Response Policy Zone (RPZ) FAQ

How much does RPZ cost?

RPZ is an open specification defined by the Internet Systems Consortium (ISC) with a reference implementation available as a BIND extension. The BIND DNS server and RPZ extension are available free of charge and can be downloaded from http://www.isc.org.

What is RPZ

The short answer is that Response Policy Zone (RPZ) enables DNS administrators to selectively block DNS resolution of sites.

Why would I want to block DNS resolution?

There are places on the Internet that could cause harm to unsuspecting users who visit the site. For example, lets say a site was put up on the Internet for the sole purpose of serving malware that is advertised via spam. One of your customers gets a spammed email advertising a link on that site and clicks on it. If the malware site's host name or domain was listed in your RPZ aware DNS server, your customer's computer would be unable to resolve the address of the bad site. Without the address, there would be no connection. You would have protected your user from losing their personal information and/or prevented one more machine from becoming a bot.

What's so great about RPZ?

Instantaneous threat mitigation. Let's say you had an enterprise that consisted of 10,000 users that pointed to 100 geographically dispersed corporate nameservers. If you identified a site that you needed to block your employees from getting to, you could enter that site in your RPZ zone and propagate it out to all your nameservers, worldwide, in a matter of seconds - seconds as in a fraction of a minute. As soon as the RPZ zonefile gets propagated, your employees would be unable to resolve the ip address of the site, effectively mitigating the threat in near real time.

How does RPZ know what to block?

RPZ uses one or more files that contain host names and/or domains you want to block. When a DNS query is made against a recursive nameserver that's using RPZ, any host in the RPZ list will not resolve to the actual IP address.

What does the DNS server return when a site gets blocked?

The RPZ file is actually a regular BIND zonefile. Most RPZ implementations will return an NXDOMAIN result when a blocked site is queried. NXDOMAIN essentially means that the DNS server was unable to resolve what you asked it. You can, however, add whatever IP address you want returned when your customer queries a blocked host or domain. Providing your own IP in response to a query on a blocked site can be useful for redirecting your customers to a warning page.

Where do the RPZ lists of bad sites come from?

RPZ needs to know which hosts or domains you want to block from DNS resolution. You provide that information to RPZ by adding a regular looking zone file on your DNS server, then populating the zone with what you want to "block". That list can be developed in-house or you can use commercially available RPZ host files. Even if you use a commercial list, you can still add your own list as well.

What are the advantages of commercial lists?

Timeliness and completeness! At the time of this writing, the two most often used commercial RPZ lists are rpz.spamhaus.org (a Spamhaus product) and rpz.surbl.org (a product of SURBL). Spamhaus and SURBL continuously update their RPZ lists and push out updates about every 5 minutes. That's every 5 minutes, every hour, every day. The domains that are listed by both Spamhaus and SURBL are generally cultivated from links appearing in spam. New lists will probably appear shortly that focus on other threat sources.

What do I need to implement RPZ?

The RPZ reference implementation is available as a BIND extension, so the first thing you'll need is a recent version of BIND that supports RPZ. The first version of BIND that natively provided RPZ support was 9.8.0. Secondly, the DNS server you install RPZ on will only work if it's a customer facing recursive nameserver. In other words, you want to install an RPZ aware resolver that your clients point to for dns resolution.

How much bandwidth does RPZ need?

A properly configured nameserver that serves or receives RPZ zonefiles would use "incremental zone transfers". With incremental zone transfers, only the differences between the old and new zonefile get transmitted. For example, if your RPZ zonefile contained 100,000 entries and you removed 10 and added 20 new hosts, the update would transmit only the 30 changes, not the entire file of 110,000. This means that the zone updates generally take less than a second to propagate to the secondaries and will result in only a few kilobits worth of traffic.

What kind of hardware do I need to support RPZ?

Generally speaking, if you're simply receiving RPZ zonefiles, probably you can continue to use the same hardware you currently have. The CPU overhead imposed by RPZ is negligible. The RPZ files essentially become memory resident, so you would need enough RAM to store whatever RPZ lists you're using. In most cases, this would require under 1 gigabyte of additional RAM.

How many secondaries could I feed from one Bind server?

In the old days, the oldest systems got relegated for use as dns servers. Today, nameservers need to be able to contend with DNSSEC, TSIG and millions of lookups per hour. If you're providing DNS services for others, you should be using modern equipment with adequate horsepower.
It's difficult to predict what you would need in the way of hardware without knowing how much use your system currently has. Let's say you have a moderately sized box that has a single Nehalem quad core CPU and 8 gigs of RAM - you should be able to support well over 250 secondary nameservers that pull incremental zone transfers from you. If you're supporting only a handful of secondaries, chances are what you have now would work just fine.

What documentation is available for RPZ?

If you download BIND you'll find that contained within the tarball is the Bind Administrators Reference Manual (ARM). Documentation for RPZ can be found in the ARM in section 6.2.16.20.