Protection using Basic Authentication

Use Case:

While majority of sensitive backend information requires some sort of authentication and that could be setup at backend or load balancing setup. In most cases the authentication is setup with external source but this is complicated procedure. Hence at times you might just want to enable basic authentication on load balancing tier to do this job without involving external AAA entities.

F5 iRules:

```
`when HTTP_REQUEST {

if {not ([string tolower [HTTP::uri]] contains "somepage.jsp")} {

return

}

binary scan [ md5 [HTTP::password]] H* password

if { [class lookup "[HTTP::username]" authorized_users] equals $password } {

log local0. "User [HTTP::username] has been authorized to access virtual server [v
irtual

name]"


} else {

if { [string length [HTTP::password]] != 0 } {

log local0. "User [HTTP::username] has been denied access to virtual server [virtu
al name]"

}

HTTP::respond 401 WWW-Authenticate "Basic realm=\"Secured Area\""

}

}`
```

URL: https://devcentral.f5.com/questions/add-basic-authentication-for-specific-page

NetScaler Solution:

```
add policy stringmap authorized_users

bind policy stringmap authorized_users abc
```

```
1527E888767CDCE15D200B870B39CFD0
```

(“freebsd” used as password with MD5)

```
add policy expression md5_hash
"HTTP.REQ.HEADER(\"Authorization\").AFTER_STR(\"Basic\").B64DECODE"


add policy expression get_username
"HTTP.REQ.HEADER(\"Authorization\").AFTER_STR(\"Basic
\").B64DECODE.BEFORE_STR(\":\")"


add responder action action_auth respondwith "\"HTTP/1.1 401
Authorization Required\r\nWWW-Authenticate: Basic realm=\\\"Secured
Area\\\"\r\n\r\n\""


add responder policy policy_auth
"get_username.IS_STRINGMAP_KEY(\"authorized_users\") &&
md5_hash.AFTER_STR(\":\").DIGEST(MD5).BLOB_TO_HEX.STRIP_CHARS(\":\")
==
get_username.MAP_STRING(\"authorized_users\").DIGEST(MD5).BLOB_TO_HE
X.STRIP_CHARS(\":\")" action_auth
```

Bind Responder policy to specific VSERVER or to Global rewrite bind point on Request flow. Here we have defined expressions to fetch username and respective md5 hash from the incoming request. With the required data we are generating response from NetScaler to request for basic authentication.