DEPLOYMENT GUIDE

Enabling a NIOS Grid Member to Forward Recursive Queries to BloxOne Threat Defense Using DFP

Table of Contents

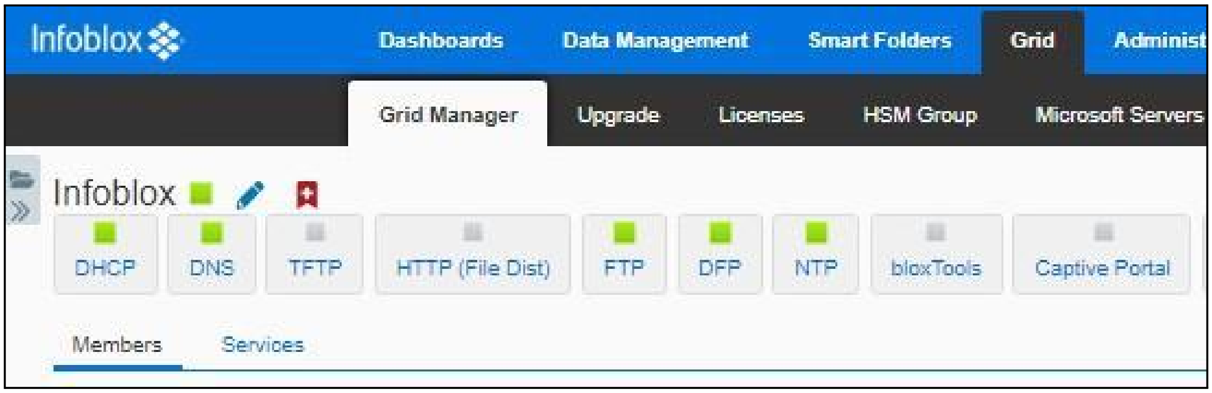
Overview

The DNS Forwarding Proxy (DFP) is a service within NIOS, used to encrypt and forward recursive DNS queries to the BloxOne Threat Defense Cloud. DFP is the preferred method for forwarding DNS traffic to BloxOne Threat Defense as opposed to standard DNS forwarders. The purpose of this guide is to supplement the official NIOS DFP configuration guide with practical guidance.

DFP Service Best Practices and Considerations

The following is a list of common areas where a best practice is recommended to maximize the Infoblox DFP service.

1. Starting in NIOS 8.5, the DFP service can be managed, started, and stopped just like other NIOS services such as DNS, DHCP, or NTP. DFP is configured either at the grid level or member level under the CSP Config properties of the Grid Properties or the DFP Grid Member Properties editor in NIOS. It is recommended to configure CSP credentials at the member level, not at the grid level.

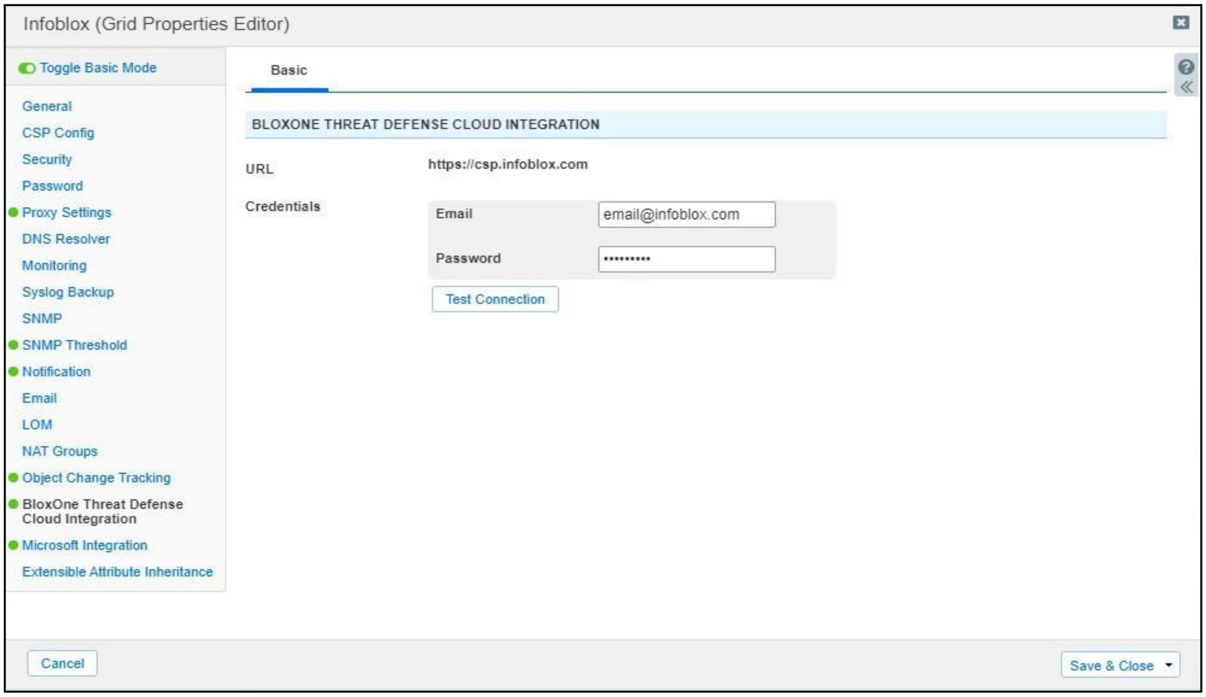


2. Be sure the firewall will allow 443 outbound access for each grid member running DFP as described in the DFP Firewall Configuration section of this doc.

3. When the CSP configuration is set for the first time, NIOS will dynamically download the required microservice containers from the CSP. If the CSP Config is set at the grid level, NIOS will download DFP containers from every device in the grid. This will create an on-prem host for each grid member. This typically takes 3-10 minutes per device depending on the size and needs of your environment. During this time, local DNS traffic will be resolved but recursive DNS requests will queue until the DFP is online. Plan for this service interruption before activating DFP.

4. You must enter your CSP credentials into the BloxOne Threat Defense Cloud Integration in your Properties menu. To enable this on the grid level, navigate to **Grid** → **Grid Manager** → **Grid**

Properties Editor. Click Toggle Advanced Mode and then navigate to **BloxOne Threat Defense Cloud Integration**. Enter your email and password credentials for the CSP.



BLOXONE THREAT DEFENSE CLOUD INTEGRATION

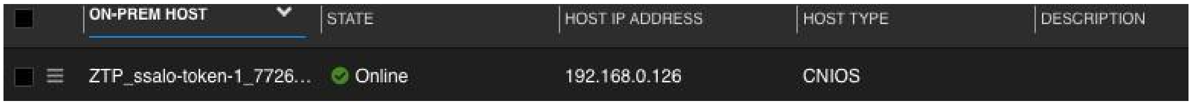
URL https://csp.infoblox.com

Credentials

Email email@infoblox.com

Password •••••••••

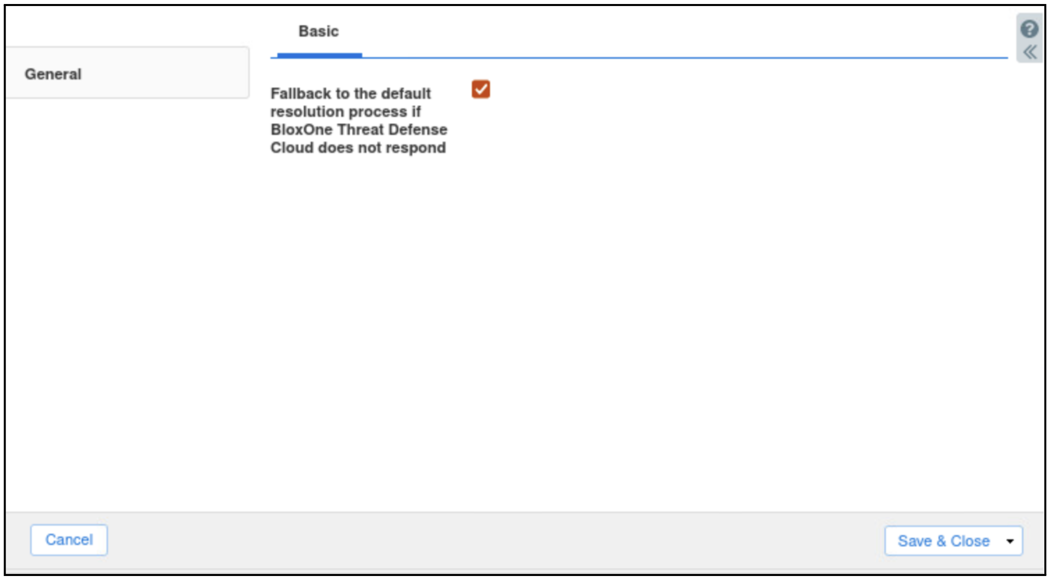
5. NIOS uses a CSP join token to authenticate to the CSP. A single join token can authenticate many NIOS devices. See [Managing Join Tokens for On-Prem Hosts]in the Infoblox Threat Defense documentation for more information about join tokens. Once NIOS authenticates to the CSP with the join token, a host will be dynamically created with the prefix ZTP_ as shown in the example below.



ON-PREM HOST	STATE	HOST IP ADDRESS	HOST TYPE	DESCRIPTION
ZTP_ssalo-token-1_7726...	Online	192.168.0.126	CNIOS	

6. Allow up to 10 minutes for the host and DFP service to fully activate. Monitor the process within the CSP by refreshing the Hosts page. Navigate to **Manage** → **Infrastructure** to ensure that the statuses for the NIOS proxies that you have registered are active.

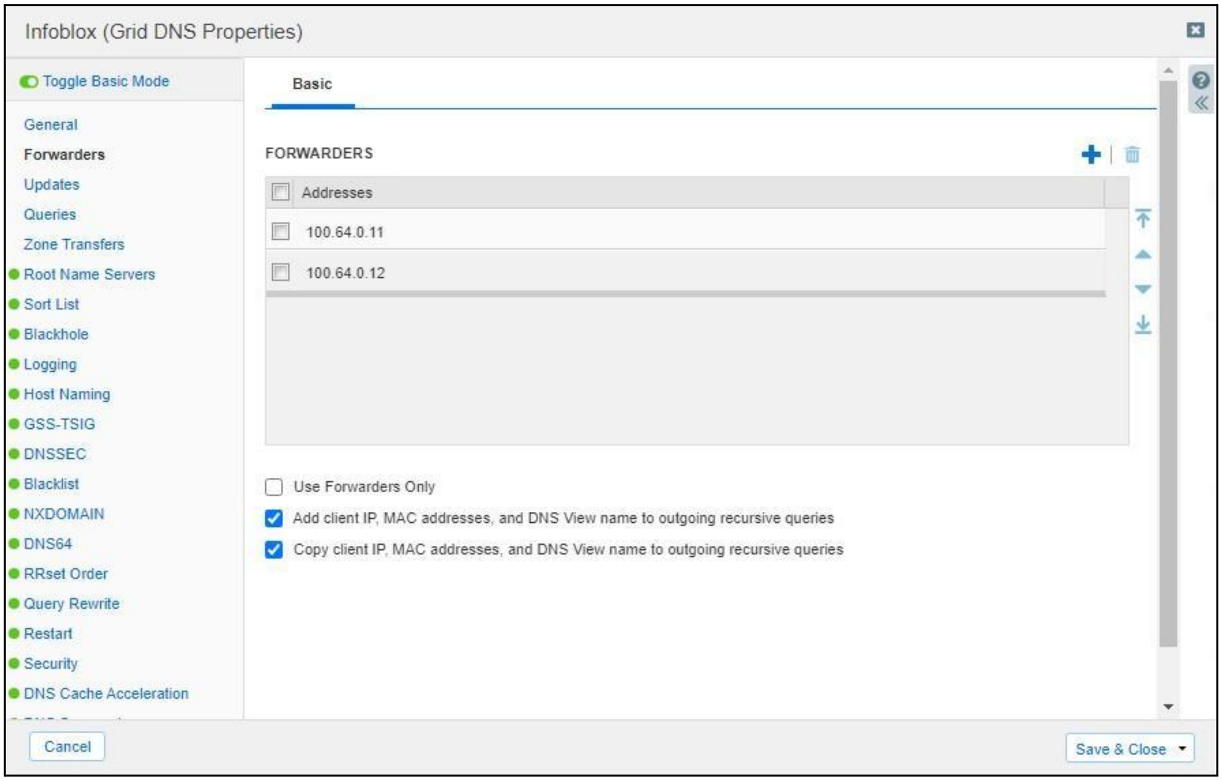
7. Be sure to configure DFP failover configuration in the DFP Service config in NIOS. In the Member DFP Properties editor, select the **Fallback to the default resolution process if BloxOne Threat Defense Cloud does not respond** check box to forward recursive queries to the local root name servers in case BloxOne Threat Defense fails or if BloxOne Threat Defense fails to resolve recursive queries.



☑ Fallback to the default resolution process if BloxOne Threat Defense Cloud does not respond

8. For newly configured DNS forwarding proxies in NIOS, Infoblox recommends that you keep this option selected until you have verified that the NIOS proxies are functioning properly. You can set these forwarders in **Grid DNS Properties** → **Forwarders** if desired.

9. Check the **Add client IP, MAC addresses and DNS View name to outgoing recursive queries** and the **Copy client IP, MAC addresses and DNS View name to outgoing recursive queries** boxes in the GridDNS Properties editor to include the client IP, MAC address and DNS view with forwarded queries.



FORWARDERS

□ Addresses
□ 100.64.0.11
□ 100.64.0.12

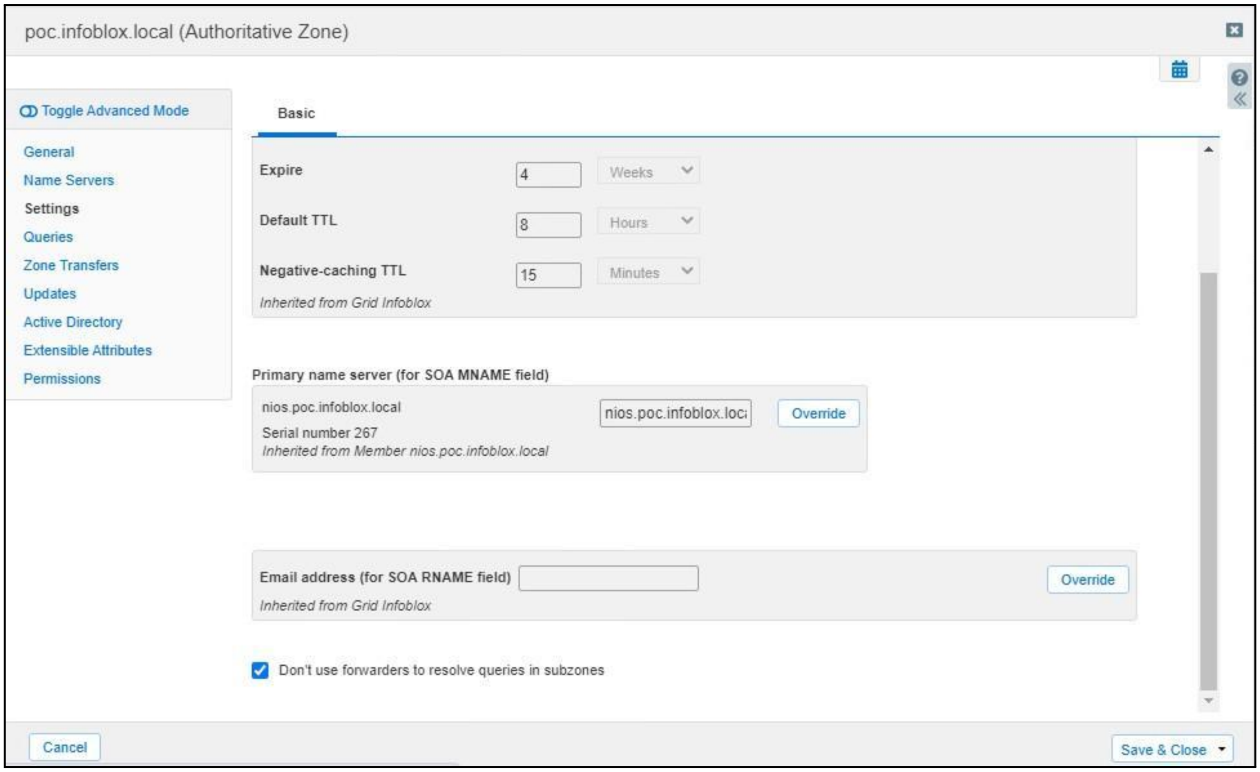
□ Use Forwarders Only

☑ Add client IP, MAC addresses, and DNS View name to outgoing recursive queries

☑ Copy client IP, MAC addresses, and DNS View name to outgoing recursive queries

DNS Forwarding Checks

If your grid contains delegated subzones, select the Don't use forwarders to resolve queries in subzones check box when configuring the Properties of the parent's authoritative zone. This causes queries that require delegation to be sent to the BloxOne Threat Defense Cloud instead of the delegated servers. Otherwise, delegations will not function properly because DNS forwarding takes precedence over delegation. See Configuring a Delegation and Configuring Authoritative Zone Properties in the Infoblox NIOS documentation for more information.



Expire 4 Weeks

Default TTL 8 Hours

Negative-caching TTL 15 Minutes

Inherited from Grid Infoblox

Primary name server (for SOA MNAME field)

nios.poc.infoblox.local nios.poc.infoblox.loc Override

Serial number 267

Inherited from Member nios.poc.infoblox.local

Email address (for SOA RNAME field) Override

Inherited from Grid Infoblox

☑ Don't use forwarders to resolve queries in subzones

DFP Firewall Configuration

Configure your firewalls to allow outbound connections to BloxOne from each grid member running DFP. The following table provides port usage for the BloxOne on-prem hosts. Every NIOS grid member that forwards to BloxOne Threat Defense will need outbound 443 access to the following addresses:

Domain	Port	Description
Cp.noa.infoblox.com app.noa.infoblox.com csp.infoblox.com grpc.csp.infoblox.com tide.infoblox.com	443	Management, logging
52.119.40.100 103.80.5.100	443, 53	DNS over TLS forwarding

Note: The source address will be the physical IP of the NIOS device, not a Virtual IP.

IPAM Metadata Upload

Follow the instructions on Collecting IPAM Metadata from a NIOS Source to upload IPAM Metadata to the CSP from NIOS. You can upload useful IPAM metadata from the NIOS grid to be enriched in BloxOne Threat Defense, such as Hostnames, DHCP Fingerprints and more.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com