

Check Point Software Technologies LTD.ä

FireWall-1 ä Version 3.0 Implicit Client Authentication Quick Reference

Authored By: Steven Yurkunas
Area Technical Consultant for NJ
CheckPoint Software Technologies LTD. ä
Date Published: April 2, 1998

The purpose of this document is to provide a guide to implementing Implicit Client Authentication.

This document was written using a FireWall-1™ Enterprise version 4.0, installed on a Microsoft NT 4.0 Server.

In order to understand the benefits of Implicit Client Authentication we must first understand each of the authentication types.

User Authentication Grants access on a per user basis, without regard to IP address. For example, if a local user is temporarily away from the office and logging in from a different host, the administrator may wish to allow that user to continue to work on the local network without extending the same privilege to all users which use that host. ***Non-transparent*** authentication is granted within the protocol. The disadvantage is that User Authentication is restricted to the following services; ftp, http, telnet, & rlogin.

Session Authentication Grants access on a per user basis, without regard to IP address. It is not restricted to certain services (as is User Authentication). Unlike Client Authentication, Session Authentication provides a ***transparent*** per-session authentication mechanism that can be integrated with any application. The disadvantage is that it requires a session authentication agent to be running on the client machine.

Client Authentication Grants access privileges on a per client (host) basis. A user authenticates himself or herself, and can then use any service (allowed by the relevant rule) from the IP address on which the authentication took place (host). Client Authentication is not restricted to certain service as is User Authentication. Client Authentication provides a mechanism for authenticating users of any application, standard or custom (without modification to the application), after a single ***non-transparent*** authentication session.

When Implicit Client Authentication is enabled and an individual successfully performs either User or Session Authentication, FireWall-1™ then “opens” the Standard Sign-On Client Authentication rules in the Rule Base. In other words, by combining the Session and Client Authentication, you don’t have to authenticate for every session, and once authenticated for one application, the authentication for another will be transparent (or implicit).

The primary reason for using Implicit Client Authentication, is to allow the connection information to be viewed in the Stateful Inspection™ engine. By combining User Authentication and Client Authentication, you can authenticate the user as a proxy within the protocol (telnet, http, ftp, rlogin), and then get the performance benefits of Stateful Inspection™.

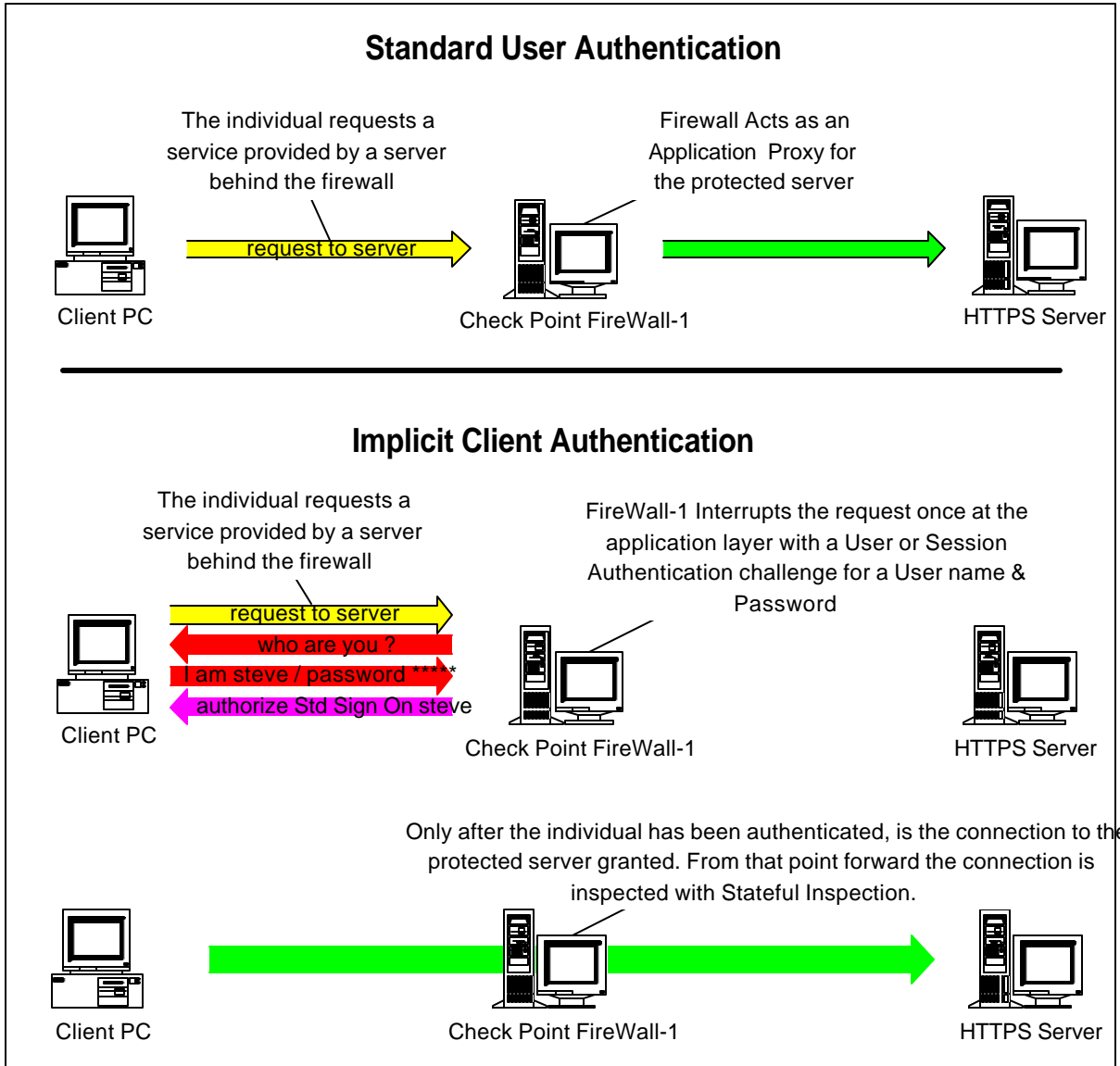


Fig-1

The rule base for an Implicit Client Authentication connection should resemble the following.

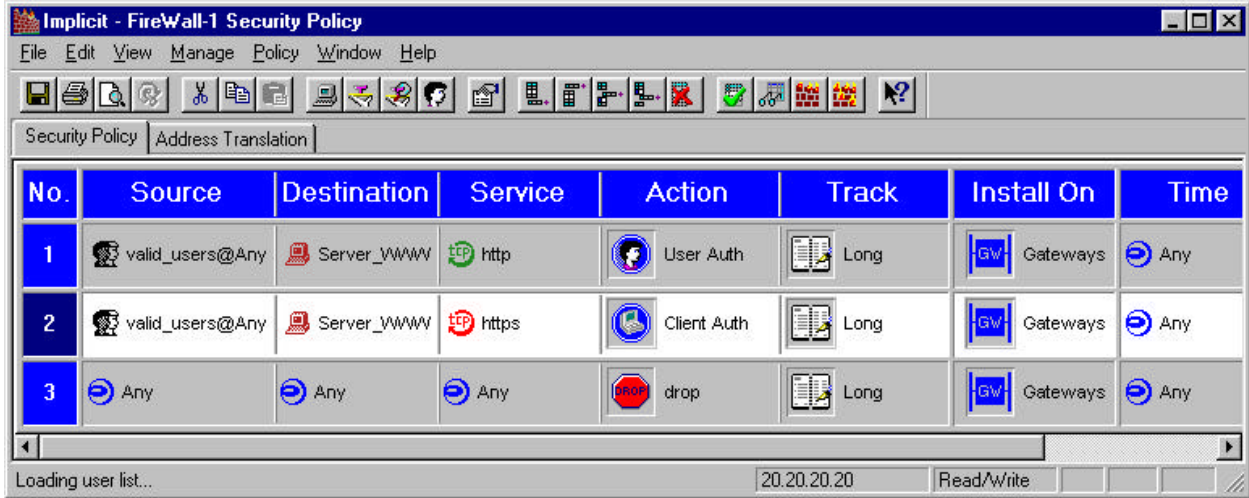


Fig-2

In order to create the above rules we first need to define the following objects.

valid_users@any	User ID's found in the Firewall-1™ database
steve	"steve" is the user name defined as a member of valid_users@any
server_WWW	Web server defined with the IP address of 20.20.20.2
http	predefined service at tcp port 80
https	predefined service at tcp port 443
User Authentication	Allows the members of valid_users@any to access the server_WWW for the services ftp, telnet, rlogin, & http, after correctly responding to the authentication challenge.
Client Authentication	Allows the members of valid_users@any to access the server_WWW with services other than ftp, telnet, rlogin, & http, without the need for further authentication.
Long	This will log all transaction information to the Firewall log file.

Rule #

- 1) Define the initial User Authentication rule, this will allow clients to be authenticated for ftp, telnet, rlogin, and http. This example sites User Authentication, Session Authentication could also be used.
- 2) Define the Client Authentication rule employing Stateful Inspection™ rather than the User or Session Authentication's Proxy Service.
- 3) The final rule is needed only for logging purposes. The last rule in the Rule Base is always an implied, any, any, any, drop, but the implied rule will not log the connection information.

Once all objects are defined, and all rules are in place, install the rule base.

The next step in the process, will be to edit the *objects.c* file.

NOTE -

FireWall-1™ overwrites this file each time the firewall is stopped. For this reason we first need to stop the FW-1 process before editing the file.

This can be done as follows;

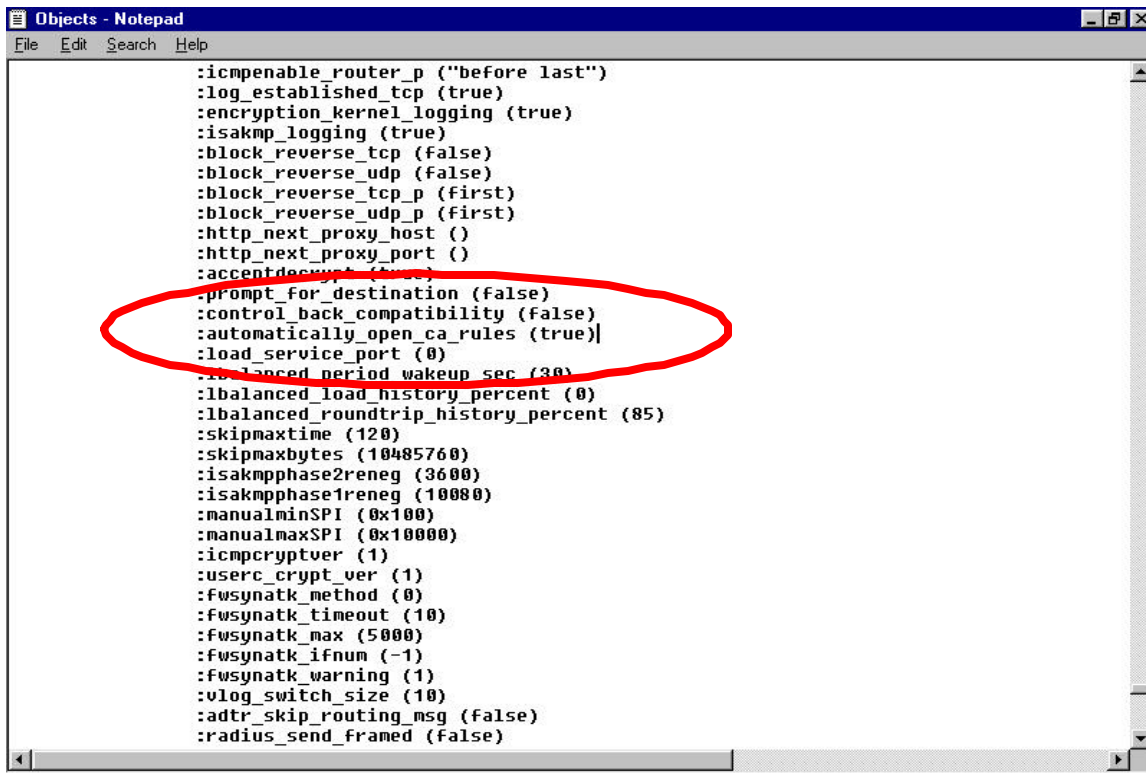
```
NT      cd \winnt\fw\bin          (change to the bin directory)
        fwstop                    (stop the firewall)

UNIX    cd /etc/fw/bin
        fwstop                    (stop the firewall)
```

The *objects.c* file will be found in the following directories, based on OS.

```
NT      \winnt\fw\conf\objects.c
UNIX    /etc/fw/conf/objects.C
```

In the *objects.c* file, change the 'automatically_open_ca_rules' parameter from (False), to (True). Seen here using Notepad as the editing tool.



```
Objects - Notepad
File Edit Search Help

:icmpeable_router_p ("before last")
:log_established_tcp (true)
:encryption_kernel_logging (true)
:isakmp_logging (true)
:block_reverse_tcp (false)
:block_reverse_udp (false)
:block_reverse_tcp_p (first)
:block_reverse_udp_p (first)
:http_next_proxy_host ()
:http_next_proxy_port ()
:accentdecrypt (true)
:prompt_for_destination (false)
:control_back_compatibility (false)
:automatically_open_ca_rules (true)
:load_service_port (0)
:balanced_period_wakeup_sec (30)
:balanced_load_history_percent (0)
:balanced_roundtrip_history_percent (85)
:skipmaxtime (120)
:skipmaxbytes (10485760)
:isakmphase2reneg (3600)
:isakmphase1reneg (10000)
:manualminSPI (0x100)
:manualmaxSPI (0x10000)
:icmptcryptver (1)
:userc_crypt_ver (1)
:fwsynatk_method (0)
:fwsynatk_timeout (10)
:fwsynatk_max (5000)
:fwsynatk_ifnum (-1)
:fwsynatk_warning (1)
:vlog_switch_size (10)
:adtr_skip_routing_msg (false)
:radius_send_framed (false)
```

Fig-3

Once this is done, restart the FW-1 process using the fwstart command.

This can be done as follows;

```
NT      cd \winnt\fw\bin          (change to the bin directory)
        fwstart                    (starts the firewall)

UNIX    cd /etc/fw/bin
        fwstart                    (starts the firewall)
```

With the Firewall running the above Rule Base, start your internet browser and enter the destination of the server_WWW. In our example this is IP address 10.10.10.2.

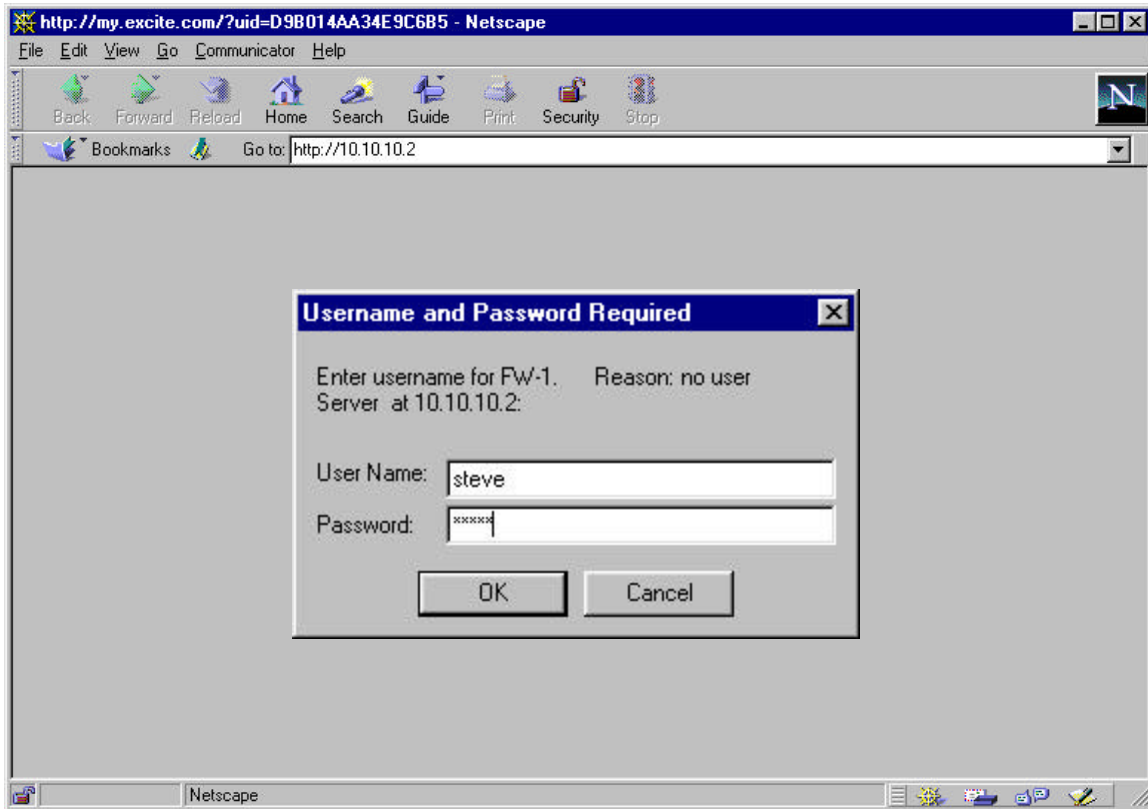


Fig-4

As you can see, the user is prompted to enter his/her Firewall-1 username and password. The Rule that prompts the user to authenticate is the User Authentication rule, rule number 1.

Once an individual authenticates with his or her username and password, an entry in the log file is created. The entry will contain the following; a service of “Std Sign On”, and an action of “authorize”.

Translating the log entries is as follows;

- A) Record 0 is the installation of the rule base.
- B) Record 1 is the authorization of the username and password
- C) Record 2 is the acceptance of the http traffic based on User Authentication in Rule 1
- D) Record 3 is the acceptance of the connection based on Implicit Client Authentication

In our example the initial rule that grants access to the client will be the Client Authentication rule, rule number 2. We determine this by reviewing the log entries. The **Info.** area of the Log Viewer for record #3 is the area of note. Note that the Log Viewer indicates that access was granted to the user *steve* based on “previous authentication”. This comment indicates to the administrator that Implicit Client Authentication is indeed working.

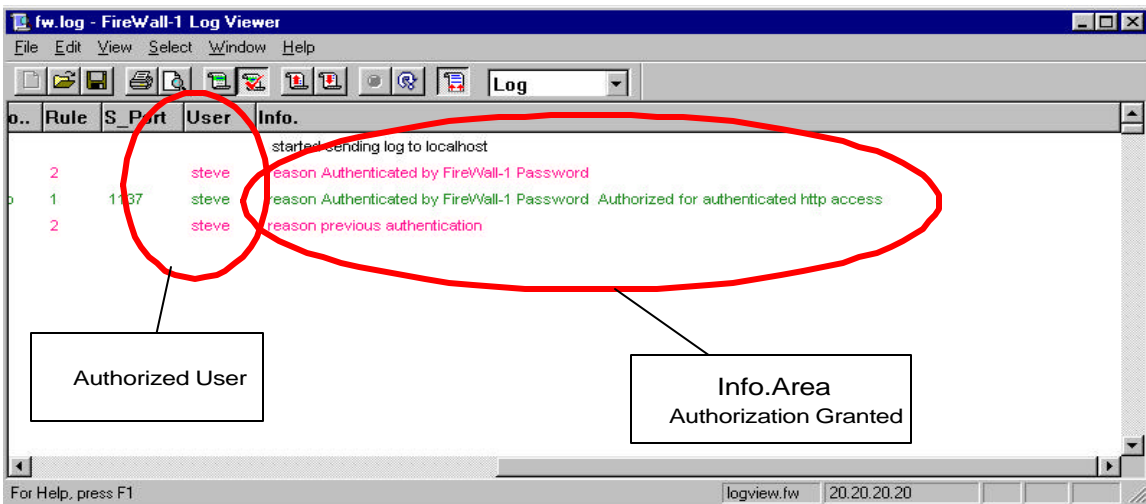
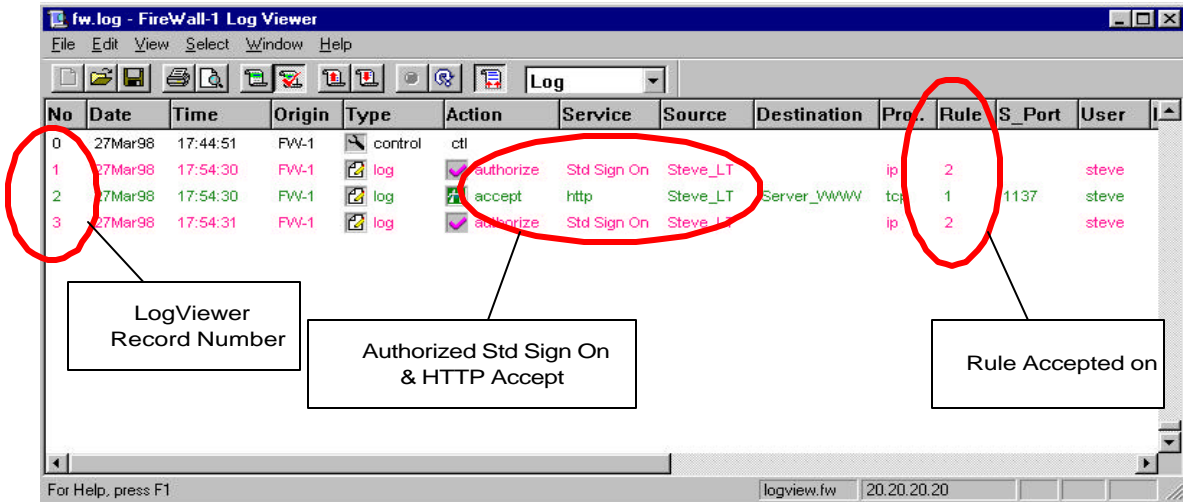


Fig-5

The page displayed by the test Web Server at IP address 10.10.10.2 using http is a personal WEB Server default page.

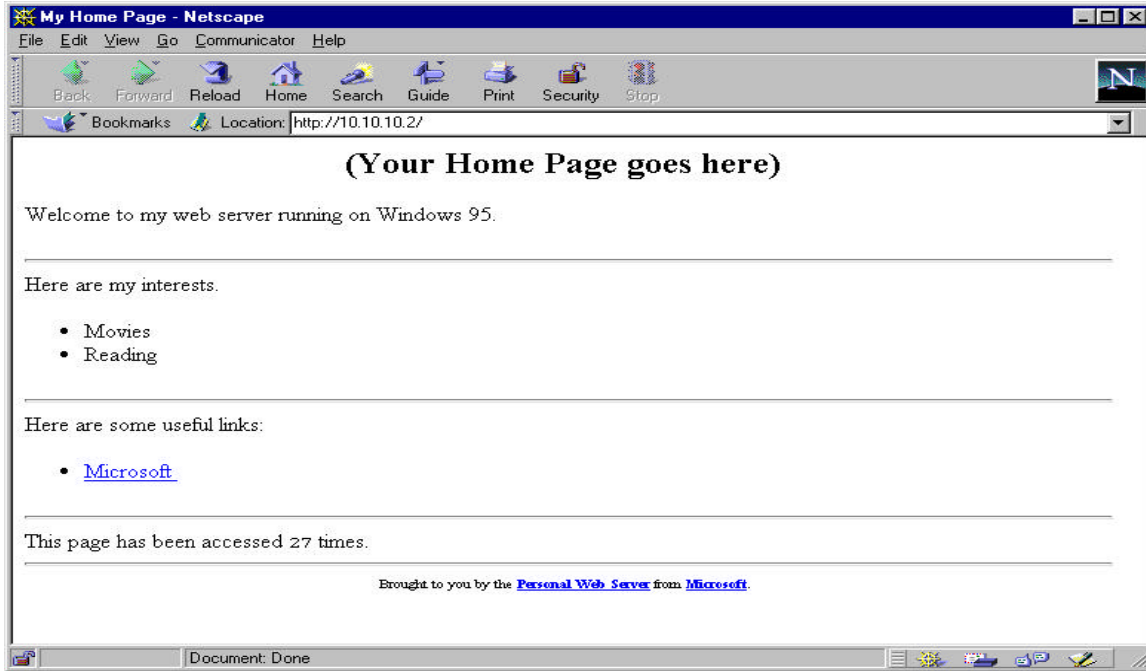


Fig-6

Lets now request the same page using the https service. This will now allow the session to be inspected using Stateful Inspection™.

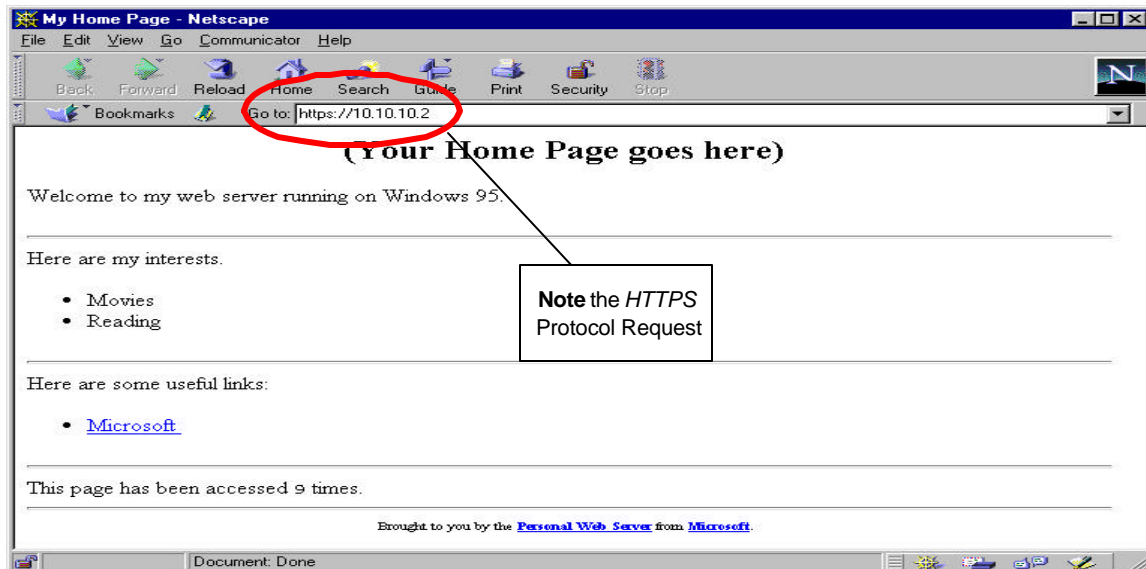


Fig-7

Here the Log Viewer displays the https traffic being accepted based on rule number 2.

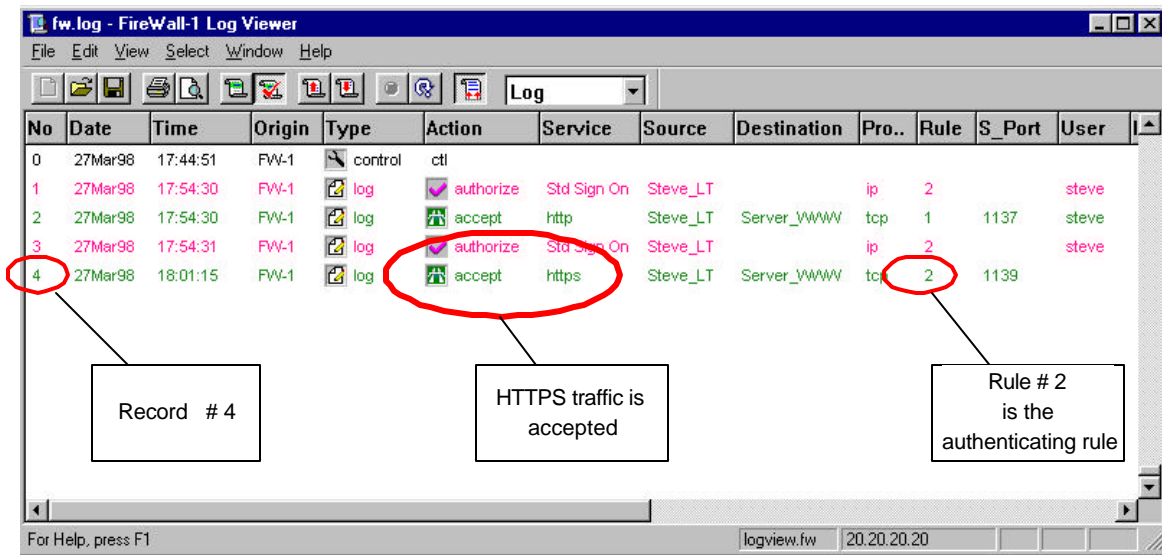


Fig-8

Please consult the FireWall-1™ documentation for more detailed information regarding the options and features of Check Point FireWall-1™.

Troubleshooting Tips:

- 1) As with any FireWall-1™ installation, be sure that the IP routing structure is correct before adding additional rules to the Rule Base.
 - Allow for only one default gateway on the firewall system
 - Make sure the firewall operating system is forwarding IP packets
 - Make sure the Client PC and the destination server have the correct default gateway
- 2) To enable Implicit Client Authentication the rules should be defined in the following order:
 - User or Session Authentication rules for the allowed service (*http*)
 - Client Authentication rules (*https*)
- 3) If you are not being prompted for a username/password combination;
 - Clear your browsers cache
 - Close the browser
 - Open the browser and reconnect to the intended server
- 4) Make sure the defined user is a member of the group defined as “Source” (valid_users@any)
- 5) Reset the password for the defined user (*steve*)
- 6) Double check the IP address assigned to the destination server (*Server_WWW*)
- 7) If you pass the authentication process once, and get prompted to re-authenticate after visiting several different sites, try the following;
 - Check the Sessions Allowed parameter in the properties of Client Authentication
 - Check the Authorization Timeout parameter in the properties of Client Authentication