Can iRules fix my cert mismatch errors?

Colin Walker, 2008-04-09

SSL encryption as a means of security on the web isn't a new concept. We've talked about it here on DevCentral many times, and it's as pedestrian a concept as a corndog on the boardwalk to most internet users. We've talked about the performance pros and cons and some of the configuration overhead, etc. But what about the effect on the user experience when things aren't working quite as intended?

As more and more applications jump on the SSL encryption bandwagon there are more people experiencing all kinds of fun issues that weren't there before. Things like un-trusted CAs, expired certs and the woefully common cert name mismatch warning. The latter of which is something that many people have come to DCLand to ask about. They inquire about the possibility of fixing this issue with an iRule. The general consensus seems to be that if they could just change the hostname before connecting to the server, the nasty mismatch warning would go away, and suddenly you have happy users. Unfortunately, even with the flexibility and power of an iRule, this just isn't something that we can solve...well...not easily, anyway. The reason is that this is really a chicken and egg scenario, or horse and cart, if you prefer.

If you look at what would need to happen in order to avoid this oh so annoying warning, I think it'll make a lot of sense. Before performing a hostname re-write or redirect, most people want to do some sort of inspection first to be sure they want to perform said action. I.E. only redirect if the hostname equals bob.com, or only rewrite if the hostname doesn't contain www, etc. That inspection is impossible, however, since the information you're looking for is encrypted. Even if you could get to it, you couldn't change it because...well...it's **encrypted**.

To get to the data you need you'd have to decrypt it first using the appropriate SSL key, which we can helpfully do right on the BIG-IP. Problem solved, right? Not so much. See, even if we decrypt the data on the BIG-IP, perform the rewrite, and re-encrypt it on the way back to the servers...we still had to use the key to decrypt the data. You know, the key that doesn't match the hostname the user entered. The one that's going to force them to accept the warning that the hostname they entered doesn't match the one on the cert. Even with the tricky tools of the BIG-IP, we can't do magic. There's just no getting around that one yet.

I wouldn't want to leave you empty handed, though, so let's look at another issue that's come up, briefly. Say you're running an SSL encrypted app that is having the SSL encryption offloaded to the BIG-IP to lighten up the load on your back-end servers. If your servers go down for some reason (maintenance window, upgrade, outage, etc.) all of the users that are trying to connect are still being forced to perform the SSL handshake with the BIG-IP before finding out that there is no server to connect to. This is a somewhat slow and intensive process that can be avoided. To immediately reject the connection, thereby speeding up the result for your users, you could do something like this with an iRule:

```
when CLIENT_ACCEPTED {
   # Check if the default pool of the VIP has no active members
   if {[active_members [LB::server pool]] < 1}{
      # Disable the client SSL profile and send a TCP reset to the client
      SSL::disable
      reject
   }
}
```

Of course that just rejects the connections. Perhaps you wanted to actually serve them some sort of maintenance page instead. You could modify the rule slightly to something like:

```
when CLIENT_ACCEPTED {
   # Check if the default pool of the VIP has no active members
   if {[active_members [LB::server pool]] < 1}{
      # Disable the client SSL profile and send users to a backup pool
      SSL::disable
```

```
        pool outagePool
    }
}
```

This would send the user to your backup or outage pool which would let them know the situation rather than just closing their connection. You could, of course, make this message as user friendly and pretty as you want. So now your users don't have to wait around for the SSL handshake to complete, your BIG-IP gets to avoid the extra load all of the failure/retry cycle, and your users get a nice message letting them know that all is under control. Thanks again, iRules.

Get the Flash Player to see this player.
20080904-SSLMisMatch.mp3

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