

20 Lines or Less #8



Colin Walker, 2008-29-05

What could you do with your code in 20 Lines or Less? That's the question I ask 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.

For this week's 20LoL sampling I've dipped into my own private stash of iRule goodness. Some of these are oldies but goodies, one of them I actually just wrote yesterday as an example for [Lori's Blog](#). As such the newly written example is the only one with a URI. The others will just have a description and the iRule source.

I'm sure I'll be diving back into the Forums and CodeShare in the coming weeks as there just seems to be an endless stream of cool stuff to dig through out there, but I wanted to toss up a few of my own rules this week. Be gentle with comments, some of these are old as I said. ;)

Content Scrubbing for Adobe Flash Exploit

<http://devcentral.f5.com/weblogs/macvittie/archive/2008/05/29/3309.aspx>

This iRule digs through the contents of the HTTP responses being sent out from your servers and looks for known exploit sites, then blocks those responses from going to your users. In this way it attempts to help protect them from the spread of [the Adobe Flash exploit Lori's been talking about](#).

```
when HTTP_RESPONSE {
    HTTP::collect
}

when HTTP_RESPONSE_DATA {
    switch -glob [string tolower [HTTP::payload]] {
        "*0novel.com*" -
        "*dota11.cn*" -
        "*wuqing17173.cn*" -
        "*woai117.cn*" -
        "*guccime.net*" -
        "*play0nlmie.com*" {
            HTTP::respond 200 content "The server is currently unable to
            serve the requested content. Please try again later."
            log local0. "Adobe Flash exploit infected Server IP:
            [IP::server_addr]."
        }
    }
    HTTP::release
}
```

This iRule was written to deal with a very high-volume need for client limiting. By storing the IPs in an array and accessing them in the most optimized format I could come up with, this rule was able to stand up to some pretty impressive numbers. If memory serves it was somewhere near 200K connections per second with nearly 3 million concurrent connections. Not too shabby!

```
when RULE_INIT {
    array set connections { }
}

when CLIENT_ACCEPTED {
    if { [info exists ::connections([IP::client_addr])] } {
        if { [incr ::connections([IP::client_addr])] > 1000 } {
            reject
        }
    } else {
        set ::connections([IP::client_addr]) 1
    }
}

when CLIENT_CLOSED {
    if { [incr ::connections([IP::client_addr]) -1] <= 0 } {
        unset ::connections([IP::client_addr])
    }
}
```

Selective HTTPS Redirect

This is a slight variant on a popular concept. This iRule does a selective redirect to HTTPS by checking a given class to see if the incoming URI is one that should be served via HTTPS. The neat part here is that it also does a port check and a preventative else statement, meaning this iRule should be able to be deployed on a global virtual, serving all ports, where most examples like this require the traffic to be broken up into two VIPs, port 80 and port 443, to avoid infinite looping.

```
when HTTP_REQUEST {
    if { [TCP::local_port] == 80 } {
        log local0. "connecting on HTTP server"
        if { [matchclass [HTTP::uri] starts_with $::secure_uris] } {
            HTTP::redirect "http://[HTTP::host][HTTP::uri]"
        }
    }
}
```

So there you have it, another few examples of what can be done via iRules in less than 21 lines of code. This 20 LoL brought to you from my personal vault, so I hope you enjoy. As always, please let me know if you have any feedback, comments, questions, suggestions, musical recommendations or other pertinent information to share. See you next week.

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

©2019 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113