AlliedWare™ OS

How To | Configure Some Basic Firewall and VPN Scenarios

Introduction

This document provides examples that illustrate common configurations for security routers. You may want to make changes or enhancements to these configurations to customize them to your particular requirements. However, with the configurations provided here, you can be quickly operational with a reliable and secure Internet connection.

What information will you find in this document?

The first section provides the basic configuration for two likely methods that will be used for an Internet connection from the security router:

- "Script A: basic Ethernet connection" on page 3
- "Script B: basic PPPoE configuration" on page 7

The second section provides three extra configurations to enable the router to support three popular forms of Virtual Private Network (VPN) connection, followed by a configuration for a Mail server on a DMZ. One or more of these additional scripts can be added to either of the basic configuration scripts:

- "Script C: internal L2TP Network Server (LNS)" on page 11
- "Script D: IPsec tunnel" on page 13
- "Script E: PPTP server on LAN behind router" on page 16

Then the second section ends with an example in which private IP addresses are used on the DMZ LAN:

- "Script F: DMZ using private addresses" on page 17

These six configuration examples are as general as possible, and no actual IP addresses have been specified. IP addresses are represented by placeholder names in angled brackets, for example, <*dmz-ip-address*>.

These six partial configurations are included in six script files. Select the files you require, remove the configuration sections that do not apply to your network, and customise the remaining command parameters, such as IP addresses and passwords required for your network. One or more of the VPN service script files can be added to either of the basic configuration files.

Which products does this information apply to?

The information provided in this document applies to the following products:

- AR400 series routers
- AR700 series routers
- Rapier and Rapier i series switches

Related How To Notes

Allied Telesis offers How To Notes with a wide range of firewall and VPN solutions, from quick and simple solutions, to advanced multi-feature setups. Notes also describe how to create a VPN between an Allied Telesis router and equipment from a number of other vendors.

For other firewall solutions, browse the How To Library at www.alliedtelesis.com/resources/literature/howto.aspx. For a complete list of VPN How To Notes, see the *Overview of VPN Solutions in How To Notes* in the library.

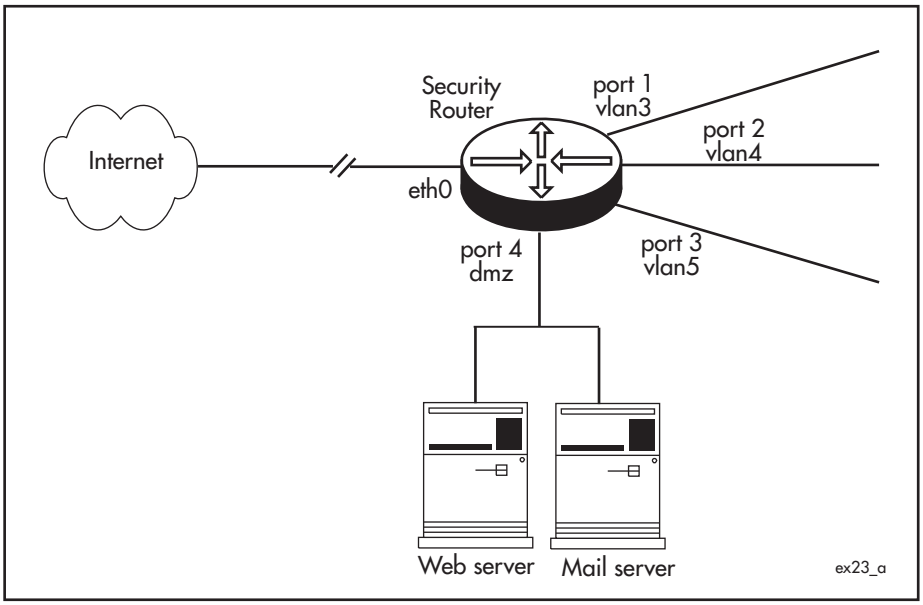
Basic configurations

Use one of the following basic configurations to connect your router to the Internet, with a standard firewall configuration.

The switch ports are all configured into separate VLANs, and the IP address for the Internet connection is learnt dynamically. These choices may not suit every user's requirements. However, the scripts can be easily altered to suit individual requirements. Some examples of variations are shown.

Script A: basic Ethernet connection

This is a basic configuration script for an Ethernet connection to the Internet, DMZ port, and partitioned LAN. The WAN IP address, the Gateway, and the Domain Name Server (DNS) are learnt by DHCP.



Configure Ethernet connection to Internet, DMZ port, and partitioned LAN, with DHCP

1. Configure the Internet connection

Enable IP on the router.

```
enable ip
```

Enable remote assignment so that the router can receive an IP address for the eth0 interface from a DHCP server.

```
enable ip remoteassign
```

Add an IP interface to eth0. Either set it to get its IP address by DHCP:

```
add ip interface=eth0 ipaddress=dhcp
```

Or, as a variation, assign a static IP address and a static default route to the eth0 interface and a DNS address.

```
add ip interface=eth0 ipaddress=<ip-address>
add ip route=0.0.0.0 interface=eth0 nexthop=<gateway-address>
set ip nameserver=<nameserver-address>
```

2. Configure the DMZ interface

Create a DMZ VLAN

```
create vlan=dmz vid=2
```

containing switch port 4.

```
add vlan=2 port=4
```

Assign the DMZ IP address to this VLAN.

```
add ip interface=vlan2 ipaddress=<dmz ip address>
```

3. Partition the LAN

Configure separate VLANs for each of switch ports 1, 2 and 3:

```
create vlan=vlan3 vid=3
create vlan=vlan4 vid=4
create vlan=vlan5 vid=5
add vlan=vlan3 port=1
add vlan=vlan4 port=2
add vlan=vlan5 port=3
```

Or, as a variation, add multiple ports to a single VLAN.

```
add vlan=vlan3 port=1,2
```

Assign IP addresses to the VLANs.

```
add ip interface=vlan3 ipaddress=<vlan3-ip-address>
add ip interface=vlan4 ipaddress=<vlan4-ip-address>
add ip interface=vlan5 ipaddress=<vlan5-ip-address>
```

4. Enable the firewall

Enable the firewall.

```
enable firewall
```

5. Configure a general firewall for LAN traffic

Create a firewall policy for traffic to and from the private LANs, and allow ICMP forwarding (PING).

```
create firewall policy=lans
enable firewall policy=lans icmp_forwarding=ping
```

Set eth0 and the DMZ VLAN (vlan2) to be public interfaces.

```
add firewall policy=lans interface=eth0 type=public
add firewall policy=lans interface=vlan2 type=public
```

Set the private LANs (vlan3, van4, vlan5) to be private interfaces.

```
add firewall policy=lans interface=vlan3 type=private
add firewall policy=lans interface=vlan4 type=private
add firewall policy=lans interface=vlan5 type=private
```

Set enhanced Network Address Translation (NAT) to translate IP addresses for traffic between the private VLANs and the public eth0 interface.

```
add firewall policy=lans nat=enhanced interface=vlan3
  gblinterface=eth0
add firewall policy=lans nat=enhanced interface=vlan4
  gblinterface=eth0
add firewall policy=lans nat=enhanced interface=vlan5
  gblinterface=eth0
```

6. Configure a general firewall for DMZ traffic

Create a firewall policy for traffic to and from the DMZ, and allow ICMP forwarding (PING).

```
create firewall policy=dmz
enable firewall policy=dmz icmp_forwarding=ping
```

Set eth0 and the private LANs (vlan3, van4, vlan5) to be public interfaces.

```
add firewall policy=dmz interface=eth0 type=public
add firewall policy=dmz interface=vlan3 type=public
add firewall policy=dmz interface=vlan4 type=public
```

```
add firewall policy=dmz interface=vlan5 type=public
```

Set the DMZ VLAN (vlan2) to be a private interface.

```
add firewall policy=dmz interface=vlan2 type=private
```

7. Allow selected traffic to the DMZ

The default *lans* and *dmz* firewall policies allow all traffic to flow between the private interfaces, and from the private to the public interfaces, but discards all traffic from public to private interfaces.

To allow particular kinds of traffic to flow from the public interface through the firewall to particular services on the DMZ, use one or more of the following firewall rules, or create other rules.

Allow HTTP traffic to the DMZ.

```
add firewall policy=dmz rule=1 action=allow interface=eth0
  protocol=tcp port=80 ip=<http-server-address>
```

Allow SMTP traffic to the DMZ.

```
add firewall policy=dmz rule=2 action=allow interface=eth0
  protocol=tcp port=25 ip=<mail-server-address>
```

Allow FTP traffic to the DMZ.

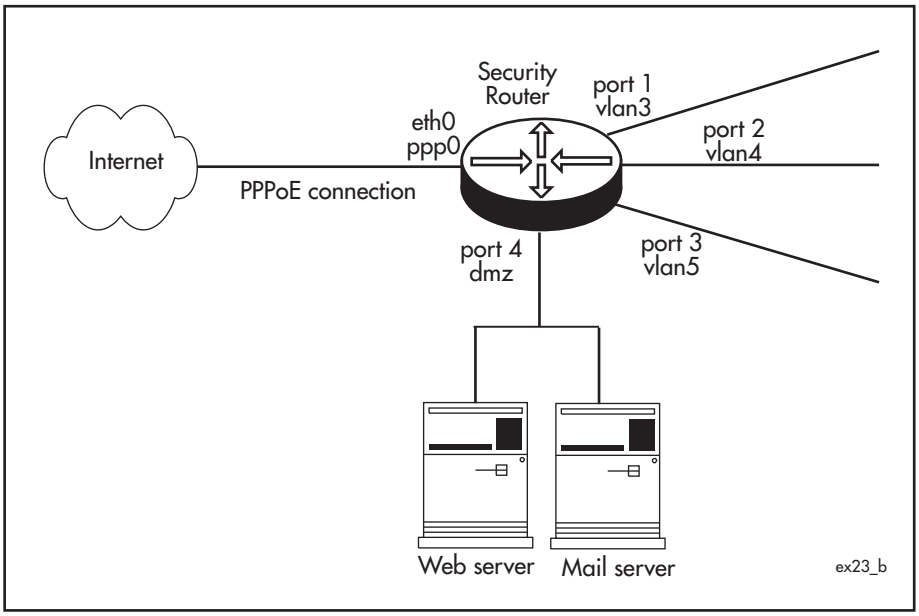
```
add firewall policy=dmz rule=3 action=allow interface=eth0
  protocol=tcp port=21 ip=<ftp-server-address>
```

Allow all traffic from the private LANs to the DMZ.

```
add firewall policy=dmz rule=10 action=allow interface=vlan3
  protocol=all
add firewall policy=dmz rule=11 action=allow interface=vlan4
  protocol=all
add firewall policy=dmz rule=12 action=allow interface=vlan5
  protocol=all
```

Script B: basic PPPoE configuration

This is a basic configuration script for a PPPoE (Point-to-Point Protocol over Ethernet) connection to the Internet, to a DMZ port, and to a partitioned LAN. The WAN IP address and Domain Name Server (DNS) are learnt by IPCP (Internet Protocol Control Protocol) negotiation.



Configure PPP over Ethernet connection to Internet, DMZ and partitioned LAN

1. Configure the Internet connection from eth0

Enable IP on the router.

```
enable ip
```

Enable remote assignment of IP addresses on the router for PPP interfaces with IP address 0.0.0.0.

```
enable ip remoteassign
```

Create a PPP interface over any PPPoE service on the eth0 interface. Set it to request an IP address during IPCP negotiation. Set the IDLE parameter to 36000 seconds (10 hours) so that the link will open on demand when there is data to send, in case the link is closed for any reason.

```
create ppp=0 over=eth0-any idle=36000 iprequest=on
```

Set the username and password that the ISP will use to authenticate the router for this PPPoE connection.

```
set ppp=0 username=<username> password=<password>
```

Give the PPP interface an IP address of 0.0.0.0 so that it can be assigned an IP address by IPCP, and a static default route.

```
add ip interface=ppp0 ipaddress=0.0.0.0
add ip route=0.0.0.0 interface=ppp0 nexthop=0.0.0.0
```

Or, as a variation, assign a static IP address and default route to the ppp0 interface, and do not set it to request an IP address.

```
create ppp=0 over=eth0-any idle=3600 username=<username>
  password=<password>
add ip interface=ppp0 ipaddress=<wan-ip-address>
add ip route=0.0.0.0 interface=ppp0 nexthop=0.0.0.0
```

2. Configure the DMZ interface

Create a DMZ VLAN

```
create vlan=dmz vid=2
```

containing switch port 4.

```
add vlan=2 port=4
```

Assign the DMZ IP address to this VLAN.

```
add ip interface=vlan2 ipaddress=<dmz-ip-address>
```

3. Partition the LAN

Configure separate VLANs for switch ports 1, 2 and 3.

```
create vlan=vlan3 vid=3
create vlan=vlan4 vid=4
create vlan=vlan5 vid=5
add vlan=vlan3 port=1
add vlan=vlan4 port=2
add vlan=vlan5 port=3
```

Or, as a variation, add multiple ports to a single VLAN.

```
add vlan=vlan3 port=1,2
```

Assign IP addresses to the VLANs.

```
add ip interface=vlan3 ipaddress=<vlan3-ip-address>
add ip interface=vlan4 ipaddress=<vlan4-ip-address>
add ip interface=vlan5 ipaddress=<vlan5-ip-address>
```

4. Enable the firewall

Enable the firewall.

```
enable firewall
```

5. Configure a general firewall for LAN traffic

Create a firewall policy for traffic to and from the private LANs, and allow ICMP forwarding (PING).

```
create firewall policy=lans
enable firewall policy=lans icmp_forwarding=ping
Set ppp0 and the DMZ VLAN (vlan2) to be public interfaces.
add firewall policy=lans interface=ppp0 type=public
add firewall policy=lans interface=vlan2 type=public
```

Set the private LANs (vlan3, van4, vlan5) to be private interfaces.

```
add firewall policy=lans interface=vlan3 type=private
add firewall policy=lans interface=vlan4 type=private
add firewall policy=lans interface=vlan5 type=private
```

Set enhanced Network Address Translation (NAT) to translate IP addresses for traffic between the private VLANs and the public ppp0 interface.

```
add firewall policy=lans nat=enhanced interface=vlan3
  gblinterface=ppp0
add firewall policy=lans nat=enhanced interface=vlan4
  gblinterface=ppp0
add firewall policy=lans nat=enhanced interface=vlan5
  gblinterface=ppp0
```

6. Configure a general firewall for DMZ traffic

Create a firewall policy for traffic to and from the DMZ, and allow ICMP forwarding (PING).

```
create firewall policy=dmz
enable firewall policy=dmz icmp_forwarding=ping
```

Set ppp0 and the private LANs (vlan3, van4, vlan5) to be public interfaces.

```
add firewall policy=dmz interface=ppp0 type=public
add firewall policy=dmz interface=vlan3 type=public
add firewall policy=dmz interface=vlan4 type=public
add firewall policy=dmz interface=vlan5 type=public
```

Set the DMZ VLAN (vlan2) to be a private interface.

```
add firewall policy=dmz interface=vlan2 type=private
```

7. Allow selected traffic to the DMZ

The default *lans* and *dmz* firewall policies allow all traffic to flow between the private interfaces, and from the private to the public interfaces, but discards all traffic from public to private interfaces.

To allow particular kinds of traffic to flow from the public interface through the firewall to particular services on the DMZ, use one or more of the following firewall rules, or create other rules.

Allow HTTP traffic to the DMZ.

```
add firewall policy=dmz rule=1 action=allow interface=ppp0
  protocol=tcp port=80 ip=<http-server-address>
```

Allow SMTP traffic to the DMZ.

```
add firewall policy=dmz rule=2 action=allow interface=ppp0
  protocol=tcp port=25 ip=<mail-server-address>
```

Allow FTP traffic to the DMZ.

```
add firewall policy=dmz rule=3 action=allow interface=ppp0
  protocol=tcp port=21 ip=<ftp-server-address>
```

Allow all traffic from the private LANs to the DMZ.

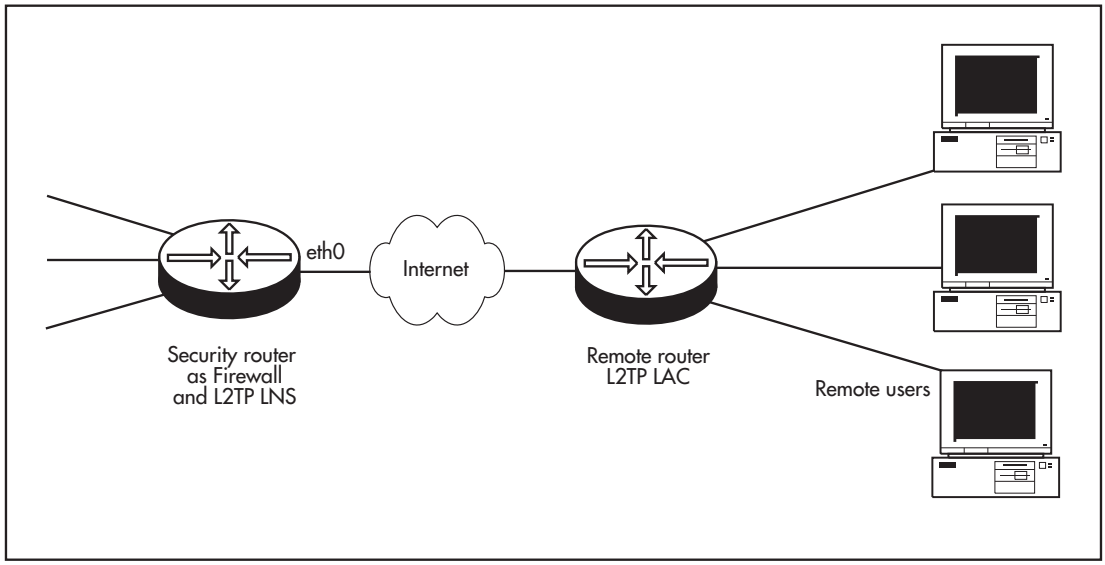
```
add firewall policy=dmz rule=10 action=allow interface=vlan3
  protocol=all
add firewall policy=dmz rule=11 action=allow interface=vlan4
  protocol=all
add firewall policy=dmz rule=12 action=allow interface=vlan5
  protocol=all
```

Additional configuration for VPN services

This section provides 3 partial configurations that can be appended to either of the basic scripts in the previous section in order to enable VPN connections into the site through the security router.

Script C: internal L2TP Network Server (LNS)

The router can act as an L2TP Network Server (LNS). In this example, the router is configured to create dynamic PPP interfaces when incoming L2TP connections are received. These interfaces are dynamically added to the firewall policy when they are created, to enable the data arriving via the L2TP tunnel to have access through the firewall.



Configure the router as an L2TP LNS

1. Configure a user

Add a user login name and password for the L2TP caller to the User Authentication Database, and do not allow this user to log into the router.

```
add user=<username-to-be-used-by-l2tp-caller> password=<password>
  login=no
```

Create a pool of IP addresses to be allocated to callers using L2TP.

```
create ip pool="l2tp" ip=<range-of-ip-addresses-to-be-allocated-
  to-l2tp-clients>
```

Create a PPP template to be used for PPP links opened by the L2TP calls, set it to use CHAP for authentication, and to use the IP pool created above for allocating IP addresses.

```
create ppp template=1 authentication=chap
set ppp template=1 ippool="l2tp"
```

2. Configure an L2TP tunnel

Enable L2TP, and both LNS and LAC modes.

```
enable l2tp
enable l2tp server=both
```

(This example configures LNS. Further configuration is required for the router to function as an L2TP Access Concentrator (LAC).)

Set the password to be used on L2TP tunnels.

```
set l2tp password=<password-to-be-used-on-l2tp-tunnels>
```

Specify the range of IP addresses from which the router should accept L2TP calls, and the PPP template to be used for these calls.

```
add l2tp ip=<ip-range-from-which-l2tp-connections-are-accepted>
  ppptemplate=1
```

3. Allow the L2TP traffic through the firewall

Create a firewall rule to allow L2TP traffic through the firewall to the private LANs.

Either, if the L2TP connection is over a PPPoE connection ("Script B: basic PPPoE configuration" on page 7):

```
add firewall policy=lans rule=1 interface=ppp0 protocol=udp
  port=1701 action=nonat
```

or, for a direct connection over eth0 ("Script A: basic Ethernet connection" on page 3):

```
add firewall policy=lans rule=1 interface=eth0 protocol=udp
  port=1701 action=nonat
```

4. Allow the traffic from the ppp0 link over the tunnel through the firewall

Add a dynamic interface template *l2tp* to the firewall policy *lans*.

```
create firewall policy=lans dynamic=l2tp
```

Add the L2TP caller's user name to the dynamic interface template.

```
add firewall policy=lans dynamic=l2tp user=<username-to-be-used-
  by-l2tp-caller>
```

Add the dynamic interface to the policy as a private interface, so that traffic is allowed between this dynamic interface and the other private interfaces defined in the basic configuration.

```
add firewall policy=lans interface=dyn-l2tp type=private
```

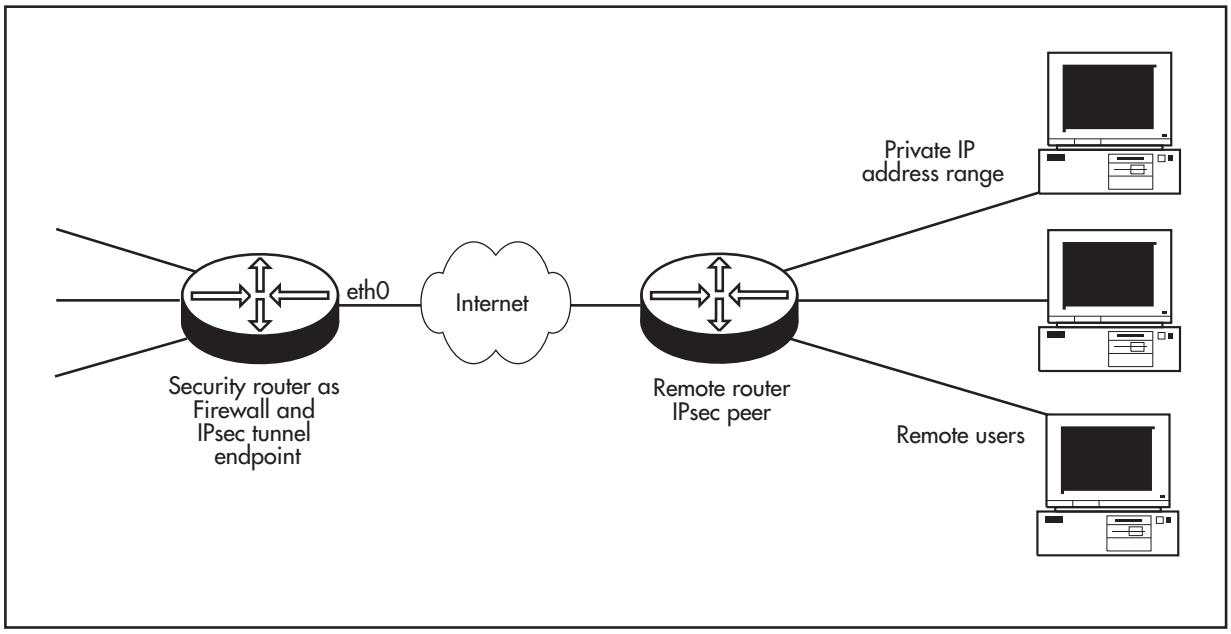
Script D: IPsec tunnel

The router has a very rich-featured IP Security (IPsec) implementation. It supports several encryption and hashing algorithms, with or without Authentication Header.

Note that incoming encrypted packets are decrypted **before** being examined by the firewall, and outgoing packets are encrypted **after** passing through the firewall. So the firewall configuration required to enable IPSEC to operate must not apply Network Address Translation (NAT) to data passing through the IPSEC tunnel.

Note: This configuration script requires an encryption key. For security reasons, any encryption key must be created manually by typing a sequence of commands on a terminal connected directly to the router's asyn0 (console/RS232) port. Before activating this script, or before entering these commands into the router, follow the steps described in "Appendix A: System security and encryption key" on page 19. If this IPsec tunnel script is combined with other commands, such as one of the basic configuration scripts, create the encryption key before running the combined script.

This example only includes the configuration to be added for an Internet connection over PPPoE ("Script B: basic PPPoE configuration" on page 7). For a direct eth0 connection ("Script A: basic Ethernet connection" on page 3), replace each instance of "ppp0" below with "eth0".



For more information on security or NAT-T

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. Notes also describe how to create a VPN between an Allied Telesis router and equipment from a number of other vendors. For a complete list of VPN How To Notes, see the *Overview of VPN Solutions in How To Notes* in the How To Library at www.alliedtelesis.com/resources/literature/howto.aspx.

Configure firewall rules to allow IPsec traffic through the firewall.

1. Allow ISAKMP key exchange

Add a firewall rule to allow incoming ISAKMP key-exchange traffic.

```
add firewall policy=lans rule=1 interface=ppp0 action=allow
  ip=0.0.0.0 protocol=udp port=500 gblip=0.0.0.0 gblport=500
```

2. Turn NAT off for IPsec traffic

Add a firewall rule to ensure that NAT is NOT applied to incoming traffic that has arrived through the IPSEC tunnel.

```
add firewall policy=lans rule=2 interface=ppp0 action=nonat
  protocol=all ip=<internal-lan-ip-range> encapsulation=ipsec
```

Add a firewall rule to ensure that NAT is NOT applied to outgoing traffic from each of the VLANs that will be sent over the IPsec tunnel to remote IP addresses.

```
add firewall policy=lans rule=3 interface=vlan3 action=nonat
  protocol=all ip=<internal-lan-ip-range>
set firewall policy=lans rule=3 remoteip=<ip-range-on-lan-at-
  other-end-of-ipsec-tunnel>
add firewall policy=lans rule=4 interface=vlan4 action=nonat
  protocol=all ip=<internal-lan-ip-range>
set firewall policy=lans rule=4 remoteip=<ip-range-on-lan-at-
  other-end-of-ipsec-tunnel>
add firewall policy=lans rule=5 interface=vlan5 action=nonat
  protocol=all ip=<internal-lan-ip-range>
set firewall policy=lans rule=5 remoteip=<ip-range-on-lan-at-
  other-end-of-ipsec-tunnel>
```

3. Configure IPsec

Configure IPsec SAs, bundles and policies.

```
enable ipsec
create ipsec saspecification=1 protocol=esp hashalg=null
  encalg=des keymanagement=isakmp
create ipsec saspecification=2 protocol=ah mode=tunnel
  hashalg=sha keymanagement=isakmp
create ipsec bundlespecification=1 keymanagement=isakmp string="1
  and 2"
create ipsec policy=isakmp interface=ppp0 action=permit lport=500
  rport=500
```

```
create ipsec policy=remoffice int=ppp0 action=ipsec
  keymanage=isakmp bundlespec=1 peeradd=<public-ip-address-of-
  remote-office> isakmppol=remoffice

set ipsec policy=remoffice laddress=<local-network-address>
  lmask=<local-netmask> raddress=<network-addr-of-lan-at-other-
  end-of-tunnel> rmask=<netmask-on-lan-at-other-end-of-tunnel>

create ipsec policy=internet interface=ppp0 action=permit
```

4. Configure ISAKMP

Create ISAKMP policies.

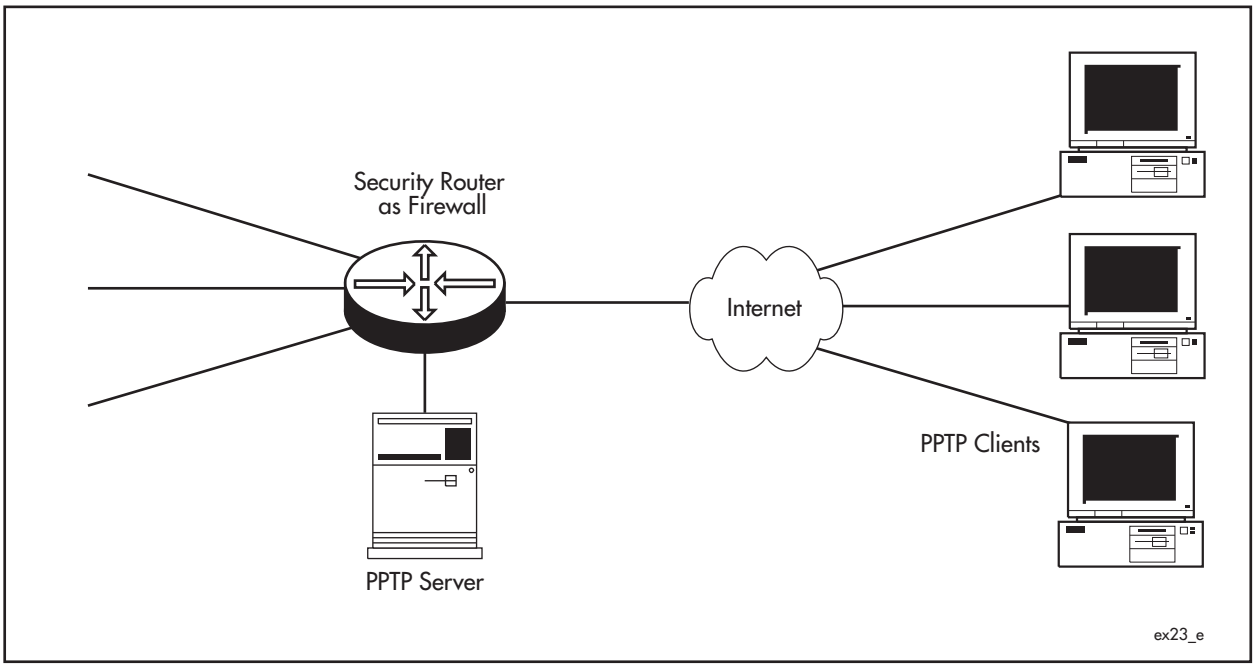
```
create isakmp policy=remoffice peer=<public-ip-address-of-remote-
  office> hashalg=sha key=1

set isakmp policy=remoffice senddeletes=on setcommitbit=on
  sendnotify=on

enable isakmp
```

Script E: PPTP server on LAN behind router

The router cannot act as a PPTP (Point to Point Tunnelling Protocol) server. If there is a separate terminating PPTP server on the private LAN behind the router, use this configuration to allow the PPTP traffic through the firewall to the PPTP server.



Allow PPTP traffic through the firewall

▶ Add rules to allow PPTP traffic thorugh the firewall

Either, if the connection is over PPPoE ("Script B: basic PPPoE configuration" on page 7)

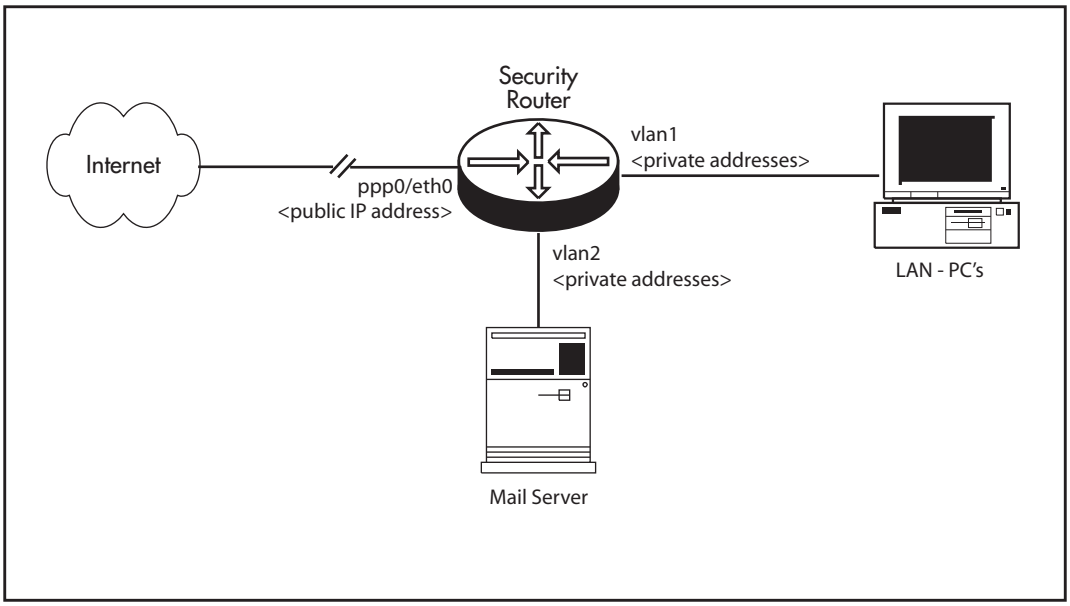
```
add firewall policy=lans rule=1 interface=ppp0 protocol=tcp
  gblport=1723 gblip=0.0.0.0 ip=<pptp-server-address> port=1723
  action=allow
add firewall policy=lans rule=2 interface=ppp0 protocol=gre
  gblip=0.0.0.0 ip=<pptp-server-address> action=allow
```

Or, for a direct connection over eth0 ("Script A: basic Ethernet connection" on page 3)

```
add firewall policy=lans rule=1 interface=eth0 protocol=tcp
  gblport=1723 gblip=0.0.0.0 ip=<pptp-server-address> port=1723
  action=allow
add firewall policy=lans rule=2 interface=eth0 protocol=gre
  gblip=0.0.0.0 ip=<pptp-server-address> action=allow
```

Script F: DMZ using private addresses

In scripts A and B, there was an implicit assumption that public IP addresses were being used on the DMZ, so no NAT was needed between the DMZ and the Internet. In this example, private addresses are being used on the DMZ.



1. Configure the VLANs

```
create vlan="dmz" vid=2
add vlan=2 port=5
```

2. Configure PPP

```
create ppp=0 over=eth0-any idle=36000 iprequest=on
set ppp=0 bap=off username=<username> password=<password>
set ppp=0 over=eth0-any lqr=off
```

3. Configure IP

```
enable ip
enable ip dnsrelay
enable ip remoteassign
add ip int=vlan1 ip=<private-ip-address>
add ip int=ppp0 ip=0.0.0.0
add ip int=vlan2 ip=<private-ip-address>
add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0
```

4. Enable the firewall

```
enable firewall
```

5. Configure the interfaces and NAT on each firewall policy

```
create firewall policy="privatelan"
enable firewall policy="privatelan" icmp_f=all
add firewall policy="privatelan" int=vlan1 type=private
add firewall policy="privatelan" int=ppp0 type=public
add firewall policy="privatelan" int=vlan2 type=public
add firewall policy="privatelan" nat=enhanced int=vlan1
  gblin=ppp0
create firewall policy="dmz"
enable firewall policy="dmz" icmp_f=ping
add firewall policy="dmz" int=vlan2 type=private
add firewall policy="dmz" int=vlan1 type=public
add firewall policy="dmz" int=ppp0 type=public
add firewall policy="dmz" nat=enhanced int=vlan2 gblin=ppp0
```

6. Create firewall rules

For example, create a pinhole to an internal mail server, on SMTP port 25:

```
add firewall policy="dmz" ru=1 ac=allo int=ppp0 prot=tcp po=25
  ip=<private-address-of-mail-server> gblip=<public-address-of-
  mail-server>
add firewall policy="dmz" ru=2 ac=allo int=vlan1 prot=all
```

Appendix A:
System security and encryption key

The script described in "Script D: IPsec tunnel" on page 13 requires an encryption key. For security reasons, any encryption key must be created manually by typing a sequence of commands on a terminal connected directly to the router's asyn0 (console/RS232) port. In order to store an encryption key, the router must be in system security mode, and system security mode requires a user with security officer privileges.

For more information about the security system on your security router, see the "User Authentication" chapter in its *Software Reference*.

To add a security officer account, create an encryption key, and enable system security, enter the commands shown in the following terminal session.

Note: Enter the following commands on the router before activating a configuration script that requires an encryption key.

```
Manager > add user=secoff password=<secret> priv=securityofficer

User Authentication Database
-------------------------------------------------------------
Username: secoff ()
   Status: enabled    Privilege: Sec Off   Telnet: no
   Logins: 0     Fails: 0       Sent: 0        Rcvd: 0
-------------------------------------------------------------

Manager > enable system security

Info (134003): Operation successful.

Manager > login secoff
Password:

Secoff >  create enco key=1 type=general value=<other-secret>

Info (1073003): Operation Successful.
```

USA Headquarters | 19800 North Creek Parkway | Suite 200 | 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

C613-16069-00 REV B