A DNS firewall for Cambridge

Tony Finch ⟨fanf2@cam.ac.uk⟩

Hostmaster
University Information Services

June 2015 *

Abstract

The hostmaster and CamCERT teams propose to block users from accessing domains that are used for malware and phishing by filtering lookups on the central DNS resolvers. We can do this using commercial RPZ data feeds augmented with locally-managed block and allow lists; a subscription from securityZONES would cost us less than £5500 per annum.

1 What is a DNS firewall and why might we want one?

A common way for members of the University to be exposed to malware is for them to browse to a malicious web site. They might be misdirected by nasty web ads or by links in spam or phishing email.

Our email servers use several commercial DNS reputation services to help identify spam. However junk email changes constantly, and block lists take some time to catch up with new variants, so a small proportion of bad email is delivered to our users.

There is often a delay between a message being delivered and being read, during which time the reputation services may learn about this new spam and start blocking it. But this block is too late to benefit us with our current setup.

A "DNS firewall" is a DNS resolver which can enforce a security policy on which domains its users are able to resolve. We are interested in blocking domains which are used purely for malware and phishing, with no legitimate activity.

*Document source ⟨https://git.csx.cam.ac.uk/x/ucs/u/fanf2/2015-06-rpz⟩
version 3 date 2015-06-19 17:40:31 +0100

Blocking bad domains on our central DNS resolvers would protect our users from known malicious web sites. It would help compensate for junk email which gets through before a block is imposed. It will reinforce existing end-user protections such as Google's "safe browsing" block list [1] and anti-virus software [2].

2 What are RPZ data feeds and how much do they cost?

Spamhaus [3] and SURBL [4] provide a variety of anti-spam / anti-phishing / anti-malware reputation services. Our email systems use these block list services (and others) via JANET's national subscription [5]. These block lists are very effective at stopping spam without disrupting legitimate email.

Email and DNS servers require their block lists to be formatted differently. DNS RPZ (Response Policy Zones) [6] is a technology for reputation services (such as Spamhaus or SURBL) to provide block lists suitable for use by DNS resolvers.

Spamhaus and SURBL provide versions of their block lists in RPZ format, but these are not covered by the JANET national subscription.

The company "securityZONES" [7] acts as a sales agent for both Spamhaus and SURBL. They appear to be the only European reseller for Spamhaus and the only reseller at all for SURBL.

I have spoken to a sales agent who indicated that a data feed of the Spamhaus DBL [8] and DROP [9] RPZ lists would cost US$4762 per annum, and a SURBL RPZ feed would cost US$4500. A subscription to both would cost US$7875, or roughly £5150.

3 What are the risks of a DNS firewall?

Some users are likely to object if we impose "censorship" on our DNS servers. We can provide an unfiltered service to address concerns like this. (Members of the University may also run their own DNS resolvers and bypass our servers.)

Our email servers have had occasional problems with false positives – messages that were blocked which should not have been. We manage this by careful choice of which block lists are used for blocking messages outright; less reliable block lists just cause a spam score penalty.

RPZ is all-or-nothing, like blocking email, so a low false positive rate is important. A successful RPZ deployment will not disrupt the work of the University or add significantly to the support burden of our service desk and CamCERT teams.

Imperial College have reported they are very pleased with their deployment of the Spamhaus DBL RPZ [10]. They have said they get one or two problem reports each month, which is acceptable.

Spamhaus and SURBL offer a one month evaluation period. This does not seem long enough to do much more than verify that it works – it is not long enough to get useful feedback from users nor to confirm that the false positive rate is small enough not to cause problems.

4 What changes do we propose to make to the DNS service?

We will deply the DNS firewall in two stages, firstly with just a local blocklist to get experience with the setup, then later adding commercial RPZ data feeds.

When a domain is blocked, users will be redirected to an `rpz-block` server managed by us. The redirection will be done with a `CNAME` record in the response from our DNS servers, instead of the response given by the blocked domain.

All connection attempts to the `rpz-block` server will be rejected with a "destination unreachable" – "host is administratively prohibited" error message (ICMP type 3 code 10) except for `http` connections on port 80. When a web browser encounters a blocked domain, the `rpz-block` web server will explain to the user what has happened.

The `rpz-block` server's firewall will log all connection attempts (both `http` connections on port 80 and rejected connections on other ports); the logs will be contributed to CamCERT's existing firewall log analysis process.

The `rpz-block` web server will reject `https` connections (same as other non-`http` protocols), since we cannot spoof TLS connections without training users to click through security warnings on malicious websites. So `https` web sites are blocked in a less friendly way than `http` sites, but either way we protect users from visiting the malicious site.

Some DNS clients (such as MCS Linux) do DNSSEC validation. If we happen to block a DNSSEC signed domain, validators will return a "server failure" instead of the `CNAME` redirection. This is similar to the `https` situation.

4.1 Initial deployment

The technical changes required are:

- Add entries to the IP Register database to allow the CamCERT team to manage DNS RPZ block and passthru items. (See appendix B for draft instructions.)
- Set up the web server that handles accesses to blocked domains, and which feeds firewall logs to CamCERT.
- Change the DNS provisioning system to create a zone containing our local RPZ items from the database.
- Change the `recdns` failover configuration to add the new unfiltered resolver addresses set out in appendix A.

- Change the `recdns` name server configuration to apply RPZ filtering to the old `testdns` addresses.
- Announce the change (see section 5).
- Promulgate new recommendations for name server configuration on the CUDN.
- On the announced date, change the `recdns` name server configuration to apply RPZ filtering to the old `recdns` resolver addresses.

4.2 Addition of commercial RPZ feeds

Once we have deployed RPZ with a local block list, it is straightforward to add commercial RPZ data feeds.

These data feeds have a default blocking policy, which is to deny that the blocked domain exists. We will follow the usual practice, to override the default policy and instead return a `CNAME` pointing at our blocked domain web server.

Our local RPZ data, managed by CamCERT, can contain "passthru" entries to disable problematic blocks. (Appendix B has draft instructions.) We can implement a blanket passthru covering `cam.ac.uk` and other important domains.

5 Draft announcement

This is a sketch announcement for users, so it reiterates some of the points above.

On *(date TBD)* we will change the central DNS resolvers to block access to bad domains which are used for malware and phishing.

When a domain is blocked, the DNS resolvers will redirect you to a web server that explains the block, ⟨`http://rpz-block.arpa.cam.ac.uk`⟩.

Initially these blocks will be configured by UIS staff. If this trial is successful, from *(date TBD)* we will start blocking domains that appear in RPZ [6] data feeds from Spamhaus [3] and SURBL [4].

Our aim is that DNS blocks will not affect legitimate usage, but will help to reinforce your existing anti-malware software. We have been using these blocklists on our mail servers for many years with negligible problems.

If you identify a domain which should be blocked, or which is incorrectly blocked, please report it to ⟨`cert@cam.ac.uk`⟩.

When a domain is blocked, the redirection is be done by discarding the original DNS response from the blocked domain, and instead returning a `CNAME` pointing at the web server ⟨`http://rpz-block.arpa.cam.ac.uk`⟩.

If you would like to try out the new configuration in advance, it is currently available on the test DNS servers. If you need unfiltered access to the DNS, we now provide alternative resolvers which do not use the block lists. The filtered and unfiltered DNS resolvers run on the same hardware; they only differ in which queries they are willing to answer. Details of our DNS resolver names and addresses are set out in appendix A.

If you run your own DNS resolvers and you would like to use these block lists, the best way is to configure your servers to forward queries to our central DNS resolvers. If you run a mail server then you should configure it to use an unfiltered DNS resolver. Details of our recommended name server configurations can be found at ⟨https://jackdaw.cam.ac.uk/ipreg/nsconfig/⟩.

Please contact us via ⟨service-desk@ucs.cam.ac.uk⟩ if you have any questions or would like any configuration advice.

A DNS resolver IP addresses

Name	IPv4	IPv6	RPZ
recdns0.csx.cam.ac.uk	131.111.8.42	2001:630:212:8::d:0	☑
recdns1.csx.cam.ac.uk	131.111.12.20	2001:630:212:12::d:1	☑
recdns2.csx.cam.ac.uk	131.111.9.99	2001:630:212:8::d:2	☐
recdns3.csx.cam.ac.uk	131.111.12.99	2001:630:212:12::d:3	☐
testdns0.csi.cam.ac.uk	131.111.8.119	2001:630:212:8::d:fff0	☑
testdns1.csi.cam.ac.uk	131.111.12.119	2001:630:212:12::d:fff1	☑
testdns2.csi.cam.ac.uk	131.111.9.118	2001:630:212:8::d:fff2	☐
testdns3.csi.cam.ac.uk	131.111.12.118	2001:630:212:12::d:fff3	☐

There are four physical servers in different locations, and all of them can host any of these service addresses. The usual allocation of services to hardware is indicated below; the services in each box move as a unit in the event of hardware failure or if maintenance is required.

recdns0 recdns2	testdns0 testdns2
recdns1 recdns3	testdns1 testdns3

B RPZ in the IP Register database

This appendix contains draft instructions describing how the CamCERT team can manage the DNS firewall using the IP Register database.

Our responze policy zone is a subdomain of arpa.cam.ac.uk which is used for special DNS infrastructure. To add an entry,

- Go to ⟨https://jackdaw.cam.ac.uk/ipreg/cname_ops⟩
- In the "name" field, enter the domain to be blocked or allowed, followed by `.rpz.arpa.cam.ac.uk`
- In the "target name" field, enter `rpz-passthru` to allow the domain, or `rpz-block.arpa.cam.ac.uk` to block the domain.
- Put an explanation in the "purpose" field.
- Click "create".

To remove an entry,

- Go to ⟨https://jackdaw.cam.ac.uk/ipreg/cname_ops⟩
- In the "name" field, enter the domain to be blocked or allowed, followed by `.rpz.arpa.cam.ac.uk`
- Click "destroy".

To search for an entry,

- Go to ⟨https://jackdaw.cam.ac.uk/ipreg/table_ops⟩
- Select object type "cname", and click "switch".
- In the "name" field, enter the search string, using "%" as a wildcard.
- Click "search".

Note that `rpz-passthru` is a single hypenated label with no parent domain; it has special meaning to the RPZ machinery. In contrast, `rpz-block.arpa.cam.ac.uk` is an ordinary fully-qualified domain name; it is the name of the web server to which blocked domains are redirected.

For example, to block `baddies.com`, create a `CNAME` with:

name	`baddies.com.rpz.arpa.cam.ac.uk`
target	`rpz-block.arpa.cam.ac.uk`
purpose	Example block

And to allow `goodies.org` when it is erroneously blocked, create a `CNAME` with:

name	`goodies.org.rpz.arpa.cam.ac.uk`
target	`rpz-passthru`
purpose	Example allow

C Acknowledgments

Thanks to John Burnham, Rachel Coleman, Kate Jeary, Jon Warbrick, and especially David McBride for their helpful comments and suggestions on earlier versions of this memo.

References

[1] Google. *Safe Browsing API*. ⟨https://developers.google.com/safe-browsing/⟩.

[2] University Information Services. *Anti-virus information*. ⟨http://www.ucs.cam.ac.uk/support/anti-virus/⟩.

[3] Steve Linford, et al. *The Spamhaus Project*. ⟨https://www.spamhaus.org/⟩.

[4] SURBL. *URI Reputation Data*. ⟨http://www.surbl.org/⟩.

[5] JANET. *DNS blocklists and whitelists*. ⟨https://community.jisc.ac.uk/library/janet-services-documentation/dns-blocklists-and-whitelists⟩.

[6] Paul Vixie and Vernon Schryver. *DNS Response Policy Zones*. ⟨https://dnsrpz.info⟩.

[7] securityZONES. ⟨http://www.securityzones.net⟩.

[8] Spamhaus. *Domain Block List*. ⟨http://www.spamhaus.org/dbl/⟩.

[9] Spamhaus. *Don't Route Or Peer List*. ⟨http://www.spamhaus.org/drop/⟩.

[10] Alex Lomas. *Implementation and use of DNS RPZ in malware and phishing defence*. Technical report, Imperial College, March 2014. ⟨http://www.sans.org/reading-room/whitepapers/dns/implementation-dns-rpz-malware-phishing-defence-34535⟩.