DNS ファイアウォールの管理

DNS ファイアウォールの管理

DNS ファイアウォールは、ネットワーク上で機能することが許可されているドメイン名、IP アドレス、およびネームサーバーを制御します。これにより、インターネット サービス プロバイダ（ISP）、企業、または組織は、FQDN、IP アドレス、サブネット、およびエンド ノードのプレフィックスのリストを定義し、既知の不正ドメインまたは存在しないドメイン（NXDOMAIN）からのDNS名の解決をリダイレクトすることでネットワークを保護するルールを設定できます。

キャッシュ DNS サーバーへのすべてのクエリは、プライオリティに従い DNS ファイアウォール ルールのリストに照らして最初に確認されます。キャッシング DNS サーバーが存在しないドメインまたは既知の不正ドメインに対するクエリを確実にリダイレクトするようにDNSファイアウォールルールを作成できます。DNS ファイアウォール ルールは、プライオリティ、ACL、アクション、およびドメイン リストで構成され、例外とフォワーダよりも優先されます。これらのクエリに対して、次のアクションを設定できます。

- **Drop**：リソースレコードクエリをドロップします。
- **Refuse**：データなしの [拒否（REFUSED）] ステータスで応答します。
- **Redirect**：指定された IP アドレスに A クエリまたは AAAA クエリをリダイレクトします。
- **Redirect-nxdomain**：照会されたドメインが存在しない場合に、特定の A アドレスまたは AAAA アドレスにリダイレクトします。
- **RPZ**：応答ポリシーゾーン（RPZ）のルールを使用します。

着信クエリが DNS ファイアウォール ルールと一致する場合は、redirect-nxdomain のルールでない限り、指定されたアクションが実行されます。redirect-nxdomain ルールは、NXDOMAIN 応答を生じさせる着信クエリにのみ適用されます。

（注） Drop、Refuse、Redirect、RPZ などのファイアウォール ルールは、通常のクエリ処理の前に行われるため、フォワーダと例外よりも優先されます。その他のアクションとトリガーは、通常のクエリ処理中またはその後に適用されます。

DNS RPZ ファイアウォールルール

Cisco Prime Network Registrar は RPZ をサポートしています。DNS ファイアウォール ルールは、権威 DNS サーバー上の特別に指定されたゾーンに対して設定できます。RPZ と RR データを DNS リゾルバと組み合わせることにより、DNS サーバーの不正使用を防ぐ有効な DNS ファイアウォールを構成できます。RPZ ファイアウォール ルールは、トリガー（query-name、ip-answers、ns-name、および ns-ip）と、対応するアクションで構成されます。

RPZ ファイアウォールルールは、権威 DNS サーバーとキャッシング DNS サーバーの両方を使用して RPZ 機能を提供します。権威 DNS サーバーは RPZ とルールのデータを保存します。キャッシュ DNS サーバーはクライアントクエリを受信してこれらのルールを適用します。

DNS RPZ ゾーン

RPZ の権威 DNS サーバーで個別の正引きゾーンを作成することを推奨します。ゾーンはプライマリまたはセカンダリのいずれかになります。また、データは手動で入力するか、サードパーティ RPZ プロバイダから転送できます。ゾーンには **rpz** という名前を付けることができます。*<customer-domain>* という名前を付けることで、グローバル DNS 空間のドメイン名との重複を回避できます。ゾーンの **Query Settings** セクションで *rpz* 属性を有効にすることで、そのゾーンは RPZ ゾーンになります。

（注） ゾーン転送で着信した RPZ は、送信元と同じ名前にする必要があります。商用 RPZ プロバイダを利用している場合、名前はプロバイダによって指定されます。

RPZ RR 名には、次の形式を使用できます。

表 *1 : RPZ* トリガー

RPZ トリガー	RR 名	例	RR 名の例
クエリ対象ドメイン	<domain>.rpz.<customer-domain>	ドメイン www.baddomain.com	www.baddomain.com.rpz.cisco.com
照会するネームサーバー	<ns-domain-name>.rpz-nsdname.rpz.<customer-domain>	ネームサーバー ns.baddomain.com	ns.baddomain.com.rpz-nsdname.rpz.cisco.com

DNS ファイアウォールの管理

照会するネームサーバー IP	32.<reversed-ip>.rpz-nsip.rpz.<customer-domain>	ネームサーバー アドレス 192.168.2.10	32.10.2.168.192.rpz-nsip.rpz.cisco.com
照会するネームサーバー IP	32.<reversed-ip>.rpz-nsip.rpz.customer-domain>	ネームサーバー アドレス 2001:db8:0:1::57	128.57.zz.1.0.db8.2001.rpz-nsip.rpz.cisco.com
応答の Answer セクションの A レコード	32.<reversed-ip>.rpz-ip.rpz.<customer-domain>	A 応答レコード 192.168.2.10	32.10.2.168.192.rpz-ip.rpz.cisco.com
応答の Answer セクションの A レコード	<subnet-mask>.<reversed-ip>.rpz-ip.rpz.<customer-domain>	サブネット 192.168.2.0/24 の A 応答レコード	24.0.2.168.192.rpz-ip.rpz.cisco.com
応答の Answer セクションの AAAA レコード	128.<reversed-ip>.rpz-ip.rpz.<customer-domain>	AAAA 応答レコード 2001:db8:0:1::57	128.57.zz.1.0.db8.2001.rpz-ip.rpz.cisco.com
応答の Answer セクションの AAAA レコード	<prefix-length>.<reversed-ip>.rpz-ip.rpz.customer-domain>	プレフィックス 2001:db8.0.1::/48 の AAAA 応答レコード	27.zz.1.0.db8.2001.rpz-ip.rpz.cisco.com

このゾーンには、ブラックリストのクエリ名に関連するすべての RR が含まれています。IP アドレスと範囲のブロッキングは *rpz-ip* ラベル内（つまり rpz-ip.rpz.cisco.com）で行われる必要があります。同じロジックを *rpz-nsdname* と *rpz-nsip* ラベルを使用してネームサーバーのブロッキングに適用できます。

（注） *rpz-ip*、*rpz-nsdname*、および *rpz-nsip* は、異なるラベルであり、実際のサブドメインまたは別のゾーンではありません。このレベルには委任ポイントが存在しません。キャッシング DNS は参照先ゾーン内の全データの検索に依存します。

（注） *rpz-nsdname* と *rpz-nsip* を使用する場合は、対応するルールが元のクエリに適用されるため、応答セクションが変更されます。最後の応答が RPZ ルールから決定された場合は、authority セクションには RPZ ゾーンの SOA が含まれます。

キャッシュ DNS サーバーが RPZ を使用するように設定されている場合は、権威 DNS サーバーにクエリを送信して RPZ ルールをルックアップします。キャッシュ DNS サーバーは、正しいクエリ名を作成し、クエリ応答を RPZ ルールとして解釈し、クライアント クエリにそのルールを適用します。RPZ ルールに基づいてキャッシュ DNS サーバーがクライアント応答を書き換えると、このデータはキャッシュされて、その後のルックアップが速くなります。キャッシュ DNS サーバー RPZ 設定によって、使用する RPZ トリガーが決まります。RPZ ルールが見つからない場合は、クエリは正常に進行します。

さらに、キャッシュ DNS サーバーで RPZ オーバーライドを設定できます。これにより、キャッシュ DNS サーバーは権威 DNS サーバーから返された RPZ アクションをオーバーライドできるようになります。これは、データがサードパーティからプルされる場合と同様に、権威 DNS データの制御がない場合に役立ちます。キャッシュ DNS サーバーは、RPZ クエリの権威 DNS サーバーから一致を取得すると、RR データで指定されたルール アクションではなく、オーバーライド アクションを実行します。

DNS RPZ アクション

RPZ ルールは標準 DNS RR（大抵は CNAME RR）を使用して作成されます。ただし、リダイレクトの場合は、任意のタイプの RR を使用できます。RR 名は「表 1 : RPZ トリガー （2 ページ）」の項で説明されている RPZ トリガーに基づく形式になります。rdata は、実行されるルール アクションを定義します。次の表で、RPZ アクションについて説明します。

表 *2 : RPZ* アクション

RPZ ルール アクション	RPZ RR RData	RPZ RR の例
NXDOMAIN	CNAME .	www.baddomain.com.rpz.cisco.com. 300 CNAME .
NODATA	CNAME *.	www.baddomain.com.rpz.cisco.com. 300 CNAME *。
NO-OP（ホワイトリスト）	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 の要件とベスト プラクティス

- すべての RPZ ゾーンで *rpz* 属性が有効になっている必要があります。変更を有効にするには、DNS のリロードが必要です。
- Cisco Prime Network Registrar 権威 DNS とキャッシング DNS の両方をエンドツーエンドの RPZ ソリューションに使用する必要があります。
- RPZ ゾーンの *restrict-query-acl* にはキャッシング DNS アドレスとローカルホストのみが含まれる必要があります。
- ゾーン転送（*restrict-xfer-acl*）は完全に拒否されるか、または特定のサーバーセットに制限される必要があります。
- RPZ ゾーンを親ゾーンから委任することはできません。これは非表示である必要があり、特別に設定されたキャッシュ DNS でのみ使用できます。
- RPZ ネームサーバーがキャッシュおよび保持されないように、ネームサーバーのアドレスレコードが存在しないようにする必要があります。
- ネームサーバー レコードは「localhost」を指している必要があります。
- キャッシング DNS サーバーの RPZ ファイアウォールルールの数は、2 ～ 3 に制限されている必要があります。RPZ ファイアウォール ルールの数が増えるにつれて、クエリの処理時間は直線的に増加します。
- 手動で作成された RPZ ゾーンのデフォルト TTL は、ゾーン データの変化のペースを反映する必要があります。推奨されるペースは 5 分～ 2 時間です。
- キャッシング DNS サーバーは、信頼性の高い送信元からの情報がキャッシュされ、信頼できるように、*max-cache-ttl* 設定を変更する必要があります。この設定は、デフォルト TTL の 5 分～ 2 時間に即している必要があります。
- 権威 DNS サーバーは、分散 RPZ データのゾーン転送のために NOTIFY、IXFR、AXFR、および TSIG を有効にする必要があります。
- RPZ ゾーンは、ホワイト リストとブラック リストに登録されたドメインのデータを含むことができますが、2 つの異なるゾーンに分けることもできます。これは、重複するデータがある場合や、ブラックリストゾーンがサードパーティによって維持されている場合（つまり RPZ サブスクリプション）に役立ちます。

権威 DNS サーバーでの RPZ プライマリ ゾーンの設定

ローカルの基本または詳細 Web UI

ステップ 1 [**デザイン**（**Design**）] メニューの [**認証DNS**（**Auth DNS**）]サブメニューの [**転送ゾーン**（**Forward Zones**）] を選択して、[転送ゾーンの一覧/追加（List/Add Forward Zones）] ページを開きます。

ステップ 2 [正引きゾーン（Forward Zones）] ペインの [正引きゾーン追加（Add Forward Zone）] アイコンをクリックして [ゾーンの追加（Add Zone）] ダイアログボックスを開きます。

ステップ 3 ゾーンの名前(つまり、**rpz.***zonename*)を入力します。ネームサーバーとして**localhost**を指定し、連絡先の電子メール、および開始シリアル番号を追加します。

ステップ 4 [ゾーンの編集（Edit Zone）] ページで、次の変更を行います。

a) [ゾーンのデフォルト TTL（Zone Default TTL）] を設定します（推奨設定は 5 分～ 2 時間）。

b) [クエリ設定（Query Settings）] セクションで *rpz* を **true** に設定し、*restrict-query-acl* 属性を使用してクエリを制限します。

（注） クエリは localhost とキャッシング DNS サーバーアドレス、**制限クエリー-acl = localhost**、***cdns* アドレス**に制限されている必要があります。

c) [ゾーン転送設定（Zone Transfer Settings）] セクション でゾーン転送と通知を制限します。

（注） ゾーン転送と通知は他の RPZ セカンダリおよび localhost にのみ許可される必要があります。

ステップ 5 [展開（Deploy）] メニューの [DNS] サブメニューで [DNS サーバー（DNS Server）] を選択して [ローカル DNS サーバー（Local DNS Server）] ページを開きます。

ステップ 6 [**サーバーの再起動（Restart Server）**] アイコンをクリックして、DNS サーバーをリロードし、RPZ ゾーンをパブリッシュします。

CLI コマンド

次の CLI コマンドを使用します。

- RPZ ゾーンを作成するには、そのゾーンが RPZ ゾーンであることを名前で示す必要があります。たとえば、rpz.example.com です。

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

- RPZ ゾーン属性（*rpz*）を有効にします。

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

- キャッシング DNS とローカルホストからのクエリのみを許可するように、クエリを制限します。

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

- 展開に応じてゾーン転送を制限または完全に拒否します。

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

- デフォルト TTL を 5 分 ～ 2 時間に設定します。

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

- 設定の変更を有効にするには、DNS サーバーをリロードして RPZ ゾーンをパブリッシュします。

```
nrcmd> dns reload
```

DNS ファイアウォール ルールの設定

次の手順で DNS ファイアウォール ルールを追加または編集します。

ローカルの基本または詳細 Web UI

ステップ 1 [設計（Design）] メニューで [DNS のキャッシュ（Cache DNS）] サブメニューの [DNS ファイアウォール（DNS Firewall）] を選択して [DNS ファイアウォールルールのリスト/追加（List/Add DNS Firewall Rules）] ページを開きます。

ステップ 2 [DNS ファイアウォール（DNS Firewall）] ペインの [**DNS ファイアウォール ルールの追加（Add DNS Firewall Rule**）] アイコンをクリックすると、[DNS ファイアウォールの追加（Add DNS Firewall）] ダイアログボックスが開きます。

ステップ 3 [ルール名（Rule Name）] フィールドにルール名を入力し、アクション タイプを指定します。

（注） **drop** および **refuse** アクションは、指定されたドメインのすべてのクエリに適用されます。一方、redirect および redirect-NXDOMAIN ルールは、A レコードと AAAA レコードのクエリにのみ適用されます。

ステップ 4 [**DNS ファイアウォールの追加（Add DNS Firewall**）] をクリックして、ファイアウォール ルールを保存します。新しく追加されたファイアウォール ルールが [DNS ファイアウォール ルールのリスト表示/追加（List/Add DNS Firewall Rules）] ページに表示されます。

（注） アクション **refuse** のルールには、ドメインまたは宛先 IP アドレスは使用されません。

ステップ 5 **drop** または **redirect** アクションを選択した場合：

- ACL リストを入力し、[追加（Add）] アイコンをクリックし、ドロップまたはリダイレクトをモニターする必要があるドメインを追加します。
- **redirect** アクションの場合は、IPv4 宛先または IPv6 宛先も入力する必要があります。

ステップ 6 **rpz** アクションを選択した場合：

1. RPZ ゾーン名と RPZ サーバー名を入力します。

   （注） RPZ ゾーンに **rpz.***customer-domain* という推奨名を付けることで、グローバル DNS スペースのドメイン名との競合を回避します。

2. オプションおよび対応するオーバーライド アクションから RPZ トリガーを選択します。

ステップ 7 [**保存（Save**）] をクリックして設定を保存するか、[**元に戻す（Revert**）] をクリックして変更をキャンセルします。

DNS ファイアウォールルールを削除するには、[DNS ファイアウォール（DNS Firewall）] ペインでルールを選択し、[削除（Delete）] アイコンをクリックした後、削除を確認します。

CLI コマンド

DNS ファイアウォールルールをスペースで区切って追加するには、**cdns-firewall** *rule-name* **create** を使用します。

ドメインリダイレクトルールのドメインのリストを表示するには、**cdns-firewall list** を使用します。

ドメインリダイレクトルールを削除するには、**cdns-firewall** *rule-name* **delete** を使用します。

DNS ファイアウォール ルールの優先順位の変更

DNS ファイアウォール ルールを作成するときに、ルールを適用する順位を指定できます。

（注） 複数の DNS ファイアウォール ルールを適用する場合は、ルールの処理順序を制御するためのルールプライオリティを設定することを推奨します。ゼロ以外の最も小さいプライオリティが最初に処理されます。プライオリティが 0（デフォルト）の DNS ファイアウォール ルールが最後に処理されます。

ローカルの基本または高度な Web UI

次の手順でプライオリティを設定するか、ルールの順序を変更します。

ステップ 1 [設計（Design）] メニューで [DNS のキャッシュ（Cache DNS）] サブメニューの [DNS ファイアウォール（DNS Firewall）] を選択して [DNS ファイアウォールルールのリスト/追加（List/Add DNS Firewall Rules）] ページを開きます。

ステップ 2 [DNS ファイアウォール（DNS Firewall）] ペインの [**DNS ファイアウォール ルールの順序変更（Reorder DNS Firewall Rules**）] アイコンをクリックすると、[順序変更（Reorder）] ダイアログボックスが開きます。

ステップ 3 次のいずれかの方法で、DNS ファイアウォールルールの優先順位を設定します。

- ルールを選択し、[上に移動（Move up）] または [下に移動（Move down）] アイコンをクリックして、ルールの順序を変更します。
- ルールを選択し、[移動先（Move to）] ボタンをクリックして、ルールを移動する行番号を入力します。

ステップ 4 [**保存（Save**）] をクリックして、順序を変更したリストを保存します。

CLI コマンド

cdns-firewall *name* **set priority**=*value* を使用して、他のルールに関連するルールの優先順位を指定します。