# Redirect HTTP requests on a SSL vserver

## Use Case:

When a content or App is hosted on SSL vserver, it is expected that all clients would connect over SSL and if they do not the connection fails at TCP layer. While it is fine to expect clients to come with https, there can be cases where clients come using HTTP request and you want to avoid such requests getting terminated at TCP layer.

## F5 iRules:

```
when HTTP_REQUEST {


   # Check if the client used an SSL cipher

   if {not ([catch {SSL::cipher version} result]) && [string tolower $result]
ne "none"}{


      # Client did use a cipher

      log local0. "\$result: $result. Allowing encrypted request."


   } else {


      # Client did not use a cipher

      log local0. "\$result: $result. Redirecting unencrypted request."

      HTTP::redirect "https://usesslplease.example.com/"

   }

}
```

URL: https://devcentral.f5.com/codeshare/redirect-non-ssl-requests-on-ssl-virtual-server-rule

## NetScaler Solution:

```
add responder action redirect_https_act redirect
'"https://"+HTTP.REQ.HOSTNAME+HTTP.REQ.URL'
```

```
add responder policy redirect_https_pol CLIENT.SSL.IS_SSL
redirect_https_act
```

Bind the responder policy to the http vserver which shares the same ip address of https vserver. In this case you will need to create a dummy http vserver with same IP so that the initial connection is successful and then do the redirect using responder policy.