Infoblox

DEPLOYMENT GUIDE

DoT and DoH Mitigation Guide

Table of Contents

Introduction

The sudden rollout of encrypted DNS services in applications has left Infoblox customers with unexpected security gaps in their network architecture. The purpose of this guide is to help our customers address these gaps by using Bloxone™ Threat Defense features in combination with their traditional security solutions.

Why Make Changes To The DNS Protocol?

The concept of openness has been a fundamental feature of the Internet since its inception. Although users transmit sensitive information such as credit card numbers, email and passwords between their web browsers and websites using the secure HTTPS protocol, initial requests for Internet addresses and subsequent responses for website locations are transmitted in plain text. As a result, DNS has traditionally suffered from what we describe as a “last mile” security problem. Communications between a DNS client and its local DNS server are almost always unencrypted, and therefore subject to spoofing, interception, hijacking, and more problems. Improvements have been made to incorporate greater end-to-end security. DNS Security Extensions added authentication and data integrity checking to DNS, but the last leg of communication to the web browser was still open to spoofing.

Introducing DoT and DoH

Industry groups within the Internet Engineering Task Force (IETF) have proposed two mechanisms to address these issues. They work by encrypting the DNS communication between your operating system’s stub resolver and your recursive DNS resolver. One is known as DNS over TLS (Transport Layer Security) or “DoT”, and the other is DNS over HTTPS or “DoH.” Both technologies ensure data privacy and authentication by encrypting communications between DNS clients and servers. However, in doing so, each point to external DNS resolvers, thereby allowing client devices to access DNS services outside of your control and exposing the enterprise to potential security risk.

DNS over TLS (DoT)

DoT is an IETF standard that uses the common Transmission Control Protocol (TCP) as a connection protocol to layer over TLS encryption and authentication between a DNS client and a DNS server. Functioning at the operating system level, it communicates over TCP port 853. This is a well-known port used for all encrypted DNS traffic, and network administrators are very familiar with it. DoT traffic is encrypted, but its use of a well-understood port makes it easier for network administrators to monitor and control encrypted DNS when it appears. DoT is also a mature standard backed by traditional players in the DNS industry.

DNS over HTTPS (DoH)

Backed by the Mozilla Foundation and Chromium Projects, DoH is the other IETF security protocol that addresses DNS client and DNS server communication security. It leverages the security protocol extension HTTPS to provide encryption and authentication between a DNS client and server. A potential problem with DoH is that it uses the same TCP port (443) that all HTTPS traffic uses. As a result, it might prove challenging to troubleshoot DoH-related DNS issues because of the inability to distinguish DoH-based DNS requests from regular HTTPS requests. For example, if a network administrator is employing DNS monitoring to block DNS requests to known malicious domains, he or she would not see those particular requests in HTTPS. Hence, that malicious traffic would go undetected. In addition, DoH operates at the application layer rather than the operating system, which introduces the potential for browser traffic to bypass enterprise DNS controls. The circumvention of DNS controls could hamper the support team’s ability to maintain the levels of network performance, security, scale, and reliability that enterprises demand from DNS.

DoT and DoH Enterprise Challenges

Please refer to this Solution Note https://www.infoblox.com/wp-content/uploads/infoblox-solution-note-dot-and-doh-present-new-challenges.pdf

Recommended Best Practices

We recommend a two-stage approach to mitigate the threat from unauthorized DNS services:

Stage 1: Observe

Footnote: Some customers may not want to leave the observation stage and may not need to block access to DoH resolvers.

Stage 2: Block

At this stage, customers would block direct DNS traffic—including DoT and DoH—between internal IP addresses and DNS servers on the Internet (Figure 1). This step will ensure that end-users employ their company's internal DNS infrastructure, allowing their IT organization to comprehensively apply DNS resolution policy and troubleshoot problems.

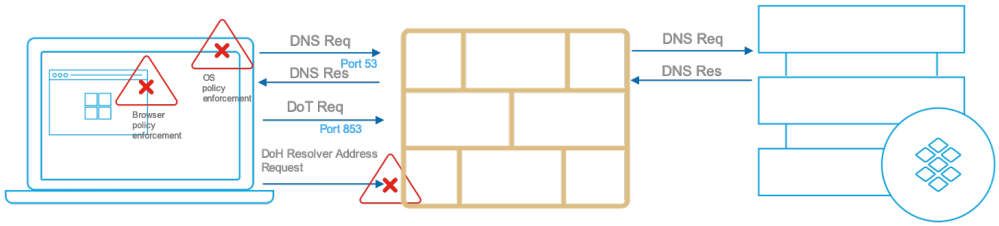


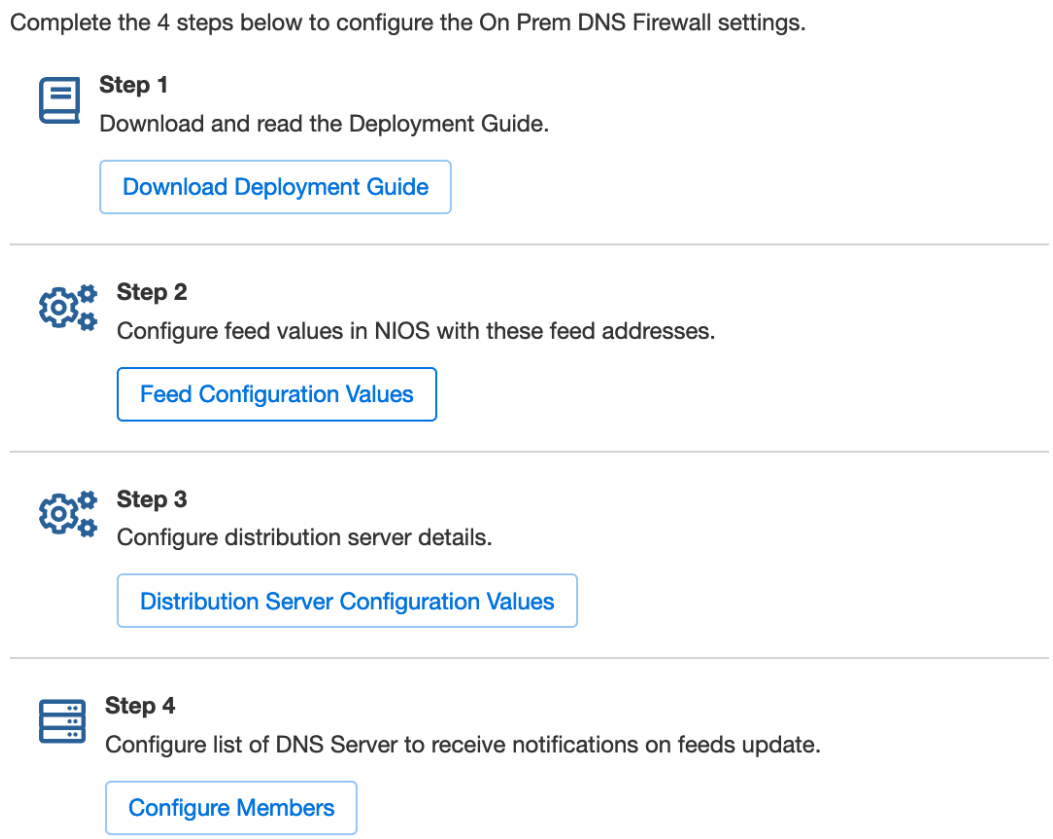
Figure 1: Block DoT and DoH

Instructions

Configuring NIOS to download the DoH feed

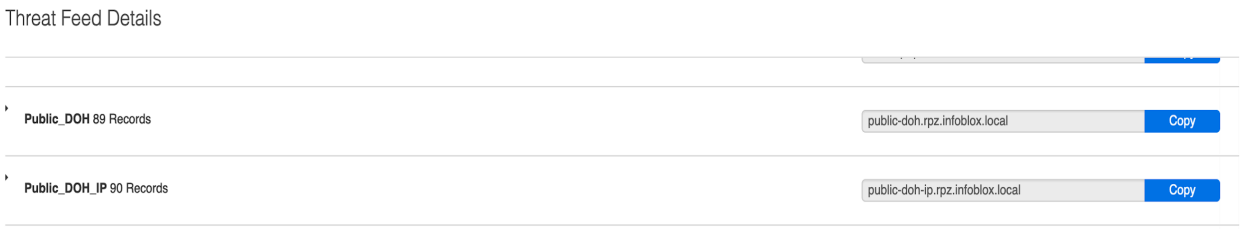
Navigate to Policies>On-Prem DNS Firewall to configure the On-Prem DNS Firewall service. Complete the four-step process to configure your On-Prem DNS Firewall settings. Please note, downloading of the Infoblox Threat Intelligence Feed Deployment Guide is Step 1 of the process. Once you have reviewed the guide, please proceed to Step 2 to begin the configuration process.

1. Click Download Deployment Guide. Read through the guide thoroughly before proceeding to the next step where you will configure your NIOS feeds.



2. Feed Configuration

Click **Feed Configuration Values** to configure the NIOS feed values with the provided feed addresses based on your subscription. Copy these values to a text editor as you require them later for NIOS configuration. Please note, the record count associated with a feed is published along with the feed's description. Once completed, click **Close** and proceed to **Step 3**.



3. Distribution Server Configuration Values

Click **Distribution Server Configuration Values** to configure your distribution servers. Both IPv4 and IPv6 IP addresses may be used to serve your feeds, depending on your specific requirements. TSIG Key encryption

algorithms supported include HMAC MD5 512-bit and HMAC 256 256-bit. Please be aware; it may take up to one hour before your newly created TSIG keys become active.

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

1. On the **Distribution Server Details** screen, for **BLOXONE HITS RPZ FEED**, toggle the switch to Enable to add the option of a custom RPZ feed to the feed distribution. When enabling the custom RPZ feed, specify the maximum number of feed indicators the custom RPZ feed will return along and an expiration date for the indicators.

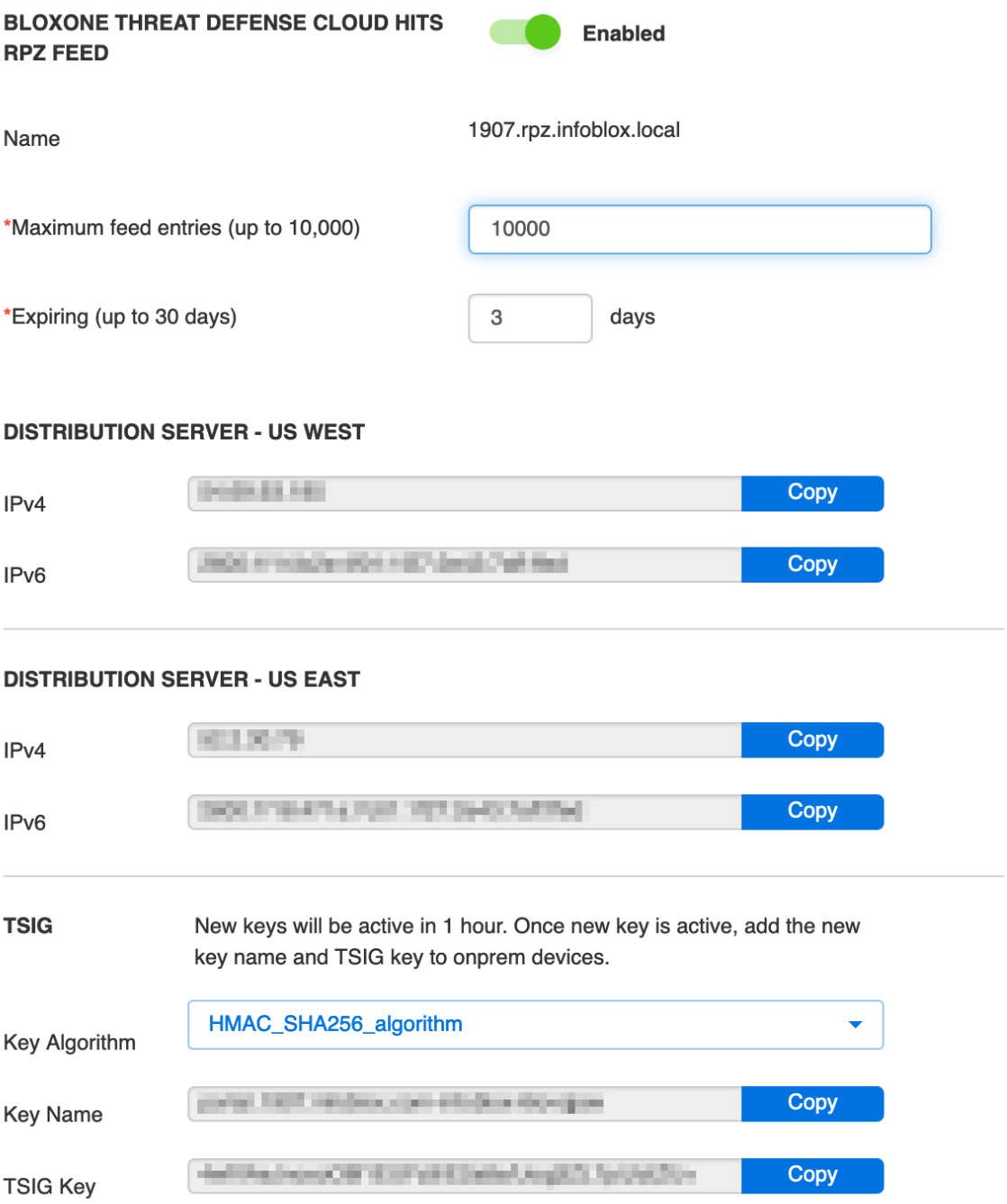
2. Select either the IPv4 or IPv6 IP options for both the US West Distribution and the East Distribution Servers.

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

4. Select a TSIG Key algorithm from among the drop-down menu choices. Algorithm choices include HMAC MD5 512-bit and HMAC 256 256-bit. Once you have made your selection, click **Generate** to generate a new TSIG key.

5. Copy and save the Key Name and TSIG Key.

6. Once completed, click **Close** and proceed to **Step 4.**



4. Configuring Threat Feed Retrieval Members

Click **Configure Members** to configure your list of threat retrieval members. You can add and remove members as suits your needs.

To add a threat retrieval member, complete the following steps:

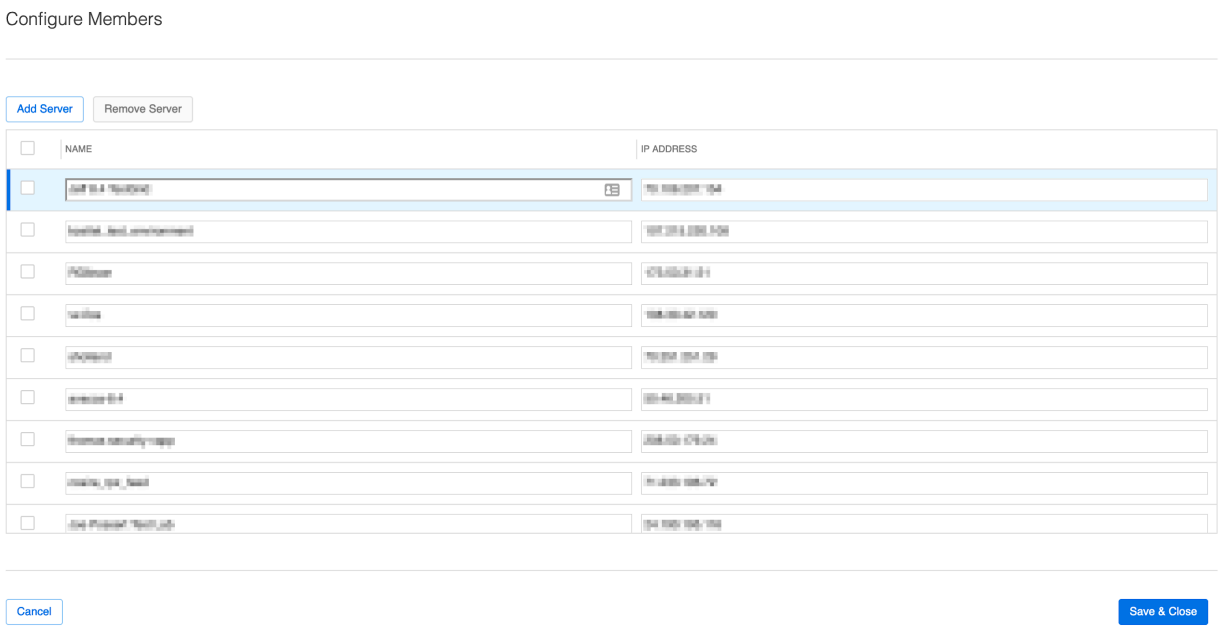
1. Click **Add.** A new row will populate at the bottom of the list.
2. Select the new row by selecting the box next to it.

3. In the **NAME** field, add a name for the member you are adding.
4. In the **IP ADDRESS** field, add the IP address you want to use for the new member.
5. Once you have finished adding members, you can remove any members you will not be using.

To remove a threat retrieval member, complete the following steps:

1. Select the configured member you want to remove by selecting the box next to it.
2. Click Remove.

Once you have configured your threat retrieval members, click **Save & Close**.



This completes the Cloud Services Portal, On-Prem DNS Firewall portion for the setup and configuration of Infoblox Threat Intelligence feeds. Please proceed to the next page to configure NIOS.

NIOS Configuration

License and Configuration Requirements

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

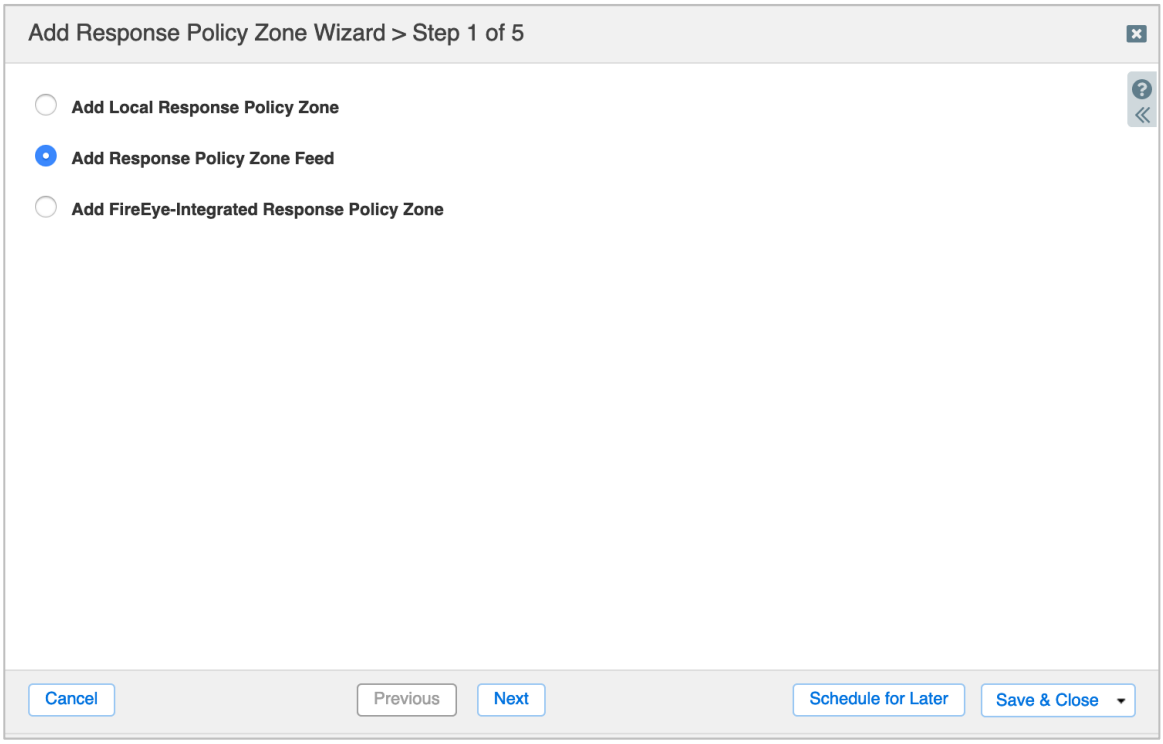
To obtain the feeds, your member will need access to our Threat Intelligence Feed servers on port 53 (UDP and TCP) as the feed data is transferred through a DNS zone transfer. Your server will also need to be able to perform recursion to obtain a response from the Internet.

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

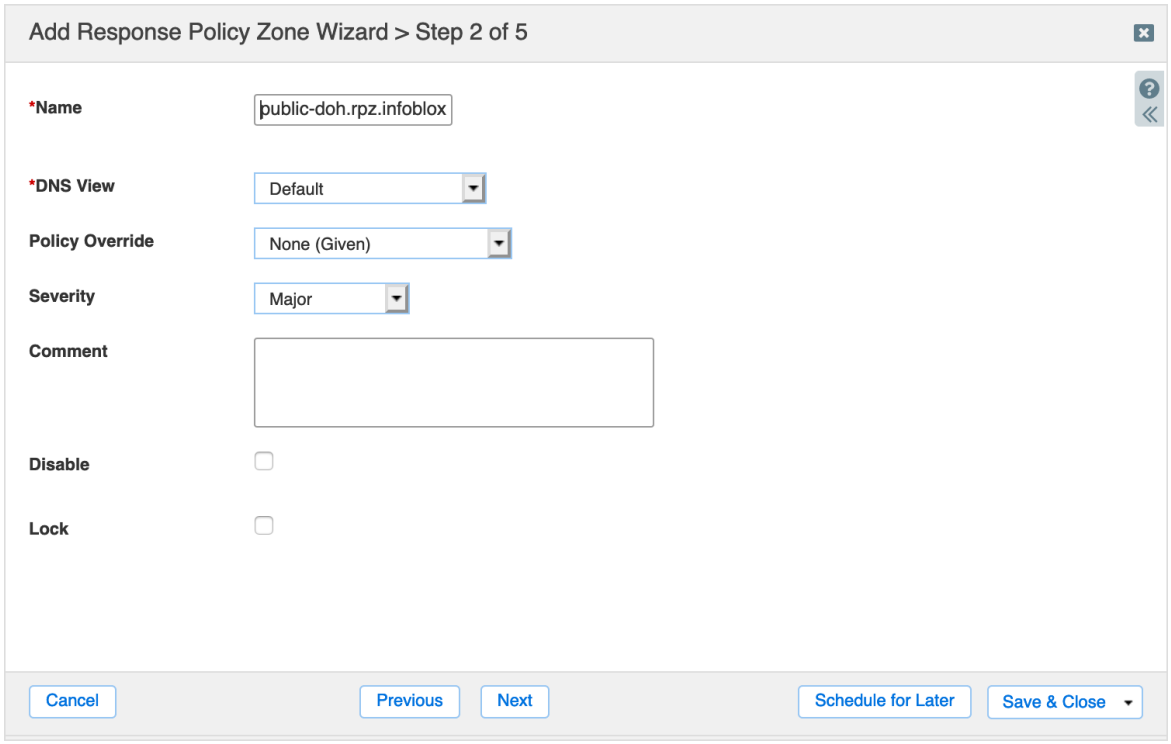
In NIOS navigate to: “Data Management” -> DNS -> “Response Policy Zones” Press the + button or use “Add” in the sidebar.

1. Select ‘Add a Response Policy Zone Feed’ then press next.



2. Add the feed you want to use. In the case of DoH feeds, choose Public_DoH and Public_DoH_IP.

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.



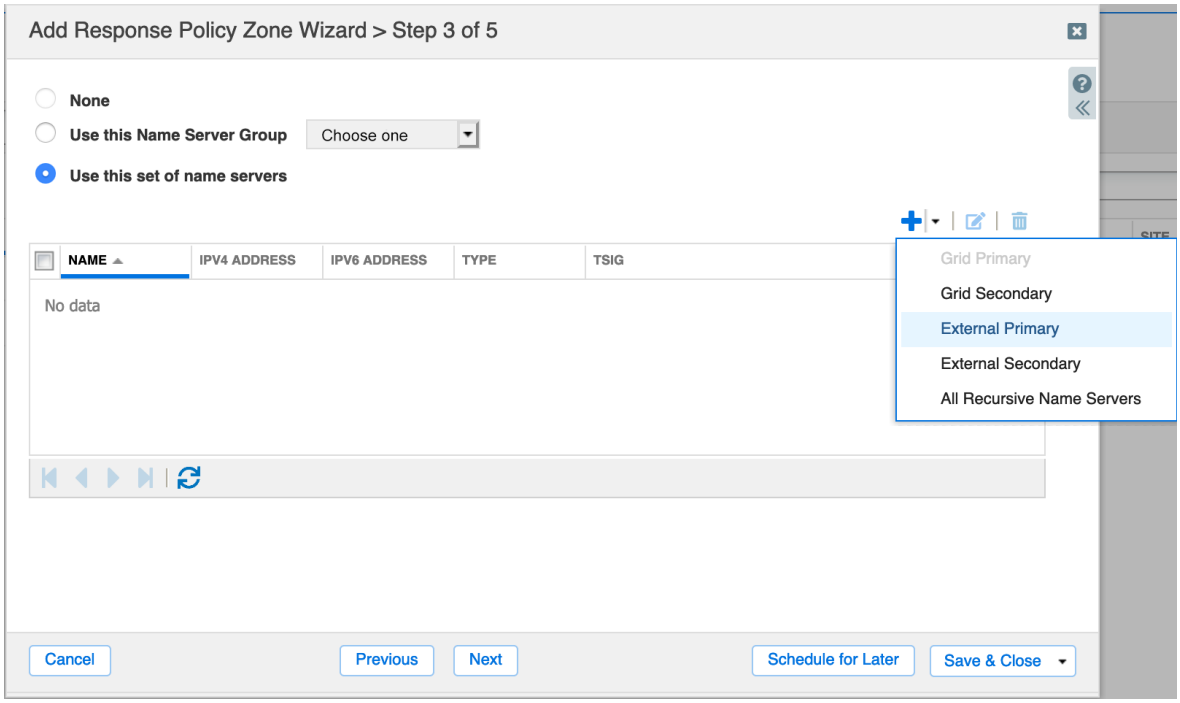
Leave Policy override on “None (Given)” for now. For the other policy override settings, please refer to the Admin Guide.

Modify logging Severity if needed

Press “Next”

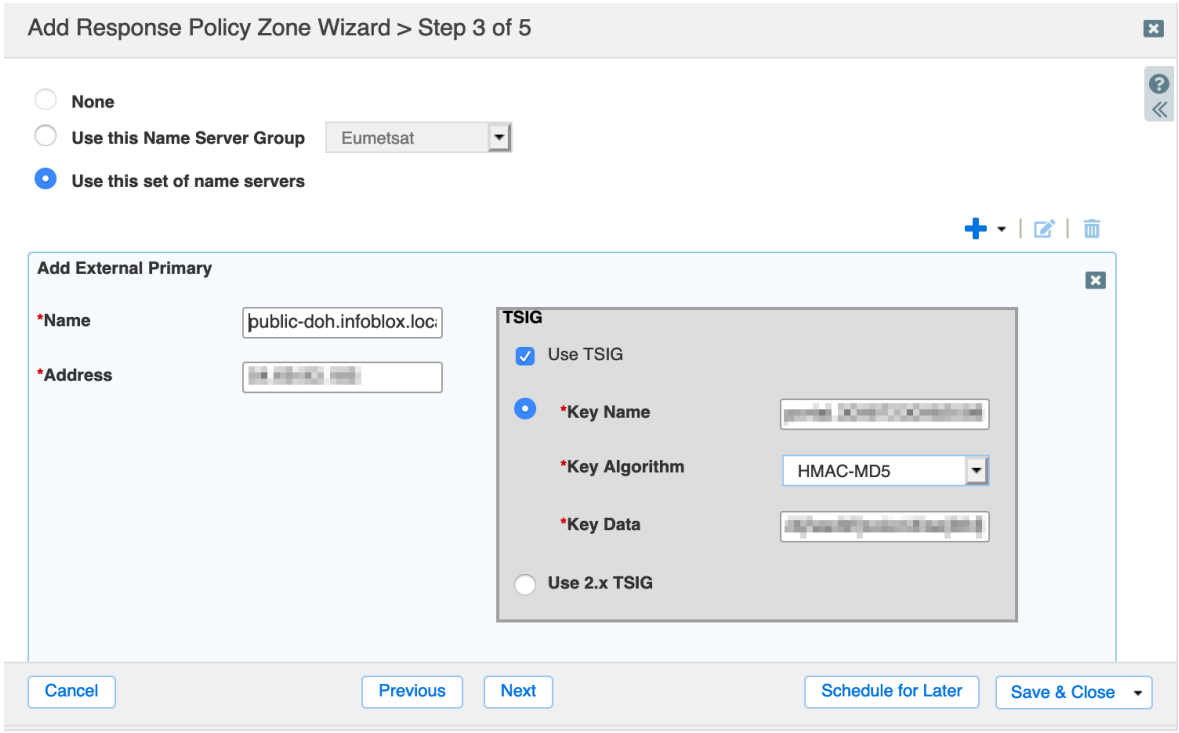
3. Add the External Primary

Use the drop-down next to the “+” sign to select External Primary

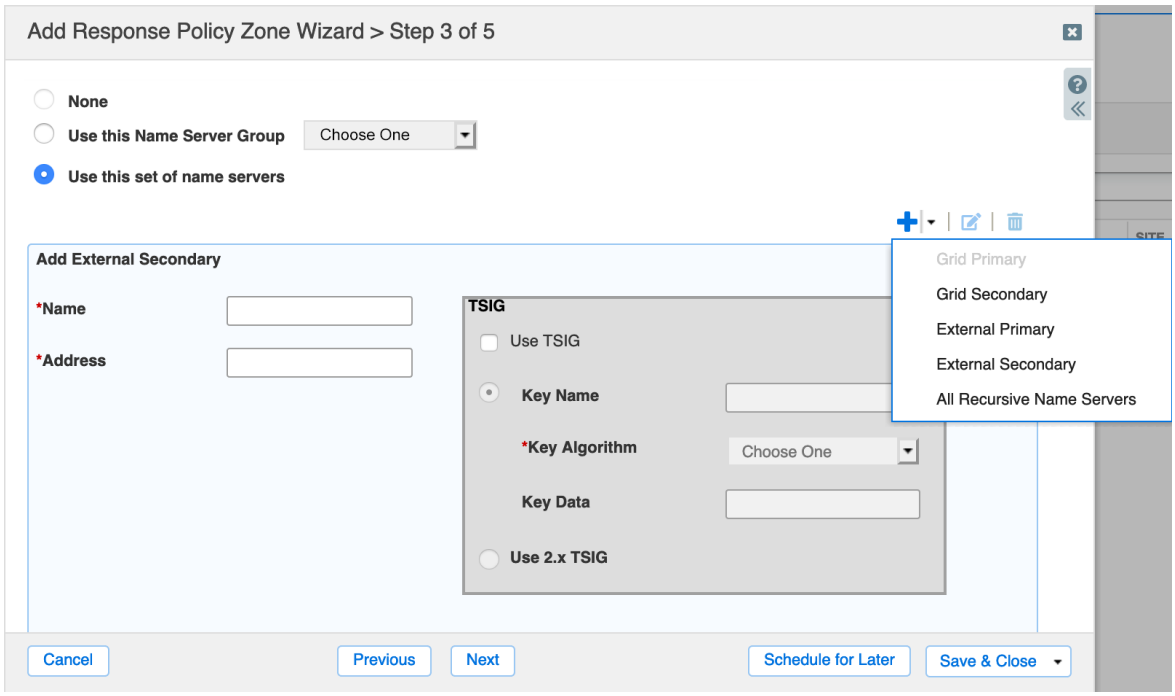


4. Define the External Primary's settings

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.



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 correct 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 a message that includes “transfer.”

Generating & Reviewing Hits

1. Navigate to the data management → dns → response policy zones.
2. Find the Public_DOH or Public_DOH_IP feed.
3. Click on one of the feeds to export to a .csv file.
4. Pick an entry from the .csv file.
5. Run nslookup or dig against the member with the IP address or name.
6. 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.

Configuring BloxOne DDI to forward all queries to BloxOne ThreatDefense

Please follow the instructions in the following link:
https://docs.infoblox.com/display/BloxOneDDI/Configuring+DNS+Forwarding+Proxy+and+BloxOne+DDI+DNS

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com