



Helpful Configuration Scripts for the AR Router Series

Revision History

Author	Revision	Date	Modifications
ST	5.8.4	5 March 2001	<p>Ex 5.6; Correction to firewall rule 1 interface</p> <p>Ex 6.3; Firewall rule 2 and 3 removed; rule 4 renumbered to 2; rule 3 (internal 'nonat') added</p> <p>Ex 6.4; Heading adjusted; Note adjusted; Firewall rule 3 added</p> <p>Ex 6.5; Heading adjusted; Comments adjusted</p> <p>Ex 6.6; Two Gateways example added</p> <p>Ex 6.7; IPsec Testing notes added</p>
ST	5.8.5	19 March 2001	<p>Ex 6.3; Add 'isa' parameter to associate ipsec policy with specific isakmp policy. Create separate isakmp policies for remote office and roaming VPN clients. Rename isakmp policies on vpn client. Added specific configuration for router B</p> <p>Ex 6.6; Add 'isa' parameter to associate ipsec policy with specific isakmp policy. Create separate isakmp policies for remote office and roaming VPN clients. Rename isakmp policies on vpn client.</p>
ST	5.8.6	3 April 2001	<p>Ex 6.3; 'sendnotify' parameter added</p> <p>Ex 6.3.1, 6.4.1, 6.7; VPN Client interface defined as 'dialup'</p> <p>Ex 6.5; Removed ppp0 on site A. Modified ADSL pinhole details. Corrected eth0 address at site B.</p> <p>Ex 6.6 becomes Ex 6.7</p> <p>Ex 6.6 inserted; IPsec and Firewall through two NAT gateways (eg: ADSL)</p>
ST	5.8.7	5 April 2001	<p>Ex 5.6; Firewall DMZ modified to dual policy firewall</p> <p>Ex 6.2; 'remoteip' parameter added to firewall rule 1</p> <p>Ex 6.5, 6.7; 'sendnotify' parameter added</p> <p>Ex 6.6; Renamed IPS and ISA policy names; Use 'isa' parameter in IPS policy; Add Internet IPS policy</p> <p>Ex 6.8; Notes extended to give basic initial debugging modes.</p> <p>Ex 6.3, 6.4, 6.5; Secoff user and securedelay defined</p>
TW	5.8.8	4 July - 24 September 2002	<p>Ex 1.4 Changed file names for section</p> <p>Ex 1.4 Added link to tftp server software</p> <p>Ex 1.5 Added client licences; Deleted Manual key generation</p> <p>Ex 4.2 Added CIR/PIR and MTU settings</p> <p>Ex 4.3 Deleted</p> <p>Ex 5.1.3 Firewall - UDP video/voice performance settings</p> <p>Ex 5.3 Deleted</p> <p>Ex 5.7 Deleted</p> <p>Ex 6.1 Deleted SA configuration details and ip settings</p> <p>Ex 6.2 Deleted SA configuration details and ip settings</p> <p>Ex 6.3 Bolded sections and removed name in router/client</p> <p>Ex 6.4 Updated for UDP VPN client</p>
TW	05/08/09	01/07/04	<p>Examples using "add ppp=0 over=syn" changed to eth1</p> <p>Deleted most of the ISDN/ppp examples</p> <p>Ex 3.1 Added PPPOE example</p> <p>Ex 2.1.3 Added ISDN settings for telecom / telstraclear</p>

ATI are manufacturers of the AR router and are specialists in Layer 3 switches and secure networking devices. More detailed information on the AR products is available on ATI's World Wide Web site www.alliedtelesyn.net.nz

Document text by Mathew Jury - ATI Technical Consultant, Taylor Wilkins – ATI Network Engineer
and Shayle Tasker - Network Engineer, ATR Customer Services Group

Allied Telesyn offers technical assistance in partnership with our authorised distributors and resellers. For technical assistance, please contact the authorised distributor or reseller in your area. Please refer to <http://www.alliedtelesyn.net.nz/> for a list of Authorised Distributors

ATI NZ Support site.

<http://www.alliedtelesyn.net.nz/>

Specifications subject to change without notice.

© ATI NZ Ltd

Contents

1.Quick Command Reference.....	5
1.1.Configurations.....	5
1.2.Filing, Reboots, and Feature Licences.....	5
1.3.Command Actions.....	5
1.4.Upgrade Process.....	6
1.5.Generating an Encryption Key.....	6
2.PPP over DDS for Internet (NAT to SMTP Server) and Private networks.....	7
2.1.PPP over ISDN Internet Access.....	8
2.1.1.Example 2.5 with 2 B channels always up.....	9
2.1.2.Example 2.5 with Cisco's at the ISP.....	9
2.1.3.ISDN territory for Telecom / Telstraclear.....	9
3.PPPOE	10
3.1.PPPOE and Firewall via Telstraclear/Woosh/ Wired Country (IHUG).....	10
4. Time Division Multiplexing (TDM)	12
5.Frame Relay.....	12
5.1.Standard Frame Relay for LMI REV 1.....	13
5.2.Standard Frame Relay ISP Access.....	14
5.3.Standard Frame Relay ISP Access with firewall and DMZ.....	15
5.4.Logical interfacing to Frame Relay, Internet connection via ISP with Private Network.....	16
5.4.1.OSPF on the private network, 4.4 continued.....	17
6.Simple Firewall over Ethernet with internal mail server	19
6.1.2.PINGING, Email notification, accounting, and logging.....	20
6.1.3.Internet Access to Firewall Router.....	20
6.1.4.UDP Video link through firewall performance tweak.....	20
6.2.Private Frame Relay with Firewall on ISP Internet PVC.....	21
6.3.Firewall over Ethernet with Private IP addresses only on the LAN.....	22
6.4.Firewall with ADSL.....	23
6.5.Firewall over PPP with a DMZ LAN.....	24
7.VPN.....	25
7.1.GRE Tunnel, NAT, and Internet.....	25
7.2.L2TP Tunnel, Firewall and Internet.....	26
7.2.IPSec (with ISAKMP), Firewall, and VPN Client.....	27
7.2.1.IPSec Client option for Example 6.3.....	28
7.3.IPSec (with Manual Key) and Firewall with NAT device (eg: ADSL), plus VPN Client(with Manual Key).....	28
7.3.1.IPSec Client option for Example 6.4.....	31
7.4. IPSec & ISAKMP (with L2TP) and Firewall router, behind NAT device (eg:ADSL).....	32
7.5.IPSec and Firewall through two NAT gateways (eg: ADSL).....	35
7.6.Two Gateways; Firewall with IPSec and ISAKMP to VPN Client & Remote Office.....	37
7.7.Notes on IPSec Testing and Verification.....	40

1.Quick Command Reference

1.1.Configurations

Task	Command
Sho the log	Sho log
View the current release and patch	Sho install
Sho the system Information	Sho sys
Save the current configuration	Create config=<config>.cfg
Change the boot configuration file	Set conf=<config>.cfg
What is the current configuration file	Sho conf
Sho the current RAM configuration	Sho conf dyn Sho conf dyn=<sub section>

1.2.Filing, Reboots, and Feature Licences

Task	Command
Sho file contents in FLASH or NVS	Sho fi=<file.ext>
Sho files	Sho fi
To Edit a file	Edit <file.ext>
Warm boot the router	Restart reboot
Quick boot (for applying new configurations)	Restart router
Enable a new feature licence	Enable feature=<feature> pass=<password>

1.3.Command Actions

To config	To Remove from Configuration	To view and modify
Add	Delete	Sho
Create	Destroy	Set
Activate	Deactivate	Reset
Enable	Disable	Purge

1.4.Upgrade Process

To load the file on the router you need a trivial ftp server software. A windows version is available here [Allied Telesyn tftp server](#)

Upgrade process	Commands
Make space, delete the old files	Del fi=<oldfile.ext>
Load files	Load fi=<file.rez> dest=flash serv=<server ip> Load fi=<file.paz> dest=flash serv=<server ip> Load fi=<file.hlp> dest=flash serv=<server ip>
Apply a Help file	Set help=<help>.hlp
Save the config	Create conf=<current config>
Enable the release licence	Enable rel=<release.rez> num=<release> pass=<password>
Set the current release and patch file	Set inst=pref rel=<release.rez> pat=<patch.paz>
Warm boot the router	Restart reboot

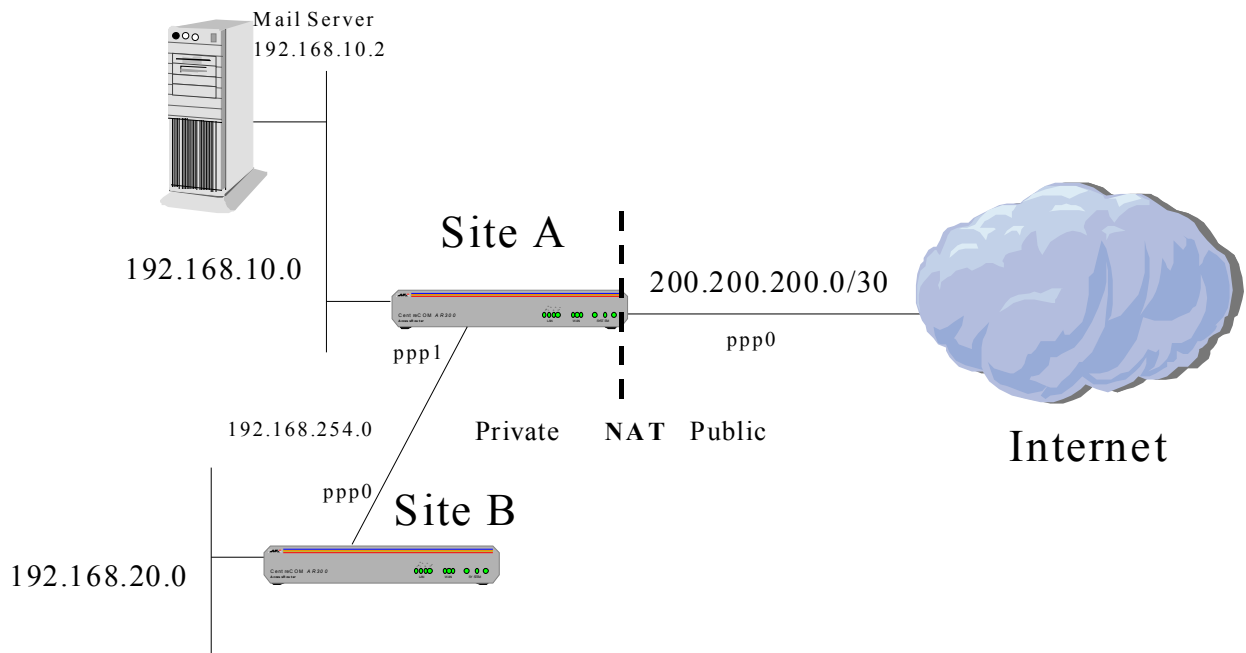
1.5.Generating an Encryption Key

Check List for Encrytion

- 1) Do you have full client licences to generate keys?
- 2) 3DES licence (export permit)
- 3) EMAC/EPAC Encryption Card?

Task	Command
Add security level user	Add user=secoff pass=secoff priv=security
Keep security officer access for 10 Minutes	Set user securedelay=600
Turn on Security at both ends	Enable system security
Create the ISAKMP key	At router 'A'>Create enco key=1 type=gen random
View the key and	At router 'A'>Sho enco key=1 (tip: copy and paste this key to router B)
Enter the ISAKMP key at the other end	At router 'B'>Create enco key=1 type=gen val=<router 'A' key>
Allow remote Security officer access and Specify remote IP address ranges	Enable user rso Add user rso ip=<remote access ip> mask=<mask>

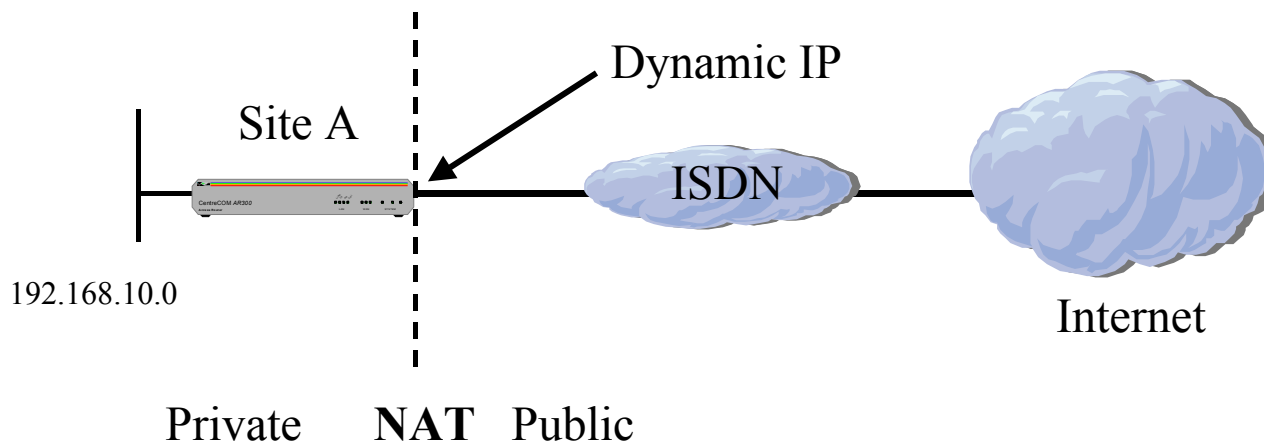
2.PPP over DDS for Internet (NAT to SMTP Server) and Private networks



Note: Be aware that with many Internet Providers it may be more suitable to turn LQR (link quality reporting) off on PPP links, and instead use LCP *Echo Request* and *Echo Reply* messages to determine link quality (echo=on). Simply add 'lqr=off echo=on' to the PPP creation command.

Router A	Router B
<pre># # PPP Configuration # create ppp=0 over=syn0 create ppp=1 over=syn1 # # IP Configuration # enable ip add ip int=eth0 ip=192.168.10.1 add ip int=ppp1 ip=192.168.254.1 add ip int=ppp0 ip=200.200.200.1 mask=255.255.255.252 add ip route=0.0.0.0 next=0.0.0.0 int=ppp0 add ip route=192.168.20.0 next=0.0.0.0 int=ppp1 enable ip nat enable ip nat log=all add ip nat ip=192.168.0.0 mask=255.255.0.0 gblip=200.200.200.1 add ip nat ip=192.168.10.2 mask=255.255.255.255 port=smt p gblip=200.200.200.1 gblport=smt p proto=tcp</pre>	<pre># # PPP Configuration # create ppp=0 over=syn0 # # IP Configuration # enable ip add ip int=eth0 ip=192.168.20.1 add ip int=ppp0 ip=192.168.254.2 add ip route=0.0.0.0 next=0.0.0.0 int=ppp0</pre>

2.1.PPP over ISDN Internet Access



Note: Be aware that with many Internet Providers it may be more suitable to turn LQR (link quality reporting) off on PPP links, and instead use LCP *Echo Request* and *Echo Reply* messages to determine link quality (echo=on). Simply add 'lqr=off echo=on' to the PPP creation command.

Router A

```
#
# System Configuration
set sys territory=<countrycode>
#
# ISDN Configuration
add isdn call=internet num=12345 prec=out
#
# PPP Configuration
# Note: 2nd B channel on demand
create ppp=0 over=isdn-internet idle=60 bap=off ipreq=on user=<username> pass=<password>
add ppp=0 over=isdn-internet type=demand
#
# IP Configuration
enable ip
enable ip rem
add ip int=eth0 ip=192.168.10.1
add ip int=ppp0 ip=0.0.0.0
add ip route=0.0.0.0 next=0.0.0.0 int=ppp0
enable ip nat
enable ip nat log=all
add ip nat ip=192.168.10.0 mask=255.255.255.0 gblint=ppp0
```

2.1.1.Example 2.5 with 2 B channels always up

Note: Some ISDN providers and /or ISP providers charge per minute and this option may not be affordable. This alternative is intended where an affordable fixed monthly charge account has been offered by ISDN and ISP providers.

Note: Be aware that with many Internet Providers it may be more suitable to turn LQR (link quality reporting) off on PPP links, and instead use LCP *Echo Request* and *Echo Reply* messages to determine link quality (echo=on). Simply add 'lqr=off echo=on' to the PPP creation command.

ISDN & PPP Configuration modifications for 2 B channels always up

```
#
# ISDN Configuration
#
add isdn call=internet num=12345 prec=out keepup=on
#
# PPP Configuration
# Note: No idle parameter, user and password required if going into an ISP
create ppp=0 over=isdn-internet num=2 bap=off [user=<username> password=<password>]
```

2.1.2.Example 2.5 with Cisco's at the ISP

PPP Configuration modifications for Cisco at the ISP

```
#
# PPP Configuration
# Note: 2nd B channel on demand
create ppp=0 over=isdn-internet idle=60 bap=off lqr=off echo=on user=<user name>
pass=<password>
add ppp=0 over=isdn-internet type=demand
```

2.1.3.ISDN territory for Telecom / Telstraclear

ISDN settings for Telecom / Telstraclear

```
#
# ISDN settings for Telecom
set system territory=newzealand
#
# ISDN settings for Telstraclear
set system territory=europe
```

3.PPPOE

3.1.PPPOE and Firewall via Telstraclear/Woosh/ Wired Country (IHUG)



Note – Proxy arp must be turned off on a Public Shared Ethernet Network

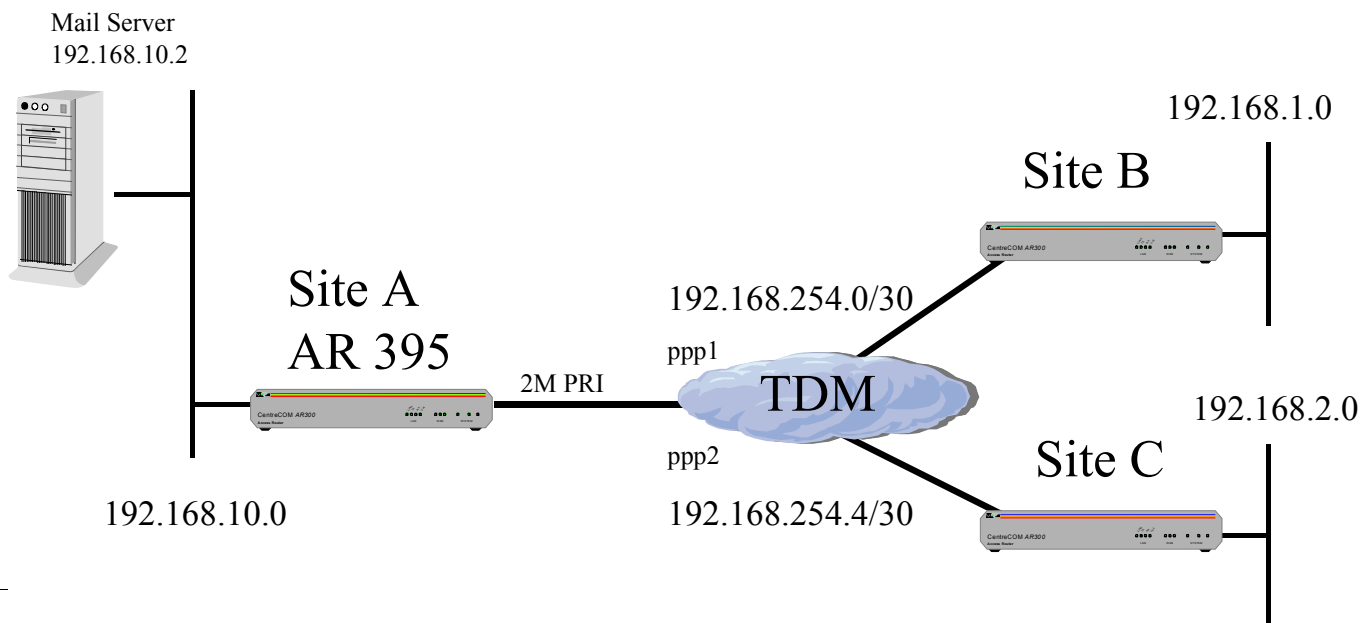
Router A

```
create ppp=0 idle=999999 over=eth0-ANY
set ppp=0 iprequest=on username="test@isp.co.nz" password="test"
set ppp=0 over=eth0-ANY lqr=off echo=10

enable ip
enable ip remote
add ip int=ppp0 ip=0.0.0.0 mask=0.0.0.0
add ip int=vlan1 ip=10.0.0.1 mask=255.255.255.0
add ip int=eth0 ip=1.1.1.1 mask=255.255.255.0
set ip int=eth0 proxy=off
add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp1 next=0.0.0.0

enable firewall
create firewall policy="pppoe"
enable firewall policy="pppoe" icmp_f=all
add firewall policy="pppoe" int=vlan1 type=private
add firewall policy="pppoe" int=ppp0 type=public
add firewall poli="pppoe" nat=enhanced int=vlan1 gblin=ppp0
```

4. Time Division Multiplexing (TDM)



```
#
# PRI configuration
# Note: "CRC" mode may need to be set to "off" or
# "checking" for the link to become active
# depending on the Telco configuration
# Note : RJ 45 Pinouts for PRI devices aren't
# standardized, check your NTU if using RJ 45.
# termination

set pri=0 mode=tdm
set pri=0 crc=reporting

#
# TDM configuration
#
create tdm group=site_b interface=pri0 slots=1
create tdm group=site_c interface=pri0 slots=6-7
#
# PPP Configuration
#
create ppp=1 over=tdm-site_b idle=60 comp=on
create ppp=2 over=tdm-site_c idle=60 comp=on
```

```
#
# IP Configuration
#
enable ip
add ip int=eth0 ip=192.168.10.1
add ip int=ppp1 ip=192.168.254.1
mask=255.255.255.252
add ip int=ppp2 ip=192.168.254.5
mask=255.255.255.252
add ip route=192.168.1.0 next=0.0.0.0 int=ppp1
add ip route=192.168.2.0 next=0.0.0.0 int=ppp2
```

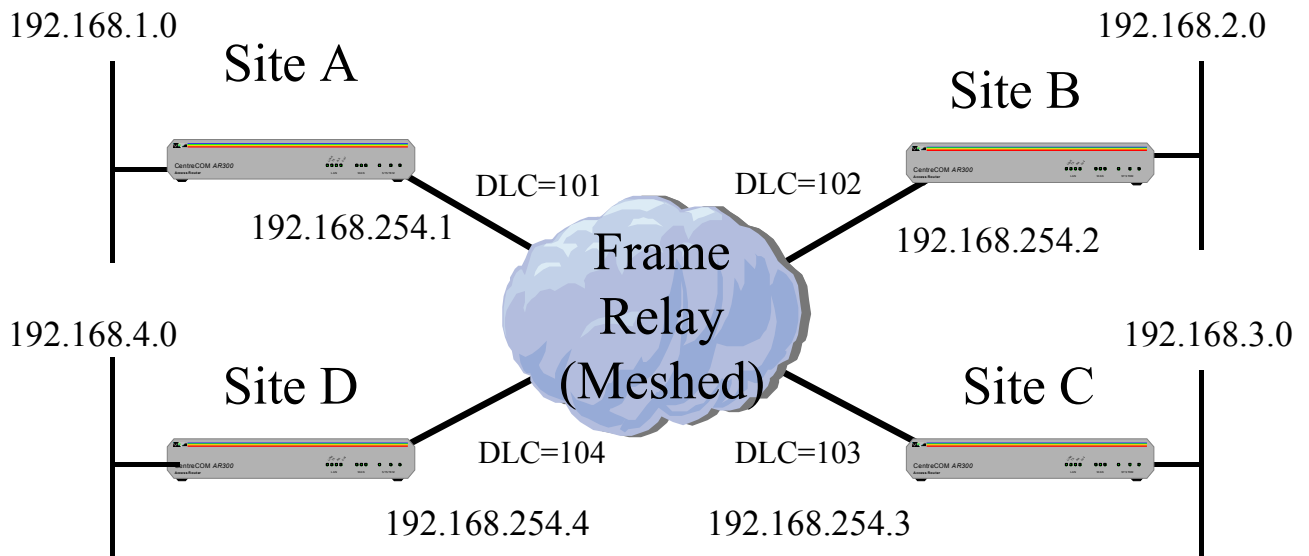
Router B

```
#
# PPP Configuration
#
create ppp=0 over=syn0
#
# IP Configuration
# Note: Router C change eth and ppp IP address
enable ip
add ip int=eth0 ip=192.168.1.1
add ip int=ppp0 ip=192.168.254.2
add ip route=0.0.0.0 next=0.0.0.0 int=ppp0
```

5. Frame Relay

5.1. Standard Frame Relay for LMI REV 1

(Sometimes referred to as "cisco" LMI type)

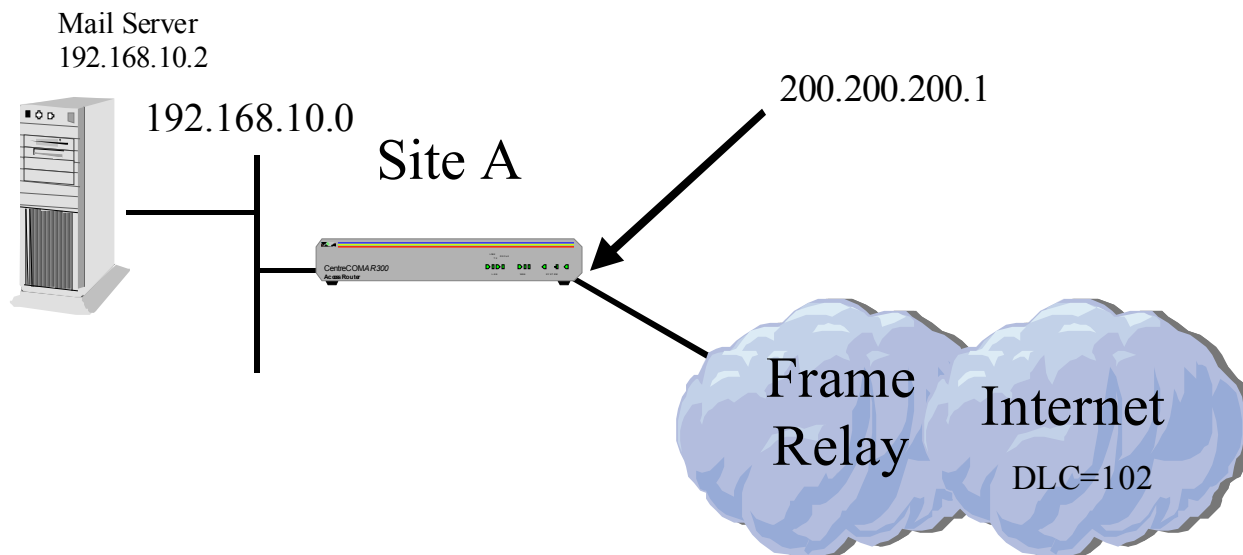


```

Router A
#
# Frame Relay Configuration
# Note: By default LMI is set to "LM1rev1" which is the same as "cisco" LMI type.
create fr=0 over=syn0
#
# IP Configuration
#
enable ip
add ip int=fr0 ip=192.168.254.1
add ip int=eth0 ip=192.168.1.1
add ip route=192.168.2.0 next=0.0.0.0 mask=255.255.255.0 int=fr0 dlc=102
add ip route=192.168.3.0 next=0.0.0.0 mask=255.255.255.0 int=fr0 dlc=103
add ip route=192.168.4.0 next=0.0.0.0 mask=255.255.255.0 int=fr0 dlc=104
Router B, C, and D must have the ip addresses and routes changed appropriately
To use RIP instead, remove the static routes and add the following lines
Add ip rip int=fr0 dlc=102
Add ip rip int=fr0 dlc=103
Add ip rip int=fr0 dlc=104
    
```

(LMI Rev 1 is default LMI for Telecom New Zealand)

5.2. Standard Frame Relay ISP Access

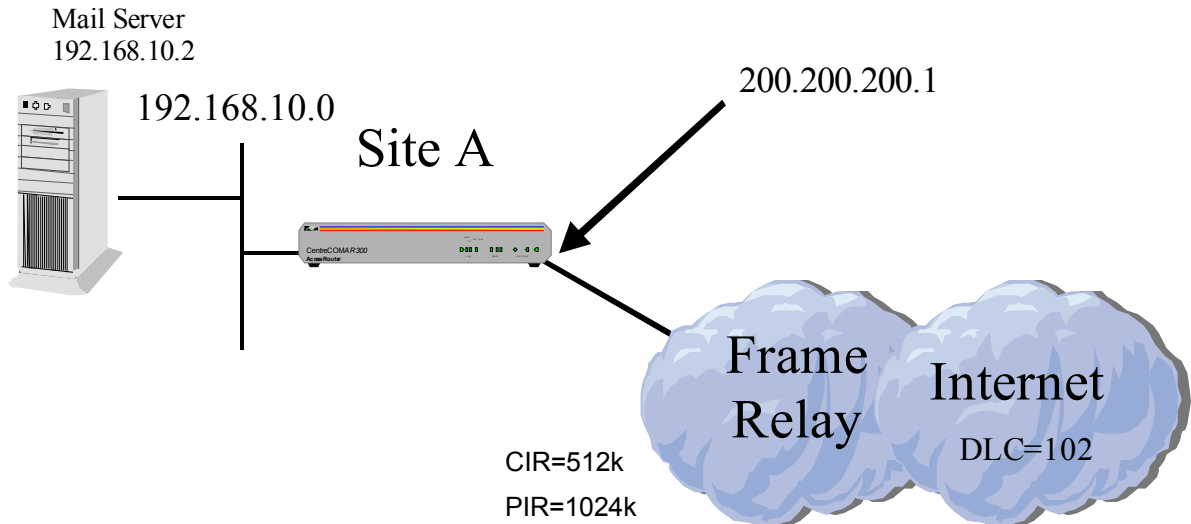


The frame network in NZ uses a MTU of 1500 this needs to be altered on the routers because the default is 1600.

Router A

```
# Syn
# set syn to the speed the telco is providing eg 1Mbit =1024000
set syn=syn0 speed=2048000
#
# Frame Relay Configuration
# Note: By default LMI is set to "LMirev1" which is the same as "cisco" LMI type.
# To "Packet shape" set the CIRLIMIT to the PIR supplied.
create fr=0 over=syn0
set fr=0 dlc=102 cir=1024000 cirlimit=yes
#
# Interfaces
set int=fr0 mtu=1500
#
# IP Configuration
enable ip
add ip int=fr0 ip=200.200.200.1 mask=255.255.255.252
add ip int=eth0 ip=192.168.10.1
add ip route=0.0.0.0 next=0.0.0.0 mask=0.0.0.0 int=fr0 dlc=102
enable ip nat
enable ip nat log=all
add ip nat ip=192.168.10.0 mask=255.255.255.0 gblip=200.200.200.1
add ip nat ip=192.168.10.2 mask=255.255.255.255 port=smtp gblip=200.200.200.1 gblport=smtp
proto=tcp
```

5.3. Standard Frame Relay ISP Access with firewall and DMZ



The frame network in NZ uses a MTU of 1500 this needs to be altered on the routers because the default is 1600.

Router A

```
# set syn to the speed the telco is providing eg 1Mbit =1024000
set syn=syn0 speed=2048000

# Frame Relay Configuration

# Note: By default LMI is set to "LMirev1" which is the same as "cisco" LMI type.
# To "Packet shape" set the CIRLIMIT to the PIR supplied.

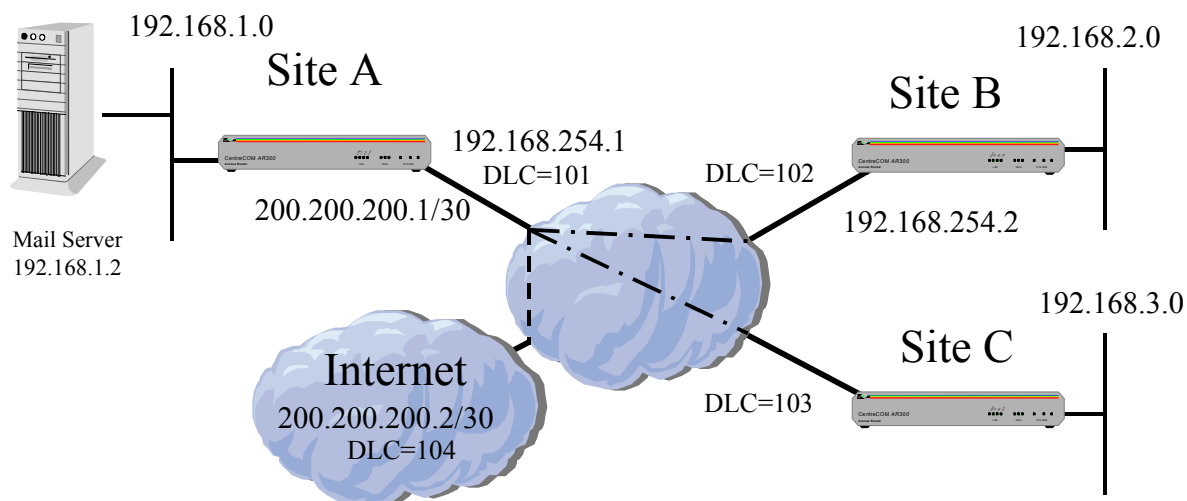
create fr=0 over=syn0
set fr=0 dlc=102 cir=1024000 cirlimit=yes

# Interfaces
set int=fr0 mtu=1500

# IP Configuration
enable ip
add ip int=fr0 ip=200.200.200.1 mask=255.255.255.252
add ip int=eth0 ip=192.168.10.1
add ip int=eth1 ip=210.1.1.1 mask=255.255.255.252
add ip route=0.0.0.0 next=0.0.0.0 mask=0.0.0.0 int=fr0 dlc=102

#Firewall
enable firewall
create firewall poli=main
add firewall poli=main int=eth0 type=private
add firewall poli=main int=eth1 type=public
add firewall poli=main int=fr0 type=public
add firewall poli=main nat=enhanced int=eth0 gblint=fr0
create firewall poli=dmz
add firewall poli=dmz int=eth0 type=public
add firewall poli=dmz int=eth1 type=private
add firewall poli=dmz int=fr0 type=public
add firewall poli=dmz ru=1 ac=allow int=fr0 ip=210.1.1.2 prot=tcp port=25
add firewall poli=dmz ru=100 ac=allow int=eth0 prot=all
```

5.4. Logical interfacing to Frame Relay, Internet connection via ISP with Private Network



Router A

```
#
# Frame Relay Configuration
# Note: By default LMI is set to "LMIrev1" which is the same as "cisco" LMI type.
create fr=0 over=syn0
add fr=0 li=1 type=ptp
add fr=0 li=2
set fr=0 dlc=102 li=2
set fr=0 dlc=103 li=2
set fr=0 dlc=104 li=1
#
# IP Configuration
#
enable ip
add ip int=fr0.2 ip=192.168.254.1
add ip int=fr0.1 ip=200.200.200.1 mask=255.255.255.252
add ip int=eth0 ip=192.168.1.1
add ip route=0.0.0.0 next=0.0.0.0 mask=0.0.0.0 int=fr0.1 dlc=104
add ip route=192.168.2.0 next=192.168.254.2 mask=255.255.255.0 int=fr0.2 dlc=102
add ip route=192.168.3.0 next=192.168.254.3 mask=255.255.255.0 int=fr0.2 dlc=103
enable ip nat
enable ip nat log=all
add ip nat ip=192.168.0.0 mask=255.255.0.0 gblip=200.200.200.1
add ip nat ip=192.168.1.2 mask=255.255.255.255 port=smtp gblip=200.200.200.1 gblport=smtp
proto=tcp
```

Router B and C would remain configured as in example 4.1 (no FRLIs)

5.4.1.OSPF on the private network, 4.4 continued

Router A (First remove the 2 static routes to the private network sites, leave default route

```
#
# Frame Relay Configuration
# Note: By default LMI is set to "LMirev1" which is the same as "cisco" LMI type.
create fr=0 over=syn0
add fr=0 li=1 type=ptp
add fr=0 li=2 type=ptp
add fr=0 li=3 type=ptp
set fr=0 dlc=102 li=2
set fr=0 dlc=103 li=3
set fr=0 dlc=104 li=1
#
# IP Configuration
#
enable ip
add ip int=fr0.2 ip=192.168.254.1 mask=255.255.255.252
add ip int=fr0.3 ip=192.168.254.5 mask=255.255.255.252
add ip int=fr0.1 ip=200.200.200.1 mask=255.255.255.252
add ip int=eth0 ip=192.168.1.1
add ip route=0.0.0.0 next=0.0.0.0 mask=0.0.0.0 int=fr0.1 dlc=104
enable ip nat
enable ip nat log=all
add ip nat ip=192.168.0.0 mask=255.255.0.0 gblip=200.200.200.1
add ip nat ip=192.168.1.2 mask=255.255.255.255 port=smtp gblip=200.200.200.1 gblport=smtp proto=tcp
#
# OSPF Configuration
#
set ospf routerid=192.168.254.1 asexternal=on
add ospf area=backbone stubarea=off summary=send
add ospf range=192.168.254.0 area=backbone mask=255.255.255.0
add ospf interface=fr0.2 area=backbone
add ospf interface=fr0.3 area=backbone
enable ospf
```

Router B

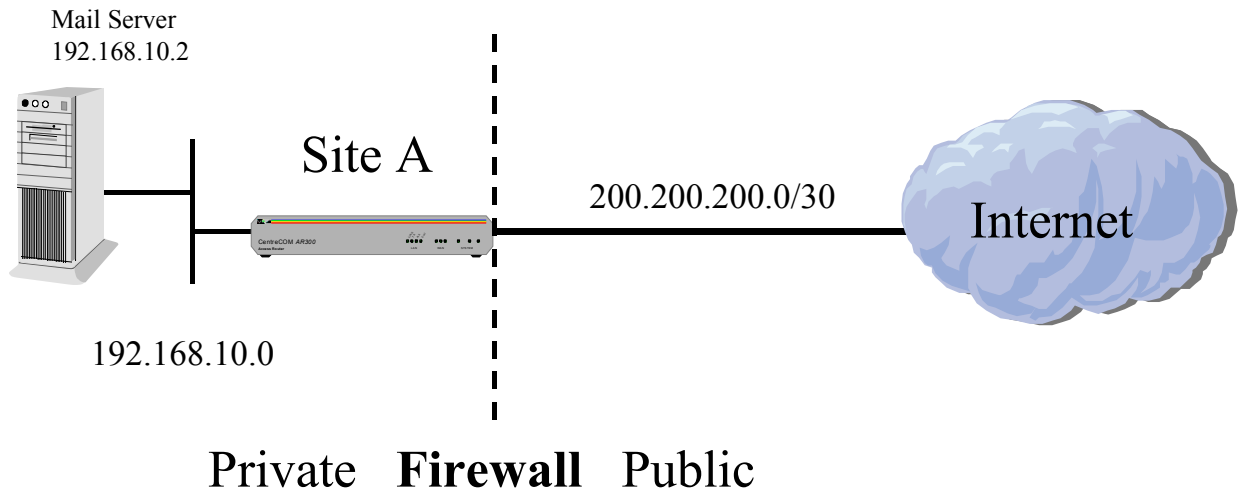
```
#
# Frame Relay Configuration
# Note: By default LMI is set to "LMIREV1" which is the same as "cisco" LMI type.
create fr=0 over=syn0
add fr=0 li=1 type=ptp
set fr=0 dlc=101 li=1
#
# IP Configuration
#
enable ip
add ip int=fr0.1 ip=192.168.254.2 mask=255.255.255.252
add ip int=eth0 ip=192.168.2.1
#
# OSPF Configuration
#
set ospf routerid=192.168.254.2 asexternal=on
add ospf area=backbone stubarea=off summary=send
add ospf range=192.168.254.0 area=backbone mask=255.255.255.0
add ospf interface=fr0.1 area=backbone
enable ospf
```

Router C

```
#
# Frame Relay Configuration
# Note: By default LMI is set to "LMIREV1" which is the same as "cisco" LMI type.
create fr=0 over=syn0
add fr=0 li=1 type=ptp
set fr=0 dlc=101 li=1
#
# IP Configuration
#
enable ip
add ip int=fr0.1 ip=192.168.254.3 mask=255.255.255.252
add ip int=eth0 ip=192.168.3.1
#
# OSPF Configuration
#
set ospf routerid=192.168.254.3 asexternal=on
add ospf area=backbone stubarea=off summary=send
add ospf range=192.168.254.0 area=backbone mask=255.255.255.0
add ospf interface=fr0.1 area=backbone
enable ospf
```

Firewall Configs

6. Simple Firewall over Ethernet with internal mail server



Router A

```
#
# IP Configuration
#
enable ip
add ip int=eth1 ip=200.200.200.1 mask=255.255.255.252
set ip int=eth1 proxy=off
add ip int=eth0 ip=192.168.10.1
add ip route=0.0.0.0 next=200.200.200.2 mask=0.0.0.0 int=eth1
#
# Firewall Configuration
# To enable out going ping see example 5.1.1
enable firewall
enable firewall notify=port,manager port=0
create firewall policy="main"
add firewall policy="main" int=eth0 type=private
add firewall policy="main" int=eth1 type=public
add firewall poli="main" nat=enhanced int=eth0 gblin=ppp0 gblip=200.200.200.1
add firewall poli="main" ru=1 ac=allo int=eth1 prot=tcp po=25 ip=192.168.10.2
gblip=200.200.200.1 gblport=25
```

6.1.2.PINGING, Email notification, accounting, and logging

Router A

```
set mail host=mydomain.mail.com
set ip nameserve=100.100.100.100
#
# Firewall Configuration
#
# Ping is blocked by default, to enable outgoing ping responses back in
enable firewall policy=main icmp_forward=ping
enable firewall policy="main" accounting
enable firewall policy="main" log=indeny
enable firewall notify=port,manager,mail port=0 to=it\_manager@support.co.ju
# Or if no Name server defined
enable firewall notify=port,manager,mail port=0 to=it\_manager@\[192.168.10.2\]
```

6.1.3.Internet Access to Firewall Router

Router A:

```
#
#Firewall
# Note. Always include a remote user ip address to maintain relatively secure access
add firewall poli="main" ru=2 ac=allo int=ppp0 prot=tcp po=23 ip=192.168.10.1
gblip=200.200.200.1 gblport=23 rem=<remote manager ip address>
```

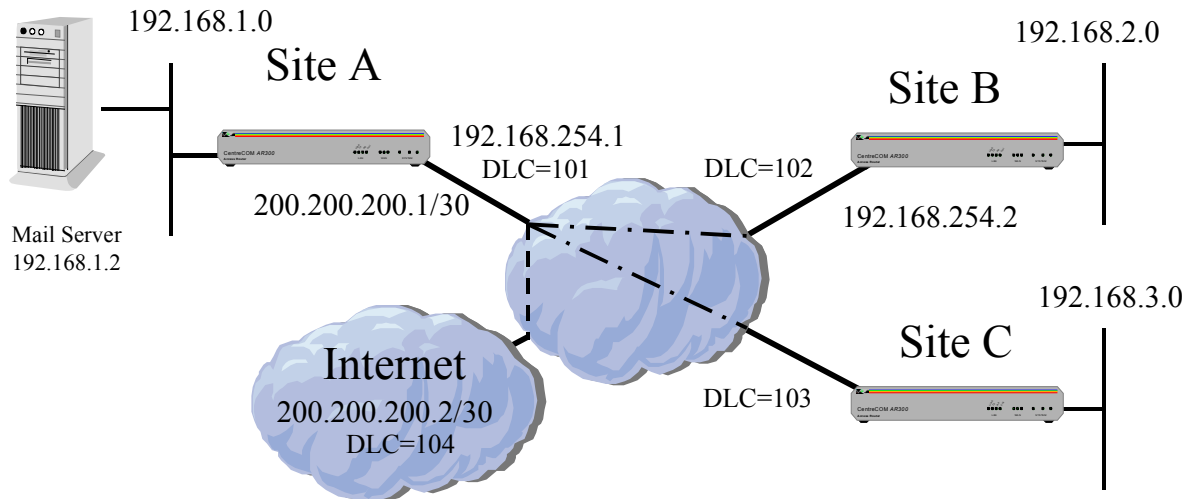
6.1.4.UDP Video link through firewall performance tweak

Are you having problems with UDP based Video conferencing or UDP based encrypted link throughput? If you have a firewall setup it could be detecting the packets as part of a UDP attack and throttling the bandwidth causing jitter, no voice and generally slow performance.

Router A:

```
#
#Firewall
# Allow higher UDP rate.
set firewall poli="main" attack=udpattack det=100
set firewall poli=main udptime=1
```

6.2. Private Frame Relay with Firewall on ISP Internet PVC

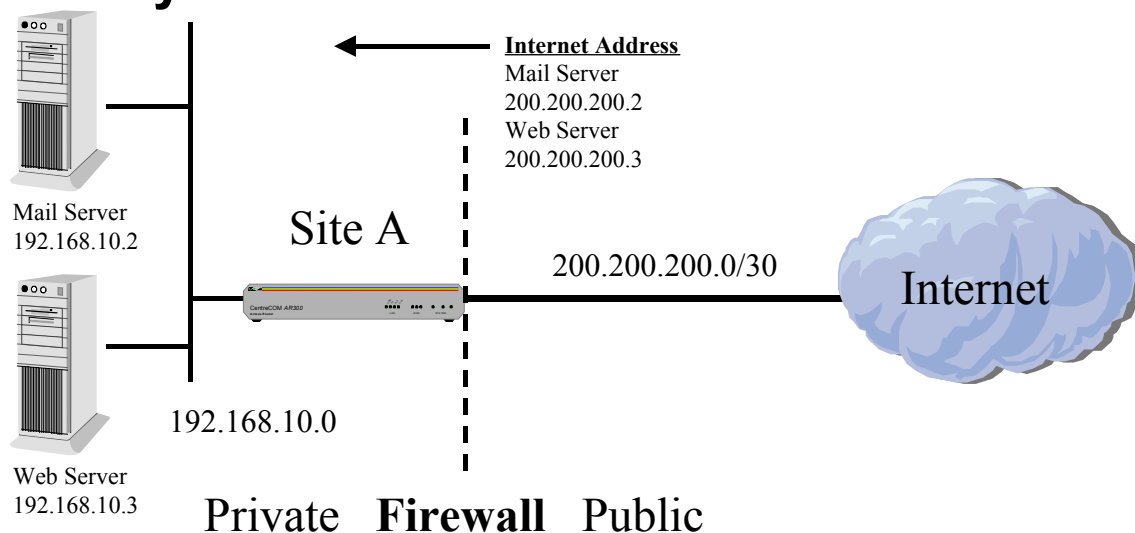


Router A

```
#
# Frame Relay Configuration
# Note: By default LMI is set to "LMirev1" which is the same as "cisco" LMI type.
create fr=0 over=syn0
add fr=0 li=1 type=ptp
add fr=0 li=2
set fr=0 dlc=102 li=2
set fr=0 dlc=103 li=2
set fr=0 dlc=104 li=1
#
# IP Configuration
#
enable ip
add ip int=fr0.2 ip=192.168.254.1
add ip int=fr0.1 ip=200.200.200.1 mask=255.255.255.252
add ip int=eth0 ip=192.168.1.1
add ip route=0.0.0.0 next=0.0.0.0 mask=0.0.0.0 int=fr0.1 dlc=104
add ip route=192.168.2.0 next=192.168.254.2 mask=255.255.255.0 int=fr0.2 dlc=102
add ip route=192.168.3.0 next=192.168.254.3 mask=255.255.255.0 int=fr0.2 dlc=103
#
# Firewall Configuration
# To enable out going ping see example 5.1.1
enable firewall
enable firewall notify=port,manager port=0
create firewall policy="main"
add firewall policy="main" int=eth0 type=private
add firewall policy="main" int=fr0.2 type=private
add firewall policy="main" int=fr0.1 type=public
add firewall poli="main" nat=enhanced int=eth0 gblin=fr0.1 gblip=200.200.200.1
add firewall poli="main" nat=enhanced int=fr0.2 gblin=fr0.1 gblip=200.200.200.1
add firewall poli="main" ru=1 ac=allo int=fr0.1 prot=tcp po=25 ip=192.168.1.2
gblip=200.200.200.1 gblport=25
```

Router B and C would be configured without Logical interfaces as in example 4.1 with a default route

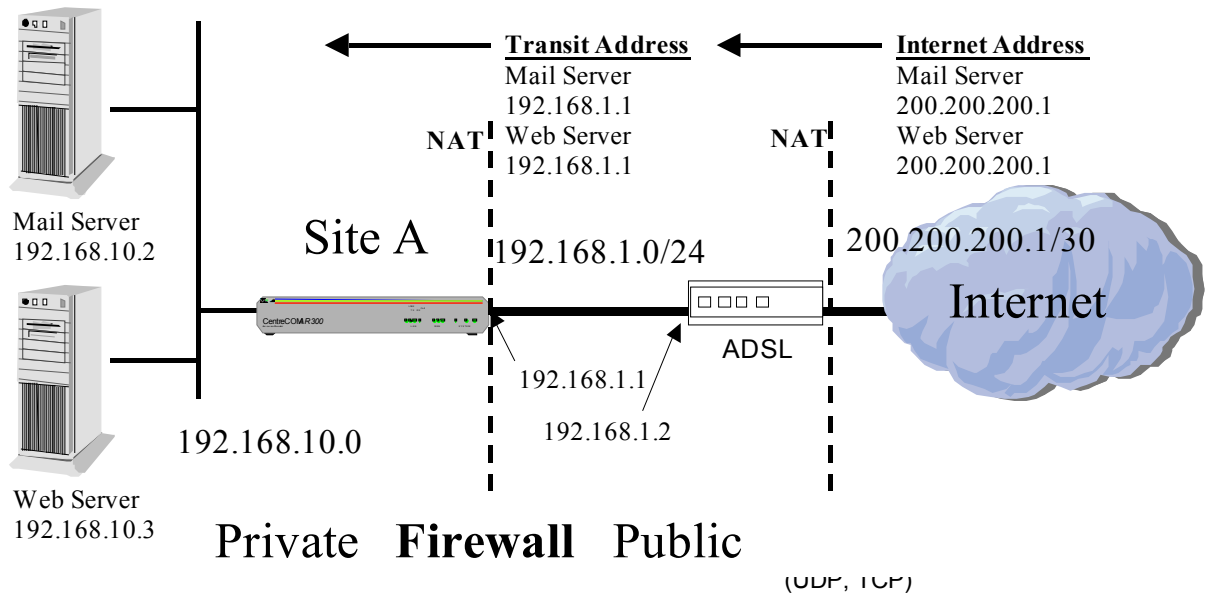
6.3. Firewall over Ethernet with Private IP addresses only on the LAN



Router A

```
#
# IP Configuration
#
enable ip
add ip int=eth1 ip=200.200.200.1 mask=255.255.255.252
add ip int=eth0 ip=192.168.10.1
add ip route=0.0.0.0 next=200.200.200.2 mask=0.0.0.0 int=eth1
#
# Firewall Configuration
# To enable out going ping see example 5.1.1
enable firewall
enable firewall notify=port,manager port=0
create firewall policy="main"
add firewall policy="main" int=eth0 type=private
add firewall policy="main" int=eth1 type=public
add firewall poli="main" nat=enhanced int=eth0 gblin=eth1 gblip=200.200.200.1-200.200.200.3
add firewall poli="main" ru=1 ac=allo int=eth1 prot=tcp po=25 ip=192.168.10.2 g
blip=200.200.200.2 gblp=25
add firewall poli="main" ru=2 ac=allo int=eth1 prot=tcp po=80 ip=192.168.10.3 g
blip=200.200.200.3 gblp=80
```

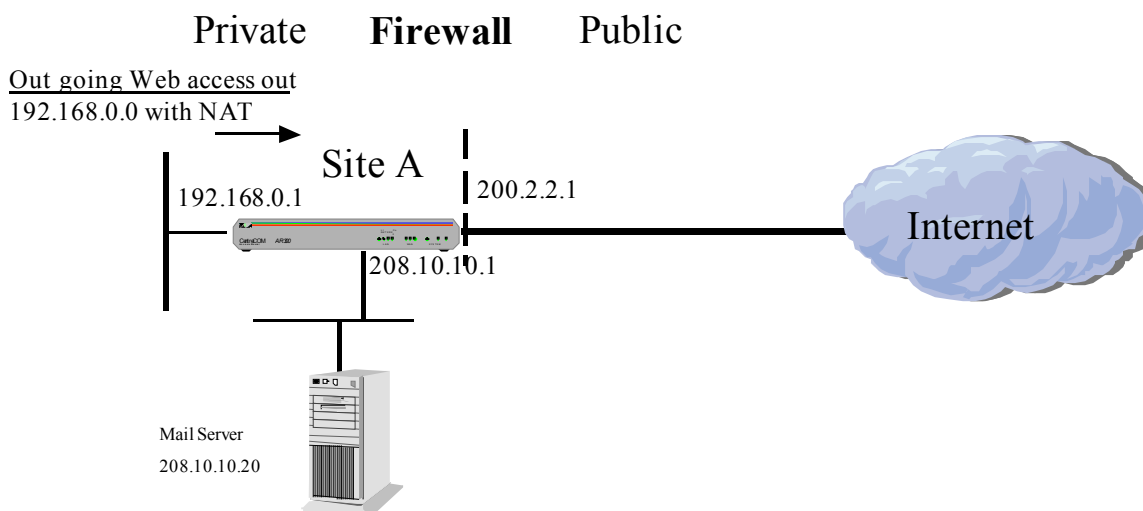
6.4.Firewall with ADSL



Router A

```
#
# IP Configuration
#
enable ip
add ip int=eth1 ip=192.168.1.1
add ip int=eth0 ip=192.168.10.1
add ip route=0.0.0.0 next=192.168.1.2 mask=0.0.0.0 int=eth1
#
# Firewall Configuration
# To enable out going ping see example 5.1.1
enable firewall
enable firewall notify=port,manager port=0
create firewall policy="main"
add firewall policy="main" int=eth0 type=private
add firewall policy="main" int=eth1 type=public
add firewall poli="main" nat=enhanced int=eth0 gblin=eth1 gblip=192.168.1.1
add firewall poli="main" ru=1 ac=allo int=eth1 prot=tcp po=25 ip=192.168.10.2 gblip=192.168.1.1
gblp=25
add firewall poli="main" ru=2 ac=allo int=eth1 prot=tcp po=80 ip=192.168.10.3 gblip=192.168.1.1
gblp=80
```

6.5.Firewall over PPP with a DMZ LAN



Note: Be aware that with many Internet Providers it may be more suitable to turn LQR (link quality reporting) off on PPP links, and instead use LCP *Echo Request* and *Echo Reply* messages to determine link quality (echo=on). Simply add 'lqr=off echo=on' to the PPP creation command.

Router A

```

create ppp=0 over=syn0
enable ip
add ip int=eth0 ip=192.168.0.1
add ip int=eth1 ip=208.10.10.1
add ip int=ppp0 ip=200.2.2.1
add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0

enable firewall
create firewall policy="LAN"
enable firewall policy="LAN" icmp_f=ping
add firewall policy="LAN" int=eth0 type=private
add firewall policy="LAN" int=ppp0 type=public
add firewall policy="LAN" int=eth1 type=public
add firewall poli="LAN" nat=enhanced int=eth0 gblin=ppp0 gblip=208.10.10.1

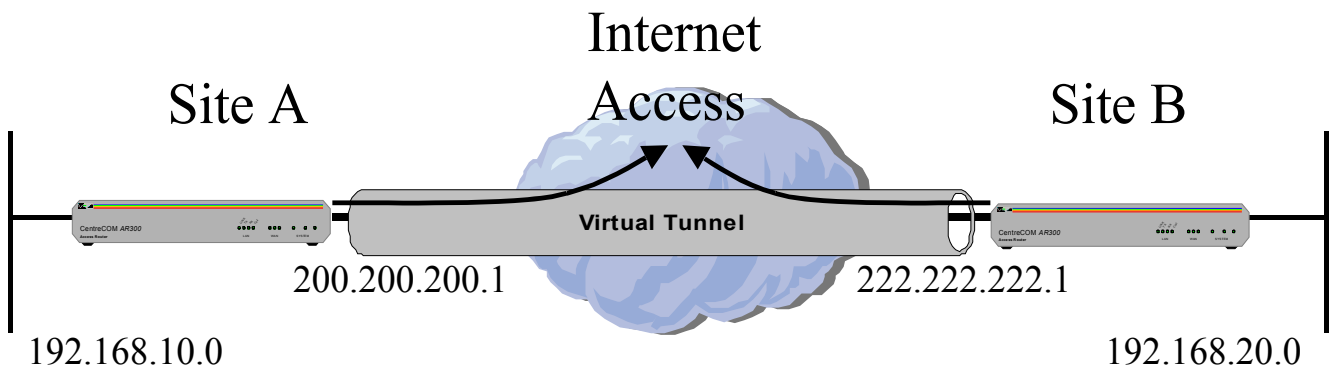
create firewall policy="DMZ"
enable firewall policy="DMZ" icmp_f=ping
add firewall policy="DMZ" int=eth1 type=private
add firewall policy="DMZ" int=ppp0 type=public
add firewall policy="DMZ" int=eth0 type=public
# Allow access from Internet to Web server (domain registered 208.10.10.20)
add firewall poli="DMZ" ru=1 ac=allo int=ppp0 prot=tcp po=80 ip=208.10.10.20
# Allow any access to DMZ from eth0 LAN
add firewall poli="DMZ" ru=100 ac=allo int=eth0 prot=ALL

```

7.VPN

7.1.GRE Tunnel, NAT, and Internet

(Preferred example uses L2TP with firewall. Refer example 6.2)

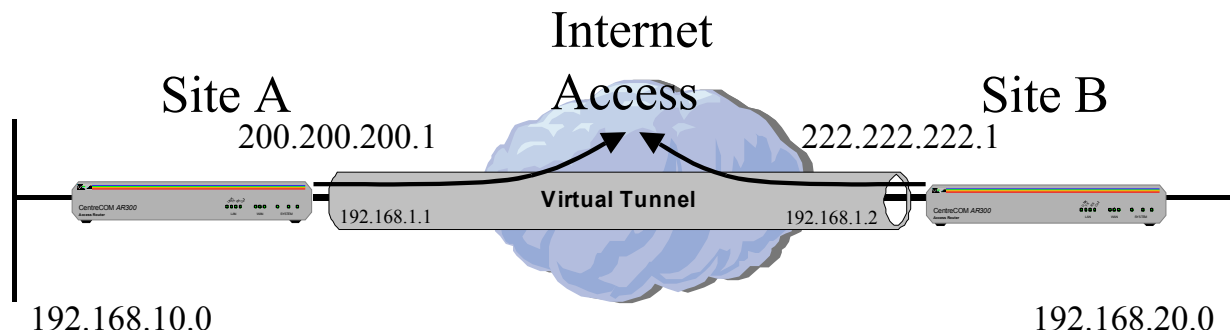


Router A (Router B, reverse IP addresses as per diagram above)

```
#
# GRE
#
enable gre
add gre=1 sour=192.168.10.0 smask=255.255.255.0 dest=192.168.20.0 dmask=255.255.255.0
target=222.222.222.1

#
# IP
#Note: NAT must be on for this configuration to work correctly
enable ip
Add ip int=eth0 ip=192.168.10.1 mask=255.255.255.0
Add ip int=eth1 ip=200.200.200.1
add ip rou=0.0.0.0 next=200.200.200.2 int=eth1
set ip int=eth0 gre=1
enable ip nat
enable ip nat log=all
add ip nat ip=192.168.10.0 mask=255.255.255.0 gblip=200.200.200.1
```

6.2.L2TP Tunnel, Firewall and Internet



Note: Be aware that with many Internet Providers it may be more suitable to turn LQR (link quality reporting) off on PPP links, and instead use LCP *Echo Request* and *Echo Reply* messages to determine link quality (echo=on). Simply add 'lqr=off echo=on' to the PPP creation command.

Router A (Router B, reverse IP addresses as per diagram above)

```
#
# L2TP Configuration
enable l2tp
enable l2tp server=both
add l2tp call="tunnel" rem="tunnel" ip=222.222.222.1 ty=virtual prec=in
set l2tp call="tunnel" pass=secret
set l2tp pass=secret

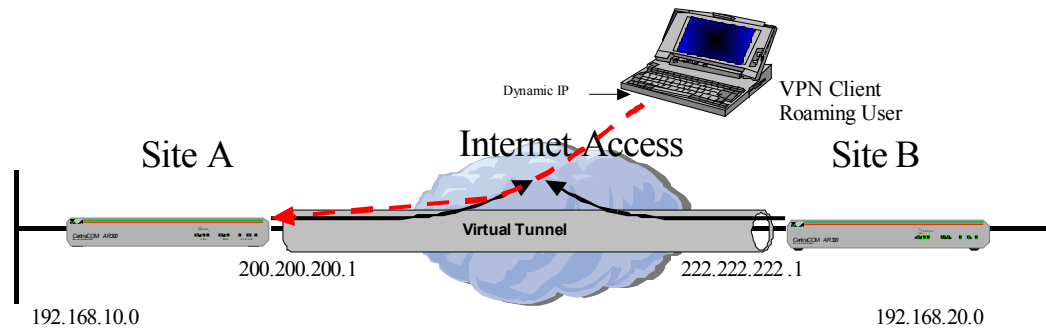
#
# ppp configuration
# Note: Tunnel is PPP10
create ppp=10 over=tnl-tunnel idle=999999999

#
# IP
#
enable ip
Add ip int=eth0 ip=192.168.10.1 mask=255.255.255.0
Add ip int=eth1 ip=200.200.200.1
add ip int=ppp10 ip=192.168.1.1
add ip rou=0.0.0.0 next=200.200.200.2 int=eth1
add ip rou=192.168.20.0 next=0.0.0.0 int=ppp10

#
# Firewall
# To enable out going ping see example 5.1.1
enable firewall
create firewall policy="main"
add firewall policy="main" int=eth0 type=private
add firewall policy="main" int=ppp10 type=private
add firewall policy="main" int=eth1 type=public
add firewall poli="main" nat=enhanced int=eth0 gblin=eth1 gblip=200.200.200.1
add fire poli=main ru=1 int=eth1 action=allow ip=200.200.200.1 proto=udp port=1701
set fire poli=main ru=1 gblip=200.200.200.1 gblp=1701 remoteip=222.222.222.1
```

7.2.IPSec (with ISAKMP), Firewall, and VPN Client

This configuration illustrates two IPSec tunnels, allowing for a remote office, a remote VPN client (roaming user), and Internet access. **The VPN client may use dynamic ip address. This example is not suitable behind a NATing device (eg: ADSL).** the introduction of the Firewall “nonat” action shown in this example.



Router A

```
set user securedelay=600
add user=secoff pass=<your password> priv=sec
# ppp configuration
create ppp=0 over=syn0
# optional set ppp=0 over=syn0 lqr=off echo=on
enable ip
Add ip int=eth0 ip=192.168.10.1 mask=255.255.255.0
Add ip int=ppp0 ip=200.200.200.1
add ip rou=0.0.0.0 next=0.0.0.0 int=ppp0
# Firewall
# To enable out going ping see example 5.1.1
enable fire
create fire poli=main
add fire poli=main int=eth0 type=private
add fire poli=main int=ppp0 type=public
add fire poli=main nat=enhanced int=eth0 gblint=ppp0
add fire poli=main rule=1 int=ppp0 action=allow ip=200.200.200.1 prot=udp port=500 gblip=200.200.200.1
gblpo=500
add fire poli=main rule=2 int=ppp0 action=nonat prot=all ip=192.168.10.1-192.168.10.254 encap=ipsec
# Rule 3 for internally initiated VPN traffic to Remote Office
add firewall poli=main ru=3 ac=nonat int=eth0 prot=all ip=192.168.10.1-192.168.10.254
set firewall poli=main ru=3 remoteip=192.168.20.1-192.168.20.254
# IPSec
# Includes VPN client configuration for user "Roaming1"
ena ipsec
create ips sas=1 prot=esp hasha=null encalg=des keym=isakmp
create ips sas=2 prot=ah mode=tunn hasha=sha keym=isakmp
create ips bundle=1 keym=isakmp string="1 and 2"
create ips pol=isakmp int=ppp0 act=permit lpo=500 rpo=500
create ips pol=remoffice int=ppp0 act=ipsec key=isakmp bund=1 peer=222.222.222.1 isa=remoffice
set ips pol=remoffice lad=192.168.10.0 lmask=255.255.255.0 rad=192.168.20.0 rmask=255.255.255.0
create ips pol=roaming1 int=ppp0 act=ipsec key=isakmp bund=1 peer=dynamic isa=roaming1
set ips pol=roaming1 lad=192.168.10.0 lma=255.255.255.0
create ips pol=internet int=ppp0 act=permit
# ISAKMP
# Note: Use Section 1.5 to enable system security and generate an Encryption Key of type GENERAL on
# router A and B
# This example uses the same network key for all ISAKMP Exchanges
cre isa pol=remoffice peer=222.222.222.1 hashalg=sha key=1
set isa pol=remoffice senddeletes=on setcommitbit=on sendnotify=on
# Only one policy is required for all dial up users.
cre isa pol=roaming1 peer=any hashalg=sha key=1 mode=aggressive
set isa pol=roaming1 senddeletes=on setcommitbit=on sendnotify=on
enable isakmp
# Optional authentication of remote sites to be done at the head office using a UAD or Radius Server
#set isa pol=roaming1 xauth=server xauthtype=generic
#add radius server=192.168.10.254 secret=secret
# OR add user=boblogin pass=bobpass
```

Router B

```

set sys name=remoffice
set user securedelay=600
add user=secoff pass=<your password> priv=sec

create ppp=0 over=syn0

enable ip
add ip int=eth0 ip=192.168.20.1
add ip int=ppp0 ip=222.222.222.1
add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0

# Firewall
# To enable out going ping see example 5.1.1
enable firewall
create firewall policy="main"
add firewall policy="main" int=eth0 type=private
add firewall policy="main" int=ppp0 type=public
add firewall poli="main" nat=enhanced int=eth0 gblin=ppp0
add firewall poli="main" ru=1 ac=allo int=ppp0 prot=udp po=500 ip=222.222.222.1 gblip=222.222.222.1
gblp=500
add firewall poli="main" ru=2 ac=non int=ppp0 prot=ALL ip=192.168.20.1-192.168.20.254 enc=ips
# Rule 3 for internally initiated VPN traffic to Head Office
add firewall poli="main" ru=3 ac=non int=eth0 prot=ALL ip=192.168.20.1-192.168.20.254
set firewall poli="main" ru=3 rem=192.168.10.1-192.168.10.254

create ipsec sas=1 key=isakmp prot=esp enc=des hasha=null
create ipsec sas=2 key=isakmp mode=tunnel prot=ah hasha=sha
create ipsec bund=1 key=isakmp string="1 and 2"
create ipsec pol=isakmp int=ppp0 act=permit lpo=500 rpo=500
create ipsec pol="remoffice" int=ppp0 ac=ipsec key=isakmp bund=1 peer=200.200.200.1 isa=remoffice
set ipsec pol="remoffice" lad=192.168.20.0 lma=255.255.255.0 rad=192.168.10.0 rmas=255.255.255.0
create ipsec pol="internet" int=ppp0 ac=permit
enable ipsec

# ISAKMP
# Note: Use Section 1.5 to enable system security and generate an Encryption Key of type GENERAL on
# router A and B
create isakmp pol=remoffice hashalg=sha pe=200.200.200.1 key=1
set isakmp pol=remoffice sendd=true setc=true sendnotify=on
enable isakmp

```

7.2.1. IPSec Client option for Example 6.3

IPSec Client Configuration for User "Roaming1"

```

#
#ISAKMP
# This example uses the same network key for all ISAKMP Exchanges
create enco key=1 type=gen val=<network key for ISAKMP Excahnge>
create isa pol=roaming1 peer=200.200.200.1 hashalg=sha key=1 mode=aggressive
set isa pol=roaming1 senddeletes=on setcommitbit=on sendnotify=on

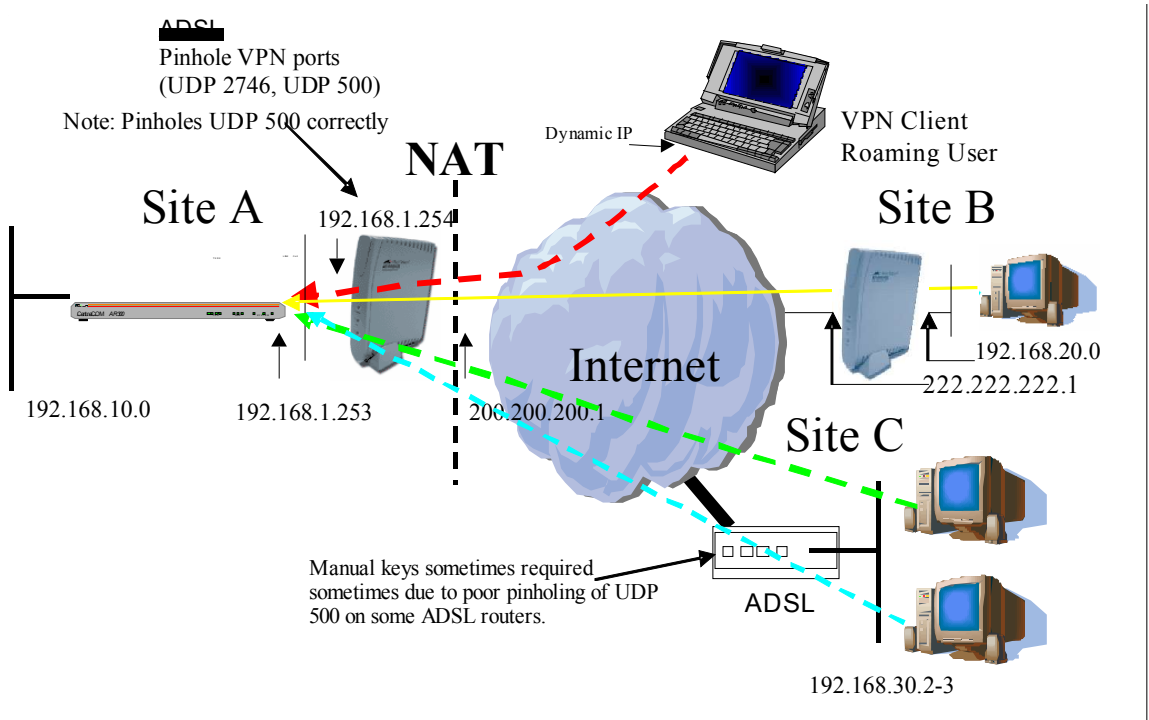
# IPSec
# Includes VPN client configuration for user "Roaming1"
create ips sas=1 prot=esp hasha=null encalg=des keym=isakmp
create ips sas=2 prot=ah mode=tunn hasha=sha keym=isakmp
create ips bundle=1 keym=isakmp string="1 and 2"
create ips pol=isakmp int=dialup act=permit lpo=500 rpo=500
create ips pol=roaming1 int=dialup act=ipsec key=isakmp bund=1 peer=200.200.200.1
set ips pol=roaming1 rad=192.168.10.0 rma=255.255.255.0
create ips pol=internet int=dialup act=permit

```

7.3. IPSec (with Manual Key) and Firewall with NAT device (eg: ADSL), plus VPN Client (with Manual Key)

This configuration illustrates two IPSec tunnels, allowing for a remote office, a remote VPN client (roaming user), and Internet access.

Note: Use the Manual Key option to get through a NATing device (eg: ADSL) between routers, or use example 6.5 (L2TP).



Router A

```

set user securedelay=600
add user=secoff pass=<your password> priv=sec
# IP
#
enable ip
Add ip int=eth0 ip=192.168.10.1
Add ip int=eth1 ip=192.168.1.253
add ip rou=0.0.0.0 next=192.168.1.254 int=eth1
# Firewall
# To enable out going ping see example 5.1.1
enable fire
create fire poli=main
add fire poli=main int=eth0 type=private
add fire poli=main int=eth1 type=public
add fire poli=main nat=enhanced int=eth0 gblint=eth1
add firewall poli=main ru=1 ac=allo int=eth1 prot=udp po=500 ip=200.200.200.1 gblip=200.200.200.1
gblpo=500
add firewall poli=main ru=2 ac=allo int=eth1 prot=udp po=2746 ip=200.200.200.1 gblip=200.200.200.1
gblpo=2746
add fire poli=main rule=3 int=eth1 action=nonat ip=192.168.10.1-192.168.10.254 prot=all encap=ipsec
# Rule 4 for internally initiated VPN traffic to Remote Office
add firewall poli=main ru=4 ac=nonat int=eth0 prot=all ip=192.168.10.1-192.168.10.254
set firewall poli=main ru=4 remoteip=192.168.20.1-192.168.20.254
add firewall poli=main ru=5 ac=nonat int=eth0 prot=all ip=192.168.10.1-192.168.10.254
set firewall poli=main ru=5 remoteip=192.168.30.2-192.168.30.3

# IPSec
# Includes VPN client configuration for user "Roaming1". The same key is used for the remote office
# and the remote VPN client PC (laptop).
# Note: Use Section 1.5 to enable system security and generate an Encryption Key of type DES on
# router A for 'Pc1' & 'Pc2' and type "general" for isakmp.
# Manual key examples are included because some adsl modems pinholes do not support isakmp correctly.
create ipsec sas=1 key=isakmp prot=esp enc=des hash=sha
create ipsec sas=3 key=manual prot=esp enc=des hash=sha enckey=1 inspi=1557 outspi=1557
create ipsec sas=4 key=manual prot=esp enc=des hash=sha enckey=1 inspi=1558 outspi=1558
create ipsec bund=1 key=isakmp string="1"
create ipsec bund=3 key=manual string="3"
create ipsec bund=4 key=manual string="4"
cre ips pol=udptunn int=eth1 act=permit lpo=2746
create ipsec pol=isakmp int=eth1 ac=permit
set ipsec pol=isakmp lp=500 rp=500
create ips pol=remoffice int=eth1 act=ipsec key=isakmp bund=1 peer=222.222.222.1 isa=global
set ips pol=remoffice lad=192.168.10.0 lmask=255.255.255.0 rad=192.168.20.1 rmask=255.255.255.0
set ipsec poli=remoffice udpt=TRUE udph=TRUE
create ipsec pol=roaming1 int=eth1 act=ipsec bund=1 peer=any key=isakmp isa=global
set ipsec pol=roaming1 lad=192.168.10.0 lma=255.255.255.0 rad=192.168.40.1
set ipsec poli=roaming1 udpt=TRUE udph=TRUE
create ipsec pol=pc1 int=eth1 act=ipsec bund=3 peer=any key=manual
set ipsec pol=pc1 lad=192.168.10.0 lma=255.255.255.0 rad=192.168.30.2
set ipsec poli=pc1 udpt=TRUE udph=TRUE
create ipsec pol=pc2 int=eth1 act=ipsec bund=4 peer=any key=manual
set ipsec pol=pc2 lad=192.168.10.0 lma=255.255.255.0 rad=192.168.30.3
set ipsec poli=pc2 udpt=TRUE udph=TRUE
create ips pol=internet int=eth1 act=permit
ena ipsec

create isakmp pol=global pe=any mode=aggressive key=2
set isakmp pol=global sendd=true sendn=true setc=true
set isakmp pol=global hear=both localid=headoffice remoteid=remote
enable isakmp

```

7.3.1. IPSec Client option for Example 6.4

IPSec Client Configuration for User "SiteB" (Isakmp key)

```
add fire poli=vpn rule=1 action=nat nattytype=enhanced int=all prot=all gblip=192.168.20.1
remoteip=192.168.10.1-192.168.10.254

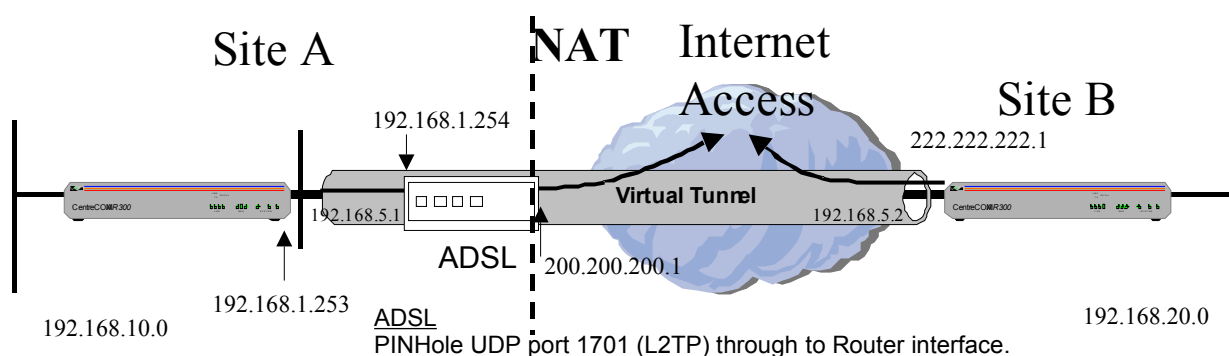
create enco key=1 type=gen val=<router A - number 2 key>
#
# IPSec
# Includes VPN client configuration for user Bob
create ips sas=1 prot=esp hash=sha encalg=des keym=isakmp enckey=1 isakmp=global
create ips bundle=1 keym=isakmp string=1
create ips pol=roaming1 int=all act=ipsec key=isakmp bund=1 peer=200.200.200.1
set ips pol=roaming1 rad=192.168.10.0 rma=255.255.255.0 lad=192.168.20.1
rmask=255.255.255.255
set ipsec poli=roaming1 udpt=TRUE udph=TRUE
create ips pol=internet int=all act=permit

create isakmp pol=global pe=200.200.200.1 mode=aggressive key=2
set isakmp pol=global sendd=true sendn=true setc=true
set isakmp pol=global hear=both localid=remote remoteid=headoffice
```

7.4. IPSec & ISAKMP (with L2TP) and Firewall router, behind NAT device (eg:ADSL)

This configuration illustrates an IPSec tunnel over L2TP to a remote office, and allows for Internet access.

Note: This solution uses Firewall with NAT and IPSec, supported from release 1.9.3. L2TP is used to Tunnel ISAKMP/IPSec through NAT process between routers (eg: ADSL). *This is NOT an IPSec client solution.*



Note: Be aware that with many Internet Providers it may be more suitable to turn LQR (link quality reporting) off on PPP links, and instead use LCP *Echo Request* and *Echo Reply* messages to determine link quality (echo=on). Simply add 'lqr=off echo=on' to the PPP creation command.

Router A

```
set user securedelay=600
add user=secoff pass=<your password> priv=sec
#
# L2TP Configuration
enable l2tp
enable l2tp server=both
add l2tp call="tunnel" rem="tunnel" ip=222.222.222.1 ty=virtual prec=in
set l2tp call="tunnel" pass=secret
set l2tp pass=secret

#
# ppp configuration
# Note: Tunnel is PPP10
create ppp=10 over=tnl-tunnel idle=999999999

#
# IP
#
enable ip
Add ip int=eth0 ip=192.168.10.1 mask=255.255.255.0
Add ip int=eth1 ip=192.168.1.253
add ip int=ppp10 ip=192.168.5.1
add ip rou=0.0.0.0 next=192.168.1.254 int=eth1
add ip rou=192.168.20.0 next=0.0.0.0 int=ppp10

#
# Firewall
# To enable out going ping see example 5.1.1
enable firewall
create firewall policy="main"
add firewall policy="main" int=eth0 type=private
add firewall policy="main" int=ppp10 type=private
add firewall policy="main" int=eth1 type=public
add firewall poli="main" nat=enhanced int=eth0 gblin=eth1 gblip=192.168.1.253
add fire poli=main ru=1 int=eth1 action=allow ip=192.168.1.253 proto=udp po=1701
set fire poli=main ru=1 gblip=192.168.1.253 gblp=1701 rem=222.222.222.1

#
# IPsec
ena ipsec
create ips sas=1 prot=esp hasha=null encalg=des keym=isakmp
create ips sas=2 prot=ah mode=tunn hasha=sha keym=isakmp
create ips bundle=1 keym=isakmp string="1 and 2"
create ips pol=isakmp int=ppp10 act=permit lpo=500 rpo=500
create ips pol=tunnel int=ppp10 act=ipsec key=isakmp bund=1 peer=192.168.5.2
set ips pol=tunnel lad=192.168.10.0 lmask=255.255.255.0 rad=192.168.20.0 rmask=255.255.255.0
#
#ISAKMP
# Note: Use Section 1.5 to enable system security and generate an Encryption Key of type GENERAL
# on router A and B
# This example uses the same network key for all ISAKMP Exchanges
cre isa pol=keys peer=192.168.5.2 hashalg=sha key=1
set isa pol=keys senddeletes=on setcommitbit=on sendnotify=on
enable isakmp
```

Router B

```
set user securedelay=600
add user=secoff pass=<your password> priv=sec
#
# L2TP Configuration
enable l2tp
enable l2tp server=both
set l2tp password="secret"
add l2tp call="tunnel" rem="tunnel" ip=200.200.200.1 ty=virtual prec=in
set l2tp call="tunnel" pass=secret

#
# ppp configuration
# Note: Tunnel is PPP10
create ppp=0 over=syn0
create ppp=10 over=tnl-tunnel idle=999999999

#
# IP
#
enable ip
Add ip int=eth0 ip=192.168.20.1 mask=255.255.255.0
Add ip int=ppp0 ip=222.222.222.1
add ip int=ppp10 ip=192.168.5.2
add ip rou=0.0.0.0 next=0.0.0.0 int=ppp0
add ip rou=192.168.10.0 next=0.0.0.0 int=ppp10

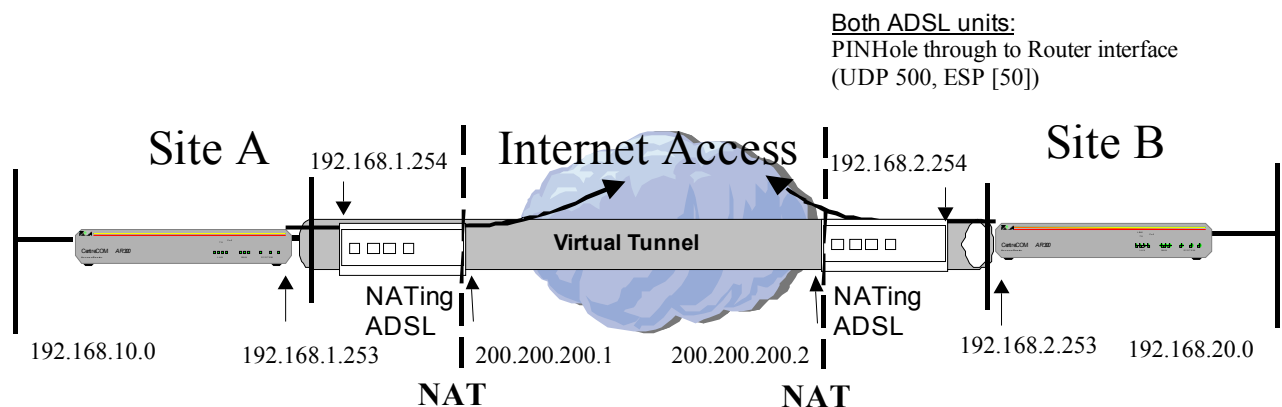
#
# Firewall
# To enable out going ping see example 5.1.1
enable firewall
create firewall policy="main"
add firewall policy="main" int=eth0 type=private
add firewall policy="main" int=ppp10 type=private
add firewall policy="main" int=ppp0 type=public
add firewall poli="main" nat=enhanced int=eth0 gblin=ppp0 gblip=222.222.222.1
add fire poli=main ru=1 int=ppp0 action=allow ip=222.222.222.1 proto=udp po=1701
set fire poli=main ru=1 gblip=222.222.222.1 gblp=1701 rem=200.200.200.1

#
# IPSec
#
ena ipsec
create ips sas=1 prot=esp hasha=null encalg=des keym=isakmp
create ips sas=2 prot=ah mode=tunn hasha=sha keym=isakmp
create ips bundle=1 keym=isakmp string="1 and 2"
create ips pol=isakmp int=ppp10 act=permit lpo=500 rpo=500
create ips pol=tunnel int=ppp10 act=ipsec key=isakmp bund=1 peer=192.168.5.1
set ips pol=tunnel lad=192.168.20.0 lmask=255.255.255.0 rad=192.168.10.0 rmask=255.255.255.0
#
#ISAKMP
# Note: Use Section 1.5 to enable system security and generate an Encryption Key of type GENERAL
# on router A and B
# This example uses the same network key for all ISAKMP Exchanges
cre isa pol=keys peer=192.168.5.1 hashalg=sha key=1
set isa pol=keys senddeletes=on setcommitbit=on sendnotify=on
enable isakmp
```

7.5. IPsec and Firewall through two NAT gateways (eg: ADSL)

This configuration illustrates an IPsec tunnel through two NATing devices (eg: NATing ADSL gateway devices). It uses release 2.2.1, which allows ISAKMP through NATing devices without the need of L2TP, because of the introduction of the 'localid' and 'remoteid' parameters. It also allows for Internet access.

A future version of this example will also accommodate VPN clients, using a new release version of the VPN client.



Router A

```
set sys name="Head Office"
set user securedelay=600
add user=secoff pass=<your password> priv=sec
# IP
#
enable ip
add ip int=eth0 ip=192.168.10.1 mask=255.255.255.0
add ip int=eth1 ip=192.168.1.253
add ip rou=0.0.0.0 next=192.168.1.254 int=eth1

# Firewall
# To enable out going ping see example 5.1.1
enable fire
create fire policy="main"
add fire policy="main" int=eth0 type=private
add fire policy="main" int=eth1 type=public
add fire poli="main" nat=enhanced int=eth0 gblin=eth1
add fire poli="main" ru=1 int=eth1 action=allow ip=192.168.1.253 prot=udp port=500
gblip=192.168.1.253 gblpo=500
add fire poli="main" ru=2 int=eth1 action=nonat prot=all ip=192.168.10.1-192.168.10.254 encap=ipsec
add fire poli="main" ru=3 int=eth0 action=nonat prot=all ip=192.168.10.1-192.168.10.254
set fire poli="main" ru=3 remoteip=192.168.20.1-192.168.20.254

# IPsec
#
ena ipsec
create ips sas=1 prot=esp hasha=null encalg=des keym=isakmp
create ips bundle=1 keym=isakmp string="1"
create ips pol=isakmp int=eth1 act=permit lpo=500
create ips pol=remoffice int=eth1 act=ipsec key=isakmp bund=1 peer=200.200.200.2 isa=remoffice
set ips pol=remoffice lad=192.168.10.0 lmask=255.255.255.0 rad=192.168.20.0 rmask=255.255.255.0
create ips pol=internet int=eth1 act=permit
#
#ISAKMP
# Note: Use Section 1.5 to enable system security and generate an Encryption Key of type GENERAL
# on router A and B
# This example uses the same network key for all ISAKMP Exchanges
cre isa pol=remoffice peer=200.200.200.2 hashalg=sha key=1
set isa pol=remoffice senddeletes=on setcommitbit=on sendnotify=on localid=headoffice
remoteid=remotel
enable isakmp
```

Router B

```
set sys name="Remote Office"
set user securedelay=600
add user=secoff pass=<your password> priv=sec

#
# IP
#
enable ip
add ip int=eth0 ip=192.168.20.1 mask=255.255.255.0
add ip int=eth1 ip=192.168.2.253
add ip rou=0.0.0.0 next=192.168.2.254 int=eth1

#
# Firewall
# To enable out going ping see example 5.1.1
enable fire
create fire policy="main"
add fire policy="main" int=eth0 type=private
add fire policy="main" int=eth1 type=public
add fire poli="main" nat=enhanced int=eth0 gblin=eth1
add fire poli="main" ru=1 int=eth1 action=allow ip=192.168.2.253 prot=udp port=500
gblip=192.168.2.253 gblpo=500
add fire poli="main" ru=2 int=eth1 action=nonat prot=all ip=192.168.20.1-192.168.20.254 encap=ipsec
add fire poli="main" ru=3 int=eth0 action=nonat prot=all ip=192.168.20.1-192.168.20.254
set fire poli="main" ru=3 remoteip=192.168.10.1-192.168.10.254

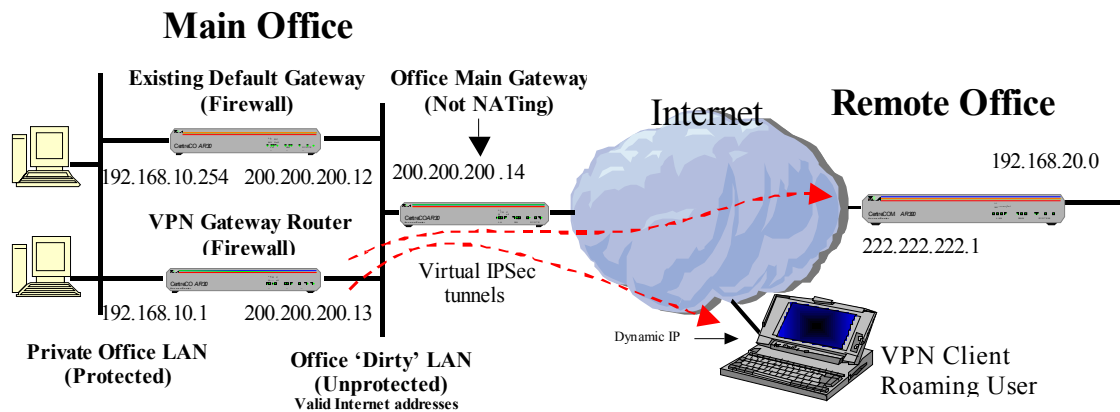
#
# IPSec
#
ena ipsec
create ips sas=1 prot=esp hasha=null encalg=des keym=isakmp
create ips bundle=1 keym=isakmp string="1"
create ips pol=isakmp int=eth1 act=permit lpo=500
create ips pol=remoffice int=eth1 act=ipsec key=isakmp bund=1 peer=200.200.200.1 isa=remoffice
set ips pol=remoffice lad=192.168.20.0 lmask=255.255.255.0 rad=192.168.10.0 rmask=255.255.255.0
create ips pol=internet int=eth1 act=permit

#
#ISAKMP
# Note: Use Section 1.5 to enable system security and generate an Encryption Key of type GENERAL
# on router A and B
# This example uses the same network key for all ISAKMP Exchanges
cre isa pol=remoffice peer=200.200.200.1 hashalg=sha key=1
set isa pol=remoffice senddeletes=on setcommitbit=on sendnotify=on localid=remotel
remoteid=headoffice
enable isakmp
```

7.6.Two Gateways; Firewall with IPsec and ISAKMP to VPN Client & Remote Office

This example is intended for networks where there is an existing default gateway (behind a 'dirty LAN') which needs to remain in service. An Allied Telesyn router is introduced as an alternative gateway, intended only for providing the IPsec VPN tunnels.

The new VPN Gateway Router defines the default gateway router as a static RIP neighbour to advertise a route to the dynamic address of the roaming VPN client.



Router A (Allied Telesyn VPN Gateway router)

```

set system name="VPN Gateway"

set user securedelay=600
add user=secoff pass=<your password> priv=sec
add user=boblogin pass=bobpass
add user=remoffice pass=remoffice

enable ip
add ip int=eth1 ip=200.200.200.13 mask=255.255.255.240
add ip int=eth0 ip=192.168.10.1
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth1 next=200.200.200.14
add ip route template=vpnclient int=eth1 next=200.200.200.14
# RIP is used to advertise a host specific route of the VPN client to the default gateway
add ip rip int=eth0 ip=192.168.10.254 send=rip2

enable firewall
create firewall policy=main
add firewall policy=main int=eth0 type=private
add firewall policy=main int=eth1 type=public
add firewall poli=main nat=enhanced int=eth0 gblin=eth1
add firewall poli=main ru=1 ac=allo int=eth1 prot=udp po=500 ip=200.200.200.13
gblip=200.200.200.13 gblpo=500
add firewall poli=main ru=2 ac=non int=eth1 prot=ALL ip=192.168.10.1-192.168.10.254 enc=ips
# Rule 3 for internally initiated VPN traffic to Remote Office
add firewall poli=main ru=3 ac=nonat int=eth0 prot=all ip=192.168.10.1-192.168.10.254
set firewall poli=main ru=3 remoteip=192.168.20.1-192.168.20.254

set enco sw stacchannels=0

create ipsec sas=1 key=isakmp prot=esp enc=des hasha=null
create ipsec sas=2 key=isakmp prot=ah mode=tunn hasha=sha
create ipsec bund=1 key=isakmp string="1 and 2"
create ipsec pol="isakmp" int=eth1 ac=permit
set ipsec pol="isakmp" lp=500 rp=500
create ips pol=remoffice int=eth1 act=ipsec key=isakmp bund=1 peer=222.222.222.1 isa=remoffice
set ips pol=remoffice lad=192.168.10.0 lmask=255.255.255.0 rad=192.168.20.0 rmask=255.255.255.0
create ipsec pol="roaming1" int=eth1 ac=ipsec key=isakmp bund=1 peer=DYNAMIC
  iproutetemplate=vpnclient isa=roaming1
set ipsec pol="roaming1" lad=192.168.10.0 lma=255.255.255.0 rname=roaming1
create ipsec pol="internet" int=eth1 ac=permit
enable ipsec
#
#ISAKMP
# Note: Use Section 1.5 to enable system security and generate an Encryption Key of type GENERAL
# on router A and B
create isakmp pol=remoffice pe=222.222.222.1 hashalg=sha key=1
set isakmp pol=remoffice sendd=true setc=true
create isakmp pol=roaming1 pe=any hashalg=sha key=1
set isakmp pol=roaming1 sendd=true setc=true sendnotify=on
set isa pol=roaming1 xauth=server xauthtype=generic
enable isakmp

```

Existing Default Gateway Router

Configured to receive RIP. The address of the VPN Gateway Router (192.168.10.1) is configured as the only trusted static RIP neighbour. Also configure static route for remote office subnet (192.168.20.0), using VPN Gateway Router as next hop.

Example of VPN Client

```

cre enco key=1 type=gen val=1234567890

cre isakmp policy=roaming1 hashalg=sha peer=200.200.200.13 key=1
set isakmp policy=roaming1 senddeletes=on setcommitbit=on
set isakmp policy=roaming1 xauth=client xauthname=boblogin xauthpass=bobpass

cre ipsec sas=1 key=isakmp prot=esp encal=des hasha=null
cre ipsec sas=2 key=isakmp prot=ah mode=tunnel hasha=sha
cre ipsec bund=1 key=isakmp string="1 and 2"

cre ipsec pol=permit int=dialup act=permit lpo=500 rpo=500
cre ipsec poli=roaming1 int=dialup act=ipsec key=isakmp bundle=1 peer=200.200.200.13
set ipsec poli=roaming1 lna=roaming1 rad=192.168.10.0 rmas=255.255.255.0
cre ipsec poli=internet int=dialup act=permit

```

Router B (Remote Office Router)

```
set system name="Remote Office"

set user securedelay=600
add user=secoff pass=<your password> priv=sec

create ppp=0 over=syn0
# optional set ppp=0 over=syn0 lqr=off echo=on

enable ip
add ip int=ppp0 ip=222.222.222.1 mask=255.255.255.0
add ip int=eth0 ip=192.168.20.1
add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0

enable firewall
create firewall policy=main
add firewall policy=main int=eth0 type=private
add firewall policy=main int=ppp0 type=public
add firewall poli=main nat=enhanced int=eth0 gblin=ppp0
add firewall poli=main ru=1 ac=allo int=ppp0 prot=udp po=500 ip=222.222.222.1 gblip=222.222.222.1
gblpo=500
add firewall poli=main ru=2 ac=non int=ppp0 prot=ALL ip=192.168.20.1-192.168.20.254 enc=ips
# Rule 3 for internally initiated VPN traffic to Main Office
add firewall poli=main ru=3 ac=nonat int=eth0 prot=all ip=192.168.20.1-192.168.20.254
set firewall poli=main ru=3 remoteip=192.168.10.1-192.168.10.254

set enco sw stacchannels=0
create ipsec sas=1 key=isakmp prot=esp enc=des hasha=null
create ipsec sas=2 key=isakmp prot=ah mode=tunn hasha=sha
create ipsec bund=1 key=isakmp string="1 and 2"
create ipsec pol="isakmp" int=ppp0 ac=permit
set ipsec pol="isakmp" lp=500 rp=500
create ips pol=mainoffice int=ppp0 act=ipsec key=isakmp bund=1 peer=200.200.200.13 isa=mainoffice
set ips pol=mainoffice lad=192.168.20.0 lmask=255.255.255.0 rad=192.168.10.0 rmask=255.255.255.0
create ipsec pol="internet" int=ppp0 ac=permit
enable ipsec
#
#ISAKMP
# Note: Use Section 1.5 to enable system security and generate an Encryption Key of type GENERAL
# on router A and B
create isakmp pol=mainoffice peer=200.200.200.13 hashalg=sha key=1
set isakmp pol=mainoffice sendd=true setc=true sendnotify=on
set isa pol=mainoffice xauth=client xauthname=remoffice xauthpass=remoffice
enable isakmp
```

7.7. Notes on IPSec Testing and Verification

Testing of an IPSec tunnel.

The following are precautions to testing through IPSec tunnels:

- The 'ip local' ip address is best left at default. If 'ip local' is set to an address other default, this may invalidate ISAKMP negotiation.
- Do not expect to test sending traffic through the IPSec tunnel by pinging from IPSec router to IPSec router. You must test between hosts or servers behind the IPSec router gateways (LAN to LAN), to ensure this traffic will match the IPSec tunnel policy address selectors.

Verification of an IPSec tunnel.

It is good practice to confirm that traffic is being encrypted. A good initial check is to observe the ISAKMP negotiation entries in the system log ('sh log'). This ISAKMP check is only valid if you are using ISAKMP (ie: not manual keys). There will be several phases of negotiation, and they should indicate successful completion. If you can see no negotiation entries in the log, or if you only see an initial start and no completed phases, then this suggests a configuration error, or no ISAKMP negotiation received from the peer. Checking 'sh fire event' will allow you to see what traffic has been received from the peer, and if it has been allowed by the firewall.

Confirmation that traffic is actually being encrypted is best seen by using a counter command such as SH IPSEC POLI=TUNNEL COUNT. Every time you ping a set of 5 pings, the "outProcessDone" counters (in the Outbound Packet Processing Counters section) should increment by 5. Also, the echo reply traffic should cause the "inProcessDone" counters (in the Inbound Packet Processing Counters section) to increment by 5.

It is important that the IPSec policies be configured in the correct order.

If you have a "permit" IPSec Policy with open policy address selectors, (intended to allow unencrypted Internet access), then this policy must be configured last – after the ACTION=IPSEC POLICIES. Otherwise this Permit Policy will process all traffic and no traffic will be encrypted. The order of the IPSec policies can be checked by the SH IPSEC POLI command. In the output of this command, each policy is assigned a position number.

Troubleshooting of an IPSec tunnel.

If problems continue, then ISAKMP and IPSec debugging modes may be used. Turning on all debug modes is rather verbose, so we recommend basic ISAKMP debugging initially. The routine below also illustrates a method to easily disable the debugging mode after testing.

- 'dis isakmp debug=all' (This may give an error, but our intention is to have this command in the command buffer)
- 'ena isakmp debug=state' (This should allow you to see if ISAKMP is operating)
- If more detail is needed then issue this command 'ena isakmp debug=trace'
- To disable debugging after your test, simply press up arrow once (or twice) to recall the disable command, then press enter. (VT-100 arrows may need to be enabled).

If the basic ISAKMP debugging modes do not reveal a problem to you, then all debugging modes should be enabled and captured to a text file and sent to your support centre. Please capture the debugging output from the router attempting to initiate IPSec and ISAKMP by using 'ena ipsec poli=tunnel debug=all' and 'ena isakmp debug=all'. Also capture 'sh log' to show ISAKMP log entries (as mentioned above), and capture 'sh fire event' and 'sh debug'. Forward all this debugging to your local technical support for analysis. Your local support center also have access to advanced support centers if necessary. (Allied Telesyn offers technical assistance in partnership with our authorised distributors and resellers. For technical assistance, please contact the authorised distributor or reseller in your area). Please refer to <http://www.alliedtelesyn.co.nz/support/support.html> for a list of Authorised Distributor & Reseller

