

Deployment Guide

# **DNS Firewall Deployment Guide**



# Table of Contents

Introduction	3
Data Flow for DNS Firewall	3
Requirements	4
Types of RPZs	4
Best Practices	4
Best Practices for FireEye Integrated RPZs	4
Deployment Summary	5
Deployment Instructions	5
Configure Local RPZ	5
Configure RPZ Feed with Infoblox Active Trust	13
Troubleshooting	20

### 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 you can implement policy controls for DNS lookups.

This deployment guide shows how to deploy DNS Firewall.

## **Data Flow for DNS Firewall**



There are five steps to a malware attack\*:

- 1. Entry downloading of the malware code from either an infected website or email with an attachment or link that hijacks the user's browser.
- 2. Distribution Initial malware redirects the user's browser to a select malicious site.
- 3. Exploit an exploit kit now probes the computer for vulnerabilities.
- 4. Infection Malicious payload is downloaded and infects the user's system with malware.
- 5. Execution The malware calls home with sensitive data or attempts to extort the user for money (ransomeware).

#### \*source: Sophos.com

Step 5 is where DNS firewall gets involved. The malware performs a command and control step to steal sensitive data. In order to talk to the command and control server, the malware makes a call to the DNS to resolve the name of the command and control server. With DNS firewall and its local reputation entries and/or reputation entries from a reputation feed, the DNS resolution can be blocked or redirected to a walled garden website. With Infoblox, indications of a reputation hit can be seen in the syslog (i.e. CEF messages) or DNS RPZ report from the reporting server. At this point, the workstation can be tracked down via IP address, username, and switchport to clean off the malware.

## **Requirements**

The following items are required for DNS Firewall:

- RPZ license per recursive DNS member that will have DNS Firewall enabled.
- Access to the Infoblox Cloud Service Platform RPZ management portal (https://csp.infoblox.com) or other reputation feeds like Spamhaus.
- Infoblox NIOS 8.0 or later is recommended.

## **Types of RPZs**

- Local RPZ–A local RPZ is a zone that allows administrators to define multiple response policies locally. Query responses sent are based on the defined rules.
- RPZ Feed–An RPZ feed receives response policies from external sources. DNS clients receive responses based on the imported rules from a reputable source.
- FireEye integrated RPZ–By integrating the NIOS appliance with the FireEye appliance, you can detect
  malware and APTs and take necessary actions to mitigate those threats by importing updates from
  FireEye appliance into a FireEye RPZ.

#### **Best Practices**

- When you enable Infoblox DNS Firewall, DNS performance for all queries, recursive or authoritative, will be affected.
- If you have multiple DNS servers in a Grid, ensure that you configure RPZs on the recursive server that is closest to your DNS clients. If you configure RPZs on second level DNS caching servers, you will not be able to identify the DNS clients because only the IP addresses of the forwarding name servers can be identified.
- Infoblox recommends that you preview your RPZ rules to ensure ruleset integrity and to avoid unexpected results. You can preview your rules by selecting Log Only (Disabled) when you configure Policy Override for an RPZ, RPZ feed, or FireEye integrated RPZ.
- The appliance logs all matching and disabled rules for all queries in the syslog. You can view the syslog to ensure that the rules are set up correctly before they take effect. Ensure that you enable rpz in the Logging Category of Grid DNS Properties editor to log these events.
- You can use the standard TSIG mechanism to ensure that feed zones come from the correct servers. Grid members can function either as a primary or secondary server for the RPZ. As with hosting any zone as a secondary, please ensure that the appliance is sized properly to hold the zone contents in memory.
- You can only export or import the RPZ local zones using the CSV export or import feature, but you cannot import or export FireEye zones using this feature.
- Note that the NIOS blacklist and NXDOMAIN features take precedence over RPZs.
- In order to leverage DNS notify messages to trigger zone transfer of the feed zone, port 53 incoming on the lead secondary must be open to receive such messages (TCP and UDP). If not, the zone will refresh based on the refresh setting in the SOA.
- The name of the zone, which is assigned to an RPZ member, must not exceed 256 characters. The name can be a combination of alphanumeric characters. When the name exceeds this limit, respective zone fails to load.

#### **Best Practices for FireEye Integrated RPZs**

Before you configure a FireEye integrated RPZ, consider the following:

- FireEye integrated RPZs inherit default values from local RPZs. You can create, edit and delete rules using the Infoblox GUI, API, and RESTful API.
- To avoid false positives, Infoblox recommends that you create a whitelist of allowed zones using a local RPZ that is sorted above the FireEye RPZ and add your own domain to the whitelist RPZ. For example, you can add your company domain name, such as corp100.com. This list must contain popular domains, such as Alexa 250, and other desired domains.

- Note that there will be an impact on the storage capacity when you create a new FireEye alert and
  map it with an RPZ rule. The processing of alerts will consume a few CPU cycles, which will have
  some impact on the system.
- You must properly configure the settings on a FireEye appliance. NIOS supports only Per Event delivery mechanism and JSON Normal message format. To ensure that the NIOS appliance process alerts properly, configure the FireEye appliance accordingly.
- You cannot add a FireEye integrated RPZ during a scheduled full upgrade. However, updates to the CNAME record are processed during a full upgrade. NIOS updates CNAME records in the database to store information that is specific to FireEye alerts.
- The rules created due to insertion of alerts will be visible through the FireEye RPZ viewer. Infoblox recommends that you do not modify any internal objects. For more information, see Viewing RPZs on page 1690.
- Note that SSL certificate validation is not supported.
- You must verify the following after you configure the FireEye and NIOS appliances:
  - The URL configured on the FireEye appliance matches the URL in the FireEye integrated RPZ on NIOS.
  - Verify the username and password for FireEye admin on the FireEye appliance.
  - Ensure that the settings are properly configured on the FireEye appliance.
  - Verify the state of the FireEye appliance.
  - Do note that all settings are case sensitive.
- Note that the frequency of alerts received from FireEye can be minimal. A very small number of alerts are generated on a weekly basis. For example, the FireEye appliance may generate only tens of alerts per day.

## **Deployment Summary**

- Install a valid RPZ license. Refer to the Infoblox NIOS administrators guide for more information.
- Enable recursion for your DNS view in which you want to deploy RPZs.
- Configure RPZ logging to ensure all matching and disabled rules for all queries are logged in the syslog. Refer to the Infoblox NIOS administrator guide for more information.
- Configure RPZs.

## **Deployment Instructions**

Configure Local RPZ.

1. Log into the Infoblox GUI.

~	<b>NI 1 1 1</b>				
2.	Navigate to	Data Manac	jement → DNS	→ Response	Policy Zones.

		Cuper Heat	Devices Diver	DND	la Distribution							
	IPAM VLANS	Super Host	Devices DHCF	DNS FI	le Distribution	eleverent Di			1004.0	<b></b>	Toolbar	
default	Name Server Groups	Shared Hecor	d Groups Respo	onse Policy Zones	Subscriber Services De	ployment BI	acklist Hules	sets DN	VS64 Groups	Qu	+ Add	
	off Filter O	In Show Eiltor									→ Open	
None		Show Piller									Edit	
→   <b>+</b>   ⊠   îi •   <b>1</b>	•   🖶						Go to			Go	Extensible	
	NAME	TYPE	SEVERITY	PRIMARY NAME S	LAST UPDATED	COMMENT	M	JLTI-MASTER 2	Z SITE		E Permissions	
No data											Order Response Policy Zones	
											Copy Rules	
											Threat Insight in the Cloud Client	
											Manage Dynamic Update Groups	
											🛓 Import Zone	
											B Move DNS View	
											Grid DNS Properties	
											C Restart Services	
											CSV Import CSV Job Manager	
											Z IDN Converter	
Click on the '+'	button to	hring u	n the RE	97 wizar	'n							
Click on the '+'	button to	b bring u	p the RF	PZ wizar	d.							
Click on the '+' Add Response	button to e Policy Zo	o bring u one Wiza	p the RF ard > Step	PZ wizar 0 1 of 5	d.							
Click on the '+' Add Response	button to e Policy Zo	o bring u one Wiza	p the RF ard > Step	PZ wizar 1 of 5	d.							
Olick on the '+' Add Response Add Local R	button to e Policy Zo esponse Poli	o bring u one Wiza icy Zone	ip the RF ard > Step	PZ wizar 1 of 5	d.							
Olick on the '+' Add Response Add Local R	button to e Policy Zo esponse Poli	o bring u one Wiza icy Zone	p the RF urd > Step	PZ wizar 1 of 5	d.							
Olick on the '+' Add Response Add Local R Add Respon	button to e Policy Zo esponse Poli se Policy Zo	o bring u one Wiza icy Zone ne Feed	p the RF urd > Step	PZ wizar	d.							
Click on the '+' Add Response Add Local R Add Respon Add FireEye	button to e Policy Zo esponse Poli se Policy Zo -Integrated R	o bring u one Wiza icy Zone ne Feed Response Po	p the RF rrd > Step olicy Zone	PZ wizar 9 1 of 5	d.							
Click on the '+' Add Response Add Local R Add Respon Add FireEye	button to e Policy Zo esponse Poli se Policy Zoo -Integrated R	o bring u one Wiza icy Zone ne Feed Response Pa	p the RF ard > Step olicy Zone	PZ wizar 9 1 of 5	<u>d.</u>							
Click on the '+' Add Response  Add Local R  Add Respon  Add FireEye	button to e Policy Zo esponse Poli se Policy Zou -Integrated R	o bring u one Wiza icy Zone ne Feed Response Po	ip the RF ard > Step olicy Zone	PZ wizar 0 1 of 5	rd.							
Click on the '+' Add Response  Add Local R  Add Respon  Add FireEye	button to e Policy Zo esponse Poli se Policy Zo -Integrated R	o bring u one Wiza icy Zone ne Feed Response Po	ip the RF ard > Step olicy Zone	PZ wizar	d.							
Click on the '+' Add Response Add Local R Add Respon Add FireEye	button to e Policy Zo esponse Poli se Policy Zo -Integrated R	o bring u one Wiza icy Zone ne Feed Response Pa	ip the RF ard > Step olicy Zone	PZ wizar	d.							
Click on the '+' Add Response Add Local R Add Respon Add FireEye	button to e Policy Zo esponse Poli se Policy Zor -Integrated R	o bring u one Wiza icy Zone ne Feed Response Pr	ip the RF ard > Step olicy Zone	PZ wizar	<u>d.</u>							
Click on the '+' Add Response Add Local R Add Respon Add FireEye	button to e Policy Zo esponse Poli se Policy Zoo -Integrated R	o bring u one Wiza icy Zone ne Feed Response Po	ip the RF ard > Step olicy Zone	PZ wizar	rd.							
Click on the '+' Add Response Add Local R Add Respon Add FireEye	button to e Policy Zo esponse Poli se Policy Zo -Integrated R	o bring u one Wiza icy Zone ne Feed Response Po	ip the RF ard > Step olicy Zone	PZ wizar	rd.							
Click on the '+' Add Response Add Local R Add Respon Add FireEye	button to e Policy Zo esponse Poli se Policy Zo -Integrated R	o bring u one Wiza icy Zone ne Feed Response Po	ip the RF ard > Step olicy Zone	PZ wizar	rd.							
Click on the '+' Add Response Add Local R Add Respon Add FireEye	button to e Policy Zo esponse Poli se Policy Zo -Integrated R	o bring u one Wiza icy Zone ne Feed Response Pa	ip the RF ard > Step olicy Zone	PZ wizar	rd.							
Click on the '+' Add Response Add Local R Add Respon Add FireEye	button to e Policy Zo esponse Poli se Policy Zo -Integrated R	o bring u one Wiza icy Zone ne Feed Response Pr	ip the RF ard > Step olicy Zone	PZ wizar	rd.							
Click on the '+' Add Response Add Local R Add Respon Add FireEye	button to e Policy Zo esponse Poli se Policy Zor -Integrated R	o bring u one Wiza icy Zone ne Feed Response Pr	ip the RF ard > Step olicy Zone	PZ wizar	rd.							
Click on the '+' Add Response Add Local R Add Respon Add FireEye	button to e Policy Zo esponse Poli se Policy Zou -Integrated R	o bring u one Wiza icy Zone ne Feed Response Po	ip the RF ard > Step olicy Zone	PZ wizar	rd.							
Click on the '+' Add Response Add Local R Add Respon Add FireEye	button to e Policy Zo se Policy Zo -Integrated R	o bring u one Wiza icy Zone ne Feed Response Po	ip the RF ard > Step olicy Zone	PZ wizar	rd.							
Click on the '+' Add Response Add Local R Add Respon Add FireEye	button to e Policy Zo esponse Poli se Policy Zo -Integrated R	o bring u one Wiza icy Zone ne Feed Response Pa	ip the RF ard > Step olicy Zone	PZ wizar	rd.							
Click on the '+' Add Response Add Local R Add Respon Add FireEye	button to e Policy Zo esponse Poli se Policy Zo -Integrated R	o bring u one Wiza icy Zone ne Feed Response Pa	ip the RF ard > Step olicy Zone	PZ wizar	rd.							

#### 4. Click on the Next button.

Add Response Polic	y Zone Wizard > Step 2 of 5		×
*Name	local-rpz		<b>?</b> «
Policy Override	None (Given)		
Severity	Major 🗘		
Comment			
Disable			
	Disabling large amounts of data may take a longer time to execute.		
Lock			
Cancel	Previous Next	Schedule for Later S	Save & Close 🔹

- 5. Type in a name for the local RPZ.
- 6. The Policy Override drop down menu allows you to override all of the policy rules for each RPZ entry. The choices are:
  - I. None means allow the policy to be enforced at the rule level.
  - II. Log only if a rule is hit, then no action will be taken and a syslog message will be logged. This setting is good for testing purposes.
  - III. Block (No data) on a rule hit, the response will contain no data.
  - IV. Block (No such domain) on a rule hit, the response will be no such domain. This is the same as NXDomain in the output of a dig command.
  - V. Passthru-sends a response without modification
  - VI. Substitute a preconfigured domain is passed back as a response such as a walled garden website.
- Severity drop down menu specifies the severity number to be assigned in the syslog entry. The choices are:
  - I. Major (default)
  - II. Critical
  - III. Warning
  - IV. Informational
- 8. Enter details of this RPZ into the comment box.
- 9. The Disable button allows for disabling this RPZ.
- 10. The Lock button allows for locking the configuration to prevent other users from making changes.

#### 11. Click Next.

dd Respons	e Policy Zone W	/izard > Step 3	of 5			×
None Use this Nar Use this set	me Server Group	Choose One				Go « Go
_1					+ +	
NAME 🔺	IPV4 ADDRESS	IPV6 ADDRESS	TYPE	TSIG	Grid	Primary
No data					Grid	Secondary
					Exte	ernal Secondary
					All F	Recursive Name Servers
	l 🕄					
						_

12. Click on 'Use this set of name servers' to assign the DNS member that will service this local RPZ.

13. Click on the '+' button to select the server. The choices are:

- I. Grid Primary this will be the primary server for the zone.
- II. Grid Secondary this will be the secondary server for the zone.
- III. External Secondary specify an external server that is outside of the Grid.
- IV. All Recursive Name Servers this zone is assigned to all recursive servers as secondary servers.

14. For this example, select Grid Primary.

Add Response Policy Zone Wizard > Step 3 of 5	×
<ul> <li>None</li> <li>Use this Name Server Group</li> <li>Choose One \$</li> <li>Use this set of name servers</li> </ul>	<b>9</b> «
	+ •   ☑   面
Add Grid Primary Select Clear	
	Add Cancel
NAME A IPV4 ADDRESS IPV6 ADDRESS TYPE TSIG	
No data	
Cancel Previous Next	Schedule for Later Save & Close •
Click on the Select button.	
Click on the Select button. Add Response Policy Zone Wizard > Step 3 of 5	×
Click on the Select button. Add Response Policy Zone Wizard > Step 3 of 5 None Use this Name Server Group Choose One	X 2 3 4
Click on the Select button. Add Response Policy Zone Wizard > Step 3 of 5 None Use this Name Server Group Choose One \$ Use this set of name servers	x ? «
Click on the Select button. Add Response Policy Zone Wizard > Step 3 of 5 None Use this Name Server Group Choose One Use this set of name servers	¥ ? ≪
Click on the Select button. Add Response Policy Zone Wizard > Step 3 of 5 None Use this Name Server Group Choose One ‡ Use this set of name servers Add Grid Primary Select Clear isedemogen testlab.com	
Click on the Select button. Add Response Policy Zone Wizard > Step 3 of 5 None Use this Name Server Group Choose One ‡ Use this set of name servers Add Grid Primary Select Clear isedemogm.testlab.com	¥ ? ∢ ↓ •   2   1
Click on the Select button. Add Response Policy Zone Wizard > Step 3 of 5 None Use this Name Server Group Choose One Use this set of name servers Add Grid Primary Select Clear isedemogm.testlab.com	
Click on the Select button. Add Response Policy Zone Wizard > Step 3 of 5 None Use this Name Server Group Choose One Use this set of name servers Add Grid Primary Select Clear isedemogm.testlab.com	X
Click on the Select button. Add Response Policy Zone Wizard > Step 3 of 5 None Use this Name Server Group Choose One Use this set of name servers Add Grid Primary Select Clear isedemogm.testlab.com	Image: Second state         Image: Second st
Click on the Select button. Add Response Policy Zone Wizard > Step 3 of 5 None Use this Name Server Group Choose One ‡ Use this set of name servers Add Grid Primary Select Clear isedemogm.testlab.com	₹
Click on the Select button. Add Response Policy Zone Wizard > Step 3 of 5 None Use this Name Server Group Choose One ‡ Use this set of name servers Add Grid Primary Select Clear isedemogm.testlab.com NAME _ IPV4 ADDRESS TYPE TSIG No data	↓ ~          □         ↓ ~          □         ↓ ~          □         ↓ ~          □         ↓ ~          □         ↓ ~          □         ↓ ~          □
Click on the Select button. Add Response Policy Zone Wizard > Step 3 of 5 None Use this Name Server Group Choose One Use this set of name servers Add Grid Primary Select Clear isedemogm.testlab.com MAME  IPV4 ADDRESS IPV6 ADDRESS TYPE TSIG No data	Image: Second seco

15.

#### 16. Click on the Add button.

None Use this Name Server Group Choose One	
Ise this set of name servers	2 () ()
Cancel     Previous     Next     Schedule for Later     Sa       lick on Save and Close.     schedule for Later     Schedule for	ave & Close •
IPAM VLANs Super Host Devices DHCP DNS File Distribution	
Zones Members Name Server Groups Shared Record Groups Response Policy Zones Subscriber Services Deployment Blacklist Rulesets DNS84 Groups Qu	ir 🚿 🤅
	pen
	slete + + + + + + + + + + + + + + + + + +
	rder Response
Image: Control of the control of t	olicy Zones opy Rules
Image: Condex and Condex an	opy Rules reat Insight the Cloud Client
Image: Second and the second and t	anage Dynamic odda Groups
Image: Conduct Conduc	Dicy Zones ppy Rules vreat Insight the Cloud Client anage Dynamic date Groups upport Zone en DND Plane
Image: Control of the control of th	blicy Zones pp Rules preat Insight the Cloud Client anage Dynamic odate Groups aport Zone ove DNS View tid DNS conselline
Image: Concernent of the concernent	por Zones oppy Rules wreat Insight the Cloud Client anage Dynamic dotte Groups uport Zone ove DNS View opperties estart Services
Image: Concert and the concert	objey Zones opy Rules reat Insight the Cloud Clent anage Dynamic odate Groups opper Zone over DNS View rid DNS coperties estart Services SV Import SV Job Manager
Image: Area and a construction of the construction of t	blicy Zones oppy Fules wreat Insight the Cloud Client anage Dynamic date Groups uport Zone over DNS View operfus sestart Services SV Import SV Job Manager N Converter

19. Click on the name of the local RPZ.

Zones Members	Name Sen	ver Groups Shared Reco	rd Groups Resp	onse Policy Zones	Subscriber Services Deployment	Blacklist Rulesets	DNS64 Groups Qu	Toolbar	
sponse Policy Zones Home								+ Add	-
cal-rpz 🛛 🔒 🥖	<b>8</b>							→ Open	
Quick Filter None	~ 0	Filter On Show Filter	ir					Edit	
								Extensible	1
• •   🗹   🛅 •   🗘	• •					Go to	Go	Attributes	
Passthru Rule	Þ	DATA		COMME	T SITE			Permissions	
Block (No Such Domain	n) Rule ▶							Order Response Policy Zones	
Substitute (Domain Na	P ne) Rule It	Block Domain Name (No	Data) Rule					Copy Rules	
Substitute (Record) Ru	e ⊧	Block IP Address (No Da Block Client IP Address (	ta) Hule No Data) Rule					Threat Insight in the Cloud Client	
								Manage Dynamic Update Groups	
								🛃 Import Zone	
								E Move DNS View	
								Grid DNS Properties	
								C Restart Services	
								📩 CSV Import	
								🔎 CSV Job Manager	
								➡ IDN Converter	

20. Click on the '+' button to select a rule type. For example, select Block (No Such Domain) → Block Domain Name.

Add a Block Domain Name (No Data) Rule > Step 1 of 3								
Name	www.yahoo.com .local-rpz Select Zone Clear	<b>?</b>						
DNS View	default							
Policy	Block (No Data)							
Comment								
Disable								
Cancel	Previous Next Schedule for Later Save & Close	•						

21. Enter a URL or domain like the above.

#### 22. Click Save and Close.

Infoblox 📚 🛛 🗖 🔤	ashboards Data M	Management Smart Fo	lders Reporti	ing Grid	Administration				Q Search	admin	•
IPA	AM VLANs S	Super Host Devices	DHCP DNS	File Distributi	on						
Zones Members Nar	me Server Groups	Shared Record Groups	Response Policy	Zones Subsc	riber Services Deployment	Blacklist Rulesets	DNS64 Groups	Qu	Toolbar	»	0
Response Policy Zones Home IOCal-rpz A P R Quick Filter None + •   2   = •   + •   E NAME OR ADDRESS P = WWW.yahoo.com B	Policy DA	Show Filter		COMMENT	SITE	Go to		Go	Add     Open     Cat     Delete     Extensible     Attributes     Permissions     Order Response     Policy Zones		

23. To test, run a dig (linux) or nslookup (windows). You should see a similar output. 10.60.16.25 is the DNS server with DNS Firewall enabled.

```
sc-l-thomasl:Documents thomasl$ dig @10.60.16.25 www.yahoo.com
; <<>> DiG 9.8.3-P1 <<>> @10.60.16.25 www.yahoo.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 10664
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; QUESTION SECTION:
;www.yahoo.com.
                                IN
                                        А
;; ADDITIONAL SECTION:
local-rpz.
                        900
                                IN
                                        SOA
                                                infoblox.localdomain. please_se
_email.absolutely.nowhere. 2 10800 3600 2419200 900
;; Query time: 3 msec
;; SERVER: 10.60.16.25#53(10.60.16.25)
;; WHEN: Thu Jan 26 19:29:18 2017
;; MSG SIZE rcvd: 131
```

24. Notice the NXDOMAIN status.

25. In addition, navigate to Administration → Logs → Syslog. Search for CEF (common event format) messages. This shows an RPZ hit did occur.



### Configure RPZ Feed with Cloud Services Portal.

- 1. Log into the Infoblox GUI.
- 2. Navigate to Data Management  $\rightarrow$  DNS  $\rightarrow$ Response Policy Zones.

Ir	roblox 📚		Dashboards	Data Management	Smart Folders	Reporting C	Grid Administration					Q Search	admin	
			IPAM VLAN	vs Super Host	Devices DHCP	DNS File	Distribution							
1	Zones	Members	Name Server Groups	s Shared Record C	Groups Response	Policy Zones	Subscriber Services Deployme	nt Blacklist Rule	esets DNS64 G	roups Qu	ery Monitoring		<b>#</b>	<b>G</b> «
	default		R											
	Quick Filte	rNone	✓ Off Filt	er On Show Filte	r									
	→   <b>+</b>	210.	1 🕹 - 1 🖶							Go to		Go		
			NAME	TYPE	SEVERITY	PRIMARY NAME S	LAST UPDATED	COMMENT	MULTI-MASTER Z	SITE				
		0	local-rpz	Local	Major	isedemogm.testl			No					

3. Click on the '+' button to bring up the RPZ wizard.

	Add Response Policy	y Zone Wizard > Step 1 of 5	×
	<ul> <li>Add Local Response</li> <li>Add Response Policy</li> <li>Add FireEye-Integrate</li> </ul>	Policy Zone y Zone Feed ed Response Policy Zone	<b>₽</b> ≪
4	Cancel	Previous Next Schedule for Later Save & C	Close •
4.	Add Response Policy	y Zone Wizard > Step 2 of 5	×
	*Name	base.rpz.infoblox.local	<b>?</b> «
	Policy Override Severity Comment	None (Given) Major	
	Disable	Disabling large amounts of data may take a longer time to execute.	
	Lock		
	Cancel	Previous Next Schedule for Later Save & C	Close •

- 5. Enter the name of the feed.
  - a. The choices for standard feeds are:

- 1. Base.rpz.infoblox.local
- 2. antimalware.rpz.infoblox.local
- 3. ransomware.rpz.infoblox.local
- 4. bogon.rpz.infoblox.local
- b. The choices for Plus or Advanced feeds are:
  - 1. Antimalware-ip.rpz.infoblox.local
  - 2. Bot-ip.rpz.infoblox.local
  - 3. Exploit-ip.rpz.infoblox.local
  - 4. Malware-dga.rpz.infoblox.local
  - 5. Tor-exit-node-ip.rpz.infoblox.local
  - 6. Multi-domain.surbl.rpz.infoblox.local
  - 7. Fresh-domain.surbl.rpz.infoblox.local
- 6. The Policy Override drop down menu allows you to override all of the policy rules for each RPZ entry. The choices are:
  - a. None means allow the policy to be enforced at the rule level.
  - b. Log only if a rule is hit, then no action will be taken and a syslog message will be logged. This setting is good for testing purposes.
  - c. Block (No data) on a rule hit, the response will contain no data.
  - d. Block (No such domain) on a rule hit, the response will be no such domain. This is the same as NXDomain in the output of a dig command.
  - e. Passthru-sends a response without modification
  - f. Substitute a preconfigured domain is passed back as a response such as a walled garden website.
- 7. Severity drop down menu specifies the severity number to be assigned in the syslog entry. The choices are:
  - a. Major (default).
  - b. Critical.
  - c. Warning.
  - d. Informational.
- 8. Enter details of this RPZ into the comment box.
- 9. The Disable button allows for disabling this RPZ.
- 10. The Lock button allows for locking the configuration to prevent other users from making changes.

#### 11. Click Next.

	Add Response Policy	Zone Wizard > Step 3	of 5			×	
	<ul> <li>None</li> <li>Use this Name Server</li> <li>Use this set of name s</li> </ul>	Group Choose One 🔹				•   12   m	
		ADDRESS IPV6 ADDRESS	ТҮРЕ	TSIG		Grid Primary	
	No data					Grid Secondary	
	NO Gala					External Primary	
						External Secondary	
						All Recursive Name S	ervers
	Cancel	Previous	Next		Schedule for Later	Save & Close 🔹	
12	For this type of RPZ	an external primar	v DNS ser	ver and Grid s	econdary serve	r need to be ad	ded
12.	Add Response Polic	v Zone Wizard > Ster	0 3 of 5				×
		,					0
	None	Chasses One	•				<b>%</b>
	Use this set of name	choose One	Ŧ				
		5 901 V01 9				<b>+</b> •   ⊠   i	Ū
	Add External Primary						×
	*Name	base.rpz.infoblox.local	TSIG				
	tê derese	54 00 00 405	🕑 Us	e TSIG			
	Address	54.69.93.185	•	Key Name	blox.com-infob	lox-rez78	
				Key Algorithm	HMAC-MD5	¢	
				Key Data	Jj2kVQydA7V4	H/hOkZ	
			O Us	e 2.x TSIG			
	Cancel	Previous	Next		Schedule for	r Later Save & C	ose 🔹
13	Add:						

- a. The name of the feed.
- b. The IP address of the feed server.
- c. Key name.

d. Key data which is the TSIG key.

Note: The feed name, external primary IP address, key name and TSIG key details will be provided from <u>https://csp.infoblox.com</u>.

- 14. Click on the 'Add' button.
- 15. Add the Grid Secondary server.

Add Response Policy Zone Wizard > Step 3 of 5							
None         Use this Name Server Group       Choose One \$         Use this set of name servers		<b>3</b>					
Add Grid Secondary         Select       Clear         Lead Secondary	+ -   🖻   🛅						
NAME _         IPV4 ADDRESS         IPV6 ADDRESS         TYPE         TSIG							
base.rpz.infob 54.69.93.185 Ext Primary blox.com-infoblox-rez788[Jj2kVQydA7V4	4H/hOkZ]						
Cancel Pravious Next Schedule for Le	star Save & Class	-					
Cancel Previous Next Schedule for La	save & Close	•					

16. Click on the one of the names. This server will store the feed when it is transferred.

Add Response Policy Zone Wizard > Step 3 of 5  None Use this set of name servers  Add Grid Secondary  Select Clour Sectemany Add Clarges  I Prev ADDRESS IPPE TER Base.rpz.intob 54.69.93.165 Ext Primary blox.com-intoblox-rez788[JBXVOydATV4HhOlk2]  Cancel Prevbous Next Schedule for Later Save 5 Cloce - Click on the 'Add' button.  Add Response Policy Zone Wizard > Step 3 of 5  None Use this set of name servers  Add Secondary  Use this set of name servers  Add Cancel Prevbous Next Click on the 'Add' button.  Add Response Policy Zone Wizard > Step 3 of 5  None Use this set of name servers  Add Response Policy Zone Wizard > Step 3 of 5  None Use this set of name servers  Add Response Policy Zone Wizard > Step 3 of 5  None Use this set of name servers  Add Response Policy Zone Wizard > Step 3 of 5  None Use this set of name servers  Add Response Policy Zone Wizard > Step 3 of 5  None Use this set of name servers  Add Response Policy Zone Wizard > Step 3 of 5  None Use this set of name servers  Add Response Policy Zone Wizard > Step 3 of 5  None Use this set of name servers  Add Response Policy Zone Wizard > Step 3 of 5  None Use this set of name servers  Add Response Policy Zone Wizard > Step 3 of 5  None Use this set of name servers  Add Response Policy Zone Wizard > Step 3 of 5  None Use this set of name servers  Add Response Policy Zone Wizard > Step 3 of 5  None Use this set of name servers  Add Response Policy Zone Wizard > Step 3 of 5  Add Response Policy Zone Wizard > Step 3 of 5  Add Response Policy Zone Wizard > Step 3 of 5  Add Response Policy Zone Wizard > Step 3 of 5  Add Response Policy Zone Wizard > Step 3 of 5  Add Response Policy Zone Wizard > Step 3 of 5  Add Response Policy Zone Wizard > Step 3 of 5  Add Response Policy Zone Wizard > Step 3 of 5  Add Response Policy Zone Wizard > Step 3 of 5  Add Response Policy Zone Wizard > Step 3 of 5  Add Response Policy Zone Mizard > Step 3 of 5  Add Response Policy Zone Mizard > Step 3 of 5  Add Response 4  Add Response Policy Zone Add Response 4  Add Respon	-							
<ul> <li>None</li> <li>Use this Name Server Group</li> <li>Choose One :</li> <li>Use this set of name servers</li> <li>+ •   <i>x</i>   <i>x</i></li> <li><i>A</i> dd Grid Secondary</li> <li>Lead Secondary</li> <li>Lead Secondary</li> <li>Lead Secondary</li> <li>Add Cancel</li> <li>None</li> <li>Use this Name Server Group</li> <li>Choose One :</li> <li>Use this Name Server Group</li> <li>Choose One :</li> <li>Use this Name Server Group</li> <li>Choose One :</li> <li>Use this Safe of name servers</li> <li>+ •   <i>x</i>   <i>x</i></li> <li>I MAK →   PY4 ADDRESS</li> <li>PY4 ADDRESS</li> <li>PY4 ADDRESS</li> <li>Previous</li> <li>None</li> <li>Use this Name Server Group</li> <li>Choose One :</li> <li>Use this set of name servers</li> <li>+ •   <i>x</i>   <i>x</i></li> <li>I MAK →   PY4 ADDRESS</li> <li>YYE&lt; TSG</li> <li>I MAK →   PY4 ADDRESS</li> <li>YYE</li> <li>I MAK →   PY4 ADDRESS</li> <li>YYE</li> <li>YYE</li> <li>Sedemogm.te 1060.22.240</li> <li>Grid Secondary No</li> </ul>	Ad	ld Response F	olicy Zone W	/izard > Step 3	of 5			
<ul> <li></li></ul>	•	None Use this Name S Use this set of r	Server Group	Choose One				
Add Grid Secondary       Image: Select Clear Isedemogm.testilab.com         Lead Secondary       Add Cancel         Image: Lead Secondary       Add Cancel         Image: Imag							+	•   🗹   💼
Select Clear Bedemogm.testlab.com Lead Secondary Add Cancel MAME  PV4 ADDRESS IPV6 ADDRESS TYPE TSIG base.rpz.inlob 54.69.93.185 Ext Primary blox.com-inloblox-rez788[Jj2kVQydA7V4H/hQkZ] Cancel Previous Next Schedule for Later Save & Close • Citck on the 'Add' button. Add Response Policy Zone Wizard > Step 3 of 5 None Use this set of name servers Vise this s	Ad	dd Grid Secondary	/					×
Lead Secondary       Add Cancel         INME       IPV4 ADDRESS       IPV4 ADDRESS       TYPE         base.rpz.infob       54.69.93.185       Ext Primary       biox.com-infoblox-rez786[Jj2k/QydAT/V4H/hOkZ]         Cancel       Previous       Next       Schedule for Later       Save & Close •         Citck on the 'Add' button.         Add Response Policy Zone Wizard > Step 3 of 5         • None       •	5	Select Clear	isedemogm.testla	ab.com				
Lead Secondary       Add Cancel         IMME _ IPV4 ADDRESS       IPV6 ADDRESS       IPV6 TSIG         base.rpz.intob       54.69.93.185       Ext Primary       blox.com-intoblox-rez788[J]2kVQydA7V4H/hOkZ]         Cancel       Previous       Next       Schedule for Later       Save & Close •         Click on the 'Add' button.         Add Response Policy Zone Wizard > Step 3 of 5         None         Use this Name Server Group       Choose One •         • Use this set of name servers         Image:       IPV6 ADDRESS       TYPE         Image:       IPV6 ADDRESS       TYPE       TSIG         Image:       Image:       Image:       Image:         Image:       Image:       Image:       Image:         Image: </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>								
Add       Cancel         Image: IPV4 ADDRESS       IPV6 ADDRESS       TYPE         Image: Intob       54.69.93.185       Ext Primary       blox.com-infobiox-rez788[J]2k/QydA7V4H/hOkZ]         Cancel       Previous       Next       Schedule for Later       Save & Close •         Click on the 'Add' button.       Add Response Policy Zone Wizard > Step 3 of 5       •       None         Use this Name Server Group       Choose One ♥       •		Lead Secondary						
INME       IPV4 ADDRESS       IPV6 ADDRESS       TVPE       TSIG         base.rpz.inlob       54.69.93.185       Ext Primary       blox.com-infoblox-rez788[Jj2kVQydA7V4H/hOkZ]         Cancel       Previous       Next       Schedule for Later       Save & Close •         Click on the 'Add' button.         Add Response Policy Zone Wizard > Step 3 of 5         None       Use this Name Server Group       Choose One \$         Use this set of name servers         INAME _       IPV4 ADDRESS       TYPE         Isedemogm.te       10.60.22.240       Grid Secondary         No       Grid Secondary       No							Ad	d Cancel
WME       IPV4 ADDRESS       IPV6       TSIG         base.rpz.infob       54.69.93.185       Ext Primary       blox.com-infoblox-rez788[Jj2kVQydA7V4H/hOkZ]         Cancel       Previous       Next       Schedule for Later       Save & Close •         Click on the 'Add' button.         Add Response Policy Zone Wizard > Step 3 of 5         None       Use this set of name servers         Use this set of name servers         Implementary       Implementary         base.rpz.infob       54.69.93.185       Ext Primary       blox.com-infoblox-rez788[Jj2kVQydA7V4H/hOkz]         isedemogm.te       10.60.22.240       Grid Secondary       No		1						
base.rpz.inlob       54.69.93.185       Ext Primary       blox.com-infoblox-rez788[ij]2kVQydA7V4H/hOkZ]         Cancel       Previous       Next       Schedule for Later       Save & Close •         Click on the 'Add' button.         Add Response Policy Zone Wizard > Step 3 of 5         None         Use this set of name servers         ▶ Next         TYPE         TSIG         base.rpz.infob         64.69.93.185         PY6 ADDRESS         TYPE         Sedemogm.te         10.60.22.240         Grid Secondary         No			IPV4 ADDRESS	IPV6 ADDRESS	TYPE	TSIG		
Cancel Previous Next Schedule for Later Save & Close •   Click on the 'Add' button. Add Response Policy Zone Wizard > Step 3 of 5  None Use this Name Server Group Choose One • Use this set of name servers • IPV4 ADDRESS IPV6 ADDRESS TYPE TSIG base.rpz.infob 54.69.93.185 Ext Primary blox.com-infoblox.rez788[J]2kVQydA7V4H/hOkZ] i sedemogm.te 10.60.22.240 Grid Secondary No		base.rpz.infob	54.69.93.185		Ext Primary	blox.com-infoblox-rez7	'88[Jj2kVQydA7V4H/h	OkZ]
Cancel Previous Next Schedule for Later Save & Close   Click on the 'Add' button.   Add Response Policy Zone Wizard > Step 3 of 5     None   Use this Name Server Group   Choose One +   Use this set of name servers     Image: Previous     Image: Previous <tr< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr<>								
Cancel     Previous     Next     Schedule for Later     Save & Close								
Chock on the 'Add' button. Add Response Policy Zone Wizard > Step 3 of 5 None Use this Name Server Group Choose One Use this set of name servers ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓								
Add Response Policy Zone Wizard > Step 3 of 5   None   Use this Name Server Group   Use this set of name servers     IPV4 ADDRESS   IPV4 ADDRESS   IPV6 ADDRESS   TYPE   TSIG   base.rpz.infob   54.69.93.185   Ext Primary   blox.com-infoblox-rez788[J]2kVQydA7V4H/hOkZ]     isedemogm.te   10.60.22.240   Grid Secondary No	С	Cancel		Previous	Next		Schedule for Later	Save & Close
<ul> <li>None</li> <li>Use this Name Server Group Choose One </li> <li>Use this set of name servers</li> </ul>	C C	cancel	' button.	Previous	Next		Schedule for Later	Save & Close
<ul> <li>Use this Name Server Group Choose One ↓</li> <li>Use this set of name servers</li> <li>▲ • ▷ ▷ ○ □</li> <li>NAME ▲ □ PV4 ADDRESS 1PV6 ADDRESS 1YPE TSIG</li> <li>base.rpz.infob 54.69.93.185 Ext Primary blox.com-infoblox-rez788[J]2kVQydA7V4H/hOkZ]</li> <li>isedemogm.te 10.60.22.240 Grid Secondary No</li> </ul>	c lick Ad	con the 'Add Response F	' button. Policy Zone W	Previous /izard > Step 3	Next		Schedule for Later	Save & Close
<ul> <li>● Use this set of name servers</li> <li> <ul> <li>If V4 ADDRESS</li> <li>IPV6 ADDRESS</li> <li>TYPE</li> <li>TSG</li> <li>base.rpz.infob</li> <li>54.69.93.185</li> <li>Ext Primary</li> <li>blox.com-infoblox-rez788[J]2kVQydA7V4H/hOkZ]</li> <li>isedemogm.te</li> <li>10.60.22.240</li> <li>Grid Secondary</li> <li>No</li> </ul> </li> </ul>	C C C C C C C C C C C C C C C C C C C	con the 'Add d Response F	' button. Policy Zone W	Previous /izard > Step 3	Next		Schedule for Later	Save & Close
Image: NAME _ IPV4 ADDRESS IPV6 ADDRESS TYPE TSIG   Image: base.rpz.infob 54.69.93.185 Ext Primary blox.com-infoblox-rez788[Jj2kVQydA7V4H/hOkZ]   Image: base.rpz.infob 10.60.22.240 Grid Secondary No	C C C C C C C C C C C C C C C C C C C	Cancel K on the 'Add' Id Response F None Use this Name S	' button. Policy Zone W Server Group	Previous /izard > Step 3 Choose One \$	Next		Schedule for Later	Save & Close
NAME       IPV4 ADDRESS       IPV6 ADDRESS       TYPE       TSIG         base.rpz.infob       54.69.93.185       Ext Primary       blox.com-infoblox-rez788[Jj2kVQydA7V4H/hOkZ]         isedemogm.te       10.60.22.240       Grid Secondary       No	C Click Ad	Cancel K on the 'Add' Id Response P None Use this Name S Use this set of r	' button. Policy Zone W Server Group	Previous /izard > Step 3 Choose One \$	Next		Schedule for Later	Save & Close
base.rpz.infob 54.69.93.185 Ext Primary blox.com-infoblox-rez788[Jj2kVQydA7V4H/hOkZ]     isedemogm.te 10.60.22.240 Grid Secondary No     No	Click Ad	Cancel c on the 'Add d Response F None Use this Name S Use this set of r	' button. Policy Zone W Server Group	Previous /izard > Step 3 Choose One \$	Next		Schedule for Later	Save & Close
□ isedemogm.te 10.60.22.240   Grid Secondary No	C Click Ad	Cancel Con the 'Add Id Response F None Use this Name S Use this set of r	' button. Policy Zone W Server Group name servers	Previous /izard > Step 3 Choose One \$	Next F of 5	TSIG	Schedule for Later	Save & Close
	C Click Ad	Cancel Con the 'Add' Id Response F None Use this Name S Use this set of r NAME	' button. Policy Zone W Server Group name servers IPV4 ADDRESS 54.69.93.185	Previous Vizard > Step 3 Choose One	Next of 5 TYPE Ext Primary	TSIG blox.com-infoblox-rez7	Schedule for Later	Save & Close
	Click Ad	Cancel Con the 'Add' Id Response P None Use this Name S Use this set of r NAME = base.rpz.infob isedemogm.te	' button. Policy Zone W Server Group name servers IPV4 ADDRESS 54.69.93.185 10.60.22.240	Previous Vizard > Step 3 Choose One	Next of 5 TYPE Ext Primary Grid Secondary	TSIG blox.com-infoblox-rez7 No	Schedule for Later	Save & Close
	C Click Ad	Cancel Con the 'Add d Response F None Use this Name S Use this set of r NAME • base.rpz.infob isedemogm.te	' button. Policy Zone W Server Group name servers IPV4 ADDRESS 54.69.93.185 10.60.22.240	Previous /izard > Step 3 Choose One	Next of 5 TYPE Ext Primary Grid Secondary	TSIG blox.com-infoblox-rez7	Schedule for Later	Save & Close
	Click Ad	Cancel Con the 'Add Id Response F None Use this Name S Use this set of r NAME base.rpz.infob isedemogm.te	' button. Policy Zone W Server Group name servers IPV4 ADDRESS 54.69.93.185 10.60.22.240	Previous Vizard > Step 3 Choose One	Next of 5 TYPE Ext Primary Grid Secondary	TSIG blox.com-infoblox-rez7 No	Schedule for Later	Save & Close
		Cancel Con the 'Add' d Response F None Use this Name S Use this set of r NAME • base.rpz.infob isedemogm.te	' button. Policy Zone W Server Group name servers 1PV4 ADDRESS 54.69.93.185 10.60.22.240	Previous Vizard > Step 3 Choose One	Next of 5 TYPE Ext Primary Grid Secondary	TSIG blox.com-infoblox-rez7 No	Schedule for Later	Save & Close
	Click Ad	Cancel Con the 'Add' Id Response F None Use this Name S Use this set of r NAME ▲ base.rpz.infob isedemogm.te	' button. Policy Zone W Server Group name servers 1PV4 ADDRESS 54.69.93.185 10.60.22.240	Previous	Next of 5 TYPE Ext Primary Grid Secondary	TSIG blox.com-infoblox-rez7 No	Schedule for Later	Save & Close
		Cancel Con the 'Add Id Response F None Use this Name S Use this set of r NAME • base.rpz.infob isedemogm.te	' button. Policy Zone W Server Group name servers 1PV4 ADDRESS 54.69.93.185 10.60.22.240	Previous         /izard > Step 3         Choose One       \$         IPV6 ADDRESS	Next Control C	TSIG blox.com-infoblox-rez7 No	Schedule for Later	Save & Close
		Cancel Con the 'Add' Id Response F None Use this Name S Use this set of r NAME A base.rpz.infob isedemogm.te	' button. Policy Zone W Server Group name servers 1PV4 ADDRESS 54.69.93.185 10.60.22.240	Previous Vizard > Step 3 Choose One	Next of 5 TYPE Ext Primary Grid Secondary	TSIG blox.com-infoblox-rez7	Schedule for Later	Save & Close

18. Click on 'Save & Close' button and then click on the 'Restart' button.

- 19. To verify that the zone transfer of the feed was correct, navigate to the Administration  $\rightarrow$  Logs  $\rightarrow$  Syslog and then select the member.
- 20. Conduct a search on the IP address of the feed server. You should see a similar following message:

		7 ₿	2017-01-2	7 12:10:35 PST	daemon	INFO	named[15220]	transfer of 'ba	se.rpz.infoblox.l	ocal/IN' from <mark>54.69.93</mark>	8 <mark>.185</mark> #53: Transfer complete	ed: 70 mess	ages,	
21.	Тс	o tes	t, navig	ate bacl	k to Data	Manager	ment $\rightarrow$ DNS	→ Response	onse Po	licy Zones				
	In	foblox 💲	•	Dashboards C	Pata Management	Smart Folders Rep	orting Grid Administrat	lon				Q Search	admin	-
				IPAM VLANs	Super Host De	wices DHCP D	NS File Distribution							
	*	Zones	Members Na	me Server Groups	Shared Record Grou	Response Policy	Zones Subscriber Services De	ployment Blacklist F	lulesets DNS64	Groups Query Monitor	ing		(	0 «
	(	default	🖉 🖪											
		Quick Filte	None	V Off Filter C	In Show Filter									
		→   <b>+</b>	🖻   🗃 -   ᆂ -	-   😝							Go to	Go		
		=	ORDER 🛋	NAME	TYPE	SEVERITY PRIMA	ARY NAME S LAST UPDATED	COMMENT	MULTI-MASTER Z	SITE				
			0	local-rpz	Local N	fajor isedem	nogm.test		No					
			1	base.rpz.infoblo	Feed N	fajor base.m	pz.infoblo		No					

- 22. Click on the feed entry to download the contents to a .CSV file.
- 23. Pick an item in the file to run a DNS resolution.
- 24. Depending upon the OS of your workstation run a 'dig' or 'nslookup' against the name server and URL. In this example, 10.60.2.2 is the DNS server with the RPZ feed enabled.

[sc-l-thomasl:Documents thomasl	.\$ dig @	@10.60.2.2 www.06x.biz			
<pre>; &lt;&lt;&gt;&gt; DiG 9.8.3-P1 &lt;&lt;&gt;&gt; @10.60.2.2 www.06x.biz ; (1 server found) ;; global options: +cmd ;; Got answer: ;; -&gt;&gt;HEADER&lt;&lt;- opcode: QUERY, status: NXDOMAIN, id: 57803 ;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0</pre>					
;; QUESTION SECTION: ;www.06x.biz.	IN	A			
<pre>;; Query time: 188 msec ;; SERVER: 10.60.2.2#53(10.60.2.2) ;; WHEN: Fri Jan 27 17:32:31 2017 ;; MSG SIZE rcvd: 29</pre>					
<pre>sc-l-thomasl:Documents thomasl\$</pre>					

- 25. Notice the status of NXDOMAIN.
- 26. In addition, navigate to Administration → Logs → Syslog and select the member that was resolving the bad entry. Search for CEF (common event format) messages.

V	ġ.	2017-01-27 17:32:31 PST	daemon	INFO	named[30112]	CEF:0IInfobloxINIOSI7.3.4-322642IRPZ-QNAMEINXDOMAINI4Iapp=DNS dst=10.60.2.2 src=10
---	----	-------------------------	--------	------	--------------	--

## 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".





Infoblox enables next level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 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) | <u>info@infoblox.com</u> | <u>www.infoblox.com</u>

in f y C

© 2019 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).