# Logon mit Captcha

**Sven Mueller, 2014-13-01**

Heute möchte ich Ihnen kurz die APM-Konfiguration zum Logon mit einem Captcha (*C*ompletely *A*utomated *P*ublic *T*uring test to tell *C*omputers and *H*umans *A*part) vorstellen.

Ein Captcha verwendet man um fest zu stellen, ob ein Nutzer menschlicher Natur ist oder ein Bot, der möglicherweise vielleicht auch einen Brute Force Angriff oder ähnliches durchführt. Typischerweise zeigt ein Captcha auf der Logon-Seite einen Text an, der z. B. durch verzerrte Buchstaben dargestellt ist. Die Idee dabei ist, dass ein Bot diesen Text nicht lesen kann, wohl aber ein Mensch. Dieser muss nun neben den Login-Credentials auch die verzerrten Buchstaben in ein Eingabefeld eintragen. Hat er dies richtig getan, ist die Anmeldung erfolgreich.

Es gibt verschiedene Anbieter, die es ermöglichen auf einfache Weise solche zusätzlichen Funktionen mit in Webseiten zu integrieren. Einer davon ist Google und man kann diesen auch im Zusammenhang mit dem APM nutzen.

Wie der Google reCAPTCHA Dienst im Detail funktioniert, kann man hier nachlesen:

http://code.google.com/apis/recaptcha/intro.html

http://code.google.com/apis/recaptcha/docs/display.html

http://code.google.com/apis/recaptcha/docs/verify.html

### Google Account fürs reCAPTCHA Project

Als erstes benötigen wir einen Google Account um den reCAPTCHA Dienst nutzen zu können. Diesen kann man hier anlegen:

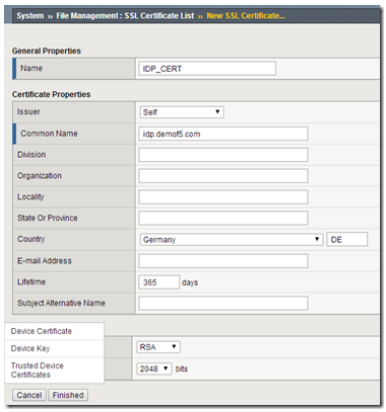
http://www.google.com/recaptcha/whyrecaptcha

In der Abfragemaske trägt man den Domain Namen, für den der Service genutzt werden soll ein. Als nächstes bekommt man für diesen dann einen Public- und Private-Key angezeigt. Beide werden wir später in unserer APM-Konfiguration benötigen. Es ist auch möglich diese Keys für mehrere Domains zu verwenden.

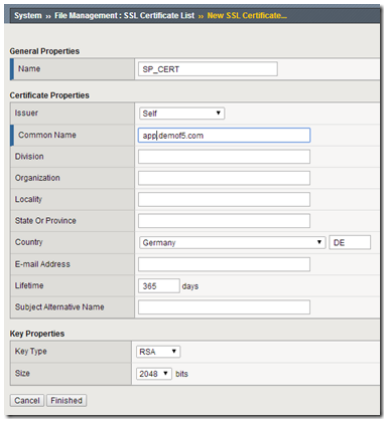
### APM Konfiguration

Im nächsten Schritt konfigurieren wir unseren APM:

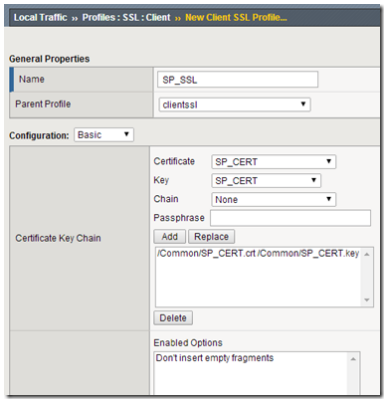
Das bedeutet, wir legen unter “Access Policy/Access Profiles/Configurations“ ein CAPTCHA Profil an, in dem auch unsere Private- und Public- Keys verwendet werden, die wir ja während unserer initialen Google Konfiguration erhalten haben.



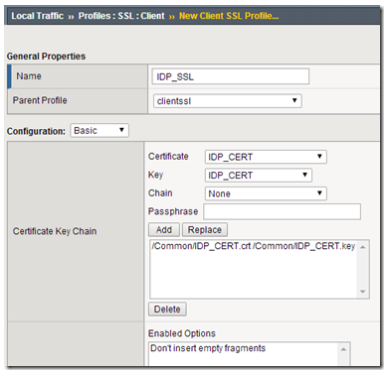

Nun erstellen wir unsere APM Policy wie gewohnt. Als erstes wähle ich innerhalb der Policy im Visual Policy Editor ein Logon Page Objekt aus. Diesem weise ich mein CAPTCHA Profil zu.




Alles weitere lasse ich in meinem Fall nun auf den Standardwerten. Es wird also noch Username und Passwort abgefragt, die ich gegen mein Active Directory überprüfe. Das nächste Objekt in meiner Policy ist ein AD-Auth, in dem ich mein Active Directory zuweise.



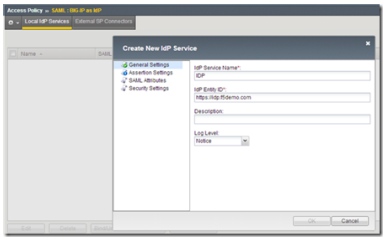

Fertig ist die Policy:




Nachdem ich die Policy „applyed“ und dem entsprechenden virtuellen Server zugewiesen habe, muss der Nutzer nun also Username, Passwort und den Captcha Text richtig eingeben, um auf die dahinter geschaltete Ressource zugreifen zu können.


**Verbindung zu Google**

Natürlich muss die BIG-IP Zugriff zu Google haben, um den Dienst nutzen zu können. Aber was ist, wenn der mal nicht gegeben ist, aus welchen Gründen auch immer? Ist dann kein Login mehr möglich? Dies kann ebenfalls eingestellt werden. Im CAPTCHA Profil kann man hier einen entsprechenden Haken bei „Allow Access if CAPTCHA Verification Cannot Complete“ setzen oder eben weglassen.




Wie das reCAPTCHA Feld aussehen soll, kann man im Drop-Down Menü (CAPTCHA Theme) des CAPTCHA Profiles auswählen. Hier gibt es von Google schon einige fertige Templates zur Auswahl. Es ist aber auch möglich eigene Kreationen zu erstellen. Diese muss man dann unter Google anlegen. Hier einige weitere Infos dazu:

https://developers.google.com/recaptcha/docs/customization?hl=de

**Sessionvariable**

Zum Schluss noch der Hinweis auf die Sessionvariable zum CAPTCHA. Denn wie wir wissen, werden alle Zustände immer in Sessionvariablen abgelegt, die es uns ermöglichen hiermit weitere Funktionen zu realisieren.

<Handbuch>

**session.logon.captcha.tracking**: The unsigned integer is treated as a bitmask. Determines whether to track successful/unsuccessful logon attempts by IP (bit in 0 position) and/or by username (bit in 1 position) when CAPTCHA is enabled. Should not be used by external modules because it is intended for very specific purposes.

</Handbuch>

So, das war es auch schon zum Thema APM-Logon Page mit einem Google CAPTURE.

Ihr F5-Blogger, Sven Müller

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