INTERNET SECURITY ROUTER FAQ

Release date: 5/4/2004

1 Introduction

This document contains the frequently asked questions (FAQ) for SL-series Internet Security Router including SL-1000, SL-500 and possibly the future SL- models.

2 FAQ

2.1 General

2.1.1 Why can't I login to the Internet Security Router? How do I know what is wrong?

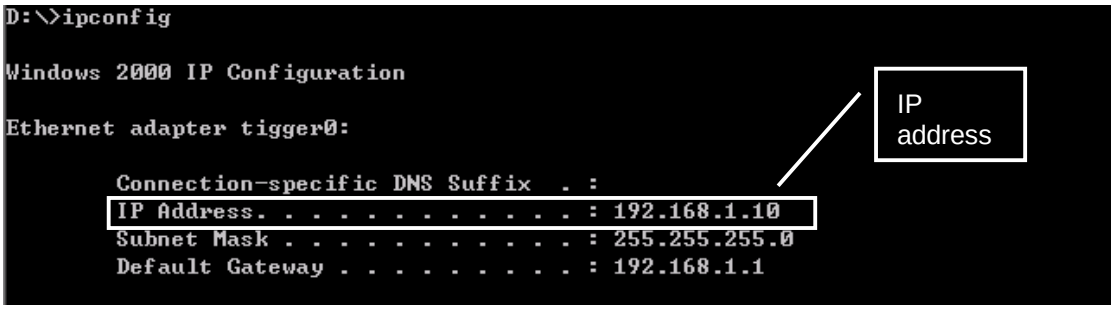
There are several reasons that you cannot login to the Internet Security Router, e.g. power not connected, Ethernet cable not connected, your PC and the Internet Security Router not in the same subnet or incorrect username and/or password. Please follow the steps below to connect back to the Internet Security Router:

1. Make sure that the Internet Security router is powered on. The color of the POWER LED is solid green. If the POWER LED is not lit, make sure that the AC adapter is connected to a power source and the connector is firmly attached to the power connector on the Internet Security Router.
2. Make sure that the Ethernet cable connecting your PC and the Internet Security Router is firmly inserted on one of the LAN ports of the Internet Security Router and the network card on your PC. You may pull the Ethernet cable to check if the cable is firmly connected. You should also verify that the LED of the corresponding LAN port is lit in solid or flashing green.
3. Check if PC's IP and LAN IP of SL-series are in the same subnet. Please see "How do I know if my PC and the LAN of my Internet Security Router are in the same subnet?" and "How to configure my PC and the Internet Security Router to reside in the same subnet?" for instructions.
4. Check if the username and login password that you entered are correct.

2.1.2 How to find out the IP address of my PC?

For Windows PC:

1. From the Start menu, select **Run**.
2. Enter **cmd** in the text field, and then click in "**OK**" button.
3. Enter **ipconfig** in the Command Prompt window. The following figure shows where the IP address of your network card is displayed. Note that if you have more than one network card installed on your computer, make sure you get the IP address from the correct network card.



2.1.3 How do I know if my PC and the LAN of my Internet Security Router are in the same subnet?

Follow the procedures below to check if your PC and the Internet Security Router are in the same subnet.

1. Get the network address of your PC and the Internet Security Router. To find out the network address, do a binary "&" operation on the IP address and the subnet mask. For example, the IP address of your Internet Security Router is 192.168.1.1 and the subnet mask is 255.255.255.0, then the network address is 192.168.1.0, which is calculated by (192.168.1.1) & (255.255.255.0).
2. If your PC and the Internet Security Router have the same network address, then they are in the same subnet.

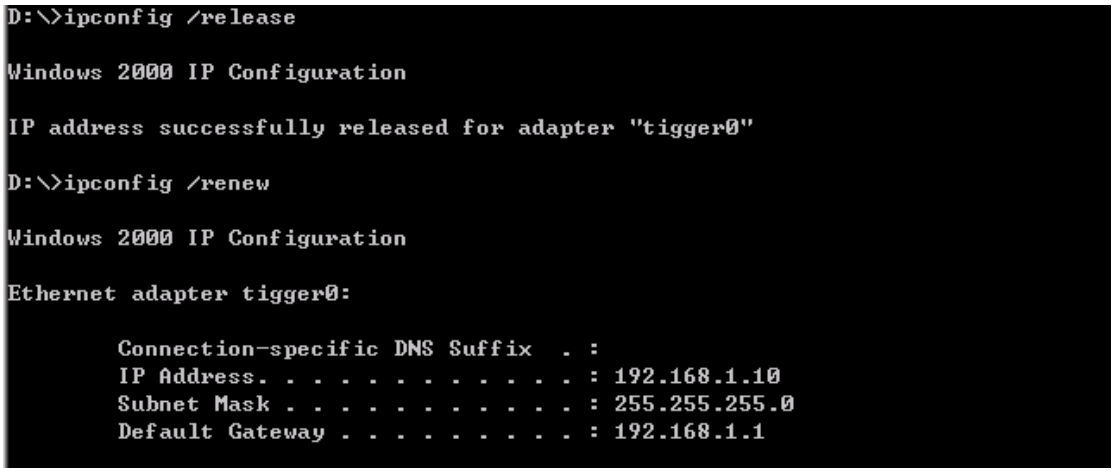
2.1.4 How to configure my PC and the Internet Security Router to reside in the same subnet?

The configuration procedure depends on whether the DHCP server is enabled or not and also the operating system on your PC. We'll only describe the procedures for the Windows 2000. For other operating systems, please refer to the user manual for details.

Scenario 1: DHCP server is enabled:

On windows 2000 computer do the flowing：

1. In the Windows task bar, click the **<Start>** button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network and Dial-up Connections** icon.
3. In the Network and Dial-up Connections window, right-click the **Local Area Connection** icon, and then select **Properties**.
4. In the Local Area Connection Properties dialog box, select **Internet Protocol (TCP/IP)**, and then click **<Properties>** button.
5. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled **Obtain an IP address automatically**. Also click the radio button labeled **Obtain DNS server address automatically** or enter IP addresses of your DNS servers.
6. Click **<OK>** button twice to confirm and save your changes, and then close the Control Panel.
7. From the Start menu, select **Run**.
8. Enter **cmd** in the open field and then click on **OK** button. You'll see the Command Window displays.
9. Enter **ipconfig/release** in the Command Window to release existing IP lease.
10. Enter **ipconfig/renew** in the Command Windows to obtain a new IP lease. The following figure shows the information you'll get after renewing an IP lease from the DNS server.



Scenario 2: DHCP server is disabled:

On windows 2000 computer do the flowing：

1. In the Windows task bar, click the **<Start>** button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network and Dial-up Connections** icon.
3. In the Network and Dial-up Connections window, right-click the **Local Area Connection** icon, and then select **Properties**.
4. In the Local Area Connection Properties dialog box, select **Internet Protocol (TCP/IP)**, and then click **<Properties>** button.
5. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled **Use the following IP address** and enter an IP address for your PC. Make sure that this IP address is in the same subnet as that for the Internet Security Router LAN IP.
6. Enter the subnet mask. The value is the same as what is configured in the LAN IP configuration page on the Internet Security Router.
7. Enter the Default Gateway IP address. This is the LAN IP of the Internet Security Router.
8. Enter IP addresses of the DNS servers provided by your ISP.
9. Click **<OK>** button twice to confirm and save your changes, and then close the Control Panel.

For example: LAN IP of your Internet Security Router is 192.168.1.1 and subnet mask is 255.255.255.0. You can then set your PC's IP address to192.168.1.10 and subnet mask to 255.255.255.0.

2.2 WAN

2.2.1 Why can't my Internet Security Router get an IP from my ISP?

Go through the following steps to eliminate the causes of failing to obtain an IP address from your ISP.

1. Check if the Internet Security Router and/or the ADSL or cable modem is powered on. Turn on the power if necessary.
2. Check if the WAN LED is in solid or flashing green. If the WAN LED is off, make sure that the Ethernet cable connecting the Internet Security Router and your modem is firmly attached to the Ethernet connectors on both devices.
3. Check if the LED indicating the connection between your ADSL or cable modem and your ISP is lit. If this LED is off, that means the connection is down. You may have to call your ISP to find out why the connection is down.
4. Open the WAN configuration page and click on the Apply button to re-establish the connection to your ISP.

2.2.2 What is Dial-on-Demand and Keep Alive? Which one shall I use?

Dial-on-demand and keep alive options are available only when the WAN connection mode is set to PPPoE. Dial-on-demand can terminate and resume traffic at the PPPoE interface based on the data inactivity timeout period configured for the interface, without any user intervention. It terminates a PPPoE session after the lapse of the inactivity timeout period and automatically re-establishes a PPPoE session after traffic resumes. This option is useful when your broadband service charge is based on the amount of time connected because the Internet Security Router will maintain connection only when there is traffic. Note that the update interval setting for the Internet time server must be greater than the inactivity timeout period configured for the dial-on-demand.

Keep alive can keep your service connected even when there is no traffic. This option will provide

2.2.3 MAC Cloning

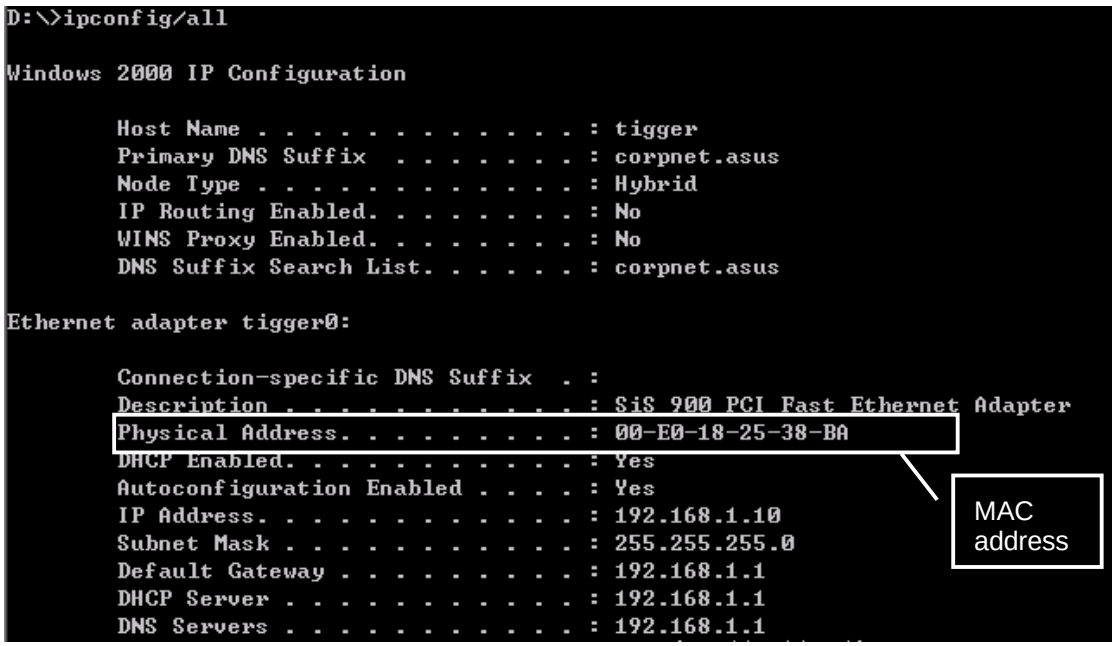
2.2.3.1 What is MAC address?

The unique hardware address programmed into the Ethernet and Token Ring adapters that identify a network card from all others.

2.2.3.2 How to find out the MAC address of my network card?

For Windows PC:

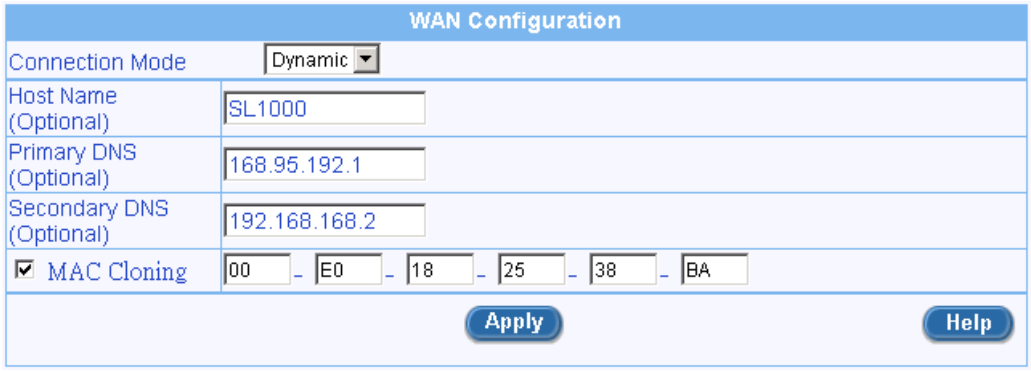
1. From the Start menu, select **Run**.
2. Enter **cmd** in the text field, and then click in "**OK**" button.
3. Enter **ipconfig/all** in the Command Prompt. The following figure shows where the MAC address of your network card is displayed. Note that if you have more than one network card installed on your computer, make sure you get the MAC address from the correct network card.



2.2.3.3 How to configure MAC cloning?

MAC cloning option is available only when Dynamic mode (i.e. DHCP client) is selected for the WAN connection mode. Follow the procedures below to configure MAC cloning. is configured Configured MAC Cloning(Only in Dynamic Mode) using WAN→WAN→MAC Cloning.

1. Open the WAN configuration page.
2. Select "Dynamic" for the WAN connection mode.
3. Check the check box for MAC Cloning and enter the MAC address in the space provided (see the following figure). To find the MAC address for your PC, please refer to "How to find out the MAC address of my network card?" for instructions.



2.2.4 Why can't I see the default gateway IP after completing the configuration for the WAN port in DHCP or PPPoE connection mode?

Sometimes this may happen. Just lick on Apply button again to refresh the screen.

2.3 LAN

2.3.1 Why is there no response from the browser after the LAN IP of the Internet Security is changed?

This is because LAN IP was changed, and the browser still waits for the response from the old IP. You'll have to connect to the router using the new IP address. Note that you may have to change the IP of your PC if you had configured its IP manually or renew the IP lease of your PC if you had configured it to receive IP from the DHCP server. Please see "How to configure my PC and the Internet Security Router to reside in the same subnet?" for instructions.

2.3.2 Why can't I login into the Internet Security Router after its LAN IP is changed?

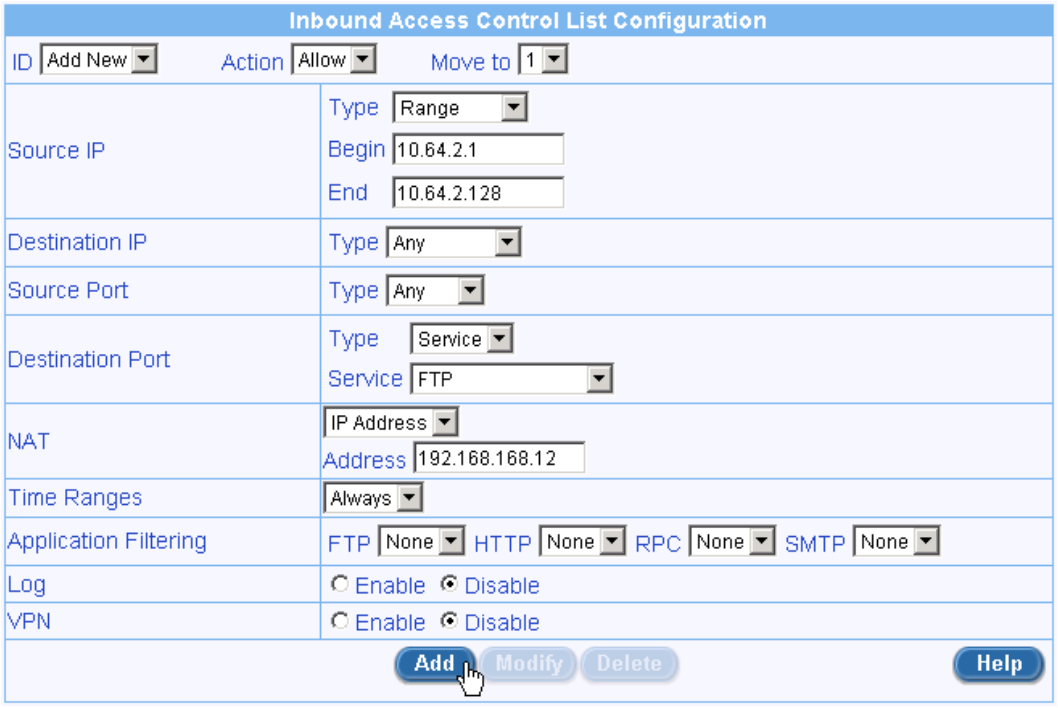
To reconnect your PC and the Internet Security Router after its LAN IP is changed, you need to make sure that your PC's IP address is in the same subnet as that of the Internet Security Router. Please see "How do I know if my PC and the LAN of my Internet Security Router are in the same subnet?" and "How to configure my PC and the Internet Security Router to reside in the same subnet?" for instructions.

2.4 Firewall and NAT

2.4.1 How to setup a virtual server?

It is best explained using an example. Let's say you want to set up a FTP server in your LAN and have the firewall control the access and offer protection for the FTP server. The following figure illustrates how an inbound ACL rule is created for the FTP server to control access of the server. This ACL rule only allows hosts with the IP in the range of 10.64.2.1 to 10.64.2.128 to access the FTP server. Note that the IP address of the FTP server is 192.168.168.12, which is a private IP address.

1. Open the inbound ACL rule configuration page (Firewall **è** Inbound ACL).
2. Enter source IP to specify which hosts are allowed to access the FTP server – in this case, hosts w/ IP in the range of 10.64.2.1 to 10.64.2.128.
3. Select "Service" for the destination port type and also select "FTP" service from the service drop-down list.
4. Enter the IP address of the FTP server
   a) Select "IP Address" as the NAT type.
   b) Enter FTP server IP address in the NAT Address field: in this case, 192.168.168.12.
5. You may enter additional options for access control, such as time range and application filtering for FTP.

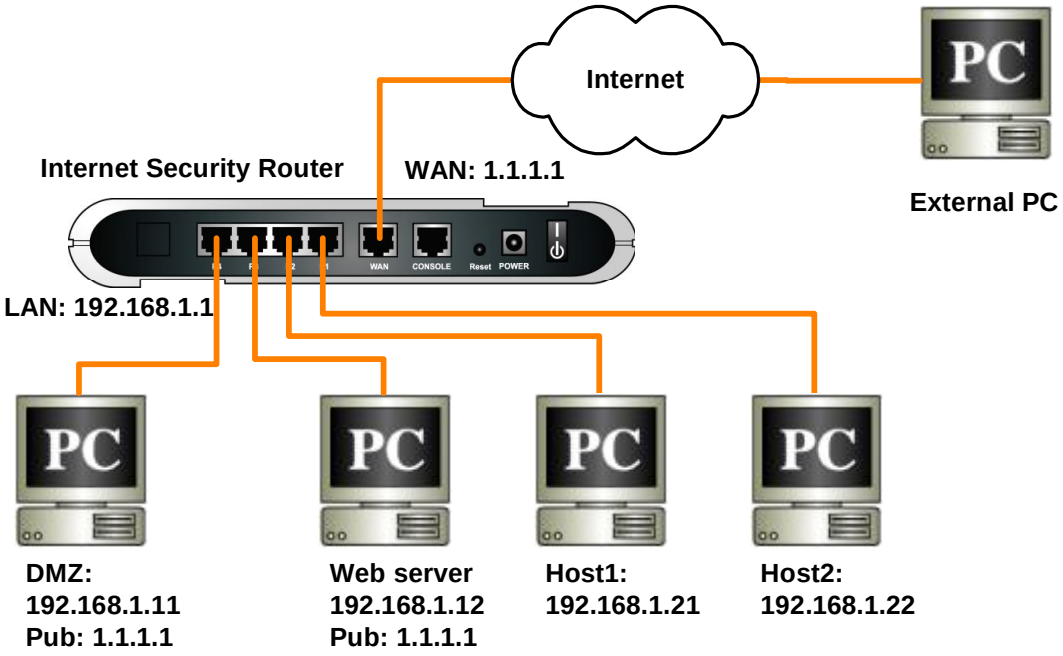


2.4.2 How to setup virtual DMZs?

The number of virtual DMZ hosts supported depends on the number of public IP addresses provided by your ISP.

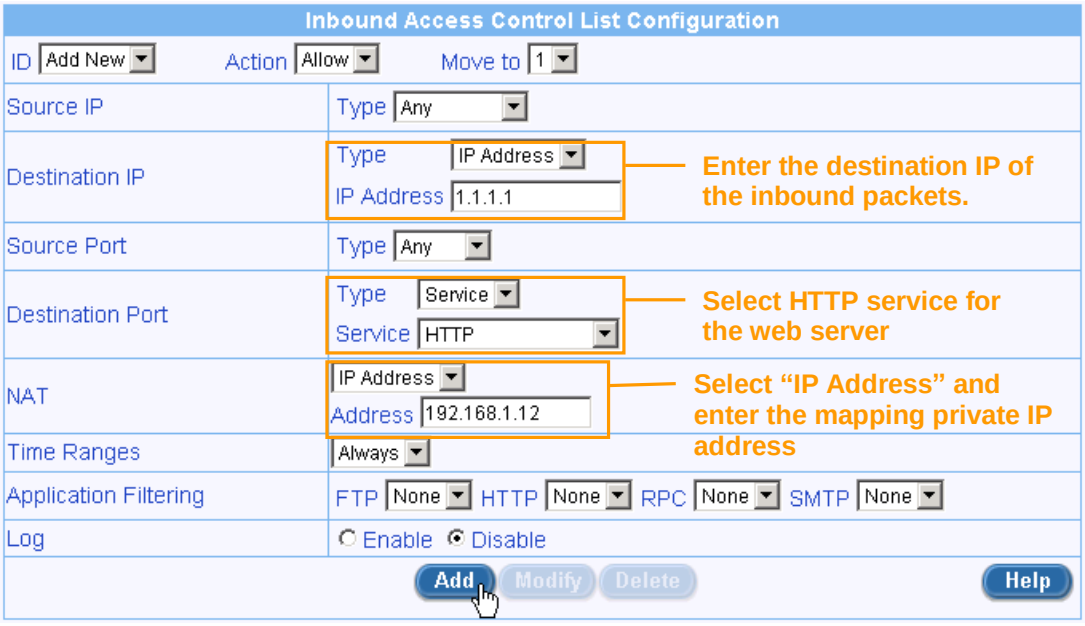
2.4.2.1 Single DMZ

The following figure shows an example of a network supporting a DMZ, a web server as well as several local hosts accessing the Internet via NAT. The address mapping for the DMZs and the web server are also illustrated in the figure – DMZ: (192.168.1.11 ↔ 1.1.1.1), and the web server (192.168.1.12 ↔ 1.1.1.1). The local hosts, host1 and host2, access the Internet using the WAN IP address: 1.1.1.1. This scenario is probably the most often encountered scenario by most users having only one public IP address provided by ISPs.

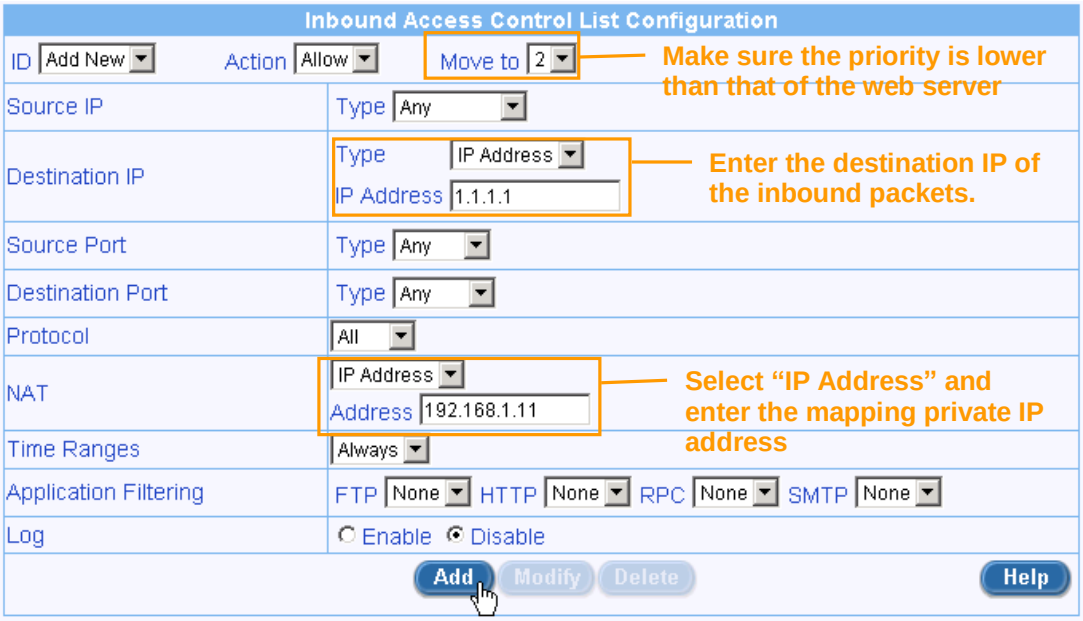


Follow these steps to set up the Internet Security Router to support multiple DMZs.

1. Create a firewall ACL rule for the web server



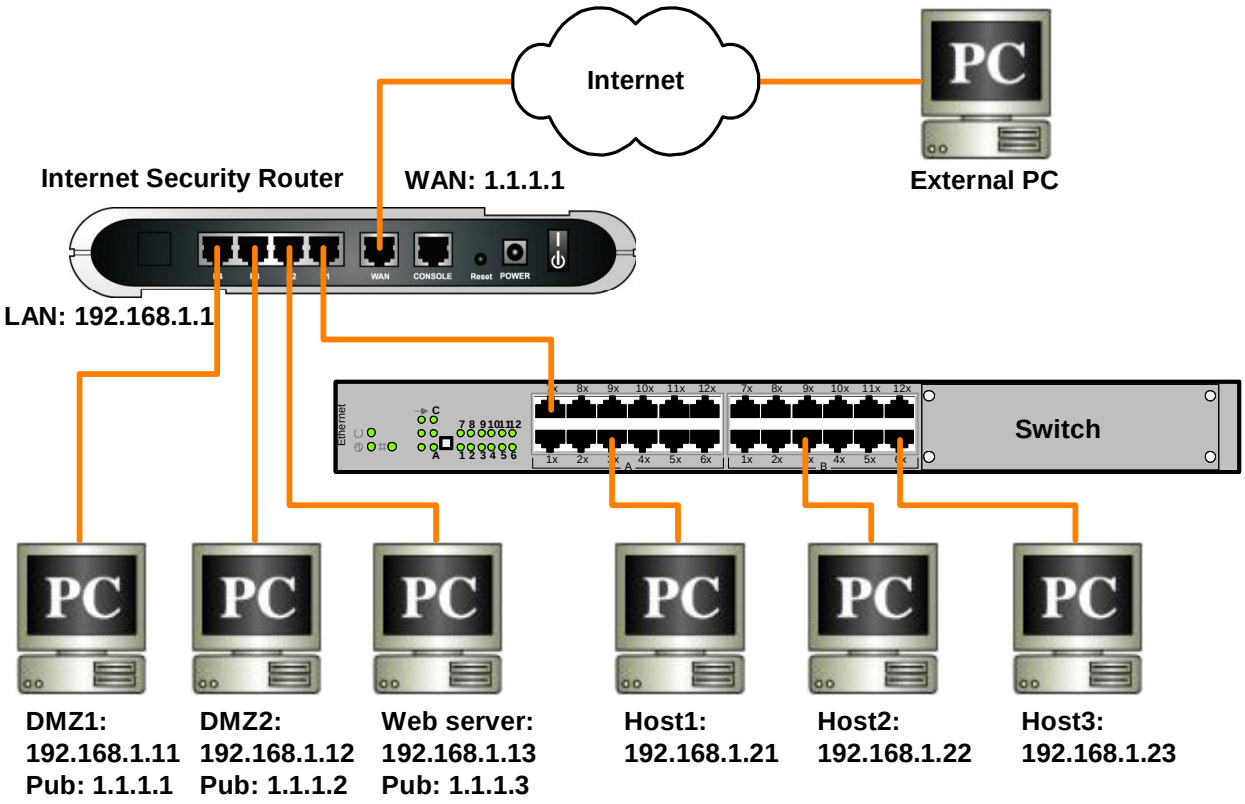
2. Create a firewall ACL rule for the DMZ



3. Create an outbound policy for local hosts to access the Internet. This step may be skipped because the Internet Security Router comes with a default firewall outbound ACL rule to allow all the outbound packets to use NAT (using the WAN IP address) to access the Internet.

2.4.2.2 Multiple DMZs

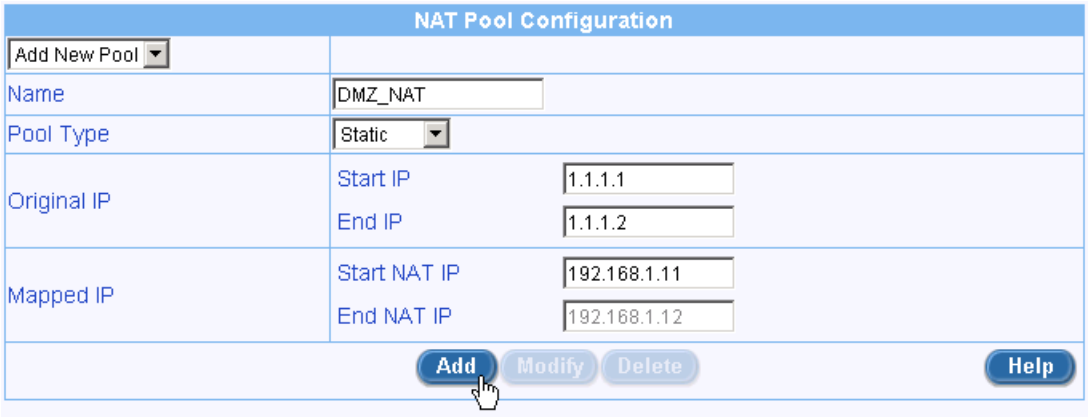
The following figure shows an example of a complicated network supporting multiple DMZs, a web server as well as several local hosts accessing the Internet via NAT. The address mapping for the DMZs and the web server are also illustrated in the figure – DMZ1: (192.168.1.11 ↔ 1.1.1.1), DMZ2: (192.168.1.12 ↔ 1.1.1.2), and the web server (192.168.1.13 ↔ 1.1.1.3). The local hosts, host1 to host3, access the Internet using the WAN IP address: 1.1.1.1.



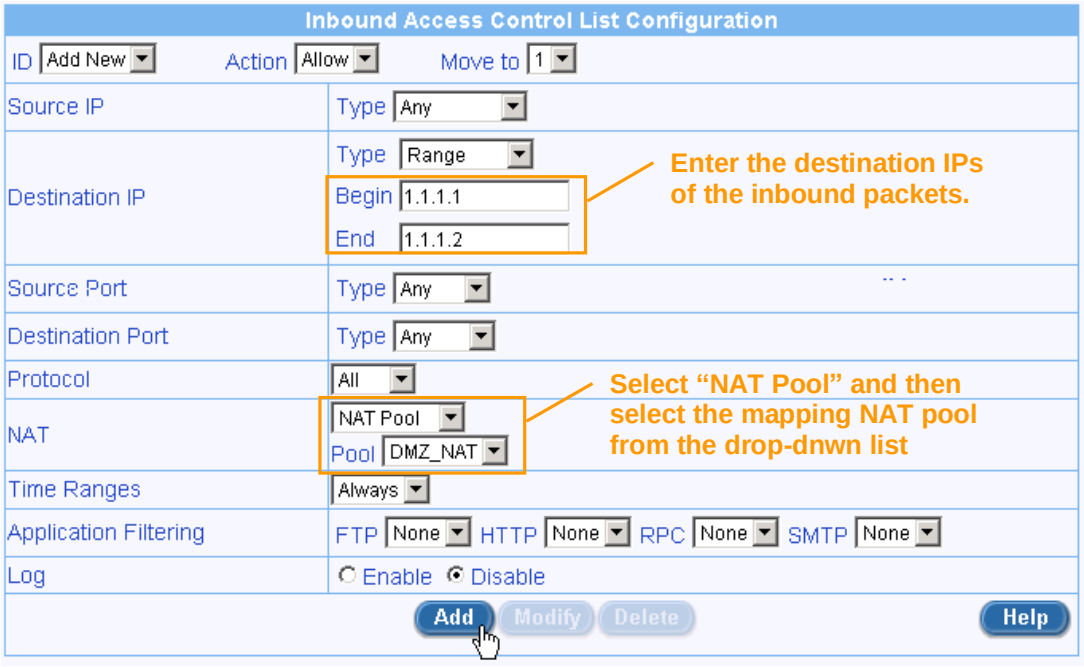
Follow these steps to set up the Internet Security Router to support multiple DMZs.

1. Setup an inbound policy for the DMZs

   a) Create a "static" NAT address pool for the block of public IP addresses provided by your ISP.

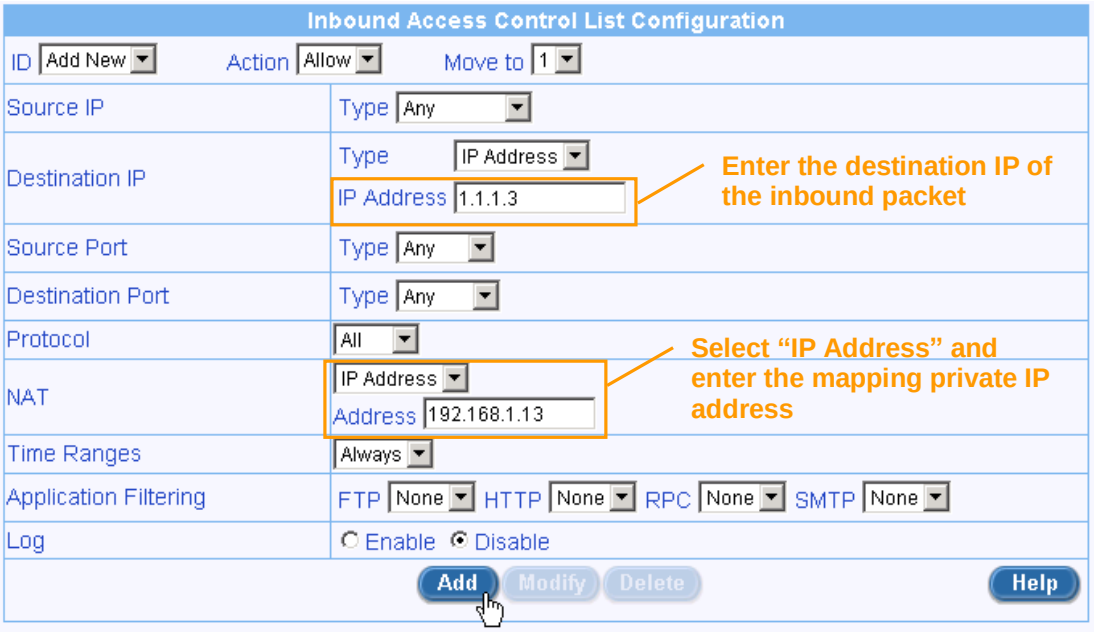


   b) Create a firewall ACL rule for the DMZs



2. Create an inbound policy for the web server

   a) Create a firewall ACL rule for the web server

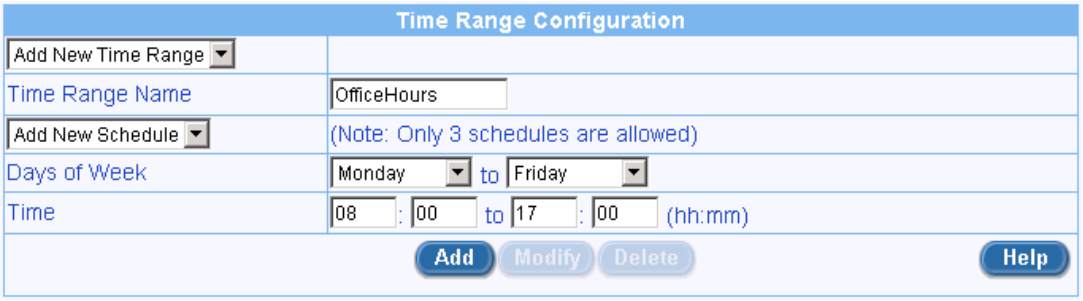


3. Create an outbound policy for local hosts to access the Internet. This step may be skipped because the Internet Security Router comes with a default firewall outbound ACL rule to allow all the outbound packets to use NAT (using the WAN IP address) to access the Internet.

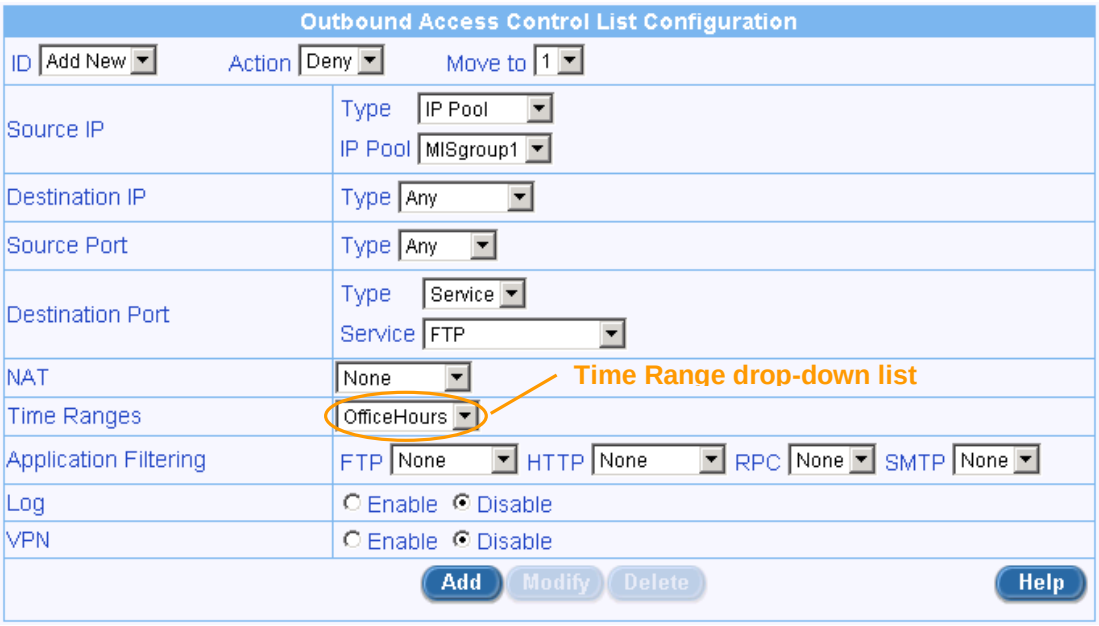
2.4.3 How to setup an ACL using time range?

Time range records can be used to set schedule for an ACL rule. ACL rules associated with a time range record will be active only during the scheduled period. The following illustrates the steps required to create a time range.

1. Create a time range: enter the information in the Time Range Name, Days of Week and Time fields and then click in the “Add” button to set up the time range.



2. Associate the time range to an outbound ACL rule (outbound, inbound or group ACL) by selecting an existing time range from the Time Range drop-down list. The following figure shows that MISgroup1 is denied TP access during office hours.



2.4.4 How to setup an ACL with a preconfigured service, e.g. ICQ- 2000?

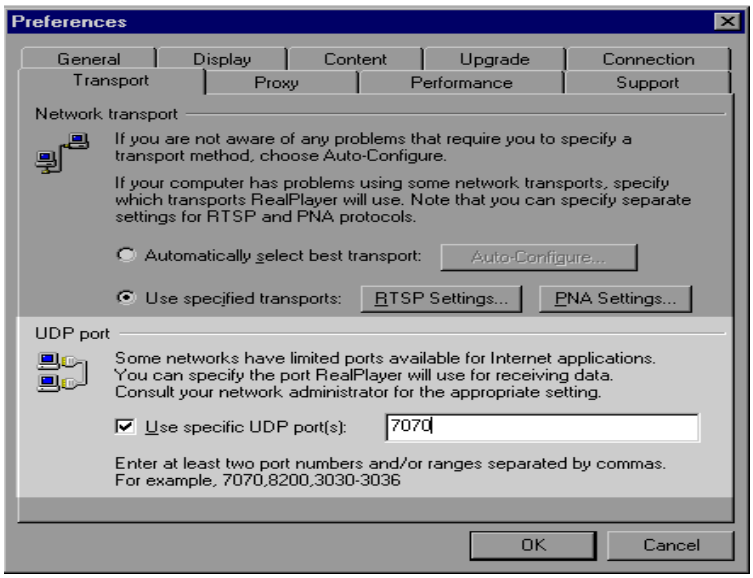
1. Open the outbound or inbound or group ACL rule configuration page (Firewall **è** Outbound ACL; Firewall **è** Inbound; Remote Access **è** Group ACL). Please refer to the following for reference.
2. Select an action type for this ACL – Deny or Allow.
3. Enter information for the source IP, destination IP and source port if necessary.
4. Select “Service” for the destination port type and then choose “ICQ-2000” from the service drop-down list.
5. You may want to enable NAT and/or time range if desired.
6. You can also enable event logging for this ACL if needed.
7. Set the ACL priority by selecting a number from the “Move to” drop-down list.
8. Click on “Add” button to save this ACL.

Outbound Access Control List Configuration	
ID Add New Action Allow Move to 1	
Source IP	Type Any
Destination IP	Type Any
Source Port	Type Any
Destination Port	Type Service Service ICQ-2000
NAT	None
Time Ranges	Always
Application Filtering	FTP None HTTP None RPC None SMTP None
Log	Enable Disable
VPN	Enable Disable
Add Modify Delete	Help

2.4.5 How to setup an ACL for a new application?

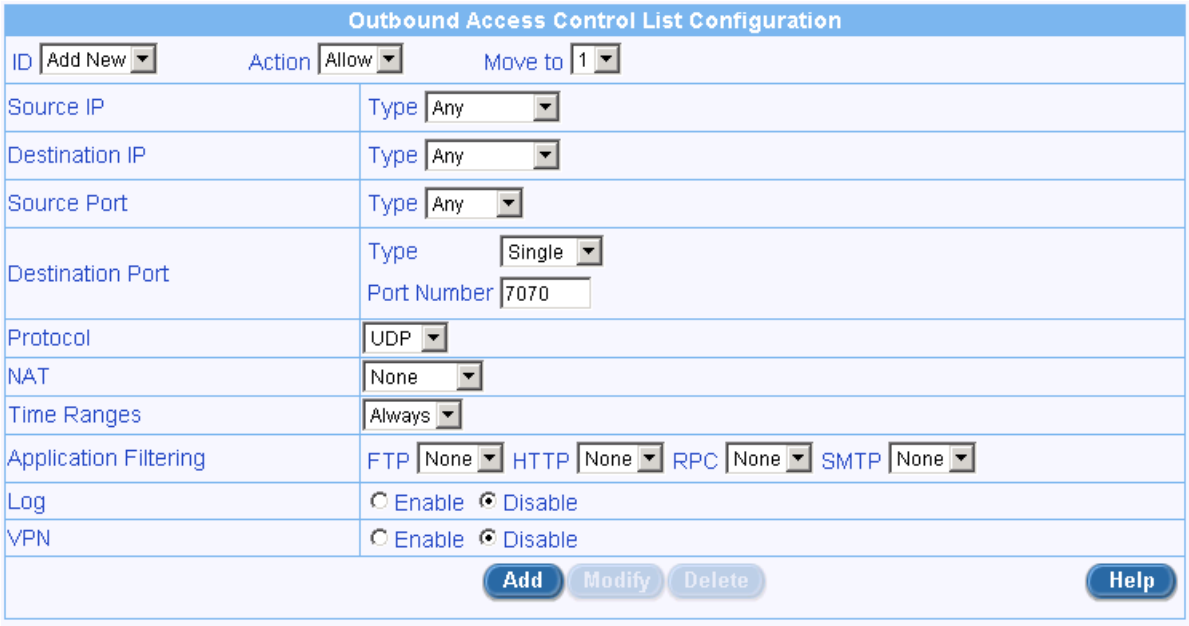
You can set up an ACL to support an application as long as the port numbers and protocol used by that application are known. To find out this information, you'll have to contact the application vendor. Usually, the web site of the application vendor is a good source to start with. Let's take the RealPlayer version 8 as an example to demonstrate how to create an ACL for a new application that you want the firewall in the Internet Security Router to support. The following procedure assumes that you want RealPlayer 8 to receive UDP packets through a single port.

1. Configure settings for RealPlayer 8.
   a) Start RealPlayer 8.
   b) Click on the **View** menu and then choose **Preferences**.
   c) Click on the **Transport** tab.
   d) Select **Use Specific UDP Port** and type the UDP port value. Ask your network administrator which port number to use, e.g. 7070.



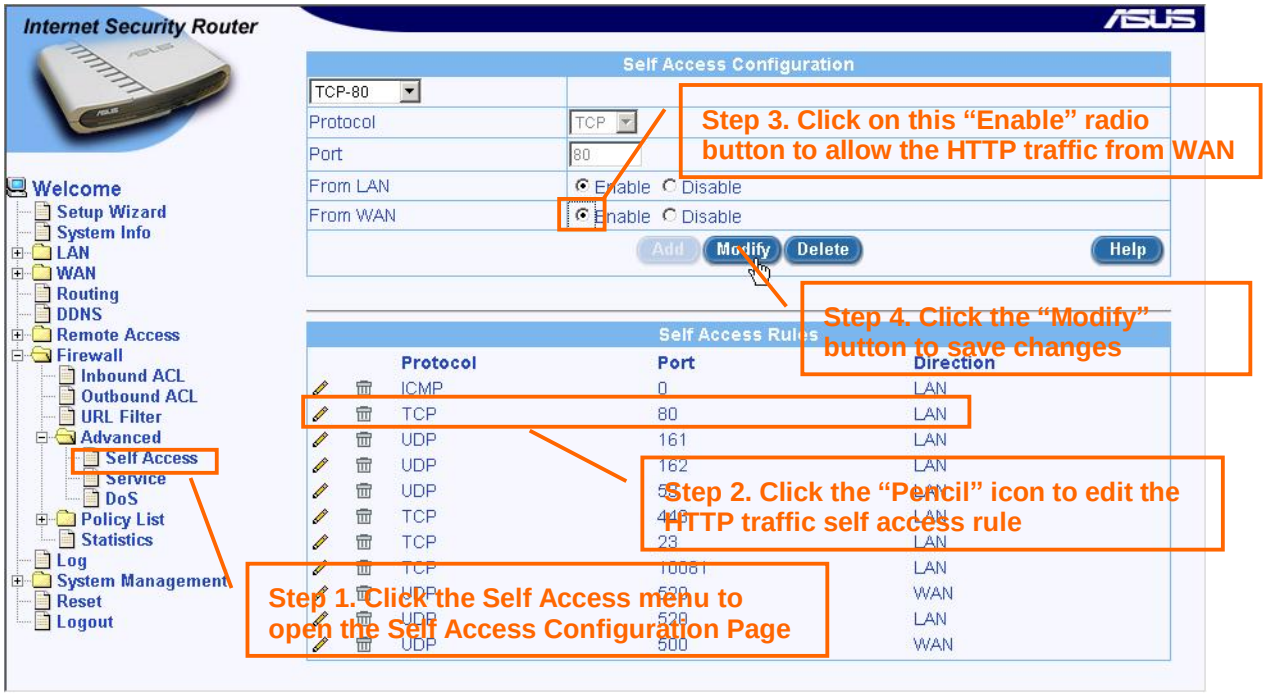
e) Click on **OK** button to save the changes.

2. Configure an ACL in the Internet Security Router (see the following figure for reference).
   a) Open the outbound ACL rule configuration page (Firewall **è** Outbound ACL)
   b) Enter information for the source IP, destination IP and source port if necessary.
   c) Select “Single” for the destination port type and enter “7070” for the port number.
   d) Select “UDP” from the protocol drop-down list.
   e) You may want to enable NAT and/or time range if desired.
   f) You can also enable event logging for this ACL if needed.
   g) Set the ACL priority by selecting a number from the “Move to” drop-down list.
   h) Click on “Add” button to save this ACL.



2.4.6 How do I access the configuration manager of the Internet Security Router via WAN port?

To access the Configuration Manager in the Internet Security Router, one needs to create a “Self Access” rule for the HTTP traffic (i.e. port 80 traffic). Please note that the inbound and outbound ACL rules are used for controlling access to the PCs behind the Internet Security Router and is not intended to control access to the Internet Security Router itself. The reason that a “Self Access” rule is not created as default to allow WAN access is to prevent un-wanted access from un-trusted networks.



1. Open the "Self Access" Configuration page (Firewall **è** Advanced **è** Self Access)
2. Click the "Pencil" icon as shown in the above figure to configure the HTTP access control to the Internet Security Router.
3. Allow the HTTP traffic from WAN by clicking on the "Enable" radio button for the "From WAN" option.
4. Check the "Modify" button to save the changes.

2.4.7 What DoS protection is provided by SL1000?

The firewall implemented in the Internet Security Router has an Attack Defense Engine that protects your networks from known types of Internet attacks. It provides automatic protection from Denial of Service (DoS) attacks such as SYN flooding, IP smurfing, LAND, Ping of Death and all re-assembly attacks. It can drop ICMP redirects and IP loose/strict source routing packets. For example, the Internet Security Router firewall provides protection from "WinNuke", a widely used program to remotely crash unprotected Windows systems in the Internet. Its firewall also provides protection from a variety of common Internet attacks such as IP Spoofing, Ping of Death, Land Attack, Reassembly and SYN flooding.

The types of attack protection provided by the Internet Security Router are listed in the following table.

Type of Attack	**Name of Attacks**
Re-assembly attacks	Bonk, Boink, Teardrop (New Tear), Overdrop, Opentear, Syndrop, Jolt
ICMP Attacks	Ping of Death, Smurf, Twinge
Flooders	ICMP Flooder, UDP Flooder, SYN Flooder
Port Scans	TCP XMAS Scan, TCP Null Scan TCP SYN Scan, TCP Stealth Scan
TCP Attacks	TCP sequence number prediction, TCP

	out-of sequence attacks
Protection with PF Rules	Echo-Chargen, Ascend Kill
Miscellaneous Attacks	IP Spoofing, LAND, Targa, Tentacle MIME Flood, Winnuke, FTP Bounce, IP unaligned time stamp attack

2.4.8 What is an ALG? What ALGs are supported?

ALG stands for Application Layer Gateway. Applications such as FTP, games etc., open connections dynamically based on the respective application parameter. To go through the firewall on the Internet Security Router, packets pertaining to an application, require a corresponding *allow* rule. In the absence of such rules, the packets will be dropped by the Internet Security Router Firewall. As it is not feasible to create policies for numerous applications dynamically (at the same time without compromising security), intelligence in the form of Application Level Gateways (ALG), is built to parse packets for applications and open dynamic associations. The Internet Security Router Firewall provides a number of ALGs for popular applications such as FTP, H.323, RTSP, Microsoft Games, SIP, etc.

The following table lists all the ALGs provided by the Internet Security Router.

ALG/Application Name	Protocol and Port	Predefined Service Name	Tested Software Version
PCAnywhere	UDP/22	PC-ANYWHERE	pcAnywhere 9.0.0
RTSP-554	TCP/554	RTSP554	RealPlayer 8 Plus QuickTime Version 6
	UDP/53	DNS	
	TCP/80	HTTP	
RTSP-7070	TCP/7070	RTSP7070	RealPlayer 8 Plus
	UDP/53	DNS	QuickTime Version 6
	TCP/80	HTTP	
Net2Phone	UDP/6801	N2P	Net2Phone CommCenter Release 1.5.0
	TCP/80	HTTP	
	TCP/443	HTTPS	
	UDP/53	DNS	
CUSeeMe	TCP/7648	CUSEEME	CUSeeMe Version 5.0.0.043
	TCP/80	HTTP	
	UDP/53	DNS	
Netmeeting	TCP/1720	H323	

ALG/Application Name	Protocol and Port	Predefined Service Name	Tested Software Version
	UDP/53	DNS	
Netmeeting with ILS	TCP/1720	H323	Windows Netmeeting Version 3.01 Opengk Version 1.2.0
	TCP/389	ILS	
	UDP/53	DNS	
Netmeeting with GK	TCP/1720	H323	
	UDP/1719	H323GK	
	UDP/53	DNS	
SIP	UDP/5060	SIP	SIP User Agent 2.0
Intel Video Phone	TCP/1720	H323	Intel Video Phone Version 5.0
	UDP/53	DNS	
FTP	TCP/21	FTP	WFTPD version 2.03 Redhat Linux 7.3
	UDP/53	DNS	
Security ALGs			
L2TP	UDP/1701	L2TP	Windows 2000 Server builtin
	UDP/53	DNS	
PPTP	TCP/1723	PPTP	Windows 2000 Server builtin
	UDP/53	DNS	
IPSec (Only Tunnel Mode with ESP)	UDP/500	IKE	Windows 2000 Server builtin
	ESP		
	UDP/53	DNS	
Chats			
AOL Chat	TCP/ 5190	AOL	AOL Instant Messenger Version 5.0.2938
	TCP/80	HTTP	
	UDP/53	DNS	
ICQ Chat	TCP /5191	ICQ_2000	ICQ 2000b

ALG/Application Name	Protocol and Port	Predefined Service Name	Tested Software Version
NB: Application should be configured to use TCP/5191	TCP/80	HTTP	
	UDP/53	DNS	
IRC	TCP/ 6667	IRC	MIRC v6.02
	TCP/80	HTTP	
	UDP/53	DNS	
MSIM	TCP/1863	MSN	MSN Messenger Service Version 3.6.0039
	TCP/80	HTTP	
	UDP/53	DNS	
Games			
Flight Simulator 2002 (Gaming Zone)	TCP/47624	MSG1	Flight Simulator 2002, Professional Edition
	TCP/28801	MSN-ZONE	
	TCP/443	HTTPS	
	TCP/80	HTTP	
	UDP/53	DNS	
Quake II (Gaming Zone)	UDP/ 27910	QUAKE	Quake II
	TCP/28801	MSN-ZONE	
	TCP/443	HTTPS	
	TCP/80	HTTP	
	UDP/53	DNS	
Age Of Empires (Gaming Zone)	TCP/47624	MSG1	Age of Empires, Gold Edition
	TCP/28801	MSN-ZONE	
	TCP/443	HTTPS	
	TCP/80	HTTP	
	UDP/53	DNS	
Diablo II (BATTLE-	TCP/4000	DIABLO-II	Diablo II

ALG/Application Name	Protocol and Port	Predefined Service Name	Tested Software Version
NET-TCP, BATTLE-NET-UDP)	TCP/ 6112	BATTLE-NET-TCP, BATTLE-NET-UDP	
	UDP/53	DNS	
	UDP/6112	Diablo II	
Other common Applications			
POP3	TCP/110	POP3	Outlook Express 5
	UDP/53	DNS	
IMAP	TCP/143	IMAP4	Outlook Express 5
	UDP/53	DNS	
SMTP	TCP/25	SMTP	Outlook Express 5
	UDP/53	DNS	
HTTPS / TLS / SSL	TCP/443	HTTPS	Internet Explorer 5
	TCP/80	HTTP	
	UDP/53	DNS	
LDAP	TCP/389	ILS	Openldap 2.0.25
	UDP/53	DNS	
NNTP	TCP/119	NNTP	Outlook Express 5
	UDP/53	DNS	
Finger	TCP/79	FINGER	Redhat Linux 7.3
	UDP/53	DNS	

2.5 Routing

2.5.1 What is default route?

A routing table entry, which is used by the router to direct packets addressed to hosts or networks not explicitly listed in the routing table.

2.5.2 What will happen if I delete the default route?

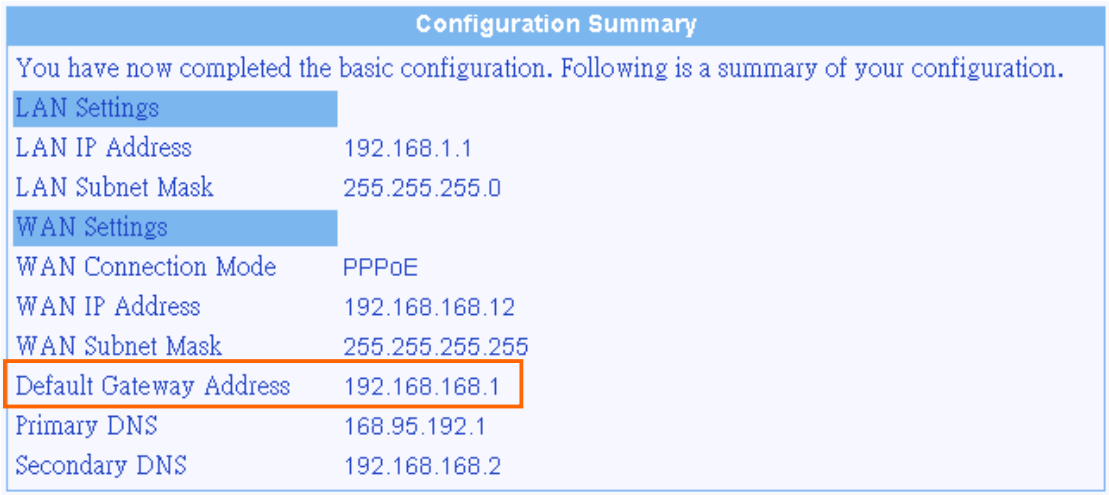
Packets cannot be sent to subnets outside of the subnet of the Internet Security Router. This is the reason why you cannot connect to the Internet, or any PCs in other networks. To add a default route, please see “How do I

find out the default gateway configured for the Internet Security Router?" for instructions. Note that default route is added automatically, after the WAN port is configured.

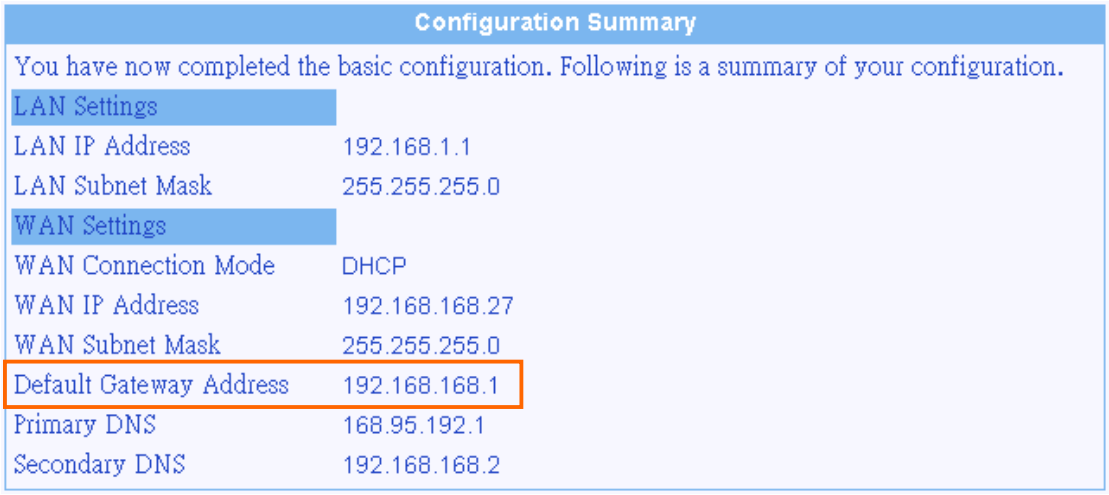
2.5.3 How do I find out the default gateway configured for the Internet Security Router?

Depending on the connection mode configured for the WAN, you can find out the default gateway IP by opening the WAN configuration page and look for the "Default Gateway Address" in the configuration summary.

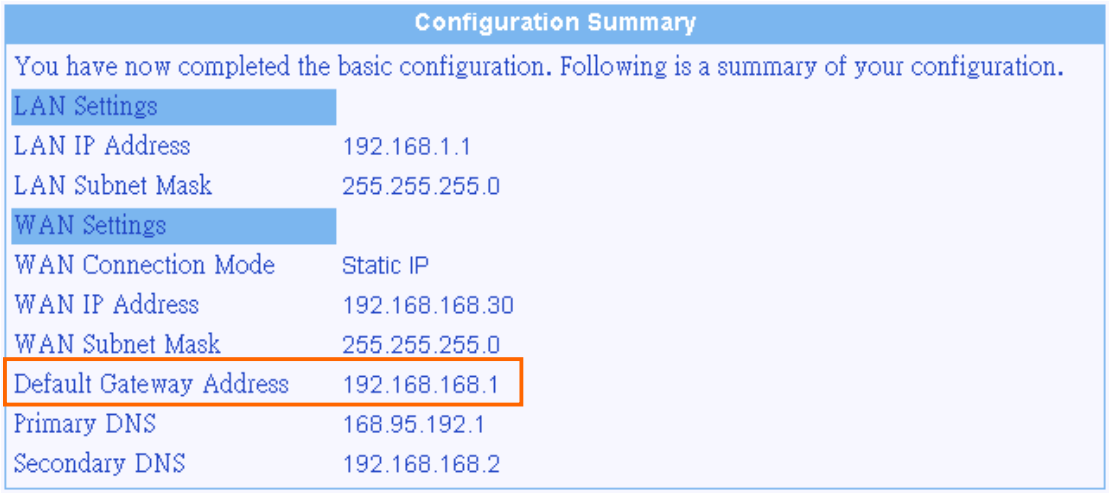
1. Connection mode is PPPoE



2. Connection mode is Dynamic (i.e. DHCP client)



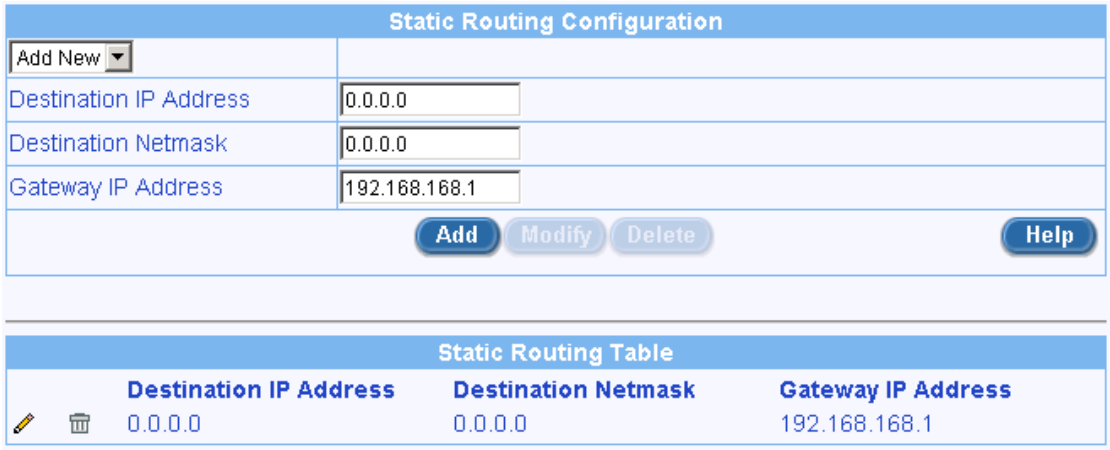
3. Connection mode is Static



2.5.4 How to add a default route?

You have two options to do this:

1. Go to the WAN configuration page and click on “Apply” button to reconfigure the WAN port setting.
2. You may also add a default route manually by following the steps below:
   a) Find out the default gateway address configured for the WAN port. See “How do I find out the default gateway configured for the Internet Security Router?” for instrcutions.
   b) Open the routing configuration page. Enter 0.0.0.0 for both the Destination IP address and Destination Netmask fields. Enter the default gateway IP in the “Gateway IP Address” text box and then click on “Add” button to add the default route. The following figure illustrates how this is done. Note that after the default route is added, you should see an entry in the “Static Routing Table”.



2.6 VPN

2.6.1 What type of VPN is supported by the Internet Security Router?

The VPN supported by the Internet Security Router is IPSec compliant. PPTP, L2TP and MPLS VPN are not supported.

2.6.2 What is IKE used for?

IKE is used in IPSec to authenticate peers, manage the generation and handling of keys used by the encryption and hashing algorithms between peers, and to negotiate IPSec SAs (security association).

2.6.3 What is Pre-shared Key?

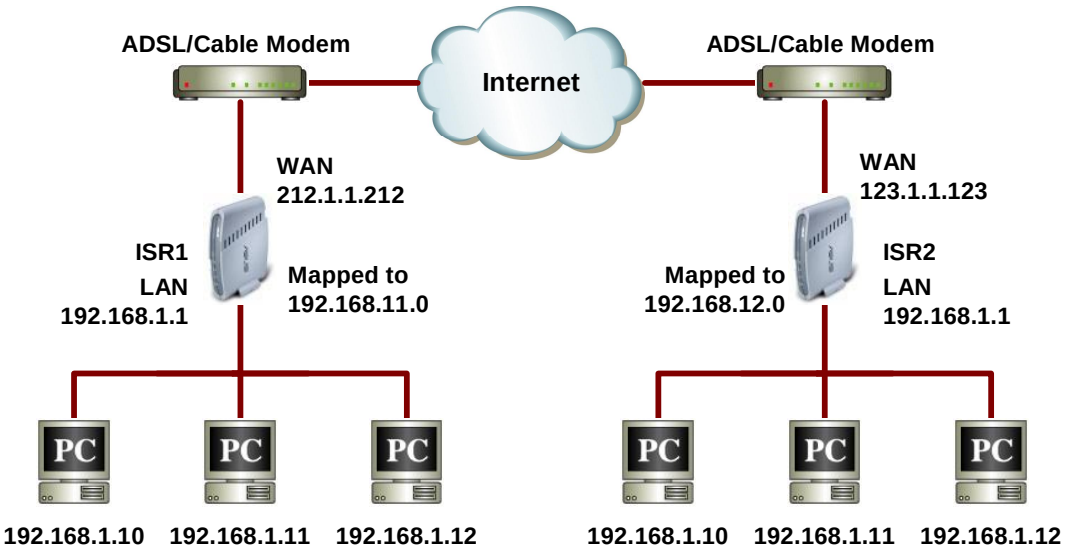
Preshared Key is a method used for IPSec tunnel authentication. If preshared key is used in IKE for authentication, the participants on both sides must be configured with the same preshared key in advance.

2.6.4 Why do I want to configure VPN w/ NAT enabled?

In the extranet scenario, the networks protected by the Internet Security Routers are under different administrative authorities. Hence, there is a possibility that the IP addresses of both networks are in the same subnet. To avoid routing problems in such scenario, IP addresses must be mapped to different ones to avoid conflict in IP addresses.

2.6.5 How to configure VPN with NAT enabled?

Let's use an example to explain the procedures involved in the configuration. The following figure shows the network diagram for this example.



Both networks behind the ISR1 and ISR2 are 192.168.1.0/255.255.255.0.

To avoid routing problems in this scenario, network IP addresses must be mapped to different ones:

- Network 192.168.1.0/255.255.255.0 behind ISR1 is translated to 192.168.11.0/255.255.255.0 before VPN processing.
- Network 192.168.1.0/255.255.255.0 behind ISR2 is translated to 192.168.12.0/255.255.255.0 before VPN processing.

The results are:

- The LAN behind ISR1 would be viewed as 192.168.11. 0/24 by the LAN behind ISR2.
- The LAN behind ISR2 would be viewed as 192.168.12. 0/24 by the LAN behind ISR1.

The configuration of each of the Internet Security Routers for extranet scenario consists of the following steps:

- Configure VPN Connection rules.
- Configure Firewall rules to allow inbound and outbound VPN traffic by performing one-to-one NAT.
- Configure a Firewall Self Access rule to allow IKE packets into the Internet Security Router.

2.6.5.1 Setup the Internet Security Routers

On ISR1

1. Configure LAN interface of ISR1 with IP address 192.168.1.1.

2. Configure DHCP pool with IP addresses from 192.168.1.10 to 192.168.1.110 on ISR1.
3. Configure WAN interface of ISR1 with IP address 212.1.1.212.
4. Add a route on ISR1 with gateway as 123.1.1.123.
5. Save the configuration.

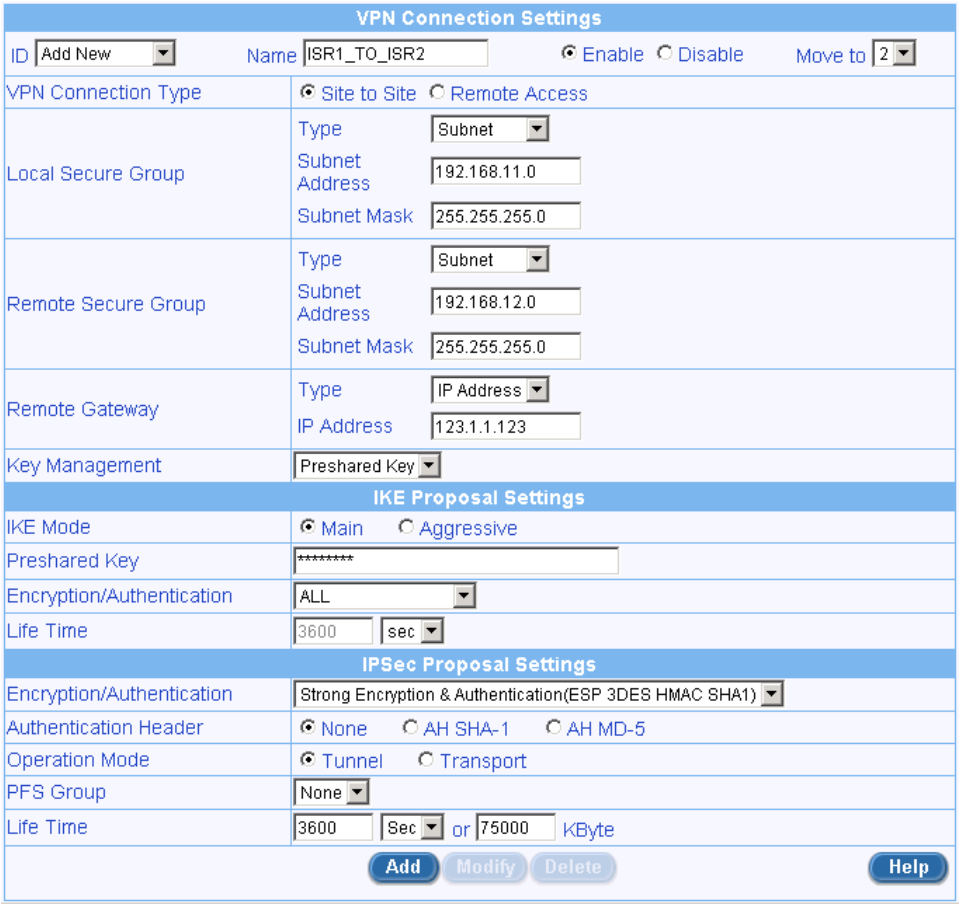
On ISR2

1. Configure LAN interface of ISR2 with IP address 192.168.1.1.
2. Configure DHCP pool with IP addresses from 192.168.1.10 to 192.168.1.110 on ISR2.
3. Configure WAN interface of ISR2 for IP address 123.1.1.123.
4. Add a default route on ISR2 with gateway as 212.1.1.212.
5. Save the configuration.

2.6.5.2 Configure VPN Rules on ISR1

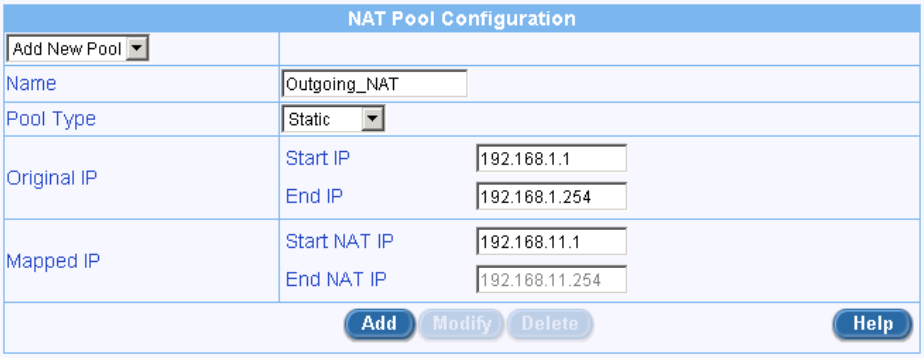
Step 1: Configure VPN Rule

1. Use 192.168.11.0/255.255.255.0 for the Local Secure Group
2. Use 192.168.12.0/255.255.255.0 for the Remote Secure Group

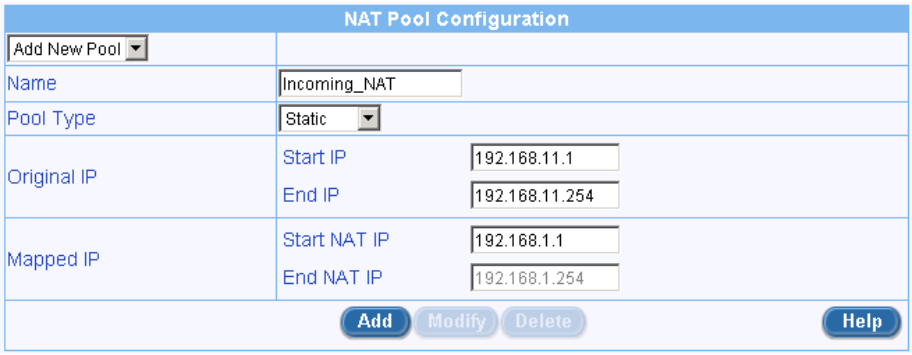


Step 2: Configure Static NAT Pools

3. Configure outgoing static NAT pool (static-NAT) for translating addresses in range 192.168.1.1-192.168.1.254 to 192.168.11. 1-192.168.11.254

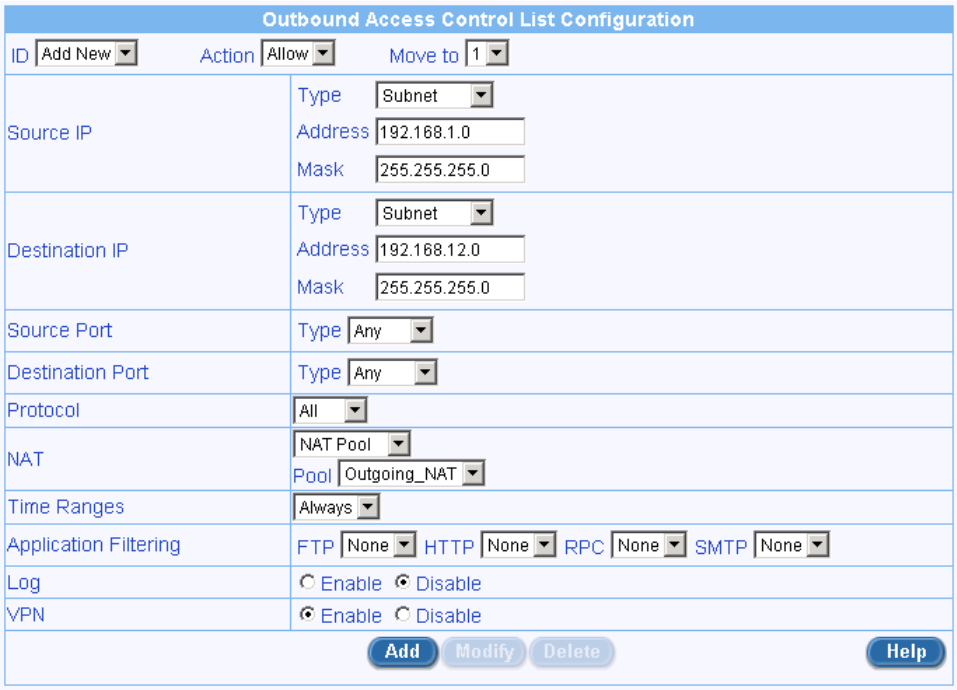


4. Configure incoming static NAT pool (reverse-static-NAT) for translating addresses in range 192.168.11.1-192.168.11.254 to 192.168.1.1-192.168.1.254

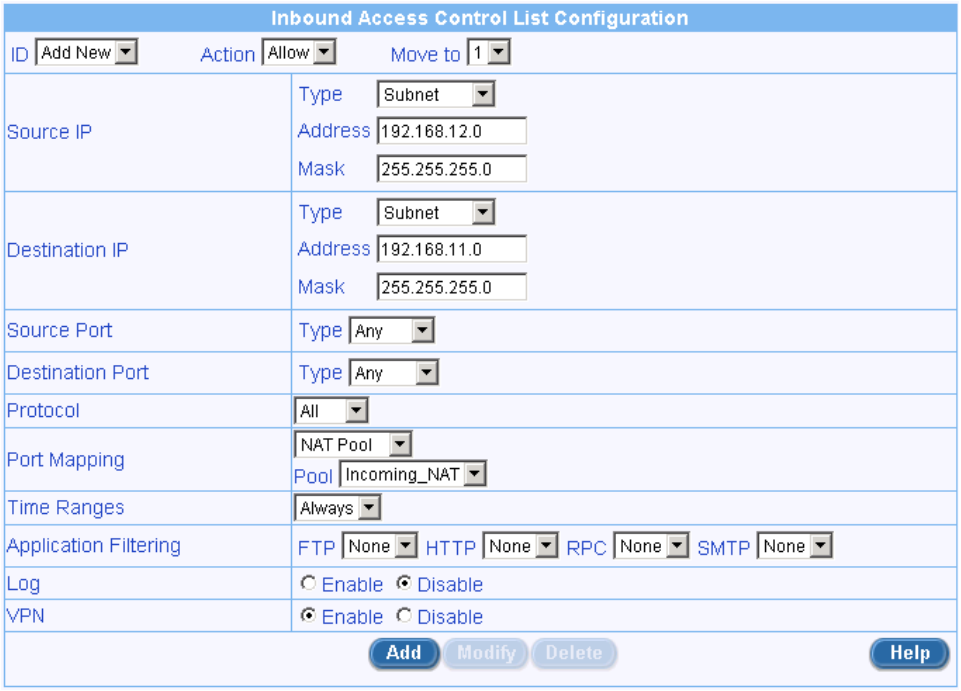


Step 3: Configure Extranet access rules

5. Configure outbound Firewall rules to map the source IP address of outbound packets from 192.168.1.x range to 192.168.11.x (defined by Outgoing_NAT pool) range before sending the packet to VPN.



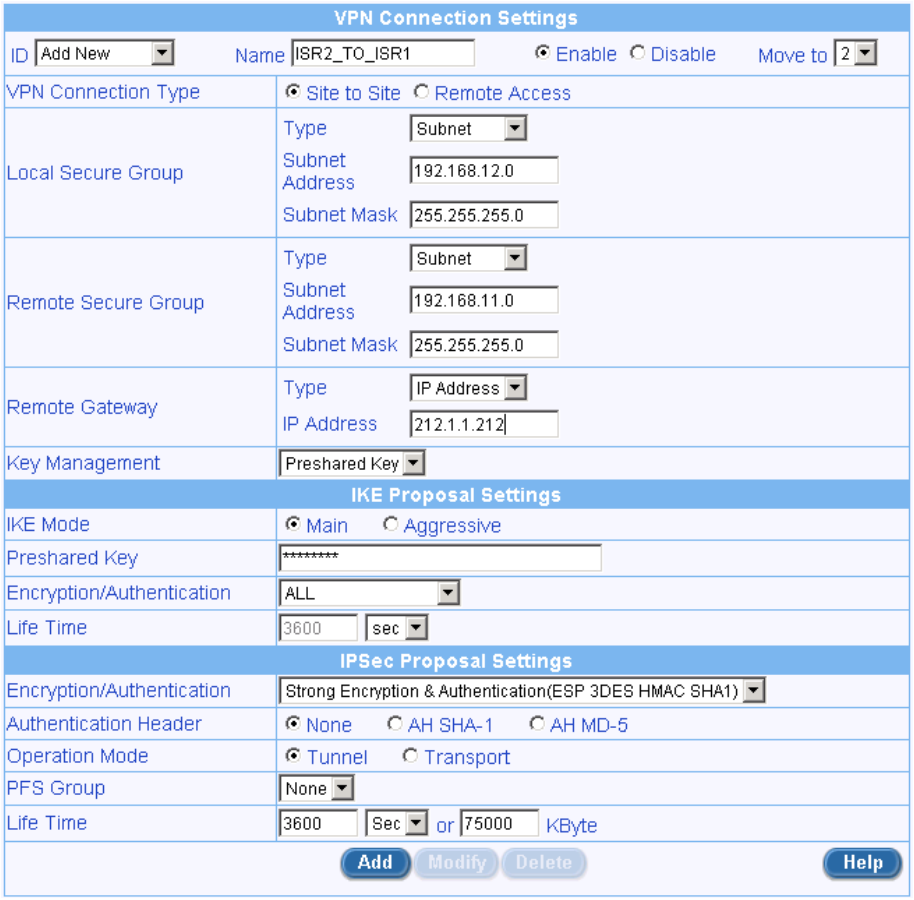
6. Configure inbound Firewall rules to map the destination IP address of inbound packets from 192.168.11.x range to 192.168.1.x (defined by Incoming_NAT pool) range after the packet is processed by VPN.



2.6.5.3 Configure VPN Rules on ISR2

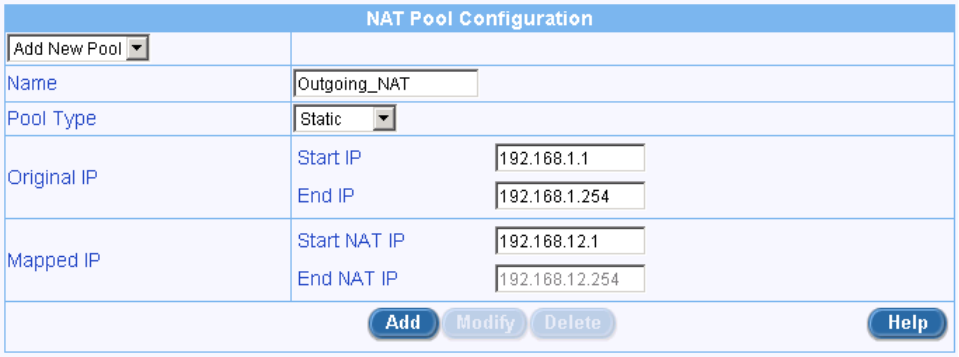
Step 1: Configure VPN connection rules

1. Use 192.168.12.0/255.255.255.0 as Local Secure Group
2. Use 192.168.11.0/255.255.255.0 as Remote Secure Group

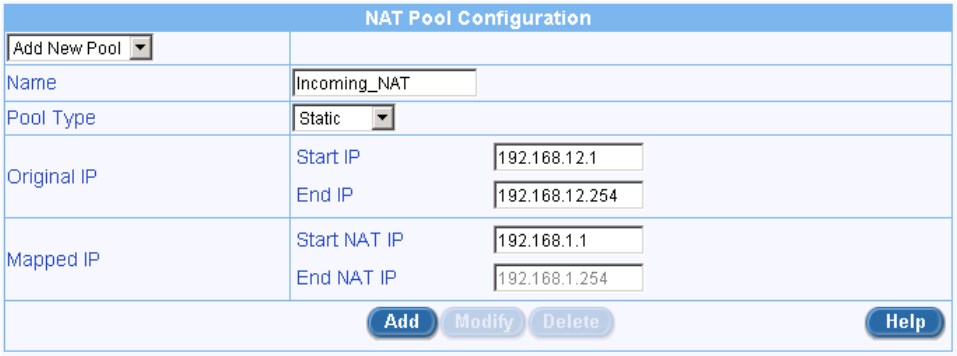


Step 2: Configure Static NAT Pools

3. Configure outgoing static NAT pool (static-NAT) for translating addresses in range 192.168.1.1-192.168.1.254 to 192.168.12.1-192.168.12.254

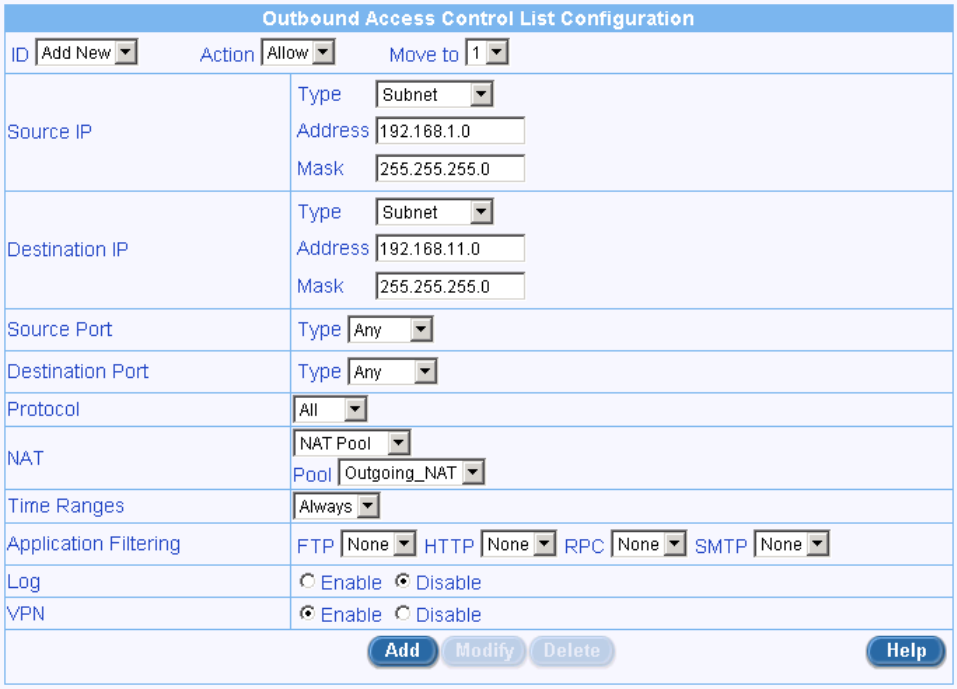


4. Configure incoming static NAT pool (reverse-static-NAT) for translating addresses in range 192.168.12.1-192.168.12.254 to 192.168.1.1-192.168.1.254

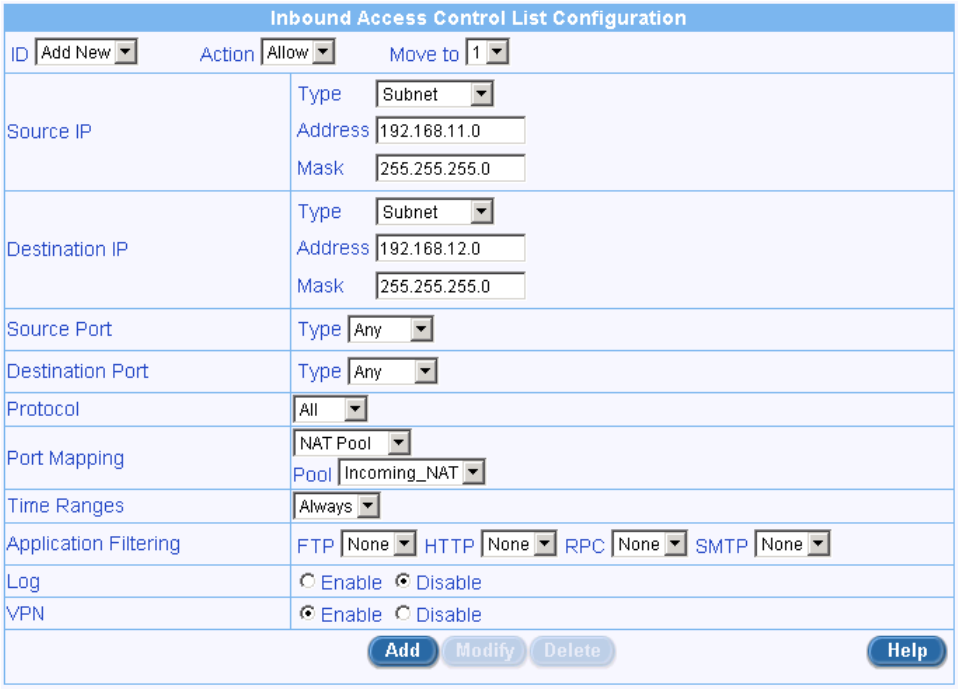


Step 3: Configure Extranet rules

5. Configure outbound Firewall rules to map the source IP address of outbound packets from 192.168.1.x range to 192.168.12.x (defined by Outgoing_NAT pool) range before sending the packet to VPN.



6. Configure inbound Firewall rules to map the destination IP address of inbound packets from 192.168.12.x range to 192.168.1.x range after the packet is processed by VPN.



2.6.5.4 Establish Tunnel and Verify

- Start continuous ping from a host on the LAN behind ISR1 to a host on the LAN behind ISR2. The first few pings would fail. After a few seconds, The host on the LAN behind ISR1 should start getting ping response.
- Ping from a host on the LAN behind ISR2 to a host on the LAN behind ISR1. Ping should be successful.
- The ping might fail due to any of the following:
  - The IP address of the host on the LAN behind ISR2 used in the ping command may not be correct. Check and give the correct IP address.
  - Default route is not configured for ISR1 or ISR2. Configure the default routes as necessary.
  - Firewall rules corresponding to VPN connection may not be configured properly. If any of the network addresses is not correctly configured, correct the parameters and apply the configuration.
  - Local and remote network addresses may not be configured correctly. The network addresses used in VPN connection rule are 192.168.11.0/255.255.255.0 and 192.168.12.0/255.255.255.0.

2.7 System management

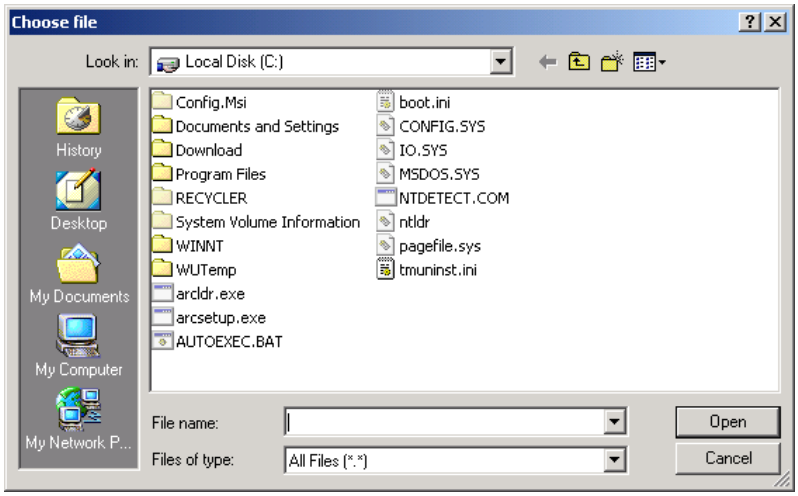
2.7.1 How to backup configuration settings?

1. Log into Configuration Manager as admin, click the **System Management** menu, click the **Configuration** submenu and then click **Backup** submenu. The Backup Configuration page displays.
2. Click on the “Apply” button to backup the system configuration.
3. A pop-up window appears to let you specify a location to save the configuration file.

2.7.2 How to restore configuration settings?

1. Log into the Configuration Manager as admin, click the **System Management** menu, click the **Configuration** submenu and then click **Restore** submenu. The Restore Configuration page displays.
2. Enter the path and name of the system configuration file that you want to restore in the “Configuration File” text box. Alternatively, you may click on the “Browse” button to search for the system configuration

file on your hard drive. A window similar to the one shown below will pop up for you to select the configuration file to restore.



3. Click on the “Apply” button to restore the system configuration. Note that the Internet Security Router will reboot to make the new system configuration in effect.

2.7.3 How to regain access to my Internet Security Router if I forget my login password?

You can reset the configuration of the Internet Security Router to the factory default by following the procedures below:

1. Power down the Internet Security Router and wait for at least 5 seconds.
2. Power up the Internet Security Router and wait for at least 5 seconds before pressing the reset switch the first time. You will see the Alarm LED flash once in about 5 seconds.
3. When you see the Alarm LED flash once, press the reset switch again. You will then see the Alarm LED flash twice in about 5 seconds. This indicates your Internet Security Router is about to revert to the factory default settings. If you change your mind, you can press the reset switch again or turn the power off to cancel this action.

2.7.4 How to regain access to my Internet Security Router if I have no way to access the Internet Security Router?

See “How to regain access to my Internet Security Router if I forget my login password?” for instructions.

2.8 Log

2.8.1 What is the log format explanation?

The Internet Security Router firewall uses the industry standard Webtrends Extended Log Format (WELF) for logging network activities. A sample log message in WELF as generated by syslog is shown below.

Oct 28 16:15:38 (none) syslog: id=firewall time="2003-10-28 16:15:38" fw=SL1000 pri=6 proto=6(tcp) src=192.168.1.10 dst=192.168.1.1 msg=”Service access request successful Src 2275 Dst 80 from CORP n/w” agent=Firewall

The fields in this sample syslog message are as follows:

- Time stamp: This is the syslog header which contains the time stamp (date and time) and IP address of the log recording event.
- id: is the type of record.

- time: is the local date and time of the event.
- fw: is the Firewall that generated the log record.
- pri: is the priority of the event.
- proto: is the protocol used by the event.
- src: is the IP address that generated the event.
- dst: is the IP address that received the event.
- msg: is a detailed log message based on the respective event.
- agent: is a Name of agent generating the log message.