Deployment Guide

Infoblox NIOS Integration with Fortinet Fortigate
Using Outbound Notifications
# TABLE OF CONTENTS

- Introduction .................................................................................................................. 3
- Prerequisites .................................................................................................................... 3
- Known Limitations .......................................................................................................... 3
- Best Practices .................................................................................................................. 3
- Configuration .................................................................................................................. 4
- Workflow ......................................................................................................................... 4
- Before you get Started ..................................................................................................... 4
- Download Templates from the Infoblox Community Web-Site ....................................... 4
- Editing Session Variables .............................................................................................. 5
- Editing Instance Variables ............................................................................................. 5
- Supported Notification ................................................................................................... 5
- Infoblox Permissions ....................................................................................................... 6
- Fortinet FortiGate Configuration .................................................................................... 6
- Adding API user (Permissions) ....................................................................................... 6
- Address Groups and Policies .......................................................................................... 8
- Infoblox NIOS Configuration ......................................................................................... 13
- Check if the Security Ecosystem License is Installed ................................................... 13
- Add/Upload Templates .................................................................................................... 14
- Modifying Templates ....................................................................................................... 15
- Add a Rest API Endpoint ................................................................................................ 17
- Adding Token ................................................................................................................ 20
- Add a Notification ........................................................................................................... 20
- Emulate an Event ............................................................................................................ 24
- Address Object Management ......................................................................................... 25
- DNS Security Event Remediation ................................................................................... 28
Introduction
Infoblox and Fortinet FortiGate: Securing your Network
From IoT to an always-on mobile workforce, organizations face increasingly complex IT infrastructures that are more exposed to attacks than ever before. By combining Infoblox’s DNS security and protection with Fortinet’s Next Generation Firewall (NGFW), users can automate the security of their network. The Outbound REST API integration framework from Infoblox provides a mechanism to create updates for both IPAM data (networks, hosts, leases) and DNS threat data into additional ecosystem solutions. Infoblox and FortiGate NGFW together enable security and incident response teams to leverage the integration of firewalls and DNS security to enhance visibility, manage assets, ease compliance and automate remediation. Thus, improving your security posture while maximizing your ROI in both products.

Prerequisites
The following are prerequisites for the integration using Outbound API notifications:

1. Infoblox:
   - NIOS 8.2 or higher.
   - Security Ecosystem License.
   - Outbound API integration templates.
   - Pre-configured services: DNS, DHCP, Discovery, RPZ, Threat Analytics and ADP.
   - NIOS API user with the following permissions (access via API only):
     - All Network Views – RW.
     - All Hosts – RW.
     - All IPv4 Networks – RW.
     - All IPv6 Networks – RW.
     - All IPv4 Ranges – RW.
     - All IPv6 Ranges – RW.
     - All IPv4 DHCP Fixed Addresses/Reservations – RW.
     - All IPv6 DHCP Fixed Addresses/Reservations – RW.

2. FortiGate NGFW
   - FortiGate v6.0.1 or higher.

Known Limitations
The current templates support DNS Firewall (RPZ), Threat Insight (DNS Tunneling), Advanced DNS Protection, Network IPv4, Network IPv6, Range IPv4, Range IPv6, Host IPv4, Host IPv6, Fixed address IPv4, Fixed address IPv6, lease, and discovery events only. If additional templates come out they will be found on the community site.

Best Practices
Outbound API templates can be found on the Infoblox community site on the partners integration page. After registering an account, you can subscribe to the relevant groups and forums. If additional templates come out, they will be found on the community site.
For production systems, it is highly recommended to set the log level for an end-point to “Info” or higher (“Warning”, “Error”). Please refer to the Infoblox NIOS Administrator’s Guide about other best practices, limitations and any
detailed information on how to develop notification templates. The NIOS Administrator’s Guide can be found through the Help panel in your Infoblox GUI, or on the Infoblox Support portal.

**Configuration**

**Workflow**

- **Fortinet:**
  1. Add the user and user group with the appropriate permissions.
  2. Add the required address groups.
  3. Add the Firewall policies.

- **Infoblox:**
  1. Install the Security Ecosystem license if it was not installed.
  2. Check that the necessary services and features are properly configured and enabled, including DNS, DHCP, Threat Insight, RPZ and Discovery.
  3. Create the required Extensible Attributes.
  4. Download (or create your own) notification templates (Fortinet_Security.json, Fortinet_Assets.json, Fortinet_Session.json) from the Infoblox community web-site.
  5. Add templates.
  6. Add a REST API Endpoint.
  7. Add Notifications.
  8. Emulate an event, check Rest API debug log and/or verify changes on the grid.

**Before you get Started**

**Download Templates from the Infoblox Community Web-Site**

Outbound API templates are an essential part of the configuration. Templates fully control the integration and steps required to execute the outbound notifications. Detailed information on how to develop templates can be found in the NIOS Administrator’s guide.

Infoblox does not distribute any templates (out-of-the-box) with the NIOS releases. Templates are available on the Infoblox community web-site. Templates for the Fortinet integration will be located in the “Partners Integrations”. You can find other templates posted in the “API & Integration” forum.

Templates may require additional extensible attributes, parameters or WAPI credentials to be created or defined. The required configuration should be provided with a template. Don’t forget to apply any changes required by the template before testing a notification.

**Table 1. Extensible Attributes**

<table>
<thead>
<tr>
<th>Extensible Attributes</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fortinet_Asset_Group</td>
<td>Defines which address group in FortiGate NGFW to add/delete objects from.</td>
<td>String</td>
</tr>
<tr>
<td>Fortinet_Asset.Sync</td>
<td>True/False: Defines if the network object is added/deleted from FortiGate NGFW.</td>
<td>List (true,false)</td>
</tr>
<tr>
<td>Fortinet_Asset_SyncedAt</td>
<td>Provides the last time the network object was</td>
<td>String</td>
</tr>
</tbody>
</table>
added/modified on FortiGate NGFW.

Fortinet_Security_Group
Defines which address group in FortiGate NGFW to add objects to, at the time of a security incident.
String

Fortinet_Security.Sync
True/False: Defines if the network object is added to FortiGate NGFW, at the time of a security incident.
List (true,false)

Fortinet_Security.SyncedAt
Provides the last time the network object was added/updated after a security event in the FortiGate NGFW.
String

**Editing Session Variables**
The Fortinet_Session template uses a session variable to login to the FortiGate appliance. Session variables can be entered through the grid GUI at “Grid” → “Ecosystem” → “Outbound Endpoint” and then selecting the endpoint you created at “Edit” → “Session Management”.

*Table 2. Session Variables*

<table>
<thead>
<tr>
<th>Session Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token</td>
<td>The token with which a user can make API calls to the FortiGate appliance</td>
</tr>
</tbody>
</table>

**Editing Instance Variables**
The Fortinet_Security template uses an instance variable to adjust the templates’ behavior. Instance variables can be entered through the grid GUI at “Grid” → “Ecosystem” → “Notification” and then selecting the notification you created at “Edit” → “Templates”.

*Table 3. Instance Variables*

<table>
<thead>
<tr>
<th>Instance Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fortinet_Security_Group</td>
<td>Defines which address group in the FortiGate NGFW the network object needs to be added to at the time of a security event</td>
</tr>
</tbody>
</table>

**Supported Notification**
A notification can be considered as a "link" between a template, an endpoint and an event. In the notification properties, you define which event triggers the notification, which template is executed and with which API endpoint NIOS will establish the connection to. The Fortinet templates support a subset of available notifications (refer to the limitations chapter in this guide for more details). In order to simplify the deployment, only create required notifications and use the relevant filters. It is highly recommended to configure deduplication for RPZ events and exclude a feed that is automatically populated by Threat Analytics.

*Table 4. Supported Notifications*

<table>
<thead>
<tr>
<th>Notification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS RPZ</td>
<td>DNS queries that are malicious or unwanted</td>
</tr>
<tr>
<td>DNS Tunneling</td>
<td>Data exfiltration that occurs on the network</td>
</tr>
<tr>
<td>ADP</td>
<td>DNS queries that are malicious or unwanted</td>
</tr>
</tbody>
</table>
DHCP Leases | Lease events that occur on the network
---|---
Object Change Network IPv4 | Added/Deleted IPv4 network objects.
Object Change Network IPv6 | Added/Deleted network IPv6 objects.
Object Change Range IPv4 | Added/Deleted Host IPv4 objects.
Object Change Range IPv6 | Added/Deleted Host IPv6 objects.
Object Change Fixed Address IPv4 | Added/Deleted fixed/reserved IPv4 objects.
Object Change Fixed Address IPv6 | Added/Deleted fixed/reserved IPv6 objects.
Object Change Host Address IPv4 | Added/Deleted Host IPv4 objects.
Object Change Host Address IPv6 | Added/Deleted Host IPv6 objects.
Object Change Discovery Data | Discovery events that occur on the network.

Infoblox Permissions

The Infoblox and Fortinet integration requires a few permissions for the integration to work. Navigate to “Administration” → “Administrators” and add a “Roles”, “Permissions”, “Groups” and “Admins” to include permissions that are required for the integrations. When creating a new group, under the “Groups” tab, select the “API” interface under the “Allowed Interfaces” category.

Fortinet FortiGate Configuration

Adding API user (Permissions)

1. Navigate to “System” → “Admin Profiles”, the click Create New.

2. Enter a name for the profile.
3. Add the “Read/Write” permission for “Firewall” and click on “OK”.

4. Navigate to “System” → “Administrators”, then click Create New, and select “REST API Admin”.

![FortiGate Interface](image-url)
5. Enter the details for the user, and select the previously created Admin Profile, and click on OK.

6. A new API key is generated for this user. For the integration, this key is used as a Token for authenticating the user. The Token is fed as a session Variable, as described Editing Session Variables chapter.

Address Groups and Policies
The Infoblox and Fortinet integration requires address groups. In order to add the address groups:
1. Navigate to “Policy & Objects” → “Addresses”, then click “Create New” and select “Address”.

2. Create a dummy address. You can use the below specified details as a reference and click on “OK”.

   - Category: dummy address
   - Type: Subnet
   - Subnet/IP Range: 1.1.1.1/32
   - Interface: any
   - Static Route Configuration: Off
   - Comments: None
   - Tags: Add Tag Category

   ![Image of address creation process]
3. To create an address group, navigate to “Policy & Objects” \(\rightarrow\) “Addresses”, then click “Create New” and select “Address Group”.

4. Create a group on which you can set the allow policy. You can use the below specified details as a reference, and click on “OK”.

\[\text{Image of FortiGate UI for creating an address group and setting allow policy.}\]
5. Similarly, create a group on which you can set the deny policy. You can use the below specified details as a reference, and click on “OK”.

6. Similarly, create a dummy IPv6 address and 2 IPv6 groups, one for the allow policy and one for the deny policy.
7. Navigate to “Policy & Objects” → “IPv4 Policy”, then click “Create New”.

8. Create a policy for the previously created allow group to allow all traffic as shown in the image below.
9. Similarly, create a policy for the previously created deny group to deny all traffic as shown in the image below.

![Policy Creation](image1.png)

10. Similarly, create the allow and deny policies for IPv6 by navigating to “Policy & Objects” → “IPv6 Policy”, then clicking “Create New”.

![IPv6 Policy](image2.png)

Infoblox NIOS Configuration

**Check if the Security Ecosystem License is Installed**

Security Ecosystem License is a “Grid Wide” License. Grid wide licenses activate services on all appliances in the same Grid.

In order to check if the license was installed navigate to “Grid” → “Licenses” → “Grid Wide”.

---

Infoblox Deployment Guide - Infoblox NIOS integration with Fortinet Fortigate Using Outbound Notifications – Nov 2018
Add/Upload Templates

In order to upload/add templates:

1. Navigate to “Grid” → “Ecosystem” → “Templates”, and click “+” or “+ Add Template”.
2. Click the “Select” button on the “Add template” window.
3. Click the “Select” button on the “Upload” window. The standard file selection dialog will open.
4. Select the file and Click the “Upload” button on the “Upload” window.
5. Click the “Add” button and the template will be added/uploaded.
6. If a template was previously uploaded, click “Yes” to overwrite the template.

7. You can review the uploaded results in the syslog or by clicking the “View Results” button.

Note: There is no difference between uploading session management and action templates.

Modifying Templates

NIOS provides the facility to modify the templates via the web-interface.
1. Navigate to “Grid” → “Ecosystem” → “Templates”, and then click the gear icon next to the template you want to modify.

2. Click the “Edit” button to open up the “Template” window.
3. Click on the **Contents** tab to view/edit the template.

The template editor is a simple interface for making changes to templates. It is recommended to only use the template editor to make minor changes. You can also edit, cut and paste template snippets from a text editor of your choice.

**Note:** You cannot delete a template if it is used by an endpoint or by a notification.

**Add a Rest API Endpoint**

A “**REST API Endpoint**” is basically a remote system which should receive changes based on a notification and a configured template. A Grid, for example, can not only send notifications, it can also receive the notifications from itself (e.g. for testing purposes).

In order to add REST API Endpoints:
1. Navigate to “Grid” → “Ecosystem” → “Outbound Endpoints” and click “+” or “+ Add REST API Endpoint” buttons. The “Add REST API Endpoint Wizard” window will open.

2. The URI and Name for the appliance you are integrating with are required.

3. The URI should be the IP/FQDN of the appliance you are integrating with, with the correct URI scheme.
4. Specify **“WAPI Integration Username”** and **“WAPI Integration Password”** (NIOS credentials).

![Image of WAPI Integration Configuration]

5. (Optional) For debug purposes only: Under **“Session Management”**, set **“Log Level”** to **“Debug”**.

![Image of Log Level Configuration]
6. The Token can be found when you create the Fortinet API user. When possible, it is recommended to send notifications from a Grid Master Candidate instead of from the Grid Master.

**Adding Token**

1. (NIOS 8.3 or later) Navigate to “Grid” → “Ecosystem” → “Outbound Endpoint” and click on the Fortinet FortiGate NGFW endpoint and click “Edit”.

2. (NIOS 8.3 or later) Navigate to the “Session Management” tab and add the “Token” to the value fields.

![Fortinet FortiGate NGFW (REST API Endpoint)](image)

**Add a Notification**

An endpoint and a template must be added before you can add a notification. In order to add notifications:
1. Navigate to “Grid”  “Ecosystem”  “Notification” and click “+” or “+ Add Notification Rule” then the “Add Notification Wizard” window will open.

2. Specify the notification’s name and select an endpoint (Target), click “Next”.

   ![Add Notification Wizard](image)
3. Select an event type and define a filter. Note: For optimal performance, it is best practice to make the filter as narrow as possible. Click “Next”.

![Add Notification Wizard Step 2 of 4](image)
4. (For Security related notifications only) Check “Enable event deduplication” and specify relevant parameters. Click “Next”.

![Image of the Add Notification Wizard Step 3 of 4]

- Enable event deduplication
- Log all dropped events due to deduplication
- Select the fields to use for deduplication

Available fields:
- RPZ Policy
- RPZ Type
- Query Type
- Network
- Network View

Selected fields:
- Source IP
- Query Name

Lockback Interval: 10 minutes
5. Select a relevant template and specify the template's parameters if any are required. Click “Save & Close”.

6. Similarly add rules for other events as well.

Emulate an Event

(Optional) On the Infoblox grid, navigate to “Grid” → “Ecosystem” → “Outbound Endpoint”, select “Fortinet”, click on the gear icon and select “Clear Debug Log”.
Address Object Management


1. To create an IPv4 reservation, navigate to "Data Management" → "IPAM". Select an IPv4 network here (say 172.0.0.0/24).

2. Click the drop down next to the "+ Add" button under the toolbar and choose "IPv4 Reservation".
3. Click **Next**, then insert the IP “172.0.0.10” into the “IP Address” field.

![Add IPv4 Reservation Wizard Step 2 of 8](image)

4. Click on “Next” till you reach the Extensible Attributes window. If the Extensible Attributes have not already been inherited from the network, set them.

![Add IPv4 Reservation Wizard > Step 7 of 8](image)

5. Click **Save & Close**.
6. Select the IP and refresh. The “Fortinet_Asset_SyncedAt” EA is now updated.

7. In the firewall, navigate to “Policy & Objects”. The “Infoblox_FixedAddress_172.0.0.10” address reservation has been added to the “Address” list and the “allow_group” Address Group. Refresh the page if necessary.

8. In the Infoblox grid, delete the “172.0.0.10” reservation by selecting the reservation and clicking the “reclaim” button. Wait about 10 seconds.
9. On the Firewall, navigate to “Policy & Objects” and verify that the “Infoblox_FixedAddress_172.0.0.10” entry has been removed from the “Address” list and the “allow_group” Address Group. Refresh the page if necessary.

<table>
<thead>
<tr>
<th>name</th>
<th>type</th>
<th>details</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIREWALL_AUTH_PORTAL_ADDRESS</td>
<td>Subnet</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>SSLVPN_TUNNEL_ADDR1</td>
<td>IP Range</td>
<td>10.212.134.200 - 10.212.134.210</td>
</tr>
<tr>
<td>all</td>
<td>Subnet</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>dummy_address</td>
<td>Subnet</td>
<td>1.1.1.1/32</td>
</tr>
<tr>
<td>google-play</td>
<td>FQDN</td>
<td>play.google.com</td>
</tr>
<tr>
<td>none</td>
<td>Subnet</td>
<td>0.0.0.0/32</td>
</tr>
<tr>
<td>swscan.apple.com</td>
<td>FQDN</td>
<td>swscan.apple.com</td>
</tr>
<tr>
<td>update.microsoft.com</td>
<td>FQDN</td>
<td>update.microsoft.com</td>
</tr>
</tbody>
</table>

**DNS Security Event Remediation**

This use case shows Infoblox DDI possibility to respond on any DNS Security events and request FortiGate Firewall to add clients to the “deny_group”.

1. Simulate a security event by querying for a domain that is blocked by your RPZ.
   a. Launch a command prompt and perform a `nslookup` request for “example.com”.
b. Optionally, you can send a dig request to “example.com”.

![Image of dig request]

2. Ensure the “Fortinet_Security_Sync” is set to “true” on the network or the IP address/host record. If the “Fortinet_Security_Group” is not set, the value specified while assigning the instance variable during the creation of notification rules is taken into account.

![Image of firewall policy]

3. In the firewall, navigate to “Policy & Objects”. The “Infoblox_RPZ_172.0.0.1” host has been added to the “Address” list and the “deny_group” Address Group. Refresh the page
4. In the Infoblox Grid, navigate to "Data Management" → "IPAM" → "172.0.0.1/24". Select the IP "172.0.0.1" and refresh. The "Fortinet_Secutiy_SyncedAt" EA is now updated.

Optionally, navigate to "Grid" → "Ecosystem" → "Outbound Endpoint", select "Fortinet", click on the gear icon and select "View Debug Log". Here you can see the debug log’s step-by-step execution flow of the template.
Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.