Deployment Guide

Infoblox Threat Intelligence Feed

Table of Contents

Click on “Next Step” located at the bottom of the page to set-up your IP address configuration. Once you click “Next Step” at the bottom of the page the following data will be displayed:

- The IP’s that serve the feed
- Your unique key name and key
- The key algorithm

Copy these values to a text editor as you require them later for NIOS configuration.

IP Address Configuration

Either IPv4 and IPv6 IP addresses may be used to serve your feeds, depending on your specific requirements.

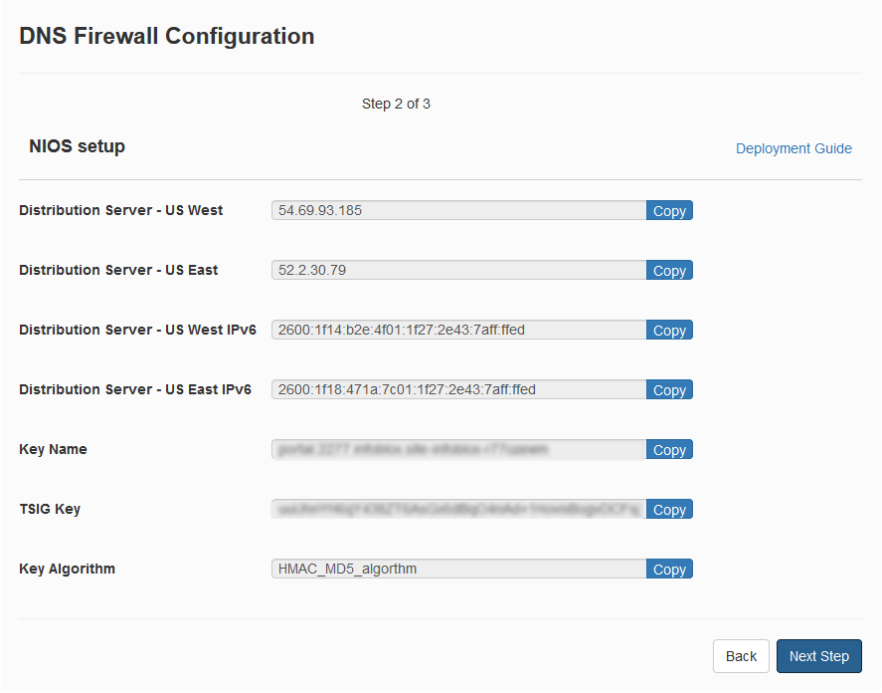
Distribution Server Set Up

To set up where your feeds distribution, complete the following steps:

1. On the **DNS Firewall Configuration** page (Step 2 of 3), select either the IPv4 or IPv6 IP options for both the US West Distribution and the East Distribution Servers.

2. Copy and save your selected IP addresses. You will need them later when configuring NIOS.

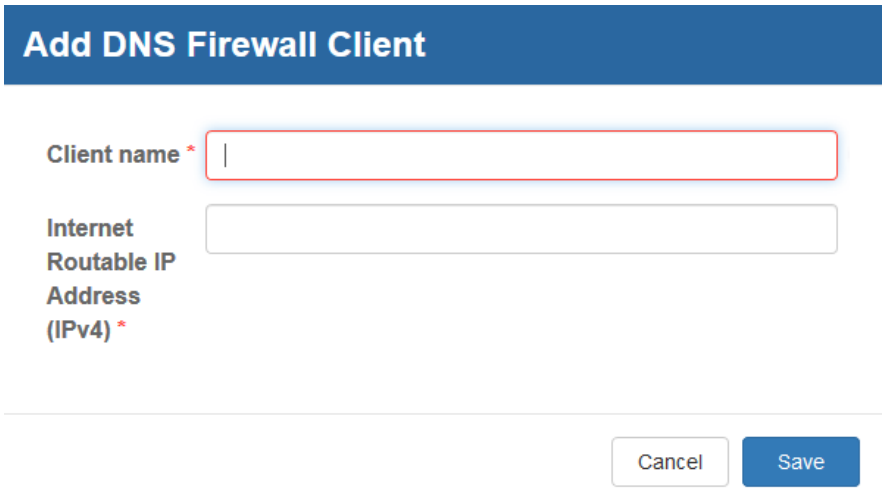
3. Click “Next Step” to set up where you want your feed notifications to be sent.



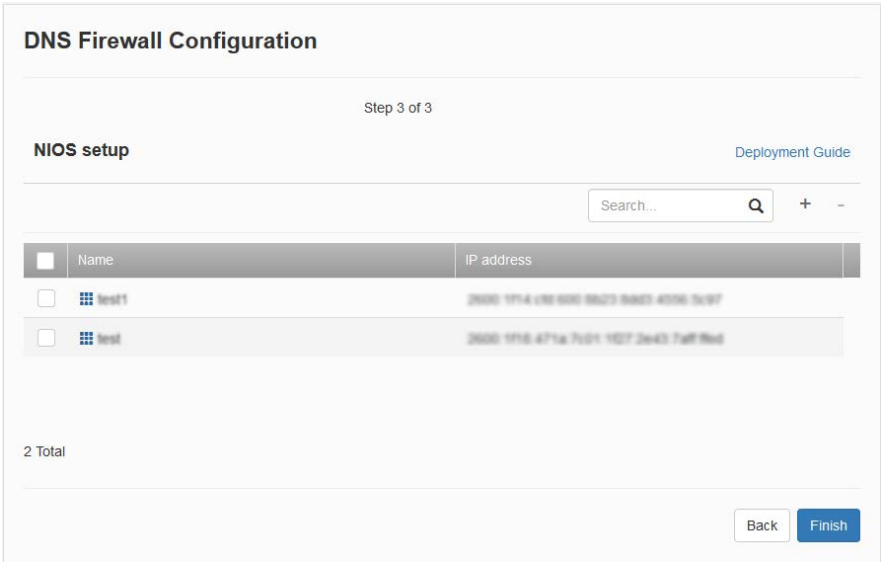
Notification Server Set Up

To set up where your feed notifications, complete the following steps:

1. On the **DNS Configuration** page (Step 3 of 3), click the “+” icon located on the top action bar.
2. In the **Add DNS Firewall Client** pop-up, add your client name in the “Client name” field.
3. In the “Internet Routable IP Address” field, add the external IP address where you want your notifications sent. Please note, the IP address may be of either IPv4 or IPv6 format.
4. Click “Save” to save your settings.

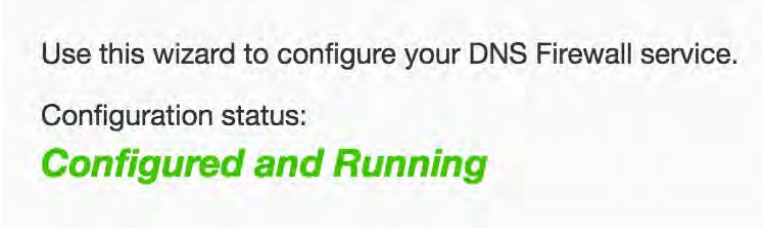


You can verify your new configuration by viewing it on the **NIOS setup** page. Once you’ve verified the configuration of your newly created list, click on “Finish” located at the bottom of the page to complete the configuration process.



You will initially see your configuration in a “Pending” status, it will move to “In Progress” and then to “Configured and Running”[2].

[2] Allow this process 10 minutes to complete


Use this wizard to configure your DNS Firewall service.
Configuration status:
Configured and Running

NIOS Configuration

License and Configuration Requirements

In order to deploy remote RPZ feeds, you will need a Grid member with at least a DNS and RPZ license.

In order to obtain the feeds your member will need access to our Threat Intelligence Feed servers on port 53 (UDP and TCP) as the feed data is transferred through a DNS zone transfer. Your server will also need to be able to perform recursion in order to obtain response from the internet.

In order to review log hits, you need to enable on the member or grid level the RPZ logging category (grid settings, toggle advanced, logging, check RPZ)

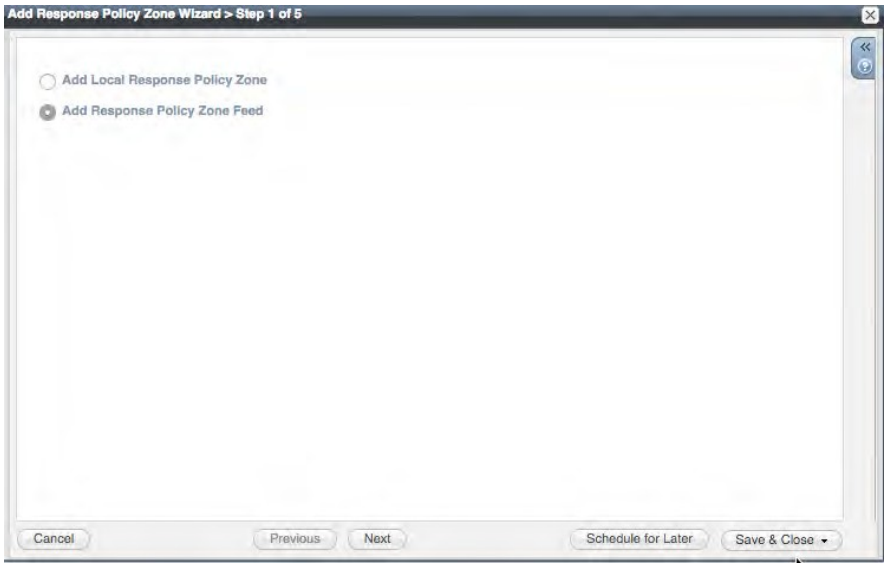
Configuration steps

In NIOS go to:

“Data Management” -> DNS -> “Response Policy Zones”

Press the + button or use “Add” in the sidebar

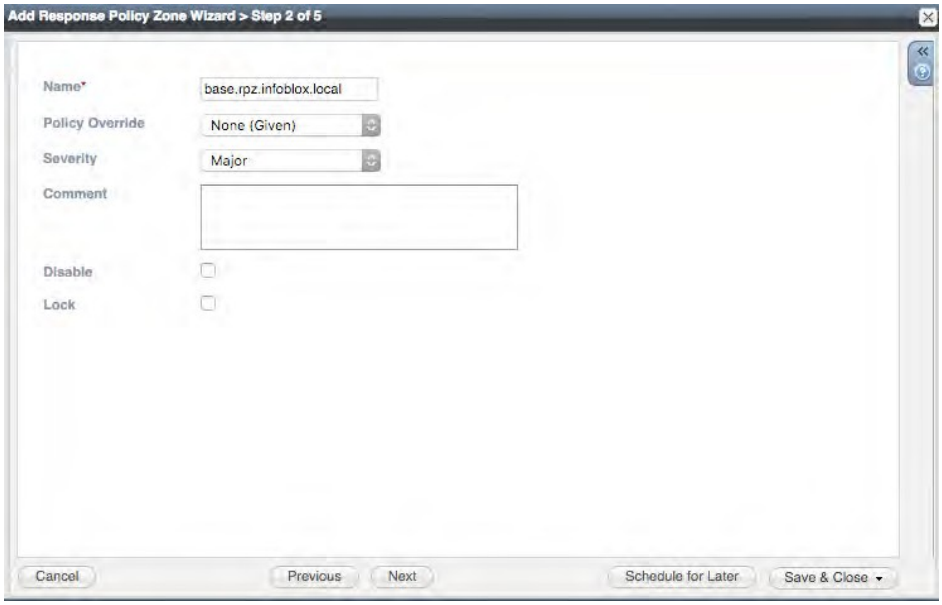
1. **Select “Add a Response Policy Zone Feed”:**



press next

2. **Add the feed you want to use.**

Note that each feed is a subset of the data and deploying multiple feeds is required to cover all bases. You will have to repeat these steps for each RPZ.



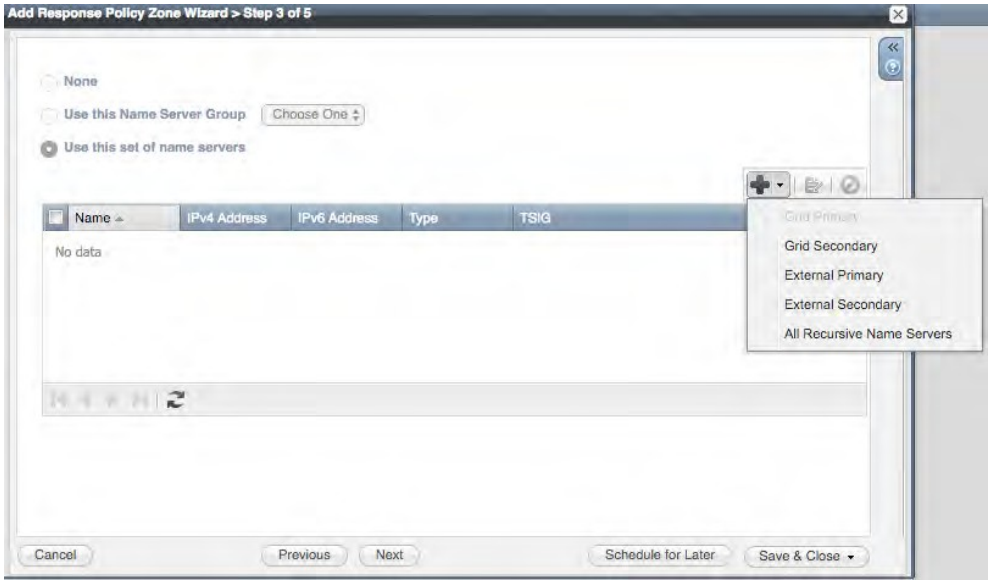
Leave Policy override on “None (Given)” for now. For the other policy override settings please refer to the Admin Guide.

Modify logging Severity if needed

Press next

3. **Add the External Primary[3]**

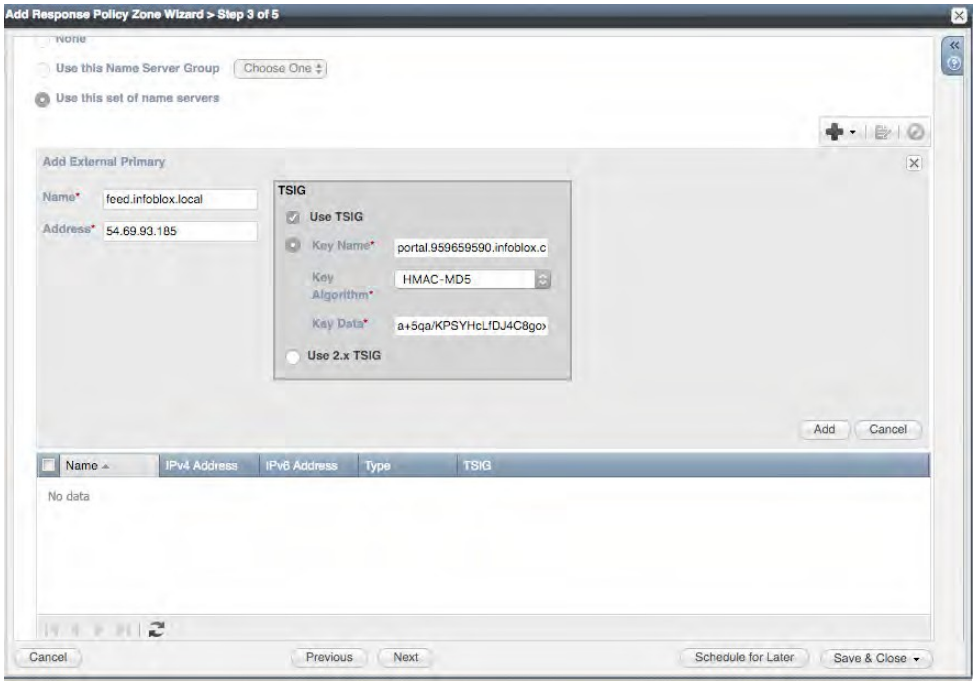
Use the dropdown next to the “+” sign to select External Primary



[3] If you want to save time, create a nameserver group with the external primaries and any grid secondaries that you want to use with this RPZ. You can then later use nameserver groups for each RPZ instead of adding the nodes one by one.

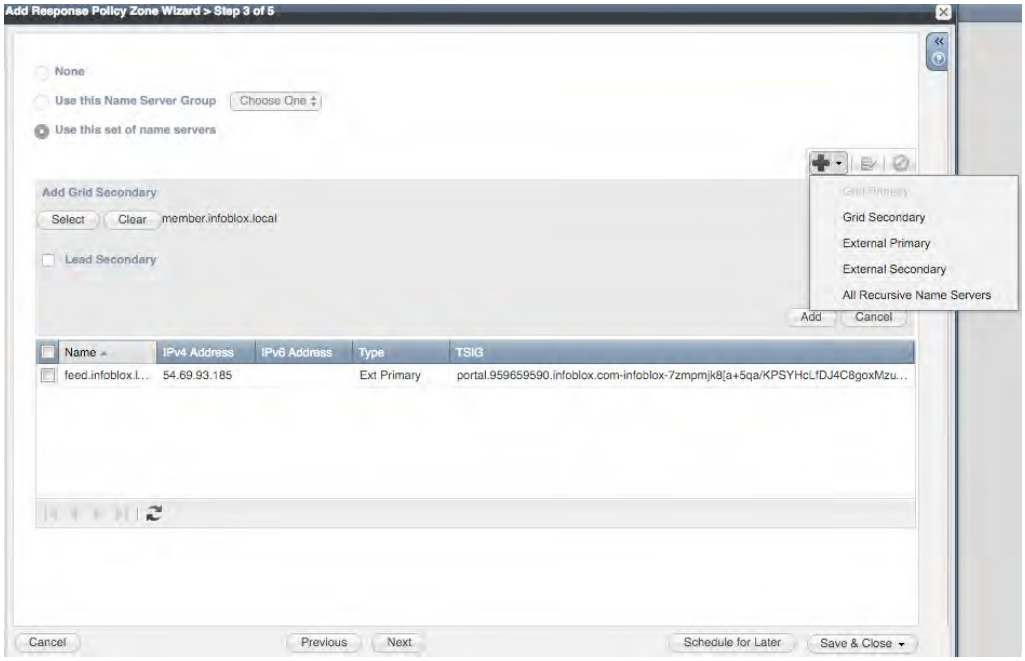
4. Define the External Primary's settings

Refer to the portal for the values from your account. Select the nearest name server and use the values you copied from csp during feed configuration. Note that the name field is only for reference purposes and you can use any name you choose to.



Press Add

5. Add a Grid Secondary



Use "Select" to select which member(s) you want to add or use "All recursive servers" if you want to add all recursive nodes with an RPZ license.

Note that you can configure a single secondary to be “Lead secondary”. If you set this up that member will be the only one to reach out to the external primary. You will then redistribute the feed internally between your members through zone transfers.

Press Add

Press Save and Close, restart services as required (use the banner at the top)

Give services 5 minutes to fetch the zone, if you refresh the gui you will see the last updated value for when the last transfer was successful.

Troubleshooting

In case you are not getting a feed from our servers verify if:

You used the right feed name
Your time is set correctly (ntp should be used)
You use the right key name, TSIG key, and algorithm

For further troubleshooting check the syslog of your (lead) secondary for message that include “transfer”

Generating & Reviewing Hits

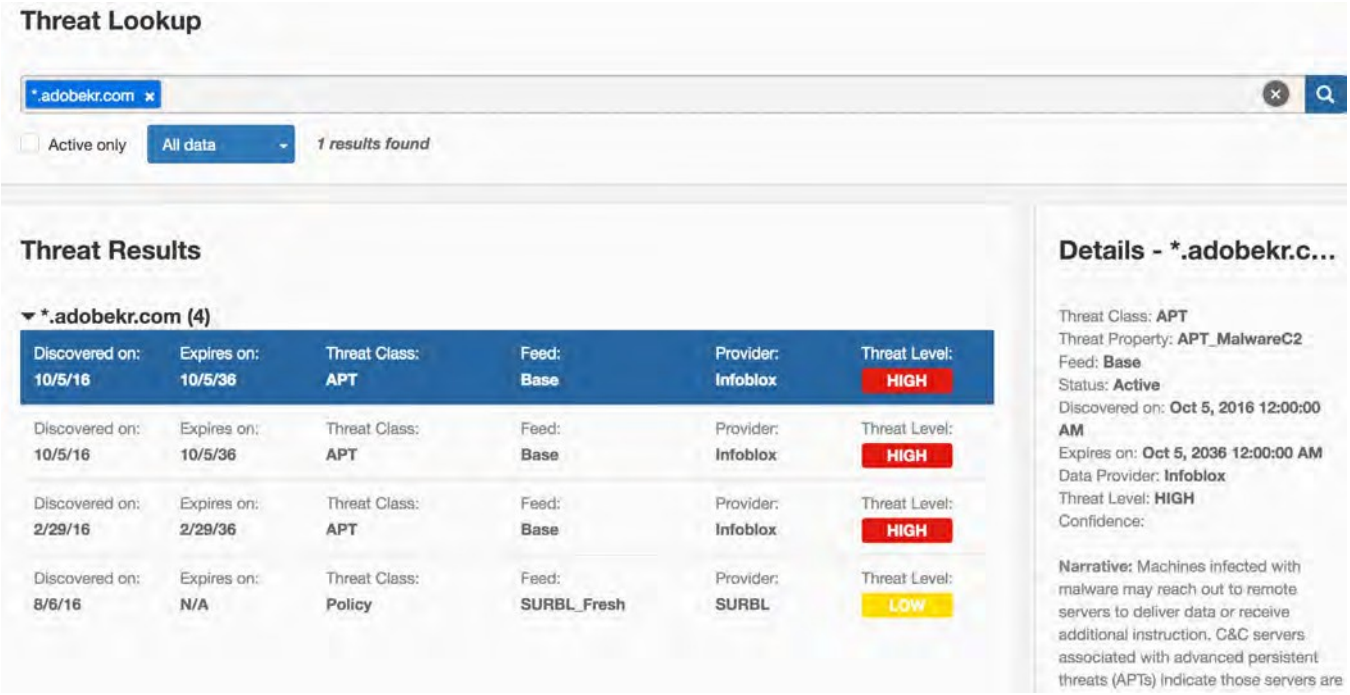
In order to generate a hit against the feed, query a member that has the zone running for “adobekr.com”

If you want more inspiration for testing, once the base.rpz.infoblox.local zone you configured is showing as “Last updated” you can click the name and download it as a csv file.

Check the syslog for security hits you should see a CEF entry with the domain(s) you are testing, you can also refer to the security dashboard for graphed out results based on the last 30 minutes of traffic.

Portal Investigation

To research suspicious indicators for more information and context, take the domain from the log entry and use the “Threat Lookup” feature under “Analyze” in top navigation to get more information and context.



You can also use IP’s from your logs, be aware that you need to inverse them and take the first octet as the hostmask.

For example: 32.1.0.0.10 becomes 10.0.0.1/32

More investigation can be done in Dossier which is accessible under Analyze and is included in ActiveTrust Plust an Advanced subscriptions.