USER GUIDE V1.1.0

SlashNext Agentless Phishing Protection Guide Infoblox DNS RPZ Feed

TABLE OF CONTENTS

INTRO	ODUCTION
INFO	BLOX CON
St	ep 1
St	ep 2
Ste	ep 3
Ste	ep 4
Ste	ep 5
St	ep 6
Ste	ep 7
Ste	ep 8
	Step 8
	Step
	Step
	Step
	Step 8
Ste	ep 9
Ste	ep 10
	Step 2
	Step 1
Ste	ep 11

TABLE OF CONTENTS

	Step 12	
	Step 13	
	Step 14	
	Step 15	
	Step 16	
	Step 17	
	Step 18	
	Step 19	
	Step 20	
	Step 21	
	Step 22	
	Step 23	
	Step 24	
3	VERIFICATION OF RPZ WORKING	
	Step 1	
	Step 2	
	Step 3	

1 | INTRODUCTION

A response policy zone (RPZ) is a mechanism to introduce a customized policy in Domain Name System servers, so that recursive resolvers return possibly modified results. By modifying a result, access to the corresponding host can be blocked. Usage of an RPZ is based on DNS data feeds, known as zone transfer, from an RPZ provider to the deploying server.

Customer shall receive a XXXX-XXXX-XX.tsig.key file from SlashNext which is to be used in Infoblox Configurations section to enable the reception of RPZ feed from SlashNext cloud

ONOTE

This guide is made using Infoblox Version: 8.2.4-366880, some menu structures and contents with Infoblox might be updated if you have a different version.

2 | INFOBLOX CONFIGURATIONS

Please follow the instructions below to enable the reception of the SlashNext RPZ feed on a Infoblox DNS server.



Login to Infoblox

	Dashboards Data Management Smart Folders Grid Administration	Q Search admin -
	Tasks Status	
Finder «	IPAM Tasks	¢ - €
Recycle Bin * Image: URL Links *	Add Networks Use this task to add IPv4IPv6 networks to the system.	
	Add A Record Use this task to add a DNS A resource record to a zone. Use this task to add P44/P46 fixed addresses to the system.	
	Add CNAME Record Use the task to add a DNS CNAME resource record to a zone.	
	Add MX Record Use this task to add a DNS MX resource record to a zone. Section 2012 CSV Import Nanager Galog.	

2.2 | STEP 2

Verify if the "DNSone with Grid (DNS, DHCP, Grid)" license is installed on Infoblox. If "DNSone with Grid" license is already installed then Grid tab will be shown adjacent to Administration tab.

Dashboards	Data Ma	nagement	Smart Folders	Grid	Administration	Q, Se	arch	admin	•
Grid Manager	Upgrade	Licenses	HSM Group						

If "DNSone with Grid" license is not installed then please access the CLI of Infoblox and execute the following command:



Please select the option "DNSone with Grid (DNS,DHCP,Grid) ", when prompted press "y" and enter the key to confirm

<pre>Infoblox > set temp_license</pre>	
 DNSone (DNS, DHCP) DNSone with Grid (DNS, DHCP, Grid) Network Services for Voice (DHCP, Grid) Add DNS Server license Add DHCP Server license Add Grid license Add Microsoft management license Add Multi-Grid Management license Add Query Redirection license Add Load Balancer license Add Response Policy Zones license Add DNS Traffic Control license Add Cloud Network Automation license Add Security Ecosystem license Add Security Ecosystem license 	
Select license (1-17) or q to quit: 2	
This action will generate a temporary 60-day DNSone (Are you sure you want to do this? (y or n): y DNS temporary license installed. DHCP temporary license installed. Grid temporary license installed.	with Grid license.
Temporary license is installed.	
The UI needs to be restarted in order to reflect li Restart UI now, this will log out all UI users? (y	cense changes. or n) <mark>:y</mark>
Are you sure you want to do this? (y or n): y UI restarted. Infoblox >	

2.3 | STEP 3

Verify that the **"Response Policy Zone"** license is installed on Infoblox . Navigate to the Data Management DNS tab. If the **"Response Policy Zone license"** is already installed then it will appear under the DNS tab.

Infoblox 🗇	Dashboards Data Managament Smart Folders Grid Administration
	IPAM DHCP DNS File Distribution
Finder «	Zones Members Name Server Groups Shared Record Groups Response Policy Zones Bladdlet Rulesels DNS64 Groups Query Monitoring
Bookmarks Bookmarks	Guick Filter None Show Filter
Lig OHL LINKS +	Go to Color . Name Type Severity Primery Name S Last Updated Commant Multi-master Zone Ste
	No deta

If "Response Policy Zone license" is not installed then access the CLI of Infoblox and execute the following command:



Select the option "Add Response Policy Zones license", when prompted press "y" and enter key to confirm

Infoblox > set temp_license DNSone (DNS, DHCP)
 DNSone with Grid (DNS, DHCP, Grid)
 Network Services for Voice (DHCP, Grid) 4. Add DNS Server license Add DHCP Server license
 Add Grid license
 Add Microsoft management license 8. Add vNIOS license 9. Add Multi-Grid Management license Add Query Redirection license
 Add Load Balancer license 12. Add Response Policy Zones license 13. Add FireEye license 14. Add DNS Traffic Control license Add Cloud Network Automation license
 Add Security Ecosystem license 17. Add Threat Analytics license Select license (1-17) or q to quit: 12 This action will generate a temporary 60-day Response Policy Zones license. Are you sure you want to do this? (y or n): y Response Policy Zones temporary license installed. Temporary license is installed. The UI needs to be restarted in order to reflect license changes. Restart UI now, this will log out all UI users? (y or n): y Are you sure you want to do this? (y or n): y UI restarted. Infoblox >

2.4 | STEP 4

Navigate to Grid → Grid Manager tab, verify that the DNS and NTP services are both running.

Infoblox 😒		Dashboards Data Management Smart Folders Grid Administration			
CONTROL YOUR NETWORK	G	arid Manager Upgrade Licenses HSM Group			
Finder	~				
Smart Folders	+				
👉 Bookmarks	+	DHCP DNS TFTP HTTP (File Dist) FTP NTP bloxTools Captive Portal			
Recycle Bin	+				
URL Links	+	Members Services			
		DNS 📕 🥖			
		Quick Filter None	M		
		Group Results Group By Choose one			
		Go to Go			
	- 1	Name - Service Status IPv4 Add	ddress	Comment	Site
	- 1		.2.78		
	- 1	172.16.2	3.2.79		

Infoblox 💸	Dashboards Data Management Smart F	olders Grid Administration			
	Grid Manager Upgrade Licenses HSM G	roup			
Finder	Infohlov 🗖 🍊 🏄				
Smart Folders					
A Bookmarks	DHCP DNS TFTP HTTP (File Dist)	FTP NTP bloxTools Captive Portal			
🛐 Recycle Bin					
🖏 URL Links	Members Services				
	NTP 📕 🥖				
	Quick Filter None	er On Show Filter			
	Group Results Group By Choese an	e 💉 🔸			
	Go to Go				
	Name	tus	IPv4 Address	Comment	Site
		e is working	172.16.2.78		
			172.16.2.79		

2.5 | STEP 5

If the DNS Service is not running, go to $\mathbf{Grid} \rightarrow \mathbf{Grid}$ Manager tab

- a. Select DNS
- b. Go to Services tab
- c. Mark checkbox for DNS Service
- d. Click on Start button
- e. Click "yes" to confirmation message
- f. Please refresh the page in order to get the latest status

	nToblox 😵 Daatibaarde Data Management Smaat Folders Entre Ont Management Uborade Hild Ross	Q Search a
And a second secon	Concentrations (Very Work Leaves Hold Group and Folders and Folders	Techar → Adi · → Adi · → Adi · → Beta ·
	The filtering for the solution of the solution	∰ Exori * ∰ Ying * CoVi vepor * CoVi vepor * CoVi vepor * CoVi vepor * EN Conventor
	1000.00 2	

2.6 | STEP 6

If the NTP Service is not running, go to **Grid** \rightarrow **Grid** Manager tab

- a. Select NTP
- b. Go to Services tab
- c. Mark checkbox for NTP Service
- d. Click on Start button
- e. Click "yes" to confirmation message
- f. Please refresh the page in order to get the latest status.

Q Search édrin
Image: Second

2.7 | STEP 7

If you want to sync with the NTP Server, please then follow Step 8 otherwise proceed to Step 10.

2.8 | STEP 8

In Infoblox navigate to "Grid" tab, select "NTP", then from right side tool bar click on the "Edit" drop-down and select "Grid NTP Properties"

		Grid Nanager Upgrade Licenses HSM Group	
nder	66		Toolbar 30
Smart Folders			💠 Add 🔹
Bookmarks		DHCP DNS TFTP HTTP(File Dist) FTP NTP bloxTools Ceptive Portal	C Bestart Services
Recycle Bin			
URL Links	+	Members Services	By Edt •
		NTP 📕 🦯	Grid NTP Properties
		Cuick Filter None	Member NTP Propertie
		Amerika Amerika Amerika	Grid Properties
			Member Properties
		Go 10 Go	Download •
		Name Service Satus IPv4 Address Comment Site	JA Export
			🖶 Print
			2 IDN Converter

2.8.1 | STEP 8.1

From the "General" tab, please mark the check box "Synchronize the Grid with these External NTP Servers"

Conversi	-					
Access Control	Synchro	nize the Grid wi	th these External NTP	Servers		
	_					+100
	Preferred	Server	Authentication	Key Number	BURST	IBURST
						• 0

2.8.2 | STEP 8.2

Click on the Add icon (+) and please Enter the NTP Server information (FQDN or IP Address)

General				
	Synchronize the Grid with	these External NTP Ser	vers	
Access Control				+ B-10
	Add NTP Server			×
	NTP Server (FQDN or IP Address)*		Resolve Na	me
	Enable Authentication			
	Authentication Key		\$	
				Add Cancel
	Proferred Server	Authentication	Key Number	BURST IBURST
	No data			

2.8.3 | STEP 8.3

Click on the Add button

			~
NTP Server (FQDN or IP Address)*	pool.ntp.org	Resolve Name	
Enable Authentication			
Authentication Key	0	\$	
		Add	Cancel

2.8.4 | STEP 8.4

"Save & Close" configuration

General						
Access Control	Synchronize	e the Grid with the	se External NTP Ser	vers		
	Taxan di Seconda Se	Laurenteen	1			+ 0
	Preferred	Server	Authentication	Key Number	BURST	IBURST
		pool.ntp.org	No		4	V
						10
						1.10

2.8.5 | STEP 8.5

Access the CLI of Infoblox & type command "reboot". Press "y" when prompted

```
[Infoblox > reboot
[ REBOOT THE SYSTEM? (y or n): y
SYSTEM REBOOTING!
SYSTEM REBOOTING!
```

2.9 | STEP 9

The time zones for both the RPZ Feed Server and Infoblox should be synced in order to transfer the zones.

a. From Grid tab, select Grid Manager tab and then click Edit from Grid Properties drop-down button in the Grid Manager Toolbar.



b. From Grid Properties Editor, check the timezone and time of Infoblox

ggle Advanced Bes	Advanced	_
General Grid N Security Shared Password Shared DNS Resolver Time Z Monitoring Date Syslog Backup Date SNMP Time Email VPN P LOM Enable Improvement Audit I NAT Groups Token Extensible Token	i Name* Infobiox red Secret*	

2.10 | STEP 10

From the Infoblox Grid Manager, go to the Administration tab and select Named ACL. Click on the Add icon (+) to configure RPZ Feed Server IP as follows:

2.10.1 | STEP 10.1

Add ACL Name and click "Next"

reame	SlashNext Appliance	
Comment		

• Note

You can change the Name field as per your liking.

2.10.2 | STEP 10.2

Click on "Add icon (+)". Click in the entry field and enter "RPZ Feed Server IP".

					K K K O
	Entry	Туре	Operation	Order	
*	72.16.2.158	IPv4 Address	Allow	1	
Ŧ					
	NA E EL				

ONOTE

Replace 172.16.2.158 with RPZ FEED SERVER IP which shall be provided by SlashNext.

After configuration Save and Close "Add Named ACL" window.

2.11 | STEP 11

From the Data Management tab, navigate to DNS → Response Policy Zone tab. From the right toolbar, click on "Grid DNS Properties", click on "Queries" from left side menu list and mark check-box "Allow recursion"

WAM DHCP Date Debutton	_
Piedra a Zone Manchen Name Server Groups Baande Record Groups Tegenetar Rolling Zones Manchens Childh Groups Caury Monduring Tegenetar Analyza Childh Chil	()) ()

2.12 | STEP 12

From the Data Management tab, please navigate to DNS Response Policy Zone tab. Click the Add icon (+) and the Add Response Policy Zone Wizard will be displayed.

	Dashboards Data Management Smart Folders Grid Administration
	IPAM DHCP DNS File Distribution
Finder	Zones Members Name Server Groups Shared Record Groups Response Policy Zones Blacklist Rulesets DNS64 Groups
Smart Folders +	
👉 Bookmarks +	default 🧪 🛠
Tecycle Bin +	Quick Filter None
📑 URL Links 🔹 🕂	Go to Go
	Type Severity Primary Name S Last Updated
	No data

2.13 | STEP 13

Select the radio button "Add Response Policy Zone Feed" and click Next

Zones Members Name Server Groups Shared Record Groups Response Policy Zones Blacklist Rulesets DNS64 Groups	•
default 🥒 🛠	
Quick Filter None	
Go to Go	
Add Response Policy Zone Wizard > Step 1 of 5	\boxtimes
Add Local Response Policy Zone	** ••
Add Response Policy Zone Feed	
Cancel Previous Next Schedule for Later Save & Close +	

2.14 | STEP 14

In the Add Response Policy Zone Wizard, specify the following

Attributes	
Name:	Enter the name "XXXX-XXXX-XX.snxblocking.rpz". Here XXXX-XXXX-XX perfix is the TSIG key name and shall
	be provided by SlashNext.
Policy Override:	Select a value from the drop-down list.
Severity:	Select the threat severity level for the RPZ zone. The threat severity level selected here determines the severity
	for the RPZ rule. Select Critical, Major, Warning, or Informational. The default threat severity level is Major.

Name*	bind.snxblocking.rpz	
Policy Override	None (Given)	
Severity	Major T	
Comment		
Disable		
Lock		

2.15 | STEP 15

Click Next

	None Use this Name	Server Group	hoose One 📩			
0 1	Use this set of	name servers				
	-					+ • ₽ 0
	Name 🔺	IPv4 Address	IPv6 Address	Туре	TSIG	
14		2				
14	I + 1	z				

2.16 | STEP 16

Click on the drop down adjacent to add icon (+)



2.17 | STEP 17

Click on "Grid Secondary"



2.18 | STEP 18

Click on the "Select" button

01	loo this Name	Server Group	baasa Ona A			
	Jse this Name	Server Group	noose One 🖡			
0	Use this set of	name servers				
						+ • ⊵ ⊘
Ade	d Grid Second	lary				×
S	elect Cle	ar				
	Lead Second	lary				Add Cancel
	Name 🔺	IPv4 Address	IPv6 Address	Туре	TSIG	
No	o data					

• Note

You can associate a lead secondary with an RPZ feed if you have more than one secondary servers by selecting check-box "Lead Secondary"

Add Grid Secondary	×	
Select Clear infoblox.localdomain		
Lead Secondary		
	Add Cancel	

2.19 | STEP 19

Click on the "Add" button.

Add	Cancel

Now Grid Secondary has been added.

	Use this Name Se Use this set of na	erver Group C	hoose One 🛊			
						+ · E C
	Name 🔺	IPv4 Address	IPv6 Address	Туре	TSIG	
	infoblox.locald	172.16.2.79		Grid Secondary	No	
14	A F FI	2				

2.20 | STEP 20

Click on the drop down adjacent to add icon (+) and select "External Primary" option. For external primary servers, specify the following:

None		
Use this Name Server Group	Choose One \$	
Use this set of name servers	8	↓ · ⊵ ⊘
Add External Primary		×
Name* Address*	TSIG Use TSIG • Key Name Key Algorithm• Key Data Use 2.x TSIG	
		Add Cancel

One state

Name:	Enter external primary server name "SlashNext RPZ Feed Server".
Address:	Enter the SlashNext RPZ Feed Server IP.
Use TSIG:	Select the check box to specify TSIG settings.
Key Name:	Enter the TSIG Key Name provided by SlashNext with format XXXX-XXXX-XX
Key Algorithm:	Select hmac-md5
Key Data:	Enter the TSIG string provided by SlashNext and click on Add button.

Click Add and then Save & Close.

2.21 | STEP 21

Click Restart if it appears at top of the screen otherwise restart it from Toolbar at right side



2.22 | STEP 22

To verify that the zone transfer is working the way it should, navigate to the Administration Logs \rightarrow Syslog and then select the member.

Dashboards	Data Manag	ement	Smart Folders	Grid Ad	ministration			
Administrators	Workflow	Logs	Network Views	Extensible Attribu	utes Authe	ntication Server Grou	ps Named ACLs	
Audit Log	Syslog							
SysLog	Log Viewer	Mem	ber infoblox.local	domain 🔻 🍳				
Quick Filter	None	\$	Off Filter On	Show Filter	Toggle	multi-line view		
			Q	4 🕨			2 2 3 1	8

2.23 | STEP 23

Conduct a search on the IP address of the feed server. You should see a similar message:

Iog message

transfer of 'XXXX-XXXX-XX.snxblocking.rpz/IN' from x.x.x.#53: Transfer completed: 1 messages, 21 record, 745 bytes, 0.001 secs (745000 bytes/sec)

2.24 | STEP 24

To test, navigate back to Data Management → DNS → Response Policy Zones.



Click on the feed entry "Name" to download the contents to a .CSV file`

3 | VERIFICATION OF RPZ WORKING

For this you will need a machine which is using above configured Infoblox as DNS server. If you don't know if an machine is using above Infoblox as DNS, please consult your network administrator. If you have a ubuntu machine with access to above Infoblox, you can configure it using following steps.

3.1 | STEP 1

Open the file /etc/resolv.conf and append the following line if its not already there.

nameserver INFOBLOX_DNS_IP

3.2 | STEP 2

Select a domain from the .CSV file downloaded in Step 24 of Infoblox Configuration section and copy it so that it can be used in the next step.

3.3 | STEP 3

Use following command on your ubuntu machine to confirm if RPZ in properly redirecting to SlashNext Sinkhole aka Walled Garden.

nslookup SELECTED_DOMAIN

Example nslookup 1929641ee50c450adb5c9e06066bbd02.336727.xyz

Server: INFOBLOX_DNS_IP Address: INFOBLOX_DNS_IP#53

Non-authoritative answer: Name: 1929641ee50c450adb5c9e06066bbd02.336727.xyz Address: SLASHNEXT_SINKHOLE_IP

Where SLASHNEXT_SINKHOLE_IP=69.25.58.50 or will be specified by SlashNext.