DNS Firewall Setup Instructions

1. DNS Firewall Zone Descriptions and Master Information

Deteque currently offers 13 DNS Firewall Threat Feeds that are split up into 5 categories:

- Standard
- Malware
- Abused
- Diverse
- ZRD

Quick Tip

You can find out which feeds you are subscribed to in your control panel under Installation and Support. To add additional feeds you will need to reach out to your reseller team.

1.1 Summary of Categories and Zones

Standard Category

- Domain Block List (DBL)

The DBL zone is based on the Spamhaus DBL. It includes domains used as spam sources and senders, known spammers and spam gangs, phishing, virus and malware-related sites.

- Bad Name Servers

Name servers that are being used almost exclusively for the purposes of hosting domains that contain and distribute malware and/or spam.

Malware Category

- Malware

A subset of the DBL zone containing domains that are associated with malware. Spam, phishing, and redirector sources are excluded from this list.

- Botnet Command & Controllers (Botnet C&C)

IPs that have been identified as known Botnet C&C servers. Any machine resolving domains pointing to an IP listed in this zone has been compromised and is hosting malware for distribution.

- Malware-Adware

Domains or IPs that have become infected with adware that attempts to install on additional servers and/or workstations.

- Malware-Aggressive

Similar to the Malware Zone except additional checks are applied and this zone includes domains that are not yet listed within the DBL or malware zones. Due to the aggressive nature of this zone, there is the potential for a slightly higher chance of false positives.

- Botnet C&C-Aggressive

This zone includes IPs that are not yet listed in the Botnet C&C zone but are associated with servers that are showing signs of being infected with Botnet malware and have had additional tests applied to them. Due to the aggressive nature of this zone, there is the potential for a slightly higher chance of false positives.

Quick Tip

You may notice that some zones have a higher potential for false positives.

The data that we do provide is run through multiple tests to prevent this from occurring, however with the more aggressive zones that are offered there is a higher potential for this to happen.

It is suggested that with these zones you implement them on a corporate network that would only impact employees and not customers/end users.

Abused Category

- Abused-legit

Servers and domains that once were deemed legitimate but are now showing signs of compromise.

- Ad servers

A collected list of ad servers. This zone behaves like an ad blocker and will block the specific ad servers at the network level.

Note: this list may cause websites to not load and should be used with caution.

- Bogon

A Bogon is unallocated IP space. This list includes Bogon ranges that are exhibiting signs of malicious activity.

Quick Tip

If you use ACLs in your BIND configuration you could consider defining Spamhaus' Master Zones in an ACL and when you define your slave zones you can use the ACL name for the masters instead of entering IPs.

Diverse Category

- Spam block list (SBL)

The SBL zone is based on the Spamhaus SBL mail blocklist. This list includes IPs that are found to be hosting spammers, malware, phishing, ransomware, virus, and redirectors.

- Tor Exit Nodes

Tor is a web proxy that allows for anonymous web requests. IPs is this zone have been identified as malicious Tor Exit Nodes.

- Crypto miners

Blocks crypto mining networks using browser-based code to hijack processing power.

Zero Reputation Domains (ZRD) Category

- ZRD

Blocks connections to newly-registered, previously dormant domains for 24 hours. Domains are removed after 24 hours or transferred to another zone feed based on reputation assessment.

1.2 Master Zone Information

You will need to setup your local recursive resolver to act as a secondary for the Deteque's zones.

Please reach out to your authorized reseller/partner for the specific information regarding Deteque's Master Zoner servers.

Quick Tip

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

1.3 Threat Feed List

Based on the zone categories you have subscribed to, include the relevant names in your **named.conf,** when defining your slaved zones:

DBL	dbl.rpz.spamhaus.org
Bad Nameservers	bdns.rpz.spamhaus.org
Malware	malware.rpz.spamhaus.org
Botnet C&C	botnetcc.rpz.spamhaus.org
Malware-Adware	malware-adware.rpz.spamhaus.org
Malware-Aggressive	malware-aggressive.rpz.spamhaus.org
Botnet C& C-Aggressive	botnetcc_aggressive.rpz.spamhaus.org
Abused-Legit	abused-legit.rpz.spamhaus.org
Adservers	adservers.rpz.spamhaus.org
Bogon	bogon.rpz.spamhaus.org
SBL	sbl.rpz.spamhaus.org
Cryptominers	cryptominer.rpz.spamhaus.org
Tor Exit Nodes	tor-exit-nodes.rpz.spamhaus.org
ZRD	zrd.rpz.spamhaus.org

2. Configuring BIND for DNS Firewall and Deteque Threat Feeds

2.1 Install/upgrade to the most recent version of BIND

Before you begin to implement DNS Firewall in your BIND install it is recommended that you upgrade to the most recent version of BIND. We suggest that the upgrade be acquired directly from ISC (https://www.isc.org/downlaods/bind/) instead of updating from a software repository. This will safeguard against downloading an out of date version, as some repositories are not regularly updated. By taking these measures you 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, **RPZ 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; };
};
```

With these settings your log file output for a DROP rewrite should look like the following:

Note: 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.

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

Quick Tip

When operating multiple feeds always put your local zone first since this will allow you to make exceptions and also mitigate any issues quickly. After the local zone list from most egregious to least.

Run any new DNS Firewall feed in POLICY RPZ-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 impactful sites on the feed.

2.3 Creating a Local Zone

A local Zone is needed for creating exceptions (passthru) to DNS Firewall feeds that you have subscribed to and also to create additional blocking 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
baddomain.comIN CNAME       .               ;local block against
baddomain.com
*.baddomain.com         IN CNAME        .       ;local block against
*.baddomain.com
```

*Note: you can name your local zone whatever you wish, just change **local.rpz** to what you wish to name your local zone file.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.

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 a DNS RPZ feed.

2.4 Defining Master and Slave Zones

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

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

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

```
zone “dbl.rpz.spamhaus.org” {
                type slave;
                file “dbl.rpz.spamhaus.org”;
                masters { MASTER ZONE IPS };
                allow-transfer { none; };
                allow-query { localhost; };
};
```

Next your slave zones will need to be defined and will look like the following:

Since the slave zones are not located locally on the server the masters must be defined in every slave zone. Furthermore the slave zones will be set to “localhost” for query. Please reference section 1.3 Zone list for the zone names.

2.5 Enabling IXFR zone transfers

DNS Firewall is designed to provide updates to malicious threats as continuously as possible, therefore it is required that incremental (IXFR) transfers be enabled when accessing our DNS Firewall feeds. This will

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

make certain that only the most up to date information is provided. This setting is enabled in your **named.conf** file:

When testing be careful if visiting a site that may have malware on it. The best course of action when doing browser testing is a virtual machine that can be deleted in the case of it becoming infected.

```
options {
        response-policy {
                        zone “local.rpz”;
                        zone “drop.rpz.spamhaus.org” POLICY
PASSTHRU;
                        zone “dbl.rpz.spamhaus.org” POLICY PASSTHRU;
        };
};
```

Quick Tip

When testing be careful if visiting a site that may have malware on it. The best course of action when doing browser testing would be a virtual machine that can be deleted in the case of it getting infected.

2.6 Enabling DNS Firewall

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

*Note: in this configuration **POLICY RPZ-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 entries in a given zone P**OLICY RPZ-PASSTHRU** should be removed.*

2.7 Testing

Once DNS Firewall is enabled in your BIND configuration, testing should take place immediately to check that the set-up is correct and working. There are various ways to test if the DNS Firewall is working as intended: by command line, browser, or by checking the logging.

i. **Command Line -** run an **nslookup** or **dig** command which will return **NXDomain** or **does not exist,** depending on what OS you are using to test.

ii. **Browsers -** these will return "This site cannot be reached", "This webpage is not available" or similar.

iii. **Logging** - check your **rpz.log** file located in **/var/named**.

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. N.B. Remember to remove **POLICY PASSTHRU** when testing if resolution is not blocked.