TheGreenBow IPSec VPN Client
Configuration Guide
Windows 2000 Server

WebSite:  http://www.thegreenbow.com
Contact:  support@thegreenbow.com
Table of contents

1 Goal of this document ........................................................................................................................................ 0
2 Windows 2000 Server VPN Configuration ........................................................................................................ 0
  2.1 Windows 2000 Server IP Security Policies .................................................................................................... 0
  2.2 Windows 2000 Server Pre Shared key ........................................................................................................... 0
  2.3 Windows 2000 Server IP Filter ..................................................................................................................... 0
  2.4 Windows 2000 Server IPSec algorithms ...................................................................................................... 0
3 TheGreenBow IPSec VPN Client configuration ............................................................................................... 0
  3.1 VPN Client Phase 1 (IKE) Configuration .................................................................................................... 0
  3.2 VPN Client Phase 2 (IPSec) Configuration .................................................................................................. 0
  3.3 Open IPSec VPN tunnels .............................................................................................................................. 0
4 Tools in case of trouble ...................................................................................................................................... 0
  4.1 A good network analyser : ethereal ............................................................................................................. 0
  4.2 Netdiag.exe ................................................................................................................................................... 0
5 VPN IPSec Troubleshooting ............................................................................................................................... 0
  5.1 « PAYLOAD MALFORMED » error .............................................................................................................. 0
  5.2 « INVALID COOKIE » error .......................................................................................................................... 0
  5.3 « no keystate » error ..................................................................................................................................... 0
  5.4 « received remote ID other than expected » error ......................................................................................... 0
  5.5 « NO PROPOSAL CHOSEN » error ............................................................................................................. 0
  5.6 « INVALID ID INFORMATION » error ......................................................................................................... 0
  5.7 I clicked on “Open tunnel”, but nothing happens ......................................................................................... 0
  5.8 The VPN tunnel is up but I can't ping ! ......................................................................................................... 0
6 Contacts ............................................................................................................................................................ 0
1 Goal of this document

This document describes VPN configuration of TheGreenBow IPSec VPN client and a host server with Microsoft Windows 2000 server. The two computers belong to the same local network. TheGreenBow VPN Client IP address is 192.168.1.3 and Windows 2000 Server IP address is 192.168.1.2.

This configuration is given as an example.
2 Windows 2000 Server VPN Configuration

2.1 Windows 2000 Server IP Security Policies

- For changing IPSec VPN configuration, click on Start, Programs, Administration tools, Local security settings.


Welcome to the IP Security Policy wizard.

This wizard helps you create an IP Security Policy. You will specify the level of security to use when communicating with specific computers or groups of computers (subnets), and for particular IP traffic types.

To continue, click Next.
- Give a name to your Security rule and a description. Then click on «Next».

- Click on «Next».
• Click on «Use this string to protect the key exchange» and fill the form with a preshared key. This value will be used by the VPN client. Then click on «Next».

• Click on «Next».

---

IP Security Policy Wizard

Default Response Rule Authentication Method
To add multiple authentication methods edit the default response rule after completing the wizard.

- Windows 2000 default (Kerberos V5 protocol)
- Use a certificate from this certificate authority (CA):

  Browse...

- Use this string to protect the key exchange (preshared key):

  abcdel

---

IP Security Policy Wizard

Completing the IP Security Policy Wizard
You have successfully completed specifying the properties for your new IP security policy.

To edit your IP security policy now, select the Edit properties check box, and then click Finish.

- Edit properties

To close this wizard, click Finish.
- Unchecked «default response» then click on «Add». We will add a security rule for the Windows 2000 server.
• Click on «Next».

This security rule concerns a tunnel between the Microsoft Windows 2000 Server and TheGreenBow VPN client. VPN client is the remote endpoint and has IP address 192.168.1.3. Use this address and click on «Next».
In our example, the computers belong to the same local area network. Click on «Local area network» then on «Next».
2.2 Windows 2000 Server Pre Shared key

- Communication between the IPsec client and the server is protected by a preshared key. Click on «Use this string to protect the key exchange (preshared key) » and fill the form with the preshared key value. Click on «Next».

![IP Security Policy Wizard](image)

2.3 Windows 2000 Server IP Filter

- Now, we must link our security rule with a IP filter. Click on «Add».
Give a name to your IP filter and a description. Then click on "Add".
• Configuration wizard begins. Click on «Next».

![IP Filter Wizard](image1)

Welcome to the IP Filter Wizard.

This wizard helps you provide the source, destination, and traffic-type information needed to filter IP traffic.

This wizard creates "mirrored" filters that match on both incoming and outgoing IP traffic.

You can add multiple filters to build an IP Filter List that matches on IP packets for multiple source or destination machines, or for many different traffic types.

To continue, click Next.

![Filter Wizard](image2)

• Give starting endpoint IP address of the VPN tunnel (Microsoft Windows 2000 Server). Then click on «Next».
• Give final endpoint IP address of the VPN tunnel (TheGreenBow VPN client). Then click on « **Next** ».

![Filter Wizard](image)

**IP Traffic Destination**
Specify the destination address of the IP traffic.

- Destination address:
  - A specific IP Address
- IP Address: 192.168.1.3
- Subnet mask: 255.255.255.255

![Filter Wizard](image)

**IP Protocol Type**
Select the IP Protocol type. If this type supports IP ports, you will also specify the IP port.

- Select a protocol type: Any

![Filter Wizard](image)
- Click on « Finish » for ending IP filter creation.

- IP filter was added. Click on « Close »
- Select in the list the IP filter you have just created, then click on « Next ».

- You must associate a filter action with a security rule. Click on « Add ».
• Click on «Next».

![Filter Action Wizard]

Welcome to the IP Security Filter Action Wizard

Use this wizard to specify properties for a new filter action.

A filter action sets the security requirements for a data transfer. These requirements are specified in a list of security methods contained in the filter action.

Data transfer is only possible when the computers involved use the same security methods. Multiple security methods increase the chance that two computers will use the same method.

To continue, click Next.

![Filter Action]

• Give a name for your Filter Action then click on «Next».
• Click on «**Negotiate security** » then on «**Next** ».

![Filter Action General Options](image)

- **Filter Action General Options**
  - Set the filter action behavior.
  - Options: Forward, Block, **Negotiate security**.

• Click on «**Do not communicate with computers that do not support IPSec** » if you want every communication between the client and the server to be secured. Then click on «**Next** ».

![Filter Action Wizard](image)

- **Filter Action Wizard**
  - **Communicating with computers that do not support IPSec**
  - Communicating with computers that do not support IPSec may expose your network to security risks.
  - Do you want to allow communication with computers that do not support IPSec?
    - **Do not communicate with computers that do not support IPSec**
    - Fall back to unsecured communication.
    - Use this option if there are computers that do not support IPSec on your network. Communication with computers that do not support IPSec may expose your network to security risks.
2.4 Windows 2000 Server IPSec algorithms

- Select « Custom » and click on « Settings ».

In our example, we are using MD5 and DES with ESP. Click on « OK » and on « Next ».

- In our example, we are using MD5 and DES with ESP. Click on « OK » and on « Next ».

- In our example, we are using MD5 and DES with ESP. Click on « OK » and on « Next ».

- In our example, we are using MD5 and DES with ESP. Click on « OK » and on « Next ».
• For finishing Filter Action configuration, click on « Finish ».

• The new IP filter action is shown in the list. Click on « Next ».
• Click on « Finish ».
- IP filter we have just created is shown in IP filter list. Click on «OK».
• We must create another Security Rule that deals with communication from TheGreenBow VPN client to Microsoft Windows 2000 Server. Click on « Add ».

1. Click on « Next ».

2. Welcome to the Create IP Security Rule Wizard.

A security rule governs how and when security is invoked based upon criteria, such as the source, destination, and type of IP traffic, in the security rule's IP filter list.

A security rule contains a collection of security actions that are activated when a communication matches the criteria in the IP filter list.

Security actions:
- IP tunneling attributes
- Authentication methods
- Filter actions

To continue, click Next.
• Give IP address of VPN tunnel final endpoint (here Microsoft Windows 2000 Server) then click on «Next».

In our example, the computers belong to the same local area network. Click on «Local area network» then on «Next».
- Traffic between the VPN client and the server is protected by a preshared key. Click on « **Use this string to protect the key exchange (preshared key)** » and fill the form with the preshared key. Click on « **Next** ».

- Click on « **Add** » in order to insert a specific IP filter to our new security rule.

---

**IP Security Policy Wizard**

**Authentication Method**

To add multiple authentication methods, edit the security rule after completing the IP security rule wizard.

Set the initial authentication method for this security rule:

- Windows 2000 default (Kerberos V5 protocol)
- Use a certificate from this Certificate Authority (CA): [Browse...]
- Use this string to protect the key exchange (preshared key):

```
abcdef
```

---

**Security Rule Wizard**

**IP Filter List**

Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

**IP Filter lists:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000 Server</td>
<td>Traffic from 2000 server to to...</td>
</tr>
<tr>
<td>All ICMP Traffic</td>
<td>Matches all ICMP packets bet...</td>
</tr>
<tr>
<td>All IP Traffic</td>
<td>Matches all IP packets from t...</td>
</tr>
</tbody>
</table>

---
• Give a name to the new IP filter then click on «Add».

• Click on «Next».
- Select « A specific IP address » and give TheGreenBow client IP address. Then click on « Next ».

- Select « My IP address » as remote destination address, then click on « Next ».
- Set protocol type then click on «Next».

- Click on «Finish»
• Click on «Close».

• Select IP filter «TheGreenBow» then click on «Next».
• Select filter action «IpSec Filters» then click on «Next».

• Click on «Finish».
- Select «TheGreenBow» in the IP Filter lists then click on «OK».

![IP Filter List Table]

- The selected IP filter list specifies which network traffic will be secured with this rule.

### IP Filter Lists:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000 Server</td>
<td>Traffic from 2000 server to TheGreenBow server</td>
</tr>
<tr>
<td>All ICMP Traffic</td>
<td>Matches all ICMP packets between GreenBow and...</td>
</tr>
<tr>
<td>All IP Traffic</td>
<td>Matches all IP packets from this and...</td>
</tr>
<tr>
<td>TheGreenBow</td>
<td>Traffic TheGreenBow client -&gt; TheGreenBow server</td>
</tr>
</tbody>
</table>
Click on «Close».

For activating the new Security policy, right-click «TheGreenBow» policy, and left-click on «Assign». A green point is shown on icon «TheGreenBow».
3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration

In « Interface » field, you can select a star (« * ») if the VPN Client gets a dynamic IP address.

In « Remote address », set remote server IP address.

Remote VPN gateway address can be an IP address or a DNS address.

abcdef
abcdef

Configuration Phase 1
3.2 VPN Client Phase 2 (IPSec) Configuration

In this window, you set up IPSec VPN configuration. «Local address» field is virtual IP address of the client inside remote network.

3.3 Open IPSec VPN tunnels

Once both Windows Server and TheGreenBow IPSec VPN Client 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.
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.

Concerning Microsoft Windows 2000 Server, read in case of trouble document Q257225 in Microsoft Knowledge base:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;q257225

4.1 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 tools 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.

The following example shows a successful connection between TheGreenBow VPN client and a Microsoft Windows 2000 Server.
4.2 Netdiag.exe

Netdiag.exe can be find in Microsoft Windows 2000 Server Support Tools. Read Knowledge base article Q257225 for more details.

In a window CMD.EXE, type “select netdiag /test :ipsec /debug”. Output will be:

![Output of netdiag.exe](image)

5 VPN IPSec Troubleshooting

5.1 « 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.

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 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.

6 Contacts
News and updates on TheGreenBow web site : http://www.thegreenbow.com
Technical support by email at support@thegreenbow.com
Sales contacts at +33 1 43 12 39 37 ou by email at info@thegreenbow.com