

# Netfee Installation

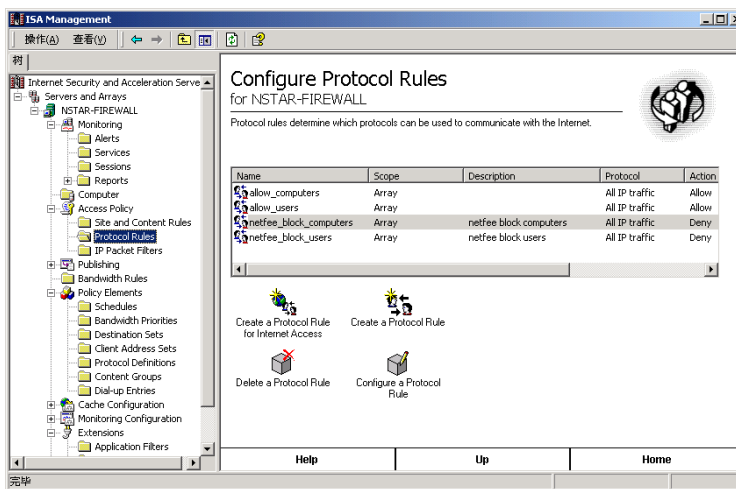
## 1. Confirm the settings of firewall

Check firewall's settings.

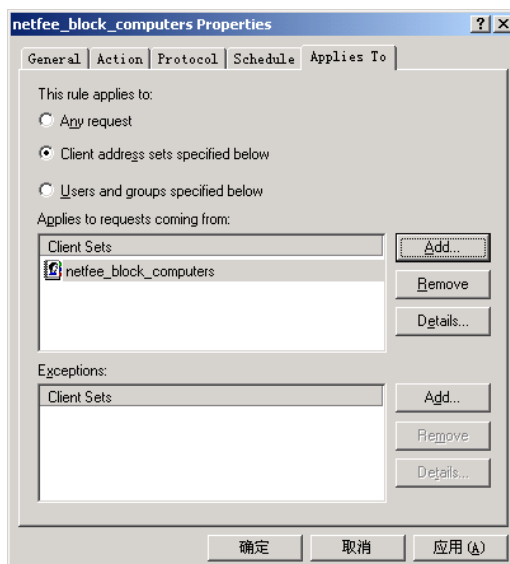
### 1.1 ISA Server 2000

Run "ISA Server 2000 mangmenet".

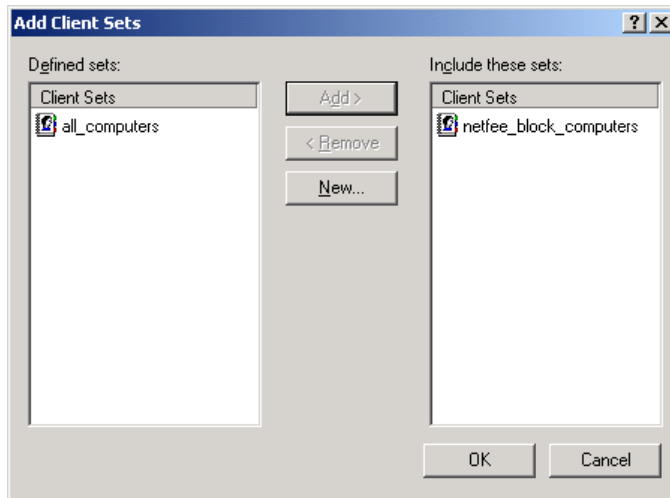
Choose "Access Policy / Protocol Rule", the two rules of "netfee\_block\_users" and "netfee\_block\_computers" are added by netfee.



Select "netfee\_block\_computers", and run "Configure a Protocol Rule".

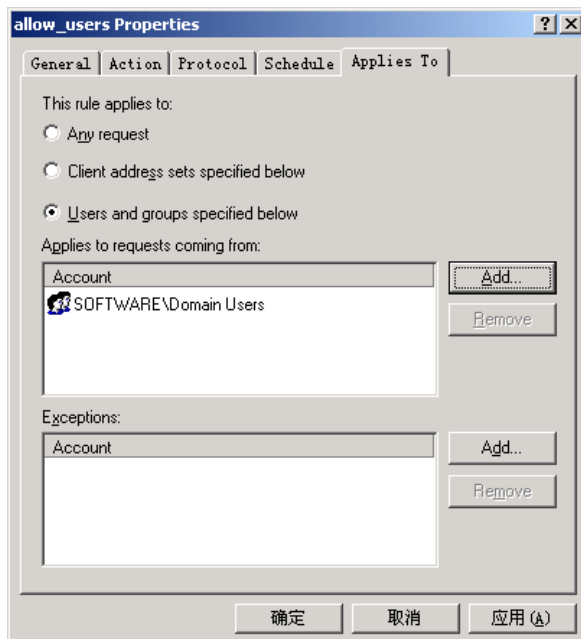


Click "Add" button, add "netfee\_block\_computers" from "Defined sets" to "Include these sets".



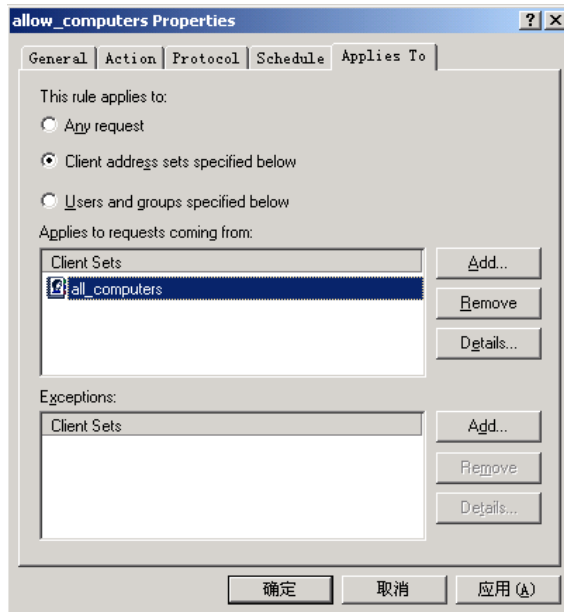
### 1.1.1 Admin by user E

If you want to admin in user mode, add Protocol Rule in "Access Policy/Protocol Rule". Select "Users and groups specified below" in "Applies To" and add users into list "Applies to request coming from".



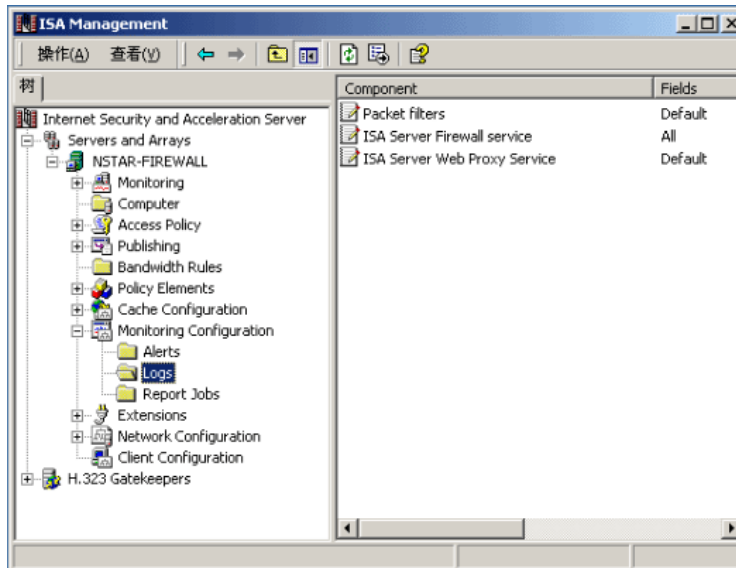
### 1.1.2 Admin by computers E

If you want to admin in computers mode, add Protocol Rule in "Access Policy/Protocol Rule". Select "Client address set specified below" in "Applies To" and add computers into list "Applies to request coming from".

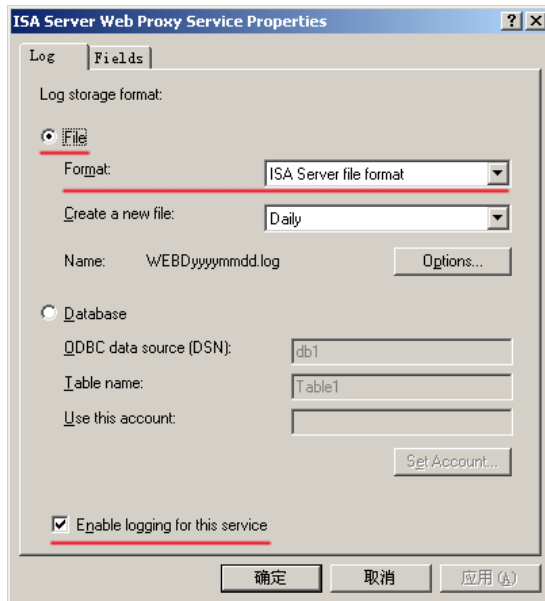


### 1.1.3 Log settings

Select "Monitoring Configuration/Logs".



Select "ISA Server format" or "W3C extended log file format" as format of Web Proxy, Firewall and Packet filter.



## Follow Fields should be included in Log files

- **Web Proxy Service:**

- Client
- Client user name
- Date
- Time
- Destination name
- Destination port
- Processing time
- Bytes sent
- Bytes received
- Protocol name
- Object name

- **Firewall service:**

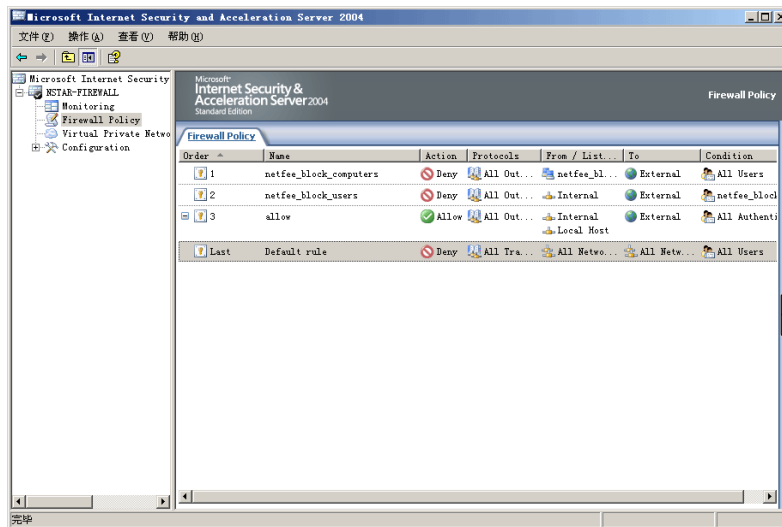
- Client IP
- Client user name
- Client agent
- Date
- Time
- Destination IP
- Destination port
- Processing time
- Bytes sent
- Bytes received

## 1.2 ISA Server 2004(2006) standard edition

### 1.2.1 Netfee policy **E**

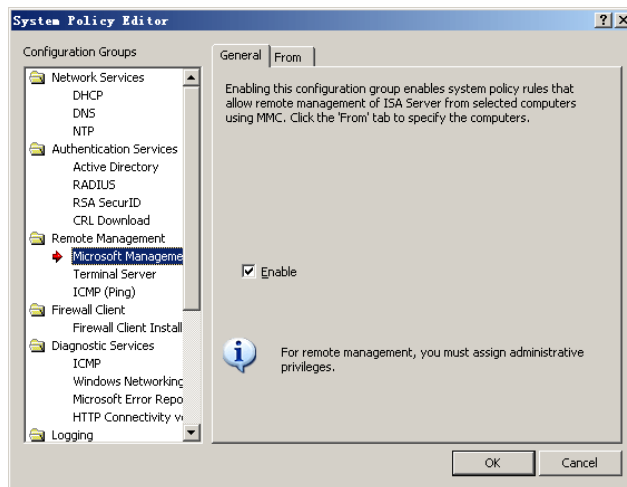
Run "ISA Server Management", select "Firewall policy". there will have two rules "netfee\_block\_users" and "netfee\_block\_computers". The two rules are created by netfee. Refer to **Netfee manual "7.1 Connect to firewall"**.

⊗ The two rules must be at the top position of rule list.



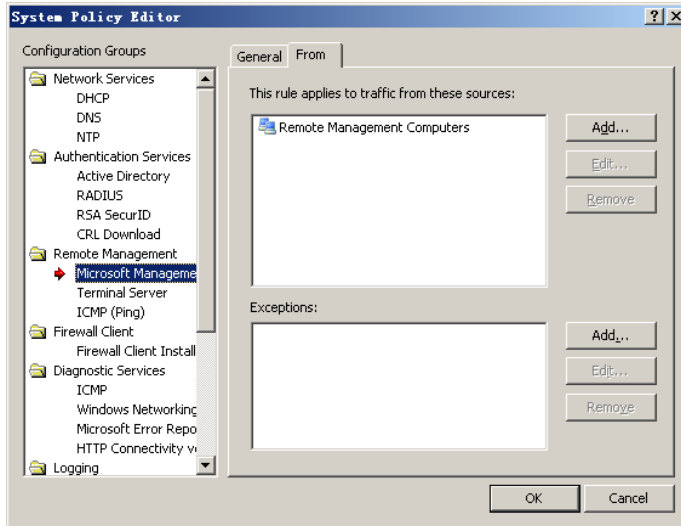
### 1.2.2 Remote management **E**

Netfee can run at local or at remote computer. When Netfee running at remote computer, need to do some settings to ISA server. Right-click on "Firewall Policy", run "Edit System Policy".

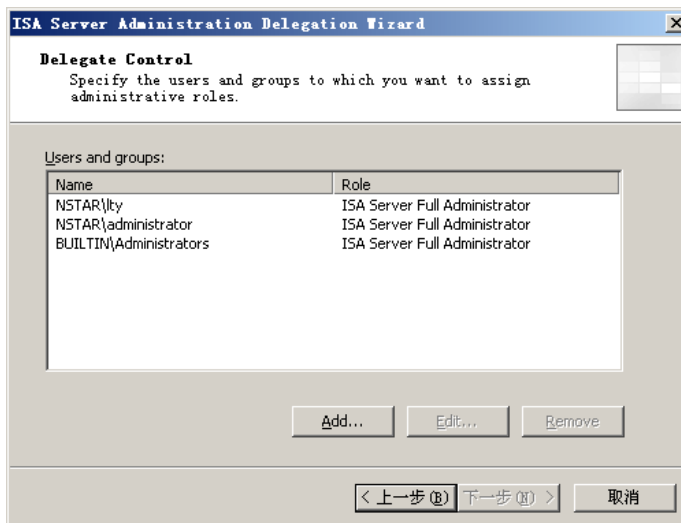


Run "Remote Management/Microsoft Management Console", put a tick in the checkbox in this option to enable it.

In the **FROM** tab you can specify one or more computers you would like to be enable Remote Administration from.

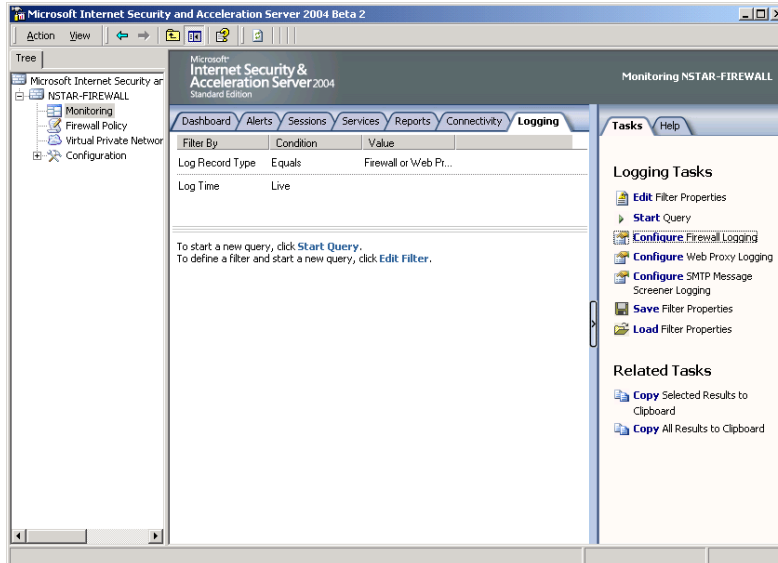


In the "Configuration/General" node choose "Administration Delegation". From there you can add or edit your firewall administrators.

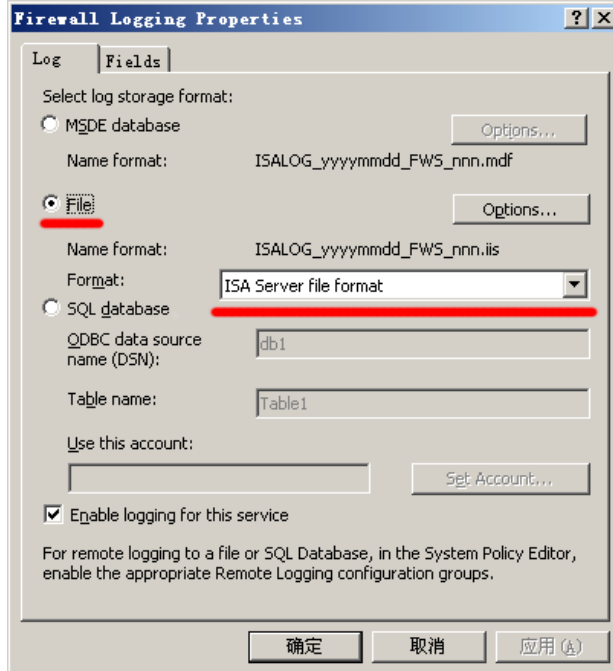


### 1.2.3 Logs

Click on "Monitoring", Select "Configure Firewall Logging" and "Configure Web proxy Logging".



Select "ISA Server file format" or "W3C extended log file format" as the format of log files of Firewall.



## Follow Fields should be included in Log files

- **Web Proxy Service:**

- Client IP
- Client user name
- Date
- Time
- Destination name
- Destination port
- Processing time
- Bytes sent
- Bytes received
- Protocol name
- Object name

- **Firewall service:**

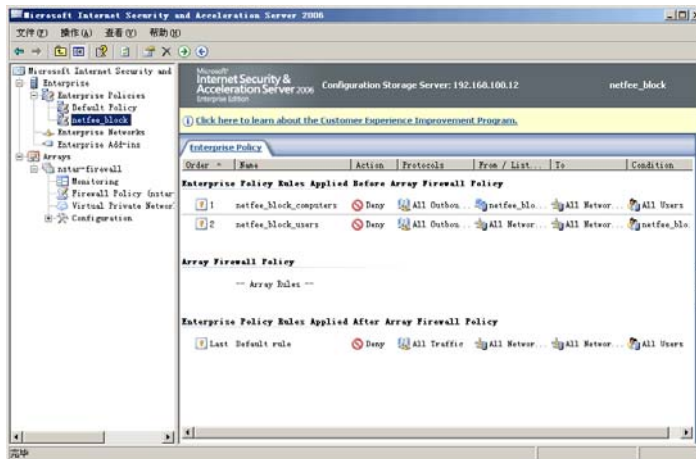
- Date
- Time
- Source
- Destination
- Result code
- Bytes sent
- Bytes received
- Connection time
- Client user name
- Client agent

## 1.3 ISA Server 2004 (2006) enterprise edition

### 1.3.1 Netfee enterprise policy E

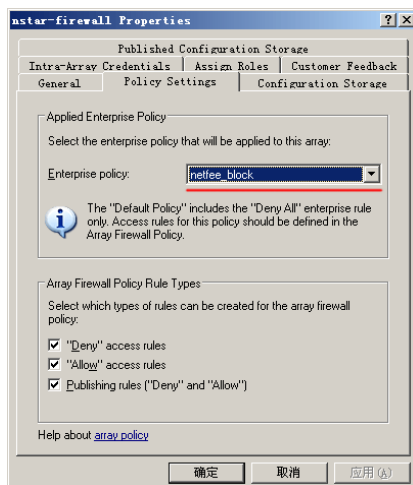
In the console tree of ISA Server Management, click on "Enterprise Policies". there will have a Enterprise Policy that contains two rules "netfee\_block\_users" and "netfee\_block\_computers". The two rules are created by netfee. Refer to **Netfee manual "5.3.4 Connect to firewall"**.

⊗ The two rules must be at the top position of rule list.



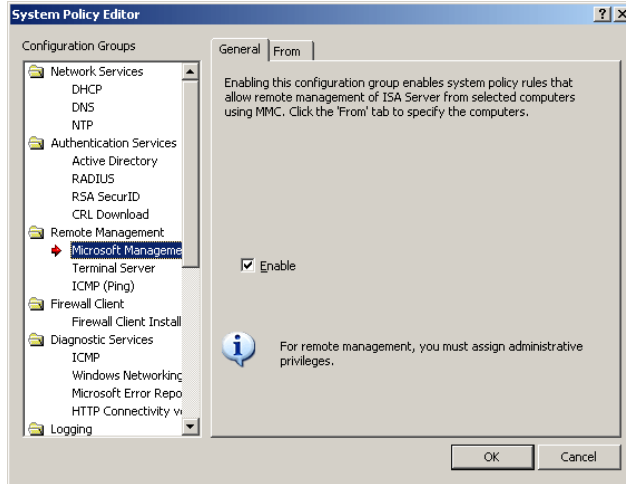
E The enterprise policy that contains the two rules should be applied to firewall array.

In the console tree of ISA Server Management, right-click "array name". Click "Properties", on the "Policy Settings", select the enterprise policy that contains the two rules to apply this array.



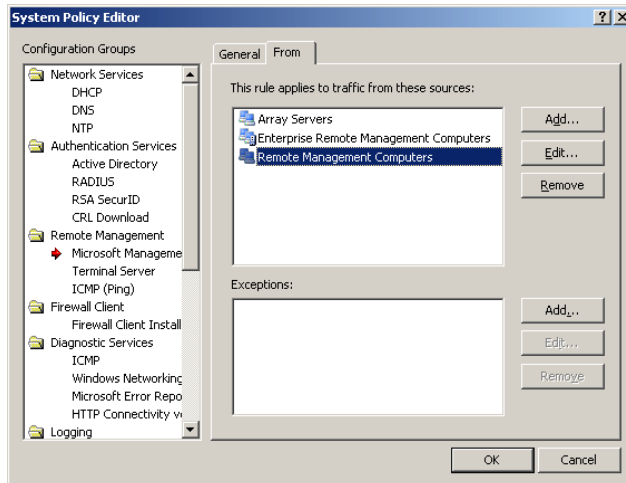
### 1.3.2 Remote management E

Netfee can run at local or at remote computer. When Netfee running at remote computer, need to do some settings to ISA server. Right-click on "Firewall Policy", run "Edit System Policy".



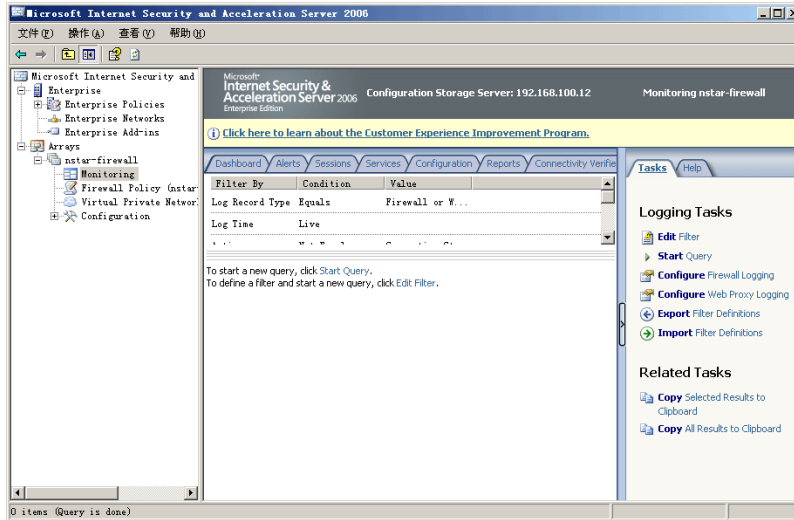
Run "Remote Management/Microsoft Management Console", put a tick in the checkbox in this option to enable it.

In the **FROM** tab you can specify one or more computers you would like to be enable Remote Administration from.

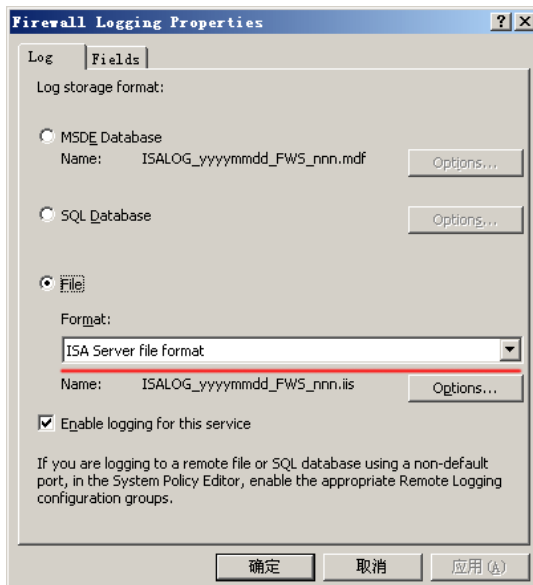


### 1.3.3 Logs

Click on "Monitoring", Select "Configure Firewall Logging" and "Configure Web proxy Logging".



Select "ISA Server file format" or "W3C extended log file format" as the format of log files of Firewall.



## Follow Fields should be included in Log files

- **Web Proxy Service:**

- Client IP
- Client user name
- Date
- Time
- Destination name
- Destination port
- Processing time
- Bytes sent
- Bytes received
- Protocol name
- Object name

- **Firewall service:**

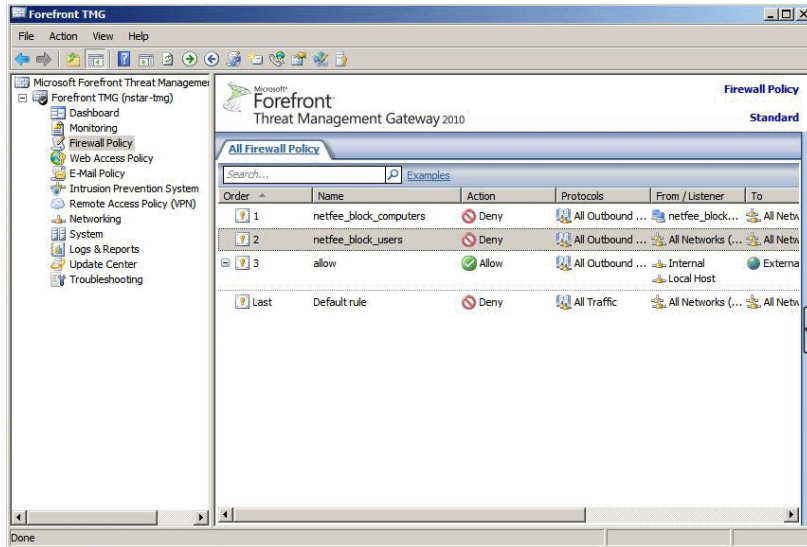
- Date
- Time
- Source
- Destination
- Result code
- Bytes sent
- Bytes received
- Connection time
- Client user name
- Client agent

## 1.4 TMG Server 2010 standard edition

### 1.4.1 Netfee policy **E**

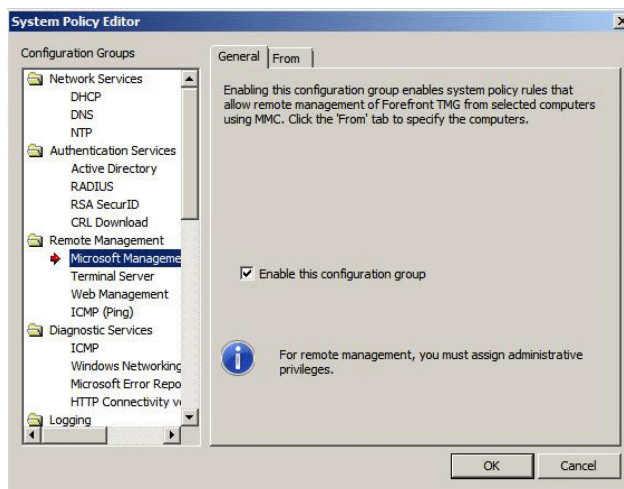
Run "TMG Server Management", select "Firewall policy". there will have two rules "netfee\_block\_users" and "netfee\_block\_computers". The two rules are created by netfee. Refer to "7.1 Connect to firewall".

⊗ The two rules must be at the top position of rule list.



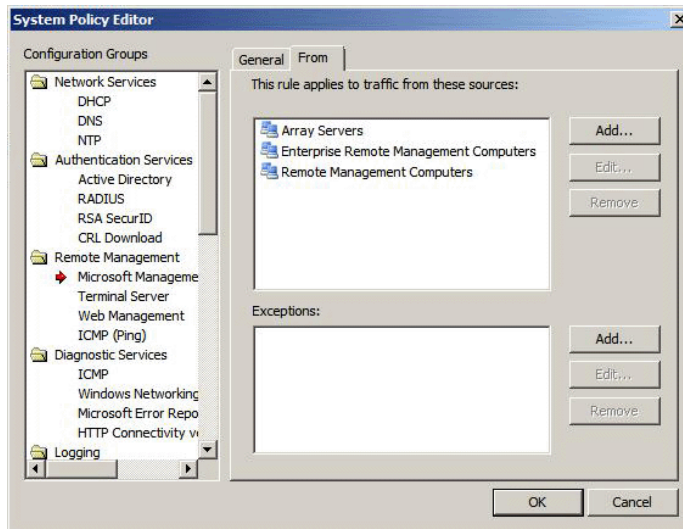
### 1.4.2 Remote management **E**

Netfee can run at local or at remote computer. When Netfee running at remote Access Policy computer, need to do some settings to TMG server. Click on "Firewall Policy", run "Edit System Policy".



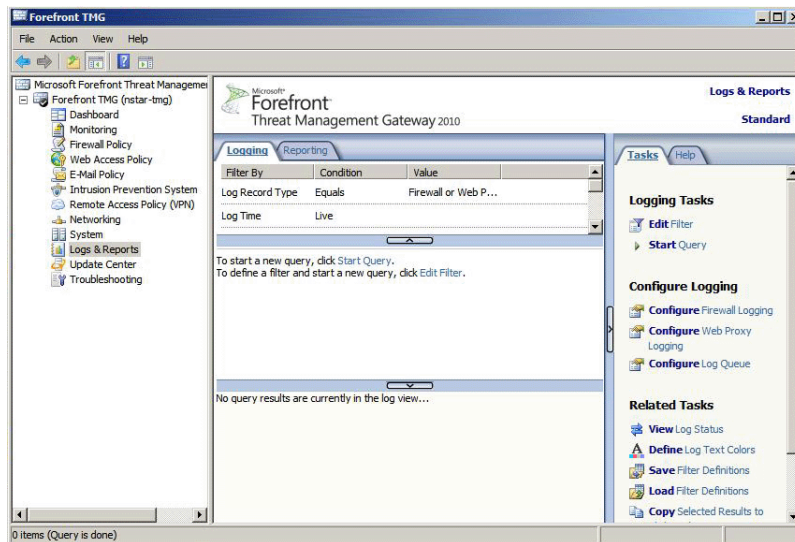
Run "Remote Management/Microsoft Management Console", put a tick in the checkbox in this option to enable it.

In the **FROM** tab you can specify one or more computers you would like to be enable Remote Administration from.

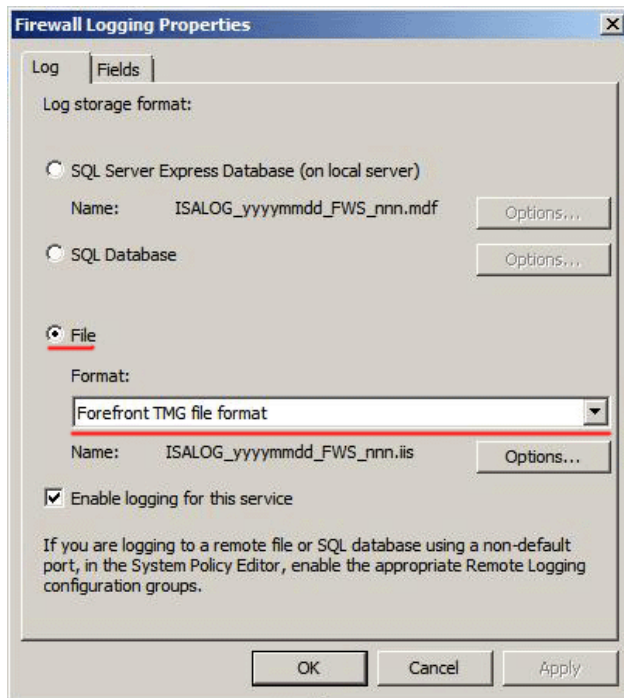


### 1.4.3 Logs

Click on "Logs & Report", Select "Logging" and "Configure Web proxy Logging".



Select "**Forefront TMG file format**" or "**W3C extended log file format**" as the format of log files of Firewall.



### Follow Fields should be included in Log files

- **Web Proxy Service:**

- Client IP
- Client user name
- Date
- Time
- Destination name
- Destination port
- Processing time
- Bytes sent
- Bytes received
- Protocol name
- Object name

- **Firewall service:**

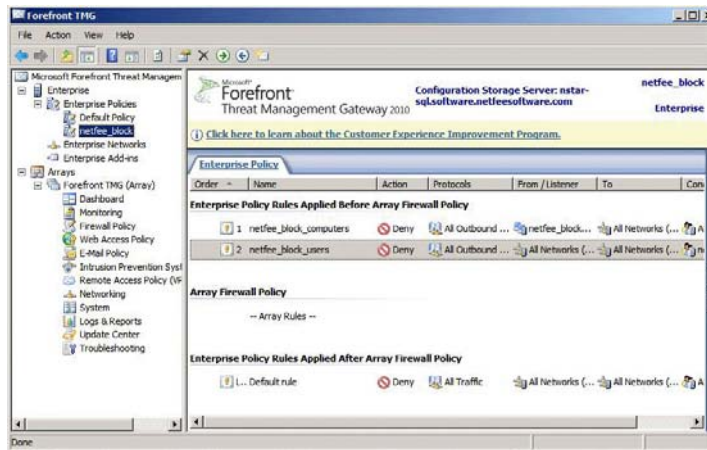
- Date
- Time
- Source
- Destination
- Result code
- Bytes sent
- Bytes received
- Connection time
- Client user name
- Client agent

## 1.5 TMG Server 2010 enterprise edition

### 1.5.1 Netfee enterprise policy E

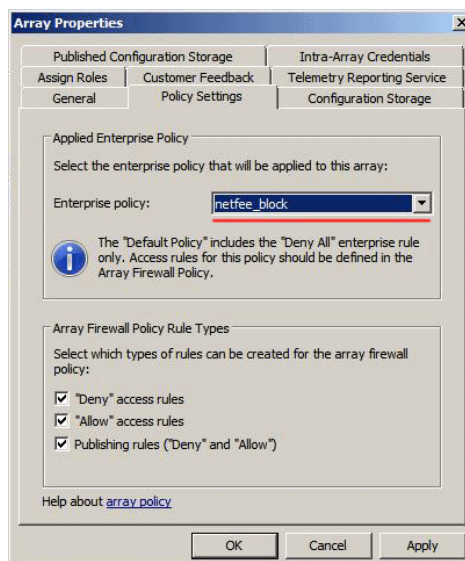
In the console tree of TMG Server Management, click on "Enterprise Policies". there will have a Enterprise Policy that contains two rules "netfee\_block\_users" and "netfee\_block\_computers". The two rules are created by netfee. Refer to "**7.1 Connect to firewall**".

⊗ The two rules must be at the top position of rule list.



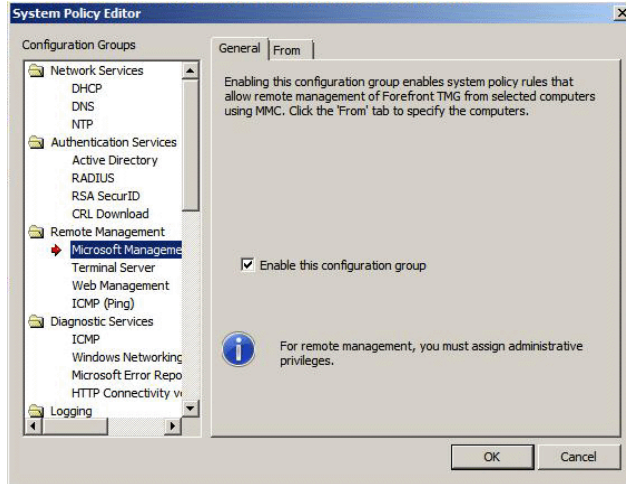
E The enterprise policy that contains the two rules should be applied to firewall array.

In the console tree of TMG Server Management, right-click "array name". Click "Properties", on the "Policy Settings", select the enterprise policy that contains the two rules to apply this array.



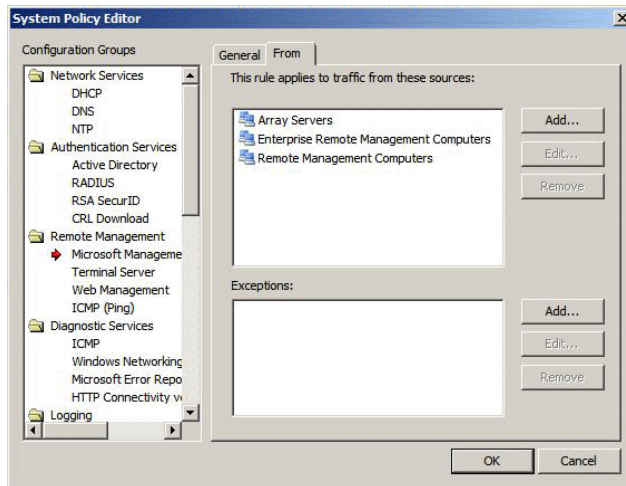
## 1.5.2 Remote management E

Netfee can run at local or at remote computer. When Netfee running at remote computer, need to do some settings to ISA server. Click on "Firewall Policy", run "Edit System Policy".



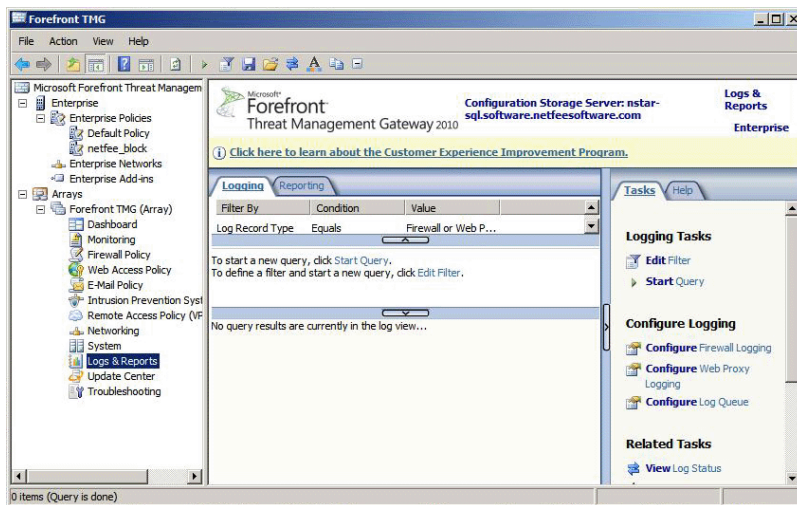
Run "Remote Management/Microsoft Management Console", put a tick in the checkbox in this option to enable it.

In the **FROM** tab you can specify one or more computers you would like to be enable Remote Administration from.

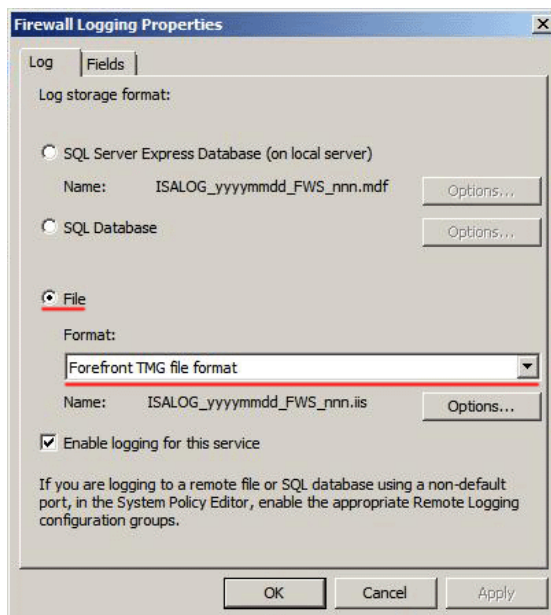


### 1.5.3 Logs

Click on "Logs & Report", Select "Logging" and "Configure Web proxy Logging".



Select "Forefront TMG file format" or "W3C extended log file format" as the format of log files of Firewall.



## Follow Fields should be included in Log files

- **Web Proxy Service:**

- Client IP
- Client user name
- Date
- Time
- Destination name
- Destination port
- Processing time
- Bytes sent
- Bytes received
- Protocol name
- Object name

- **Firewall service:**

- Date
- Time
- Source
- Destination
- Result code
- Bytes sent
- Bytes received
- Connection time
- Client user name
- Client agent

## 1.6 WinRoute 6.0

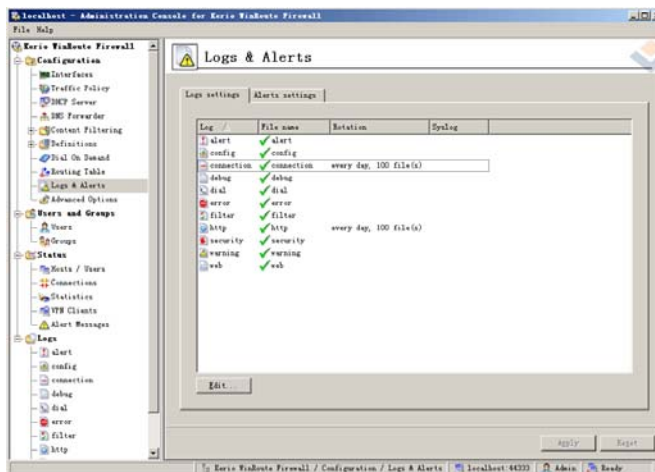
At "Administration console", select "Configuration/Traffic policy".



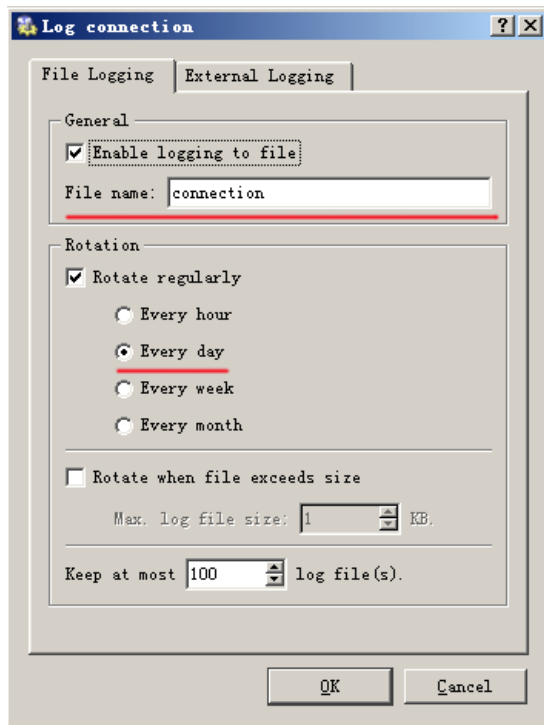
Edit each rules,run "Log matching connections" to produce logs.



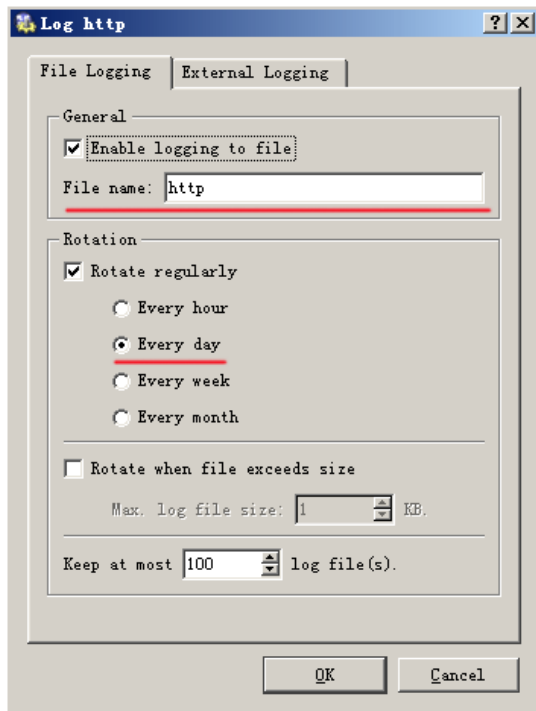
At "Administration console",Select "Configuration / Logs & Alerts / Logs settings".



Edit "Connection" settings. Select "Enable logging to file", and fill "File name" with "connection". Set "Rotation/Rotate regularly" to "Every day".

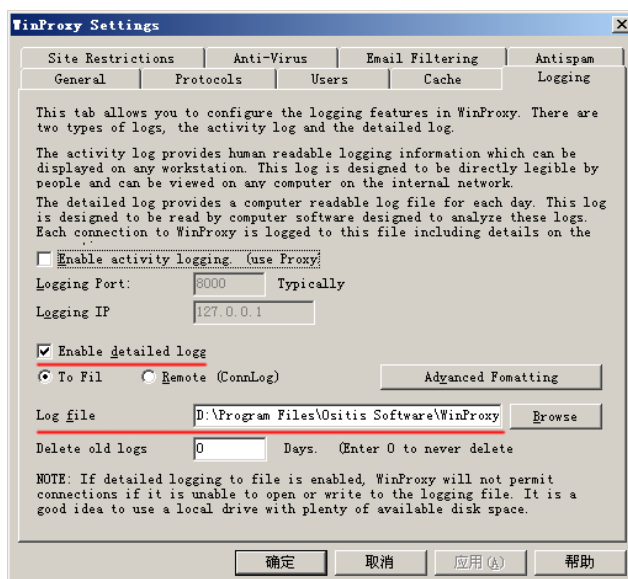


Edit "Http" settings. Select "Enable logging to file", and fill "File name" with "http". Set "Rotation/Rotate regularly" to "Every day".



## 1.7 WinProxy 5.1

Run "File / Settings / Logging", select "Enable detailed logging".



## 2. Installation

### 2.1 Install ISA(TM)G server Management

Netfee can run at local or at remote computer. When Netfee running at remote computer, need to install ISA(TM)G server Management at the computer running netfee.

Firstly you should configure firewall for remote administration. Refer to "**4.2.2 (4.3.2) Remote management**".

Then can install "ISA(TM)G server Management" onto the computer to netfee. To do this we use the ISA(TM)G Server CD. Just run the setup the usual way on the local computer, however, when you get to the menu options you should choose "Custom Setup". In the Custom Setup you should choose only the ISA(TM)G Server Management and hit "Next". The necessary files will be installed and you will be on your way to remote admin.

### 2.2 Install SQL server express

If want to save data to SQL server express, must install "SQL server express". Can download "SQL server express" from mictosoft website..

 **For 64-bits netfee, must install "SQL server express".**

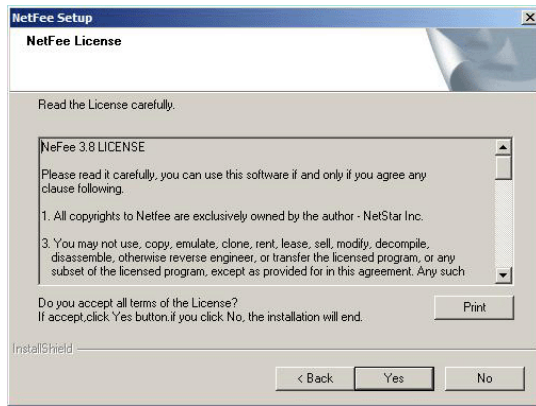
### 2.3 Install Excel

If want to output in excel, must install Excel.

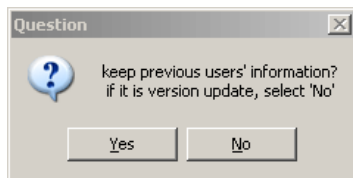
### 2.4 Install Netfee

Run Netfee.exe in install disk

First License agreement appears, if you accept the clauses listed in it, click "**Yes**", otherwise, click "**No**", exit.



Then select the install location of NetFee, click **"next"**  
If it is not first time to install netfee, system will query "keep previous users' information"?



If select "Yes", system will keep all previous users information.  
If select "No", after finish installation and Start NetFee, run **"File/Restore user information"** to restore user information backed up previously.

**⊘ If update netfee to a new version, must select "No".**

After installation finished, you can select to run immediately. You also can run **"Start/programs/NetFee/NetFee"** for the first use.

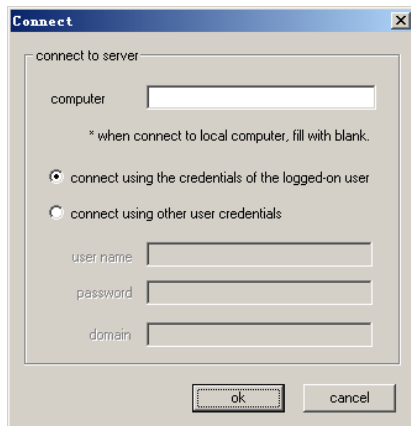
When netFee run, an icon will shown at low-right corner of screen.

## 2.5 Initial running the system

### 2.5.1 Connect

Netfee management connect to netfee service. About netfee service, refer to **Netfee manual "6.1 Netfee service"**.

Run "File/Connect", Connect window appears..

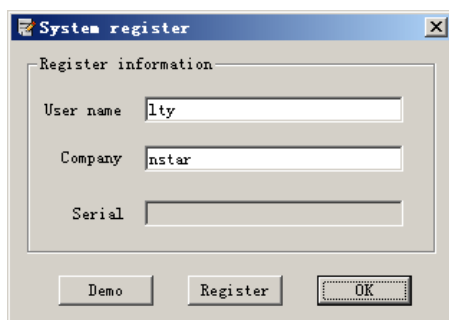


If Netfee service running on another computer, input address of computer running netfee service at the "**computer**".

If Netfee service running on local, leave Blank, or input "." or "Local" at the "**computer**".

### 2.5.2 Register

Run "Help/Register", system registry window appears.



If you want to use DEMO edition of NetFee, Click "DEMO"

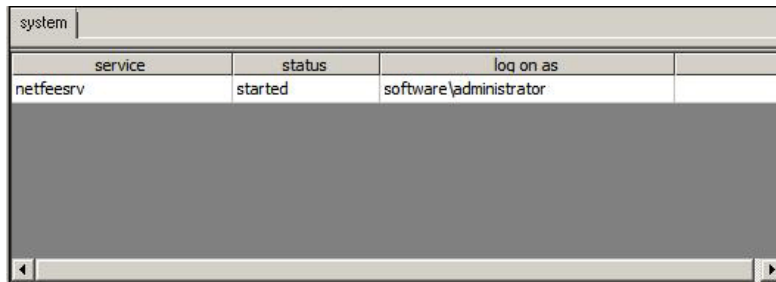
If you are a legal user, click "**register**", "System register" window appears. Input your register information.

 For DEMO edition, period of validity is 60 days (from installation).

### 2.5.3 Netfee service E

Netfee(Enterprise edition) can be run as service.

At "**Manage pane**" of netfee, click "system". Then will show status of netfee service (netfeesrv) at right pane. Right click on it, can "**start**" or "**stop**" netfee service.



The screenshot shows a window titled "system" containing a table with the following data:

service	status	log on as
netfeesrv	started	software\administrator

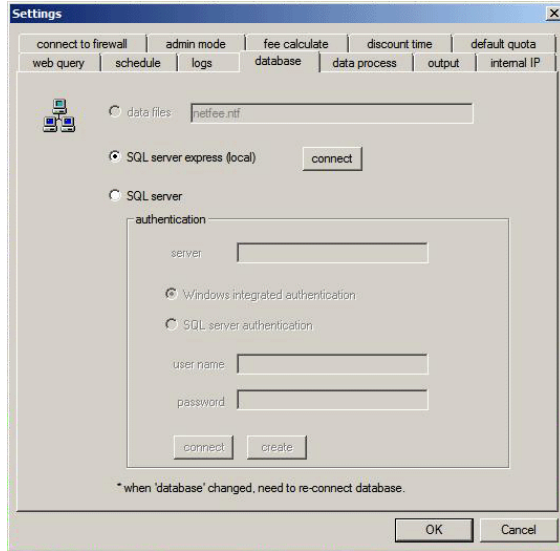
### 2.5.4 Database

When run netfee, system will connect database automatically. The default database is data file - **netfee.ntf** (at "../programe files/netfee").

⊘ If the number of users or computers is more than 100, suggest using Sql server or Sql server express as database.

E If you want to select "SQL server" as database, you should create database firstly.

Run "**Tools/Settings/Databse**", fill in the address of SQL server, user name and password, then click "**Create**".

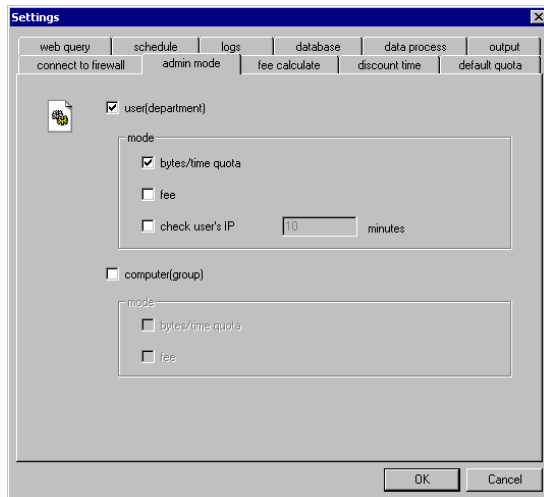


⊘ The user to create database must have "Create database" priority to the SQL server.

After database is created, you can specify another user to connect database. The user doesn't have to own the "Create database" priority.

### 2.5.5 Select admin mode

You can select admin mode to admin users and computers. Refer to "7.2 Admin mode".



### 2.5.6 Add user/computer

"Add department", refers to **Netfee manual "8.1.1 Add department"**.

"Add user", refers to **Netfee manual "8.2.1 Add user"**.

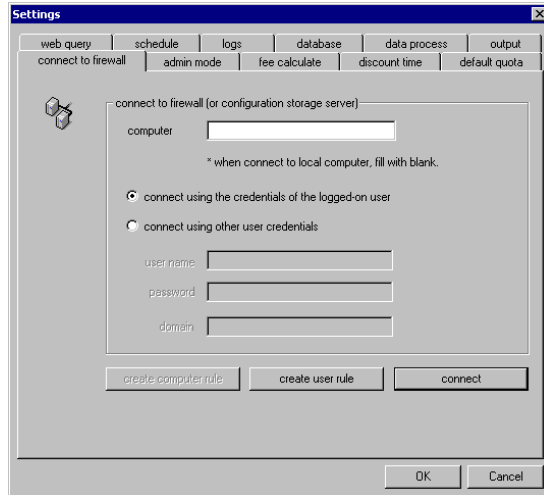
"Add group", refers to **Netfee manual "9.1.1 Add group"**.

"Add computer", refers to **Netfee manual "9.2.1 Add computer"**.

## 2.5.7 Connect to firewall

Netfee can run at local or at remote computer. When Netfee running at remote computer, need to connect to remote ISA(TM)G server.

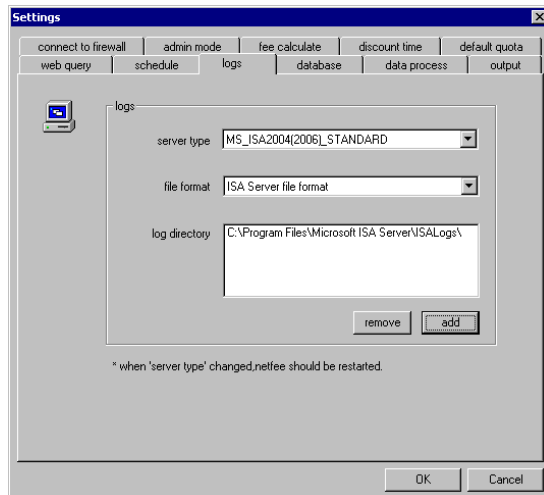
Run "**Tools/Settings/Connect to firewall**".



Specify name of computer running ISA(TM)G server firewall or Configuration storage server with *computer\_name* or IP address. Then, type the user name, password, and domain for the user who will remotely manage. Refer to **Netfee manual "7.1 Connect to firewall"**.

## 2.5.8 Log

Run "**Tools/Settings/Logs**".

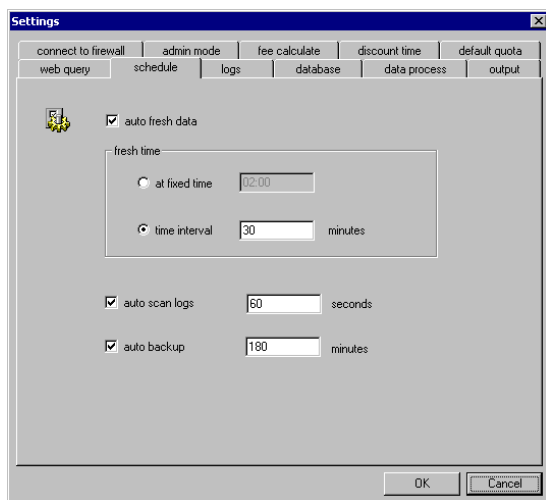


Select "**ISA(TM)G Server file format**" or "**W3C extended log file format**" as the format of log files of Firewall.

Then select the location of log file. If system log file is not in the Local computer, you can find the directory through "network Places". Or The path can be specified in the UNC format. for example, "\\ISAserver\ISALogs\".

### 2.5.9 Schedule

Run "**Tools/Settings/Schedule**", confirm "**Auto scan data**" is selected.



### 2.5.10 Scan log

Run "**Data Process/start Data-scan**" to scan log. you can see users information at "**real-time pane**".

start time	name	source addr	dest addr	category	protocol	port	applicator
11-08-02 16:11:39	software\admini...	192.168.100.10	stat.youku.com	Streaming M...	http	80	msie
11-08-02 16:11:34	software\admini...	192.168.100.10	119.167.222.15	Unknown	http	80	msie
11-08-02 16:11:33	software\admini...	192.168.100.10	www.netfeesoftware.com:...	Unknown	http	2082	msie
11-08-02 16:11:31	software\admini...	192.168.100.10	f.youku.com	Streaming M...	http	80	msie
11-08-02 16:10:36	anonymous	127.0.0.1	rs.microsoft.com:443	Internet Ser...	ssl-tunnel	443	ms-webse
11-08-02 16:10:57	software\admini...	192.168.100.10	tree.1ting.com	General Ent...	http	80	msie
11-08-02 16:10:34	software\admini...	192.168.100.10	commentmsg.youku.com	Streaming M...	http	80	msie
11-08-02 16:09:34	software\admini...	192.168.100.10	commentmsg.youku.com	Streaming M...	http	80	msie
11-08-02 16:07:46	software\admini...	192.168.100.10	61.55.175.94	Unknown	http	80	msie
11-08-02 16:08:48	software\admini...	192.168.100.10	stat.youku.com	Streaming M...	http	80	msie

At the same time, you can see log files being scanned.

file name	size M	progress rate
\\NSTAR-TMG\logs\ISALOG_20110802_FWS_000.w3c	3.19	Complete
\\NSTAR-TMG\logs\ISALOG_20110802_WEB_000.w3c	2.29	Complete

### 2.5.11 Fresh data

Run "**Data Process / Fresh data**" (or Ctrl + F5) to save data into database.

- ⊘ Only after "Fresh data" can query information.
- ⊘ For the change to user/department quota, only after "Fresh data" to take effect.

### 2.5.12 Query

Select the user/computer you want to query, run "**Query**".

### 2.5.13 Archive E

Run "**File/Archive data**" to set archive schedule and content. Refer to **Netfee manual "11.7 Data archive"**.

### 2.5.14 Event

At "**Real-time pane/Event**", can see the system return warning or error message.

time	content
11-08-02 19:20:06	Enable user 'software\administrator' to 2011-08-06
11-08-02 19:18:25	Disable user 'software\administrator' - 500.00(-124.88)M/month
11-08-02 19:16:36	Netfee server init finished.
11-08-02 19:16:30	Can not find log files! Netfee can only support W3C or Forefront TMG file format. confirm file format and location.
11-08-02 19:15:29	Netfee server init.

\traffic\url trace\block requests\malware\nis\file transfer\warning\scanning files\output\events