How to Modify AWS CloudFormation Templates to Retrieve the PAR File from a Control Center

If you are using the NextGen Control Center, you can modify your firewall's AWS CloudFormation template to retrieve the PAR file for the new F-Series Firewall Instance from the Control Center. The script authenticates either with CC admin credentials or a shared secret. Licenses that are already installed on PAYG firewall Instances are pushed to the Control Center before retrieving the PAR file. Firewalls using the BYOL images use the licenses configured on the Control Center.

getpar command line parameters usage

- **-a|--address <address>** – Control Center IP address.
- **-u|--username <username>** – CC admin user used to connect to the Control Center
- **-c|--cluster <cluster>** – Cluster name
- **-r|--range <range>** – Range number
- **-b|--boxname <boxname>** – Firewall name.
- **-d|--destination <dest>** – Destination directory and filename for the par file. E.g., /opt/phion/update/box.par
- **-s|-spoe** – Use Single Point of Entry to connect to the Control Center.
- **-l|--pushlic auto|always|never** – Configures if the licenses should be pushed to the Control Center before retrieving the PAR file.

Before you begin

- Create an AWS CloudFormation template to deploy your F-Series Firewall.

Step 1. Create the firewall configuration in the Control Center

Create the F-Series Firewall configuration in the Control Center.

For more information, see How to Add a new F-Series Firewall to the Control Center.

Step 2. Configure the authentication

The newly deployed firewall can authenticate either through a CC Admin account or with a shared key. The shared key is defined on a per-firewall level.

CC Admin Authentication

Create a CC admin and assign it an Administrative role with the following permissions:

- **CC Configuration Permission** – Click the **Get PAR File** check box.

For more information, see Control Center Admins and How to Configure Administrative Roles.

Shared Key Authentication

1. Log in to the Control Center.
2. Go to ***your firewall* > Box Properties.**
3. In the left menu, click **Operational**.
4. In the left menu, expand **Configuration Mode** and click **Switch to Advanced View**.
5. Click **Lock**.
6. Enter the **PAR File Retrieval Shared Key**.
7. Click **Send Changes** and **Activate**.

Step 3. Add the parameters to the template

You must add the parameters you need to the **Parameters** section of the template.

1. Add the following mandatory parameters to the **parameter** section of the template:
   - **CCIPAddress** – The IP address of your Control Center if it is directly reachable, or the IP address of the border firewall forwarding the traffic to the Control Center.
   - **Range** – The range number.
   - **Cluster** – The cluster name.
   - **FirewallName** – The name of the Firewall.
2. Add the authentication parameters:
   Control Center Admin:
   - **CCUser** – The CC admin.
   - **CCPassword** – The password for the CC admin.

   Shared Key Authentication:
   - **CCSharedKey** – The shared key used to authenticate to the Control Center.

Click here to see the parameter definitions for shared key authentication...

Shared parameters

```
"CCIPAddress": { "Description": "IP Address or hostname of the Control Center",
"Type": "String", "Default": "127.0.0.1" }, "Cluster": { "Description": "Case
sensitive Control Center cluster name", "Type": "String" }, "Range": {
"Description": "Control Center range number", "Type": "String" }, "FirewallName": {
"Description": "Case sensitive name of the Firewall on the Control Center", "Type":
"String" }
```

Additional required parameters for Control Center authentication:

```
"CCUser": { "Description": "CC admin username", "Type": "String", "Default": "" },
"CCPassword": { "Description": "CC admin user password", "Type": "String",
"Default": "", "NoEcho": "true" },
```

Additional required parameters for shared key authentication:

```
"CCSharedKey": { "Description": "shared key to retrieve PAR file", "Type": "String",
"Default": "", "NoEcho": "true" },
```

Step 2. Modify the template to retrieve the PAR file

Add a script to the userData element of the template. Use the parameters defined above.

1. Locate the **Gateway** section.
2. Add the getparfile script to the **UserData** parameter with the desired authentication method:
   Control Center Admin:

```
"Gateway": { "Type": "AWS::EC2::Instance", "Properties": { "ImageId": "ami-
XXXXXXXX", "InstanceType": { "Ref": "InstanceType" }, "KeyName": { "Ref":
"KeyName" }, "SecurityGroups" : [{ "Ref" : "NGSecurityGroup" }], "UserData": {
"Fn::Base64": { "Fn::Join": [ "", [ "#!/bin/bash\n\n", "echo \"userdata\" >>
/tmp/userdata.txt\n", "/opt/aws/bin/cfn-init -v --region ", { "Ref":
"AWS::Region" }, " -s ", { "Ref": "AWS::StackName" }, " -r ", "Gateway\n",
"/opt/aws/bin/cfn-hup-config -r", { "Ref": "AWS::Region" }, " -s ", { "Ref":
```

```
"AWS::StackName" }, "\n" ] ] } } }, "Metadata": { "AWS::CloudFormation::Init":
{ "configSets": { "default": [ "getparfile" ] }, "getparfile": { "files": {
"/etc/cfn/hooks.d/test.conf": { "content": { "Fn::Join": [ "", [
"[testhook]\n", "triggers=post.add\n", "path=Resources.Gateway\n",
"action=\"echo blabla > /tmp/hook.log\"\n", "runas=root" ]]}, "mode": "000644",
"owner": "root", "group": "root" } }, "commands": { "retrievepar": { "command":
{ "Fn::Join": ["", [ "echo \"", { "Ref": "CCPassword" }, "\" |
/opt/phion/bin/getpar -a ", { "Ref": "CCIPAddress" }, " -u ", { "Ref": "CCUser"
}, " -c ", { "Ref": "Cluster" }, " -r ", { "Ref": "Range" }, " -b ", { "Ref":
"FirewallName" }, " -d /opt/phion/update/box.par -s", " --verbosity 10 ", " >>
/tmp/getpar.log" ]] } } } } } } }
```

Shared key authentication:

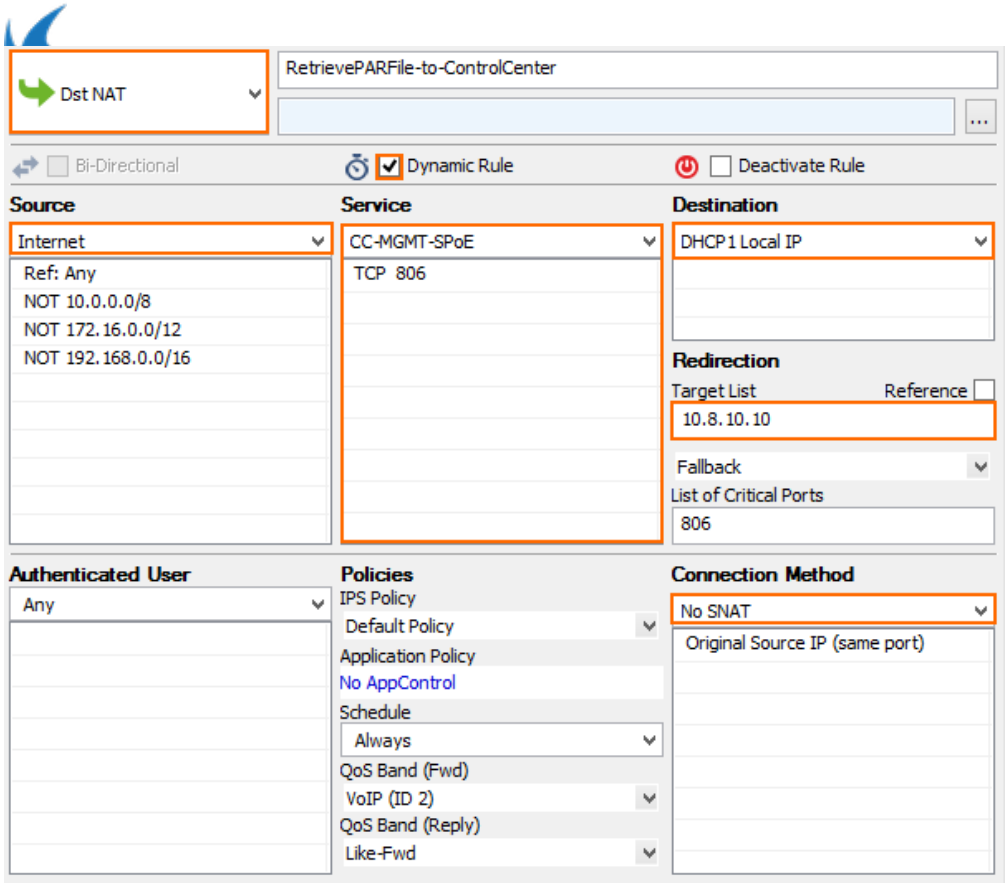
```
"Gateway": { "Type": "AWS::EC2::Instance", "Properties": { "ImageId": "ami-
XXXXXXXX", "InstanceType": { "Ref": "InstanceType" }, "KeyName": { "Ref":
"KeyName" }, "SecurityGroups" : [{ "Ref" : "NGSecurityGroup" }], "UserData": {
"Fn::Base64": { "Fn::Join": [ "", [ "#!/bin/bash\n\n", "echo \"userdata\" >>
/tmp/userdata.txt\n", "/opt/aws/bin/cfn-init -v --region ", { "Ref":
"AWS::Region" }, " -s ", { "Ref": "AWS::StackName" }, " -r ", "Gateway\n",
"/opt/aws/bin/cfn-hup-config -r", { "Ref": "AWS::Region" }, " -s ", { "Ref":
"AWS::StackName" }, "\n" ] ] } } }, "Metadata": { "AWS::CloudFormation::Init":
{ "configSets": { "default": [ "getparfile" ] }, "getparfile": { "files": {
"/etc/cfn/hooks.d/test.conf": { "content": { "Fn::Join": [ "", [
"[testhook]\n", "triggers=post.add\n", "path=Resources.Gateway\n",
"action=\"echo blabla > /tmp/hook.log\"\n", "runas=root" ]]}, "mode": "000644",
"owner": "root", "group": "root" } }, "commands": { "retrievepar": { "command":
{ "Fn::Join": ["", [ "echo \"", { "Ref": "CCSharedKey" }, "\" |
/opt/phion/bin/getpar -a ", { "Ref": "CCIPAddress" }, " -c ", { "Ref":
"Cluster" }, " -r ", { "Ref": "Range" }, " -b ", { "Ref": "FirewallName" }, " -
d /opt/phion/update/box.par -s", " --verbosity 10 ", " >> /tmp/getpar.log" ]] }
} } } } } }
```

3. Save the template.

Step 5. (optional) Allow access to the Control Center

If the firewall VM cannot directly reach the Control Center, you must create a dynamic access rule on the border firewall. Using dynamic rules allows you to enable access only when deploying a new firewall. If SPoE is used, you must open port TCP 806.

- **Action** – Select **Dst NAT**.
- **Source** – If known, enter the public IP address of the Firewall, or select **Internet**.
- **Service** – Create and select a service object for TCP 806. For more information, see Service Objects.
- **Destination** – Enter the **Point of Entry** IP address of the border firewall.
- **Redirect to** – Enter the IP address of the Control Center.
- **Connection Method** – Select **No SNAT**.



Next steps

Deploy the firewall via the AWS CloudFormation template.

Figures