

Procedure for SSL User Authentication Using A Netscape Browser Client and Check Point Firewall-1 v4.0:

This procedure will allow you to connect to the Firewall using a Netscape SSL compliant browser and establish an authenticated VPN from an Internet Browser to the Firewall for Remote Access.

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. Currently this is a Firewall-1 generic certificate scheme for the SSL Server.

On the Management Server type the following;

```
fw ca genkey "ou=<machine name>, o=<org name>, c=<country>"
```

<machine name> is the name of the FW-1 management machine name . Example: **natasha**.

<org name> is your organization name . Example **Checkpoint**.

<country> is your country. Example **il**

So this command line should look like this:

```
fw ca genkey "ou=natasha, o=checkpoint, c=il"
```

This command will generate a Certificate for the management Certificate Authority.

Next you must install the Certificate on the Management Server.

```
fw ca putkey <machine name>
```

<machine name> is your management machine name.

So this command line should look like this:

```
fw ca putkey natasha
```

This command will ask you to enter a secret key. You can use simple key like **aaaa**.

Next you must certify the relationship between the Management Server and Firewall Module for the Certificate Authority.

```
fw certify ssl <management name> <machine name>
```

<management name> is the management machine name. Example **natasha**.

<machine name> is the firewall machine name. Example **natasha**.

So this command line should look like this:

```
fw certify ssl natasha natasha
```

This command will ask you to enter a key. You can use simple key like **aaaa**.

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.ahhttpd 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.

Example For SSL from Browser to Firewall Only:

80 in.ahhttpd wait 0 ec

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;

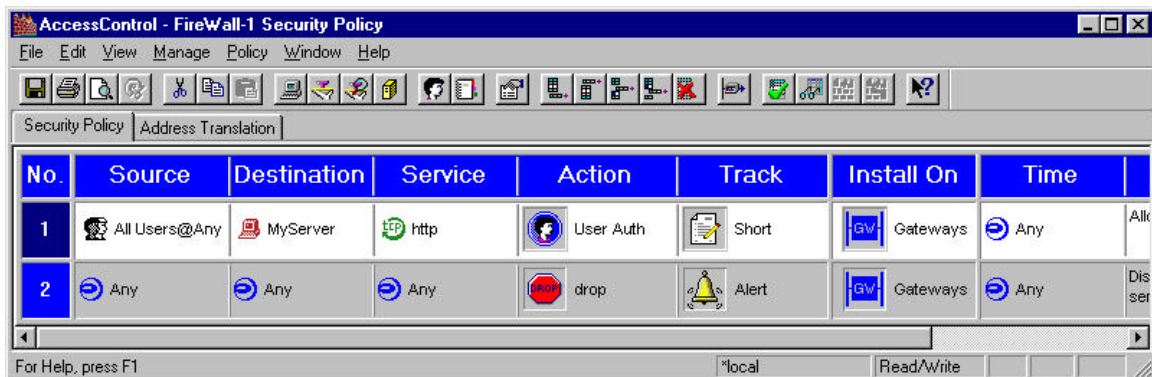
prompt_for_destination (false)

Set the attribute to **true**.

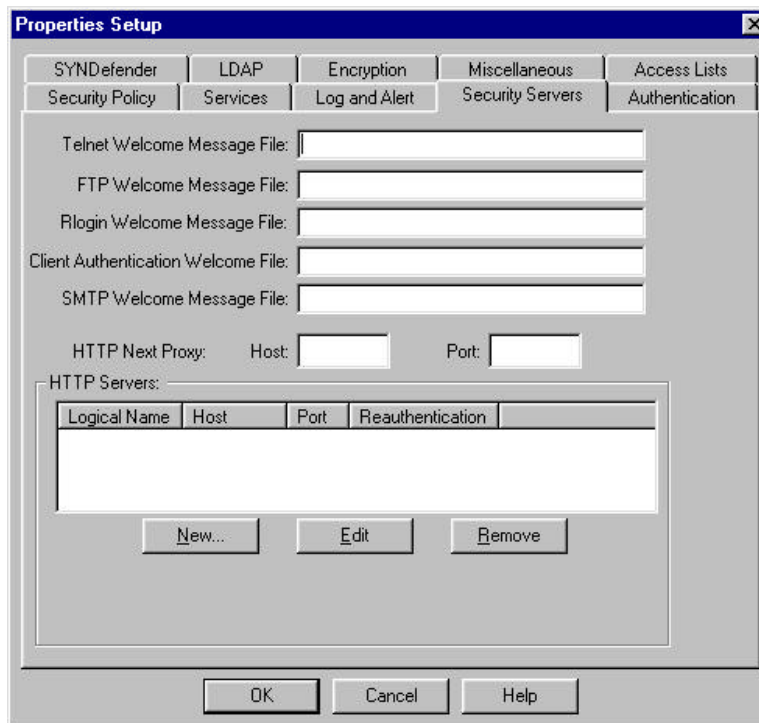
Example: ***prompt_for_destination (true)***

Start the firewall.

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

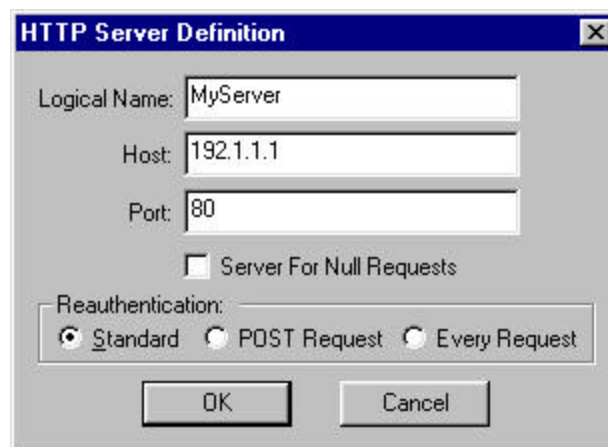


Open the Policy Editor and goto Policy -> Properties -> SecurityServers.



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>

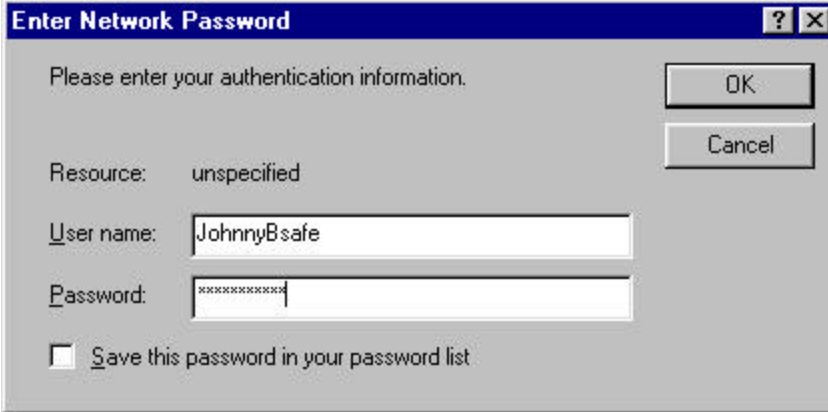
natasha = firewall at port 80 (The Security Server is running on port 80 for SSL)

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: xxxxxxxxxxxx

Save this password in your password list

OK

Cancel

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