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**—Redirects to a specific A or AAAA address if the queried domain does not exist.
- **RPZ**—Uses RPZ rules.

When the incoming query matches the DNS firewall rule, the specified action will be taken unless the rule is for redirect-nxdomain. A redirect-nxdomain rule takes effect only for incoming queries that would result in an NXDOMAIN response.

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 RPZ Firewall Rules

Cisco Prime Network Registrar supports 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 rules utilize both the Authoritative DNS and Caching DNS servers to provide the RPZ functionality.

RPZ - Cache DNS

From CPNR 11.2, CDNS queries ADNS for RPZ rule data using zone transfers or notifies and operate on the rule data locally.

The rpz-trigger in the firewall object is removed. Because the data is available locally, this feature greatly increases the performance of processing RPZ data.

Note The *nrcmd> cdns execute* expert mode command will have a new option, *transfer-zone*. It takes the name of an RPZ as parameter. This command causes CDNS to start a probe for any changes to the specified RPZ. For example:

```
nrcmd> cdns execute transfer-zone rpz.example.com
```

When a query received from client for www.example.com, then CDNS can operate on the rule data locally without querying ADNS.

RPZ - Authoritative DNS

We recommend that you create a separate forward zone on the Authoritative DNS 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 the zone's **Query Settings** section, enable the *rpz* attribute to make it an RPZ.

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.

Each policy consists of a trigger and an action. The trigger describes when the policy should be applied. The action describes what action should be taken if the policy needs to be applied.

In RPZ zone, each trigger and action combination is defined as a Resource Record (RR). The owner of the RR states the trigger, and the type, and RDATA state the action.

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
Client IP	<subnet-mask>.<client-ip>.rpz-client-ip.<customer-domain>	Client IP in the subnet 192.0.2.0/24	24.0.2.0.192.rpz-client-ip.rpz.cisco.com
Client IP	<client-ip>.rpz-client-ip.<customer-domain>	Client IP 192.2.0.64	64.2.0.192.rpz-client-ip.rpz.cisco.com

This zone contains all the RRs related to query names which are in block list. Blocking IP addresses and ranges must be done within the *rpz-ip* label (that is, rpz-ip.rpz.cisco.com). The same logic can be applied to blocking name servers and clients using the *rpz-nsdname*, *rpz-nsip*, and *rpz-client-ip* labels.

Note *rpz-ip*, *rpz-nsdname*, *rpz-nsip*, and *rpz-client-ip* are just another labels and are not real subdomains or separate zones. No delegation points will exist at this level and Caching DNS server 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 SOA will be included in the authority section.

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. Based on the RPZ zone data, the CDNS server applies the triggers and actions. 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 (allowed list)	CNAME rpz-passthru. CNAME FQDN	www.gooddomain.com.rpz.cisco.com. 300 CNAME rpz-passthru. 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. www.baddomain.com.rpz.cisco.com. 300 A 192.168.2.10 www.baddomain.com.rpz.cisco.com. 300 AAAA 2001:db8:0:1::57

DNS RPZ Requirements and Best Practices

- All RPZs must have the *rpz* attribute enabled. A DNS reload is necessary for this change to take effect.

- Both Cisco Prime Network Registrar Authoritative DNS and Caching DNS must be used for end to end RPZ solutions.
- The *restrict-query-acl* on the RPZ 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 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 rules on a Caching DNS server should be limited to 2-3. The time to process a query increases linearly for each RPZ Firewall rule specified.
- The default TTL, for manually created RPZs, 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* setting 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 the distributed RPZ data.
- An RPZ may contain data for domains (allowed list or block list), but can also be separated into two distinct zones. This can be helpful when there is overlapping data or the block list zone is maintained by a third party (that is, RPZ subscription).

Setting Up RPZ Primary Zones on the Authoritative DNS Server

Local Web UI

Step 1 From the **Design** menu, choose **Forward Zones** under the **Auth DNS** submenu to open the List/Add Forward Zones page.

Step 2 Click the **Add Forward Zone** icon in the **Forward Zones** pane to open the Add Zone dialog box

Step 3 Enter the name of the zone (that is, **rpz.***zonename*), specify **localhost** as the name server, add a contact E-mail, and a starting serial number.

Step 4 Make the following changes in the Edit Zone page:

a) Set the Zone Default TTL (recommended setting is between 5m and 2h).

b) Under the **Query Settings** section, set the *rpz* attribute to **true** and restrict queries using the *restrict-query-acl* attribute.

Note Queries should be restricted to localhost and the Caching DNS server address(es), **restrict-query-acl=localhost, *cdns-address*)**.

c) Under the **Zone Transfer Settings** section, restrict zone transfers and notifies.

Note Zone transfers and notifies should only be allowed to other RPZ secondaries and localhost.

Step 5 From the **Deploy** menu, choose **DNS Server** under the **DNS** submenu to open the Local DNS Server page.

Step 6 Click the **Restart Server** icon to reload the DNS server and publish the RPZ.

CLI Commands

Use the following CLI commands:

- To create an RPZ, the zone name should indicate that it is an RPZ. For example, rpz.example.com.

```
nrcmd> zone rpz.example.com. create primary localhost admin
```

- Enable the RPZ attribute (*rpz*).

```
nrcmd> zone rpz.example.com. enable rpz
```

- Restrict queries to only be allowed from Caching DNS and localhost.

```
nrcmd> zone rpz.example.com. set restrict-query-acl="localhost, cdns-server"
```

- Restrict or completely deny zone transfers depending on deployment.

```
nrcmd> zone rpz.example.com. set restrict-xfer-acl=none
```

- Set the default TTL between 5m and 2h.

```
nrcmd> zone rpz.example.com. set defttl=5m
```

- Reload the DNS server to publish the RPZ and for the configuration changes to take effect.

```
nrcmd> dns reload
```

Setting Up DNS Firewall Rules

To add or edit DNS firewall rules:

Local Advanced and Regional 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:

- Enter the RPZ name and the name of RPZ server.

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

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

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 **cdns-firewall** *rule-name* **create** to add the DNS firewall rules, separated by spaces.

Use **cdns-firewall list** to list the domains the domain redirect rule.

Use **cdns-firewall** *rule-name* **delete** to remove domain redirect rule.

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.

Note When using more than one DNS firewall rule, it is recommended to set the rules priority to control the order in which rules are processed. The lowest non-zero priority will be processed first. DNS firewall rules with a priority of 0 (default), will be processed last.

Local Advanced and Regional Advanced Web UI

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.

CLI Commands

Use **cdns-firewall** *name* **set priority**=*value* to specify the rule priority relative to the other rules.

Enabling TLS for RPZ

Starting from Cisco Prime Network Registrar 11.0, the Caching DNS Firewall RPZ action supports TLS for communication with the RPZ server.

Local Advanced and Regional Advanced Web UI

To enable TLS for the RPZ server, do the following:

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 Enable the *rpz-tls* attribute by selecting the **enabled** option. If you enable this, you should configure a tls-cert-bundle to load the CA certificates, otherwise the connections cannot be authenticated.

The *rpz-tls-auth-name* attribute defines the auth name for the RPZ server. If TLS is enabled, the Caching DNS server checks the TLS authentication certificates with that name sent by the RPZ server.

CLI Command

Use **cdns-firewall** *name* **set rpz-tls=true** to enable TLS for the RPZ server.