

SSL User Authentication with the HTTP Security Server

Authored By: Lewis Colascione/Udi Ben-Reuven
Date: April 2000
Purpose: To describe and document how to configure SSL User Authentication
Credits:
Version: 1.1

Procedure for SSL User Authentication Using Check Point FireWall-1 v4.1 & Verisign Free-Trial:

This procedure will allow you to connect to the Firewall using an SSL compliant browser and establish an authenticated VPN from an Internet Browser to the Firewall for Remote Access. The FireWall will be using a certificate issued by Verisign "Free-Trial".

This Document assumes that you have a User Group and ID established for Authentication.

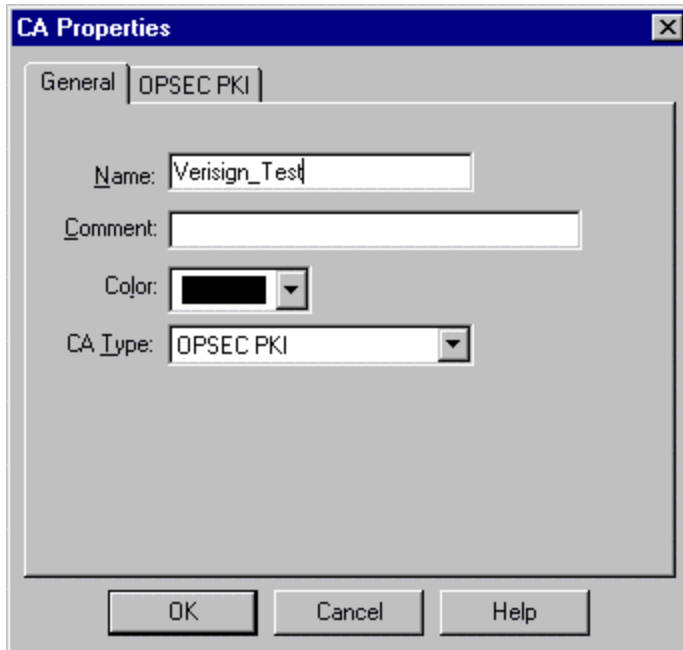
First You need to generate a Certificate for the FW-1 HTTP Security Server to perform the SSL Communication. In order to generate it from Verisign do the following.

Download Verisign Test CA Root:

Go to <http://www.verisign.com/server/trial/welcome/caroot.html>

And press the "Accept" on the bottom. You will be asked to OPEN or SAVE getcacert. Disregard the instruction to open this file and instead save it as "getcacert.crt". Check that you have the ".crt" extension at the end of the file name.

Next go to the Fw's Policy Editor. Go to the "Manage Servers" dialog box and create a New CA object. Assign an arbitrary name for this object (e.g. Verisign_Test) and select the CA Type to be OPSEC PKI:

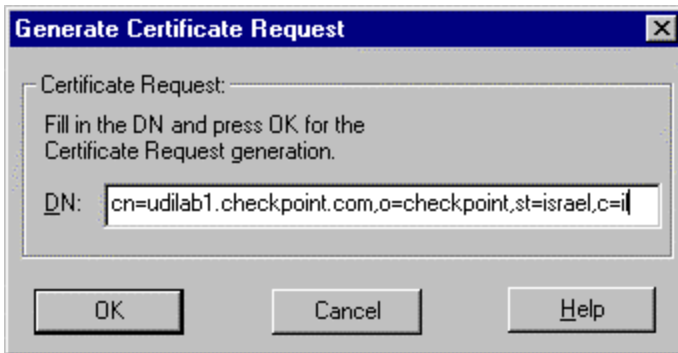


In the "OPSEC PKI" tab remove the check from "HTTP Server(s)" (disregard the warning message) and press the "Get" button. Pick the file getcacert.crt from the previous step.

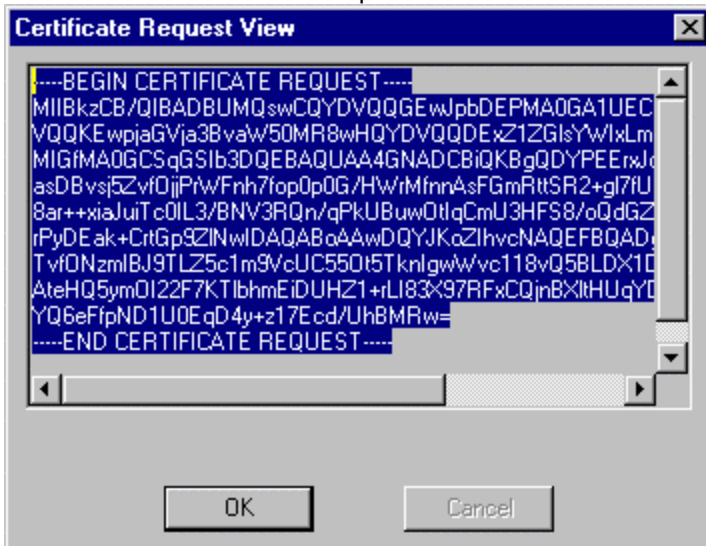
Next you will need to issue a certificate request for the FW-1 module running the SSL proxy. Go to the FW's object definition and select the "Certificates" tab. Press the "Add" button.



Enter an arbitrary nick-name (for example “fwsslcert”.) Select the “CA Server” to be the CA object you defined in the previous step (“Verisign_Test”.) And press the “Generate” button. Enter the following DN “cn=<full DNS name of your firewall>, o=<org name>, st=<unabridged state name>, c=<country>”
 For example:



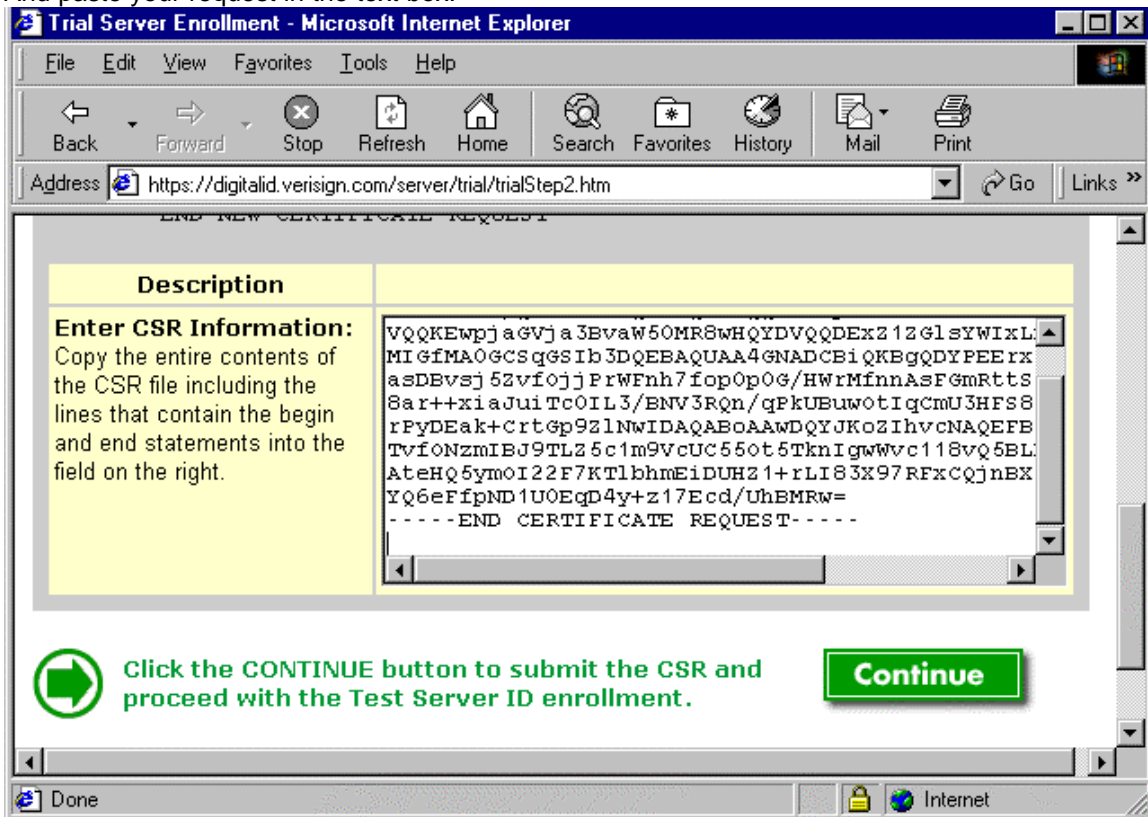
Another example:
 cn=farmboy.us.checkpoint.com,o=checkpoint,st=california,c=us
 Press the OK button and then press the “View” button:



Copy the Certificate Request to clipboard (mark it and press Ctrl-C) and press OK.

Sign your Certificate Request at Verisign. Go to <https://digitalid.verisign.com/server/trial/trialStep2.htm>

And paste your request in the text box:



Press on "Continue". Fill your customers details in the next page. It is very important to enter the correct email at the bottom of the page. Press the "Accept" button at the bottom.

The signed certificate will be sent to the email address you have entered in the previous step. Save it as a file with ".cert" extension (for example "fwsslcert.cert"). Now go back to the "Certificate Properties" window and press the Get button and select the file you have just stored. Press on OK. You now have a valid certificate.

Next you will need to edit two setup files to define the mode of the HTTP Security Server.

Stop the firewall.

Edit the \$FWDIR/conf/fwauthd.conf file.

Look for the following line;

"80 in.ahhttp wait 0"

Append the line with one of the following options:

- ec** – If you require SSL from Browser Client to Firewall.
- es** – If you require SSL from Firewall to Internal WWW Server.
- eb** – If you require Both.

To the right of the option append a column ':' and the nick-name of the certificate you want to use with the SSL.

Example For SSL from Browser to Firewall Only:

```
80 in.ahhttpd wait 0 ec:fwsslcert
```

Next we must configure the Security Server to utilize the Pre Defined Servers option of the Security Server. For the remote client to SSL to the Firewall, Authenticate, then access a Web Enabled server behind the Firewall you must Pre Define the Internal Servers in the Policy Properties Section of the HTTP Security Server.

Edit \$FWDIR/conf/object.C.

Look for the following line;

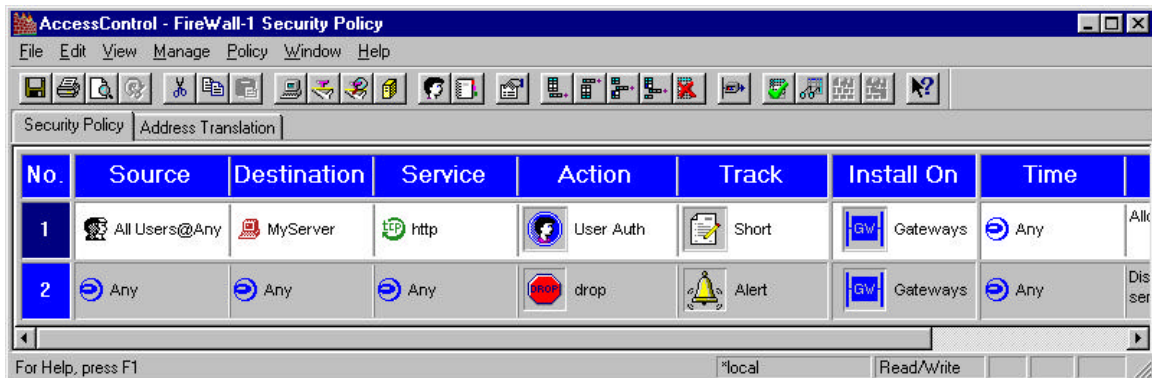
```
prompt_for_destination (false)
```

Set the attribute to **true**.

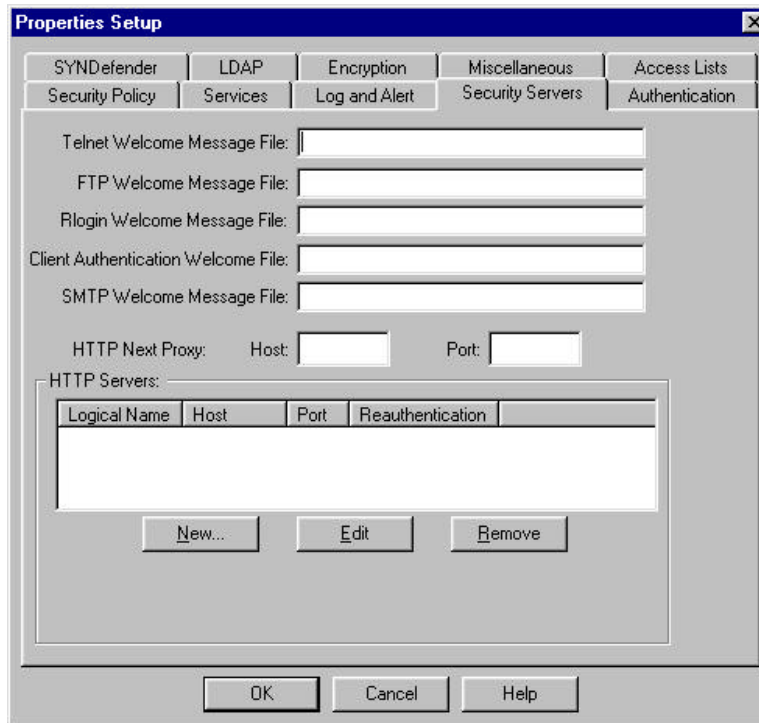
Example: **prompt_for_destination (true)**

Start the firewall.

Be sure to create a User Authentication Rule for HTTP to the Client Server.

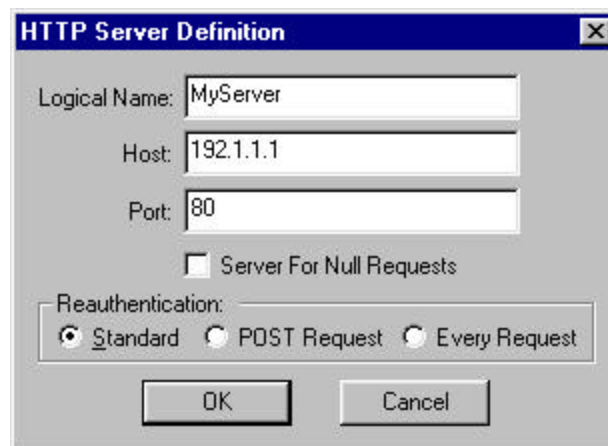


Open the Policy Editor and goto Policy -> Properties -> SecurityServers.



Define the internal Web Enabled servers in the **HTTP Servers** dialog box;

Click on **New**. Enter the information for each internal Web Enabled server you wish the SSL client to access. You must define a unique logical name for each server. Example: **MyServer**



Install your Security Policy: **Policy -> Install**

With your Netscape Browser from the Outside of the Firewall you will attempt to access the Logical Server you defined behind the firewall with the following URL Format;

<https://natasha:80/MyServer>

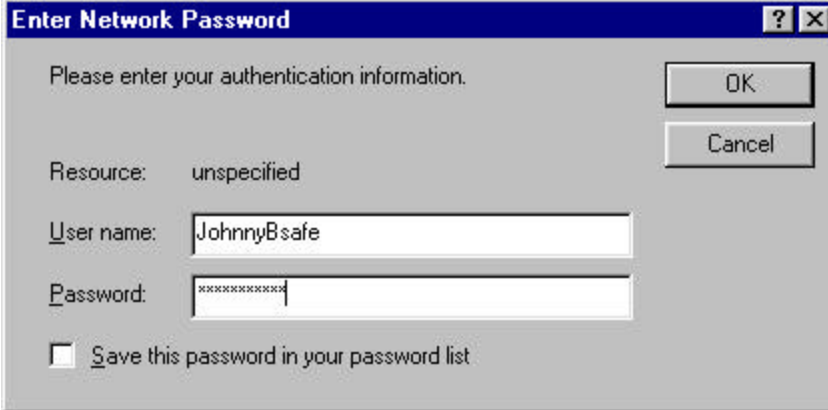
natasha = firewall at port 80 (The Security Server is running on port 80 for SSL)

MyServer = Pre Defined Server for HTTP behind the Firewall.

You must first establish the SSL connection to the Firewall on port 80 (Not 443) then tell the Firewall where you are going once you authenticate in the URL.

NOTE: On the first connection attempt the Netscape browser will challenge you to accept a Non – Standard Certificate to establish the SSL VPN. Once you accept this Certificate for All Sessions this will not challenge you again.

Next you will be challenged by Check Point User Authentication in your browser;



Enter Network Password

Please enter your authentication information.

Resource: unspecified

User name: JohnnyBsafe

Password: *****

Save this password in your password list

OK

Cancel

Once authenticated you are in using 40 Bit SSL to encrypt from Client to Firewall.