20 Lines or Less #31 – Traffic shaping, header re-writing and TLS renegotiation

Colin Walker, 2009-06-11

What could you do with your code in 20 Lines or Less? That's the question I ask (almost) every week for the devcentral community, and every week I go looking to find cool new examples that show just how flexible and powerful iRules can be without getting in over your head.

This week not only are the examples cool and interesting, but one of them at least is extremely timely. You've no doubt heard about the client-initiated MITM attack for TLS that was recently disclosed. It's front-page news around the web and for good reason. While research needs to be done and a real fix needs to be put in place, one crafty community member was quick to draft up a simple fix to at least help mitigate their own issues. And in under 20 lines, no less. Here are this week's offerings:

Simple traffic shaping

http://devcentral.f5.com/wiki/default.aspx/iRules/Simple_traffic_shaping.html

User JackofallTrades brings us a great example of iRules simplicity via the codeshare. If you're looking for a way to send folks to different rateclasses based on their usage, this is one way you can get there. It's highly customizable, too, since it's an iRule.

```
when SERVER_DATA {               set srvAge [IP::stats age]               set srvBytes [IP::
```

Rewrite Host header to server name

http://devcentral.f5.com/wiki/default.aspx/iRules/rewrite_host_header_to_server_name.html

Hoolio's at it again with his latest codeshare entry. In this example he shows how you can write in custom host address headers based on the destination server your request is being sent to. Fun stuff.

```
when HTTP_REQUEST_SEND {   # Need to force the host header replacement and HTTP:: commands int
```

Mitigating the TLS client-initiated renegotiation MITM attack

http://devcentral.f5.com/Default.aspx?tabid=53&forumid=5&postid=86456&view=topic

Last but certainly not least, user Lupo comes to us with a simple yet hawesome iRule to show an easy way to put a stop to renegotiation MITM attacks in your environment…just so long as you have iRules handy (and don't need to renegotiate your SSL connections). I love it when users share cool things they're doing. I love it even more when those cool things are timely, interesting, and almost certainly useful to many other people. Way to go Lupo, thanks for sharing. Note that this, as with all 20LoL entries, isn't tested/guaranteed/endorsed, etc. But it's pretty sound logic and I don't see any good reason it shouldn't work. Test it in your environment and see for yourself.

```
when CLIENT_ACCEPTED {
   # initialize TLS/SSL handshake count for this connection
   set sslhandshakecount 0
 }

 # if you have lower priority iRules on the CLIENTSSL_HANDSHAKE event, you have to make sure,
 when CLIENTSSL_HANDSHAKE priority 100 {
   # a handshake just occurred
   incr sslhandshakecount

   # is this the first handshake in this connection?
   if { $sslhandshakecount != 1 } {
     # log (rate limited) the event (to /var/log/tmm)
     log "\[VS [virtual] client [IP::client_addr]:[TCP::client_port]\]: TLS/SSL renegotiation
     # close the clientside connection
     TCP::close
   }
 }
```

There are three more awesome examples for you. 20 lines of code or less packed with all sorts of iRuley goodness to make your lives easier, better, faster or safer. How can you not love that? See you next time.

#Colin

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