CLEARSWIFT

SECURE Web Gateway

HTTPS/SSL Technical FAQ

Version 1.1

Date 04/10/12

Introduction

This Technical FAQ explains the operation of the HTTPS/SSL scanning and how it is deployed.

How does the SECURE Web Gateway inspect encrypted HTTPS traffic?

When a user's browser requests a connection to an HTTPS site the Web Gateway will automatically create and sign an HTTPS web server certificate for the site being requested. This process of automatic certificate creation occurs for each new HTTPS website requested.

The sequence of events:

1. The user requests an HTTPS URL via their browser i.e. https://www.clearswift.com.
2. The Web Gateway automatically creates and signs an HTTPS web server certificate for the site being requested and returns the certificate to the browser.

   Note: Users browsers must be configured to trust the website certificates created and signed by the Web Gateway - as a trusted certificate authority. Failure to import the web gateway root signing certificate into the users' browser certificate store (see next section below) will cause the user's browser to display a certificate warning, because certificates signed by the Web Gateway will not be trusted.

3. The encrypted session is then established between the browser and the Web Gateway using the details provided by the certificate provided from the Web Gateway.
4. The Web Gateway also connects to the remote web server requested (https://www.clearswift.com) and inspects that server's certificate to ensure it is valid and can be trusted
5. If the certificate is valid then an encrypted session is established between the Web Gateway and the remote server.
6. The data that passes between a user's browser and the Web Gateway is encrypted.
7. The data that passes between the Web Gateway and the remote web server is encrypted.
8. The data passing within the Web Gateway's own analysis engine is not encrypted, and according to policy may be content checked against an acceptable use policy (AUP) as well as being automatically scanned for web malware.

Importing the Clearswift Web Gateway MIMEsweeper root CA into users' browsers

As detailed above it is essential that the users' browsers trust the certificates signed by the Web Gateway. To enable the browser to trust the Web Gateway's certificate authority (CA) you will need to export the Web Gateway root CA certificate and import it into each user's browser certificate store. After first exporting the root certificate from the Web Gateway (see below) it is then imported into Internet Explorer and Firefox via the browser's certificate import option as follows:

> *Internet Explorer:* Tools > Internet Options > Content tab > Certificates > Trusted Root Certification Authorities > Import

Firefox: Tools > Option > Advanced > Encryption tab > View Certificates > Authorities > Import and select to trust this certificate to identify web sites.

The certificate will appear in the browser certificate store and will be shown under the name MIMEsweeper Web Gateway Root CA as shown below.

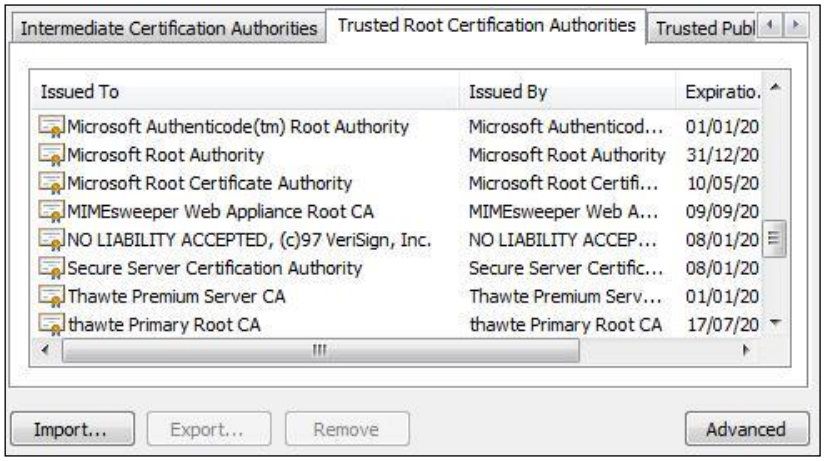

***Fig 1**: Imported SECURE Web Gateway Root CA certificate as seen in Internet Explorer*

***Note**:* Active Directory Group Policy may be used to import the certificates into all users' browsers.

Exporting the root certificate from the SECURE Web Gateway

The Root CA certificate is exported from the following location:

System Center > Proxy Settings > Proxy Mode & Listening Port > Download HTTPS Certificate.

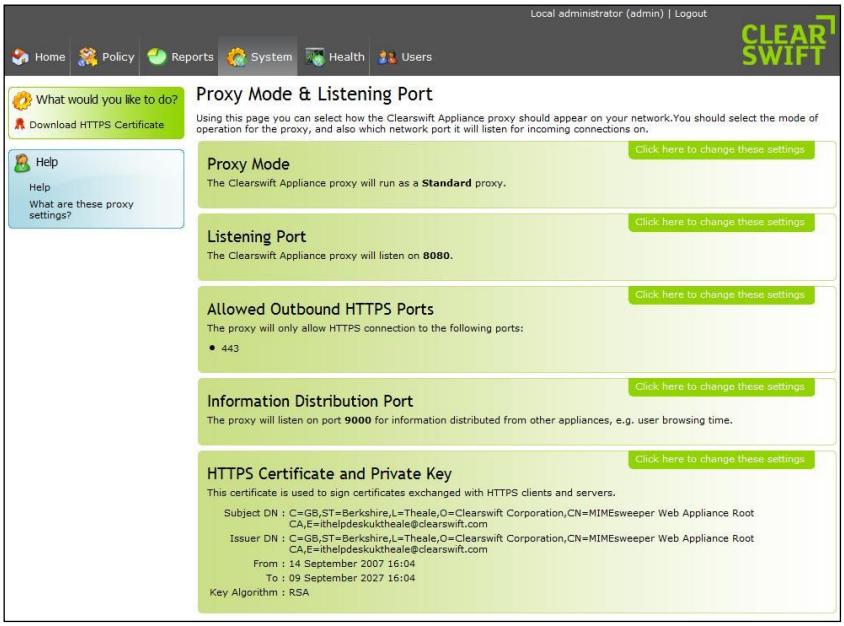

***Figure 2**: Downloading the HTTPS certificate*

The certificate exported from the location above must then be imported into all your users' browsers as described above, and before the HTTPS decryption option is enabled.

Enabling the HTTPS decryption option

The HTTPS decryption option is enabled in the following location:

Policy Center > Global Web Policy > HTTPS Content Scanning.

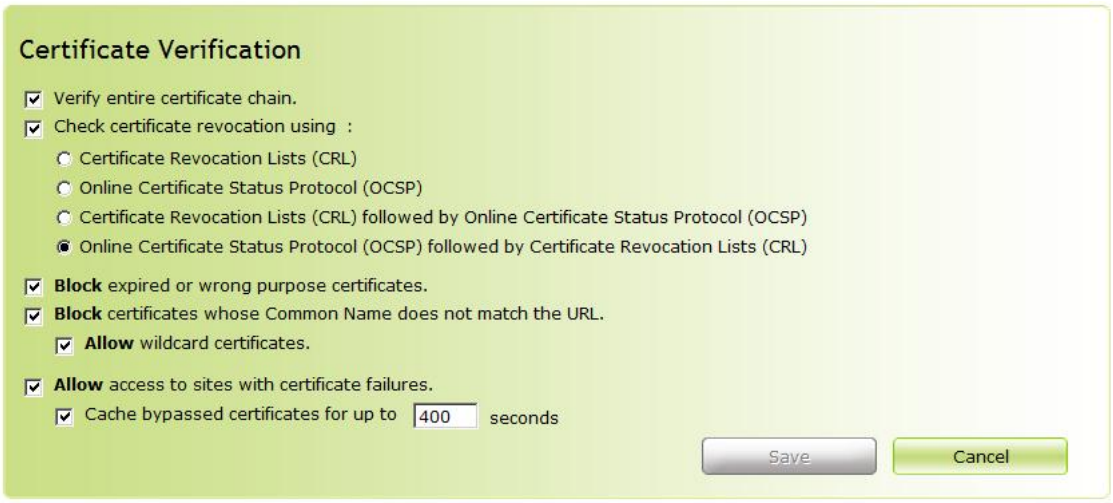

***Figure 3**: Enabling HTTP decryption*

When enabling the decryption option you are also able to stop users' from accessing sites with certificate failures, or by selecting the 'Allow access to sites with certificate failures' as shown above, users' will be warned of the certificate failure reason but still permitted to 'Visit Site Anyway' as shown in Figure 4 below.

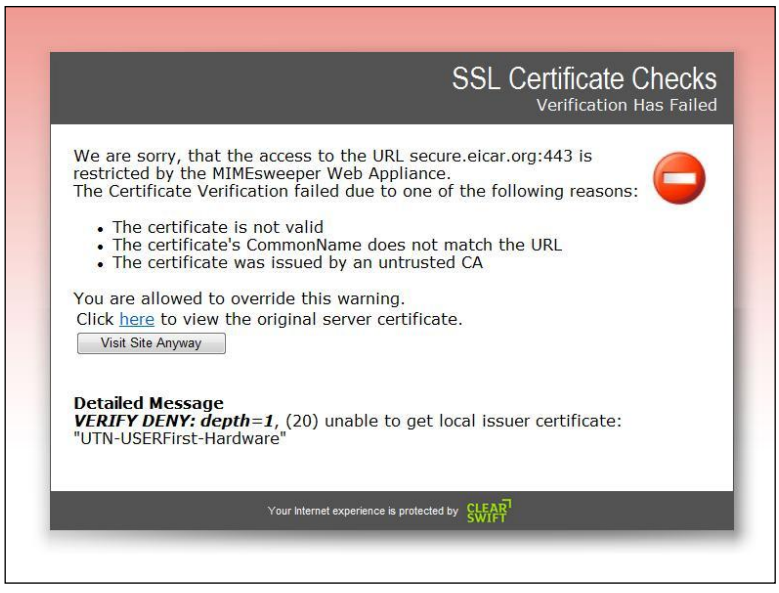

***Figure 4**: User certificate failure notification & override page.*

Creating your own signing certificate and importing it into the Web Gateway

1. Create a folder where certificates will be created, e.g. mkdir /root/certs
2. Change to that folder, e.g. cd /root/certs
3. Copy one files:

cp /etc/ssl/misc/CA.sh .

cp /etc/ssl/openssl.cnf .

4. Edit the openssl.cnf file to set the number of DAYS higher than the default 365 to increase the time the certificate remains valid. E.g. vi openssl.cnf. Look for default_days and set this higher, e.g. 3650
5. Run ./CA.sh –newca
6. Hit enter for default file name
7. Enter the passphrase and confirm it
8. Enter all of the details asked which are required to create your certificate. It is very important that all these are set otherwise the Web Gateway GUI may accept the certificate when imported but it may fail to work. What you are about to enter is called a Distinguished Name or a DN

   Country Name (2 Letter code) [GB]

   State or Province Name (Full name) [Berkshire]

   Locality Name (e.g., City) [Theale]

   Cd demoCAOrganization Name (e.g., Company) [Clearswift Limited]

   Organizational Unit Name (e.g., Section) [IT Support]

   Common Name (e.g., YOUR name) [webgateway3.ocean.tld]

   Email Address e.g., [admin@gateway3.ocean.tld]

9. This will create a folder called demoCA. Change to this folder, e.g. cd demoCA
10. In this folder will be found the root CA certificate called 'cacert.pem' and in the private folder will be the key which is called 'cakey.pem'. FTP both these files off the system
11. Edit the cacert.pem file and remove all the top text until -----BEGIN CERTIFICATE-----

These two files may then be imported into the Web Gateway GUI and the certificate may also be used in users' browsers so that they trust it.

System Center > Proxy Settings > Proxy Mode & Listening Port > HTTPS Certificate and Private Key.

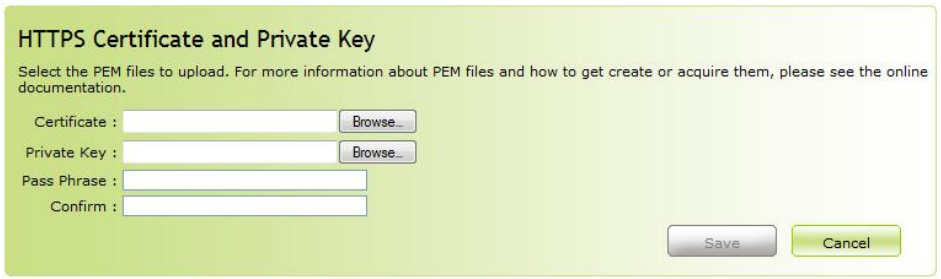

***Figure 5**: Importing your own certificate*

Notes:

1. This certificate will need to be imported into the browser so that it is trusted
2. When importing the certificate the file filter must be set to '*' see the file with Internet Explorer
3. When importing the certificate into the Web Gateway the following log can be checked to see if any errors occurred: /tmp/.csmds.log.

To view this just: cat /tmp/.csmds.log

- END -