iTrust

Configuration Guide

Intelligent
WAPPLES

Best Defense Against Web Attack

Penta SECURITY

Table of Contents

A. Overview

The WAPPLES Configuration Guide explains how to set the service port and apply the security policies that must be completed to operate WAPPLES. It also describes how to set the WAPPLES Administration Tools UI to the customer's convenience and how to define additional WAPPLES operation settings. If you have any trouble or inquiry while setting WAPPLES according to the guide, please contact your distributor.

B. WAPPLES Basic Setting

❑ The basic settings for WAPPLES are divided into service port setting and security policy application. (For details on the service port setting and security policy application, refer to Appendix A.)

Service Port Setting		Security Policy Application	
Set WAPPLES Proxy IP*.	➡ Register Web Server IP.	Add Website.	➡ Allocate Policy.
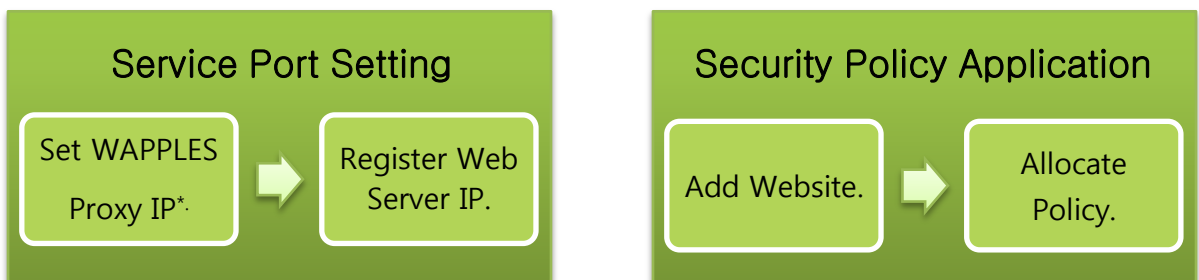
- Service Port Setting
  - For In-Line mode, select "In-Line Mode" instead of registering IP in "WAPPLES Proxy IP Setting."
  - For Reverse Proxy Mode, register the WAPPLES Proxy IP to allocate to the service port. Likewise, register the gateway of the network where WAPPLES belongs.
  - Web Server IP Registration
    Register in WAPPLES the IP of the web server to be protected.

- Security Policy Application
  - Addition of website
    Add the Websites of the web server to be protected.
  - Allocation of Security Policy
    You can apply the security policy in different security levels for each website.
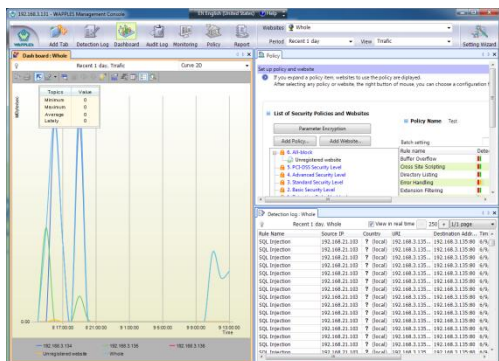
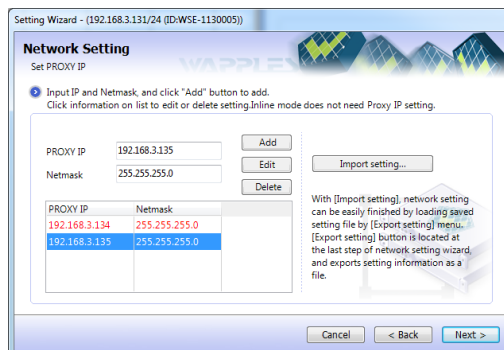# 2. WAPPLES Service Port Setting

A. WAPPLES Proxy IP Setting

- ❑ Adding the WAPPLES Proxy IP
  - Click the Proxy IP Setting Wizard on the upper right side and select WAPPLES to set.

WAPPLES Administration Tool Main Window

WAPPLES System Select Window
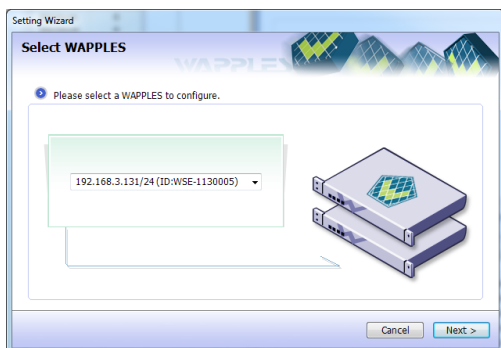
- Select Network Settings.

Proxy IP Settings Wizard – Select Settings Window

- Set the WAPPLES Proxy IP.

Proxy IP Setting Window

- ▪ In-Line Mode
  - ✓ You need not set the Proxy IP separately.
- ▪ Reverse Proxy Mode
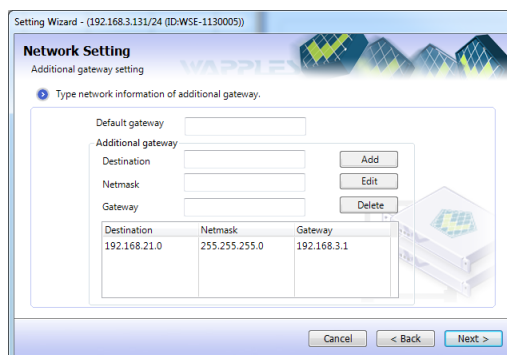 - ✓ One Proxy IP is required for each web server for the network setting of WAPPLES.

- ❑ Adding a Gateway
  - Register the gateway.

Additional Gateway Settings Window

- ❖ Tip: To add a gateway, check Additional Gateway Setting, enter Destination, Netmask, and gateway, and click the Add button.
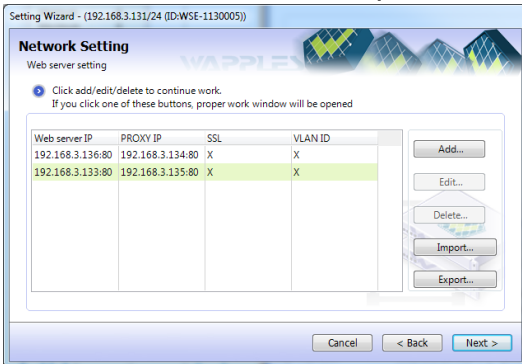
2. WAPPLES Service Port Setting

B. Web Server IP Registration

❑ Web Server Registration

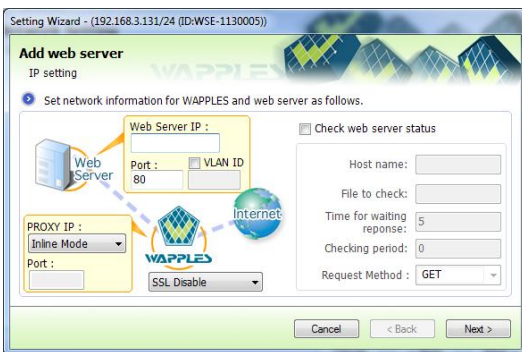• Add the web server to be protected.

Web Server Settings Window

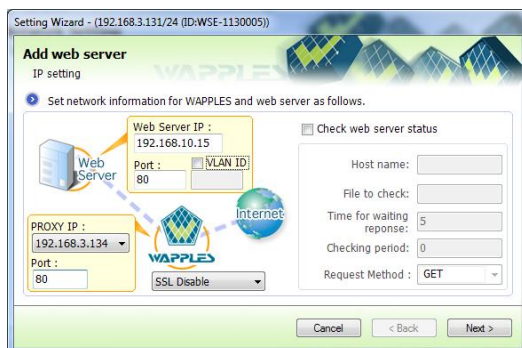• Enter the web server IP and click Next.

▪ In-Line Mode

Set the Proxy IP to In-Line Mode. The Web Service Port is automatically configured.

Window for Adding Web Server – Inline mode

▪ Reverse Proxy Mode
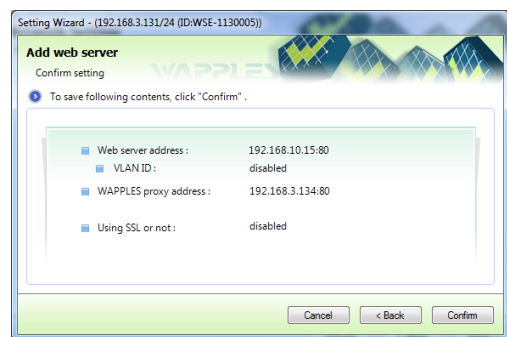
Enter the port number to the Web Service Port.

Window for Adding a Web Server – Reverse Proxy mode

▪ For HTTP, it is generally set to 80, although a different port can be selected according to the network environment.

✓ Tip: If the web server uses SSL communication, check Use SSL and add the related SSL certificate and private key file.
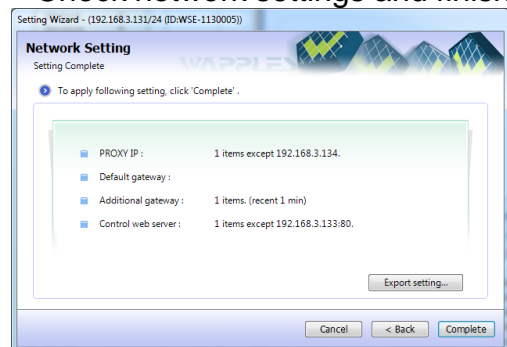
• Finish the web server setting.

Proxy IP Settings Wizard – Selection Window

❑ End of Network Setting

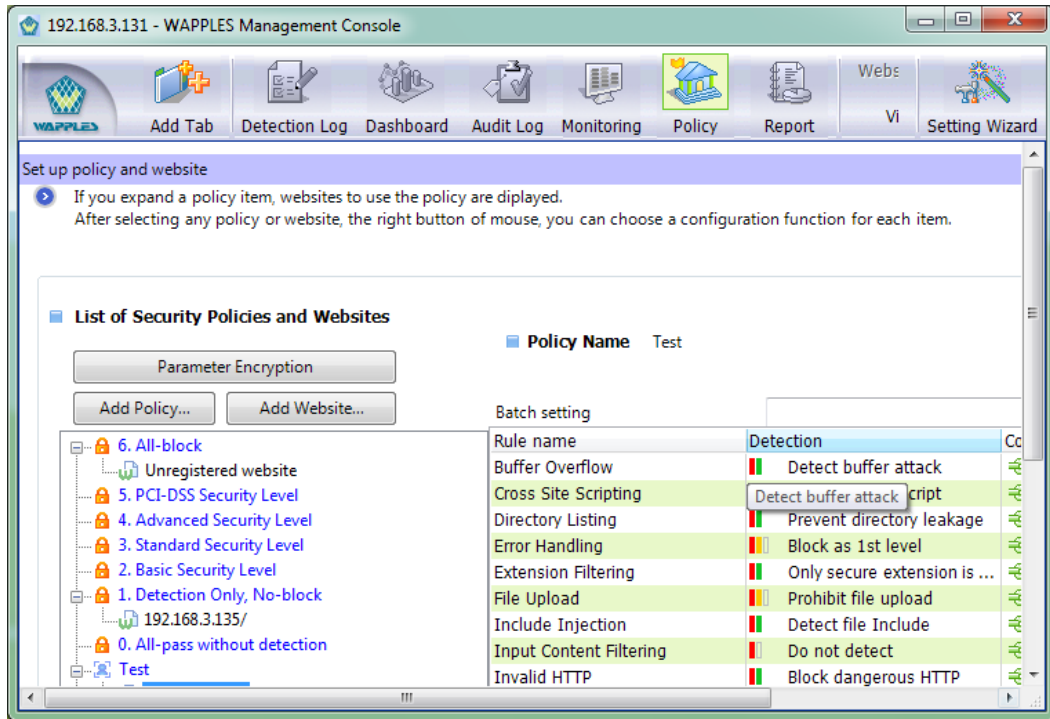• Check network settings and finish.

Network Settings Completed

▪ For Reverse Proxy Mode, change the DNS properties of the web server environment after finishing the network settings to set the WAPPLES Proxy IP to the IP of the web server that is actually in service.

❑ Adding a Website

- Click Policy Setting in the toolbar.

Policy Setting Tab

- Select the policy suitable for WAPPLES operation.
    - Policy Presets
    ① Block All Security Policy
       : Blocks all sites
    ② PCI-DSS Security Policy
       : Policy applicable to systems observing the PCI-DSS certification
    ③ Advanced Security Policy
       : High-level security policy for blocking even low-impact attacks
    ④ Standard Security Policy
       : Policy that is most optimized for general web environment
    ⑤ Basic Security Policy
       : Policy for preventing popularized, high-impact basic web attack
    ⑥ Detect Only Security Policy
       : Detects sites but does not block them
    ⑦ Pass Without Detection Security Policy
       : Passes all sites without detection

- Click the Add Website button and register the address and port of the website to be protected.

Website Addition Window

- Register the secret key for secure access.

Secure Access Settings Window

- When using ISSAC-Web, Penta Security System's web security solution, check "Use ISSAC-Web." If you decide to use ISSAC-WEB, you need to register the web server secret key file used by ISSAC-Web using the [Open Secret Key] button and click [Next].

- Register the trusted IP such as website administrator or developer.
  - ✓ Tip: To register the reliable IP, enter the IP or IP/Netmask.

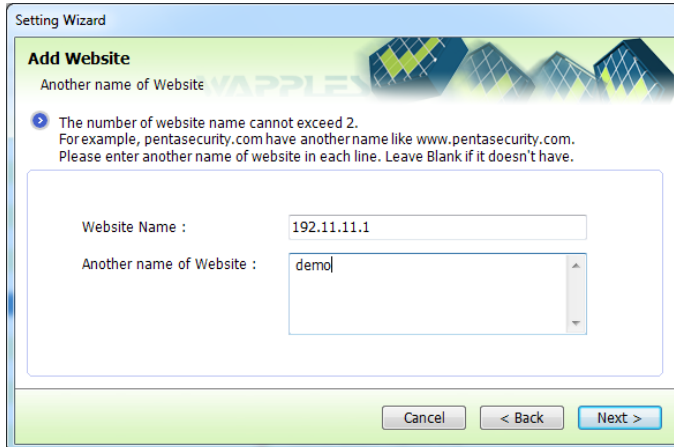Trusted IP

- Register the web server security key.

Web Server Security Key Window

- ✓ Tip: Do not change the security key while operating WAPPLES. Once this key is changed during operation, all keys used in WAPPLES will be changed as well; thus causing temporary misdetection.

- Modify the values based on the web server environment and click Next.

Web Server Environment Window

- Add an alias of the website.
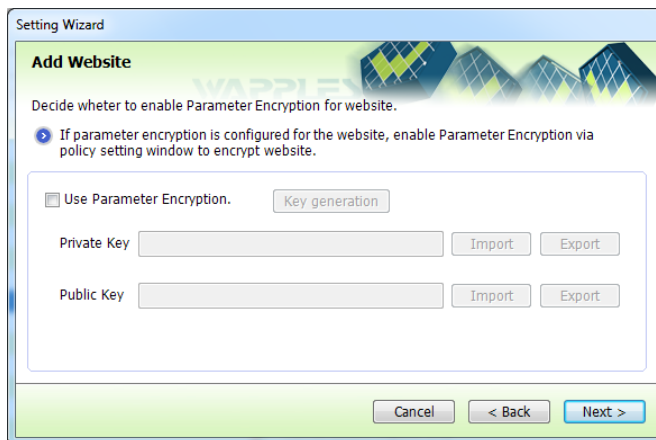
Website Alias Window

- Set whether to use Parameter Encryption or not(supported for R9 or higher)
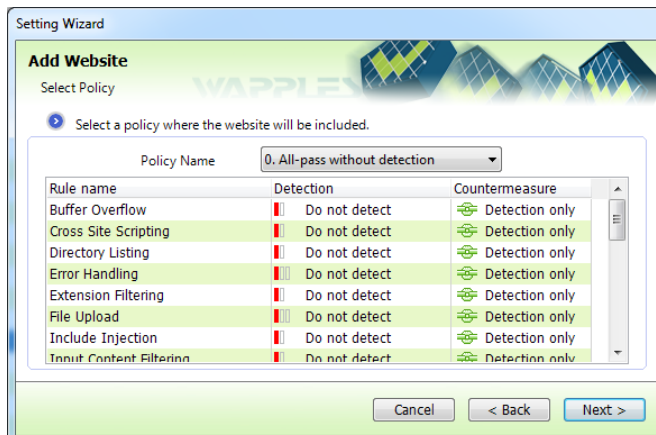
Parameter Encryption Setting

- Select the policy suitable for the website.

Policy Selection Window

- Confirm the website settings.

Website Setting Confirmation Window

A. UI Configuration

❑ Administration Tool Configuration

- The administration tool window basically consists of the toolbar at the top and the tab window at the bottom.
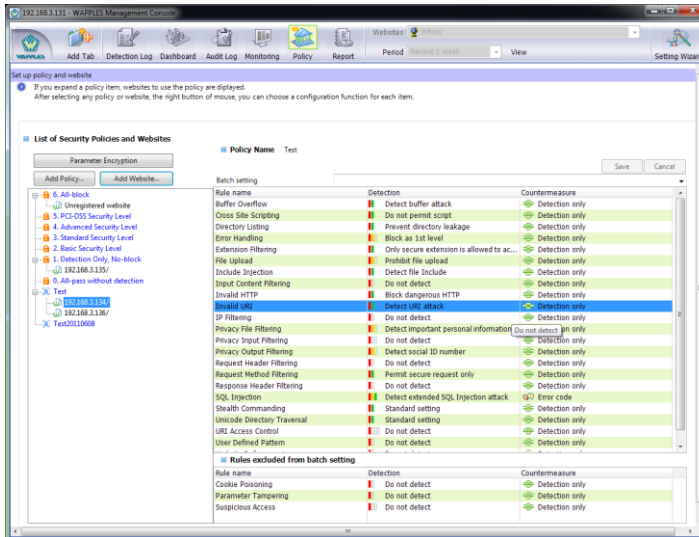
WAPPLES Administration Tool

❑ Toolbar
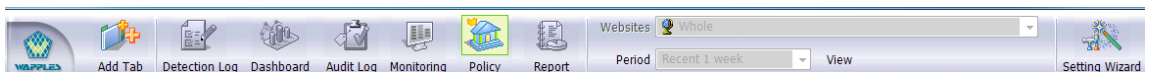
WAPPLES Administration Toolbar

- Add Tab
  - Button for adding a maximum of 10 tabs
- Tab Window
  - [Detection Log] Displays the log detected under each WAPPLES rule
  - [Dashboard] Displays the web server traffic data and detection data in the form of graphs
  - [Audit Log] Displays audit logs including the administrator's log in information and changes in the setting
  - [Monitoring] Displays the system status of WAPPLES
  - [Policy Setting] Sets policies suitable for the website
  - [Report] Print report by site and period
- Filter
  - Group for filtering the various contents displayed on the tab screen
- Setting Wizard
  - Button for defining the operation settings and network settings

❑ Tab Window

- The administrator's window basically consists of the toolbar on the top and the tab window at the bottom.
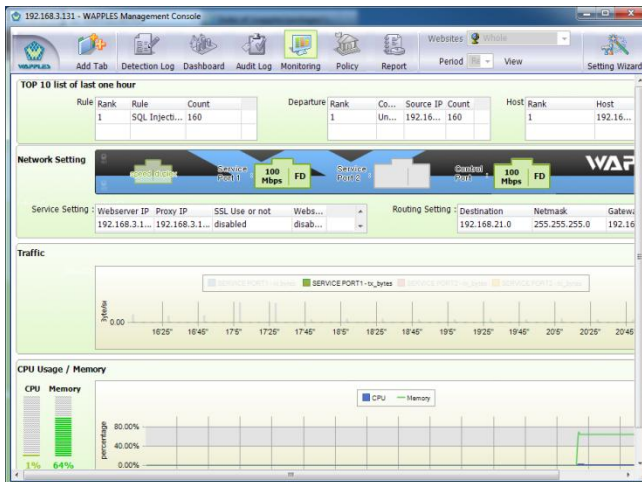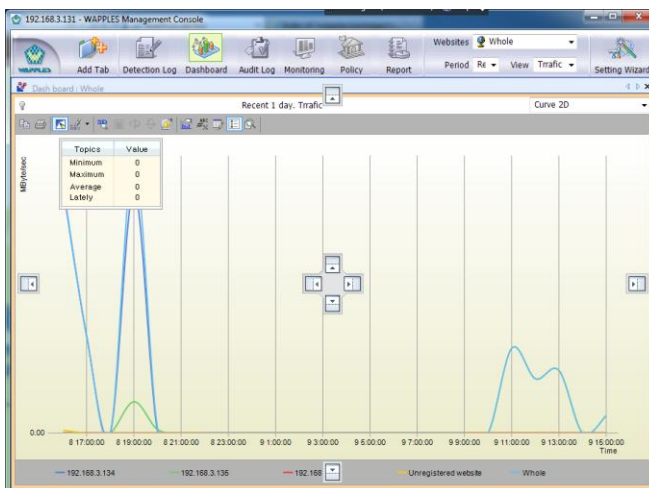

WAPPLES Administrator's Window –Ex) Monitoring

- You can adjust the position of the tab window through tab window splitting.

**Administration Tools Tab Window
Splitting**

✓ Tip: Click the name of the tab window [Dashboard: All] and drag the window. The window above will then appear to split the tab.

✓ Small icons will appear on the top, bottom, left, and right sides of the tab window. Drag the window toward each direction to split the tab toward the corresponding direction. The icons on the edge determines the top/bottom/left/ right direction on the entire screen, with the icons at the center determining the position on the current window.

✓ You can set the WAPPLES administration tools window differently to monitor various information at once; you can adjust the size of each window by moving the border between windows.

B. Recommended User Window

❑ 3-Frame Administration Tool
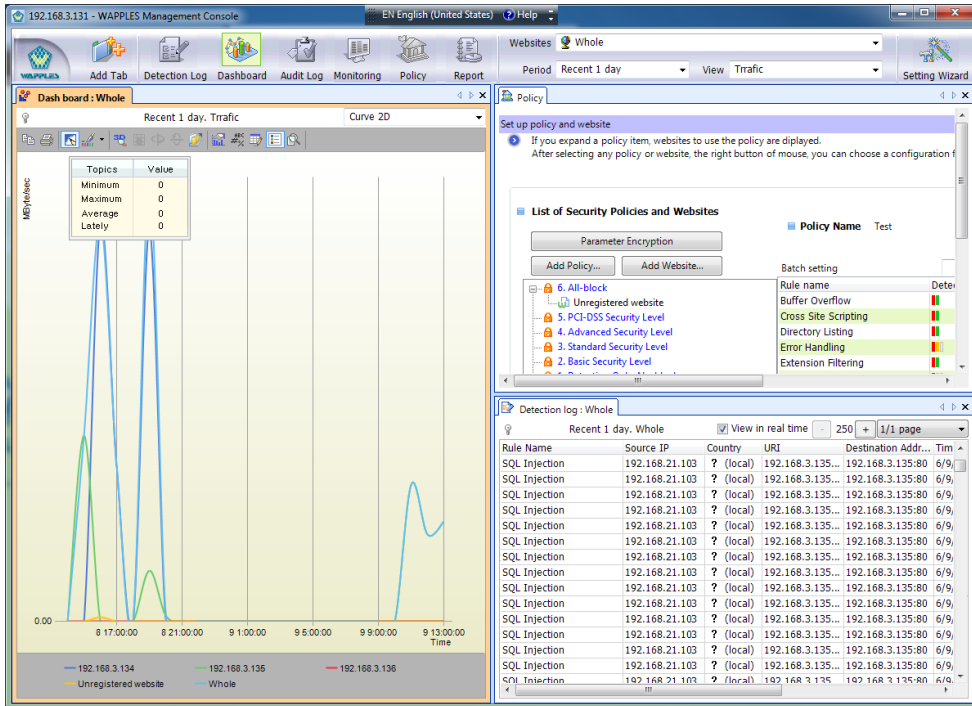
Recommended User Window 3-Frame
Administration Tool

❑ Locate the recent detection logs on the left.

❑ Locate the detection log for the rules that the administrator specifically wants to monitor only, and then locate the dashboard tab on the lower right side.

✓ Tip: Select the detection log tab and click the drop box of the View button on the toolbar. Select User-Defined followed by "View only the selected rules in the rule name tab." When the WAPPLES rule list appears, select the desired rules and click OK.

✓ The window can be configured freely and flexibly according to the administrator's need. This window configuration will be saved automatically, thereby remaining the same when you restart the administrative tool.

A. Backup and Restoration Setting

❑ Backup Method

- To save a backup file in WAPPLES, execute the "configure terminal" and " wapples" commands and use the backup command.

  ✓ To back up detection and audit logs only, enter the backup [filename] local.

  ```
  penta-np(config-wapples)# backup data local
  Starting Local Backup...
  Please wait...
  Backup ...[OK]
  ```

  CLI mode Window

  ✓ To back up the log as well as the settings, enter the backup [filename] image.

  ```
  penta-np(config-wapples)# backup data2 image
  Starting Image Backup...
  Please wait...
  Backup...[OK]
  Restart WAPPLES Service...
  Please wait...
  Restart WAPPLES ...[OK]
  ```

  CLI mode Window

- You can check the saved backup files with the "restore list" command.

  ```
  penta-np(config-wapples)# restore list

  Database files
  ================================================================
  WAPPLES-IMAGE_backup-test1-20100217102503.tar.bz2
  WAPPLES-DB_Backup-data-201002161416.tar.gz
  WAPPLES-DB_Backup-test-201002171023.tar.gz
  ```

  CLI mode Window

  ✓ Tip: You can view the backup files with the "restore list" command.

❏ Restoration Method

● Do the following to restore with a backup file:

```
WAPPLES(config) >> restore list
 > WAPPLES-DB_Backup-data1-201002080912.tar.gz
 > WAPPLES-DB_Backup-help-201002080906.tar.gz
WAPPLES(config) >> restore WAPPLES-DB_Backup-data1-201002080912.tar.gz
Starting restore ...
Please wait...
Restore WAPPLES-DB_Backup-data1-201002080912.tar.gz...[OK]
```

CLI mode Window

✓ Execute the "restore filename" command to restore with a backup file.

● Do the following to restore the initial values of WAPPLES:

```
penta-np(config-wapples)# restore factory
Warnning! reset all of configuration... GO on ?[y/n] :y
Clear...[OK]
```

CLI mode Window

✓ To initialize the values to factory setting, use the "restore factory" command.

B. WAPPLES Update Setting

❑ Preparations

- When you make settings for the update server, communication from the WAPPLES administration port to the update server will take place. For this, you need to register the gateway to allow access from the administration port IP to the update server IP.

- To register the gateway, use "rt add" in CLI.

    ex.) If the gateway IP address is 192.168.3.1.

    → penta-np (config-network)# rt add default 192.168.3.1 ctl0

    If it is not registered, use "show rt all" commands to check whether the route table contains information for the network of the same band as 192.168.3.1.

❑ Online Update Service Setting

- Click [Operation Settings] in [Settings Wizard].

Settings Wizard Selection Window
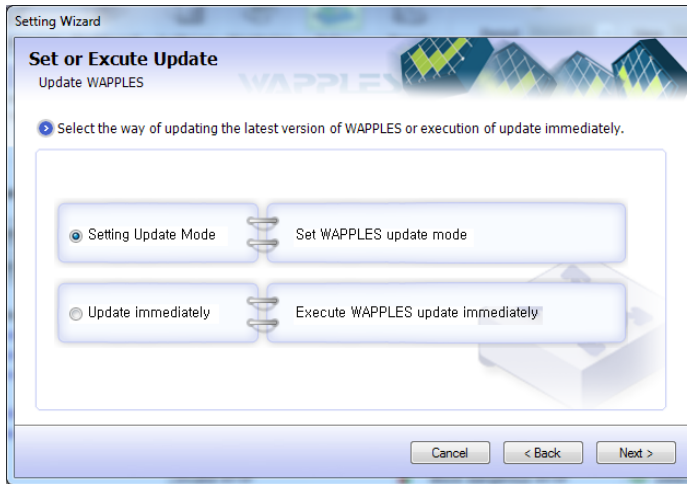
- Click the [Update Setting and Execution] button.
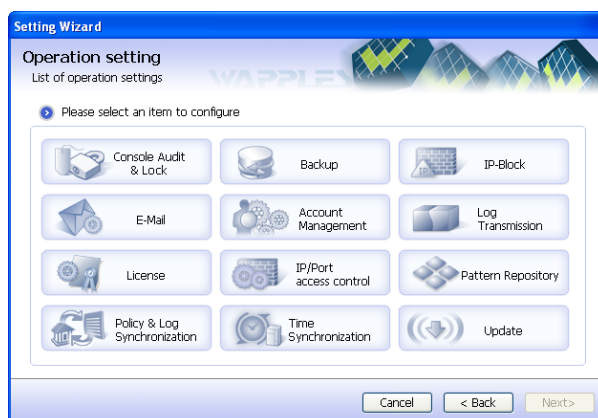
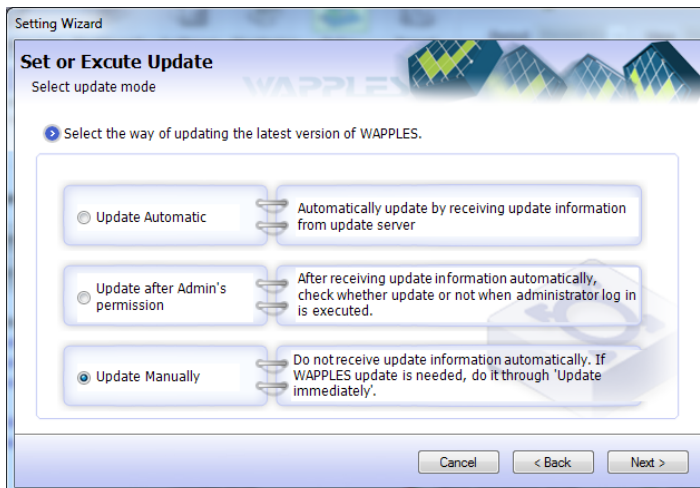
Operation Settings Selection Window

- Select Update Mode Setting.

WAPPLES Version Update Window

- Update Mode

Update Mode Selection Window

- [Automatic Update] - Checks for new updates in the update time and cycle specified by the administrator and updates automatically
- [Update After Administrator Approval] – Checks for new updates in the update time and cycle specified by the administrator and asks the administrator for confirmation on the update
- [Manual Update] – The administrator has to update manually instead of receiving update information automatically.

- Set the update server IP and update cycle.

Auxiliary Update Server Registration Window
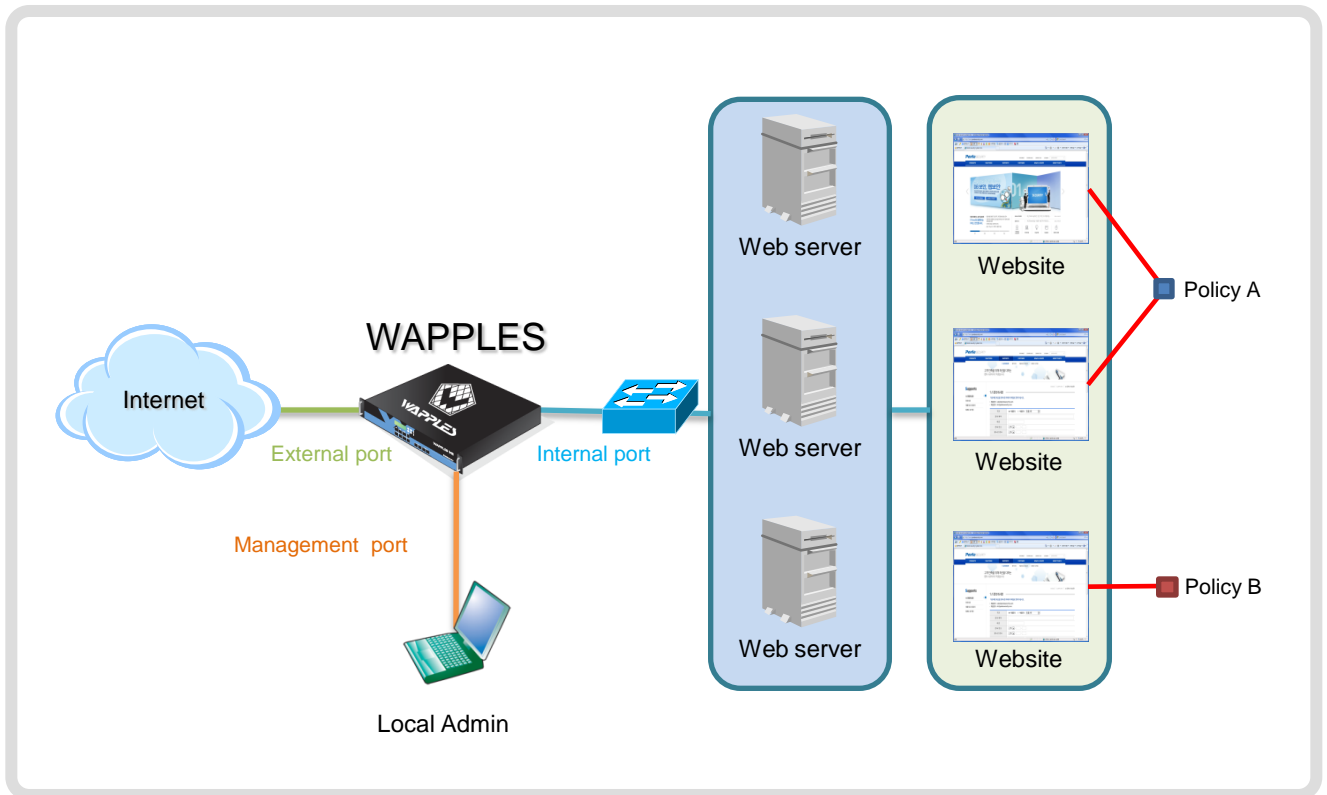
- Check the update setting.

Update Setting Completed

❑ Checking the Update Result
- The update result can be checked in the audit log.

6. Appendix

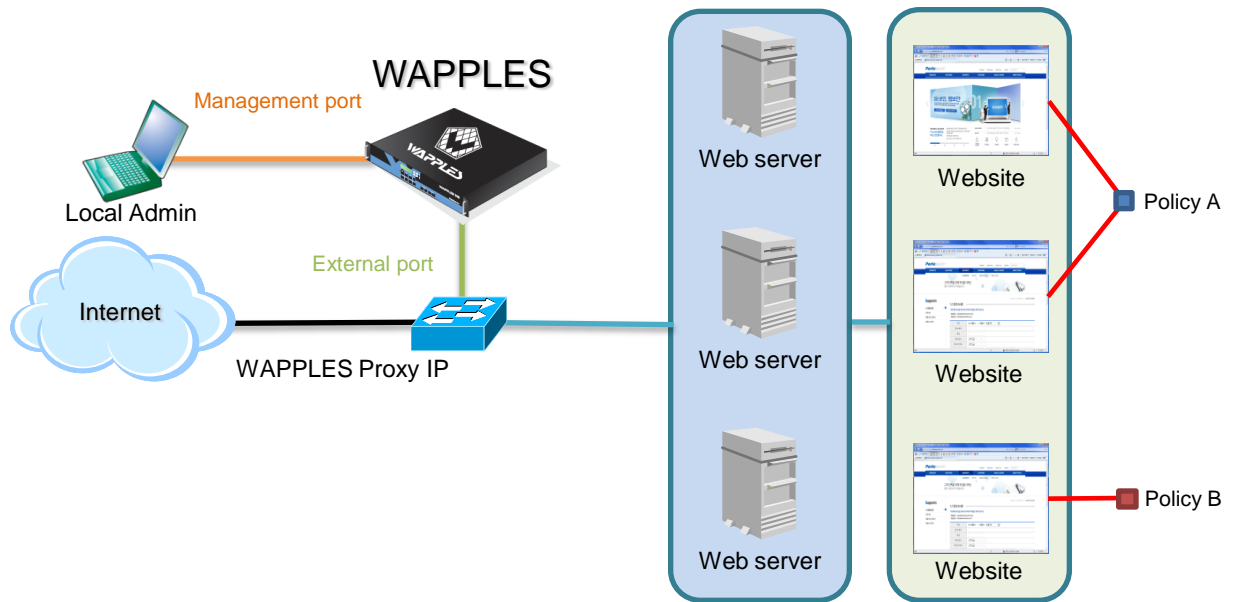## A. WAPPLES Service Port Setting and Security Policy Application

❑ In In-Line Mode

- In case of inline mode, there is no need to set Proxy IP.
- For details, please refer to Reference Manual.

6. Appendix

A. WAPPLES Service Port Setting and Security Policy Application

❑ Reverse Proxy Mode

- In Reverse Proxy mode, traffics are heading for WAPPLES Proxy IP not actual web server's IP.
- Needs 1 or more Proxy IP.
- For details, please refer to Reference Manual.

B. Fail-Open and Fail-Close Setting

❑ Fail-open

- H/W bypass after power-off: hw-default-act set bypass
- H/W bypass after power-on: hw-default-act set bypass
- S/W bypass after WAPPLES failure: hw-default-act set bypass

❑ Fail-close

- H/W bypass after power-off: hw-default-act set disconn
- H/W bypass after power-on: hw-default-act set disconn
- S/W bypass after WAPPLES failure: hw-default-act set disconn

Penta SECURITY