DEPLOYMENT GUIDE

PAN Firewall & Infoblox NIOS Outbound API Integration

Table of Contents

Introduction

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 Palo Alto Firewall together enable security and incident response teams to leverage the integration of vulnerability scanners 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 Outbound API notifications:

Infoblox

1. NIOS 8.4 or higher
2. Security Ecosystem license
3. Outbound API integration templates
    - Available for free download on the Infoblox community site after creating an account.
4. Prerequisites for templates
    - ex. Configured and set extensible attributes.
5. Preconfigured services. You may only need some if you need to sync only certain event types to the PAN firewall depending on your needs.
    - DNS
    - DHCP
    - RPZ
    - Threat Analytics
    - Discovery
6. NIOS API user with the following permissions (access via API only)
    - All Hosts – R-W
    - All DHCP Fixed Addresses/Reservations – R-W
    - All IPv4 Networks – R-W

PAN Firewall

1. Installed and configured PAN Firewall
    - Tested with PAN 8.1, 9, and 10.1
2. User credentials for the PAN Firewall
    - User requires access to Address and Address group objects within PAN

Static and Dynamic Address Groups

To simplify the creation of security policies, addresses that require the same security settings can be combined into address groups. An address group can be static or dynamic. Depending on your needs, you may decide that one is better for you (or both). A static address group can include address objects that are static, other dynamic address groups, or both. A dynamic address group populates its members dynamically via tag-based filters.

Known Limitations

When force rebooting the firewall, it may cause IP to tag mappings loss.

Best Practices

Outbound API templates are available on the Infoblox community site. For production systems it is highly recommended to set the log level for an endpoint to Info or higher (Warning, Error). Please refer to the NIOS Administration guide about other best practices, limitations, and any detailed information on how to develop notification templates.

Workflow

Use the following workflow to enable, configure and test outbound notifications:

1. Install licenses and configure services.
    - The **Security Ecosystem is required** for this integration.
    - Install other licenses and services as necessary. You may only need some if you need to sync only certain event types to the PAN firewall depending on your needs.
2. Create Extensible Attributes.
3. Create or download appropriate templates from the Infoblox community website: Palo Alto Dynamic Assets, Palo Alto Dynamic Security, Palo Alto Static Assets, Palo Alto Static Security, PaloAlto_login, PaloAlto_logout, and Palo Alto Session.
4. Add/upload the notification templates.
5. Add a REST API Endpoint.
6. Add Notifications.
7. Emulate an event, then check the debug log and/or verify changes on the REST API Endpoint.

Infoblox Community Website Templates

The templates are executed when applicable events occur in NIOS and match Notification rules. They contain the code that sync events to an outbound endpoint. Detailed information on how to develop templates can be found in the NIOS Administrator guide. Infoblox does not distribute any templates with NIOS releases (out-of-box). Templates are available on the Infoblox community website. Templates may require additional extensible attributes to be created, parameters, or WAPI credentials defined.

Session Variables

Name	*Description*
Host_Allow	The static address group object which needs to be populated on the firewall for allowed hosts. This should be the same as the address group object created through the Palo Alto configuration. Set a default value (Iblox_Host_Allow).
Host_Deny	The static address group object which needs to be populated on the firewall for denied hosts. This should be the same as the address group object created through the Palo Alto configuration. Set a default value (Iblox_Host_Deny).

Extensible Attributes

Name	*Description*	*Type*
PaloAlto_Asset_Sync	Serves as a toggle to turn on/off sync for Asset Events.	List (true, false)
PaloAlto_Security_Sync	Serves as toggle to turn on/off sync for Security Events.	List (true, false)
PaloAlto_Asset_SyncedAt	Update timestamp on an asset event. This attribute is created on the specific IP by the WAPI call when not present.	String
PaloAlto_Security_SyncedAt	Update timestamp on a security event. This attribute is created on the specific IP by the WAPI call when not present.	String
PaloAlto_Asset_Tag	[Dynamic Only] - Tag that attaches to an IP in a Dynamic Address Group.	String
PaloAlto_Security_Tag	[Dynamic Only] - Tag that attaches to an IP in a Dynamic Address Group.	String
PaloAlto_Timeout	[Dynamic Only] - Starting with PAN-OS 9.0 a tag can contain an optional timeout attribute. Default is 0 (never expires) or a timeout value in seconds for the tag. Maximum timeout is 2592000 (30 days). In older versions of PAN-OS, this attribute cannot be accessed and IPs never timeout	Integer

Supported Notifications

A notification can be considered as a link between a template, an endpoint, and an event. In the notification properties, you can define the event and rules that trigger the notification, the template to execute, and the external endpoint. The templates support a subset of available notifications It is highly recommended to configure deduplication for RPZ events and exclude a feed that is automatically populated by Threat Analytics.

Notification	*Description*
DNS RPZ	Malicious or unwanted DNS queries
DNS Tunneling	Data exfiltration occurring on the network
Security ADP	Malicious or unwanted DNS queries (via ADP)
Object Change Fixed Address IPv4	Added/Deleted fixed/reserved IPv4 objects
Object Change Host Address IPv4	Added/Deleted host IPv4 objects
Object Change Fixed Address IPv6	[Dynamic Only] - Added/Deleted fixed/reserved IPv6 objects
Object Change Host Address IPv6	[Dynamic Only] - Added/Deleted host IPv6 objects
Object Change Network IPv4	Added/Deleted network IPv4 objects
DHCP Leases	DHCP lease events
Discovery & vDiscovery	Added/Deleted discovered addresses

Template Parameters

Template parameters (or instance variables) are variables set in the template. They can be modified directly in the template or in a relevant Notification.

The following are exclusive to Discovery events for Dynamic Address Groups.

Parameter	*Description*	*Type*
Discovery_PaloAlto_Asset_Tag	[Dynamic Only] - Tag that attaches to an IP in a Dynamic Address Group. For Discovery events.	String
Discovery_PaloAlto_Asset_Sync	[Dynamic Only] - Serves as a toggle to turn on/off sync for Discovery events.	String (will only sync if set to ‘true’)

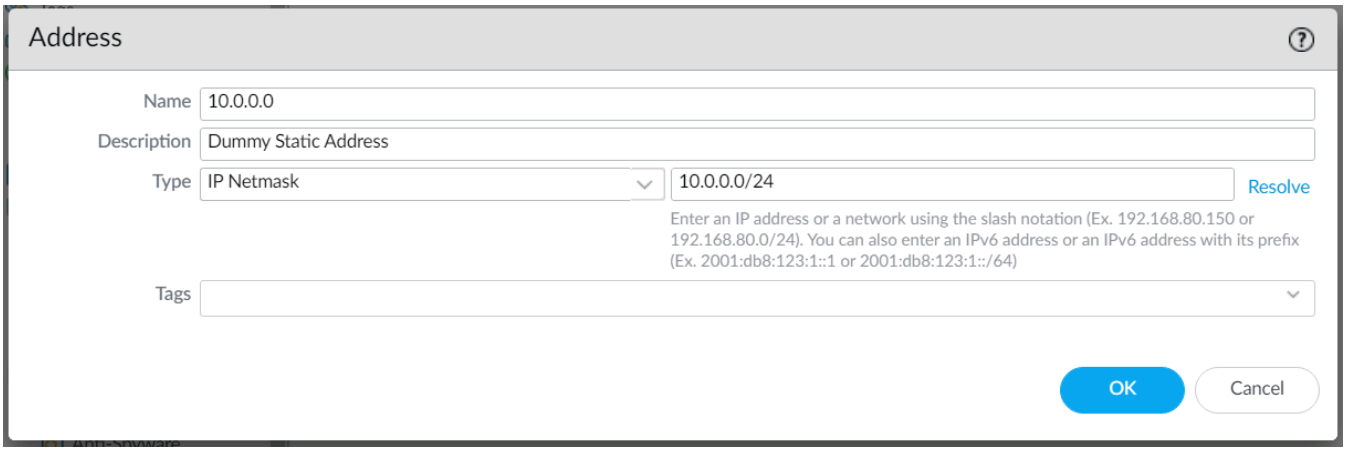
PAN Firewall Configuration for Static Address Groups

A static address group can include address objects that are static, dynamic address groups, or it can be a combination of both address objects and dynamic address groups.

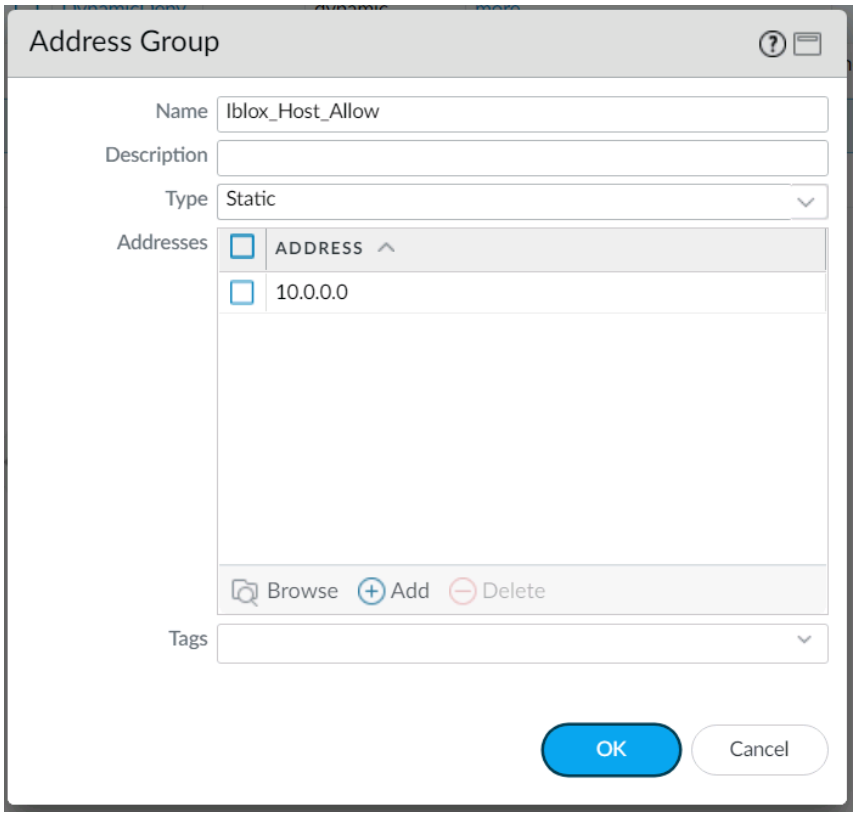
Create appropriate policies in the firewall to allow or deny hosts. A policy requires an existing address group object as part of the policy creation process. Let's create two Static Address Groups for allowing and denying hosts access to the firewall.

1. Login to the PAN Firewall.

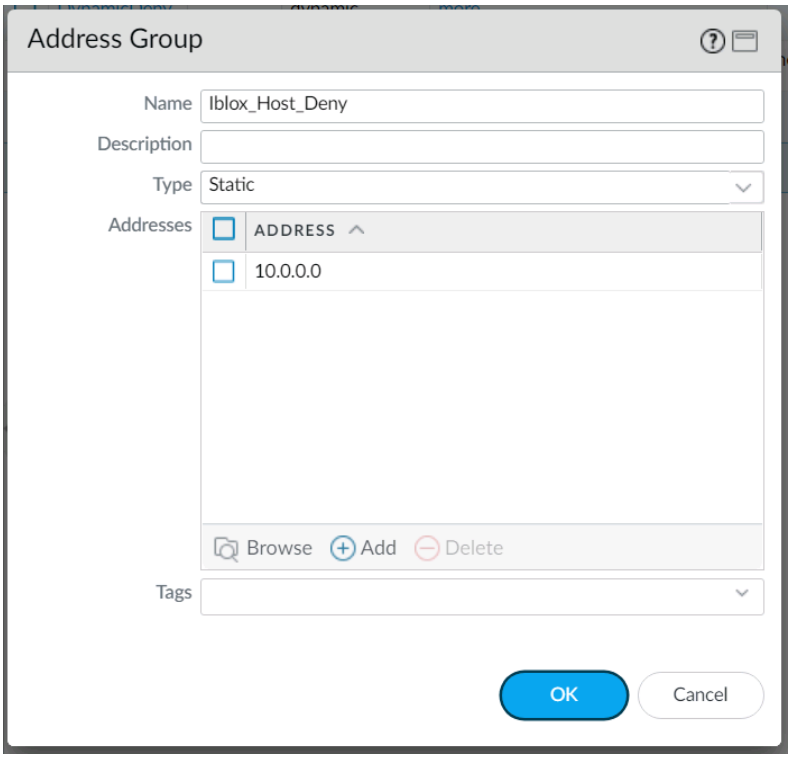
2. For a Static Address Group, you will need to create a dummy address to fill it with initially. Navigate to **Objects** → **Addresses**. Click ⊕ **Add** at the bottom of the screen.
    a. Enter a name, such as the IP. Set the type to IP Netmask. Enter 10.0.0.0/24 for the IP address.



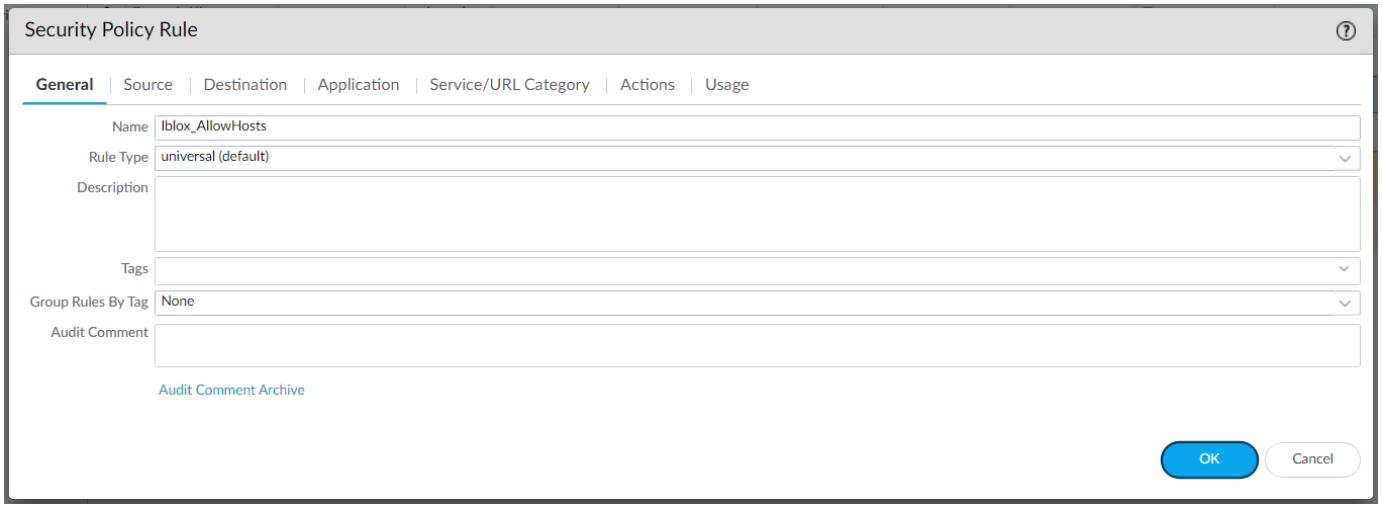
3. Create the two Static Address Groups that will hold hosts you wish to either allow or deny firewall access. Let's create the allowed group. Navigate to **Objects** → **Address Groups**. Click ⊕ **Add** at the bottom of the screen.
    a. Give the Address Group a comprehensible name, such as **Iblox_Host_Allow**. Set the type to Static. Click ⊕ **Add** and select the dummy address you just created. Click **OK**.



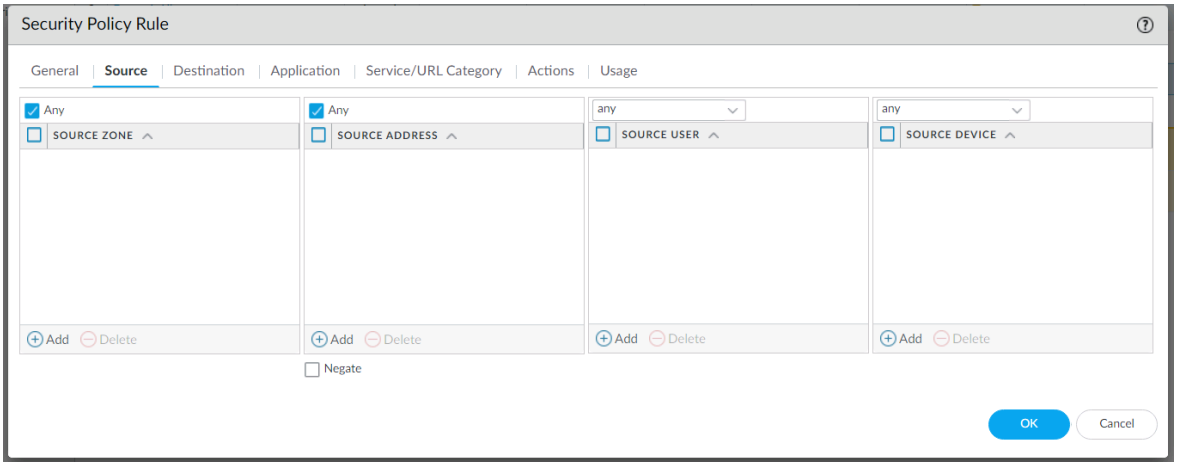
4. Now create the deny group. Navigate to **Objects** → **Address Groups**. Click ⊕ **Add** at the bottom of the screen.
    a. Give the Address Group a comprehensible name, such as **Iblox_Host_Deny**. Set the type to **Static**. Click ⊕ **Add** and select the dummy address you just created. Click **OK**.



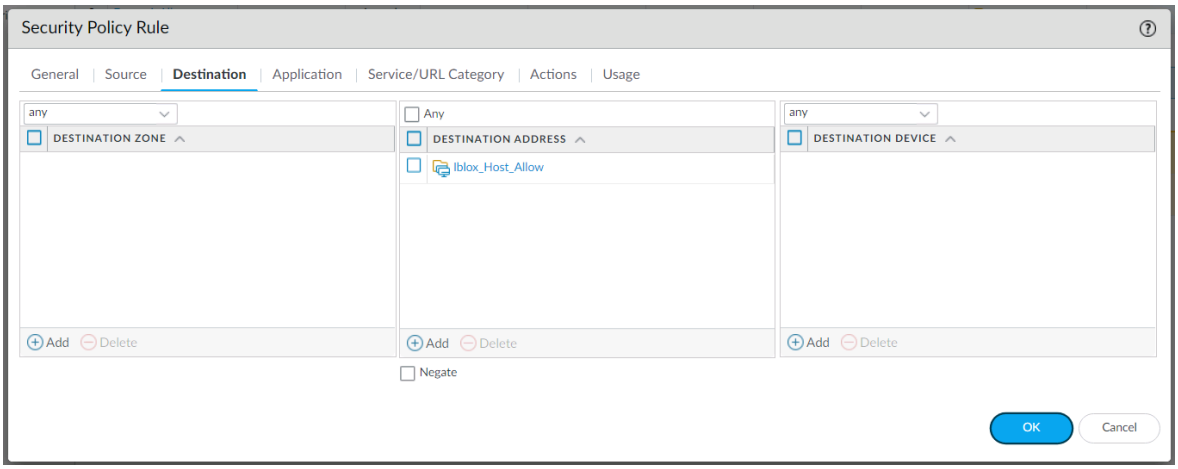
5. Create one policy for each of the Static Address Groups we just created so that PAN knows how to handle inbound hosts. Let's create a policy that will allow Infoblox hosts. Navigate to **Policies** → **Security**. Click ⊕ **Add** at the bottom of the screen.
    a. Under the General tab, name the policy.



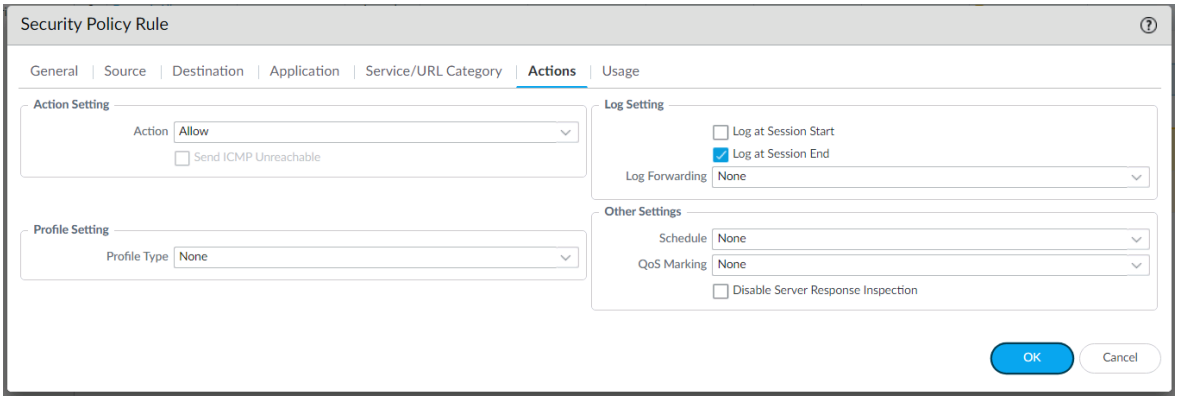
b. Under the Source tab, check the Any box above the SOURCE ZONE and SOURCE ADDRESS areas. Select any from the dropdown above the SOURCE USER and SOURCE DEVICE areas.



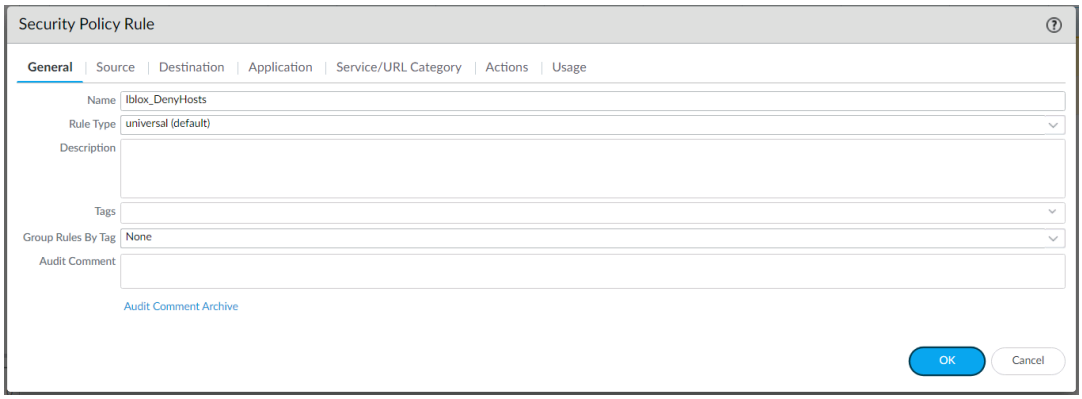
c. Under the Destination tab, select any from the dropdown above the DESTINATION ZONE and DESTINATION DEVICE areas. Click the ⊕ **Add** button under the DESTINATION ADDRESS area and select the Iblox_Host_Allow Address Group created earlier for allowed hosts.



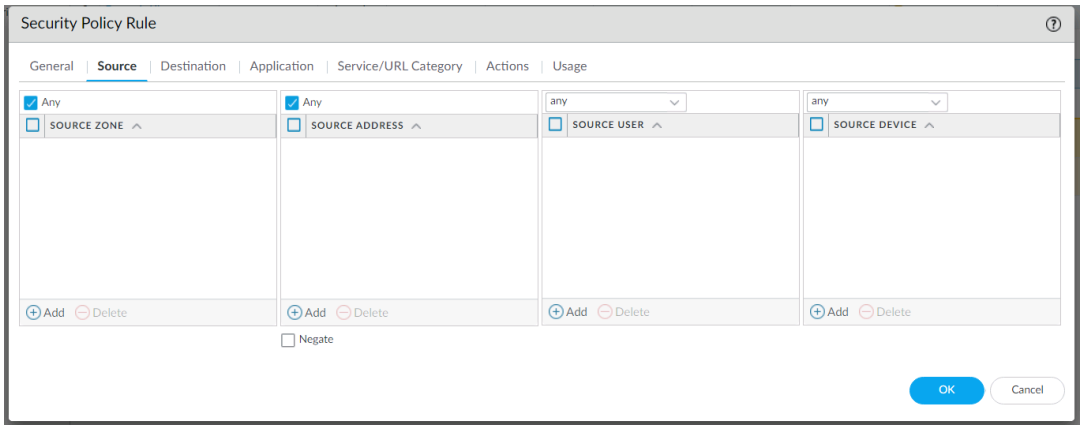
d. Under the Actions tab, set the Action Setting Action to Allow. Click **OK**.



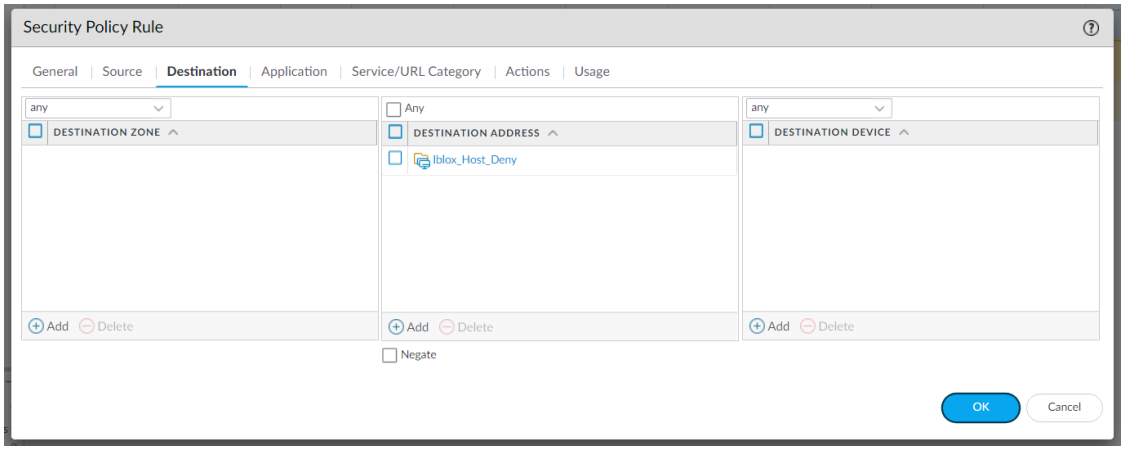
6. Let's create a policy that will deny Infoblox hosts. Navigate to **Policies** → **Security**. Click **Add** at the bottom of the screen.
    a. Under the General tab, name the policy.



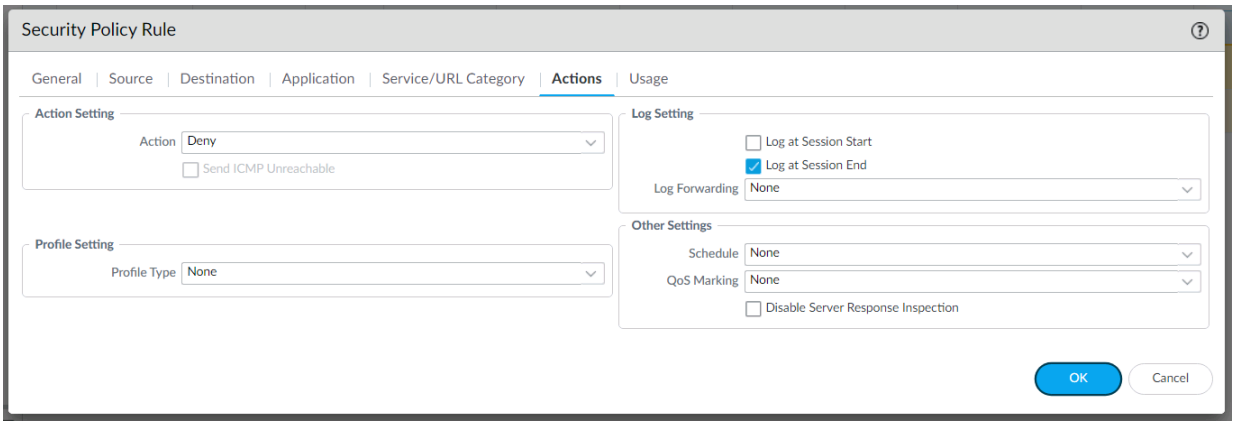
    b. Under the Source tab, check the Any box above the SOURCE ZONE and SOURCE ADDRESS areas. Select any from the dropdown above the SOURCE USER and SOURCE DEVICE areas.



    c. Under the Destination tab, select any from the dropdown above the DESTINATION ZONE and DESTINATION DEVICE areas. Click the **Add** button under the DESTINATION ADDRESS area and select the Iblox_Host_Deny Address Group created earlier for denied hosts.



d. Under the Actions tab, set the Action Setting Action to Deny. Click **OK**.



7. Click 

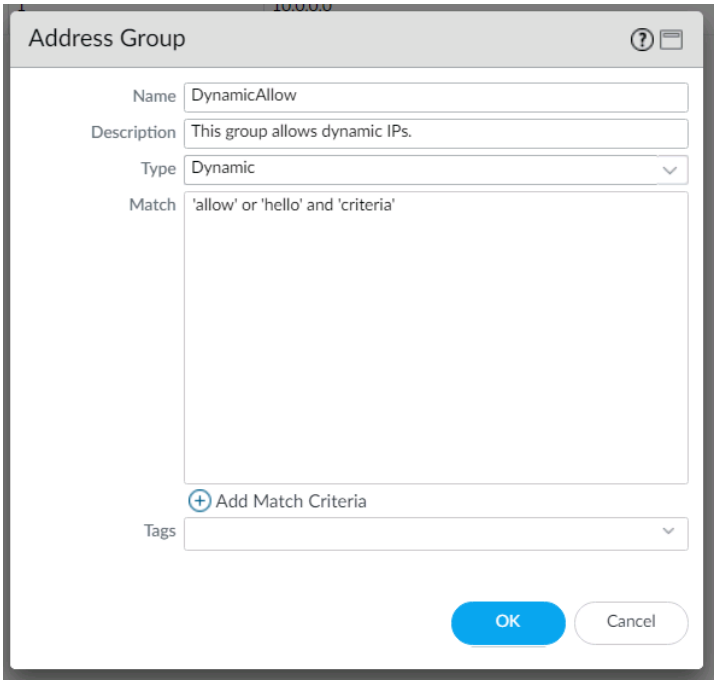
Commit in the upper right corner of the screen. This will activate your newly created Address, Address Groups and Policies on the running configuration of the firewall.

PAN Firewall Config for Dynamic Address Groups

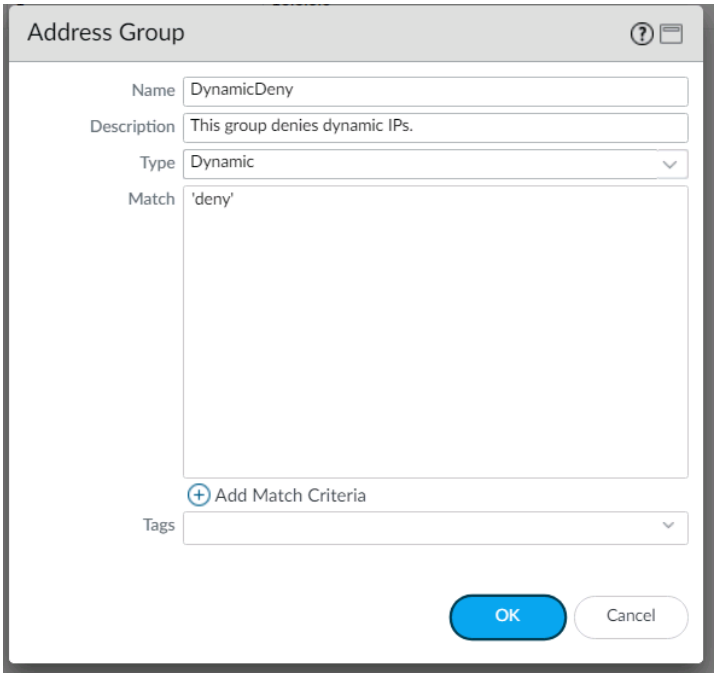
A dynamic address group populates its members dynamically using tag-based filters. Dynamic address groups are very useful if you have an extensive virtual infrastructure where changes in virtual machine location/IP address are frequent. For example, you have a sophisticated failover setup or provision new virtual machines frequently and would like to apply policy to traffic from or to the new machine without modifying the configuration/rules on the firewall.

Create appropriate policies in the firewall to allow or deny IP addresses. A policy requires an existing address group object as part of the policy creation process. Let's create two Dynamic Address Groups for allowing and denying hosts access to the firewall.

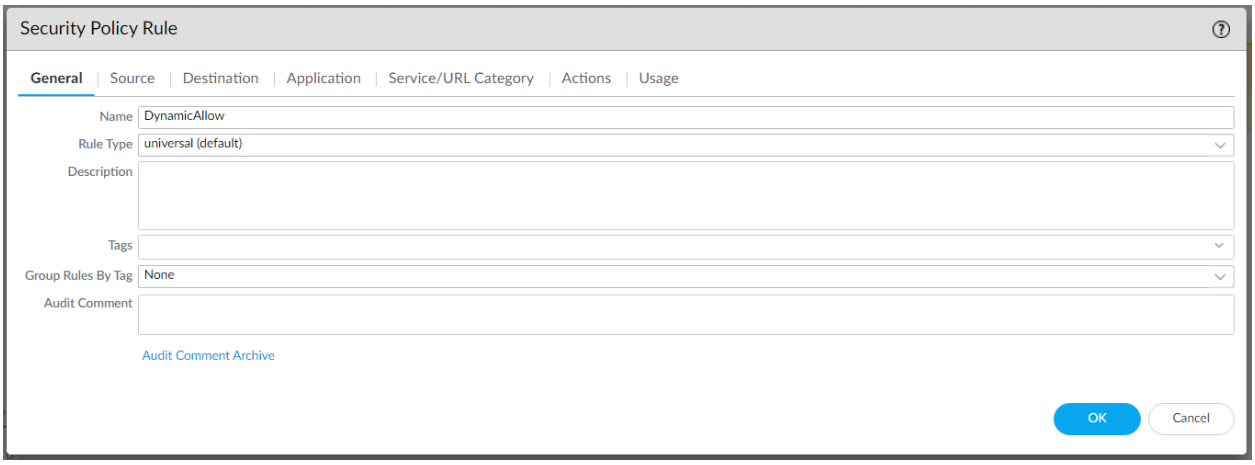
1. Login to the PAN Firewall.
2. Create the two Dynamic Address Groups that will hold hosts you wish to either allow or deny firewall access. Let's create the allow group. Navigate to **Objects** → **Address Groups**. Click **Add** at the bottom of the screen.
   a. Give the Address Group a comprehensible name, such as DynamicAllow. Set the type to Dynamic. To add match criteria, you can either click on **Add Match Criteria** and select existing static Tags to match the group with (you can create these under **Objects** → **Tags**), or you can type them in manually by putting single quotes around each criterion and separating them with terms and or or. Enter 'allow' for the match criteria. Click **OK**.



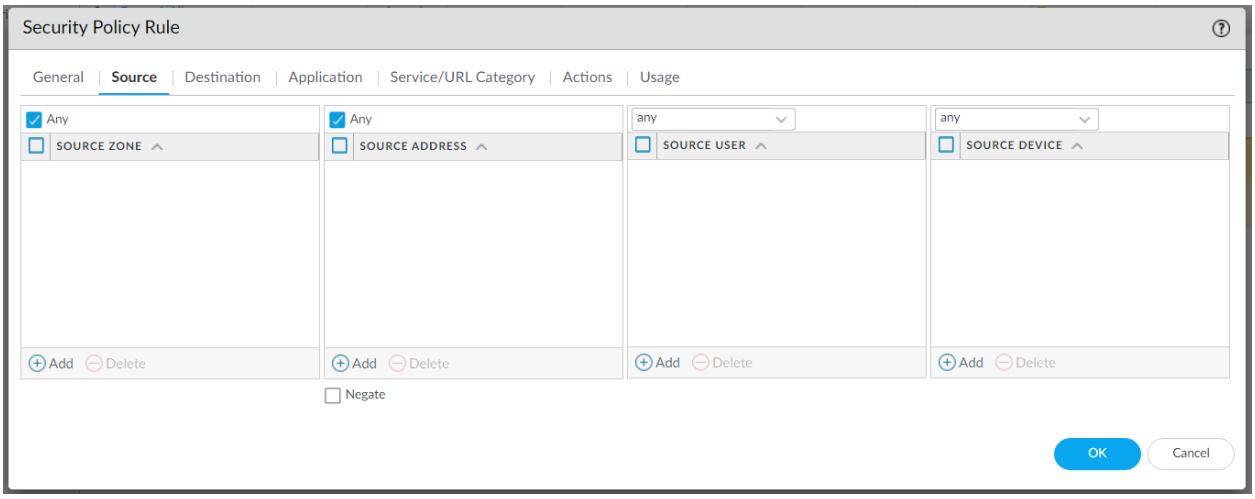
3. Now create the deny group. Navigate to **Objects** → **Address Groups**. Click **Add** at the bottom of the screen.
   a. Give the Address Group a comprehensible name, such as DynamicDeny. Set the type to Dynamic. To add match criteria, you can either click on **Add Match Criteria** and select existing static Tags to match the group with (you can create these under **Objects** → **Tags**), or you can type them in manually by putting single quotes around each criterion and separating them with terms **and** or **or**. Enter 'deny' for the match criteria. Click **OK**.



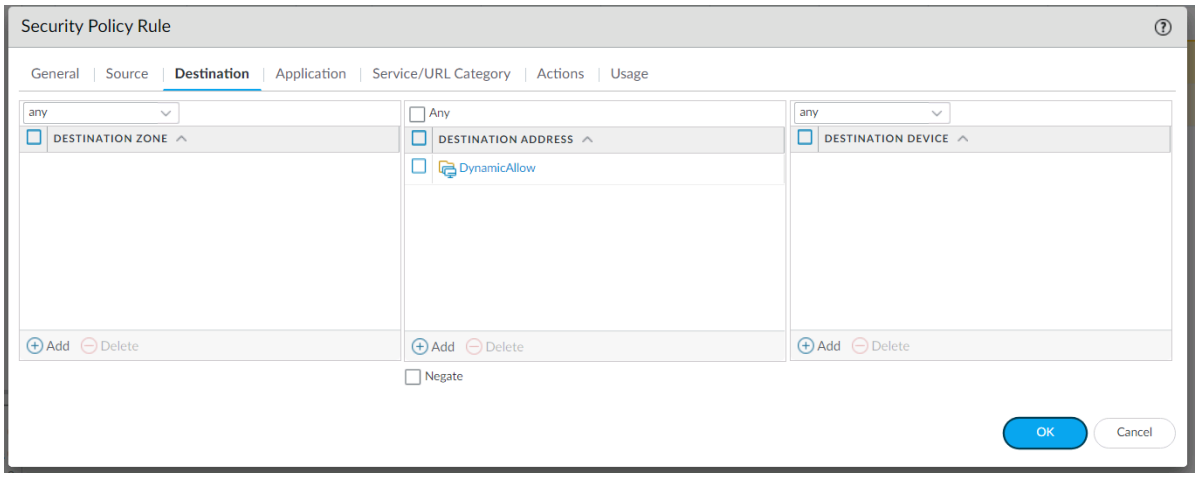
4. Create one policy for each of the Dynamic Address Groups we just created so that PAN knows how to handle inbound hosts. Let's create the policy that will allow Infoblox hosts. Navigate to **Policies** → **Security**. Click ⊕ **Add** at the bottom of the screen.
   a. Under the General tab, name the policy.



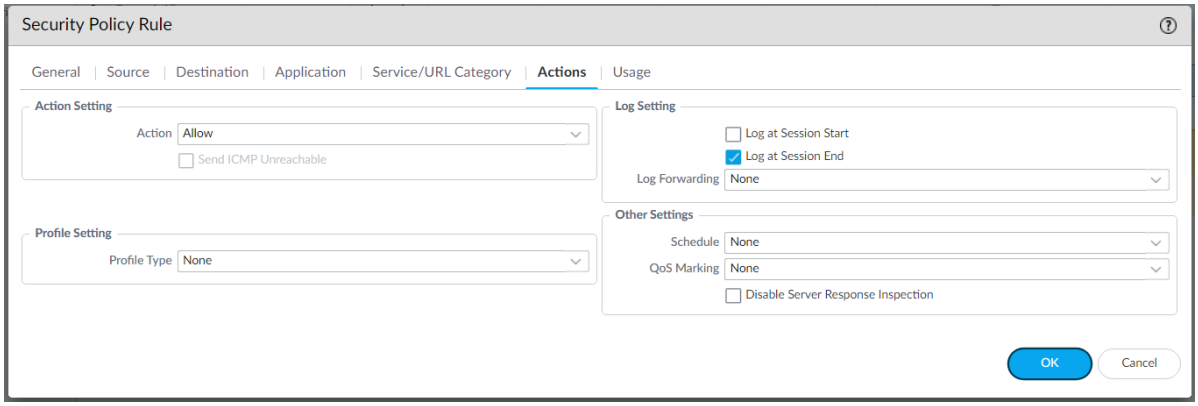
   b. Under the Source tab, check the Any box above the SOURCE ZONE and SOURCE ADDRESS areas. Select any from the dropdown above the SOURCE USER and SOURCE DEVICE areas.



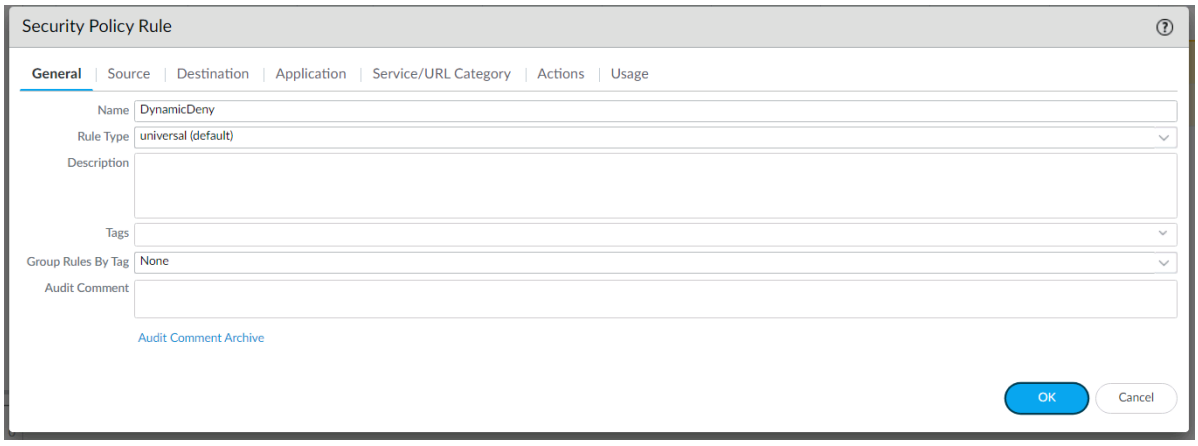
c. Under the Destination tab, select any from the dropdown above the DESTINATION ZONE and DESTINATION DEVICE areas. Click the **Add** button under the DESTINATION ADDRESS area and select the Dynamic Allow Address Group created earlier for allowed hosts.



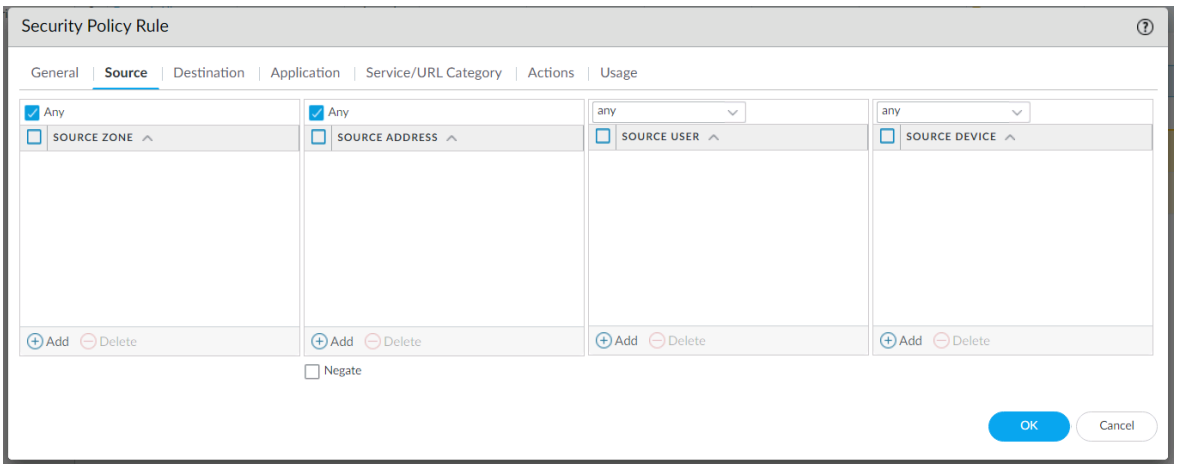
d. Under the Actions tab, set the Action Setting Action to Allow. Click **OK**.



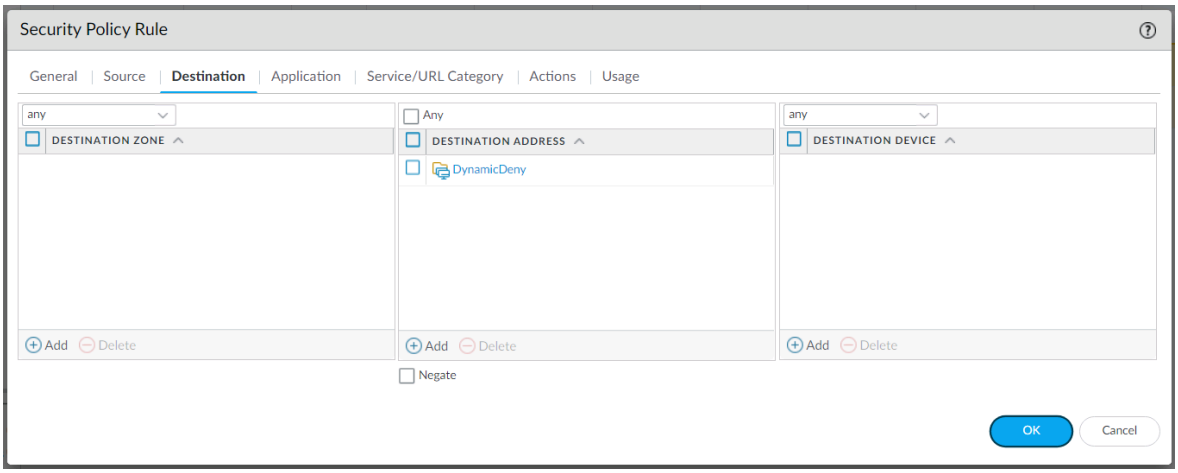
5. Let's create the policy that will deny Infoblox hosts. Navigate to **Policies** → **Security**. Click **Add** at the bottom of the screen.
   a. Under the General tab, name the policy.



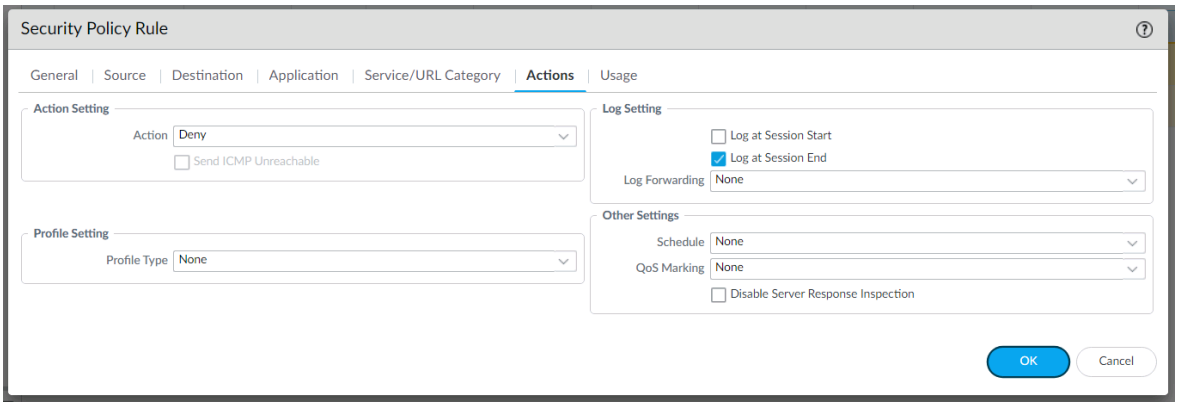
b. Under the Source tab, check the Any box above the SOURCE ZONE and SOURCE ADDRESS areas. Select any from the dropdown above the SOURCE USER and SOURCE DEVICE areas.



c. Under the Destination tab, select any from the dropdown above the DESTINATION ZONE and DESTINATION DEVICE areas. Click the ⊕ **Add** button under the DESTINATION ADDRESS area and select the DynamicDeny Address Group created earlier for denied hosts.



d. Under the Actions tab, set the Action Setting Action to Deny. Click **OK**.



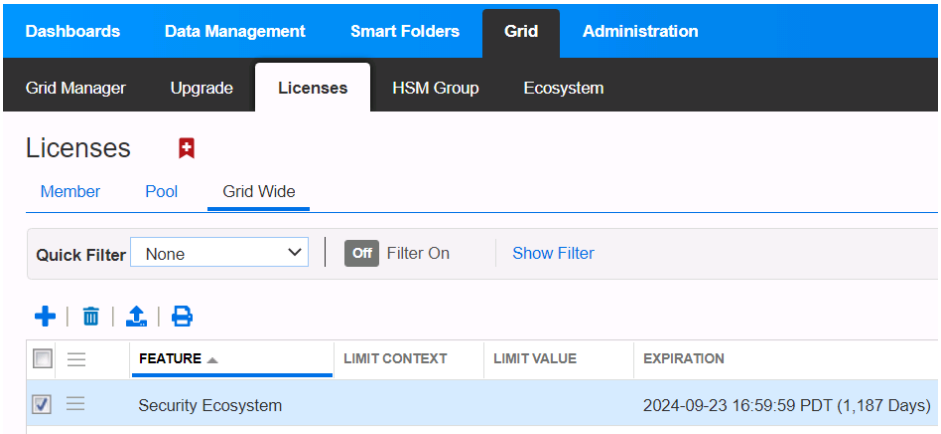
6. Click 

Commit in the upper right corner of the screen. This will activate your newly created Address, Address Groups and Policies on the running configuration of the firewall.

Infoblox NIOS Configuration

Verify Security Ecosystem License is Installed

The Security Ecosystem license is a Grid Wide license. Grid wide licenses activate services on all appliances in the same Grid. To verify if the license is installed, navigate to **Grid → Licenses → Grid Wide.**



Add/Upload Templates

Add the correct templates from the Infoblox community site.

For all features of PAN Dynamic Address Groups to work, you'll need these templates:

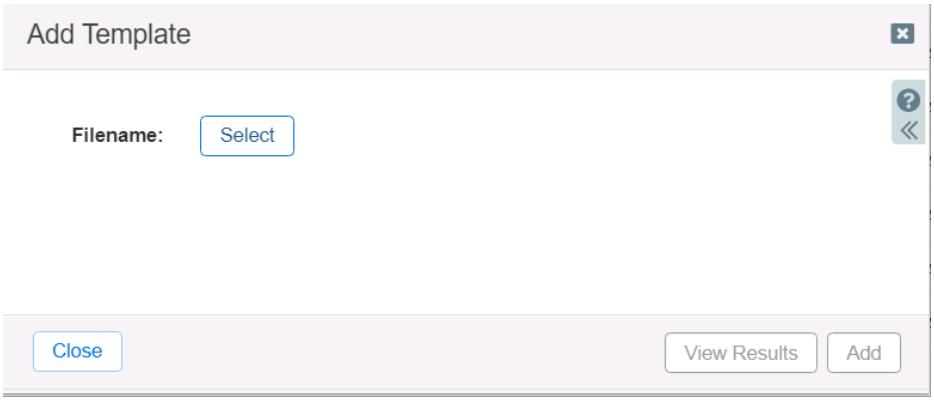
- Palo Alto Dynamic Assets
- Palo Alto Dynamic Security
- PaloAlto_login
- PaloAlto_logout
- Palo Alto Session

For all features of PAN Static Address Groups to work, you'll need these templates:

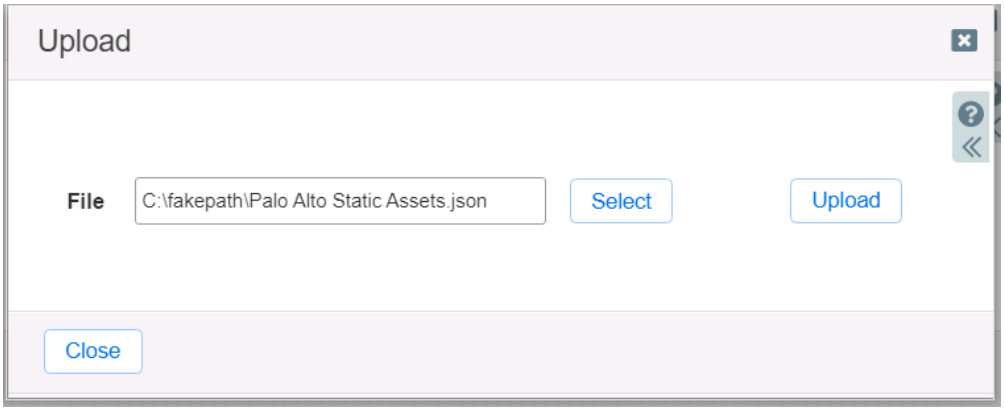
- Palo Alto Static Assets
- Palo Alto Static Security
- PaloAlto_login
- PaloAlto_logout
- Palo Alto Session

You can use one or both types of Address Groups simultaneously.

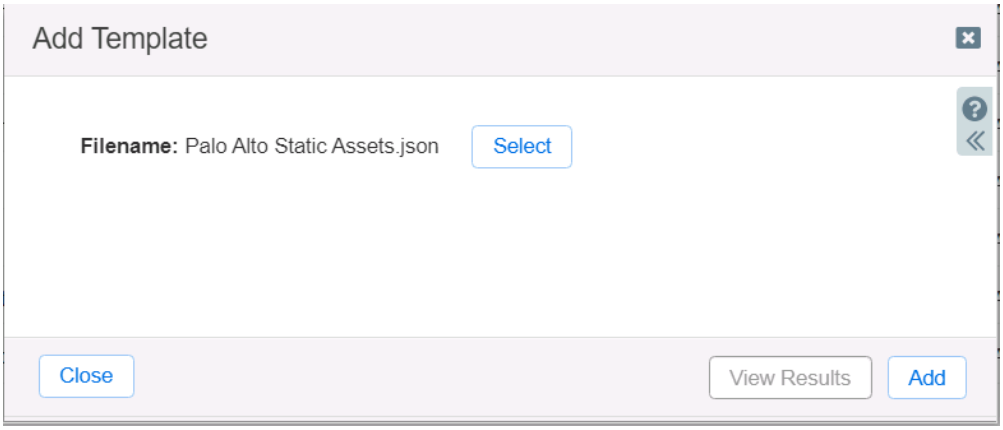
1. Navigate to **Grid** → **Ecosystem** → **Templates**. Click **Add Template** in the Toolbar or the **Add** button.
2. In the Add Template window that appears, click **Select**.



3. Click **Select** again in the Upload window that appears and browse for the template file you wish to add (.json or .txt). Click **Upload**.



4. Click **Add** again in the Add Template window.



5. Repeat steps 1-4 for all other desired templates.

Modify Templates

NIOS provides the ability to modify the templates via the web interface. 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. Copy the text into a text editor of your choice for major editing. NOTE: You cannot delete a template if it is used by an endpoint or by a notification.

1. Navigate to **Grid** → **Ecosystem** → **Templates**. Click the  hamburger button next to the name of the template you wish to modify then click **Edit**, or select it and click the  **edit** button.

2. Edit the template as you wish.

Add a Rest API Endpoint

A REST API Endpoint is a remote system which receives 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 (ex. for testing purposes).

In this integration, the PAN Firewall is the endpoint. Let's add the endpoint.

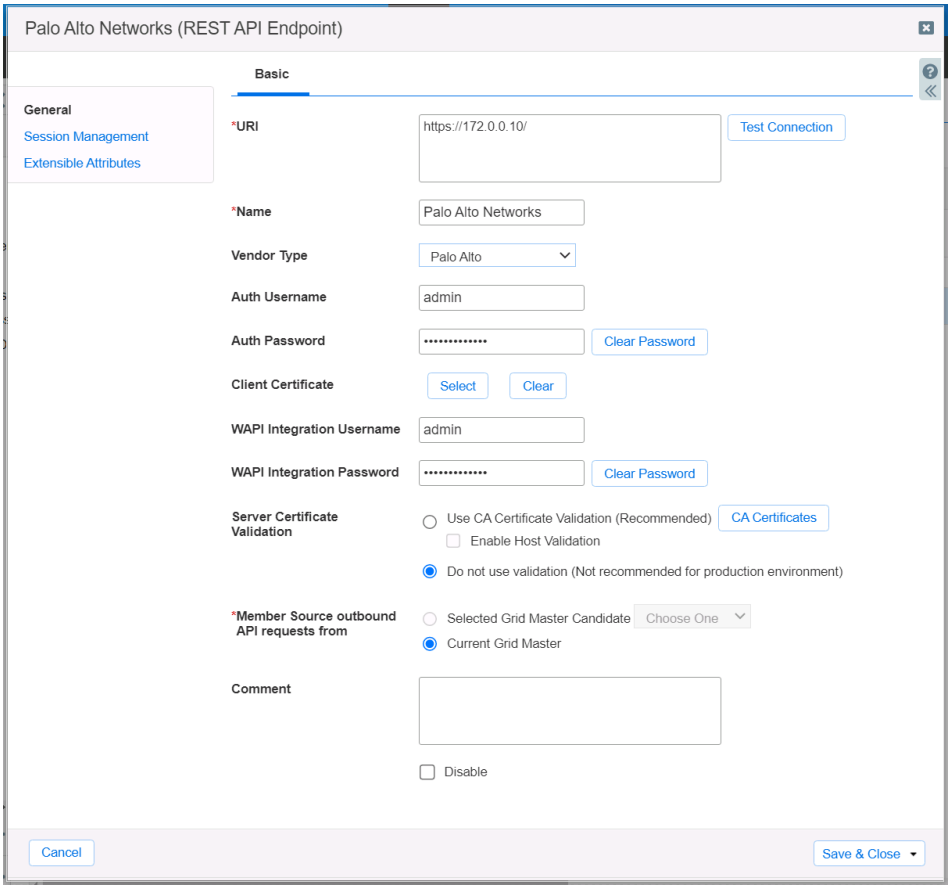
1. Navigate to **Grid** → **Ecosystem** → **Outbound Endpoint**. Click the  **Add** button and select Add REST API Endpoint.

2. Fill in all the fields as required.

NOTE: The Auth Username and Auth Password are the credentials of the PAN Firewall. The WAPI Integration Username and WAPI Integration Password are the credentials of your NIOS grid.

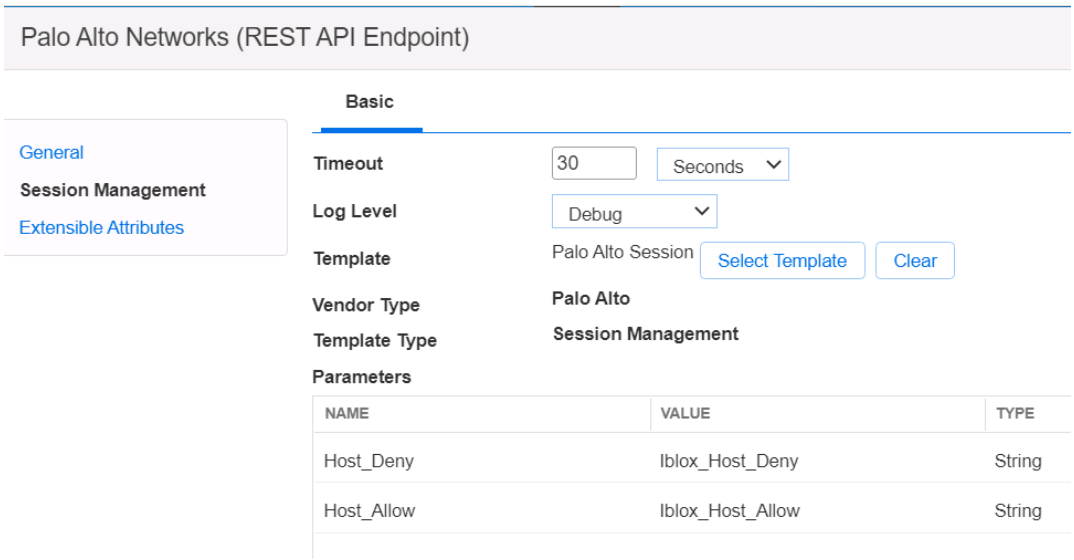
3. Click **Test Connection**.

NOTE: This only checks TCP communication with the URI. It does not verify authentication.



NOTE: It is recommended to send notifications from a Grid Master Candidate if there is one available instead of Grid Master.

4. Under the Session Management tab, set the Log Level to Debug for debug purposes during initial configuration.



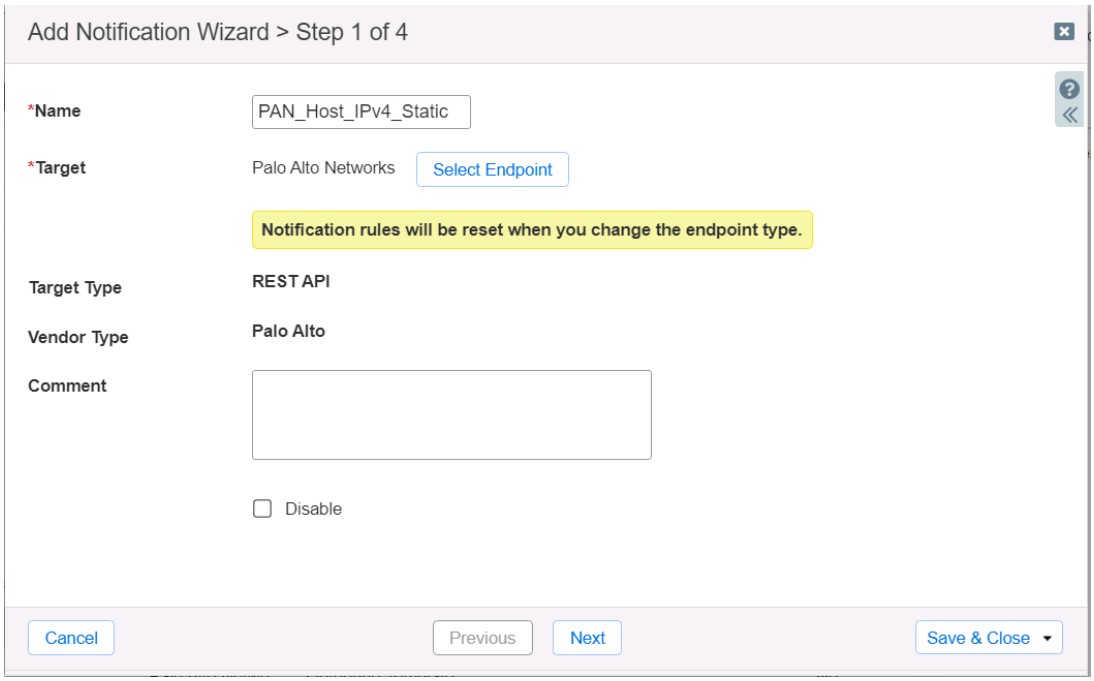
Add Notifications

A notification is a link between a template, an endpoint, and an event. In the notification you define the event which triggers the notification, executed template, and the API endpoint of which the Grid will establish a connection. To simplify deployment, create only required notifications and use relevant filters. It is highly recommended to configure deduplication for RPZ events and exclude a feed automatically populated by Threat Analytics. NOTE: when using Test Rule, rules for that notification apply.

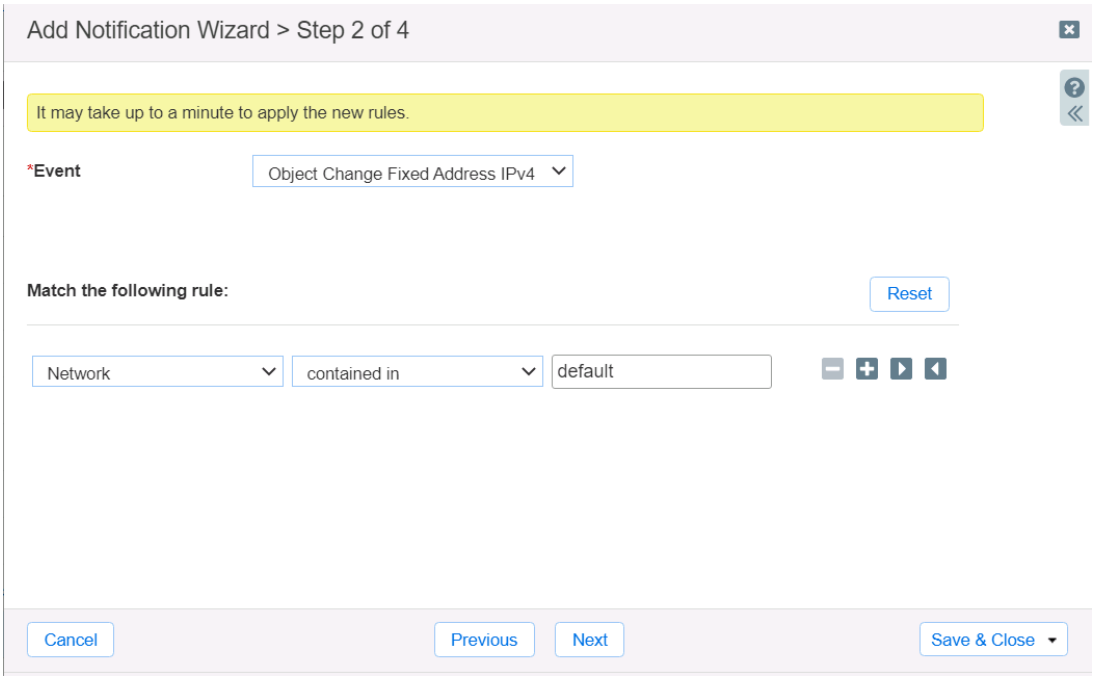
An endpoint and a template must be added before you can add a notification. Let's add a notification.

1. Navigate to **Grid** → **Ecosystem** → **Notification**. Click **Add** Notification Rule in the Toolbar or the **Add** button.

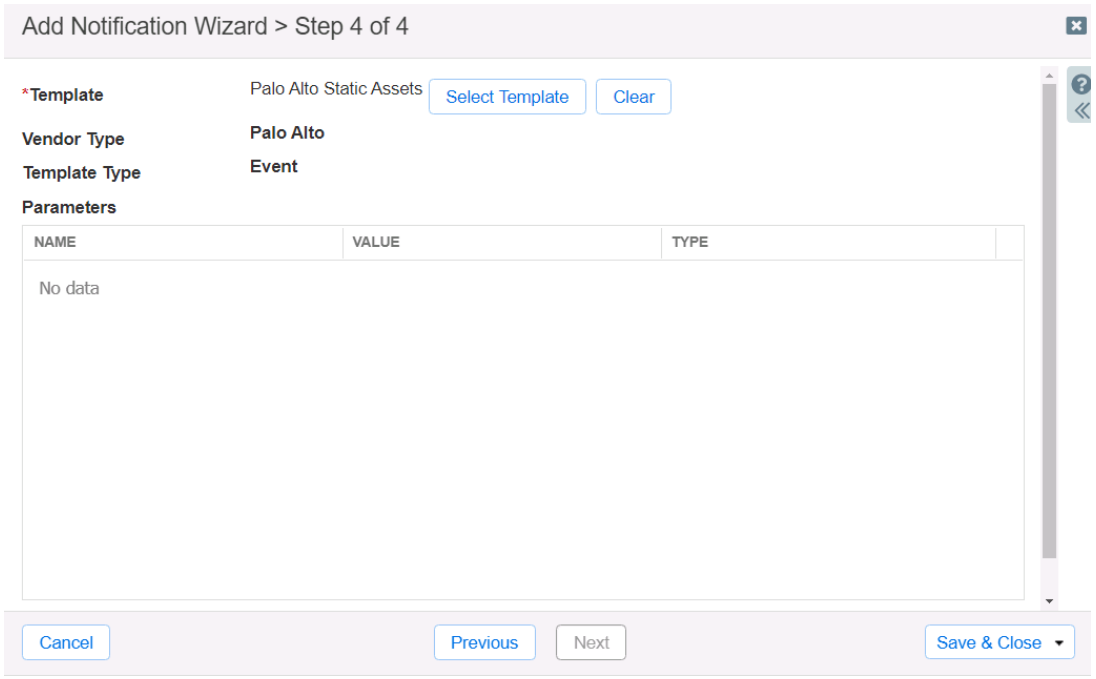
2. Enter a Name and select the Target Endpoint. *You cannot change the name later*. Click **Next**.



3. Select the Event and define rules that will trigger the Outbound API template to execute. Rules act as a filter in which only when they are satisfied will the template execute. You can choose to match all rules or any of multiple. Click **Next**. NOTE: For optimal performance, it is best practice to make the rule filter as narrow as possible.



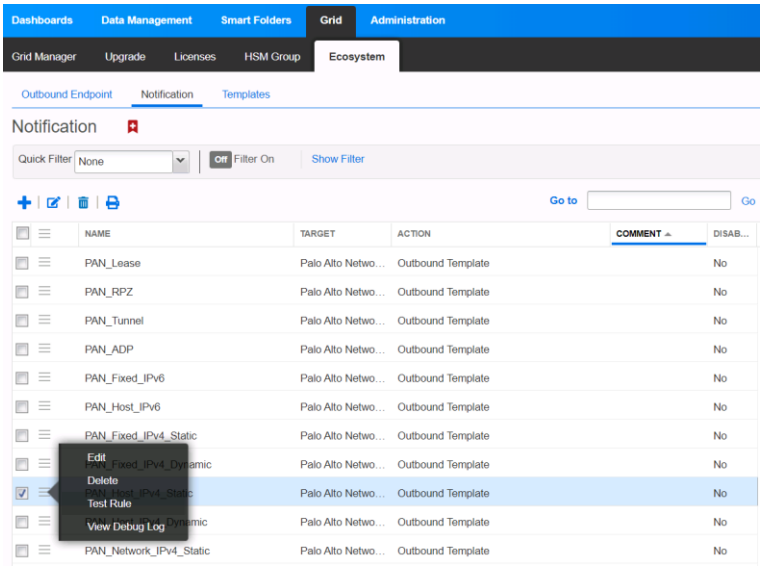
4. Select Enable event deduplication if desired and applicable. Click **Next**.
5. Select the desired/applicable template to execute. Click **Save & Close**.



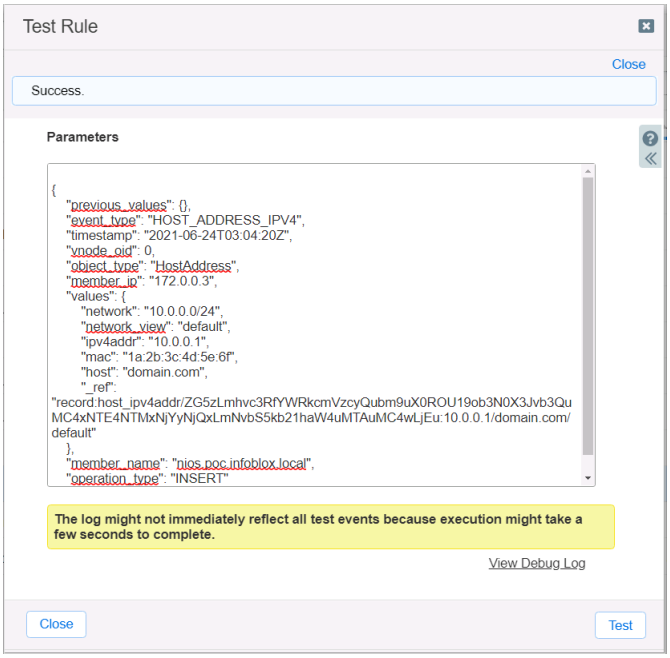
Validate Configuration

NIOS provides the ability to simulate an event for which a notification was created for. Let's test a notification.

1. Navigate to **Grid** → **Ecosystem** → **Notification**. Click the ☰ hamburger button next to the name of the notification you wish to verify then click Test Rule.



2. Modify test parameters as desired. Click **Test**. Click **View Debug Log** to view the debug log and verify the event was successful. NOTE: You may not see the event reflect in PAN if the appropriate parameters are not set, such as the EAs. Test with a real event to fully validate the whole configuration.



Appendix

Alternatively curl commands can be used to create Palo Alto objects.

Dynamic Address Groups commands

1. Command to register tag to an IP:

```
curl -k https://[firewall]/api/?key=[key]&type=user-id&cmd=<uid-
message><version>2.0</version><type>update</type><payload><register><entry
ip="[addressIP]"><tag><member>[tag]</member></tag></entry></register></payloa
d></uid-message>
```

For example:

```
https://172.0.0.10/api/?key=xxxxx&type=user-id&cmd=<uid-
message><version>2.0</version><type>update</type><payload><register><entry
ip="10.0.0.1"><tag><member>allow</member></tag></entry></register></payload><
/uid-message>
```

2. Command to unregister tag from an IP:

```
curl -k https://[firewall]/api/?key=[key]&type=user-id&cmd=<uid-
message><version>2.0</version><type>update</type><payload><unregister><entry
ip="[IP-
address]"><tag><member>[tag]</member></tag></entry></unregister></payload></u
id-message>
```

Static Address Groups commands

1. Command to add address to list of addresses:

```
curl -k
https://[firewall]/api/?key=[key]&type=config&action=set&xpath=/config/shared
/address/entry[@name='[address name']&element=<ip-netmask>[addressIP]</ip-
netmask>
```

For example:

```
https://172.0.0.10/api/?key=xxxxx&type=config&action=set&xpath=/config/shared
/address/entry[@name='10.0.0.0']& element=<ip-netmask>10.0.0.0</ip-netmask>
```

2. Commands to add address to static address group:

```
curl -k
https://[firewall]/api/?key=[key]&action=set&xpath=/config/shared/address-
group/entry[@name='[address group
name’]&element=<static><member>[addressIP]</member></static>
```

```
curl -k
https://172.0.0.10/api/?key=xxxxx&action=set&xpath=/config/shared/address-
group/entry[@name='IBlox_Host_Allow’]&element=<static><member>10.0.0.0
</member></static>
```

3. Commit to firewall:

```
curl -k
https://[firewall]/api/?key=[key]&type=commit&cmd=<commit><force></force></co
mmit>
```

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