SSL Client認証の証明書情報をサーバに渡すiRule

ichiro, 2010-28-02

はじめに:
近年ますます厳しくなるセキュリティ監査に対する取組みとして、2ファクター認証が検討されるケースがあります。
WEBアプリケーションにおいて2ファクター認証を実装する場合、SSLの証明書によるクライアント認証の仕組みを利用した以下のような2段階の認証を行うソリューションが考えられます。
PCにクライアント証明書がインストールされていることで機器を認証
アプリケーションでユーザーネームおよびパスワードを入力をさせることでユーザを認証
通常のSSLオフロード構成では、BIG-IPがクライアントのSSLセッションを終端するので、バックエンドのサーバはどのような証明書が使用されたのか分かりません。従ってサーバアプリケーションがユーザを認証したとしても、使用されているクライアントマシンを特定したい場合などは手掛かりがありません。何らかの方法でサーバがクライアント証明書の情報を取得できれば、認証システムもより強固なものにできるのではないでしょうか。

今回はクライアント証明書の情報を抜き出し、ロードバランス先のサーバへの接続時にHTTPヘッダとして埋め込む方法をご紹介します。

下記URLでもご確認いただけます。
http://devcentral.f5.com/Wiki/default.aspx/iRules/InsertCertInServerHeaders.html

タイトル:SSL Client認証の証明書情報をサーバに渡すiRule

メリット:
SSLオフロード下においてもクライアント証明書の認証結果をサーバが利用できるようになることで、柔軟で強固な認証アプリケーションの開発が可能となる。

機能説明:
クライアントとのSSLハンドシェイクにおいてBIG-IPが証明書を受け取った後、証明書に含まれる情報および認証結果を変数として格納します。
サーバへのHTTPコネクションを張る際にHTTPヘッダとしてそれらの情報を埋め込み、またBase64エンコードされた証明書全体も埋め込みます。
証明書認証に失敗した場合は、エラーページへリダイレクトします。

設定概要:
HTTPSのVirtual Serverを登録
Virtual ServerにてHTTP Profileを選択
SSL Profile (Client) にてClient Authenticationを設定
該当Virtual ServerにiRuleを登録

【iRule定義】

```
when CLIENTSSL_CLIENTCERT {
  # set time to maintain session data (in seconds)
  set session_timeout 7200

  set ssl_cert [SSL::cert 0]
  set ssl_errstr [X509::verify_cert_error_string [SSL::verify_result]]
  set ssl_stuff [list [b64encode $ssl_cert] $ssl_errstr]
  session add ssl [SSL::sessionid] $ssl_stuff $session_timeout
}
when HTTP_REQUEST {
```

```
  set ssl_stuff2 [session lookup ssl [SSL::sessionid]]
  set ssl_cert2 [lindex $ssl_stuff2 0]
  set ssl_errstr2 [lindex $ssl_stuff2 1]
  if { $ssl_errstr2 eq "ok" } {
    HTTP::header insert SSLClientCertStatus $ssl_errstr2
    HTTP::header insert SSLClientCertSN [X509::serial_number [b64decode $ssl_cert2]]
    HTTP::header insert SSLClientCertb64 $ssl_cert2
  } else {
    # send HTTP 302 redirect to an error page
    HTTP::redirect "http://192.168.0.64/error.html"
  }
}
```

補足：
iRuleの証明書に関するパラメータについては下記URLでご確認いただけます。
http://devcentral.f5.com/wiki/default.aspx/iRules.X509

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com	F5 Networks Asia-Pacific apacinfo@f5.com	F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com	F5 Networks Japan K.K. f5j-info@f5.com