Infoblox
NEXT LEVEL NETWORKING

DEPLOYMENT GUIDE

Infoblox DNS Firewall with BloxOne Threat Feed

TABLE OF CONTENTS

Overview

Introduction

Infoblox DNS Firewall employs DNS RPZs (Response Policy Zones), a technology developed by ISC (Internet System Consortium) for allowing reputable sources to dynamically communicate domain name reputation so that you can implement policy controls for DNS lookups.

Concepts

- **BloxOne Threat Defense Cloud**: Infoblox solution which bundles the DNS Firewall, Infoblox Threat Intelligence Data Exchange (TIDE) and Infoblox Dossier services.
- **DNS Firewall**: Also referred to as **RPZ**, or **Response Policy Zones**. The engine which analyzes DNS traffic, categorizes it and applies a matching policy action.
- **Feed**: The threat data used for the categorization and application of policy data on DNS traffic.
- **Rule**: The policy action used to determine how a query should be processed.
- **TIDE**: The Infoblox Threat Intelligence Data Exchange. TIDE enables organizations to aggregate, curate and enable distribution of threat data.
- **Dossier**: A threat indicator research tool, which provides contextual information from multiple sources simultaneously.
- **Infoblox Data Connector**: Used to collect DNS query and response data from Infoblox Grid members and transfer this data to Infoblox Reporting in a managed fashion.

Prerequisites

The following items are required to use BloxOne feeds with DNS Firewall:

- One or more Infoblox appliances, which support the DNS license (installed in either in a single Grid, as standalone servers or a combination thereof).
- The Response Policy Zones license installed on each Infoblox server where DNS Firewall will be enabled.
- The DNS service must be started and in normal running condition.
- Access to the BloxOne feed (UDP and TCP port 53 between servers where the feed will be transferred from/to).
- Recursion enabled in order for rules to work properly.

Limitations

- DNS Firewall will not process queries sent from another Infoblox server which also the DNS Firewall service license is installed. The intention is that the DNS Firewall processing should only be performed once for a given query.
    - The DNS servers should be in the same Grid. If DNS servers are in different Grids they will always process the requests.
- Queries can timeout if DNS Firewall processing time exceeds the client's timeout limit.
- Grid replication is not supported for the transfer of feed data to Grid secondary name servers. Feeds are updated using DNS zone transfers.

Best Practices

- Anticipate that DNS performance for all queries, both authoritative and recursive, will be affected.

- DNS Firewall should not be enabled on multiple 'layers', such as on both client facing servers and forwarders.
- Employ multiple feeds to provide protection for as many different threat categories as possible. For performance reasons, only enable necessary local policies and feeds.
- Name Server Groups should be used when configuring Name Servers for local policies and feeds.
- Preview how rules will work prior to enforcing them by setting the **Policy Override** configuration to **Log Only (Disabled)** in the properties for your feed/local policy.
- Use the correctly sized Infoblox server for the services being deployed. Sizing recommendations can be found in step 1 of the **On-prem DNS Firewall Configuration**, which is documented in the **BloxOne Threat Feed** Configuration section below.

Use Cases

The following are common use cases for DNS Firewall with BloxOne feeds:

Automated malware protection

A common use case is to use a BloxOne Threat Feed to provide malware protection for clients on your network. By enabling DNS Firewall with BloxOne feed within your Grid, clients resolving DNS queries using these servers will be protected from known malicious sites with an extremely low false positive hit ratio. Using multiple BloxOne Threat Feeds for different categories provides more robust protection.

Blocking access to restricted sites

Many environments frequently require that access to restricted or sensitive sites are blocked and/or logged. DNS Firewall enables you to add local policies, providing the ability to add custom rules in addition to the BloxOne feed.

Whitelisting trusted sites

With local policies, access can be allowed to restricted sites when exceptions are required in conjunction with a BloxOne threat feed.

Reporting on potentially malicious traffic and infected clients

When malicious activity occurs on your network, detailed reports may be required.

Getting Started with BloxOne Threat Defense

Signing Up

BloxOne Threat Defense requires a subscription before it can be used. You can sign up for a subscription by requesting an evaluation at https://www.infoblox.com/products/bloxone-threat-defense or by purchasing a subscription. Contact Infoblox Sales (sales@infoblox.com) for more information on purchasing a subscription.

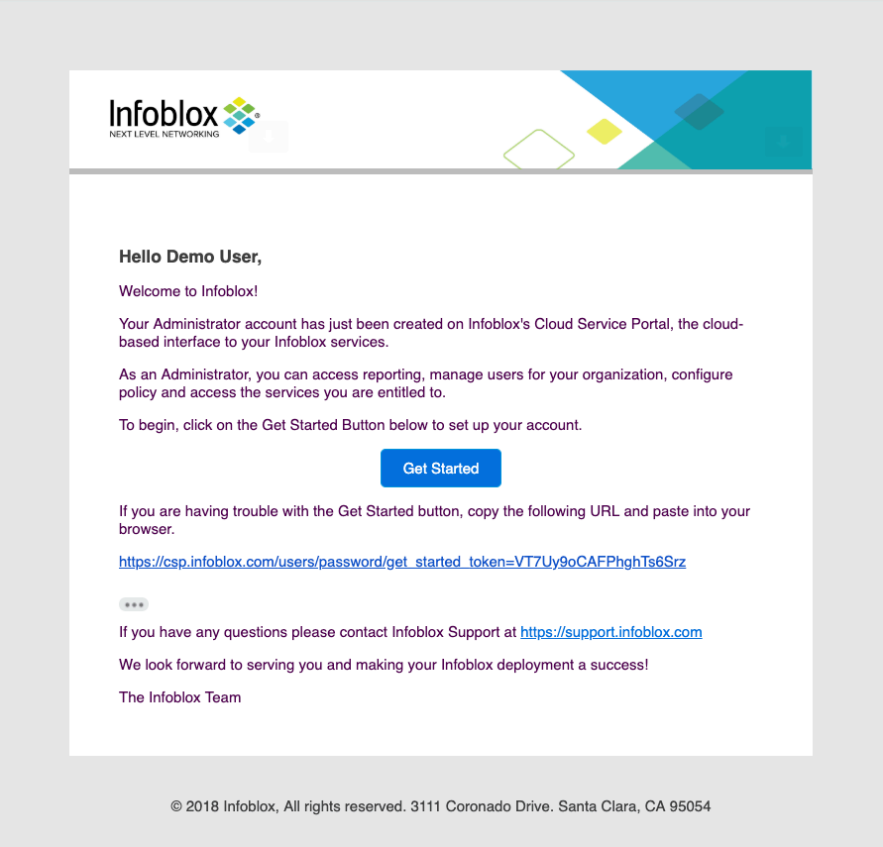
Managing BloxOne Threat Defense

Enable the Cloud Portal Manager

The Cloud Portal Manager enables administrators to manage their BloxOne Threat Defense subscriptions and users, threat intelligence data feeds and use the Threat Lookup Tool for clear and actionable threat data. Once your subscription to BloxOne Threat Defense has been activated, a notification email will be sent to the email address registered for that account. Enclosed in this notification email which is a link to

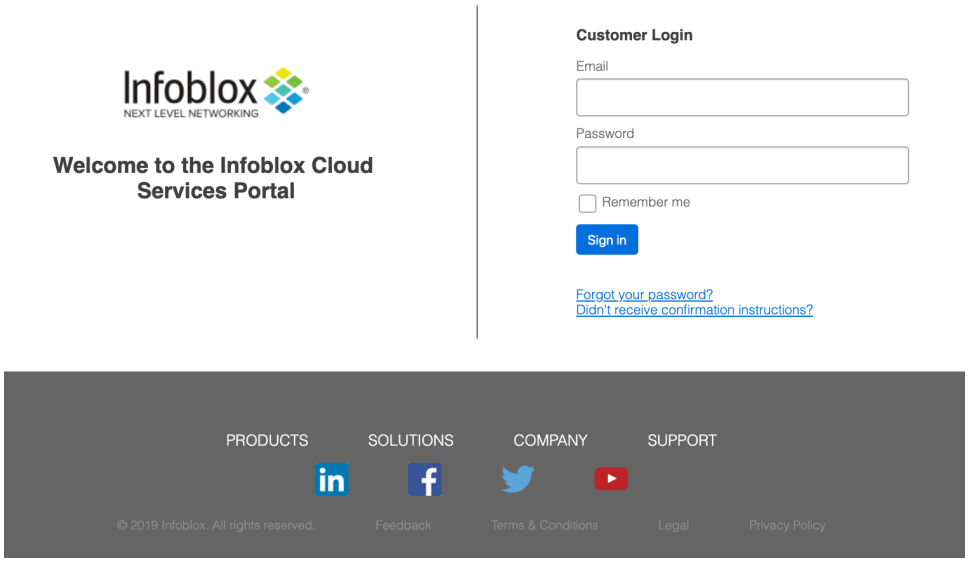
the Infoblox Cloud Services Portal.

Note: If you do not see the notification email shortly after enabling the option, check the spam/junk folder in your mailbox. If you still cannot find the notification email, visit https://csp.infoblox.com/users/confirmation/new, provide your email address and click "**Resend Confirmation Instructions"**.



Accessing the Cloud Services Portal

Once you have completed the Cloud Portal Manager registration process, navigate to https://csp.infoblox.com/users/sign_in to sign in.

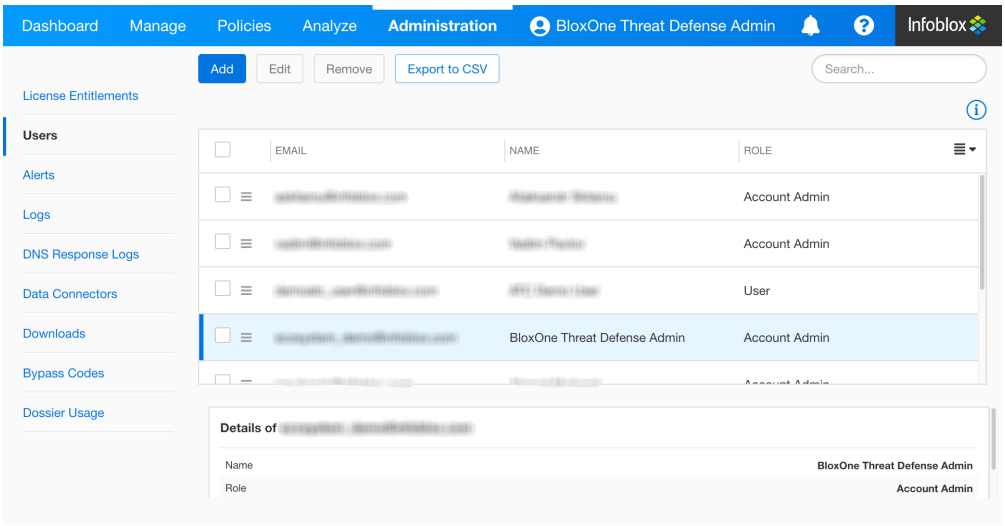


Manage Cloud Services Portal Users

The Cloud Services Portal allows you to add and manage users who will be using the portal. Two levels of access are available:

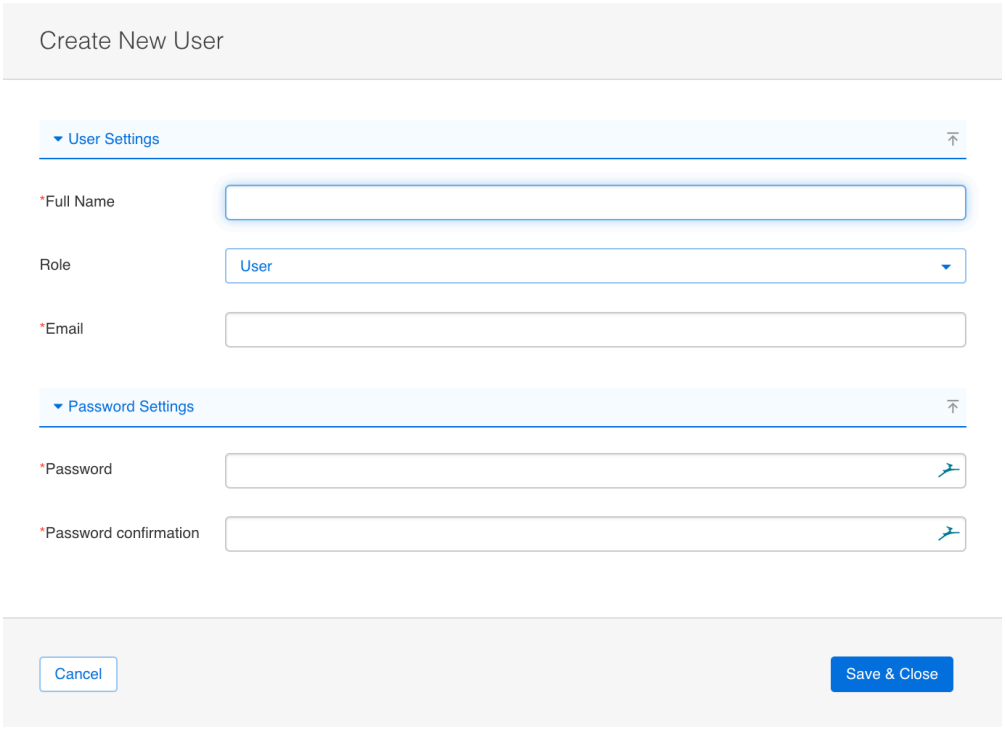
- Account Admin: Full (read/write) access to the Cloud Services Portal.
- Users: Read-only access to the Cloud Services Portal.

Portal users are managed under **"Administration" → "Users"**.



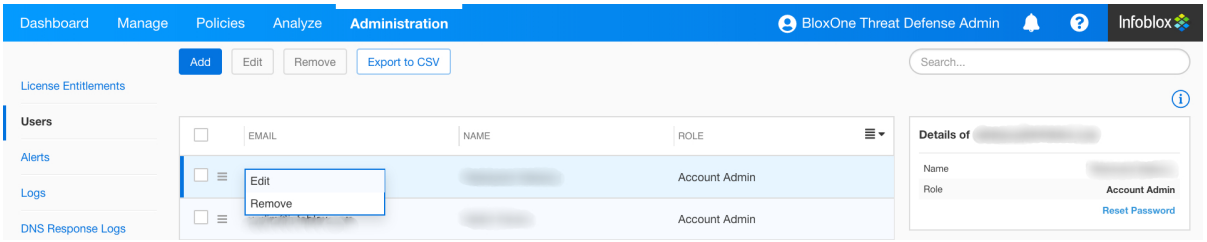
Create a new Cloud Services Portal user:

1. Click the **"Add"** button.
2. Complete the required and optional fields and select the role to be assigned to the user.
3. Click **"Save & Close"**.



Edit an existing Cloud Services Portal user:

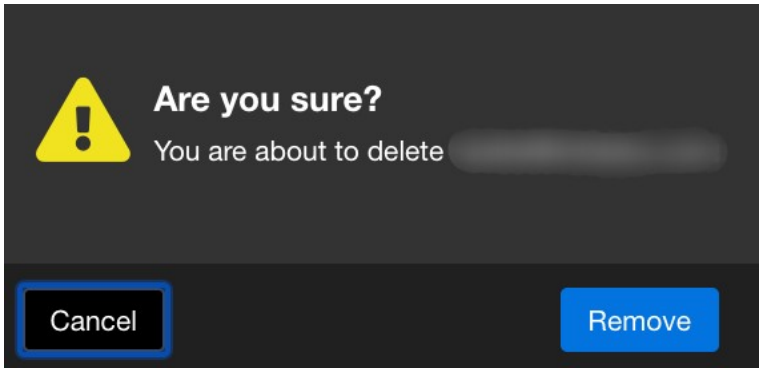
1. Click ☰ and select “Edit”.



2. Modify the name or role (the email address cannot be changed once user has been added).
3. Click “**Save & Close**”.

Delete an existing Cloud Services Portal user:

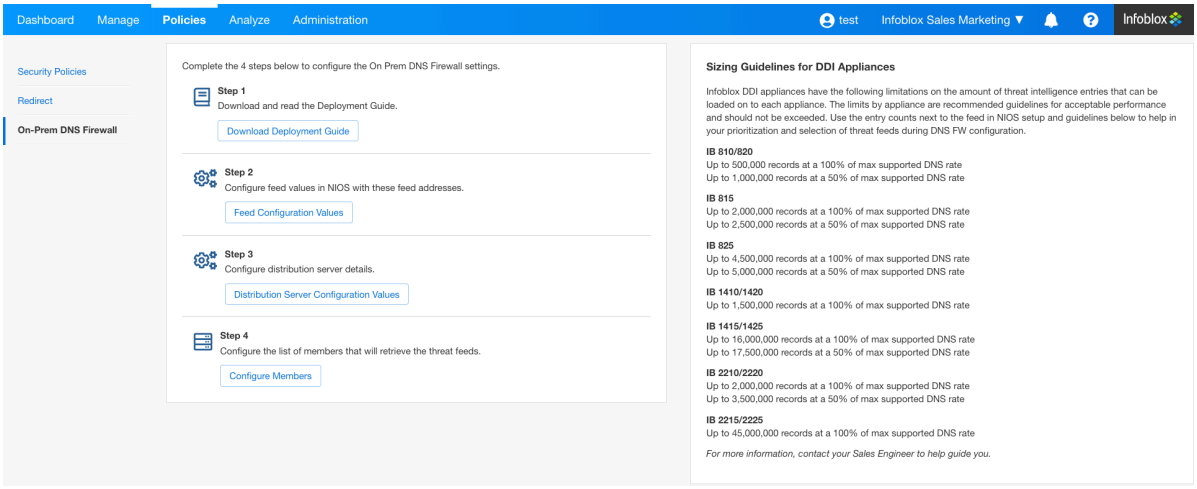
1. Click ☰ and select **“Remove”**.
2. Click **“Remove”** to confirm.



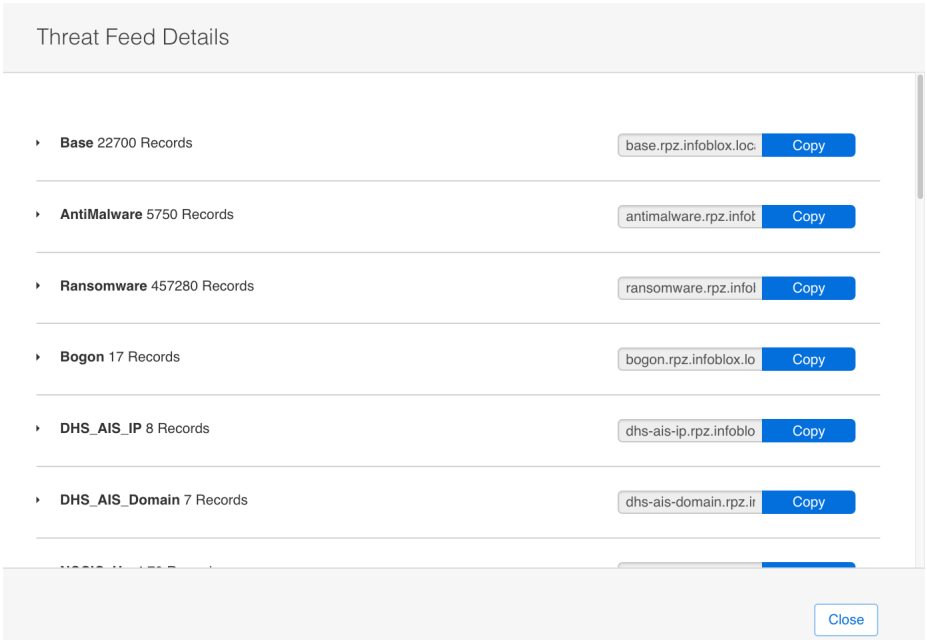
BloxOne Threat Feed Configuration

Before you can employ BloxOne Threat Defense feeds, you must first complete the **DNS Firewall Configuration** in the Cloud Services Portal. To begin the configuration steps:

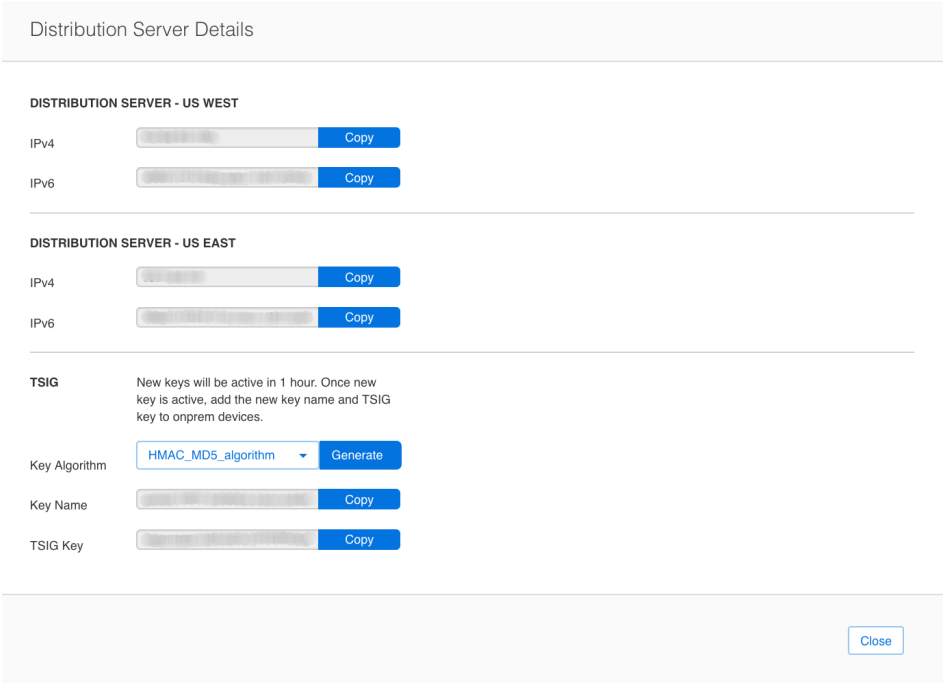
1. Navigate to **“Policies”** → **“On-Prem DNS Firewall”**.



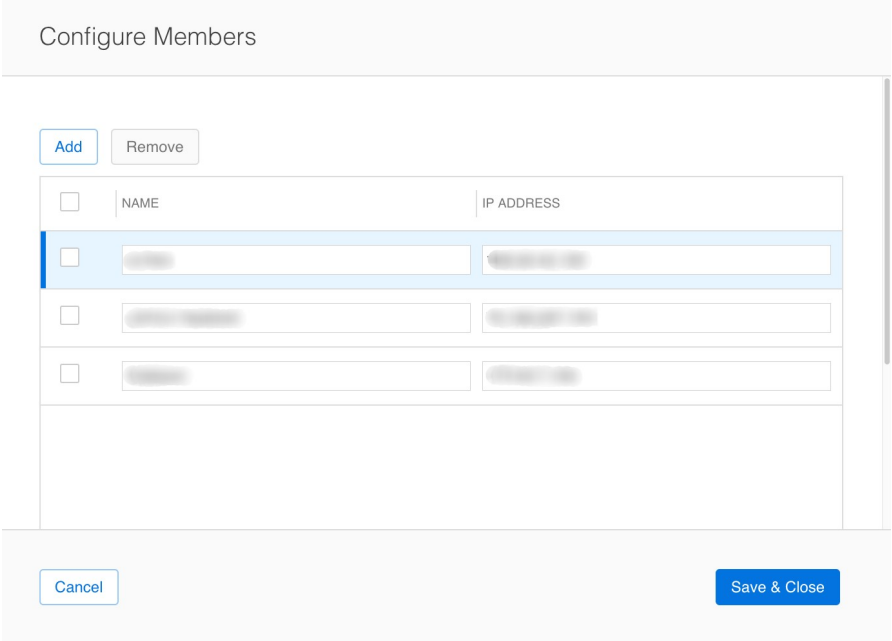
2. Step 1 of 4 provides a downloadable guide on how to configure the On Prem DNS Firewall settings and the same steps this document is providing.
3. Step 2 of 4 provides a listing of the available BloxOne feeds with details for what each is used for and the current number of records included in the feed. Sizing guidelines are also provided in the sidebar on the right-hand side of the page. Copy the URL(s) for the feed(s) that you intend to use.



4. For step 3 of 4, take note of the distribution server IP(s) for where you will be synchronizing the feeds from, “**Key Name”**, “**TSIG Key”** and “**Key Algorithm”**. These will be used later to configure the feed(s) on your Infoblox server.



5. In step 4 of 4, you will add the Infoblox server(s) to send notifications to the IP's if a feed was updated. Click **"Add"**.



Note: Customers must open port 53 for UDP to accept notifications.

6. Enter a client name, which will be used to identify the endpoint where the feed will be synchronized from, along with its publicly accessible/internet routable IP address.
7. Click **"Save & Close"**.

Usage and Deployment Scenarios

DNS Firewall with BloxOne Feeds and Local Policies

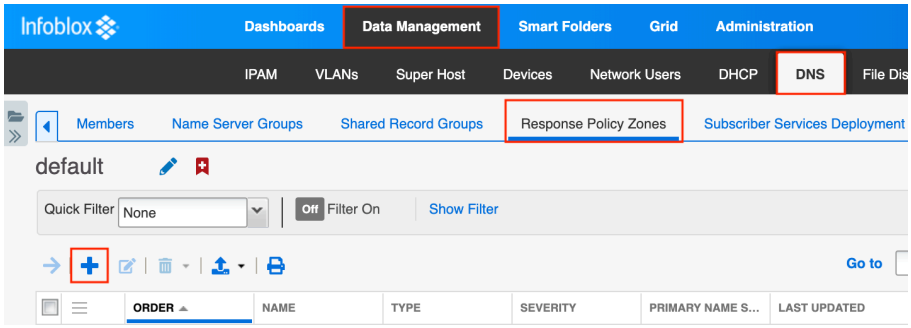
BloxOne Feed (automated malware protection)

DNS Firewall with BloxOne feeds provide automated malware protection for your DNS clients with no additional configuration required on the clients themselves. A listing of all available feeds can be found in the Cloud Portal Manager. These feeds provide protection for different categories of threats and all appropriate feeds should be added to ensure that users are protected from as many different types of threats as possible.

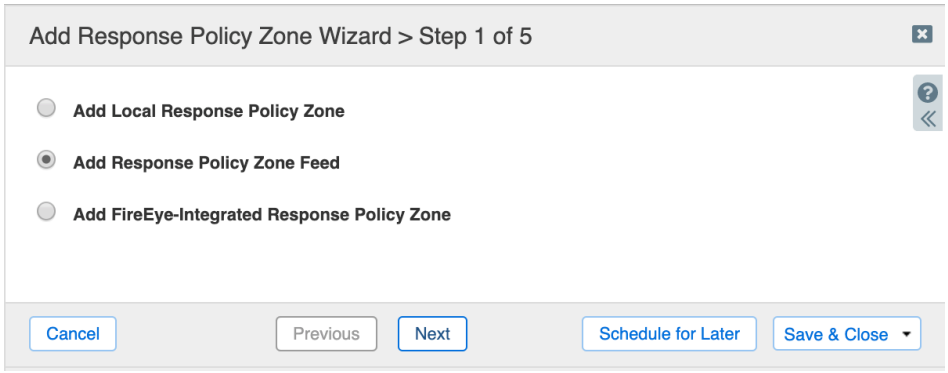
To add a feed to an Infoblox Grid or single server which has been licensed for Response Policy Zones:

Note: To implement the feed in a pilot/test only mode, refer to the section titled **"Testing/Monitoring Only"** further down in this guide before completing the following steps. Additionally, verify that recursion is enabled on your server prior to proceeding as this is required.

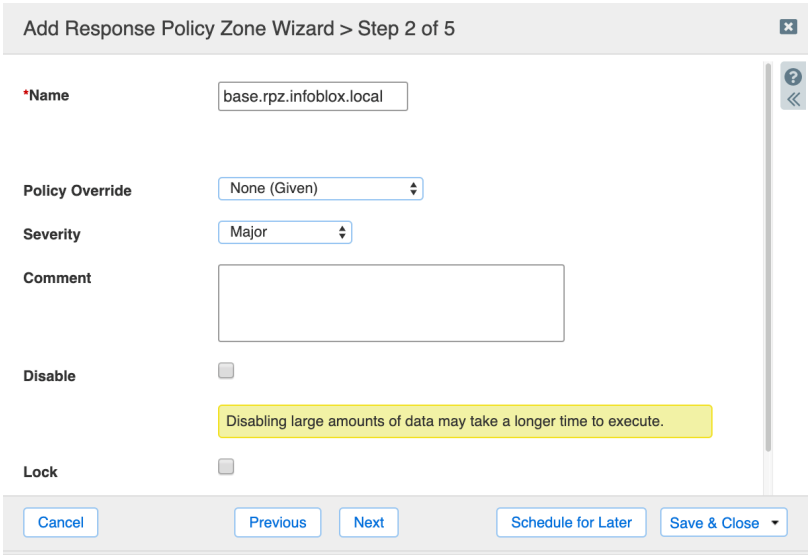
1. In your Grid Manager GUI, go to the **"Data Management" → "DNS" → "Response Policy Zones"** tab.
2. Click **"+"** in the horizontal toolbar.



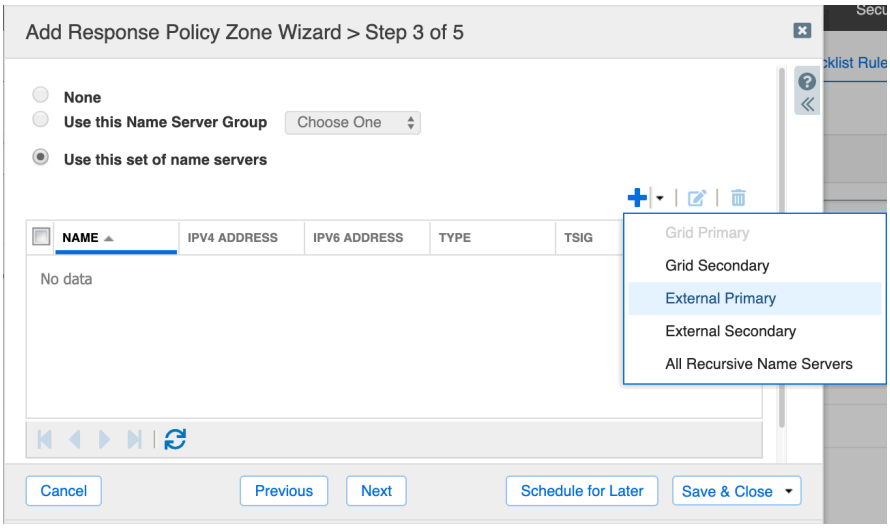
3. Select **"Add Response Policy Zone Feed"** and click **"Next"**.



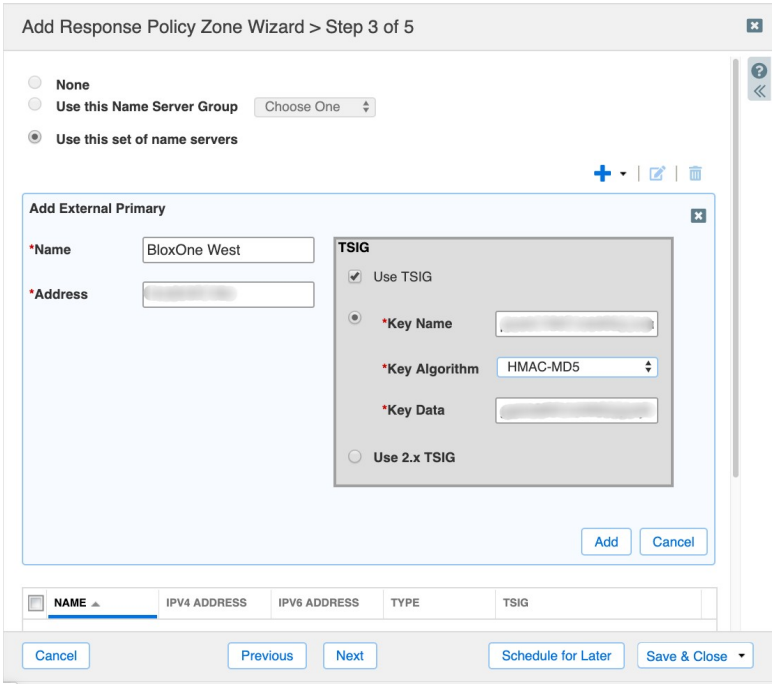
4. Enter the name of the feed and click **"Next"**.



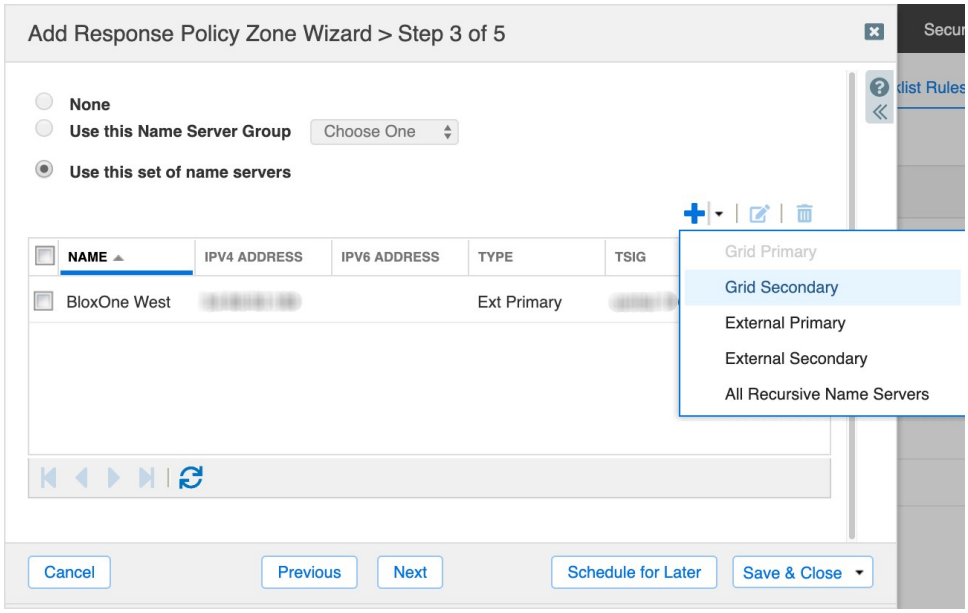
5. Select Use this set of name servers.
6. Click on the downwards facing drop down arrow and select External Primary.



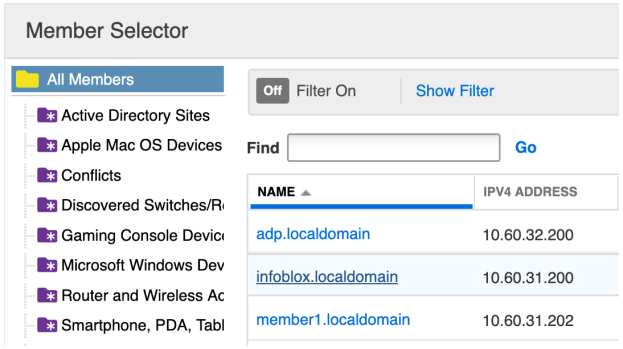
7. Using the details saved from step 2 of 5 in the BloxOne Threat Feed Configuration section above, enter a descriptive name (does not need to be a valid DNS name) for the distribution server where the feed will be synchronized from and its IP address in the corresponding Name and Address fields. Click **"Add"**.



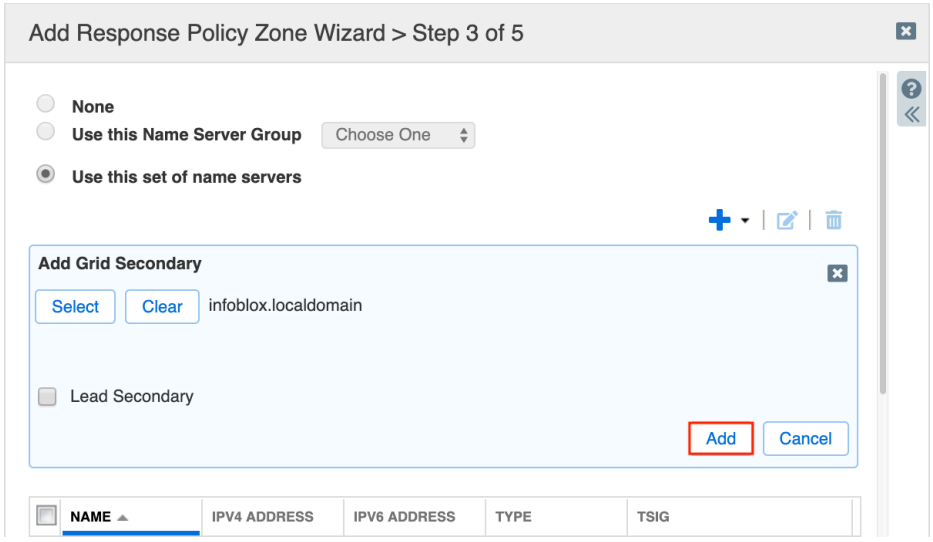
8. Click on the downwards facing drop down arrow and select "**Grid Secondary"**.



9. Click **"Select"**.
10. In Grids with more than one server, the "**Member Selector"** dialogue will appear. Click on the server you want to serve the BloxOne Threat Defense feed from to by selecting it. For Grids with a single Infoblox server or with a standalone server, it will be selected for you automatically.



11. Click **“Add”**.



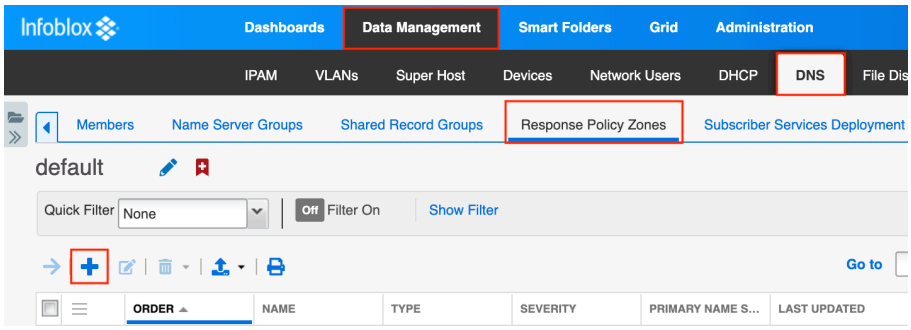
12. Additional servers can be added as required. Once completed with the name server configuration, click “**Next**”.
13. If required, add and configure any needed Extensible Attributes. Click “**Save & Close**”.

Local Policy (blacklist and whitelist)

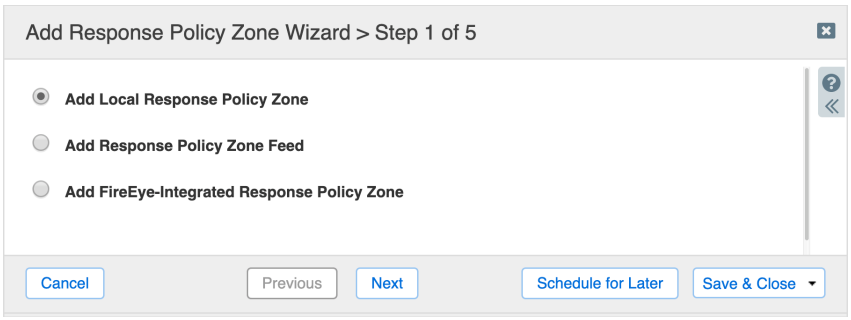
There are many times where you may find that there are specific sites that you want to restrict access to, or add exceptions for sites that are blocked in a feed. Local policies can be used to enforce custom rules to allow or block these queries, commonly referred to as whitelisting or blacklisting.

To add a local policy:

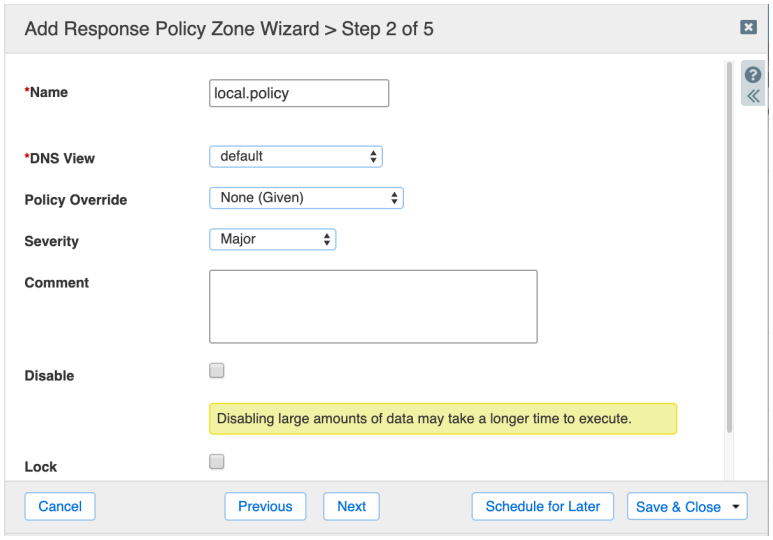
1. On the **“Data Management” → “DNS” → “Response Policy Zones”** tab, click **“+”** in the horizontal toolbar.



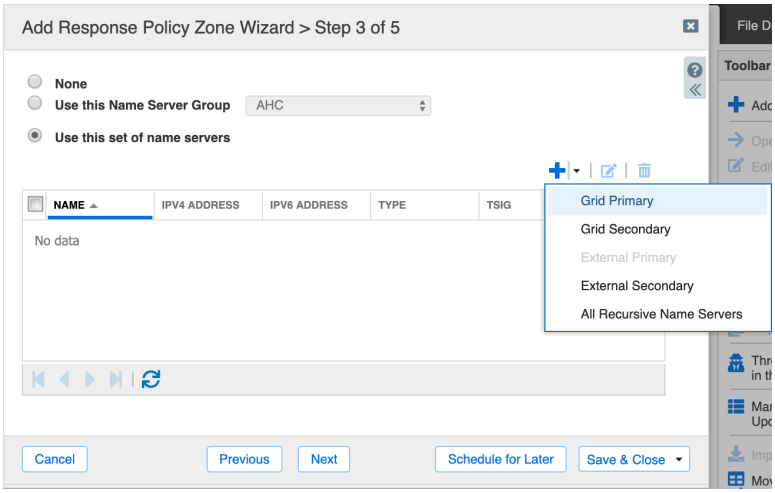
2. Select Add Local Response Policy Zone and click “**Next**”.



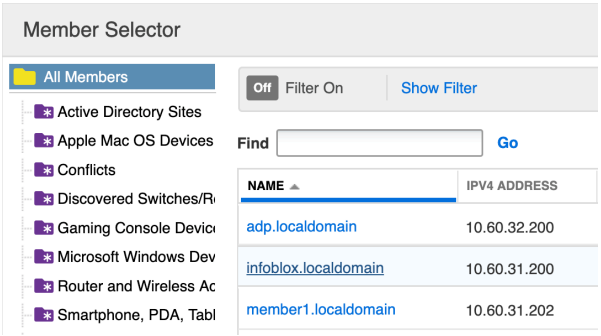
3. Enter a descriptive name (in a zone type name format) and click “**Next”**.



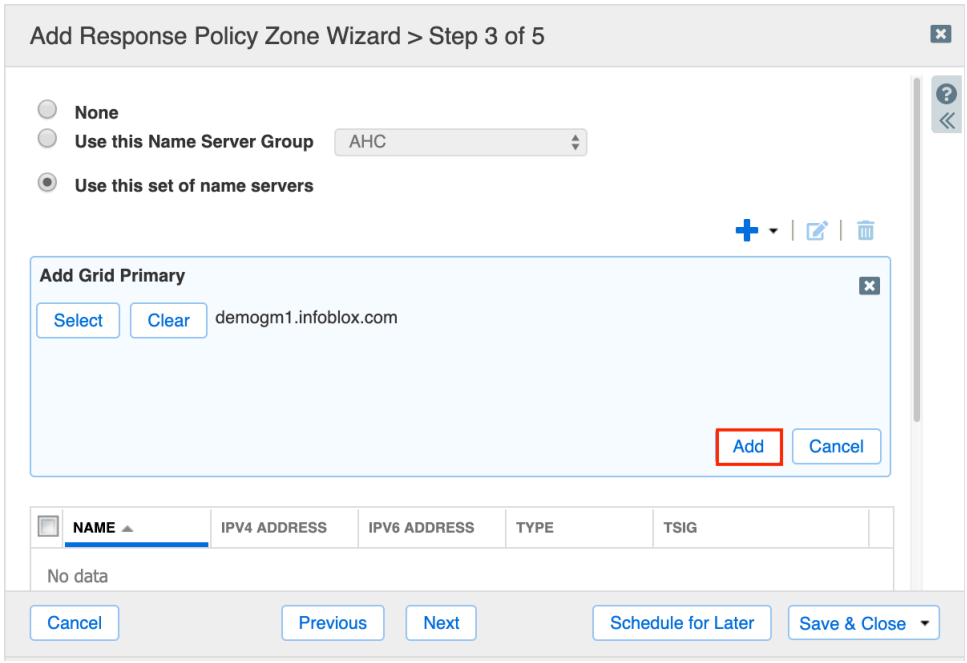
4. Click on the drop-down arrow adjacent to the **“+”** button and select “**Grid Primary”**.



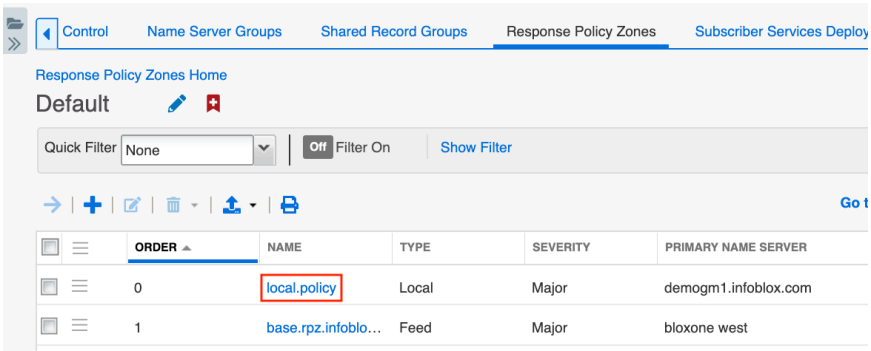
5. In Grids with more than one server, the **“Member Selector”** dialogue will appear. Click on the server you want to serve the BloxOne feed from to select it. For Grids with a single Infoblox server or with a standalone server, it will be selected for you automatically.



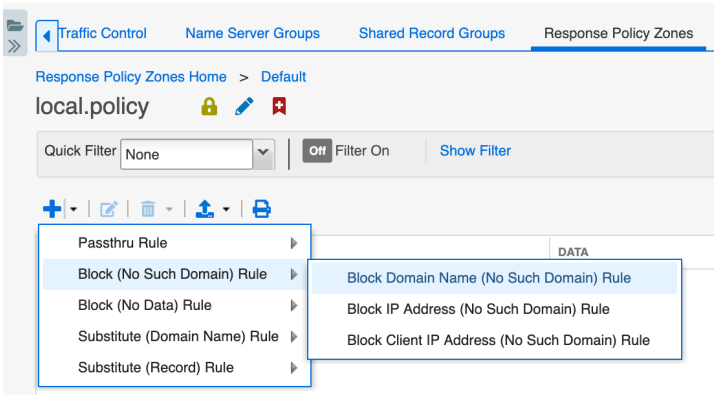
6. Click **“Add”**.



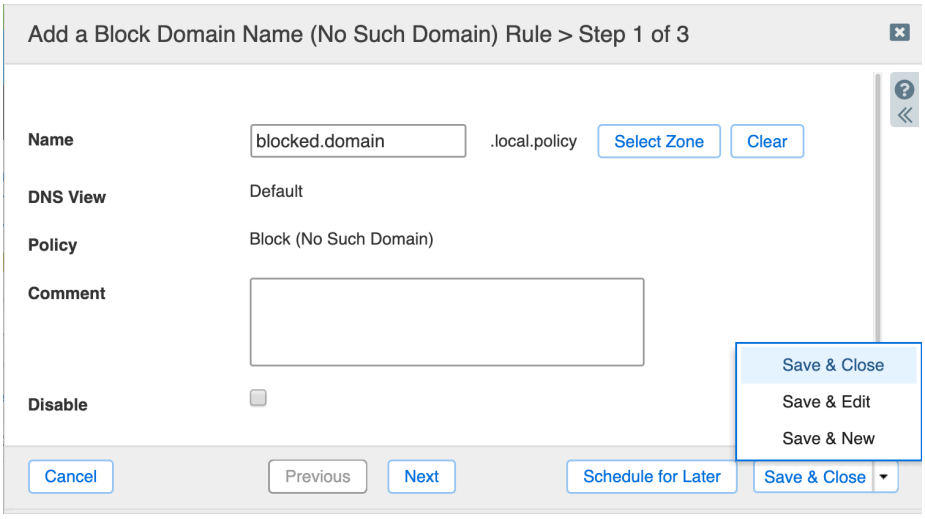
7. Additional servers can be added as required. Once completed with the name server configuration, click **“Next”**.
8. If required, add and configure any needed Extensible Attributes. Once complete, click **“Save & Close”**.
9. Click on the name for the local policy that was just added.



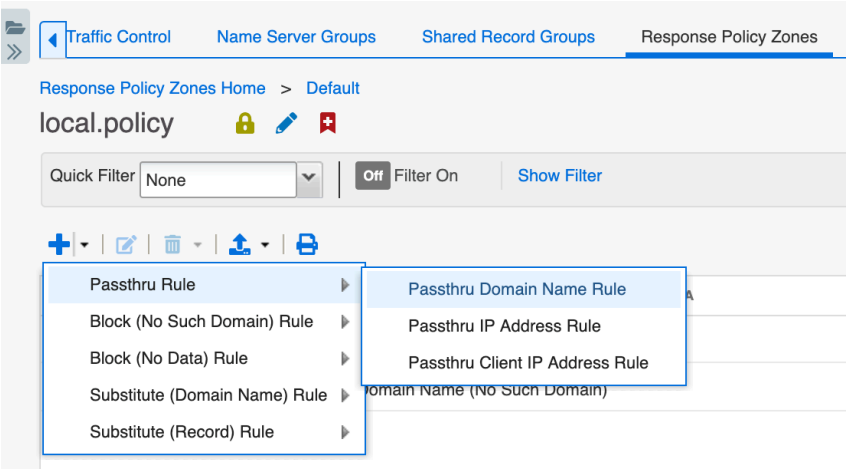
10. Click on the drop-down arrow adjacent to the **“+”** button, expand the **Block (No Such Domain) Rule** menu option and select **Block Domain Name (No Such Domain) Rule**.



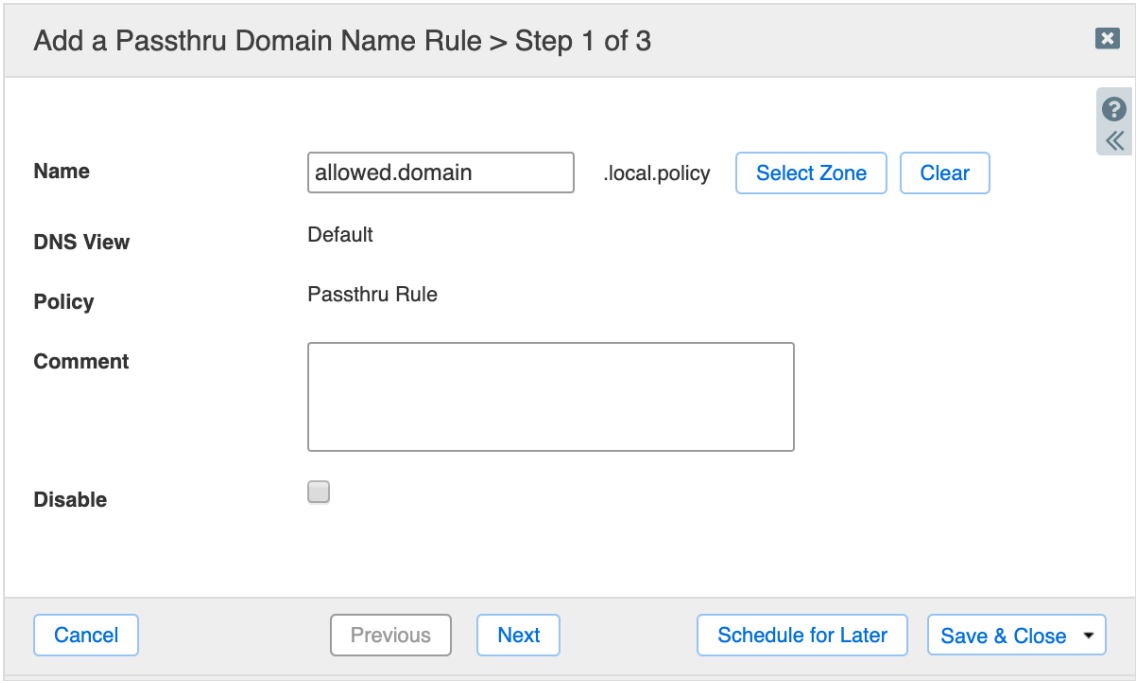
11. Enter the name of a domain that you would like to test a blacklist rule against. Click **"Next"**.
    a. Note: Any domain (zone) name can be used here as long as it is resolvable. A valid zone name is easier to test against here; however, use caution when choosing this name as any DNS clients using this server will be impacted.



12. If required, add and configure any needed Extensible Attributes. Once complete, click "**Save & New**".
13. Enter the same domain name entered for the previous rule, prefixed with a wildcard label. Example: **"*.blocked.domain"**
14. Click **"Next"**.
15. If required, add and configure any needed Extensible Attributes. Once complete, click "**Save & Close**".
16. Click on the drop-down arrow adjacent to the **"+"** button, expand the **"Passthru Rule"** menu option and select **"Passthru Domain Name Rule"**.



17. Enter the name of a domain that you would like to test a whitelist rule against. Click **"Next"**.



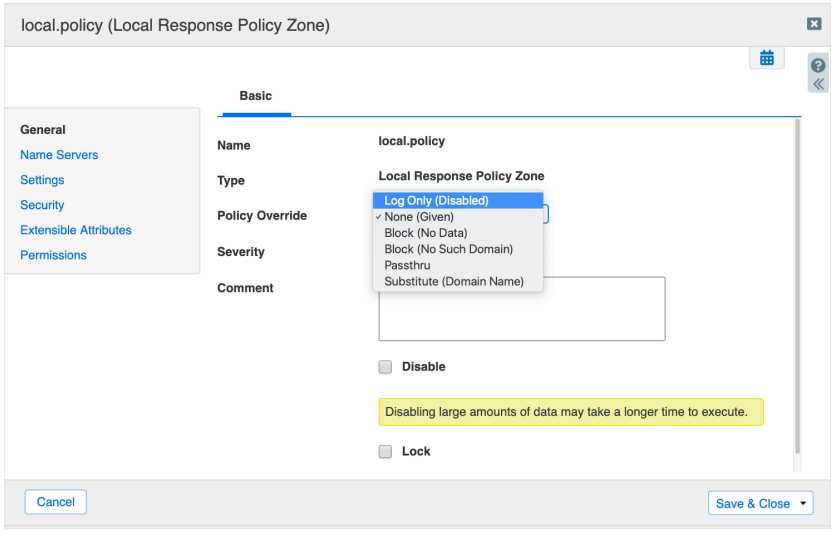
18. If required, add and configure any needed Extensible Attributes. Once complete, click **"Save & New"**.
19. Enter the same domain name entered for the previous rule, prefixed with a wildcard label. Example: **"*.allowed.domain"**.
20. Click **"Next"**.
21. If required, add and configure any needed Extensible Attributes. Once complete, click **"Save & Close"**.

Testing/Monitoring Only (Policy Override)

DNS Firewall with BloxOne Threat Defense is also useful when in a testing only phase, or if you only want to monitor DNS traffic and see what, if any, policy actions would be triggered without affecting DNS queries as they are taking place. To accommodate this use case, the Policy Override setting in the feed or local policy settings can be used.

When configuring a feed or local policy, the **"Policy Override"** setting can be found on step 2 of 5. Alternatively, you can edit the properties for an existing feed or zone and manage this setting under the General panel.

Setting this to **"Log Only (Disabled)"** will effectively disable all policy actions within the feed or zone but any DNS queries which match against a rule will be logged nearly the same as they would be if this was not set.



Monitoring and Testing

Cloud Services Portal Reports and Tools

The Cloud Services Portal provides you with a number of tools to customize, monitor and analyze your BloxOne activity. This portal includes four main areas:

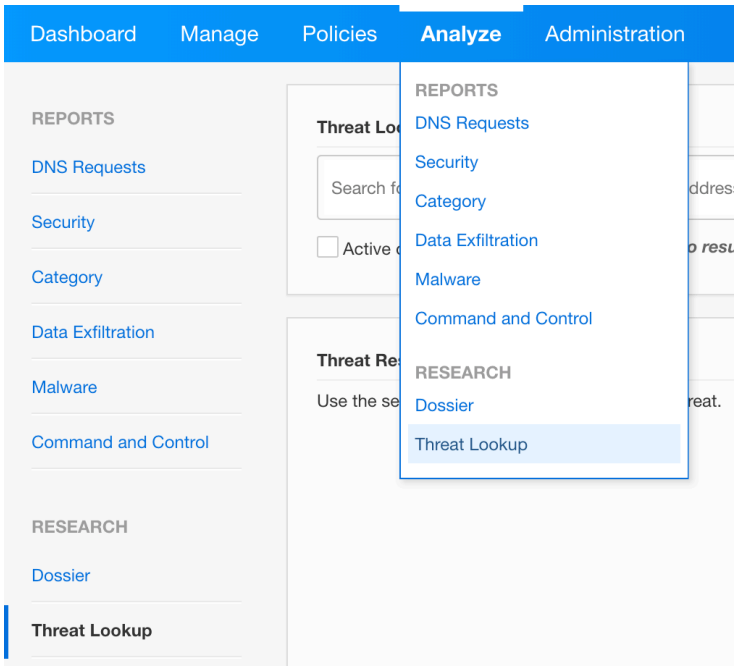
- **Dashboard**: Displays real time and statistical data.
- **Manage**: Configure networks, roaming end users (for BloxOne Cloud), On-Prem hosts, bypass domains rules and access to TIDE.
- **Policies:** Configure custom lists, security policies, Category Filters, the redirect page and configuring the On-Prem DNS Firewall.
- **Analyze**: Statistical data on all security and DNS events and the **Threat Lookup** and **Dossier** tools.
- **Administration**: Review descriptions for threat feeds, alerts, on-prem DNS Firewall configuration and manage portal users.

The Dashboard and Analyze panels in the Cloud Services Portal provide information on BloxOne Threat Defense activity, along with reports and the Threat Lookup tool.

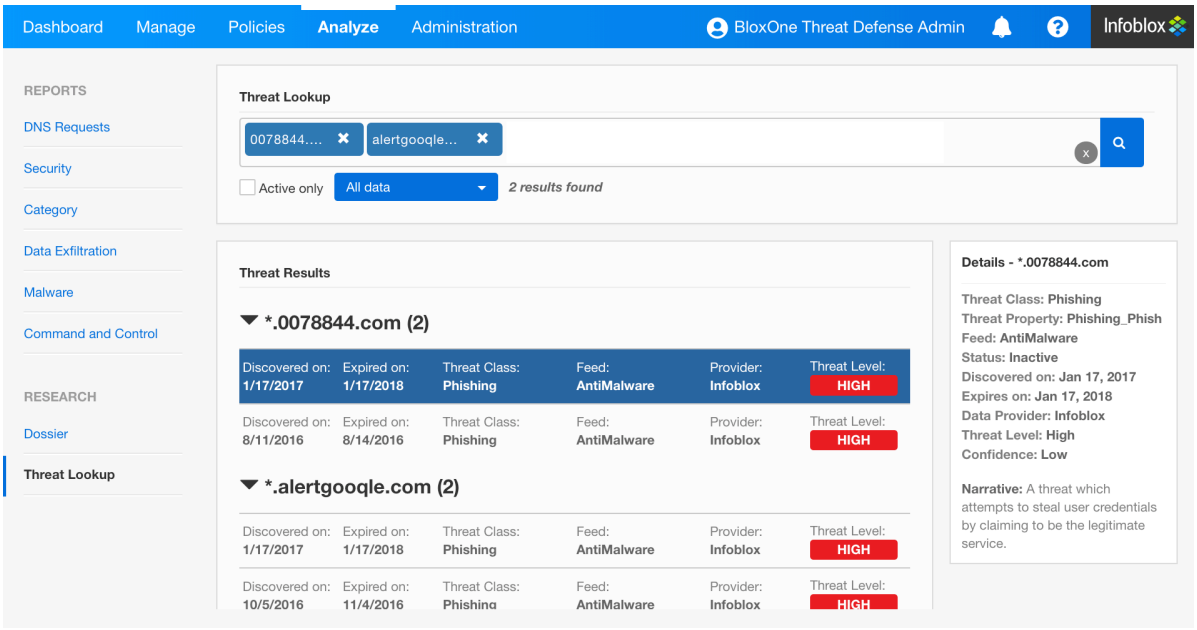
Threat Lookup Tool

Threat Lookup is a tool used to get threat information for domains and/or IP addresses. To use the Threat Lookup tool:

1. In the Cloud Services Portal, navigate to "**Analyze"** → "**Threat Lookup"**.



2. Input a domain name or IP address that you want to lookup. Press **"Enter"**.
3. Review the results.



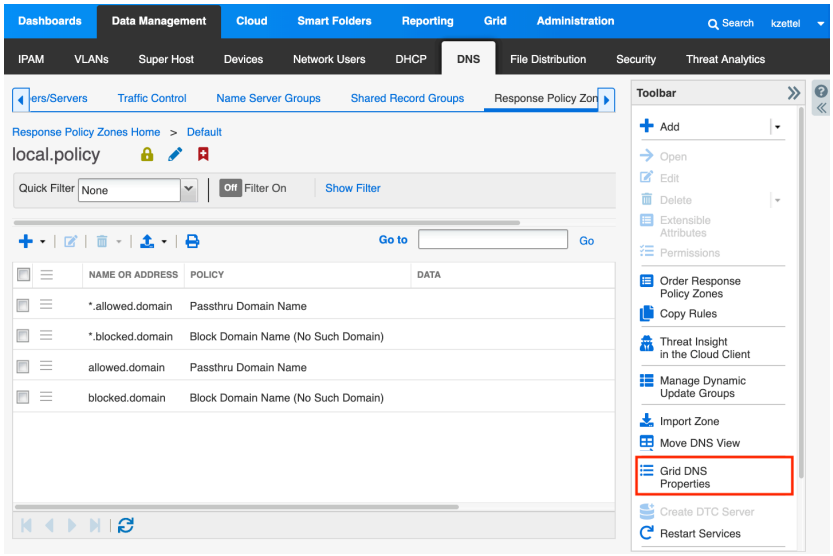
Logging and Reporting

In addition to being able to stop malicious DNS queries in their tracks, the logging and reporting capabilities, that are also available with DNS Firewall, greatly enhance your ability to monitor and respond to activity on your network.

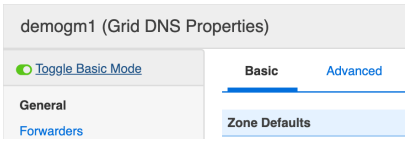
RPZ Logging

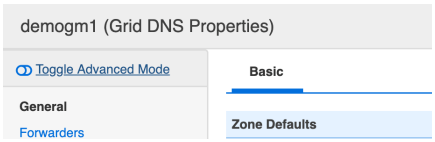
Logging for DNS Firewall (RPZ) is not enabled by default and must be enabled prior to completing the following section in this guide. To enable logging:

1. Under **“Data Management”** → **“DNS”**, click **“Grid DNS Properties”** in the vertical toolbar found on the right-hand side of the page.

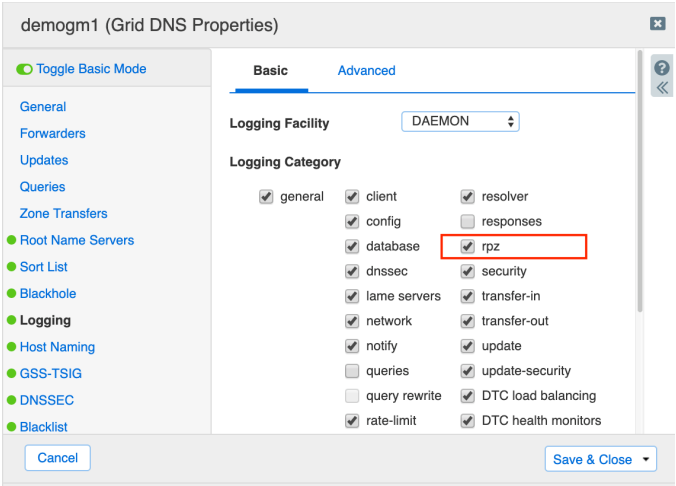


2. Click **“Toggle Advanced Mode”** (if not already enabled).





3. Go to the **“Logging”** tab.
4. Enable the **“rpz”** category.



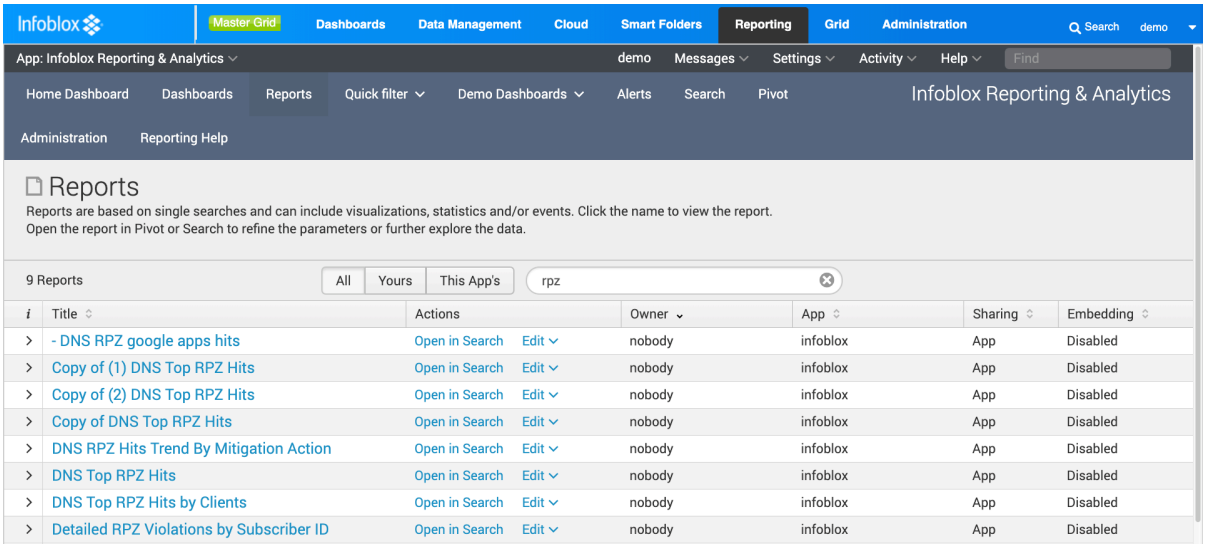
5. Click **“Save & Close”**.

Infoblox Reporting

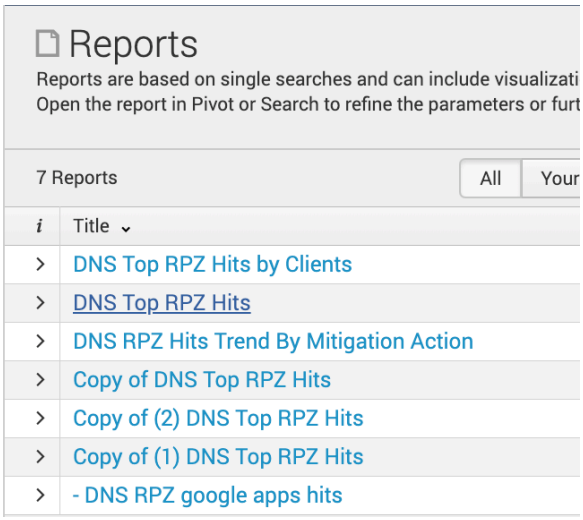
The Infoblox Reporting solution is also useful for tracking DNS Firewall activity within your Grid Manager GUI. In a Grid which has a Reporting server as a Grid member already running:

1. In your Grid Manager GUI, go to “**Reporting**” → “**Reports**”.
2. In the **filter** text box, type **“rpz”**.

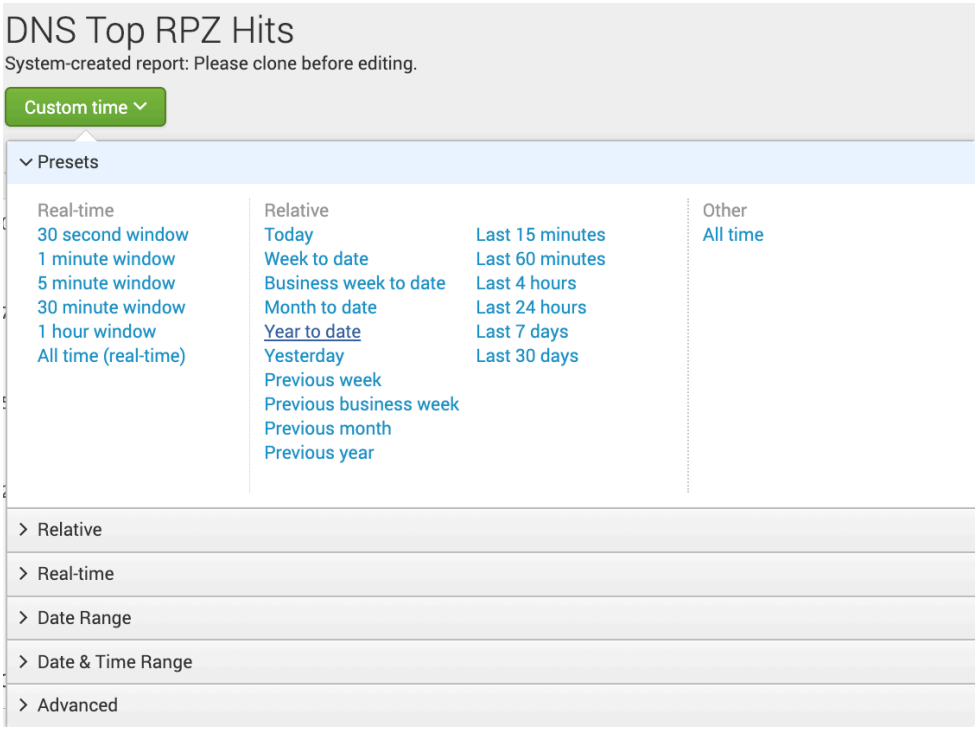
Note: The reports that will be available will vary depending on your version of NIOS. This example demonstrates NIOS version 8.4.



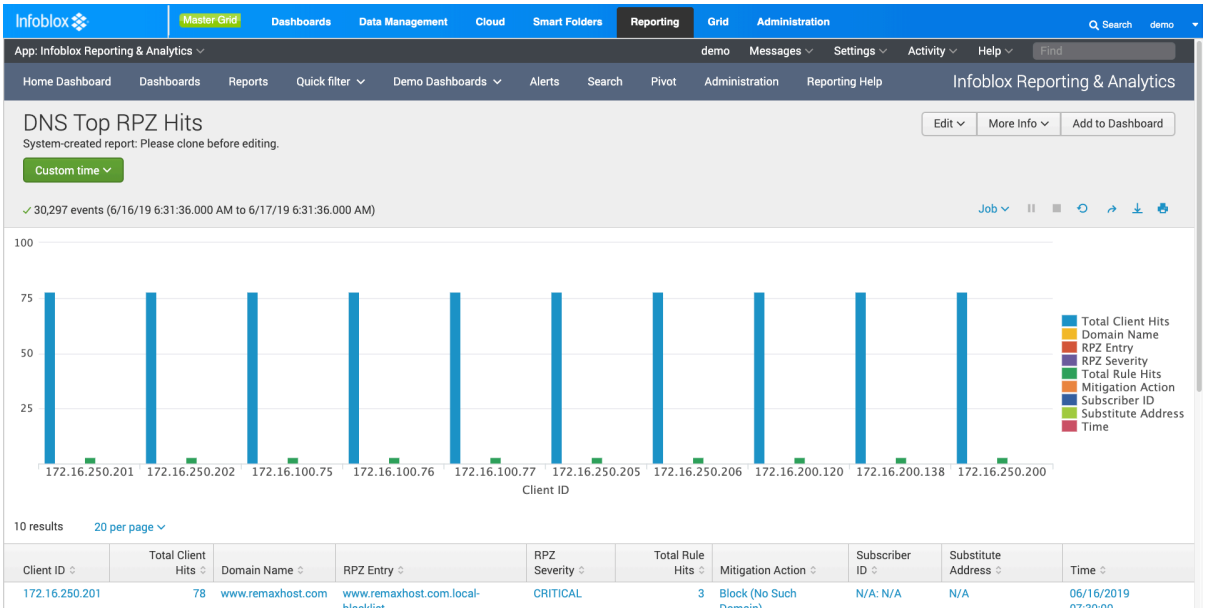
3. Click on DNS Top RPZ Hits.



4. Expand the "**Custom Time"** menu and select "**Year to date"**.



5. Review the available reporting data.

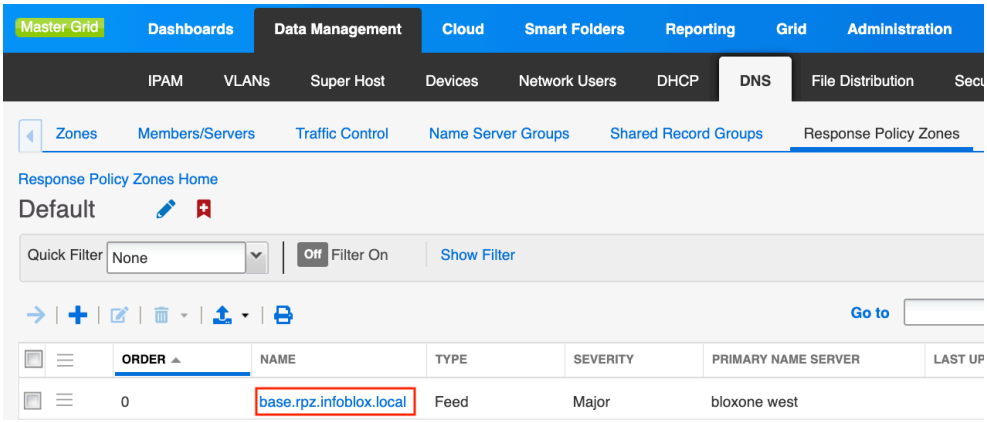


Testing BloxOne Threat Defense

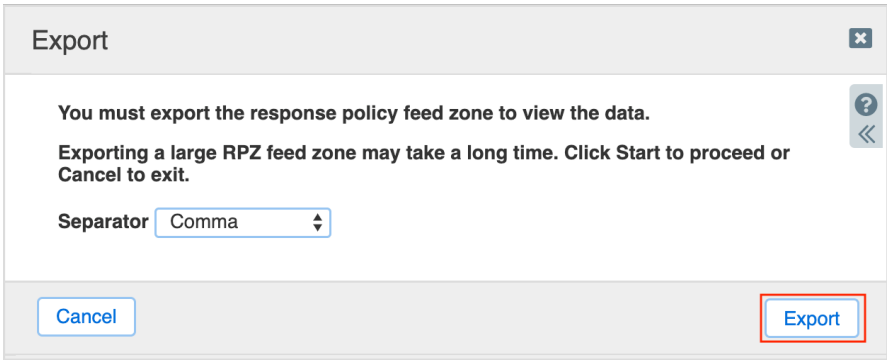
Any clients resolving DNS queries using the servers assigned to this feed are now protected with BloxOne. To test your BloxOne feed, first export the feed and then review the feed data included in the downloaded CSV file. With this data, you can then test your server to validate that it is working by sending DNS queries to it.

Export and view BloxOne feed

1. Click on the name for your BloxOne feed.



2. Click **"Export"**.



3. Depending on your browser settings, the export may be saved automatically to a preset location (such as a Downloads folder), or you may be prompted to save the export. Follow any prompts you may see to save the export.
4. Locate and open the export data using a standard spreadsheet application or text editor.
5. The feed data will be listed in the following format:

   'Name or Address' , 'Policy' , 'Data'

Note: You will also frequently see two entries for each domain name listed, one being the domain name itself and another with a wildcard prefix. For example:

domain.label

***.domain.label**

The wildcard rule allows DNS Firewall to apply actions on any name being queried for that domain, while the explicit rule (without the wildcard character) will only be applied for queries matching that exact name.

6. Review the contents and take note of a domain name listed.

Test BloxOne Feed

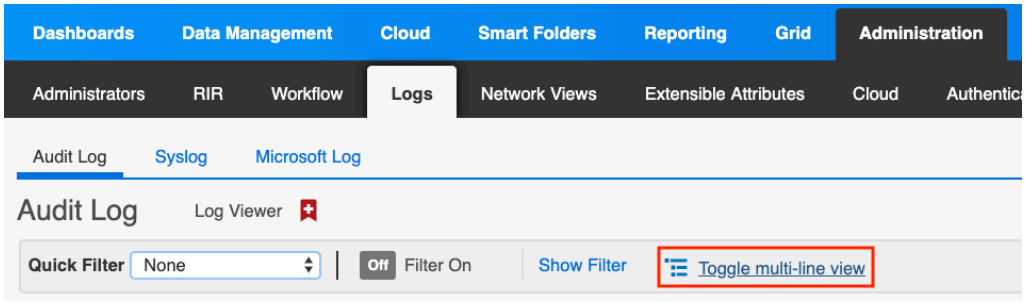
1. Query the server for a name found in the list and verify that the response matches the policy action set for it.

```
> www.0078844.com.
Server:  [10.60.27.235]
Address:  10.60.27.235

*** [10.60.27.235] can't find www.0078844.com.: Non-existent domain
```

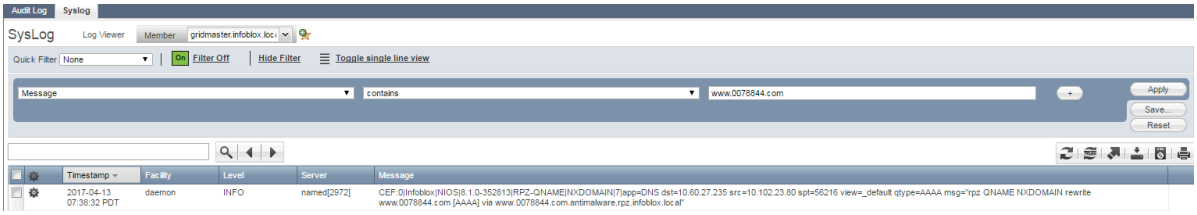
2. (Optional): Send the same query to a different name server which does not have DNS Firewall protection (or optionally, the local policy can be disabled for this test) and verify that the query works.

```
> server 8.8.8.8
Default Server:  google-public-dns-a.google.com
Address:  8.8.8.8

> www.0078844.com.
Server:  [8.8.8.8]
Address:  8.8.8.8

Non-authoritative answer:
Name:    0078844.com
Address:  50.63.202.34
Aliases:  www.0078844.com
```

3. In your Grid Manager GUI, go to **"Administration" → "Logs" → "Syslog"**.
4. Click **Toggle multi-line view**.



5. Click **"Show Filter"**.
6. Set the Choose Filter drop down menu to Message. The operator (middle) menu should default to contains.
7. In the text box, input the name you used in your test query and press **Enter**, or click on the **"Apply"** button.

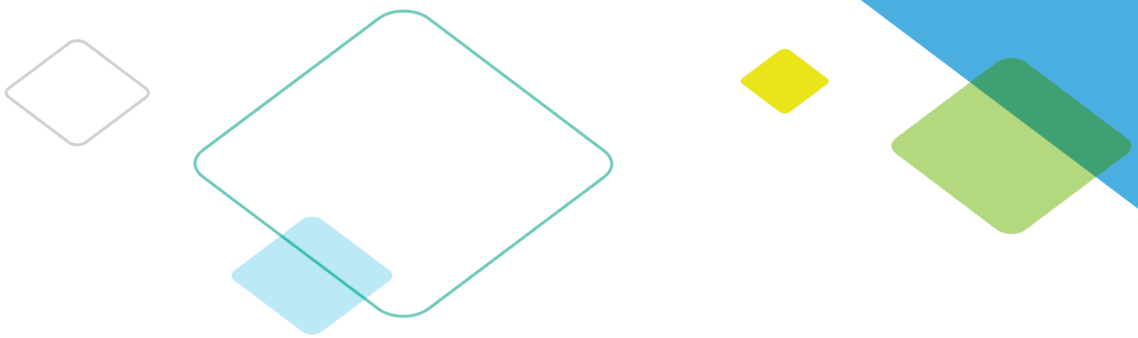


8. Review the log message(s) for the DNS Firewall related log messages and confirm that the event was logged as expected. The following is a text-based example of the log message:

   2017-04-13T14:38:29+00:00 daemon gridmaster.infoblox.localdomain named[2972]: info CEF:0|Infoblox|NIOS|8.1.0-352813|RPZ-QNAME|NXDOMAIN|7|app=DNS dst=10.60.27.235 src=10.102.23.80 spt=56212 view=_default qtype=A msg="rpz QNAME NXDOMAIN rewrite www.0078844.com [A] via www.0078844.com.antimalware.rpz.infoblox.local"

9. Using the above example as a reference, the log message structure includes: the **NIOS version** from the Infoblox server (8.1.0-352813), **the trigger** (RPZ-QNAME), **policy action** executed (NXDOMAIN), **responding DNS Firewall server** (dst=10.60.27.235), **source/DNS client** where the query was received from (src=10.102.23.80), **DNS View** (view=_default), **record type** queried (qtype=A), **DNS name queried** (rewrite www.0078844.com) and the **feed or local policy where the query matched against** (antimalware.rpz.infoblox.local).

Note: If the expected log messages are not found, verify that the steps for enabling RPZ logging (provided in the **"RPZ Logging"** section earlier in this guide) were completed and the selected logs for the correct server were chosen and that the test DNS query was sent to the correct server.



Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054

+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com