Blocking Requests from Range of IP’s

Use case:

Most of the client requests come through a proxy and the original client IP is in the HTTP Headers and there is requirement to take specific actions based on the client ip which is present in the header.

F5 iRules

```
when HTTP_REQUEST {

set json "{ \"success\": false, \"errors\": { \"reason\": \"Access Forbidden\"} }"

if { [HTTP::header exists "x-client-ip"] }
       {
         set trueIP [HTTP::header "x-client-ip"]
          if {[class match $trueIP equals client_Allowed_List]}
          {
            pool TEST_POOL_8080
          }
         else {HTTP::respond 403 content $json "Content-Type" "application/json"}
     }
}
```

NetScaler Solution:

```
add responder action act1 respondwith q<"HTTP/1.1 403 Forbidden\r\nContent-Type:
application/json\r\nServer: netScaler\r\n\r\n{ \"success\": false, \"errors\": { \"reason\":
\"Access Forbidden\"} }\r\n\r\n">
add location 10.105.158.10 10.105.158.40 "customerloc.*.*.*.*.*"
add location 192.168.1.10 192.168.1.35 "customerloc.*.*.*.*.*"
add responder policy testip "HTTP.REQ.HEADER(\"x-client-
ip\").TYPECAST_IP_ADDRESS_T.MATCHES_LOCATION(\"customerloc.*.*.*.*.*\")" act1
```