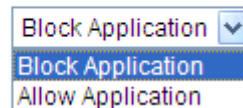# L7 Management

User Manual

Content

1. L7 Management

1.1 Outbound L7 Filter

- Outbound L7 Filter has two modes: Block Application and Allow Application.

- Block Application mode (black list) is to set the applications blocked, so intranet can not access these applications, but the traffic for other applications will still work.
- Allow Application mode (whitelist) is dening all applications except "Application Allowed".
- These two modes are different in the control level for network security, so UI setting is the same. The description below will use Block Application as example.

 (1) Rule list:

(2) Add new rule: click [Add New Rule]

▶ Add Rule

Rule Name : [   ]

Category	Item
Instant Messenger	
P2P Software	
Online Game	
Web Objects	
File Format	
Stocks Software	
Social Network Website	
Online Video Website	
Media Player	
Blog	
Application Define	

[>>>>]

Category ▲	Item ▲	Delete

[Application Define]

▶ Scheduling

Apply this rule	Always ▼	[ ] : [ ] to [ ] : [ ]	(24-Hour Format)		
	Everyday	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat			

▶ These settings will apply to all rules of this application

☐ Exception QQ Number

☐ Exception Source IP Address

[Apply] [Cancel]

5

Below are the steps for rule setting with an exmple in the enterprise:

Step 1: Name the rule

The name of the rule will be shown on the list, so administrator could name the rule by users or usages.

Step 2: Choose the application

※Figures are used for reference. Please visit the official website for the actual application support list.

(1) After choosing [Category], the [Item] column will show the crosponding list.

Hint:

- Directly click on the applications to put them effective.
- Cancel the application by double clicks.
- Click [Choose All] to put all applications into effective, and click unnecessary items for cancel.
- Items could be choosing in multiple categories.

(2) Click [>>>>] to drop the applications into the right column.

Step 3: Make sure the time setting is correct to make the rule in effective only during the set time.

All time is set as the default.   The time frame could be modified in the following settings.

◉ **Scheduling**

Apply this rule Always ▼	☐ : ☐ to ☐ : ☐ (24-Hour Format)	
☐ Everyday	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat	

Step 4: Set exceptaional users (IP or QQ number)

◉ **These settings will apply to all rules of this application**

☐   Exception QQ Number

☐   Exception Source IP Address

● Administrator can set IP address or QQ numbers (if QQ is blocked) in the exceptional user setting.

● Please note that the exceptional user setting will be applied to all the rules in the application.

For example, if there is a Google Talk rule with no exceptional IP, when adding a new Google Talk rule with the exceptional IP 192.168.1.100, 192.168.1.100 could use Google Talk anyway no matter applied to the original rule or the new rule.

Step 5: Click [Apply] **to save the rule setting.**

1.2 Inbound L7 Filter

If administrator setup servers in intranet, and functions like [Virtual Server] and [DMZ Server] are directed to the intranet server hosts and port numbers, the server security level could be higher to allow the identified application traffic only in Inbound L7 Filter function.

(1)Rule list:

Exceptional External Users

External users are not controlled by Inbound L7 Filter. For example, one enterprise headquater in New York has an ERP server, which is used by internal employees in New York as well as the branches in Boston and Brentwood. By adding the IP ranges of both Boston and Brentwood branches into exceptional external users, when system recognizes the imcoming traffic is from either Boston and Brentwood branches, the system will allow the traffic to pass without enterinig filtering process.

Exceptional external user can be not only assigned by IP range, but also choose from destination IP groups in Group Management.
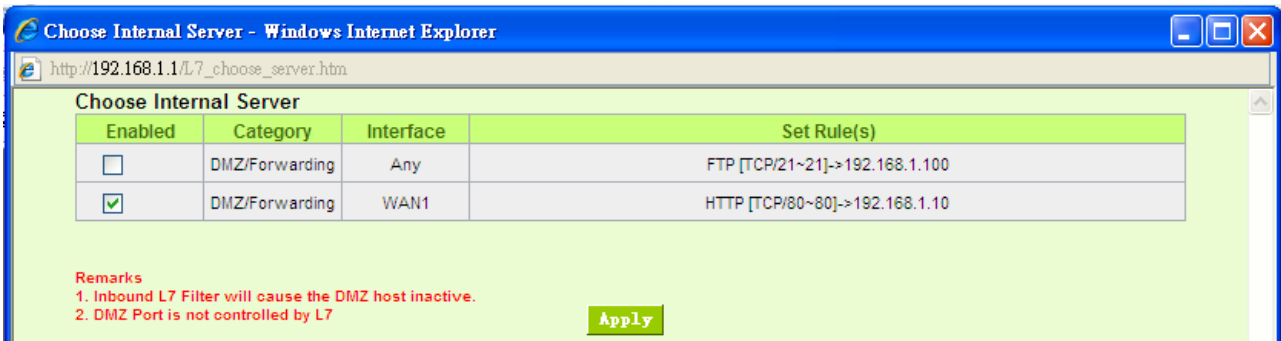
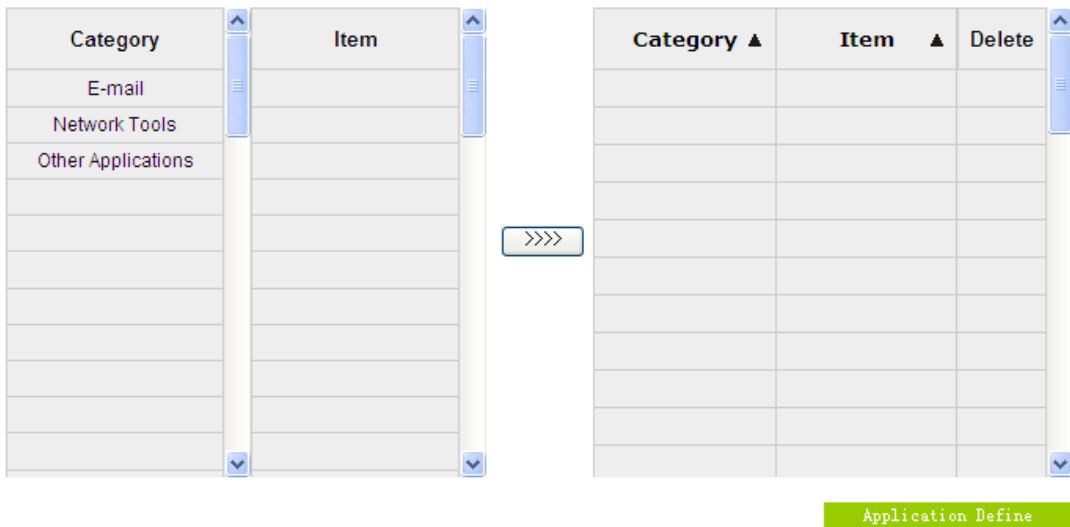**(2) Add new rule:** click Add New Rule

○ Rule Name

Rule Name : [   ]

○ Choose Internal Server

Choose

○ Choose an application

◉ Set this host as exception server.
○ Choose allowed items.

Category
E-mail
Network Tools
Other Applications

Category ▲	Item ▲	Delete

Application Define

☐ Add external client's IP as filtering condition

Apply   Cancel

Step 1: Name the rule

The name of the rule will be shown on the list, so administrator could name the rule by users or usages.

Rule Name : `Company WEB`

Step 2: Choose the server

Choose the rule set for virtual or DMZ servers.

○ **Choose Internal Server**

`edit`

Step 3: Choose the application

※Figures are used for reference. Please visit the official website for the actual application support list.

(1) Set this host as exception server:

The seleced server will not be controlled by Inbound L7 Filter if the item is checked. Inbound traffic will be allowed directly.

(2) After choosing [Category], the [Item] column will show the crosponding list.

Hint:

- Directly click on the applications to put them effective.
- Cancel the application by double clicks.
- Click [Choose All] to put all applications into effective, and click unnecessary items for cancel.
- Items could be chosen in multiple categories.

(3) Click [>>>>] to drop the applications into the right column.

Step 4: Add external client's IP as filtering condition

☐ Add external client's IP as filtering condition

Inbound traffic not only should match allowed application but selected external IP range.

For an example, one enterprise headquater in New York has an ERPserver, which is used by internal employees in New York as well as the branches in Boston and Brentwood. By adding ERP traffic as allowed traffic, and adding the IP ranges of both Boston and Brentwood branches into exceptional external users. The traffic doesn't match the allowed application and IP range will be blocked.

Step 5: Click [Apply] to save the configuration.

2. L7 VIP Priority Channel

(1)Rule List:

(2)Add New Rule: Click

Basic Setting

Rule Name :	
interface :	☐ WAN 1 ☐ WAN 2 ☐ WAN 3 ☐ WAN 4 ☐ USB1
	☐ USB2

Set Application or IP as VIP

☐ VIP Application

☐ VIP Source IP/Group

Scheduling

Apply this rule Always ▾	☐ : ☐ to ☐ : ☐ (24-Hour Format)	
Everyday	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat	

Apply   Cancel

Step1: Basic Setting

Basic Setting

Rule Name :	
interface :	☐ WAN 1 ☐ WAN 2 ☐ WAN 3 ☐ WAN 4 ☐ USB1
	☐ USB2

- The name of the rule will be shown on the list, so administrator could name the rule by users or usages.
- Select one WAN as VIP. For example, only the traffic of president room on WAN1 and WAN2 is VIP, traffic on other WAN ports is not VIP.
  Hint:
  If users want traffic only run on VIP WAN, users can also configure "L7 Application Binding".

Step2: Set Application or IP as VIP

🔵 Set Application or IP as VIP

☐ VIP Application

☐ VIP Source IP/Group

- Set application as VIP. For instance, [Webpage] is selected. When the system recognizes the IP is using webpage service, the system will give VIP priority.

- Set source IP/Group as VIP. For instance, if [General Manager Room] IP group is chosen, they will have VIP priority no matter what application is used.

- Set VIP application and source IP/Group at the same time. If [Webpage] and [General Manager Room] are configured at the same time, it means when general manager room use webpage service, the system will give them VIP bandwidth. But VIP bandwidth will not allowed when they use other network service.

Take a community for an example:

The community will ensure VIP authority when internal users browse webpage, the administrator should check [VIP Application] and [webpage] at Item column.

(1) After choosing [Category], the [Item] column will show the crosponding list.

Hint：

- Directly click on the applications to put them effective.
- Cancel the application by double clicks.
- Click [Choose All] to put all applications into effective, and click unnecessary items for cancel.
- Items could be chosen in multiple categories.

(2) Click [>>>] to drop the applications into the right column.

Step 3: Make sure the time setting is correct to make the rule in effective only during the set time.
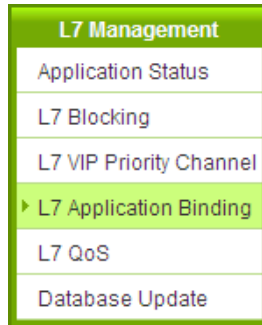
Always is set as the default. The time frame could be modified in the following settings.

Step 4: Click **to save the rules.**

3. L7 Application Binding

(1) Rule List:

> ● Summary

Priority	Enabled	Name	Interface	IP Range/Group	Time	Edit	Delete
1 ▾	☑	Skype	WAN4	192.168.1.200~254	Always	Edit	🗑
2 ▾	☑	Media Player	WAN3	Any	Always	Edit	🗑

Jump to 1 ▾ /Page   5 ▾ entries per page

Add New Rule

(2) Add New Rule: Click Add New Rule

◉ Choose an application

Rule Name : [   ]

Category	Item
P2P Software	
Media Player	
Other Applications	
Application Define	

>>>>

Category ▲	Item ▲	Delete

Application Define

◉ Setting

Bind to interface:	WAN 1 ▾
	☐ Remove traffic to another WAN when the selected interface was dropped.
Source IP/Group:	ANY ▾

◉ Scheduling

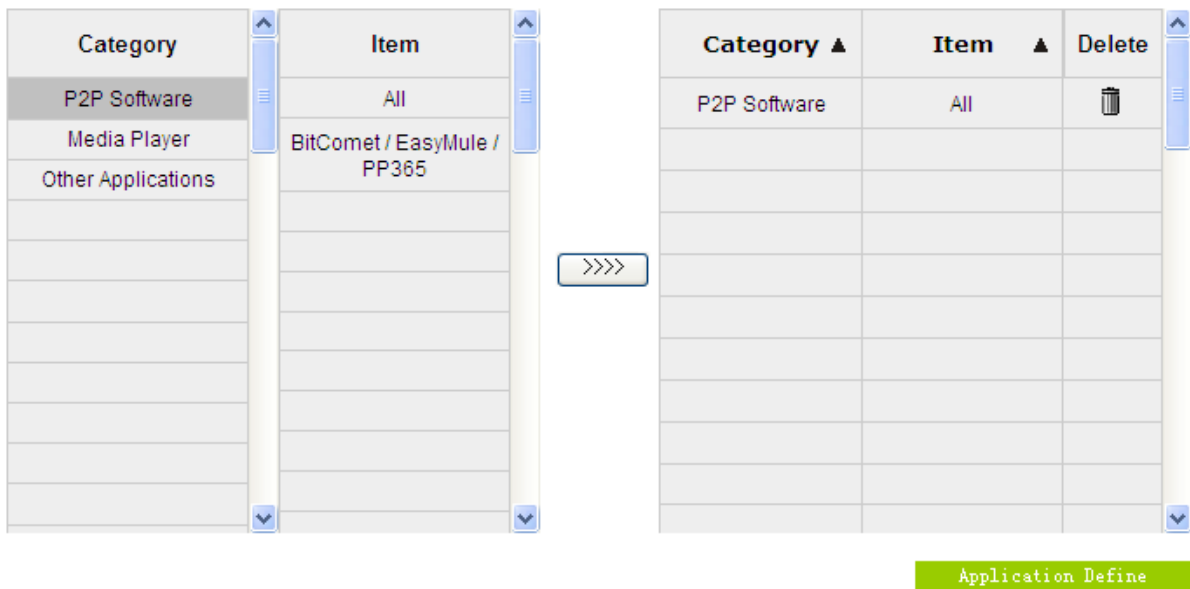|	
Apply this rule Always ▾	[ ] : [ ] to [ ] : [ ] (24-Hour Format)
☐ Everyday	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Apply   Cancel

Take a community for an example:

This community applies for two ADSL with different bandwidth. General Webpage bowsing and P2P applications which occupy more bandwidth will be allocated to different WAN ports to avoid affect each other.

Step 1: Name the rule

The name of the rule will be shown on the list, so administrator could name the rule by users or usages.

Rule Name : P2P

Step 2: Choose selected application

※Figures are used for reference. Please visit the official website for the actual application support list.

(1) After choosing [Category], the [Item] column will show the corresponding list.

Hint:

- Directly click on the applications to put them effective.
- Cancel the application by double clicks.
- Click [Choose All] to put all applications into effective, and click unnecessary items for cancel.
- Items could be chosen in multiple categories.

(2) Click to drop the applications into the right column.

Step 3: configure selected rule

O   Setting

Bind to interface:	WAN 4 ▾
	☐ Remove traffic to another WAN when the selected interface was dropped.
Source IP/Group:	Range ▾ 192 . 168 . 1 . 200 to 254

Bind to interface	Choose which interface the application or IP should be binded to.
Remove traffic to another WAN when the selected interface was dropped.	If this item is checked, the system will direct traffic to another WAN when it detect this interface was dropped.
Source IP/Group	Configure IP range.

Step 4: Make sure the time setting is correct to make the rule in effective only during the set time.

Always is set as the default.   The time frame could be modified in the following settings.

O   Scheduling

Apply this rule Always ▾	___ : ___ to ___ : ___ (24-Hour Format)
☐ Everyday	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Step 5: Click [Apply] to save the rules.

In this case, the administrator will set another rule to bind webpage to another WAN. The setting process is the same, so we won't explain again.

4. L7 QoS

(1) Rule List：

The Maximum Bandwidth provided by ISP

Interface	Upstream Bandwidth (Kbit/sec)	Remnant guarantee Upstream Bandwidth (Kbit/sec)	Downstream Bandwidth (Kbit/sec)	Remnant guarantee Downstream Bandwidth (Kbit/sec)
WAN 1	10000	10000	10000	10000
WAN 2	10000	10000	10000	10000
WAN 3	10000	9400	10000	10000
WAN 4	10000	10000	10000	10000
USB1	256	256	2048	2048
USB2	256	256	2048	2048

Apply   Show QoS Table

Summary

Jump to 1 /Page   5 entries per page

Priority	Enabled	Name	Interface	IP Range/Group	Upstream/Downstream	Bandwidth	Time	Edit	Delete
1	☑	WEB page	WAN3	192.168.1.200~205	Upstream	100~500Kbit	Always	Edit	🗑

Add New Rule

The Maximum Bandwidth provided by ISP： This table is relative to general QoS function.

- Filling WAN Upstream/Downstream bandwidth with realistic broadband network bandwidth which user applying by ISP, QoS Bandwidth control is according to the bandwidth number that user filling to calculate. Click **Apply** to save the set-up.
- Bandwidth unit is kbit, some of the software applications display by KB, 1KB=8kbit.
- Calculating bandwidth utility of QoS rule: minimize of bandwidth × IP set-up number. For example, IP range is 192.168.1.101~110, minimize bandwidth by each IP is 500kbit/sec, the total bandwidth utility of QoS rule is 500kbit/sec × 10(by IP) ＝ 5000kbit/sec.
- Remnant guarantee Bandwidth＝Bandwidth – QoS Policy. The Remnant guarantee displays as a negative number in red when the bandwidth of QoS Policy is over the WAN bandwidth.
- **Show QoS Table** ： Display the QoS Policy, including the L7 QoS and general QoS. The L7 QoS has a higher priority then the general QoS if both overlapping.

(2) Add New Rule：Click [Add New Rule]

● **Add Restrict Rule**

Rule Name : [_____]

Category	Item
P2P Software	
Media Player	
Other Applications	
Application Define	

[>>>>]

Category ▲	Item ▲	Delete

[Application Define]

● **Quality of Service**

Interface :	☐ WAN 1 ☐ WAN 2 ☐ WAN 3 ☐ WAN 4 ☐ USB1 ☐ USB2
Source IP/Group :	Range ▼ [___] . [___] . [___] . [___] to [___]
Bandwidth :	Mini. Rate : [0] Kbit/sec Max. Rate : [0] Kbit/sec
Upstream/Downstream :	Downstream ▼
Bandwidth sharing :	○ Share total bandwidth with all IP addresses. ◉ Assign bandwidth for each IP address.

● **Scheduling**

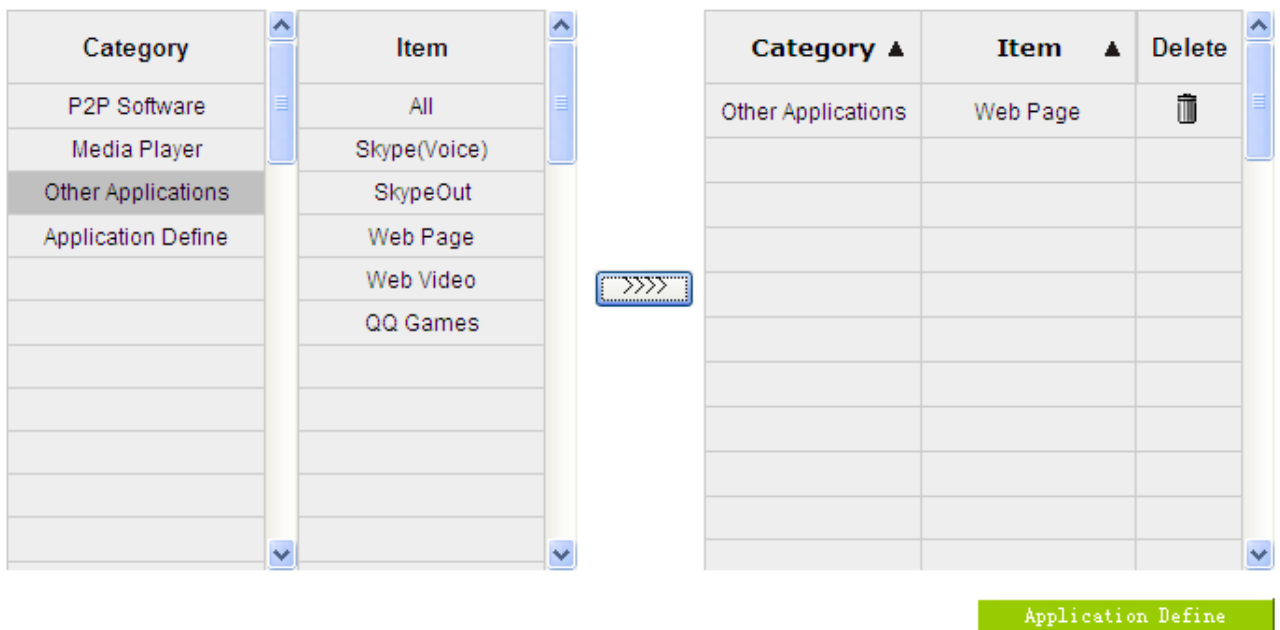|	
Apply this rule Always ▼	[__] : [__] to [__] : [__] (24-Hour Format)
☐ Everyday	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

(Apply) (Cancel)

Step 1: Name the rule

The name of the rule will be shown on the list, so administrator could name the rule by users or usages.

Rule Name : WEB page

Step 2: Choose the application

※Figures are used for reference. Please visit the official website for the actual application support list.

(1) After choosing [Category], the [Item] column will show the crosponding list.

Hints:

- Directly click on the applications to put them effective.
- Cancel the application by double clicks.
- Click [Choose All] to put all applications into effective, and click unnecessary items for cancel.
- Items could be chosen in multiple categories.

(2) Click [>>>>] to drop the applications into the right column.

Step 3: QoS Configuration

Interface	Select on which WAN the QoS rule should be executed. It can be a single selection or multiple selections.
Source IP/Group	This is to select which user is to be controlled. If only a single IP is to be restricted, input this IP address, such as "192.168.1.100 to 100". The rule will control only the IP 192.168.1.100. If an IP range is to be controlled, input the range, such as "192.168.1.100 ~ 149". The rule will control IP addresses from 192.168.1.100 to 149.
Upstream/Downstream	Upstream : Means the upload bandwidth for Intranet IP. Downstream : Means the download bandwidth for Intranet IP.
Bandwidth sharing	**Sharing total bandwidth with all IP addresses:** If this option is selected, all IP addresses or Service Ports will share the bandwidth range (from minimum to maximum bandwidth). **Assign bandwidth for each IP address:** If this option is selected, every IP or Service Port in this range can have this bandwidth (minimum to maximum). For example, If the rule is set for the IP of each PC, the IP of each PC will have the same bandwidth. ※**Attention:** If "Share-Bandwidth" is selected, be aware of the actual usage conditions and avoid an improper configuration that might cause a malfunction of the network when the bandwidth is too small. For example, if users do not want an FTP to occupy too much bandwidth, users can select the "Share-Bandwidth Mode", so that no matter how much users use FTPs to download information, the total occupied bandwidth is fixed.

Step 4: Make sure the time setting is correct to make the rule in effective only during the set time.

All time is set as the default. The time frame could be modified in the following settings.

◉ Scheduling

Apply this rule Always ▾	___ : ___ to ___ : ___ (24-Hour Format)	
☐ Everyday	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat	

Step 5: Click ⬭Apply **to save the rule setting.**

5. Application Define

When you set up the L7 Management rules, not only you can select the application that is defined by Qno, but also you can add your own L7 applications by the URL, destination IP address or the port number.

You can see the Application Define feature on the Application Status Table or on the APP List of all L7 Management features.

※Application Status

※Figures are used for reference. Please visit the official website for the actual application support list.

※Each function of L7 Management APP List

※Figures are used for reference. Please visit the official website for the actual application support list.

Application Define-Add New Rule

Step 1：**Name the Application**

Step 2：**Define the application by the URL, destination or the port number.** The definable parameter as below：

Dest. IP	If only a single IP is to be restricted, input this IP address, such as "100.100.100.105". The rule will control only the IP 100.100.100.105. If an IP range is to be controlled, input the range, such as "100.100.100.105~200".
Dest. IP Group	Apply the Dest. IP Group from the [Group Management] function.
Domain Name	Use Domain Name to define the application, for example, input the "speed.hinet.net" such as http://speed.hinet.net.
Service Port	Set up the TCP、UDP port number or apply the port group from the [Group Management] function.

Step 3：**Click** [Add to list] **to add your own L7 application to the list right side to finish the setting.**

Step 4: Apply your own application to the L7 management; you can see your own L7 application on the 'Application Define'.
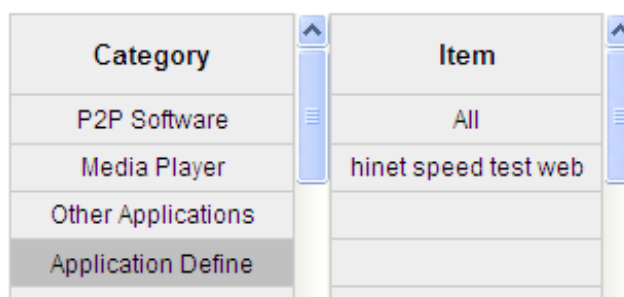
6. Applicatios Status
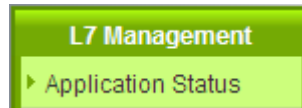
The Administrator can check the whole applied applications from the Application Status function, including the ID of the policies.

1	Sorting and ordering the applications	Sorting the applications or ordering the applications by the name.
2	Jump to 1 /Page	Jump to the specific page.
3	10 entries per page	Identify the lines in one page.
4	Next Page>>	Next page.
5	L7 VIP Priority Channel	Display policy which made by the application, presses the ID to edit the policy.

7. Database Update
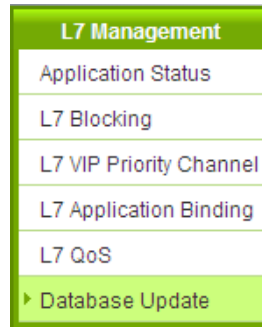
Database Update function provides administrator to know the server side informations on this web page whether the newest version to update, moreover to set-up the update time of database and version check frequency.

◑ Version Check

No New Version Is Available
Version Number : V1.0.0.0
File Size : 0KB
[Download Now]

Latest Version Check : [Check Now]

◑ Advanced Function

Version Management	Previous Version : V0.0.0.0 [Roll Back]
	Current Version : V1.0.0.0
	Downloaded Version : --- [Update Now]
Automatic Version Check	○ Enable Automatic Version Check Every 24 Hours
	⊙ Disable
Automatic Update Installation	⊙ Disable
	○ Enable Automatic Update Installation
	○ Define Update Schedule 23 : 00(24-Hour Format)
	☑ Mon. ☑ Tue. ☑ Wed. ☑ Thu. ☑ Fri. ☑ Sat. ☑ Sun.
Update Server	⊙ Default Server(Recommended Option)
	○ Backup Server
	IP/Domain :
	Service Port : 443

[Apply] [Cancel]

Version Check：

1	Version status check field	When your router connected with database server and the availible new version has been checked to download, the prompt of version status, newest version number and file size will be displayed on this filed.
2	Download Now	Download this version immediately after click this button. If you do not update immediatly after you downloaded, this version will reserve in system, you can download manually from downloaded version in [Version Management].
3	Latest Version Check	The latest time of server version checking by router. Click ![Check Now] manually to check again immediately. The frequency of check time can be adjusted in [Advance Setting].

Version Management：

Previous Version	Previous version of database server that system has been used.
Current Version	Cuurent version of database server that system is being used.
Downloaded Version	The version you downloaded by [Download Now] in version check function. You can click ![Update Now] to manually update.

Automatic Version Check：

Enable Automatic Version Check Every__Hours	Adjust the frequency of server version check time.
Disable	System will not update the database automatically, administrator can still use **Check Now** to comfirm if the server has the newest version or to adjust the check frequency manually.

(Advance Setting) Automatic Update Installation：

Disable the Automatic Update Installation	System will not update the database, administrator can update the database manually by press the **Update Now**
Enable Automatic Update Installastion	Download and update automatically if the system notice the new version.
Define Update Schedule__: 00 (24hr)	Download and update automatically in the specific time if the system notice the new version.

Update Sever：Do not change the set-up by self

Default Server	The setting of the system default server.
Backup Server	Set up the backup server, including the IP address or the URL, along with the service port number.