

Cloud NGFW for Azure Azure CLI

From On-Prem to Azure, Seamlessly Secure.

Palo Alto Networks Software Firewalls

Anton Budilovskiy - Senior Technical Marketing Engineer

Cloud NGFW for Azure - Azure CLI

- Cloud NGFW and Local Rulestack resource can be created and managed using Azure CLI [palo-alto-networks](#) extension for the Azure CLI (version 2.51.0 or higher).

Microsoft | Learn [Documentation](#) [Training](#) [Credentials](#) [Q&A](#) [Code Samples](#) [Assessments](#) [Shows](#) [Sign in](#)

Azure [Product documentation](#) [Architecture](#) [Learn Azure](#) [Develop](#) [Troubleshooting](#) [Resources](#) [Portal](#) [Free account](#)

Version: [Azure CLI \(Latest\)](#)

[Filter by title](#)

- ▼ Palo Alto Networks
 - Summary
 - ▼ palo-alto
 - Summary**
 - ▼ cloudngfw
 - Summary
 - > firewall
 - > local-rulestack

[Learn / Azure / Azure CLI / Reference / Palo Alto Networks /](#)

az palo-alto

Reference [Feedback](#)

Note

This reference is part of the **palo-alto-networks** extension for the Azure CLI (version 2.51.0 or higher). The extension will automatically install the first time you run an **az palo-alto** command. [Learn more about extensions.](#)

Manage palo-alto networks resource.

Cloud NGFW for Azure - Azure CLI

- Install by running any palo-alto commands:

```
azureuser@test-cli-vm:~$ az palo-alto cloudngfw list
'palo-alto' is misspelled or not recognized by the system.
```

Examples from AI knowledge base:

https://aka.ms/cli_ref

Read more about the command in reference docs

```
azureuser@test-cli-vm:~$ az palo-alto cloudngfw firewall list
```

```
The command requires the extension palo-alto-networks. Do you want to install it now? The command
will continue to run after the extension is installed. (Y/n):
```

or install explicitly:

```
az extension add --name palo-alto-networks
```

Local Rulestack

Cloud NGFW for Azure - Azure CLI - Create Rulestack

```
az palo-alto cloudngfw local-rulestack create -g <rg-name> -n <lrs-name> --identity  
"{type:None}" --location <region> --default-mode IPS --description "Local Rulestack"  
--min-app-id-version "8595-7473" --scope "LOCAL" --security-services  
"{vulnerability-profile:BestPractice,anti-spyware-profile:BestPractice,anti-virus-profile:Bes  
tPractice,url-filtering-profile:BestPractice,file-blocking-profile:BestPractice,dns-subscript  
ion:BestPractice}"
```

Cloud NGFW for Azure - Azure CLI - Delete Rulestack

```
az palo-alto cloudngfw local-rulestack delete -g <rg-name> -n <lrs-name>
```

Cloud NGFW for Azure - Azure CLI - Create a Rule

```
az palo-alto cloudngfw local-rulestack local-rule create -g <rg>  
--local-rulestack-name <lrs-name> --rule-name <rule-name> --priority  
"<priority>" --destination "{cidrs:[<cidr>]}" --applications "<app-id-name>"  
--action-type "<action>" --enable-logging "ENABLED" --rule-state "ENABLED"
```

Actions: Allow, DenyResetBoth, DenyResetServer, DenySilent

Cloud NGFW for Azure - Azure CLI - Delete a Rule

```
az palo-alto cloudngfw local-rulestack local-  
rule delete --local-rulestack-name <lrs-name> --resource-group <rg-name>  
--priority "<priority>"
```


Cloud NGFW for Azure - Azure CLI - Deploy Rulestack

```
az palo-alto cloudngfw local-rulestack commit --resource-group <rg-name>  
--local-rulestack-name <lrs-name>
```

Cloud NGFW

Cloud NGFW for Azure - Azure CLI - Create Cloud NGFW

VNet + Local Rulestack policy management:

```
az palo-alto cloudngfw firewall create --name <cngfw-name> --resource-group <rg_name> --location <region> --dns-settings
"{enable-dns-proxy:DISABLED,enabled-dns-type:CUSTOM}" --marketplace-details
"{marketplace-subscription-status:Subscribed,offer-id:pan_swfw_cloud_ngfw,publisher-id:paloaltonetworks}" --plan-data
"{billing-cycle:MONTHLY,plan-id:panw-cloud-ngfw-payg,usage-type:PAYG}" --is-panorama-managed FALSE --associated-rulestack
"{location:<region>,resource-id:/subscriptions/<sub-id>/resourceGroups/<rg-name>/providers/PaloAltoNetworks.Cloudngfw/localRulestacks/
<lrs-name>}" --network-profile
"{network-type:VNET,public-ips:[{address <cngfw-pip>,resource-id:/subscriptions/<sub-id>/resourceGroups/<rg-name>/providers/Microsoft.N
etwork/publicIPAddresses/cngfw-public-ip}],enable-egress-nat:DISABLED,vnet-configuration:{ip-of-trust-subnet-for-udr:{address<private-
subnet-cidr>},trust-subnet:{resource-id:/subscriptions/<sub-id>/resourceGroups/<rg-name>/providers/Microsoft.Network/virtualNetworks/<h
ub-vnet-name>/subnets/<private-subnet-name>},un-trust-subnet:{resource-id:/subscriptions/<sub-id>/resourceGroups/<rg-name>/providers/Mi
crosoft.Network/virtualNetworks/<hub-vnet-name>/subnets/<public-subnet-name>},vnet:{resource-id:/subscriptions/<sub-id>/resourceGroups/
<rg-name>/providers/Microsoft.Network/virtualNetworks/<hub-vnet-clip>}}}" --no-wait
```

Cloud NGFW for Azure - Azure CLI - Create Cloud NGFW

VNet + Panorama policy management

```
az palo-alto cloudngfw firewall create --name <cnfgw-name> --resource-group <rg-name> --location <region> --dns-settings
"{enable-dns-proxy:DISABLED,enabled-dns-type:CUSTOM}" --marketplace-details
"{marketplace-subscription-status:Subscribed,offer-id:pan_swfw_cloud_ngfw,publisher-id:paloaltonetworks}" --plan-data
"{billing-cycle:MONTHLY,plan-id:panw-cloud-ngfw-payg,usage-type:PAYG}" --is-panorama-managed TRUE --panorama-config
"{config-string: <panorama-registration-string>}" --associated-rulestack
"{location: <region>, resource-id:/subscriptions/ <sub-id>/resourceGroups/ <rg-name>/providers/PaloAltoNetworks.Cloudngfw/localRulestacks/ <
lrs-name>}" --network-profile
"{network-type:VNET,public-ips:[{address: <cnfgw-pip>, resource-id:/subscriptions/ <sub-id>/resourceGroups/ <rg-name>/providers/Microsoft.N
etwork/publicIPAddresses/ <cnfgw-public-name>}],enable-egress-nat:DISABLED,vnet-configuration:{ip-of-trust-subnet-for-udr:{address: <priv
ate-subnet-cidr>},trust-subnet:{resource-id:/subscriptions/ <sub-id>/resourceGroups/ <rg-name>/providers/Microsoft.Network/virtualNetwork
s/ <hub-vnet-name>/subnets/ <private-subnet-name>},un-trust-subnet:{resource-id:/subscriptions/ <sub-id>/resourceGroups/ <rg-name>/provider
s/Microsoft.Network/virtualNetworks/ <hub-vnet-name>/subnets/ <public-subnet-name>},vnet:{resource-id:/subscriptions/ <sub-id>/resourceGro
ups/ <rg-name>/providers/Microsoft.Network/virtualNetworks/ <hub-vnet-name>}}}"
```

Cloud NGFW for Azure - Azure CLI - Create NVA object

Required for vWAN Hub Cloud NGFW deployment:

```
az network virtual-appliance create --name <cngfw-nva-name> --resource-group <rg-name>
--location <region> --vhub
/subscriptions/<sub-id>/resourceGroups/<rg-name>/providers/Microsoft.Network/virtualHubs/<hub
-name> --delegation "{service-name:PaloAltoNetworks.Cloudngfw/firewalls}"
```

Cloud NGFW for Azure - Azure CLI - Create Cloud NGFW

vWAN Hub + Local Rulestack :

```
az palo-alto cloudngfw firewall create --name<cngfw-name> --resource-group <rg-name> --location <region>
--dns-settings "{enable-dns-proxy:DISABLED,enabled-dns-type:CUSTOM}" --marketplace-details
"{marketplace-subscription-status:Subscribed,offer-id:pan_swfw_cloud_ngfw,publisher-id:paloaltonetworks}"
--plan-data "{billing-cycle:MONTHLY,plan-id:panw-cloud-ngfw-payg,usage-type:PAYG}" --is-panorama-managed FALSE
--associated-rulestack
"{location:<region>,resource-id:/subscriptions<sub-id>/resourceGroups/<rg-name>/providers/PaloAltoNetworks.Cloudn
gfw/localRulestacks/<lrs-name>}" --network-profile
"{network-type:VWAN,public-ips:[{address<cngfw-pip>,resource-id:/subscriptions<sub-id>/resourceGroups/<rg-name>/
providers/Microsoft.Network/publicIPAddresses/<cngfw-pip-name>}],vwan-configuration:{v-hub:{resource-id:/subscript
ions/<sub-id>/resourceGroups/<rg-name>/providers/Microsoft.Network/virtualHubs/<hub-name>,network-virtual-applianc
e-id:/subscriptions/<sub-id>/resourceGroups/<rg-name>/providers/Microsoft.Network/networkVirtualAppliances/<nva-na
me>},enable-egress-nat:DISABLED}" --no-wait
```

Cloud NGFW for Azure - Azure CLI - Create Cloud NGFW

vWAN Hub + Panorama :

```
az palo-alto cloudngfw firewall create --name <cngfw-name> --resource-group <rg-name> --location <region> --dns-settings
"{enable-dns-proxy:DISABLED,enabled-dns-type:CUSTOM}" --marketplace-details
"{marketplace-subscription-status:Subscribed,offer-id:pan_swfw_cloud_ngfw,publisher-id:paloaltonetworks}"
--network-profile
"{network-type:VWAN,vwan-configuration:{v-hub:{resource-id:/subscriptions/<sub-id>/resourceGroups/<rg-name>/providers/Mic
rosoft.Network/virtualHubs/<hub-name>},network-virtual-appliance-id:/subscriptions/<sub-id>/resourceGroups/<rg-name>/prov
iders/Microsoft.Network/networkVirtualAppliances/<nva-name>},
enable-egress-nat:DISABLED,public-ips:[{address:<cngfw-pip>,resource-id:/subscriptions/<sub-id>/resourceGroups/<rg-name>/
providers/Microsoft.Network/publicIPAddresses/<cngfw-pip-name>}]}" --plan-data
"{billing-cycle:MONTHLY,plan-id:panw-cloud-ngfw-payg,usage-type:PAYG}" --is-panorama-managed TRUE --panorama-config
"{config-string:<panorama-registration-string>}"
```

Cloud NGFW for Azure - Azure CLI - Delete Cloud NGFW

```
az palo-alto cloudngfw firewall delete --resource-group <rg-name> -n <cngfw-name>
```


Cloud NGFW for Azure - Azure CLI - Log Settings

Azure Rulestack policy management:

1. Create a LAW

```
az monitor log-analytics workspace create -g <rg-name> -n <law-name> --location <region>
```

2. Fetch "CustomerId" attribute which is then used as "workspace" attribute

```
az monitor log-analytics workspace show --name <law-name> --resource-group <rg-name> --query customerId | tr -d '"'
```

3. Fetch "primarySharedKey" and "secondarySharedKey" attributes

```
az monitor log-analytics workspace get-shared-keys --resource-group <rg-name> --workspace-name <law-name> --query "primarySharedKey" | tr -d '"'
```

```
az monitor log-analytics workspace get-shared-keys --resource-group <rg-name> --workspace-name <law-name> --query "secondarySharedKey" | tr -d '"'
```

4. Associate the LAW with the Cloud NGFW resource

```
az palo-alto cloudngfw firewall save-log-profile --log-option SAME_DESTINATION --log-type TRAFFIC --resource-group <rg-name> --common-destination
```

```
"{monitor-configurations:{id:/subscriptions/<sub-id>/resourceGroups/<rg-name>/providers/Microsoft.OperationalInsights/workspaces/<law-name>,workspace:<CustomerId>,primary-key:<primary-key>,secondary-key:<secondary-key>}}" --firewall-name <cngfw-name>
```

THANK YOU