Deteque Free Threat Feeds Setup

1. DNS Firewall Free Threat Feeds Description and Master Information

The **Don't Route Or Peer** (DROP) zone contains netblocks that are "hijacked" or leased by professional spam or cyber-crime operations (used for dissemination of malware, ransomware, botnet controllers, and other malicious content).

The **cryptominer** zone contains domains that are known sources of cryptojacking scripts. These scripts execute when a user visits a site and proceeds to use the user's system resources to mine crypto currency while the site is open.

In order to consume Deteque's free threat feeds you will need to setup your local recursive resolver to act as a secondary for the freezone feeds with our masters which are the following:

IPv4: 34.194.195.25
IPv4: 35.156.219.71

Note that these servers are setup to distribute via IXFR.

Quick Tip

Before you get started create a backup of your BIND configuration (named.conf) so you will have an original reference in case there is an issue with your configuration after enabling DNS Firewall

2. Configuring BIND for DNS Firewall and Deteque's free feeds

2.1 Install/Upgrade the most recent version of BIND

It is recommended that before you begin to implement DNS Firewall in your BIND install you upgrade to the most recent version of BIND. It is suggested that the upgrade is acquired directly from ISC (https://www.isc.org/downloads/) instead of updating from a software repository as some repositories will have out of date versions. This will ensure that you have the best possible support for DNS Firewall.

2.2 Enabling Logging of DNS Firewall rewrites

To monitor evaluate, and troubleshoot DNS Firewall, logging needs to be enabled in your configuration (etc/named.conf).

```
logging {
        channel rpzlog {
                file "rpz.log" versions unlimited size 1000m;
                print-time yes;
                print-category yes;
                print-severity yes;
                severity info;
                };
        category rpz { rpzlog; };
};
```

Deteque Free Threat Feeds Setup

With these settings your log file output for rewrites should look like the following:

```
1-Jan-2010 00:00:00.000 rpz: info: client @0x8ac7921a21d0 172.0.172.2#1286
(baddomain.invalid.com): rpz IP NXDOMAIN rewrite baddomain.invalid.com via
2.152.24.172.rpz-ip.drop.spamhaus.org
```

Note that only IPs are included in the DROP zone but the hostname will be displayed in the log if the user/machine attempted to access a hostname.

Quick Tip
Consider exporting your logs into a database or log analysis software to have a better visualization of the data produced in the DNS Firewall logs.

2.3 Creating a Local DNS Firewall Zone

A local DNS Firewall Zone is needed for creating exceptions (passthru) to feeds that you have subscribed to and also create additional blocking or whitelisted actions. This zone is created in /var/named:

```
$TTL 300
@       IN SOA  localhost.local.rpz. (
                                20170913        ; Serial number
                                60              ; Refresh every minute
                                60              ; Retry every minute
                                432000          ; Expire in 5 days
                                60 )            ; negative caching ttl 1 minute
                        IN NS LOCALHOST.
deteque.com             IN CNAME        rpz-passthru.
*.deteque.com           IN CNAME        rpz-passthru.
32.25.195.34.rpz-ip     IN CNAME        rpz-passthru.   ;whitelist 34.194.195.25/32
32.71.219.35.rpz-ip     IN CNAME        rpz-passthru.   ;whitelist 35.156.219.71/32
invalid.com             IN CNAME        .               ;local block against invalid.com
*.invalid.com           IN CNAME        .               ;local block against *.invalid.com
```

You can name your local zone whatever you wish. Anything after IN SOA localhost. is what your local zone will be named. Remember to include a. at the end of the name. The following 4 record details after Serial Number (Refresh, Retry, Expire, Negative result TTL) are displayed in seconds and are always listed in this order.

It is recommended that anything that is critical to your network be added into this zone as a rpz-passthru. Any internal domains and network IPs should be included in this zone.

Deteque Free Threat Feeds Setup

2.4 Defining Master and Slave Zones

BIND requests that you define which zones that will be used to action on DNS queries to your resolver in your named.conf file. First the local master zone should be defined.

Quick Tip
When putting DNS Firewall on your resolver ensure that you have a low TTL. This will avoid having a malicious or compromised site still resolve when it is included in an DNS Firewall feed.

```
zone “local.rpz” {
                type master;
                file “local.rpz”;
                allow-transfer { none; } ;
                allow-query { localhost; };
};
```

The reason that allow-query is set to localhost is so only the resolver will be able to access the zones defined.

Next your slave zones that will pull from Spamhaus' masters will need to be defined and will look like the following:

```
zone “drop.rpz.spamhaus.org” {
                type slave;
                file “dbl.rpz.spamhaus.org”;
                masters { 34.194.195.25; 35.156.219.17; };
                allow-transfer { none; };
                allow-query { localhost; };
};
```

Since the slave zones are not located locally on the resolver the master zones must be defined in every slave zone. Also the slave zones will be set to localhost.

2.5 Enabling IXFR zone transfers

Since DNS Firewall is designed to provided updates to malicious threats as quickly as possible it is required that incremental (IXFR) transfers be enabled when accessing our DNS Firewall feeds. This will ensure that only the most up to date information is provided. This setting is enabled in your named.conf file:

```
options {
                ixfr-from-difference yes;
};
```

Deteque Free Threat Feeds Setup

2.6 Enabling DNS Firewall

The last step is adding response policy to your named.conf file:

```
options {
        response-policy {

                        zone “local.rpz”;
                        zone “drop.rpz.spamhaus.org" POLICY PASSTHRU;
                        zone “cryptominers.rpz.spamhaus.org” POLICY
PASSTHRU;
                        };
};
```

Quick Tip
Run any new DNS Firewall feed in POLICY PASSTHRU for 10 to 14 days. This will allow logs to still be generated for the rewrites that would have happened if the feed was enforcing. With this information you will know if there are any impacted sites on the feed.

In this configuration POLICY PASSTHRU is included in enabling DNS Firewall. With passthru no enforcement will take place but the action of the passthru will be logged. In order to enforce the entires in a given zone POLICY PASSTHRU should be removed.

2.7 Testing

Now that DNS Firewall is enabled in your BIND configuration, testing that everything is setup correctly should be done. There are a few ways to test if DNS Firewall is working as intended, by command line, browser, or checking logging.

To test via command line running an nslookup or dig command will return NXDomain or does not exist depending on what OS you are using to test.

Testing in a browsers will return "This site cannot be reached", "This webpage is not available" or similar.

With logging you will need to check your rpz.log file located in /var/named. Note that you will only get a result if you attempted to access something that is contained in one of your zones.

When testing in a browser or via command line, if there is resolution of the domain or IP address there is a misconfiguration in your DNS Firewall. (Remember to remove POLICY PASSTHRU when testing if resolution is being blocked)