

Fujitsu mPollux

WebFront

White Paper

Fujitsu mPollux Version 2.0

December 2008



The programs described in this document may only be used in accordance with the conditions under which Fujitsu Services Oy supplies them.

This document is provided to your organization on the understanding that its content is and remains the intellectual property of Fujitsu Services Oy. The document is provided on the understanding that its use is confined to the people in your organization who are responsible for evaluating its content and that there is an obligation on your organization and such people within your organization to keep its content in confidence. This document may not, without the prior written authority of Fujitsu Services Oy, be copied or shown in whole or in part to any third party. When no longer required for the agreed purpose, the document is to be returned to Fujitsu Services Oy.

Fujitsu Services Oy endeavors to ensure that the information in this document is correct and fairly stated but does not accept liability for any error or omission.

The development of Fujitsu Services Oy products and services is continuous and published information may not be up to date. It is important to check the current position with Fujitsu Services Oy. This document is not part of a contract or license save insofar as may be expressly agreed.

Fujitsu and the Fujitsu logo are registered trademarks of Fujitsu Limited. The Possibilities are Infinite is a trademark of Fujitsu Limited. mPollux, mPollux security options are trademarks or registered trademarks of Fujitsu Services Oy and Fujitsu Limited. Other product and company names mentioned herein may be trademarks or tradenames of their respective owners.

Table of Contents

1	INTRODUCTION	4
2	BASIC FUNCTIONALITY	4
3	WEBFRONT USE SCENARIOS	6
	3.1 Controllable Firewall	6
	3.2 HTTP Proxy Mode.....	8
4	WEBFRONT BENEFITS	9
5	WEBFRONT FEATURES.....	9

1 INTRODUCTION

Fujitsu mPollux™ Security Server is Fujitsu Services' multifunction security solution, which can be easily adapted for the diverse needs and security level requirements of user organizations. This is made possible by the modular architecture of mPollux™ Security Server: the Server offers a number of Security Options and the user organization chooses the Option(s) that best suit(s) its needs.

This white paper describes the functionality of **mPollux™ WebFront Access Control** that is designed to provide access control in multichannel environments.

2 BASIC FUNCTIONALITY

The mPollux™ WebFront is a module that can be used to implement access control for Web and non-Web applications. mPollux™ WebFront is a dedicated module in separate hardware.

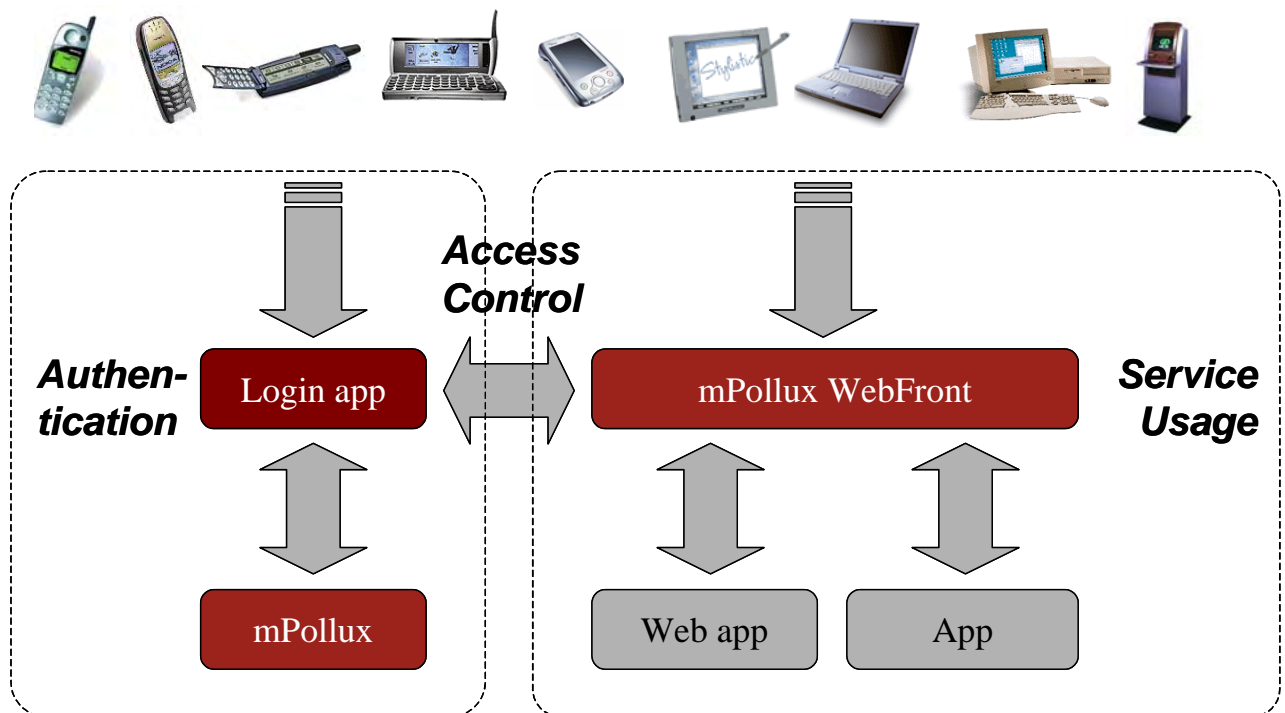


Figure 1. WebFront Usage Environment

The normal working environment for mPollux™ WebFront is described in *Figure 1*.

Users are accessing different applications using a variety of devices. The applications can be either Web applications, i.e. accessed with a Web browser. Or they can be non-Web applications, where they are accessed using a dedicated client.

mPollux™ WebFront is installed from the network point of view in front of the applications so that it is able to control all communication targeted to the applications. mPollux™ WebFront checks whether the users trying to access the applications have been authenticated, and relays the requests of authenti-

cated users to the desired applications. Requests from non-authenticated users are relayed to login applications.

Login applications are responsible for the authentication of the users and controlling mPollux™ WebFront according to the authentication results. Users can be authenticated in different ways utilizing **mPollux™ Security Server**, e.g. using userid and password, mobile phone or smartcards. After successful authentication, the login application will command mPollux™ WebFront to allow the user to access the desired application.

The applications controlled by mPollux™ WebFront fall into two categories: **firewall mode applications** and **HTTP proxy mode applications**.

In the firewall mode mPollux™ WebFront is acting as a controllable firewall. It performs IP level access control based on static and dynamically established rules. The latter ones can be given by login applications using a simple remote control Application Programming Interface (API)

The second category includes Web applications, where mPollux™ WebFront is acting as an HTTP reverse proxy controlling all HTTP requests sent to configured applications. It takes the role of the HTTP or HTTPS server it is controlling access to, and verifies authentication tokens included in the HTTP data stream. The authentication tokens are generated for the client's browser application by a login application upon a successful login, and the browser sends the tokens with every HTTP request to prove its authorization. mPollux™ WebFront forwards the request to the actual content server only if the client's authentication token is accepted, or redirects the client back to the login application if the token fails verification.

Which usage mode can be used depends on the network configuration and the application type due to the different nature of the modes. A rule of thumb is that HTTP proxy mode should be used for Web applications and the firewall mode for other applications. The following chapter describes more detailed the differences between modes.

3 WEBFRONT USE SCENARIOS

The different modes of mPollux™ WebFront are described using two scenarios where mPollux™ WebFront is controlling access to different types of applications.

3.1 CONTROLLABLE FIREWALL

In the first usage scenario mPollux™ WebFront is acting as a controllable firewall controlling all access to servers in the internal network. After successful authentication, the user is given access to configured servers. The scenario is built as follows:

- The user is accessing from the public network a server within a company's internal network.
- The client is accessing the server using TCP/IP.
- The login application is a web application that allows the user to select the service to be accessed and performs the authentication of the user. It utilizes mPollux™ Security Server and mPollux CallSign™ for authentication. Also other authentication mechanisms could be used.

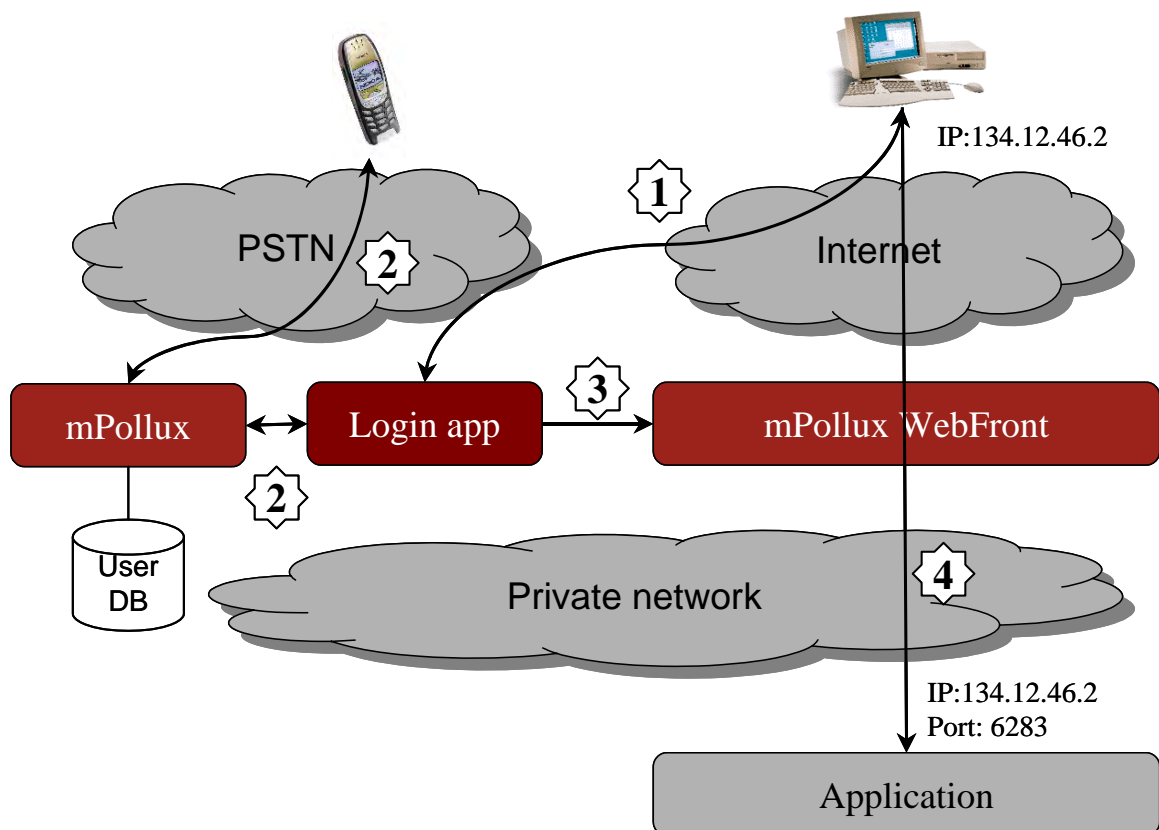


Figure 2. mPollux™ WebFront Firewall mode

The user is accessing the service in the following steps:

1. The user connects to the login application using his browser and identifies himself e.g. by his phone number. The login application also identifies the user's IP address (134.12.46.2)
2. The login application requests mPollux™ to authenticate the user using mPollux CallSign™.
3. After successful authentication, the login application commands mPollux™ WebFront to open path from the user's IP address to IP address of server with a given port number. The login application also defines timeout values for the session.
4. The user starts the client application and connects to the server.

IP level access control is applicable only when the client's IP address can be discovered by the login application and when the address is guaranteed not to change during the session. Most particularly the Web protocols HTTP and HTTPS do not fall into this category – due to the proxied nature of the protocols. The source addresses cannot be guaranteed either to be unique nor unchanging during the session to be authenticated. In this case, the HTTP Proxy mode should be used to control the access.

The firewall mode is best suited for connection-oriented TCP protocols such as SMTP, IMAP, and Windows Terminal Server RDP, where the connection is opened exactly once for the duration of the session and the connection endpoints cannot change after the connection establishment.

3.2 HTTP PROXY MODE

The second usage scenario covers access control to Web applications in the internal network, i.e. the cases where connectionless HTTP protocol is used. An HTTP session consists of a number of TCP connections, typically one connection per object in a web page, and it is often proxied by caching intermediary systems, causing the source address of the connections to change in an unpredictable fashion. When the source address cannot be relied upon, IP level access control as performed by traditional firewalls and mPollux™ WebFront firewall mode becomes impossible.

There can be several web applications whose access is controlled by mPollux WebFront™.

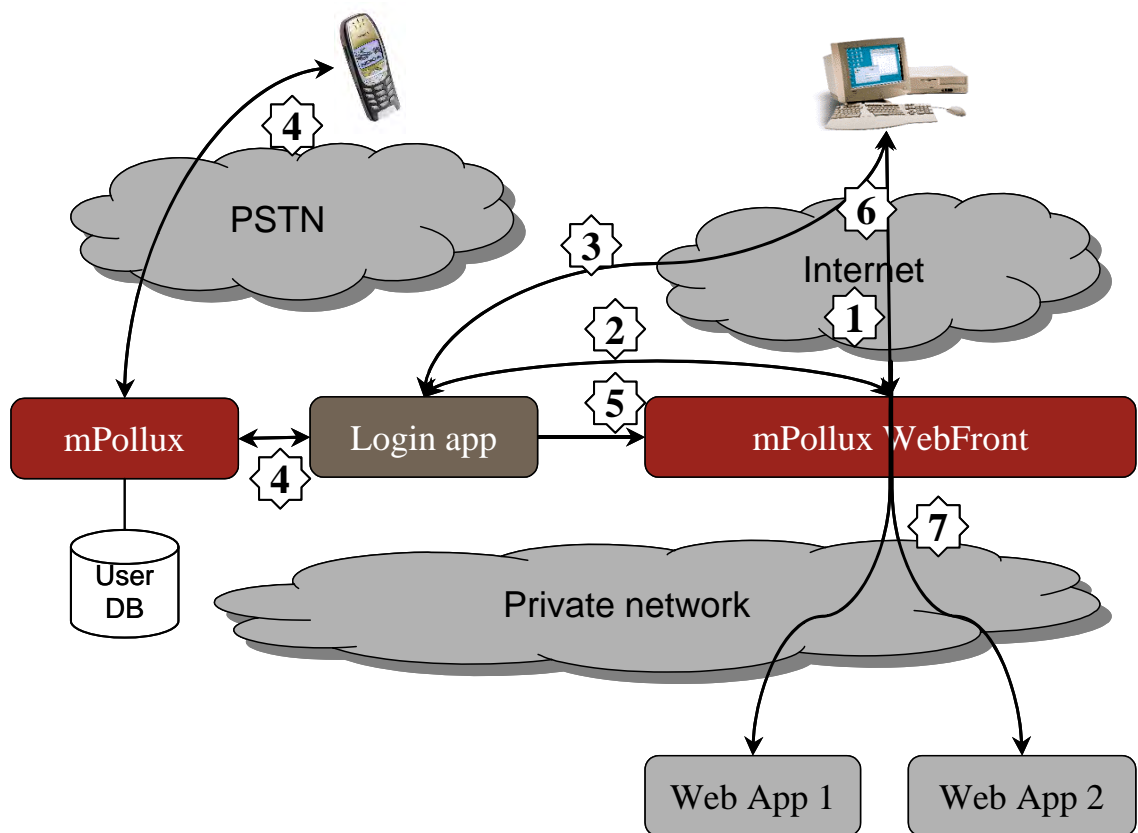


Figure 3. HTTP Proxy mode

1. The user enters to the browser the URL for the service. mPollux™ WebFront will receive the related HTTP request.
2. mPollux™ WebFront recognizes from the missing authentication cookie a non-authenticated user and redirects the user to the login application.
3. The user identifies himself through the web screen provided by the login application e.g. by entering his phone number.
4. The login application authenticates the user utilizing mPollux™.
5. After successful authentication, the login application commands mPollux™ WebFront to create a session for the user. The session information includes an authentication cookie and custom cookies.

6. The authentication cookie is stored into the user's browser as a session cookie and is verified by mPollux™ WebFront for each request.
7. Custom cookies can be used to deliver user information to target applications. They can contain e.g. user ids and groups and other information identified by the login application.
8. Finally, the user id redirected to the target application.

mPollux™ WebFront supports the building of Single Sign-On solutions in different ways. First, mPollux™ WebFront can deliver customizable user identification information to applications. This information includes basic authentication information and customized cookies controlled by login applications. Secondly, the URL used to redirect to the application in the step 8 can emulate a request created by a login page for an application including id and password information. Login applications for mPollux™ WebFront can also perform emulated logins to applications where more complicated logins can be automated.

mPollux™ Security Server supports also storing of SSO related data to its database, such as user ids and passwords for different applications.

4 WEBFRONT BENEFITS

- Access to company's internal applications from Internet
Using mPollux™ WebFront you can securely provide access to internal applications, such as e-mail, calendar, from Internet.
- Simplify application logic by isolating authentication and access control
Using WebFront you do not have to implement authentication and/or access control within your application, but in a separate module. In this way, the application logic is much simpler since you do not need to check for session or authentication information in all pages.
- No need to modify applications
Since mPollux™ WebFront performs authentication and access control in separate modules, you can also secure access to existing applications without the need to modify them.
- Single sign-on, there are several features in WebFront supporting the building of SSO solutions. See the previous chapter for more information.
- Authentication, access control and session management for applications not having them
- Tailorable login applications
With mPollux WebFront™, you can freely choose the way to authenticate users.

5 WEBFRONT FEATURES

General features:

- Runs on Linux Red Hat Enterprise Edition 5, CentOS 5, Suse 10 and Solaris 10 operating system
- Up to three 10/100 Mbps or 1 GB Ethernet links
- Up to 15 IEEE 802.1q tagged VLAN interfaces,
- Multiple alias addresses for each interface
- Bandwidth limiter allowing fine-grained traffic flow control;
- Full IP NAT and address redirection control;

- IPSEC for IPv4 traffic encryption and authentication for VPN solutions;
- An optional domain name service (DNS);
- An optional dynamic host configuration protocol service (DHCP);
- Full IPv6 support.
- XML configuration
- Comprehensive logging facility collecting information about connection requests and sessions. Supports also redirection of logs to an external logging server.
- The automatic control of session lifetime. After specific time WebFront will destroy the session and reject requests sent to target applications. Timeout value can be defined as an absolute time or an idle time.
- Control interfaces available as a Java API, C-language API and a COM+-interface.

HTTP Proxy mode features:

- Both HTTP and HTTPS protocols supported. Supports the mixture of protocols, e.g. HTTPS in the public network and HTTP in the private network. In this way also applications supporting only HTTP can be accessed confidentially from public networks.
- Automatic redirection of non-authenticated clients to the pre-configured login page.
- Authentication information stored as default into a built-in cookie, which is DES encrypted session information. The system supports also the customization of the cookies by adding external cookie validation servers.
- Internal configurable error pages

Firewall mode features:

- Traffic can be controlled by source and target IP addresses and ports.