TrafficShield® Installation and Configuration Manual

version 3.2.1

MAN-0141-01

Service and Support Information

Product Version

This manual applies to product version 3.2.1 of the TrafficShield® Application Firewall.

Legal Notices

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable Control user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

F5, F5 Networks, the F5 logo, BIG-IP, 3-DNS, iControl, FireGuard, Internet Control Architecture, IP Application Switch, iRules, OneConnect, Packet Velocity, SYN Check, Control Your World, ZoneRunner, uRoam, FirePass, TrafficShield, WebAccelerator, and WANJet are registered trademarks or trademarks of F5 Networks, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. F5 Networks' trademarks may not be used in connection with any product or service except as permitted in writing by F5.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This class A digital apparatus complies with Canadian I CES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Table of Contents

1
Introduction

2
Installation and Topology Configuration

3
Configuration and Licensing

4
Web Applications

5
Monitoring

6
Administration

Glossary

1

Introduction

- Product overview
- Document objectives
- How this manual is organized
- Audience and assumed knowledge
- Related documentation

Product overview

Web applications are the single greatest point of contact most people have with corporations today. However, these applications let users through the traditional security perimeter around the company's IT infrastructure, allowing access to sensitive internal data. Today, the web application is the security perimeter. That is, enterprises are relying on the security of each application to keep users from accessing restricted data or systems. Browser-based applications are inherently difficult to secure, and full of vulnerabilities.

F5® Networks TrafficShield® Application Firewall is a dedicated appliance built to protect applications by preventing hackers from stealing customer and corporate data. TrafficShield Application Firewall can map each application to determine every legal user action, and then can block actions not known to be legal according to this map.

This manual describes how you can deploy the single-unit in your system, and how you can deploy the optional standby unit configuration.

Administrative operations are performed using the TrafficShield Management Station (TSMS), a web-based tool built into the TrafficShield Application Firewall units.

Document objectives

This manual describes how to configure and manage the TrafficShield Application Firewall.

How this manual is organized

The manual's focus is on the first-time user performing the initial steps to install the TrafficShield Application Firewall:

- Pre-configure the unit outside the TSMS.
- Open the TSMS user interface and complete the unit configuration.
- Activate a production license.
- Define all relevant Web Applications.

Once you have completed these tasks, you can then create policies, and utilize the other configuration and policy management features of this product.

This manual consists of the following chapters:

Chapter 1- Introduction: This chapter provides an overview of the TrafficShield Application Firewall, states the document objectives, and details how the manual is organized, specifies the targeted audience and their assumed knowledge, and includes a note about related documents.

Chapter 2 - Installation and Topology Configuration: This chapter explains how to perform an initial installation of the TrafficShield Application Firewall.

Chapter 3 - Configuration and Licensing: The installation process is followed by a network configuration stage. In this stage, you can define a Standby unit, if not defined during the installation, set static routes, and assign aliases to the network cards. This chapter focuses on these topics, as well as on additional configuration parameters and Licensing.

Chapter 4 - Web Applications: This chapter explains how to create a web application definition in the TSMS, and how to continue to maintain it.

Chapter 5 - Monitoring: This chapter describes the tools that can be used by the network and policy administrators to monitor request traffic. It also explains how to use the TrafficShield Application Firewall monitoring tools to follow up potential attacks.

Chapter 6 - Administration: This chapter describes administrative operations such as defining additional users, creating backups, restoring backups, downloading helpful utilities, and using support tools.

Glossary - The glossary provides a glossary of terms and abbreviations used throughout the document.

Audience and assumed knowledge

This document is intended for network operators and security administrators.

Related documentation

The ***TrafficShield® Security Policy User Manual*** explains how to set up a TrafficShield Application Firewall security policy and how to apply it to a Web application. The manual presents the TrafficShield® Application Firewall concepts, and shows how the concepts are implemented in the security policy context for your environment.

The ***TrafficShield® Application Firewall Release Note*** provides information on installing an upgrade (including installation limitations), rolling back an upgrade, and activating a license. The Release Note also provides information on new features and fixes, and known issues.

You can get additional technical documentation and product information from **http://tech.f5.com**, the F5® Networks Technical Support web site.

2

Installation and Topology Configuration

- Network terminology
- Installation and configuration workflow
- Installing a TrafficShield Application Firewall unit
- Configuring TrafficShield Application Firewall in a Single unit topology

Network terminology

Before you install and configure the TrafficShield Application Firewall unit, you need to determine several IP addresses. This section describes the function of each address.

TrafficShield Application Firewall private network

A TrafficShield Application Firewall private network is the network which all TrafficShield Application Firewall units use to communicate between each other for management purposes. No other network device should have an IP address in the TrafficShield Application Firewall private network.

Private IP

A Private IP address is an IP address uniquely assigned to a TrafficShield Application Firewall unit. Each unit may have only one Private IP address. TrafficShield Application Firewall assigns the Private IP address as an alias of the Eth0.11 network card. If the intended topology of the TrafficShield Application Firewall consists of more than one unit, then the internal communication between the units is based on Private IP addresses. The Private IP address must be configured as a class C network, for example, **255.255.255.0**.

Service IP

A Service IP address is the IP address at which the TrafficShield Application Firewall unit receives requests directed to the web application. In a network not protected by the TrafficShield Application Firewall, this is the IP address of the web server. After installing the TrafficShield Application Firewall, you can assign the web server's current IP address to the TrafficShield Application Firewall unit as a service IP (the Web server gets a different address).

◆ **Note**

In some cases, the Service IP address is the IP address which is mapped to the ***DNS A*** *record of the web server. Usually this is an external IP address.*

Each TrafficShield Application Firewall unit may have up to 199 different Service IP addresses and up to 200 web applications. One Service IP address may have many web applications. TrafficShield Application Firewall assigns Service IP addresses to either the Eth0.11 or Eth0.12 card, according to the unit’s installation and system configuration.

IP to Web server

An IP to Web server address is the IP address allocated on the TrafficShield Application Firewall unit for communicating with the web server. This IP address is used by all web applications. This IP address is usually an internal address. This address is disabled when the unit is in standby mode.

You can set both the IP to Web Server and the Service IP to the same address, if the Service IP addresses are attached to Eth0.11.

Server IP

A Server IP address is the IP address of the real web server to which the TrafficShield Application Firewall forwards the requests.

Trusted IP

A Trusted IP address is an IP address authorized to send to the Web server extended HTTP methods such as PUT and DELETE.

Permanent IP

A Permanent IP address is an IP address allocated to the TrafficShield Application Firewall unit that allows an Administrator to access the unit even when it is in standby mode. The Administrator is able to access a unit in standby mode using SSH, and not through the TrafficShield user interface.

One TrafficShield Application Firewall unit may have multiple Permanent IP addresses.

Permanent IP addresses may be assigned either to Eth0.11 or to Eth0.12 cards, depending on whether the Administrator intends to install and administer the unit internally or externally.

◆ **Note**

*Eth0 in the TSMS user interface is mapped to **Eth0.11** in the TrafficShield Application Firewall and Eth1 in the TSMS user interface is mapped to **Eth0.12** in the TrafficShield Application Firewall.*

Gateway

Gateway refers to the default gateway for the TrafficShield Application Firewall unit.

Alias IP

An Alias IP is an optional IP address that you can use for management purposes. This address is published only on the active unit. If the active unit fails, TrafficShield Application Firewall transfers this address to the Standby unit once it becomes active.

◆ **Note**

The Permanent IP address and the Alias IP address can be configured for the internal interface as well. Alias IP addresses may be assigned either to Eth0 or to Eth1 interfaces.

Installation and configuration workflow

You can configure TrafficShield Application Firewall in the following topologies:

- Single (Active) unit
- Primary (Active) unit with one Standby unit

In all topologies, you start the configuration by running the **tsconfig.pl** script on the common line prompt of the Active unit.

The following sections describe the installation and configuration workflow for these topologies.

Installation workflow for a Single unit topology

The following workflow describes the process required to install and configure TrafficShield Application Firewall units in a Single unit topology.

You must follow these procedures in the order given:

1. Run the **tsconfig.pl** script on the Primary unit (see *Running tsconfig.pl for the Primary (Active) unit*, on page 2-8).
2. Open the TrafficShield Management Station (TSMS) and follow the instructions of the Configuration Wizard (see *Accessing the TrafficShield Management Station*, on page 3-1).
3. Install the license using the Configuration Wizard (see *Activating the license*, on page 3-12).
4. Configure a web application (see *Web Application Wizard*, on page 4-2).

Installation workflow for a Primary with Standby unit topology

In the Primary and Standby units configuration, you install the TrafficShield Application Firewall on the two units. Both units are identical. The Standby unit is automatically activated when the active unit fails.

The following workflow describes the process required to install and configure TrafficShield Application Firewall units, including the different step-by-step procedures.

You must follow these procedures in the order given:

1. Run the **tsconfig.pl** script on the Primary unit (see *Running tsconfig.pl for the Primary (Active) unit*, on page 2-8).
2. Open the TrafficShield Management Station (TSMS) on the Primary unit (see *Accessing the TrafficShield Management Station*, on page 3-1).

3. From the TSMS on the Primary unit, use the TrafficShield Application Firewall Configuration Wizard to define the Standby unit (see *Configuring TrafficShield Application Firewall units using the configuration wizard*, on page 3-2).
4. Restart the Primary unit.
5. On the Standby unit, run the **tsconfig.pl** script (see *Running tsconfig.pl for the Standby unit*, on page 2-11).
6. From the TSMS on the Primary unit, install and activate the license (see *Activating the license*, on page 3-12).
7. Configure a web application (see *Web Application Wizard*, on page 4-2).

◆ **Important**

Configuring a web application without installing the license prevents TrafficShield Application Firewall from performing any kind of traffic blocking.

◆ **Important**

You should always install the TrafficShield Application Firewall behind a network firewall before deploying it on a network.

Installing a TrafficShield Application Firewall unit

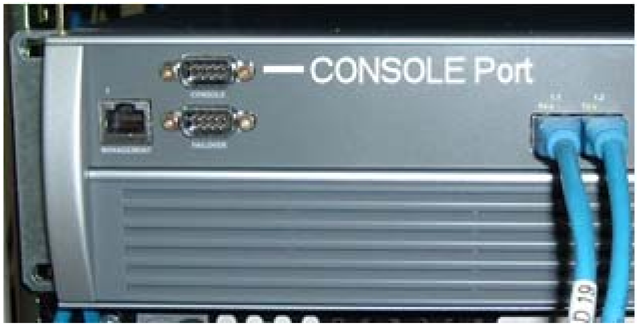
This section explains how to install a TrafficShield Application Firewall unit. This section is valid regardless of which topology you use to configure the unit.

To install a TrafficShield Application Firewall unit

1. Connect a power cable to the TrafficShield Application Firewall unit.
2. Connect the TrafficShield Application Firewall unit to the network.

   The TrafficShield Application Firewall supports two types of network configuration:

   - **(Eth0 only)** - A single network cable, plugged into the Eth0.11 card (port 1.1), connects the TrafficShield Application Firewall unit, Web server's internal network, and service network. This option may be selected when there is no security need to physically separate the client-to-unit traffic from the unit-to-web server traffic. Accordingly, the Service IP addresses should be attached to Eth0 at the System Configuration step in the graphical user interface. See Chapter 3, *Configuration and Licensing*.
   - **(Eth0 and Eth1)** - Two network cables, plugged into the Eth0 card (port 1.1) and Eth1 card (port 1.2) respectively. The Eth0 card connects the TrafficShield Application Firewall unit to the Web server's internal network and to additional TrafficShield Application units. This option ensures a total separation between external and internal traffic. Accordingly, the Service IP addresses should be attached to Eth1 at the System Configuration step in the user interface. See Chapter 3, *Configuration and Licensing*.
3. Prepare a serial console terminal.
   This can be any PC with any serial console software installed on it.
   For example: Microsoft® Hyper terminal.
4. Attach a serial cable from the serial console terminal to the RS232 serial console port on the TrafficShield Application Firewall unit's front panel. Please see photograph below.



5. Launch your serial console software per the software manufacturer's instructions.
6. Configure your serial console software as follows:
   - Bits per second: 19200
   - Data bits: 8
   - Parity: None
   - Stop bits: 8N1
7. Log on to the TrafficShield Application Firewall unit using the following user name and password:
   - User: root
   - Password: default

Configuring TrafficShield Application Firewall in a Single unit topology

This section explains how to configure TrafficShield Application Firewall in a Single unit topology, for Primary/Standby units, after they have been physically connected to the network.

Running tsconfig.pl for the Primary (Active) unit

You start configuring TrafficShield Application Firewall by running the **tsconfig.pl** script on the Primary (Active) unit. This script defines the minimal parameters needed by the TrafficShield Management Station (TSMS) to continue the configuration using the user interface.

Type **/ts/install/tsconfig.pl** and press Enter. The installation process starts. You are required to enter a series of configuration parameters.

◆ **Note**

All IP addresses and values displayed in this section are examples only. Some IP addresses entered during the configuration process may have multiple instances. In such cases, the installation program allows you to enter one address. You can later add other instances, using the TSMS.

◆ **Tip**

It is important to prepare all of the required information before beginning the configuration. If you already have TrafficShield Application Firewall installed and are upgrading to a higher version, we recommend that you save your pervious settings.

When you installed the TrafficShield Application Firewall unit, you logged in by entering the system password of the unit. This password has been delivered to you by the TrafficShield Application Firewall supplier. You can change this password now, in order to ensure maximum security.

Enter current system password:
Enter the current password.

Enter new password:
Enter a new password for the unit. This replaces the root password with your own private and secure password.

◆ **Important**

The new password must contain at least 6 characters and must be from at least two different character groups. The character groups are: uppercase, lowercase, numbers, and special characters (like ! and @).

◆ **Important**

You may not use the following special characters: **` ; | " ' ( ) &**

Re-enter new password:
Re-enter the new password.

Which TrafficShield topology would you like to configure?

(1) Single Unit topology

(2) External Load Balancer topology

The system prompts you to choose a topology.
Type **1** to configure a Single/Standby unit topology.

Which type of unit would you like to configure?

(1) Single Unit system

(2) Standby for Single Unit

Enter **1** to continue configuring the active unit.

The current system time is (12:37:52 06/01/2005). Do you want to change the system time? (y/n) [n]:
Enter **n** to accept the current date and time, or enter **y** if the date and time shown are not correct.

Please enter the current date (mm/dd/yyyy):
This and the next two questions appear if you entered **y** in the previous question. Enter the current date in the format shown in the prompt.

Please enter the current time (hh:mm:ss):
Enter the current time in the format shown in the prompt.

The new system time will be (13:38:50 09/15/2005). Is this correct? (y/n) [y]:
Confirm the new date and time by entering **y**, or enter n to restart the date-time entry cycle.

Please enter the TrafficShield private network [192.168.223.0]:
Specify the unit's private network address (first 3 octets of the unit's IP address, followed by zero).

Please complete TrafficShield private IP [192.168.223.X].
Complete the unit's private IP address by entering the last octet.

◆ **Important**

*You cannot use **253** as the last octet of the unit's private IP address.*

Would you like to set permanent IP? (y/n) [n]:
Enter **y** if you want to define a permanent IP address for the unit.

Enter permanent IP:
Enter the permanent IP address, for example, **192.168.1.237**.

Enter permanent IP Mask [255.255.255.0]:
Enter the network IP mask for the permanent IP. Press Enter to accept **255.255.255.0** as the permanent IP mask.

Enter network interface (eth) [0, 1]
Specify the network interface card through which the TrafficShield Application Firewall user will access the TrafficShield Application Firewall unit. Enter **0** for interface 1.1 (eth0) or **1** for interface 1.2 (eth1).

◆ **Important**

*If you are only using one network connection, it must be connected to the 1.1 network port and you must type **0** here.*

Would you like to set a static route for the permanent IP? (y/n) [y]:
Enter y if you want to define a static route.

Enter Destination Network:
If you answered **y** to the previous question, specify the network address of the internal network from where the permanent IP can be accessed.

Enter Netmask [255.255.255.0]:
Enter the network mask of the internal network's address.

Enter Gateway:
Enter the gateway address.

Please enter the TrafficShield web administrator's access IP/Network (remote manager host):
You activate the TrafficShield Management Station user interface through a Web browser from any PC on the network to which the unit is connected. Specify the IP address of the PC from which you will access the TSMS in order to define policies. You can define the network as well. This would define the network or a single host, from which both the TSMS user interface and CLI may be accessed.

Please enter the Access IP/Network netmask [255.255.255.0]:
Specify the network address and network mask for the Web administrator's access IP address.

Please enter the initial TrafficShield Web administrator's username:
Enter the user name to specify when accessing the TrafficShield Management Station using its Web interface.

Please enter the initial TrafficShield Web administrator's password:
Enter the password to specify when accessing the TrafficShield Management Station using its Web interface.

Important

The new password must contain at least 6 characters and must be from at least two different character groups. The character groups are: uppercase, lowercase, numbers, and special characters (like ! and @).

Important

You may not use the following special characters: ` ; | " ' ( ) &

Please confirm password:
Re-enter the password.

Please confirm the following settings:
Examine the settings displayed. Enter **y** to confirm them or **n** to restart the configuration cycle.

Would you like to apply these settings (y/n) [y]
Enter **y** to apply the settings to the single unit.

The script is run and the TrafficShield Application Firewall Active unit is configured. Upon completion, you are prompted that the configuration finished successfully.

To complete the single unit installation, please start the TSMS user interface (see *Accessing the TrafficShield Management Station*, on page 3-1).

To install a Standby unit, use the procedure described in the following section.

Running tsconfig.pl for the Standby unit

The Primary (Active) unit must be configured before you configure the Standby unit.

To configure the Standby unit

1. Configure the Standby unit in the TSMS application.
2. Restart the Primary (Active) unit.
3. Run the **/ts/install/tsconfig.pl** script on the Standby unit

Important

*Verify that you configured the Standby unit in the TSMS user interface and restarted the Primary (Active) unit machine before running **tsconfig.pl** on the Standby unit, otherwise the Primary unit does not recognize the Standby unit.*

To run the **tsconfig.pl** script on the Standby unit, type **/ts/install/tsconfig.pl** and press Enter. The installation process starts.

Enter current system password:
Enter the system password of the unit. This password was delivered to you by the TrafficShield Application Firewall supplier.

Enter new password:
Enter a new password for the unit. This replaces the root password with your own private and secure password.

◆ **Important**

The new password must contain at least 6 characters and must be from at least two different character groups. The character groups are: uppercase, lowercase, numbers, and special characters (like ! and @).

◆ **Important**

You may not use the following special characters: **` ; | " ' ( ) &**

◆ **Important**

The password for the standby unit must be the same as the password for the primary unit.

Re-enter new password:
Re-enter the new password.

Which TrafficShield topology would you like to configure?

(1) Single Unit topology

(2) External Load Balancer topology

The system prompts you to choose a topology.
Type **1** to configure a Single/Standby unit topology.

Which type of unit would you like to configure?

(1) Single Unit system

(2) Standby for Single Unit

Type **2** to configure a Standby unit.

Please enter the TrafficShield private network [192.168.223.0]:
Specify the standby unit's private network address (first 3 octets of the unit's IP address, followed by zero).

◆ **Important**

This Private Network must be the same as the Active unit Private network. These IP addresses should not be used by other non-TrafficShield Application Firewall machines.

Please complete TrafficShield private IP [192.168.223.X]:
Complete the Standby unit's private IP address by entering the last octet of the unit's IP address in the private network.

◆ **Important**

You cannot use ***253*** *as the last octet of the unit's private IP address.*

◆ **Important**

The Standby unit's private IP address must be different from that defined on the Active unit.

Would you like to set permanent IP? (y/n) [n]:
If you want to set a permanent IP address for the standby unit as well, enter **y**.

Enter permanent IP:
Enter the permanent IP address of the standby unit, for example **192.168.1.237**.

Enter permanent IP mask
Enter the network mask for the permanent IP of the standby unit.

Enter network interface (eth)
Specify the network interface card through which the TrafficShield Application Firewall user will access the TrafficShield Application Firewall unit. Enter **0** for 1.1 (eth0), or **1** for 1.2 (eth1).

◆ **Important**

If you are only using one network connection it must be connected to the 1.1 network port and you must enter ***0*** *here.*

Would you like to set a static route for the permanent IP? (y/n) [y]:
Enter **y** if you want to define a static route.

Enter destination network:
If you answered **y** to the previous question, specify the network address of the internal network from where the permanent IP can be accessed.

Enter Netmask:
Enter the network mask of the internal network's address.

Enter Gateway:
Enter the gateway address.

Please confirm the following settings:
Examine the settings displayed. Enter **y** to confirm them or **n** to restart the Standby unit configuration cycle.

Would you like to apply these settings (y/n) [y]
Enter **y** to apply the settings to the Standby unit.

The script is run and the TrafficShield Application Firewall Standby unit is configured. Upon completion, you are prompted that the configuration finished successfully.

3

Configuration and Licensing

- Accessing the TrafficShield Management Station
- Configuring TrafficShield Application Firewall units using the configuration wizard
- Configuring TrafficShield Application Firewall units manually
- Licensing

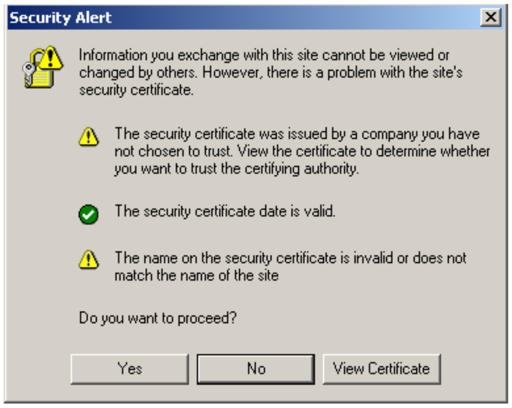
Accessing the TrafficShield Management Station

You may perform TrafficShield® Application Firewall configuration, in addition to many other functions, through the TrafficShield Application Firewall user interface, called the TrafficShield Management Station (TSMS).

To access the TSMS

1. On a PC from which the TrafficShield Application Firewall unit can be reached, use your Web browser to connect to the TrafficShield Application Firewall management portal. Point your Web browser to the TrafficShield Application Firewall Permanent IP specified during the initial configuration script. Use the custom SSL port 1043:
   Example: **https://172.20.221.1:1043**

   A security alert message may appear.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

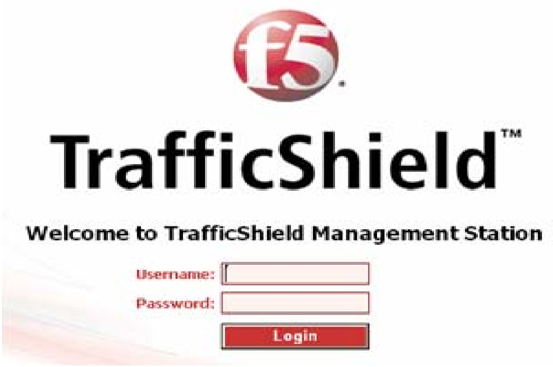
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

2. Click **Yes** to continue. The logon screen opens.



3. Enter the TrafficShield Application Firewall Web Administrator's user name and password that you defined while you ran the **tsconfig.pl** script, and click **Login**.

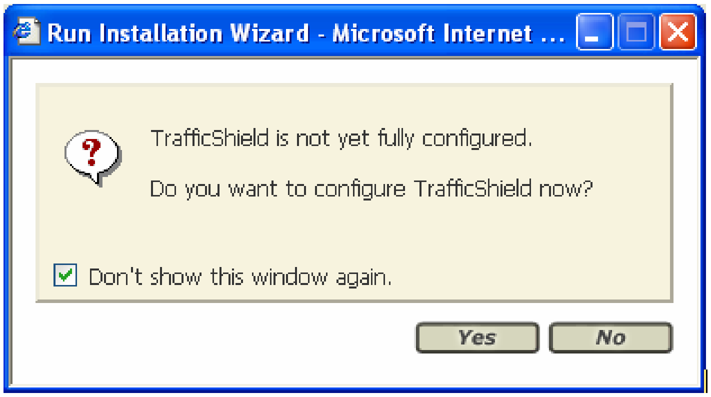
Configuring TrafficShield Application Firewall units using the configuration wizard

After installing the TrafficShield Application Firewall unit, the next tasks are: configuring the TrafficShield Application Firewall unit, activating the license, and creating/configuring Web applications. Creating and configuring Web applications is discussed in Chapter 4, *Web Applications*.

TrafficShield Management Station (TSMS) offers a wizard that you can use to configure the unit according to the required network configuration. Using this wizard is mandatory for the initial TrafficShield Application Firewall installation. All the information you see entered into the Wizard's fields of the various sample screens in this Manual is for demonstration purposes only

First-time access

When you access TSMS for the first time, or after re-installing the unit software, the Configuration wizard starts automatically and asks you whether you want to configure the TrafficShield Application Firewall unit.



Run Installation Wizard - Microsoft Internet ...

TrafficShield is not yet fully configured.

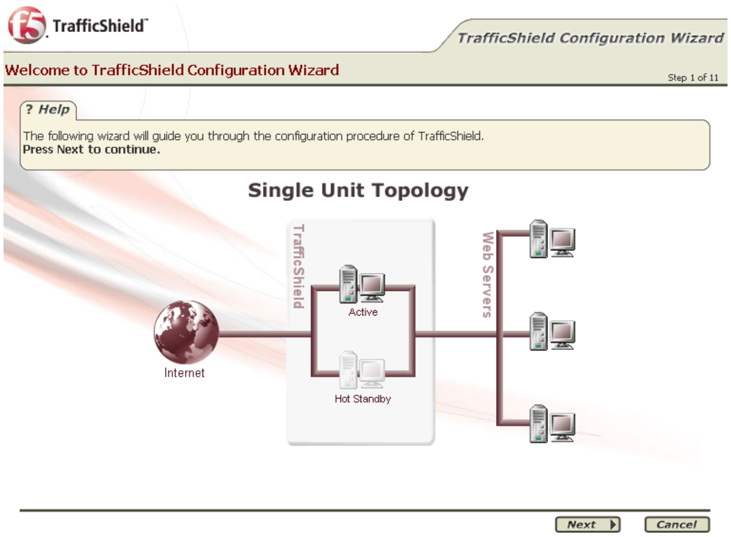
Do you want to configure TrafficShield now?

☑ Don't show this window again.

The following pages describe the steps of the wizard.

To configure TrafficShield Application Firewall using the Configuration wizard

1. Click **Yes** to start the wizard.
   The TrafficShield Configuration Wizard Step 1 screen appears.



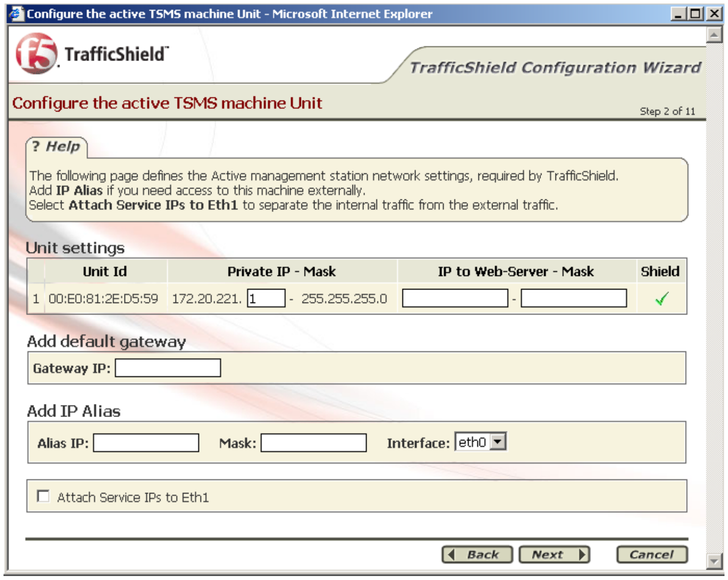
Welcome to TrafficShield Configuration Wizard

Step 1 of 11

? Help

The following wizard will guide you through the configuration procedure of TrafficShield.
Press Next to continue.

2. Click **Next**.
   The TrafficShield Configuration Wizard Step 2 screen appears.


Configure the active TSMS machine Unit - Microsoft Internet Explorer
TrafficShield
TrafficShield Configuration Wizard
Back
Next
Cancel

Configure the active TSMS machine Unit

Step 2 of 11

? Help

The following page defines the Active management station network settings, required by TrafficShield.
Add **IP Alias** if you need access to this machine externally.
Select **Attach Service IPs to Eth1** to separate the internal traffic from the external traffic.

Unit settings

	Unit Id	Private IP - Mask	IP to Web-Server - Mask	Shield
1	00:E0:81:2E:D5:59	172.20.221. 1 - 255.255.255.0	-	✓

Add default gateway

Gateway IP:

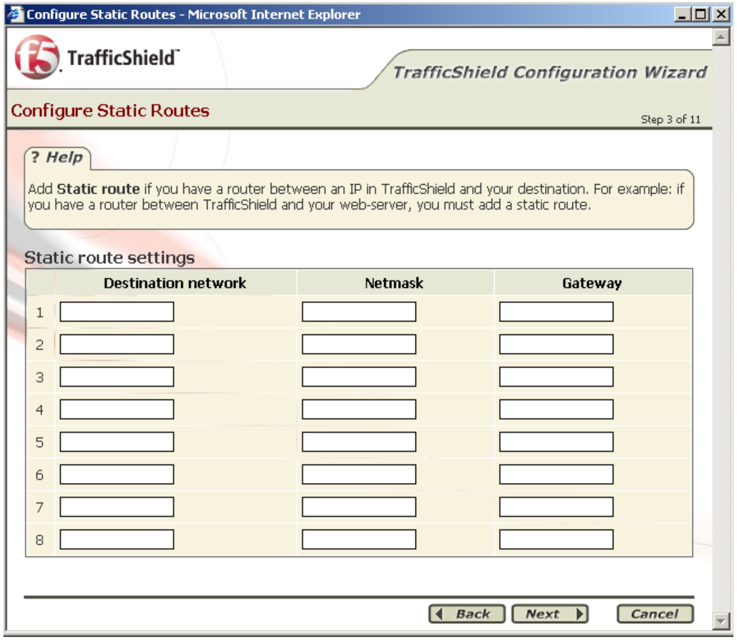
Add IP Alias

Alias IP: Mask: Interface: eth0

☐ Attach Service IPs to Eth1

3. Fill in the required IP addresses. Please note that you must enter the IP to Web-Server address and its Mask.

4. Click **Next**.
   The TrafficShield Configuration Wizard Step 3 screen appears.
   If a router is located between the TrafficShield Application Firewall unit and the web-server, you can use this screen to configure a static route for the web server machine.


Configure Static Routes - Microsoft Internet Explorer
TrafficShield™
TrafficShield Configuration Wizard

Configure Static Routes

Step 3 of 11

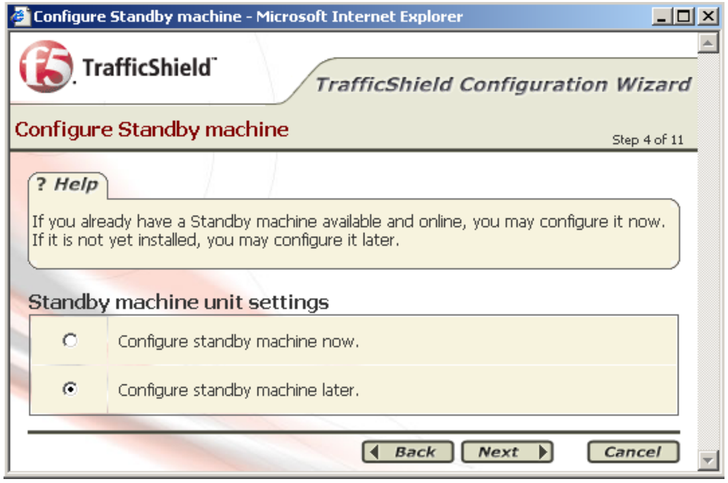
? Help

Add **Static route** if you have a router between an IP in TrafficShield and your destination. For example: if you have a router between TrafficShield and your web-server, you must add a static route.

Static route settings

	Destination network	Netmask	Gateway
1			
2			
3			
4			
5			
6			
7			
8			

5. Click **Next**.
   The TrafficShield Configuration Wizard Step 4 screen appears.


Configure Standby machine - Microsoft Internet Explorer
TrafficShield™
TrafficShield Configuration Wizard

Configure Standby machine

Step 4 of 11

? Help

If you already have a Standby machine available and online, you may configure it now. If it is not yet installed, you may configure it later.

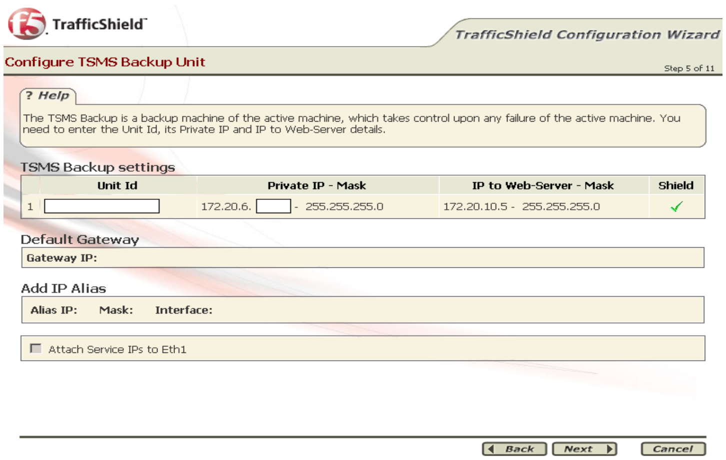
Standby machine unit settings

○ Configure standby machine now.

● Configure standby machine later.

6. Decide whether you want to configure the Standby unit now or later.

If you want to configure the Standby machine, select **Configure standby machine now**, and click **Next**.
Fill in the **Unit ID**, and complete the **Private IP**.



Configure TSMS Backup Unit

Step 5 of 11

? Help

The TSMS Backup is a backup machine of the active machine, which takes control upon any failure of the active machine. You need to enter the Unit Id, its Private IP and IP to Web-Server details.

TSMS Backup settings

	Unit Id	Private IP - Mask	IP to Web-Server - Mask	Shield
1		172.20.6. - 255.255.255.0	172.20.10.5 - 255.255.255.0	✓

Default Gateway

Gateway IP:

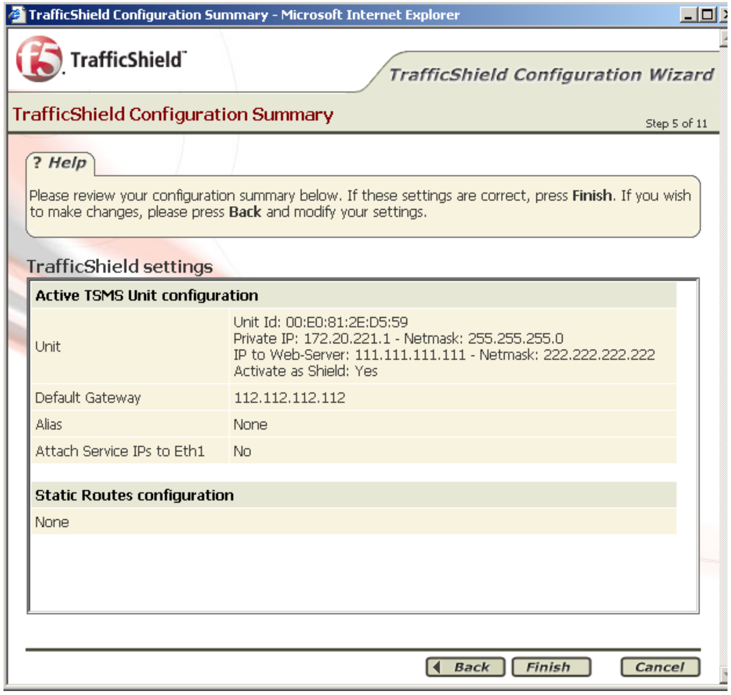
Add IP Alias

Alias IP: Mask: Interface:

□ Attach Service IPs to Eth1

Alternately, if you want to configure only the Primary unit, select **Configure standby machine later**.

7. Click **Next**.
   The TrafficShield Configuration Wizard Summary screen appears. If you only configured the Primary unit, you see a summary of the Active TSMS unit configuration settings. If you also configured a Backup unit, you also see a summary of the TSMS Backup unit configuration settings on this screen.


TrafficShield Configuration Summary - Microsoft Internet Explorer
TrafficShield
TrafficShield Configuration Wizard
Back
Finish
Cancel

TrafficShield Configuration Summary

Step 5 of 11

? Help

Please review your configuration summary below. If these settings are correct, press **Finish**. If you wish to make changes, please press **Back** and modify your settings.

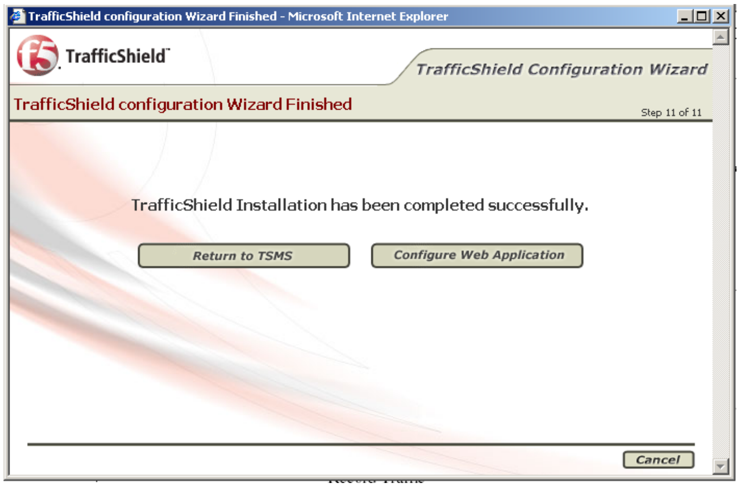
TrafficShield settings

Active TSMS Unit configuration	
Unit	Unit Id: 00:E0:81:2E:D5:59 Private IP: 172.20.221.1 - Netmask: 255.255.255.0 IP to Web-Server: 111.111.111.111 - Netmask: 222.222.222.222 Activate as Shield: Yes
Default Gateway	112.112.112.112
Alias	None
Attach Service IPs to Eth1	No

Static Routes configuration

None

8. Click **Finish** to confirm the unit configuration settings.
   The TrafficShield Configuration Wizard last screen appears, offering you the choice of either returning to TSMS or configuring a new web application. You may choose either option at this stage. Configuring a web application is discussed in the section *Web Application Wizard*, on page 4-2.


TrafficShield configuration Wizard Finished - Microsoft Internet Explorer
TrafficShield™
TrafficShield Configuration Wizard
Return to TSMS
Configure Web Application
Cancel

TrafficShield configuration Wizard Finished

Step 11 of 11

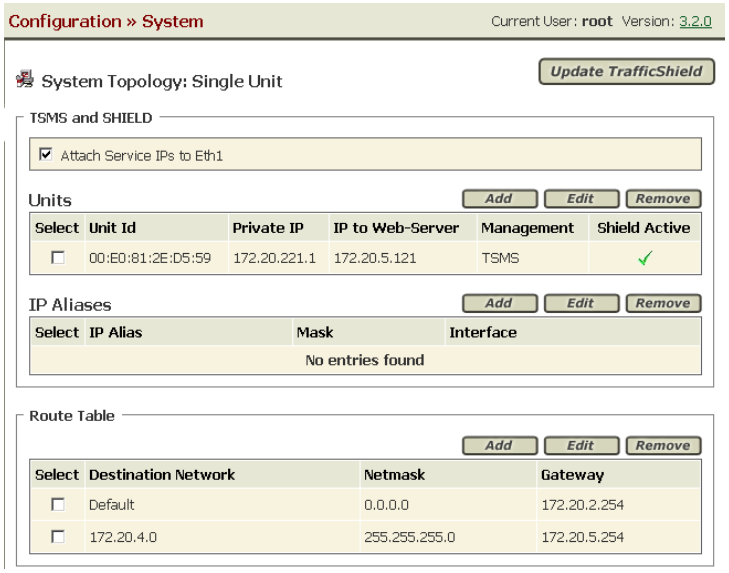
TrafficShield Installation has been completed successfully.

9. Restart the unit.

Configuring TrafficShield Application Firewall units manually

To manually configure TrafficShield Application Firewall from the TSMS, select **Administration > Configuration > System**. The Configuration-System screen opens.

Click the icon to reconfigure TrafficShield Application Firewall using the Installation wizard. The TrafficShield Configuration Wizard is discussed in *Configuring TrafficShield Application Firewall units using the configuration wizard*, on page 3-2



Configuration » System

Current User: **root** Version: 3.2.0

System Topology: Single Unit

TSMS and SHIELD

☑ Attach Service IPs to Eth1

Units

Select	Unit Id	Private IP	IP to Web-Server	Management	Shield Active
□	00:E0:81:2E:D5:59	172.20.221.1	172.20.5.121	TSMS	✓

IP Aliases

Select	IP Alias	Mask	Interface
	No entries found		

Route Table

Select	Destination Network	Netmask	Gateway
□	Default	0.0.0.0	172.20.2.254
□	172.20.4.0	255.255.255.0	172.20.5.254

The Configuration-System screen includes the following sections:

- TSMS and Shield
- Units
- IP Aliases
- Route Table

TSMS and Shield

Check the **Attach service IPs to ETH1** check box to channel the service traffic to the second network (eth1) card.

Important

*If you check the **Attach service IPs to ETH1** check box, make sure that both ports 1.1 and 1.2 are connected (port 1.1 to the internal network and port 1.2 to the external network.)*

Units

In the Units section you can perform the following:

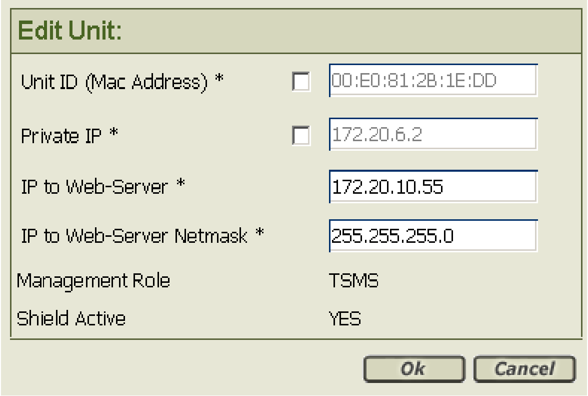
- Add the IP to Web-Server address and the IP to Web-Server network mask for the TrafficShield Application Firewall unit, if you did not define it using the TrafficShield Application Firewall unit configuration wizard.
- Add the MAC address and the Private IP address for the Standby unit.

◆ **Tip**

*To obtain the MAC address of the Standby unit, from the console of the Standby unit, run the command **ifconfig eth0.11**. The address that appears after **HWaddr** is the MAC address.*

To manually add the IP to Web-Server and IP to Web-Server Netmask to a configured unit

1. In the Units section, select the unit for which you want to add the addresses, and click **Edit**.
   The Edit Unit screen opens.



Edit Unit:

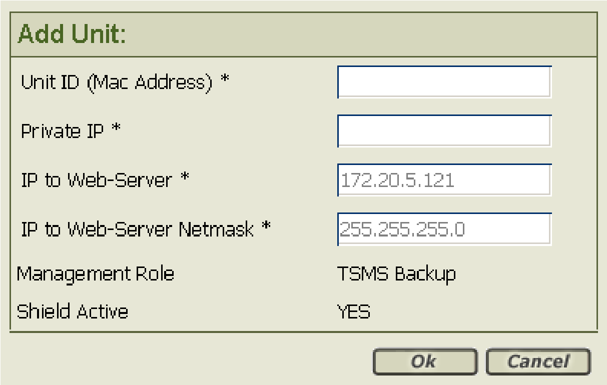
Unit ID (Mac Address) *	☐	00:E0:81:2B:1E:DD
Private IP *	☐	172.20.6.2
IP to Web-Server *		172.20.10.55
IP to Web-Server Netmask *		255.255.255.0
Management Role		TSMS
Shield Active		YES

2. Enter the unit's IP to Web-Server address and its IP to Web-Server netmask.

3. Click **OK**.

To manually add the Standby unit

1. In the Units section, click **Add**.
   The Add Unit screen opens.



Add Unit:

Unit ID (Mac Address) *	
Private IP *	
IP to Web-Server *	172.20.5.121
IP to Web-Server Netmask *	255.255.255.0
Management Role	TSMS Backup
Shield Active	YES

2. Enter the unit's ID (MAC address) and its private IP address.

   Important: *You cannot use* ***253*** *as the last octet of the unit's private IP address.*

   Important: *Both the main (Active) and Standby units use the same IP address to Web-server address.*

   For more information about configuring a Standby unit, see *Running tsconfig.pl for the Standby unit*, on page 2-11.

3. Click **OK**.

IP aliases

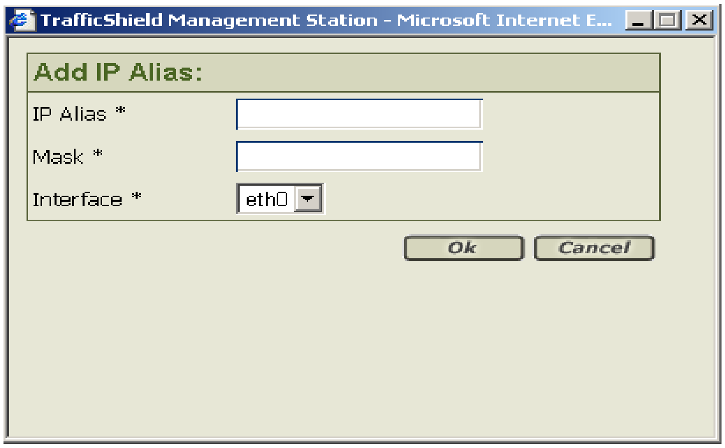
The IP aliases section is designed to assign additional IP addresses to one of the network cards, for management purposes. For example, you may want to access the TSMS user interface using an alias or directly by SSH.

◆ **Note**

The alias IP address is automatically directed to the Active unit and is replicated to the Standby unit in case the Active unit fails.

To assign IP addresses to the network card

1. In the IP Aliases section, click **Add**.
   The Add IP Alias dialog box opens.



2. Enter the following information:
   IP Alias: Specify the IP address.
   Mask: Specify the network mask.
   Interface: Select the network card to which you want to assign this address.
3. Click **OK**.
   The IP alias definition appears on the main page.
4. Repeat the above procedure for all the aliases you intend to use.
5. When you are done, click **Update TrafficShield**.
   Upon completion, a message appears informing you about the successful update.

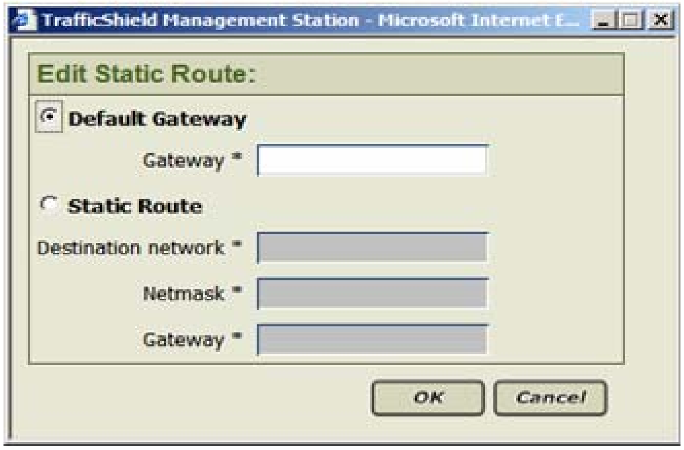
Route table

If a gateway different from the default gateway exists in your network, use the Static Route feature to specify the gateway details.
TrafficShield Application Firewall looks first for the static route and uses the default gateway if it does not find one.

The procedure described below allows you to add more routes.

To enter or modify static routes

1. In the **Route Table** section, click the **Add** button or select the unit by checking the check box located to the left of the relevant unit and click the **Edit** button.
   The Add or Edit Static Route dialog box opens.



TrafficShield Management Station - Microsoft Internet E...

Edit Static Route:

● Default Gateway

Gateway *

○ Static Route

Destination network *

Netmask *

Gateway *

2. You can handle incoming requests either using the default gateway or a static route of your choice.

   a) If you chose to accept requests using the default gateway, select **Default Gateway**, and in the Gateway box, enter its IP address.

   b) If you chose to accept requests using another route, select **Static Route**, and enter the following information:
   Destination Network: Specify the destination network address which the gateway is used for.
   Netmask: Specify the network mask.
   Gateway: Specify the gateway's IP address.

3. Click **OK**.
   The static route definition appears on the main page.

4. Repeat the above procedure for all the static routes you intend to use.

5. When you are done, click **Update TrafficShield**.

Licensing

The TrafficShield Application Firewall comes with a registration key which is used to generate a dossier, which is used to retrieve a license from the F5 License server. The license is then installed to the product. The license must be activated before you are allowed to administer core functions of the product.

You may also need to activate the license after changing the TrafficShield Application Firewall, for example, after upgrading it.

When you acquire a TrafficShield Application Firewall for the first time, the TrafficShield Application Firewall units are delivered to you with a registration key recorded in them, and therefore, you do not need to obtain one. In any other case where the license should be updated, you need to obtain the registration key before you can activate the license.

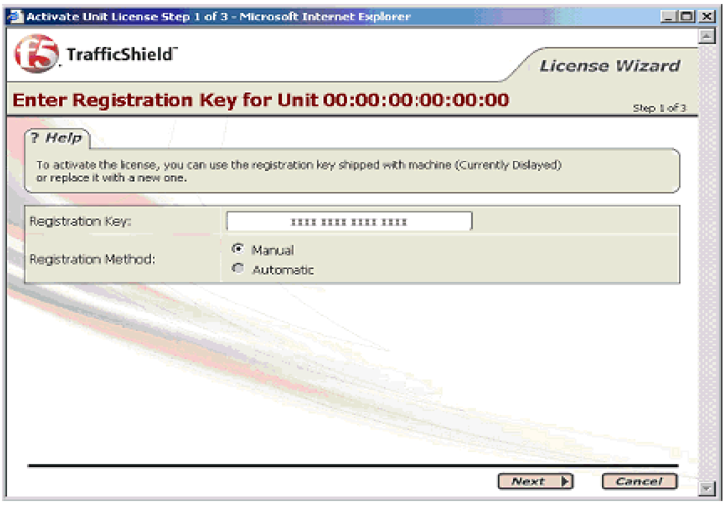
◆ **Important**

If the license expires, you are alerted by a system event. TrafficShield Application Firewall avoids blocking of any kind, and most of the TSMS user interface becomes inaccessible. However, you are able to view the Monitoring Events screen and the Licensing screen in order to renew the license.

Activating the license

To activate the license

1. From the TSMS, select **Administration > Maintenance > Licensing**.
   A list of the installed TrafficShield Application Firewall units appears. You need to license each unit separately.
2. Click **Activate License** next to the unit you want to activate. This starts the License Wizard, and opens the Enter Registration Key screen.


Activate Unit License Step 1 of 3 - Microsoft Internet Explorer
TrafficShield
License Wizard
Step 1 of 3
? Help
Next
Cancel

Enter Registration Key for Unit 00:00:00:00:00:00

To activate the license, you can use the registration key shipped with machine (Currently Dislayed) or replace it with a new one.

Registration Key: xxxx xxxx xxxx xxxx

Registration Method: ● Manual ○ Automatic

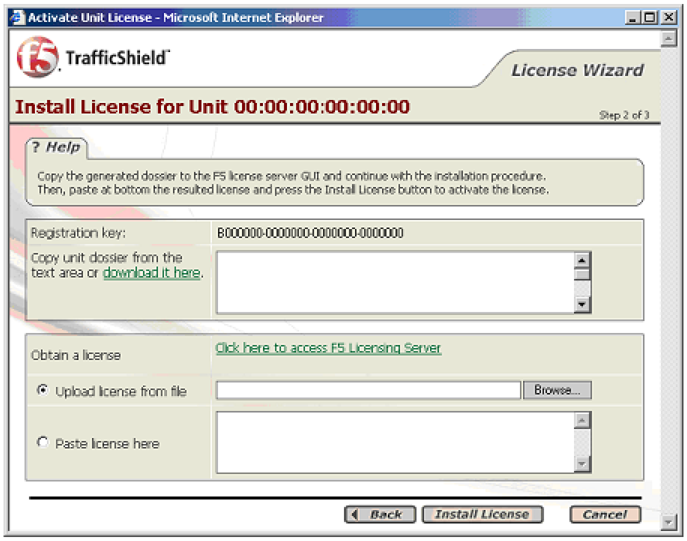
The Registration Key box displays the key currently stored in the selected TrafficShield Application Firewall unit.
You have two options: **Manual** or **Automatic**.

3. To download the license automatically from the F5 server, select **Automatic** and then click **Next**. The license is automatically downloaded, and the license activation procedure is complete.
   Important: *In order to download the license automatically from the F5 server, you must be working on a computer that has access to the Internet.*

4. If you select **Manual**, do one of the following:

   - If this is your first licensing, click **Next**.

   - If you are performing the licensing operation as a result of system changes that require a new registration key, enter the key in the **Registration Key** box, and click **Next**.
     The Install License for Unit screen appears.



Install License for Unit 00:00:00:00:00:00

Copy the generated dossier to the F5 license server GUI and continue with the installation procedure. Then, paste at bottom the resulted license and press the Install License button to activate the license.

Registration key: B000000-0000000-0000000-0000000

Copy unit dossier from the text area or download it here.

Obtain a license: Click here to access F5 Licensing Server

● Upload license from file

○ Paste license here

This screen displays a dossier that you need to save on your computer. You will use it in subsequent steps.

***Note:** The dossier is an encryption of a string containing a set of physical hardware elements of the machine.*

5. Choose either option:

   To save the dossier information in a file for loading the F5 License Activation Screen:

   a) Click the **download it here** link.
   The File download screen opens.

   b) Click **Save**.
   The Save As screen opens.

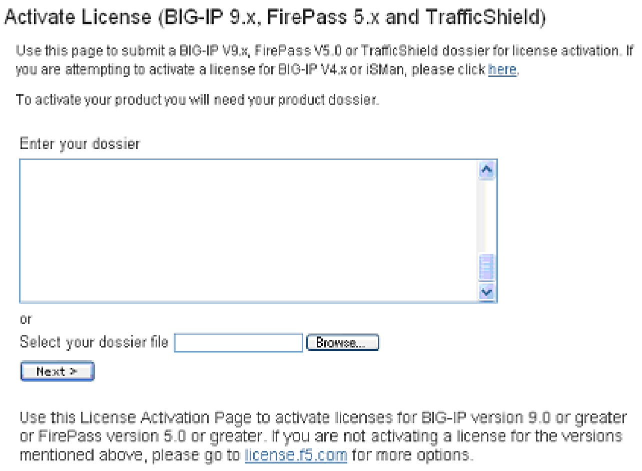
   c) Select a location on your computer where you would like the **dossier.txt** file to be saved.

   d) Click **Save**.
   The dossier information is saved and you are returned to the Install License for Unit screen.

   -Or-
   To copy the dossier information directly to the F5 license activation screen:

   a) Copy the dossier information from the text area. You will paste this information in another screen.

6. Click the **Click here to access F5 Licensing Server** link.
   A new browser window opens and connects you to the F5 licensing server.



Activate License (BIG-IP 9.x, FirePass 5.x and TrafficShield)

Use this page to submit a BIG-IP V9.x, FirePass V5.0 or TrafficShield dossier for license activation. If you are attempting to activate a license for BIG-IP V4.x or iSMan, please click here.

To activate your product you will need your product dossier.

Enter your dossier

or

Select your dossier file

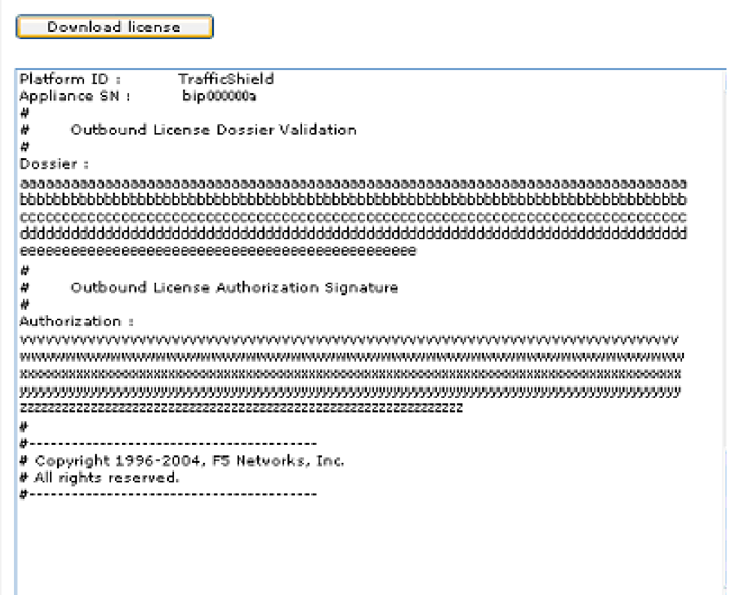
Use this License Activation Page to activate licenses for BIG-IP version 9.0 or greater or FirePass version 5.0 or greater. If you are not activating a license for the versions mentioned above, please go to license.f5.com for more options.

7. Save your information in the way consistent with your previous choice:

   - If you saved the dossier information to a file, click **Browse** to load the file.

- If you copied the dossier information, paste it in the dossier window.

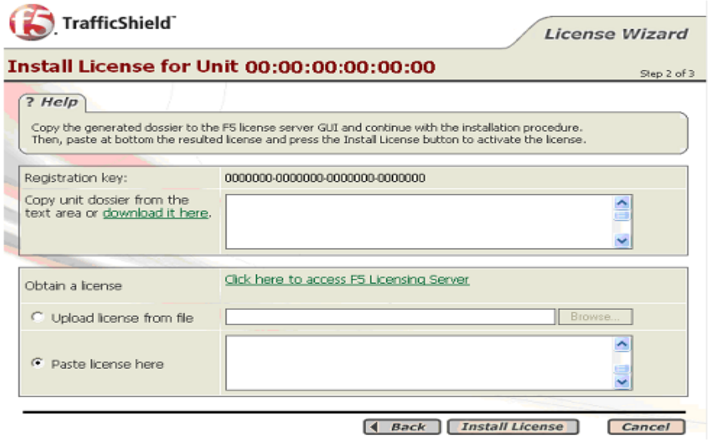
8. Click **Next** to continue.
   The dossier information is processed and the following F5 Networks licensing screen is displayed.



```
Platform ID :        TrafficShield
Appliance SN :        bip000000a
#
#      Outbound License Dossier Validation
#
Dossier :
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
dddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddd
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
#
#      Outbound License Authorization Signature
#
Authorization :
vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
#
#----------------------------------------
# Copyright 1996-2004, F5 Networks, Inc.
# All rights reserved.
#----------------------------------------
```

9. Copy the full form to the Clipboard, or click **Download license** to download a copy of the license file.

10. Return to the TSMS Install License for Unit screen.



Install License for Unit 00:00:00:00:00:00

Step 2 of 3

? Help

Copy the generated dossier to the F5 license server GUI and continue with the installation procedure.
Then, paste at bottom the resulted license and press the Install License button to activate the license.

Registration key: 0000000-0000000-0000000-0000000

Copy unit dossier from the text area or download it here.

Obtain a license — Click here to access F5 Licensing Server

○ Upload license from file

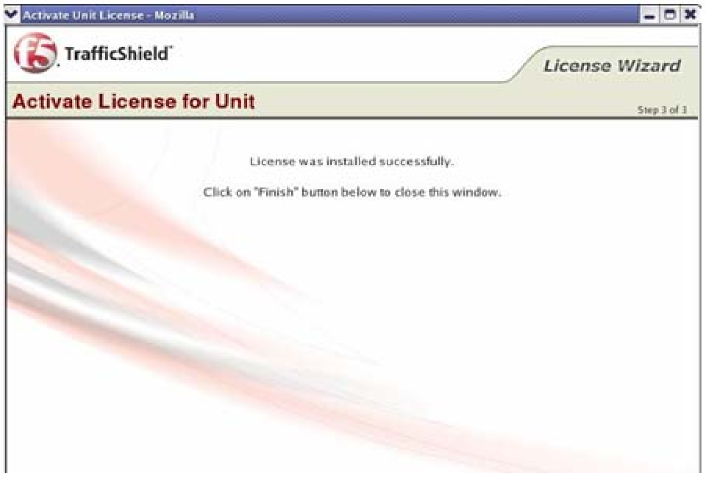
● Paste license here

11. You must now enter the license information received from F5.

- If you downloaded the information and saved it in a file, select **Upload license from file**, click **Browse**, and select the license file created by the F5 licensing server.

- If you copied the file to the Clipboard, select **Paste license here**, and paste the contents of the license file.

12. Click **Install License**.
    The Activate License for Unit screen appears.



License was installed successfully.

Click on "Finish" button below to close this window.

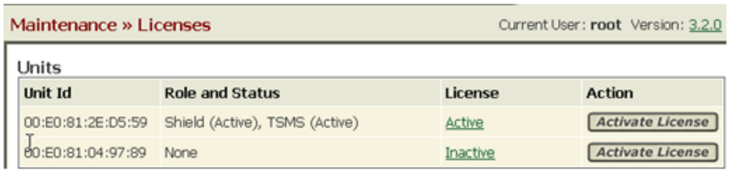
13. Click **Back** to return to previous step.
14. Click **Finish** to close the screen.

Viewing the license information

You can view the details of a specific license.

To view License Information

1. From the TSMS, select **Administration > Maintenance > Licensing**.
2. Click the **Active** link of the license about which you want to view information.



Units

Unit Id	Role and Status	License	Action
00:E0:81:2E:D5:59	Shield (Active), TSMS (Active)	Active	Activate License
00:E0:81:04:97:89	None	Inactive	Activate License

The Currently Installed License screen displays the full license details.

4

Web Applications

Defining a new web application

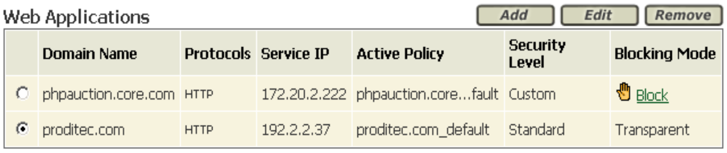
This section explains how to create and define a new web application in the F5® Networks TrafficShield® Management Station (TSMS) using the Web Application Wizard that guides you step-by-step through the required procedures.

To configure or maintain an existing web application, or remove any of its definitions, see *Editing an existing web application*, on page 4-12.

TrafficShield Application Firewall only allows traffic that is routed through it to known web applications. In other words, each web application sitting behind the TrafficShield Application Firewall in the network must be defined individually.

To define a new web application

1. From the TSMS screen, select **Administration > Configuration > Web Applications**.
   If this is not the first time you are defining a web application, a list of existing web application definitions will be displayed.



Web Applications

	Domain Name	Protocols	Service IP	Active Policy	Security Level	Blocking Mode
○	phpauction.core.com	HTTP	172.20.2.222	phpauction.core...fault	Custom	Block
●	proditec.com	HTTP	192.2.2.37	proditec.com_default	Standard	Transparent

2. Click **Add** to open the Web Application Wizard
   The Web Application Wizard Step 1 page appears.

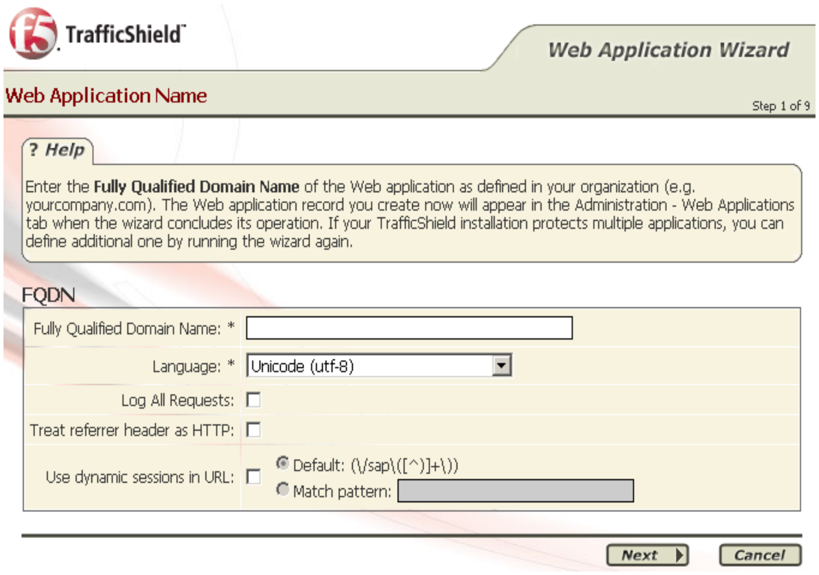
Web Application Wizard

All the information you see entered into the wizard's fields of the various sample screens in this Manual is for demonstration purposes only.

Web Application Wizard will guide you through the entire process of defining a new web application.

Step 1: Web Application Name

In the Web Application Wizard Step 1 screen, you define the name of the web application, its Fully Qualified Domain Name (FQDN), its language/encoding, whether it will log all requests, whether to treat the Referrer header as HTTP, and whether to use dynamic sessions in the URL or not.



Web Application Name

Step 1 of 9

? Help

Enter the **Fully Qualified Domain Name** of the Web application as defined in your organization (e.g. yourcompany.com). The Web application record you create now will appear in the Administration - Web Applications tab when the wizard concludes its operation. If your TrafficShield installation protects multiple applications, you can define additional one by running the wizard again.

FQDN

Fully Qualified Domain Name: *	
Language: *	Unicode (utf-8)
Log All Requests:	□
Treat referrer header as HTTP:	□
Use dynamic sessions in URL:	□ ● Default: (\/sap\([^)]+\)) ○ Match pattern:

To define the Web Application Name

Fill in the appropriate details in the following fields.

Fully Qualified Domain Name (FQDN)
To define the Fully Qualified Domain Name, enter the fully qualified domain name (FQDN) of the web application as defined in your organization (for example, **www.siterequest.com**).

Language/encoding
From the Language box, select the web application Primary language encoding.

Log All Requests
Check the **Log All Requests** check box to log all requests, including the valid ones. The requests are logged to the Policy Management > Forensics > Illegal requests screen. The valid requests are used to fill in the blanks when investigating gaps between illegal

requests. Both types of requests can be filtered out. Valid requests are marked with a green checkmark, and invalid requests are marked with a red X.

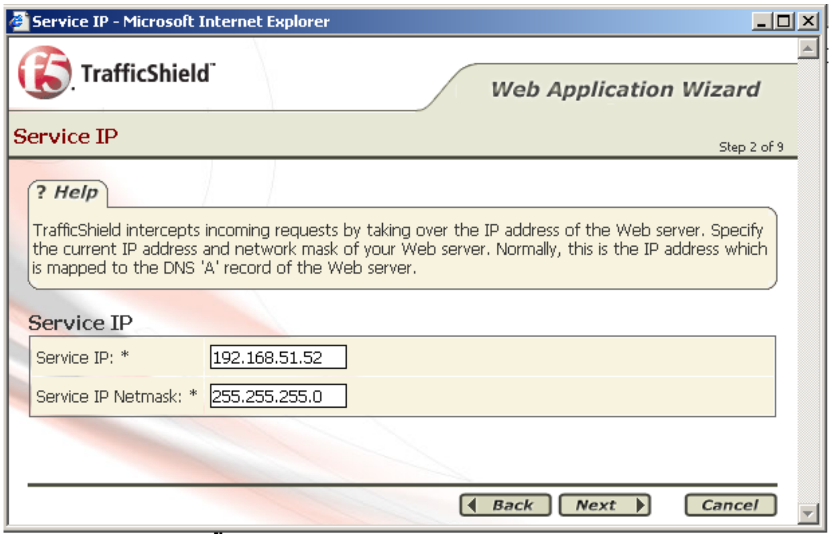
Treat Referrer header as HTTP
Check the **Treat Referrer header as HTTP** check box if required. TrafficShield Application Firewall may forward HTTP traffic even though the web application uses SSL (for example, if a Load Balancer applies an SSL termination), in which case the policy contains only HTTP objects. The Learning module considers the referrer header which may include an SSL object. In cases like this, be sure to select the **Treat Referrer option as HTTP** check box in order to prevent problems in the Learning process.

Use dynamic sessions in URL
Check the **Use dynamic sessions in URL** check box if you are using SAP or an application which will insert a dynamic session in the request's URL. Then, select either **Default** or **Match pattern**, and enter a string that matches the dynamic parameter in the URL.

Click **Next** to continue.

Step 2: Service IP

In the Web Application Wizard Step 2 screen, you define the Web Application IP address and the corresponding network mask.



TrafficShield intercepts incoming requests by taking over the IP address of the Web server. Specify the current IP address and network mask of your Web server. Normally, this is the IP address which is mapped to the DNS 'A' record of the Web server.

Service IP

Service IP: * 192.168.51.52

Service IP Netmask: * 255.255.255.0

To define the Service IP and Service IP Netmask

Fill in the appropriate details in the following fields.

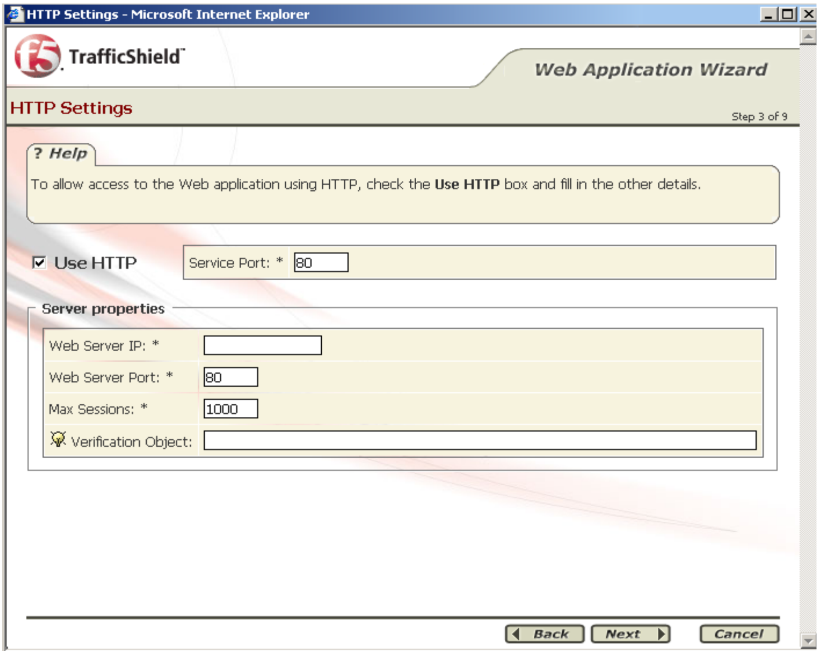
Service IP
Enter the web application IP address.

Service IP Netmask
Enter the corresponding network mask.

Click **Back** to go back to the previous step or **Next** to continue.

Step 3: HTTP Settings

In the Web Application Wizard Step 3 screen, you define the web application HTTP settings.



To allow access to the Web application using HTTP, check the **Use HTTP** box and fill in the other details.

☑ Use HTTP

Service Port: * 80

Server properties

Web Server IP: *

Web Server Port: * 80

Max Sessions: * 1000

Verification Object:

To define the Web Application HTTP Settings

Fill in the appropriate details in the following fields.

Use HTTP
To allow HTTP access to the web application, check the **Use HTTP** check box and enter the appropriate information.

◆ **Important**

You must configure at least one protocol: HTTP or HTTPS (see the next step).

Service Port
For the HTTP protocol, the service port **80** is automatically entered.

Web Server IP
Specify the web server's IP address on which the application resides.

Web Server Port
Specify the web server's port.

Max. Sessions
Specify the maximum number of simultaneous sessions TrafficShield Application Firewall can open in its interactions with the web server.

The number of sessions that can be opened, and therefore the number of visitors that can be served simultaneously, depends on the capacity of the web server.

◆ **Note**

"The number of visitors that can be served simultaneously" refers to the actual number of established connections, while in reality there is a greater number of connections in the process being established or closed. The maximum session should reflect the total of all three session statuses.

◆ **Tip**

If you are not familiar with your server configuration, please consult your system administrator about the maximum number of simultaneous clients and connection time-out definitions.

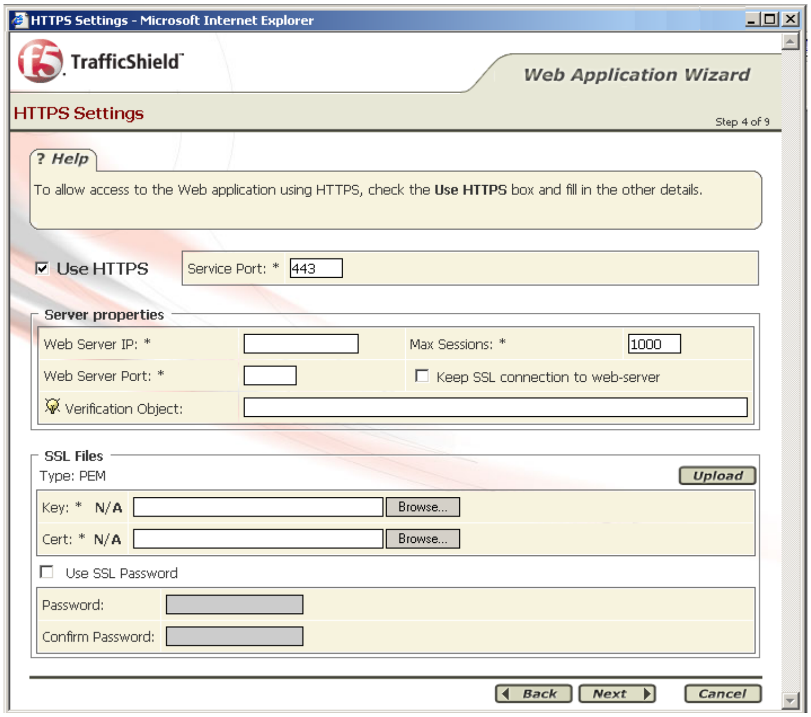
Verification Object
This is an optional field that enables you to verify that the TrafficShield Application Firewall responds correctly to a pre-defined test object. Selecting this option initializes the TrafficShield Application Firewall Hang detection mechanism.

This operation requires that you restart TrafficShield Application Firewall.

Click **Back**, to go back to the previous step, or **Next** to continue.

Step 4: HTTPS Settings

In the Web Application Wizard Step 4 screen, you define the web application HTTPS settings.



HTTPS Settings

Step 4 of 9

? Help

To allow access to the Web application using HTTPS, check the **Use HTTPS** box and fill in the other details.

☑ Use HTTPS

Service Port: * 443

Server properties

Web Server IP: *

Max Sessions: * 1000

Web Server Port: *

□ Keep SSL connection to web-server

Verification Object:

SSL Files

Type: PEM

Key: * N/A

Cert: * N/A

□ Use SSL Password

Password:

Confirm Password:

To define the Web Application HTTPS Settings

Fill in the appropriate details in the following fields.

Use HTTPS
To allow HTTPS access to the web application, select the **Use HTTPS** check box. All the fields in the section become enabled.

◆ **Important**

You need to configure at least one protocol: HTTP (see the previous step) or HTTPS.

Service Port
For the HTTPS protocol, the service port **443** is automatically entered.

Web Server IP, Web Server Port
Specify the web server's internal IP address and port.

Max. Sessions
Specify the maximum number of simultaneous sessions TrafficShield Application Firewall can open in its interactions with the web server. The number of sessions that can be opened, and therefore the number of visitors that can be served simultaneously, depends on the capacity of the web server.

◆ **Note**

"The number of visitors that can be served simultaneously" refers to the actual number of established connections, while in reality there is a greater number of connections in the process being established or being closed. The maximum session should reflect the total of all three session statuses.

◆ **Tip**

If you are not familiar with your server configuration, please consult your system administrator about the maximum number of simultaneous clients and connection time-out definitions.

Keep SSL connection to web-server
Checking this check box causes the TrafficShield Application Firewall to maintain the SSL connections to the web server. If you choose not to enable this option, TrafficShield Application Firewall will decrypt the SSL traffic, and use HTTP to send the requests to the web server.

◆ **Note**

Requests flow to the server quicker without encryption.

Verification Object
This is an optional field that enables you to verify that the TrafficShield Application Firewall responds correctly to a pre-defined test object. Selecting this option initializes the TrafficShield Application Firewall Hang detection mechanism.
This operation requires that you restart TrafficShield Application Firewall.

Key and Certificate SSL Files
Click Browse and select the files that hold the SSL key and certificate. Then, click Upload. The files should be in PEM format.

Use SSL Password
If the SSL key file is password-protected, check the Use SSL Password check box.

Password
Specify the password for key file.

Confirm Password
Type the password again for confirmation.

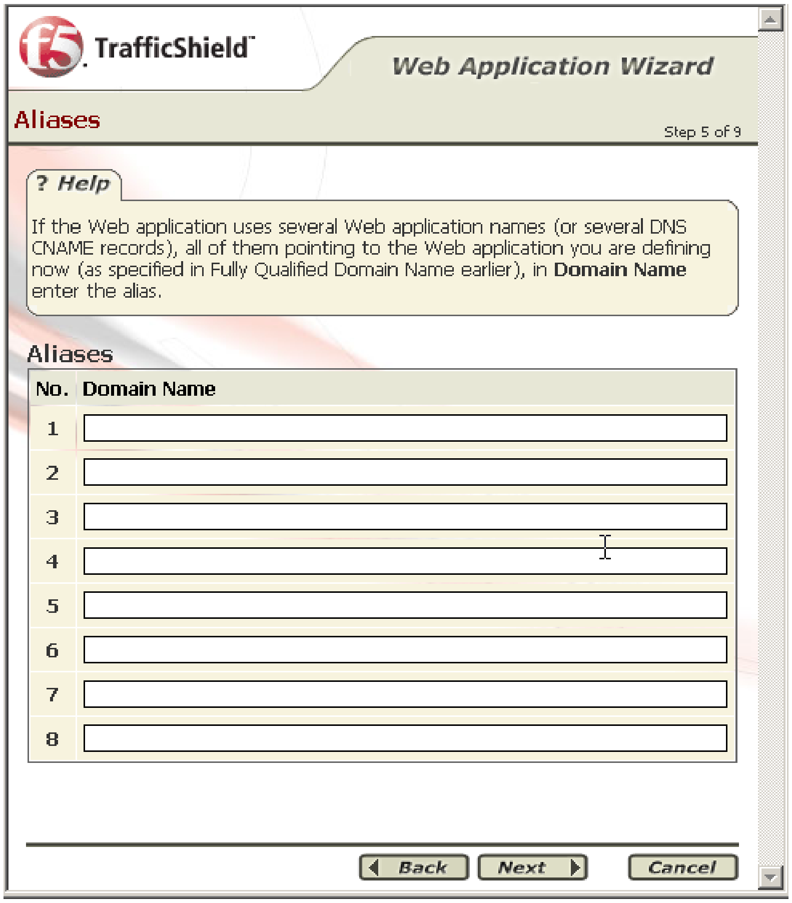
◆ **Important**

The password that protects the SSL key should be re-entered every time you reboot TrafficShield Application Firewall because TrafficShield Application Firewall keeps the password in RAM and not on the hard drive.

Click **Back**, to go back to the previous step or **Next** to continue.

Step 5: Aliases

In the Web Application Wizard Step 5 screen, you define the aliases if the web application uses several web application names.



If the Web application uses several Web application names (or several DNS CNAME records), all of them pointing to the Web application you are defining now (as specified in Fully Qualified Domain Name earlier), in **Domain Name** enter the alias.

Aliases

No.	Domain Name
1	
2	
3	
4	
5	
6	
7	
8	

To define the Web Application Aliases

Enter a new alias if the web application uses several web application names (or several DNS CNAME records), all of them pointing to the web application you are defining now (as specified in the Fully Qualified Domain Name in step 1).

You need to define in advance all of the aliases that might appear in requests addressed to this web application. TrafficShield Application Firewall blocks requests containing undefined destinations.

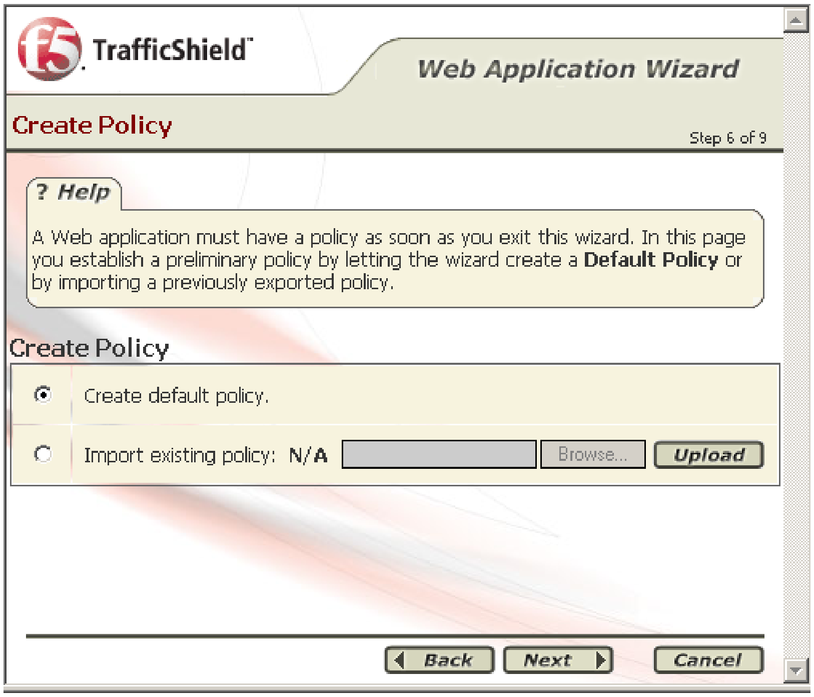
◆ **Important**

If you want to allow access to the web application by specifying its actual IP address, define the IP address as an alias by entering it in the Domain Name box.

Click **Back** to go back to the previous step or **Next** to continue.

Step 6: Create Policy

A web application must have a policy as soon as you exit this wizard. In the Web Application Wizard Step 6 screen, you establish a preliminary policy either by letting the wizard create a default policy or by importing a previously exported policy.



Create Policy

Step 6 of 9

A Web application must have a policy as soon as you exit this wizard. In this page you establish a preliminary policy by letting the wizard create a **Default Policy** or by importing a previously exported policy.

Create Policy

● Create default policy.

○ Import existing policy: N/A

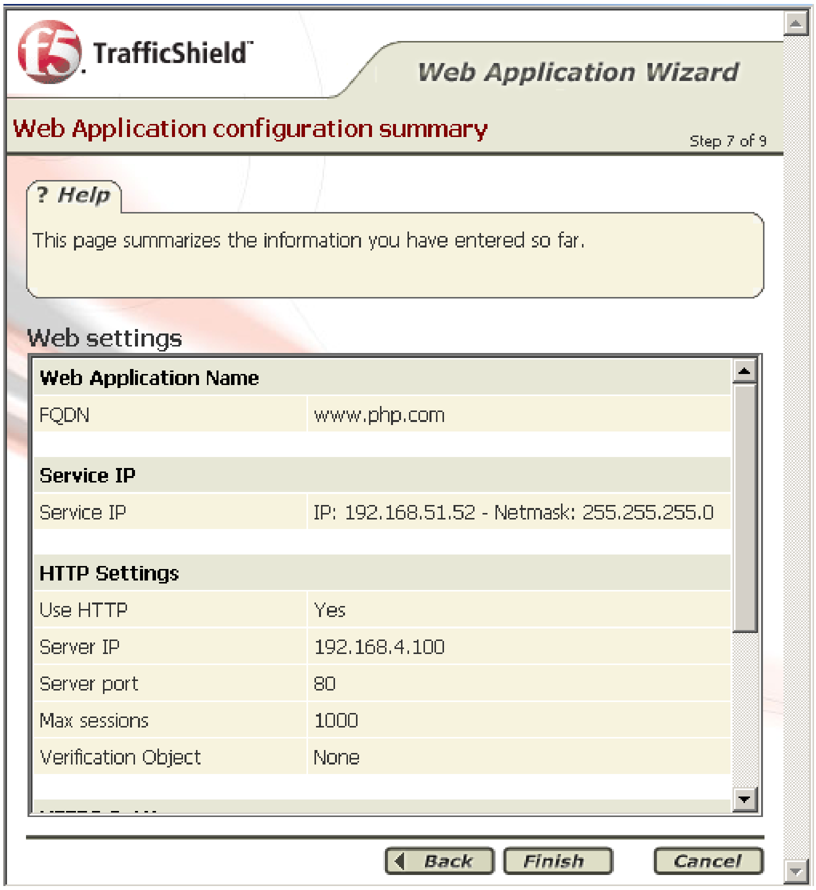
To establish a Policy for the Web Application

Select **Create default policy** if you do not have an existing policy and want the wizard to create a default policy. If you want to import an existing policy, select **Import existing policy**, click **Browse**, and **Upload**. Policies have a **.plc** file extension.

Click **Back** to go back to the previous step or **Next** to continue.

Step 7: Web Application configuration summary

Upon completion of the wizard configuration, the web application configuration summary screen is displayed.



Web Application configuration summary

Step 7 of 9

? Help

This page summarizes the information you have entered so far.

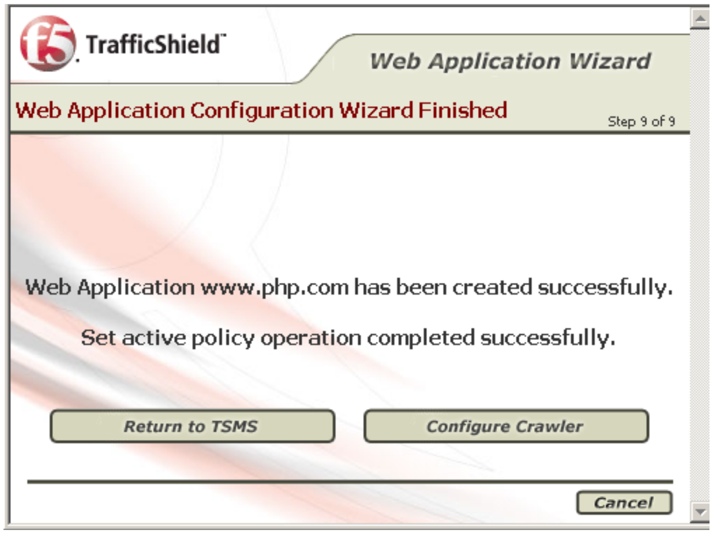
Web settings

Web Application Name	
FQDN	www.php.com
Service IP	
Service IP	IP: 192.168.51.52 - Netmask: 255.255.255.0
HTTP Settings	
Use HTTP	Yes
Server IP	192.168.4.100
Server port	80
Max sessions	1000
Verification Object	None

Review this information and proceed in one of these ways:

- Click **Back** to go back to the previous step.
- Click **Cancel** to exit without saving.
- Click **Finish** button to save and exit the wizard.

If you clicked **Finish**, the following screen appears.



Web Application Configuration Wizard Finished

Step 9 of 9

Web Application www.php.com has been created successfully.

Set active policy operation completed successfully.

This screen offers these options:

- **Return to TSMS** and **Cancel** - Exits the wizard.
- **Configure Crawler** - Automatically opens the Crawler configuration wizard. For more information about the Crawler tool and the Crawler configuration wizard, see the ***TrafficShield*® *Security Policy User Manual, version 3.2.1***.

Editing an existing web application

The TSMS enables you to edit an existing web application.

To edit an existing web application

1. Select **Administration > Configuration > Web Applications**.
2. Select the web application you want to edit.
3. Click **Edit**.

This screen includes the following sections:

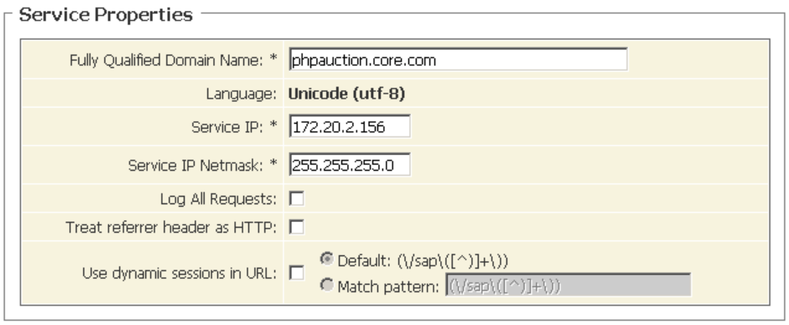
- Service Properties
- Active Policy Properties
- HTTP Settings
- HTTPS Settings
- Aliases
- Trusted IPs for allowed methods

◆ **Important**

After you make any changes, you must click ***Update TrafficShield****.*

Service Properties

The Service Properties section is designed to specify the web application's domain name and IP address.



Service Properties

Fully Qualified Domain Name: *	phpauction.core.com	
Language:	**Unicode (utf-8)**	
Service IP: *	172.20.2.156	
Service IP Netmask: *	255.255.255.0	
Log All Requests:	□	
Treat referrer header as HTTP:	□	
Use dynamic sessions in URL:	□	● Default: (\/sap\([^)]+\)) ○ Match pattern: (\/sap\([^)]+\))

You may edit the following information:

Fully Qualified Domain Name
Edit the fully qualified domain name of the web application as defined in your organization (for example, **www.siterequest.com**).

Service IP, Service IP Netmask
Specify the web application IP address and the corresponding network mask.

◆ **Note**

The web application IP address is the TSMS unit's service IP address.

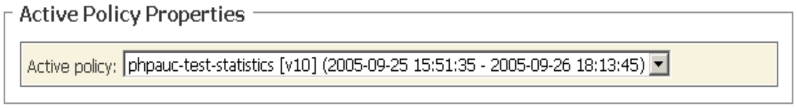
Log All Requests
Check Log All Requests to direct all incoming requests, including the valid ones, to the Illegal Requests screen (found in **Policy Management > Forensics > Illegal Requests**).
The valid requests are used to fill in the blanks when investigating gaps between illegal requests. Both types of requests can be filtered out in Forensics. The valid requests are marked with a green checkmark and the invalid requests are marked with a red X.

Treat referrer header as HTTP
Check the **Treat Referrer header as HTTP** check box if required. TrafficShield Application Firewall may forward HTTP traffic even though the web application uses SSL (for example, if a Load Balancer applies an SSL termination), in which case the policy contains only HTTP objects. The Learning module considers the referrer header which may include an SSL object. In cases like this, be sure to select the **Treat Referrer option as HTTP** check box in order to prevent problems in the Learning process.

Use Dynamic Sessions in URL
Check the **Use dynamic sessions in URL** check box if you are using SAP or an application which will insert a dynamic session in the request’s URL. Then, select either **Default** or **Match pattern** and enter a string that matches the dynamic parameter in the URL.

Active Policy Properties

From the **Active policy** drop down list select the policy you want to make active.

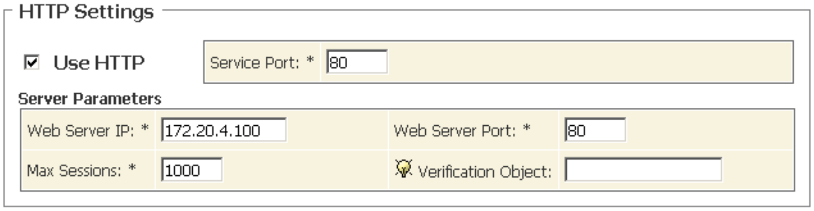


Active Policy Properties

Active policy: phpauc-test-statistics [v10] (2005-09-25 15:51:35 - 2005-09-26 18:13:45)

HTTP Settings

Use this section if the web application can be accessed using HTTP.



HTTP Settings

☑ Use HTTP

Service Port: * 80

Server Parameters

Web Server IP: * 172.20.4.100

Web Server Port: * 80

Max Sessions: * 1000

Verification Object:

Enter the following information:

Use HTTP
To allow HTTP access to the web application, select this option and enter the information described below.

Important

You need to configure at least one protocol: HTTP or HTTPS (next step).

Service Port
Specify the service port.

Web Server IP, Web Server Port
Specify the web server's IP address and port. The address is used for communications with the TrafficShield Application Firewall.

Max. Sessions
Specify the maximum number of simultaneous sessions TrafficShield Application Firewall can open in its interactions with the web server. The number of sessions that can be opened, and therefore the number of visitors that can be served simultaneously depends on the capacity of the web server.

Note

“The number of visitors that can be served simultaneously” mentioned above, refers to the actual number of established connections, while in reality there is a greater number of connections in the process being established or being closed. The maximum session should reflect the total of all three session statuses.

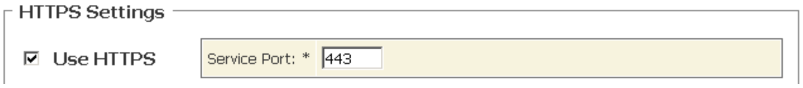
Tip

If you are not familiar with your server configuration, you need to consult with your system administrator about the maximum number of simultaneous clients and connection time-out definitions.

Verification Object
This optional field enables the user to verify that the TrafficShield Application Firewall is responding correctly to a pre-defined test object.

HTTPS Settings

Use this section if the web application can be accessed using HTTPS.



HTTPS Settings

☑ Use HTTPS

Service Port: * 443

Use HTTPS
To allow HTTPS access to the web application, check this check box and the section becomes enabled.

◆ **Note**

You need to configure at least one protocol: HTTP (previous step) or HTTPS.

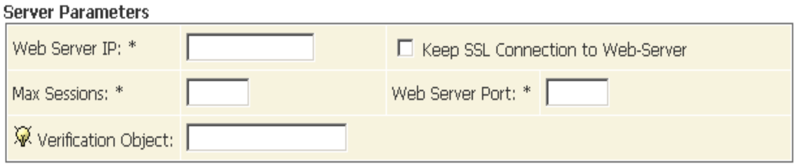
Service Port
Specify the service port.

The HTTPS section is divided into the following subsections:

- Server Parameters
- Server Certificate
- Client Certificate
- Client Certificate Headers

Server Parameters

The Server Parameters subsection appears as shown here.



Server Parameters

Web Server IP: *

□ Keep SSL Connection to Web-Server

Max Sessions: *

Web Server Port: *

Verification Object:

Enter the following information:

Web Server IP
Specify the web server's internal IP address. The address is used for internal communications with TrafficShield Application Firewall.

Keep SSL connection to web-server
Checking this box causes TrafficShield Application Firewall to maintain SSL connections to the web server. If you choose not to enable this option, TrafficShield Application Firewall will decrypt the SSL traffic and will use HTTP requests to access the web server.

◆ **Note**

Requests will flow to the server more quickly without encryption.

Max. Sessions
Specify the maximum number of simultaneous sessions TrafficShield Application Firewall can open in its interactions with the web server. The number of sessions that can be opened, and therefore the number of visitors that can be served simultaneously, depends on the capacity of the web server.

◆ **Note**

"The number of visitors that can be served simultaneously" mentioned above, refers to the actual number of established connections, while in reality there is a greater number of connections in the process being established or being closed. The maximum session should reflect the total of all three session statuses.

◆ **Tip**

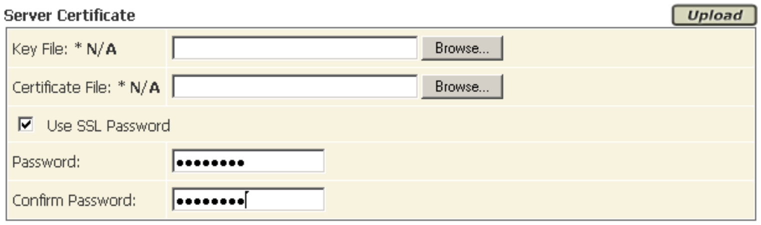
If you are not familiar with your server configuration, you need to consult with your system administrator about the maximum number of simultaneous clients and connection time-out definitions.

Web Server Port
Specify the web server's port.

Verification Object
This optional field enables the user to verify that the TrafficShield Application Firewall is responding correctly to a pre-defined test object.

Server Certificate

The Server Certificate subsection appears as shown here.



Server Certificate

Key File: * N/A	
Certificate File: * N/A	
☑ Use SSL Password	
Password:	••••••••
Confirm Password:	••••••••

Enter the following information:

Key and Certificate Files
Click the Browse button and select the files that hold the SSL key and certificate. Then, click the Upload button. The files should be in PEM format.

Use SSL Password
If the SSL key file is password-protected, check the **Use SSL Password** check box.

Password
Specify the password for key file.

Confirm Password
Type the password again for confirmation.

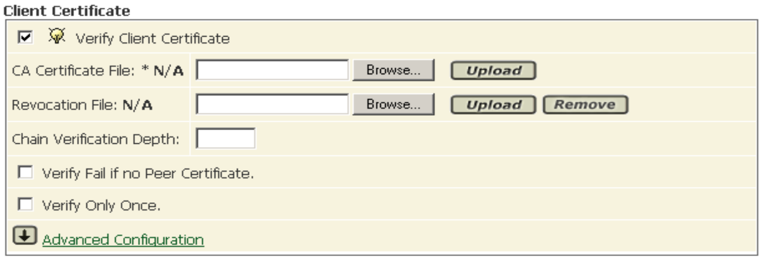
Important

If the TrafficShield Application Firewall server is rebooted, you need to reset the SSL password.

Client Certificate

If application end-users are required to present a certificate when accessing the web application, you will need to complete this information in the Client Certificate Window.

The Client Certificate subsection appears as shown here.



Client Certificate

☑ Verify Client Certificate

CA Certificate File: * N/A

Revocation File: N/A

Chain Verification Depth:

□ Verify Fail if no Peer Certificate.

□ Verify Only Once.

Enter the following information:

Verify Client Certificate
Check the Verify Client Certificate box to instruct TrafficShield Application Firewall to request Client certificate information. You must check the **Verify Client Certificate** check box to enable the boxes in the Client Certificate subsection.

CA Certificate File
Click **Browse** to select the CA (Certificate Authority) certificate to verify client certificates, and then click **Upload**.

Revocation File
Click **Browse** to select the appropriate client's certificate revocation file, if applicable, and then click Upload. You can remove the revocation file by clicking Remove.

Chain Verification Depth
The chain verification depth is used to define the level of CA verification required to verify the authenticity of the CA File.

Verify Fail if no Peer Certificate
Check this check box to terminate the SSL handshake if no client certificate was provided.

Verify Only Once
Check this check box to verify the client certificate only during the initial handshake. If this box is not checked, client certificate verification is performed for each request.

◆ **Important**

We highly recommended that you check the ***Verify Fail if no Peer Certificate*** *check box to ensure SSL handshake termination if no client certificate was provided; the client may use versions SSLv2 or SSLv3.*

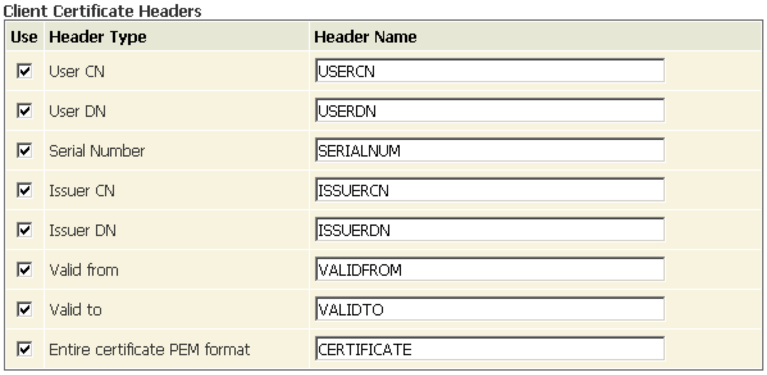
Client Certificate Headers

TrafficShield Application Firewall supports the forwarding of all, or a partial set of, client certificate information from the TrafficShield enforcer to the web server. You are able to define which certificate token will be forwarded to the web server in the Client Certificate Headers subsection.

To view the Client Certificate Headers subsection

1. Ensure that the **Verify Client Certificate** check box in the Client Certificate subsection is checked.
2. Click the **Advanced Configuration** link in the Client Certificate subsection.

The Client Certificate Headers subsection appears as shown here.



Client Certificate Headers

Use	Header Type	Header Name
☑	User CN	USERCN
☑	User DN	USERDN
☑	Serial Number	SERIALNUM
☑	Issuer CN	ISSUERCN
☑	Issuer DN	ISSUERDN
☑	Valid from	VALIDFROM
☑	Valid to	VALIDTO
☑	Entire certificate PEM format	CERTIFICATE

Check the check box next to each header type you want to be forwarded.

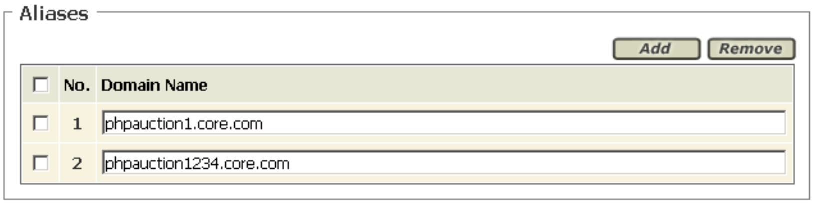
Choose from the following list of header types:

- User CN
- User DN
- Serial Number
- Issuer CN
- Issuer DN
- Valid from
- Valid to
- Entire certificate PEM format

Aliases

This step is designed to define aliases for the current application.

The Aliases section appears as shown here.



□	No.	Domain Name
□	1	phpauction1.core.com
□	2	phpauction1234.core.com

Enter a new alias if the web application uses several web application names (or several DNS CNAME records), all of them pointing to the web application you are defining now (as specified in Fully Qualified Domain Name earlier).

You need to define in advance all of the aliases that might appear in requests addressed to this web application. TrafficShield Application Firewall blocks requests containing undefined destinations.

To add an alias to TrafficShield Application Firewall, click **Add**. A new row is opened. Type the alias.

◆ **Important**

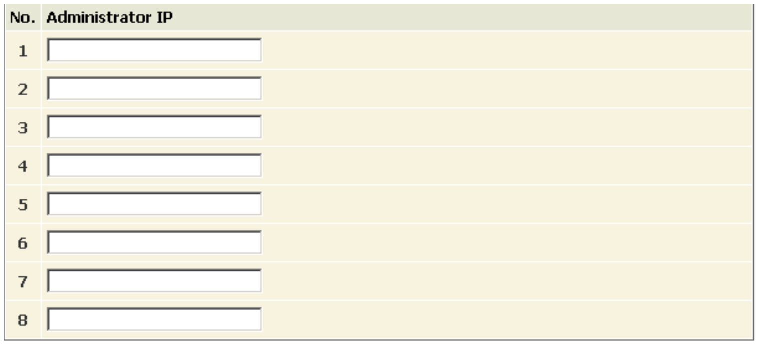
If you want to allow access to the web application by specifying its IP address, add the IP address as an alias.

To remove an alias from TrafficShield Application Firewall, check the check box next to the alias you want to remove, and click **Remove**.

Trusted IPs for Allowed Methods

Use this section to specify source IP addresses that are allowed to send requests containing extended HTTP methods, such as PUT or DELETE.

The Trusted IPs for allowed methods section appears as shown here.



No.	Administrator IP
1	
2	
3	
4	
5	
6	
7	
8	

◆ **Important**

After making all of your changes to the web application, you must click ***Update TrafficShield****.*

5

Monitoring

- Monitoring tools
- System monitoring
- Security monitoring
- Reports on illegal requests
- Activity monitoring

Monitoring tools

Monitoring tools allow the network and policy administrators to monitor request traffic. This chapter explains how to use the TrafficShield® Application Firewall monitoring tools to follow up on potential attacks and workload.

The monitoring tools described in this chapter are designed to help network and policy administrators examine both legitimate and potentially malicious traffic. The data collected by the Monitoring tool helps to identify overloaded units and make the necessary decisions on needed deployment changes.

All of the events tracked in Monitoring can also be exported as SNMP traps as well as Syslog messages.

To access the monitoring functions

To access the monitoring functions, click **Monitoring** at the top of the TrafficShield Application Firewall.

The Monitoring tool is divided into four areas, which this chapter explains in detail:

- The **System** area monitors the TrafficShield Application Firewall units and their system status, for example, whether the unit is active or in standby mode. System logs can also be monitored from here.
- The **Security** area monitors the security events generated by the TrafficShield Application Firewall units.
- The **Reports** area generates reports and graphs on the ongoing attacks that have occurred on the TrafficShield Application Firewall units.
- The **Activity** area monitors the authorized users' activities on the TrafficShield Application Firewall units.

At the top of almost every screen in each of these areas appears a filter. The filtering tool enables you to retrieve and focus on a set of events of particular interest to you. For example, you can focus on events that took place in the last hour, or events that involve requests that contained a specific text string.

System monitoring

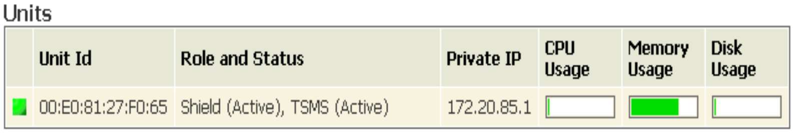
The Status screen displays information about the current status of the TrafficShield Application Firewall units and web applications, while system events are displayed on the Events screen.

System status

Select **Monitoring > System > Status** to open the System-Status screen. The System-Status screen displays information about the status of TrafficShield Application Firewall units and web applications.

TrafficShield Application Firewall unit status in case of no error

The Units section of the System-Status screen displays the current status of all TrafficShield Application Firewall units.



Units

	Unit Id	Role and Status	Private IP	CPU Usage	Memory Usage	Disk Usage
🟩	00:E0:81:27:F0:65	Shield (Active), TSMS (Active)	172.20.85.1			

The columns displayed are:

Unit Id
This is the MAC address of the relevant unit.

Role and Status
There are three possible roles:

- **Shield -** This tool is responsible for blocking requests that violated the security definitions and alerting the user.
- **TSMS** - This tool is responsible for monitoring, configuring and managing the TrafficShield Application Firewall components and graphical user interface.
- **TSMS Backup -** indicates whether the Hot Backup unit is active.

Private IP
The unique IP address assigned to the TrafficShield Application Firewall unit.

CPU Usage
The current level of CPU Usage.

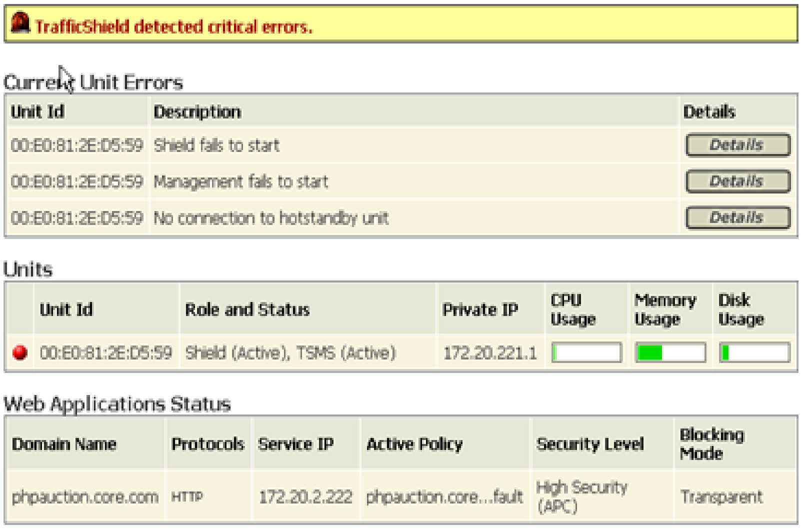
Memory Usage
The current level of memory usage.

Disk Usage
The current level of disk usage.

TrafficShield Application Firewall unit status in case of error

When TrafficShield Application Firewall detects a critical error on one of the units, a yellow notification bar is displayed on all user graphical interface screens.

Click the notification bar to display the Current Units Errors window.



TrafficShield detected critical errors.

Current Unit Errors

Unit Id	Description	Details
00:E0:81:2E:D5:59	Shield fails to start	Details
00:E0:81:2E:D5:59	Management fails to start	Details
00:E0:81:2E:D5:59	No connection to hotstandby unit	Details

Units

	Unit Id	Role and Status	Private IP	CPU Usage	Memory Usage	Disk Usage
●	00:E0:81:2E:D5:59	Shield (Active), TSMS (Active)	172.20.221.1			

Web Applications Status

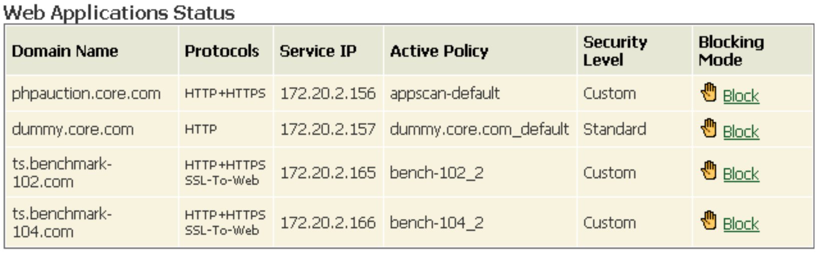
Domain Name	Protocols	Service IP	Active Policy	Security Level	Blocking Mode
phpauction.core.com	HTTP	172.20.2.222	phpauction.core...fault	High Security (APC)	Transparent

This window displays all the critical errors that were detected.

Click **Details** to open a window that displays a full description of the error with troubleshooting instructions.

Web applications status

The Web Applications Status section of the System-Status screen displays the current status of all web applications.



Web Applications Status

Domain Name	Protocols	Service IP	Active Policy	Security Level	Blocking Mode
phpauction.core.com	HTTP+HTTPS	172.20.2.156	appscan-default	Custom	Block
dummy.core.com	HTTP	172.20.2.157	dummy.core.com_default	Standard	Block
ts.benchmark-102.com	HTTP+HTTPS SSL-To-Web	172.20.2.165	bench-102_2	Custom	Block
ts.benchmark-104.com	HTTP+HTTPS SSL-To-Web	172.20.2.166	bench-104_2	Custom	Block

The columns displayed are:

Domain Name
The name of the domain in which the monitored web application is operating.

Protocols
The protocols used by the web application

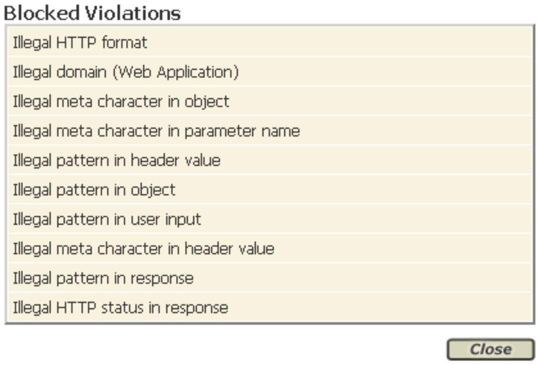
Service IP
The service IP address of the unit on which the web application is running.

Active Policy
The currently active policy that protects the web application.

Security Level
The security level defined by the user.

Blocking Mode
Defines whether the web application runs in Transparent mode or in Blocking mode.

Click the Hand icon to open the Blocked Violations screen. The Blocked Violations screen lists the violations that are blocked if the Blocking option is active.



Blocked Violations

Illegal HTTP format
Illegal domain (Web Application)
Illegal meta character in object
Illegal meta character in parameter name
Illegal pattern in header value
Illegal pattern in object
Illegal pattern in user input
Illegal meta character in header value
Illegal pattern in response
Illegal HTTP status in response

System events

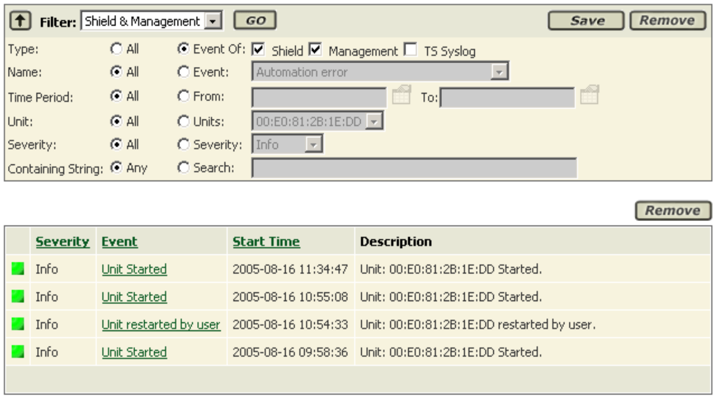
Select **Monitoring > System > Events** to open the System-Events screen. This screen displays the system events that have occurred and been recorded in TrafficShield Application Firewall.

Filtering the events

Use this screen with its advanced filter to concentrate on events pertinent to your needs.

To filter events

1. Open the filtering tool by clicking the down-arrow icon displayed on the Filter row (you can close it by clicking the button again).



Filter: Shield & Management ▾ GO Save Remove

Type:	○ All	● Event Of: ☑ Shield ☑ Management □ TS Syslog
Name:	● All	○ Event: Automation error
Time Period:	● All	○ From: To:
Unit:	● All	○ Units: 00:E0:81:2B:1E:DD
Severity:	● All	○ Severity: Info
Containing String:	● Any	○ Search:

Remove

	Severity	Event	Start Time	Description
🟩	Info	Unit Started	2005-08-16 11:34:47	Unit: 00:E0:81:2B:1E:DD Started.
🟩	Info	Unit Started	2005-08-16 10:55:08	Unit: 00:E0:81:2B:1E:DD Started.
🟩	Info	Unit restarted by user	2005-08-16 10:54:33	Unit: 00:E0:81:2B:1E:DD restarted by user.
🟩	Info	Unit Started	2005-08-16 09:58:36	Unit: 00:E0:81:2B:1E:DD Started.

2. Select one or more filtering options.
   The filtering options are those that have a radio button next to them. For example, click the **Severity** radio button, select a severity level from the drop down list, and click **Go**. Only events with the selected severity level will be displayed.

   You can select multiple filtering options to further limit the scope of the retrieval. For example, setting a time period in the **From/To** area and selecting a severity, lists the events of the selected severity level that took place within the specified time period.

◆ **Note**

To cancel the filter in a certain category, select its corresponding ***All*** *radio button, and click* ***Go****.*

The following table describes each of the filtering options available.

Criteria	Description
Filter	A predefined set of filtering parameters.
Type: Event Of	Filters the events that took place in the units, and events that have been posted to the operating system's log (system Log). Check the box that corresponds to the events you want to retrieve. You can select more than one option.
Name: Event	If you want to focus on a specific event, select the **Event** radio button and then select the event you want in the drop-down list.
Time Period: From/To	To retrieve events that took place in a certain period, select the **From** radio button. Then, use the 📅 (calendar) icon in the From/To fields to select the start date/time and end date/time of the period. Note that you can select the time by clicking the time fields at the bottom of the calendar box.

Criteria	Description
Unit: Units	If you want to focus on events that took place in a certain unit, select the **Units** radio button and then select the unit's ID.
Severity: Severity	To retrieve only events of a certain severity level, select the **Severity** radio button and then select a level from the drop-down list.
Containing String: Search	Use this option to pinpoint events whose message contains a certain text. Select the **Search** radio button and type the text.

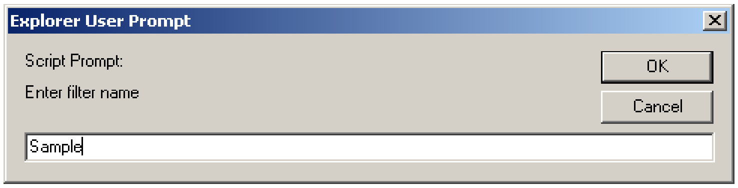
3. Click **Go** to activate the filter.

Saving custom made filters

If you created a custom made filter, you might want to save the filtering criteria so that you can re-run the same filter without having to reset the filtering criteria.

To save a custom made filter

1. Create and run the filter.
2. After receiving the retrieval criteria, click **Save**.
   This opens the following screen.



Script Prompt:
Enter filter name

Sample

3. Type a name for your custom made filter, and click **OK**.

Removing a filter

To delete a filter from the Filter list

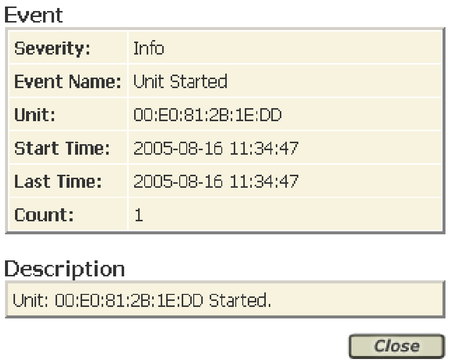
Select the filter you want to delete in the Filter list, and click **Remove**.

Unit events

If you want to focus on events that took place in a certain unit, select the **Units** radio button and then select the unit's ID.

To display more information about the event

1. Click the link of the event under the **Event** column**.**
   A description of the event is displayed.



Event

Severity:	Info
Event Name:	Unit Started
Unit:	00:E0:81:2B:1E:DD
Start Time:	2005-08-16 11:34:47
Last Time:	2005-08-16 11:34:47
Count:	1

Description

Unit: 00:E0:81:2B:1E:DD Started.

2. When you have read the event summary, click the **Close** button.

Security monitoring

Security violations are displayed in the Status screen, and the day/time security violations occur are displayed in the Events screen.

Security status

Select **Monitoring > Security > Status** to open the Security-Status screen.

The Security-Status screen displays a list of security violations that have occurred.

There are two report types available from the **Report Type** drop down list.

Select one of the following:

- **Violation Report** to display a list of violations, or
- **IP's Report** to display the IP addresses that committed the violations.

Both reports display the number of requests and the percentage of those requests that occurred from the total requests.

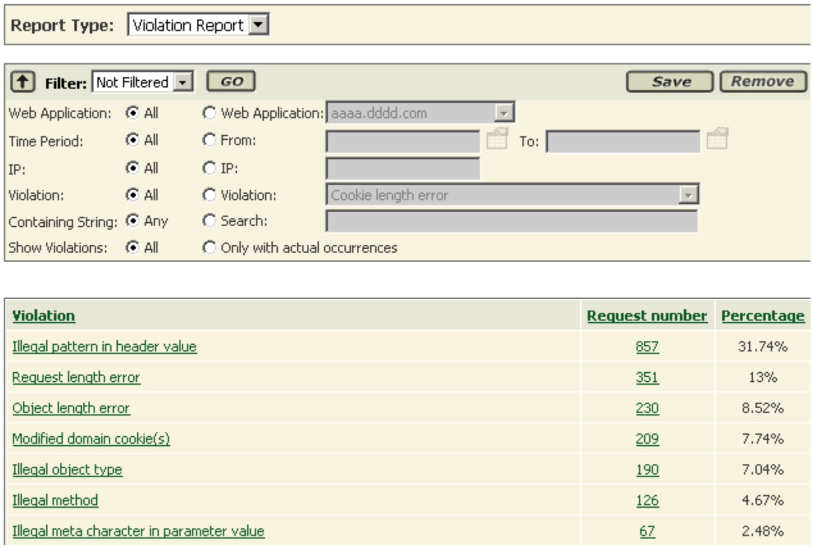
To define the filter criteria

1. Open the filtering tool by clicking the down-arrow icon displayed on the Filter row (you can close it by clicking the button again).
2. Use the radio buttons to select your filtering criteria.
3. Click **Go** to update the violation display using the selected filter criteria.
4. Click **Save** to save the changes made to the filter criteria, thus creating a customized filter.
5. Use **Remove** to remove customized filters.

◆ **Note**

It is not possible to delete the built in filters.

The filter criteria are displayed in the top part of the window while the filtered violation list is displayed in the bottom part of the window.



Report Type: Violation Report

Filter: Not Filtered

Web Application:	● All	○ Web Application:	aaaa.dddd.com
Time Period:	● All	○ From:	To:
IP:	● All	○ IP:	
Violation:	● All	○ Violation:	Cookie length error
Containing String:	● Any	○ Search:	
Show Violations:	● All	○ Only with actual occurrences	

Violation	Request number	Percentage
Illegal pattern in header value	857	31.74%
Request length error	351	13%
Object length error	230	8.52%
Modified domain cookie(s)	209	7.74%
Illegal object type	190	7.04%
Illegal method	126	4.67%
Illegal meta character in parameter value	67	2.48%

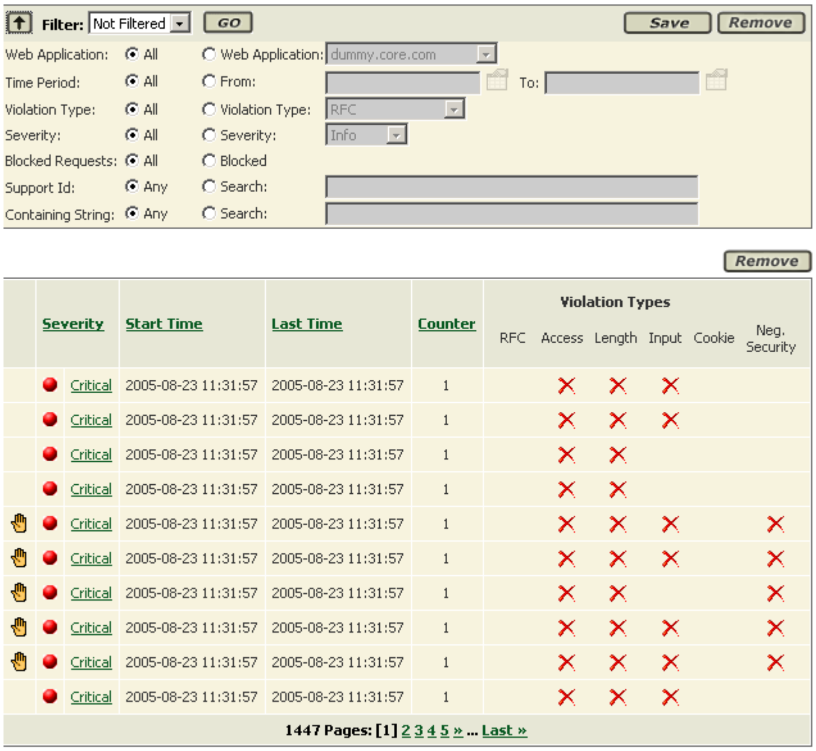
The following table describes each of the filtering options available.

Criteria	Description
Filter	A predefined set of filtering parameters
Web Application	To focus on events relating to one of the protected Web applications, select the **Web Application** radio button and then select the Web application from the drop-down list.
Time Period From/To	To retrieve events that took place in a certain period, select the **From** radio button. Then, use the icon in the From/To fields to select the start date/time and end date/time of the period. Note that you can select the time by clicking the time fields at the bottom of the calendar box.
IP	To retrieve events originating from an IP address, select the **IP** radio button and then enter the address in the adjacent box.
Violations	To list the events that were registered as a result of a specific attack type, select the **Violation** radio button and then select the standard attack name from the drop-down list.
Containing String: Search	Use this option to pinpoint events whose message contains a certain text. Select the **Search** radio button and type the text.
Show Violations	To display all of the violations or only those with occurrences.

Security events

Select **Monitoring > Security > Events** to open the Security-Events screen.

The Security-Events screen lists the events relating to requests that do not comply with the applied security policies. For example, you can see a list of events relating to requests that committed a length violation or a cookie violation.



Web Application:	● All	○ Web Application:	dummy.core.com
Time Period:	● All	○ From:	To:
Violation Type:	● All	○ Violation Type:	RFC
Severity:	● All	○ Severity:	Info
Blocked Requests:	● All	○ Blocked	
Support Id:	● Any	○ Search:	
Containing String:	● Any	○ Search:	

	Severity	Start Time	Last Time	Counter	Violation Types					
					RFC	Access	Length	Input	Cookie	Neg. Security
	● Critical	2005-08-23 11:31:57	2005-08-23 11:31:57	1		✕	✕	✕		
	● Critical	2005-08-23 11:31:57	2005-08-23 11:31:57	1		✕	✕	✕		
	● Critical	2005-08-23 11:31:57	2005-08-23 11:31:57	1		✕	✕			
	● Critical	2005-08-23 11:31:57	2005-08-23 11:31:57	1		✕	✕			
✋	● Critical	2005-08-23 11:31:57	2005-08-23 11:31:57	1		✕	✕	✕		✕
✋	● Critical	2005-08-23 11:31:57	2005-08-23 11:31:57	1		✕	✕	✕		✕
✋	● Critical	2005-08-23 11:31:57	2005-08-23 11:31:57	1		✕	✕			✕
✋	● Critical	2005-08-23 11:31:57	2005-08-23 11:31:57	1		✕	✕	✕		✕
✋	● Critical	2005-08-23 11:31:57	2005-08-23 11:31:57	1		✕	✕	✕		✕
	● Critical	2005-08-23 11:31:57	2005-08-23 11:31:57	1		✕	✕	✕		

1447 Pages: [1] 2 3 4 5 » ... Last »

Events that have been blocked are marked with the ✋ (blocked request) icon.

To define the filter criteria

1. Open the filtering tool by clicking the down-arrow icon displayed on the Filter row (you can close it by clicking the button again).
2. Use the radio buttons to select your filtering criteria.
3. Click **Go** to update the violation display using the selected filter criteria.
4. Click **Save** to save the changes made to the filter criteria, thus creating a customized filter.

5. Use **Remove** to remove customized filters.

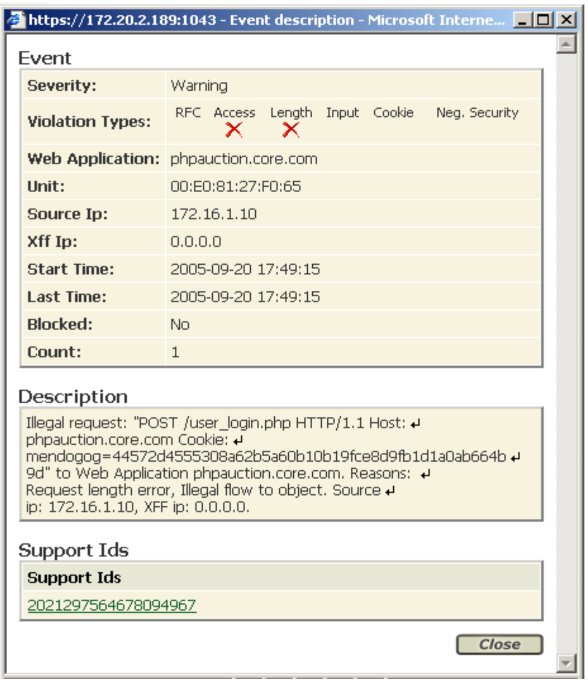
◆ **Note**

It is not possible to delete the built in filters.

The following table describes each of the filtering options available.

Criteria	Description
Filter	A predefined set of filtering parameters
Web Application	To focus on events relating to one of the protected Web applications, select the **Web Application** radio button and then select the Web application from the drop-down list.
Time Period From/To	To retrieve events that took place in a certain period, select the **From** radio button. Then, use the icon in the From/To fields to select the start date/time and end date/time of the period. Note that you can select the time by clicking the time fields at the bottom of the calendar box.
Violation Type	To list the events that were registered as a result of a specific attack type, select the **Violation Type** radio button and then select the standard attack name from the drop-down list.
Severity	To list the events that were registered as a specific severity level, select the **Severity** radio button and then select the severity level from the drop-down list.
Blocked Requests	To view the events that were blocked, select the **Blocked** radio button.
Support ID	Shield creates an ID for every request that causes a violation. To view the events with a specific ID, select the **Search** radio button and type the ID number.
Containing String	Use this option to pinpoint events whose message contains a certain text. Select the **Search** radio button and type the text.

To display more information about an event, click the link of the event under the Severity column. The Event Description screen displays.



https://172.20.2.189:1043 - Event description - Microsoft Interne...

Event

Severity:	Warning
Violation Types:	RFC ✗Access ✗Length Input Cookie Neg. Security
Web Application:	phpauction.core.com
Unit:	00:E0:81:27:F0:65
Source Ip:	172.16.1.10
Xff Ip:	0.0.0.0
Start Time:	2005-09-20 17:49:15
Last Time:	2005-09-20 17:49:15
Blocked:	No
Count:	1

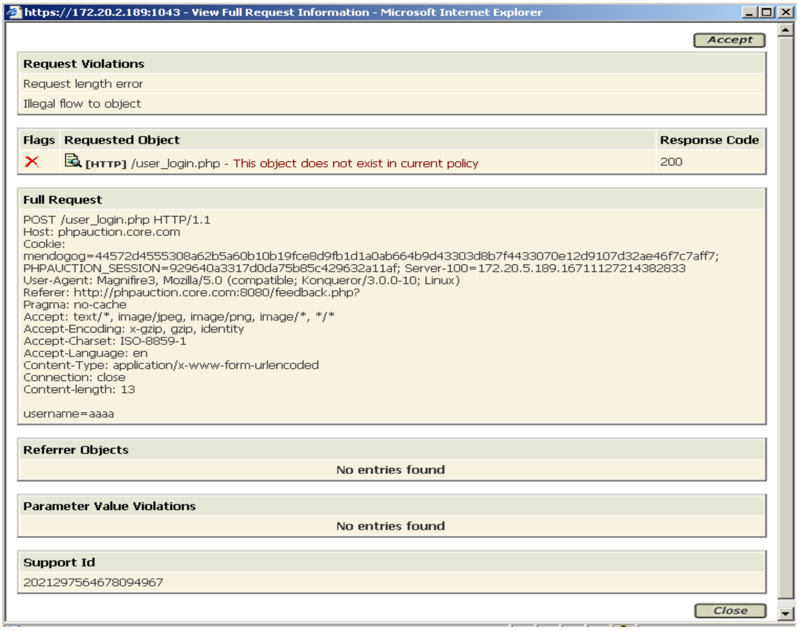
Description

Illegal request: "POST /user_login.php HTTP/1.1 Host: ↵
phpauction.core.com Cookie: ↵
mendogog=44572d4555308a62b5a60b10b19fce8d9fb1d1a0ab664b ↵
9d" to Web Application phpauction.core.com. Reasons: ↵
Request length error, Illegal flow to object. Source ↵
ip: 172.16.1.10, XFF ip: 0.0.0.0.

Support Ids

Support Ids
2021297564678094967

For more information about the event, click the **Support ID** number link. The View Full Request Information screen opens.



https://172.20.2.189:1043 - View Full Request Information - Microsoft Internet Explorer

Request Violations
Request length error
Illegal flow to object

Flags	Requested Object	Response Code
✗	[HTTP] /user_login.php - This object does not exist in current policy	200

Full Request

```
POST /user_login.php HTTP/1.1
Host: phpauction.core.com
Cookie:
mendogog=44572d4555308a62b5a60b10b19fce8d9fb1d1a0ab664b9d43303d8b7f4433070e12d9107d32ae46f7c7aff7;
PHPAUCTION_SESSION=929640a3317d0da75b85c429632a11af; Server-100=172.20.5.189.16711127214382833
User-Agent: Magnifire3, Mozilla/5.0 (compatible; Konqueror/3.0.0-10; Linux)
Referer: http://phpauction.core.com:8080/feedback.php?
Pragma: no-cache
Accept: text/*, image/jpeg, image/png, image/*, */*
Accept-Encoding: x-gzip, gzip, identity
Accept-Charset: ISO-8859-1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: close
Content-length: 13

username=aaaa
```

Referrer Objects
No entries found

Parameter Value Violations
No entries found

Support Id
2021297564678094967

After viewing the information, either click **Accept** to accept the event, or click **Close**.

Reports on illegal requests

TrafficShield Application Firewall generates the following types of reports on detected illegal requests.

- Attacks report
- Executive report

Attacks report

Select **Monitoring > Reports > Attacks** to open the Attacks screen.

The Attacks screen displays a report of illegal requests that provides a more global view on a number of illegal requests of a given type.

When sent at a high frequency, these illegal requests are considered a clear indication that someone intends to cause specific damage to your application. For example, the TrafficShield Application Firewall detects such attack types as “buffer overflow,” “parameter value tempering,” and “forceful browsing”.

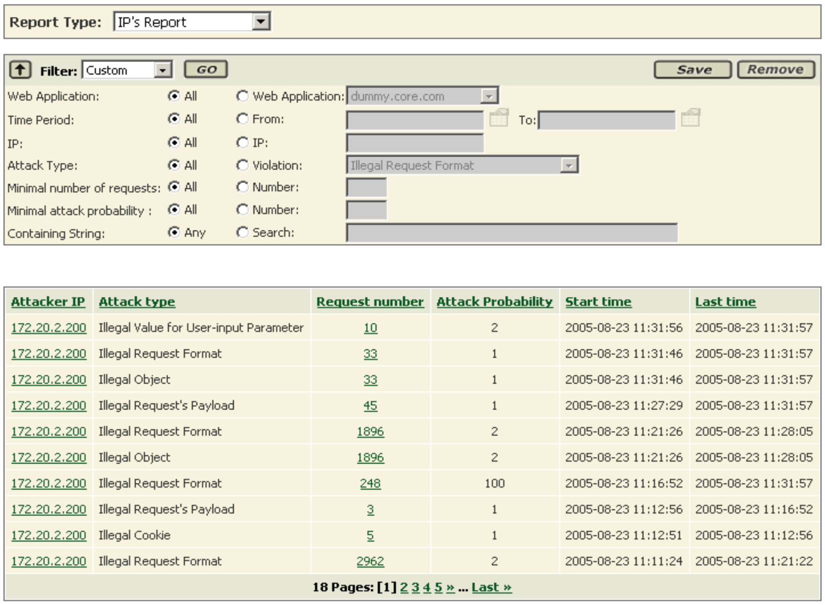
There are two report types available from the **Report Type** drop down list.

Select one of the following:

- **IP’s Report** to display the IP addresses of the computers from which the attacks came, or
- **Attack Types Report** to display the types of attacks made on your application.

To display illegal requests of a given type

1. Open the filtering tool by clicking the down-arrow icon displayed on the Filter row (you can close it by clicking the button again)



Report Type: IP's Report

Filter: Custom GO Save Remove

Web Application:	● All	○ Web Application:	dummy.core.com
Time Period:	● All	○ From:	To:
IP:	● All	○ IP:	
Attack Type:	● All	○ Violation:	Illegal Request Format
Minimal number of requests:	● All	○ Number:	
Minimal attack probability :	● All	○ Number:	
Containing String:	● Any	○ Search:	

Attacker IP	Attack type	Request number	Attack Probability	Start time	Last time
172.20.2.200	Illegal Value for User-input Parameter	10	2	2005-08-23 11:31:56	2005-08-23 11:31:57
172.20.2.200	Illegal Request Format	33	1	2005-08-23 11:31:46	2005-08-23 11:31:57
172.20.2.200	Illegal Object	33	1	2005-08-23 11:31:46	2005-08-23 11:31:57
172.20.2.200	Illegal Request's Payload	45	1	2005-08-23 11:27:29	2005-08-23 11:31:57
172.20.2.200	Illegal Request Format	1896	2	2005-08-23 11:21:26	2005-08-23 11:28:05
172.20.2.200	Illegal Object	1896	2	2005-08-23 11:21:26	2005-08-23 11:28:05
172.20.2.200	Illegal Request Format	248	100	2005-08-23 11:16:52	2005-08-23 11:31:57
172.20.2.200	Illegal Request's Payload	3	1	2005-08-23 11:12:56	2005-08-23 11:16:52
172.20.2.200	Illegal Cookie	5	1	2005-08-23 11:12:51	2005-08-23 11:12:56
172.20.2.200	Illegal Request Format	2962	2	2005-08-23 11:11:24	2005-08-23 11:21:22

18 Pages: [1] 2 3 4 5 » ... Last »

The options in the Filter section are as follows:

Criteria	Description
Filter	A predefined set of filtering parameters. The options are: Not FIltered, Last Hour, Last Day, Last Week, Last Month, and Custom
Web application	To focus on events relating to one of the protected Web applications, click the **Web Application** button, and then select the Web application from the list.
Time Period From/To	To retrieve events that took place in a certain period, select the **From** radio button. Then, use the icon in the From/To fields to select the start date/time and end date/time of the period. Note that you can select the time by clicking the time fields at the bottom of the calendar box.
IP	To retrieve events originating from an IP address, select the **IP** radio button and then enter the address in the adjacent box.

Criteria	Description
Attack Type	Select an attack type. This applies, especially, to the Attacks Report that groups together requests that have the characteristics of a standard attack type. You can use it in conjunction with “Minimal number of requests”.
Minimal number of requests	Use this parameter to list attacks that included at least a specified number of requests that characterize standard attack types.
Minimal attack probability	This is a sorting option that displays the attacks from the lowest probability.
Containing String	Use this option to pinpoint events whose message contains a certain text. Select the **Search** radio button and type the text.

2. Use the **Go** button to update the attack display using the latest filter criteria.
3. Use the **Save** button to save the changes made to the filter criteria, thus creating a customized filter.
4. Use the **Remove** button to remove customized filters.

The columns displayed are:

Attacker IP
The Attacker IP is the IP of the computer from which the attacks came.

Attack Type
The type of attack.

Request Number
The Request Number column indicates the number of requests of the specific attack type. Click a number to display the requests.

Attack Probability
The TrafficShield Application Firewall calculates and suggests a probability that the certain set of requests already launched an attack. The numbers that appear in this field represent the percentage of attack probability. While **100** is the highest probability and **1** is the lowest, **0** means no probability at all.

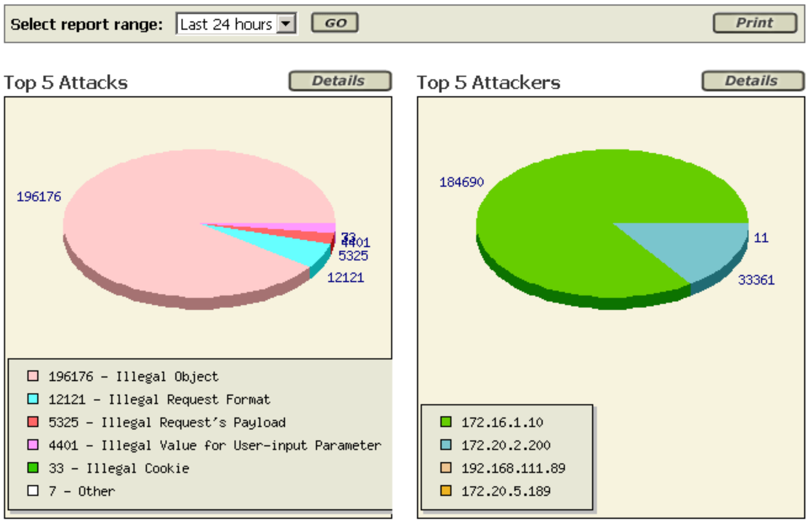
Start Time
This is the first time this attack was noted.

Last Time
This is the last time this attack was noted.

Executive report

Select **Monitoring > Reports > Executive** to open the Executive screen.

The Executive screen graphically displays the attack statistics.



Select report range: Last 24 hours GO Print

Top 5 Attacks Details

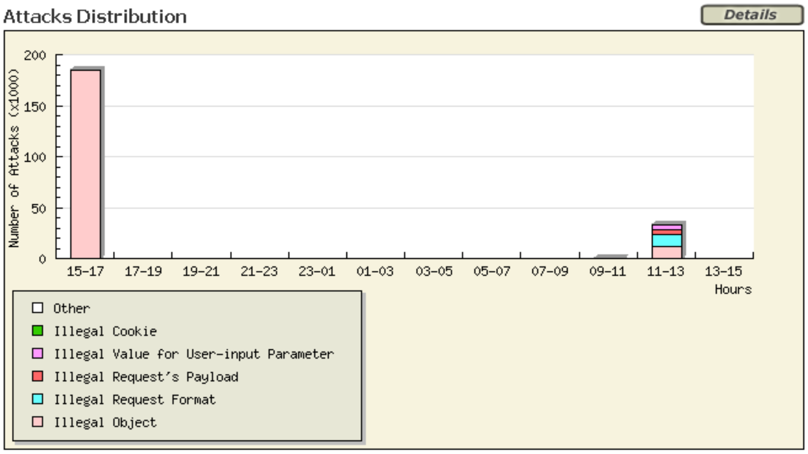
- 🟪 196176 - Illegal Object
- 🟦 12121 - Illegal Request Format
- 🟥 5325 - Illegal Request's Payload
- 🟪 4401 - Illegal Value for User-input Parameter
- 🟩 33 - Illegal Cookie
- □ 7 - Other

Top 5 Attackers Details

- 🟩 172.16.1.10
- 🟦 172.20.2.200
- 🟧 192.168.111.89
- 🟧 172.20.5.189

This report contains the same type of information as in the Attacks report, only it retrieves the five most frequent attacks or attackers (IP). The **Details** button functions like the links in the Attacks report, listing attacks or IP addresses.

The Attacks Distribution section displays the attack types over time. The **Details** button displays the same information in textual format.



Attacks Distribution Details

- □ Other
- 🟩 Illegal Cookie
- 🟪 Illegal Value for User-input Parameter
- 🟥 Illegal Request's Payload
- 🟦 Illegal Request Format
- 🟪 Illegal Object

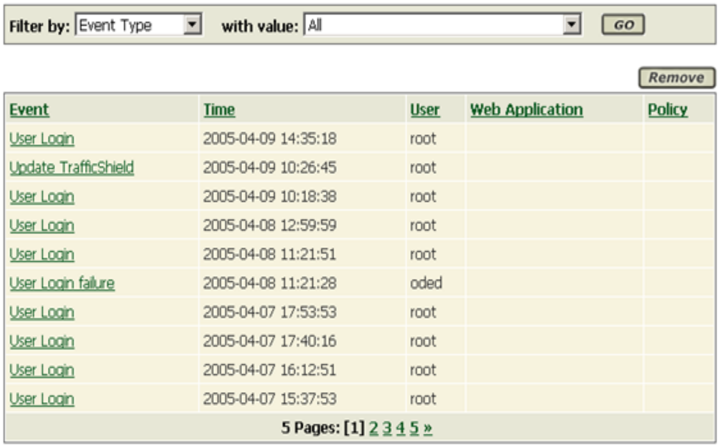
Activity monitoring

You can use the monitoring tool to examine the user activities that have taken place in the system.

User activity consists of operations such as logging on to TSMS or adding a new policy, removing a policy, adding a web application, modifying the Server SSL files, changing the blocking policy, changing the system configuration, change the character set, restarting the unit, adding a user, and adding a Regexp pool.

Users

Select **Monitoring > Activity > Users** to open the Users screen.



Filter by: Event Type with value: All

Event	Time	User	Web Application	Policy
User Login	2005-04-09 14:35:18	root		
Update TrafficShield	2005-04-09 10:26:45	root		
User Login	2005-04-09 10:18:38	root		
User Login	2005-04-08 12:59:59	root		
User Login	2005-04-08 11:21:51	root		
User Login failure	2005-04-08 11:21:28	oded		
User Login	2005-04-07 17:53:53	root		
User Login	2005-04-07 17:40:16	root		
User Login	2005-04-07 16:12:51	root		
User Login	2005-04-07 15:37:53	root		

5 Pages: [1] 2 3 4 5 »

To monitor user activities

1. In the **Filter By** box, select the type of events to display.
   In the **with value** box, select the value to be filtered.
   For example, in **Filter By**, select **Policy**, and in **with value**, select the name of a policy to list user activities that took place in relation with the indicated policy.
2. To list the events that meet the criteria, click **Go**.
3. To delete all of the listed events, click **Remove**.

6

Administration

- Administration tools
- Users
- Alerts
- Maintenance-System
- Upgrades
- Backing up
- Restoring
- Permanent IP addresses
- Downloads
- Support tools
- Undefined aliases

Administration tools

Administration tools allow the network and policy administrators to perform administrative functions in TrafficShield® Application Firewall.

To access the administration functions

To access the administration functions, click **Administration** at the top of the TrafficShield Application Firewall.

The Administration tool is divided into two main areas: the **Configuration** area and the **Maintenance** area.

From the **Configuration** area, the administrator is able to add, edit or remove web applications, users, units, IP aliases, alerts, and regular expressions.

From the **Maintenance** area, the administrator is able to restart, shut down, upgrade and backup units, add, edit and remove permanent IPs, activate a TrafficShield Application Firewall licence, download system files, export support tools, and accept undefined aliases.

The **Configuration** area is divided into the following sections:

- Web Applications
- System
- Users
- Alerts
- Defaults

The **Maintenance** area is divided into the following sections:

- System
- Upgrades
- Backup
- Permanent IPs
- Licensing
- Downloads
- Support Tools
- Undefined Aliases

The Configuration-Web Applications screen is discussed in *Editing an existing web application*, on page 4-12.

The Configuration-System screen is discussed in *Configuring TrafficShield Application Firewall units manually*, on page 3-7.

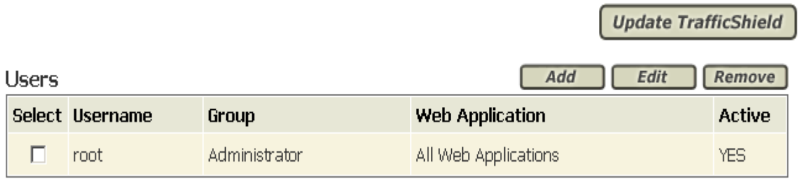
The Configuration-Defaults screen is discussed in the ***TrafficShield® Security Policy User Manual version 3.2.1***, Chapter 4, *Policy Management Configuration*, in the section *Creating a Pool of Regular Expressions*.

The Maintenance-Licensing screen is discussed in *Licensing*, on page 3-12. The remaining sections are explained in this chapter in detail.

Users

During the installation stage you were asked to define the TrafficShield Management Station (TSMS) Administrator as the initial super user. It is possible to add additional users through the TSMS graphic user interface.

Select **Administration > Configuration > Users** to open the Users screen.



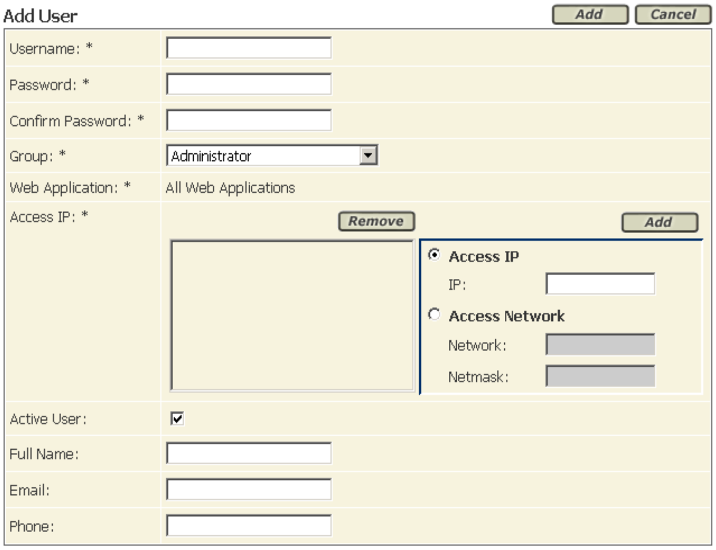
Users

Select	Username	Group	Web Application	Active
□	root	Administrator	All Web Applications	YES

Adding users

To add users

1. Select **Administration > Configuration > Users**.
   The Users screen opens.
2. Click **Add**.
   The Add User screen opens.
   Note: *Every field with an asterisk is a mandatory field.*



Add User

Username: *	
Password: *	
Confirm Password: *	
Group: *	Administrator
Web Application: *	All Web Applications
Access IP: *	● Access IP IP: ○ Access Network Network: Netmask:
Active User:	☑
Full Name:	
Email:	
Phone:	

3. In the **Username** field, enter the name that the user should type when accessing the TSMS.
4. In the **Password** field, enter the password that the user should type when accessing the TSMS.

5. In the **Confirm Password** field, enter the password again.
6. In the **Group** field, select the group to which you would like this user to belong. The group determines the operations that this user will be allowed to perform in the TrafficShield Application Firewall.

   The following table describes the attributes of each group.

User Type	Authorization
Administrator	The Administrator has access to all web applications defined in the TSMS and can perform all operations in the TSMS.
Web Application Administrator	Access only to an assigned web application. This user can only create additional users for his allowed web application. The web application assignment is made in the **Web Application** box.
Policy Editor	Access to the Policy Management tool only within the context of an assigned application. The web application assignment is made in the **Web Application** box. The user cannot view the Administration and Monitoring tabs.
Monitoring	Access to the Monitoring tool only. Users in this group can only view data.

7. In the **Web Application** field, select the web application that this user will be authorized to access.
   Each user may access one application. To allow a user to access more than one Web application, define a separate user record for each user.
   This field is not accessible if the user group is Administrator or Monitoring, as administrators have access to all applications and monitors are only allowed to view data.
8. You can restrict user access to the TSMS based on either an IP address or a network segment.
   a) If you want to specify the IP address of the computer from which the user is entitled to access the TSMS, select the **Access IP** radio button and enter the IP address.
   b) To allow access from any IP address in a network, select the **Access Network** radio button and enter the network address and netmask.
9. In the Access IP area, click **Add**.
   The address moves to the box on the left.

   ***Note**: You can remove an address by selecting it in the left box and clicking **Remove**.*

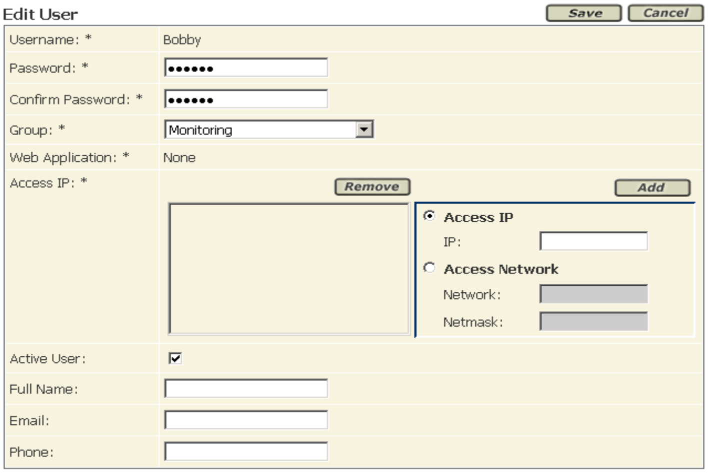
10. Uncheck the **Active User** check box to withdraw this user's access permissions without deleting the user record.
    Check the check box again to re-enable the user.
11. In the **Full Name**, **E-mail** and **Phone** boxes, enter the full name, e-mail address and the telephone number of this user.
12. To complete the process of adding a user, click the **Add** button found at the top of the screen.
    This closes the Add User screen. The user record appears in the Users screen.
13. Click **Update TrafficShield**.
14. Repeat the procedure for all relevant addresses.

Editing users

You can edit each user's personal information or change the user's IP access.

To edit user information

1. Select **Administration > Configuration > Users**.
   The Users screen appears.
2. Select the user whose information you want to edit, and click **Edit**.
   The Edit User screen opens.



Edit User

Username: *	Bobby
Password: *	••••••
Confirm Password: *	••••••
Group: *	Monitoring
Web Application: *	None
Access IP: *	● Access IP IP: ○ Access Network Network: Netmask:
Active User:	☑
Full Name:	
Email:	
Phone:	

3. Edit the information as needed.
4. Click **Save**.
   This closes the Edit User screen and opens the Users screen.
5. Click **Update TrafficShield**.

Removing users

You can remove a user from the system.

To remove a user

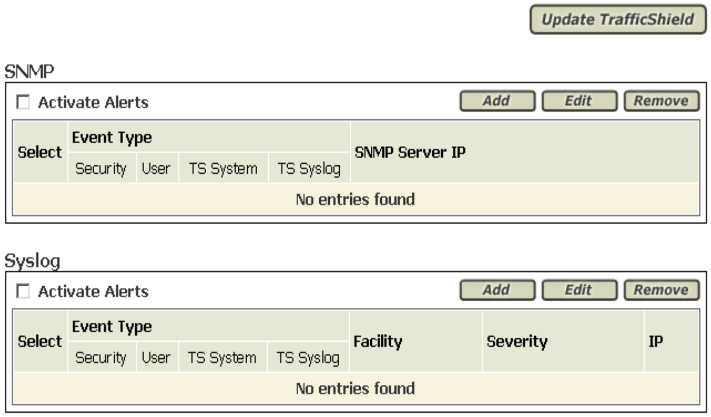
1. Select **Administration > Configuration > Users**.
   The Users screen appears.
2. Select the user who you want to remove, and click **Remove**.
3. Click **Update TrafficShield**.

Alerts

The alerts feature enables you to configure the remote notifications for security, user, and system events to be sent to SNMP traps and Syslog servers. The TrafficShield Application Firewall Alerts mechanism can collect events of different types.

To add an event to be sent to the SNMP server

1. Select **Administration > Configuration** > **Alerts**.
   The Alerts screen opens.



SNMP

☐ Activate Alerts

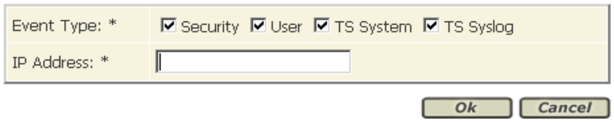
Select	Event Type				SNMP Server IP
	Security	User	TS System	TS Syslog	
No entries found					

Syslog

☐ Activate Alerts

Select	Event Type				Facility	Severity	IP
	Security	User	TS System	TS Syslog			
No entries found							

2. From the SNMP area, click **Add**.
   The **Add SNMP** screen opens.



Event Type: *	☑ Security ☑ User ☑ TS System ☑ TS Syslog
IP Address: *	

3. Select the types of events to capture by checking one or more of the options described in the following table.

Option	Collects
Security	Events identified as policy violations.
User	Operations performed by TSMS users. For example, logging in to TSMS is a user event.
TrafficShield System	Events related to Shield and management operations. For example, rebooting units is a system event.
TrafficShield Syslog	Events registered at the OS system log.

4. Enter the SNMP server IP address of the server that will receive the events, and click **OK**.
   When you add your first SNMP alert, the **Activate Alerts** check box is automatically selected.

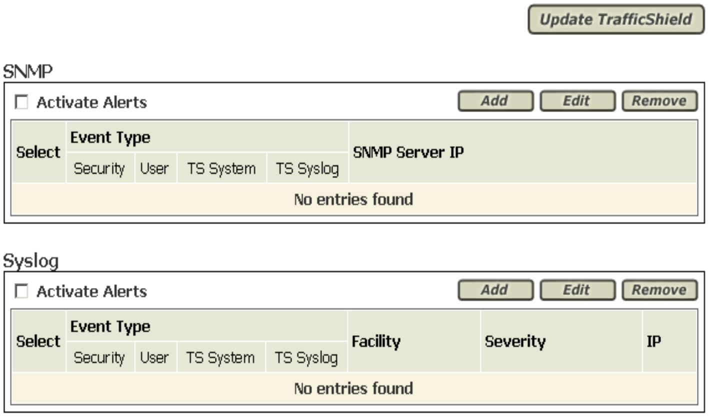
5. If necessary, repeat the operation to create alert collection records that send alerts to different servers.

6. Click **Update TrafficShield**.

TrafficShield Application Firewall enables you to download an SNMP MIB file. For more information, refer to *SNMP MIB*, on page 6-26.

To add an event to be sent to the Syslog server

1. Select **Administration > Configuration** > **Alerts**.
   The Alerts screen opens.



SNMP

□ Activate Alerts

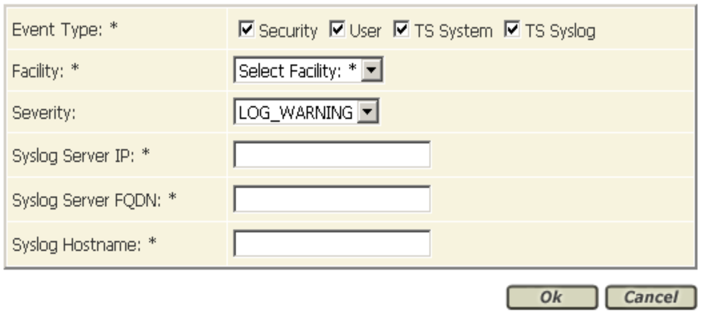
Select	Event Type				SNMP Server IP
	Security	User	TS System	TS Syslog	
No entries found					

Syslog

□ Activate Alerts

Select	Event Type				Facility	Severity	IP
	Security	User	TS System	TS Syslog			
No entries found							

2. From the Syslog area, click **Add**.
   The Add Syslog screen opens.



Event Type: *	☑ Security ☑ User ☑ TS System ☑ TS Syslog
Facility: *	Select Facility: * ▾
Severity:	LOG_WARNING ▾
Syslog Server IP: *	
Syslog Server FQDN: *	
Syslog Hostname: *	

3. In the **Event Type** box, select the types of events to log, as described in the following table.

Option	Collects
Security	Events identified as policy violations.
User	Operations performed by TSMS users. For example, logging in to TSMS is a user event.
TrafficShield System	Events related to Shield and management operations. For example, rebooting units is a system event.
TrafficShield Syslog	Events registered at the OS system log.

4. In the **Facility** box, select the facility type as defined on the Syslog server.
5. In the **Severity** box, select the severity as defined on the Syslog server.
6. In the **Syslog Server IP** box, enter the server IP address of the server that will receive the events.
7. In the **Syslog Server FQDN** box, enter the fully qualified domain name.
8. In the **Syslog Hostname** box, enter the host name.
9. When you have finished entering all of the information, click **OK**. When you add your first SNMP alert, the **Activate Alerts** check box is automatically selected.
10. If necessary, repeat the operation to create alert collection records that combine different types of alerts.
11. Click **Update TrafficShield**.

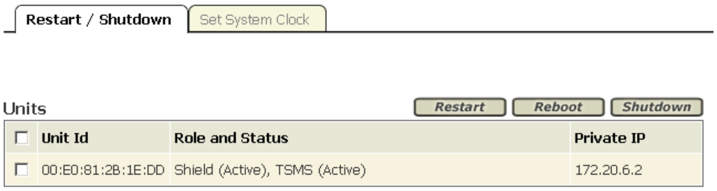
Maintenance-System

From the Maintenance-System screen you can restart, reboot, shut down and set the time for TrafficShield Application Firewall units. Major modifications in the configuration require you to restart the units.

Restarting, rebooting, and shutting down

To restart, reboot, or shut down TrafficShield Application Firewall

1. Select **Administration > Maintenance > System**.
2. Ensure that the Restart/Shutdown tab is selected.
   The existing TrafficShield Application Firewall units are listed.



Units

□	Unit Id	Role and Status	Private IP
□	00:E0:81:2B:1E:DD	Shield (Active), TSMS (Active)	172.20.6.2

3. Select the unit by checking its check box in the leftmost column.
4. Click the appropriate button: **Restart**, **Reboot**, or **Shutdown**. The differences between them are explained in the following sections.

Restart

Restart restarts all TrafficShield Application Firewall related software components.

◆ **Note**

Restart affects only the TrafficShield Application Firewall components and not the Operating System.

The following actions require you to Restart TrafficShield Application Firewall components:

- Changing a Verification Object in the HTTP/HTTPS protocol.
- Changing any parameter in the client certificate.
- Changing any internal parameter.
- Changing any parameter in the System screen.
- Changing the Service IP and/or the Service port if the verification object has been defined.

Reboot

Reboot halts the system and resets the hardware. You must wait several minutes before connecting to your unit.

◆ **Note**

If you have a Standby unit installed, it will become the Active unit and the other re-booted unit will become the Standby unit.

Shutdown

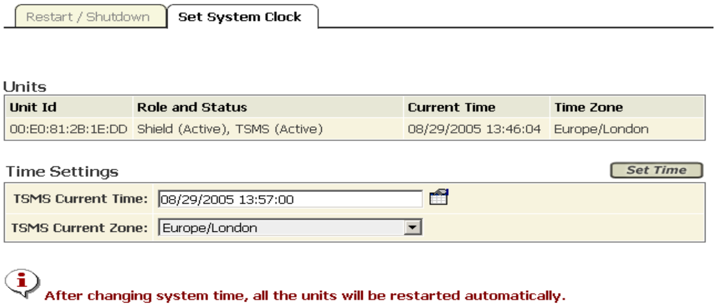
Shutdown powers the unit down.

To turn the power back on, you will need to manually turn on the unit by using the power button.

Setting the system date and time

To set the system date and time

1. Select **Administration > Maintenance > System**.
2. In the screen that appears, click the **Set System Clock** tab.



Units

Unit Id	Role and Status	Current Time	Time Zone
00:E0:81:2B:1E:DD	Shield (Active), TSMS (Active)	08/29/2005 13:46:04	Europe/London

Time Settings

TSMS Current Time: 08/29/2005 13:57:00

TSMS Current Zone: Europe/London

After changing system time, all the units will be restarted automatically.

3. In the **TSMS Current Time** box, either enter the current date and time, or click the calendar icon to set the current date and time.
4. In the **TSMS Current Zone** box, select the correct time zone.
5. When you are complete setting the date and time, click **Set Time**. All units are restarted, and you are sent to the Login page.

◆ **Important**

Changing the date and/or the time requires a system restart.

Upgrades

This section describes the upgrade process of TrafficShield Application Firewall software.

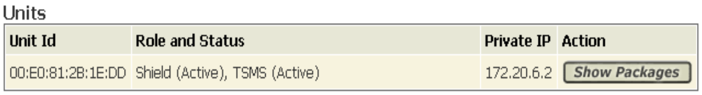
New software upgrade packages are installed using the Install Package Wizard.

At the end of the installation, depending on the package contents, you may be required to restart or reboot the TrafficShield Application Firewall unit.

Installing a software package

To install a Software Package

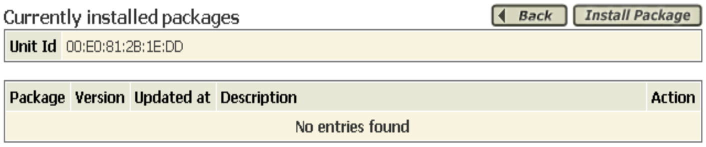
1. Select **Administration** > **Maintenance** > **Upgrades**.
   A list of the installed TrafficShield Application Firewall units appears.



Units

Unit Id	Role and Status	Private IP	Action
00:E0:81:2B:1E:DD	Shield (Active), TSMS (Active)	172.20.6.2	Show Packages

2. Choose the relevant unit to upgrade and click **Show Packages**. The Currently Installed packages screen is opened. If this is the first upgrade you perform on the system, no rows are displayed.



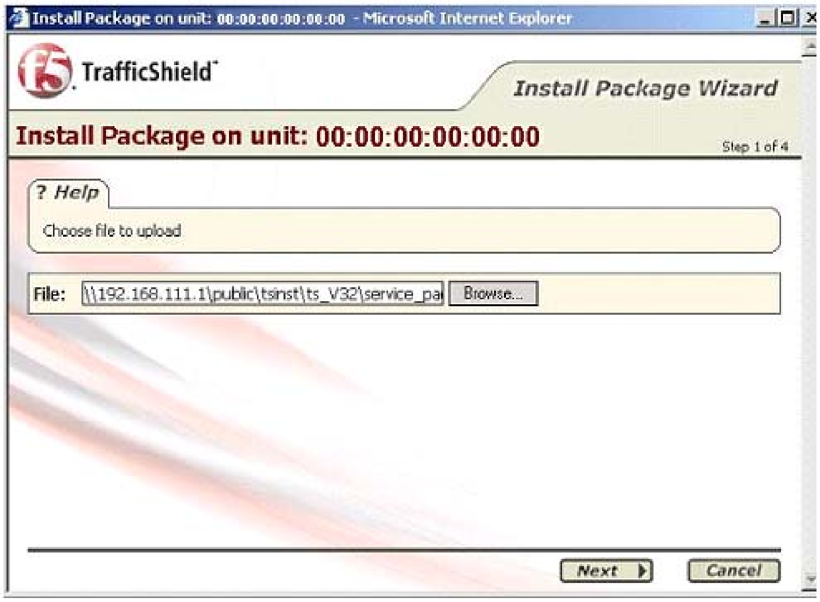
Currently installed packages

Unit Id 00:E0:81:2B:1E:DD

Package	Version	Updated at	Description	Action
			No entries found	

3. Click **Install Package** to open the Install Package Wizard.

Install Package Wizard


Install Package on unit: 00:00:00:00:00:00 - Microsoft Internet Explorer
TrafficShield
Install Package Wizard
? Help
Browse...
Next
Cancel

Install Package on unit: 00:00:00:00:00:00

Step 1 of 4

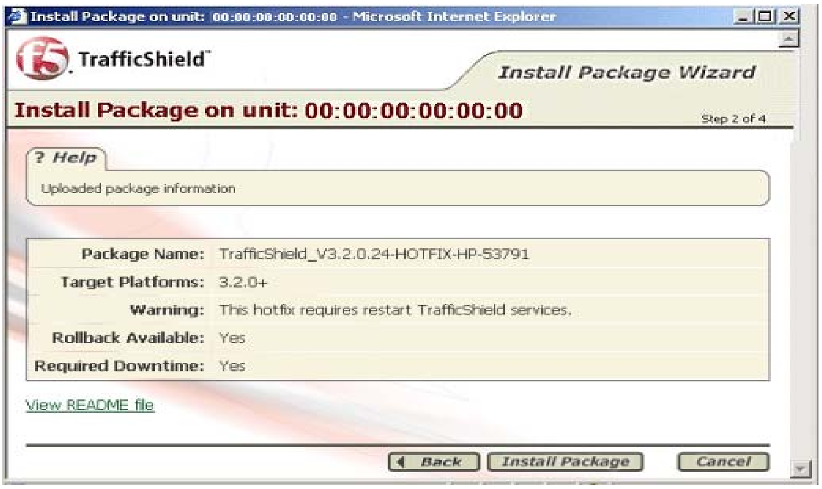
Choose file to upload

File: \\192.168.111.1\public\tsinst\ts_V32\service_pa

Step 1: Upload the package file

1. Click **Browse** to locate the package file you want to upgrade.
2. Click **Next**.

Step 2: Package information uploaded and displayed



Install Package on unit: 00:00:00:00:00:00

Step 2 of 4

Uploaded package information

Package Name:	TrafficShield_V3.2.0.24-HOTFIX-HP-53791
Target Platforms:	3.2.0+
Warning:	This hotfix requires restart TrafficShield services.
Rollback Available:	Yes
Required Downtime:	Yes

Read the following information displayed on this screen.

Package Name
Note that the package name is not necessarily identical to the file name.

Target Platforms
This is the TrafficShield Application Firewall minimum version number required to install this package.

Warning
Sometimes this area displays a certain risk or problem that the installation of this package may cause under specific circumstances (examples: "You must reboot the unit", or, "You must reactivate the policy.")

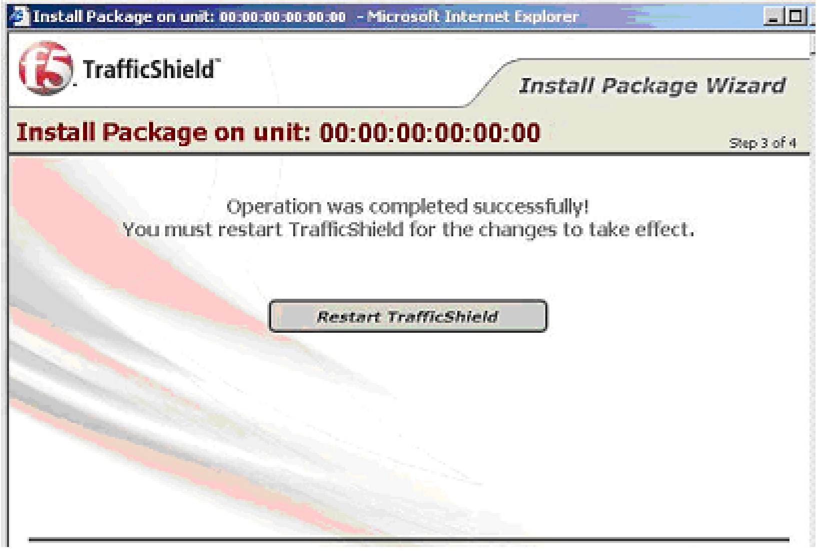
We highly recommend that you read the notes and explanations provided in the README file that can be accessed by clicking the **View README file** link.

Rollback Available
This field indicates whether it is possible to roll back to previous status after installation, should problems occur.

Required Downtime
Sometimes the new package takes effect only after the TrafficShield Application Firewall unit has been reactivated. Required downtime means that the TrafficShield Application Firewall will not protect the application during the installation time.

Click **Back** to go to the previous step, or click **Install Package** to continue.

Step 3: Package successfully installed


Install Package on unit: 00:00:00:00:00:00 - Microsoft Internet Explorer
TrafficShield
Install Package Wizard
Restart TrafficShield

Install Package on unit: 00:00:00:00:00:00

Step 3 of 4

Operation was completed successfully!
You must restart TrafficShield for the changes to take effect.

This screen indicates the successful completion of the package installation to TrafficShield Application Firewall. In the example above, the specific package requires you to restart the unit. Depending on the package, you may be required to either restart or reboot the unit. Should this not be required, the **Restart TrafficShield/Reboot** button will not be displayed.

Click **Finish**, to close the Wizard without restarting the unit.

In this case, it is your responsibility to reboot the unit or restart TrafficShield Application Firewall later, in order to activate the changes created by the package installation.

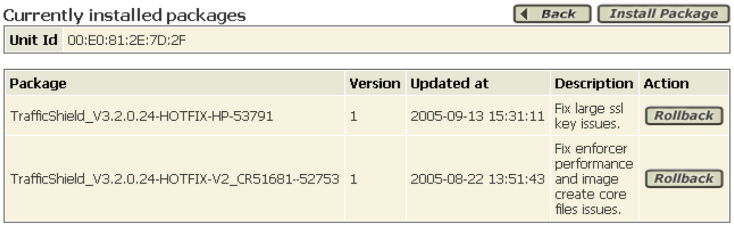
Rolling back an installation

After installing a new software package, problems may occur due to unforeseen circumstances. In some cases it is possible to roll back to a previous software version after installing a new software package.
If you have already installed five sequential packages and you roll back the fifth package, you will roll back to the fourth package.

To roll back from an installation

1. Select **Administration** > **Maintenance** > **Upgrades**.
   A list of the installed TrafficShield Application Firewall units appears.
   If you have an Active unit and a Standby unit and a Shield unit, you need to roll back each unit separately.

2. Choose the relevant Unit to roll back and click the **Show Packages** button. The Currently Installed packages screen is displayed.



Currently installed packages

Unit Id	00:E0:81:2E:7D:2F

Package	Version	Updated at	Description	Action
TrafficShield_V3.2.0.24-HOTFIX-HP-53791	1	2005-09-13 15:31:11	Fix large ssl key issues.	Rollback
TrafficShield_V3.2.0.24-HOTFIX-V2_CR51681--52753	1	2005-08-22 13:51:43	Fix enforcer performance and image create core files issues.	Rollback

3. Click **Rollback** next to the relevant package to roll back. A message is displayed only if the rollback was unsuccessful.

4. Click **Reboot** to reboot the unit.
   A unit reboot or restarting TrafficShield Application Firewall may be required in order to activate the rollback changes.

◆ **Important**

If you have installed several packages, and you want to roll back to a specific package, please roll back in an orderly sequence without skipping any of them (5, 4, 3, etc.).

Backing up

You can set a schedule for automatically backing up the TrafficShield Application Firewall configuration parameters and the security policies. The configuration parameters and the security policies can be backed up separately, or in a single operation. You can also define different backup schedules for the same material and thus create backup ***generations***. You can even create different schedules that direct the data to different backup computers.

Restoring a copy of a full backup allows the complete restoration of TrafficShield Application Firewall configuration, including the security policies.

The backup procedure utilizes the SSH protocol. The TrafficShield Application Firewall initiates an SCP procedure to the backup server, using the backup server user name and password that is acceptable by the backup server and must be supplied from the TSMS user interface.

The backup file is compressed using the **tar.gz** compression software.

The backup file size is dependent on TrafficShield Application Firewall configuration, however, it can reach up to 100MB.

A built in test backup feature enables you to check the accuracy of your settings.

◆ **Important**

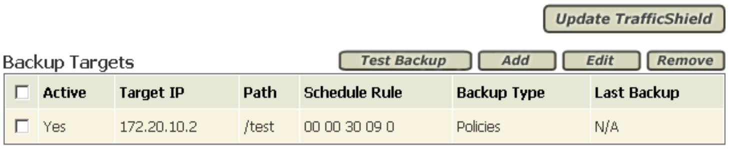
The entire backup procedure is only available if the backup server is running an SSH server.

Defining backup schedules

To secure yourself against hardware failures or unintended modifications to the system, in which case you might want to rollback to the system previous stage, we recommend that you regularly schedule backups.

To schedule backups

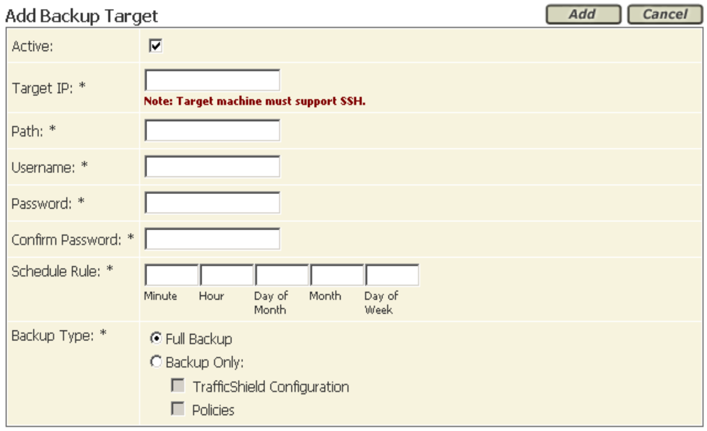
1. Select **Administration > Maintenance > Backup**.
   The Backup Targets screen opens.



Backup Targets

□	Active	Target IP	Path	Schedule Rule	Backup Type	Last Backup
□	Yes	172.20.10.2	/test	00 00 30 09 0	Policies	N/A

2. Click **Add**.
   The Add Backup Target screen opens.



Add Backup Target

Active:	☑
Target IP: *	□ Note: Target machine must support SSH.
Path: *	□
Username: *	□
Password: *	□
Confirm Password: *	□
Schedule Rule: *	□ Minute □ Hour □ Day of Month □ Month □ Day of Week
Backup Type: *	● Full Backup ○ Backup Only: □ TrafficShield Configuration □ Policies

3. Enter the information described here.

   Active
   The Active check box must be checked in order for the schedule to run.
   At first, you may want to create schedules with this box cleared in order to prevent the system from running backups before you are ready to do so. You can activate a schedule at any time by checking this box.

   Target IP
   Specify the IP address of the computer where the backed up data will be stored.
   Note that the backup procedure uses Secure Shell (SSH). The target computer should be configured to use this protocol.

   Path
   Specify the path to the folder where you want to store the data on the backup computer's disk.

   Username, Password
   Specify the user name and the password that are needed to access the backup computer.
   Important: *The password for a backup target cannot contain the single quote, semi colon, vertical bar, double quotes, opening parenthesis, closing parenthesis, or the ampersand* [**‘ ; | " ( ) &**].

   Confirm Password
   Type the password again.

   Schedule Rule
   Specify the schedule using the UNIX cron syntax.
   The Format is in this order: minute, hour, day, month, weekday. The command is: Minute: Minutes after the hour (0-59), Hour: 24 hour format (0-23), Day: Day of the month (1-31), Month: Month of the year (1-12), Weekday: Day of the week (0-6; the 0 refers to Sunday).

Backup Type
Select what to back up:
- If you want to perform a full backup, select **Full Backup**.
- If you want to only backup the TrafficShield Application Firewall configuration, select the **Backup Only** radio button, and check the **TrafficShield Configuration** check box.
- If you want to only backup the policies, select the **Backup Only** radio button, and check the **Policies** check box.
You may select the **Backup Only** radio button and check both the **TrafficShield Configuration** and the **Policies** check boxes.

4. Click **Add**.
   The backup definition appears on the Backup Targets.

5. Repeat the above procedure for all the backup schedules you want to define.
   Defining different schedules for the same material creates ***generations***. A ***generation*** helps you restore data as it was at the time the ***generation*** was created.

6. Click **Update TrafficShield**.

Testing the destinations

This procedure is designed to check that the data supplied in the backup definition is correct. The test checks the correctness of the destination IP address, the user name and password, and the path, as entered in the backup definition.

To test a destination

1. Select **Administration > Maintenance > Backup**.
   The Backup Targets screen opens.

2. Select the backup entry to test by checking its check box on the leftmost column. You can test one backup entry at a time.

3. Click **Test Backup**.
   If all data is correct, a confirmation message appears.

Restoring

TrafficShield Application Firewall enables you to restore what you have backed up from the **Backup Type** field of the Add Backup Target screen. For more information about the Add Backup Target screen, see *Defining backup schedules*, on page 6-15.

- If you selected **Full Backup**, you need to run the **restore_backup.pl** script.
- If you selected **Backup Only: TrafficShield Configuration**, you need to run the **restore_config.pl** script.
- If you selected **Backup Only: Policies**, you need to run the **restore_policies.pl** script.
- If you selected **Backup Only: TrafficShield Configuration** and **Policies**, you need to run both the **restore_config.pl** and the **restore_policy.pl** scripts.

◆ **Important**

If you run both the ***restore_config.pl*** *and the* ***restore_policy.pl*** *scripts, you must first run the* ***restore_config.pl*** *script and then the* ***restore_policy.pl*** *script.*

To restore TrafficShield Application Firewall on a machine

1. Plug in the machine to be restored.
2. Copy the backup file onto the machine.
3. From the command line, stop TrafficShield Application Firewall by running the script
   /ts/tools/kill_procs.pl all
4. From the command line, run the appropriate script (for example, **/ts/tools/restore_backup.pl**) with the relevant command line parameters.

The **required** parameters using the **restore_backup.pl** and **restore_config.pl** scripts are as follows:

Parameter	Description
-f	The file name
-r	The unit role (A if Active, B if Backup)

The **optional** parameters using the **restore_backup.pl** and **restore_config.pl** scripts are as follows:

Parameter	Description
-b	The MAC address of the backup unit
-m	The Permanent IP to be assigned to the unit
-n	The Permanent IP netmask

◆ **Important**

If you are using the ***restore_policy.pl script****, only the required parameter* ***-f*** *is available.*

Example:

```
/ts/tools/restore_backup.pl -f <filename> -r A
-b <backup_mac_address> -m <permanent_ip> -n
<permanent_ip_netmask>
```

where **<filename>** is replaced with the appropriate file name depending on what you are restoring.

Examples of different file names:

- Backup_FullBackup_2005_9_12_16_45.tar.gz
- Backup_TSConfiguration_2005_9_12_16_45.tar.gz
- Backup_TSPolicies_2005_9_12_16_45.tar.gz

Permanent IP addresses

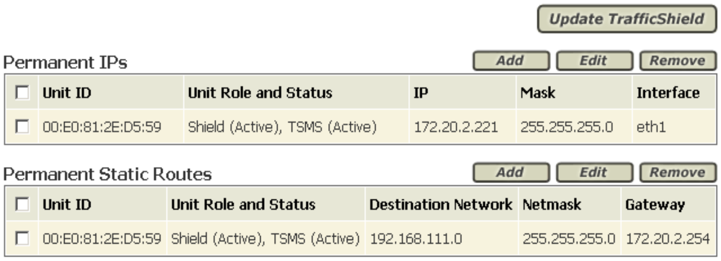
Each TrafficShield Application Firewall unit may have one or more permanent IP addresses that remain usable even when TrafficShield Application Firewall processes are down. This is not mandatory. If you need permanent addresses, define them as explained below. You can either add/edit a Permanent IP address. For more information on Permanent IP, see *Network terminology*, on page 2-1.

◆ **Important**

TrafficShield Application Firewall supports up to nine permanent IP addresses.

To add a permanent IP address

1. Select **Administration** > **Maintenance** > **Permanent IPs**.



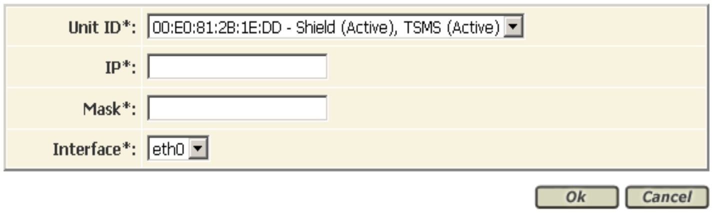
Permanent IPs

□	Unit ID	Unit Role and Status	IP	Mask	Interface
□	00:E0:81:2E:D5:59	Shield (Active), TSMS (Active)	172.20.2.221	255.255.255.0	eth1

Permanent Static Routes

□	Unit ID	Unit Role and Status	Destination Network	Netmask	Gateway
□	00:E0:81:2E:D5:59	Shield (Active), TSMS (Active)	192.168.111.0	255.255.255.0	172.20.2.254

2. Click **Add** above the Permanent IPs area.
   The Add Permanent IP screen opens.



Unit ID*: 00:E0:81:2B:1E:DD - Shield (Active), TSMS (Active)

IP*:

Mask*:

Interface*: eth0

3. Enter the following information:

   Unit ID
   Select the unit to which you want to assign a permanent IP address.

   IP, Mask
   Enter the unit's permanent IP address and its network mask.

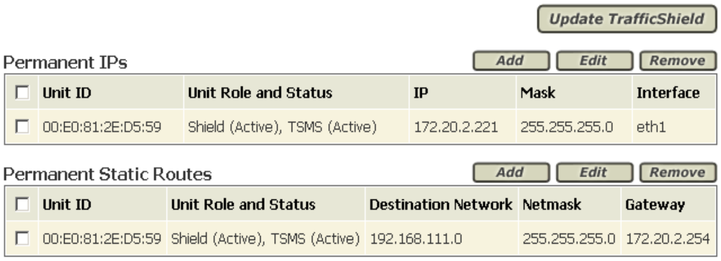
   Interface
   Each unit has two network interfaces. Select the interface to which you want to assign a permanent IP address.

4. Click **OK**.
   The permanent IP address definition appears on the Permanent IPs screen.

5. Repeat the above procedure for all the permanent IP addresses you want to define.
6. Click **Update TrafficShield** to update the unit.

To edit a permanent IP address

1. Select **Administration** > **Maintenance** > **Permanent IPs**.



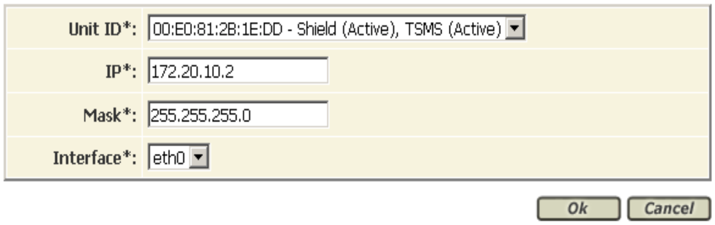
Permanent IPs

☐ Unit ID	Unit Role and Status	IP	Mask	Interface
☐ 00:E0:81:2E:D5:59	Shield (Active), TSMS (Active)	172.20.2.221	255.255.255.0	eth1

Permanent Static Routes

☐ Unit ID	Unit Role and Status	Destination Network	Netmask	Gateway
☐ 00:E0:81:2E:D5:59	Shield (Active), TSMS (Active)	192.168.111.0	255.255.255.0	172.20.2.254

2. Check the check box next to the IP address you want to edit, and click **Edit** above the Permanent IPs area.
   The Edit Permanent IP screen opens.



Unit ID*:	00:E0:81:2B:1E:DD - Shield (Active), TSMS (Active)
IP*:	172.20.10.2
Mask*:	255.255.255.0
Interface*:	eth0

3. Edit the following information:

   Unit ID
   Select the unit to which you want to assign a permanent IP address.

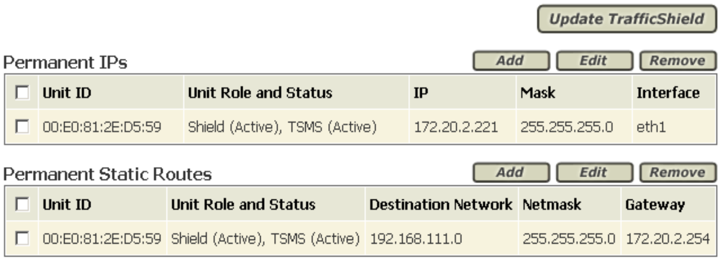
   IP, Mask
   Enter the unit's permanent IP address and its network mask.

   Interface
   Each unit has two network interfaces. Select the interface to which you want to assign a permanent IP address.

4. Click **OK**.
   The permanent IP address definition appears on the Permanent IPs screen.
5. Repeat the above procedure for all the permanent IP addresses you want to edit.
6. Click **Update TrafficShield** to update the unit.

To remove a permanent IP address

1. Select **Administration** > **Maintenance** > **Permanent IPs**.



Permanent IPs

□	Unit ID	Unit Role and Status	IP	Mask	Interface
□	00:E0:81:2E:D5:59	Shield (Active), TSMS (Active)	172.20.2.221	255.255.255.0	eth1

Permanent Static Routes

□	Unit ID	Unit Role and Status	Destination Network	Netmask	Gateway
□	00:E0:81:2E:D5:59	Shield (Active), TSMS (Active)	192.168.111.0	255.255.255.0	172.20.2.254

2. Check the check box/boxes next to all of the IP address you want to remove, and click **Remove** above the Permanent IPs area.
3. Click **Update TrafficShield** to update the unit.

Adding a Static Route

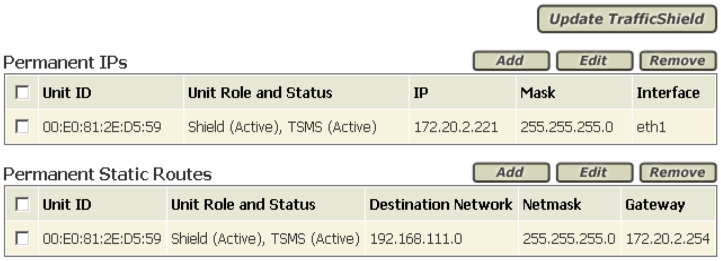
If the host, from which the TSMS Administrator attempts to access the unit, resides in a network different from those of TrafficShield Application Firewall, then the communication between the host and the TSMS is done through a router (gateway). In this case, you need to add a permanent static route.

Permanent static routes are operating system level routes that remain present even if TrafficShield Application Firewall processes are down.

In the Permanent Static Route section you can add/edit a permanent static route, and set a default gateway.

To add a permanent Static Route

1. Select **Administration** > **Maintenance** > **Permanent IPs**.



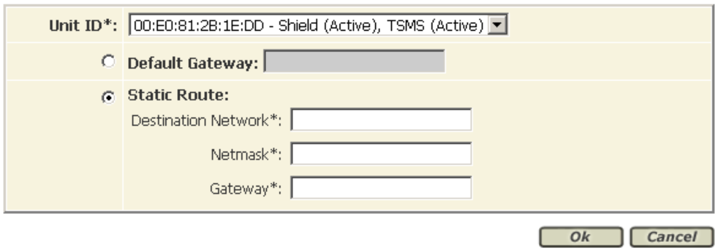
Permanent IPs

□	Unit ID	Unit Role and Status	IP	Mask	Interface
□	00:E0:81:2E:D5:59	Shield (Active), TSMS (Active)	172.20.2.221	255.255.255.0	eth1

Permanent Static Routes

□	Unit ID	Unit Role and Status	Destination Network	Netmask	Gateway
□	00:E0:81:2E:D5:59	Shield (Active), TSMS (Active)	192.168.111.0	255.255.255.0	172.20.2.254

2. Click **Add** above the Permanent Static Routes area.
   The Add Permanent Static Route screen opens.



Unit ID*:	00:E0:81:2B:1E:DD - Shield (Active), TSMS (Active)
○	Default Gateway:
●	Static Route:
	Destination Network*:
	Netmask*:
	Gateway*:

3. Enter the following:

   Unit ID
   Select the unit to which you want to assign a permanent static route.

   Default Gateway
   The IP address of the default gateway

   Static Route Destination Network
   The IP address of the destination network.

   Static Route Destination Netmask
   The netmask of the destination network address.

   Static Route Destination Gateway
   The IP address of the gateway

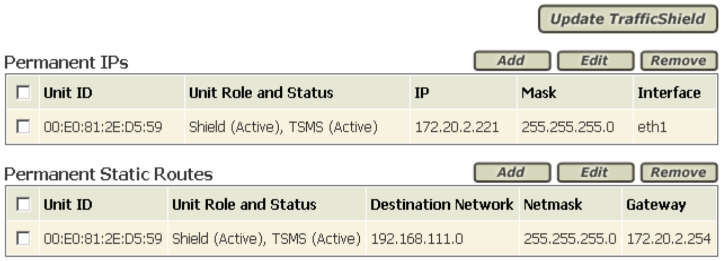
4. Click **OK**.
   The permanent Static Route definition appears on the Permanent IPs screen.

5. Repeat the above procedure for all the permanent Static Route addresses you want to define.

6. Click **Update TrafficShield** to update the unit.

To edit a permanent Static Route

1. Select **Administration** > **Maintenance** > **Permanent IPs**.



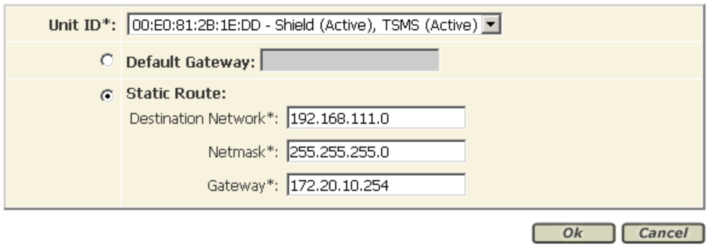
Permanent IPs

□	Unit ID	Unit Role and Status	IP	Mask	Interface
□	00:E0:81:2E:D5:59	Shield (Active), TSMS (Active)	172.20.2.221	255.255.255.0	eth1

Permanent Static Routes

□	Unit ID	Unit Role and Status	Destination Network	Netmask	Gateway
□	00:E0:81:2E:D5:59	Shield (Active), TSMS (Active)	192.168.111.0	255.255.255.0	172.20.2.254

2. Check the check box next to the permanent static route you want to edit, and click **Edit** above the Permanent Static Routes area.
   The Edit Permanent Static Route screen opens.



Unit ID*:	00:E0:81:2B:1E:DD - Shield (Active), TSMS (Active)
○ Default Gateway:	
● Static Route:	
Destination Network*:	192.168.111.0
Netmask*:	255.255.255.0
Gateway*:	172.20.10.254

3. If the PC resides in an external network, edit the following:

   Unit ID
   Select the unit to which you want to assign a permanent static route.

   Default Gateway
   The IP address of the default gateway

   Static Route Destination Network
   The IP address of the destination network.

   Static Route Destination Netmask
   The netmask of the destination network address.

   Static Route Destination Gateway
   The IP address of the gateway

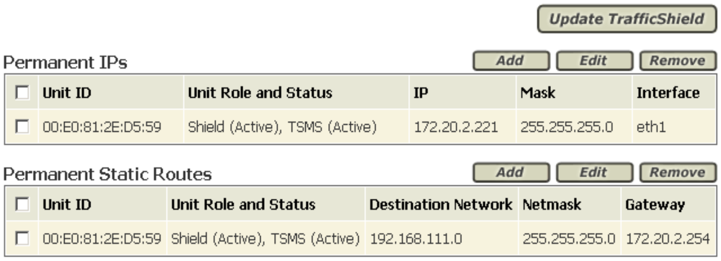
4. Click **OK**.
   The permanent Static Route definition appears on the Permanent IPs screen.

5. Repeat the above procedure for all the permanent Static Route addresses you want to edit.

6. Click **Update TrafficShield** to update the unit.

To remove a permanent static route

1. Select **Administration** > **Maintenance** > **Permanent IPs**.



Permanent IPs

□	Unit ID	Unit Role and Status	IP	Mask	Interface
□	00:E0:81:2E:D5:59	Shield (Active), TSMS (Active)	172.20.2.221	255.255.255.0	eth1

Permanent Static Routes

□	Unit ID	Unit Role and Status	Destination Network	Netmask	Gateway
□	00:E0:81:2E:D5:59	Shield (Active), TSMS (Active)	192.168.111.0	255.255.255.0	172.20.2.254

2. Check the check box/boxes next to all of the permanent static routes you want to remove, and click **Remove** above the Permanent Static Routes area.

3. Click **Update TrafficShield** to update the unit.

Downloads

TrafficShield Application Firewall supports four types of Policy Browser downloads, two for the Windows® platform, and two for the Linux platform. For each platform you may download the Policy Browser Install Kit with VM or without VM. The packages with VM include the Sun® Java Virtual Machine, and the packages without VM do not.

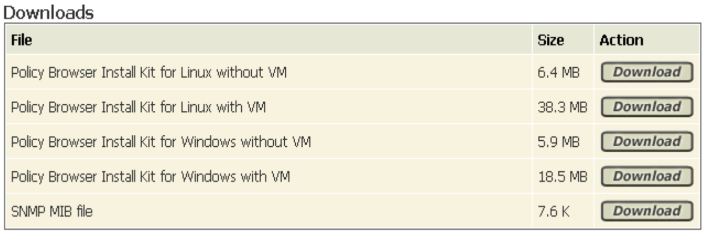
In addition, TrafficShield Application Firewall supports one SNMP MIB file download.

Policy Browser

The Policy Browser is an add-on tool that enables you to record your browsing activities on your website into an output file. This output file can be loaded later onto the TrafficShield Application Firewall security policy, and can be used to build up the TrafficShield Application Firewall security policy.

To download the Policy Browser software

1. Select **Administration > Maintenance > Downloads**.



Downloads

File	Size	Action
Policy Browser Install Kit for Linux without VM	6.4 MB	Download
Policy Browser Install Kit for Linux with VM	38.3 MB	Download
Policy Browser Install Kit for Windows without VM	5.9 MB	Download
Policy Browser Install Kit for Windows with VM	18.5 MB	Download
SNMP MIB file	7.6 K	Download

2. Choose the appropriate file that corresponds to your system configuration. Click **Download** next to the policy browser install kit you choose to download.
3. Save the file to a selected folder.
4. Run the downloaded executable file to install the policy browser on your machine.
5. At the end of the installation, run the policy browser.

◆ **Note**

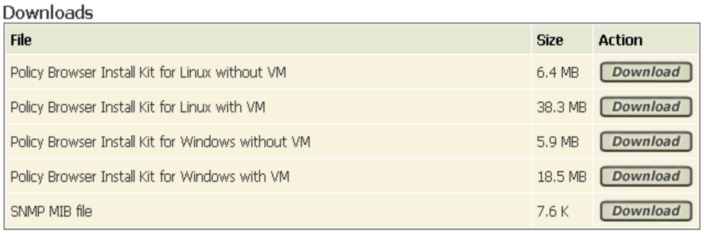
*The recorded browsing session is saved in **mybrowser.csv**. Load this file from browser recordings. For information on loading the browser recordings, see **TrafficShield® Security Policy User Manual version 3.2.1**, Chapter 5, The Crawler Tool.*

SNMP MIB

Within the SNMP architecture, a Management Information Base (MIB) models each managed subsystem with a subsystem-specific definition. A MIB module specifies precisely the management data and operations that a subagent makes possible. So, in case of TrafficShield Application Firewall, the MIB file is used by the SNMP management station to identify and classify the SNMP traps arriving from TrafficShield Application Firewall. The SNMP MIB file is not necessary to configure/enable SNMP Alerts on the TrafficShield Application Firewall itself. For more information regarding the SNMP Alerts feature, see *Alerts*, on page 6-6.

To download the SNMP MIB file

1. Select **Administration > Maintenance > Downloads**.



Downloads

File	Size	Action
Policy Browser Install Kit for Linux without VM	6.4 MB	Download
Policy Browser Install Kit for Linux with VM	38.3 MB	Download
Policy Browser Install Kit for Windows without VM	5.9 MB	Download
Policy Browser Install Kit for Windows with VM	18.5 MB	Download
SNMP MIB file	7.6 K	Download

2. Click **Download** next to **SNMP MIB file**.
3. Save the file to a selected folder.

Support tools

The TrafficShield Application Firewall offers you the following support tools:

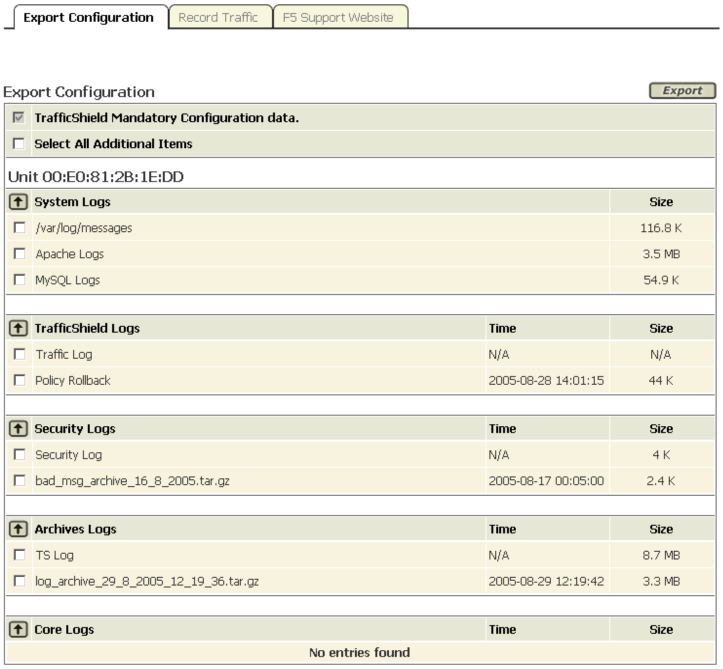
- Export configuration
- Record traffic
- Running a diagnostics test
- F5 support website

Export configuration data and logs

Using the Export Configuration tool, you can export TrafficShield Application Firewall log activity and configuration data from all defined units. The export tool performance is influenced by the unit performance at the time the export process is run. This feature is available for F5 support purposes.

To export your configuration to a disk

1. Select **Administration > Maintenance > Support Tools**.
2. Click the **Export Configuration** tab.
   The Export Configuration tab opens



Export Configuration

☑ TrafficShield Mandatory Configuration data.

□ Select All Additional Items

Unit 00:E0:81:2B:1E:DD

System Logs	Size
□ /var/log/messages	116.8 K
□ Apache Logs	3.5 MB
□ MySQL Logs	54.9 K

TrafficShield Logs	Time	Size
□ Traffic Log	N/A	N/A
□ Policy Rollback	2005-08-28 14:01:15	44 K

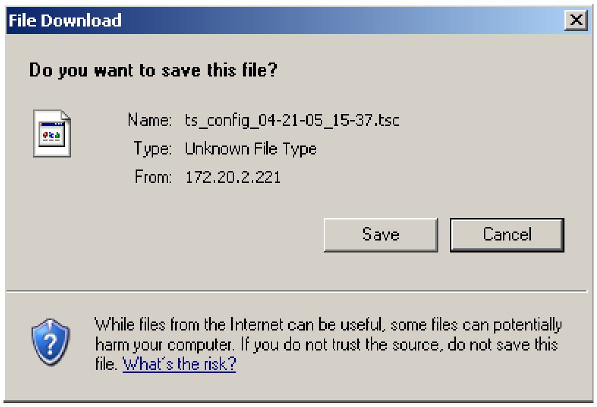
Security Logs	Time	Size
□ Security Log	N/A	4 K
□ bad_msg_archive_16_8_2005.tar.gz	2005-08-17 00:05:00	2.4 K

Archives Logs	Time	Size
□ TS Log	N/A	8.7 MB
□ log_archive_29_8_2005_12_19_36.tar.gz	2005-08-29 12:19:42	3.3 MB

Core Logs	Time	Size
No entries found		

3. Check the check boxes next to the logs you want to export.
   If you want to select all of the items in the list, check the **Select All Additional Items** check box.

4. Click **Export**.
   The File Download screen opens.



Do you want to save this file?

Name: ts_config_04-21-05_15-37.tsc
Type: Unknown File Type
From: 172.20.2.221

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

5. Click **Save** to open the Save As screen.
6. Select the export target folder, and click **Save**.
   The file is saved to the disk and the Download complete screen appears.
7. Click **Close** to return to the TrafficShield Application Firewall.
   The file is saved with a default name:
   ts_config_mm-dd-yy_hh-mm.tsc
   You can modify that name before saving it.

Record traffic

The Record Traffic tool is used to record the traffic between the clients and the TrafficShield Application Firewall, through either HTTP or HTTPS service ports. The Record Traffic tool collects packets from interfaces 1.1 or 1.2, depending on which you are using. This output is used for support purposes only, and is exported as part of the system configuration or copied directly. Record Traffic uses a **tcpdump** utility and collects all traffic passing through ports **80** and **443** on the TrafficShield Application Firewall.

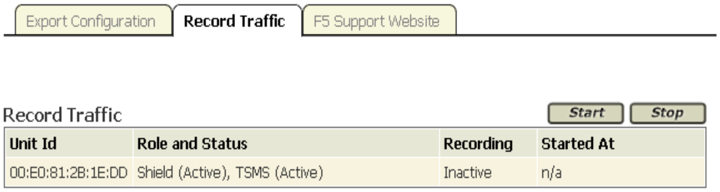
Traffic is recorded in the following files: **/ts/log/temp/rec_traffic.new** and **/ts/log/temp/rec_traffic.old**.

The recording filing procedure works as follows:

- The first recording is recorded in a file named **rec_traffic.new**.
- When the file **rec_traffic.new** reaches its size limit of 100MB, the file **rec_traffic.new** is automatically renamed **rec_traffic.old**.
  Further recordings are recorded in a new **rec_traffic.new** file.
- When the new **rec_traffic.new** file reaches its size limit of 100MB, it is renamed **rec_traffic.old**, overwriting the old information in the old **rec_traffic.old file**.
  Further recordings are recorded in a new **rec_traffic.new** file.

To record traffic

1. Select **Administration > Maintenance > Support Tools**.
2. Click the Record Traffic tab.
   The Record Traffic tab opens.



Record Traffic

Unit Id	Role and Status	Recording	Started At
00:E0:81:2B:1E:DD	Shield (Active), TSMS (Active)	Inactive	n/a

3. Click **Start**.
   You are required to confirm the action, and upon confirmation, the recording operation starts.
4. To end the recording, click **Stop**.
   You are required to confirm the action, and upon confirmation, the recording operation stops.

To view the recording files

1. Select **Administration > Maintenance > Support Tools**.
2. Click the **Export Configuration** tab.
3. In the TrafficShield Logs area, check the **Traffic Log** check box, and click **Export**.
4. Save the file.
5. Open the exported file using tar (UNIX/Linux) or WinRAR (Windows) and extract the recording file named **traffic_log.tar.gz**.
   Important: *If you are using Windows, you must change the exported file's extension from* ***.tsc*** *to* ***.tar.gz*** *before running WinRAR.*
6. Open this archive again using an archiving software, and extract the recording files from it.
7. Open the recorded files with a network analyzer software (such as Ethereal).

◆ **Important**

We recommend that you not leave the tool running for long periods of time while TrafficShield Application Firewall is under stress, otherwise the output file may reach its maximum size limit of 100MB and the oldest part of the recording might be lost.

Running a diagnostics test

Running a diagnostics test will help verify that your hardware machine is fully operational.

To run the diagnostics test

1. Run the **$/ts/tools/runeud.pl** command through the command line. This command can only be run through a serial console since it restarts the host. The command is blocked if it is run through SSH.
2. Follow the instructions on the screen.

The diagnostics test is interactive. It lists the tests which may be performed, and you select which hardware components you would like tested.

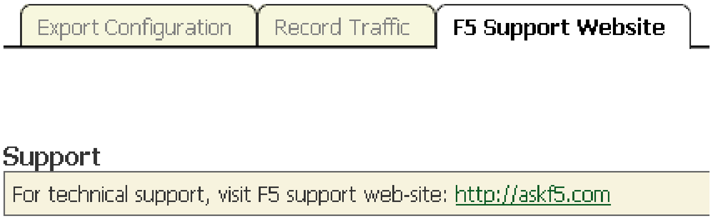
The test results may saved as a report.

F5 support website

This tool provides a link to the Ask F5 Technical Support Center, where you can find additional information, solutions, and documentation for the product.

To access the F5 support website

1. Select **Administration > Maintenance > Support Tools**.
2. Click the **F5 Support Website** tab to display the relevant web site details.



Support

For technical support, visit F5 support web-site: http://askf5.com

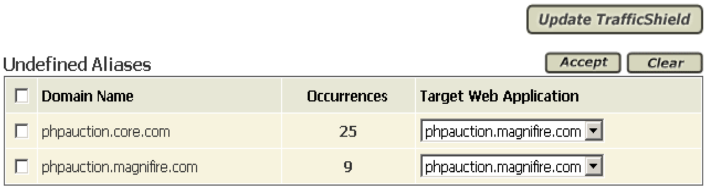
3. Click the **http://askf5.com** link.
   The F5 support web site opens, where you can check on solutions, and locate additional product documentation.

Undefined aliases

The Undefined Aliases tool enables you to accept or reject undefined aliases. Undefined aliases are fully qualified domain names rejected by TrafficShield Application Firewall because they are not configured as the names of TrafficShield Application Firewall Web Applications or their aliases. If any of the addresses in the list appears to be a valid alias of the frequently qualified domain name of your web application, you can accept it. If any address appears to be invalid, you can reject it.

To accept and reject undefined aliases

1. Select **Administration > Maintenance > Undefined Aliases.** The Undefined Aliases screen opens.



☐	Domain Name	Occurrences	Target Web Application
☐	phpauction.core.com	25	phpauction.magnifire.com ▾
☐	phpauction.magnifire.com	9	phpauction.magnifire.com ▾

2. Check the check box next to the domain name you want to accept or reject.
3. For each domain name, select the target web application from the **Target Web Application** box.
4. Click **Accept** to accept the selected domain name or **Clear** to reject the selected domain name.
5. Click **Update TrafficShield**.

Glossary

ARP

Address Request Protocol: (a networking protocol). A method for finding a host's IP address from its Ethernet address. The sender broadcasts an ARP packet containing the IP address of another host and waits for it (or some other host) to send back its Ethernet address. Each host maintains a cache of address translations to reduce delay and loading. ARP allows the IP address to be independent of the Ethernet address, but it only works if all hosts support it.

ARP is defined in RFC 826.

The alternative for hosts that do not do ARP is constant mapping.

Check Object

Indicates whether TrafficShield Application Firewall should check the Object requested in the HTTP/HTTPS request against the list of its known objects before it forwards the request to the server. In case it doesn't find the requested object in the list, it generates a violation that, based on the blocking policy, can cause the request to be blocked.

Cookie

A packet of information sent by an HTTP server to a World-Wide Web browser and then sent back by the browser each time it accesses that server. Cookies can contain any arbitrary information the server chooses and are used to maintain state between otherwise stateless HTTP transactions. Typically this is used to authenticate or identify a registered user of a Web application without requiring them to sign in again every time they access that Web application. Other uses are: maintaining a "shopping basket" of goods you have selected to purchase during a session at a web application, web application personalization (presenting different pages to different users), and tracking a particular user's access to a web application.

DELETE

An HTTP request type that requests to delete a resource on the web server.

Domain Name

A series of alphanumeric strings separated by periods, such as **www.siterequest.com**, that is an address of a computer network connection, and that identifies the owner of the address.

Dynamic Parameter

A dynamic parameter is a parameter in a request where the set of legal values this parameter can have is changing dynamically, and usually depends of the user session. For example, in a banking application the account number is a dynamic parameter, since each user has its own set of legal account numbers that this parameter can have. This set of legal account numbers is dynamically generated by the server and embedded in the web page sent to the user. TrafficShield Application Firewall extracts this list of legal values from the web page that is sent to the user, and uses them to verify that the value sent in the request for the dynamic parameter is legal.

Dynamic Value

See *Dynamic Parameter*.

Entry Point

A web page that could be the first requested page in the web application. An end-user could get to the Entry Point by typing a URL in the browser window, opening a favorites menu, or be linked from a different Web application or e-mail client. The end user could also get to the Entry Point by clicking a Back button of the browser.

Flow

The defined access path for a browser to get from one object to another specific object.

GET

A type of HTTP request that does not have a content body.

Learning

A process of making a policy more accurate by verifying how the policy complies with the traffic requests, and if there are discrepancies between the policy and the traffic requests, then translating these discrepancies into a suggestion for modifying the policy. The learning phase also enables the system administrator to verify that the policy is not generating any false positives before turning on the blocking feature. The learning process can be used to fine-tune any policy component such as requests length, parameters, and values. In case new objects are added in the Web application, TrafficShield Application Firewall can learn those objects and their flows using the learning engine.

Length-Cookie

The length of the cookie.

Length-Post Data

The length of the Data that comes with a POST request.

Length-Query String

The length of the Query string.

Length-Request

See *Request Length*.

Length-URI

The length of the URI in characters.

Meta character

A character or a sequence of characters that has a special meaning (<SCRIPT >, \ , SELECT, INSERT, ; ,`, <).

Method

The HTTP/HTTPS request method, for example, GET, POST, HEAD, PUT, and DELETE.

Non Existent Object

An object not found in the policy’s list of web objects.

Object

A file or a script that generates web pages on the web server that can be requested by a user.

Object is Allowed to modify domain Cookie

In case an Object (for example, a web page) includes a JavaScript/java applet/flash as part of the client-side and can change a domain cookie value, the object should by defined as "Object is allowed to modify Cookie."

Path Traversal

An HTTP Attack that uses patterns like ../../ to get access to files not intended to be viewed above the WWW root, or in order to cross directories on the server.

Policy

A set of rules that enables TrafficShield Application Firewall to understand if a request is valid.

POST

A type of HTTP request, in which a query is put into a content body and possibly compressed or encoded.

PUT

An HTTP request type that requests a content change on the web server.

Query String

Part of an HTTP request that specifies a list of parameters and values into a CGI script. For instance:

http://www.siterequest.com/index.cgi?param1=value1&param2=value2

Anything that comes after the question mark in the example above is a query string.

Referrer

A web page that requests other objects. An HTML page could request picture files and other HTML objects to be downloaded, but pictures cannot cause other objects to be downloaded. For example, HTML, ASP, or PHP pages are usually Referrers, while GIF and JPEG images are not.

Regular Expression

Used by UNIX utilities such as **grep**, **sed** and **awk**, and by editors such as **vi** and **Emacs**. A regular expression (**regexp**) is a sequence of characters which provides the user with a powerful, flexible and efficient test processing tool.

For more details on how to write regular expressions please refer to the many books written on this subject; for example: ***Mastering Regular Expressions***, by Jeffrey E.F. Frieldl, published by O'Reilly & Associates, Inc.

Request Length

The total Length of the HTTP request (in characters) which includes the request line, all headers, cookies, and post data.

Server IP

The IP address of the Web Server that TrafficShield Application Firewall is protecting (usually this is an internal IP address).

Service IP

The external IP address on which TrafficShield Application Firewall is listening for HTTP requests. (Usually this is the IP address that the DNS **A** record of the Web Server is mapped to.)

Shield Unit

The on-line enforcing mechanism responsible for TCP session termination, requests parsing, and analyzing.

Static Parameter

A parameter in the request where its values are chosen from a known set of values: Name of a Country, Yes/No, etc.

Static Value

See *Static Parameter*.

Target Frame

The frame to which the object is loaded.

Undefined Flow

The flow did not match the defined flows.

URI

Part of the URL that specifies the name of the object requested: in **http://www.siterequest.com/index.html**, **index.html** is the URI.