DNS Firewalls In Action - RPZ vs. Spam

Jan 03, 2013 9:21 PM PDT | Comments: 0 | Views: 28,242

By **Paul Vixie**

In general, a network firewall is just a traffic filter — letting some traffic through and keeping other traffic out. Filtering rules can be anything from "allow my web server to hear and answer web requests but not other kinds of requests" to "let my users Ping the outside world but do not let outsiders Ping anything on my network." The Internet industry has used firewalls since the mid-1980's and there are now many kinds, from packet layer firewalls to web firewalls to e-mail firewalls. Recently the DNS (Domain Name System) industry has explored the firewall idea and the results have been quite compelling.

In this article I'm going to demonstrate a DNS firewall built using RPZ (Response Policy Zones) and show its potential impact on e-mail "spam". My goal is to pique the interest of I.T. professionals whether they are decision makers, system administrators, hard core DNS developers, or small office / home office power users.

Response Policy Zones

In the bad old days, every network element whether it was a switch or router or server — or firewall — was configured independently. There was no sense of clustering whereby an entire network could be configured from one MIB (management information base) even though we've had monitoring for entire networks for a long time now. In addition, every network element had its own configuration language which meant retraining for human operators if a new vendor entered the mix.

The designers of DNS RPZ learned the lessons of history and so the configuration language itself is the product, and network elements that speak this standardized DNS firewall configuration language are merely "implementation details". Of course there is a free and open-source implementation of RPZ, to seed the market and prove the point. That implementation is ISC BIND9, a free and open-source DNS implementation that serves about 85% of the world's DNS needs. Still, it's important at every stage of evaluation and planning for DNS firewalls to remember that DNS RPZ as an unencumbered standard is expected to be supported by every DNS

implementation out there, sooner or later. If you find yourself wanting to try RPZ and you're not running ISC BIND9, you can try it out in your lab and consider whether to ask your existing DNS vendor to add support for RPZ.

The name "Response Policy Zone" refers to the method of both describing and delivering DNS firewall configuration data. It's done with a specially formatted DNS "zone file" which is edited or generated the same way other DNS zone files are done, and is then propagated to all of your DNS firewalls using the same DNS "zone transfer" protocols used for any other DNS zone. Because DNS zone transfers are now incremental and because changes to DNS zones are now signaled in real time, the synchronization of your DNS firewall cluster is both efficient, robust, and timely.

The kind of filtering you can do in a DNS firewall that's based on RPZ is similar to any other kind of firewall, except that the filtering is on the data path not the messages. So whereas in an IP or TCP firewall has rules like "do not let this IP packet through" or "do not let this TCP session start up", a DNS firewall has instead rules like "do not let this answer be seen". So a DNS firewall does not stop answers from being sent, it just changes whether the answer that's sent is the truth or not. In the specific example of RPZ, it's possible to override the real answer with either a negative answer, an empty answer, an alias answer, or a full replacement of data answer.

E-mail "Spam"

Most e-mail traffic is unwanted, and there is a vibrant and ever-profitable industry for filtering this unwanted traffic. Many of us outsource our e-mail hosting just to avoid the cost and complexity of this filtering, because there is so much "spam" nowadays that the minimum filtering protections for an e-mail server now require high wizardry. Such wizardry is rare enough and expensive enough that it's often better to save the wizards for activities that simply cannot be outsourced, such as product development or service delivery. But no matter how much filtering you apply to your incoming e-mail, it is likely that at least a trickle of unwanted traffic will get through and will reach your inboxes. This is because the spammers are in business to make money and they are incentivized to constantly improve their emissions to make filtering harder. So, generally speaking, you can filter out the easy stuff, and what gets through will be the highest quality traffic sent by the most inventive and motivated spammers.

The economics of e-mail "spam" are based on the idea that recipients will click on an embedded link thus causing the web browser to go visit the spammer's website. That first click is worth money since it proves that you got the spam and that you were beguiled by whatever promises were contained within. It's also possible for that single "click" to cause the web browser or the computer itself to become infected with some kind of malicious software (sometimes called "malware"). You could wind up with a "key logger", or you could find yourself to be the newest addition to a robot network (sometimes called a "botnet") and thus ready and willing to relay new spam to more victims. Or if the spam e-mail was a "phishing attack" then the web browser will visit a rogue web

site that looks suspiciously like PayPal or perhaps some bank (maybe even your bank) where you will then be invited to update your credit card information.

The possibilities are in fact endless — we know this since we see a new kind of scam every month or so. But the gateway to success for the spammers is sending you an embedded link and getting you to click on that link. And that's where DNS firewalls come into play, since the embedded link will invariably contain a "throwaway" domain name. Such domain names are created and destroyed by the millions every day, because they cost near to nothing and because there is no accountability for the people who register them. In the olden days, a domain cost USD 35 per year or more — prepaid! And there was no refund if it was cancelled. Additionally, your registration and billing postal addresses had to be real places where someone could send a real Legal Summons if you used the domain in commission of a crime. No longer. Today a domain name can be created for pennies and those pennies are often charged to a stolen credit card. Domain "Whois" is useless: either because the address is of someone whose credit card was stolen, or because of "Whois privacy" whereby you have to send your Legal Summons to a proxy in some country where you don't have a local attorney.

What this domain "free for all" means for spammers is that: they can get a new domain name for every hour of the year; no one will be able to predict the next domain name they use; and no one will be able to send a complaint to anybody about the spam. In many parts of the world it can take a minimum of three business days to get a domain "taken down" and that's assuming that a "takedown" request is ever heard or even sent. And if you tie this "cheapness factor" and lack of accountability back to the fact that spammers make money from the first click, it looks like the victims and the security companies who try to protect these users are fighting a lost battle. And so, it was until the advent of DNS firewalls based on RPZ.

New Economics

Spammers make money. Spammers make a lot of money. And they will keep spamming to make more money. The skilled and inventive spammers will continuously vary their tactics to make it hard to filter their traffic. When they lose ground because some security company comes up with a better spam filter, these spammers triple or quadruple their efforts to get back in the game — to get back to where they make a lot of money. This is the game board as of January 2013, and this will be the game board as long as spamming continues to be a money making activity.

Since the Internet has no regulator and is an extra-national entity possessing neither sovereignty nor accountability, every effort toward making "domain takedown" more reliable and faster or to make "domain Whois" more reliable and accountable has been completely ineffective. So, the "spam value" of a throwaway domain name is measured in how long it can be used in spam as an embedded link to malicious web content before it will be taken down by its registry or registrar. That time value tends to be in the small number of days, but some spammers assume that it's time to throw away a throwaway domain name after a small number of hours.

To make any change to this game it will be necessary to reduce the time value of a throwaway domain name down to a small number of minutes, or perhaps even less than one minute. Even for a well-intentioned and well-resourced registrar, takedowns on the order of one minute would be very hard to implement. This means as long as domain names are cheap and unaccountable, we will need some other way to limit the usability of throwaway domain names as a connector between an embedded spam link and a malicious web site.

On the Internet, new technology can radically alter the economics of an industry — for examples, consider the advertising industry before and after Google Search, or the music industry before and after Apple iTunes. To reduce the time value of a throwaway domain name, it was necessary to create a standard configuration language for DNS firewalls which would support a vast number of subscribing name servers and extremely rapid end-to-end propagation of new firewall rules. Thus, DNS RPZ, about which you can read more at the ISC Knowledge Base.

RPZ in Action

In preparation for writing this article I checked my e-mail in order to find out what spam had leaked through my e-mail firewall in the last f>ew minutes. I found this:

```
Return-Path: <engravings7@multiform.at>
To: <vixie@vix.com>
Subject: Re:Re:ON- LINE/ My Pharmacy -
Date: Wed, 3 Jan 2013 01:33:00 +0100
From: "Stacy Burris" <engravings7@multiform.at>
Message-ID: <0F3001B269FFED906512C96CB8FDBC8D@multiform.at>
X-Mailer: PHPMailer 5.1 (phpmailer.sourceforge.net)
X-Virus-Scanned: ClamAV using ClamSMTP

http://mockurl.com/?271a6
```

I have to say that as spam goes, this one wasn't very well done. There's no "come on", no incentive given as to why I would click on this link. However, I tried to click on it, and got an error from my web browser, telling me that the web site did not exist. In checking the lower level DNS results for this lookup, I found this:

```
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 1040
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; AUTHORITY SECTION:
rpz.surbl.org. SOA dev.null. zone.surbl.org. 1325647120 180 180
604800 180
```

```
;; Query time: 1 msec
;; SERVER: 2001:4f8:3:30::3#53(2001:4f8:3:30::3)
;; WHEN: Wed Jan 4 03:20:28 2013
;; MSG SIZE rcvd: 102
```

What this told me is that my friends over at SURBL had added this domain (mockurl.com) to their RPZ feed. I am a subscriber to this feed. I don't have an easy way to find out when they added "mockurl.com" to their RPZ, but I've worked in the DNS field long enough to know that it could not have been added less than about ten seconds ago or I would not be seeing it yet. Since I kibitzed a little as to how SURBL's RPZ was set up, I figure it takes a little under a minute for their subscribers (like me) to see the rule changes they make. Becoming an RPZ provider is not difficult — a single "1U" rack mount server can probably support about ten thousand customers, and it's easy to add "fan out" for larger scale.

I also subscribe to an RPZ feed from SpamHaus, and one from Internet Identity, and another from Umbra Data. It so happens that for this spam and for this domain name, SURBL drew "first blood". When I designed RPZ, my vision was a robust economy of RPZ providers who would compete for subscribers, and a robust economy of RPZ subscribers ("customers") who would each likely subscribe to several competing RPZ feeds as well as maintaining their own private RPZ feed for local policies — as I do. My ISC BIND9 configuration file has the following logic inside its "options { }" block:

```
response-policy {
   zone "dns-policy.vix.com";
   zone "rpz.surbl.org";
   zone "rpz.spamhaus.org";
   zone "rpz.iidrpz.net";
};
```

Note that you can't just add the above to your own ISC BIND9 configuration, you'll first have to arrange for subscription access. The above is meant as an example of RPZ's triviality, please contact any potential RPZ vendor before you try to access their feed.

Roads Not Taken

Many people who have evaluated or adopted DNS RPZ have told me that they'd prefer a reputation system so that they could use the presence of a domain name in a spam-embedded link URL as an input to a scoring system. For them, the DNS reputation industry already works fine. If that's what you think you need, search the web for "RHSBL" and "URIBL". Chances are good that your existing spam filter already knows how to access this and already knows how to find embedded domain names in e-mail bodies. This is not the purpose of a DNS firewall and the absence of this feature is not an omission in the design of DNS RPZ.

Some other people who have evaluated DNS RPZ as a method of enforcing government controls over Internet DNS names that are used for infringement, piracy, counterfeiting, or child abuse materials, have told me that they really think DNS RPZ is a fit for their needs and proof that such controls are practical. For them, the DNS provides no such capability, and DNS RPZ is not a get-out-of-reality-free card. Most firewalls only work properly if the firewall operator is on friendly terms with the people "inside", because these folks have all the time in the world to find some proxy or VPN or tunnel or other gap that will let them keep doing what they want to do. DNS firewalls are a fine example of this — they work if the interests of the protected population and the interests of the DNS firewall operator are closely aligned. Otherwise a DNS firewall is just bad (and by bad I mean "not funny") security theatre.

Conclusion

The Internet and its DNS are extremely robust and they serve a population of billions of people including many criminals. DNS RPZ is an attempt to offer differentiated service levels, so that DNS works better for the good guys than for the bad guys, where "good" and "bad" are necessarily and completely subjective. We can't stop domain names from being "too cheap to meter" and we can't demand accountability for those who register throwaway domain names and we can't demand rapid enough takedown from the DNS industry when a domain name is clearly being used for malicious purposes. But even though we can't stop throwaway domain names from existing, we can — with DNS RPZ — severely degrade the utility of those throwaways.

By Paul Vixie, CEO, Farsight Security. Visit the blog maintained by Paul Vixie here.

Related topics: Cybersecurity, DNS, Networks, Spam

Comments