



InstaGate 305



Administrator's Guide

Table of Contents

1	Overview	1
2	Hardware Installation	2
2.1	Front Panel	2
2.2	LED Indicators	2
2.3	Rear Panel	2
2.4	Console Port	2
2.5	Reset Button	2
2.6	10/100 Mbps Ethernet WAN	3
2.7	Auto-negotiating 10/100 Mbps Ethernet DMZ	3
2.8	Auto-negotiating 10/100 Mbps Ethernet LAN	3
2.9	Battery Warning	3
3	Initial Setup	4
3.1	The Web User Interface	4
3.2	The Command Line Interface	6
3.2.1	LAN Interface Setup	7
3.2.2	Get Interface Information	8
3.2.3	Additional Help	8
4	Setup Wizard	9
4.1	System Setup Wizard	9
4.1.1	Setup Time	9
4.1.2	Network Mode Setup	9
4.1.3	Configure WAN IP	10
4.1.3.1	PPPoE Connection Settings	10
4.1.3.2	Dynamic (DHCP) Connection Settings	11
4.1.3.3	Static Connection Settings	11
4.1.4	Configure LAN IP	12
4.1.5	Configure DHCP Server	13
4.1.6	Registration	13
4.2	VPN Setup Wizard	14
4.2.1	New Automatic Key (IKE) Policy	14
4.2.2	Network Setup	16
4.2.3	Gateway Settings	16
4.2.4	IKE Settings	19
4.2.5	IPSec Settings	20
5	System Setup	21
5.1	Setup time	21
5.2	Administrator	22
5.3	Setup interface	23
5.3.1	WAN Interface	23
5.3.1.1	Get IP by PPPoE	23
5.3.1.2	Get IP by DHCP	24
5.3.1.3	Static Configuration	25
5.3.1.4	Options for WAN interface	26
5.3.2	LAN Interface	26

5.3.3	DMZ Interface	28
5.4	Configure DHCP Server	28
5.5	Maintenance	31
5.6	Diagnostics	32
5.7	Secure HTTP Proxy	33
6	Define Objects	35
6.1	Define Subnet Object	35
6.2	Defining IP Address Groups	36
6.3	Defining Gateway Objects	36
6.4	Define Service Objects	39
6.4.1	Default Service	39
6.4.2	Add a New Service	40
6.4.2.1	Re-Defined Service Configuration	40
6.4.2.2	Custom Defined Service Configuration	41
6.5	Schedule	41
6.6	Define Certificate Objects	42
6.6.1	Certificate Management	42
6.6.2	Certificate Request	43
7	Network Address Translation	45
7.1	NAT Rules	45
7.2	DMZ Host	48
7.3	Virtual Server	49
7.4	NAPT	51
8	Routing	53
8.1	Static Routing	53
8.2	RIP	54
9	Firewalls	57
9.1	Firewall Policies	57
9.1.1	Adding a new firewall policy	59
9.1.1.1	Adding a policy	59
9.2	Address Filters	64
9.2.1	MAC Filtering	64
9.2.2	IP Filtering	65
10	Virtual Private Network	67
10.1	IPSec VPN	67
10.1.1	Automatic Key Exchange (IKE)	67
10.1.1.1	Private Network Definition	68
10.1.1.2	The IPSec Tunnel End Points	69
10.1.1.3	IKE Proposal	69
10.1.1.4	IPSec Proposal	70
10.1.2	IKE Example	70
10.1.3	Manual Key	71
10.1.3.1	Private Network Definition	71
10.1.3.2	The IPSec Tunnel End Point	71
10.1.3.3	IPSec Security Association	72
10.2	L2TP/PPTP VPN	73

10.2.1	L2TP Server	74
10.2.2	PPTP Server	75
10.2.3	PPTP Client	75
10.2.4	User Management	80
11	URL Filter	81
11.1	Filtering Action	81
11.2	URL Keyword	82
11.3	Refuse Transfer Protocols	82
11.4	Filtering web programs	82
11.5	Client Proxy setting	83
12	Intrusion Prevention	84
12.1	Intrusion Attack Types	84
12.2	Scan Prevention	85
13	Dynamic DNS	86
14	Proxy DNS	87
15	Status	91
15.1	Log Setting	91
15.2	System Info.	92
15.3	VPN Status	93
15.4	ARP Table	93
15.5	DHCP Table	94
15.6	System Log	94
16	SoftPak Director	96
16.1	Registration	96
16.2	Catalog	96
16.2.1	Subscribing to a SoftPak	96
16.2.2	Viewing SoftPak Details	97
16.3	Enabled	98
16.4	User License	98
17	Global Management	100
17.1	Client Settings	100

Appendix A: Win2K IPSec VPN to the InstaGate

Appendix B: Win2K PPTP VPN client to the InstaGate

Appendix C: Dynamic DNS with DNS Made Easy

Appendix D: Documentation License

List of Figures

Figure 1: Front Panel of the InstaGate	2
Figure 2: Local Area Connection Status	4
Figure 3: Local Area Connection Properties	5
Figure 4: TCP/IP Properties	5
Figure 5: Login screen	6
Figure 6: System time setup	9
Figure 7: Network Mode (Static configuration)	10
Figure 8: PPPoE Information	11
Figure 9: Network Mode (DHCP Client)	11
Figure 10: Configure WAN IP	12
Figure 11: Configure LAN IP	12
Figure 12: Configure DHCP Server	13
Figure 13: Registration	14
Figure 14: Policy Name	15
Figure 15: Local and Remote Network	16
Figure 16: Define New Gateway	17
Figure 17: Define a New local Gateway	17
Figure 18: Remote Gateway	18
Figure 19: Gateway	19
Figure 20: IKE Proposal	19
Figure 21: IPSec Proposal	20
Figure 22: Automatic key information Table	20
Figure 23: Setup time	21
Figure 24: Setup time	22
Figure 25: Administrator Management	22
Figure 26: Get IP by PPPoE	24
Figure 27: Get IP by DHCP Server	25
Figure 28: WAN interface static configuration	25
Figure 29: The options for WAN interface	26
Figure 30: LAN interface	26
Figure 31: Multiple LAN	27
Figure 32: Existing LANs	27
Figure 33: DMZ Interface	28
Figure 34: DHCP Server Settings	29
Figure 35: Configuration for DHCP server	30
Figure 36: System Maintenance	31
Figure 37: System Upgrade Reboot	31
Figure 38: System Diagnostics	32
Figure 39: System Diagnostics Ping Results	32
Figure 40: System Diagnostics Traceroute Results	33
Figure 41: System Diagnostics SoftPak Director Connectivity	33
Figure 42: Secure HTTP Proxy	34
Figure 43: Define a Subnet Object	35

Figure 44: Subnet Object List	36
Figure 45: New IP Address Group	36
Figure 46: Define a local gateway object	37
Figure 47: Define a remote gateway object	38
Figure 48: The Gateway Object List	38
Figure 49: Built-in Standard Service Object	39
Figure 50: Service Objects List	40
Figure 51: New Service Object	41
Figure 52: Customer Define Service Configuration.	41
Figure 53: Schedule	42
Figure 54: New Schedule Settings	42
Figure 55: Certificate Management	42
Figure 56: Certificate Request Form	43
Figure 57: Certificate Request	44
Figure 58: Loading the Device Certificate	44
Figure 59: Network Address Translation	45
Figure 60: Add NAT Rule	45
Figure 61: Example of “one-to-one NAT”	46
Figure 62: Example of “many-to-one NAT”	47
Figure 63: Example of “many-to-many NAT”	47
Figure 64: NAT Rule List	48
Figure 65: DMZ Host	48
Figure 66: DMZ Host example	49
Figure 67: Example of Virtual Server rule.	50
Figure 68: Virtual Server List	51
Figure 69: Add NAPT Rule	51
Figure 70: Adding routing entry	53
Figure 71: Static Routes	53
Figure 72: RIP Information Management window	54
Figure 73: The Routing Table list	54
Figure 74: The interface edit window	55
Figure 75: The options of the “send” action.	55
Figure 76: The options of the “receive” action	55
Figure 77: An illustration of the functions of a Firewall	57
Figure 78: Firewall Management Configuration	57
Figure 79: Add a Firewall Rule	59
Figure 80: Move the policy	60
Figure 81: Test environment for testing firewall policy	61
Figure 82: Default NAT Policies	62
Figure 83: NAT Rules	62
Figure 84: New Firewall Policy	63
Figure 85: New Firewall Policy	63
Figure 86: Firewall Policies	64
Figure 87: New MAC Filter	65
Figure 88: MAC Filter List	65
Figure 89: New IP Address Filter	66

Figure 90: IP Address Filter List	66
Figure 91: IPSec VPN	67
Figure 92: Automatic Key Example	68
Figure 93: New automatic key policy	68
Figure 94: Select the gateway object for automatic key policy	69
Figure 95: Define authentication method for automatic key policy	69
Figure 96: IKE SA lifetime	69
Figure 97: IPSec Proposal	70
Figure 98: IPSec SA lifetime	70
Figure 99: Automatic Key Policy Example	71
Figure 100: Automatic key Policy List	71
Figure 101: New Manual Key Policy for Local Gateway	73
Figure 102: Remote access VPN	74
Figure 103: L2TP Configuration	74
Figure 104: PPTP Configuration	75
Figure 105: The InstaGate PPTP Client	76
Figure 106: PPTP client example	76
Figure 107: Firewall Policy Rule	77
Figure 108: PPTP Server Settings	77
Figure 109: Remote VPN User Management	78
Figure 110: PPTP Client Settings	78
Figure 111: PTP Client Routing Table	79
Figure 112: PPTP Client Settings	79
Figure 113: PPTP Client Routes	80
Figure 114: L2TP/PPP User Management	80
Figure 115: The Web Filtering option	81
Figure 116: The Web Filtering Management page	81
Figure 117: The Transfer Protocols configuration	82
Figure 118: The URL Filtering Functions Configuration	82
Figure 119: The proxy setting of the client machine	83
Figure 120: Intrusion Prevention Settings	84
Figure 121: Detailed items of Intrusion Attack Types	85
Figure 122: Dynamic DNS Settings	86
Figure 123: Network Connection Status	87
Figure 124: Network Connection Properties	88
Figure 125: TCP/IP Properties	88
Figure 126: DNS Server Address	89
Figure 127: Proxy DNS	89
Figure 128: Proxy DNS List	90
Figure 129: Mailing setting of Log	91
Figure 130: Scheduler Setting	92
Figure 131: Syslog Output to external server	92
Figure 132: The summary of system information	92
Figure 133: VPN Status	93
Figure 134: VPN Status Search	93
Figure 135: VPN Status Search Results	93

Figure 136: ARP Cache Table	94
Figure 137: DHCP IP Assignment Table	94
Figure 138: System Log	95
Figure 139: SoftPak Director Registration	96
Figure 140: SoftPak Director Catalog	97
Figure 141: SoftPak Director Enabled	98
Figure 142: SoftPak Director User License	99
Figure 143: Global Management Settings	100

1 Overview

The InstaGate 305 is a high-performance security appliance tailored to protect small-to-medium networks from modern-day threats such as Viruses, Worms, Trojans, Spyware, Intrusions, DoS Attacks, Hacking, Unauthorized Access and more. The InstaGate 305 also features a sophisticated toolset of virtual private network (VPN) utilities, allowing remote users and remote locations easily and securely connect with one another.

The InstaGate 305 is an intelligent security appliance that integrates multiple security functions into a single, easy to install and manage platform. The InstaGate features a Deep Packet Inspection Firewall, IPSec VPN, Advanced NAT modes, Intrusion Prevention, Gateway Antivirus, Content Filtering, and more. The device also features a secure, intuitive and easy-to-use web-based management interface for management across the Internet, and features a complete command-line interface for local management.

The InstaGate is ideal for small-but-data-intensive network environments, providing high performance through each of its 5 interfaces (including a 10/100 Mbps Ethernet WAN port, a 10/100 Mbps Ethernet DMZ (Demilitarized Zone) port and an integrated three-port 10/100 Mbps Ethernet LAN switch).

2 Hardware Installation

2.1 Front Panel

The front panel of the InstaGate is shown below. (see Figure 1)

Error! Objects cannot be created from editing field codes.

Figure 1: Front Panel of the InstaGate

2.2 LED Indicators

LED	Status	Indication
Power LED		
Power	Green	Normal operation
	OFF	Power failed
Testing LED		
Ready	Green	Power on system testing is ok.
	OFF	Power on system testing is processing now.
LAN LED / DMZ LED / WAN LED		
Link/Act	Green	A port has established a valid 10/100Mbps network connection.
	Green (Blinking)	Incoming traffic is entering the port.
FDX/Col	Yellow	The port is operating in full duplex mode.
	OFF	The port is operating in half duplex mode.
	Yellow (Blinking)	When collision in the segment occurs, the LED's will be blinking.
Speed	Green	The port is operating in 100Mbps mode.
	OFF	The port is operating in 10Mbps mode.

Table 1: LED Indicators

2.3 Rear Panel

The rear panel of the InstaGate connects with the power cord. The InstaGate is compatible with 100~240 AC and 50~60 Hz.

2.4 Console Port

To configure the system using the console port, connect one end of a RS232 serial cable to a COM port on a PC or notebook computer and the other end of the cable to the Console Port of the InstaGate.

2.5 Reset Button

The reset button is used to reboot the system.

2.6 10/100 Mbps Ethernet WAN

The 10/100 Mbps Ethernet WAN port connects to Internet via broadband modem or router.

2.7 Auto-negotiating 10/100 Mbps Ethernet DMZ

DeMilitarized Zone port can be attached with public servers. (Web, FTP, etc.)

2.8 Auto-negotiating 10/100 Mbps Ethernet LAN

The LAN interface automatically detects the speed mode of 10 Mbps or a 100 Mbps.

2.9 Battery Warning

CAUTION

There is danger of explosion if the battery is not replaced correctly. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to manufacturer's instructions.

3 Initial Setup

3.1 The Web User Interface

To perform the initial configuration through the Web user interface, change the IP address of the managed PC to the same subnet as the LAN interface of the InstaGate and connect the managed PC to the InstaGate by Ethernet.

To Receive a Dynamic IP Address by configuring Windows:

1. Select **Start**, then choose **Settings > Network and Dial-up Connections**.
2. Select the Local Area Connection.

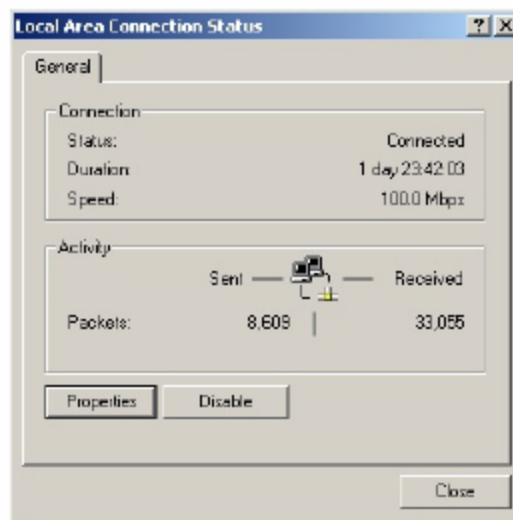


Figure 2: Local Area Connection Status

3. Select **Properties**.

The Local Area Connection Properties dialog box appears as:

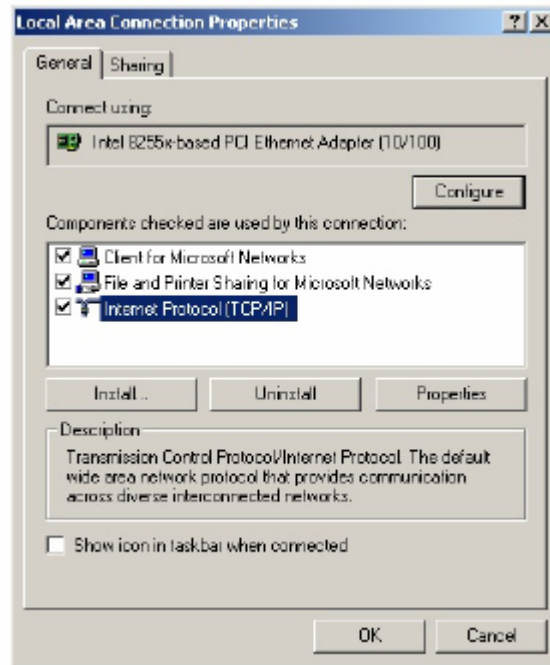


Figure 3: Local Area Connection Properties

4. Select **Internet Protocol (TCP/IP)** then select **Properties**.
The Internet protocol (TCP/IP) Properties dialog box appears as:

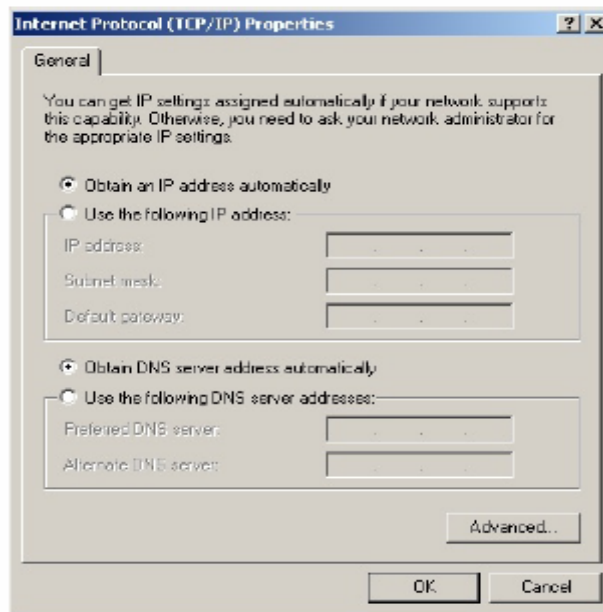


Figure 4: TCP/IP Properties

5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.

6. Select **OK**. You may need to restart your computer for the settings to take effect.

Note - The procedural steps above is applicable to Windows 2000 only. For Windows 95/98/ME/NT/XP, refer to your Windows Documentation.

To Configure the IP Address of the managed PC manually:

If not using DHCP, you need to assign an IP address to each computer manually.

The InstaGate default IP address and the corresponding netmask are 192.168.1.1 and 255.255.255.0 respectively. You can log on through a Web browser and configure the InstaGate via the URL “https://192.168.1.1”. After you connect to the InstaGate the login page appears (see Figure 5). You may login the system by using the default username and password. The default user name is “**admin**” with a password of “**123456**”.



Figure 5: Login screen

3.2 The Command Line Interface

The command line interface provides the basic configuration functions. To configure the InstaGate via the command line interface, you must connect the InstaGate and the management station by an RS-232 console cable. You also have to run the “HyperTerminal” program or a VT100 terminal emulator on the management station.

The following steps are the guideline for connecting the InstaGate and the management station.

1. Connect the serial cable from the management station to the console port on the InstaGate.
2. Start the HyperTerminal or the terminal emulator on the management station.
3. To create a new connection, type the name and select an icon, and then select OK.
4. The Connect To dialog box is appeared.
5. Select the serial port to which the serial cable is connected to the management station (usually COM1 or COM2), and select OK.
6. The COM1 (or COM2) Properties dialog box is appeared.
7. Configure the port settings as follows, and then select OK:
 - serial communications 115200 bps
 - 8 bit
 - no parity
 - 1 stop bit
 - no flow control
8. Press the ENTER key to see the login prompt.
9. Log in using the admin username and password. The default username is “*admin*” with a password of “*123456*”.

3.2.1 LAN Interface Setup

To setup the LAN interface or to get the interface information use the following steps:

1. Enter “*system*” and then press the ENTER key
2. Enter “*interface*” and press the ENTER key
3. Enter “*lan*” and press the ENTER key
4. Enter “*ip 192.168.1.1 netmask 255.255.255.0*” and press the ENTER key.
Substitute the IP address that will be assigned to the InstaGate for 192.168.1.1 and choose the appropriate netmask for your network environment.
5. After you press the ENTER key, the following message appears.

```
Setup/System/Interface/LAN>ip 192.168.1.1 netmask
255.255.255.0

LAN INTERFACE
Enable NAT Policy = yes
IP Address = 192.168.2.1
Netmask = 255.255.255.0

To Apply These Settings please reboot
```

Reboot the InstaGate for the LAN interface changes to take affect. Connect to the Web interface as outlined in section 3.1 to complete the configuration of the InstaGate using the Setup Wizard.

3.2.2 Get Interface Information

You can get the system interface information by entering “*status*” and pressing the ENTER key.

3.2.3 Additional Help

To see a list of available command press the “?” key at any time. A list of available command or options will be displayed similar to the following.

4 Setup Wizard

4.1 System Setup Wizard

Step 1:

4.1.1 Setup Time

The user interface of the InstaGate provides an easy way to setup the system time. All you have to do is select the “Synchronize Now” button under “Main Menu>Step Wizard>System Setup>”. After you select this button, the system clock is synchronized with the administrator’s workstation as shown in Figure 6.

The screenshot displays the InstaGate 305 web interface for the System Setup wizard, specifically the 'Date & Time' step. The breadcrumb trail at the top reads 'Main Menu > Setup Wizard > System Setup'. The left sidebar contains a navigation menu with options: Setup Wizard (expanded), System Setup (selected), Advanced, SoftPak Director, Global Management, Online Help, and Logout. The main content area is titled 'System Setup: Step 1 — Date & Time' and 'Date & Time Settings'. It shows the current system time as '2005, Jul, 25, Monday, 14 : 53 : 16'. There are two radio button options for synchronization: 'Synchronize with Network Time Protocol (NTP) server' (unselected) and 'Synchronize with client' (selected). Under the NTP server option, there is a 'Time Zone' dropdown menu set to '(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London', a 'Daylight Savings' section with 'Enabled' and 'Disable' radio buttons (the latter is selected), and a 'Timer Server' dropdown menu set to 'North America - 192.43.244.18'. Under the 'Other' radio button option, there are four empty input fields for IP address. At the bottom right, there are two buttons: 'Synchronize Now' and 'Next'.

Figure 6: System time setup

Select on the “Next” button to move to the next step.

Step 2:

4.1.2 Network Mode Setup

The user interface of the InstaGate provides an efficient way to configure WAN interface. It provides three methods mentioned below for configuring the WAN interface

- PPPoE
- Dynamic (DHCP), and

- Static.

Step 3

4.1.3 Configure WAN IP

The InstaGate provides a way to configure the WAN. For this please select the “PPPoE”, “Dynamic (DHCP)” or “Static” option depending on your connection to the Internet. The “Enable NAT” allows you to enable/disable the default NAT rule. To enable the default NAT rule, select the “Enable NAT” check box. NAT function allows many hosts on the private network with private IP address to access Internet using one public IP address.

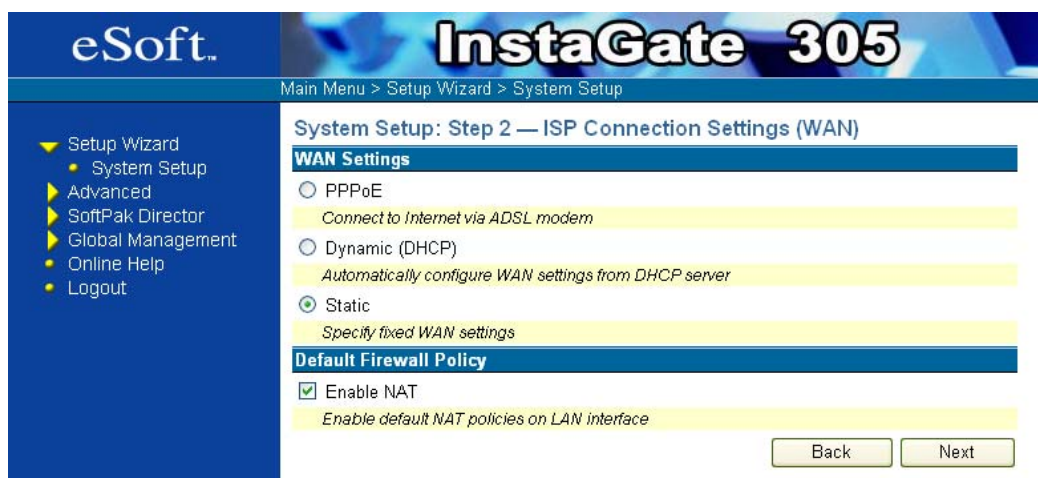


Figure 7: Network Mode (Static configuration)

4.1.3.1 PPPoE Connection Settings

If you want to access the Internet via a DSL modem that uses PPPoE, select the “PPPoE” option. The “Enable NAT” allows you to enable/disable the default NAT rule. To enable the default NAT rule, select the “Enable NAT” check box. Then select on the “Next” button to move over to the next step.

If you connect to the internet via a DSL modem you require username, password and the server name (optional) that you got from your ISP to be filled as shown in Figure 8. If you want your DSL connection to always be on, please choose the “Always connected” option.

Alternatively you can choose “On-demand with disconnect after idle time” which means that when you transmit any data to the Internet, the InstaGate will connect to the ISP automatically. The “idle time” means that after idle time expires, the system will suspend the Internet connection.

The option “CLAMP the MSS to 1360 for AOL” means that for some special ISP like AOL you need to CLAMP the MSS to 1360. The “MTU” means that you can specify MTU for PPPoE. After you fill up the user name, password and server name select the “Next” button to move on to the next step.

eSoft. InstaGate 305

Main Menu > Setup Wizard > System Setup

System Setup: Step 3 — ISP Connection Settings (WAN) — PPPoE

PPPoE Settings

Username

Username specified by your service provider

Password

Password specified by your service provider

Server Address (if required)

Server Address if specified by your service provider

Always connected

On-demand with disconnect after idle time of minute(s)

CLAMP the MSS to 1360 For AOL

MTU

Back Next

Figure 8: PPPoE Information

4.1.3.2 Dynamic (DHCP) Connection Settings

The InstaGate provides an efficient way to get WAN interface configuration from an external DHCP server. For this please select “Dynamic (DHCP)” option. Then select on the “Next” button to move over to the next step.

eSoft. InstaGate 305

Main Menu > Setup Wizard > System Setup

System Setup: Step 2 — ISP Connection Settings (WAN)

WAN Settings

PPPoE
Connect to Internet via ADSL modem

Dynamic (DHCP)
Automatically configure WAN settings from DHCP server

Static
Specify fixed WAN settings

Default Firewall Policy

Enable NAT
Enable default NAT policies on LAN interface

Back Next

Figure 9: Network Mode (DHCP Client)

4.1.3.3 Static Connection Settings

To configure the WAN interface manually you need to specify the IP address, network mask, default gateway and Domain Name Server (DNS) IP address for the WAN interface. IP address is the IP address of your WAN interface. Network mask is the network mask of your WAN interface.

The *default gateway* is the default gateway of the host. The DNS IP address is the IP address of your Domain Name Server. After you finish up filling these fields select on the “Next” button to move on to the next step.

The screenshot shows the 'System Setup: Step 3 — ISP Connection Settings (WAN) — Static' screen. The left sidebar contains a navigation menu with 'Setup Wizard' expanded to show 'System Setup' and 'Automatic Key VPN'. The main content area has a title bar 'Static Settings' and several input fields: 'IP Address' (192.168.1.1), 'IP Address of your WAN interface' (highlighted), 'Netmask' (255.255.255.0), 'Netmask of your WAN interface' (highlighted), 'Gateway IP Address' (192.168.1.1), 'Default Gateway IP Address for your WAN interface' (highlighted), 'DNS Server IP Address' (168.95.192.1), and 'DNS Server IP address for your WAN interface' (highlighted). 'Back' and 'Next' buttons are at the bottom right.

Figure 10: Configure WAN IP

Step 4

4.1.4 Configure LAN IP

In order to access the Internet through a DSL modem, you need to specify the IP address and network mask of your LAN interface as shown in the Figure 11. The IP is the LAN interface IP. All hosts in the sub-network reach the InstaGate by this LAN interface IP. The LAN interface may be a public IP address that you got from NIC (Network Information Center) or a private IP address. If the IP address is private, you have to enable the NAT (Network Address Translation) function. After you finish select on the “Next” button to move on to the next step.

The screenshot shows the 'System Setup: Local Network (LAN)' screen. The left sidebar contains a navigation menu with 'Setup Wizard' expanded to show 'System Setup', 'Advanced', 'SoftPak Director', 'Global Management', 'Online Help', and 'Logout'. The main content area has a title bar 'LAN Settings' and several input fields: 'IP Address' (192.168.2.1), 'IP Address of your LAN interface' (highlighted), 'Netmask' (255.255.255.0), and 'Netmask of your LAN interface' (highlighted). 'Back' and 'Next' buttons are at the bottom right.

Figure 11: Configure LAN IP

Step 5

4.1.5 Configure DHCP Server

In order to access Internet through a DSL modem, you need to configure the DHCP Server. By selecting “Enable DHCP server” you get the IP address automatically from the range specified in the “IP range” field. If you disable DHCP server then you will not obtain the IP address automatically. Then select on the “Next” button to move over to the next step as shown in the Figure 12. After you select the “Finish” button the device will reboot automatically with the appropriate setting.



The screenshot shows the InstaGate 305 web interface. The top banner includes the eSoft logo and the product name 'InstaGate 305'. Below the banner, a breadcrumb trail reads 'Main Menu > Setup Wizard > System Setup'. A left-hand navigation menu lists: Setup Wizard (expanded), System Setup (selected), Advanced, SoftPak Director, Global Management, Online Help, and Logout. The main content area is titled 'System Setup: DHCP Server' and contains a section for 'DHCP Server Settings'. In this section, the checkbox 'Enable DHCP Server' is checked. Below it, the 'IP Address range' is set to '192.168.2.11' through '192.168.2.50'. A yellow tooltip message states: 'If you enable the DHCP server, specify the range of IP addresses for clients on the network'. At the bottom right of the settings area are 'Back' and 'Next' buttons.

Figure 12: Configure DHCP Server

4.1.6 Registration

Enter your contact information to access important services such as the SoftPak Director and InstaGate Software Care, Hardware Care, and Phone/Email support. Correct billing information is required in order to purchase SoftPaks through the SoftPak Director. After you select the “Finish” button the device will reboot automatically with the appropriate settings.

eSoft InstaGate 305

Main Menu > Setup Wizard > System Setup

System Setup: Registration

Please keep your InstaGate registration information up-to-date in order to access important services such as the SoftPak Director and InstaGate Software Care, Hardware Care, and Phone/Email Care support. Correct billing information is required in order to purchase SoftPaks through the SoftPak Director.

Registration has been previously sent : Thu Jun 30 16:27:24 UTC 2005

Billing Address

Name of Organization	<input type="text" value="My Company"/>	Billing Contact	<input type="text" value="John Doe"/>
Address	<input type="text" value="1 Main St"/>	City	<input type="text" value="Broomfield"/>
Country	<input type="text" value="United States"/>	State or Province	<input type="text" value="Colorado"/>
		Postal Code	<input type="text" value="80021"/>

Administrative Contact

First Name	<input type="text" value="John"/>	Last Name	<input type="text" value="Doe"/>
E-mail Address	<input type="text" value="jdoe@mycompany.com"/>	Phone Number	<input type="text" value="555-555-5555"/>

Keep Me Informed!

eSoft Updates *Notify me of eSoft software updates, security patches, and feature enhancements.*

eSoft Announcements *Notify me of eSoft SoftPak applications and product promotions.*

* By subscribing to these notification lists you are authorizing eSoft to provide you with the above requested information by email. Your contact information is never provided to any third party.

Figure 13: Registration

4.2 VPN Setup Wizard

The InstaGate supports RFC 2049 Internet key exchange protocol (IKE). Using IKE, encryption keys are automatically negotiated and selected by two connected security appliances. To establish a secure tunnel in the Internet, two security appliances have to work together. One appliance encrypts the data and the other decrypts the encrypted data, and vice versa. As shown in Figure 14, these two security appliances are referred to as the *local gateway* and the *remote gateway*. The local network is a subnet that connects the local gateway and the remote network is a subnet that connects the remote gateway.

Step 1

4.2.1 New Automatic Key (IKE) Policy

First you have to give the policy a name as shown in Figure 14 below. After you finish select on the “Next” button to move on to the next step.



Figure 14: Policy Name

Step 2

4.2.2 Network Setup

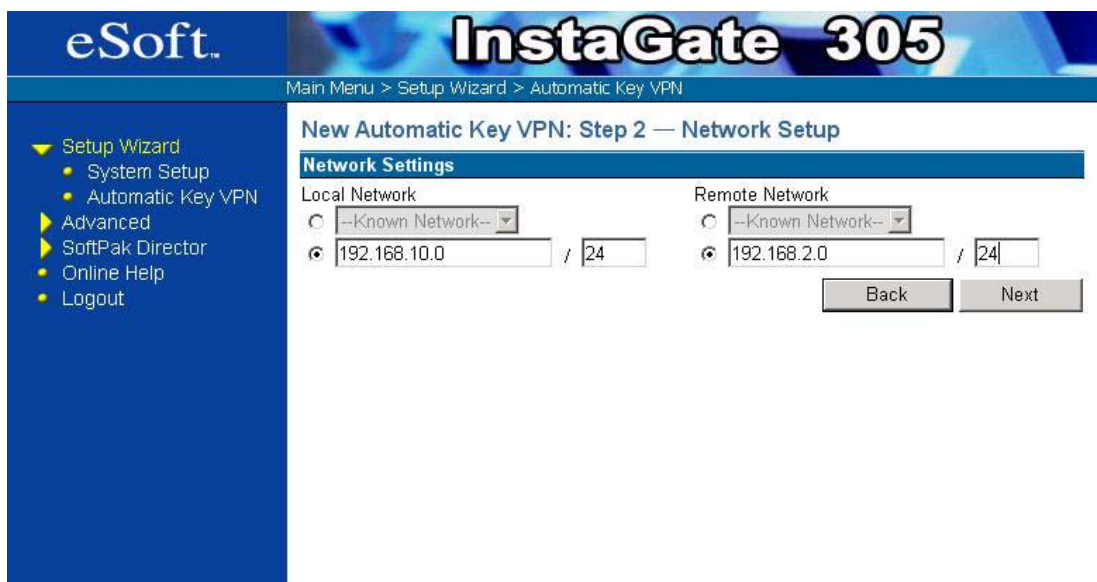


Figure 15: Local and Remote Network

The virtual private network that we want to define is from subnet 192.168.10.0/24 to subnet 192.168.2.0/24. As it is shown in Figure 15, the local network is 192.168.10.0/24, while the remote network is 192.168.2.0/24.

If you've already defined the corresponding subnet objects, you may also select the local and/or remote network by selecting the subnet object from the pull-down menu "Known Network".

To define a subnet object, please refer to section 6.1. After you finish please select "Next" button to move to the next step.

Step 3

4.2.3 Gateway Settings

Before creating the automatic key policy, you must define two gateway objects local and remote. You can define a new gateway object by just clicking the "New Gateway" button as shown in the Figure 16.



Figure 16: Define New Gateway

After you select the “New Gateway” Button you may need to provide gateway information as shown in the Figure 17. Here is an example for defining a local gateway WAN interface with IPv4 identity type (**for more information see: Defining Gateway Objects – section 6.3**)

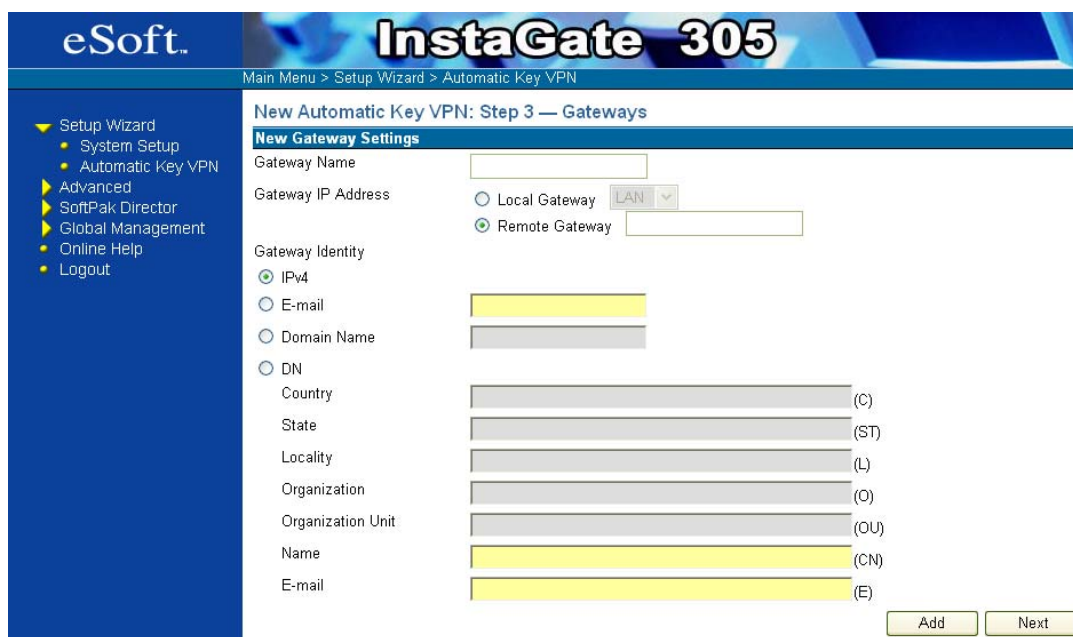


Figure 17: Define a New local Gateway

The screenshot shows the 'New Gateway Settings' form in the InstaGate 305 interface. The form is titled 'New Automatic Key VPN: Step 3 — Gateways'. It includes a navigation menu on the left with options like 'Setup Wizard', 'System Setup', 'Automatic Key VPN', 'Advanced', 'SoftPak Director', 'Global Management', 'Online Help', and 'Logout'. The main form area contains the following fields and options:

- Gateway Name:** A text input field containing the value 'remote'.
- Gateway IP Address:** Two radio buttons are present: 'Local Gateway' (unselected) and 'Remote Gateway' (selected). The 'Remote Gateway' option has a text input field next to it containing the IP address '192.168.1.64'. A dropdown menu next to 'Local Gateway' shows 'LAN' selected.
- Gateway Identity:** Four radio buttons are present: 'IPv4' (selected), 'E-mail', 'Domain Name', and 'DN'.
- Country:** A text input field with '(C)' as a placeholder.
- State:** A text input field with '(ST)' as a placeholder.
- Locality:** A text input field with '(L)' as a placeholder.
- Organization:** A text input field with '(O)' as a placeholder.
- Organization Unit:** A text input field with '(OU)' as a placeholder.
- Name:** A text input field with '(CN)' as a placeholder.
- E-mail:** A text input field with '(E)' as a placeholder.

At the bottom right of the form, there are two buttons: 'Add' and 'Next'.

Figure 18: Remote Gateway

First, you must give every gateway a unique name for reference. Then, you must specify the gateway IP. There are two types of gateway objects: the *local gateway* and the *remote gateway*. The local gateway is the gateway which the management station connects to. All other gateways are referred as the remote gateway.

If the gateway object that you want to define is a local gateway, please select the “Local Gateway” item. In such case, you only have to select the interface (WAN, LAN or DMZ) from the pull down menu. The InstaGate will get a gateway IP automatically from the interface information database.

If the gateway object that you want to define is a remote gateway, please select the “Remote Gateway” item and fill the IP address of that gateway.

Now, you have to specify the gateway identity. The gateway identity will be used when the Internet Key Exchange (IKE) protocol negotiates the key with peer IKE gateway. The security gateway provides four types of identities: IPv4 address, E-mail address, gateway domain name, and distinguish name (DN).

Please select the identity type and fill in the corresponding fields and Select the “Add” button, the respective gateway will then be automatically added to the pull down list as shown in the Figure below then select the appropriate remote and local gateway and select “Next” button. If you’ve already defined the corresponding gateway object, then you may select the local and/or remote gateway by selecting the gateway object from the pull-down menu.

eSoft. InstaGate 305

Main Menu > Setup Wizard > Automatic Key VPN

New Automatic Key VPN: Step 3 — Gateways

Gateway Settings

Local Gateway: local[WAN192.168.1.78]

Remote Gateway: remote[192.168.1.64]

New Gateway

Back Next

Figure 19: Gateway

Step 4

4.2.4 IKE Settings

The InstaGate provides two methods of Key Management. Pre-shared key or RSA certificates. For pre-shared key select the option and enter a key. The maximum length of the key is 20 characters (see Figure 20: IKE Proposal). For RSA select the option and select a certificate. Refer to section 6.6 for more information on defining certificate options. It is very important that two security appliances at the ends of the security tunnel use the same authentication method. To define the IKE SA lifetime, please fill in the time to the IKE SA lifetime field as shown in the Figure. After you finish please select the “Next” button to move to the next step.

eSoft. InstaGate 305

Main Menu > Setup Wizard > Automatic Key VPN

New Automatic Key VPN: Step 4 — IKE

IKE Settings

Key Management Settings

Preshared Key:

Confirm:

IKE Proposal: High Security(AES 256-bit Enc, SHA-1 Auth)

IKE SA Lifetime: 24 Hour(s)

Back Next

Figure 20: IKE Proposal

Step 5

4.2.5 IPSec Settings

The IPSec proposal consists of 1) Perfect Forward Secrecy (PFS) and 2) IPSec security association (SA) lifetime time. (see Figure 21: IPSec Proposal) The InstaGate configures all other parameters automatically.



Figure 21: IPSec Proposal

To define the IPSec SA lifetime, fill in the time to the IPSec SA lifetime field.

If you select the “Perfect Forward Secrecy” item, the IKE will randomly re-generate the secret when it negotiates a new key; otherwise, IKE will re-generate the secret based on the previous secret.

After you finish select on the “Finish” button the policy will be automatically added to the Automatic key information management table as shown in the Figure. For more details, refer to section 10.1.



Figure 22: Automatic key information Table

5 System Setup

5.1 Setup time

The user interface of the InstaGate provides an easy way to setup the system time. The “Current System Time” option displays the system clock with current date and day. The “Synchronize with Client” option synchronizes system time with the administrator’s workstation. To do this please select the “Synchronize with Client” option and select “Synchronize Now” button as shown in the Figure 23: Setup time.

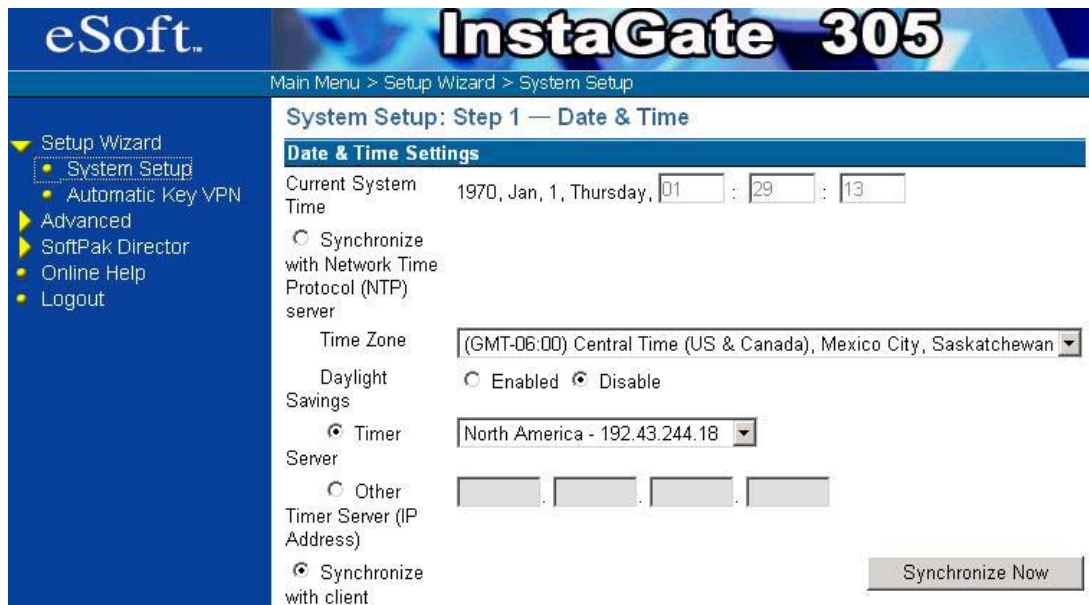


Figure 23: Setup time

Alternative option:

An alternative is “Synchronize System Clock with Network Time Protocol (NTP) Server” option which synchronizes the system time to an internet Time Server. It includes a large list of Time servers and Time zones organized by country. You can select any Time Server and Time Zone to synchronize your system time. The “Daylight Saving” options adds one hour to your time zone during the time period specified in the “Daylight Period” field. You can enable or disable the “Daylight Saving” option by clicking the “Daylight Saving” option box. After you finish, select the “Synchronize Now” button as shown in the Figure 24: Setup time.

eSoft. InstaGate 305

Main Menu > Setup Wizard > System Setup

System Setup: Step 1 — Date & Time

Date & Time Settings

Current System Time: 2005, Jul, 7, Thursday, 13 : 39 : 50

Synchronize with Network Time Protocol (NTP) server

Time Zone: (GMT-06:00) Central Time (US & Canada), Mexico City, Saskatchewan

Daylight Savings: Enabled Disable

Timer Server: North America - 192.43.244.18

Other Timer Server (IP Address):

Synchronize with client

Figure 24: Setup time

5.2 Administrator

As shown in Figure 25, under “Main Menu > Advanced > System > Administrator” page, there is an option to let you manage this InstaGate remotely. If you want to allow all HTTPS request to manage this InstaGate remotely, select the checkbox of "Allows HTTPS management via the WAN interface". You have to select the “Apply” button to validate the setting.

Main Menu > Advanced > System > Administrator

Administrator

Remote Support

Allow HTTPS management via the WAN interface

Account Management

Username	Password	Confirm Password	Privilege	Lock	Num	
			1	NO		<input type="button" value="Add / Modify"/>
admin	*****		4	no	0	<input type="button" value="Modify"/> <input type="button" value="Delete"/>

Privilege Levels

- 1 Account can only read some forms, but can't make any configuration changes.
- 2 Account can read all forms, but can't make any configuration changes.
- 3 Account can read all forms and make some configuration changes.
- 4 Account has full access to read all forms and make configuration changes.

Figure 25: Administrator Management

Also you can configure administrator accounts. The “admin” is the default account which has privilege 4. There are four levels of privilege, as shown below:

Privilege	
1	This account only can read some of web pages, but can't write any of web pages.
2	This account can read all of web pages, but can't write any of web pages.
3	This account can read all of web pages, and can write some of web pages.
4	This account can read all of web pages, and can write all of web pages.

Table 2: Administrator Privileges

If you want to change the password of the “admin” account, insert “admin” into User Name field and insert the password that you want into Password field then select the “Add/Modify” button to validate the setting. Except for the “admin” account, you can create up to 20 accounts.

To add a new administrator account, you must fill the user name and the corresponding password then select the “Add/Modify” button. The "Modify" button can put the selected account into "User Name" field automatically. To delete the existing account, all you have to do is to select the “Delete” button of the corresponding account.

5.3 Setup interface

The InstaGate provides three different interfaces: WAN, LAN and DMZ. You may setup the interfaces under “Main Menu > Advanced > System > Interfaces” page.

5.3.1 WAN Interface

5.3.1.1 Get IP by PPPoE

If you connect to Internet via the ADSL modem, you must select “Get IP by PPPoE” item when configuring the WAN interface



Figure 26: Get IP by PPPoE

As shown in Figure 26, you have to fill in the user name, the password and the server name (optional) that you got from the ISP. The option “CLAMP the MSS to 1360 for AOL” means that for some special ISP like AOL you need to CLAMP the MSS to 1360. The “MTU for PPPoE” means that you can specify MTU for PPPoE. If you want your ADSL connection always on, please choose the “Always connected” radio box. Alternatively you can choose “On-demand with disconnect” which means that when you transmit any data to the Internet, the InstaGate will connect to your ISP automatically. The “idle time” means that after the idle time expires, the system will suspend the Internet connection. After you fill in the user name and the password, you must select the “Apply” button, and the device will reboot automatically.

5.3.1.2 Get IP by DHCP

As shown in Figure 27, if you connect to Internet via other routers and there is a DHCP server in your network environment, you may select “Dynamic (DHCP)” and select the “Apply” button.

In some areas, people use a DHCP client to get the IP of the WAN interface from MSOs, but access the Internet by PPTP tunnel to ISPs. Thus you have to select the “Add static route to DHCP server” box for adding a static route to a DHCP server. The “Force Renew” button will renew a DHCP request to the DHCP server to get an IP address.



Figure 27: Get IP by DHCP Server

5.3.1.3 Static Configuration

You may also configure the WAN interface manually. To configure the WAN interface manually, you have to select “Static”. As shown in Figure 28, you have to fill in the IP address of the WAN interface, the subnet mask, default gateway and the name server fields. After you fill in these fields, select the “Apply” button and the device will be rebooted automatically.

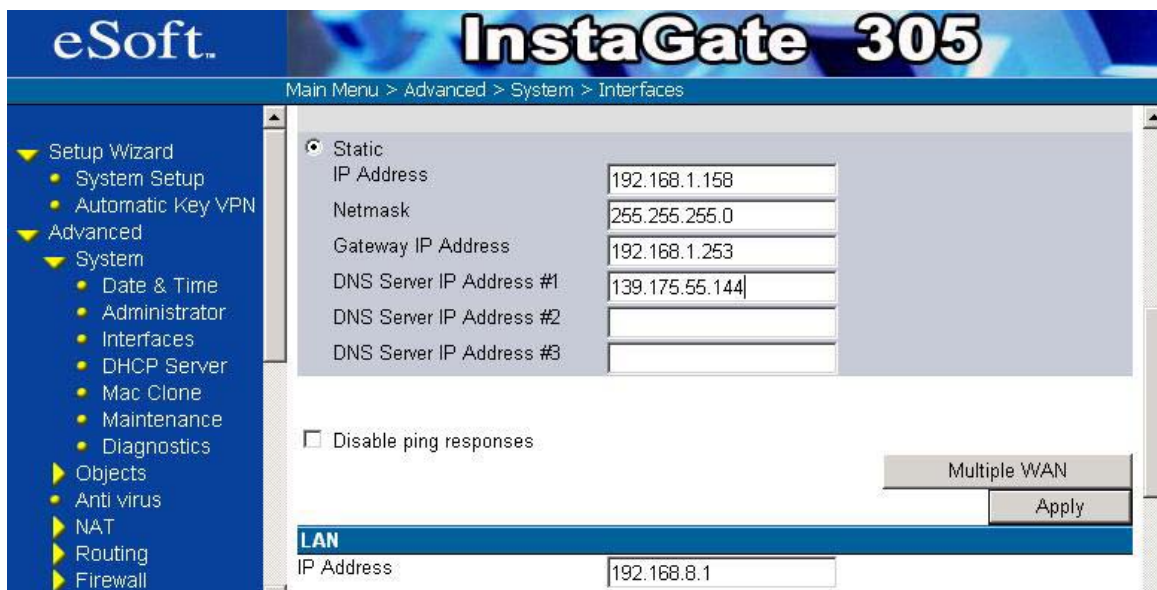


Figure 28: WAN interface static configuration

5.3.1.4 Options for WAN interface

As shown in Figure 29, you can set the MTU (Maximum Transmit Unit) value in the “MTU for WAN interface” field. The default value is 1,500. If you select the “Disable Ping Responses” checkbox, the WAN interface will not respond to pings. This can help make the network less acceptable to Denial of Service (DoS) attacks.



Figure 29: The options for WAN interface

5.3.2 LAN Interface

As shown in Figure 30, the LAN Interface parameter consists of the IP address and the subnet mask. The IP is the LAN interface IP. All hosts in the sub network reach the InstaGate by this LAN interface IP. The LAN interface may be a public or a private IP address. If the IP address is private, you have to enable the NAT (Network Address Translation) function (discussed in section 7).



Figure 30: LAN interface

After you fill in the IP address and the mask fields, you have to select the “Apply” button to affect the setting.

If you want to use the WAN interface IP address to be the default global IP address for the default NAT rules, select the checkbox of “Enabled Default NAT Policies”. This option can help users to connect to Internet easily when their global IP is a dynamic IP address that they received from an ISP.

If you want multiple LAN interfaces, just select the “Multiple LAN” button. After you select the “Multiple LAN” button you need to fill the IP address and the subnet mask. After you finish just select the “Add” button. After you select the “Add” button the respective filed will get automatically added to the Multiple LAN table as shown in the Figure.

Figure 31: Multiple LAN

Figure 32: Existing LANs

5.3.3 DMZ Interface

The DMZ parameters also consists of an IP address and the subnet mask. After you fill the IP address and the mask fields, you have to select the “Apply” button to validate the setting.

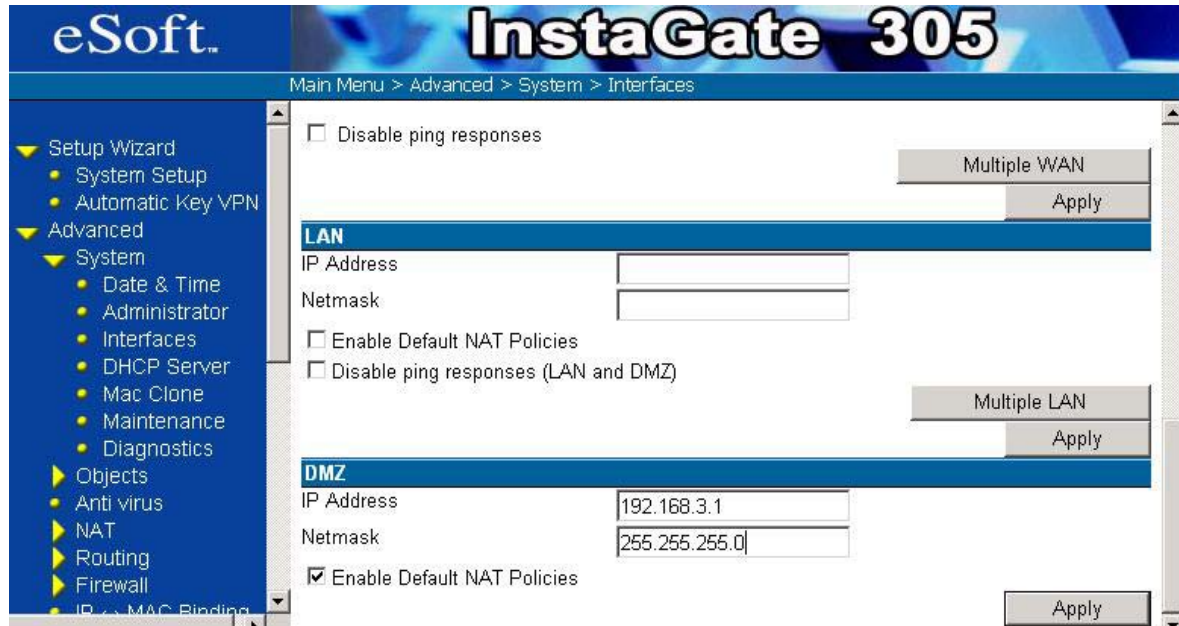


Figure 33: DMZ Interface

5.4 Configure DHCP Server

The DHCP (Dynamic Host Configuration Protocol) server allows the host stations to obtain their TCP/IP configuration from the server at start-up. To configure the DHCP server, you must select the “DHCP Server” option under the “System” menu.

To configure the DHCP server, you have to fill the “Lease Time” field, the “Default Gateway IP Address” field, the “Domain Name” field, the “DNS Server” field and the “WINS Server” field.

The “Lease Time” field is the lease time of DHCP service. The “Domain Name” field is the domain name of the subnet that the DHCP server covers. The “Default Gateway IP address is the default gateway of the host. You can apply LAN interface IP as default gateway by just selecting “LAN Interface IP Address” option button, otherwise you can specify user defined IP by selecting “Other IP Address” option button and specify the IP address for the default gateway.

The “DNS Server” field is the IP address of the domain name server. You can apply LAN Interface IP as the IP address of the Domain name server by just clicking the “LAN Interface IP” option button, otherwise you can have an user defined IP address for the domain name server for this you need to select “User defined IP” option button and fill in the appropriate IP address.

The *WINS server* field is the IP address of the WINS name server. After you finish filling in these fields, you should select the “Apply” button to make the configuration take effect.

Figure 34: DHCP Server Settings

You may allocate a range of IP addresses for clients or specify every client that is identified by the MAC address with a unique IP address. As it is shown in Figure 35, you may also add an IP range for the DHCP service by filling in the *range start* and *range end* fields and select the “Add” button. To delete an existing IP range, you only have to select the “Delete” button of the corresponding range.

You may also assign a specific IP address to a specific client. The client host is identified by its MAC address. To do this, you have to fill in the IP address and the MAC address of the client and select the “Add” button. To delete the configuration, you only have to select the “Delete” button of the corresponding configuration.

Figure 35: Configuration for DHCP server

5.5 Maintenance

The InstaGate provides functions for system maintenance. You may access these features under the “Main Menu > Advanced > System > Maintenance” page.

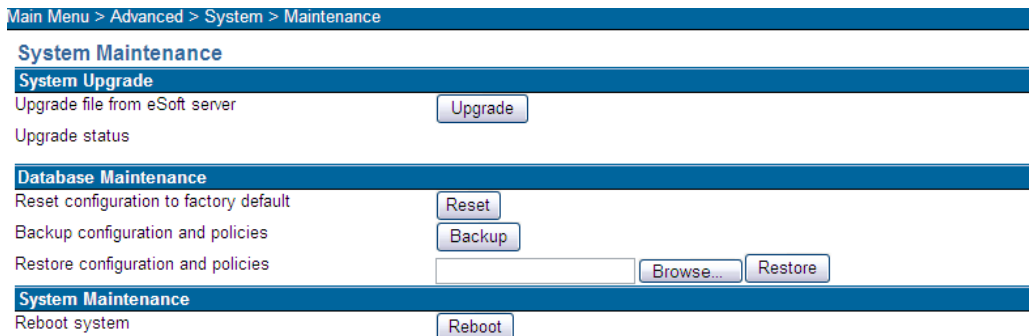


Figure 36: System Maintenance

As shown in Figure 36, the “System Upgrade” function lets you upgrade the latest version of device firmware.

When you have selected the firmware, select the “Upgrade” button. After 80~90 seconds, you can see a dialog show “System upgrade complete!” and then the device will reboot. The Web User Interface will be auto reconnected after 60 seconds.

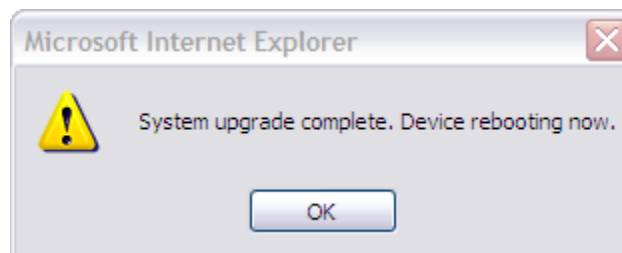


Figure 37: System Upgrade Reboot

If you want to reset the system to the factory default values, select the “Reset” button. Clicking the “Backup” button can save all of the system configuration and policies to your PC, while the “Restore” button allows you restore all of the system configuration and policies to the InstaGate.

The “Reboot” button allows you reboot the device without resetting to factory defaults.

5.6 Diagnostics

```

Main Menu
Diagnostics
Perform System Diagnostics
Ping to Destination Address      www.yahoo.com      Apply
Trace Route to Destination Address  [ ] 10 Hops      Apply
SoftPak Director Connectivity Test      Apply

Result
PING www.yahoo.akadns.net (68.142.197.77): 56 data bytes
64 bytes from 68.142.197.77: icmp_seq=0 ttl=57 time=53.2 ms
64 bytes from 68.142.197.77: icmp_seq=1 ttl=57 time=53.2 ms
64 bytes from 68.142.197.77: icmp_seq=2 ttl=57 time=52.8 ms
64 bytes from 68.142.197.77: icmp_seq=3 ttl=57 time=52.4 ms

--- www.yahoo.akadns.net ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 52.4/52.9/53.2 ms

```

Figure 38: System Diagnostics

As shown in Figure 38, the InstaGate provides you with three useful diagnostic tools. One is “*Ping*”, and the other is “*Trace Route*”, and the third is “*SoftPak Director Connectivity*”. *Ping* verifies L3 connectivity to remote computers. It sends Internet Control Message Protocol (ICMP) echo packets to a computer and listens for echo reply packets. *Ping* waits for up to 1 second for each packet sent, and prints the number of packets transmitted and received to the console. You can check the connection to Internet with this function. Please insert a domain name or IP address into “*Ping*” field and select the “*Apply*” button. You can see the result as follows.

```

Main Menu
Diagnostics
Perform System Diagnostics
Ping to Destination Address      www.yahoo.com      Apply
Trace Route to Destination Address  [ ] 10 Hops      Apply
SoftPak Director Connectivity Test      Apply

Result
PING www.yahoo.akadns.net (68.142.197.77): 56 data bytes
64 bytes from 68.142.197.77: icmp_seq=0 ttl=57 time=53.2 ms
64 bytes from 68.142.197.77: icmp_seq=1 ttl=57 time=53.2 ms
64 bytes from 68.142.197.77: icmp_seq=2 ttl=57 time=52.8 ms
64 bytes from 68.142.197.77: icmp_seq=3 ttl=57 time=52.4 ms

--- www.yahoo.akadns.net ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 52.4/52.9/53.2 ms

```

Figure 39: System Diagnostics Ping Results

“*Trace route*” determines the route taken to a destination by sending ICMP echo packets with varying time-to-live (TTL) values to the destination. Before forwarding a packet, each router along the path is required to decrement the TTL value on a packet by at least 1, so the TTL value is effectively a hop count.

When the TTL value on a packet reaches 0, the router sends back an ICMP "Time Exceeded" message to the source computer. It determines the route by sending the first echo packet with a TTL value of 1 and incrementing the TTL value by 1 on each subsequent transmission until the target responds, or the maximum TTL value is reached.

- The route is determined by examining the ICMP "Time Exceeded" messages sent back by intermediate routers. Some routers silently drop packets with expired TTL values and are invisible to "Trace route". It is particularly useful if you're experiencing problems connecting to a specific site. Simply enter the site address, and the trace will show where performance bottlenecks might be occurring--whether they're at your local provider, the site itself or somewhere in between. Once you discover the source of the problem, you can contact that particular host or provider for more information or to report the problem.

Main Menu > Advanced > System > Diagnostics

Diagnostics

Perform System Diagnostics

Ping to Destination Address

Trace Route to Destination Address Hops

SoftPak Director Connectivity Test

Result

```

1 10.10.10.3 (10.10.10.3) 1.338 ms 1.213 ms 1.197 ms
2 199.45.143.1 (199.45.143.1) 2.051 ms 2.058 ms 2.013 ms
3 s6-0-0-10-15-0.ar4.DEN2.gblx.net (64.212.41.141) 5.211 ms 4.836 ms 5.16 ms
4 so5-0-0-2488M.ar1.SJC2.gblx.net (67.17.67.154) 36.863 ms 36.661 ms 36.518 ms
5 so-4-0-0.edge1.SanJose1.Level3.net (4.68.127.53) 35.28 ms 36.391 ms 35.504 ms
6 * so-1-2-0.bbr2.SanJose1.Level3.net (209.244.3.141) 36.756 ms 38.293 ms
7 as-1-0.bbr2.Dallas1.Level3.net (64.159.0.245) 48.869 ms ae-0-0.bbr1.Dallas1.Level3.net (64.159.1.109) 51.405 ms as-1-0.bbr2.Dallas1.Level3.net (64.159.0.245) 54.262 ms
8 ae-11-51.car1.Dallas1.Level3.net (4.68.122.13) 47.689 ms ae-21-56.car1.Dallas1.Level3.net (4.68.122.173) 48.236 ms ae-11-53.car1.Dallas1.Level3.net (4.68.122.77) 48.052 ms
9 4.79.180.10 (4.79.180.10) 63.138 ms 52.43 ms 52.003 ms
10 ten-8-1.bas1.mud.yahoo.com (68.142.193.27) 52.444 ms ten-8-1.bas2.mud.yahoo.com (68.142.193.27) 52.439 ms 54.338 ms

```

Figure 40: System Diagnostics Traceroute Results

The last diagnostic option performs a "SoftPak Director Connectivity Test". The test is used to ensure that the InstaGate has connectivity support with the SoftPak Director in order to receive regular updates. Select the "Apply" button and check the results as in the figure below.

Main Menu > Advanced > System > Diagnostics

Diagnostics

Perform System Diagnostics

Ping to Destination Address

Trace Route to Destination Address Hops

SoftPak Director Connectivity Test

Result

HTTPS Passed

SCP Passed

Figure 41: System Diagnostics SoftPak Director Connectivity

5.7 Secure HTTP Proxy

Some ISPs require that all HTTPS connection requests be passed to a dedicated proxy server located at the ISP. InstaGate uses HTTPS to contact the SoftPak Director for product updates and registration. Therefore, if required by your ISP, you must select the Enable Proxy for HTTPS connections check box in order to contact the SoftPak Director.

You must also enter the proxy server's "Proxy Address" and "Proxy Port" (which can be obtained from your ISP). If the proxy server requires a login enter the "Proxy username" and "Proxy password" that will be used by the InstaGate to authenticate with the proxy server. Select "Apply" to save the changes.

Main Menu > Advanced > System > Secure HTTP Proxy

Secure HTTP Proxy

Secure HTTP Proxy Settings

Enable Proxy for HTTPS connections

Proxy address

Proxy port

Proxy username

Proxy password

Figure 42: Secure HTTP Proxy

6 Define Objects

You may define *subnet*, *gateway* or *service* objects before you edit the firewall, automatic key or manual key policies. These objects help you edit policies more easily. In this chapter, we discuss how to define objects.

6.1 Define Subnet Object

Under “Main Menu > Advanced > Objects > Subnet” page, you may define a subnet object. As it was shown in Figure 43, you must give every subnet a unique name for reference. If the object you want to define is a single host, please select the “Host” item and fill the host IP. If the object you want to define is a subnet, please select the “Network” item and fill the subnet in CIDR format.

Figure 43 gives an example for defining a subnet object. We define a subnet object called “eSoft”, and it specifies all hosts in the 192.168.2.0/24 area. After filling in the fields in this page select the “Add” button to add this object. The object that you add will be listed in the object list (see Figure 44). To delete existing subnet object, you only have to select the “Delete” icon of the corresponding object record. This device supports a default object called “Any_Network” that specifies *all hosts in the Internet*.



Figure 43: Define a Subnet Object

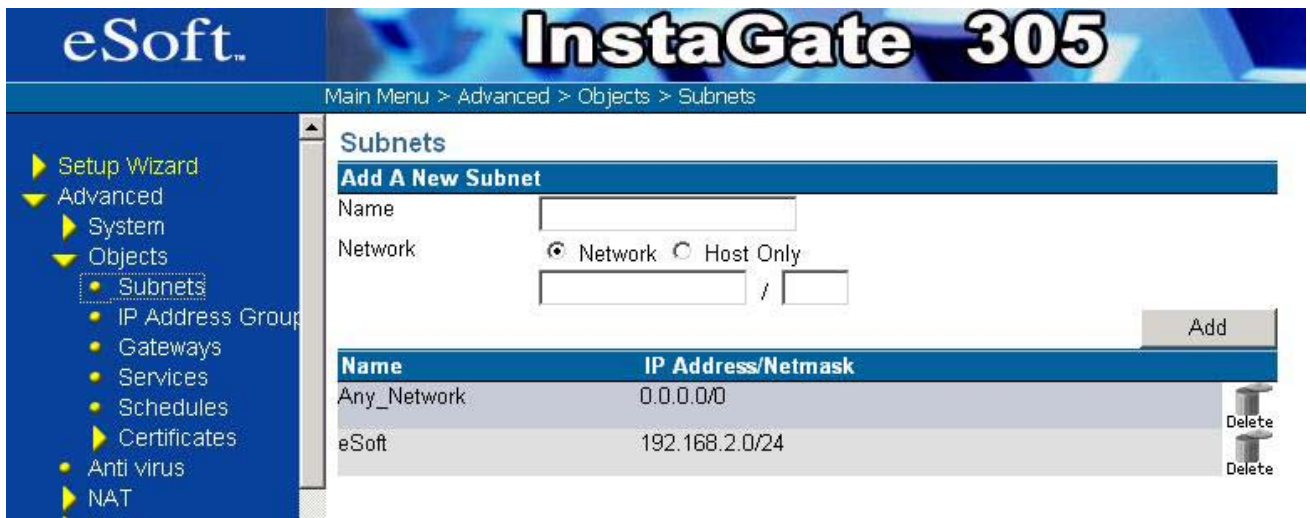


Figure 44: Subnet Object List

6.2 Defining IP Address Groups

Under “Main Menu > Advanced > Objects > IP Address Groups” page, you may define a group of subnet objects. As it was shown in Figure 45, you must give every group a unique name for reference.

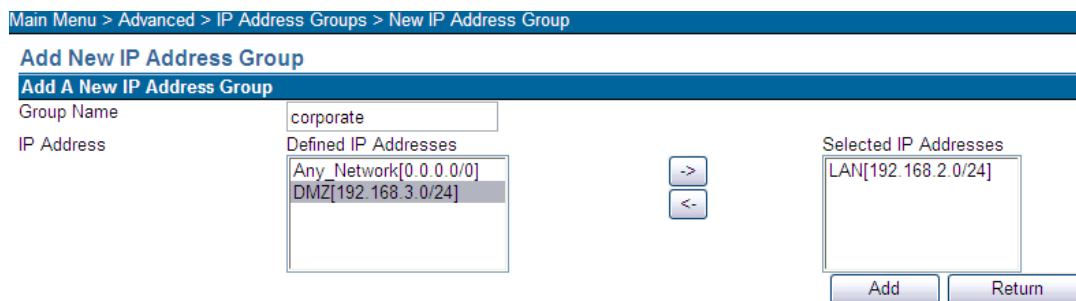


Figure 45: New IP Address Group

Figure 48 gives an example for defining a group object. We define a group object called “corporate” that includes the LAN and DMZ subnet objects. Select the Subnet Objects from the “*Defined IP Addresses*” and select the arrow to add the object(s) to the “*Selected IP Addresses*” list. After adding all of the subnets to the “*Selected IP Addresses*” that will be included in a group, select the “Add” button to add this object. The object that you add will be listed in the object list (see Figure 44). To delete existing subnet object, you only have to select the “Delete” icon of the corresponding object record.

6.3 Defining Gateway Objects

Under the “Main Menu > Advanced > Objects > Gateway” page, you may define a gateway object. The gateway object will be referenced by the automatic key policy (see section 10.1.1) when creating a VPN. Select the “Add” button to create a new Gateway. First, you must give every subnet a unique name for reference. Then, you must specify the gateway IP. There are two types of gateway objects: the *local gateway* and the *remote*

gateway. The local gateway is the gateway which the management station connects to. All other gateways are referred as the remote gateway.

If the gateway object that you want to define is a local gateway, please select the “Local Gateway” item. In such case, you only have to select the interface (WAN, LAN or DMZ) from the pull down menu. The InstaGate will get the gateway IP automatically from the interface information database.

If the gateway object that you want to define is a remote gateway, select the “Remote Gateway” item and fill the IP address of that gateway.

Now, you have to specify the gateway identity. The gateway identity will be used when the Internet key exchange (IKE) protocol negotiates the key with remote gateway. The security gateway provides four types of identities: IPv4 address, E-mail address, gateway domain name, and distinguish name (DN). Please select the identity type and fill in the corresponding fields.

Figure 46 gives an example for defining a local gateway object in WAN interface with IPv4 identity type.

The screenshot shows the 'Add A New Gateway' configuration page in the InstaGate 305 web interface. The page title is 'Add A New Gateway' and the breadcrumb trail is 'Main Menu > Advanced > Objects > Gateways'. The form includes the following fields and options:

- Name:** A text input field containing the value 'local'.
- Address:** A section with two radio buttons: 'Local Gateway' (selected) and 'Remote Gateway'. The 'Local Gateway' option has a dropdown menu showing 'LAN'.
- Identity:** A section with four radio buttons: 'IPv4' (selected), 'Email', 'Domain Name', and 'DN'.
- Country:** A text input field with '(C)' to its right.
- State:** A text input field with '(ST)' to its right.
- Locality:** A text input field with '(L)' to its right.
- Organization:** A text input field with '(O)' to its right.

A left sidebar contains a navigation menu with the following items:

- Setup Wizard
 - System Setup
 - Automatic Key VPN
- Advanced
 - System
 - Objects
 - Subnets
 - IP Address Group
 - Gateways
 - Services
 - Schedules
 - Certificates
 - Anti virus
 - NAT
 - Routing
 - Firewall
 - IP - MAC Binding

Figure 46: Define a local gateway object

Figure 47 gives an example for defining a remote gateway object with Domain Name identity type.

Figure 47 shows the 'Add A New Gateway' form in the InstaGate 305 interface. The form is titled 'Add A New Gateway' and is part of the 'Gateways' section. It contains several fields:

- Name:** remote
- Address:** Local Gateway (selected), LAN (dropdown), Remote Gateway (192.168.1.64)
- Identity:** IPv4, Email, Domain Name (192.168.1.64), DN, Country, State, Locality, Organization, Organization Unit

Figure 47: Define a remote gateway object

After you select the “Add” button on the page, the object will be added to the database and the gateway object list will reserve this record (see Figure 48).

Figure 48 shows the 'Gateways' list in the InstaGate 305 interface. The list has columns for Name, IP Address, and Identity. It shows two entries:

Name	IP Address	Identity	
remote	192.168.1.64	192.168.1.64	Edit Delete
local	WAN	WAN	Edit Delete

Figure 48: The Gateway Object List

Click the “Edit” button to modify any existing gateway objects. To delete existing subnet object, you only have to select the “Delete” icon of the corresponding object record.

6.4 Define Service Objects

Compared with a traditional firewall, the InstaGate provides an easy mechanism to define and manage service types. Where many allow users to add customized services, they are typically limited to IP, ICMP layer 2 and 3 protocols, hence have no application-layer awareness. The InstaGate is service oriented. It provides original protocol service inspection and customized port inspection where the administrator may customize a service, including the protocol service inspection in the same rule.

6.4.1 Default Service

As shown in Figure 49, the InstaGate has built-in standard services for the most popular protocol families. These are standard service types and normally should not be edited.



Figure 49: Built-in Standard Service Object

As shown in Figure 50, the InstaGate also provides the user with many useful service objects. Users can edit these service objects when changes are needed. You can add some of these services into a firewall rule to manage the traffic on your network.

Main Menu > Advanced > Objects > Services

Name	Protocol	Source Port	Destination Port	Edit	Delete
DNS_forTCP	TCP(6)	1024 — 65535	53		
TCP_AnyPort	TCP(6)	1 — 65535	1 — 65535		
UDP_AnyPort	UDP(17)	1 — 65535	1 — 65535		
SSH(22)	TCP(6)	1024 — 65535	22		
SMTP(25)	TCP(6)	1024 — 65535	25		
TFTP(69)	UDP(17)	1024 — 65535	69		
GOPHER(70)	TCP(6)	1024 — 65535	70		
POP3(110)	TCP(6)	1024 — 65535	110		
NNTP(119)	TCP(6)	1024 — 65535	119		
NTP(123)	UDP(17)	1024 — 65535	123		
IMAP(143)	TCP(6)	1024 — 65535	143		

Figure 50: Service Objects List

6.4.2 Add a New Service

The InstaGate provides two service types: re-defined traditional services, and custom defined services. The detail is shown in Figure 51 and Figure 52.

6.4.2.1 Re-Defined Service Configuration

Main Menu > Advanced > Objects > Services > New

New Service

Service Settings

Name:

Redefine Existing to new port number

Custom Service

Protocol:

Source Port: —

Destination Port: —

NOTE: The Source Port range is usually is 1024 — 65535

Figure 51: New Service Object

Under the service page, select the "New Service" icon. The administrator clicks the "Re-defined Service Port" radio-box, picks up the service from drop-down window, assigns the re-defined port number and then clicks the "Add" button. For example, there are some ftp sites which don't use the standard port 21 (such as port 999) as their service port. You can re-define the service port to map their private port.

6.4.2.2 Custom Defined Service Configuration

The screenshot shows the 'New Service' configuration page in the InstaGate 305 interface. The page title is 'New Service' and the breadcrumb is 'Main Menu > Advanced > Objects > Services > New'. The left sidebar shows a navigation menu with 'Objects' expanded. The main content area is titled 'Service Settings' and contains the following fields:

- Name: xxx_game
- Service: Redefine Existing (FTP) to new port number 999
- Service: Custom Service
- Protocol: TCP(6) UDP(17) ICMP(1) Other
- Source Port: 1024 - 65535
- Destination Port: 1024 - 65535

NOTE: The Source Port range is usually is 1024 - 65535

Buttons: Add, Return

Figure 52: Customer Define Service Configuration.

Under the service page, select the "New Service" icon. The administrator clicks the "Custom Service" button, selects the protocol type, fills in the source port range and destination port range and then clicks the "Add" button. If you select the "Custom Service" option, you have to type your customized protocol number. For Example, TCP is 6 and UDP is 17.

6.5 Schedule

Under the "Main Menu > Advanced > Objects > Schedules" page, you can set the schedule for Policy Activation. First you must specify a Schedule name. Then set the Start time by selecting the day of the Activating Policy (it can be either Everyday or any week day from Monday-Sunday), and the time you want the policy to be activated. End Time indicates the day and time from which the policy will be deactivated. After you fill in the required information, you must select the "Add" button in order to save the settings.



Figure 53: Schedule

You can view all Policy schedules in the Policy Table along with the new policy that is been added, as shown below.

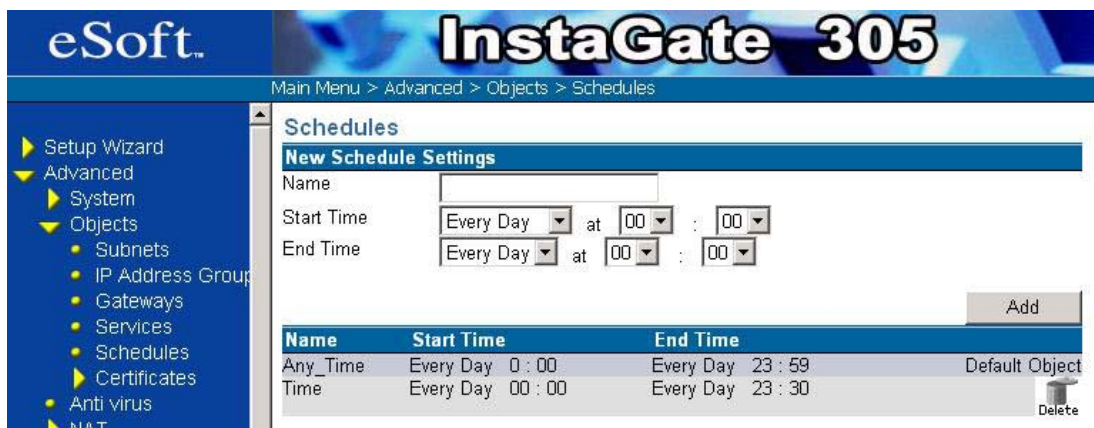


Figure 54: New Schedule Settings

6.6 Define Certificate Objects

6.6.1 Certificate Management

Under the “Main Menu > Advanced > Objects > Certificate > Cert. Management” page (see Figure 55), you may manage the certificates on the device.

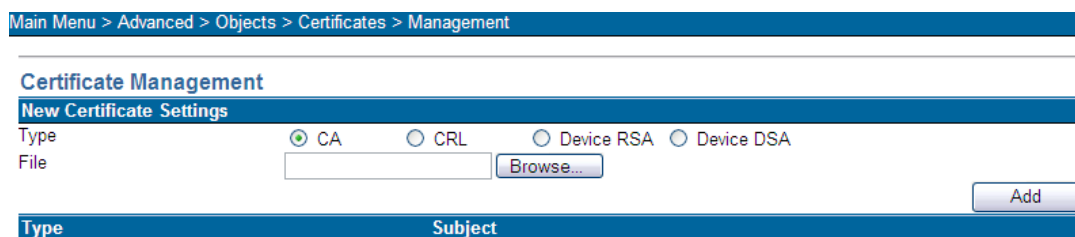


Figure 55: Certificate Management

If you want to load a certificate from a certificate authority (CA) into the InstaGate, please select the “CA” item and select the certificate file from the management station. Then, select the “Load” button. If you want to load a certificate revocation list (CRL) of a CA into the InstaGate, please select the “CRL” item and select the CRL file from the management station. Then, select the “Load” button. Before you load the CRL, you have to load the CA certificate. After you load the certificate and the certificate revocation list, the certificate management list keeps these two records.

To view the detailed information of a certificate in the certificate management list, select the “Detail” button of the corresponding record.

6.6.2 Certificate Request

Main Menu > Advanced > Objects > Certificates > Request

Certificate Request

Device	Subject Information
Country	US (C) Detail information refer to: ISO-3166
State	CO (ST)
Locality	Broomfield (L)
Organization	eSoft, Inc (O)
Organization Unit	(OU)
Name	esoft (CN)
Email	support@esoft.com (E)
Key Length	<input type="radio"/> 512 bits <input checked="" type="radio"/> 1024 bits <input type="radio"/> 2048 bits

Figure 56: Certificate Request Form

Under the “Main Menu > Advanced > Objects > Certificate > Cert. Request” page (see Figure 56), you may fill the certificate request form and generate the device certificate request. The “RSA” and “DSS” item specify the signature algorithm of the certificate request. The “512 bits”, “1024 bits” and “2048 bits” items specify the key length of the certificate request. The link “ISO-3166” displays a list containing English country name and code for your reference.

After you fill the form and select the suitable algorithm and the key length, please select the “Generate” button to generate the certificate request. The process may take several minutes. After the InstaGate completes the key generation process, the following page (Figure 57) appears. You may select and copy the certificate request; paste it to an empty file; then, save this file. The simplest way is to select the “Save to File” checkbox and to select “Return” button. Then, you may save the certificate request to a file.

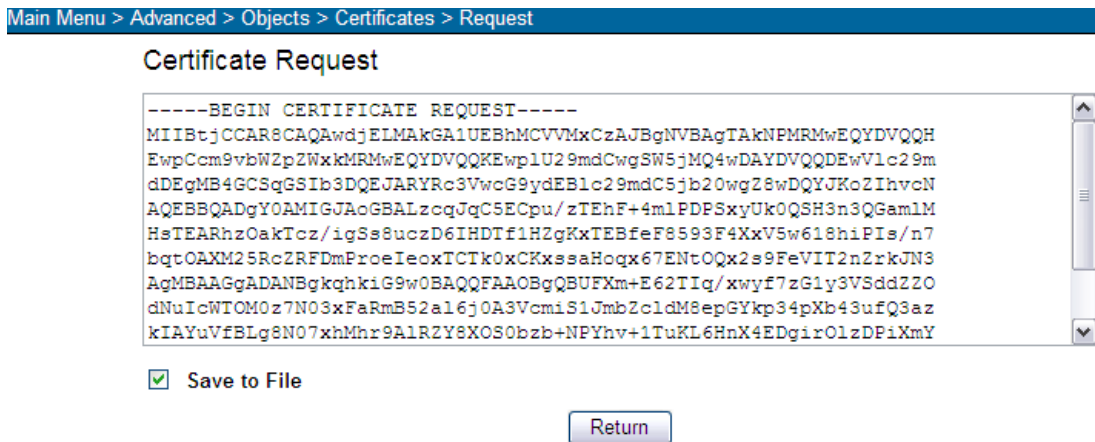


Figure 57: Certificate Request

Please send this certificate request to a CA and sign it. The CA will then send you the official certificate. Please load this certificate into this InstaGate under “Main Menu > Advanced > Objects > Certificate > Cert. Management”. As was shown in Figure 58, select the “Device RSA Cert.” item. Select this certificate file and load it by clicking the “Load” button”. Similarly, you can do the same for “Device DSS Cert”.

Before loading the device certificate, load the CA certificate and the CRL. Since the InstaGate will check the correctness of the certificate when you load a certificate, if you do not load the CA certificate first, the check will fail. If you load the device certificate successfully, the certificate management list will keep this record.

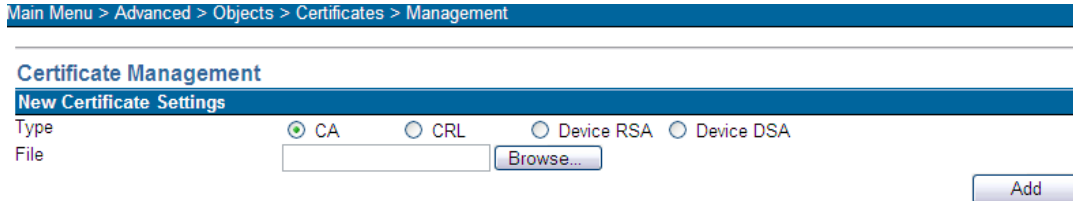


Figure 58: Loading the Device Certificate

7 Network Address Translation

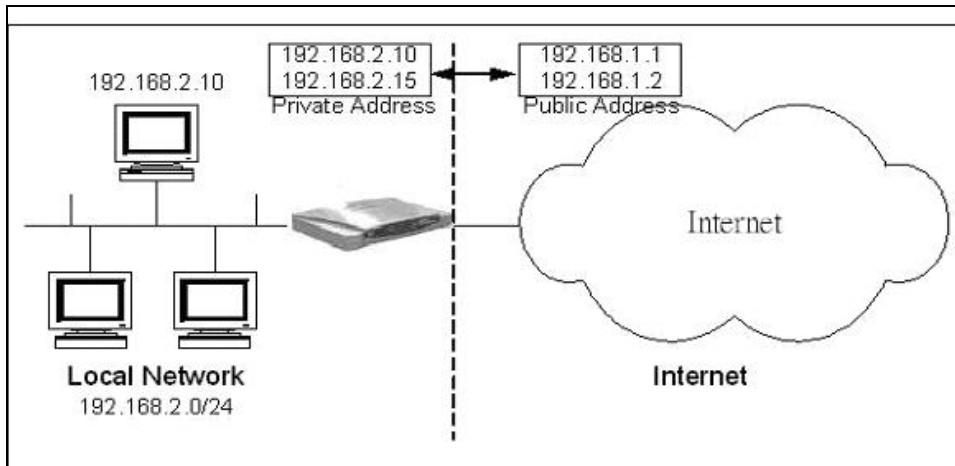


Figure 59: Network Address Translation

Network address translation (NAT; RFC 1631) translates the source or destination IP addresses in an IP packet. In Figure 59, the network at the left of the InstaGate is a local network and the network at the right is the Internet. The IP addresses in the local network are all private addresses that are not accessible on the Internet.

When a host in the local network sends an IP packet to the Internet, NAT translates the source IP address in the IP packet to a global public IP address before forwarding this IP packet to the Internet. When the response IP packet comes back to the InstaGate, NAT translates the destination address back to the private IP address of the original host.

7.1 NAT Rules

Under the “Main Menu > Advanced > NAT > Rules” page, you may define NAT rules. To add a new NAT rule, please select the “Add” button. After you select the “Add” button, a page shows as Figure 60.

Figure 60: Add NAT Rule

You must specify each NAT rule with a unique name. First, you have to specify the public IP information. If you have only one public IP address, select the “IP Address” item and fill in the IP address. If you have a range of public IP addresses, please select “IP Address Range” item and fill in the starting IP address and the ending IP address. *Be sure that you do not include the InstaGate WAN IP be between the start value and end value.* For example, if the InstaGate WAN IP is 210.66.39.99, you cannot insert start value to 210.66.39.98 and end value to 210.66.39.100.

Next, specify the private IP information. If there is only one private IP to specify, select the “IP Address” item and fill in the IP address. You may also specify a sub-network of IP addresses with the “IP Address/Netmask” option.

The “NAT rules” is a very useful function. You can use it to do “one-to-one NAT”, “many-to-one NAT” and “many-to-many NAT” functions. Figure 61 gives an example for adding a “one-to-one NAT” rule.

The screenshot displays the 'Add New NAT Rule' configuration page in the InstaGate 305 web interface. The breadcrumb trail is 'Main Menu > Advanced > NAT > Rules'. The page title is 'Add New NAT Rule'. The 'NAT Rule Settings' section is visible, showing the following configuration:

- Name:** one-to-one-NAT
- Public Network:**
 - IP Address
 - IP Address Range
- Private Network:**
 - IP Address
 - IP Address/Netmask

Additional settings include:

- Apply WAN Interface IP Address
- User
- Defined:** 210.66.39.97
- Private IP:** 192.168.2.200

Buttons for 'Add' and 'Return' are located at the bottom right of the configuration area.

Figure 61: Example of “one-to-one NAT”

In this example, we can see that all the packets with the source address of 192.168.2.200 will be translated to 210.66.39.97 then go to the Internet. Also, all the Internet traffic with destination address of 210.66.39.97 will be translated to 192.168.2.200 then go to the mapping local machine. The mapping is bi-directional.

Figure 62 gives an example for adding a “many-to-one NAT” rule.

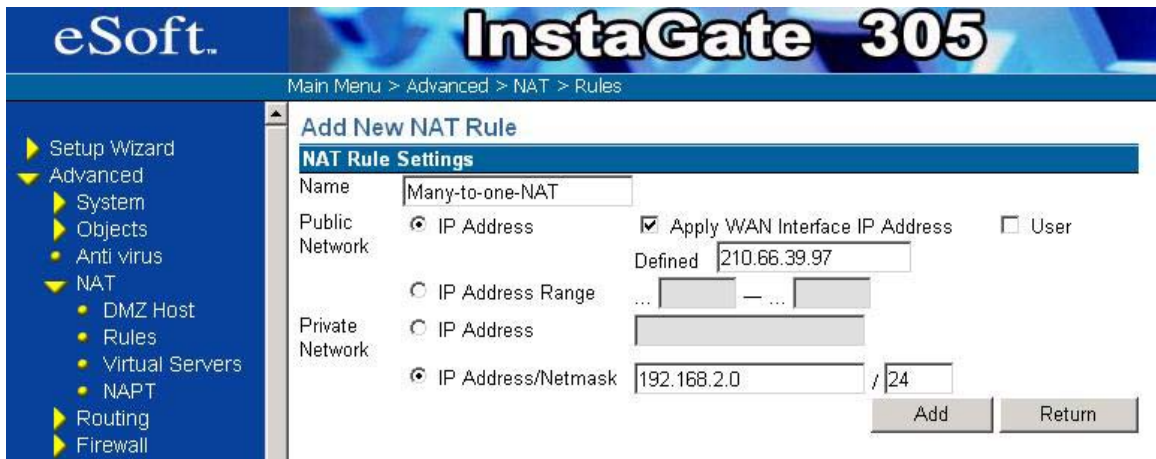


Figure 62: Example of “many-to-one NAT”

In this example, we can see that all the packets within the 192.168.2.0/24 will be translated to 210.66.39.97 then go to the Internet. The mapping is just for outgoing packets.

Figure 63 gives an example for adding “many-to-many NAT” rule.

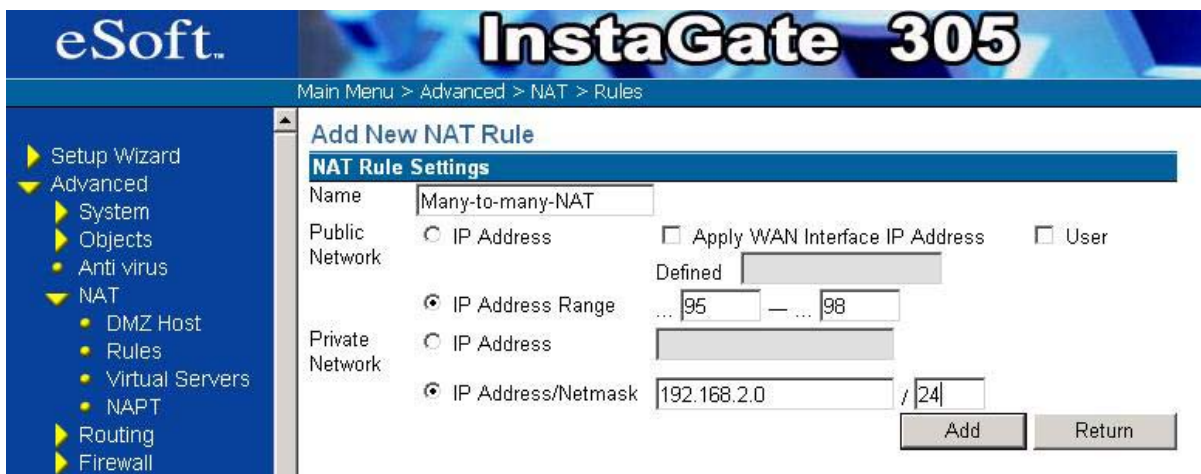


Figure 63: Example of “many-to-many NAT”

In this example, we see that all the packets within 192.168.2.0/24 will be translated to the IP range from 210.66.39.95 to 210.66.39.98 randomly then go to the Internet. The mapping is just for outgoing packets.

After you fill in the parameters of this rule and select the “Add” button, the new rule is added into the database and the rule list contains this record. Now, you may select the *active checkbox* of the NAT rule to activate the policy (see Figure 64).



Figure 64: NAT Rule List

7.2 DMZ Host

Under the “Main Menu > Advanced > NAT > DMZ Host page, you can expose one or more client PCs in your network to the Internet. It is often used for VoIP phones or online games that require unrestricted two-way communications.

As shown in Figure 65, there are one basic DMZ Host binding with WAN gateway IP and five advanced DMZ Hosts binding with others’ global IP. After you fill the IP address, you have to select the “Apply” button to save the setting. Also you must select the “Enable” button to start the mapping function.

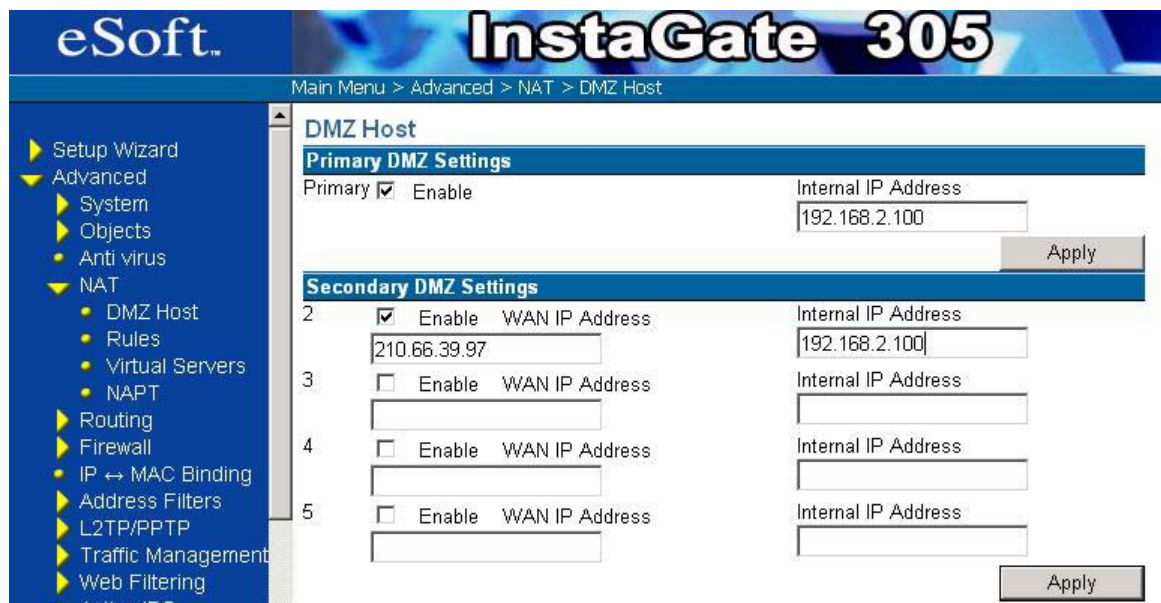


Figure 65: DMZ Host

How to use the “DMZ Host” function? Let’s see the following example.

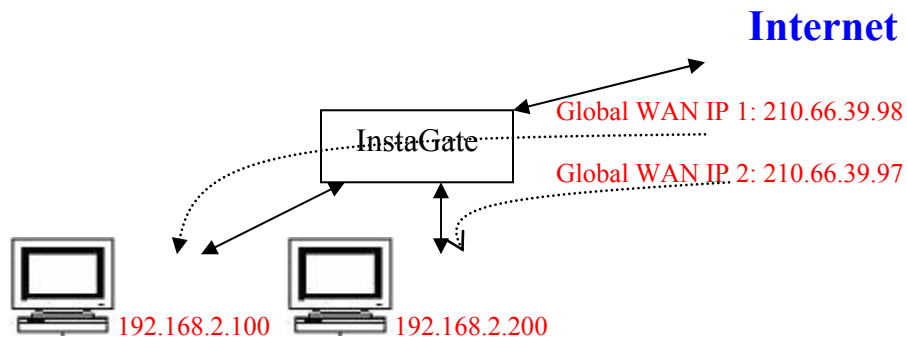


Figure 66: DMZ Host example

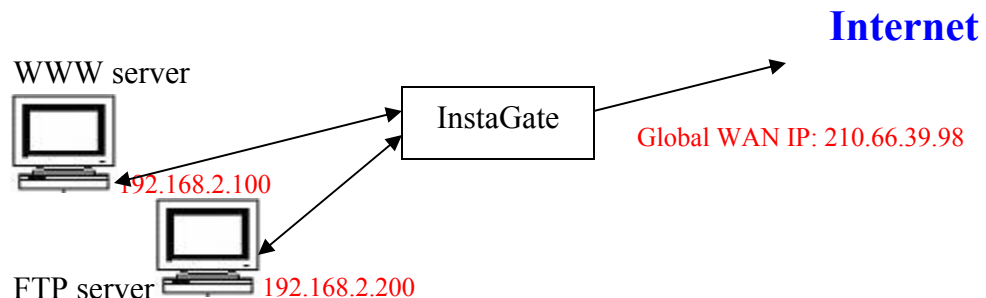
As shown in Figure 65 and Figure 66, the InstaGate’s default WAN IP is 210.66.39.98. We set a DMZ host (IP: 192.168.2.100) binding with 210.66.39.98. It means that any packet with a destination IP of 210.66.39.98 will be transferred to a PC whose IP is 192.168.2.100. In the same way, if we have an extra global IP (210.66.39.97), we can map a DMZ host (IP: 192.168.2.200) to this global IP. It means that any packet’s destination IP is 210.66.39.97 will be transferred to the PC whose IP is 192.168.2.200.

7.3 Virtual Server

The virtual server rule translates the incoming IP packet that has the specific protocol (TCP or UDP) and port number to the host in the local network. Although there are many servers (WWW server, FTP server, ...etc) in the local network, *a client in the Internet may access these servers by specifying the WAN IP address of the InstaGate with a different port number.*

Under the “Main Menu > Advanced > NAT > Virtual Server” page, you may define the virtual server rules. To add a new virtual server, please select the “Add” button. You have to specify the rule with a unique name. The protocol and the incoming port number fields specify the protocol and port number of the incoming IP packet. The internal virtual server IP and port fields specify the private IP address and the port number of the server.

Figure 67 gives an example for adding a “Virtual Server” rule.



eSoft™ InstaGate 305

Main Menu > Advanced > NAT > Virtual Servers

Setup Wizard
 Advanced
 System
 Objects
 Anti virus
 NAT
 DMZ Host
 Rules
 Virtual Servers
 NAT
 Routing
 Firewall

Add New Virtual Server

Virtual Server Settings

Name: WWW

Public IP Address: Apply WAN Interface IP Address
 User Defined

Public Protocol: TCP

Public Port Number: 80

Private IP Address: 192.168.2.100

Private Port Number: 80

Add Return

eSoft™ InstaGate 305

Main Menu > Advanced > NAT > Virtual Servers

Setup Wizard
 Advanced
 System
 Objects
 Anti virus
 NAT
 DMZ Host
 Rules
 Virtual Servers
 NAT
 Routing
 Firewall

Add New Virtual Server

Virtual Server Settings

Name: FTP

Public IP Address: Apply WAN Interface IP Address
 User Defined

Public Protocol: TCP

Public Port Number: 21

Private IP Address: 192.168.2.200

Private Port Number: 21

Add Return

Figure 67: Example of Virtual Server rule.

In this example, we see that all the Internet traffic with destination address of the InstaGate WAN IP to port 80 will be translated to 192.168.2.100 port 80. In the same way, all the Internet traffic with destination address of the InstaGate WAN IP to port 21 will be translated to 192.168.2.200 port 21.

After you fill the parameters of this rule and select the “Add” button, the new rule is added into the database and the rule list keeps this record (see Figure 68). Now, you may select the *active checkbox* of the virtual server rule to activate the policy.

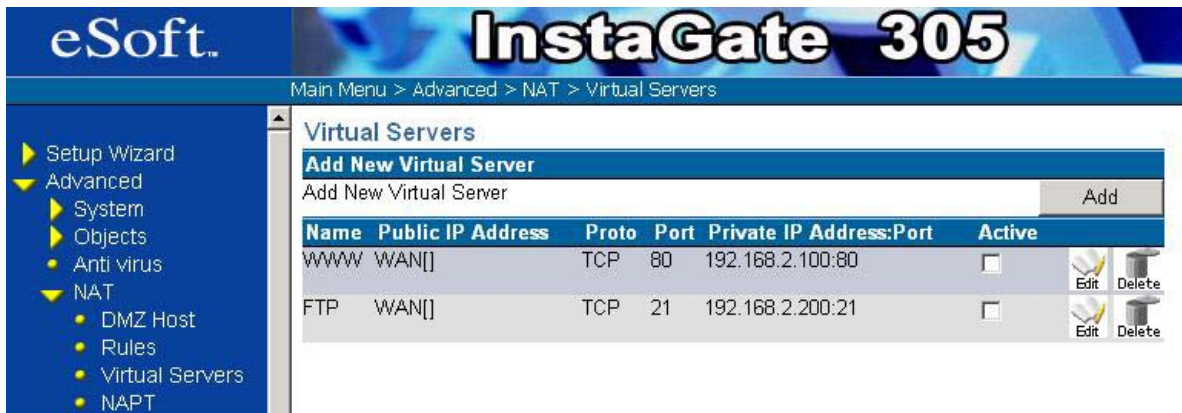


Figure 68: Virtual Server List

7.4 NAPT

If the number of available public IP addresses is outnumbered by the number of hosts in the local network, you have to specify the NAPT rule to let all hosts in the local network access Internet. The NAPT rules are only for applications that are based on TCP or UDP protocols.

Under the “Main Menu > Advanced > NAT > NAPT” page, you may define NAPT rules. To add a NAPT rule, please select the “Add ” button. After you select the “Add” button, a page shown as Figure 69 is displayed.

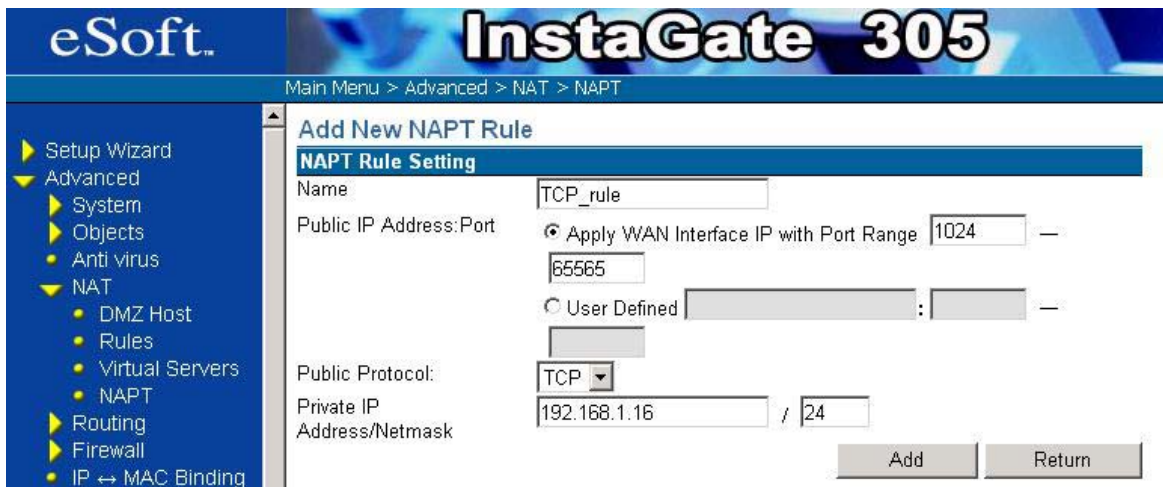


Figure 69: Add NAPT Rule

You have to specify the rule with a unique name. The private IP fields specify the hosts in the local network that will apply this rule. The public IP field specifies the public IP address. You can add the public IP address manually or the InstaGate may select the WAN interface IP if the option “Apply WAN Interface IP” is selected. The port range specifies the port range that the NAPT rule may use.

Each time a host in the local network matches this NAPT rule, a port number is used to identify this host. The protocol specifies the protocol (TCP or UDP) that this NAPT rule matches. After you fill the parameters of this rule and select the “Add” button, the new rule is added into the database and the rule list keeps this record. Now, you may select the *active checkbox* of the NAPT rule to activate the policy.

8 Routing

8.1 Static Routing

You may configure the routing information under the “Main Menu > Advanced > Routing > Static Routes” page. Initially, the InstaGate only learns the routing information from the interface. Static routing tells the InstaGate routing information it cannot learn automatically.

To add a routing entry, you have to fill in the fields in Figure 70. The *destination* field specifies the IP network address at the final destination. The *netmask* field specifies the subnet mask of the destination. If you want to specify a single host, the subnet mask should be 255.255.255.255. The *gateway* field is the immediate neighbor that the InstaGate will forward the packets to as the destination. The *metric* field specifies the cost of transmission for the routing process. The *interface* field specifies the outgoing interface of the packets.

Figure 70: Adding routing entry

After specifying all this fields, please select the “Add” button to add the routing entry. To delete a route, you only have to select the “Delete” button of the corresponding routing entry in the static routing table as shown below.

Destination Network	Netmask	Gateway IP Address	Metric	Interface
192.168.3.0	255.255.255.0	*	0	DMZ
192.168.8.0	255.255.255.0	*	0	LAN
210.66.39.0	255.255.255.0	*	0	WAN

Figure 71: Static Routes

8.2 RIP

If your network routes via RIP, you could turn on the InstaGate's "RIP" functions to communicate with other RIP devices automatically (see Figure 72).



Figure 72: RIP Information Management window

You can configure the InstaGate's RIP functions under the "Main Menu > Advanced > Routing > RIP" page. In the page, the InstaGate provides the "Routing Table" button at the right-top for your reference. You could check your current routing table status by select the button any time if you wish. The routing table looks like Figure 73. Before you enable the RIP functions, you should define some parameters in the RIP Information Management page. First, you should select the RIP protocol version: RIP v1 or RIP v2. If you don't know what version protocol under your network, please check your administrator. We suggest you to select "RIP v2" (default setting) if you are still not clear what version you have. Then, assign the "RIP update time" – it will send out the system RIP information to the other devices cyclically through the interfaces that you select.

Routing Table				
Destination Network	Netmask	Gateway IP Address	Metric	Interfaces
192.168.3.0	255.255.255.0	*	0	DMZ
192.168.8.0	255.255.255.0	*	0	LAN
210.66.39.0	255.255.255.0	*	0	WAN

Refresh

Figure 73: The Routing Table list

In the Interface section, it will show all interfaces that the device connected, including WAN, LAN, DMZ and current settings.

You should select the “Edit” button from the interface that you want to enter as an edit screen, as shown in Figure 74. The Interface Name, IP, and Mask fields are not editable, hence are in a gray background. You need to configure the “Send”, “Receive”, and “Authentication” fields.

InterfaceName:	WAN
IP:	192.168.1.115
Mask:	255.255.255.0
Send	RIPv2 Broadcast
Receive	RIPv1 & RIPv2
Authentication	<input checked="" type="radio"/> NO <input type="radio"/> YES

Figure 74: The interface edit window

By clicking the pull-down menu of the “Send” field, you see all of the options. Please refer to Figure 75 and select what you want.

Figure 75: The options of the “send” action.

Option	Description
RIPv2 Broadcast	The update information will be sent with RIPv2 broadcast format.
RIPv1 Broadcast	The update information will be sent with RIPv1 broadcast format.
Do Not Send	The Interface will not send any of the RIP update information to the other devices.

Table 3: RIP Sending Options

By clicking the pull bar of the “Receive” field, you could see all the options. Please refer to Figure 76 and select what you want.

Figure 76: The options of the “receive” action

Option	Description
RIPv1 & RIPv2	The interface could receive the update information with RIP v2 and v1 format.
RIPv2	The interface only receives the RIP v2 update information format.
RIPv1	The interface only receives the RIP v1 update information format.
Do Not Receive	The interface won't receive any of RIP update information packets.

Table 4: RIP Receiving Options

For “Authentication”, if you select “Yes”, you have to fill the authentication string in the field. All of the devices in the domain of the interface should be configured as a same authentication value otherwise it will fail to access.

After completing the configuration, select the “Modify” button to store the modification and go back to the RIP Information Management window, or select “Return” to disregard all the changes and go back to the RIP Information Management window. Now, you should select the interfaces that you want run the RIP protocols on by clicking the “Active” check box. Finally, you should turn on the RIP protocol for the system by clicking the “Enable RIP” check box.

9 Firewalls

The major function of a firewall is to inspect the traffic passing from one interface to another (LAN/WAN/DMZ), and to decide which traffic should be allowed to pass and which should be dropped. The firewall makes separate decisions for both inbound and outbound traffic. For example, in the WAN interface, there are two directions. One is from the Internet to the Enterprise, and the other is from the enterprise to the Internet. Thus, the administrator of the InstaGate must specify the direction when setting a firewall policy. Figure 77 shows an example to illustrate the concept and the functions of a Firewall.

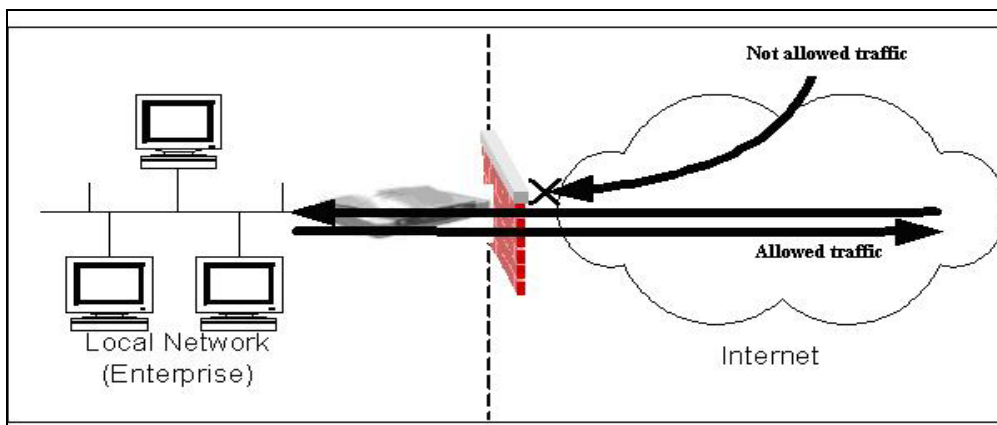


Figure 77: An illustration of the functions of a Firewall

9.1 Firewall Policies

Figure 78: Firewall Management Configuration

Under the “Main Menu > Advanced > Firewall” page, all the firewall rules that exist in the InstaGate are listed. For example, in Figure 78, there are two firewall rules in the device.

In the Figure, you can find that a firewall policy consists of the following parameters:

Field	Description
#	Denotes the policy number of the policy. Each policy will have a unique policy number.
Name	This is an identifier of the policy. Administrator can have a meaningful name for easy management.
Source	Denotes the source IP condition of the rule.
Destination	Denotes the destination IP condition of the rule.
Direction	Denotes the traffic direction applied on in the firewall rule. There are six “direction” options in the InstaGate: WAN-to-LAN, LAN-to-WAN, WAN-to-DMZ, DMZ-to-WAN, LAN-to-DMZ, DMZ-to-LAN.
Services	Denotes service conditions of the rule. There are some predefined

	services in this InstaGate (refer to 6.3 - Defining Service Object). The administrator can also define a new service. When moving the mouse to the service indication icon, it will show all the services applied in the firewall rules on the screen.
Schedule	Denotes the Policy Activation time period. Activation of the policy with respect to the time specified in the Schedule depends on the Active parameter value.
Action	Denotes the action of the rule. The three actions can be taken for a firewall policy are ACCEPT , DROP , and REJECT . ACCEPT : accept packets and allow carrying out any further processing. DROP : drops packets and refuse carrying out any further processing. REJECT : works basically the same way as the DROP action, but in addition it sends back an error message to the host sending the packets that have been blocked. Note: Comparing to DROP action, REJECT action may be considered as wasting time and bandwidth. The right choice depends on whether to know where the blocked packets from is important.
Log	Denotes whether the matched packet information is stored in the system log. If its value is yes then you can find the matched packet information in the system log otherwise the system does not log the information
Active	Denotes the status of the policy. When the check box is selected, it represents that the firewall rule is provisioned in the InstaGate. The administrator can easily select the check box to turn on or off the policy.
Policy Status	Denotes the current status of the policies. Three status levels can be taken for the policy: Running, Waiting and Stop. But the status depends on the Schedule and Active parameter values. The status of the policy is "Running" during the time period specified in the Schedule parameter otherwise "Waiting" if the time period elapses. The status of the policy is "Stop" only if the Active parameter is unset.
Configure	The configuration option can be applied to the firewall rule. The three configuration actions are: EDIT , DELETE , and MOVE .

Table 5: Firewall Parameters

9.1.1 Adding a new firewall policy

In a typical deployment, it will be necessary to add custom firewall rules above and beyond ‘factory default’. Since the firewall enforces rules sequentially, it is important to have a well designed set of policies... both for performance, and for security. When designing policies, it is best to start with the most specific (restrictive) rules first. This allows the firewall to stop a packet before it exercised the complete policy table, greatly enhancing system performance. The InstaGate provides an intuitive, easy-to-use configuration tool for adding and editing firewall policies.

9.1.1.1 Adding a policy

The InstaGate has a user friendly interface with all of configuration shown on the same page. The administrator can easily follow the configuration table to complete the policy rule definition and select the “Apply” to save it. The unique policy name helps the administrator to identify the policy.

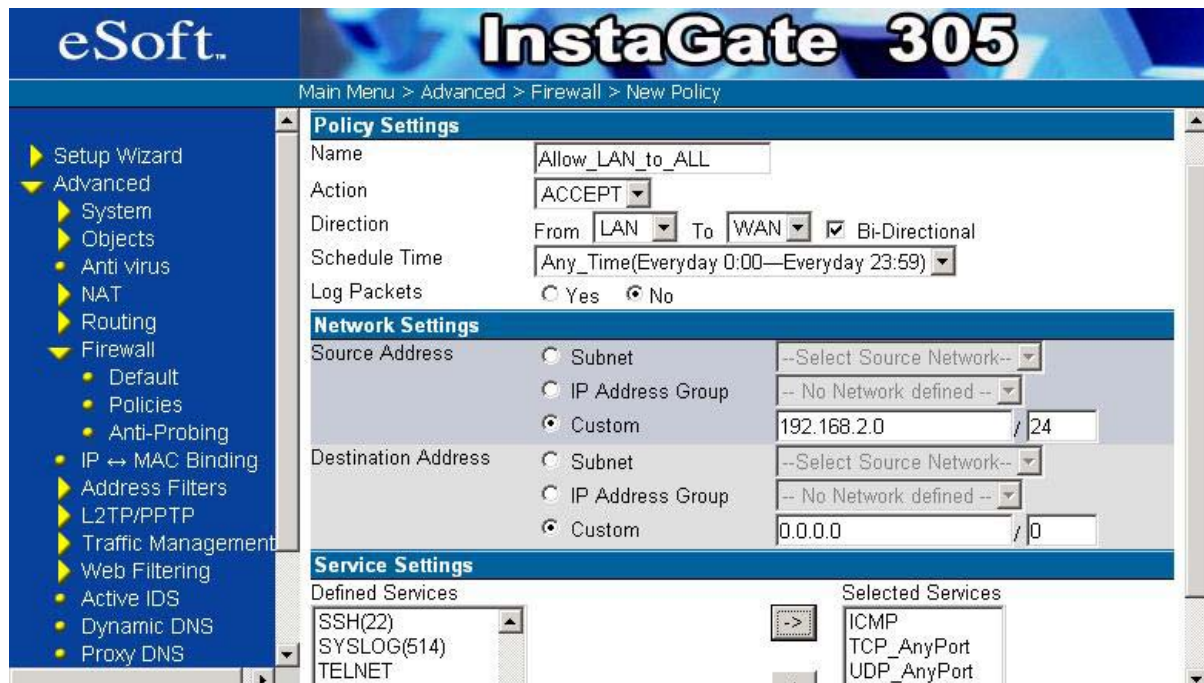


Figure 79: Add a Firewall Rule

The source address is to restrict the source of a packet. You may fill in the source address in the CIDR format, or select the subnet object from the pull down menu. The destination address is to restrict the destination of a packet. You may fill the destination address in the CIDR format, or select the subnet object from the pull down menu. Please refer to section 6.1 for defining a Subnet Object.

You may restrict the traffic directions in a firewall rule. The InstaGate has three interfaces. Therefore, in total, there are six different directions of traffic flow: WAN to LAN, WAN to DMZ, LAN to WAN, LAN to DMZ, DMZ to WAN and DMZ to LAN. If

the traffic is bi-directional, instead of setting two rules, you only have to select the “Apply to bi-directional” checkbox.

The InstaGate provides “Deep Packet Inspection” technology. There are six default services: DNS, FTP, HTTP, SSL/TLS (HTTPS), TELNET and ICMP. You may also define your service object and select multiple services in a single firewall rule.

To select the services, you only have to select the services in the left selection area and move the selected services to the right selection area.

The InstaGate provides a Time schedule in order to activate the firewall policy. You may select the time schedule from the drop down “Time schedule” option.

The InstaGate provides a way to store the matched packet information in the system log. You can select the “Yes” option of “Need log the matched pattern” to store the matched packet information in the system log and “No” otherwise.

There are three different actions for the firewall in the InstaGate. These are ACCEPT, DROP and REJECT.

- **ACCEPT:** Accept and forward the packet if the packet matches the policy condition.
- **DROP:** Drop the packet if the packet matches the policy condition.
- **REJECT:** Drop the packet and feedback an ICMP message if the packet matches the policy condition.

To define the firewall action, you only have to select the action from the pull down menu.

After you set all fields discussed above, please select the “Apply” button to add the policy. To delete existing firewall rule, you only have to select the “Delete” icon of the corresponding rule. You may also modify the firewall rule by select the “Edit” icon.

The order of the firewall rules is very important. The InstaGate provides a very easy management interface for adjusting the order of rules. After you select the “Move” icon of the rule that you want to move, the page of Figure 80 appears. All you have to do is clicking one of “Move” icons. The selected rule will move to the location that you select.

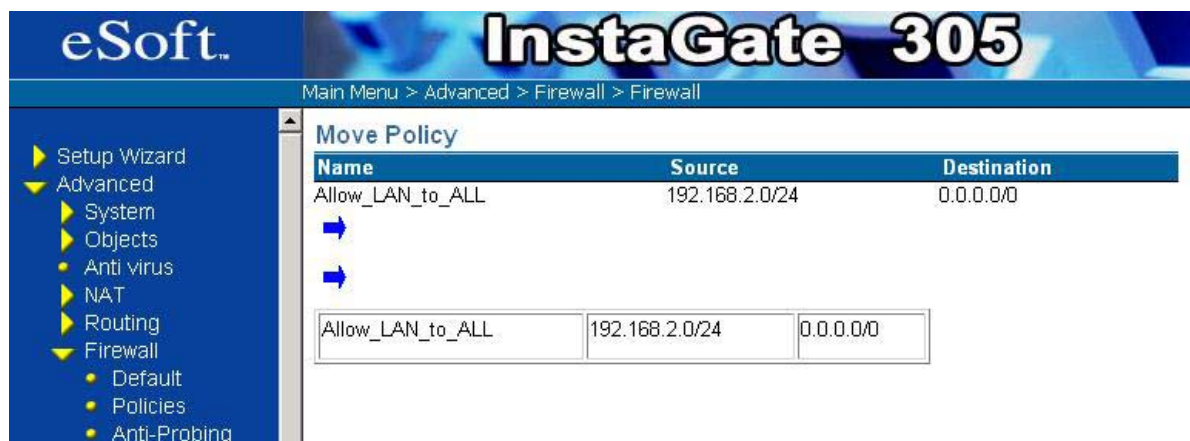
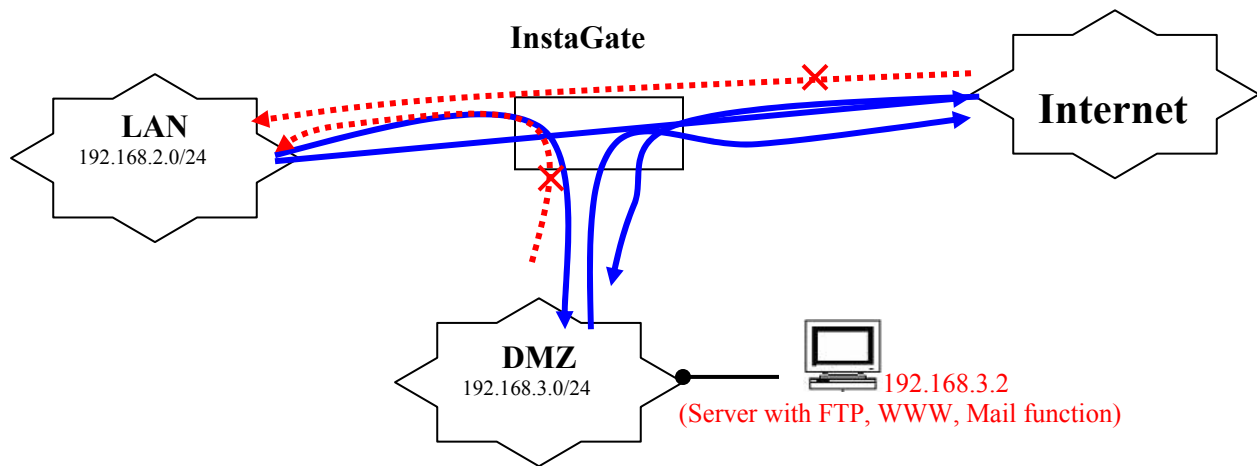


Figure 80: Move the policy

Figure 81 shows a basic example to manage the configuration of the firewall policies.



Solid Line: Permit connection. (Accept action).

Dotted Line: Deny connection. (Drop action).

Figure 81: Test environment for testing firewall policy

Assumptions:

1. Any hosts in LAN can access DMZ zone and WAN zone with ICMP and all TCP and all UDP ports.
2. Any hosts in DMZ can access WAN zone with DNS, FTP, HTTP, POP3, SMTP and TELNET functions, but can't access LAN zone.
3. Any hosts in WAN can access DMZ zone with DNS, FTP, HTTP, POP3, SMTP and TELNET functions, but can't access LAN zone.
4. Select "Enable Default NAT Policies" for default firewall policy (see to).
5. InstaGate's public WAN gateway IP is **210.66.39.99**, LAN gateway IP is **192.168.2.1**, DMZ gateway IP is **192.168.3.1**.
6. The subnet "0.0.0.0/0" represents "ALL Network".

NAT Setting:

1. Use NAT from LAN to WAN, please enable "Enabled Default NAT Policies". (Refer to 5.3.2 LAN Interface).

LAN Interface

IP Address / Mask: 192.168.2.1 / 255.255.255.0

Enable DHCP Server

Enable Default NAT Policies

Disable Private Interface Ping (LAN & DMZ)

Figure 82: Default NAT Policies

2. There is one public IP (210.66.39.98) mapped to a server (192.168.3.2) in DMZ zone. The others (192.168.3.0/24) are mapped to 210.66.39.99.

Main Menu > Advance > NAT > Pooled

NAT Rules

Name	Public IP	Private IP	Active	Configure
server1_in_DMZ	210.66.39.98	192.168.3.2	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
All_Host_in_DMZ	210.66.39.99	192.168.3.0/24	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Figure 83: NAT Rules

Note: It is necessary to follow the top-down sequences.

Firewall Setting:

1. Any hosts in LAN can access DMZ zone and WAN zone with ICMP and all TCP and all UDP ports.



Figure 84: New Firewall Policy

2. Any hosts in DMZ can access WAN zone with DNS, FTP, HTTP, HTTPS, POP3, SMTP, TELNET functions, but can't access LAN zone.



Figure 85: New Firewall Policy

3. Firewall policy table shows as follows:



Figure 86: Firewall Policies

9.2 Address Filters

9.2.1 MAC Filtering

The InstaGate provides a method to restrict unauthorized stations from accessing the network. This provides an additional control layer in which only the stations with registered MAC addresses can have access to the network. This approach requires the MAC addresses to be configured. Under the "Main Menu > Advanced > Firewall > Address Filters > MAC" page, an administrator can allow or block nodes from the network address depending upon the Filter Action selected. Filter Action is set according to the option being selected in Firewall Management page.

Only the MAC addresses present in the MAC table are allowed to access the Network (whereas all other stations are denied).

You need to specify the MAC address and then select the "ADD" button. Thus according to the Filter Action setting, an appropriate action is taken for the MAC addresses present in the MAC Filter Table.

- Here the Filter Action "Deny the following MAC Address" is selected, meaning that it will block all traffic originating from the node with MAC address 00:00:00:00:00:01. All other traffic will be permitted



Figure 87: New MAC Filter

2. Here you can see the MAC address in the MAC Filter Table. By clicking the “Delete” button you can easily delete that particular MAC address field from the table.



Figure 88: MAC Filter List

9.2.2 IP Filtering

The InstaGate provides an easy method to restrict unauthorized stations from accessing the network. This provides an additional control layer in which only the stations with registered IP addresses can have access to the network. This approach requires the IP addresses to be configured. Under the "Main Menu > Advanced > Firewall > Address Filters > IP Address" page, user can allow the station from the network address.

Only the IP addresses present in the IP table are allowed to access the Network. All other stations are denied.

1. Here the filter action “Permit the Following IP Address” is set. The administrator needs to fill in the IP address, and select the “Add” button so that appropriate action is taken.



Figure 89: New IP Address Filter

2. Here you can see the IP address in the IP Filter Table. By clicking the “Delete” button you can easily delete that particular IP address field from the table



Figure 90: IP Address Filter List

10 Virtual Private Network

10.1 IPSec VPN

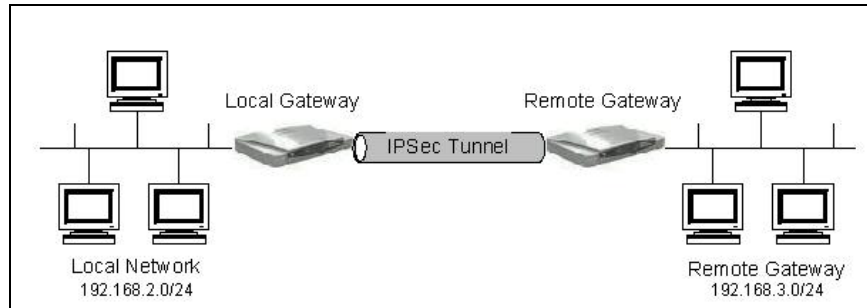


Figure 91: IPSec VPN

The concept of the VPN (Virtual Private Network) is to build a ‘secure’ virtual network over the ‘insecure’ public Internet. An IPSec VPN guarantees that all hosts in this virtual network have secure communications over the Internet as if they were behind a firewall in the same LAN. The secure communication is established by building secure tunnels. To establish a secure tunnel in the Internet, two security appliances have to work together. One appliance encrypts the data and the other decrypts the encrypted data (and vice-versa). As shown in Figure 91, these two security appliances are referred as the *local gateway* and the *remote gateway*. The local network is a subnet that connects the local gateway and the remote network is a subnet that connects the remote gateway.

A secure tunnel is established by choosing a suitable security algorithm. There are two protocols, the *authentication header* (AH) protocol (RFC 2402) and the *encapsulating security payload* (ESP) protocol (RFC 2406). The AH protocol is designed for data integrity, authentication, sequence integrity and non-repudiation, where the ESP protocol is designed for data encryption and all services offered by AH.

Currently, the InstaGate supports *HMAC-MD5* and *HMAC-SHA1* hash algorithm for authentication.

It also supports *3DES-CBC* and *AES* algorithms for encryption.

The InstaGate supports both manual key and automatic key management. Automatic key management is done by Internet key exchange (IKE) protocol. Using IKE, the encryption keys are automatically negotiated by two security appliances.

10.1.1 Automatic Key Exchange (IKE)

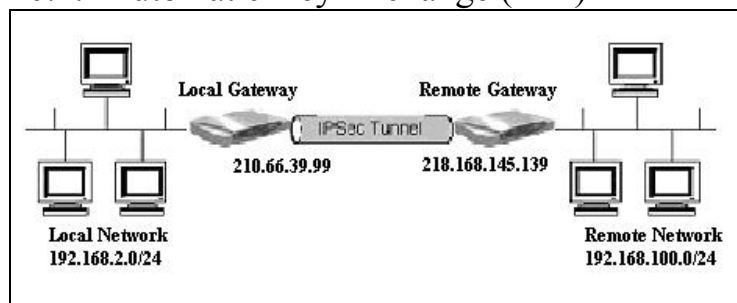


Figure 92: Automatic Key Example

The InstaGate supports RFC 2049 Internet key exchange protocol (IKE). Using IKE, encryption keys are automatically negotiated and selected by two connected security appliances. This provides the easiest and most efficient way to manage keys for your security appliance.

To setup an IPsec VPN, you have to configure the following parameters: 1) private network definition; 2) the IPsec tunnel end points; 3) IKE proposal; 4) IPsec proposal. In the next sub-section, we discuss how to setup an automatic key IPsec tunnel using the example in Figure 92.

10.1.1.1 Private Network Definition

To add a new automatic key policy, please select the “Add” button under the “Main Menu > Advanced > VPN > Automatic Key VPN” page.

First, you need to give this policy a name. An automatic key policy concerns two security appliances. The security appliance connecting the management station is the *local gateway*. The subnet connected to the local gateway is the *local network*.

Main Menu > Advanced > VPN > Automatic Key (IKE)

New Automatic Key (IKE) Policy

Automatic Key (IKE) Settings

Name	New_AutoKey	
Local Gateway	<input checked="" type="radio"/> Custom <input type="radio"/> Gateway	210.66.39.99
Local Network	<input checked="" type="radio"/> Custom <input type="radio"/> Subnet	192.168.2.0 /24
Remote Gateway	<input checked="" type="radio"/> Custom <input type="radio"/> Gateway	210.168.145.139
Remote Network	<input checked="" type="radio"/> Custom <input type="radio"/> Subnet	192.168.100.0 /24
Key Management Settings	<input checked="" type="radio"/> Preshared Key <input type="radio"/> RSA	Confirm
IKE Proposal	High Security(AES 256-bit Enc, SHA-1 Auth)	
IPSec Proposal	High Security(AES 256-bit Enc, SHA-1 Auth)	

Perfect Forward Secrecy

IKE SA Lifetime: 8 Hour(s)

IPSec SA Lifetime: 1 Hour(s)

Add Return

Figure 93: New automatic key policy

Referring to Figure 92, the virtual private network that we want to define is from subnet 192.168.2.0/24 to subnet 192.168.100.0/24. As it is shown in Figure 93, the local network field is 192.168.2.0/24 and the remote network is 192.168.100.0/24. If you've already defined the corresponding subnet objects, you may also select the local and/or remote network by selecting the subnet object from the pull-down menu. To define subnet objects, please refer to 6.1.

10.1.1.2 The IPSec Tunnel End Points

As shown in Figure 92, an IPSec tunnel consists of two end points. Their IPs are 210.66.39.99 and 218.168.145.139. Before you create the automatic key policy, you must define two gateway objects that consist of these two IPs respectively. (To define a gateway object, please refer to section 6.3.) To define the IPSec tunnel end point, you only have to select the local gateway object and the remote gateway object from the pull-down menu (see Figure 94).

Figure 94: Select the gateway object for automatic key policy

10.1.1.3 IKE Proposal

The IKE proposal consists of 1) authentication method for security appliances; 2) encryption algorithm; 3) authentication algorithm; 4) Diffie-Hellman group; 5) IKE security association (SA) lifetime time. To configure the InstaGate, you only have to set the authentication method and the IKE SA lifetime. The InstaGate configures all other parameters automatically.

The “authentication method” refers to the method of authenticating the security appliances at both ends of the security tunnel. The InstaGate provides two different authentication methods: digital signatures and pre-shared key authentication. If you want to use the pre-shared key authentication method, select “Preshared Key”. The maximum length of the key is 20 characters (see Figure 95). It is very important that both security appliances at the ends of the security tunnel have the same authentication method selected.

Figure 95: Define authentication method for automatic key policy

The InstaGate also provides the RSA digital signature algorithm and DSS signatures. It is very important if you want to use digital signatures for authentication to have a RSA certificate if using the RSA algorithm, and a DSA certificate if using the DSS algorithm. Refer 6.6 to generate RSA and DSS certificates.

To define the IKE SA lifetime, fill in the time to the IKE SA lifetime field (see Figure 96).

Figure 96: IKE SA lifetime

The InstaGate processes all other parameters automatically. Here, the parameters with the higher security level will be chosen first. Therefore, DH group 2 will be chosen before DH group 1; AES will be chosen before 3DES and SHA-1 will be chosen before MD5.

10.1.1.4 IPSec Proposal

The IPSec proposal consists of 1) active protocols AH or ESP; 2) Perfect Forward Secrecy (PFS); 3) IPSec security association (SA) lifetime time. You only have to configure the active protocol, PFS and the IPSec SA lifetime (see Figure 97). The InstaGate configures all other parameters automatically.

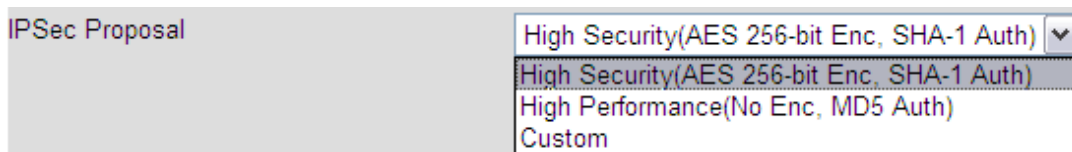


Figure 97: IPSec Proposal

To define the IPSec SA lifetime, fill in the time in the IPSec SA lifetime field (see Figure 98).

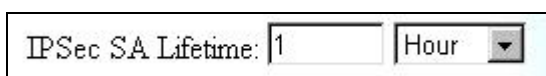


Figure 98: IPSec SA lifetime

For the ESP protocol, you have to specify whether you want to use authentication or encryption. The algorithms HMAC-SHA1 and HMAC-MD5 are both acceptable, although the InstaGate prefers the HMAC-SHA1 algorithm. If you select to use encryption, the algorithms AES and 3DES-CBC are both acceptable, however the InstaGate prefers the AES algorithm.

If you select “Perfect Forward Secrecy”, the IKE will randomly re-generate the secret when it negotiates a new key; otherwise, IKE will re-generate the secret based on the previous secret.

10.1.2 IKE Example

Figure 99 is an automatic key policy example for the network configuration in Figure 92. The local network and remote network are 192.168.2.0/24 and 192.168.100.0/24 respectively. The authentication method is a pre-shared key; ESP authentication, ESP encryption and PFS are enabled for an IPSec proposal. The IKE SA lifetime and the IPSec SA lifetime are 8 hours and 1 hour respectively.

After you fill in all these parameters, select the “Add” button to add this automatic key policy to the database. This policy will appear in the automatic key policy list (see Figure 100). Now you may select the “Active” checkbox in this policy list to activate the policy.

Main Menu > Advanced > VPN > Automatic Key (IKE)

New Automatic Key (IKE) Policy

Automatic Key (IKE) Settings

Name:

Local Gateway: Custom

Local Network: Custom /

Remote Gateway: Custom

Remote Network: Custom /

Key Management Settings: Preshared Key

 RSA

IKE Proposal:

IPSec Proposal:

Perfect Forward Secrecy

IKE SA Lifetime:

IPSec SA Lifetime:

Figure 99: Automatic Key Policy Example

Main Menu > Advanced > VPN > Automatic Key (IKE)

Automatic Key (IKE) VPNs

Add A New AutoKey VPN

Add A New AutoKey VPN

Name	Local Network	Remote Network	Local Gateway	Remote Gateway	Description	Active
New_AutoKey	192.168.2.0/24	192.168.100.0/24	210.66.39.99	210.168.145.139	PSK PFS	<input type="checkbox"/>

Figure 100: Automatic key Policy List

10.1.3 Manual Key

When using IKE, encryption and authentication keys are automatically negotiated and selected by the security appliances. However, sometimes you may want to configure the security information yourself. In that case you could use manual key method to setup your IPsec VPN.

To setup a manual key IPsec virtual private network, you have to configure the following parameters: 1) private network definition; 2) the IPsec tunnel end points; 3) IPsec Security Association. In the following of this sub-section, we discuss how to setup a manual key IPsec tunnel by the example in Figure 92.

To add a new manual key policy, select the “New Manual Key Object” button under the “Main Menu > Advanced > VPN > Manual Key” page.

10.1.3.1 Private Network Definition

Please refer to 10.1.1.1.

10.1.3.2 The IPsec Tunnel End Point

Please refer to 10.1.1.2.

10.1.3.3 IPSec Security Association

The IPSec security association consists of 1) active protocols AH and/or ESP; 2) security parameter index (SPI) pair: Local SPI and Peer SPI; 3) authentication and/or encryption algorithm; 4) authentication and/or encryption keys. You must configure all parameters manually.

You should first select an active protocol by checking the AH or ESP checkbox. After selecting an active protocol, only the parameters related to the active protocol would be enabled.

Then you need to specify the SPI pair. The SPI field is the hex value of SPI and must be greater than 255. It must also be unique in your manual key system. The SPI pair must be symmetrical to the other tunnel end point, this means your local SPI is equal to the other tunnel end point's peer SPI and your peer SPI is equal to the other tunnel end point's local SPI.

If you select the AH protocol, you choose the authentication algorithm (currently, this device supports MD5 and SHA-1). If you select the ESP protocol, you could choose the authentication algorithm (currently, this device supports MD5 and SHA-1) or the encryption algorithm (currently, this device supports AES, DES and 3DES).

The authentication key length is different from the authentication algorithm. MD5 needs a **16** byte key and SHA-1 needs a **20** byte key. For MD5 you should type in a **32** hex value and for SHA-1 you should type in a **40** hex value.

The encryption key length is also different from encryption algorithm. DES needs an **8** byte key and 3DES needs a **24** byte key. For DES you should type in a **16** hex value and for 3DES you should type in a **48** hex value.

Example

Figure 101 is a manual key policy example of the Local Gateway and Figure 101 is the symmetrical manual key policy example of the Remote Gateway for the network configuration in Figure 92.

The policy name is "Manualkey_example". The local network and remote network are 192.168.2.0/24 and 192.168.100.0/24 respectively. The active protocol is ESP; authentication algorithm is SHA-1 and encryption algorithm is 3DES.

After you fill all the parameters, select the "Add" button to add this manual key policy to the database. This policy will appear in the manual key policy list. Now, you may select the *active* checkbox in this policy list to activate the policy.

Main Menu > Advanced > VPN > Manual Key

Add A New Manual Key VPN

Manual Key VPN Settings

Name	Manualkey_example	
Local Gateway IP Address	210.66.39.99	
Local Network	<input type="radio"/> Custom <input type="text"/> / <input type="text"/> <input checked="" type="radio"/> Subnet LAN[192.168.2.0/24]	
Remote Gateway IP	218.168.145.139	
Remote Network	<input checked="" type="radio"/> Custom 192.168.100.0 / 24 <input type="radio"/> Subnet --Select Source Network--	
<input type="checkbox"/> Authentication Header (AH)		
Local SPI	0x <input type="text"/>	(0x100~0xff)
Peer SPI	0x <input type="text"/>	(0x100~0xff)
Algorithm	SHA-1	
Authentication Key	0x <input type="text"/>	
<input checked="" type="checkbox"/> Encapsulating Security Payload (ESP)		
Local SPI	0x <input type="text"/>	(0x100~0xff)
Peer SPI	0x <input type="text"/>	(0x100~0xff)
Authentication Algorithm	SHA-1	
Authentication Key	0x 12345678901234567890	
Encryption Algorithm	3DES	
Encryption Key	0x 12345678901234567890	

Figure 101: New Manual Key Policy for Local Gateway

10.2 L2TP/PPTP VPN

The remote access VPN is typically used between corporations to remote VPN clients (such as mobile workers, telecommuters, or home computers). The remote users use the dial-up or dynamic address accessing the VPN server (such as this InstaGate), entering the corporation's network, getting the supplied services (such as e-mail, shared files, or shared printer).

It looks like the remote users logically connect to the corporation's local network to get the network service (see Figure 102). A remote access VPN enables corporations to reduce communications expenses by leveraging the local dial-up infrastructures of Internet Service Providers and to take advantages of broadband connectivity.

The InstaGate supports two types of remote access: Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP).

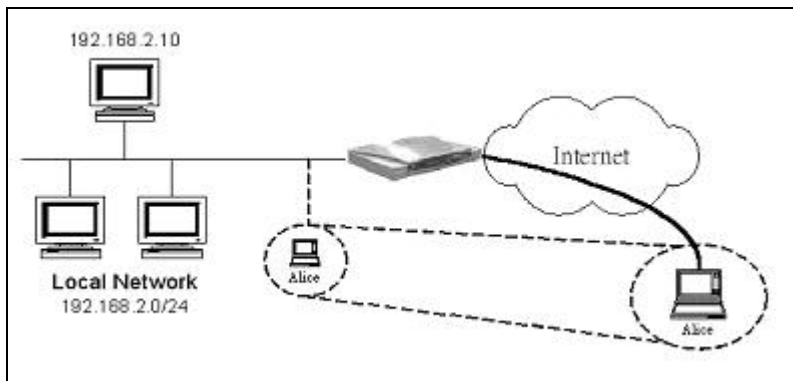


Figure 102: Remote access VPN

10.2.1 L2TP Server



Figure 103: L2TP Configuration

As shown in Figure 103, to setup a L2TP virtual private network, under “Main Menu > Advanced > VPN > L2TP/PPTP > L2TP Server”, you have to define the L2TP Server Name that is the name of the LNS.

Then you choose the Authentication Method used by PPP (CHAP, PAP or both). After you specify the local network IP address range, IPs are dynamically assigned to clients that attempt to access the LAN remotely (the assigned IP address range must be in the LAN interface domain). You must select the “Apply” button to affect the settings.

After the configuration is done, select the “Enable L2TP Server” checkbox to enable L2TP service and setup for remote access user accounts (see section 10.2.4). If you want to assign a static IP address for some remote access users, refer to section for more detailed information.

10.2.2 PPTP Server

To setup a PPTP virtual private network, like L2TP, under “Main Menu > Advanced > VPN > L2TP/PPTP > PPTP Configuration”, you define the Authentication Method used by PPP (CHAP or PAP), and specify the local network IP address range dynamically assigned to clients that attempt to remotely access the network. The assigned IP address range must be in the LAN interface domain. You must select the “Apply” button to affect the settings.

After the configuration is done, select the “Enable PPTP Server” checkbox to enable the PPTP service (see Figure 104) and setup the remote access user accounts (see section 10.2.4). If you want to assign a static IP address for some remote access users, refer to section 10.2.4 for more detailed information.

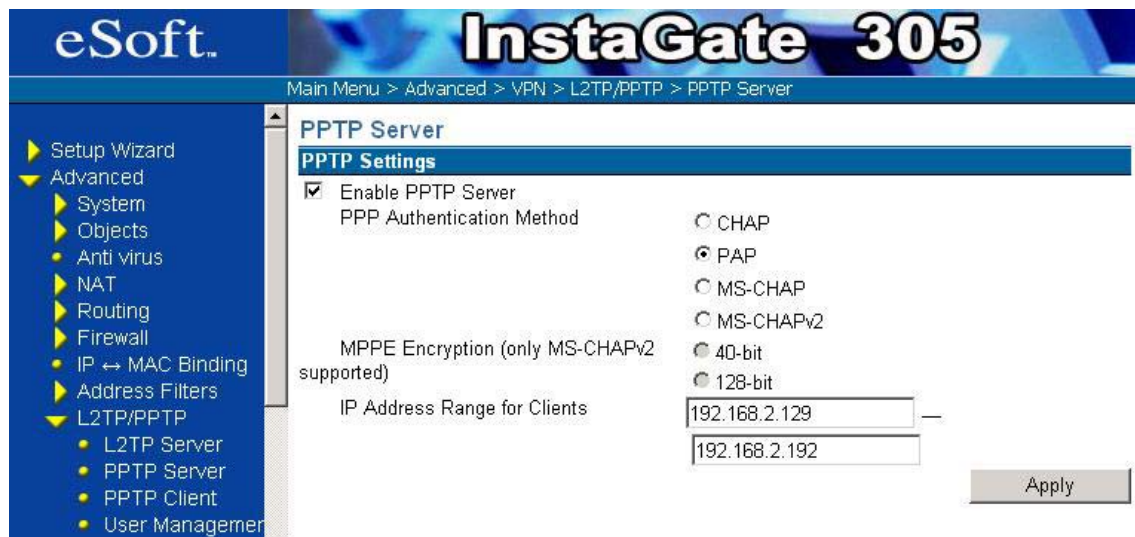


Figure 104: PPTP Configuration

10.2.3 PPTP Client

As shown in Figure 105, the InstaGate supports one PPTP client function. If you would like to access the private data at your office from your house, it is very convenient for you to use the PPTP client that creates a secure tunnel between your local InstaGate and the remote PPTP server.

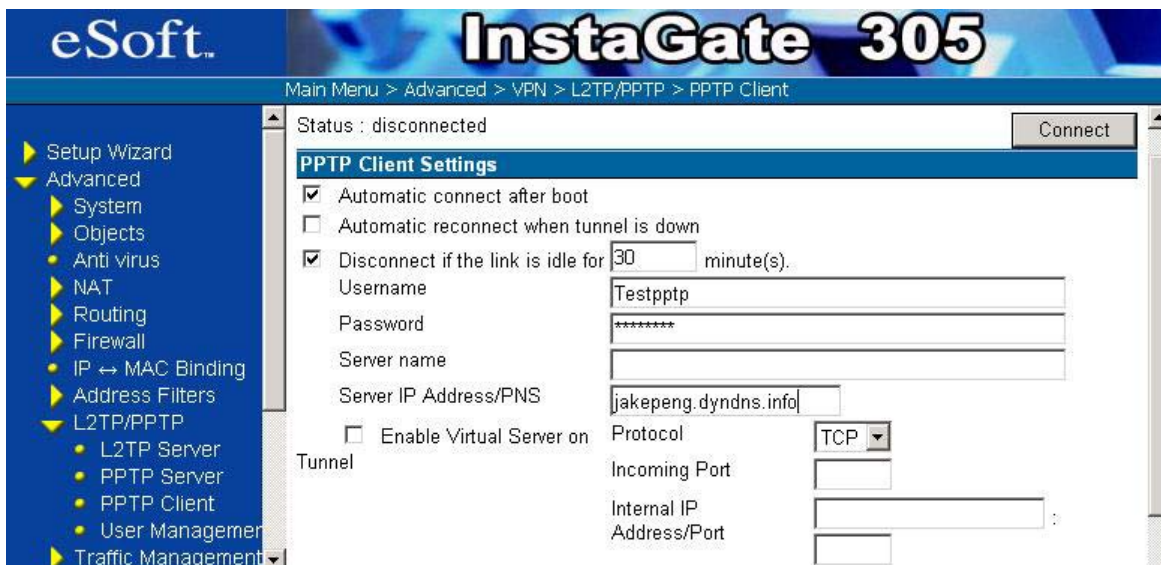


Figure 105: The InstaGate PPTP Client

Figure 106 shows a basic example for using a PPTP client.

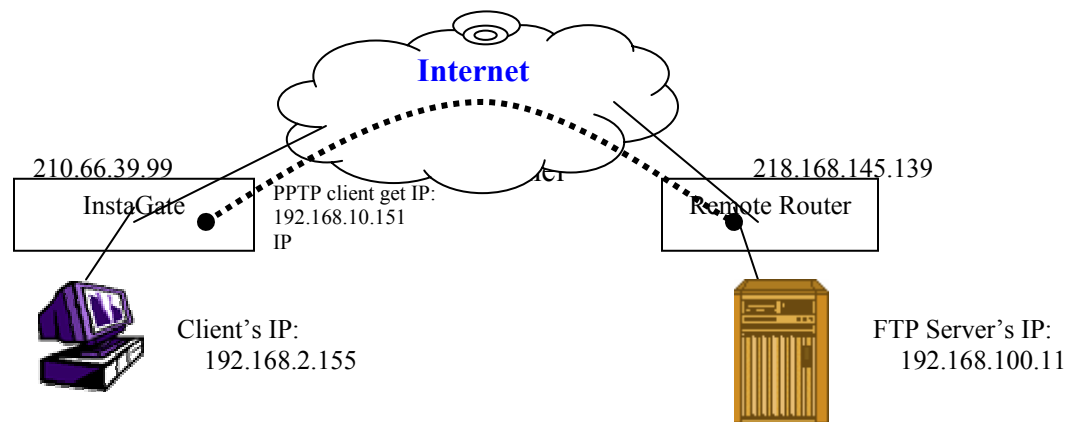


Figure 106: PPTP client example

Assumptions:

Remote Server: WAN Interface: 218.168.145.139

LAN Interface: 192.168.100.254

. Firewall policy: pass all traffic

New Policy Object										
#	Name	Source	Destination	Direction	Services	Actions	Active	Configure		
1	passall	0.0.0.0/0	0.0.0.0/0	LAN WAN		ACCEPT	<input checked="" type="checkbox"/>	Edit	Delete	MOVE

Figure 107: Firewall Policy Rule

PPTP server configuration:

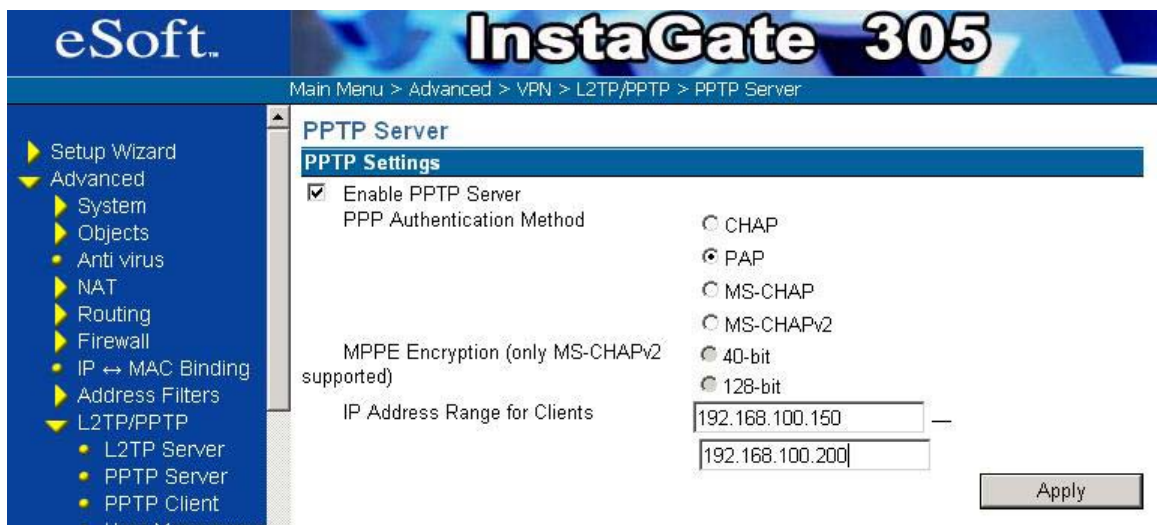


Figure 108: PPTP Server Settings

PPTP User management:

User name: testpntp

Password: testpntp

Assign IP: blank this field will assign IP automatically.

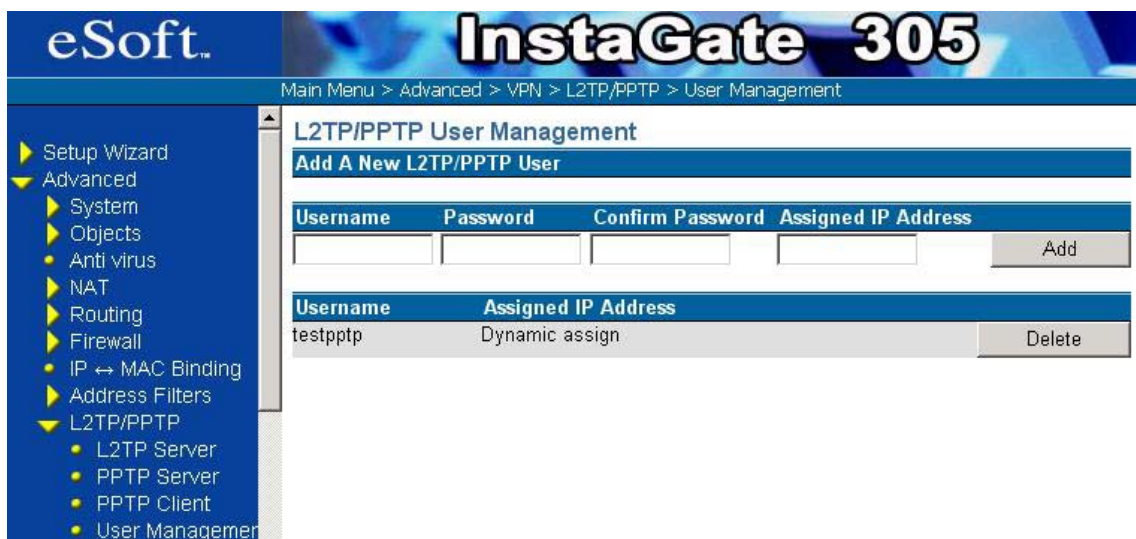


Figure 109: Remote VPN User Management

Local Router: WAN Interface: 210.66.39.99

LAN Interface: 192.168.2.1
(Must enable NAT function)

PPTP client setting:




Figure 110: PPTP Client Settings



Client's IP: 192.168.2.155

GW: 192.168.2.1

	FTP Server's IP: 192.168.100.11 GW: 192.168.100.254
---	--

Before the InstaGate connects to remote router, the routing table in local router is as follows:

Destination	Netmask	Gateway	Metric	Interface
192.168.3.0	255.255.255.0	*	0	DMZ
192.168.2.0	255.255.255.0	*	0	LAN
210.66.39.0	255.255.255.0	*	0	WAN
default	0.0.0.0	210.66.39.102	0	WAN

Figure 111: PTP Client Routing Table

Also if you want to ping from 192.168.2.155 to ping 192.168.100.11, it will fail.

After local router connects to remote router successfully, you can see the routing table has been updated:

Main Menu > Advance > VPN > L2TP/PPTP > PPTP Client

PPTP Client

Status : connected Disconnect

Tunnel end points: Local IP: 192.168.100.152 Remote IP: 192.168.100.150

Configuration information

- Automatic connect after boot
- Automatic reconnect when tunnel is down
- Disconnect if the link is idle for minute(s).

Username :

Password :

Server name :

Server IP/PNS :

Figure 112: PPTP Client Settings

Destination	Netmask	Gateway	Metric	Interface	
192.168.100.150	255.255.255.255	*	0	PPP	
218.168.145.139	255.255.255.255	210.66.39.102	0	WAN	
192.168.3.0	255.255.255.0	*	0	DMZ	
192.168.2.0	255.255.255.0	*	0	LAN	
210.66.39.0	255.255.255.0	*	0	WAN	
default	0.0.0.0	192.168.100.150	0	PPP	

Figure 113: PPTP Client Routes

And you can ping from 192.168.2.155 to ping 192.168.100.11 successfully.

10.2.4 User Management

In Sections 10.2.1 and 10.2.2, we described how to configure L2TP and PPTP services. Both of the services need to have user authentication for those who wish to remotely access the LAN. Under “Main Menu > Advanced > VPN > L2TP/PPTP > User Management”, you can configure the remote access user’s name and password. If you want to assign a static IP address to this remote access user, you could type the static IP address in the “Assign IP” field. If you leave the “Assign IP” blank, then the InstaGate will dynamically assign an IP address in the range specified by L2TP Configuration (see Section 10.2.1) or PPTP Configuration (see Section 10.2.2) to the remote access user, it depends on which service the user is using (see Figure 114).

The screenshot shows the InstaGate 305 web interface. The breadcrumb trail is: Main Menu > Advanced > VPN > L2TP/PPTP > User Management. The page title is "L2TP/PPTP User Management". Below the title is a section "Add A New L2TP/PPTP User" with a form containing fields for Username, Password, Confirm Password, and Assigned IP Address, followed by an "Add" button. Below this is a table listing existing users:

Username	Assigned IP Address	
testpptp	Dynamic assign	Delete
Bob	192.168.2.193	Delete

Figure 114: L2TP/PPP User Management

Note: The IP ranges of DHCP, L2TP, and PPTP should be different. Overlapped IP addresses will operate unexpectedly.

11 URL Filter

For all of the efficiencies and economies-of-scale offered by the Internet and web browsing, there are many risks and ‘inefficiencies’ associated with it as well. For instance, it is estimated by many analysts and reporting groups that over 30% of a “desk” employees time is actually occupied by non-work-related Internet surfing, email checking and the like. Likewise, especially in litigious countries such as the United States, there is much more risk to lawsuits due to inappropriate or illegal Internet content being displayed in public or other restricted locations. What’s more, many of the recent major Internet Viruses, Worms, Trojans and Spyware threats are delivered via web browsing. The InstaGate was designed to help mitigate these threats and more. For example, URL web address filtering restricts users from accessing definable improper web sites, while the web page program filter prevents against malicious attacks both from the Internet, and inside of the Intranet.

If you wish to enable/disable the Web filter function, you should go into the “Web Filtering” page in the main menu and select the checkbox to turn on or turn off the function as shown in Figure 115.



Figure 115: The Web Filtering option

11.1 Filtering Action

To restrict the types of web sites users have access to, the administrator can either “Refuse sites with a keywords in the URL” or “Accept sites with the keywords in the URL”. The function will also automatically ban any derivatives of the web site name, and make the specific URL inaccessible. *Note that the function filters by the hyperlink address name, not a filter based on the content of the page.*

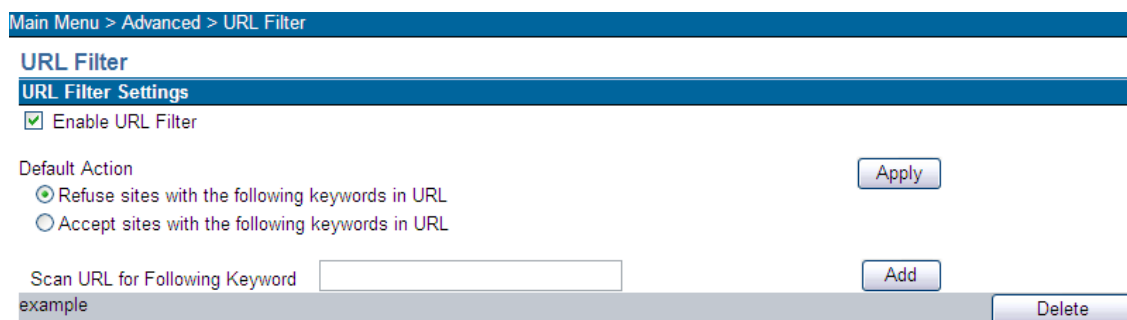


Figure 116: The Web Filtering Management page

11.2 URL Keyword

If you want to perform this function, enter the “Web Filtering” page and move to the “Scan URL for the Following Keyword” section. If you want to add a new web site, type the web site name or address and then select “Add”. To delete the record, select the “Del” button in the name/address that you want to delete. If the URL contains the keyword the default action will either allow or deny access to the web page.

11.3 Refuse Transfer Protocols

The simple URL address filter is not enough to prevent improper web sites and malicious attacks. We need to check the web page content and the external hyperlinks to reduce the hidden risks while visiting the web page.

If you want to perform URL address filtering function, select the “Web Filtering” page and move to the “Refuse the following transfer protocols” section. Select the checkbox that you want to disable the protocol on then select “Apply” button as shown in Figure 105 below.

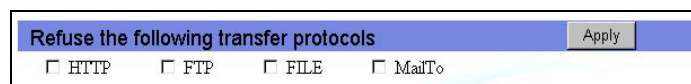


Figure 117: The Transfer Protocols configuration

11.4 Filtering web programs

Web browsers give the user a virtually unlimited number of options for accessing content. It enables the web content not only display the information but also interact with the user while accessing the Internet information. Unfortunately, there are almost as many harmful and malicious forms of content than there are legitimate forms of content. For instance, it is often times very difficult to tell the difference between a well-behaved or a malicious ActiveX control, because most of the activity is actually going on behind the scenes. Popular web applications that can carry harmful threats are Microsoft ActiveX controls, Java script, Java Applets and the like. The InstaGate is designed to filter the specific program that embedded in the web page to disable the programs while you visit the web page.

If you want to perform web filtering, enter the “Web Filtering” page and move to the “Refuse the following functions” section. Select the checkbox that you want to disable the program pass through the Internet access then select “Apply” button to apply your option. The detail is shown in Figure 106.



Figure 118: The URL Filtering Functions Configuration

11.5 Client Proxy setting

You have to configure the Internet proxy server settings on all remote client devices for web content filtering to operate properly.

If your browser is IE, double select the IE icon to run the IE program. Select the [Tools] on the menu bar. Go to “Internet Options” -> “Connections” -> “LAN Setting”. In the proxy server checkbox, fill in the LAN IP address of your InstaGate and the port number 1080 (see Figure 119).

If you use another web browser, please find the Proxy server configuration of your Internet browser. Fill in the InstaGate’s LAN IP address and Port number 1080 in the proxy configuration.

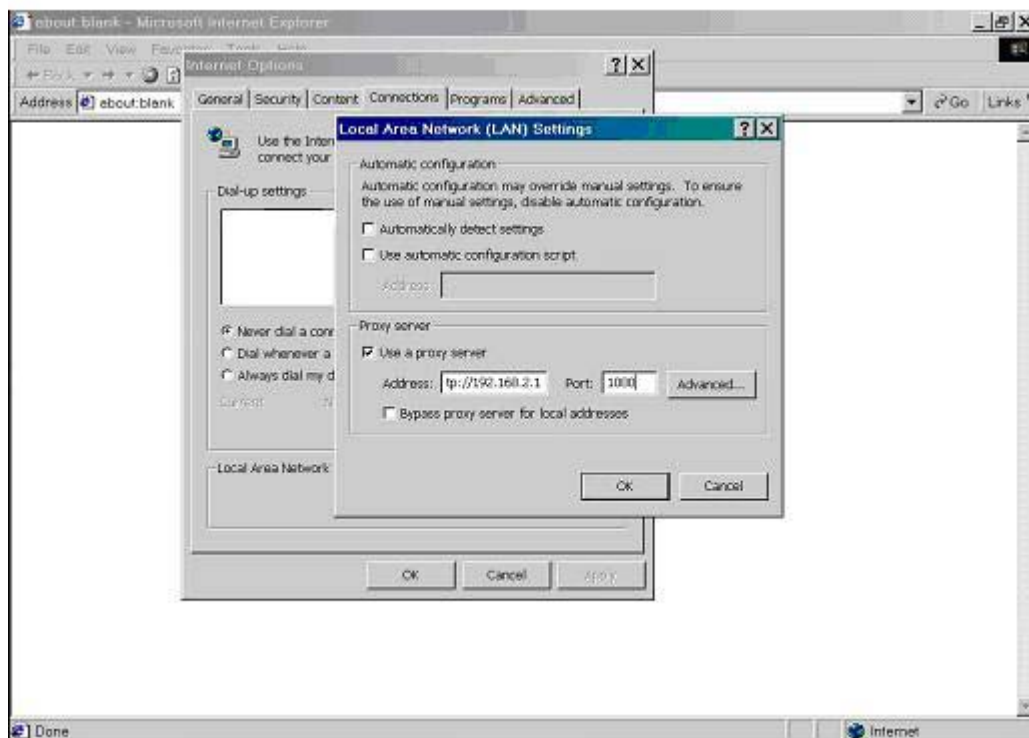


Figure 119: The proxy setting of the client machine

12 Intrusion Prevention

Perhaps the only thing growing faster than the rapid advances in network and internet technology, is the type and number of illegal and criminal activities that utilize these networks. From simple port scans and Denial of Service (DoS) attacks, to complicated polymorphic attacks that target the application level, the threats are real... and getting more sophisticated. The InstaGate provides two major functions to help detect and mitigate these attacks: “Intrusion Attack Types” and “Scan Prevention”.

12.1 Intrusion Attack Types

Packet normalization is a tool designed to detect and prevent DoS attacks, which are attacks that intend to limit the availability of network resources (such as a server or the firewall) by barraging it with traffic, or even crashing the system entirely (with buffer overflows, etc.) The earlier we detect the attack, the less damage we are likely to incur. To be effective, however, the pattern database needs to be updated with Software Care to detect the attacks. The normalization is not based on invading the pattern database. The InstaGate can base on the standard definition of IP, TCP, UDP and ICMP protocols to log and/or drop the violated packets. This is a more efficient way to defend attacks.

If you want to perform Packet Normalization, enter the “Intrusion Prevention” page, and go to the “Intrusion Attack Types” section. Select the protocol(s) that you would like to normalize.

To enable/disable normalization, select the “Active” checkbox. To log the event, please select the “Log” checkbox. To delete the suspected packets, select the “Drop” checkbox.

Main Menu > Advanced > Intrusion Prevention

Intrusion Prevention

Intrusion Prevention Settings

Enable Intrusion Prevention

Intrusion Attack Types

IP	<input type="checkbox"/> Select	<input checked="" type="checkbox"/> Activate All	<input checked="" type="checkbox"/> Log All	<input type="checkbox"/> DROP All
TCP	<input type="checkbox"/> Select	<input checked="" type="checkbox"/> Activate All	<input checked="" type="checkbox"/> Log All	<input type="checkbox"/> DROP All
UDP	<input type="checkbox"/> Select	<input checked="" type="checkbox"/> Activate All	<input checked="" type="checkbox"/> Log All	<input type="checkbox"/> DROP All
ICMP	<input type="checkbox"/> Select	<input checked="" type="checkbox"/> Activate All	<input checked="" type="checkbox"/> Log All	<input type="checkbox"/> DROP All
Other	<input type="checkbox"/> Select	<input checked="" type="checkbox"/> Activate All	<input checked="" type="checkbox"/> Log All	<input type="checkbox"/> DROP All

Scan Prevention

Anti-Fingerprinting Activate Log DROP

Apply

Figure 120: Intrusion Prevention Settings

You can select the “+” button next to each protocol to select the individual items (see Figure 121).

Intrusion Prevention

Intrusion Prevention Settings

Enable Intrusion Prevention

Intrusion Attack Types				
IP	<input checked="" type="checkbox"/> Select	<input checked="" type="checkbox"/> Activate All	<input checked="" type="checkbox"/> Log All	<input type="checkbox"/> DROP All
TCP	<input checked="" type="checkbox"/> Select	<input checked="" type="checkbox"/> Activate All	<input checked="" type="checkbox"/> Log All	<input type="checkbox"/> DROP All
UDP	<input checked="" type="checkbox"/> Select	<input checked="" type="checkbox"/> Activate All	<input checked="" type="checkbox"/> Log All	<input type="checkbox"/> DROP All
ICMP	<input type="checkbox"/> Select	<input checked="" type="checkbox"/> Activate All	<input checked="" type="checkbox"/> Log All	<input type="checkbox"/> DROP All
Ping of Death	<input checked="" type="checkbox"/> Activate	<input checked="" type="checkbox"/> Log	<input type="checkbox"/> DROP	
ICMP Type	<input checked="" type="checkbox"/> Activate	<input checked="" type="checkbox"/> Log	<input type="checkbox"/> DROP	
ICMP Chksum	<input checked="" type="checkbox"/> Activate	<input checked="" type="checkbox"/> Log	<input type="checkbox"/> DROP	
ICMP Broadcast	<input checked="" type="checkbox"/> Activate	<input checked="" type="checkbox"/> Log	<input type="checkbox"/> DROP	
ICMP Multicast	<input checked="" type="checkbox"/> Activate	<input checked="" type="checkbox"/> Log	<input type="checkbox"/> DROP	
Other	<input checked="" type="checkbox"/> Select	<input checked="" type="checkbox"/> Activate All	<input checked="" type="checkbox"/> Log All	<input type="checkbox"/> DROP All

Figure 121: Detailed items of Intrusion Attack Types

12.2 Scan Prevention

The network scan is the basis for many hacker intrusions. Intruders need to collect information and pick suitable model(s) to attack your machine. If we detect the intrusion attempt in advance, it is highly likely that we will be able to prevent the intrusion. The InstaGate provides you with the “*Scan Prevention*” function. This function helps “confuse” the intruders by hiding vital system information such as the version of OS.

Enter the “Intrusion Prevention” page and go to “Scan Prevention” section to perform the function, as shown in Figure 120.

To enable/disable the functions, please select the “Active” checkbox. To log the event, select the “Log” checkbox. To delete questionable packet, select the “Drop” checkbox.

13 Dynamic DNS

Under the “Main Menu > Advanced > Dynamic DNS” page, you can bind your domain name with a dynamic DNS provider. DDNS providers allow you to associate static hostnames with a dynamic IP address, allowing you to use your dynamically assigned IP address (from your ISP). This reduces the costs associated with static IPs. The InstaGate supports two dynamic DNS providers: Dynamic DNS Network Services (<http://www.dyndns.org>) and DNS Made Easy (<http://www.dnsmadeeasy.com>) .

After you create your account successfully and register a dynamic domain name. You will be given a Record ID or Hostname. Check the “Enable Dynamic DNS” checkbox and select the “Dynamic DNS Service”. Now enter the “Host Name or Record ID”, “Username” and “Password” for the Dynamic DNS Service you selected as shown in Figure 122.

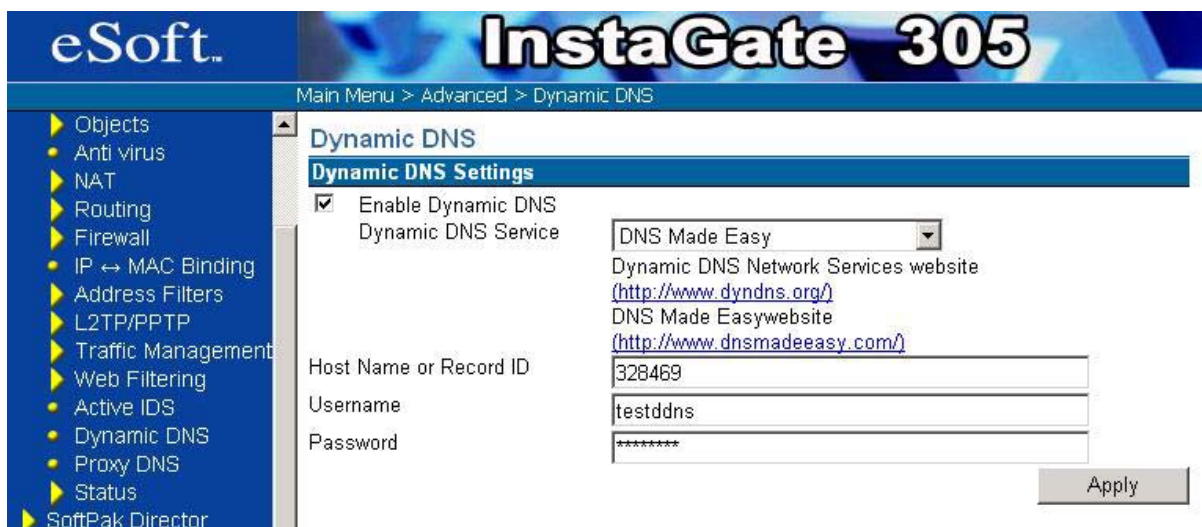


Figure 122: Dynamic DNS Settings

Last, you select the “Apply” button. If the InstaGate gets the new dynamic IP, it will update the IP information to “DNS Made Easy” automatically. You can see the update information under the “Main Menu > Advanced > Status > System Log” page.

14 Proxy DNS

Under the "Main Menu > Advanced > Proxy DNS " page, you can map a domain name to a server IP address. Acting as a DNS server for internal networks, it allows you to connect to local machines in your network without using an external DNS server, simplifying the configuration and management of our network. Before mapping the domain name to a Server IP address, however, it is necessary to specify your InstaGate DNS server address as follows.

1. Select **Start**, then choose **Settings > Network and Dial-up Connections**.
2. Select the Local Area Connection.

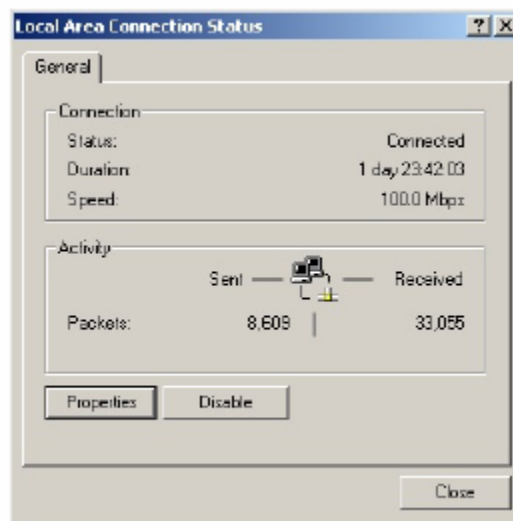


Figure 123: Network Connection Status

3. Select **Properties**.

The Local Area Connection Properties dialog box appears as:

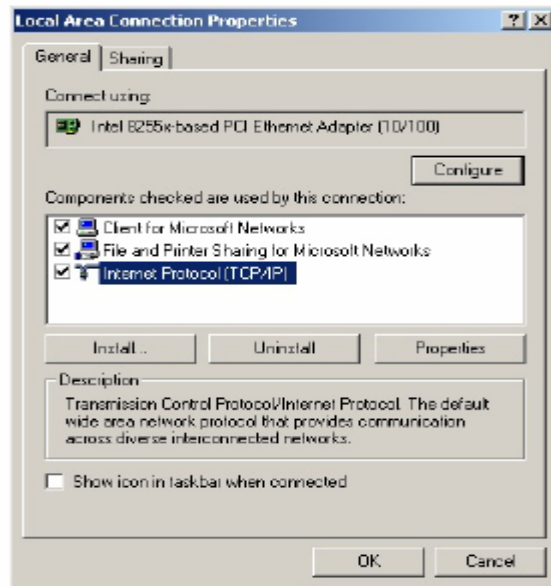


Figure 124: Network Connection Properties

4. Select **Internet Protocol (TCP/IP)**, then select **Properties**.

The Internet protocol (TCP/IP) Properties dialog box appears as:

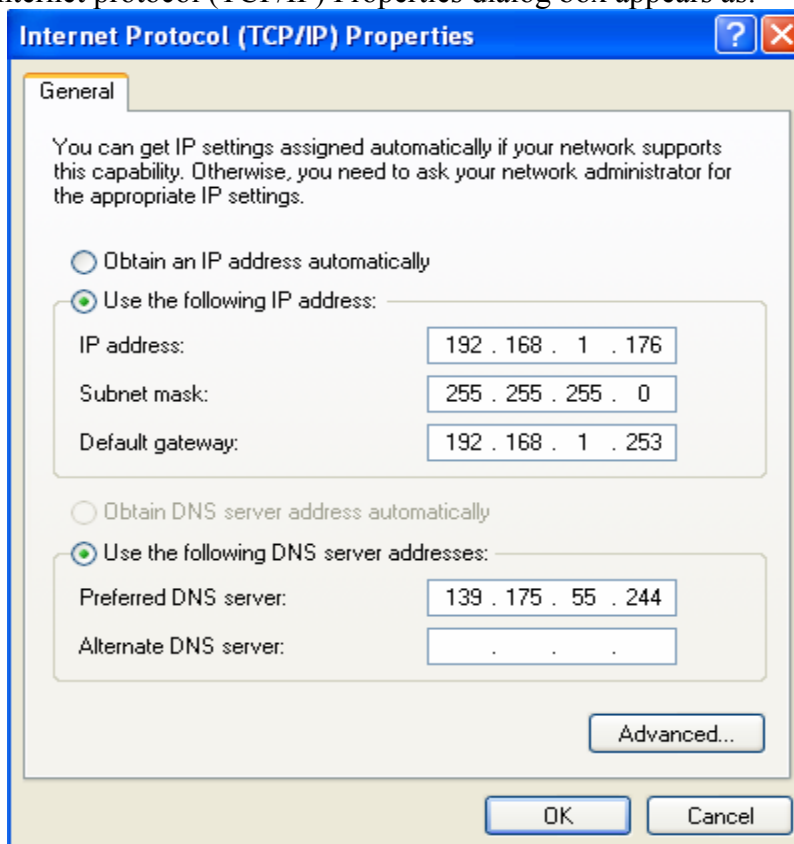


Figure 125: TCP/IP Properties

5. Then in Alternate DNS server specify the DNS server address of your InstaGate and select OK.

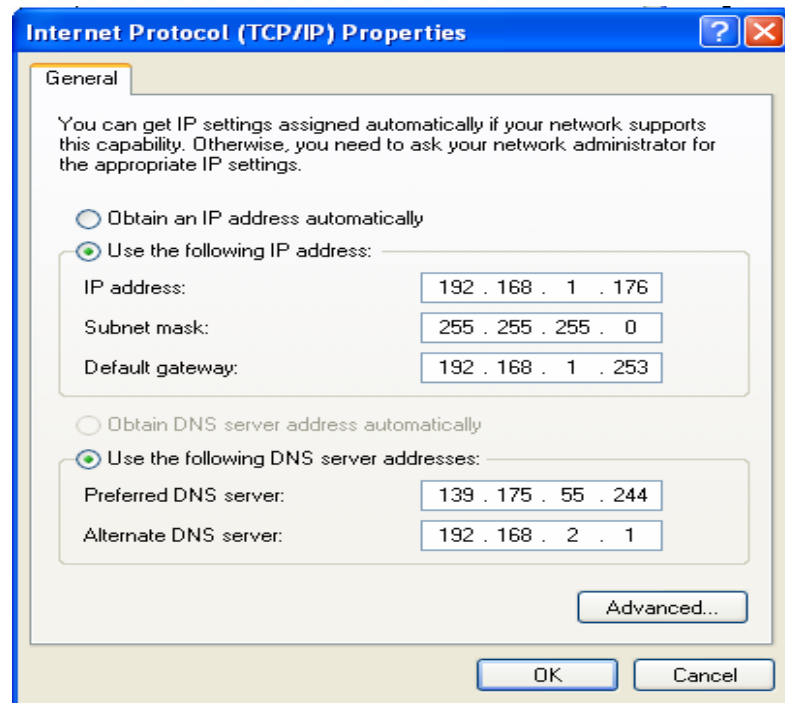


Figure 126: DNS Server Address

It is necessary to specify your security device DNS server name because the Domain name by which you are going to bind server IP address is not known by the network (that is its invalid for the Internet).

Then in the "Main Menu > Advanced > Proxy DNS " page, you need to specify the Server IP address, unique Domain name and unique Alias of it. No two fields can have same Domain name and Alias. After you finish, select "Add/Modify". The record will get automatically added into the Proxy DNS table. If you want to modify some contents you can select the respective "Modify" button.

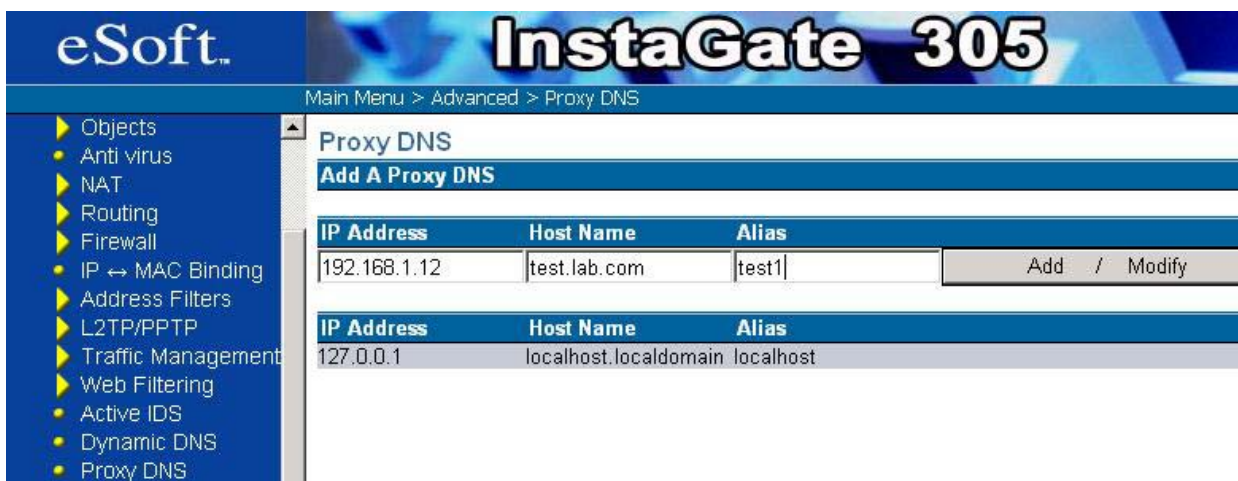


Figure 127: Proxy DNS

After you select “Add Modify” button the record gets added to the Proxy DNS table automatically as shown the Figure below.

The screenshot shows the InstaGate 305 web interface. The breadcrumb trail is "Main Menu > Advanced > Proxy DNS". The left sidebar menu includes "Setup Wizard", "Advanced" (expanded), "System", "Objects", "Anti virus", "NAT", "Routing", "Firewall", "IP ↔ MAC Binding", "Address Filters", "L2TP/PPTP", "Traffic Management", "Web Filtering", "Active IDS", "Dynamic DNS", and "Proxy DNS".

The main content area is titled "Proxy DNS" and contains an "Add A Proxy DNS" button. Below this is a table with the following data:

IP Address	Host Name	Alias	
			Add / Modify
127.0.0.1	localhost.localdomain	localhost	
192.168.1.12	test.lab.com	test1	Modify Delete

Figure 128: Proxy DNS List

15 Status

15.1 Log Setting

Under the “Main Menu > Advanced > Status > Log Setup” page, the InstaGate provides you with “Email Setting” and “Scheduler Setting”. You can send the whole system log information to a valid email account. As shown in Figure 129, you have to provide a “Mail subject”, the “Administrator Email account”, “SMTP Server IP”, and if required, a “username” and “password” of the SMTP server. Then select the “Apply” button to save the settings. If you want to mail the log immediately, select the “Mail log now” button.

The screenshot shows the InstaGate 305 web interface. The breadcrumb trail is "Main Menu > Advanced > Status > Log Setup". The left sidebar contains a navigation menu with categories like Address Filters, L2TP/PPTP, Traffic Management, Web Filtering, Active IDS, Dynamic DNS, Proxy DNS, Status (with sub-items Log Setup, System, VPN, ARP, DHCP), and SoftPak Director. The main content area is divided into two sections: "Mailing Setting" and "Scheduler Setting".

Mailing Setting:

- Administrator Email Address:
- Message Subject:
- SMTP Server Address:
- Use Authentication
 - Username:
 - Password:

Buttons:

Scheduler Setting:

- Mail disabled

Figure 129: Mailing setting of Log

You can decide when the system will send the log information to your email account. As shown in Figure 130, this InstaGate supports five pre-set schedules to match your needs.

The screenshot shows the InstaGate 305 web interface. The breadcrumb trail is "Main Menu > Advanced > Status > Log Setup". The left sidebar is the same as in Figure 129. The main content area shows the "Mailing Setting" section is empty, and the "Scheduler Setting" section has five radio button options.

Mailing Setting:

- Administrator Email Address:
- Message Subject:
- SMTP Server Address:
- Use Authentication
 - Username:
 - Password:

Buttons:

Scheduler Setting:

- Mail disabled
- Mail the system log if it more than 100K
- Mail the system log if it more than 500K
- Mail the system log daily
- Mail the system log weekly

Button:

Figure 130: Scheduler Setting

If you want to send syslog information to an external server then you can select the “Enable syslog output to external server” check box and specify the IP address of the external syslog server and select the “Apply” button (see Figure 131). By this method, you can get previous syslog information from the external Server if your InstaGates syslog tables have been cleared.



Figure 131: Syslog Output to external server

15.2 System Info.

Under the “Main Menu > Advanced > Status > System” page, you can see the summary of system information (see Figure 132). The “Refresh” button will reload this summary page.

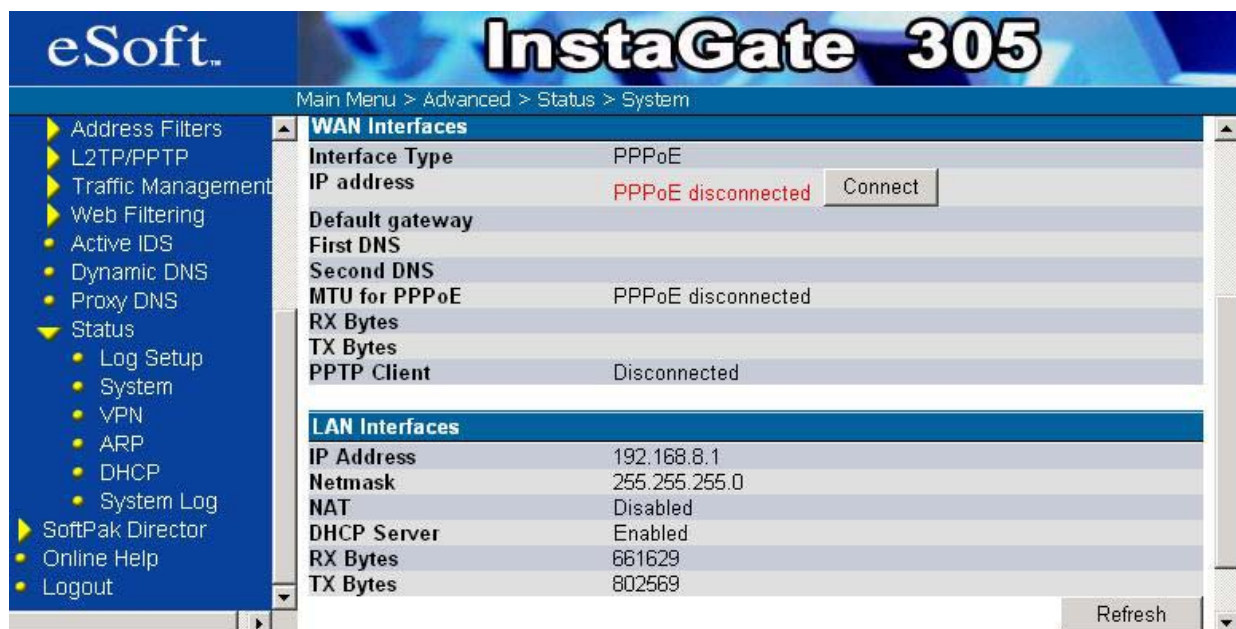


Figure 132: The summary of system information

15.3 VPN Status

Under the "Main Menu > Advanced > Status > VPN Status " page, you can see a subset of VPN configuration information of the device. The "VPN SP Status" shows the status of security policies such as "Source IP/Subnet", "Destination IP/Subnet", "Source Gateway IP", "Destination Gateway IP", "Type" for Auto-Key or Manual-key, "State" for Connected or Disconnected. "VPN SA Status" shows the status of security association including the "security parameter index (SPI)", "Destination Gateway IP", "Proposal", "Source IP/Subnet", "Destination IP/Subnet", "Source Port", "Destination Port".

The screenshot shows the VPN Status page with a search bar and two tables. The first table, 'VPN SP Status', lists two security policies. The second table, 'VPN SA Status', lists two security associations.

Main Menu > Advance > VPN > VPN Status							
Search keyword: <input type="text"/> <input type="button" value="search"/>							
VPN SP Status							
No	Name	Src IP/Subnet	Dst IP/Subnet	Src GW IP	Dst GW IP	Type	State
1	autokey1	192.168.2.0/255.255.255.0	192.168.10.0/255.255.255.0	192.168.1.64	192.168.1.84	AutoKey	Connected
2	autokey1	192.168.10.0/255.255.255.0	192.168.2.0/255.255.255.0	192.168.1.84	192.168.1.64	AutoKey	Connected

VPN SA Status							
No	SPI	Dst GW IP	Proposal	Src IP/Subnet	Dst IP/Subnet	Src Port	Dst Port
1	14d1de23	192.168.1.64	ESP	192.168.10.0/255.255.255.0	192.168.2.0/255.255.255.0	0-65535	0-65535
2	ed42866	192.168.1.84	ESP	192.168.2.0/255.255.255.0	192.168.10.0/255.255.255.0	0-65535	0-65535

Figure 133: VPN Status

You can also search a particular record by specifying the search keyword and then clicking the “search” button as shown in the Figure below.

The screenshot shows the VPN Status page with the search bar containing the text 'autokey1' and the search button.

Main Menu > Advance > VPN > VPN Status

Search keyword:

Figure 134: VPN Status Search

After you select the “search” button the following results are displayed.

The screenshot shows the VPN Status page with search results for 'autokey1'. The search bar is empty, and the results table is displayed.

Main Menu > Advance > VPN > VPN Status							
VPN SP Status							
No	Name	Src IP/Subnet	Dst IP/Subnet	Src GW IP	Dst GW IP	Type	State
1	autokey1	192.168.2.0/255.255.255.0	192.168.10.0/255.255.255.0	192.168.1.64	192.168.1.84	AutoKey	Connected
2	autokey1	192.168.10.0/255.255.255.0	192.168.2.0/255.255.255.0	192.168.1.84	192.168.1.64	AutoKey	Connected

Figure 135: VPN Status Search Results

15.4 ARP Table

Under the “Main Menu > Advanced > Status > ARP” page, you can see the ARP table (which is a cache of IP/MAC address mappings). When you want to send a packet to a

local host, your software looks up the IP in the ARP cache, gets the MAC address, constructs an Ethernet header with the correct source/destination MAC addresses (see Figure 136).

IP Address	MAC Address
192.168.8.11	00:50:EB:0E:80:FF

Figure 136: ARP Cache Table

15.5 DHCP Table

Under the “Main Menu > Advanced > Status > DHCP” page, you can see the DHCP IP assignment table. It contains the information of IP address, MAC address, released and expire time and host name (see Figure 137).

IP Address	MAC Address	Leased Time	Host
192.168.8.11	00:50:eb:0e:80:ff	1970/01/01 02:13:46 — 1970/01/01 12:13:46	john

Figure 137: DHCP IP Assignment Table

15.6 System Log

Under the “Main Menu > Advanced > Status > System Log” page, the administrator can see pertinent system information for this device. In the log table, you can find out when the event happened, what process invoked it and detailed information about the event. For example, you can find out the login name, login time and login IP address in the

login event. You can select how many lines to display by clicking the pull-down menu, and you can also select which page you want to jump to. The “Refresh” button will reload the latest contents of the system. If you want to clear the whole log, select “Clear Log” (see Figure 138).

The screenshot shows the InstaGate 305 web interface. The left sidebar contains a navigation menu with the following items: Address Filters, L2TP/PPTP, Traffic Management, Web Filtering, Active IDS, Dynamic DNS, Proxy DNS, Status (expanded), Log Setup, System, VPN, ARP, DHCP, System Log (highlighted), SoftPak Director, Online Help, and Logout. The main content area is titled 'Logging' and includes a 'Display Settings' section with dropdown menus for '100 lines/page', 'Page. 1', and 'All information'. Below these are a 'GO' button, a search box with a 'Search' button, and 'Refresh' and 'Clear Log' buttons. The log entries are as follows:

Date & Time	Process	Message
Jan 1 00:00:17	pftpd[319]	[SGLOG7] MGR: Bad IP address () in config file!
Jan 1 00:01:02	httpd	[SGLOG6] admin login from 192.168.8.11 successfully.
Jan 1 00:00:20	IKE[304]	[SGLOG6] IKE (v1.0) task start
Jan 1 00:00:20	l2tpd[313]	[SGLOG6] l2tpd version 0.69 started on (none) PID:313
Jan 1 00:00:20	pftpd[319]	[SGLOG7] MGR: Bad IP address () in config file!
Jan 1 02:13:45	dhcpcd	[SGLOG6] DHCPDISCOVER from 00:50:eb:0e:80:ff via ixp0

Figure 138: System Log

16 SoftPak Director

SoftPak applications are security and IT software modules that add functionality to your InstaGate. SoftPaks are delivered via SoftPak Director. SoftPak Director allows you to perform the following functions:

- Subscribing to SoftPaks
- Viewing Enabled SoftPaks
- Changing your User License Level

16.1 Registration

Enter your contact information to access important services such as the SoftPak Director and InstaGate Software Care, Hardware Care, and Phone/Email support.

Main Menu > SoftPak Director > Registration

System Setup: Registration

Please keep your InstaGate registration information up-to-date in order to access important services such as the SoftPak Director and InstaGate Software Care, Hardware Care, and Phone/Email Care support.
Correct billing information is required in order to purchase SoftPaks through the SoftPak Director.

Registration has been previously sent : Mon Jul 25 16:10:18 UTC 2005

Billing Address

Name of Organization	<input type="text" value="eSoft, Inc."/>	Billing Contact	<input type="text" value="Accounting"/>
Address	<input type="text" value="295 Interlocken Blvd"/>	City	<input type="text" value="Broomfield"/>
Country	<input type="text" value="United States"/>		
State or Province	<input type="text" value="Colorado"/>	Postal Code	<input type="text" value="80021"/>

Administrative Contact

First Name	<input type="text" value="Tech"/>	Last Name	<input type="text" value="Support"/>
E-mail Address	<input type="text" value="support@esoft.com"/>	Phone Number	<input type="text" value="303-444-1600"/>

Keep Me Informed!

<input checked="" type="checkbox"/> eSoft Updates	<i>Notify me of eSoft software updates, security patches, and feature enhancements.</i>
<input checked="" type="checkbox"/> eSoft Announcements	<i>Notify me of eSoft SoftPak applications and product promotions.</i>

* By subscribing to these notification lists you are authorizing eSoft to provide you with the above requested information by email.
Your contact information is never provided to any third party.

Figure 139: SoftPak Director Registration

16.2 Catalog

16.2.1 Subscribing to a SoftPak

To subscribe to a SoftPak:

1. Select Catalog from the SoftPak Director menu. A list of available SoftPaks is displayed along with a brief description and pricing information for each application.
2. Select the SoftPak you wish to subscribe to, and click Subscribe. A confirmation page appears listing the fees associated with the selected SoftPak.
 - Note: To view additional information about the selected SoftPak, click Details. See .Viewing SoftPak Details below for more information.
3. Click Yes. The Billing Information page appears.
4. Enter your billing information, and click Next. A confirmation page appears listing the details of your order.
5. Click Purchase to subscribe to the SoftPak. If your order is processed successfully a receipt is displayed. Please print the receipt and keep it for your records.
6. Click Download Now to immediately download the SoftPak.
7. A status bar displays the progress of the download. When the download is complete, the Apply Updates page appears listing the system administrators who will be notified when the installation is complete. Click Install to install the SoftPak.

If you do not wish to install the SoftPak at this time, click Cancel to exit the SoftPak Director. The next time you access the administrative interface a message will appear instructing you to install the SoftPak. To install the SoftPak, click the Install Now button.

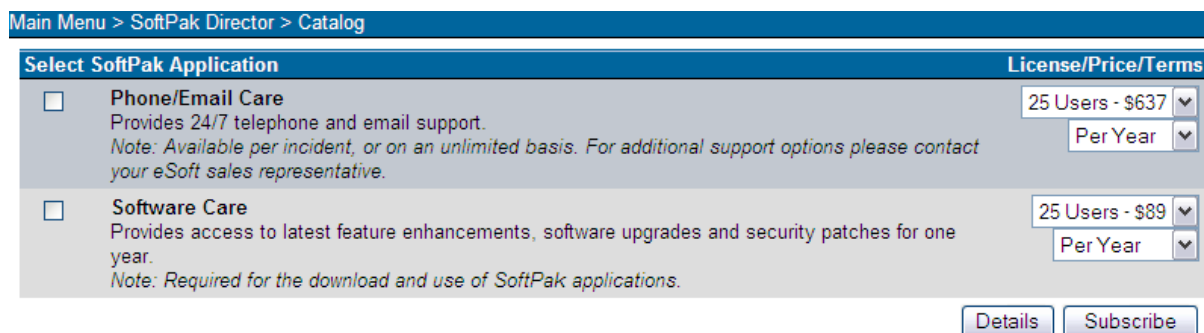


Figure 140: SoftPak Director Catalog

16.2.2 Viewing SoftPak Details

The Details page provides a brief product description and pricing information for the selected SoftPak. To exit the Details page, click Done.

If you have already subscribed to the SoftPak, the Details page may provide a Renew button so that you can quickly renew your SoftPak subscription.

If you have not subscribed to the SoftPak, a Subscribe button is provided.

16.3 Enabled

The SoftPak Director Enabled page lists the SoftPaks to which you are currently subscribed. You can also check for software updates and renew SoftPak subscriptions on this page.

To view enabled SoftPaks:

1. Select Enabled from the SoftPak Director menu. A list of SoftPaks you are currently subscribed to appears, along with the expiration date for each SoftPak (if applicable). Both installed SoftPaks and SoftPaks that have been downloaded but not yet installed are listed.
2. InstaGate automatically contacts the SoftPak Director every week to see if new SoftPaks are available. To force an immediate check for updates, click Check Now.
3. To view additional information about an enabled SoftPak, click Details. See section 16.2.2 (Viewing SoftPak Details).
4. To renew your subscription to a SoftPak, select the SoftPak and click Renew. A confirmation page appears listing the fees associated with the selected SoftPak. Click Yes to renew your subscription.

Select	SoftPak Application	Status
<input type="checkbox"/>	Extended Hardware Care Extends 1st-year warranty for hardware repair by one year. <i>Note: Required to qualify for "Hardware Hot Swap" purchase.</i>	Installed: Yes Expires: 20 June 2006 25 Users - \$99 Per Year
<input type="checkbox"/>	Gateway Anti-Virus Scan HTTP, FTP, POP3 and SMTP for virus content	Installed: Yes Expires: 08 July 2006 25 Users - \$175 Per Year

[Details](#) [Upgrade](#) [Renew](#)

Figure 141: SoftPak Director Enabled

16.4 User License

InstaGate can be licensed for 25, or Unlimited users. Through SoftPak Director, you can upgrade the number of users supported by your system as needed.

To change your user license level:

1. Select User License from the SoftPak Director menu. The number of users currently supported by your system is selected.
2. Select the new user license level from the drop-down list, and click Change. A confirmation page appears listing the relevant changes to the user license and fees.
3. Click Yes to update your user license level, or Cancel to exit without updating.

Main Menu > SoftPak Director > User License

Select	User License Level
<input checked="" type="radio"/>	25 Maximum Users (Current)
<input type="radio"/>	Unlimited Users

Change

Figure 142: SoftPak Director User License

17 Global Management

eSoft's Global Management technology allows a central administrator to configure and manage network security and access policies for multiple InstaGate devices. Participating InstaGates use global management clients to connect to a global management server (such as, VPN Manager).

Once connected, a device continually exchanges configuration information with the management server and reconfigures as necessary.

17.1 Client Settings

To enable Global Management configure the Client Settings as shown in Figure 143

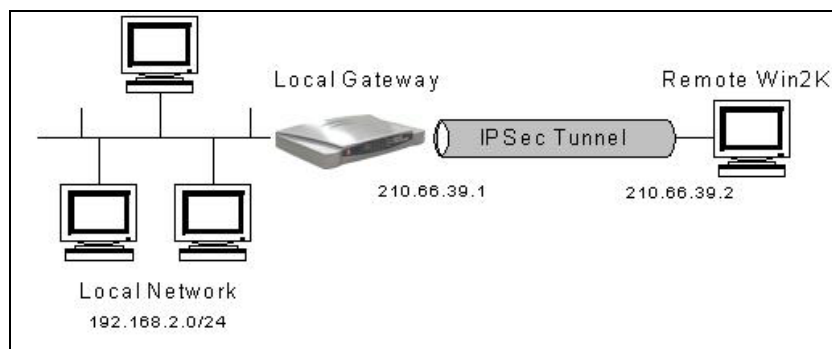
1. Select "*Global Management*" menu.
2. Select the "Global Management Enabled" check box. This enables the InstaGate's global management client, allowing it to connect to a global management server.
3. Enter the IP address or host name of the Management Server in the "Remote Address" field.
4. Enter the "Domain" for management. The domain name is used to identify and group the clients managed by the global management server.
5. Enter a "Login Name" and "Password" for the client. The name and password specified are used to authenticate (or register) the client when connecting to the global management server.
6. Click "Apply" to save your settings, or "Cancel" to exit without saving.

The screenshot shows a web-based configuration interface. At the top, a blue breadcrumb trail reads: "Main Menu > SoftPak Director > Global Management > Client Settings". Below this, the page title "Client Settings" is displayed in blue. Underneath, a sub-header "Global Management Client Settings" is shown in white text on a blue background. The main content area contains a checkbox labeled "Enabled Global Management". Below the checkbox are four text input fields: "Remote Address", "Domain", "Login Name", and "Password". To the right of these fields are two buttons: "Apply" and "Cancel".

Figure 143: Global Management Settings

Appendix A: Win2K IPSec VPN to the InstaGate

This example guides users through the setup of an IPSec VPN Tunnel between a Win2K Client and the InstaGate. As shown below, we assume the local gateway's name is Security-Router and remote PC is with a Win2K IPSec Client. The local network and remote network is connected through an IPSec tunnel. The IP addresses we used in this example are shown as below.



Local Gateway (Security-Router)	Remote PC (Win2K)
WAN: 210.66.39.1 LAN: 192.168.2.1	WAN: 210.66.39.2

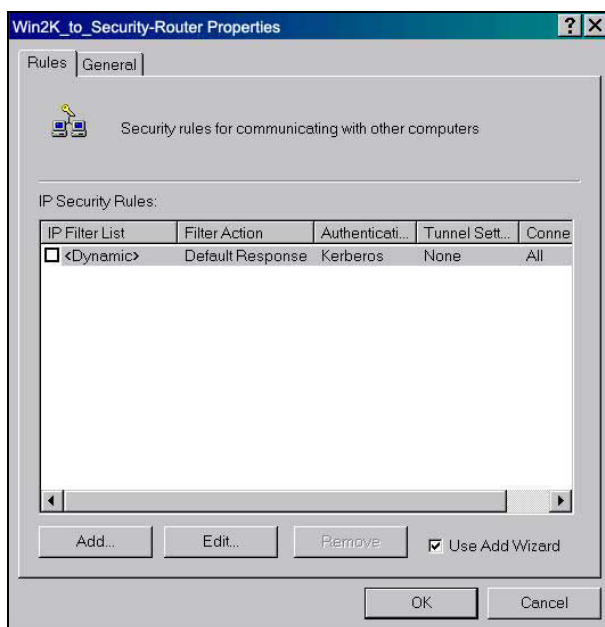
I.Setup Win2K IPSec VPN

A. Create IPSec Policy

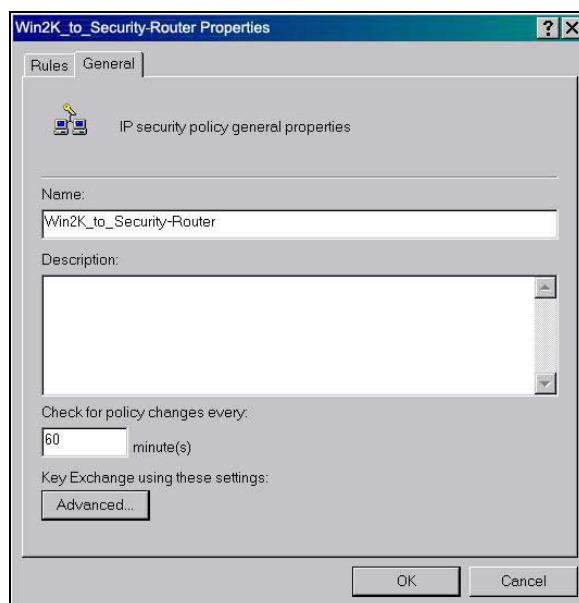
Typically, the Win2K client is not a member of a domain, so a local IPSec policy is created. If your Win2K client is a member of a domain, there already exists a local IPSec policy. In this case, you can create an Organization Unit (OU) in Active Directory to make your Win2K as a member of this OU by assigning the IPSec policy to the Group Policy Object (GPO) of this OU. For more information, please refer to the Assigning IPSec Policy section of Win2K online help.

1. From Window desktop, **Start** → **Run**, enter **SECPOL.MSC**, select **OK**.
2. Right-select **IP Security Policies on Local Machine**, and then select **Create IP Security Policy**.
3. Select **Next**, and enter name and description for your policy. For example, Win2K_to_Security-Router.

4. Uncheck *Activate the default response rule* check box, and select *Next*.
5. Keep the *Edit properties* check box selected and select *Finish*.
6. A dialog will pop-up for you to configure two filter rules for this policy.



NOTE: The IPsec policy is created with default IKE main mode (phase 1) on the *General* tab. Please check details by select the *Advanced...* on this tab.

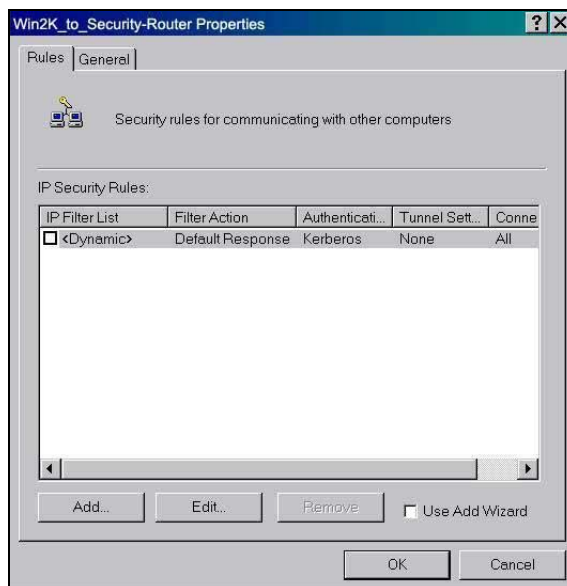


B. Create Filter Rules for IPsec Policy

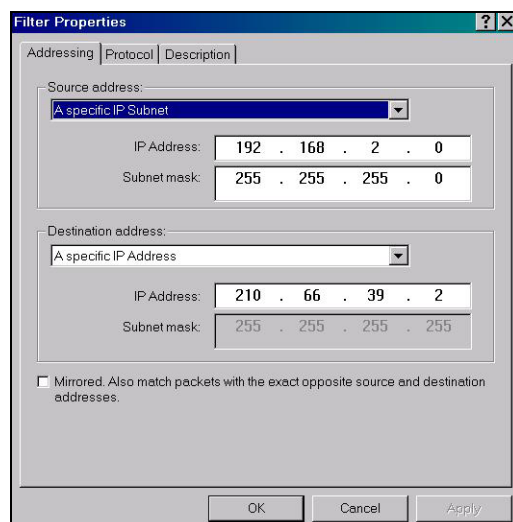
The IPsec tunnel consists of two filter rules, each of which specifies a tunnel endpoint. One is for the direction from Security-Router to Win2K client, and the other is from Win2K client to Security-Router. In each filter rule, a source IP and destination IP for local and remote VPN clients are required.

C. Build a filter rule from Security-Router to Win2K client

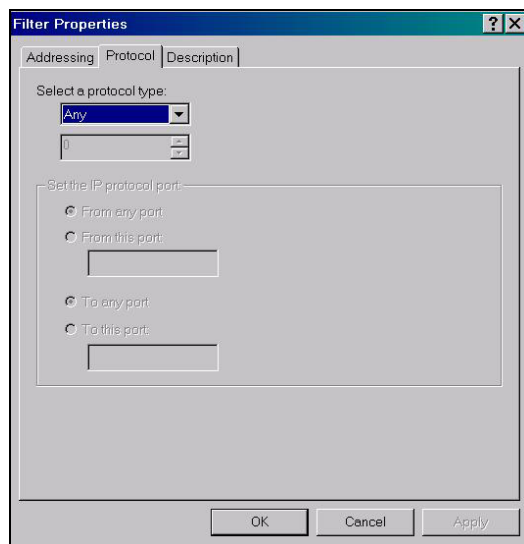
1. In the policy dialog, uncheck *Use Add Wizard* check box, and select *Add....*



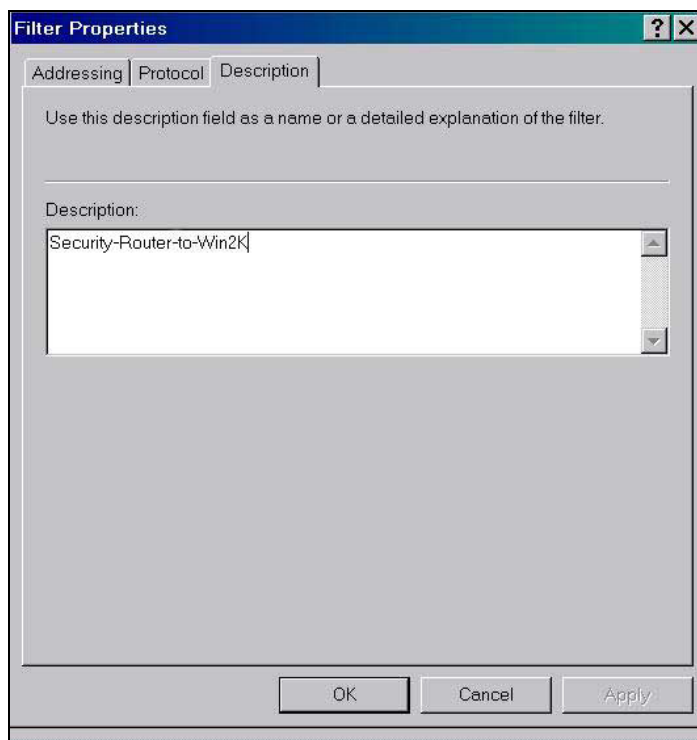
2. On *IP Filter List* tab, select *Add....*
3. Enter a name for this filter rule (e.g., Security-Router to Win2K), uncheck *Use Add Wizard* check box, and select *Add....*
4. Select *A specific IP Subnet* in the *Source address*, and enter the IP addresses of Local Network.
5. Select *A specific IP Address* in the *Destination address*, and enter the IP addresses of Remote PC.
6. Uncheck *Mirrored* check box.



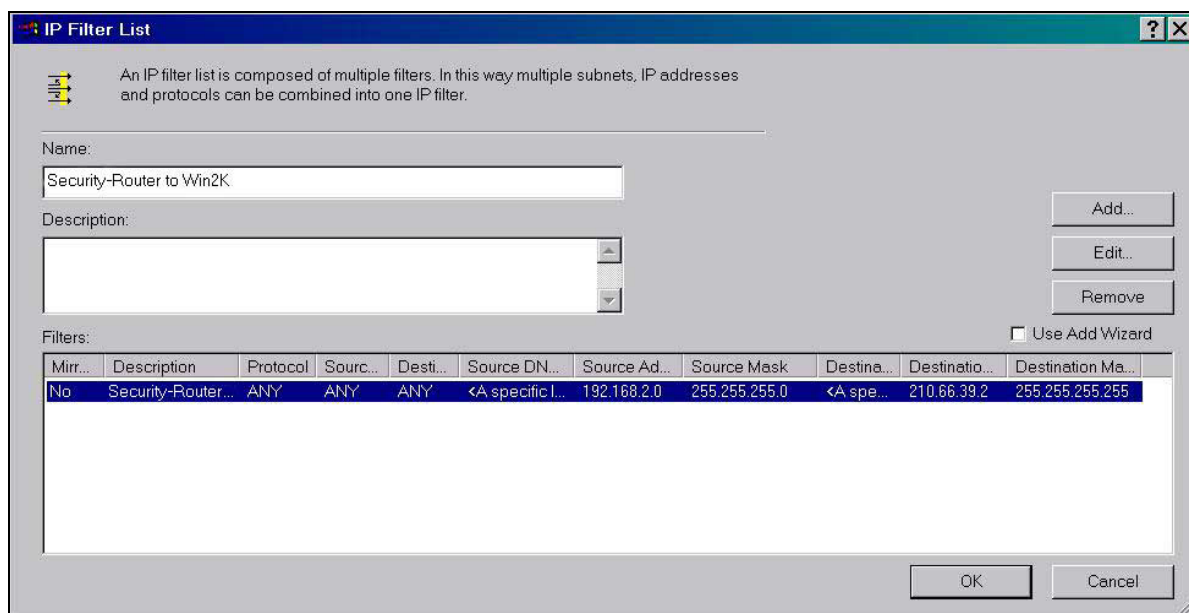
7. On the *Protocol* tab, leave the protocol type to *Any*. Because IPSec tunnels do not support protocol-specific or port specific filters.



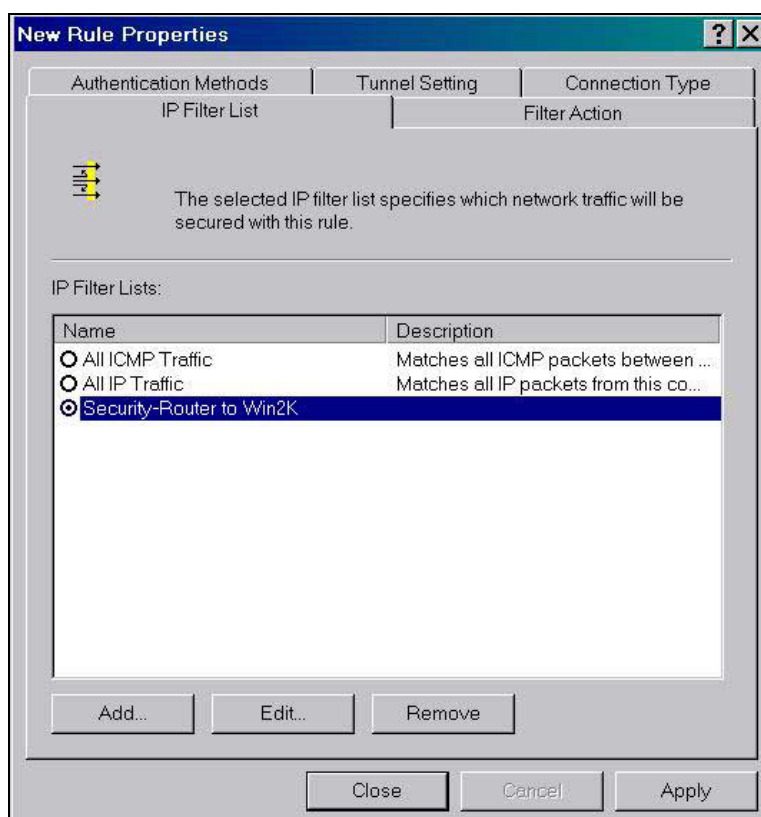
8. On the *Description* tab, you can give a description for this filter.



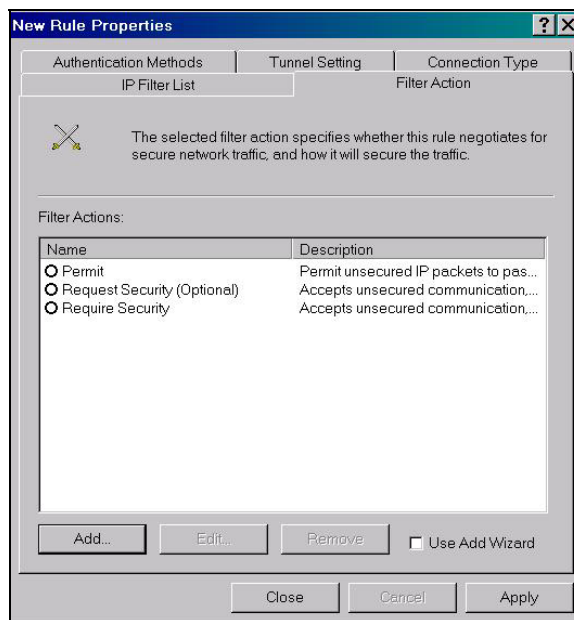
9. Select *OK*, and then select *Close*.



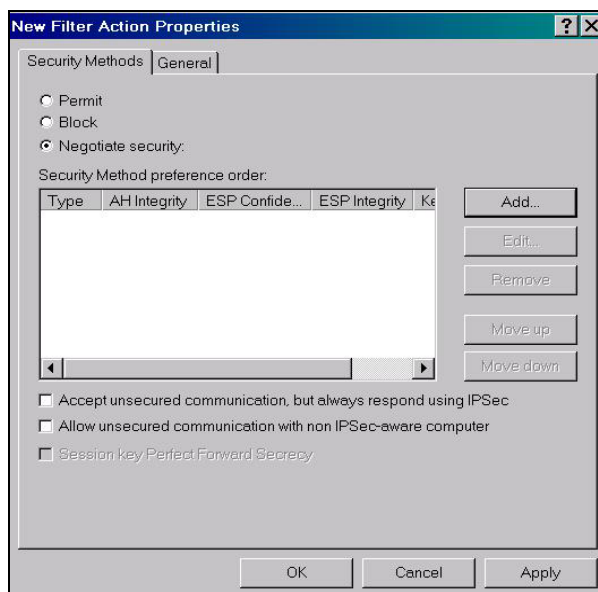
It will create a filter and select the filter we just created.



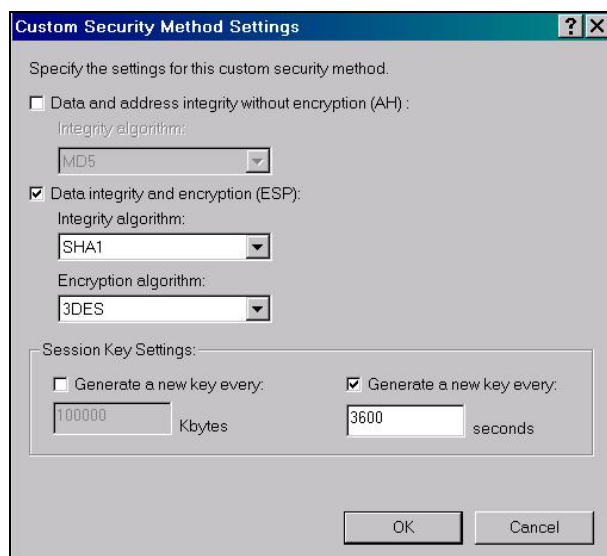
10. On **Filter Action** tab, uncheck **Use Add Wizard** check box, and select **Add...**



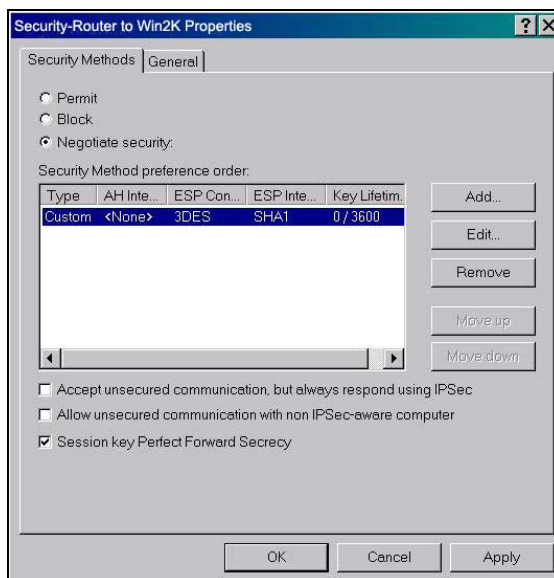
11. Leave *Negotiate security* is checked, and uncheck *Accept unsecured communication, but always respond using IPSec* check box. You must do this to ensure secure connections.



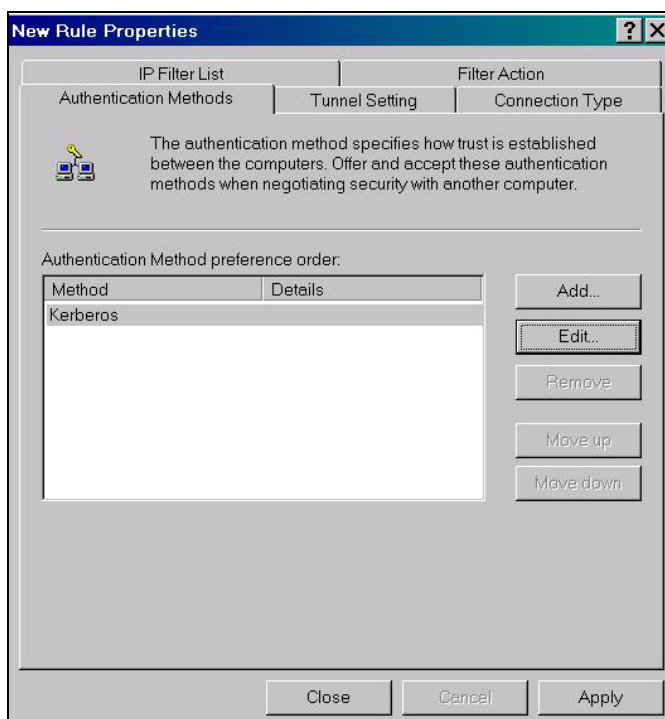
12. Select *Add...* and select *Custom (for expert users)* if you want to define specific algorithms and key lifetimes. Please make sure the settings match whatever we will configure in Security-Router.

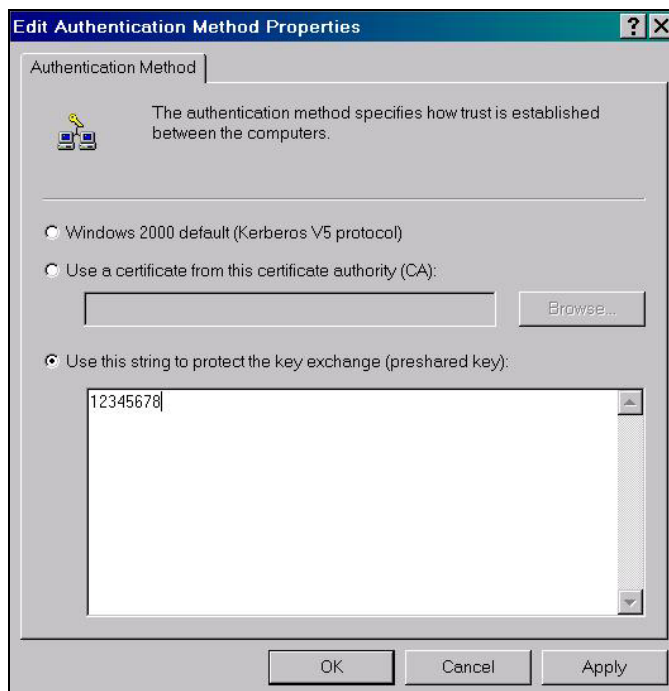


13. Select **OK**, check **Session key Perfect Forward Secrecy** check box if you want to enable the PFS function.

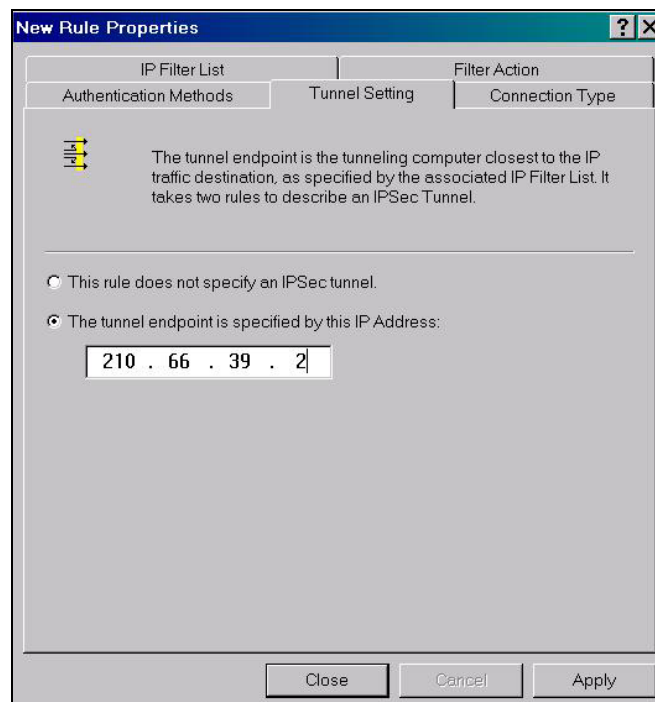


14. On **General** tab, give a name to this filter action, for example, Security-Router to Win2K, and select **OK**.
15. Select the filter action you just created.
16. On **Authentication Methods** tab, select **Edit**, select **Use this string to protect the key exchange (preshared key)** option, and enter the string **12345678** in the text box, select **OK**.



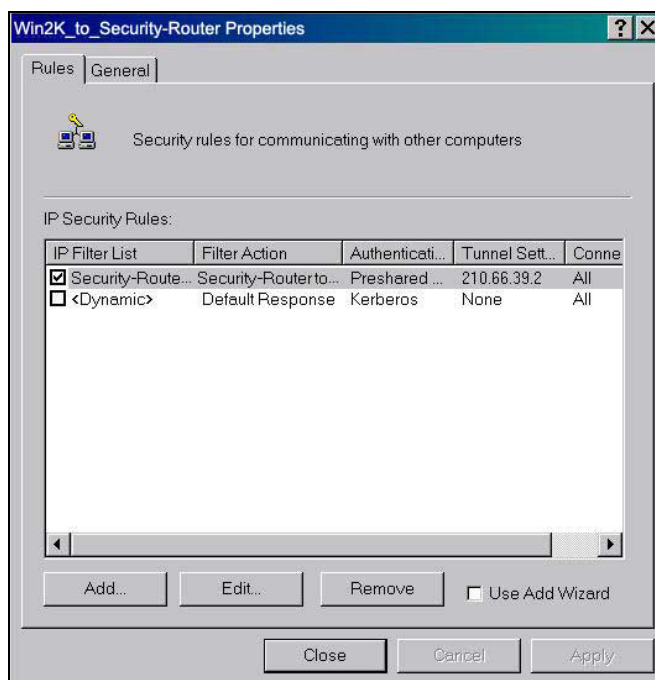


17. On **Tunnel Setting** tab, select **The tunnel endpoint is specified by this IP address**, and enters the WAN IP address of Win2K client.



18. On **Connection Type** tab, choose the connection type you want to apply this rule (e.g. All network connections).
19. Select **Close**.

It will create a filter rule and check the filter rule we just created.



D. Build a filter rule from Win2K client to Security-Router

1. In the policy dialog window, uncheck *Use Add Wizard* check box, and select *Add....*
2. On *IP Filter List* tab, select *Add....*
3. Enter a name for this filter rule (e.g., Win2K to Security-Router), uncheck *Use Add Wizard* check box, and select *Add....*
4. Select *A specific IP Address* in the *Source address*, and enter the IP addresses of Remote PC.
5. Select *A specific IP Subnet* in the *Destination address*, and enter the IP addresses of Local Network.
6. Uncheck *Mirrored* check box.

Filter Properties

Addressing | Protocol | Description

Source address:

A specific IP Address

IP Address: 210 . 66 . 39 . 2

Subnet mask: 255 . 255 . 255 . 255

Destination address:

A specific IP Subnet

IP Address: 192 . 168 . 2 . 0

Subnet mask: 255 . 255 . 255 . 0

Mirrored. Also match packets with the exact opposite source and destination addresses.

OK Cancel Apply

7. On the **Protocol** tab, leave the protocol type to **Any**. Because IPSec tunnels do not support protocol-specific or port specific filters.
8. On the **Description** tab, you can give a description for this filter.
9. Select **OK**, and then select **Close**.

IP Filter List

An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: Win2K to Security-Router

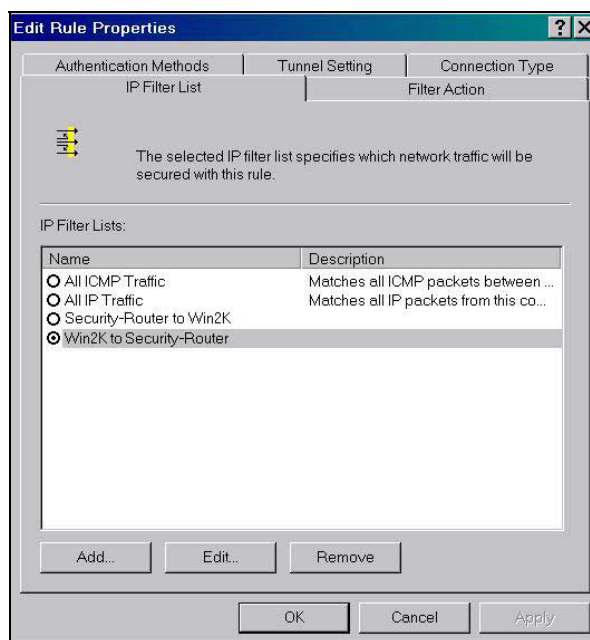
Description:

Filters: Use Add Wizard

M...	Description	Pr...	Sou...	De...	Source DNS Name	Source A...	Source Mask	Destination DNS Na...	Destinati...	Destination Ma...
No	Security-Router...	ANY	ANY	ANY	<A specific IP Address>	210.66.39.2	255.255.255.255	<A specific IP Subnet>	192.168.2.0	255.255.255.0

OK Cancel

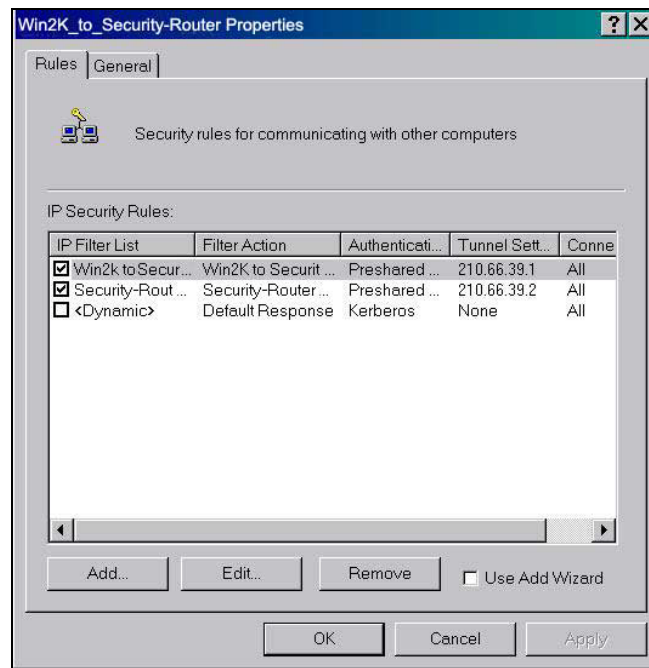
It will create a filter and select the filter we just created.



On **Filter Action** tab, uncheck **Use Add Wizard** check box, and select **Add...**

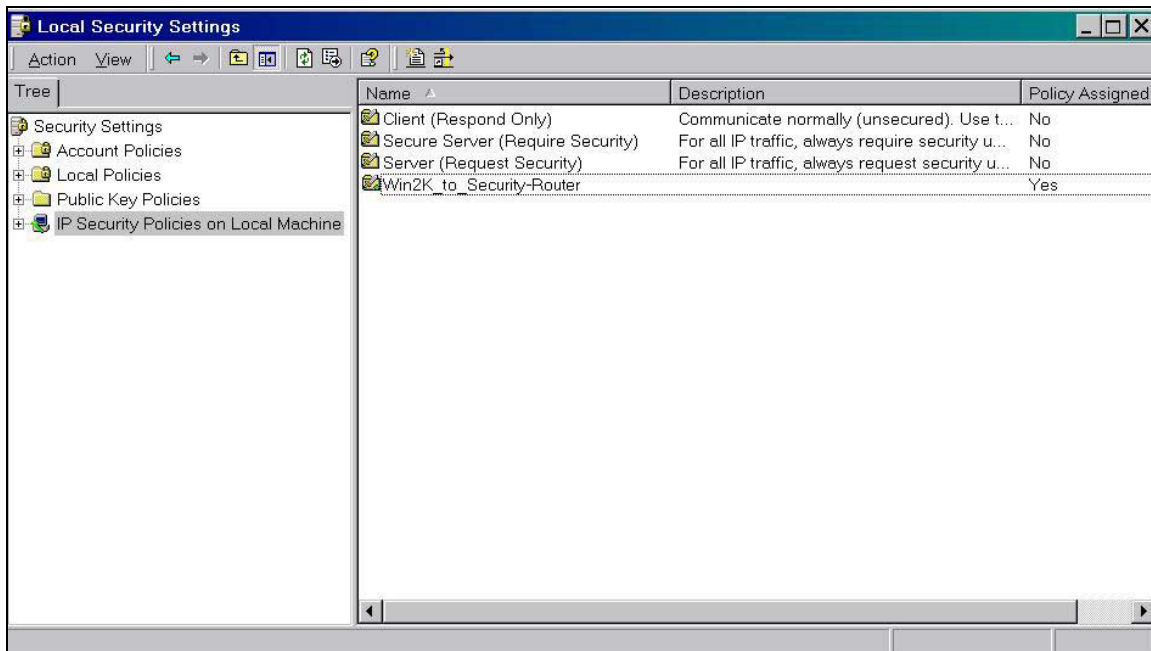
10. Leave **Negotiate security** is checked, and uncheck **Accept unsecured communication, but always respond using IPSec** check box. You must do this to ensure secure connections.
11. Select **Add...**, and select **Custom (for expert users)** if you want to define specific algorithms and key lifetimes. Please make sure the settings match whatever we will configure in Security-Router.
12. Select **OK**, check **Session key Perfect Forward Secrecy** check box if you want to enable PFS function.
13. On **General** tab, give a name to this filter action, for example, Win2K to Security-Router, and select **OK**.
14. Select the filter action you just created.
15. On **Authentication Methods** tab, select **Edit...**, select **Use this string to protect the key exchange (preshared key)** option, and enter the string **12345678** in the text box, select **OK**.
16. On **Tunnel Setting** tab, select **The tunnel endpoint is specified by this IP address**, and enters the WAN IP address of Security-Router (e.g. 210.66.39.1).
17. On **Connection Type** tab, choose the connection type you want to apply this rule.
18. Select **Close**.

It will create a filter rule and check the filter rule we just created.



E. Enable IPSec Policy

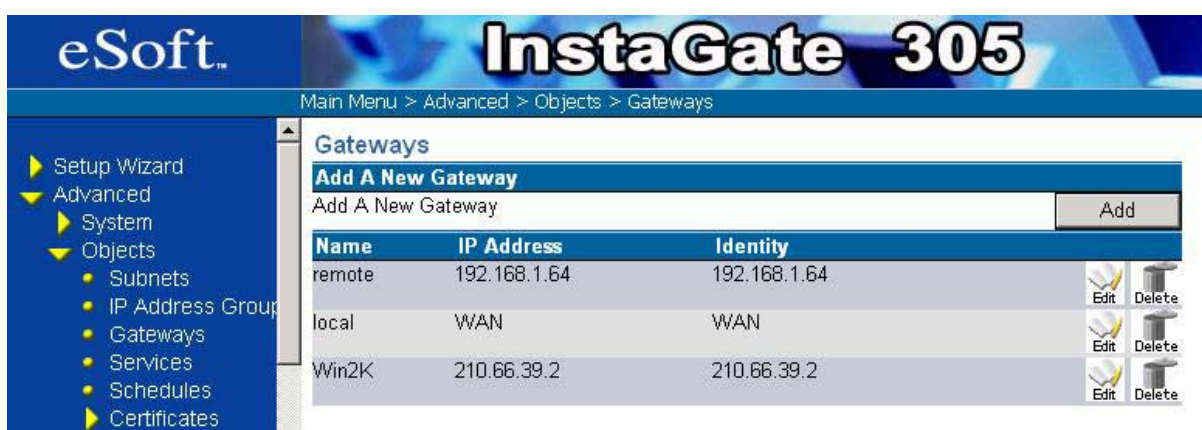
Right-select the IPSec policy we created before and select *Assign* to enable this policy.



II. Setup Security-Router IPSec VPN

1. *Objects*→*Gateways*, select *Add*.
2. Enter name of Gateway, e.g. Security-Router.
3. Select **Local Gateway** ratio and select *WAN* option.
4. Leave *IPv4* ratio is checked, and select *Add*.
5. *Objects*→*Gateways*, select *Add*.
6. Enter name of Gateway, e.g. Win2K.
7. Select **Remote Gateway** ratio and enter the WAN IP address of Win2K client.
8. Leave *IPv4* ratio is checked, and select *Add*.

It will create two Gateway Objects, one for Security-Router itself and the other one for Win2K client.



9. *Main Menu*→*VPN*→*AutoKey(IKE)*, select *New AutoKey Object*.
10. Enter a name for this policy, e.g. Security-Router _Win2K.
11. In **Local Network**, select blank field and enter the IP addresses of Local Network.
12. In **Remote Network**, select blank field and enter the IP addresses of Remote Network.
13. Select **Security-Router** for **Local Gateway** and **Win2K** for **Remote Gateway**.
14. Check **Preshared Key** ratio and enter **12345678** for key and confirm.
15. Check **IPSec Proposal** options to consist to Win2K settings.
16. Leave **IKE SA Lifetime** and **IPSec SA Lifetime** unchanged.
17. Select **Finish**.

eSoft. InstaGate 305

Main Menu > Setup Wizard > Automatic Key VPN

New Automatic Key VPN: Step 1 — Policy Name

Policy Settings

Policy Name

eSoft. InstaGate 305

Main Menu > Setup Wizard > Automatic Key VPN

New Automatic Key VPN: Step 2 — Network Setup

Network Settings

Local Network --Known Network-- /

Remote Network --Known Network-- /

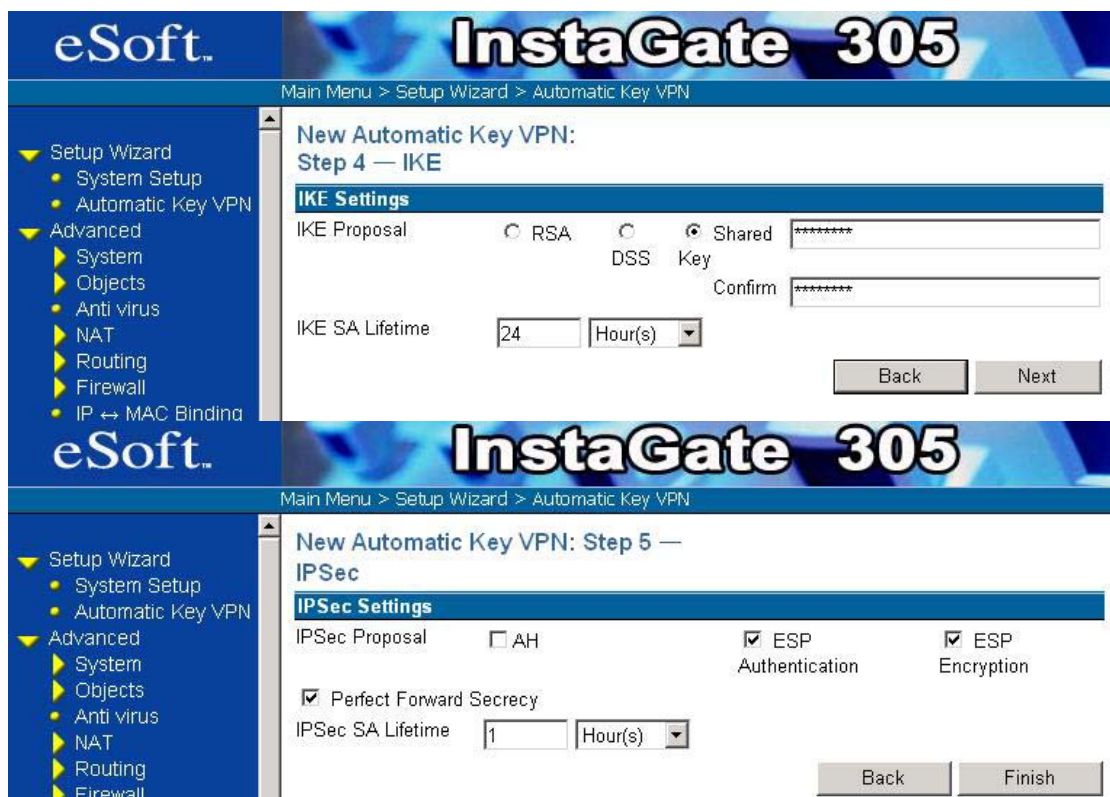
eSoft. InstaGate 305

Main Menu > Setup Wizard > Automatic Key VPN

New Automatic Key VPN: Step 3 — Gateways

Gateway Settings

Local Gateway Remote Gateway



18. Check *Active* for the policy we just created.



Now this InstaGate is ready to build IPsec tunnel with Win2K client.

Appendix B: Win2K PPTP VPN client to the InstaGate

This example guides users to set up a PPTP VPN Tunnel between the Win2K PPTP VPN Client and the InstaGate. As the Figure-1 shown below, Alice want to build a PPTP VPN Tunnel to access the local network through Internet just like she is in the local network. The IP addresses and id/password we use in this example are shown in Figure-2.

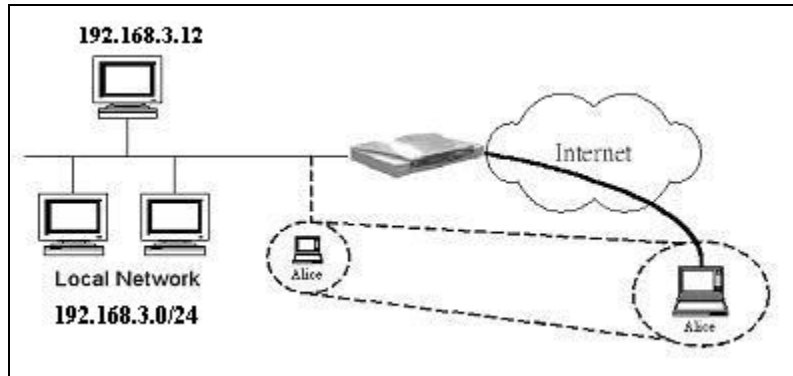


Figure-1

Alice	Security Router
210.66.39.2	WAN: 210.66.39.1
ID: Alice	LAN: 192.168.3.1
PASSWD: Alice	

Figure-2

I. Setup Win2K PPTP VPN Client

A. Create a custom PPTP VPN tunnel

1. Right-select *My Network Places*, and then select *Properties*.
2. Double-select *Make New Connection*.
3. In the *Network Connection Wizard*, select *Next*.
4. Check *Connect to a private network through the Internet* select *Next*.

5. Select *Next*, and then enter *Destination Address* (for the example, 210.66.39.1).
6. Select *Next*, select *Next*, select *Next*, enter *Connection Name* (for example, PPTP_to_Security-Router).
7. Select *Finish*.

After create a custom dial-up tunnel (for the example, the PPTP_to_Security-Router tunnel), Win2K will pop a *Connection* dialog and add a *PPTP_to_Security-Router* icon in the *Network and Dial-up Connections* window. see Figure-3 and Figure-4.



Figure-3

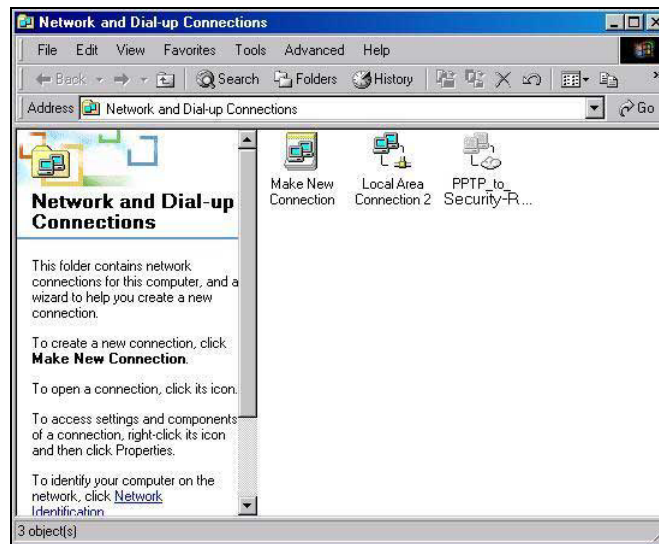


Figure-4

B. Configure the PPTP VPN tunnel

1. Right-select **PPTP_to_Security-Router** in the **Network and Dial-up Connections** window and then select **Properties**, or select **Properties** in the **Connection** dialog. It will pop a dial-up tunnel configuration dialog like Figure-5
2. Select **Security** tab, check **Advanced**, and then select **Settings**.
3. Select **Optional encryption (connect even if no encryption)**, for Logon security, check **Allow these protocols**, enable **Unencrypted password(PAP)** and/or **Challenge Handshake Authentication Protocol(CHAP)**, select **OK**. Shown as Figure-6.
4. Select **Networking** tab, select **Point-to-Point Tunneling Protocol (PPTP)** for **Type of VPN server**, select **OK**. Shown as Figure-7.

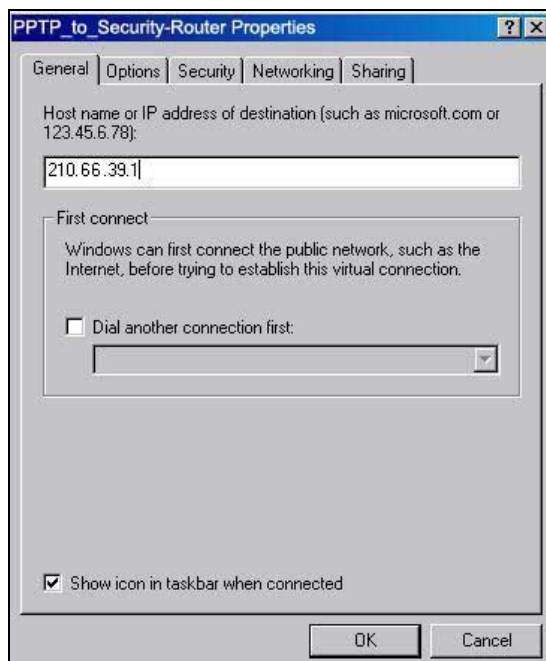


Figure-5

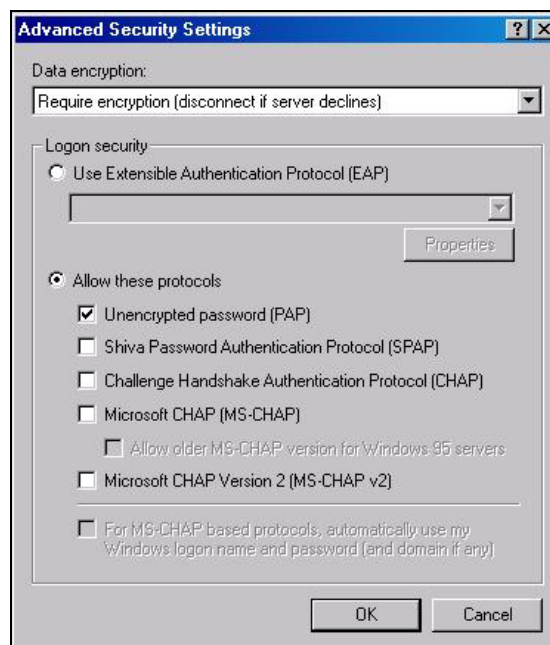


Figure-6

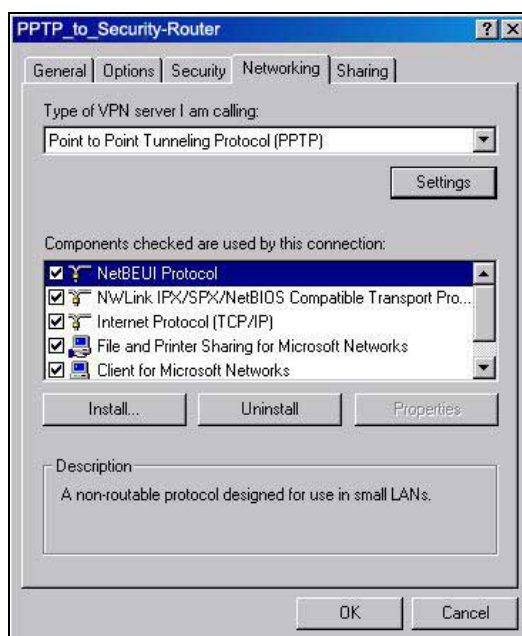


Figure-7

II. Setup Security-Router PPTP VPN Server

1. **Main Menu** → **VPN** → **L2TP/PPTP** → **User Management**, enter Alice's name and password (for the example, Alice/Alice) and the IP address assigned to Alice if you want Alice to use static IP address in the local network. see Figure-8.
2. **Main Menu** → **VPN** → **L2TP/PPTP** → **PPTP Configuration**, select authentication method you wish to use, and set the IP addresses range in local network you want to assign to PPTP Clients.
3. Enable the PPTP Server.

Now Security-Router is waiting for PPTP Clients to build PPTP VPN tunnels.



Figure-8

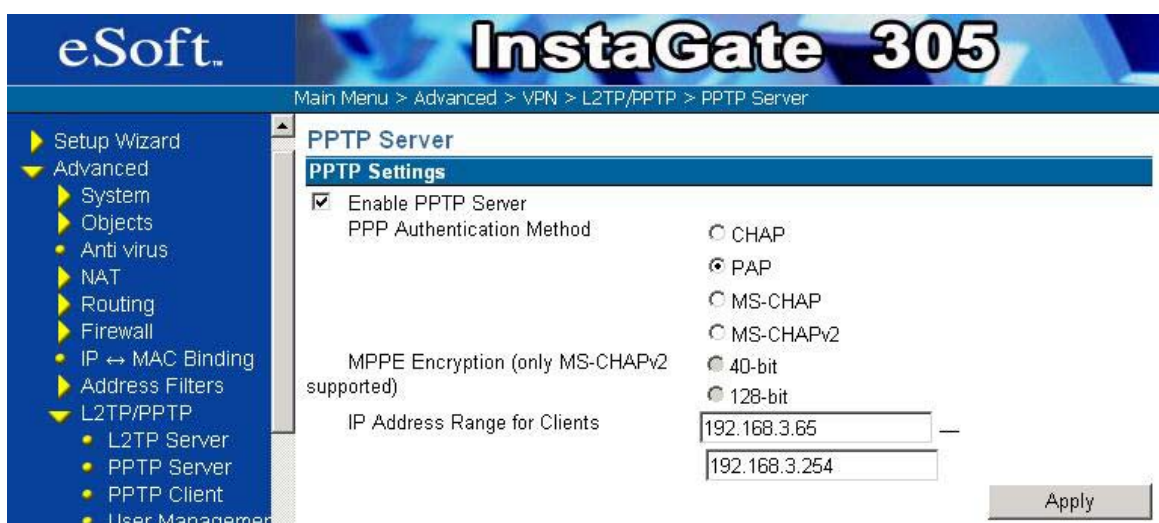


Figure-9

III. Build PPTP VPN Tunnel

From Win2K:

1. *Start*→*Setting*→ *Network and Dial-up Connections* →*PPTP_to_Security-Router*, or Right-select *My Network Places* and select *Properties* and then double-select *PPTP_to_Security-Router*. Win2K will pop a *Connection* dialog.
2. Enter ID and Password (for the example, Alice/Alice).
3. If you want Win2K to save your password, enable *save password*. After you have connected to Security-Router using this L2TP Tunnel, Win2K will save your password.
4. Select *Connection*.

Then Win2K will pop-up message dialogs to show that you are connecting to Security-Router. After connected to Security-Router Win2K will pop-up a success dialog as Figure-10 and Figure-11.



Figure-10



Figure-11

Let's see the final result shown in Figure-12.

```

C:\WINNT\System32\cmd.exe
Ping statistics for 192.168.3.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .                : 210.66.39.2
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : 210.66.39.254

PPP adapter PPTP_to_SG305:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .                : 192.168.3.65
    Subnet Mask . . . . .              : 255.255.255.255
    Default Gateway . . . . .          : 192.168.3.65

C:\>

```

Figure-12

Appendix C: Dynamic DNS with DNS Made Easy

Under the “Main Menu > Advanced > Dynamic DNS” page, you can bind your domain name with a dynamic DNS provider. DDNS providers allow you to associate static hostnames with a dynamic IP address, allowing you to use your dynamically assigned IP address (from your ISP). This reduces the costs associated with static IPs. The InstaGate supports two dynamic DNS providers: Dynamic DNS Network Services <http://www.dyndns.org/> and DNS Made Easy <http://www.dnsmadeeasy.com/>.

Below is an example of setting up a DNS Made Easy account:

Step1 At first, go to the DNS Made Easy website to create your account.

The screenshot shows the DNS Made Easy website homepage. The browser address bar displays <http://www.dnsmadeeasy.com/index.html>. The page layout includes a navigation menu on the left with links for LOG IN, CREATE ACCOUNT, SERVICES / PRODUCTS, PRICES, AFFILIATE PROGRAM, RESOURCES / HELP, POLICIES, ABOUT US, OTHER SERVICES, and HOME. The main content area features a banner with the slogan "Making enterprise services an option for the entire world." and the DNS MADE EASY logo. Below the banner, there are several promotional sections: "Enterprise Mail services" with a list of services and a "Learn more" link; "Premium Membership" with a "Purchase Now!" button; "Enterprise DNS services" with a "Purchase Now!" button; and a "Find out about our products:" section listing various services like Managed DNS, Secondary DNS, Free DNS, Revenue Park, DNS Failover, System Monitoring, POP / IMAP / Webmail, Backup Mail Services, and SMTP Service. The page also includes a "Log In | Create Account" link in the top right corner and a "Create Account >> Compare our prices >>" link in the middle right section.

Step2 Follow the instructions and insert your information.

網址 <https://www.dnsmadeeasy.com/servlet/usermodifycreate>

User Information - Add New User

Instructions:
Please enter your user information.
Your email addresses will be sent a confirmation email. You must verify your email address before you can purchase any products. However you can start using DNS Made Easy's free services immediately.

Username: *

New Password: *

Re-Type New Password: *

First Name: *

Middle Name:

Last Name: *

Email: *

Country: *

If you ever require a password reset over the phone then you must enter in your secret question and answer. We will use this along with other information in your account to verify your identity.

Secret Question:

Secret Answer:

Company Name (if any):

URL (http://):

Step3 After you create your account successfully, the administrator of DNS Made Easy will send you a confirmation email to your email address. Receive this email and enter the confirmation.

DNS MADE EASY

Please enter the correct username and confirmation value.

Email Confirmation

Please enter your username and the confirmation code that was sent to your email.

Username:

Confirmation Code:

Step4 After confirmation, re-login their web site.

網址 http://www.dnsmadeeasy.com/index.html

DNS MADE EASY Log In | Create Account

"Making enterprise services an option for the entire world."

DNS MADE EASY

- LOG IN
- CREATE ACCOUNT
- SERVICES / PRODUCTS
- PRICES
- AFFILIATE PROGRAM
- RESOURCES / HELP
- POLICIES
- ABOUT US
- OTHER SERVICES
- HOME

Enterprise Mail services.
Backup Mail, POP3, IMAP, Webmail, SMTP, Mail Server Forwarding....
Switch to DNS Made Easy to handle all of your email needs and start saving. Most clients are saving over 200% by switching to DNS Made Easy email services.
[Learn more](#)

DNS Made Easy is one of the largest service providers in the world and we are passing the savings directly to you. With years of DNS experience and 100% uptime history there is no wonder why DNS Made Easy is the #1 choice for companies today!
[Create Account »](#)
[Compare our prices »](#)

DNS MADE EASY

Premium Membership

Enterprise DNS!
with 5 Name Servers!
Unbelievable savings!

[Purchase Now!](#)

Enterprise DNS services.
Use our domains for free (Free DNS) or configure enterprise DNS for your

Find out about our products:

- Managed DNS - 100% DNS uptime guarantee
- Secondary DNS - extra DNS redundancy
- Free DNS - free service to help you get started
- Revenue Park - make money with free hosting!
- DNS Failover - never have downtime again
- System Monitoring - enterprise monitoring
- POP / IMAP / Webmail - enterprise email
- Backup Mail Services - email redundancy
- SMTP Service - outgoing email service
- and much more!

• DNS 100% uptime guarantee!
DNS Made Easy is so proud of it's record that we have the best service level agreement in the business. That is why all businesses that require stable DNS decide to use DNS Made Easy. We credit all accounts 500% of the downtime. [View our SLA here.](#)

http://www.dnsmadeeasy.com/0306/prod/secdns.html

DNS MADE EASY

Log In	
Username:	<input type="text" value="testddns"/>
Password:	<input type="password"/>
<input type="button" value="Log In"/>	<input type="button" value="Cancel"/>
Forgot your password? click here	

Step5 After you login successfully, you need to register a dynamic domain name. Select "DNS Made Easy Domains".

DNS MADE EASY

User: jake peng (testddns) IP: 210.66.39.100

Main Menu	News
<p>Managed DNS Manage your DNS for your own domain. Configure enterprise primary and secondary DNS for your domain.</p> <p>Advanced DNS Settings Create record sets, SOA records, or allow additional systems to allow transfer for your domains.</p> <p>Secondary DNS If you already have a primary DNS server and you just need extra redundancy.</p> <p>Revenue Park Service Configuring and reporting your Revenue Park sites. Free hosting, free advertising, and we pay you!</p> <p>Mail Services Configuring POP accounts, mail account forwarding, mail server forwarding, and backup mail servers.</p> <p>DNS Made Easy Domains Use our own domains for free to get your website online fast. All domains include free HTTP redirection.</p> <p>Affiliate Program View your stats for your account or create a link to start making money today.</p> <p>Support Center Fill out a trouble ticket if you have problems or questions.</p> <p>Modify User Information Manage your personal information in DNS Made Easy.</p> <p>Purchase / Upgrade / Renew Upgrade your account or purchase new products.</p> <p>Log Off</p>	<p>Revenue Park Service The Revenue Park Service has been opened to the public. Start making money from your unused domains today! Many users are now earning over \$100 per day on their unused domains. These are the largest payouts on the net. Click here for more information.</p> <p>New Support Center Submit your trouble ticket or view our collection of already answered questions at http://support.dnsmadeeasy.com Click here for more information.</p> <p>Domains Made Easy To celebrate the release of the new services by DNS Made Easy, Domains Made Easy has slashed all prices on domain registrations. COM registrations are as low as \$7.75! This is a limited time special so renew or sign up for your domains today! Click here for more information.</p>

Step6 Select the “Add Record” button

DNS MADE EASY

DNS Made Easy Domains

Instructions:
To add a new record select the appropriate domain and record type. Click on the “Remove” link for that record to remove it from the system. Click on the record name to change the values for that record.

Tips and Tutorials:
[What are these different record types?](#)
[What are DNS Made Easy domains?](#)

Domain: <input type="text" value="easydns.us"/>	<input type="button" value="Main Menu"/>
Record Type: <input type="text" value="A"/>	<input type="button" value="Add Record"/>

Name	Value	Rec. Type
There are no DNS Made Easy records configured.		
<input type="button" value="Main Menu"/>		

Step7 Insert the name of the DDNS, for example “testddns.easydns.us”. Next, insert the IP address of the InstaGate’s WAN interface. You can use the default value of TTL (1800 seconds). Last, select “Continue” and select the “Yes” button.

WAN Interface	Interface Type	PPPoE
	IP address	218.168.135.247
	Default gateway	218.168.128.254
	First DNS	168.95.192.1
	Second DNS	168.95.1.1
	MTU	1492
	RX Bytes	536483
	TX Bytes	275934
	PPTP Client	Disconnected

DNS MADE EASY

Record Management - DNSME Domain easydns.us

A (Address) Record

Instructions:
Enter the name of the record. Leave it blank if you want to create the root record.
Enter the IP of the record. If your record is on a dynamic IP then you want to enter your current IP address.
Enter the TTL of the record.
Check the Dynamic DNS box if you want the record to be updated by the Dynamic DNS clients.

Tips and Tutorials:
[What is an A record?](#)
[What is a wildcard record?](#)
[How do I know my IP address?](#)
[What is a TTL \(time to live\)?](#)

? Name: .easydns.us.

? IP:

? TTL: (seconds)

? Dynamic DNS:

Review of your configuration.

Your record **testddns.easydns.us.**
will point to IP **218.168.135.247**
and will cache for **1800** seconds.

Step8 Select the “DDNS ID” then it will show the Record ID of the “testddns.easydns.us”. Please write this information down.

DNS MADE EASY

Record modification request canceled.

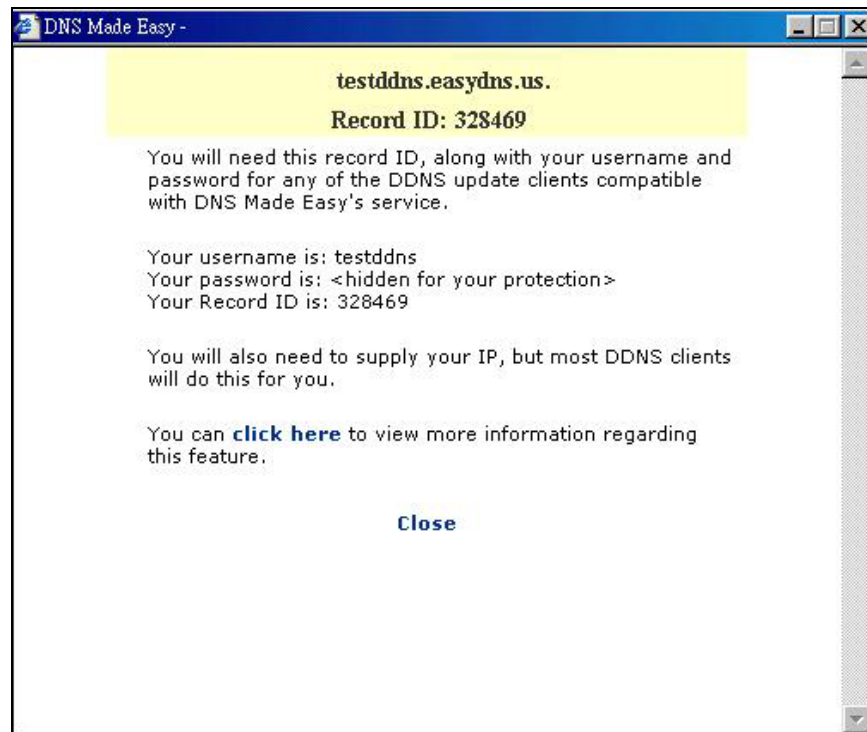
DNS Made Easy Domains

Instructions:
 To add a new record select the appropriate domain and record type.
 Click on the "Remove" link for that record to remove it from the system.
 Click on the record name to change the values for that record.

Tips and Tutorials:
[What are these different record types?](#)
[What are DNS Made Easy domains?](#)

Domain: <input type="text" value="easydns.us"/>	<input type="button" value="Add Record"/>	<input type="button" value="Main Menu"/>
Record Type: <input type="text" value="A"/>		

Name	Value	Rec. Type
testddns.easydns.us.	218.168.135.247	A-DDNS ID Remove



Step9: Set up the configuration of DDNS under the “Main Menu > Advanced > Dynamic DNS” page.

(Please ensure that you have clicked the “Enable” checkbox, and selected the DNS Made Easy option in the pull-down menu)



Figure 144: Dynamic DNS Settings

Last, you select the “Apply” button. If the InstaGate gets the new dynamic IP, it will update the IP information to “DNS Made Easy” automatically. You can see the update information under the “Main Menu > Advanced > Status > System Log” page.

May 20 07:41:14	pppd[249]	[SGLOG5] primary DNS address 168.95.192.1
May 20 07:41:14	pppd[249]	[SGLOG5] secondary DNS address 168.95.1.1
May 20 07:41:14	pppd[249]	[SGLOG7] Script /etc/ppp/ip-up started (pid 301)
May 20 07:41:17	dns[329]	[SGLOG6] using nameserver 168.95.1.1 port:53
May 20 07:41:17	dns[329]	[SGLOG6] using nameserver 168.95.192.1 port:53
May 20 07:41:19	IKE[335]	[SGLOG6] IKE (v1.0) task start
May 20 07:41:23	ddns	[SGLOG6] 218.168.135.247: The one and only good message.
May 20 07:41:23	pppd[249]	[SGLOG7] Script /etc/ppp/ip-up finished (pid 301), status = 0x0

Figure 145: Dynamic DNS Log Entry

Appendix D: Documentation License

The software included in this device is licensed under the license of MontaVista Linux which is subject to several public licenses, including the Free Software Foundation's GNU General Public License (the "GPL") and its own proprietary licenses. Attached is the GPL license text for your reference.

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
Place, Suite 330, Boston, MA 02111-1307 USA

59 Temple

(Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.)

Preamble:

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights. We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by

someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contain a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".
Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.
2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
 - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
 - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.
4. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you, rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

You may copy and distribute the Program (or a work based on it under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code,

to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange or,

- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you have received the program in form of objects code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
8. If as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this

License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system, it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program are restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

12. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

13. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.