TheGreenBow IPSec VPN Client
Configuration Guide

AlliedTelesis
AT-AR700 Series
with Radius Server

WebSite: http://www.thegreenbow.com
Contact: support@thegreenbow.com

Configuration Guide written by:
Writer: AlliedTelesis Engineering Team
Company: www.alliedtelesis.com
Table of contents

1 Introduction .................................................................................................................................................... 3
1.1 Goal of this document ............................................................................................................................ 3
1.2 VPN Network topology ........................................................................................................................... 3
1.3 AlliedTelesis AT-AR700 Series VPN Gateway...................................................................................... 3
1.4 AlliedTelesis AT-AR700 Series VPN Gateway product info................................................................. 3
2 AT-AR700 Series VPN configuration ............................................................................................................. 4
2.1 AT-AR700 Series Pre-Requisite Configuration ...................................................................................... 4
   Command file................................................................................................................................................ 7
2.2 AT-AR700 Series configuration of IPSec with Pre-Shared Key (PSK) & Firewall .................................. 7
   Command file................................................................................................................................................ 10
2.3 Configuring X-Auth............................................................................................................................... 11
   Command file................................................................................................................................................ 11
2.4 Save Configuration ............................................................................................................................... 11
   Command file................................................................................................................................................ 11
3 TheGreenBow IPSec VPN Client configuration ........................................................................................... 12
3.1 VPN Client Phase 1 (IKE) Configuration .............................................................................................. 12
3.2 VPN Client Phase 1 (P1 Advanced) Configuration .............................................................................. 13
3.3 VPN Client Phase 2 (IPSec) Configuration .......................................................................................... 14
3.4 Open IPSec VPN tunnels ..................................................................................................................... 14
4 Setup Windows 2003 Server (Radius Server) ............................................................................................. 16
4.1 Add New Radius Client ........................................................................................................................ 16
4.2 Set the Secret Key ............................................................................................................................... 17
5 Tools in case of trouble ................................................................................................................................ 18
5.1 A good network analyser: Wireshark ............................................................................................... 18
6 VPN IPSec Troubleshooting ...................................................................................................................... 19
6.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA])................................................................. 19
6.2 « INVALID COOKIE » error................................................................................................................ 19
6.3 « no keystate » error ............................................................................................................................ 19
6.4 « received remote ID other than expected » error.............................................................................. 19
6.5 « NO PROPOSAL CHOSEN » error.................................................................................................... 20
6.6 « INVALID ID INFORMATION » error............................................................................................. 20
6.7 I clicked on "Open tunnel", but nothing happens ............................................................................... 20
6.8 The VPN tunnel is up but I can’t ping ! ......................................................................................... 20
7 Contacts ....................................................................................................................................................... 22
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client software with an AlliedTelesis AT-AR700 Series VPN router to establish VPN connections for remote access to corporate network. User Authentication is checked against a Windows 2003 server configured as a Radius Server.

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 AlliedTelesis AT-AR700 Series router. 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 AlliedTelesis AT-AR700 Series VPN Gateway

Our tests and VPN configuration have been conducted with AlliedTelesis AT-AR700 Series firmware release 2.9.2-00

1.4 AlliedTelesis AT-AR700 Series VPN Gateway product info

It is critical that users find all necessary information about AlliedTelesis AT-AR700 Series VPN Gateway. All product info, User Guide and knowledge base for the AlliedTelesis AT-AR700 Series VPN Gateway can be found on the AlliedTelesis website: www.alliedtelesis.com

| AT-AR700 Series User Guide   | www.alliedtelesis.com/media/datasheets/reference/ar700_family_m_a_v291.zip |
2 AT-AR700 Series VPN configuration

This section describes how to build an IPSec VPN configuration with your AT-AR700 Series VPN router.

Once connected to your AT-AR700 Series VPN gateway

2.1 AT-AR700 Series Pre-Requisite Configuration

INFO: Self tests beginning.
INFO: RAM test beginning.
PASS: RAM test, 65536k bytes found.
INFO: Self tests complete.
INFO: Downloading router software.
Force EPROM download (Y) ?
INFO: Initial download successful.
INFO: Initialising Flash File System.
INFO: Executing configuration script <flash:boot.cfg>
INFO: Router startup complete

Login: manager
Password: friend

Manager > set user securedelay=600
User module configuration and counters

Security parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>login failures before lockout</td>
<td>5</td>
<td>(LOGINFAIL)</td>
</tr>
<tr>
<td>lockout period</td>
<td>600 seconds</td>
<td>(LOCKOUTPD)</td>
</tr>
<tr>
<td>manager password failures before logoff</td>
<td>3</td>
<td>(MANPWDFAIL)</td>
</tr>
<tr>
<td>maximum security command interval</td>
<td>600 seconds</td>
<td>(SECURDELAY)</td>
</tr>
<tr>
<td>minimum password length</td>
<td>6 characters</td>
<td>(MINPWDLEN)</td>
</tr>
<tr>
<td>TACACS retries</td>
<td>3</td>
<td>(TACRETRIES)</td>
</tr>
<tr>
<td>TACACS timeout period</td>
<td>5 seconds</td>
<td>(TACTIMEOUT)</td>
</tr>
<tr>
<td>minimum password categories to match</td>
<td>1</td>
<td>(PWDMINCAT)</td>
</tr>
<tr>
<td>previous passwords to match</td>
<td>disabled</td>
<td>(PWDHISTORY)</td>
</tr>
<tr>
<td>password lifetime</td>
<td>disabled</td>
<td>(PWDLIFETIME)</td>
</tr>
<tr>
<td>force password change at logon</td>
<td>disabled</td>
<td>(PWDFORCE)</td>
</tr>
<tr>
<td>semi-permanent manager port</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>
Security counters

<table>
<thead>
<tr>
<th>Counter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>logins</td>
<td>1</td>
</tr>
<tr>
<td>managerPwdChanges</td>
<td>1</td>
</tr>
<tr>
<td>unknownLoginNames</td>
<td>0</td>
</tr>
<tr>
<td>totalPwdFails</td>
<td>0</td>
</tr>
<tr>
<td>managerPwdFails</td>
<td>0</td>
</tr>
<tr>
<td>securityCmdLogoffs</td>
<td>0</td>
</tr>
<tr>
<td>loginLockouts</td>
<td>0</td>
</tr>
<tr>
<td>authentications</td>
<td>0</td>
</tr>
<tr>
<td>defaultAcctRecoveries</td>
<td>1</td>
</tr>
<tr>
<td>tacacsLoginReqs</td>
<td>0</td>
</tr>
<tr>
<td>tacacsLoginRejs</td>
<td>0</td>
</tr>
<tr>
<td>tacacsReqTimeouts</td>
<td>0</td>
</tr>
<tr>
<td>tacacsReqFails</td>
<td>0</td>
</tr>
<tr>
<td>databaseClearTotallys</td>
<td>0</td>
</tr>
</tbody>
</table>

Manager > **add user=allied pass=allied lo=yes**
Number of Radius-backup users..... 0
User Authentication Database

Username: allied ()
    Status: enabled  Privilege: user  Telnet: no  Login: yes  RBU: no
    Logins: 0  Fails: 0  Sent: 0  Rcvd: 0
    Authentications: 0 Fails: 0

Manager > **set user=allied telnet=no netmask=255.255.255.255**
Number of Radius-backup users..... 0
User Authentication Database

Username: allied ()
    Status: enabled  Privilege: user  Telnet: no  Login: yes  RBU: no
    Logins: 0  Fails: 0  Sent: 0  Rcvd: 0
    Authentications: 0 Fails: 0

Manager > **set user=manager pass=friend priv=manager lo=yes**
Number of Radius-backup users..... 0
User Authentication Database

Username: manager (Manager Account)
    Status: enabled  Privilege: manager  Telnet: yes  Login: yes  RBU: no
    Logins: 1  Fails: 0  Sent: 0  Rcvd: 0
    Authentications: 0 Fails: 0

Manager > **set user=manager telnet=yes desc="Manager Account"**
Number of Radius-backup users..... 0
User Authentication Database
Username: manager (Manager Account)
 Status: enabled Privilege: manager Telnet: yes Login: yes RBU: no
 Logins: 1 Fails: 0 Sent: 0 Rcvd: 0
 Authentications: 0 Fails: 0

Manager > **add user=secoff pass=secoff priv=securityOfficer lo=yes**
Number of Radius-backup users..... 0
User Authentication Database

Username: secoff ()
 Status: enabled Privilege: Sec Off Telnet: no Login: yes RBU: no
 Logins: 0 Fails: 0 Sent: 0 Rcvd: 0
 Authentications: 0 Fails: 0

Manager > **set user=secoff telnet=no netmask=255.255.255.255**
Number of Radius-backup users..... 0
User Authentication Database

Username: secoff ()
 Status: enabled Privilege: Sec Off Telnet: no Login: yes RBU: no
 Logins: 0 Fails: 0 Sent: 0 Rcvd: 0
 Authentications: 0 Fails: 0

Manager > **logon secoff**
Password: secoff
SecOff > enable system security_mode
Info (1034003): Operation successful.
SecOff > create enco key=1 type=general value=secret
Info (1073003): Operation successful.
SecOff > create vlan=vlan100 vid=100
Info (1089003): Operation successful.
SecOff > add vlan=100 port=1-5
Info (1089003): Operation successful.
SecOff > enable ip
Info (1005287): IP module has been enabled.
SecOff > add ip int=eth0 ip=172.28.40.41
Info (1005275): interface successfully added.
SecOff > add ip int=vlan100 ip=172.174.1.254 mask=255.255.255.0
Info (1005275): interface successfully added.
SecOff > add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=172.28.40.40
Info (1005275): IP route successfully added.

Command file
This is the sequence of command lines shown above without expected results. Cut and paste to use in your environment.

```
enable system security_mode
create enco key=1 type=general value=secret
create vlan=vlan100 vid=100
add vlan=100 port=1-5
enable ip
add ip int=eth0 ip=172.28.40.41
add ip int=vlan100 ip=172.174.1.254 mask=255.255.255.0
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=172.28.40.40
```

2.2 AT-AR700 Series configuration of IPSec with Pre-Shared Key (PSK) & Firewall

SecOff > create isakmp pol="windows_isakmp" pe=any mod=aggressive key=1 xau=server
Info (1082003): Operation successful.
SecOff > set isakmp pol=windows_isakmp gro=2
Info (1082003): Operation successful.
SecOff > set isakmp pol=windows_isakmp sendi=true
Info (1082003): Operation successful.
SecOff > set isakmp pol=windows_isakmp localid=172.28.40.41 remotei=sample@a.com
Info (1082003): Operation successful.
SecOff > create ipsec sas=1 key=isakmp prot=esp enc=des hasha=sha
Info (1081003): Operation successful.
SecOff > create ipsec bund=0 key=isakmp string=1
Info (1081003): Operation successful.
SecOff > create ipsec pol="peer" int=eth0 ac=ipsec key=isakmp bund=0 peer=ANY isa=windows_isakmp
Info (1081003): Operation successful.
SecOff > set ipsec pol="peer" lad=172.174.1.0 lma=255.255.255.0
Info (1081003): Operation successful.
SecOff > set ipsec pol="peer" usepfsk=TRUE gro=2
Info (1081003): Operation successful.
SecOff > create ipsec pol="internet" int=eth0 ac=permit
Info (1081003): Operation successful.
SecOff > create ipsec pol="isakmp" int=eth0 ac=permit
Info (1081003): Operation successful.
SecOff > set ipsec pol="isakmp" lp=500
Info (1081003): Operation successful.
SecOff > enable ipsec
Info (1081003): Operation successful.
SecOff > enable isakmp
Info (1082057): ISAKMP has been enabled.
SecOff > enable firewall
Info (1077257): 05-Feb-2010 13:40:22
   Firewall enabled.
Info (1077003): Operation successful.
SecOff > enable firewall notify@mail to=<administrator-email-address>
Info (1077003): Operation successful.
SecOff > create firewall policy="fw"
Info (1077003): Operation successful.
SecOff > create firewall policy="fw" dy=dynamic
Info (1077003): Operation successful.
SecOff > add firewall policy="fw" dy=dynamic us=ANY
Info (1077003): Operation successful.
SecOff > enable firewall policy="fw" icmp_f=all
Info (1077003): Operation successful.
SecOff > add firewall policy="fw" int=vlan100 type=private
Info (1077003): Operation successful.

SecOff > add firewall policy="fw" int=dyndynamic type=private
Info (1077003): Operation successful.

SecOff > add firewall policy="fw" int=eth0 type=public
Info (1077003): Operation successful.

SecOff > add firewall policy="fw" nat=enhanced int=vlan100 gblin=eth0
Info (1077003): Operation successful

SecOff > add firewall policy="fw" nat=enhanced int=dyndynamic gblin=eth0
Info (1077003): Operation successful.

SecOff > add firewall policy="fw" ru=1 ac=allo int=eth0 prot=udp po=500 ip=172.28.40.41 gblip=172.28.40.41 gblp=500
Info (1077003): Operation successful.

SecOff > add firewall policy="fw" ru=2 ac=non int=eth0 prot=ALL ip=172.174.1.0-172.174.1.254 enc=ips
Info (1077003): Operation successful.

SecOff > add firewall policy="fw" ru=3 ac=non int=vlan100 prot=ALL ip=172.174.1.0-172.174.1.254
Info (1077003): Operation successful.

SecOff > set firewall policy="fw" ru=3 rem=192.0.0.0-192.255.255.254
Info (1077003): Operation successful.

SecOff >.
Command file
This is the sequence of command lines shown above without expected results. Cut and paste to use in your environment.

```bash
create isakmp pol="windows_isakmp" pe=any mod=aggressive key=1 xau=server
set isakmp pol=windows_isakmp gro=2
set isakmp pol=windows_isakmp sendi=true
set isakmp pol=windows_isakmp localid=172.28.40.41 remotei@example@a.com
create ipsec sas=1 key=isakmp prot=esp enc=des hasha=sha
create ipsec bund=0 key=isakmp string=1
create ipsec pol="peer" int=eth0 ac=ipsec key=isakmp bund=0 peer=ANY
isa=windows_isakmp
set ipsec pol="peer" lad=172.174.1.0 lma=255.255.255.0
set ipsec pol="peer" usepfsk=TRUE gro=2
create ipsec pol="internet" int=eth0 ac=permit
create ipsec pol="isakmp" int=eth0 ac=permit
set ipsec pol="isakmp" lp=500
enable ipsec
enable isakmp
enable firewall
enable firewall notify@mail to=<administrator-email-address>
create firewall policy="fw"
create firewall policy="fw" dy=dynamic
add firewall policy="fw" dy=dynamic us=ANY
enable firewall policy="fw" icmp_f=all
add firewall policy="fw" int=_vlan100 type=private
add firewall policy="fw" int=dyn-dynamic type=private
add firewall policy="fw" int=eth0 type=public
add firewall poli="fw" nat=enhanced int=_vlan100 gblin=eth0
add firewall poli="fw" nat=enhanced int=dyn-dynamic gblin=eth0
add firewall poli="fw" ru=1 ac=allo int=eth0 prot=udp po=500 ip=172.28.40.41 gbip=172.28.40.41 gbip=500
add firewall poli="fw" ru=2 ac=non int=eth0 prot=ALL ip=172.174.1.0-172.174.1.254 enc=ips
add firewall poli="fw" ru=3 ac=non int=_vlan100 prot=ALL ip=172.174.1.0-172.174.1.254
set firewall poli="fw" ru=3 rem=192.0.0.0-192.255.255.254
```

2.3 Configuring X-Auth

SecOff > add radius server=172.174.1.100 secret=secret
Info (1077003): Operation successful.
SecOff > enable portauth=8021x
Info (1077003): Operation successful.

Command file
This is the sequence of command lines shown above without expected results. Cut and paste to use in your environment.

```
add radius server=172.174.1.100 secret=secret
enable portauth=8021x
```

2.4 Save Configuration

SecOff > create conf=vpn.cfg
Info (1034003): Operation successful.
SecOff > set conf=vpn.cfg
Warning: Config file MUST add a user with SECURITY OFFICER privilege
Do you wish to proceed with setting config?(y/n) y
Info (1049003): Operation successful.

Command file
This is the sequence of command lines shown above without expected results. Cut and paste to use in your environment.

```
create conf=vpn.cfg
set conf=vpn.cfg
y
```
3 TheGreenBow IPSec VPN Client configuration

This section describes the required configuration to connect to an AlliedTelesis AT-AR700 Series VPN router via VPN connections.

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

3.1 VPN Client Phase 1 (IKE) Configuration

![Phase 1 configuration]

The remote VPN Gateway IP address is either an explicit IP address or a DNS Name

Phase 1 configuration

You may use either Preshared key, Certificates, USB Tokens, OTP Token (One Time Password) or X-Auth combined with RADIUS Server for User Authentication with the AlliedTelesis AT-AR700 Series router. This configuration is one example of what can be accomplished in term of User Authentication. You may want to refer to either the AlliedTelesis AT-AR700 Series router user guide or TheGreenBow IPSec VPN Client software User Guide for more details on User Authentication options.
3.2 VPN Client Phase 1 (P1 Advanced) Configuration

P1 Advanced Configuration
3.3 VPN Client Phase 2 (IPSec) Configuration

![VPN Client Phase 2 Configuration](image)

**Phase 2 Configuration**

VPN Client Virtual IP address
Enter the IP address (and subnet mask) of the remote LAN.

3.4 Open IPSec VPN tunnels

Once both AlliedTelesis AT-AR700 Series router 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 after entering Login & Password. (e.g. ping, IE browser)

![Open Tunnel](image)

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 an AlliedTelesis AT-AR700 Series VPN router.

![Console](image)
20090630 104525 Default [SA Gateway-2-F1] SEND phase 1 Main Mode [SA] [MD] [MD] [MD] [MD]
20090630 104525 Default [SA Gateway-2-F1] RECVR phase 1 Main Mode [SA] [MD] [MD]
20090630 104525 Default [SA Gateway-2-F1] SEND phase 1 Main Mode [KEY EXCH] [NONCE] [NAT-D] [NAT-D]
20090630 104525 Default [SA Gateway-2-F1] RECVR phase 1 Main Mode [KEY EXCH] [NONCE] [NAT-D] [NAT-D]
20090630 104525 Default [SA Gateway-2-F1] SEND phase 1 Main Mode [HASH] [ID] [NOTIFY]
20090630 104525 Default [SA Gateway-2-F1] RECVR phase 1 Main Mode [HASH] [ID]
20090630 104525 Default phase 1 done initiator id 192.168.205.151 responder id mgateway.dyndns.org
20090630 104525 Default [SA Gateway-2-Tunnel3-P2] SEND phase 2 Quick Mode [HASH] [SA] [KEY EXCH] [NONCE] [ID] [ID]
20090630 104527 Default [SA Gateway-2-Tunnel3-P2] RECVR phase 2 Quick Mode [HASH] [SA] [KEY EXCH] [NONCE] [ID] [ID]
20090630 104527 Default [SA Gateway-2-Tunnel3-P2] SEND phase 2 Quick Mode [HASH]
20090630 104555 Default [SA Gateway-2-F1] RECVR phase 2 Quick Mode [HASH] [ID] [NOTIFY] type DPD R U THERE
20090630 104555 Default [SA Gateway-2-F1] SEND phase 2 Quick Mode [HASH] [ID] [NOTIFY] type DPD R U THERE ACK
4 Setup Radius Server (Windows 2003 Server)

4.1 Add New Radius Client

Add Radius Client

Configure Radius Client
4.2 Set the Secret Key
5  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.

5.1  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/)).
6 VPN IPSec Troubleshooting

6.1 « 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.

6.2 « 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.

6.3 « 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.

6.4 « received remote ID other than expected » error

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.
6.5 « 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:

6.6 « 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 an IPV4_ADDR type (and not a IPV4_SUBNET type).

6.7 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).

6.8 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.
7 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