20 Lines or Less #24

Colin Walker, 2009-03-06

What could you do with your code in 20 Lines or Less? That's the question I ask (almost) every week, 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 is apparently the week of encryption! I bring to you from my fellow DevCentralites a trio of encryption/hashing goodness via iRules. Two of today's iRules were pulled from the samples page, one was recommended to me by Jason. All are very cool examples of iRules geekery and creativity, and they just happen to share a common theme. Even though hashing and encryption aren't quite the same thing, they've always fell somewhere in the same region to me, so I'm lumping them together. I get to do that, it's my blog. So roll up your sleeves for some hashing, non-decrypting goodness, and let's go.

FNV Calculation

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

In the first of two hashing iRules that the ever crafty Nat has posted, he gives us a look at FNV hash formulation via iRules. What is FNV? Wikipedia will tell you all about it, just go take a peek.

```
when RULE_INIT {    set fnv_hash 0x811c9dc5    # 2166136261    set fnv_prime 0x01000193    # 1
```

HMAC Calculation

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

In his next trick, Nat shows us how to create a Hash Message Authentication Code (HMAC) via iRules. This one I had to massage a little to get in under the 20 line limit, and even then it just barely squeaks by. It was worth it though…cool stuff!

```
when RULE_INIT {
  set input { "1234"
"12345678901234567890123456789012345678901234567890123456789xxxx"
"yyyy12345678901234567890123456789012345678901234567890123456789xxxx"
}
  foreach prekey $input {
    switch [string length $prekey] {
      "64" { set key [sha256 $prekey] }
      default { key $prekey }
    }
    set ipad ""
    set opad ""
    for { set j 0 }{ $j < [string length $key] }{ incr j }{
        binary scan $key @${j}H2 k
        append ipad [format %c [expr 0x$k ^ 0x36]]
        append opad [format %c [expr 0x$k ^ 0x5c]]
    }
    for { }{ $j < 64 }{ incr j }{
        append ipad 6 \\
    }
    binary scan [sha256 $opad[sha256 "${ipad}test"]] H* hextoken
    log -noname local0. [string toupper "result  = $hextoken"]
  }
}
```

HTTPS Passthrough Fallback URL

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

This example was pointed out to me by Jason and is brought to you courtesy of the ever active hoolio. This is a very cool way to pass SSL traffic without decrypting, yet hang on to some failover and redirection capabilities if things go down. Dig it.

```
when CLIENT_ACCEPTED {
   log local0. "[IP::client_addr]:[TCP::client_port]: Received
connection with active members: [active_members [LB::server pool]]"
   # Check if there are members available in the VIP's default pool
   if {[active_members [LB::server pool]]}{
      # Disable the client SSL profile so the HTTPS traffic is passed
through encrypted to the node
      SSL::disable
      # Disable the HTTP profile as we're not going to redirect this
request
      HTTP::disable
      log local0. "[IP::client_addr]:[TCP::client_port]: Members
available"
   }
}
when HTTP_REQUEST {
   # The HTTP_REQUEST event is only triggered if the pool members are
down and the client SSL and HTTP profiles are left enabled
   # Redirect the client
   HTTP::redirect https://maintenance.example.com
   # Close the TCP connection so that the pool is checked for every
HTTP request
   #   This should prevent clients from being continuing to be
redirected after the pool comes up
   #   (which would happen if they re-used the same TCP connection).
   TCP::close
   log local0. "[IP::client_addr]:[TCP::client_port]: Redirecting
request"
}
```

Thanks to everyone that keeps on contributing awesome iRules. It's a privilege to get to write about them. Keep 'em coming, and let me know if you've got any questions or suggestions.

#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