Security Irules 101: DNS Gravitational Disturbance

Josh Michaels, 2012-29-11

Introduction

iRules are a powerful tool in the F5 administrators arsenal. They allow administrators to adapt and customize the F5 to their needs. They provide extensive power for security engineers as well. We've decided it's time to revisit the Security iRules 101, with updated content, and 100% more monkeys!

In section 4 of the series, let's talk about DNS. Domain Name System is the address book of the internet. Any time you type letters into a browser and hit enter, some form of DNS action is happening, whether it grabs the IP from local cache or sends out requests to the far corners of the tubes to get the address it needs to go to.

I won't bore you with a long winded DNS lesson. DNS boiled down:

Clients ask "Where the hell is devcentral.f5.com"

DNS Server responds either "Here: response " or " I don't know"

Why do we care about DNS?

So, why do we, as security admins care about DNS? DNS is a quick way to implement a layer of control in your network. If your network architecture includes an internal DNS resolver (DNS server that will resolve all requests for internal clients), you could potentially drop all DNS requests headed outside your network that are not sourced from that resolver. What does that get you? Well, if client machines can't query any DNS servers outside of the internal network, you gain control (not complete, there are always ways around it.. ahem host files.. ahem) over the DNS world. With control of DNS, you can manage what domains resolve for your clients, which in turn can help control acceptable use policy and malware.

How does controlling DNS help?

Acceptable use policy

Working from a negative enforcement security policy (because it could be darn near impossible to create a DNS whitelist for most user browsing), we create a list of domains that we don't want clients to access. This can be a big task and you are never going to get them all. An example for acceptable use policy list might be:

socialmediasite.com bobssitethatisNSFW.com

.xxx

Malware:

Malware lists are dynamic and do better with proper care and feeding. You can get a good start by using something akin to: http://mirror1.malwaredomains.com/

With that data, we would create a data group akin to:

> ".sacklunch.com" := "harmful",
>
> ".evilmalwaresite.com" := "morrisworm",
>
> ".xxx":="adult materials"

So, now our clients have no DNS options other than the authorized internal LDNS and we have lists of domains that we don't want clients to access, what's next? Well, it wouldn't be an iRules series without the iRule eh? Much thanks to Hugh O'Donnell and Jason Rahm for the following amazing DNS rules.

The iRule Way

Caveat

For the LTM iRule solution below, the DNS Services module or the GTM module is required to be licensed. These frames redirect to the iRules codeshare housing the most up to date version of the code.

Essentially, this rule looks for DNS queries coming into the unit, rips out the question, checks against the naughty list and reacts. If it's on the naughty list, the requester is given a DNS answer that points them to a simple response server (in our case, hosted on the LTM). If the question is not on the list, it gets allowed through.

Check out the response page code below:

With these two simple rules, the LTM extends itself to acting as a DNS filtration system. Another slick day in DNS paradise.

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