Issuer Validation from Client Certificate

Use Case:

Client certificate based authentication is quite common use case in current secure infrastructure. Best aspect is that Client cert based authentication can be done transparently and end user does not need to worry about it every time. In this scenario, when Client certificate is received, the configuration checks for multiple fields and ensures that Issuer for this certificate is known.

F5 iRules:

```
when HTTP_REQUEST {
        set cert [SSL::cert 0]
        set appName "DirectAccess"

        log local0. "DirectAccess: Start"

        if { not ($cert eq "") } {
                set result [SSL::verify_result]
                set subject [X509::subject $cert]
                set issuer [X509::issuer $cert]
                set serial [X509::serial_number $cert]
                set notValidBefore [X509::not_valid_before $cert]
                set notValidAfter [X509::not_valid_after $cert]

                if {$result > 0} {
                        log local0. "DirectAccess: No valid certificate"
                        reject
                } else {
                        if { $issuer equals "CN=LAB-ISSUING-
CA,CN=LAB,CN=RICHARDHICKS,CN=NET" } {
                                log local0. "DirectAccess: Issuer OK. Access granted for
$subject"
                                pool DirectAccess
                        } else {
                                log local0. "DirectAccess: Issuer NOK. Access NOT
granted for $subject"
                                reject
                        }
                }
        } else {
                log local0. "DirectAccess: No certificate received from client."
                reject
        }
}
```

NetScaler Solution:

add responder policy check_issuer CLIENT.SSL.CLIENT_CERT.ISSUER.EQ("CN=LAB-ISSUING-CA,CN=LAB,CN=RICHARDHICKS,CN=NET").NOT RESET

NetScaler has the most innovative advance policy infrastructure where such tasks can be achieved by single policy using advance expression which checks for the Issuer field. This is based on the assumption that received certificate is a valid client certificate.