Cloud NGFW on AWS

Deployment Guide

Version-2.0

Author- Nidhi Pandey

 ©2022 Palo Alto Networks, Inc

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support.html

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentaon@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.

www.paloaltonetworks.com

©2021–2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/ trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised December 13, 2021

Table of Contents

About This Guide **5**

Challenges **5**

Solution **5**

Licensing **6**

Cloud NGFW Configuration Options **9**

Subscribe to the NGFW service **16**
- Overview 16
- Subscribe to CloudNGFW 16
  - Create a Tenant 19

Cloud NGFW Concepts **27**
- Components 27
  - Roles and Permissions 27
  - Rulestack 30
    - Cloud NGFW Security Rule Object 31
    - How to configure Intelligent Feed 35
    - Configure Application Based Control (App-ID) 38
    - Configure Adv URL-Filtering 39
    - TLS Decryption 41
    - Security Profile 42
    - How to configure Rules 46
  - How to Create Cloud NGFW Endpoints 49

Logging **51**
- Configure Log Destination in AWS for Cloud NGFW 51

Use Cases **52**

Deployment Options **56**
- Deployment of Centralized Design with Cloud NGFW 56
- Reference Architecture 56
  - Step 1 - Create VPCs, Create Subnets, and Attach Internet Gateway. 57
  - Step 2 - Create Transit Gateway and Attachments. 60
  - Step 3 - Create Security Group, Instances and Allocate Elastic IP 63
  - Step 4 - Configure Cloud NGFW endpoint, Security RuleStack. 64

 ©2022 Palo Alto Networks, Inc

Step 5 - Configure Route Tables and Routes for VPCs and Transit Gateway 66
Step 6 - Configure Logging Settings 71
Validation 72
Traffic Flow for E-W traffic in Centralized Deployment . 74
Traffic Flow with Outbound Traffic with Centralized Design. 75
Distributed Deployment 76
Combined Model 81

Summary **82**

References **82**

 ©2022 Palo Alto Networks, Inc

About This Guide

Cloud NGFW is the industry's only machine learning (ML)-powered NGFW delivered as a cloud-native service on AWS. With Cloud NGFW you can run more apps securely at cloud speed and cloud scale with a true cloud-native experience. There is no trade-off between cloud agility and sophisticated, multi-layered security. You get to experience the best of both worlds with natively integrated network security delivered as a service on AWS.

This guide explains how to configure cloud NGFW in AWS, enabling the users to utilize the benefits of Palo Alto Networks next-generation firewall as a service. The sections in the document provide details about the architecture, and various components of this service. This document also provides guidance on how to set up and configure Cloud NGFW using a simplified configuration workflow.

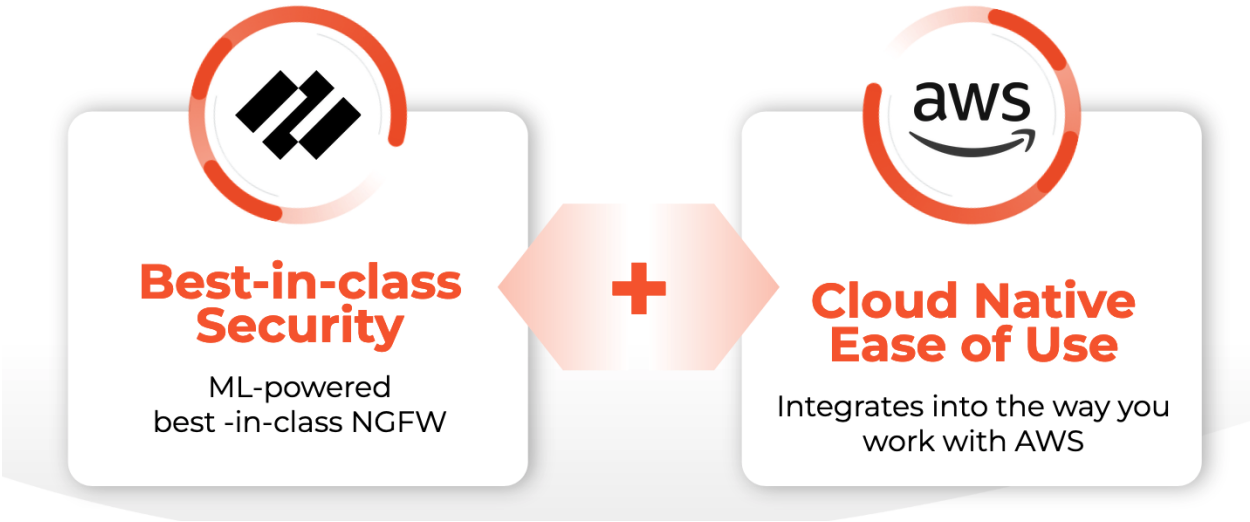
Challenges

Traditionally, NGFWs were deployed as hardware appliances that were within physical network architecture. And as organizations began moving to the cloud, NGFWs evolved. Today, software-based NGFWs protect just as well as their physical predecessors, and they automatically follow applications and workloads in a virtualized environment. For AWS environments, that means more advanced protection.
But as organizations grow their cloud footprint, NGFWs must evolve to maintain advanced, modern cybersecurity without hampering the speed and agility of the cloud. The factors like configuration and control can delay the implementation and slow down the business and cloud adoption.
Today's security teams want to know: How can they have the best of both worlds—NGFW protection and the ease of use of the cloud.

Solution

Cloud NGFW is delivered as a fully managed cloud native service by Palo alto networks. It simplifies the deployment of security control and utilizes the best-in-class security provided by the ML-powered NGFW. It is built on a set of principles to provide :

 ©2022 Palo Alto Networks, Inc



- **Simpler and easier configuration workflow** to provide network security faster with just a few clicks. The customer can focus on their security rules alone and avoid all other device configurations. The reduced configuration knobs provide an intuitive workflow for security professionals.
- **Operational simplicity** to automatically deliver scalability and resiliency like any other cloud service
- **Best-in-breed security** to provide industry-recognized advanced security capabilities provided by Palo Alto Networks.
- **Native AWS experience** to provide familiar controls with IAM, S3, Cloudwatch, Kinesis, etc. For monitoring, the AWS console will show metrics in AWS UI itself.

Note-*This document focuses on the configuration using the cloud NGFW console. It is assumed that the reader is familiar with Palo Alto Networks NGFW concept, AWS components, and architecture. Please refer to the References section for more information.*

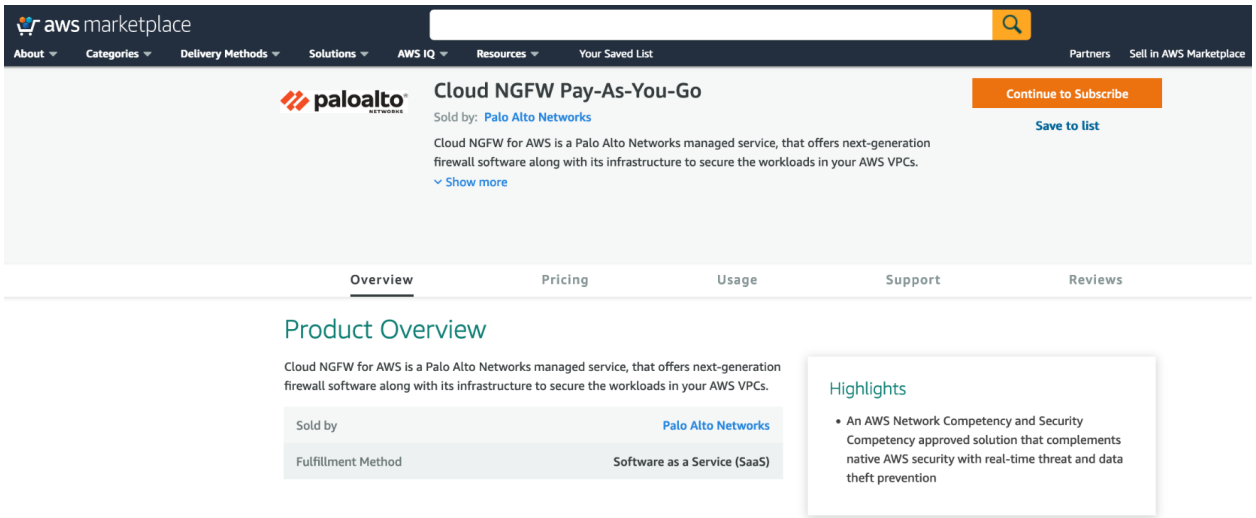
Licensing

Cloud NGFW is a service owned by PaloAlto Networks, available in the native cloud service provider portal. The pricing structure aligns with the cloud consumption model for network services.
Cloud NGFW consumption is based on a Pay As You Go (PAYG) basis. Once the user subscribes to the service, the charges will show up in their monthly AWS billing statements.

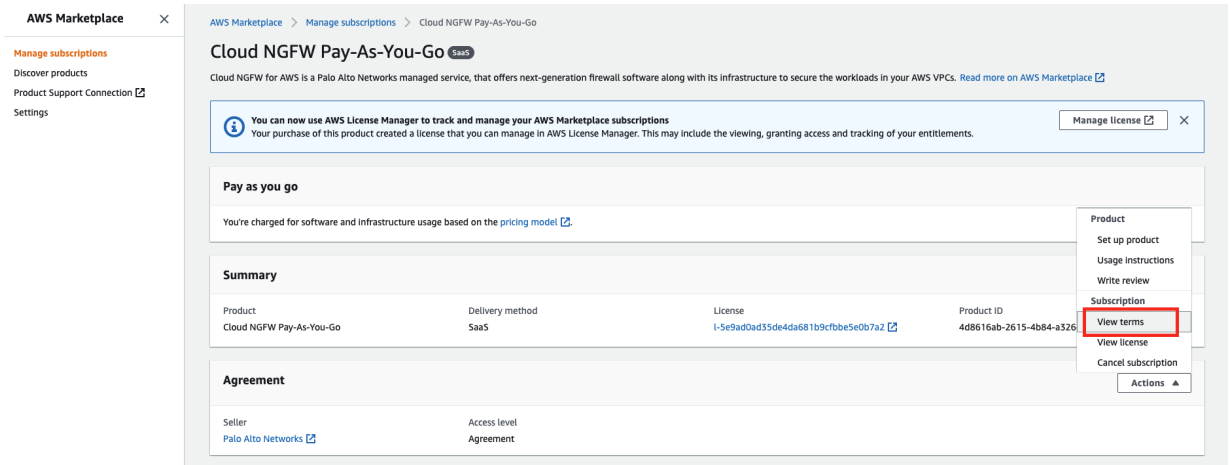
 ©2022 Palo Alto Networks, Inc

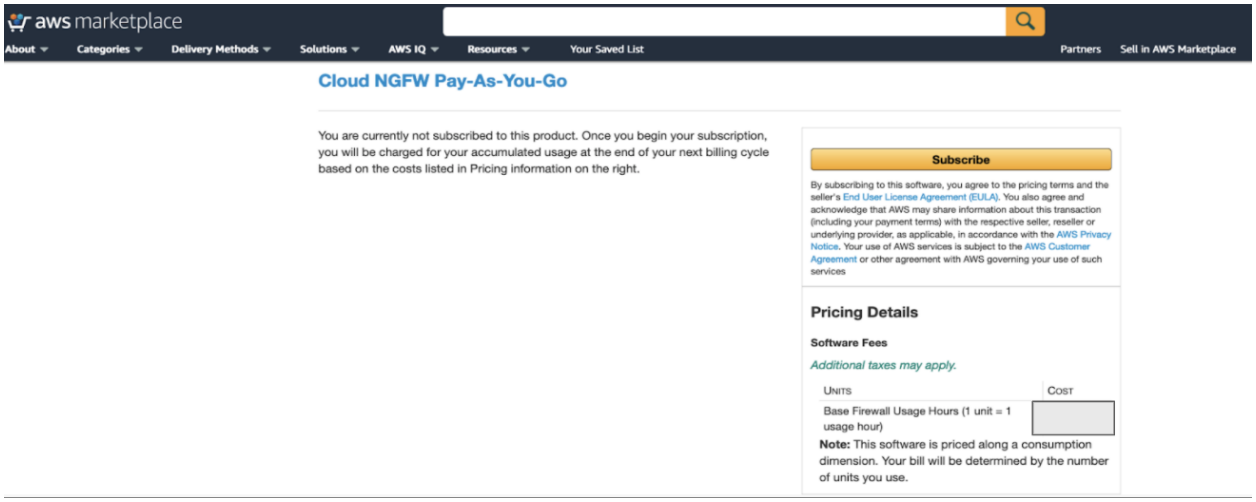
The charges are based on base firewall price and per GB utilization; thus providing better visibility and control over the spending.
There are two components to pricing. **Per hour charge** and **per GB charge** for traffic secured by NGFW. Customers need not worry about scaling. If more traffic need to be secured, more NGFW VMs will be launched in the backend and hence providing a seamless experience.

To get started, users need to subscribe to the service in AWS Marketplace.



You can verify the pricing details under the “view terms’ section



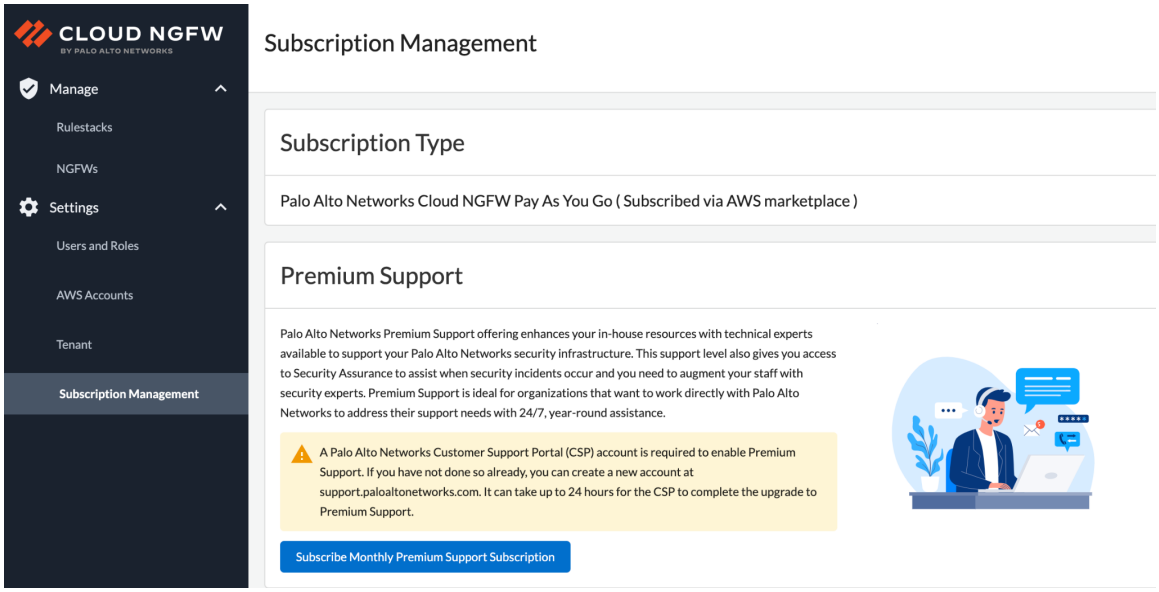


The **digital support** option is included with the base subscription. **Premium support** can be added with an extra charge, which will provide access to live support with service level objectives. Please find the table below for support inclusion.

Support	Digital	Premium
Product documentation	yes	yes
Proactive notification	yes	yes
Access to communities	yes	yes
Chat support	yes	yes
Community support	yes	yes
Customer support portal	yes	yes
Phone support - call back	No	Yes
Enhanced SLO	No	S1:1hr, S2:4hr
Access to online training	Yes	Yes

You can subscribe to premium support from the cloud NGFW console as shown in the image below. Navigate to **Settings-Subscription Management** to access the page.

 ©2022 Palo Alto Networks, Inc



Reader Tip - *Palo Alto Networks Customer Support Portal (CSP) account is required to enable Premium support*

Cloud NGFW Configuration Options

You can deploy the Cloud NGFW in your AWS environment in three way.

- Cloud NGFW console
- AWS Firewall Manager
- Programmatic Access.

Option1- Cloud NGFW console

Use Case- This method is recommended if you want to have independent cloud NGFW service with local rulestacks to protect applications in your account. Each account is associated with a separate cloud NGFW console.
The users can subscribe to cloud NGFW service from each AWS account and create a dedicated Cloud NGFW tenant for the firewalls and rules. To use the cloud NGFW console-

- Subscribe to Cloud NGFW and create a tenant
- Onboard AWS account to cloud NGFW tenant
- Create NGFW and endpoints
- Configure rulestacks, associated rules and security profiles.

Note- *This document covers configuration details using Cloud NGFW console.*

 ©2022 Palo Alto Networks, Inc

Option 2- AWS Firewall Manager

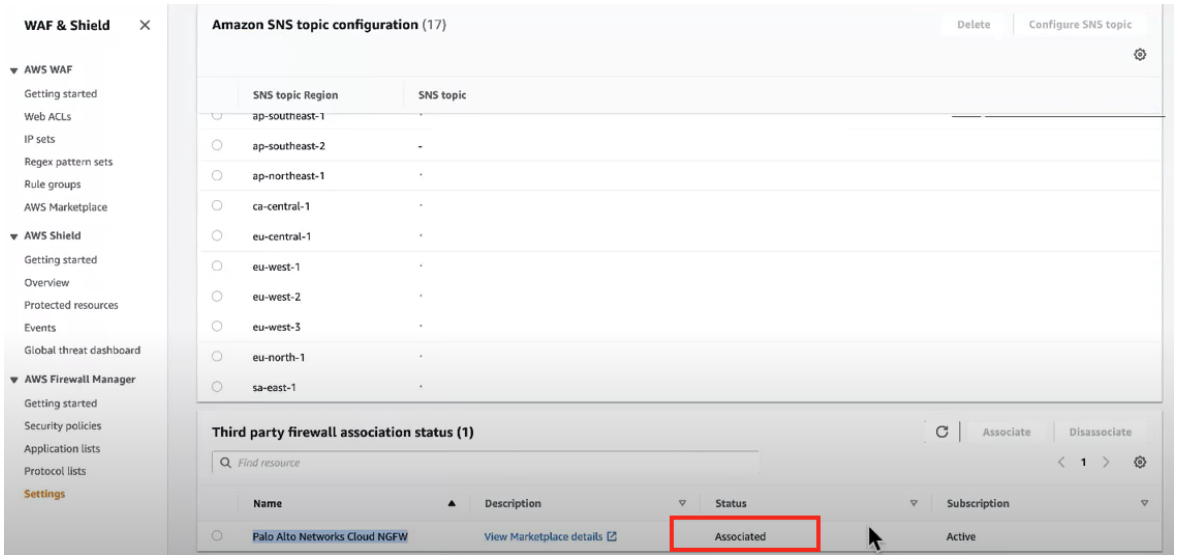
The second option to configure cloud NGFW is using the AWS firewall manager.

Use Case- This option can be used to deploy NGFWs across multiple accounts**.**You can use the **AWS Firewall Manager console** to create global rulestacks and deploy the Cloud NGFW across multiple AWS accounts in an AWS Organization. The Firewall Manager deploys the Cloud NGFW components including creation of the AWS marketplace subscription, management of the Cloud NGFW tenant, creation of NGFWs, and NGFW endpoints in your VPCs. The FMS console redirects you to the Cloud NGFW tenant to author rules for your global rulestacks.
The AWS Firewall Manager provides a workflow that allows you to deploy the Cloud NGFW as a FMS policy, select a deployment mode and region, create a global rulestack, configure NGFW endpoints, and define the scope of the Cloud NGFW across your organization.

Note-*To configure the Cloud NGFW policy, your AWS account must be a member of your AWS Organization and set as the AWS Firewall Manager administrator account. The account you use to subscribe to the Cloud NGFW service must be the same AWS Firewall Manager administrator account.*

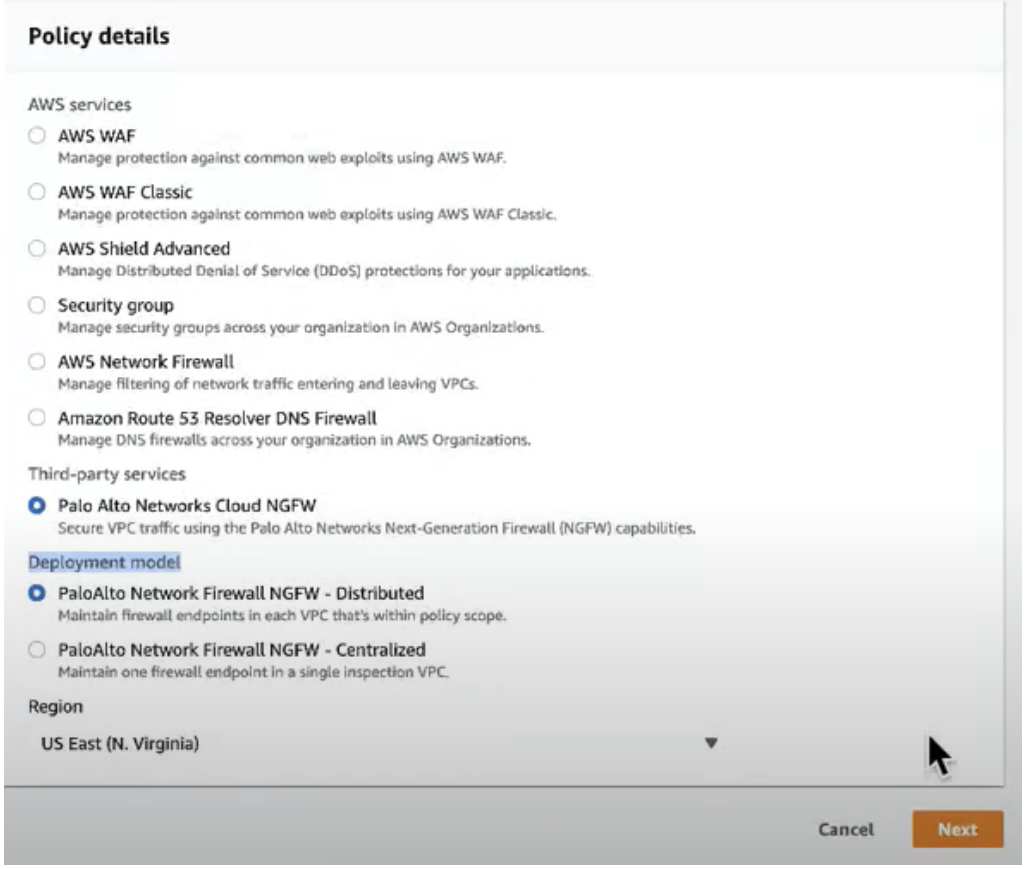
AWS Firewall Manager admin subscribes to Cloud NGFW via AWS Marketplace. The user can create a new cloud NGFW tenant.

1. Subscribe to the Cloud NGFW Service. The AWS account you use to subscribe to the Cloud NGFW service must be the same AWS Firewall Manager administrator account.
2. Associate the Palo Alto Cloud NGFW Service with the Firewall Manager.
   Log in to the AWS Console and select Services > AWS Firewall Manager >Settings.
   Under Third Party Firewall Association Status, select Palo Alto Networks Cloud NGFW. Click Associate



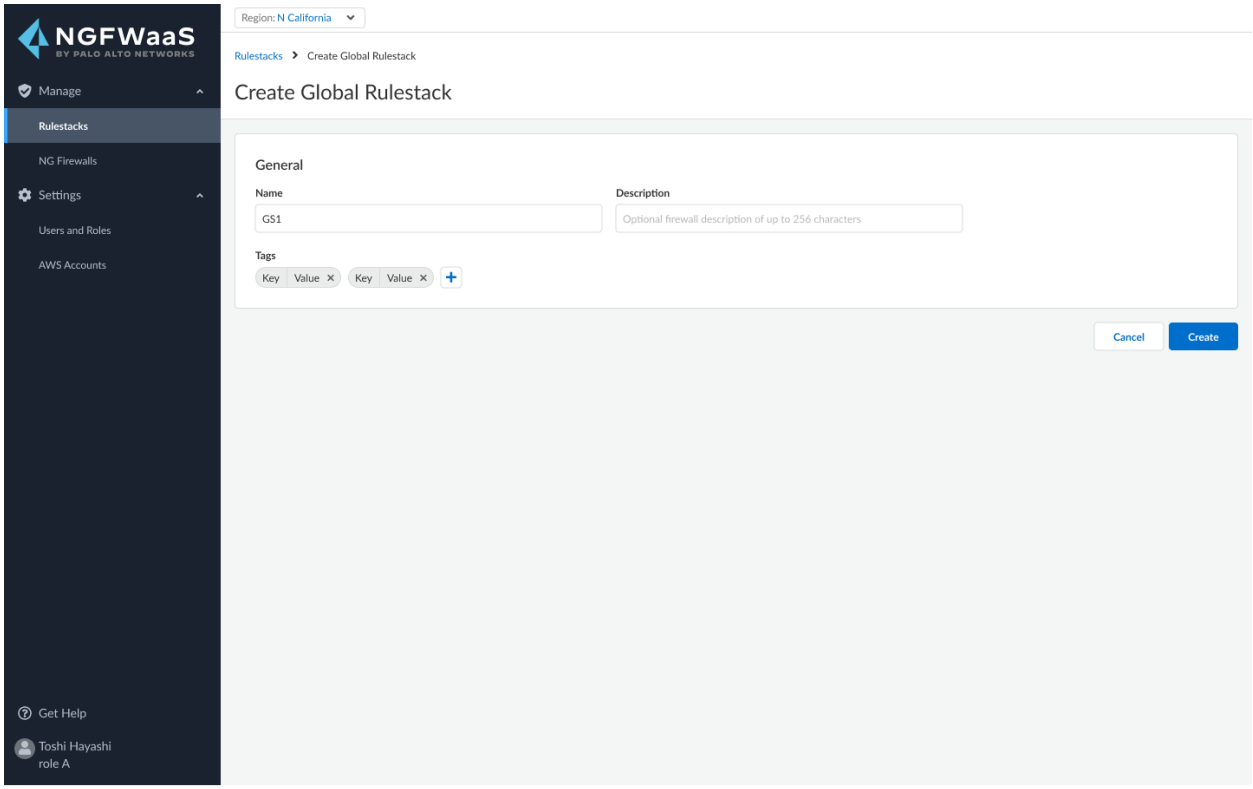
 ©2022 Palo Alto Networks, Inc

3. Go to **Security Policies-Create policy**
4. Select PaloAlto Networks Cloud NGFW under Third-party service.
5. Select the deployment model and the region



6. In the policy page, enter a descriptive name
7. Create the Firewall Policy Creation. Firewall Policy Configuration refers to a global rulestack in the context of the Cloud NGFW. If you have already created one or more global rulestacks, they are listed here. If you have not created a global rulestack, you can create one by clicking Create Firewall Policy. This redirects you to the Cloud NGFW console.

 ©2022 Palo Alto Networks, Inc

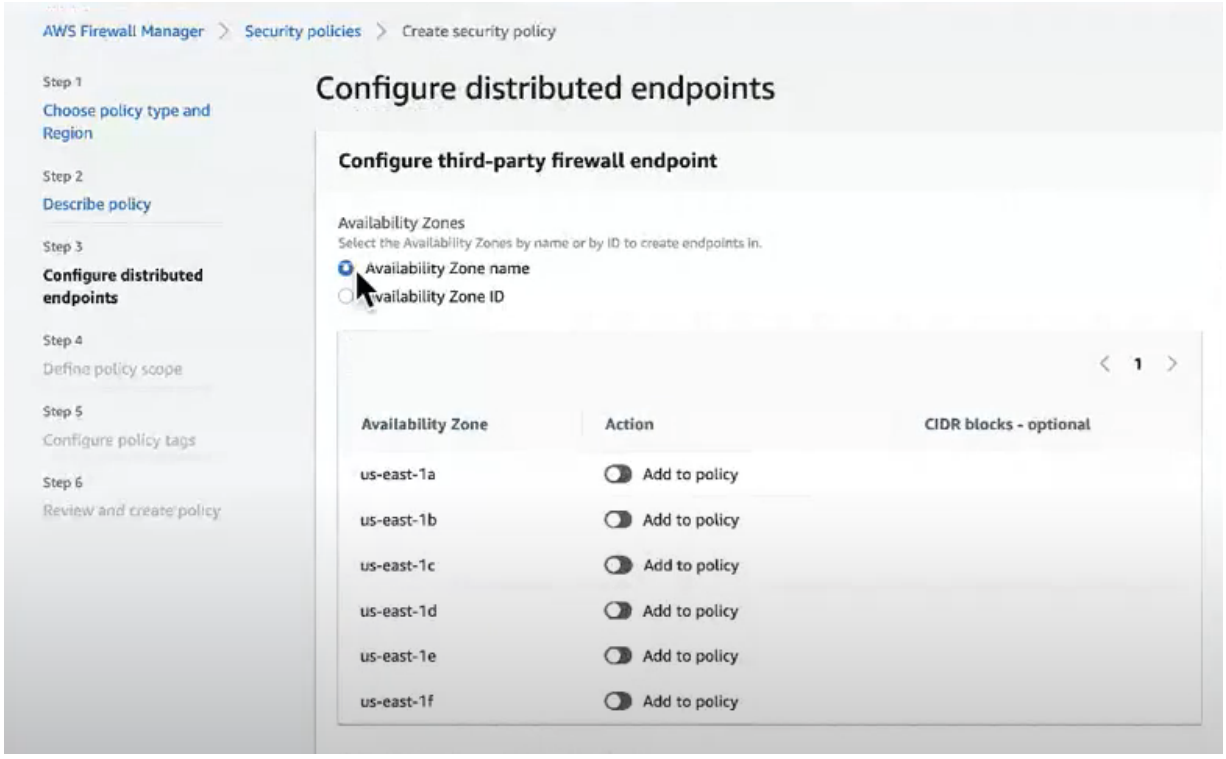


8. Select Traffic, Decryption, and/or Threat logs. And for each type, select the destination and click Next
9. **Select** Availability Zone Name **or** Availability Zone ID**. This selection determines what options—names or IDs—the FMS console lists.**
10. In the **Action** column, click the slider to add an **availability zone** to the Cloud NFGW FMS policy.

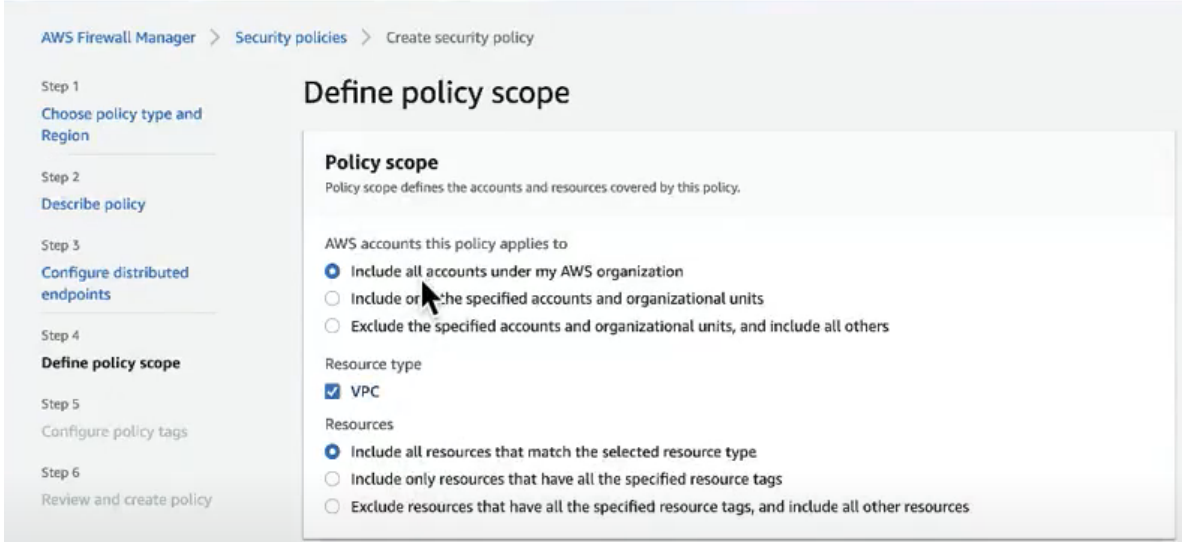
    You can specify a CIDR block for each selected availability zone or create a list of CIDR blocks for the FMS to assign to the selected availability zones. Each CIDR block must be a /28 CIDR block.

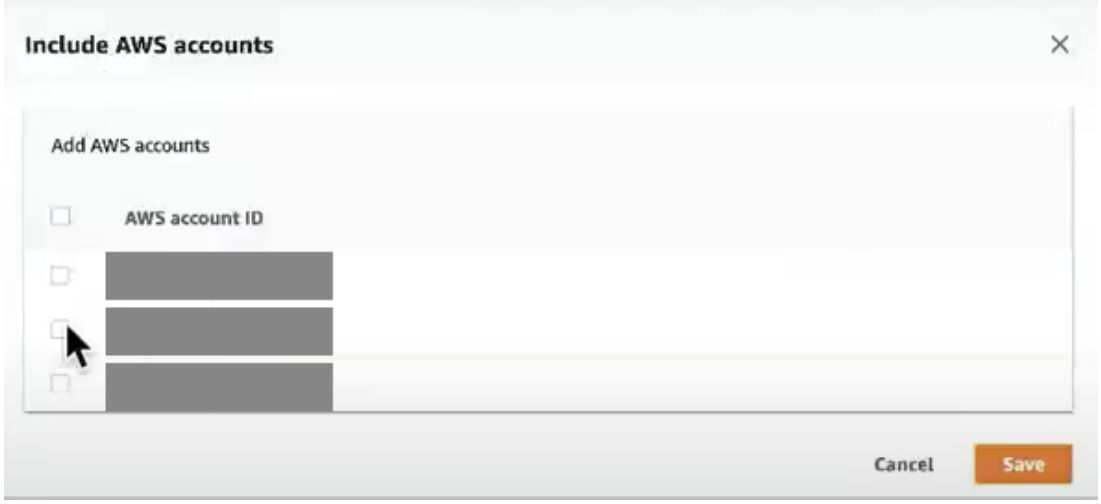
    If you do not specify any CIDR blocks, the FMS will take a best effort approach to find unassigned CIDR blocks in your VPC to create subnets for the NGFW endpoints. If no CIDR blocks are available in your VPC, the FMS displays a non-compliant error.

11. Click **Next**

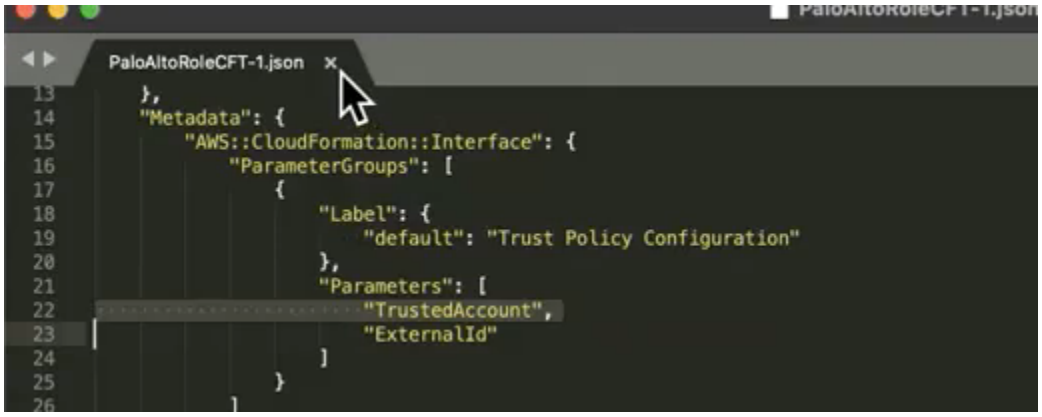


12. In the next step, you will have to define the scope of Cloud NGFW policy. You can specify all the accounts, select few accounts or add exceptions to accounts.



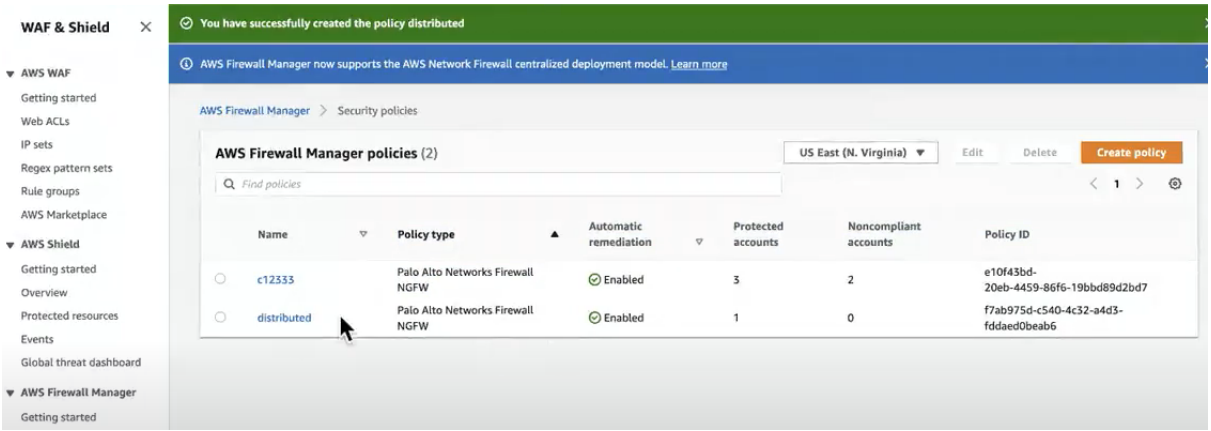


13. Download the CloudFormation template. There are two input parameters necessary here . ‘TrustedAccount’ and ‘ExternalId’. This information will be available in the console.



Note- This CFT needs to be run from each member account which we had selected in the previous step.

14. Click **Next**
15. Click **Create policy**



16. To edit the policy, you can click on the policy and edit individual sections

---

Note- *It takes approximately 20 minutes to provision the firewall and show up under* ***Accounts and resources*** *section.*

You have now successfully deployed Cloud NGFW using AWS Firewall Manager.

Reader Tip - *For information about Cloud NGFW visit the Live Community for Cloud NGFW*

Option 3- Programmatic Access

Programmatic access allows you to create and manage NGFWs and rulestacks using the API. AWS provides an access key ID and secret access to sign your requests for authorization to AWS. You must implement best practices to protect access key IDs and secret keys to prevent accidental or malicious account activity. Alternatively, you can use an IAM role in your AWS account to enable programmatic access. By using IAM roles for programmatic access, you can grant Cloud NGFW access without needing to hardcode an access key ID and secret access key into configuration files.

Note-*Programmatic access is disabled by default.*

Before enabling programmatic access, make sure the tenant meets the following requirements.

 ©2022 Palo Alto Networks, Inc

- Onboarded through AWS Marketplace and the CloudNGFW console. This makes the tenant a first-SaaS user automatically.
- At least one account is onboarded successfully including CFT creation.
- Programmatic access is enabled for the user by the Tenant Admin.
- AWS IAM roles created with respective AWS IAM PrincipalTags assigned to roles in the customer AWS account. These roles must have APIGatewayInvoke permission.
- AWS IAM users are permitted to assume the assigned AWS IAM Roles. The PrincipalTags and
- APIGatewayInvoke permissions can also be directly assigned to the users.
- Credentials for IAM user must be saved on the device making the programmatic access call.

Subscribe to the NGFW service

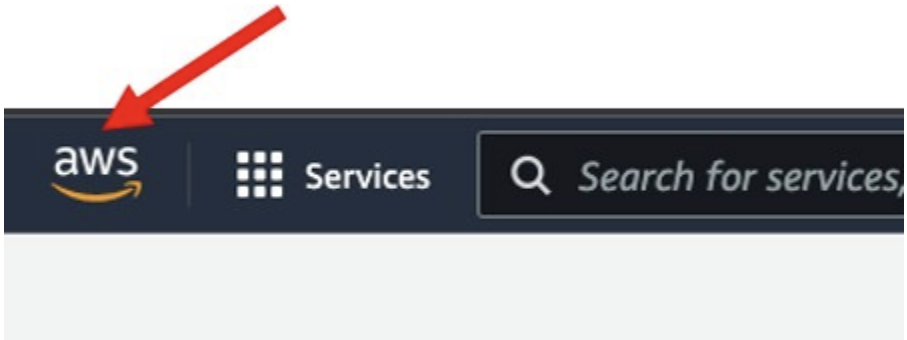
Overview

- Subscribe to the Cloud NGFW service in the AWS Marketplace.
- Create a Tenant Administrator – A **Tenant Administrator** is required to be able to add AWS Accounts and Users for accessing the Cloud NGFW service.
- Login/Change Password – Initial Tenant Administrator account setup.
- Add AWS account – Once the Tenant Administrator has been registered and logged in, the AWS account to be monitored must be added to the service.

Subscribe to CloudNGFW

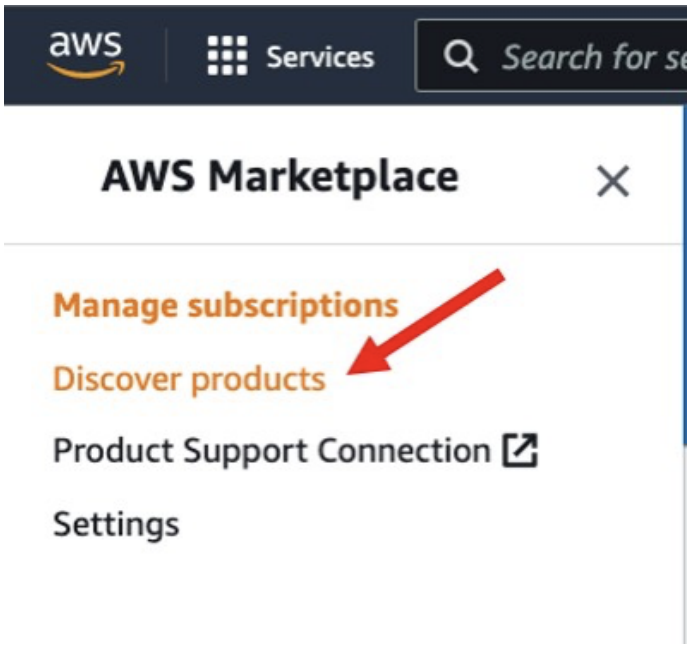
We will now subscribe to Palo Alto Networks CloudNGFW service. Please follow the instructions listed below.

1. Use the AWS link to navigate back to Console

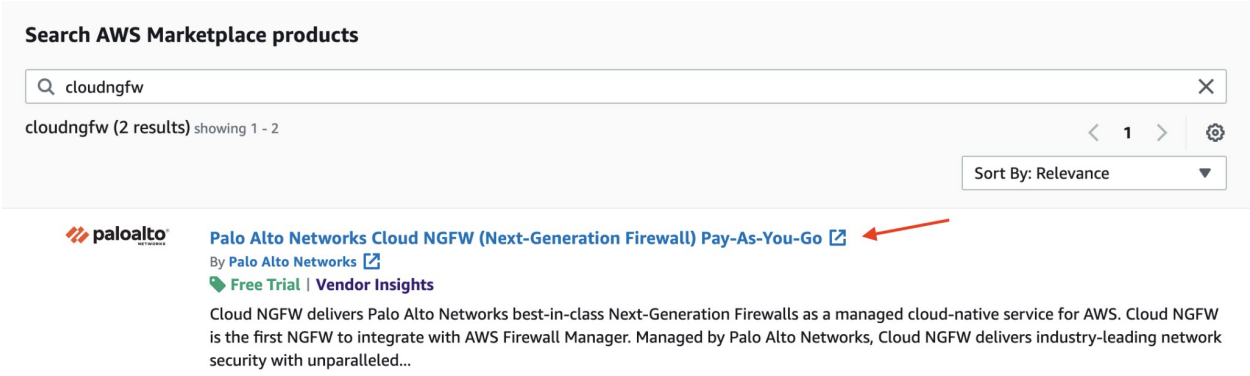


2. Search for “marketplace” on the search window and click on ‘AWS Marketplace Subscriptions’

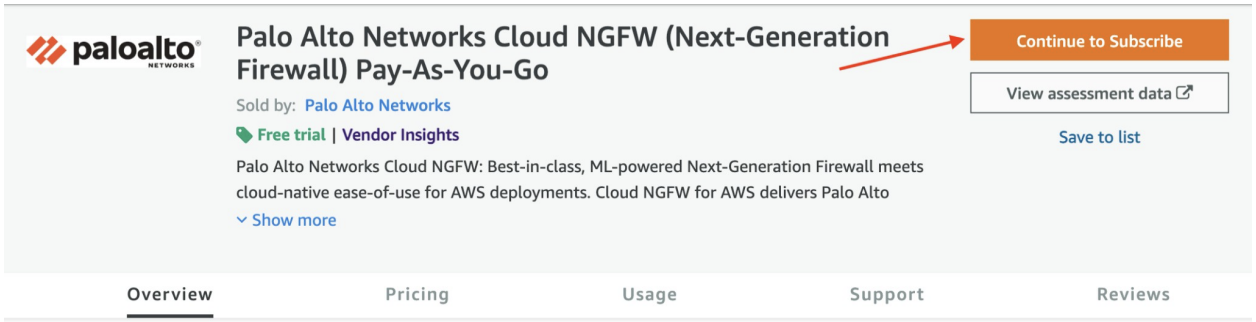
3. Now, Click on ‘Discover Products’ on the left hand menu.



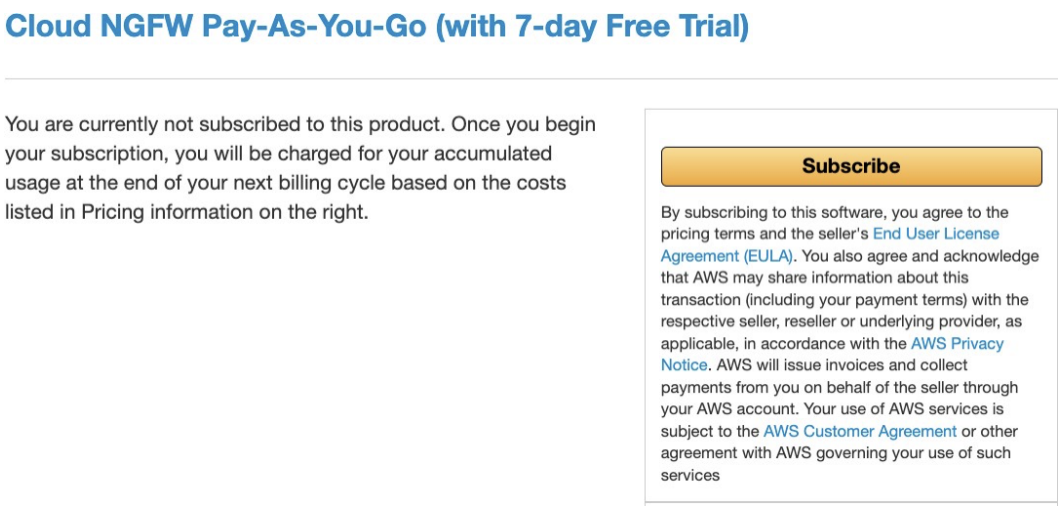
4. Search for ‘cloudngfw’ and from the search results that appear, click on the “Cloud NGFW Pay-As-You-Go” link.

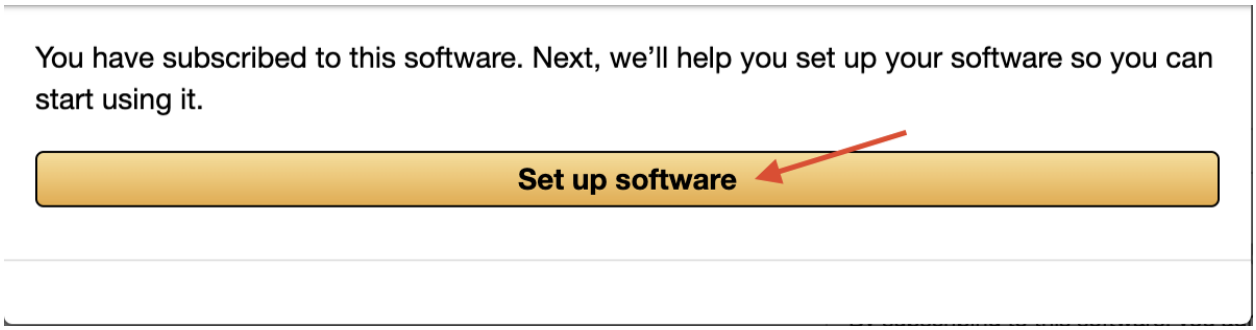


5. Click on the ‘Subscribe’ button to start your subscription of Palo Alto CloudNGFW Service.

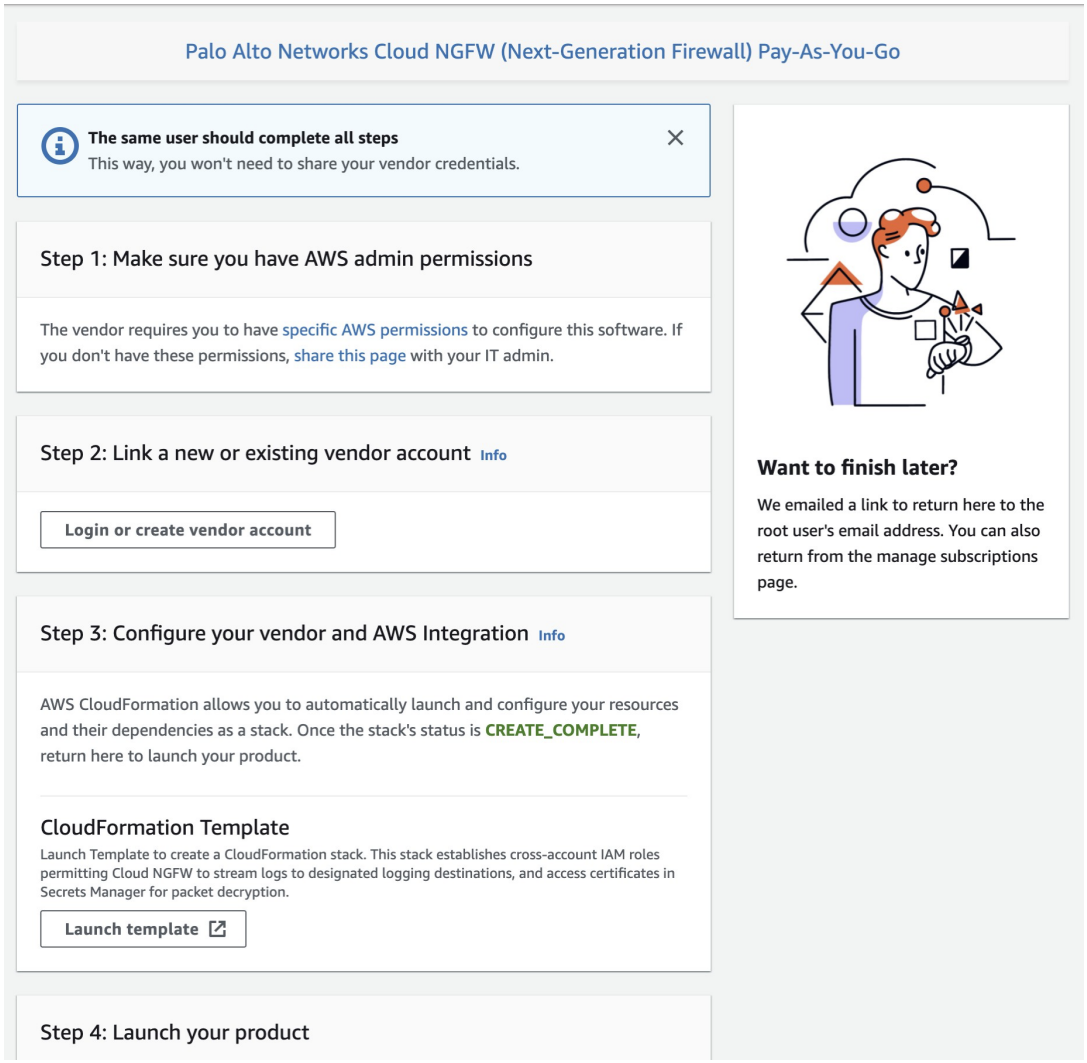


6. You can review the pricing details and click on ‘Subscribe’ and then, on the popup that shows, click on “Set up software”



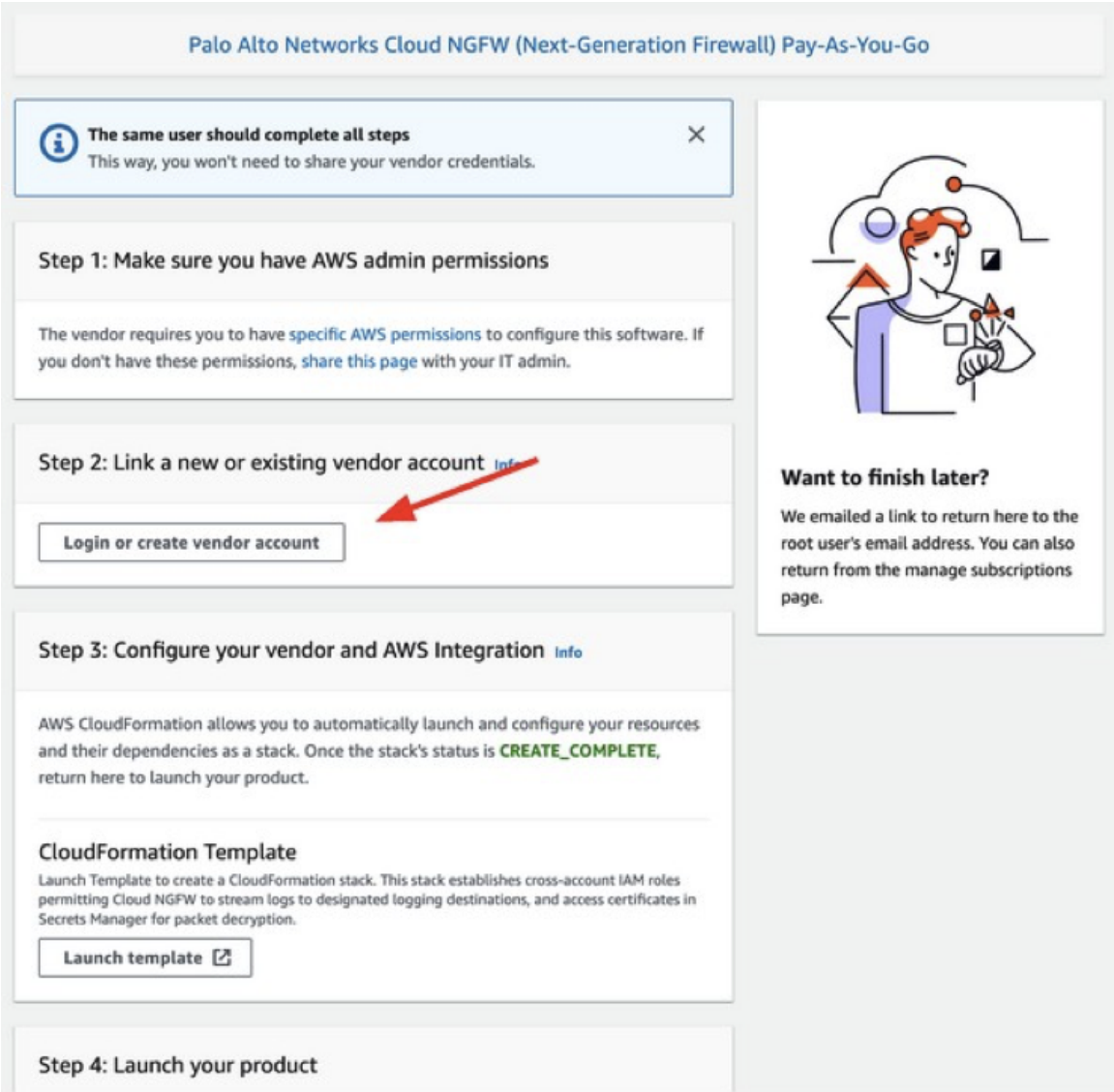


7. This will open up a new page on the AWS Console where you can register for using the AWS CloudNGW service and also set up your account for usage.

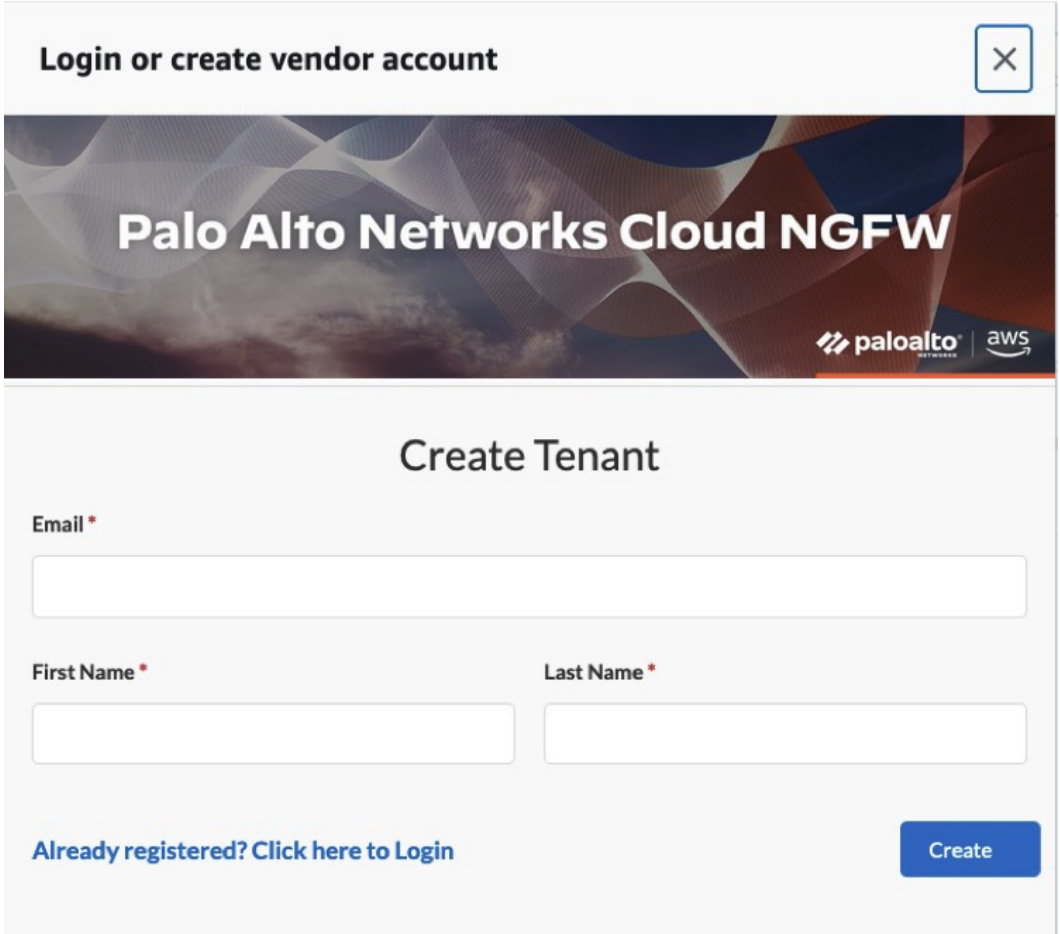


Create a Tenant

1. Click on the “login or create vendor account” to create a Tenant



2. .Provide an email address, first and last name.



3. Once you click on Create, an email will be sent to your email address with temporary credentials. Sign in to you email account and check for email from noreply-cloudngfw-aws@paloaltonetworks.com

- Copy the temporary password provided in the email.

 ©2022 Palo Alto Networks, Inc

Welcome to Palo Alto Networks Cloud NGFW for AWS.

Please use the temporary password bellow to proceed with your registration

Temporary Password: 3l

SUBSCRIPTION TYPE: Cloud NGFW Pay-as-you-go (via AWS Marketplace)

USERNAME: ssy

If you have interrupted the login process, you can resume it here.

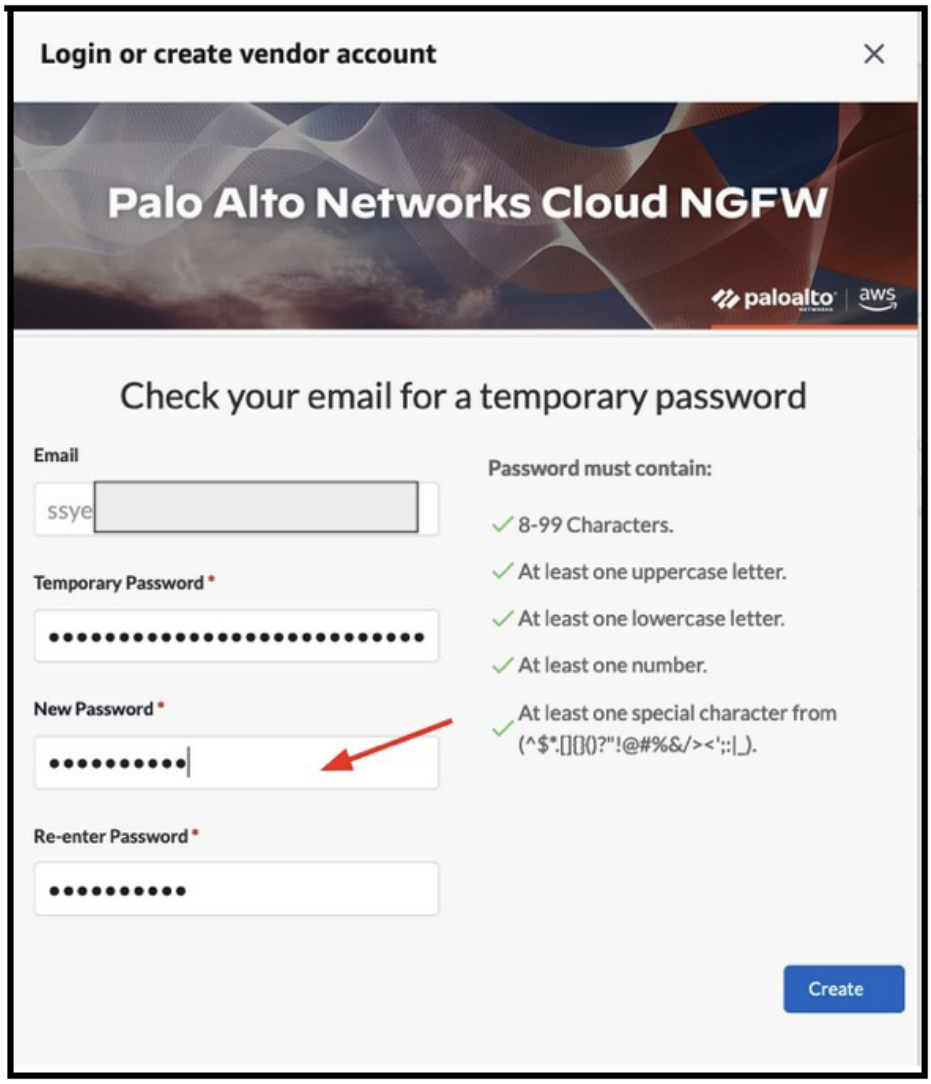
If you didn't make this request, please ignore this email.

Thanks

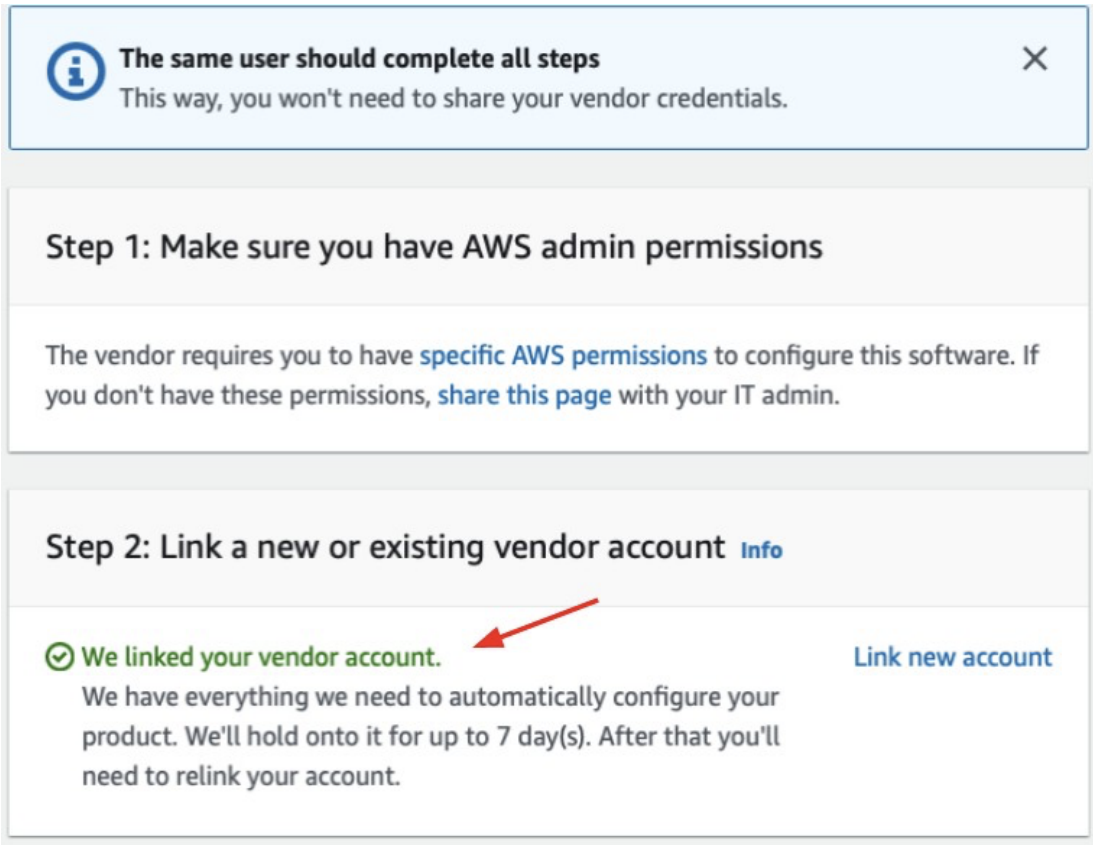
Palo Alto Networks Cloud NGFW Team.

4. Go back to the AWS Console. You will be prompted to change your password. After you have set a new password click on ‘Create’.

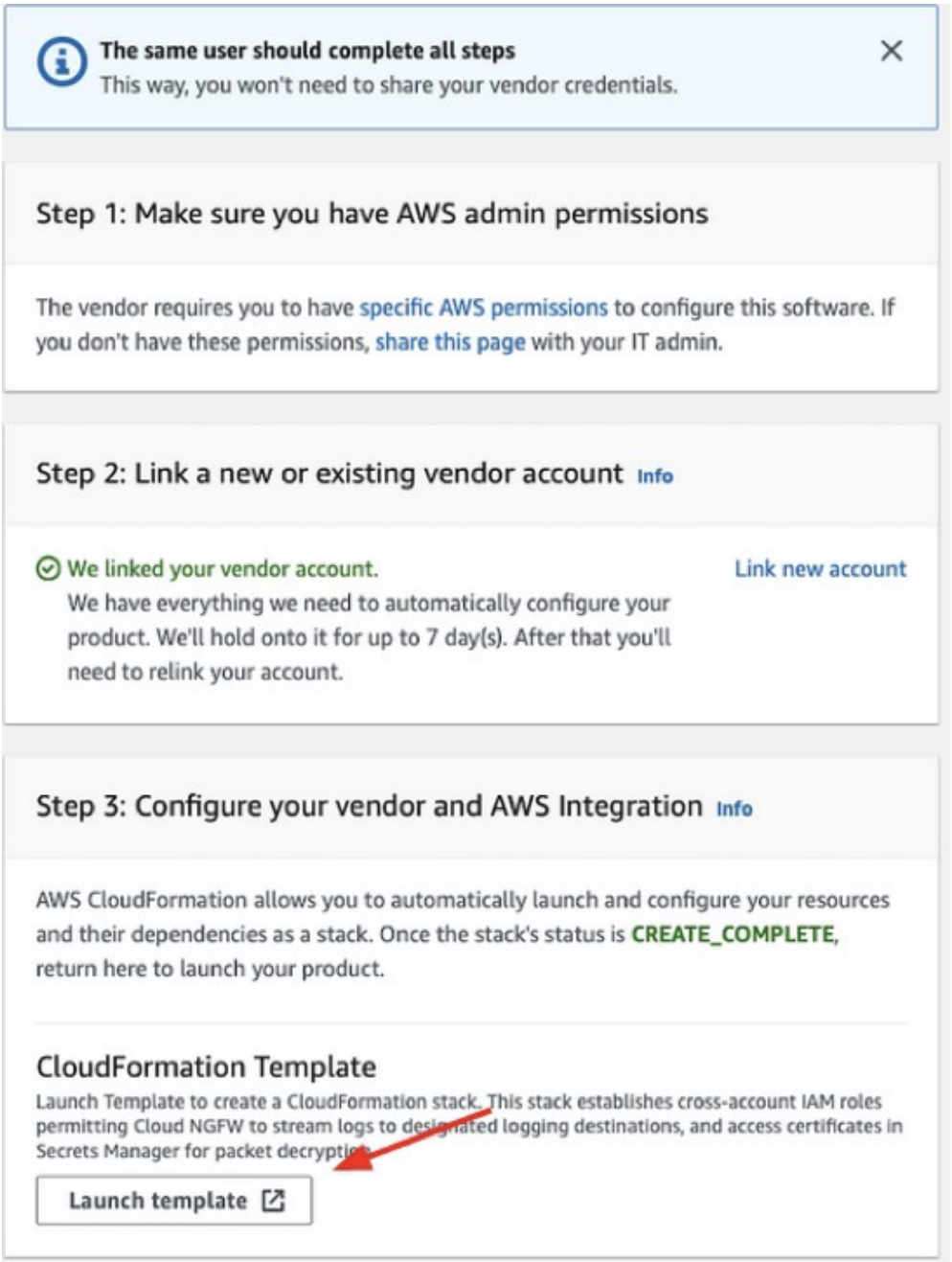
 ©2022 Palo Alto Networks, Inc



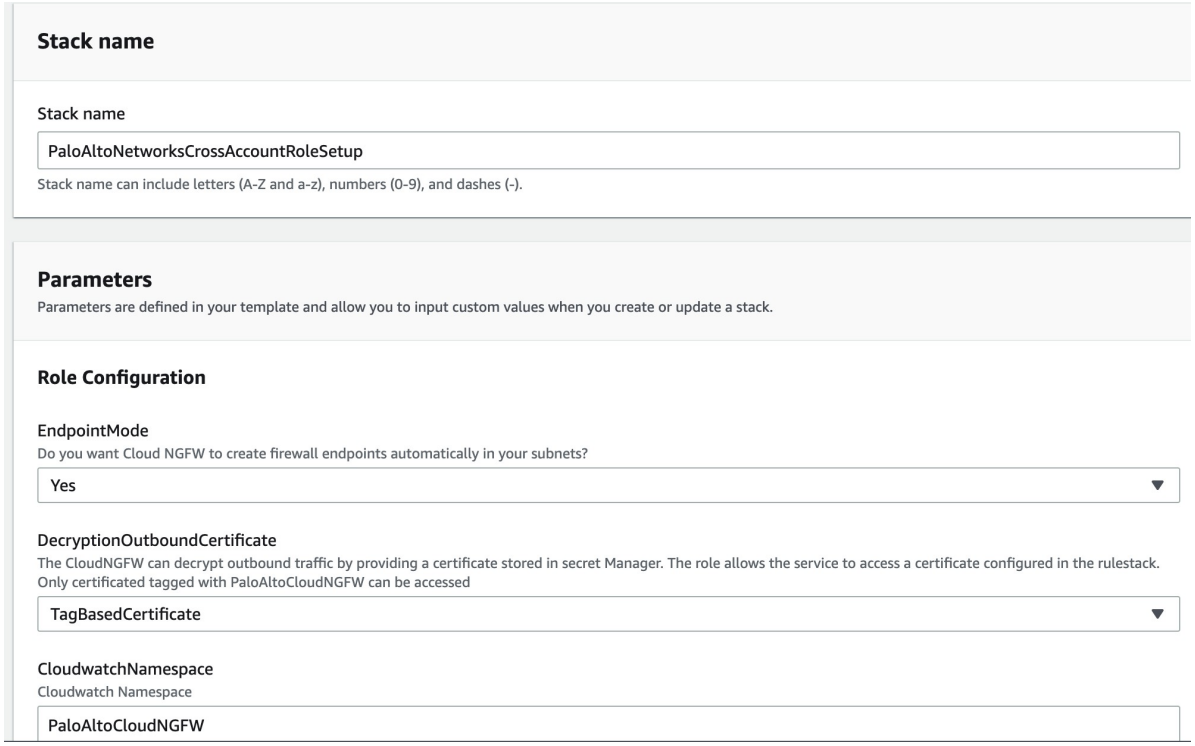
5. Link new account status will be changed to “We linked your vendor account”.



6. Next click on “Launch Template” to configure “Your vendor and AWS Integration. This will launch the AWS CFT console.



7. The “Stack name” field will be pre-populated with the value “PaloAltoNetworksCrossAccountRoleSetup”. This must be changed to something unique to avoid any conflicts. In the case of a conflict, you will see an error saying that the “Stack already exists”.

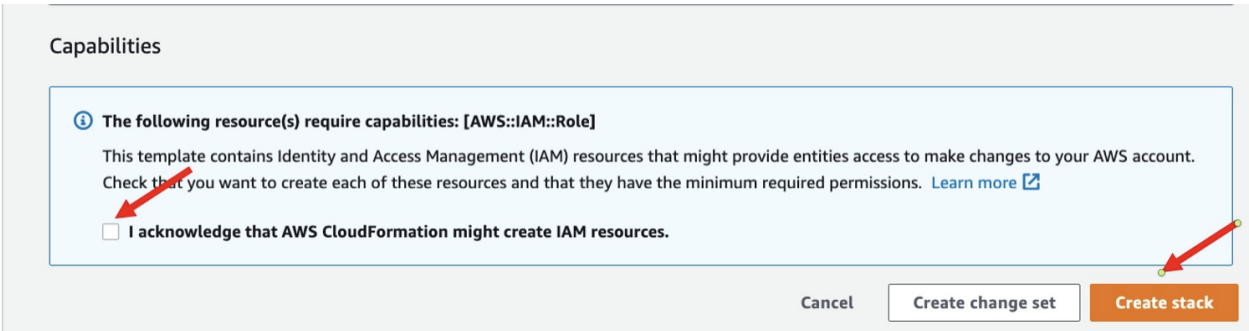


8. .For all other fields on the form, we will keep all default values. Scroll to the end of the Form.

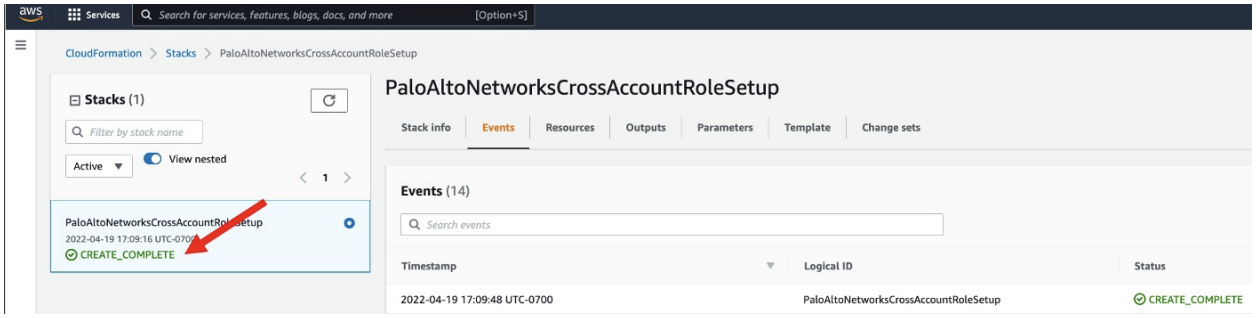
Note the Cloudwatch log folder name **'PaloAltoCloudNGFW'**. We will be using this later.

9. Select the check box to acknowledge.

10. Click on 'Create Stack'



11. Monitor the CFT deployment to ensure that it is successful. You might need to refresh for the latest status.



you have successfully subscribed to CloudNGFW service, created a tenant and associated your AWS account.

Reader Tip - *For more information, please refer to the deployment videos link here - Cloud NGFW YouTube Channel*

Cloud NGFW Concepts

Components

Roles and Permissions

Within Cloud NGFW, users can be assigned multiple roles for different operations. For example, user roles can be created for local vs global tasks associated with configuration and administration.
You can also invite additional users to help manage your Cloud NGFW deployment. You can then place these new users into the roles necessary for their level of access.
The below table outlines the roles and associated permissions.

Roles	Permissions
Tenant Administrator	• Add AWS Accounts • Invite users and assign roles. • Create global and local firewalls. • Create global and local rule stacks.
Global Firewall Administrator	• Create global and local firewalls. • Create global and local rule stacks.
Local Firewall Administrator	• Create local firewalls. • Create local rule stacks.

 ©2022 Palo Alto Networks, Inc

Local Rulestack Administrators	• Create local rule stacks

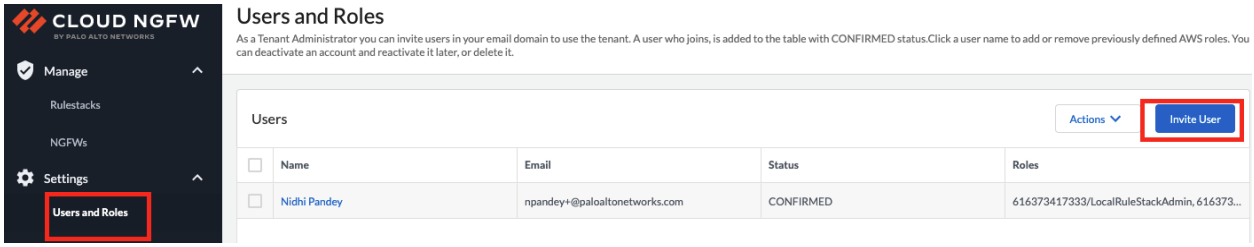
Note: *Local firewall administrators can only create firewalls and rule stacks within a specified AWS account.*

Inviting users to Cloud NGFW service

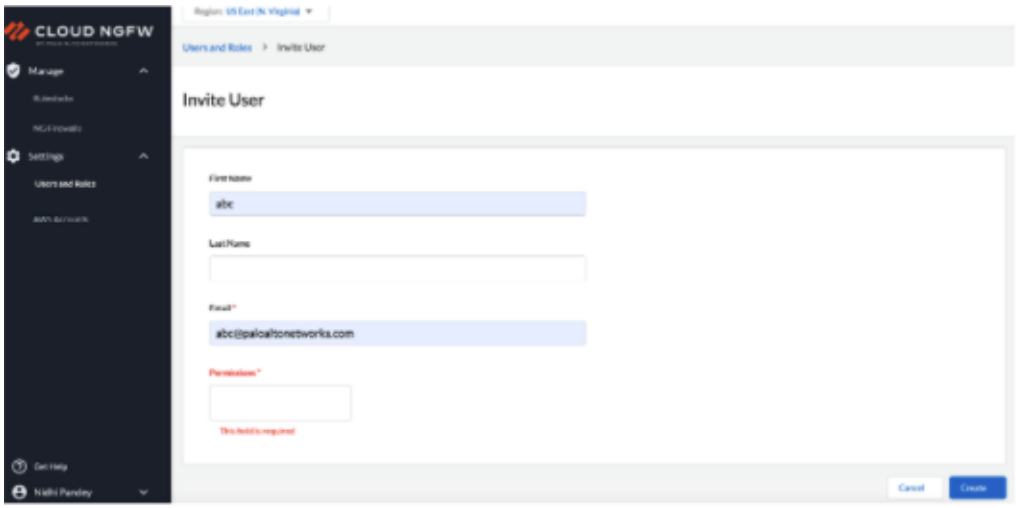
You can invite users to the cloud NGFW service. Please note that the email address domain of users invited by the tenant admin must match the email address domain of the tenant admin's login credentials.

From the cloud NGFW console window,

1. Select **Settings** > **Users and Roles** > **Invite User**.



2. Enter the first name, last name, and email address of the invitee.
3. Select the new user's role or roles from the Roles drop-down.
4. Click invite



Manage User Roles

At any time, you can modify a user's role or roles to expand or reduce their access and permissions. You can also delete a user. And individual users can view their roles and change their name or password as necessary.

1. Select **Settings** > **User and Roles**.
2. Click on the name of the user to be modified.
3. Modify the First Name and Last Name if necessary.
4. Modify the user's Roles & Scope.
5. **To add a role:**
    a. Click **Add Role**.
    b. Select the Role and Scope from the respective drop-downs.
6. **To delete a role:**Click the delete icon located to the right of the rule to be deleted.
7. Click Save.

How to Delete a User

If you need to completely remove a user's access and permissions, you can delete that user.

1. Select **Settings** > **User and Roles**.
2. Select the checkbox to the left of the user's name.
3. Select **Actions** > **Delete**.

How to Edit User Information

A non-Tenant Administrator can update their name or change their password if needed. However, they cannot modify their assigned roles.

1. Select **Settings** > **User and Roles**.
2. Click the user name.
3. Modify the First Name and Last Name if necessary.
4. **To change a password:**Click Change Password.
5. Enter the Current Password.
    a. Enter and re-enter the New Password.
    b. Click Change.
6. Click **Save**

Note: *Changing the password logs you out of the Cloud NGFW tenant. You must log back in using the new password.*

Reader Tip - *For more information, please refer to the deployment videos link here - Cloud NGFW YouTube Channel*

 ©2022 Palo Alto Networks, Inc

Rulestack

Rulestack is synonymous with security policies. It includes any configuration related to the security configuration and policy settings. In the Cloud NGFW, individual security policy rules are grouped together in a rule stack. An **object** is a setting that is referenced in a rule. For ex- FQDN,CIDR, prefix list etc.

A Rulestack can be associated with one or more firewalls. You can create two types of rule stacks—**local** and **global**.

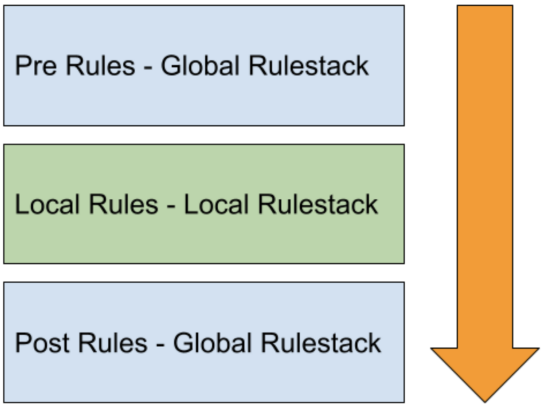
- **Global**—Rules in a global rulestack are divided into two types—pre rules and post rules—and these types determine when a rule is applied to traffic. Pre rules and post rules allow you to create a layered approach for implementing policy.
    - Pre Rules—Rules that are added to the top of the rule order and are evaluated first.
    - Post Rules—Rules that are added at the bottom of the rule order and are evaluated after the pre-rules and rules that are locally defined on an individual firewall.

- **Local**—Rules in a local rulestack can be applied to any firewall in your Cloud NGFW subscription.

A user's ability to create and modify a local or global rulestack depends on their level of access.

- A local administrator can create and modify rules on local rule stack only.
- Global administrators and tenant administrators can create and modify global rule stacks in addition to local rule stacks.

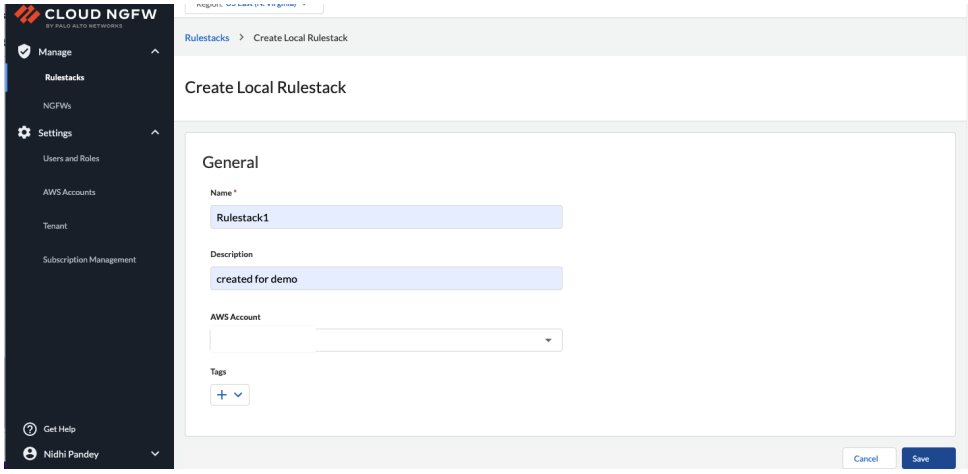
The combination of local and global rulestacks allows you to create a hierarchical rulestack. The pre-rules of a global rulestacks can act as global default rules for all associated firewalls. Then you can use a local rulestack to define rules for specific applications or users. The post rules can be used to allow or deny traffic that does not match any pre-rules or those rules defined in the local rulestack.



 ©2022 Palo Alto Networks, Inc

Create a Rulestack for Cloud NGFW

1. Complete the following procedure to create a global or local rulestack.
2. From the Cloud NGFW tenant, select **Manage** > **Rulestacks** > **Create Rulestack**.
3. Select **Local Rulestack** from the drop-down.
4. Enter a descriptive Name for your rulestack.
5. (optional) Enter a Description for your rulestack.
6. Select the AWS account
7. Optionally, add a tag
8. Click **Save**.



To delete a rulestack, select the rule stack and select delete from the dropdown option.

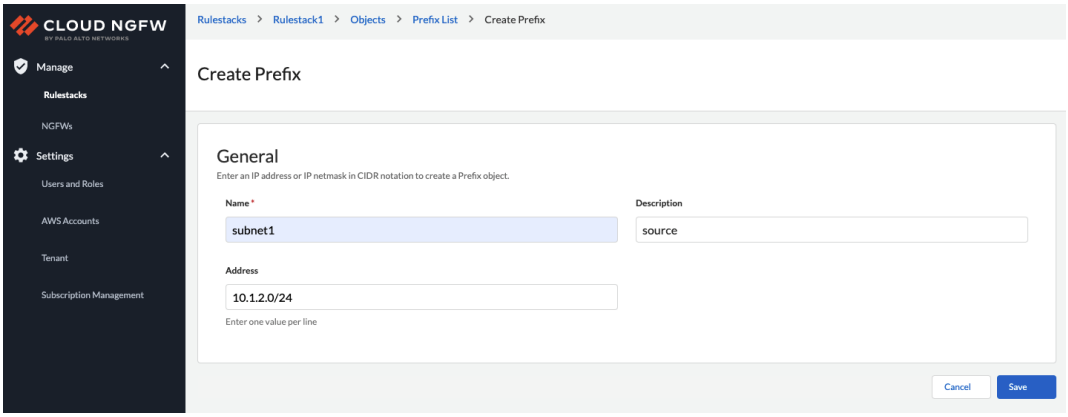
Note: *The user needs to create the objects before it can be used as a match criteria.*

Cloud NGFW Security Rule Object

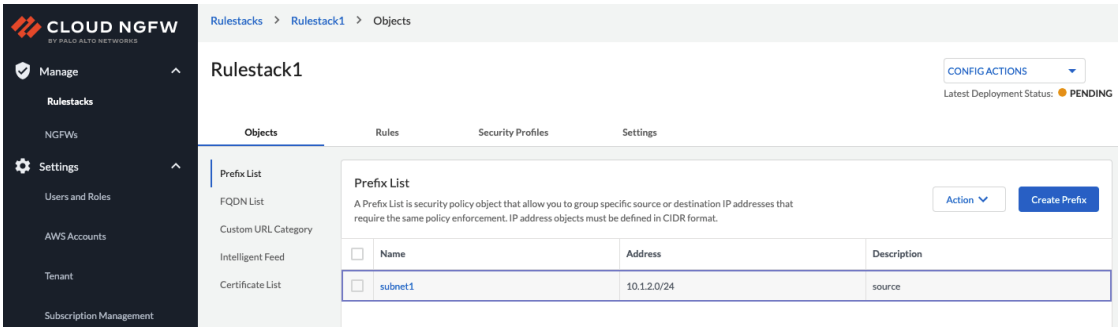
A security rule object is a single object or collective unit that groups discrete identities such as IP addresses, fully-qualified domain names (FQDN), intelligent feeds, or certificates. Typically, when creating a policy object, you group objects that require similar permissions in policy. Group object allows you to significantly reduce the administrative overhead in creating rules.
Prefix Lists—prefix lists allows you to group specific source or destination IP addresses that require the same policy enforcement. A prefix list can contain one or more IP addresses or IP netmask in CIDR notation. To create an object with prefix list, follow the steps below-

 ©2022 Palo Alto Networks, Inc

1. Select **Rulestacks** and select a previously-created rulestack on which to configure a prefix list.
2. Select **Objects** > **Prefix List** > **Create Prefix**.
3. Enter a descriptive Name for your prefix list.
4. (optional) Enter a description for your prefix list.
5. Enter the address. You can enter IP addresses or IP netmasks in CIDR format and one value per line.
6. Click **Save**. .

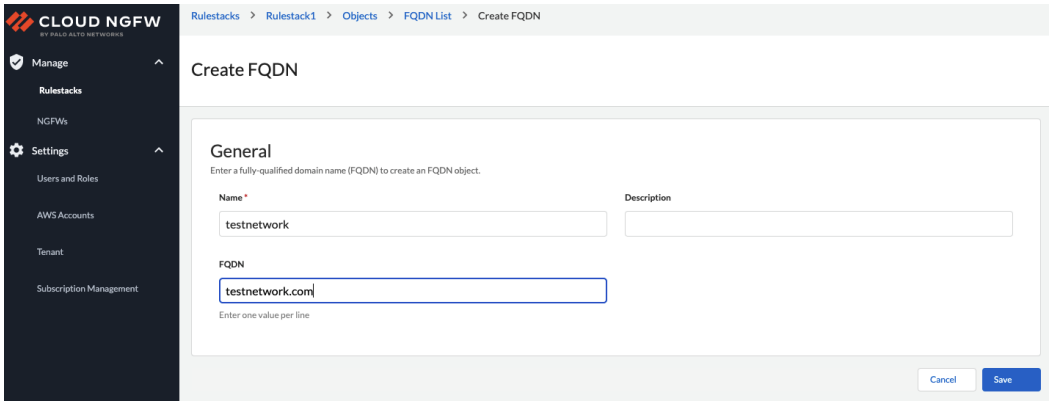


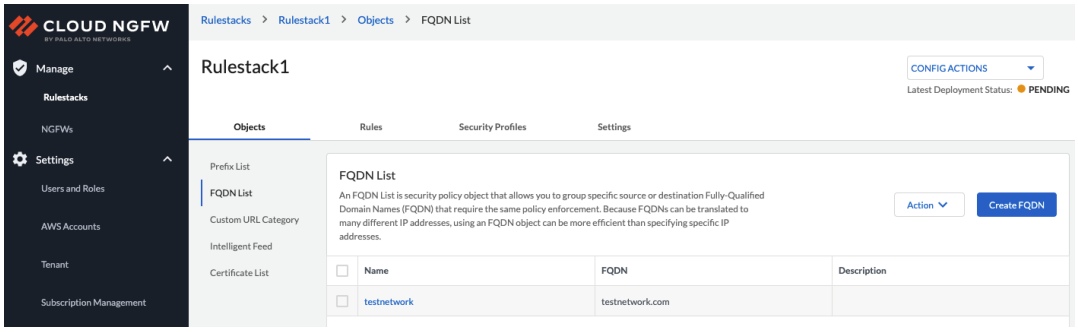
The prefix created will show up in the list under the prefix list section. To delete a prefix, select the prefix , select action drop down and select delete.



- **FQDN List-** An FQDN (for example, paloaltonetworks.com) object provides further ease of use because DNS provides the FQDN resolution to the IP addresses. Hence instead of you needing to know the IP addresses and manually updating them every time the FQDN resolves to new IP addresses. Administrators can use FQDN as an object and use it in the match criteria for traffic. To create an object with a FQDN list, follow the steps below.
    1. Select **Rulestacks** and select a previously-created rulestack on which to configure FQDN list.
    2. Select **Objects** > **FQDN List** > **Create FQDN**.
    3. Enter a descriptive Name for your FQDN list.
    4. (optional) Enter a description for your FQDN list.
    5. Enter one or more FQDN, one per line.
    6. Click **Save**. Check the FQDN created in the object page.

 ©2022 Palo Alto Networks, Inc





Custom URL Category—A custom URL category allows you to specify exceptions to a URL category enforcement. You can also create a custom URL category based on multiple existing categories.Few points to remember-

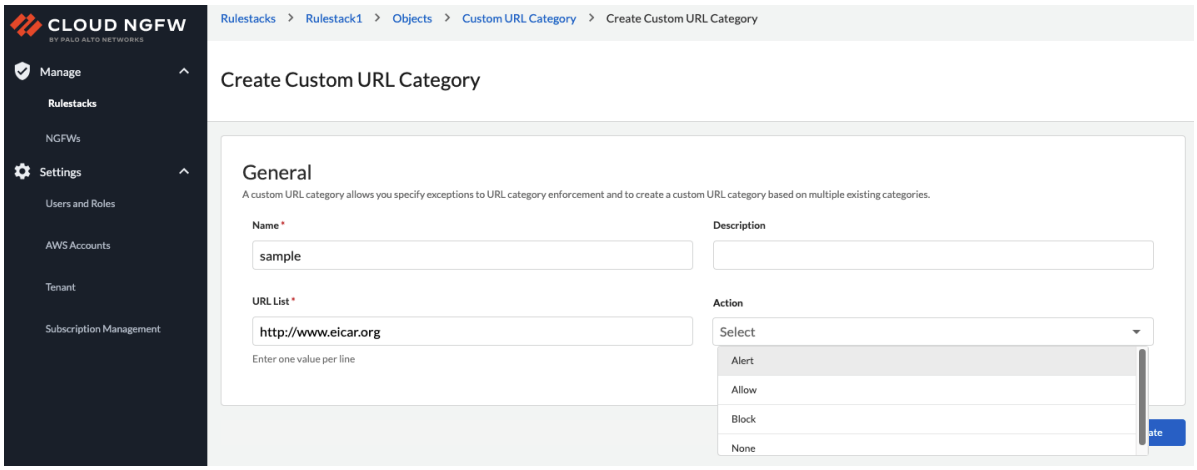
- Enter the URLs of websites that you want to enforce separately from the associated URL category.
- List entries must be an exact match and are case-insensitive.
- Enter a string that is an exact match to the website (and possibly, specific subdomain) for which you want to control access.
- You can use wildcards in URL category exception lists to easily configure a single entry to match to multiple website subdomains and pages, without having to specify exact subdomains and pages. Users can choose actions based on the URL list. These actions are -

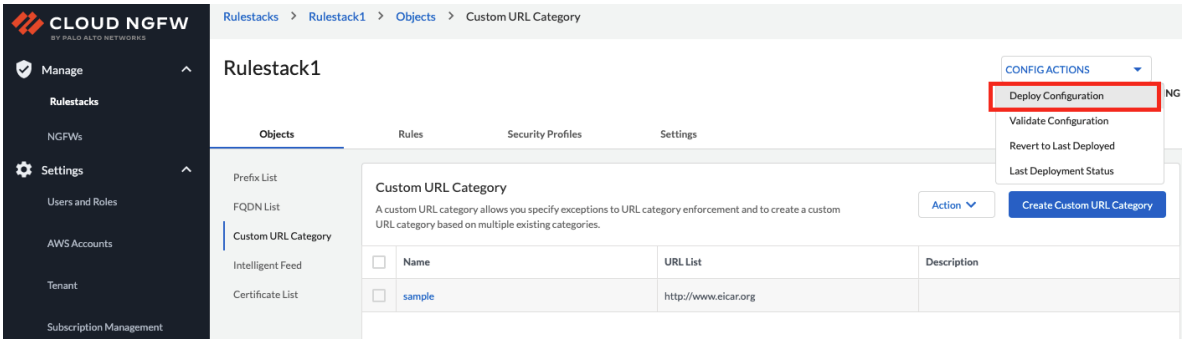
Alert - The website is allowed and a log entry is generated in the URL filtering log.
Allow - The website is allowed and no log entry is generated.
Block - The website is blocked and the user will see a response page and will not be able to continue to the website. A log entry is generated in the URL filtering log.
Blocking site access for a URL category also sets User Credential Submissions for that URL category to block.

None - no action is needed for this category

Follow the steps below for creating custom URL category

1. Select **Rulestacks** and select a previously-created rulestack on which to configure a custom URL category.
2. Select **Objects** > **Custom URL Category** > **Create Custom URL Category**.
3. Enter a descriptive Name for your custom URL category.
4. (optional) Enter a description for your custom URL category.
5. Enter one or more URL List, one per line.
6. Select an action
7. Click **Create**.
8. Click **Deploy Configuration** from the **Config Actions** drop down



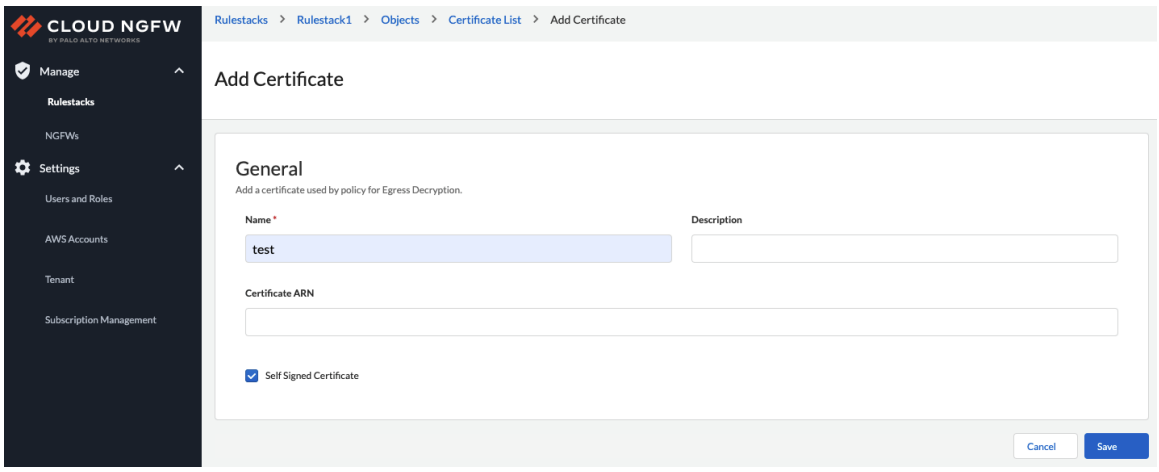


Certificate List- A certificate list is a collection of certificates used by your NGFirewall for egress decryption. The Cloud NGFW uses certificates to access an intelligent feed and to enable egress decryption. These certificates are stored in the AWS Secrets Manager.
To enable the NGFirewall to perform egress decryption, you must set up the certificates required to establish the NGFirewall as a trusted third party (proxy) to the session between the client and the server. The NGFirewall can use certificates signed by an enterprise certificate authority (CA) or self-signed certificates generated on the NGFirewall as Trust certificates to authenticate the

SSL session with the client. You can use an **Enterprise CA-signed Certificates or Self-signed Certificates**

Follow the steps below to configure the certificate object

1. Select **Rulestacks** and select a previously-created rulestack
2. Select **Objects** > **Certificate List** > **Add Certificate**.
3. Enter a descriptive Name for your certificate.
4. (optional) Enter a description for your certificate.
5. Enter the Certificate ARN from dropdown.
6. If the certificate is self-signed, check Self Signed Certificate.
7. Click **Save** and **Deploy Configuration**.



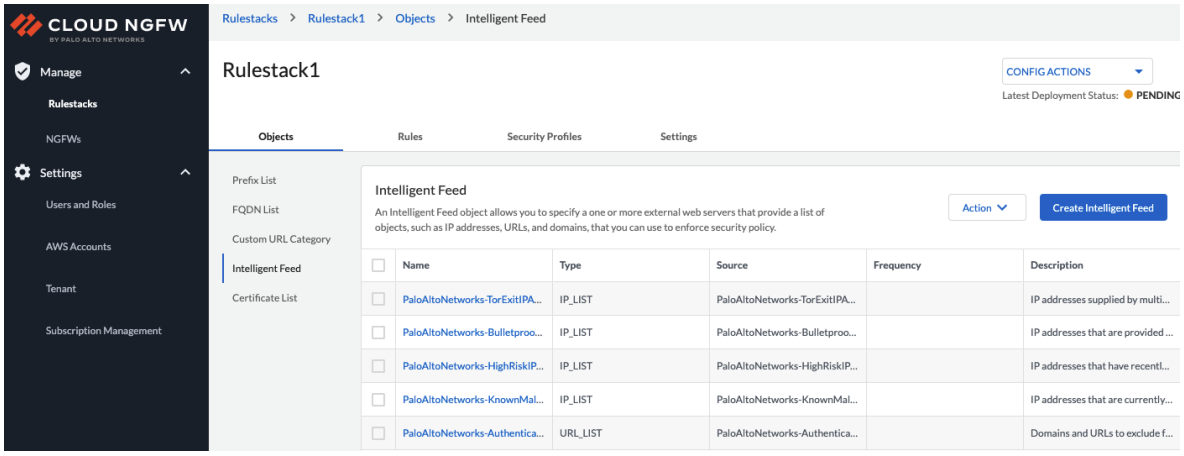
How to configure Intelligent Feed

An intelligent feed, also called a threat intelligence feed, is an ongoing stream of data related to potential or current threats to an organization's security. It is an external dynamic list, which is a text file that is hosted on an external web server. An intelligent feed records and tracks IP addresses and URLs that are associated with threats such as phishing scams, malware, bots, spyware, ransomware, and more. You can connect your NGFirewall with intelligent feeds to provide up-to-date information about threats to your network. The certificates used by your NGFirewall for accessing an intelligent feed are stored in the AWS Secrets Manager.
The NGFirewall checks the hosted list at configured intervals, and enforces policy based on the latest updates without requiring you to make any configuration changes.

IP List—You can enforce policy for a list of source or destination IP addresses and configure the NGFirewall to deny or allow access to the IP addresses included in the list. The NGFirewall treats an IP List intelligent feed as an address object, and all IP addresses included are handled as one address object.

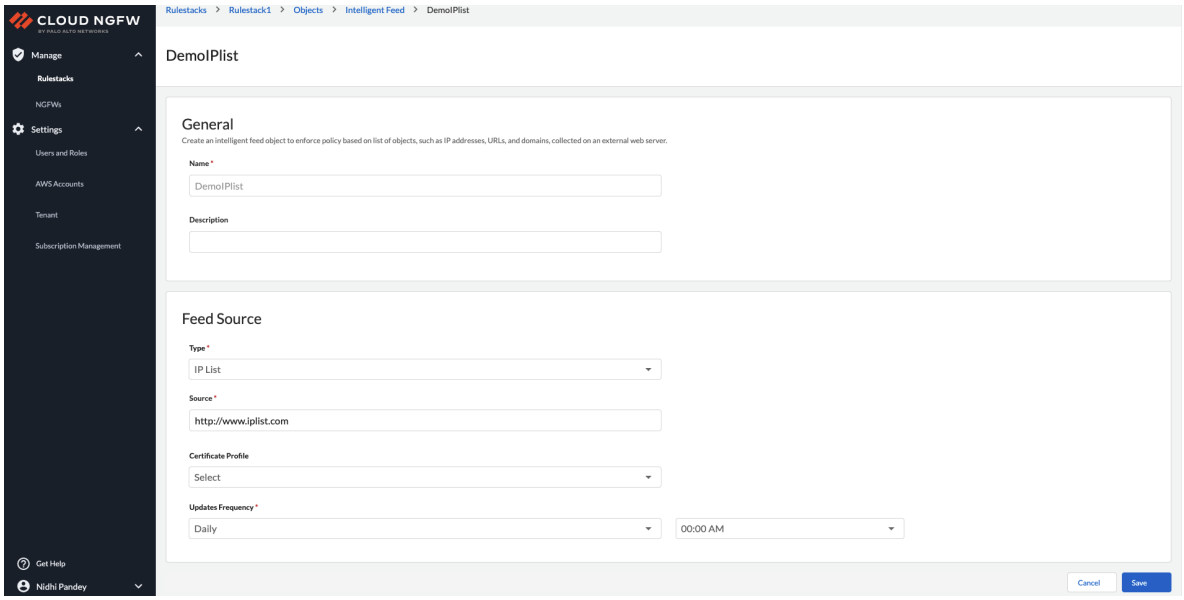
URL List—You can protect your network from new sources of threat or malware using URLs. The NGFirewall handles an intelligent feed with URLs like a custom URL category.

PaloAlto Networks provide a default list of feed objects for you to start using from day 1.



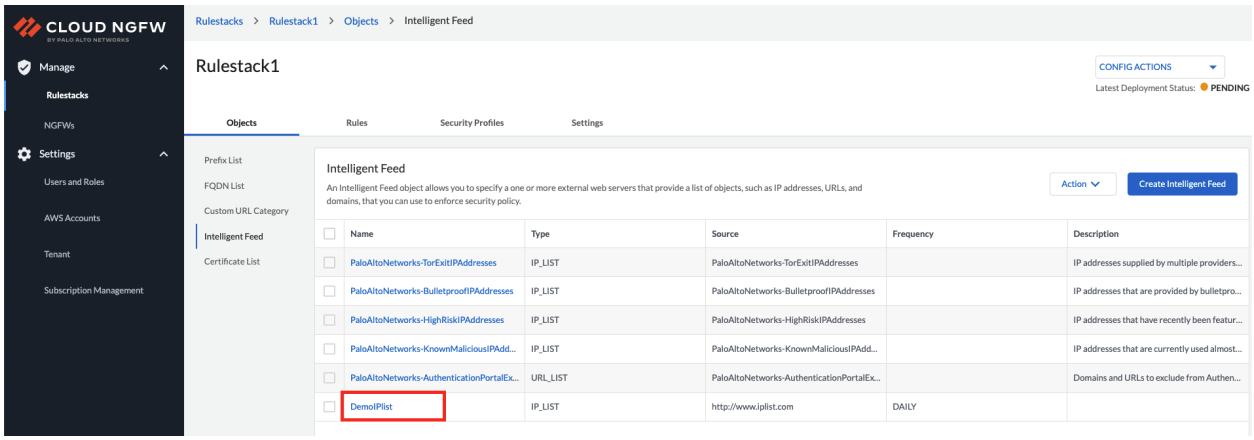
To create a custom intelligent feed, follow the steps below.

1. Select **Rulestacks** and select a previously-created rulestack on which to configure file Blocking.
2. Select **Objects** > **Intelligent Feed** > **Create Intelligent Feed**.
3. Enter a descriptive Name for your intelligent feed.
4. (optional) Enter a description for your intelligent feed.
5. Select the intelligent feed **Type**.
6. Enter the Source URL.
7. Set the **Update Frequency**—Hourly or Daily.
8. Click **Save** and **Deploy Configuration**



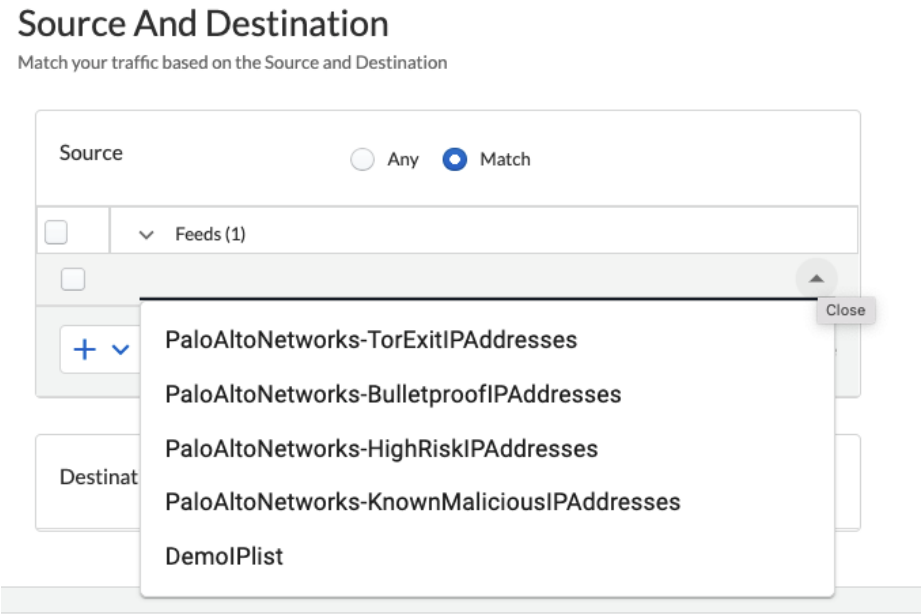
 ©2022 Palo Alto Networks, Inc

The newly created feed will be added to the intelligent feed list.

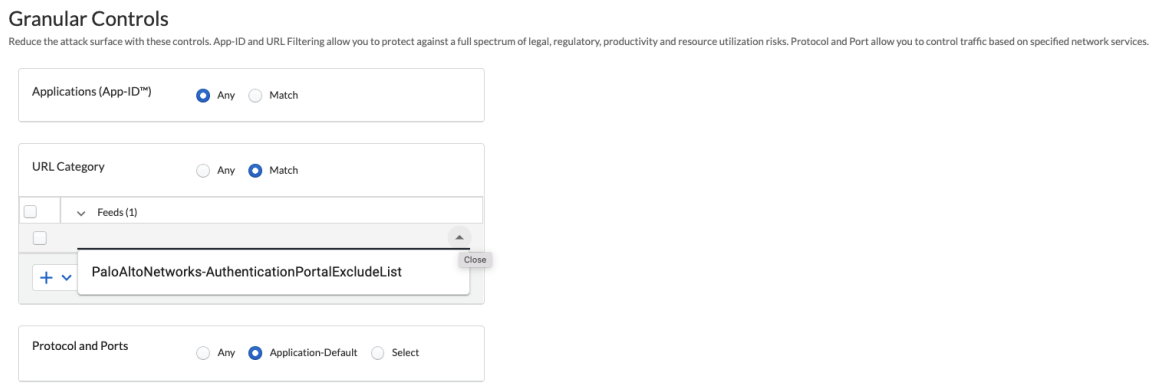


You can now use the feed objects in rule creation. Below is an example to add a feed object to Source

1. Go to **Rules** tab and click on **Create**.
2. After entering the name and rule priority, scroll down to the **Source And Destination** section
3. Click on **Match** for **Source**
4. Select the dropdown
5. Select **Feeds**,
6. Select the feed object from the drop down as shown below.



Similarly, you can use feed objects for **Destination**. You also have an option to use feed object of type URL, in **URL Category** section



Reader Tip - *For more information, please refer to the deployment videos link here - Cloud NGFW YouTube Channel*

Configure Application Based Control (App-ID)

App-ID enables visibility into the applications on the network. you can learn how they work and understand their behavioral characteristics and their relative risk. This application knowledge allows you to create and enforce security policy rules to enable, inspect and block unwanted applications. When you define policy rules to allow traffic, App-ID begins to classify traffic without any additional configuration.

It determines what an application is irrespective of port, protocol, encryption (SSH or SSL) or any other evasive tactic used by the application. It applies multiple classification mechanisms—application signatures, application protocol decoding, and heuristics—to your network traffic stream to accurately identify applications.
When the application is identified, the policy check determines how to treat the application

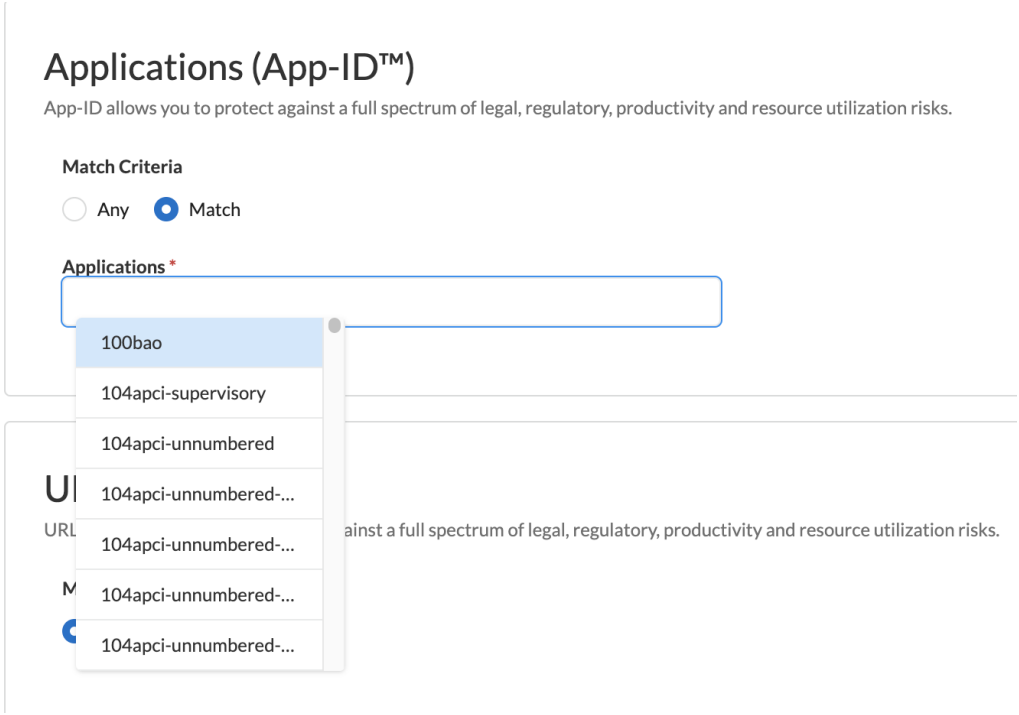
You do not need to create a specific object for App-ID. However, when you create a security rule, you will have the option to specify applications from a drop-down and add them to your rule. Follow the steps below to create application based control.

1. Select **Rulestacks** and select a previously-created rulestack for which you want to create application based filtering policy
2. From the rules page, scroll down to the **Application ID** section
3. Select **any** if you do not want to create any specific app based restriction.
4. Select **Match** if you want to filter based on application.
5. Click on **the text box**
6. Select the Application from the drop down menu
7. Under Protocol and Ports section, select

 ©2022 Palo Alto Networks, Inc

a. **Any** - if you want to block the specific application on any port
b. **Application-default** - if you want to block the application on the default port only
c. **Select** - if you want to use a custom defined port, you can chose this option and specify the port and protocol

8. To implement the App-ID based policy, once you configure the rest of the configuration, define the action and save the rule.



Reader Tip - *For more information, please refer to the deployment videos link here - Cloud NGFW YouTube Channel*

Configure Adv URL-Filtering

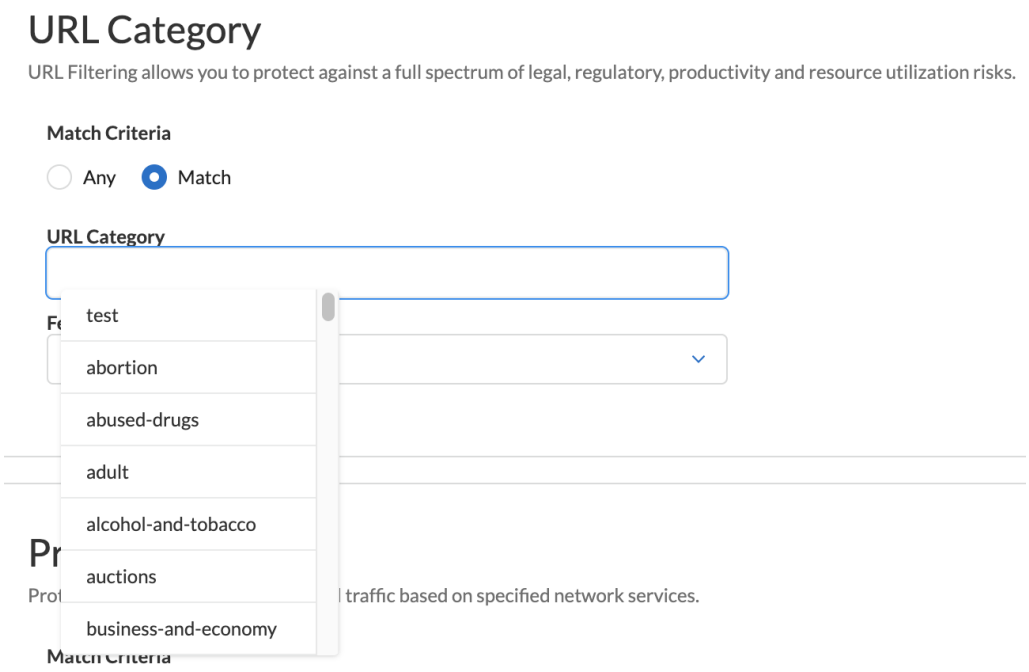
URL filtering limits access by comparing web traffic and providing real time verdict to prevent employees from accessing harmful sites such as phishing pages. It enables secure web access and protection from increasingly sophisticated threats, including malware and phishing sites. Advance URL-Filtering mechanism uses ML to perform highly accurate detection of new and unknown web attacks.
Users have an option to make use of feeds created under Objects to select as a match criteria or use the predefined URL category names.
Follow the steps below to configure URL filtering based policy.

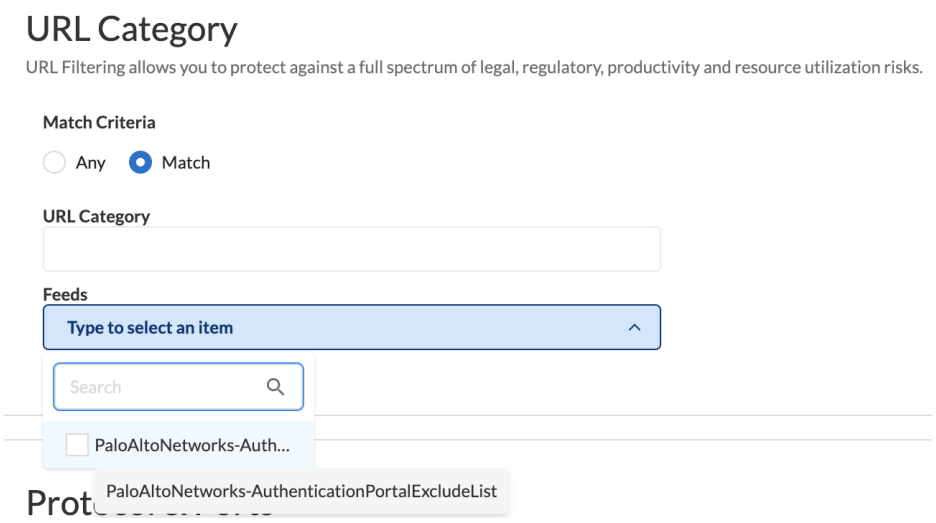
 ©2022 Palo Alto Networks, Inc

Note- *If you want to use Feed as selection criteria for URL filtering, please create the URL feed under **Objects** before proceeding.*

---

1. Select **rulestacks** for which you want to create policy.
2. Click on **create rule**.
3. Scroll down to the **URL Category** Section
4. You can leave Any as an option if you do not want to create specific policy restrictions
5. Select **Match** and choose the option for any feed created or/and URL category available as shown in the figure below. You can scroll the list to make the right selection.
6. You can use custom feed or/and predefined categories.



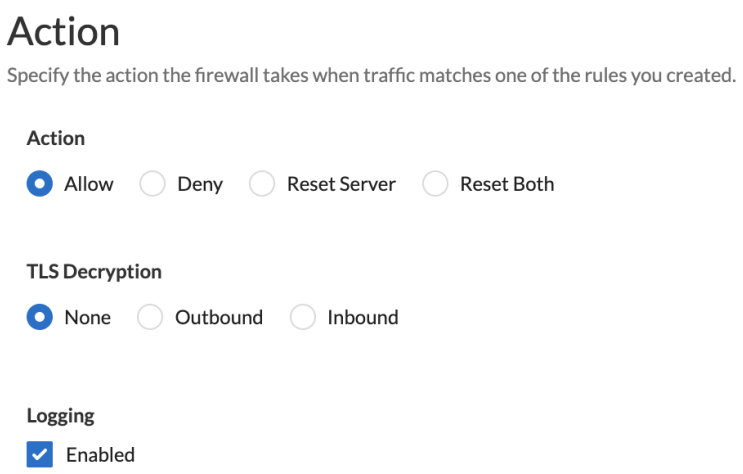


7. Specify the **Action** towards the end of the screen. **Save** and Deploy Configuration for the policy to take effect.

TLS Decryption

Cloud NGFW provides ability to view inside an encrypted packet as it passes the firewall. You can configure NGFW to decrypt and inspect SSL traffic outbound to external sites. NGFW uses certificate to transparently represent client to the server and server to the client. Follow the steps below to enable TLS decryption.

1. Click on Rulestack-Rules-<rulename>. Or create a new rule.
2. Scroll down to the Action section and select to enable TLS decryption.



 ©2022 Palo Alto Networks, Inc

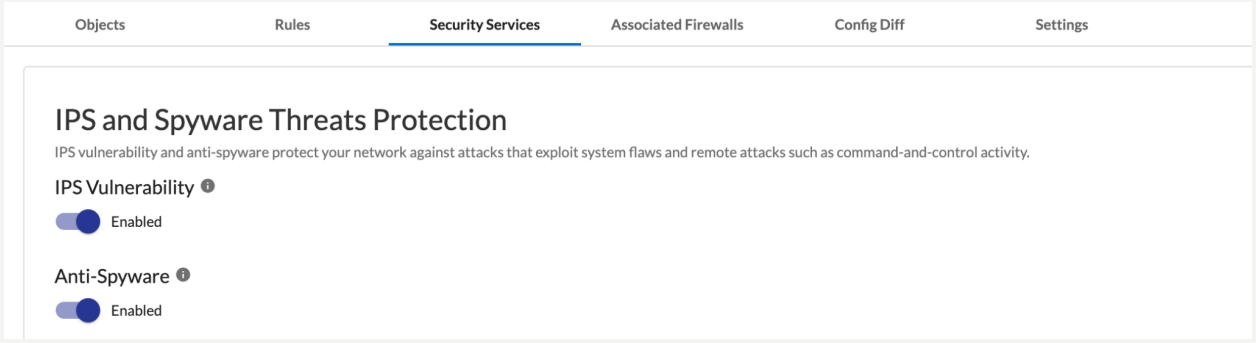
To add a certificate for TLS decryption, you will have to add a certificate from the certificate list under Objects. Refer the certificate list section under Cloud NGFW Security Rule Object

Security Profile

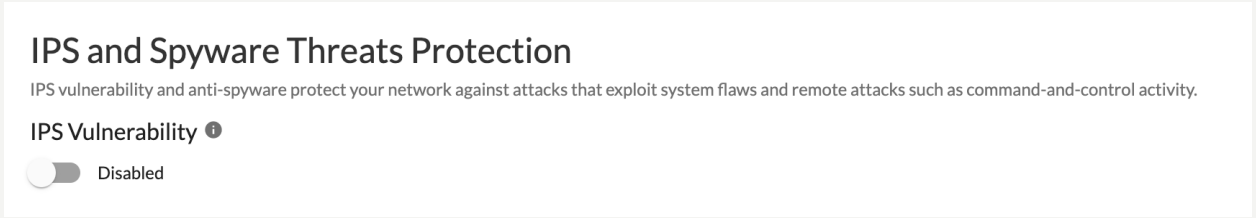
Security profiles provide threat protection capabilities. With security profiles, the allowed applications are further scanned for threats like viruses, malware, spyware and DDos attacks. When traffic matches the allow rule, the traffic is further scanned based on the settings with security profiles. The cloud NGFW provides default security profiles that you can use out of the box to begin protecting your network from threats. Following are the profiles available in Cloud NGFW.

IPS and Spyware Threat Profiles
IPS Vulnerability - Vulnerability Protection profiles stop attempts to exploit system flaws or gain unauthorized access to systems. IPS Vulnerability profiles protect
against threats entering the network. For example, Vulnerability Protection profiles help protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. The default Vulnerability Protection profile protects clients and servers from all known critical, high, and medium-severity threats.
Anti-Spyware - Anti-Spyware profiles blocks spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing you to detect malicious traffic leaving the network from infected clients.

By default these are set to a predefined profile for **Best Practice**.
You can access the security profiles from **<Rulestack Name > -Security Services**



To disable the check, drag to left and save the changes.

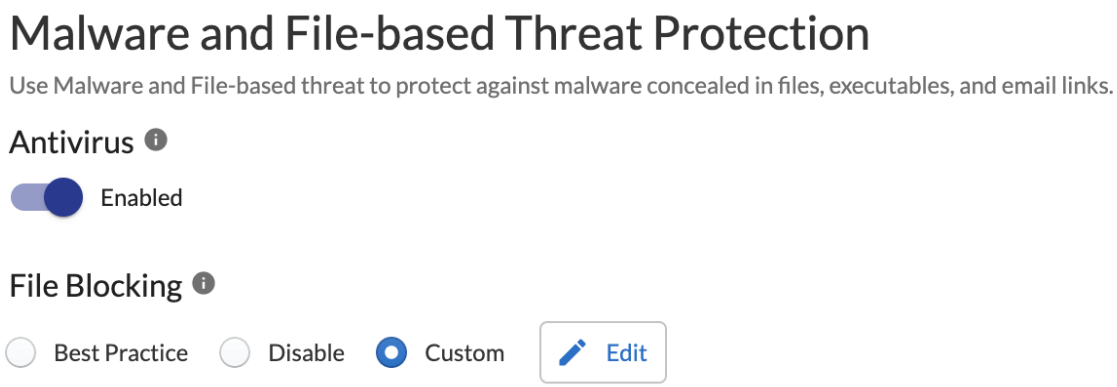


Malware and File-based Threat Protection

 ©2022 Palo Alto Networks, Inc

Antivirus - This service is also enabled and set to 'best practice' by default. Antivirus profiles protect against viruses, worms, and trojans as well as spyware downloads. Using a stream-based malware prevention engine, which inspects traffic the moment the first packet is received, the Palo Alto Networks antivirus solution can provide protection for clients without significantly impacting the performance of the firewall.
File Blocking - file blocking is enabled and set to best practise by default. The cloud NGFW uses file blocking profiles to block specific file types over specified applications and in the specified session flow direction (inbound/outbound/both). You can set the profile to alert or block on upload and/or download and you can specify which applications will be subject to the file blocking profile.
To configure a custom file blocking profile,

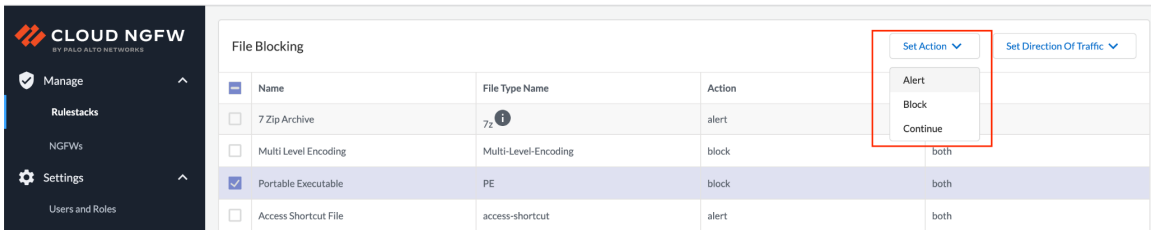
1. Click the dropdown menu under **File Blocking**.
2. Select **Custom** and chose **Edit**

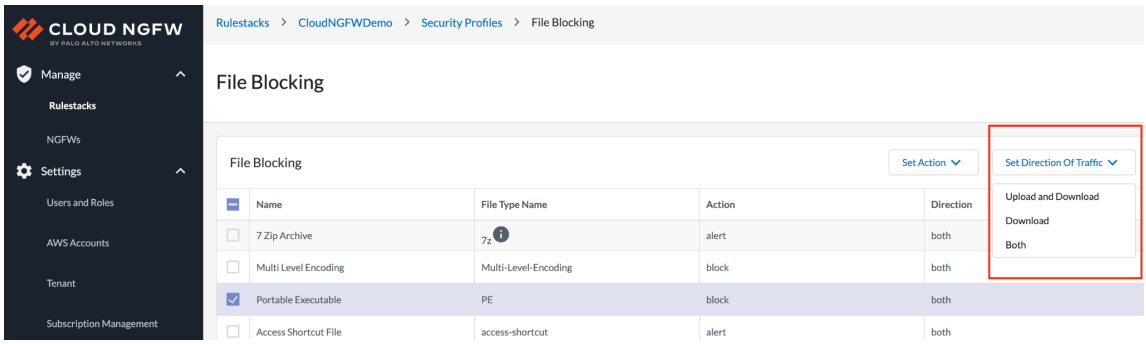


In the edit page , You can view the different file types and default actions.

3. Select the file you want to change the default action for.
4. Click on action drop down, select one of the actions.
    a. **Alert**—When the specified file type is detected, a log is generated in the data filtering log.
    b. **Block**—When the specified file type is detected, the file is blocked and a customizable block page is presented to the user. A log is also generated in the data filtering log.
    c. **Continue**—When the specified file type is detected, a customizable response page is presented to the user. The user can click through the page to download the file. A log is also generated in the data filtering log. Because this type of forwarding action requires user interaction, it is only applicable for web traffic.
5. You can also edit the direction of the traffic flow and associated action. Once you have made your changes, go back to security profiles screen, **Save** and **Deploy Configurations** for the changes to take effect.

 ©2022 Palo Alto Networks, Inc



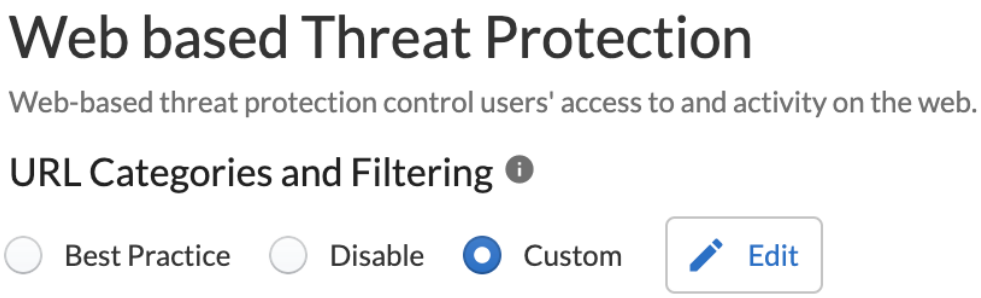


Web based Threat Protection

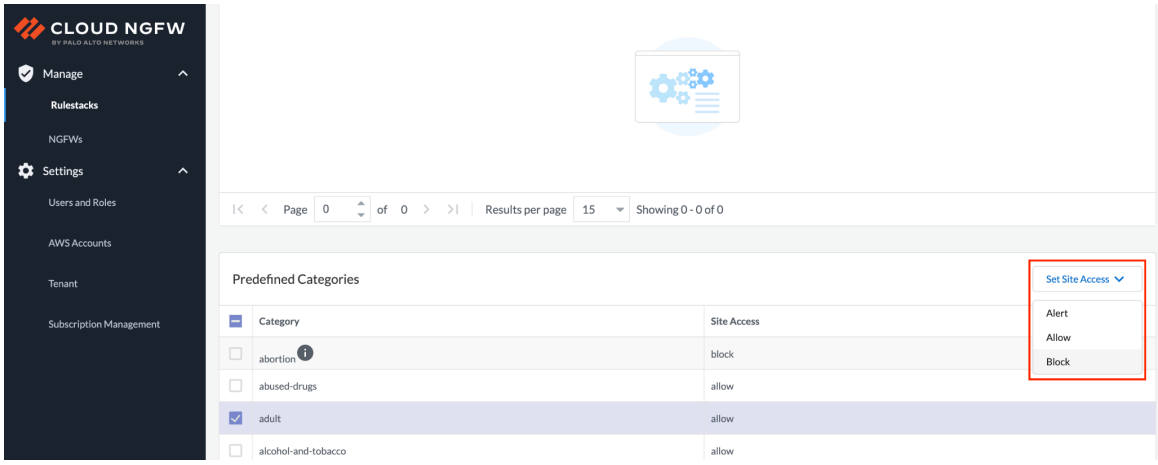
URL Categories and Filtering - URL Filtering profiles enable you to monitor and control how users access the web over HTTP and HTTPS. The cloud NGFW comes with a default profile that is configured to block websites such as known malware sites, phishing sites, and adult content sites. The profile is set to ‘best practices’ by default. You can customize the newly added URL profiles and add lists of specific websites that should always be blocked or allowed, which provides more granular control over URL categories.

To configure a custom profile-

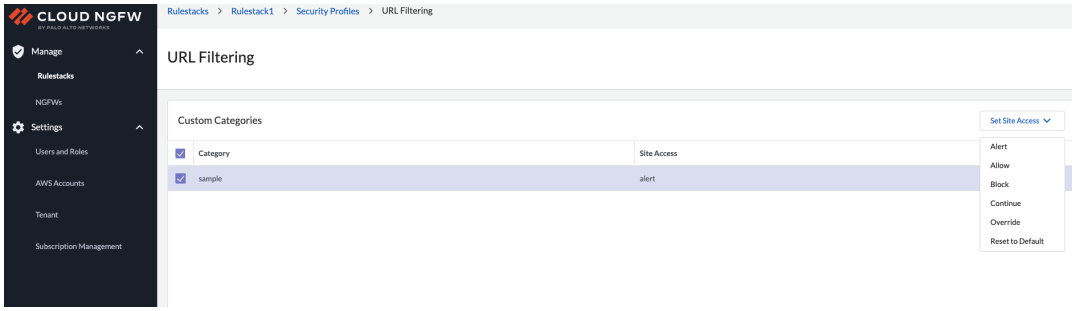
1. Click on custom, and click edit.



2. In the edit window, you can see the predefined categories and the default actions. To change this default action, select the category and change the site access from the options as shown.



3. If you have the custom URL feed object created, you can edit the default behavior and change the site access.



4. Once you have made your changes, **Deploy Configuration**.

Encrypted Threat Protection

Outbound Decryption - Outbound Decryption profile enables you to specify traffic to decrypt by destination, source, service, or URL category, and to block, restrict, or forward the specified traffic according to the security settings in the associated Decryption profile.

Egress decryption requires two certificates—Trust and Untrust. The Cloud NGFW presents the trust certificate to clients during decryption. The Cloud NGFW presents the untrust certificate to the client if the site the client is attempting to connect to, has a certificate signed by a CA that the NGFW does not trust.This procedure only defines the certificates that the firewall uses for Outbound TLS Decryption.

Note-*You must enable Outbound TLS Decryption during rule creation.*

---

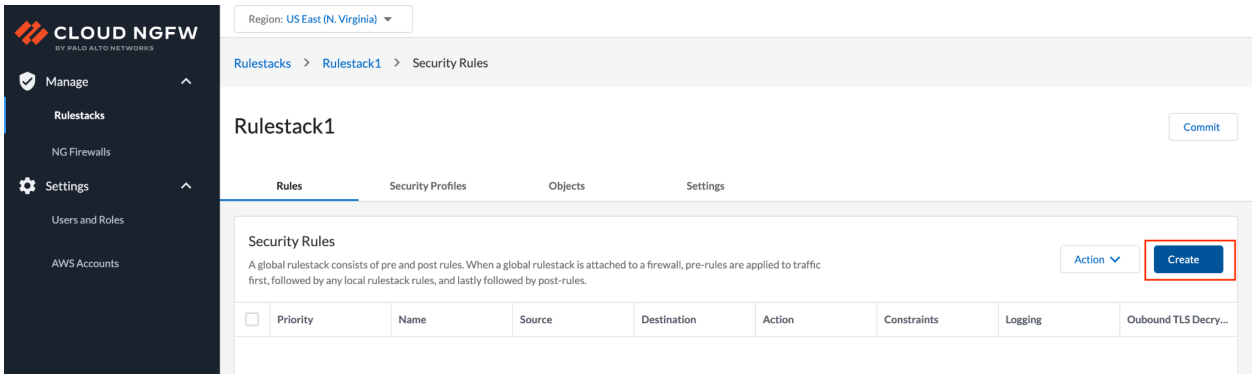
1. To add the certificate, select edit under outbound decryption
2. Select a trust certificate and untrust certificate
3. Save and commit.

 ©2022 Palo Alto Networks, Inc

How to configure Rules

Now that we understand various components, let us configure a rule for the rulestack.
The next step is to create the rules for the rulestack.
There are 4 sections to creating a rule- **General, Source And Destination, Granular Controls and Action**
To create a rule, follow the steps below -

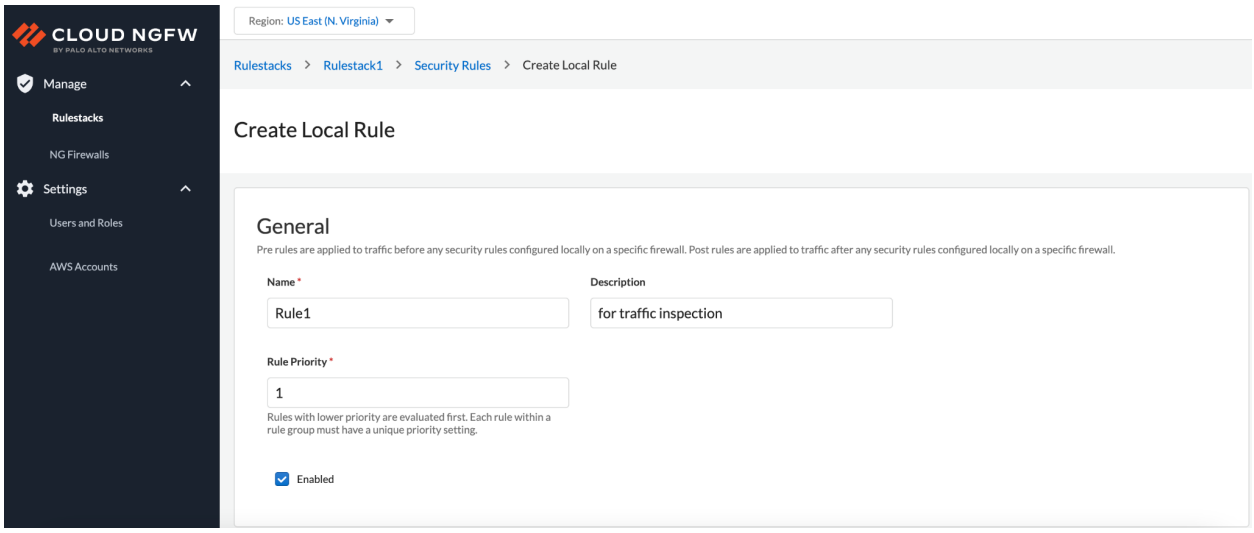
1. Select **Manage** > **Rulestacks** and select the target rulestack for your new rule.
2. Click **Create**. This takes you to the create rule page.



On the Create rule page, enter the details as described in the steps below.

General Section

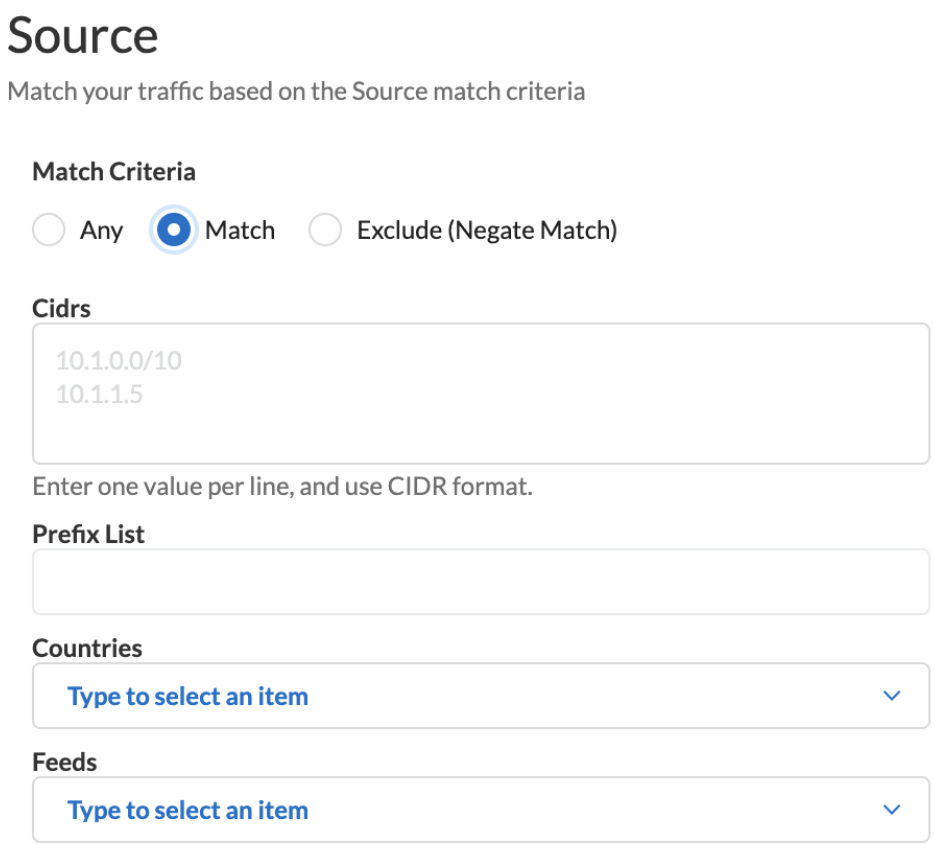
1. Enter a descriptive **Name** for your rule.
2. (Optional) Enter a Description of your rule.
3. Set the **Rule Priority**.
4. *The rule priority determines the order in which the rules are evaluated. Rules with a lower priority are evaluated first. Hence the best practice is to add the strict check rules with least priority.*
5. By default, the security rule is **Enabled**. You can disable the option for the rule to be ignored.



 ©2022 Palo Alto Networks, Inc

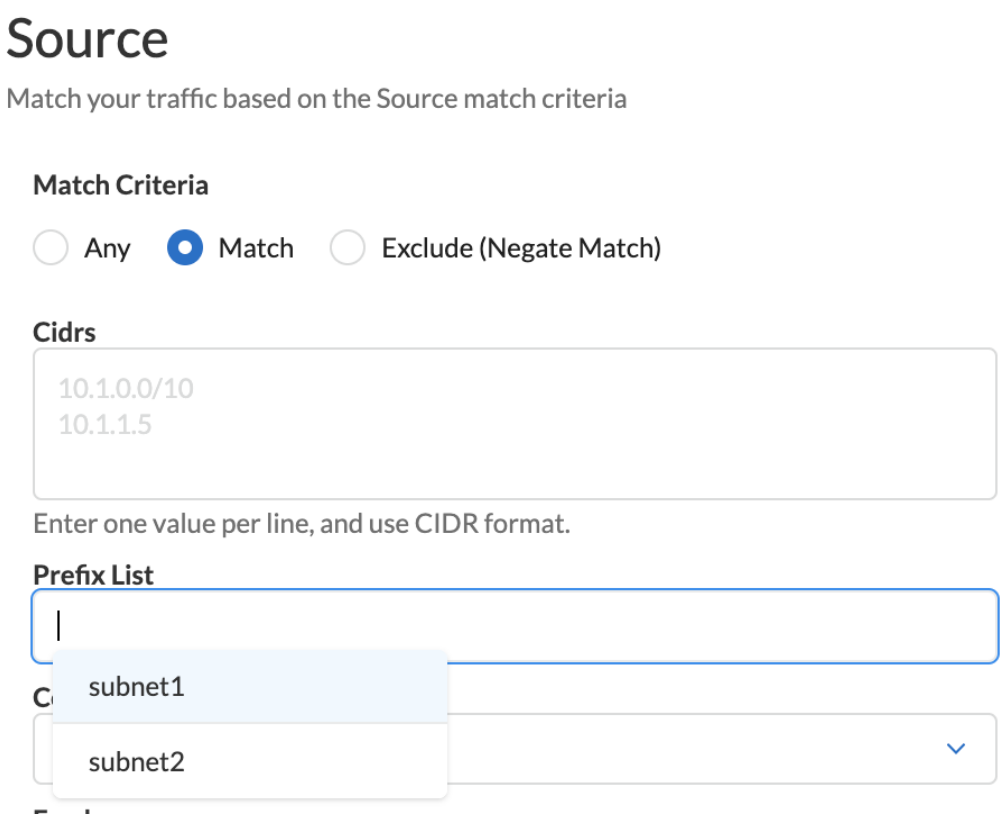
Source And Destination

6. Scroll down to the next section to enter the source and destination match criteria for the rules.
7. Select **'Any'**., if you need to match with any source. For specific match criterias, select **Match** and click the dropdown. Select **Prefix list** from the options.



8. Click the dropdown and select the prefix list which were preconfigured with objects.

 ©2022 Palo Alto Networks, Inc



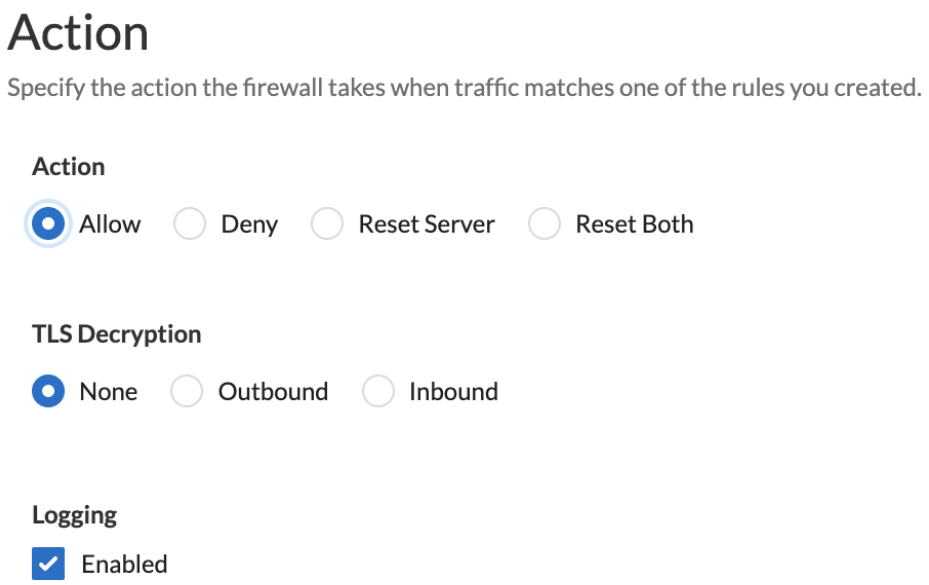
9. Similarly, you can have multiple match criterias of the same or different types. For example, the screen below shows the source match with different categories.

10. Follow the same to configure the destination match.

Action

11. Under the Action section, select the action for the rule, you can disable or enable the TLS decryption and enable logging.

 ©2022 Palo Alto Networks, Inc



12. **Save** the changes and **Deploy Configuration**.

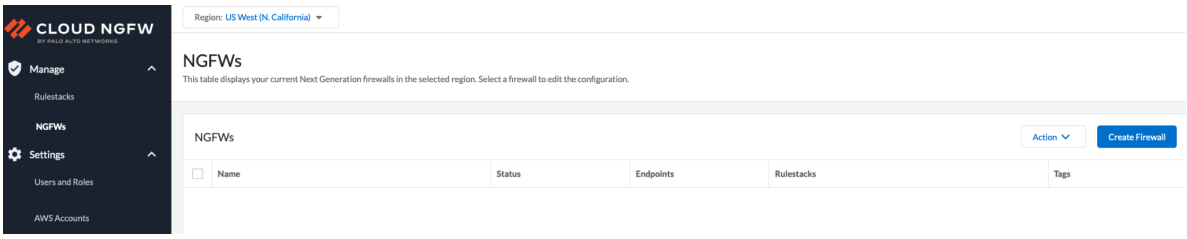
How to Create Cloud NGFW Endpoints

After adding the AWS account to cloud NGFW, you can now start creating cloud NGFW endpoints. The endpoints are deployed in the centralized design, the endpoints are deployed in the centralized security VPC or in individual VPCs in a distributed model.
NGFW endpoints are AWS gateway load balancer endpoints and are responsible for directing the traffic to the NGFW for inspection and checks. In the backend, it deploys two NGFW with default AWS autoscaling .
The endpoints can be created manually or automatically in either of the two ways.
Service-managed deployment- In this method, the endpoint gets created automatically from the cloud NGFW tenant. The user need to specify the subnet and VPC information
Customer-managed deployment- You choose existing availability zones that need to be secured in your specified VPC and then manually create the NGFW endpoints in existing subnets in the chosen availability zones. After the NGFW has been created, you must go to the AWS console to complete the NGFW endpoint creation process.

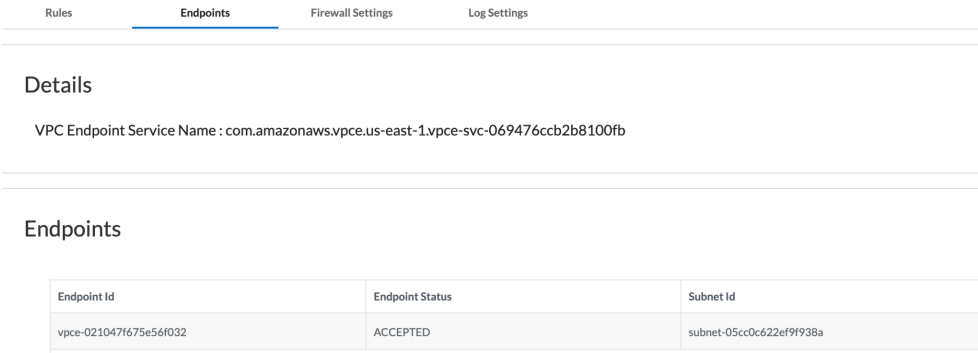
Follow the steps below to configure the endpoints.

1. From the cloud NGFW console, go to **Manage**-**NGFWs**-**Create Firewall**

 ©2022 Palo Alto Networks, Inc



2. Enter a Name, description (optional), Select an AWS account and the VPC in which you want to configure the endpoints.
3. Select a rulestack
4. Under **Specify AWS availability zones and subnets** section, specify whether you want the cloud NGFW tenant to create the endpoint or not.
   Yes - NGFW endpoint is automatically created in the VPC and subnet specified.
   No - User will have to manually create the NGFW endpoints in each availability zone you specify.
5. Click **Create**.
6. If you selected No in step 5, follow the steps below
7. From the cloud NGFW console, select **NGFW** and click on the firewall.
8. Note the VPC endpoint service name.



9. From the AWS VPC console, go to **Endpoints**-**Create Endpoint**
10. Select the VPC endpoint service name you noted in step 8.
11. Select the VPC which you specified during firewall creation
12. Select the subnet for the NGFW endpoint
13. Click **Create**.

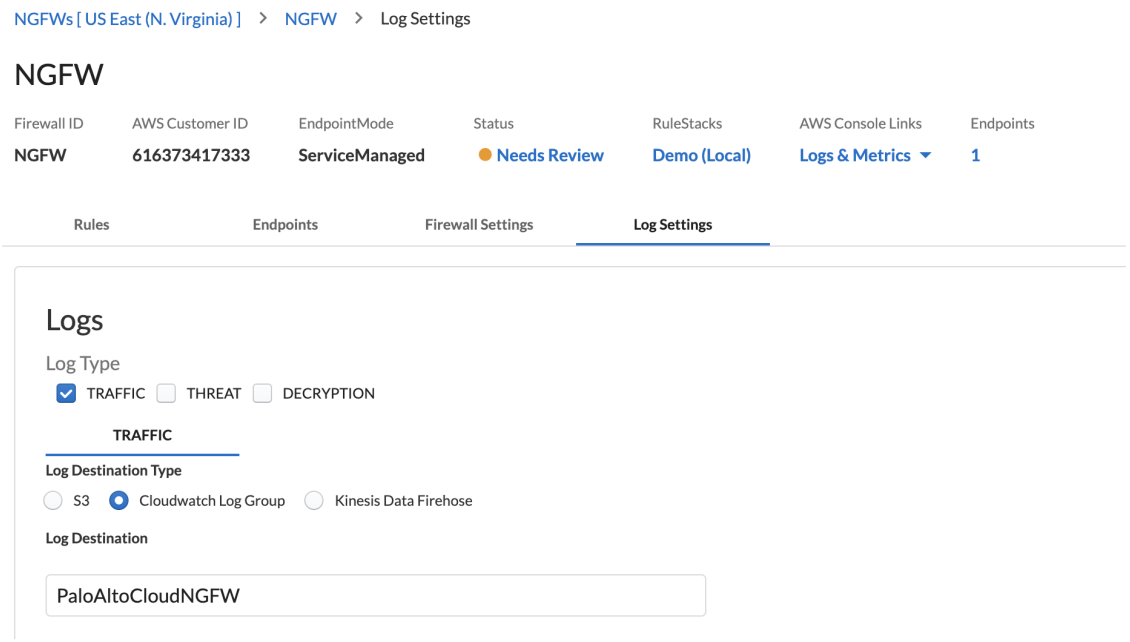
Note- I*t takes 5-10 minutes for the endpoints to be created. After creating the NGFW and NGFW endpoints, AWS route table should be updated to ensure that traffic is routed to NGFW appropriately.*

Reader Tip - *For more information, please refer How-to videos here - Cloud NGFW YouTube Channel*

 ©2022 Palo Alto Networks, Inc

Logging

It is important to log information about the traffic traversing the NGFirewall. A log represents an event within the Cloud NGFW. The logs are generated for the following events.



Traffic - traffic logs contain details with respect to a session. The logs are generated for he start and end of the session.
Threat - Threat logs display entries when traffic matches one of the Security Profiles attached to a security rule on the firewall. Each entry includes the following information: date and time; type of threat (such as virus or spyware); threat description or URL (Name column); alarm action (such as allow or block); and severity level (**Critical,High,Medium,Low,Informational**).
Decryption - Decryption—Decryption logs display entries for unsuccessful TLS handshakes by default and can display entries for successful TLS handshakes if you enable them in Decryption policy.

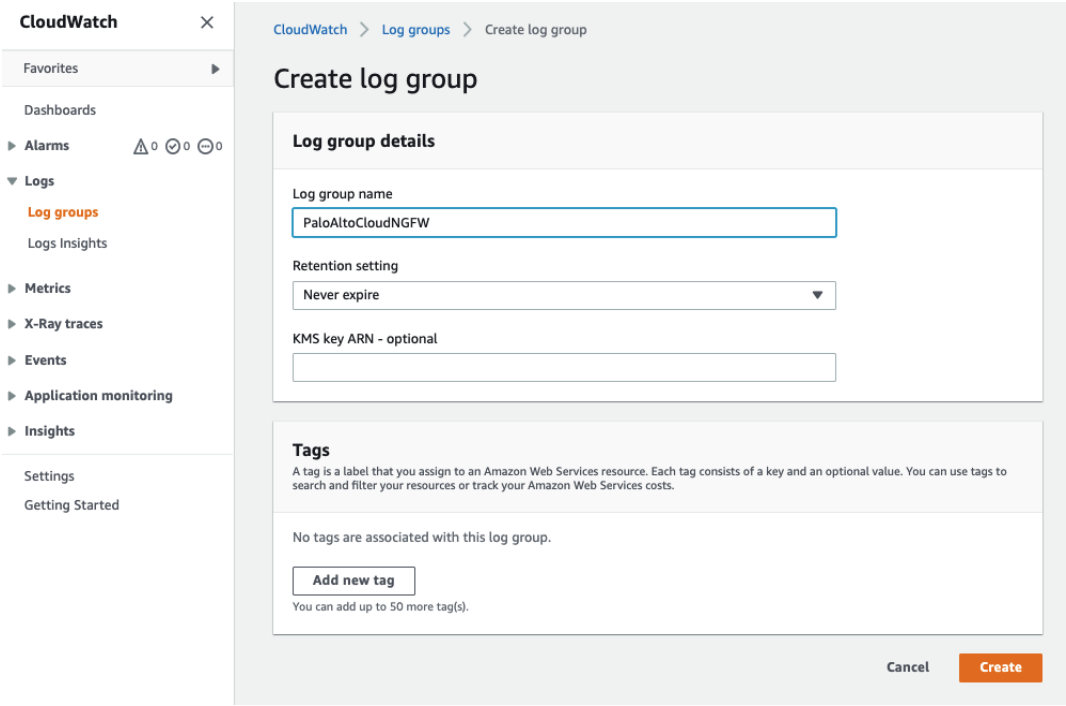
Configure Log Destination in AWS for Cloud NGFW

Users have an option to choose between S3 bucket, Cloudwatch log group or Kinesis data firehose, as destination for Cloud NGFW logs.The log file generated is in JSON file.
If you send log files to a Kinesis Firehose, logs are sent to the stream name that you specify and then to the final destination; such as an S3 Bucket, Datadog, or Splunk. In addition to the log information, each log entry also contains a header that records the date, priority, time, firewall hostname, log type, year, month, day, hour, minute, second, region, firewall name, and AWS account ID. The NGFirewall adds the region, firewall name, and AWS account ID to the logs to

 ©2022 Palo Alto Networks, Inc

help identify where the log was generated because this information is not included in the log file name. You can then download the JSON file for viewing. Follow the below instructions to configure logging with cloudwatch log group.

1. From the Cloud NGFW console, Select **NGFirewall,**click on the firewall created earlier.
2. Go to **Log Settings**
3. Select **Traffic** log type. You can choose more than one log type. If you select more than One log type, you will need to specify the destination separately. For purpose of this Document, we will select only one.
4. For the **Log Destination Type**, select **Cloudwatch Log Group**.
5. Provide the name which you had entered in the section “subscribe to NGFW service” In this document, we used PaloAltoCloudNGFW. Save the changes.
6. From the AWS console, go to **CloudWatch** service.
7. Navigate to **Logs-Log groups**, click **Create log group**
8. Enter the same name you mentioned in the **Cloud NGFW console** (PaloAltoCloudNGFW), leave the rest of the settings to default and click **Create** Cloudwatch logs are ready to receive log now.

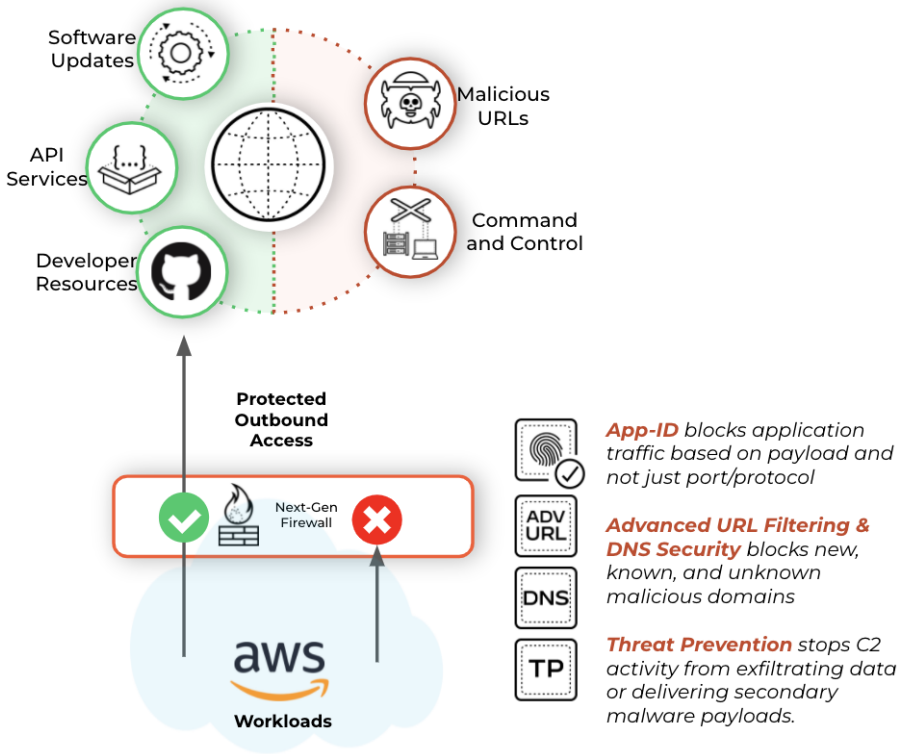


Use Cases

Outbound Traffic Protection from known and unknown threats:

With workloads moving to the cloud, Preventing known threats is paramount. If you know that something on the network is malicious, you must stop it. You can't let identified malware or spyware traverse the environment or let endpoints communicate with known malicious sites.

Outbound access to the internet for cloud applications is critical since there could be a need to access URLs, cloud repositories, resources, and other saas applications. But access to the internet translates to the applications being prone to unknown threats from the ever-evolving threat landscape. While traditional firewalls can provide some protection against web-based traffic, with limited security controls, it is not very effective with various other threat vectors. Hence threat prevention is crucial and can speed the prevention of unknown threats to near real-time.



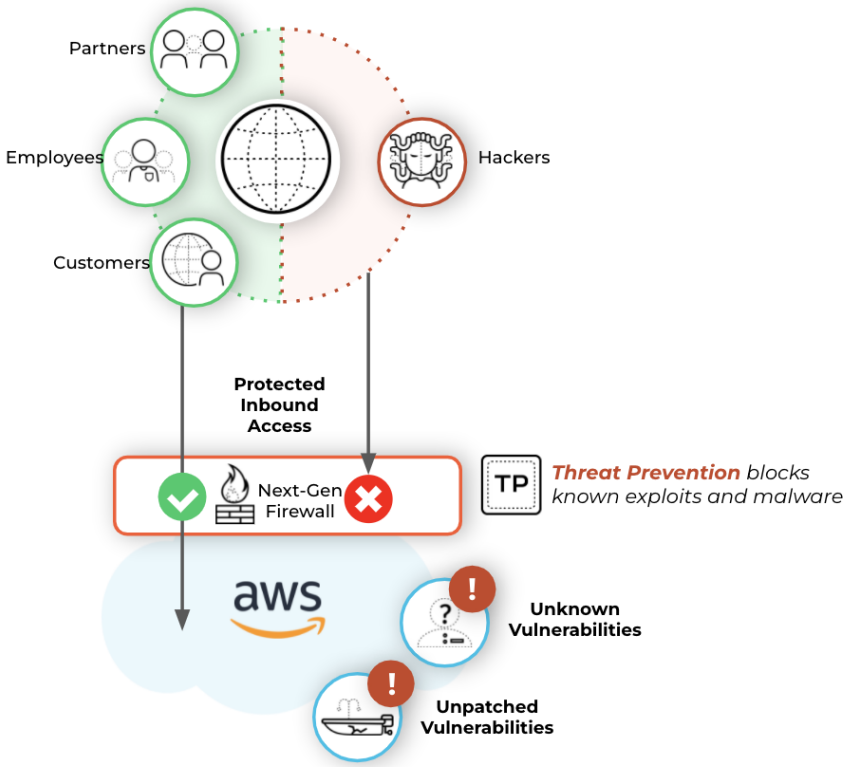
With outbound traffic from cloud workloads to the internet, applying threat prevention policies to allowed apps can help block known threats, including vulnerability exploits, malware, and malware-generated command-and-control traffic. Using ML, unknown and potentially malicious files are analyzed based on hundreds of behaviors. If a file is deemed malicious, a prevention mechanism can be delivered to secure the environment. An intrusion prevention system (IPS) also provides protection based on signature matching and anomaly detection and making sure all allowed traffic is well-intentioned and devoid of evasion techniques. VM-Series firewalls provide URL Filtering to ensure that developers can only access known good repositories
The customer need not depend on a separate IPS device and deploy multiple firewalls. Using Cloud NGFW, the customer gets the benefit of threat prevention from NGFW capabilities. The

 ©2022 Palo Alto Networks, Inc

deployment is with few simple clicks and hence takes operational complexity away. The customer can get the security architecture in place within a few minutes.

Inbound Protection

Attackers today use multiple ways to exploit vulnerabilities and compromise workloads and environments. These include several web-based and non-web-based attacks. Hence it is also critical to provide threat protection against inbound traffic from the internet. While WAF can provide some amount of protection against web traffic, but will not discover threats that exploit open ports (e.g., 80/443) or target vulnerabilities in non-web apps.
Deploying a firewall can provide advanced security controls against these vulnerabilities but it comes with its challenges around deployment complexity. These complexities can introduce delay in securing the cloud workloads.



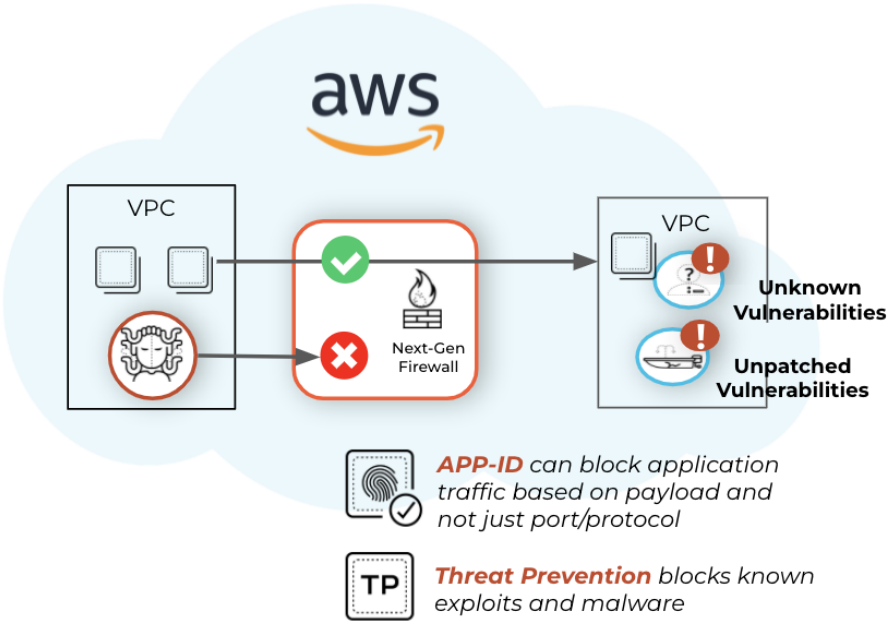
Cloud NGFW, powered by Palo Alto Networks VM-Series firewalls, inspect every inbound packet and block suspicious traffic based on application type or user identity, going beyond simple port blocking to protect traffic over open ports. For ex- you can create and apply threat prevention profiles to the MySQL app-specific policy to prevent app vulnerabilities, SQL injection attacks, and malware. This type of app-specific traffic inspection strengthens your security posture by limiting access based on apps. The service also provides advanced security capabilities, such as intrusion prevention systems (IPS) and sandboxing, to

 ©2022 Palo Alto Networks, Inc

defend against both known and unknown vulnerabilities at the edge of a public cloud environment. The user needs to only input the intent in the UI and the security controls are configured in the backend. This takes away the complexity of deployment and provides cloud security within no time.

East-West Traffic Protection

In a cloud environment, customers can have different VPCs that might contain different app tiers or different apps entirely. E-W traffic is common communication between VPCs in public clouds where high-value database servers, shared cloud servers, development environments, and partner resources are deployed.



Cloud NGFW using the Palo Alto Networks NGFW capabilities can protect the communication between the workloads. The App-ID capability can identify and categorize the applications using various methods. Users can create security policies based on applications to allow only legitimate traffic to flow between the workloads. For example, App-specific policies are used to allow only MySQL traffic to flow between the web server VPC and the database VPC. With threat prevention capabilities, Cloud NGFW can inspect traffic to and from the applications and enforce security measures for required compliance. Being a cloud-native service, this also takes away the complexity associated with configuring legacy firewalls and IPS systems.

 ©2022 Palo Alto Networks, Inc

Deployment Options

Palo Alto Networks provide deployment flexibility for cloud NGFW. Following are the different options available.

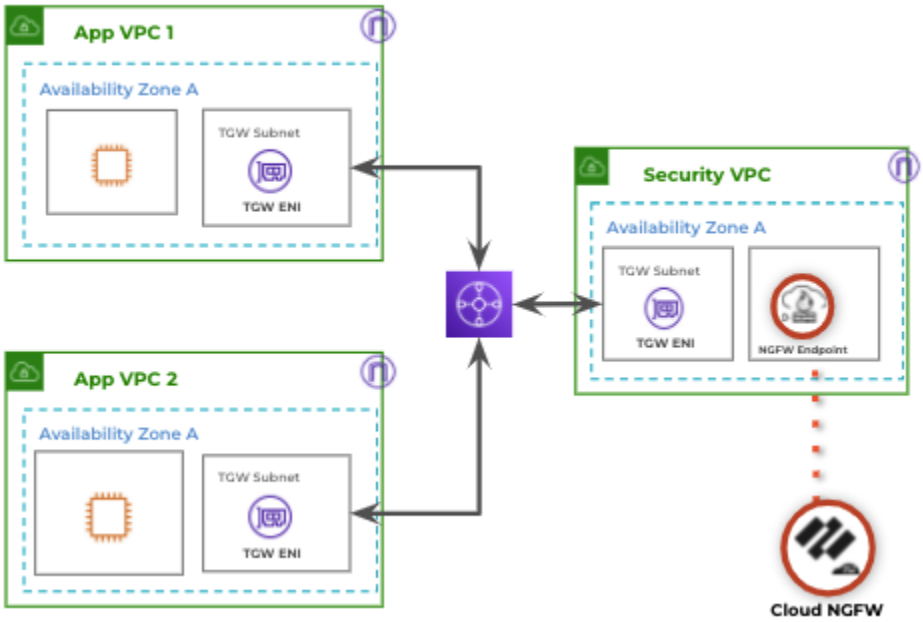
- Distributed Deployment - Cloud NGFW is deployed in each VPC which requires protection.
- Centralized Deployment - Cloud NGFW is deployed in a centralized VPC.AWS transit gateway is configured to provide connectivity between VPCs
- Combined Deployment - combination of centralized and distributed to protect against different traffic types.

Deployment of Centralized Design with Cloud NGFW

In the following sections below, we will walk you through deployment of a centralized design.

Reference Architecture

For the purpose of this document, we will consider the following architecture with centralized deployment with Cloud NGFW. We will be validating east- west traffic flow in this deployment



We will create 3 VPCs. one of the VPC will serve as a centralized security VPC, hosting the Cloud NGFW endpoint. The other two VPCs will host workloads . In this design, the transit gateway acts as the main building block. It provides hub and spoke design for connecting the VPCs and controls how traffic is routed between the VPCs. .

In the following sections we will walk through building this architecture from ground zero.

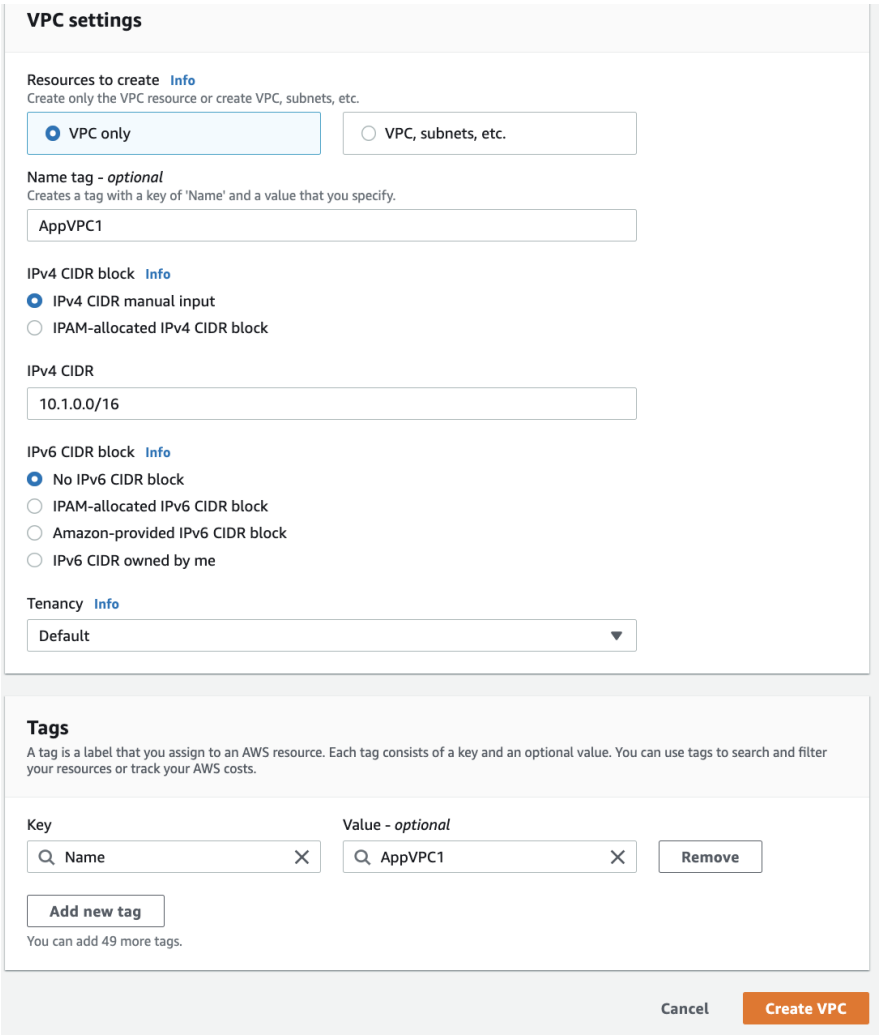
 ©2022 Palo Alto Networks, Inc

Step 1 - Create VPCs, Create Subnets, and Attach Internet Gateway.

We will create 3 VPCs with the following subnets

- AppVPC1 - 10.1.0.0/16
- AppVPC2 - 10.2.0.0/16
- Security VPC - 10.3.0.0/16

1. Open Amazon VPC console and go to your VPCs section and choose "**Create VPC** " from the top right corner
2. Enter the information as shown in the image below to configure the first VPC.and click on **Create VPC.**

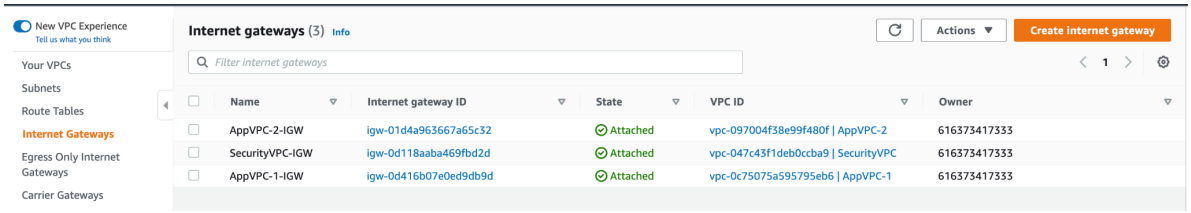


3. Similarly create **AppVPC2** and **Security VPC** with the specified subnet. Creation of VPC takes some time.
4. Once created successfully, it will show as Available.
5. Create Internet Gateway for the VPCs and attach it to the VPCs. This is needed to Provide access to and from the internet for your instances.

 ©2022 Palo Alto Networks, Inc

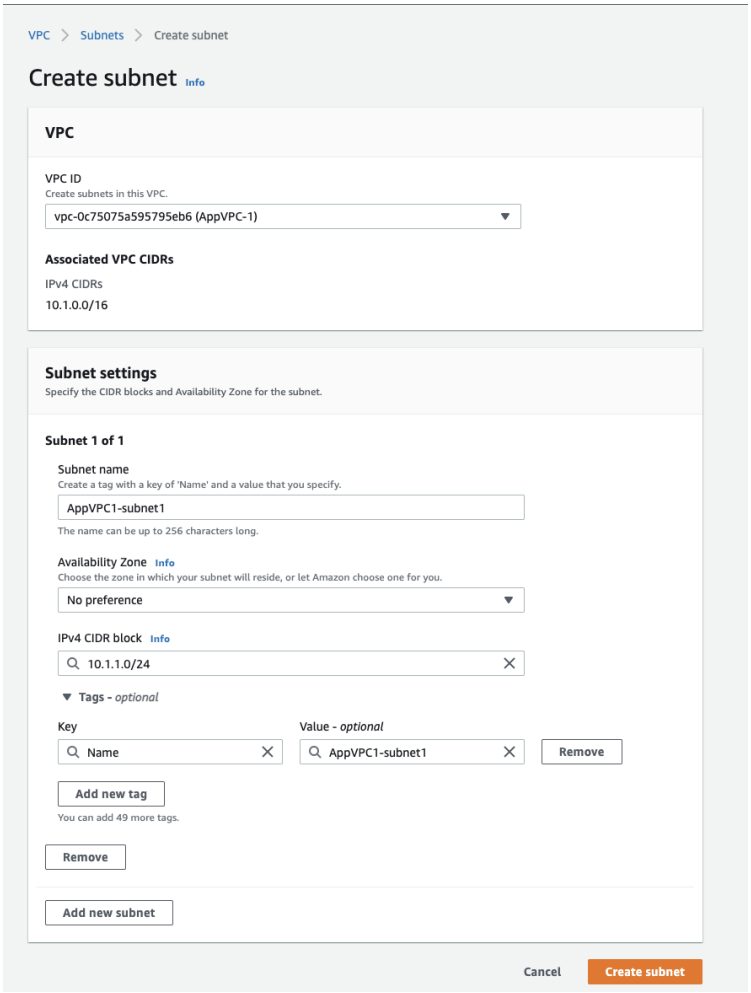
a. From the AWS VPC console, navigate to **Internet Gateway.**
b. Click on **Create internet gateway**.
c. Optionally Name your internet gateway and click on **create internet gateway.**

6. Once the gateway is created, Choose **Actions, Attach to VPC**
   a. Select the AppVPC1.
   b. Repeat the steps for creating and attaching the internet gateway for other two VPCs as shown below.



7. Create 2 subnets each for the 3 VPCs. We need one for the instances and the other one for providing connectivity to the transit gateway.
   a. In the AWS VPC console navigation plan, select **subnets,create subnet**
   b. Select the VPC for which you are creating the subnet.
   c. Provide a user understandable Name for your subnet and enter the CIDR block.
   d. You can leave the remaining settings to default.
   e. Add the 2nd subnet and select **create**

 ©2022 Palo Alto Networks, Inc



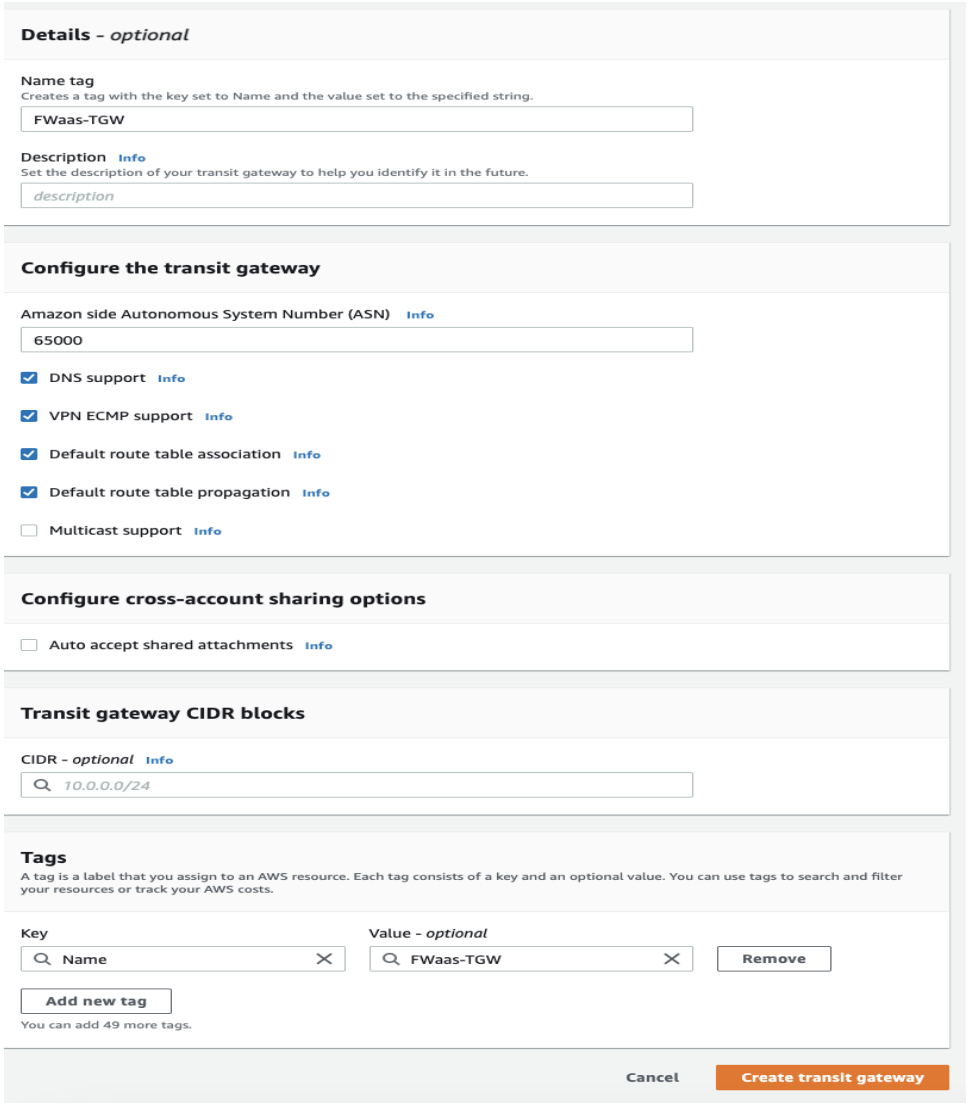
8. Follow the table below for remaining subnets.

Name	VPC	CIDR
AppVPC1-subnet1	AppVPC1	10.1.1.0/24
AppVPC1-TGWsubnet	AppVPC1	10.1.2.0/24
AppVPC2-subnet1	AppVPC2	10.2.1.0/24
AppVPC2-TGWsubnet	AppVPC2	10.2.2.0/24
SecurityVPC-TGWsubnet	SecurityVPC	10.3.1.0/24
SecurityVPC-FWsubnet	SecurityVPC	10.3.2.0/24

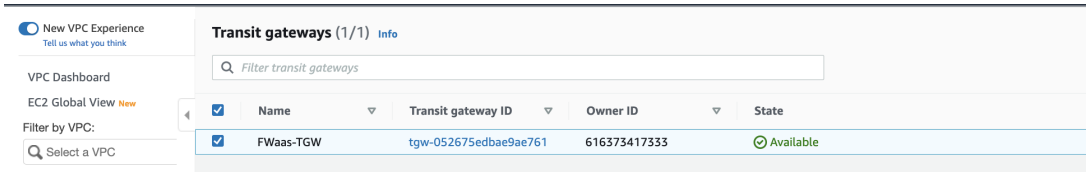
 ©2022 Palo Alto Networks, Inc

Step 2 - Create Transit Gateway and Attachments.

1. From the AWS VPC console, navigate to **Transit gateways, Create transit gateway**
2. In the next screen, enter a user friendly name and ASN number as shown below. You can leave the remaining options default, click **Create transit gateway.**



3. It takes a while for the transit gateway to come to an available state.



4. The next step is to create the Transit gateway attachments for the 3 VPCs. Navigate to **Transit gateway attachments,** and click on **create transit gateway attachment.**
5. Enter a name for the Name tag. Select the transit gateway created earlier for Transit gateway ID.
6. Choose VPC for **Attachment type.**
7. For **VPC ID**, Select AppVPC1
8. Choose **Create transit gateway attachment**.
9. Repeat the steps for creating the attachment for remaining two VPCs as shown in the image below.

 ©2022 Palo Alto Networks, Inc

Details

Name tag - *optional*
Creates a tag with the key set to Name and the value set to the specified string.

TGWattach-AppVPC1

Transit gateway ID Info

tgw-052675edbae9ae761 (FWaas-TGW)

Attachment type Info

VPC

VPC attachment

Select and configure your VPC attachment.

☑ DNS support Info

☐ IPv6 support Info

VPC ID
Select the VPC to attach to the transit gateway.

vpc-0c75075a595795eb6 (AppVPC-1)

Subnet IDs Info
Select the subnets in which to create the transit gateway VPC attachment.

☐ us-east-1a	No subnet available
☐ us-east-1b	No subnet available
☑ us-east-1c	subnet-0a23eddfc12438b3f (AppVPC1-subnet1)
☐ us-east-1d	No subnet available
☐ us-east-1e	No subnet available
☐ us-east-1f	No subnet available

subnet-0a23eddfc12438b3f ✕

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	TGWattach-AppVPC1	Remove

Add new tag

You can add 49 more tags.

Cancel | Create transit gateway attachment

Transit gateway attachments (3) Info

Filter transit gateway attachments

Name	Transit gateway attachment ID	Transit gateway ID	Resource type	Resource ID	State
TGWattch-AppVPC-1	tgw-attach-01ca96fd4f4e77cd7	tgw-052675edbae9ae761	VPC	vpc-0c75075a595795eb6	Available
TGWattch-AppVPC-2	tgw-attach-026ceca29f5a89b62	tgw-052675edbae9ae761	VPC	vpc-097004f38e99f480f	Available
TGWattch-security...	tgw-attach-0eaecdf78da940d47	tgw-052675edbae9ae761	VPC	vpc-047c43f1deb0ccba9	Available

 ©2022 Palo Alto Networks, Inc

Step 3 - Create Security Group, Instances and Allocate Elastic IP

In the steps below, we will create the instances in the VPC attached to the newly created security group.

1. Go to **Instances** in the left navigation plane and select **Launch instances.**
2. In the next screen select **Community AMI Select** the image **ubuntu/images/hvm-ssd/ubuntu-bionic-18.04-amd64-server-20211129**
3. Select **t2.medium** in the next screen and click **Next:configure Instance Details.**
4. Enter the following details in this page, and leave the remaining options default.
    a. **Number of Instances** = 1
    b. **Network** = AppVPC1
    c. **Subnet** = AppVPC1-subnet1 (10.1.1.0)
    d. **Auto-assign Public IP** = Enable
    e. Click **Next:Add Storage**
5. You can leave the options default in this page
6. Add a **Name** tag as AppVPC1-EC2 and click **Next:Configure Security Group**
7. Select Create a new security group. **Name** it "EC2-AppVPC1-SG"
8. Add the rules as below-

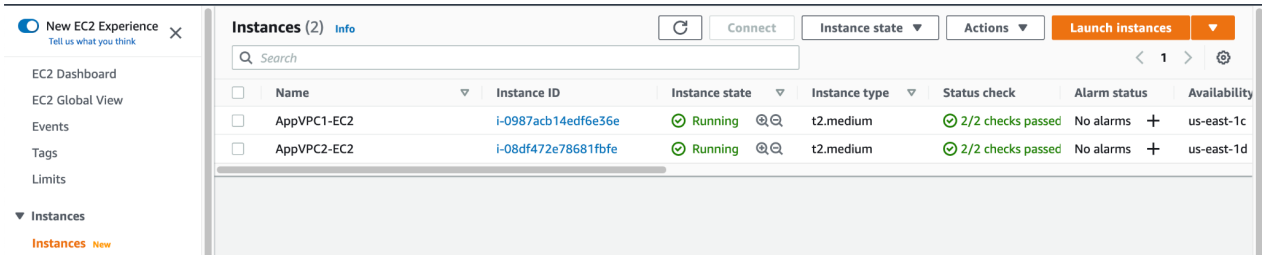
Type	Protocol	Port Range	Source
SSH	TCP	22	0.0.0.0/0
Custom TCP	TCP	8888	10.2.1.0/24
Custom TCP	TCP	1389	10.2.1.0/24
All ICMP-IPv4	ICMP	All	0.0.0.0/0

9. Click Review and Launch .
10. Similarly launch a second EC2 instance in AppVPC2 with subnet AppVPC2-subnet1. Create a new security group for the second instance as below.

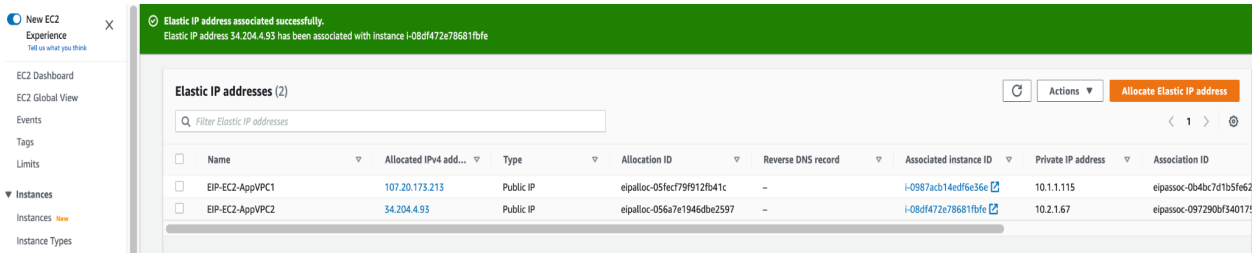
Type	Protocol	Port Range	Source
SSH	TCP	22	0.0.0.0/0
Custom TCP	TCP	8080	10.1.1.0/24
All Traffic	TCP	All	0.0.0.0/0

11. It will take some time for the instances to show in the "Running" state.

 ©2022 Palo Alto Networks, Inc



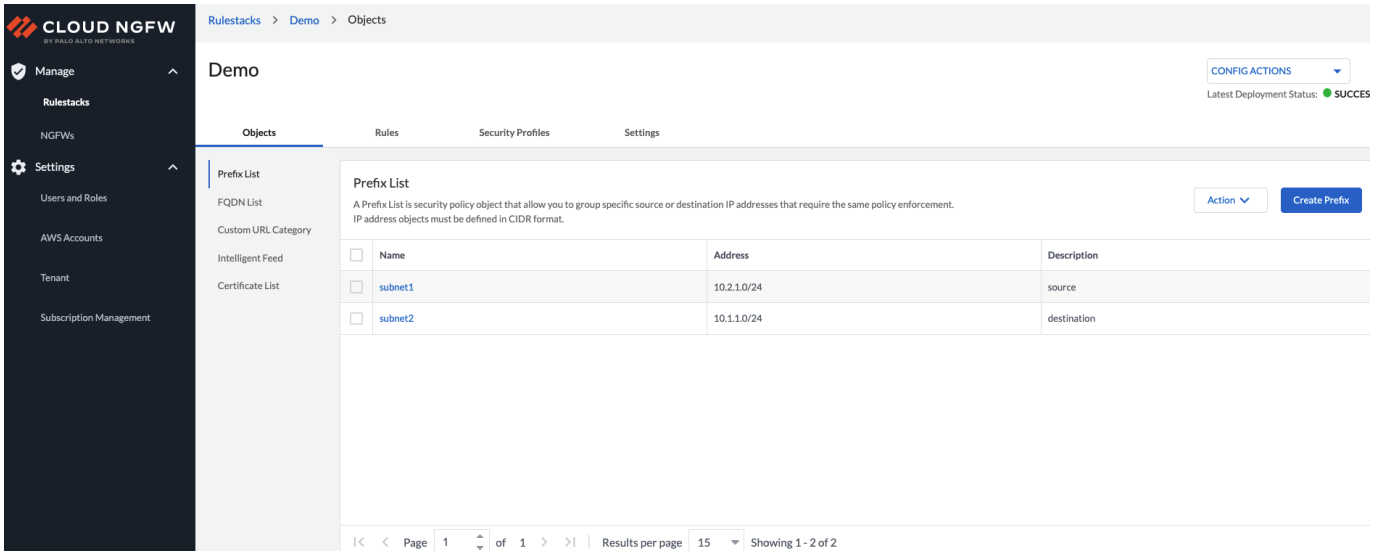
12. You can now assign Elastic IPs to the two instances created.
    a. Go to **Elastic IPs** under **Network & Security** in AWS EC2 console.
    b. Click on **Allocate elastic IP.**
    c. Add a **Name** tag as EIP-EC2-AppVPC1, Click **Allocate**
    d. Click on **Allocate**, **Associate Elastic IP address**
    e. In the next screen, **Resource type** as instance, **Instance** as AppVPC1-EC2,
    f. Select the Private IP address, click **Associate**
    g. Repeat the steps for elastic IP for second instance on VPC2



Step 4 - Configure Cloud NGFW endpoint, Security RuleStack.

Make sure you have subscribed to the Cloud NGFW service, added the AWS account and roles assigned are of LocalRuleStackAdmin and LocalFirewallAdmin.

1. In the first step, we will create the Rulestack.
    a. From the cloud NGFW consol, go to **Manage-Rulestacks-Create Rulestacks-Local**.
    b. Name it Demo and **Save** it.
    c. Click on the rulestack created, select **Objects** tab.
    d. Create **objects** of type **Prefix List** as shown below.



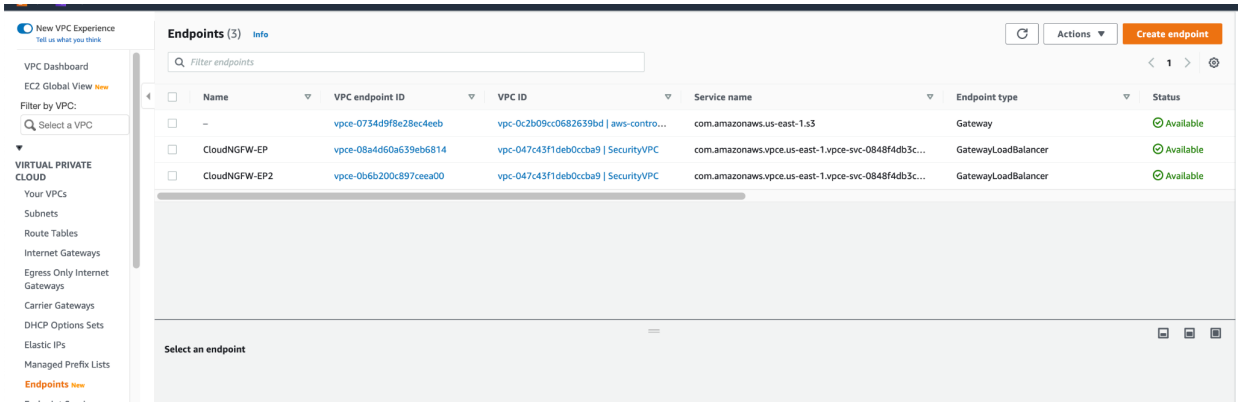
e. Go to the **Rules** tab and click **Create**.
f. Enter the **Name 'EWtrafficRule"**, **rule priority** as 1 and select Enabled.
g. In the next section, select **match** for source and select subnet1 as prefix list.
h. Select **match** for destination and select subnet2 as destination prefix.
i. Select **Allow** under **Action**, enable the logging checkbox
j. **Save** the rule.
k. Go to **Security Profiles** tab and make sure **IPS and Spyware threat protection Malware and File-based Threat Protection** is set to Best Practice.
l. Click on **Save**

2. In this step, we will configure the NGFW.
   a. Go to **Manage-NGFWs-Create Firewall**
   b. Under **General** section, enter
      i. **Name** - NGFW
      ii. **AWS Account** - account ID attached to the console.
      iii. **VPC**- Security VPC.
   c. Select the Rulestack 'Demo' created earlier.
   d. Under **AWS availability Zones & Subnets**, select **Yes** to create firewall endpoints. Select the firewall subnet created earlier (10.3.2.0/24).
   e. Click **Save**. You will see the status turning to **Creating** state. This process will approximately take 10-15 min to complete.
   f. The state should turn to Create_Complete

3. Click on the NGFW created above. Go to **Endpoints** tab. And notice the VPC Endpoint service name under Details section.

4. Go to VPC Dashboard in AWS console and click on Endpoints. You will notice the endpoint created.

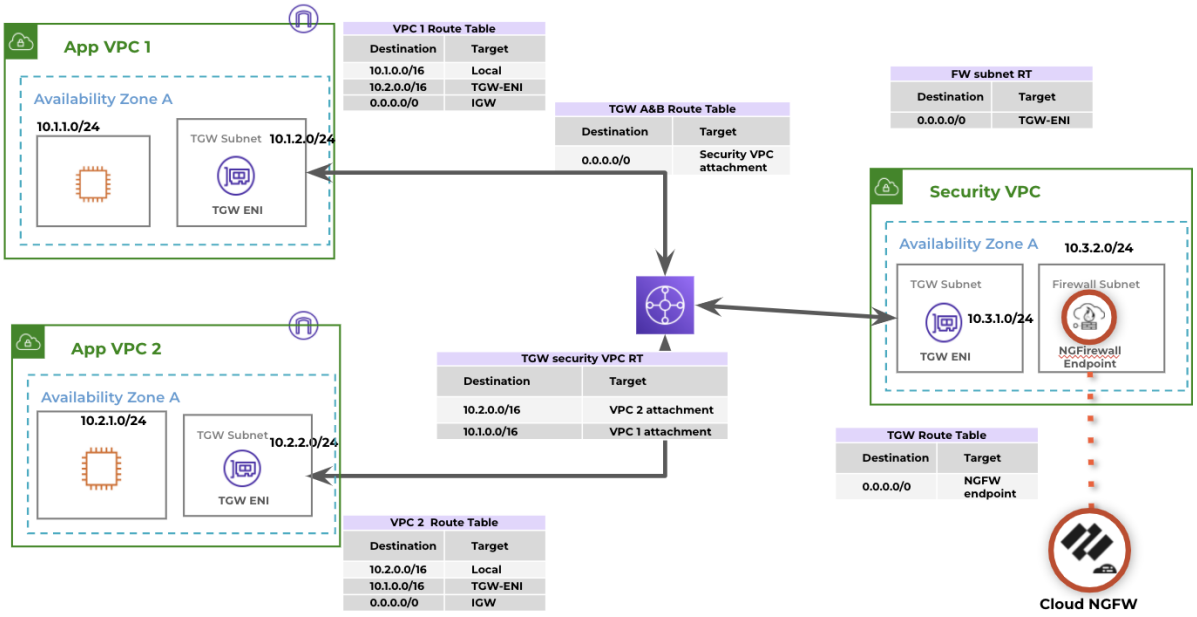
 ©2022 Palo Alto Networks, Inc



Step 5 - Configure Route Tables and Routes for VPCs and Transit Gateway

In the following steps we will define how the traffic gets forwarded from VPC. We will configure routing with **centralized design for East-West traffic** between the VPCs.

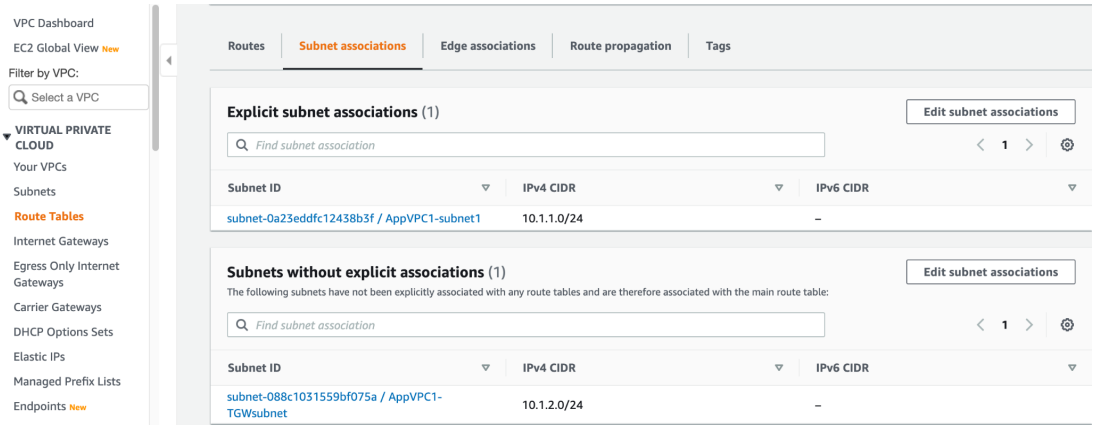
Consider the topology below for the sample routing configuration



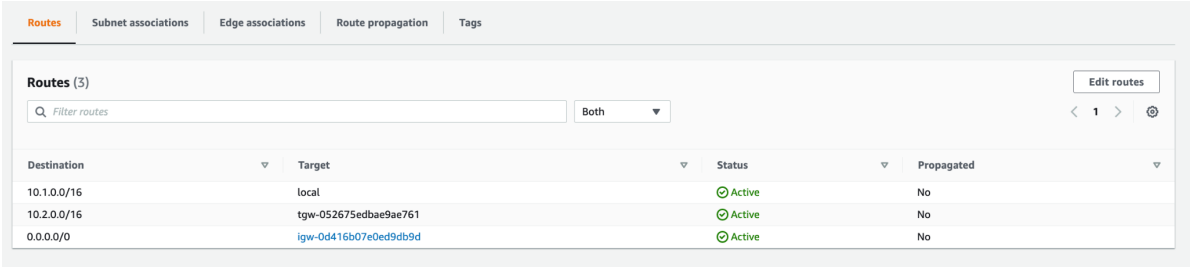
A. Create route table for AppVPC1, AppVPC2 and Security VPC

1. From the AWS VPC console, navigate to **Route Tables**, select **Create route table**
2. Give a name as AppVPC1-RT, VPC as AppVPC1, add the tag ,click **Create route table**
3. From the **Route Tables** page, click on the route table created.
4. Scroll down and click **subnet associations**, **Edit subnet associations**

5. In the **Explicit subnet associations**, select the instance subnet (10.1.1.0/24)
6. Under **subnets without explicit associations**, select the transit gateway subnet (10.1.2.0/24)

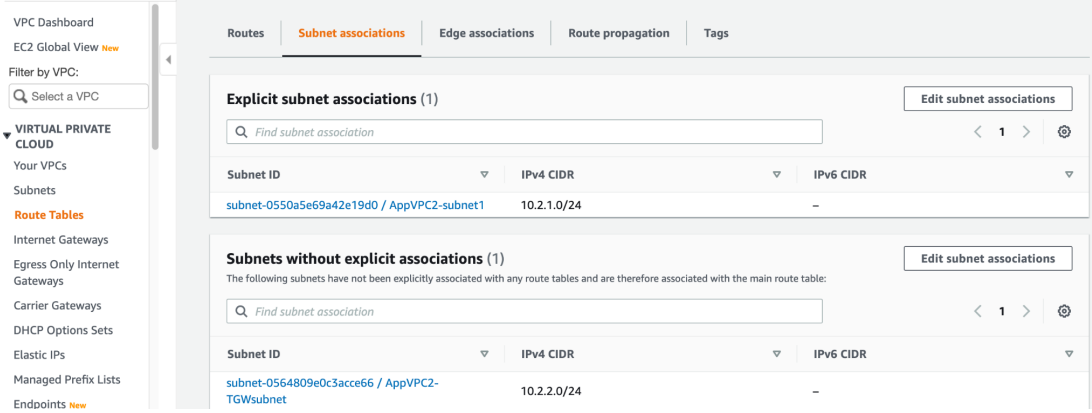


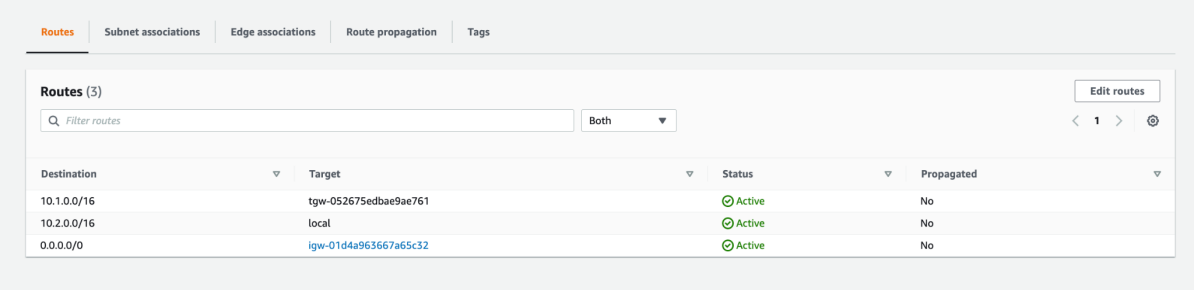
7. Go to the Routes tab and add the routes as below. Here, we are specifying-, any traffic towards VPC2 subnet should traverse via the transit gateway attachment.



i.

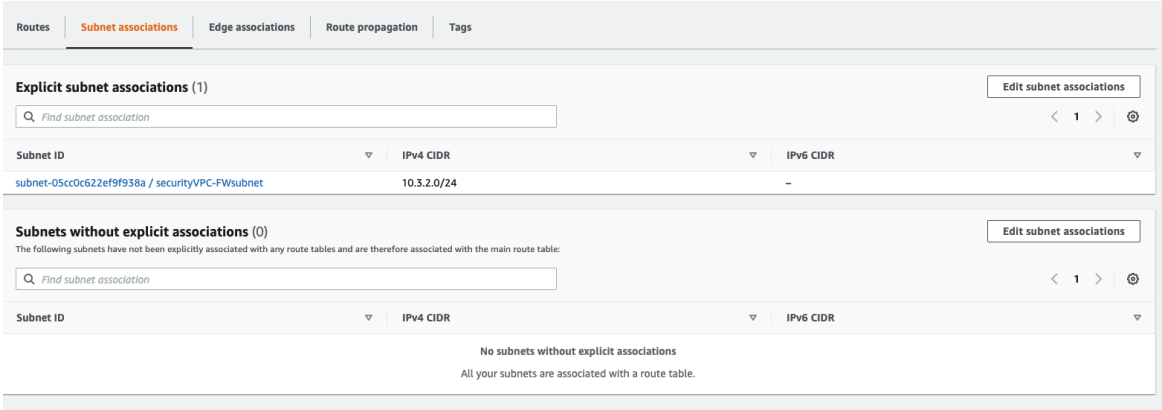
8. Similarly, create a Route table AppVPC2-RT for AppVPC2, with subnet association and routes as shown below.



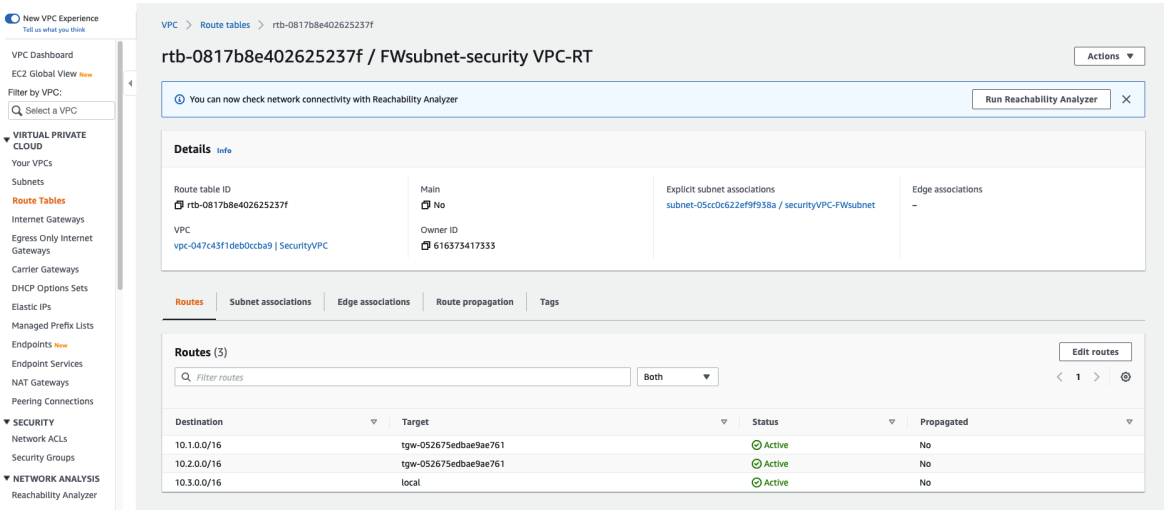


9. Next, we add the routes for our security VPC. We need two route tables here as mentioned in the diagram above.

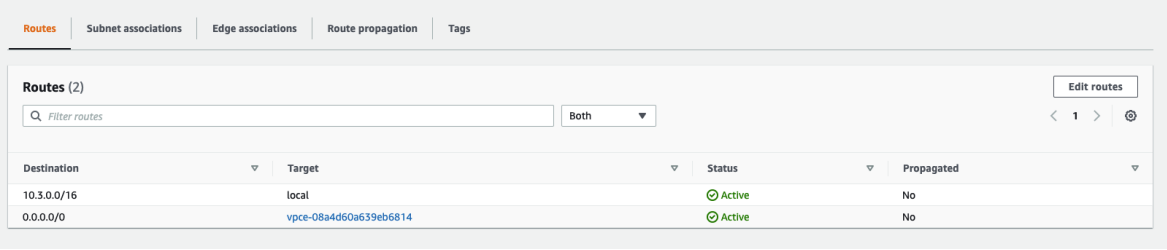
    a. Add the first route table for the firewall endpoint subnet. Name is FWsubnet-security VPC-RT. This route table says that any traffic towards VPC1 or VPC2 subnet should go via the transit gateway attachment of securityVPC.
    b. Associate it with the FW subnet.

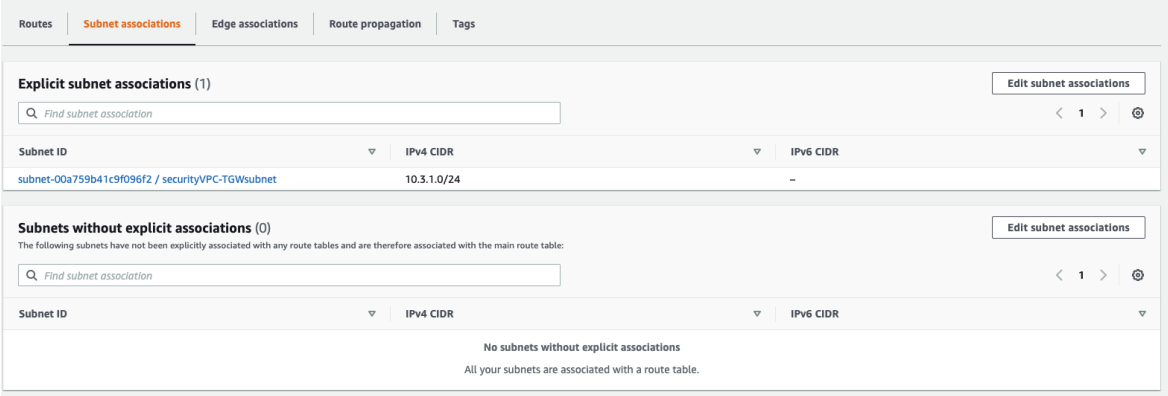


=



c. Add the second route table to forward all the traffic to the FW endpoints.Here the target will be the endpoint created in step 4 . This will be of type Gateway Load Balancer endpoint

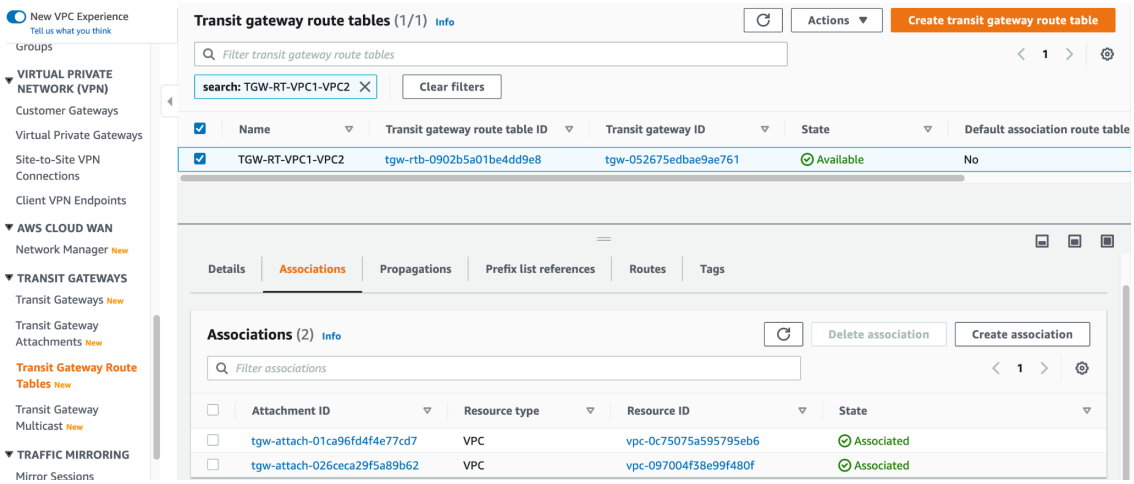




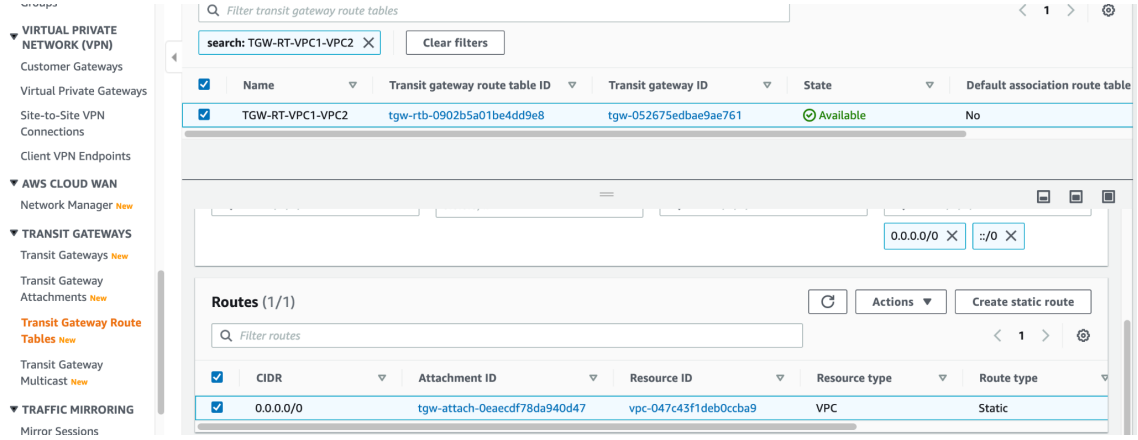
B. Now we need to create transit gateway route table

The first route table will be associated with AppVPC1 and AppVPC2. We want any traffic originating from the two VPCs to be inspected. Hence we want the transit gateway to send it to the security VPC which hosts the NGFW. The Path for this traffic will be the transit gateway attachment for security VPC.

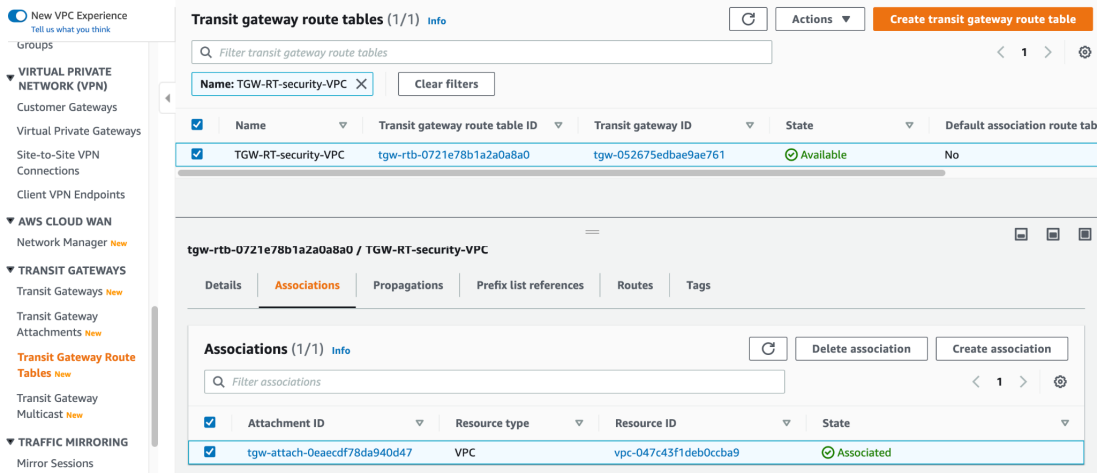
1. Select **Transit Gateway Route Tables**, **Create transit gateway route table** in AWS VPC console.
2. In the next screen, enter **Name** and **Tag** as TGW-RT-VPC1-VPC2 and click on **Create transit gateway route table**.
3. Create the association with transit gateway attachment of VPC1 and VPC2 as shown below.



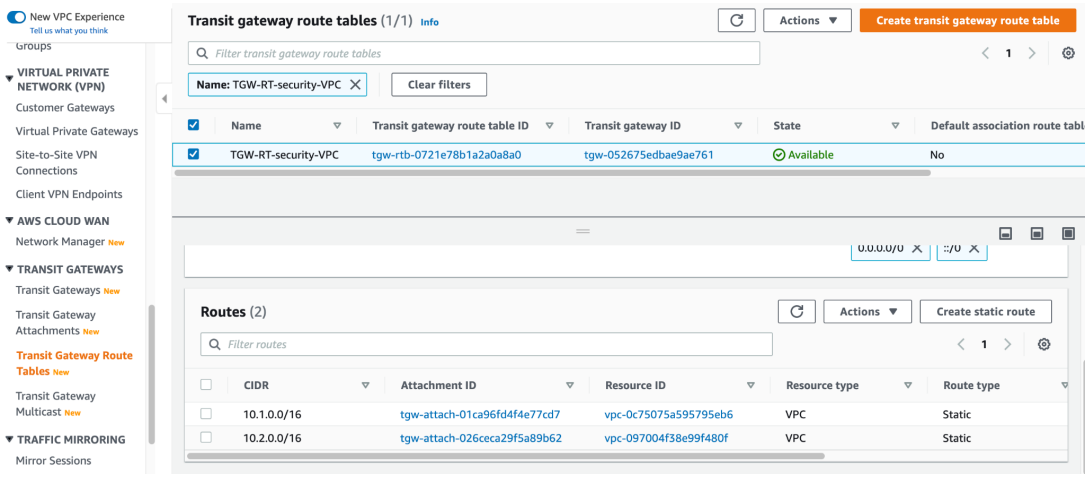
4. Add the default route pointing to the transit gateway attachment for security VPC.



5. Add the second route table for the security VPC in TGW RT.
6. Create a transit gateway route table and Name it TGW-RT-security-VPC
7. This route table will be associated with the transit gateway attachment of security VPC as show below.

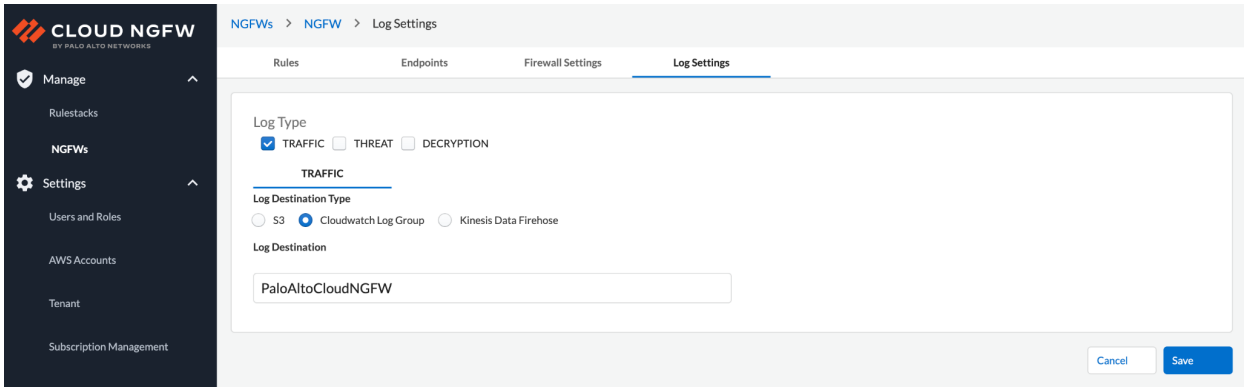


8. Routes would be such that, any traffic to VPC1 subnet should traverse via the transit gateway attachment of VPC1, and any traffic for VPC2 subnet should traverse via the transit gateway attachment of VPC2, as shown below.

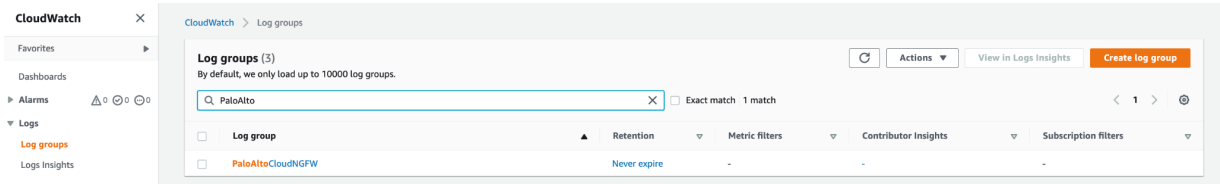


Step 6 - Configure Logging Settings

1. Follow the steps below to enable logging settings for the cloud NGFW.
2. Go to **Manage-NGFWs--<NGFW name>-settings.**
3. Select **log type** as **Traffic**, destination as **Cloudwatch log Group** and LogDestination as **PaloAltoCloudNGFW**



4. Make sure to create this cloudwatch log group from the AWS CloudWatch console. Refer the Logging section below for more details.



Validation

1. Connect to the EC2 instance in App VPC 2 using its Elastic IP and the secret key generated earlier using the command below.

   ssh -i <key> ubuntu@<elastic IP>

2. From the console, try to ping the private IP address of the instance in App VPC 1. You can find the private IP from the EC2 console under details tab
3. You would see successful ping traffic.

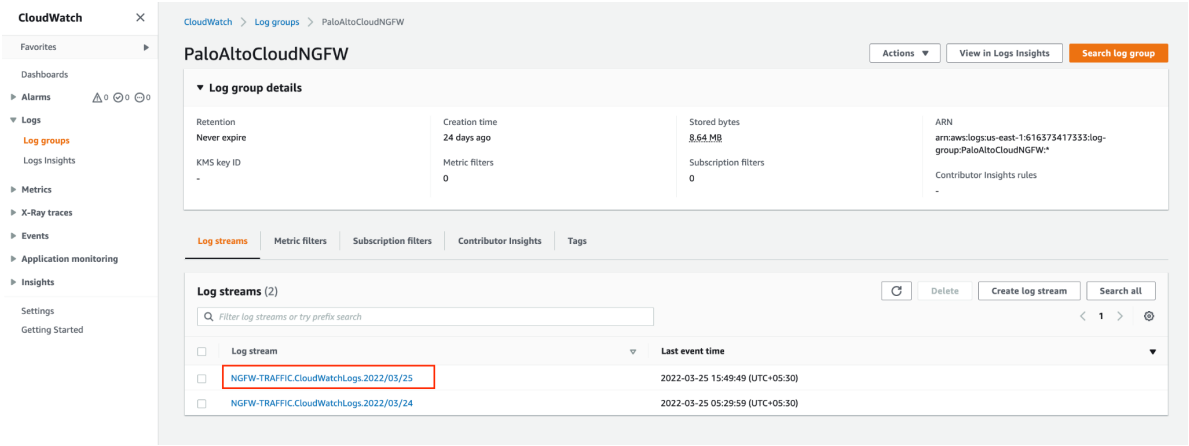
```
To see these additional updates run: apt list --upgradable

New release '20.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** System restart required ***
Last login: Fri Mar 25 10:22:18 2022 from 49.207.199.31
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-2-1-67:~$ ping 10.1.1.115
PING 10.1.1.115 (10.1.1.115) 56(84) bytes of data.
64 bytes from 10.1.1.115: icmp_seq=1 ttl=60 time=54.9 ms
64 bytes from 10.1.1.115: icmp_seq=2 ttl=60 time=10.3 ms
64 bytes from 10.1.1.115: icmp_seq=3 ttl=60 time=3.65 ms
64 bytes from 10.1.1.115: icmp_seq=4 ttl=60 time=2.85 ms
```

4. Go to AWS Cloudwatch console and click on **Logs**-**Log Group.** Click on the log group **PaloAltoCloudNGFW**
5. Click on the most recent traffic stream.



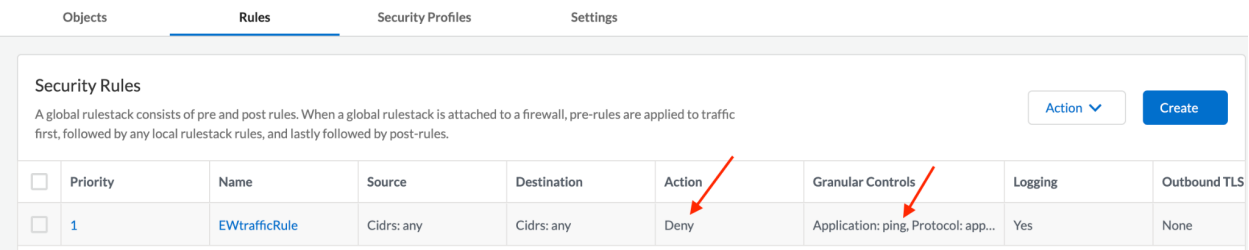
6. Check the log at the latest timestamp. Use filter to search with destination.
7. In the log, check the message section to verify the source IP,destination IP, rule hit, application, bytes sent and received and action.

 ©2022 Palo Alto Networks, Inc

```
2022-04-05T17:35:07.000+05:30        {"src_ip":"10.2.1.67", "sport":

{
    "src_ip": "10.2.1.67",
    "sport": "0",
    "dst_ip": "10.1.1.115",
    "dport": "0",
    "proto": "icmp",
    "app": "ping",
    "rule": "EWtrafficRule",
    "action": "allow",
    "bytes_recv": "392",
    "bytes_sent": "392",
    "pkts_received": "4",
    "pkts_sent": "4",
    "start_time": "2022/04/05 12:04:52",
    "elapsed_time": "0",
    "repeat_count": "4",
    "category": "any",
    "src country": "10.0.0.0-10.255.255.255",
    "dst country": "10.0.0.0-10.255.255.255",
    "session_end_reason": "aged-out",
    "xff_ip": ""
}
```


8. Edit Rule1. Select Ping from App-ID section and set the action to **Deny**.



9. Repeat the test and observe that the request does not go through. Verify the logs from cloudwatch log group.

```
ubuntu@ip-10-2-1-67:~$ ping 10.1.1.115
PING 10.1.1.115 (10.1.1.115) 56(84) bytes of data.
^C
--- 10.1.1.115 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8185ms

ubuntu@ip-10-2-1-67:~$
```

Verify the logs generated.

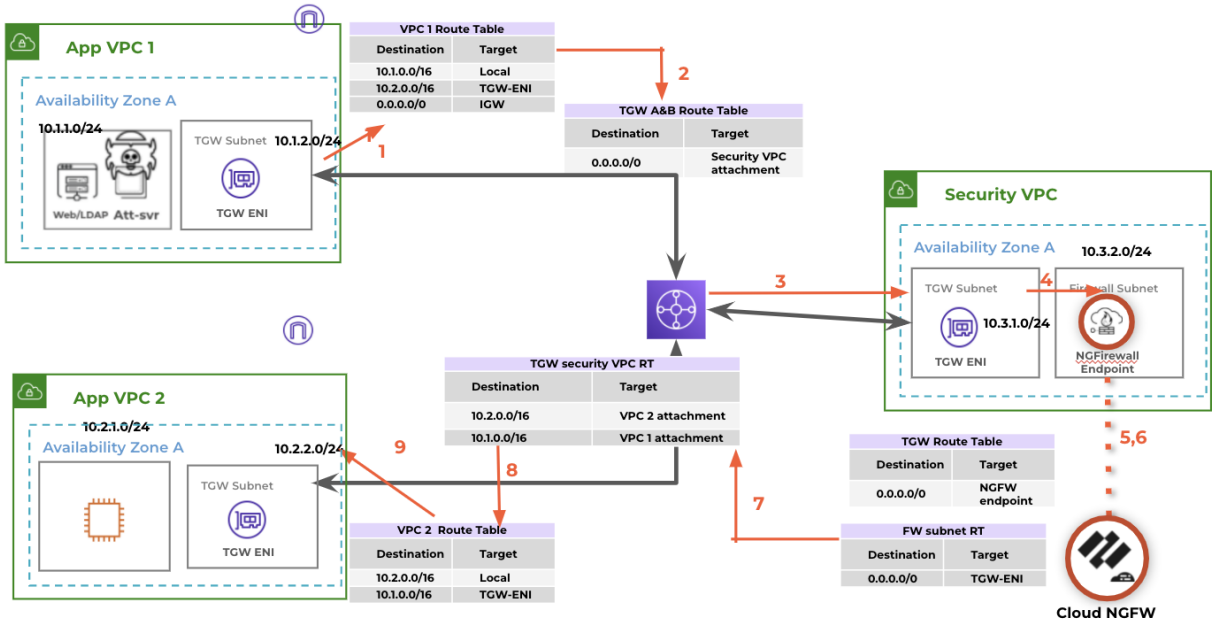
 ©2022 Palo Alto Networks, Inc

```
2022-04-05T16:16:41.000+05:30      {"src_ip":"10.2.1.67",

{
    "src_ip": "10.2.1.67",
    "sport": "0",
    "dst_ip": "10.1.1.115",
    "dport": "0",
    "proto": "icmp",
    "app": "ping",
    "rule": "EWtrafficRule",
    "action": "drop",
    "bytes_recv": "0",
    "bytes_sent": "0",
    "pkts_received": "0",
    "pkts_sent": "5",
    "start_time": "2022/04/05 10:46:34",
    "elapsed_time": "0",
    "repeat_count": "5",
    "category": "any",
    "src country": "10.0.0.0-10.255.255.255",
    "dst country": "10.0.0.0-10.255.255.255",
    "session_end_reason": "policy-deny",
    "xff_ip": ""
}
```


Traffic Flow for E-W traffic in Centralized Deployment .

Considering the setup we built in previous steps, let us understand how the traffic is forwarded for E-W flows.



 ©2022 Palo Alto Networks, Inc

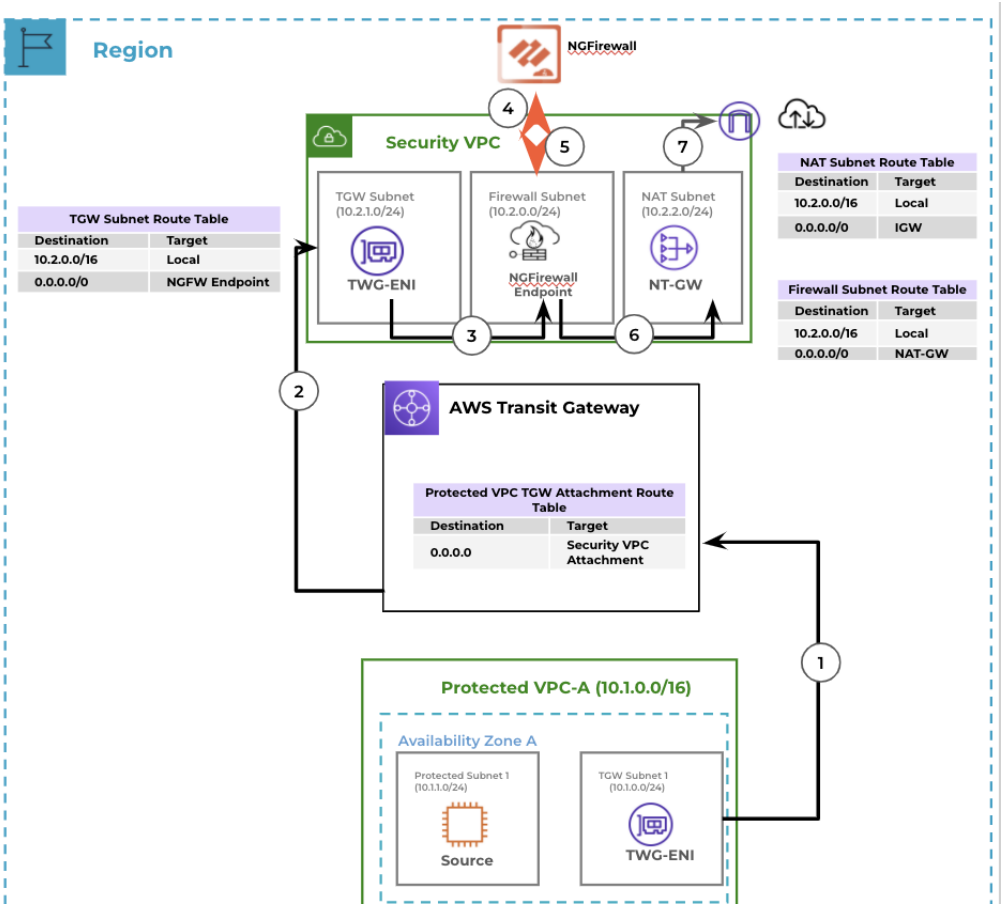
1. Traffic originates through VPC 2. The destination is in VPC 1.
2. Route table associated with the subnet is checked. There exists a route towards the TGW attachment for this destination.
3. Traffic gets forwarded to the TGW. Here, the route table for VPC 2 is looked up and finds the route via security VPC attachment.
4. Traffic is forwarded to the NGFW endpoint.
5. Traffic gets forwarded to the NGFW based on the default route.
6. NGFW performs the check.
7. If the traffic is allowed based on the configured rule, it is sent back to the NGFW endpoint
8. NGFW endpoint routes the traffic back to the TGW.
9. TGW does a route check again for the destination and forwards the traffic to the destination VPC via the attachment.

Reader Tip *-For more information please check out Centralized E-W Traffic Flow*

Traffic Flow with Outbound Traffic with Centralized Design.

Consider the diagram below. If you want to inspect and apply firewall policies for outbound traffic (internet), the security VPC can be the centralized point of exit. You will need to deploy a NAT gateway and the Internet Gateway in the security VPC which is hosting the NGFirewalls.

 ©2022 Palo Alto Networks, Inc



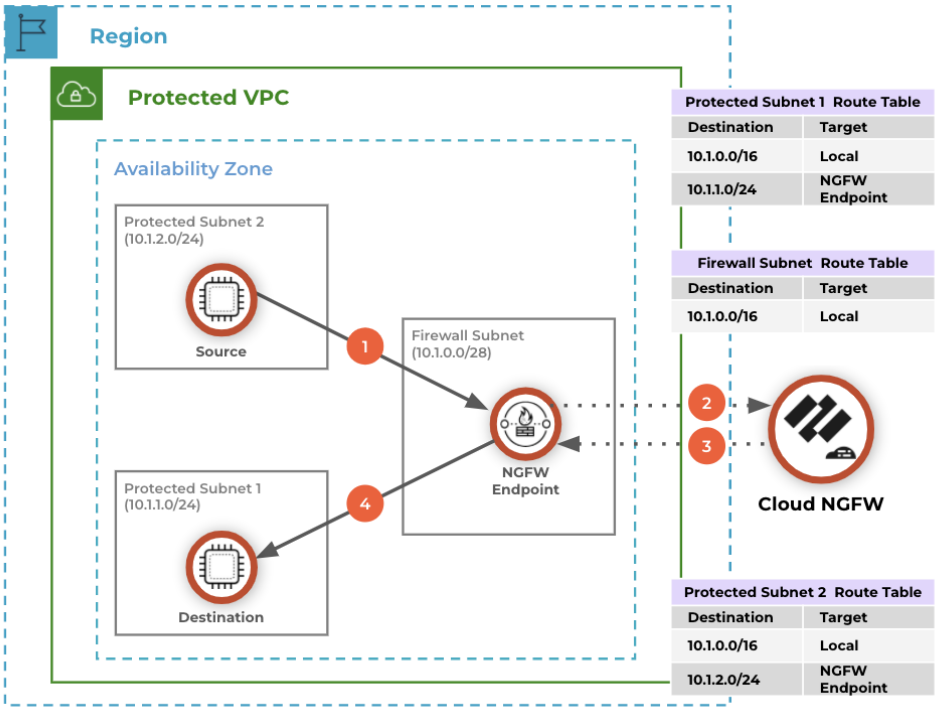
1. Traffic towards the internet matches the default prefix in the route table.
2. Traffic gets forwarded to the TGW.
3. Transit gateway has a default route towards the security VPC attachment. Traffic is Forwarded to the security VPC.
4. Traffic is forwarded to the NGFirewall endpoints.
5. Firewall performs the check.
6. Returns the traffic back to NGFirewall.
7. NGFirewall does a route lookup and finds a match with default route towards NAT Gateway, forwards the traffic to it.
8. NAT gateway checks the route table and finds the default route towards IGW. The traffic Exits towards the internet via the IGW.

Distributed Deployment

In a distributed deployment, cloud NGFW is deployed individually in each VPC which requires protection. Traffic from each VPC will be routed to its own cloud NGFW endpoint. This method

reduces the possibility of misconfiguration and limits the scope of impact. Let us take few examples and understand the traffic flow with distributed deployment.

E-W traffic flow with distributed deployment -
Consider the example below. Here, we have a protected VPC. This VPC is running applications/instances in 2 separate subnets (subnet 1 and subnet 2). The requirement here is to inspect any east-west traffic between the subnets in this VPC. The user can deploy the cloud NGFW endpoint in the same VPC. The route table for the subnets are configured such that, to reach another subnet, the next hop gateway is the cloud NGFW endpoint.

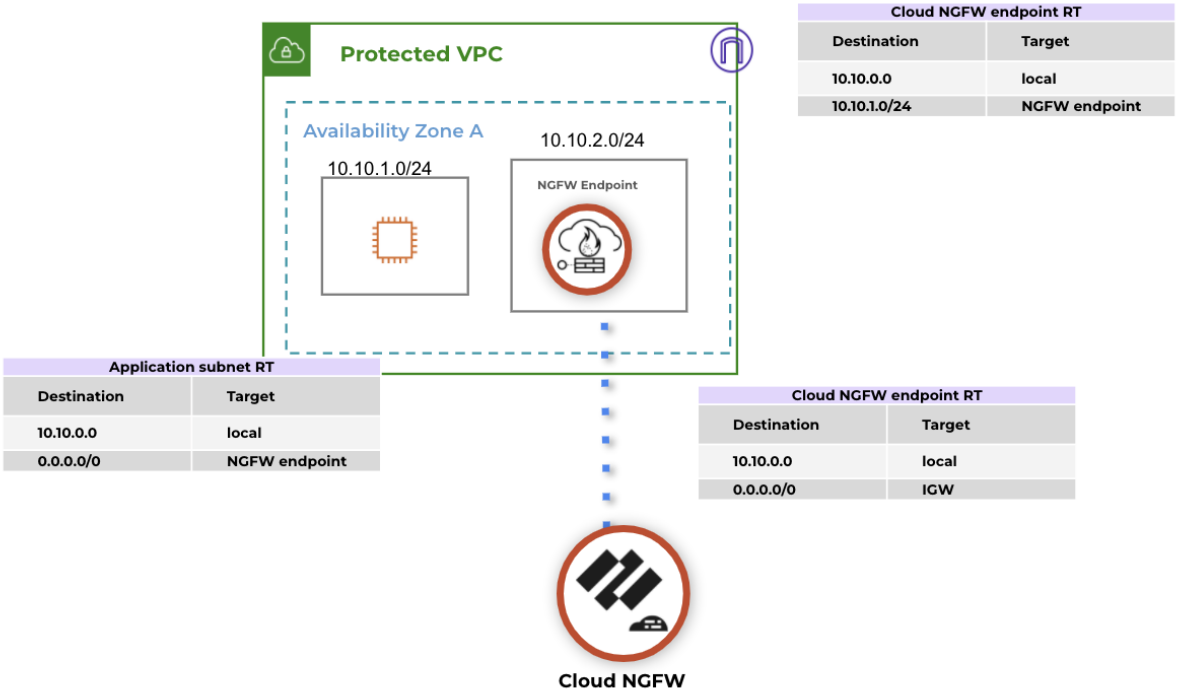


Let us understand the traffic flow with this model.
Traffic is initiated from source subnet (subnet 2) to destination (subnet1).

1. Based on the route table of the source subnet, we have an entry for the destination subnet to go via the NGFW endpoint. Traffic is hence forwarded to cloud NGFW endpoint.
2. Cloud NGFW endpoint forwards the traffic to NGFW for inspections and checks.
3. If the traffic is allowed, traffic is sent back to the cloud NGFW endpoint.
4. NGFW endpoint forwards the traffic to the destination.

Outbound traffic flow with distributed deployment-
For outbound traffic protection, the requirement is to inspect every egress / internet bound traffic. As you can see from the example below, to achieve this, there needs to be a default route pointing to cloud NGFW endpoint in every subnet which need internet access. The NGFW route table in turn will have a default route entry pointing to Internet Gateway.

 ©2022 Palo Alto Networks, Inc



Let us understand the traffic flow in this case. Let us assume that instance in 10.10.1.0/24 subnet need to access an internet location.

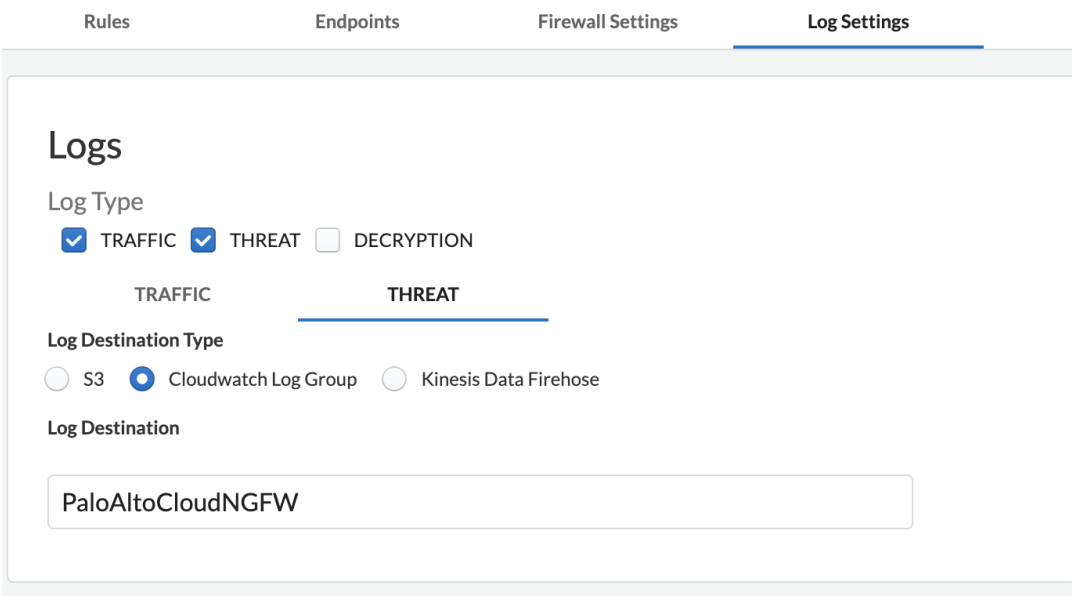
1. Since the route table has a default route pointing to cloud NGFW endpoint, traffic from the instance is routed to the cloud NGFW endpoint.
2. The Cloud NGFW endpoint will forward the traffic to the NGFW for further inspection and checks.
3. If the traffic is allowed, the traffic is sent back to the cloud NGFW endpoint.
4. Firewall subnet route table has a default route towards Internet-GW. The traffic is hence sent to the IGW

Considering the example above, we have rules defined with default security profile in Cloud NGFW.

Validation

Make sure you have configured the threat log destination for the cloud NGFW endpoint as below.

 ©2022 Palo Alto Networks, Inc



Connect to the instance as shown below and try to download a malicious file from the eicar website using the command “

```
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Mar 31 16:13:00 UTC 2022

  System load:  0.0                 Processes:           96
  Usage of /:   20.2% of 7.69GB     Users logged in:     0
  Memory usage: 43%                 IP address for ens5: 10.10.1.239
  Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

76 updates can be applied immediately.
60 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

New release '20.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Thu Mar 31 12:21:16 2022 from 49.207.195.168
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-10-1-239:~$ curl http://www.eicar.org/download/eicar.com.txt
```

”.

The output on console shows that the file download has been blocked.

```
BfqXXqIWE5GT1CX+AIUXLmhlWq15sKmpLVC7pNlmCMV8cv065L34ImQdPw47BYXde+ECZDQ0nCeidmytp7ahuM1QAbGTwa
agLDL2Ol1uRNZ5cJjb33wT9pw7JwgSCp/Hg7YzbO/NPXMGn0yDAG2V7e2t/nJm9ymxyNgLNxIwFnTObgf7q6+C9vnnw4qJ
Qk6+8YZwnNnQ4BctKDnkby6NjJwfaGrqPNTe/i6WMbtPKR4z9gsLi/D4T7cgo7gYh2jY9u7PP990nBumPUYEKPrUtWttD0
wmS53F4hS16plIt9XgaHncPwDQ1QU5J8XvHOFzu6naoWkgD4NKpTqPr6kFxXX5RErhoU1fHeiHjFJD2KG+W9D7k1DqB3gs
ybBpfZ++T7sgo7oaIg32UjL8jSPNzSWSFBQ3wxKwWiGtvByigaqmBpZ5/gVqQTF3iDnEeAe/o9A7v/wS0goLN00lIwl+Fs
EguR7qWktuoLLAqdUQLWTksziez5GcoEvLbDY0FAs6Po7j6Hsoprri9fqljbDaIVIsGGaRNN+sqLuRcUaE1ziNfjEmlNUb
j6yHUhvL/dTWVK9ftReoHpem/Zuv4hLL0PBI0Pp5lwv6+gfD1uf6Q6Q8nZAhEsNGe6sQGWoJn8Vxo6ICSxSvQK8XHlsJVk
5bjyMg1K4Qmqwsqnrr8Ff7huryYIXMy3FuTuuY1MRTY4oOxcl69lkQg8dmIxlBvltyi+0ymQx8Pt/aiwMHYHl4WAhpaEA7
iAmUnbBC8gAEyzYbqkxTgmcpcW/l3jQ9rj0K8x9/DGLAHk0SHqLeg+1XHI5uzORvE7SI2Mr+wWFIVDam/7jGRliamMCTpX
ovZpvGzWZMdoDj1i2gBX804pCu4vE2QfF6Hxw279x+Dx6T1FeikUXWiNbBONT0HLU4W7NNVO/p7QVPb+8o6Z038HVAG/r0
sQboITOjd27/FZzOWUg0Tn/3FGRmZgjH3IkTsPRZF7ju3g2bqVeTeT+2w2GfSZHuw54/+/77eLieYOaswyMOsl4l7TtjZ6
aBu9IG+rNnhZXNUKCYqzMzYdshdpKM9jx6hKugZn+ZjOe5bpA6JITiz/4Ept56S7CTocAQi0Z0tLNEzD9sFBPh+qxWk5yT
d0AyQBIm/O+vQXZdnZDD3An4g0zfvAleh+Pq4fb281vrOfxnwDpsJvPQmPw/mFGHDH/+9p9BMTYmiEqzNIKgvXQRb05srJ
N49Fa/E9oK5z/o67MZZHLezMnhqNRsKjlJw7ZCknzmLR2gINmpNJIgziDBv1yrBblOJwx7FBBnTNgj0eOTWBOFvOrxeK7g
2lGIz5I+QmdR8h0BhSVmAIaswPf8V0j5AXFIsLhIcgF5a2HXwQrgKiu7V0dtL1S1to6G+6ykENRP3+BQC4mxLwYUNgA8Xi
iG1zJVHrwBlCSVoH7QEXOc7LQMZEeJbEZS5DdxTqIIXm3XyfO+d6sqKiwgkv8DR1QQUUMZmhsAAAAASUVORK5CYII=" al
t="Error">
    <h1>Virus/Spyware Download Blocked</h1>
    <p>The file you are trying to download has been blocked in accordance with company policy
regarding viruses and spyware. Please contact your system administrator if you believe this is
 an error.</p>
    <div class="response">
        <p><b>File name:</b> eicar.com.txt </p>
    </div>
</div>
</body>
</html>
ubuntu@ip-10-10-1-239:~$
```


Check the Log group for the latest threat log stream in cloudwatch console from AWS.


```
2022-03-31T17:51:59.000+05:30    {"src_ip":"10.10.1.239", "sport":"33110", "dst":"89.238.73.97", "dport":"80", "proto":"tcp", "
{
    "src_ip": "10.10.1.239",
    "sport": "33110",
    "dst": "89.238.73.97",
    "dport": "80",
    "proto": "tcp",
    "app": "web-browsing",
    "rule": "Rule-outbound",
    "action": "reset-server",
    "threat_category": "js",
    "sub_type": "virus",
    "threat_content_name": "Eicar Test File(100000)",
    "severity": "medium",
    "direction": "server-to-client",
    "repeatcnt": "1",
    "data_filter_reason": "",
    "filetype": "",
    "contentver": "Antivirus-4037-4548"
}
```

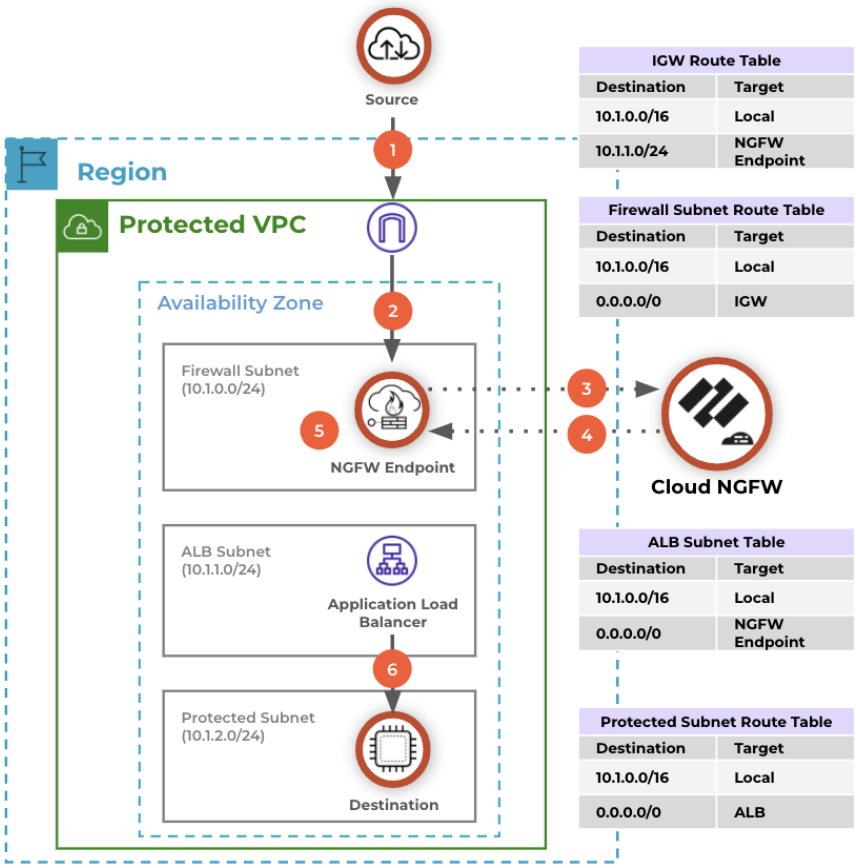

You can see from the logs that, file was blocked. The content version used, file type can also be seen in the logs apart from the other traffic parameters.

Reader Tip *- For more information, please check out Distributed-Outbound-Traffic-Flow*

Inbound traffic flow with distributed deployment-

The use case is to inspect and scan inbound traffic coming from internet. The route table at application load balancer forwards the traffic to or from the NGFW endpoint.

 ©2022 Palo Alto Networks, Inc



Let's take a look at the traffic flow

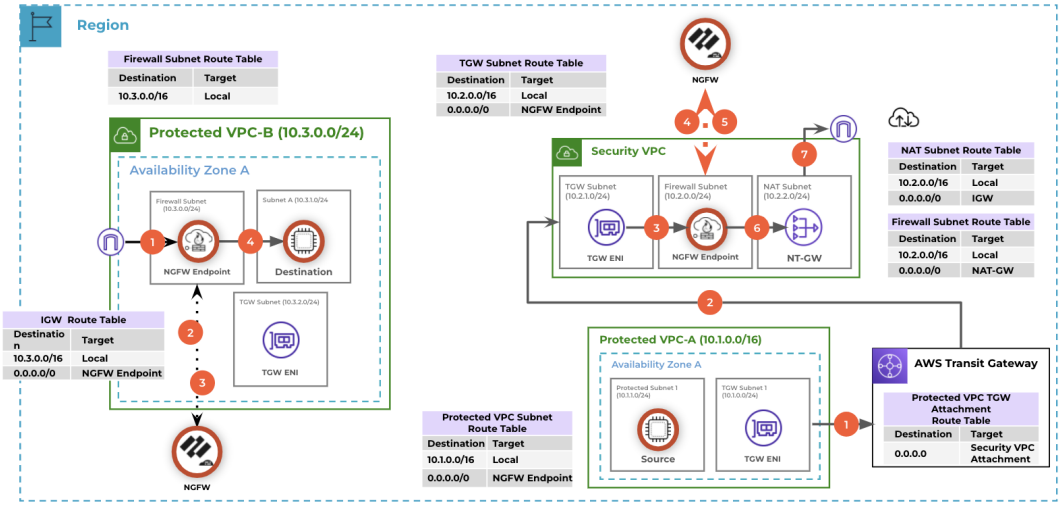
1. Traffic from the internet reaches the internet gateway.
2. Based on the route table of internet gateway, traffic is sent to the NGFW endpoint.
3. NGFW endpoint sends the traffic to the NGFW for inspection.
4. If the traffic is allowed, it is sent back to the NGFW endpoint.
5. NGFW endpoint sends the traffic back to the ALB
6. ALB then forwards the traffic to the destination.

Reader Tip *- For more information, please check out Distributed-Inbound-Traffic-Flow*

Combined Model

In a combined model, you have an option to deploy a distributed model along with a centralized model. Few examples for this use case are - customers would want to use a dedicated cloud

NGFW for inbound traffic from the internet and use a central VPC for any outbound traffic. This is shown in the figure below.
Another use case can be, using the centralized design for any E-W traffic and using a dedicated Cloud NGFW console for outbound traffic.



Summary

Cloud NGFW is Palo Alto Networks best-in-class NGFW delivered as a managed cloud-native service on AWS. Under the hood, the service is built using the VM-Series. Our patented App-ID, threat prevention and URL filtering subscriptions are best-in-class. This provides AWS native experience and fits in the way you work with AWS.

For more information, please visit the [Live Community Page for Cloud NGFW]

You can get a quick hands-on experience with Cloud NGFW lab on qwiklabs- https://paloaltonetworks.qwiklabs.com/

References

Cloud NGFW Live Community - Cloud NGFW LiveCommunity Page
Cloud NGFW Youtube Channel - Cloud NGFW Youtube Channel
VM Series Deployment Guide - VM Series Deployment Guide
VM-Series with GWLB design - VM-Series integration with gateway load balancer

 ©2022 Palo Alto Networks, Inc

 ©2022 Palo Alto Networks, Inc