

DEPLOYMENT GUIDE

Infoblox NIOS Integration with Palo Alto Networks Firewall using the Outbound REST API

NIOS version 8.2 | May 2018

Contents

- INTRODUCTION..... 3
- PREREQUISITES 3
- KNOWN LIMITATION..... 3
- BEST PRACTICE 3
- WORKFLOW 3
- TEMPLATES ON THE INFOBLOX COMMUNITY WEB-SITE 4
- EXTENSIBLE ATTRIBUTES 4
- SESSION VARIABLES 4
- SUPPORTED NOTIFICATION..... 5
- PALO ALTO FIREWALL CONFIGURATION..... 5
- INFOBLOX NIOS CONFIGURATION..... 9
 - CHECK IF THE SECURITY ECOSYSTEM LICENSE IS INSTALLED 9
 - ADD/UPLOAD TEMPLATES 10
 - MODIFYING TEMPLATES 10
 - ADDING HOST_ALLOW AND HOST_DENY..... 11
 - ADD A REST API ENDPOINT 11
 - ADD A NOTIFICATION 12
 - VALIDATE CONFIGURATION 14
- APPENDIX 15
- REFERENCES 15

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 8.2 or higher.
 2. Security Ecosystem License.
 3. Outbound API integration templates.
 4. Prerequisites for the templates (e.g. configured and set extensible attributes).
 5. Pre-configured required services: DNS, DHCP, RPZ, Threat Analytics.
 6. NIOS API user with the following permissions (access via API only):
 - AllHost – RW.
 - All IPv4 DHCP Fixed Addresses/Reservations – RW.
 - All IPv4 Networks – RW.
- Palo Alto Firewall:
 1. Installed and configured Palo Alto firewall.
 2. User credentials for the Palo Alto firewall (user requires access to Address and Address group objects).

Known Limitation

The current templates support DNS Firewall(RPZ), Threat Insight (DNS Tunneling), Host IPv4, Fixed address IPv4 and IPv4 Lease events only. Any additional templates created later will be added to the community site.

Best Practice

Outbound API templates are available on the Infoblox community site. After registering an account, (<https://community.infoblox.com>) you can subscribe to the relevant groups and forums. 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 NIOS Administration guide about other best practices, limitations and any detailed information on how to develop notification templates.

Workflow

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

- Install the Security Ecosystem license if not already installed.
- Check that necessary services DHCP, DNS, RPZ, Threat Analytics are configured.
- Create Extensible Attributes.

- Create or download from the Infoblox community web-site session (PaloAlto_Session.json), login (PaloAlto_Login.json) and logout (PaloAlto_Logout.json)
- Add/upload login,logout and the session template.
- Create or download from the Infoblox community web-site the notification templates (PaloAlto_Assets.json, PaloAlto_Security.json).
- Add/upload the notification templates.
- Add a REST API Endpoint.
- Add Notifications.
- Emulate an event, then check the debug log and/or verify changes on the REST API Endpoint.

Templates on the Infoblox community web-site

Outbound API notifications template is 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 guide. Infoblox does not distribute any templates with the NIOS releases (out-of-box). Templates are available on the Infoblox community web site. Templates may require additional extensible attributes to be created, parameters or WAPI credentials defined. The required configuration should be provided with a template. Do not forget to apply changes required by the template before testing a notification.

Extensible Attributes

Name	Description	Type
PaloAlto_Asset_Sync	Serves as toggle to turn on/off sync for Asset events. Enable "Inheritance" in the setup wizard and the external attribute can be inherited from the network settings. Default value can be set true.	List (true,false)
PaloAlto_Security_Sync	Serves as toggle to turn on/off sync for Security events. Enable "Inheritance" in the setup wizard and the external attribute from the network level is inherited and used. Default value can be set true.	List (true,false)
PaloAlto_Security_SyncedAt	Updated with timestamp on a security event. This attribute is created on the specific IP by the WAPI call when not present.	String
PaloAlto_Asset_SyncedAt	Updated with timestamp on an asset event. This attribute is created on the specific IP by the WAPI call when not present.	String

Session variables

Name	Description
PaloAlto_Host_Allow	The 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 (eg: lbox_Host_Allow).

PaloAlto_Host_Deny	The 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 (eg: Iblox_Host_Deny).
--------------------	--

Supported Notification

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 triggers for the notification, the template to execute and the external endpoint. The Palo Alto templates support a subset of available notifications (refer to the limitations chapter in this guide for more details). In order to simplify the deployment, 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.

Notification	Description
DNS RPZ	DNS queries that are Malicious or unwanted.
DNS Tunneling	Data exfiltration that occurs on the network.
Object Change Fixed Address IPv4	Added/Deleted fixed/reserved IPv4 objects.
Object Change Host Address IPv4	Added/Deleted Host IPv4 object.
Lease	Lease events.

Palo Alto Firewall Configuration

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. In turn, an address group object requires at least one IP during creation. To handle this situation, it is suggested to create an address group object with a dummy IP.

1. Ensure that "Multi System Virtual Capability" is checked in Device → Setup → Management. In the General Settings window select the Gear Icon to edit the settings. This is required to create shared objects.

2. Use the Palo Alto credentials created as per the prerequisite section.

3. Navigate to Objects → Addresses and create a dummy address object to add to the address group. Check the “Shared” option.

4. Create the address group object containing the address object above by navigating to Objects → Address Groups. The default address group object name is set to Iblox_Host_Allow. Check the “Shared” option.

Name	Location	Members Count	Addresses	Tags
Iblox_Host_Allow	Shared	1	10.0.0.0	
Iblox_Host_Deny	Shared	1	10.0.0.0	
Test	vsys1	1	10.0.0.1	shared
Test2	vsys1	1	10.0.0.0	

5. Navigate to Policies → Security and create an appropriate policy with allow action for this group following the steps below.

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Name: Iblax_AllowHosts

Rule Type: universal (default)

Description:

Tags:

OK Cancel

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Any

Source Zone: Any

Source Address: Any

Negate

OK Cancel

6. Select the Address group created in the step 4.

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

any

Source Zone: any

Source Address: 10.60.192.13, Iblax_Host_Allow

Negate

OK Cancel

7. Set the action to Allow in the Actions tab of the window.

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Action Setting

Action: Allow

Send ICMP Unreachable

Profile Setting

Profile Type: None

Log Setting

Log at Session Start

Log at Session End

Log Forwarding: None

Other Settings

Schedule: None

QoS Marking: None

Disable Server Response Inspection

OK Cancel

8. Create the second address group object for the deny policy, the same dummy ip address as above can be reused here. Check the “Shared” option.

Address Group

Name: Iblox_Host_Deny

☒ Shared

Description:

Type: Static

Addresses:

- Address
- 10.0.0.0

Browse Add Delete

Tags:

OK Cancel

9. Create a second policy with a new name as shown in screenshot below.

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Name: Iblox_DenyHosts

Rule Type: universal (default)

Description:

Tags:

OK Cancel

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Source Zone: trust

Source Address: Any

Add Delete

Negate

OK Cancel

10. Select the second address group object, eg: Iblox_Host_Deny created in step 8.

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Destination Zone: any

Destination Address: Iblox_Host_Deny

Add Delete

Negate

OK Cancel

11. Set the action to Deny in the Actions tab of the window.

The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The 'Action Setting' section has 'Action' set to 'Deny' and 'Send ICMP Unreachable' unchecked. The 'Log Setting' section has 'Log at Session End' checked and 'Log Forwarding' set to 'None'. The 'Profile Setting' section has 'Profile Type' set to 'None'. The 'Other Settings' section has 'Schedule' and 'QoS Marking' set to 'None' and 'Disable Server Response Inspection' unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

12. Commit all the changes as below by selecting the commit button on the top right corner.

The screenshot shows the 'Commit' dialog box. It states: 'Doing a commit will overwrite the running configuration with the commit scope.' There are two radio buttons: 'Commit All Changes' (unselected) and 'Commit Changes Made By: (1) admin' (selected). Below is a table with columns 'Commit Scope', 'Location Type', and 'Include in Commit'. The table contains two rows: 'vsys1' with 'Virtual Systems' and 'Include in Commit' unchecked, and 'shared-object' with 'Virtual Systems' and 'Include in Commit' checked. At the bottom are buttons for 'Preview Changes', 'Change Summary', 'Validate Commit', and 'Commit'. A 'Group By Location Type' checkbox is also present.

13. Note the URL and the Address Objects of the Palo Alto firewall to use in the NIOS configurations.

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.

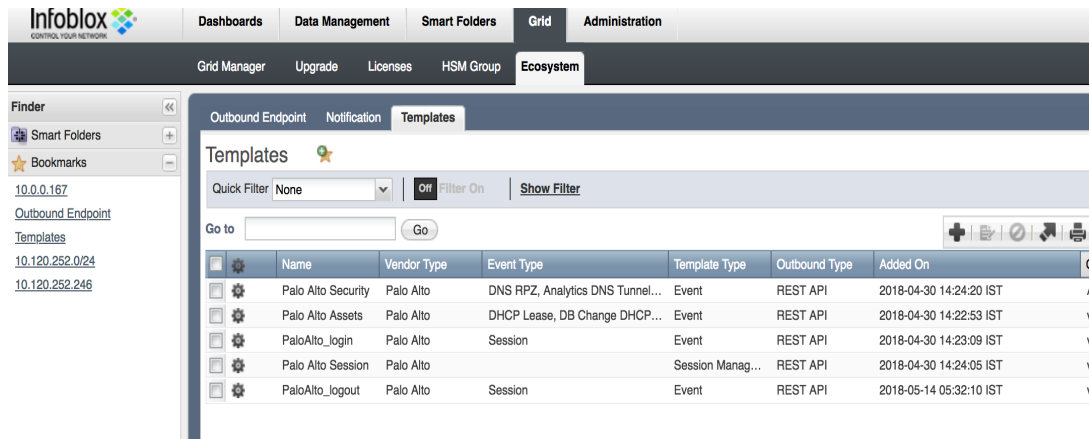
The screenshot shows the Infoblox NIOS interface. The top navigation bar includes 'Dashboards', 'Data Management', 'Smart Folders', 'Grid', and 'Administration'. The 'Grid' tab is selected, and the 'Licenses' sub-tab is active. The 'Licenses' section shows a table with columns: 'Feature', 'Limit Context', 'Limit Value', and 'Expiration'. The table contains two rows: 'RPZ' and 'Security Ecosystem'. Both have an expiration date of '2018-05-25 16:59:59 PDT (46 Days)' and '2018-05-20 16:59:59 PDT (41 Days)' respectively.

Feature	Limit Context	Limit Value	Expiration
RPZ			2018-05-25 16:59:59 PDT (46 Days)
Security Ecosystem			2018-05-20 16:59:59 PDT (41 Days)

In order to check if the license was installed go to **Grid → Licenses → Grid Wide**.

Add/Upload Templates

1. In order to upload/add templates go to **Grid** → **Ecosystem** → **Templates**, and press “+” or “+ Add Template” buttons.

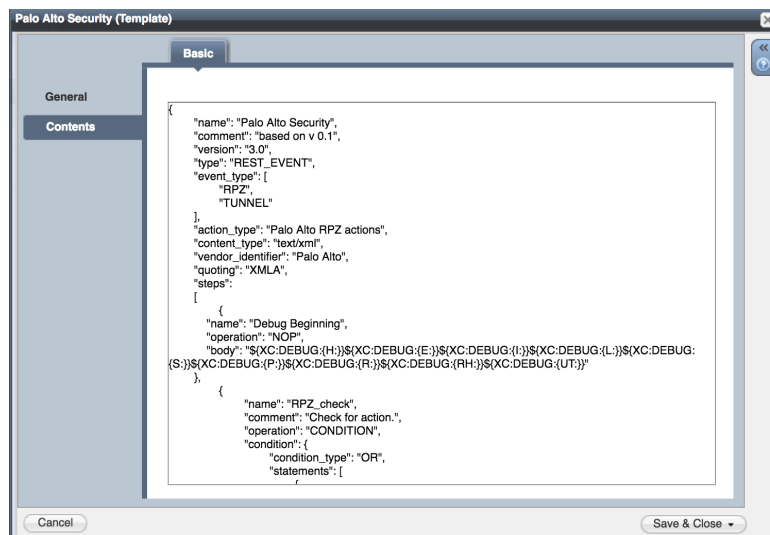


2. In the “Add template” window add the PA_login template followed by the other templates.
3. Press the “Select” button on the “Add template” window.
4. Press the “Select” button on the “Upload” window. The standard file selection dialog will be opened.
5. Select the file and press the “Upload” button on the “Upload” window.

Modifying Templates

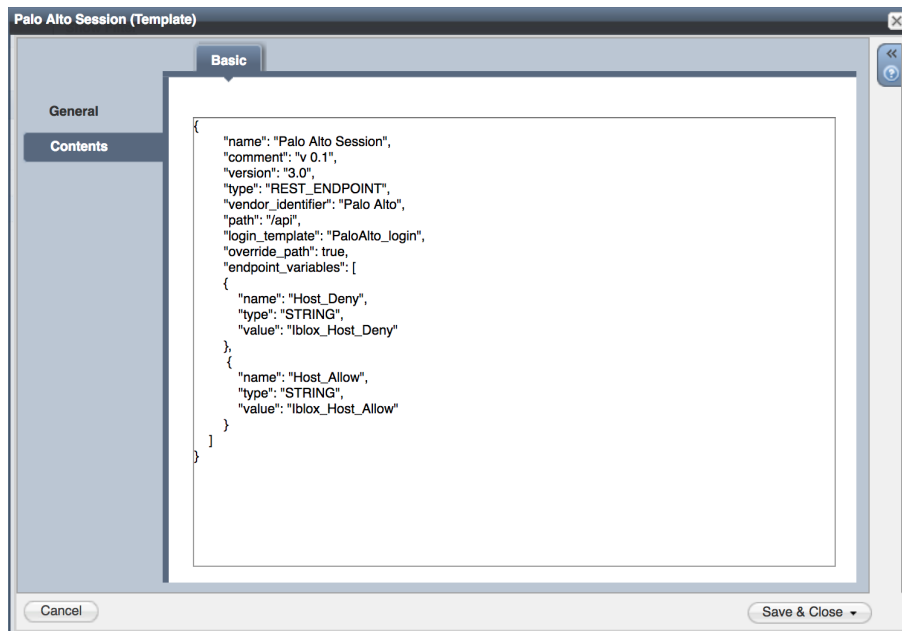
NIOS provides the facility to modify the templates via the web-interface.

1. Navigate to “Grid” → “Ecosystem” → “Templates”, and then press the gear icon next to the template you want to modify.
2. Press the “Edit” button to open up the “Template” window.
3. 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.**



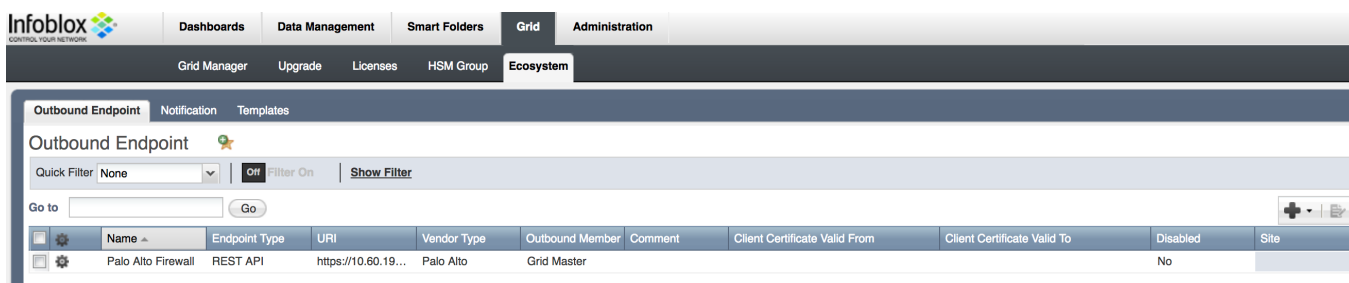
Adding Host_Allow and Host_Deny

1. Navigate to “Grid” → “Ecosystem” → “Templates” and then press the gear icon next to the “PaloAlto_Session.json” template and click edit to modify it.
2. Inside the “PaloAlto_Session.json” template insert the “Host_Allow”, key into the “value” field of the “endpoint_variables” with the value of the address object created in Palo Alto Configuration step.
3. Inside the “PaloAlto_Session.json” template insert the “Host_Deny”, key into the “value” field of the “endpoint_variables” with the value of the address object created in Palo Alto Configuration step.



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).



1. In order to add REST API Endpoints go to **Grid → Ecosystem → Outbound Endpoint** and press “+” or “++ **Add REST API Endpoint**” buttons.
2. The “Add REST API Endpoint Wizard” window will open. The URI and Name are the required fields. Enter the complete URI including http or https (eg: <https://10.5.6.12>).
3. Enter the credentials for the Rest API endpoint. The permissions required here is a user with shared access as mentioned in step 2 of the Palo Alto configuration.

- Specify “Auth Username”, “Auth Password” (Palo Alto Firewall credentials), “WAPI Integration Username” and “WAPI Integration Password” (NIOS credentials).
- Please be aware that “Test Connection” only checks communication (establish TCP connection with a remote system) with the URI. It does not check the authentication/authorization credentials.

The screenshot shows the 'Palo Alto Firewall (REST API Endpoint)' configuration window. The 'Basic' tab is selected. The 'URI' field contains 'https://192.60.192.115'. The 'Name' field contains 'Palo Alto Firewall'. The 'Vendor Type' is set to 'Palo Alto'. The 'Auth Username' is 'admin' and the 'Auth Password' is masked. The 'WAPI Integration Username' is 'admin' and the 'WAPI Integration Password' is masked. The 'Server Certificate Validation' section has three options: 'Use CA Certificate Validation (Recommended)' (selected), 'Enable Host Validation', and 'Do not use validation (Not recommended for production environment)'. The 'Member Source outbound API requests from' section has two options: 'Selected Grid Master Candidate' and 'Current Grid Master' (selected). The 'Comment' field is empty. The 'Test Connection' button is located next to the URI field.

- For debug purposes (during initial configuration only) set Log Level to “Debug”.
- It is recommended to send notifications from a Grid Master Candidate if there is one available instead of Grid Master.

Add a Notification

A notification is a link between a template, an endpoint, and an event. In the notification you define the event which triggers the notification, the template which is executed and the API endpoint unto which the Grid will establish a connection. The Palo Alto templates support all available notifications. In order to simplify the 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.

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

- Navigate to “Grid → Ecosystem → Notification” and press “+” or “+ Add Notification Rule” then the “Add Notification Wizard” window will open.

The screenshot shows the Infoblox NIOS interface. The 'Grid' tab is selected, and the 'Ecosystem' sub-tab is active. The 'Notification' tab is selected, showing a list of notifications. The table has columns for Name, Target, Action, Comment, and Disabled. The notifications listed are:

Name	Target	Action	Comment	Disabled
PaloAlto_Host_Ipv4	Palo Alto Firewall	Outbound Temp...		No
PaloAlto_Host_IPv6	Palo Alto Firewall	Outbound Temp...		No
PaloAlto_Lease	Palo Alto Firewall	Outbound Temp...		No
PaloAlto_RPZ	Palo Alto Firewall	Outbound Temp...		No
PaloAlto_Fixed_Ipv4	Palo Alto Firewall	Outbound Temp...		No
PaloAlto_Security_Tunnel	Palo Alto Firewall	Outbound Temp...		No

- Enter a name to identify the notification type and select the target endpoint.

PaloAlto_Host_Ipv4 (Notification)

Basic

Name: PaloAlto_Host_Ipv4

Target: Palo Alto Firewall Select Endpoint

Target Type: REST API

Vendor Type: Palo Alto

Comment:

☐ Disable

Notification rules will be reset when you change the endpoint type.

Cancel Save & Close

- Click **“Next”**, select an event type and define the rule. Note: For optimal performance, it is best practice to make the rule filter as narrow as possible.

PaloAlto_Host_Ipv4 (Notification)

Basic

It may take up to a minute to apply the new rules.

Event: Object Change Host Adc

Match the following rule:

Network View equals default

Reset

Cancel Save & Close

- Click **“Next”**. Select the relevant template and specify templates parameters if any.

Validate Configuration

You can now emulate an event for which a notification was added (click on a gear icon next to the notification and select “Test Rule”). E.g. create a host record or add a DHCP lease. If you have the debug log enabled, you can check for any problems or errors.

	Target	Action	Comment	Disabled
<input checked="" type="checkbox"/>	Palo Alto Firewall	Outbound Temp...		No
<input type="checkbox"/>	Palo Alto Firewall	Outbound Temp...		No
<input type="checkbox"/>	Palo Alto Firewall	Outbound Temp...		No
<input type="checkbox"/>	Palo Alto Firewall	Outbound Temp...		No
<input type="checkbox"/>	Palo Alto Firewall	Outbound Temp...		No
<input type="checkbox"/>	Palo Alto Firewall	Outbound Temp...		No

To check a debug log for an endpoint, go to **Grid→Ecosystem→Outbound Endpoints**, click on the gear icon and select “View Debug Log”. Depending on the browser the debug log will be downloaded or opened in a new tab, you may need to check your popup blocker settings.

Appendix

Alternatively curl commands can be used to create the Palo Alto objects:

1. Command to create address object:

```
curl -k "https://<firewall-host>/api/?key=<add-key>&type=config&action=set&xpath=/config/shared/address/entry[@name='10.0.0.0']&element=<ip-netmask>10.0.0.0/32</ip-netmask>"
```

Replace <firewall-host> and <add-key> with appropriate values.

2. Commands to create the two address group objects:

```
curl -k "https://<firewall-host>/api/?key=<add-key>&action=set&xpath=/config/shared/addressgroup/entry[@name='Iblox_Host_Allow']&element=<static><member>10.0.0.0</member></static>"
```

```
curl -k "https://<firewall-host>/api/?key=<add-key>&action=set&xpath=/config/shared/addressgroup/entry[@name='Iblox_Host_Deny']&element=<static><member>10.0.0.0</member></static>"
```

3. Commit the changes:

```
curl -k "https://<firewall-host>/api/?key=<add-key>&type=commit&cmd=<commit><partial><shared-object></shared-object></partial></commit>"
```

References

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/technical-documentation/81/pan-os/pan-os-admin/pan-os-admin.pdf