Using SSL/TLS termination at F5 Load Balancer

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT™ version 7 and later

QUESTION

How can I use SSL/TLS termination at F5 Load Balancer?

ANSWER

For the Load Balancer to be used as a termination point for SSL, the following needs to be implemented. This procedure allows the Load Balancer to be in charge of the encryption for an SSL connection instead of EFT. This allows for the customer to have multiple SSL applications use a central repository for certificates. EFT will just make an HTTP connection to the DMZ and the DMZ will make an HTTP connection to the Load Balancer. The Load Balancer will then make an HTTPS connection to the remote connecting party.

Overview of problem:

1. Client makes request to F5 as "HTTPS://<address>"
2. F5 acts as a reverse proxy and converts the HTTPS request to HTTP.
3. F5 sends this request to the DMZ Gateway as HTTP.
4. This request is shuttled through DMZ to EFT as HTTP.
5. Since a partial address was used, EFT responds with "302 Moved temporarily" and sends the full address of http://<ip address>/EFTClient/Account/Login.htm. It sends http because the connection to the Proxy>EFT was over HTTP, so it assumes http is the correct protocol to send in the response for the redirect.
6. Connection is sent back to F5 over HTTP.
7. F5 receives server response and attempts to reroute back to source/client.
8. Client receives the address http://<ip address>/EFTClient/Account/Login.htm and tries to connect to it. This is invalid. The F5 does not accept HTTP requests.

What needs to happen:

1. F5 receives server response and proxies the connection back to the X-Original-Protocol: HTTPS.
2. Client receives the address https://<ip address>/EFTClient/Account/Login.htm and

successfully connects.

Resolution:

1. Create a certificate to use on F5 for SSL offloading, if not already done.
2. Ensure that the HTTPS virtual server SSL Profile (Client) property is configured to use the certificate.
3. Change the default pool for the HTTPS virtual server to point to the HTTP pool.
4. Create an iRule (as shown below) to add the appropriate header and add it to the HTTPS virtual server.

Here is the iRule:

```
when HTTP_REQUEST {

HTTP::header insert "X-ORIGINAL-PROTOCOL" "https";

}
```

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11407/Using-SSLTLS-termination-at-...