

How To | Create a VPN, (including dynamic DNS) between Apple products running Mac OS X and an Allied Telesis Router

Introduction

Allied Telesis embraces the Internet as a standards driven environment where maximised inter-operability to a range of different Internet-vendor devices is important. Virtual Private Networks (VPNs) is an example of an inter-networking technology where this inter-operability is very important.

This How To note details one of the inter-operation solutions from Allied Telesis: creating Virtual Private Networks between Allied Telesis routers and a Mac OS X device, or **iPhone**, including Dynamic DNS.

Windows XP clients are also compatible with the router configuration shown. Refer to: *How To Create a VPN between an Allied Telesis Router and a Microsoft Windows XP1 Client, over NAT-T*, located at: http://www.alliedtelesis.com/media/datasheets/howto/conf_vpn_natt_xp_sd_e.pdf



List of terms:

DNS

Domain Name System - the Internet system that translates human-understandable hostnames (like www.dyndns.com) into computer-understandable IP addresses (like 204.13.248.117) and back again.

Collision domain

A physical region of a local area network (LAN) in which data collisions can occur.

Broadcast domain

A section of an Ethernet network comprising all the devices that will receive broadcast packets sent by any device in the domain. Separated from the rest of the network by a Layer 3 switch.

VLAN classification

A packet can be allocated VLAN membership based on its protocol, subnet, or port.

What information will you find in this document?

The configuration is described in the following sections:

Introduction	1
What information will you find in this document?	2
Related How To Notes	2
Which products and software version does it apply to?	3
Some points to note about the solution	3
NAT-Traversal	3
Dynamic-DNS	3
Scalability /Robustness	4
Compatibility Issues	4
Network diagram	4
Configuring the Allied Telesis router	5
Initial security	5
VPN configuration	6
How to configure a Dynamic DNS service	14
Setting up a DNS Service	14
Configuring the VPN Client on Mac OS X 10.5 (Leopard) or later version	21
Compatibility Issues	21
Setup steps	21
Test the connection	26
Configuring an iPhone VPN	28
Troubleshooting your iPhone VPN	30
General troubleshooting	31

Related How To Notes

Allied Telesis offers How To Notes with a wide range of VPN solutions, from quick and simple solutions for connecting home and remote offices, to advanced multi-feature setups.

These Notes also describe how to create a VPN between an Allied Telesis router and equipment from a number of other vendors. A summary of these solutions, can be seen in the Overview of VPN Solutions in How To Notes document in the How To Library at www.alliedtelesis.com/resources/literature/howto.aspx.

The collection includes Notes that describe how to interoperate with Windows 2000, XP and Vista VPN Clients

Which products and software version does it apply to?

This solution is compatible with:

- AR415S
- AR440S, AR441S, AR442S
- AR750S, AR750S-DP, AR770S
- AlliedWare version 291-20 or later (version 291-20 or later provides the best provision for the example given in this How To note - a VPN to a dynamically assigned WAN interface where the router includes a NATing Firewall).
- Mac device running OS X 10.5 or later.

Some points to note about the solution

Here are some items to keep in mind as you go through the details of the solution.

NAT-Traversal

This solution also supports ISAKMP NAT-Traversal, which allows VPN access for any NAT-T supporting client located behind a NAT gateway. NAT gateways are commonly used by many networks, such as corporate and accommodation locations, that travelling staff may visit, and also home networks - for staff needing work access from home.

NAT devices are installed to alleviate the exhaustion of the IPv4 address space by allowing the use of private IP addresses on home and corporate networks (internal networks) behind routers with a single public IP address facing the public Internet. Support for NAT-T is often essential for today's VPN needs.

Dynamic-DNS

The router connection with your Internet Provider may be a fixed or dynamically assigned IP address.

This How To Note demonstrates a situation where the Internet Provider connection (your WAN interface) is **dynamically** assigned an IP address. Traditionally, all VPN Access Concentrators had to have a fixed IP address defined on their WAN interface. Dynamic allocation of WAN IP addresses necessitates using the Dynamic DNS (DDNS) facility so that VPN Clients can connect to the VPN server by looking up a Fully Qualified Domain Name address, rather than nominating the traditional fixed IP address.

This How To Note demonstrates a DDNS setup example. For a thorough introduction to DDNS and for information about debugging DDNS, please refer to: *How To Use Dynamic DNS To Allow You To Host Servers Behind A Dynamically-Assigned Public IP Address*, available at: http://www.alliedtelesis.com/media/datasheets/howto/dns-host-servers_sd_a.pdf

Scalability /Robustness

This solution has also been tested for multiple clients connecting simultaneously, and for reconnection robustness.

Compatibility Issues

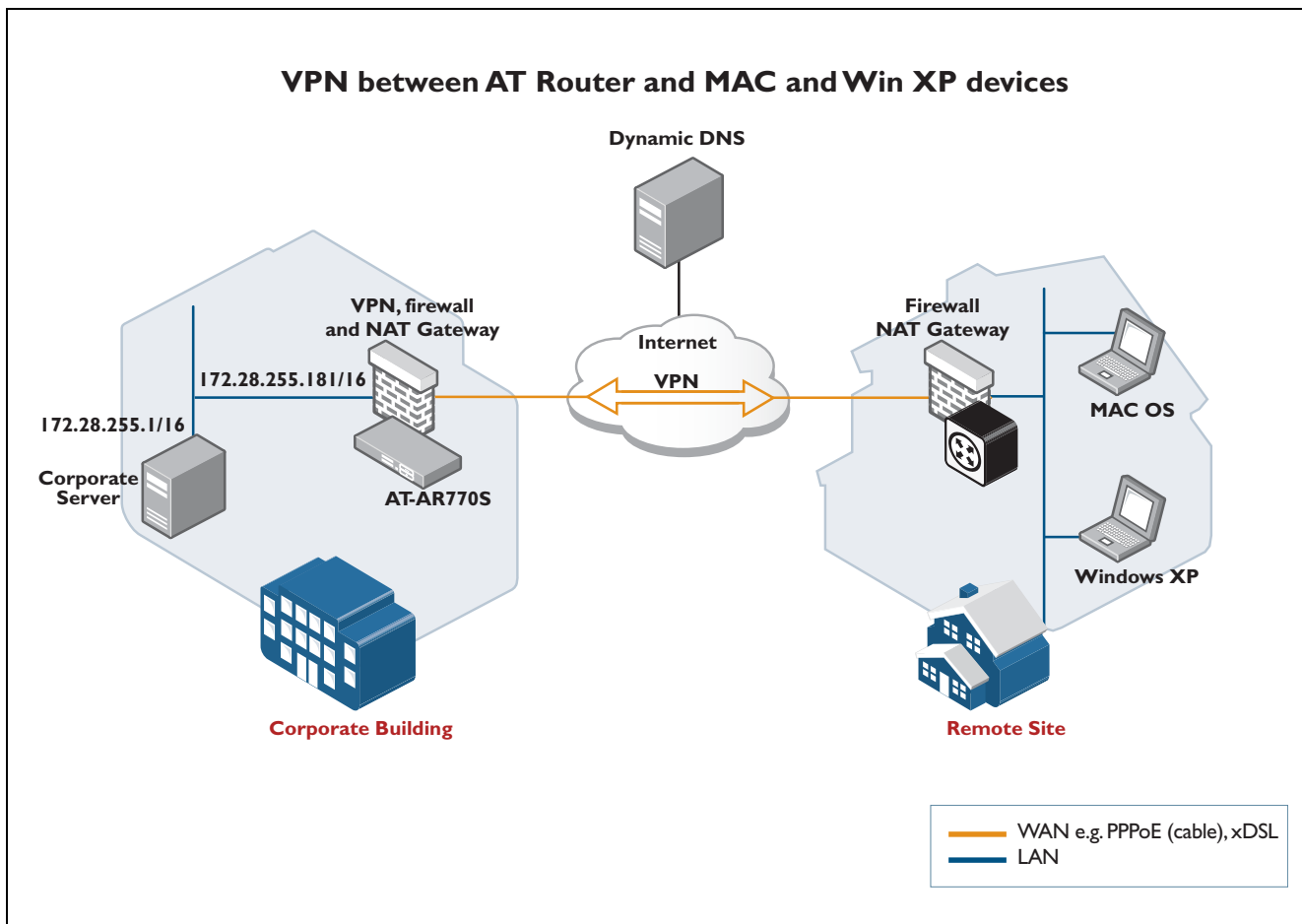
ISAKMP Delete Messages

Note that this solution (tested on OS X 10.5) has the sending of ISAKMP Delete messages disabled for compatibility reasons. Mac OS X 10.6 (Snow Leopard) introduces support for ISAKMP Delete messages, therefore if you have this version or later it is recommended to enable the ISAKMP Delete messages. See the router ISAKMP configuration section for more comments.

Support for NAT-T

For full inter-operable support of NAT-T we recommend using Mac OS X 10.5 or later. However, if you do not need NAT-Traversal in your VPN solution, we have tested and proven that Mac OS X 10.3 and later can successfully provide a non-NATT IPsec VPN solution.

Network diagram



Configuring the Allied Telesis router

This configuration section is divided into two parts:

- Initial security
- VPN configuration

Note: You will need an appropriate 3DES or AES feature license. Use the command **show feature** to check. Contact your distributor for license sales. e.g. AT-AR-3DES

Initial security

Before the main VPN configuration, you need to set up System Security Mode. This sets the router into a more secure mode, and ensures that encryption keys are preserved over power-cycles.

1. Define a security officer.

```
add user=secoff password=<your-password> priv=securityofficer
```

This command must be in the configuration script as well.

2. Enable system security.

```
enable system security
```

Unless you do this, rebooting the router destroys encryption keys.

3. Log in as the security officer (provide password when prompted).

```
login secoff
```

4. Create an encryption key for use as the ISAKMP pre-shared key.

```
create enco key=1 type=general value=<alphanumeric-string>
```

Note: Record the value of the string you have entered so that you can load it on the PC clients. This shared key will be used to encrypt ISAKMP negotiation.

5. Create additional keys for SSH if you want secure remote access to the router.

```
create enco key=2 description="Server Key" type=rsa length=768
  format=ssh
create enco key=3 description="Host Key" type=rsa length=1024
  format=ssh
```

Refer to the Secure Shell chapter and example in your router's Software Reference for more information.

6. Save your initial configuration.

```
create conf=vpn.cfg
set conf=vpn.cfg
```

VPN configuration

1. Define a suitable router system name.

```
set system name="VPN Gateway for iMac client"
```

2. Optionally, extend Security Officer inactivity timeout delay.

```
set user securedelay=600
```

The default is 60 seconds. During setup you can instead use 600 seconds if desired.

3. Ensure a Security Officer has been added.

```
add user=secoff password=<your-password> priv=securityofficer
set user=secoff telnet=yes login=yes
```

As mentioned above, your configuration must include a security officer user definition.

4. Define users for incoming VPN calls.

```
add user=vpnuser1 pass=friend1 login=no telnet=no
set user=vpnuser1 ipaddr=192.168.8.50 netmask=255.255.255.255
add user=vpnuser2 pass=friend2 login=no telnet=no
```

The incoming L2TP /VPN calls will be CHAP authenticated. They may be authenticated against the router's user database as configured above, or against a RADIUS server if configured. IP addresses will be assigned from the IP Pool, or you can assign individual

addresses to individual users using the router user database or your Radius server. IP addresses defined in the user database or Radius Server take precedence over the IP pool addresses.

5. Optionally, add a RADIUS server address.

```
add radius server=<RADIUS-server-address> secret=<secret-key>
```

6. Optionally set a faster console port speed.

```
set asyn=asyn0 speed=115200
```

If desired, the speed of the console terminal port can be set faster - useful if you intend to use ISAKMP or other debugging. The default speed of the asynchronous port is 9600 bps.

7. Create a PPP Template to accommodate incoming VPN /PPP calls.

```
create ppp template=1 bap=off ippool="myippool" mssheader=120  
set ppp template=1 authentication=chap echo=30 lqr=off
```

All dynamic incoming L2TP calls will associate with this PPP template. It is recommended to use the PPP echo mechanism, rather than LQR, to detect if the link is still up.

8. Enable an L2TP Service.

```
enable l2tp  
enable l2tp server=both  
add l2tp ip=1.1.1.1-255.255.255.254 pptemplate=1
```

This service will allow the dynamic creation of the incoming VPN /L2TP calls. It is associated with the PPP Template 1.

9. Create a suitable WAN Interface.

```
create ppp=0 over=eth0-any bap=off iprequest=on  
set ppp=0 username="internet1" password="internet1"  
set ppp=0 over=eth0-any lqr=off echo=10
```

This example illustrates PPPoE as the WAN interface. Your WAN interface may be something else such as a VLAN, Ethernet port, PPP over ATM /xDSL, or another interface type. Other VPN How To notes have examples of other WAN interface types, or refer to the Software Reference Manual.

10. Configure IP Protocol.

```
enable ip
enable ip remote
```

This is the public WAN interface.

```
add ip int=ppp0 ip=0.0.0.0 mask=0.0.0.0
```

This is the private LAN interface.

```
add ip int=vlan1 ip=172.28.255.181 mask=255.255.0.0
add ip route=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0
```

11. Optionally, add an IP filter to block NetBIOS traffic.

```
add ip filt=1 source=0.0.0.0 entry=1 act=exclude prot=udp
dp=137:138
```

Typically NetBIOS traffic should be contained in the local LAN and should not need to be routed. This filter will stop, what is often a chatty protocol, from appearing in the Firewall session list, and from unnecessarily consuming available firewall sessions.

12. If filtering, add an **include-all-else** filter entry.

Any IP filter ends with an implied **exclude all else** entry. In this case, we only want NetBIOS filtered, therefore we need an **include all else** entry

```
add ip filt=1 source=0.0.0.0 entry=2 act=include
```

Add the filter to the local interface.

```
set ip int=vlan1 filter=1
```

Note: Filter activity can be inspected with the **show ip filter** command.

13. Create the IP Pool for VPN addresses.

```
create ip pool="myippool" ip=<your ip pool range of addresses eg:
192.168.8.1-192.168.8.10>
```

The IP pool addresses are the internal address ranges you want to allocate to your VPN clients (e.g. ip=192.168.8.1-192.168.8.254). Remember that any individual user addresses defined in the user database or RADIUS Server will take precedence over these IP pool addresses.

14. Optionally, add a DNS Server address.

```
add ip dns primary=<your preferred dns server address>
```

Any defined DNS Server address will also be allocated to the incoming VPN /PPP calls.

Note: Even if you do not configure a DNS address here, any DNS address that this router has dynamically learnt through its dynamic WAN interface will also be allocated to the incoming VPN /PPP calls. Therefore, it is possible for these incoming VPN calls to browse the Internet via this VPN gateway router.

15. Enable Firewall Protection.

This example also sets up a Firewall with Network Address Translation (NAT) facilities. These are optional, but are recommended especially if the VPN Router also serves as your Internet gateway.

```
enable firewall
create firewall policy="net"
```

This example enables any firewall denied activity to be logged, and it allows any ICMP traffic (such as ping) to be forwarded.

```
enable firewall policy="net" log=deny
enable firewall policy="net" icmp_forward=all
```

16. Create a Firewall Dynamic User Template to cater for incoming authenticated dynamic calls.

```
create firewall policy="net" dynamic=roaming
add firewall policy="net" dynamic=roaming user=any
```

This will ensure that the dynamic PPP interfaces created over incoming L2TP calls will be automatically added to the firewall as dynamic interfaces.

17. Add the public and private interfaces to the Firewall.

```
add firewall policy="net" int=vlan1 type=private
add firewall policy="net" int=ppp0 type=public
```

18. Add the dynamic interface template to the Firewall.

```
add firewall policy="net" int=dyn-roaming type=private
```

This determines that the dynamic firewall interfaces will be private interfaces of the firewall.

19. Add the Network Address Translation Interface Relationships.

```
add firewall poli="net" nat=enhanced int=vlan1 gblint=ppp0
add firewall poli="net" nat=enhanced int=dyn-roaming gblin=ppp0
```

This includes a NAT relationship for any trusted dynamic interfaces.

20. Add Firewall Allow Rules for ISAKMP and NAT-T Traffic.

```
add firewall poli="net" rule=1 act=allo int=ppp0 prot=udp
port=500 ip=0.0.0.0 gblip=0.0.0.0 gblport=500
add firewall poli="net" rule=2 act=allo int=ppp0 prot=udp
port=4500 ip=0.0.0.0 gblip=0.0.0.0 gblport=4500
```

Note: These rules use the 0.0.0.0 address place holder to represent that the dynamically assigned WAN interface address will be applied when it is learnt from the ISP. In this case, both the global IP and local IP fields will apply the dynamic WAN address, meaning that this traffic will not be NAT translated by the firewall. This is important to allow NAT-T to operate, especially if there is also a server-end NAT gateway external to this device. Release 29I-20 added support for ip=0.0.0.0.

21. Add Firewall Allow Rule for L2TP traffic that has been IPsec encoded.

```
add firewall poli="net" rule=3 act=allo int=ppp0 prot=udp
port=1701 ip=0.0.0.0 gblip=0.0.0.0 gblport=1701 enc=ipsec
```

The command **enc=ipsec** ensures that ONLY L2TP traffic that was decoded by the IPsec module will be permitted. Raw L2TP traffic from the Internet will be denied.

22. Add Firewall **nonat** rules for any VPN payload traffic.

The internal VPN addresses need to be exempt from any NAT translations, so **nonat** rules are used. There should be one rule for the public interface and one rule for the private interface.

```
add firewall poli="net" rule=4 action=nonat int=ppp0 prot=ALL
enc=ips
```

```
add firewall poli="net" rule=5 action=nonat int=vlan1 prot=ALL
ip=172.28.0.0-172.28.255.254
```

Ensure you include all the addresses that could be assigned to your VPN Clients in the **remoteip** field below. Include both ip pool, and individual user ip assignments from the user database or RADIUS.

```
set firewall poli="net" rule=5 REMoteip=<range of addresses that
may be allocated to your VPN Clients, eg: 192.168.8.1-
192.168.8.50>
```

23. Optionally, enable SSH server.

```
enable ssh server serverkey=2 hostkey=3 expirytime=12
logintimeout=60
add ssh user=secoff password=<secoff password> ipaddress=<trusted
remote ip>
```

Note: We recommend you use Secure Shell for remote management. Telnet should **not** be used to a secure gateway.

If secureshell access will be permitted from a trusted host on the Internet, you will need to add a firewall allow rule for secureshell port 22 TCP. For example:

```
add firewall poli=net rule=6 action=allow int=ppp0 prot=tcp
port=22 ip=0.0.0.0 gblip=0.0.0.0 gblpo=22
remoteip=<trustedhost>
```

24. Create a set of IPsec Security Association Specifications to cater for incoming VPN requests.

```
create ipsec saspec=1 key=isakmp prot=esp encalg=3desouter
hashalg=sha mode=transport
create ipsec saspec=2 key=isakmp prot=esp encalg=3desouter
hashalg=md5 mode=transport
create ipsec saspec=3 key=isakmp prot=esp encalg=des hashalg=sha
mode=transport
create ipsec saspec=4 key=isakmp prot=esp encalg=des hashalg=md5
mode=transport
```

The IPsec Protocol uses a proposal system, to maximise compatibility with a range of different vendors.

25. Create an IPsec proposal bundle.

```
create ipsec bundle=1 key=isakmp string="1 or 2 or 3 or 4"
```

The order is important, we need to propose the strongest encryption first.

26. Create IPsec permit policies for ISAKMP and NAT-T.

```
create ipsec policy="isakmp" int=ppp0 act=permit
set ipsec policy="isakmp" lport=500 rport=500
create ipsec policy="natt" int=ppp0 lport=4500 act=permit
```

These traffic types need to be permitted past the IPsec security module, so that the ISAKMP module and NAT-T facility can inspect them. Any NAT-T encapsulated IPsec traffic will be fed back to the IPsec module for decapsulation and decoding.

27. Create an IPsec encryption policy for the VPN /L2TP Client connections.

```
create ipsec policy="roaming" int=ppp0 act=ipsec key=isakmp
bundle=1 peer=ANY isakmp=roaming
set ipsec policy="roaming" lport=1701 transport=UDP
```

Even in the case of NAT-T translated connections, local port of 1701 should still be a distinguishing factor for VPN traffic.

28. Optionally, create an Internet access permit policy.

```
create ipsec policy="internet" int=ppp0 act=permit
```

If this router is also intended to be used for Internet access, you will need this open permit policy, so that all traffic not going over the VPN is just sent unencrypted to the Internet.

If it is not intended for Internet access and you don't include the permit policy shown above, but if secureshell access is intended from the Internet, then you will need an IPsec permit policy for secureshell TCP port 22.

29. Ensure the IPsec module has been enabled.

```
enable ipsec
```

30. Create an ISAKMP policy for the VPN Clients.

ISAKMP is the protocol used to negotiate IPsec Security Associations with the VPN Clients. NAT-Traversal is also enabled to provide support through NAT gateways. Note that the **senddelete** option is not enabled, to provide for support with Mac OS X 10.5 and earlier. Also note that you will need to run Mac OS X 10.5 or later if you need NAT-Traversal support.

```
create isakmp policy="roaming" peer=any encalg=3desouter key=1
set isakmp policy="roaming" group=2 natt=true sendnotify=true
```

If you are running OS X 10.6 or later, we recommend you enable send deletes to maximise VPN robustness.

```
set isakmp policy="roaming" senddeletes=true
```

31. Ensure the ISAKMP module is enabled.

```
enable isakmp
```

32. Save your final router configuration—enter the commands.

```
create conf=vpn.cfg
set conf=vpn.cfg
```

Note: The configuration above can also support incoming Windows XP clients, therefore supporting a mixed network where some clients are Mac and some Windows. Refer to the How To on setting up Windows XP VPN Clients.

How to configure a Dynamic DNS service

As mentioned earlier, the router connection with your Internet Provider may be a fixed IP address or a dynamically assigned IP address.

This How To Note demonstrates a situation where the Internet Provider connection (your WAN interface) is dynamically assigned an IP address. Traditionally all VPN Access Concentrators had to have a fixed WAN address so that the VPN peers had a known IP address to connect to. However, if you have a dynamic WAN address, then the VPN peers can connect via an FQDN address, if the router has a mechanism to dynamically update the IP for that FQDN address. This can be done through a service called DynDNS.

AlliedWare does provide mechanism to dynamically update, through a built in DynDNS Update Client. For a thorough introduction to DDNS and for information about debugging DDNS, please refer to:

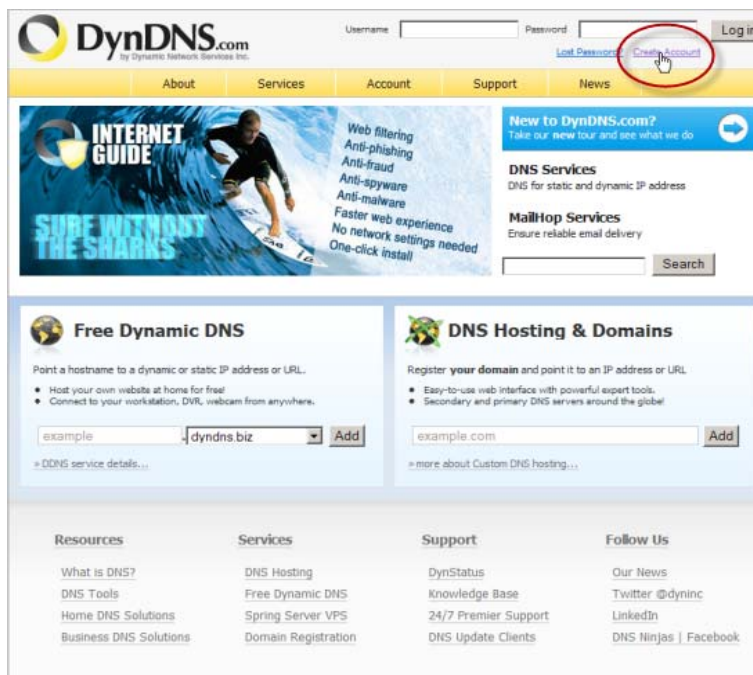
How To Use Dynamic DNS To Allow You To Host Servers Behind A Dynamically-Assigned Public IP Address

http://www.alliedtelesis.com/media/datasheets/howto/dns-host-servers_sd_a.pdf

Setting up a DNS Service

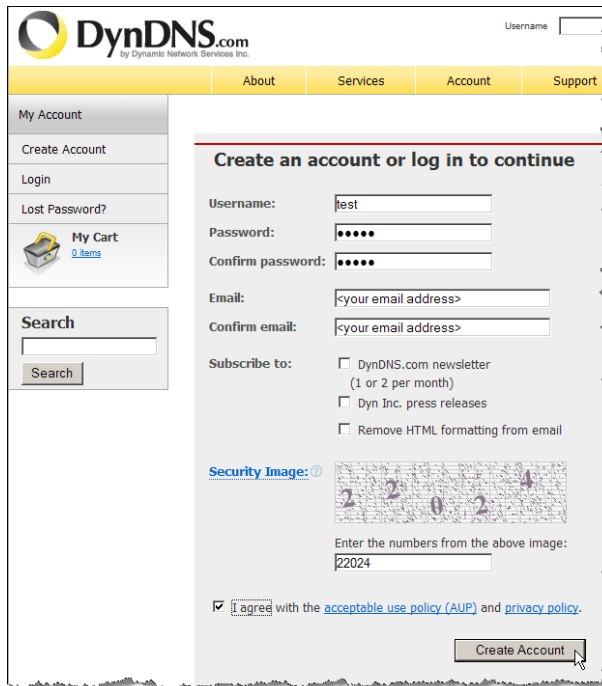
To set up a DDNS Service perform the following steps:

1. Go to the **DynDNS.com** website, and click **Create Account**.



2. Create an Account.

- Type in the account details.
- Click **Create Account**.



The screenshot shows the DynDNS.com account creation page. The page has a yellow header with the DynDNS.com logo and navigation links: About, Services, Account, and Support. On the left, there is a 'My Account' sidebar with links for 'Create Account', 'Login', 'Lost Password?', and 'My Cart' (0 items). Below the sidebar is a search box. The main content area is titled 'Create an account or log in to continue'. It contains the following fields and options:

- Username: test
- Password: [masked]
- Confirm password: [masked]
- Email: <your email address>
- Confirm email: <your email address>
- Subscribe to:
 - DynDNS.com newsletter (1 or 2 per month)
 - Dyn Inc. press releases
 - Remove HTML formatting from email
- Security Image: 2 2 0 2 4
- Enter the numbers from the above image: 22024
- I agree with the [acceptable use policy \(AUP\)](#) and [privacy policy](#).
- Create Account button

- After you have created the account, a confirmation email will be sent. Click on the link supplied in the confirmation email.
- If successful, you will be taken to an **Account Confirmation** page.



3. Login to your new account, and click **Add Host Services**.



4. Add the details for the new **Hostname**.

- Select a domain name from the drop-down list, and type in your desired **Hostname**.
- Select **Host with IP address**.
- Type in your router's current dynamic WAN **IP Address**.
- Click **Add to Cart** (this will be a free purchase).

A screenshot of the 'Add New Hostname' form. At the top, there is a note: 'Note: You currently don't have any active Dynamic DNS Pro upgrades in your account. You cannot use [?] features. Paying for an Dynamic DNS Pro upgrade will make this form fully functional and will add sev'. The form has several sections: 1. 'Hostname': A text input field containing 'Test51' and a dropdown menu showing 'dyndns.info'. A red arrow points to the text input. 2. 'Wildcard Status': A label 'Disabled' with a link '[Want Wildcard support?]'. 3. 'Service Type': Three radio button options: 'Host with IP address [?]' (selected), 'WebHop Redirect [?]', and 'Offline Hostname [?]'. A red arrow points to the selected radio button. 4. 'IP Address': A text input field containing '<your current WAN address>'. Below it, there is a link 'Use auto detected IP address 202.49.72.33.' and a note 'TTL value is 60 seconds. Edit TTL.'. 5. 'Mail Routing': A checkbox labeled 'Yes, let me configure Email routing. [?]'. 6. At the bottom right, there is a grey 'Add To Cart' button with a red arrow pointing to it.

5. Confirm the details of your Shopping Cart Purchase.

The **Order Total** should be \$0.00.

Shopping Cart

test51.dyndns.info added to cart. **You must checkout to activate.**

Your cart contains **free services only**. You will not be asked for credit card information.

Upgrade Options

Free accounts allow only five Dynamic DNS hosts.
• To add more and enjoy **additional benefits** for only \$15.00 per year, [purchase Dynamic DNS Pro](#).
• To get Dynamic DNS for **your own domain**, use [Custom DNS](#).

Dynamic DNS Hosts

test51.dyndns.info	-	remove	\$0.00
------------------------------------	---	--------	--------

Please enter coupons in the box below and click "Add Coupon".

Sub-Total: **\$0.00**

Order Total: **\$0.00**

Would you like to [print an estimate/quote](#)?

6. Activate the service.

- Click **Activate Services**

Free Services Checkout

Once you have confirmed the contents of your cart your services will be instantly activated.

Service	Period	Price
Dynamic DNS Hosts		
test51.dyndns.info	-	\$0.00
Sub-Total:		\$0.00

[view our refund policy](#)

7. Confirm the details of your activated account.

DynDNS.com by Dynamic Network Services Inc.

Logged In User: [carin](#)
[My Cart](#) [My Services](#) [Log Out](#)

About Services Account Support News

My Account **Host Services** [Add New Hostname](#) - [Host Update Logs](#)

[test51.dyndns.info](#) successfully activated.

Hostname	Service	Details	Last Updated
test51.dyndns.info	Host	<your current WAN address>	Nov. 02, 2009 3:37 PM

8. Configure the router for the DDNS Service.

Ensure that the router has a valid DNS Server configured, or that it has been able to dynamically learn a DNS Server address.

Either **add** a fixed DNS Server.

```
add ip dns primary=<your preferred dns server address>
```

Or use the **show** command to confirm you have dynamically learnt a DNS server address.

```
show ip dns
```

9. Enable and configure the dynamic DDNS update service on the router.

```
enable ddns  
set ddns dynamichost=<your ddns URL eg: test.dyndns.org>  
set ddns primaryinterface=ppp0  
set ddns user=<your ddns account username>  
set ddns password=<your ddns account password>
```

10. Testing DDNS Functionality.

Ensure that your WAN interface is up and has had a dynamic IP address assigned.

There are a couple of ways to confirm if a dynamically assigned WAN address has been correctly updated to the DDNS Server.

As shown below, the DDNS Operation Information section of the command **show ddns** will confirm the server details and the last time DDNS was updated.

```

SecOff VPN Gateway for iMac client> show ddns

DDNS Config Information:
  Client State ..... ENABLED
  Debug ..... DISABLED
  Server ..... members.dyndns.org
  Port ..... 80
  User ..... <your username>
  Password ..... ****
  system name ..... dyndns
  hosts ..... <your ddns URL>
  Wildcard ..... off
  Offline ..... no
  Primary WAN Interface ..... ppp0
  Secondary WAN Interface ..... none

DDNS Operation Information:
  Server IP ..... 204.13.248.112
  IP in DynDns ..... <your dynamic address>
  Current IP ..... <your dynamic address>
  Last update time ..... 3934

```

The router's log will also display if the Dynamic DNS update was successful.

```

SecOff VPN Gateway for iMac client> sh log module=ddns

Date/Time   S Mod  Type  SType Message
-----
09 13:03:33 5 DDNS MSG   INFO  Dynamic DNS update succeed. Host
                                     <your ddns URL> is <your dynamic address>.

```

If desired, you can also **enable ddns debugging**. A successful connection will look similar to this. Look for "result=0x00000001" at the end.

```

SecOff VPN Gateway for iMac client>
ddnsIpDNSsetupNotify
ddnsIpgSetDynamicIpAddrNotify int=ppp0, ip=<your dynamic address>

ecOff VPN Gateway for iMac client>
ddnsReadDdnsRecord:
DynDns record file read IP=<your dynamic address>, unicode=0x44444353
ddnsIpDNSServerName
ddnsIpDNSCallback server ip 204.13.248.112
idleflag=0x00000030, result=0x01000000
ddnsStartRequest
ddnsHttpCreateRequestHeader
[cont...]

```

```
ddnsHttpClientCallback sessionId=0x010d2c5c statusCode=200
ddnsHttpClientCallback sessionId=0x010d2c5c statusCode=1
HTTP Done
ddnsProcessReturnCodeTop
return code:
11
good <your dynamic address>
0

search for numhost
search for dnserr
search for 911
search for badsys
search for badagent
search for badauth
search for !donator
search for good from 11
search for nochg from 11
search for notfqdn from 11
search for nohost from 11
search for !yours from 11
search for abuse from 11
search for good from good <your dynamic address>
Host <your ddns URL> is <your dynamic address>.
search for good from 0
search for nochg from 0
search for notfqdn from 0
search for nohost from 0
search for !yours from 0
search for abuse from 0
result=0x00000001
action=0x00000000
ddnsProcessUpdateResult
```

Configuring the VPN Client on Mac OS X 10.5 (Leopard) or later version

These instructions apply to an appropriate PowerBook, iMac, or any device running Mac OS X 10.5 or later. The instructions should also be equivalent for an iPhone running iPhone OS 3.1 or later.

Compatibility Issues

Please refer to the earlier section titled: "[Compatibility Issues](#)" on page 4.

Setup steps

- Ensure your iMAC has a valid network gateway or Internet access.
- Ensure you know the IP address (or FQDN address) of the IPsec Server, in this case the AR router configured for IPsec.

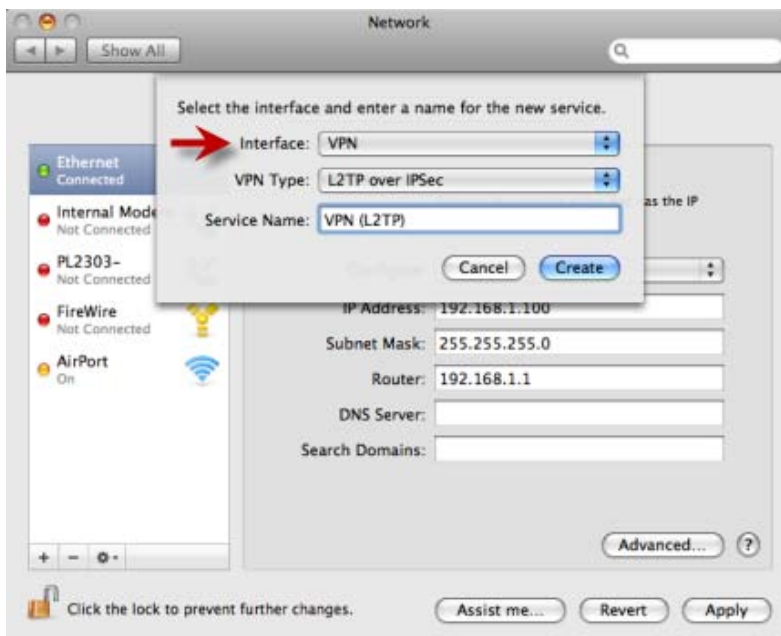
1. In the Apple **Network Control Panel** choose: **System Preferences > Network**.



The **Network** window will open.

2. Make a new connection.

- In the **Network** window, there is a list of network connections on the left side.
- Click the '+' icon to make a new connection for the VPN.

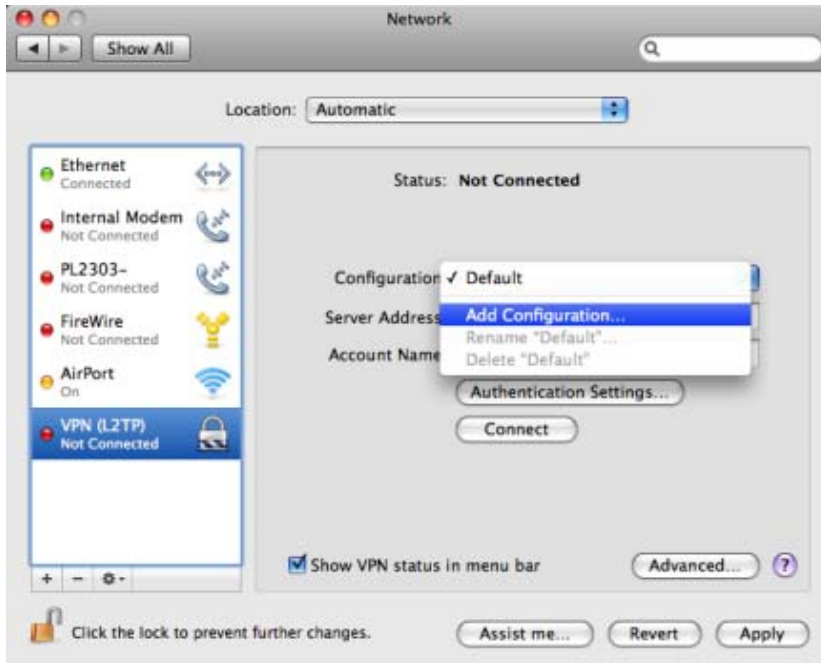


- Select **VPN** from the **Interface** drop down list.
- Select **L2TP over IPSec** as the **VPN Type**.
- You may change the **Service Name** field to name your connection.
- Click **Create** to finish.

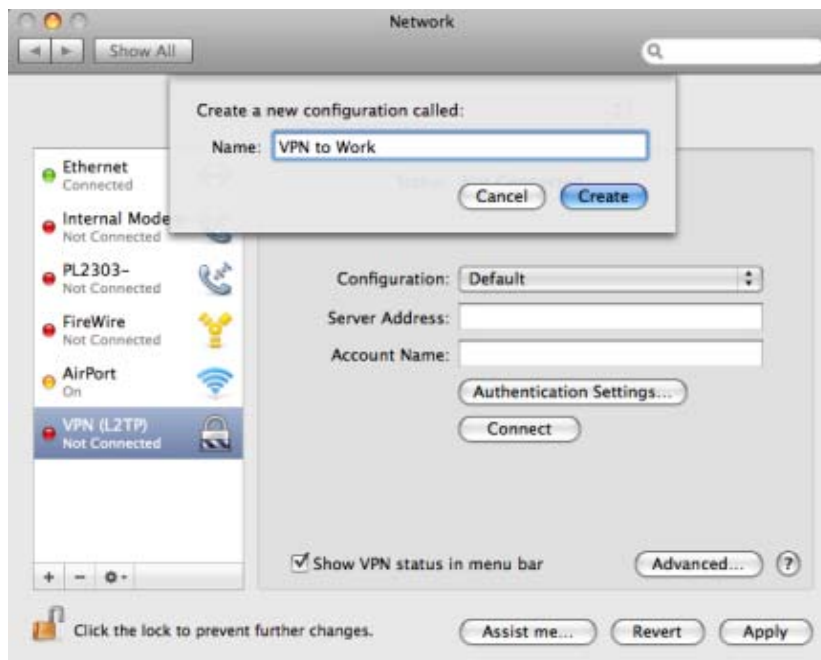
3. Make a new configuration.

Now that you have a VPN connection, you'll need to make a configuration for it.

- Select **Add Configuration...** from the **Configuration** drop down list.



- Type in a **Name** to identify the VPN by - e.g. *VPN to Work*.



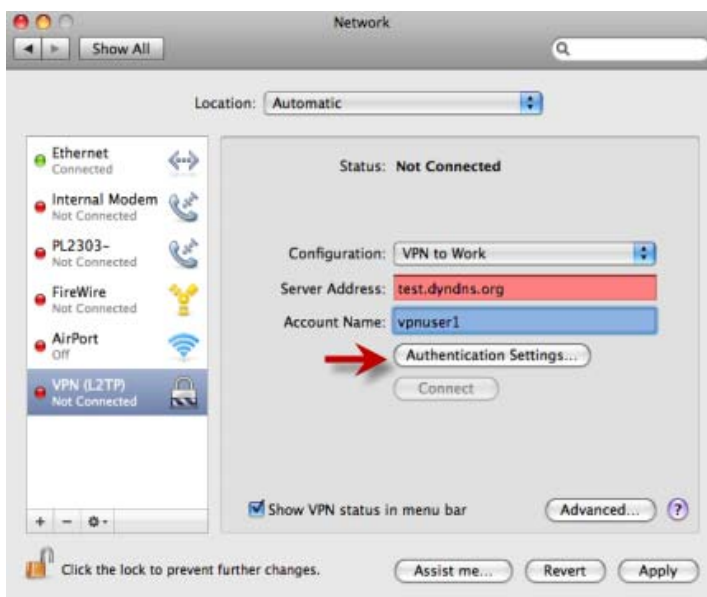
4. Set Server and Account information.

Now that we've created the configuration, we can start entering your VPN information.

- Type in the IP address or URL as the **Server Address** (in the red box).
- Type in the Username of this VPN client as the **Account Name** (in the blue box).

This is the user name that the MAC will send for PPP authentication. It must be the same as one of the user names configured on the AR router with the **add user** command, or it must be one of the usernames stored on the RADIUS server, if the AR router is configured to use RADIUS for user authentication.

- Click **Authentication Settings...** a new menu appears.



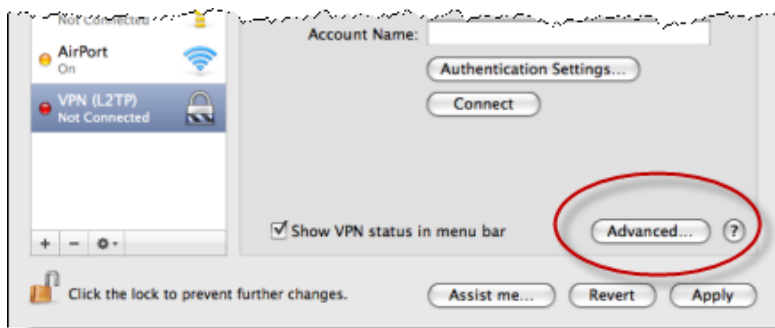
- Type in the **Password** for the VPN client (in the red box shown above).

This is the password that the MAC will send for PPP authentication. It must be the same as the password configured with the username on the AR router using the **add user** command, or it must be the password stored with the username on the RADIUS server, if the AR router is configured to use RADIUS for user authentication.

- Type in the **Shared Secret**, that you configured on the router as the enco key 1 (in the blue box shown above). Refer to "[Configuring the Allied Telesis router](#)", step 4 on page 5.
- Click **OK**.

5. Select the **Advanced** settings.

Next, we'll need to adjust some of the advanced VPN settings. To do that, first click the **Advanced...** button.



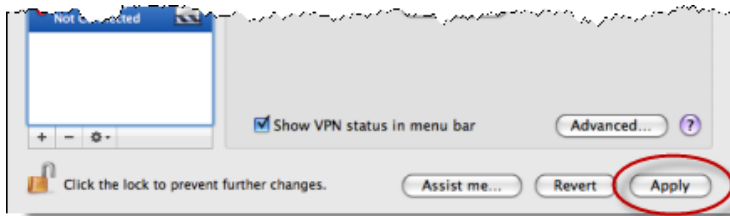
For the VPN to work effectively, select:

- **Send all traffic over VPN connection**
- Optionally, select **Use verbose logging**. That will make it easier to see what's happening if you are having connection problems.
- Click **OK**.



6. Apply the changes.

To actually save the configuration, click the **Apply** button in the bottom right of the window.



Test the connection

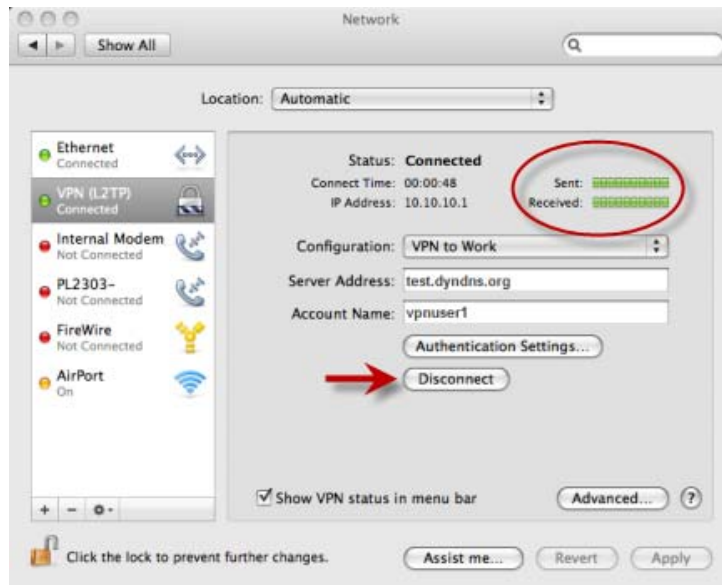
Now when you want to connect to the VPN, you can either choose the VPN configuration from the VPN menu, or in the **Network** window, select your VPN connection from the connection list at left, and click **Connect**.



- The connection is negotiating, and the rotating arrow progress icon is shown.



- The VPN connection **Status** is displayed as **Connected**.
- The **Sent** and **Received** green traffic bars indicate when the VPN connection is busy.



- When you are finished using the VPN Connection, click **Disconnect**.

Configuring an iPhone VPN

VPNs works over both Wi-Fi and cellular data network connections. iPhone and iPod touch support VPNs that use the L2TP, PPTP, or Cisco IPSec VPN protocols.

1. In the **Settings** screen, select **VPN ON**.

Once you've created a VPN configuration, the option to turn VPN on or off appears in the main Settings screen. When you are connected using VPN, the VPN icon appears in the status bar.



2. In the **General** screen, select **Network**.



3. In the **Network** screen, select **VPN** and **Add VPN Configuration**.

4. In the **Add VPN Configuration** screen, for IPsec over L2TP choose the **L2TP** tab.

The IPsec tab is for the inbuilt Cisco VPN client.

- Enter a **Description**, **Server** address, **Account** name, and **Password**. You can either enter a password here and have it saved, or if you leave the password blank, you will be prompted for the password on each connection (more secure).
- **Save** the configuration.

The screenshot shows the 'Add Configuration' screen for L2TP VPN. At the top, it says 'Enter your VPN account information.' Below this are 'Cancel' and 'Save' buttons. The 'L2TP' tab is selected, with 'PPTP' and 'IPSec' tabs also visible. The form contains the following fields and controls:

- Description**: Required (text input)
- Server**: Required (text input)
- Account**: Required (text input)
- RSA SecurID**: Toggle switch set to OFF
- Password**: Ask Every Time (text input)
- Secret**: (text input)
- Send All Traffic**: Toggle switch set to ON

You can also set up a manual or automatic **Proxy** if required while the VPN is connected.

The screenshot shows the 'Add Configuration' screen for Proxy settings. At the top, it says 'Enter your VPN account information.' Below this are 'Cancel' and 'Save' buttons. The 'Proxy' section is expanded, showing the following fields and controls:

- Password**: Ask Every Time (text input)
- Secret**: (text input)
- Send All Traffic**: Toggle switch set to ON
- Proxy**: Radio buttons for Off, Manual (selected), and Auto
- Server**: (text input)
- Port**: (text input)
- Authentication**: Toggle switch set to OFF

Troubleshooting your iPhone VPN

If you are unable to connect to your VPN connection, or if you see an alert that says "Shared Secret is missing," your VPN settings may be incorrect or incomplete. If you have questions about what your VPN settings are or what your Shared Secret key is, you should contact your network administrator or IT Department. For more information on setting up VPNs on an iPhone, go to the Apple support site located at: <http://support.apple.com/kb/HT1424>

General troubleshooting

Here are some useful general troubleshooting pointers:

- Re-check your configuration settings on the router and iMac client. Check that the pre-shared ISAKMP key and User password details are correct.
- A number of VPN debug modes are available on the router. The most useful command is:

```
enable isakmp debug.
```

It allows you to see how far negotiation proceeds.
- Other useful commands to confirm establishment is:

```
show isakmp sa, show ipsec sa, show ppp
```
- There is a VPN troubleshooting guide available on the Allied Telesis website, refer to: http://www.alliedtelesis.com/media/datasheets/howto/troubleshoot-vpn_sd_c.pdf

USA Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

© 2010 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. Allied Telesis is a trademark or registered trademark of Allied Telesis, Inc. in the United States and other countries. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.

C613-16148-00 REV B