DNS Firewall (RPZ) Setup Instructions with Bind

1. DNS RPZ Zone Descriptions and Master Information

1.1. Summary of Categories and Zones

Coinblocker*
(coinblocker.srv)
Multiple lists of IP addresses and domains that are hosting crypto-jacking scripts, which utilize the resources of an end user's computer to mine crypto-currency.

1.2 Master Servers information

Master Server IP : 45.77.35.92

1.3 Preparation at User(Customer) end

User need to share his current recursive nameserver IP.If recursive nameserver IP remain under NAT ,It require to share the public IP.

Please check your current IP from your linux terminal using:

$wget -qO- icanhazip.com

Please check you have shared correct public IP with Pipeline Security.

*Communication with masters will be established on TCP 53 port. Its require to open this port towards master destination IPs if there is any firewall in place.

2. Configuring BIND for DNS Firewall (RPZ) with Pipeline zone feeds

After installation or if you already have existing installation check bind version,(Bind version 9.8 or later required for DNS firewall (RPZ)) :

```
$named -v
BIND 9.11.3-1ubuntu1.9-Ubuntu (Extended Support Version)
```

All the configuration files of BIND 9 is in **/etc/bind** and **/var/cache/bind** directory by default.

Now configure add the policy zones in options of Bind configuration.
A local policy zone file rpz.local has used to use for custom policy. Bind supports 32 policy zones.

```
root@rpz01:~# vim /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";
        recursion yes;
        dnssec-validation auto;
        allow-query { localhost; };
        allow-recursion { localhost;  };
        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
response-policy {
zone "rpz.local";
### threat Feeds
zone "coinblocker.srv" ;

};
};
```

Configure the zones in named.conf file to transfer from masters.

```
root@rpz01:~# vim /etc/bind/named.conf
zone "rpz.local" {
type master;
file "rpz.local";
allow-query { localhost; };
};
zone "coinblocker.srv" {
type slave;
file " coinblocker.srv ";
masters {xx.xx.xx.xx;};
allow-query { localhost; };
};
```

Add all the zone names in the /etc/bind/named.conf file according to the zone names in /etc/bind/named.conf.options.

2.2. Configure Bind logging for DNS Firewall (RPZ)

For Debian/Ubuntu add the configuration for logging

```
vim /etc/bind/named.conf
logging {
channel null {
null; };
channel bindlog {
        file "bind.log";
        print-time yes;
        print-category yes;
        print-severity yes;
        severity info;
};
```

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

category default { bindlog; };
category general { bindlog; };
category database { null; };
category config { bindlog; };
category resolver { bindlog; };
category xfer-in { bindlog; };
category xfer-out { bindlog; };
category notify { null; };
category client { null; };
category unmatched { null; };
category network { null; };
category update { bindlog; };
category update-security { null; };
category queries { bindlog; };
category dispatch { null; };
category lame-servers { null; };
category delegation-only { bindlog; };
category edns-disabled { null; };
category rpz { rpzlog; };
};
```

```
root@rpz01:~# named-checkconf /etc/bind/named.conf
```

It will not show anything if there is no error.So you are okay if you can't see any error.named-checkconf only can check general procedural errors and it can't fix ny errors.

2.3 Configure local policy zone (rpz.local)

Local RPZ zone file (here it is rpz.local) is a zone file created by the user by his own. It can be used as custom policy zone file for:

- False positive
- For the purpose to apply custom policy for regulation or for any other reason.

```
#vim /var/cache/bind/rpz.local

$TTL 60
@          IN    SOA  localhost. root.localhost.  (
                      7   ; serial
                      3H  ; refresh
                      1H  ; retry
                      1W  ; expiry
                      1H ) ; minimum
               IN    NS    localhost.
infected34346x.com    IN CNAME .    ;Block the domain
coinbase.com CNAME rpz-passthru.  ;Allow the domain
*.coinbase.com CNAME rpz-passthru.  ;Allow all the sub domains
```

Finalize Implementation:

```
root@rpz01:~# systemctl reload bind9
root@rpz01:~# systemctl restart bind9
```

Now need to check the bind log . For a successful zone transfer it will show the transfers. Check the transfers for every zone.

```
root@rpz01:~# tail -f /var/cache/bind/bind.log
16-Oct-2019 15:13:40.445 xfer-in: info: transfer of 'zrd.host.dtq/IN' from
xx.xx.xx.xx#53: connected using zz.zz.zz.zz#37445
16-Oct-2019 15:13:43.405 general: info: zone zrd.host.dtq/IN: transferred serial
8581296321
16-Oct-2019 15:13:43.406 xfer-in: info: transfer of 'zrd.host.dtq/IN' from
xx.xx.xx.xx#53: Transfer status: success
16-Oct-2019 15:13:43.406 xfer-in: info: transfer of 'zrd.host.dtq/IN' from
xx.xx.xx.xx#53: Transfer completed: 885 messages, 430817 records, 8641970 bytes,
2.960 secs (2919584 bytes/sec)
```

3. Testing-

Now test the service with a test domain.

```
root@rpz01:~# dig @localhost www.minez.zone
```