# Managing DNS Firewall



# Managing DNS Firewall

DNS firewall controls the domain names, IP addresses, and name servers that are allowed to function on the network. This enables Internet Service Providers (ISP), enterprises, or organizations to define lists of FQDNs, IP addresses, subnets and prefixes of end nodes, and configure rules to secure the network by redirecting the resolution of DNS name away from known bad domains or non-existing domains (NXDOMAIN).

Every query to a Caching DNS server is first verified against the list of DNS firewall rules in the order of priority. To ensure that the caching DNS server redirects queries for non-existing or known bad domains, you can create DNS firewall rules. The DNS firewall rule comprises of a priority, an ACL, an action, and a list of domains and takes precedence over exceptions and forwarders. You can configure the following actions for these queries:

- **Drop** - Drops the resource record query.
- **Refuse** - Responds with no data and the REFUSED status.
- **Redirect** - Redirects A or AAAA queries to the specified IP address.
- **Redirect-nxdomain** - Redirect to a specific A or AAAA address if the queried domain does not exist.
- **RPZ** - Use Response Policy Zones (RPZ) rules.

When a resource record query matches the criteria of rule, the specified action is taken. If the resource record query action results for redirect-nxdomain, the query is performed in the normal process and if it results in an NXDOMAIN status, then it is redirected to the specified destination.

**Note** The firewall rules such as Drop, Refuse, Redirect, and the RPZ query-name trigger take place before regular query processing and therefore take precedence over forwarders and exceptions. The other actions and triggers are applied during or after regular query processing.

### DNS Response Policy Zone (RPZ) Firewall Rules

Cisco Prime Network Registrar 8.3 and later supports Response Policy Zones (RPZ). The DNS firewall rules can be set up for specially designated zones on the Authoritative DNS server. The RPZ and RR data combined

with DNS resolver effectively creates a DNS Firewall to prevent misuse of the DNS server. The RPZ firewall rule comprises of a trigger (query-name, ip-answers, ns-name, and ns-ip) and a corresponding action.

The RPZ firewall rules utilize both the Authoritative DNS and the Caching DNS servers to provide the RPZ functionality. The Authoritative DNS server stores the data for RPZ and the rules whereas the Caching DNS server takes the client queries and applies these rules.

### DNS RPZ Zones

We recommend that you create a separate forward zone on the authoritative server for RPZ. The zone can be either primary or secondary and the data can either be manually entered or transferred from a third party RPZ provider. The zones can be named as **rpz.<customer-domain>** to avoid conflict with domain names in the Global DNS space. In Query Settings, enable the RPZ to make this domain as RPZ domain.

**Note** If the RPZ comes via zone transfer it must be named the same as at the source. If using a commercial RPZ provider, the name is specified by the provider.

The RPZ RR names can take the following forms:

***Table 1: RPZ Triggers***

| RPZ Trigger | RR Name | Example | Example RR Name |
|---|---|---|---|
| Domain being queried | <domain>.rpz.<customer-domain> | Domain www.baddomain.com | www.baddomain.com.rpz.cisco.com |
| Name Server to query | <ns-domain-name>.rpz-nsdname.rpz.<customer-domain> | Name Server ns.baddomain.com | ns.baddomain.com.rpz-nsdname.rpz.cisco.com |
| Name Server IP to query | 32.<reversed-ip>.rpz-nsip.rpz.<customer-domain> | Name Server Address 192.168.2.10 | 32.10.2.168.192.rpz-nsip.rpz.cisco.com |
| Name Server IP to query | 32.<reversed-ip>.rpz-nsip.rpz.customer-domain> | Name Server Address 2001:db8:0:1::57 | 128.57.zz.1.0.db8.2001.rpz-nsip.rpz.cisco.com |
| A Records in Answer Section of Response | 32.<reversed-ip>.rpz-ip.rpz.<customer-domain> | A answer record 192.168.2.10 | 32.10.2.168.192.rpz-ip.rpz.cisco.com |
| A Records in Answer Section of Response | <subnet-mask>.<reversed-ip>.rpz-ip.rpz.<customer-domain> | A answer record in subnet 192.168.2.0/24 | 24.0.2.168.192.rpz-ip.rpz.cisco.com |
| AAAA Records in Answer Section of Response | 128.<reversed-ip>.rpz-ip.rpz.<customer-domain> | AAAA answer record 2001:db8:0:1::57 | 128.57.zz.1.0.db8.2001.rpz-ip.rpz.cisco.com |

| | | | |
|---|---|---|---|
| AAAA Records in Answer Section of Response | <prefix-length>.<reversed-ip>.rpz-ip.rpz.customer-domain> | AAAA answer record in prefix 2001:db8.0.1::/48 | 27.zz.1.0.db8.2001.rpz-ip.rpz.cisco.com |

This zone contains all the RRs related to black listing query names. Blocking IP addresses and ranges must be done within the rpz-ip label (i.e. rpz-ip.rpz.cisco.com). The same logic can be applied to blocking name servers using the rpz-nsdname and rpz-nsip labels.

**Note** rpz-ip, rpz-nsdname, and rpz-nsip are just another label and is not a real subdomain or separate zone. No delegation points will exist at this level and CDNS relies on finding all the data within the referenced zone.

**Note** When using rpz-nsdname and rpz-nsip, the corresponding rule is applied to the original query and will therefore change the answer section. In cases when the final answer is determined from the RPZ rule(s), the rpz zone SOA will be included in the authority section.

When the Caching DNS server is configured to use RPZ, it queries the Authoritative DNS server to lookup the RPZ rules. The Caching DNS server formulates the correct query name, interprets the query response as an RPZ rule, and applies the rule to the client query. If the RPZ rule causes Caching DNS server to rewrite the client response, this data is cached to make future lookups faster. The Caching DNS server RPZ configuration determines which RPZ trigger should be used. If no RPZ rule is found, the query proceeds normally.

In addition, RPZ overrides can be configured on the Caching DNS server. This enables the Caching DNS server to override the RPZ action returned by the Authoritative DNS server. This is useful when you do not have control over the Authoritative DNS data as is the case when the data is pulled from a third party. When the Caching DNS server gets a match from the Authoritative DNS server for the RPZ query, it performs the override action rather than the rule action specified in the RR data.

### DNS RPZ Actions

RPZ rules are created using standard DNS RRs, mostly CNAME RRs. However, for redirecting you can use any type of RR. The RR name follows the format based on the RPZ trigger as described in the Table 1: RPZ Triggers, on page 2 section. The rdata defines the rule action to be taken. The following table describes the RPZ actions.

***Table 2: RPZ Actions***

| RPZ Rule Action | RPZ RR RData | RPZ RR Example |
|---|---|---|
| NXDOMAIN | CNAME . | www.baddomain.com.rpz.cisco.com. 300 CNAME . |
| NODATA | CNAME *. | www.baddomain.com.rpz.cisco.com. 300 CNAME *. |

| | | |
|---|---|---|
| NO-OP (whitelist) | CNAME rpz-passthru.<br>CNAME FQDN | www.gooddomain.com.rpz.cisco.com. 300 CNAME rpz-passthru.<br>www.gooddomain.com.rpz.cisco.com. 300 CNAME www.gooddomain.com. |
| DROP | CNAME rpz-drop. | www.baddomain.com.rpz.cisco.com. 300 CNAME rpz-drop. |
| Redirect | <any RR type> <redirect-data> | www.wrongdomain.com.rpz.cisco.com. 300 CNAME walledgarden.cisco.com.<br>www.baddomain.com.rpz.cisco.com. 300 A 192.168.2.10<br>www.baddomain.com.rpz.cisco.com. 300 AAAA 2001:db8:0:1::57 |

### DNS RPZ Best Practices

- CPNR Authoritative DNS and Caching DNS are used for end to end RPZ solutions.
- The ***restrict-query-acl*** on the RPZ zone must include only the Caching DNS address and localhost.
- Zone transfers ( ***restrict-xfer-acl*****)** must be either completely denied or restricted only to a specific set of servers.
- RPZ zone must not be delegated from the parent zone. It must be hidden and only available to a specially configured Caching DNS.
- There must be no RPZ nameserver address record to avoid caching and keeping the name server.
- The name server record must point to "localhost".
- The number of RPZ Firewall entries on a CDNS server should be limited to 2-3. The time to process a query increases linearly for each RPZ Firewall entry specified.
- The default TTL, for manually created RPZ zones, must reflect the rate of change in the zone data. The recommended rate ranges from 5m to 2h.
- The Caching DNS server must revise its max-cache-ttl settings to assure that the cached information is from a reliable source and can be trusted. This setting should be in line with the default TTL of 5m to 2h.
- The Authoritative DNS servers must enable NOTIFY, IXFR, AXFR and TSIG for zone transfers of distributed RPZ data.

# Setting Up DNS Firewall Rules

To add or edit DNS firewall rules:

## Local Basic or Advanced Web UI

**Step 1** From the **Design** menu, choose **DNS Firewall** under the Cache DNS submenu to open the List/Add DNS Firewall Rules page.

**Step 2** Click the **Add DNS Firewall Rule** icon in the DNS Firewall pane to open the Add DNS Firewall dialog box.

**Step 3** Enter a rule name in the Rule Name field and specify the action type.

**Note** The drop and refuse actions are applicable to all the queries for the specified domains, while the redirect and redirect-NXDOMAIN rules are applicable only to the queries of A and AAAA records.

**Step 4** Click **Add DNS Firewall** to save the firewall rule. The List/Add DNS Firewall Rules page appears with the newly added firewall rule.

**Note** The rules with the action **refuse** do not use a domain or destination IP address.

**Step 5** If you selected the **drop** or **redirect** action:

- Enter the ACL List, and click the **Add** icon to add the domains that need to be monitored for the drop or redirection
- For the **redirect** action, you also need to enter the IPv4 Destination or IPv6 Destination.

**Step 6** If you selected the **rpz** action:

**a.** Enter the RPZ Zone Name and the name of RPZ server.

**Note** The recommended RPZ zone name should be **rpz.<customer-domain>** to avoid conflicting with domain names in the Global DNS space.

**b.** Select the RPZ Trigger from the options and the corresponding override action.

**Step 7** Click **Save** to save your settings, or click Revert to cancel the changes.

**Note** To delete a DNS Firewall rule, select the rule on the DNS Firewall pane, click the **Delete** icon, and then confirm the deletion.

## CLI Commands

Use the following CLI commands to:

- Add the DNS firewall rules, separated by spaces, use **cdns-firewall** *rule-name* **create**.
- List the domains the domain redirect rule, use **cdns-firewall list**.
- Remove domain redirect rule, use **cdns-firewall** *rule-name* **delete**.

## Changing Priority of DNS Firewall Rules

When you create a set of DNS firewall rules, you can specify the priority in which order the rules will apply. To set the priority or reorder the rules:

**Step 1** From the **Design** menu, choose **DNS Firewall** under the Cache DNS submenu to open the List/Add DNS Firewall Rules page.

**Step 2** Click the **Reorder DNS Firewall Rules** icon in the DNS Firewall pane to open the Reorder dialog box.

**Step 3** Set the priority for the DNS Firewall rules by either of the following methods:

- Select the rule and click the Move up or Move down icon to reorder the rules.
- Select the rule and click the Move to button, and enter the row number to move the rule.

**Step 4** Click **Save** to save the reordered list.