Allied Telesis

How To | Configure An Allied Telesis Router For Multiple Microsoft® Point-to-Point Tunnelling Protocol (PPTP) Clients

Introduction

Point-to-Point Tunnelling Protocol (PPTP) is a networking protocol that allows you to securely transfer data from your travelling staff to your office network using a Virtual Private Network (VPN) across TCP/IP-based data networks.

PPTP is provided on a variety of Microsoft® Windows® platforms.

Which products and software version does it apply to?

This How To Note applies to the following products, running software version 2.7.1 or later:

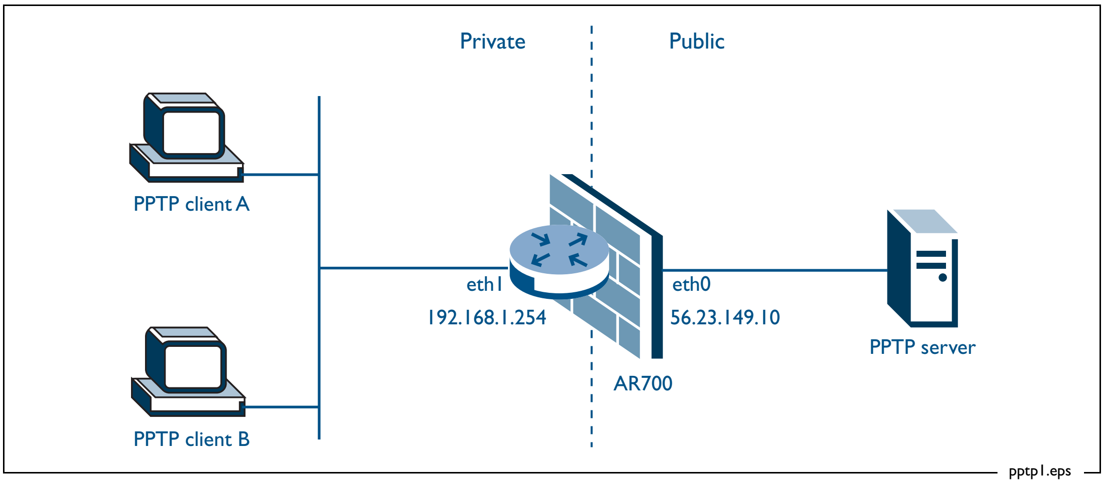
- AR400 and AR700 series routers
- Rapier, Rapier i, AT-8800 and AT-9800 series switches

Scenario

A PPTP session is initiated by a TCP connection from the client to port 1723 on the server. Then, the actual data transfer is performed on an unrelated GRE connection.

The AlliedWare firewall includes a PPTP proxy agent. This allows the firewall to manipulate, and keep track of, the 'session ID' fields in the packets belonging to different GRE sessions. The proxy agent supports multiple PPTP clients on the private side of the firewall, even if they are all connecting to a single PPTP server.

In this How To Note, we present the minimum configuration required to support the scenario illustrated in the following figure.



Configuration

The simple fact is that **no** specific configuration is required on the firewall to support multiple PPTP clients. So, a basic firewall NAT configuration is all that is required.

1. Configure IP

```
enable ip

add ip interface=eth0 ip=56.23.149.10 mask=255.255.255.248

add ip interface=eth1 ip=192.168.1.254 mask=255.255.255.0
```

2. Configure the firewall

```
enable firewall

create firewall policy=name

add firewall policy=name interface=eth0 type=public

add firewall policy=name interface=eth1 type=private

enable firewall policy=name icmp_forwarding=all

add firewall policy=name nat=enhanced interface=eth1
  gblinterface=eth0
```

Client connections from the public side

If you have a PPTP server on your private network, and you wish to allow external PPTP clients to establish connections to it from the public side, you need to configure a firewall rule to allow the PPTP sessions in through the firewall.

For example, if you had a PPTP server at 192.168.1.10 then you would need to configure rules like:

```
add firewall policy=name rule=1 interface=eth0 protocol=gre
   ip=192.168.1.10 gblip=56.23.149.10 action=allow

add firewall policy=name rule=2 interface=eth0 protocol=tcp
   port=1723 ip=192.168.1.10 gblip=56.23.149.10 gblport=1723
   action=allow
```