, but nothing happens ............................................................................... 11
  5.8 The VPN tunnel is up but I can’t ping ! ............................................................................................... 11
6 Contacts....................................................................................................................................................... 13
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client software with a Juniper NetScreen 5GT firewall to establish VPN connections for remote access to corporate network.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client software to the LAN behind the Juniper NetScreen 5GT firewall. The VPN client is connected to the Internet with a DSL connection or through a LAN. All the addresses in this document are given for example purpose.

1.3 Juniper NetScreen 5GT Firewall

Our tests and VPN configuration have been conducted with Juniper NetScreen 5GT firmware release 5.0.0r10.0.

1.4 Juniper NetScreen 5GT Firewall product info

It is critical that users find all necessary information about Juniper NetScreen 5GT firewall. All product info, User Guide and knowledge base for the Juniper NetScreen 5GT firewall can be found on the juniper website:

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Juniper NetScreen 5GT FAQ/Knowledge Base</td>
<td><a href="http://www.juniper.net/customers/support/">http://www.juniper.net/customers/support/</a></td>
</tr>
</tbody>
</table>
2 Juniper NetScreen 5GT VPN configuration

This section describes how to build an IPSec VPN configuration with your Juniper NetScreen 5GT firewall. Once connected to your Juniper NetScreen 5GT firewall, you must select “VPN” and “GateWay” tabs.

2.1 Create GateWay

![VPN configuration interface](image)

2.2 Set Advanced

![Advanced configuration interface](image)
2.3 Create IKE

VPN Name: thegreenbow
Security Level: Custom
Remote Gateway: Create a Simple Gateway
Gateway Name: thegreenbow
Type: Static IP
Address/Hostname: 
Peer ID: 
User Role: 
Group Role: 
Local ID: (optional)
Pre-shared Key: Use As Seed
Security Level: Custom
Outgoing Interface: untrust

2.4 Set Advanced

Security Level: Custom
Predefined: Standard, Compatible, Basic
User Defined: Custom
Phase 2 Proposal:
Key Exchange: 
Hash: 
Group: 
Replay Protection:
Transport Mode: (For L2TP-over-IPSec only)
Bind to: None, Tunnel Interface, Tunnel Zone

VPN Monitor:
Source Interface: default
Destination IP: 0.0.0.0
Optimized:
Rekey:

2.5 Create VPN policy

Policy from trust to untrust:

Name (optional):
Source Address:
Address Book Entry: 192.168.3.0/24, Multiple
Destination Address:
Address Book Entry: 192.168.10.122/16, Multiple
Service: IRC
Application: None
Action: Tunnel
Tunnel VPN: thegreenbow
Modify matching bidirectional VPN policy
L2TP: None
Logging:

OK Cancel Advanced
Policy from untrust to trust:

Name (optional)  
Source Address  
- New Address  
  - Address Book Entry 192.168.10.122/32  
Destination Address  
- New Address  
  - Address Book Entry 192.168.3.924  
Service  
Application  
Action  
Tunnel  
VPN  
Modify matching bidirectional VPN policy  
L2TP  
Logging  

[OK] [Cancel] [Advanced]
3 TheGreenBow IPSec VPN Client configuration

This section describes the required configuration to connect to a Juniper NetScreen 5GT VPN connections.

To download the latest release of TheGreenBow IPSec VPN Client software, please go to [http://www.thegreenbow.com/vpn_down.html](http://www.thegreenbow.com/vpn_down.html).

3.1 VPN Client Phase 1 (IKE) Configuration

You may use either Preshad key, Certificates, USB Tokens, OTP Token (One Time Password) or X-Auth combined with RADIUS Server for User Authentication with the Juniper NetScreen 5GT firewall. This configuration is one example of what can be accomplished in term of User Authentication. You may want to refer to either the Juniper NetScreen 5GT firewall user guide or TheGreenBow IPSec VPN Client software User Guide for more details on User Authentication options.
3.2 VPN Client Phase 2 (IPSec) Configuration

3.3 Open IPSec VPN tunnels

Once both Juniper NetScreen 5GT firewall and TheGreenBow IPSec VPN Client software have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPSec traffic.

1. Click on "Save & Apply" to take into account all modifications we’ve made on your VPN Client configuration
2. Click on "Open Tunnel", or generate traffic that will automatically open a secure IPSec VPN Tunnel (e.g. ping, IE browser)
3. Select "Connections" to see opened VPN Tunnels
4. Select "Console" if you want to access to the IPSec VPN logs and adjust filters to display less IPSec messaging. The following example shows a successful connection between TheGreenBow IPSec VPN Client and a Juniper NetScreen 5GT VPN router.

```
2009/06/30 10:45:25 Default (SA Gateway2-P1) SEND phase 1 Main Mode [HA][MD][MD][MD][MD][MD]
2009/06/30 10:45:25 Default (SA Gateway2-P1) RECV phase 1 Main Mode [SA][MD][MD][MD][MD][MD]
2009/06/30 10:45:25 Default (SA Gateway2-P1) SEND phase 1 Main Mode [KEY_EXCH][NONCE][NAT-D][NAT-D]
2009/06/30 10:45:25 Default (SA Gateway2-P1) RECV phase 1 Main Mode [KEY_EXCH][NONCE][NAT-D][NAT-D]
2009/06/30 10:45:25 Default (SA Gateway2-P1) SEND phase 1 Main Mode [HASH] [ID][NOTIFY]
2009/06/30 10:45:25 Default (SA Gateway2-P1) RECV phase 1 Main Mode [HASH] [ID][NOTIFY]
2009/06/30 10:45:25 Default (SA Gateway2-P1) SEND phase 2 Quick Mode [HASH] [SA][KEY_EXCH][NONCE][ID][ID]
2009/06/30 10:45:25 Default (SA Gateway2-P1) RECV phase 2 Quick Mode [HASH] [SA][KEY_EXCH][NONCE][ID][ID]
2009/06/30 10:45:25 Default (SA Gateway2-P1) SEND phase 2 Quick Mode [HASH] [SA][KEY_EXCH][NONCE][ID][ID]
2009/06/30 10:45:25 Default (SA Gateway2-P1) RECV phase 2 Quick Mode [HASH] [SA][KEY_EXCH][NONCE][ID][ID]
2009/06/30 10:45:25 Default (SA Gateway2-P1) SEND phase 3 Quick Mode [HASH] [SA][KEY_EXCH][NONCE][ID][ID]
2009/06/30 10:45:25 Default (SA Gateway2-P1) RECV phase 3 Quick Mode [HASH] [SA][KEY_EXCH][NONCE][ID][ID]
```

VPN Client Virtual IP address

Enter the IP address (and subnet mask) of the remote LAN.
4 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.

4.1 A good network analyser: Wireshark

Wireshark 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.wireshark.org](http://www.wireshark.org). It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation ([http://www.wireshark.org/docs/](http://www.wireshark.org/docs/)).
5 VPN IPSec Troubleshooting

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

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.

5.2 « INVALID COOKIE » 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.

5.3 « 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.

5.4 « received remote ID other than expected » error

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.
5.5 « NO PROPOSAL CHOSEN » error

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:

5.6 « INVALID ID INFORMATION » error

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).

5.7 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).

5.8 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 Wireshark 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 Wireshark (http://www.wireshark.org) on one of your target computer. You can check that your pings arrive inside the LAN.
6 Contacts

News and updates on TheGreenBow web site: http://www.thegreenbow.com
Technical support by email at support@thegreenbow.com
Sales contacts by email at sales@thegreenbow.com
Secure, Strong, Simple.
TheGreenBow Security Software