

KEREVAL

4 rue Hélène Boucher

Z.A Bellevue

35 235 THORIGNE FOUILLARD - FRANCE

Tél. : +33 (0) 223 203 664

RCS : B 442 789 210

APE : 722 C

***KEREVAL HEALTHLAB - Project IHE EUROPE*****User Guide*****Proxy – V3.x***

Version : 1.02

Date: 03/09/2014

Author: Thomas DOLOUE

Function: Quality Assistant

Reference:

KER3-MAN-HEALTHLAB-PROXY_USER-1.02

Status: approved



■ KEREVAL Approval

Name	Function	Date	Visa
Eric POISEAU	Lab Manager	03/09/2014	OK

■ Diffusion

Internal	Recipient	Date	Exemplary
KEREVAL	HealthLab	03/09/2014	Electronic version

External	Recipient	Date	Exemplary
Proxy users		03/09/2014	Electronic version

■ Document history

Version	Date	Author	Modifications
V0.01	02/09/2014	Thomas DOLOUE	Creation
V1.01	03/09/2014	Thomas DOLOUE	For review
V1.02	03/09/2014	Eric POISEAU	Approve

■ Table of content

1	GAZELLE PROXY - OVERVIEW	4
1.1	Project Overview	4
1.2	Usage	4
1.3	Channel List.....	4
1.4	New channel	4
1.5	Messages list.....	4
1.6	TLS channels.....	5
1.6.1	Gazelle integration.....	5
2	PROXY - USER GUIDE.....	7
2.1	Introduction	7
2.1.1	Limitations	8
2.2	How does it work ?.....	8
2.3	Automated filtering	8
2.4	Finding captured messages manually	9
2.5	WebService API.....	9

1 Gazelle Proxy - Overview

1.1 Project Overview

The proxy is used to capture TCP/IP packets exchanged by test participants. The packed flow is analyzed and stored in a database for further analysis by protocol specific analysers.

The packet analyser availables are :

- HTTP
- DICOM
- HL7V2
- Syslog
- Raw

Each message is saved with the network details, including an id of the socket (named channel id) used for that message as a socket can transport many messages (HTTP, DICOM).

The proxy is set up on ovh1.ihe-europe.net, and accessed with [the web interface](#). ovh1.ihe-europe.net has a limited range of port numbers available from the Internet. Ports from 10200 to 11000 must be used for channel creation.

1.2 Usage

The web interface allows to create channels. A channel opens a port on the server hosting the proxy and redirecting all traffic to a configured server on a specific port.

Data stream is not modified, but analyzed using the chosen packet analyser.

1.3 Channel List

This page displays the list of current running channels. A channel can be deleted if password is known.

1.4 New channel

It allows to create a new channel if password is known. All fields are required.

1.5 Messages list

A grid displays all messages matching provided filter. Reset button sets all fields to default value.

Each row allows to display message details if id is clicked. Network details can also be clicked to define filter values.

For HTTP(S) messages, matching request/response is displayed in parenthesis.

Filter panel is collapsable, to provide more space for grid.

1.6 TLS channels

The proxy allows to capture HTTP messages sent over a TLS channel. **However, as we are not yet able to decode encrypted frames** (like in a man in the middle attack), the proxy acts as a TLS server and a TLS client. Decoding of the frame is planned for a future release.

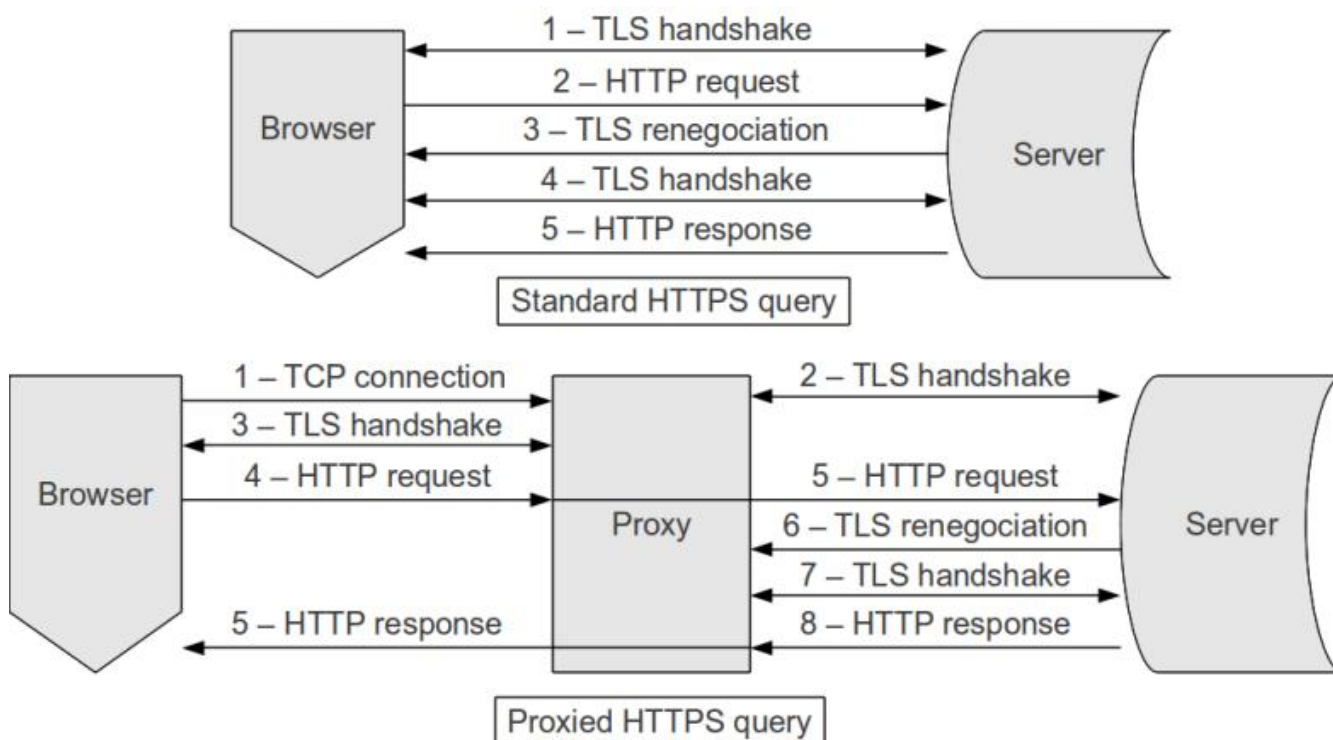
If the proxy has to be used transparently, clients and servers should not check for the mapping between the ip and the certificate (server : DN = TCP qualified name, client : validation of certificate based on IP).

When a TLS channel is created, a PKCS12 (.p12) file **MUST** be provided for the TLS server socket. The p12 should contain a private key and certificates. The .p12 **MUST** be protected by a password, provided in the matching form input.

The server p12 should mimic the real server certificates, as clients could validate the TLS channel against a truststore.

Also, the proxy supports TLS authentication. When a client connects to the proxy, it first connects to the real server without using any certificate. When the TLS channel is open, data from client is forwarded to the server. The server then can ask a renegotiation to the proxy for authentication. The key used is then the p12 provided for client.

At the moment, if the proxy failed to authenticate on server, the source connection is closed without the source error transmitted.



1.6.1 Gazelle integration

The proxy is integrated with Gazelle using web standards.

It publishes a web service allowing Gazelle to send test instance steps and configurations. Also, when a step is done, Gazelle calls the web service.

The proxy then opens the needed channels and listen on specified ports (provided in the system configurations). It also records the test instance chronology for further searches.

In Gazelle, if the test instance has proxy enabled, a link is available on each step. This link opens the proxy with the Gazelle step technical id as a parameter. The proxy then builds a filter to get messages matching the step and displays the matching messages.

2 Proxy - User guide

2.1 Introduction

Gazelle TestManagement tools can be used in conjunction with a proxy for the capture of the messages exchanged between a test participants.

The proxy is able to capture :

- HL7v2 messages
- Dicom Transactions
- Webservices messages
- Syslog messages

The advantages of using the proxy when running a test are the followings :

- the Proxy is a neutral way to capture the exchanged messages.
- the Proxy displays the captured messages in a unified way for all the tests performed, simplifying the work of the monitors when examining the logs
- the Proxy provides permanent link to the captured messages that can be linked to test instance steps and avoid the cut and paste of logs in the chat window of the test instance. It then helps linking the logs to the test and enables all the participants to the test to see the entire set of messages exchanges between the test participants.
- the Proxy helps verifying the captured messages through a direct link to the EVS Client GUI.

The screenshot shows a web browser window titled "Gazelle Proxy - Mozilla Firefox". The address bar displays "gazelle.ihe.net/proxy/messages/hl7.seam?id=9918". The page content is titled "HL7 Message" and includes the following details:

- Permanent link : [Permanent link](#)
- ID : 9918
- Date Received : 4/11/2011
- Initiator IP : 131.114.254.185
- Initiator Port : 3078
- Proxy Port : 10640
- Responder IP : 131.114.254.191
- Responder Port : 26000
- Side :
- Message length : 799

Below these details are links for "Download file", "View inline", and "Validate using EVSClient". The main content area displays an HL7v2 message in MSH format:

```
MSH|^~\&|OP_DEDALUS|DEDALUS^1.3.6.1.4.1.21367.2011.2.2.369|GLINTT|HS|20110411170209||OMP^009^OMP_009|eecd99f7-b8b7-4af6-b5de-022c02ee463b|P|2.6
PID|||HWN-0000001^CAT2011^PI||DOE^JOHN||19680306|M|||V. BREDE 6^COSTA VOLPINO^L
PV1||I|Cardiology^CATEUR_WARDS&&L^Cardiology|||110500321^DEDALUS^VN
ORC|NW|1271021400||127102140|||20110411170040||07402^SMITH^ROBERT^Dr.^Cardiology|||07402^SMITH^ROBERT||Cardiology
TQ1|1|1^Tab&Tablets&99FCS|TID|0800-1600-2300||20110411170000
RXO|S0010^amoxicillin+clavulanate 875+125 mg^995CS|1000|mg^milligram^99UCS|Tab&Tablets^99FCS|^notes||G|||I05.1^Rheumatic mitral
RXR|PO|MOUTH
RXC|B|J01CR02^amoxicillin+clavulanate^ATC|1000|mg^milligram^ANS+
```

2.1.1 Limitations

- Proxy acts as a network relay between two SUTs. As a result, system configuration has to be modified. The TCP connection must be established on the proxy on the system configuration's proxy port instead of opening a connection to the responder SUT directly.

2.2 How does it work ?

For each system in Gazelle TestManagement tool there is a set of configuration parameters. For each port that an SUT needs to open, there is a mirror port number on the proxy.

All proxy ports must be opened by a Gazelle admin, each system configuration being mapped to a proxy port.

The proxy GUI can be access at the following URL : <http://gazelle.ihe.net/proxy>

2.3 Automated filtering

Proxy and Gazelle know each other, and each test step in Gazelle has a proxy link.

Step	Trans.	Message Type	Opt.	Sending Actor	Receiving Actor	Comments	Last changed	Last modifier	Status	Validation Status	Validation Status
10		NONE	R	INIT_GATEWAY (OTHER_IHE2TEST_Proxy2)	INIT_GATEWAY (OTHER_IHE2TEST_Proxy2)		Mar 2, 2012 4:12:35 PM	glondais			Proxy messages
Description: The Initiating and Responding GWs should be prepared to capture copies of the messages sent/received in this test. Copy them into the chat window.											
20	ITI-19	Authenticate Node	R	INIT_GATEWAY (OTHER_IHE2TEST_Proxy2)	RESP_GATEWAY (OTHER_IHE_MGR_PROXY_1)		Mar 2, 2012 4:12:35 PM	glondais			Proxy messages
Description: Begin TLS communication.											
30	ITI-33	XCPD Query	R	INIT_GATEWAY (OTHER_IHE2TEST_Proxy2)	RESP_GATEWAY (OTHER_IHE_MGR_PROXY_1)		Mar 2, 2012 4:12:35 PM	glondais			Proxy messages
Description: Query for the female patient XcpdPat (is whose Pat ID is NA5420). The parameters the Initiating GW uses for the query depend on whether the Init GW assumes a shared Identifier. See the Description section above.											
40		NONE	R	INIT_GATEWAY (OTHER_IHE2TEST_Proxy2)	INIT_GATEWAY (OTHER_IHE2TEST_Proxy2)		Mar 2, 2012 4:12:04 PM	glondais			
Description: Capture query/response in the chat window.											
50	ITI-35	XCPD Query	R	INIT_GATEWAY (OTHER_IHE2TEST_Proxy2)	RESP_GATEWAY (OTHER_IHE_MGR_PROXY_1)		Mar 2, 2012 4:12:04 PM	glondais			

This link displays the list of the messages matching the test step configuration. It also filters the messages by time, showing only messages sent after the last test step marked as verified (or test instance started) and this test step marked as to be verified.

Id	Date	From	To	Proxy	Connection Id	Type	Info
139	3/2/12 5:13:23 PM	127.0.0.1:55202	192.168.20.168:80	20107	7545192	🔴	text/html
138 (137)	3/2/12 5:13:23 PM	127.0.0.1:55202	192.168.20.168:80	20107	7545192	🔴	text/html
137 (138)	3/2/12 5:13:22 PM	127.0.0.1:55202	192.168.20.168:80	20107	7545192	🟢	
140	3/2/12 5:13:23 PM	127.0.0.1:55202	192.168.20.168:80	20107	7545192	🟢	

2.4 Finding captured messages manually

By accessing proxy directly using <http://gazelle.ihe.net/proxy>, messages can be filtered on different criterias. By clicking a value in the table, it either opens the message details for id column, or set the filter for other columns.

The messages list displays only one type of message, if HTTP is selected, HL7v2 messages are not shown.

Each captured message has a permanent link that can be used in Gazelle. The best way to use it is to add this link to a test step instance. The monitor will be then able to validate the message using EVSClient.

2.5 Webservice API

- **startAllChannels** : It takes "List<Configuration> configurations" in argument. It start a new channel in proxy for each configuration set.
- **startTestInstance** : It takes "TestInstance testInstance" in argument. It start a new channel in proxy for a test instance.

- *markTestStep* : It takes "int testStepId" in argument. It set the date of a test step with the current.
- *getMinProxyPort* : It return the min_proxy_port define in proxy configuration.
- *getMaxProxyPort* : It return the max_proxy_port define in proxy configuration.