

Cloud NGFW For AWS

Technical Overview

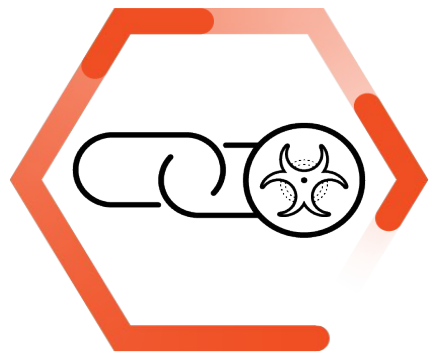
Costin-Alexandru Gherghe

Systems Engineer

Security Challenges

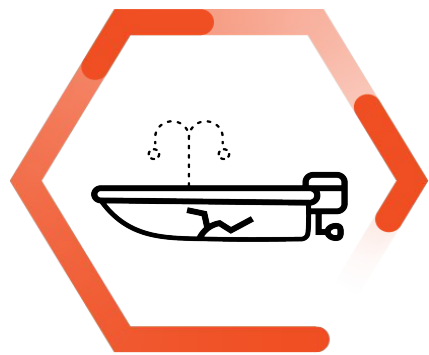
Why Next-Generation Firewalls are needed in the Cloud

Risk:



Outbound Connections

When connections to the Internet are allowed, customers are at risk of misuse with acts such as crypto-mining, command-and-control, and data exfiltration



Unknown and Unpatched Vulnerabilities

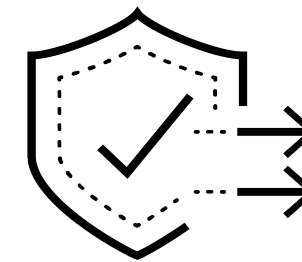
Unknown vulnerabilities (example Log4J) and unpatched vulnerabilities are able to be exploited by attackers before updates become available.



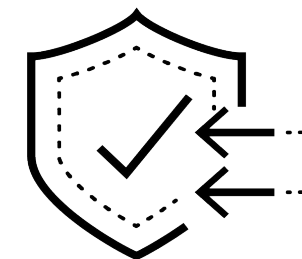
Lateral Movement

Applications connected to the internet may be penetrated by a threat and then spread laterally to compromise other applications.

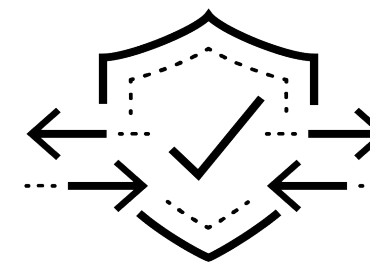
How Does NGFW Address This Risk?



NGFW provides the next layer of workload inspection for potential malware or threats, and can block malicious connections



While WAFs secure HTTP connections, inbound connections protected by an NGFW block attackers from exploiting vulnerabilities while you work on patching

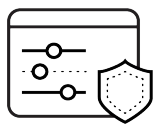


NGFW enables a Zero Trust strategy by protecting inbound connections from the Internet, as well as connections from other applications

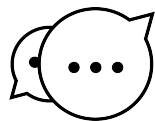
Enterprises Need: Best-in-Class Security + Cloud Native Ease of Use



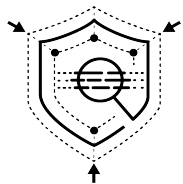
Best-in-Class Security



Layer 7 Firewall controls traffic at the application layer



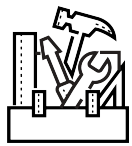
Real-time updates protect against the latest threats



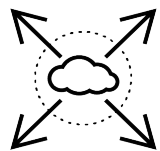
ML-powered threat prevention protects against zero-day attacks



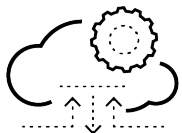
Cloud Native Ease of Use



Zero maintenance with no infrastructure to manage



Built-in scalability and resiliency



Integration with other AWS services for automation of end-to-end workflows

Introducing Cloud NGFW

Introducing Cloud NGFW for AWS

Best-in-Class Security Meets **Cloud-Native Ease of Use**



**Best-in-Class
Security**

Built to stop Zero-Day
threats



**Cloud-Native
Ease of Use**

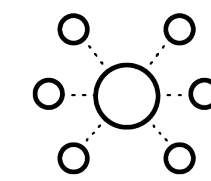
Designed for the way you
work with AWS

Cloud NGFW | Key Capabilities

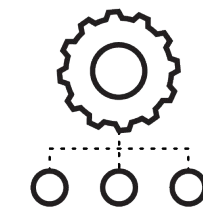


Cloud NGFW

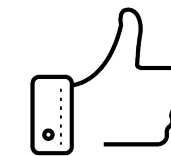
Best-in-class NGFW
delivered as a managed
cloud-native service for
AWS



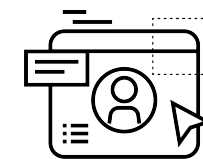
Managed cloud
native service



Deploy in just a
few clicks



Best-in-class security



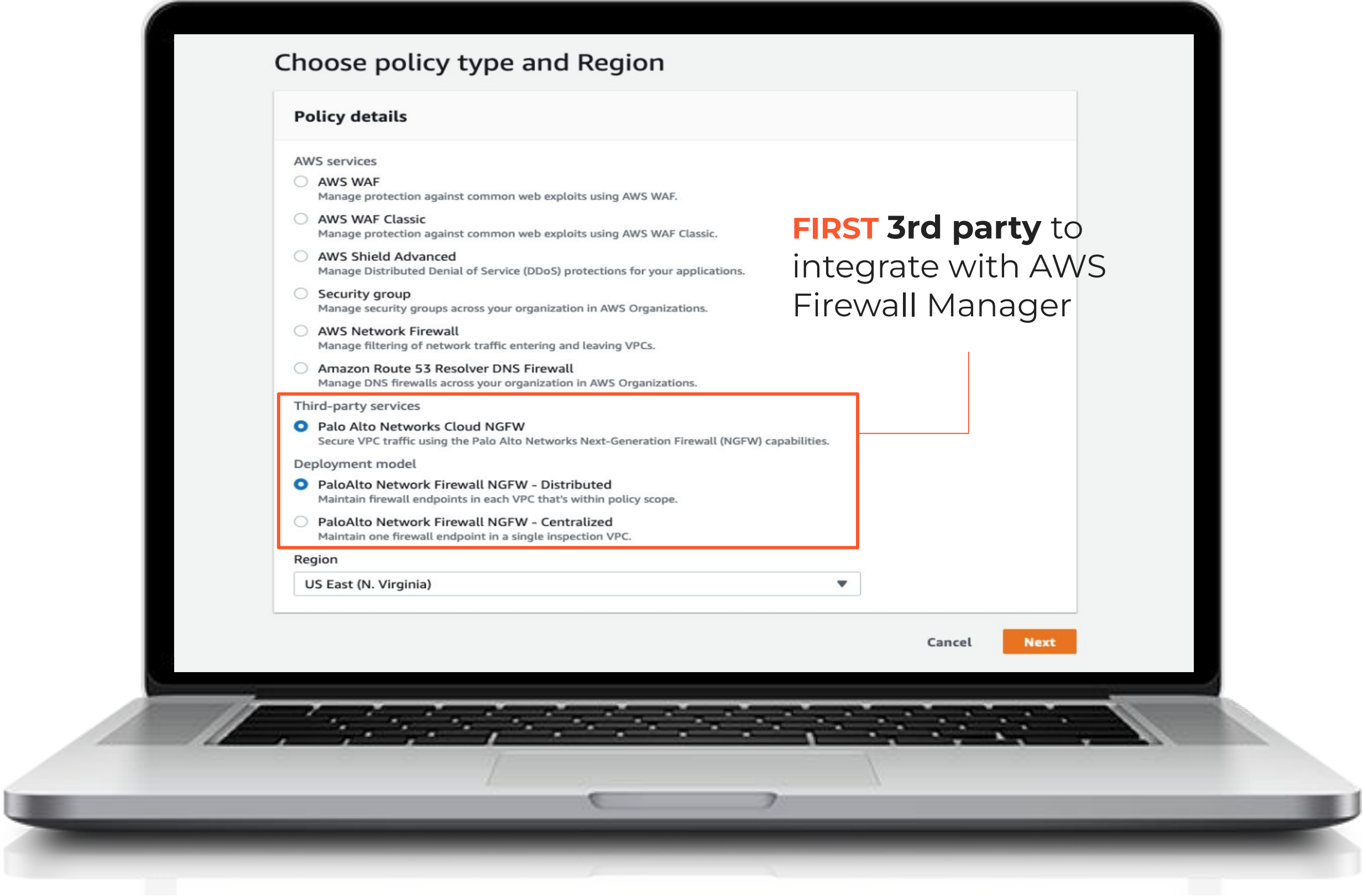
Integrated with AWS
Firewall Manager

Cloud NGFW Best-In-Class Security

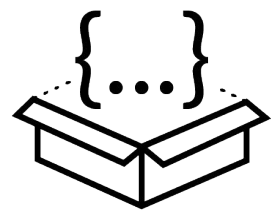
Built to Stop Zero-Day threats



Cloud NGFW | Integrates into the way you work with AWS today



Infrastructure as Code (Iac) Capabilities



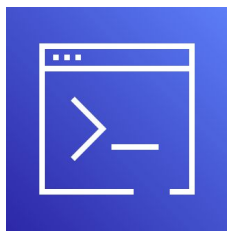
Application
Programming
Interface



Cloud
Formation
Template



Terraform
Provider



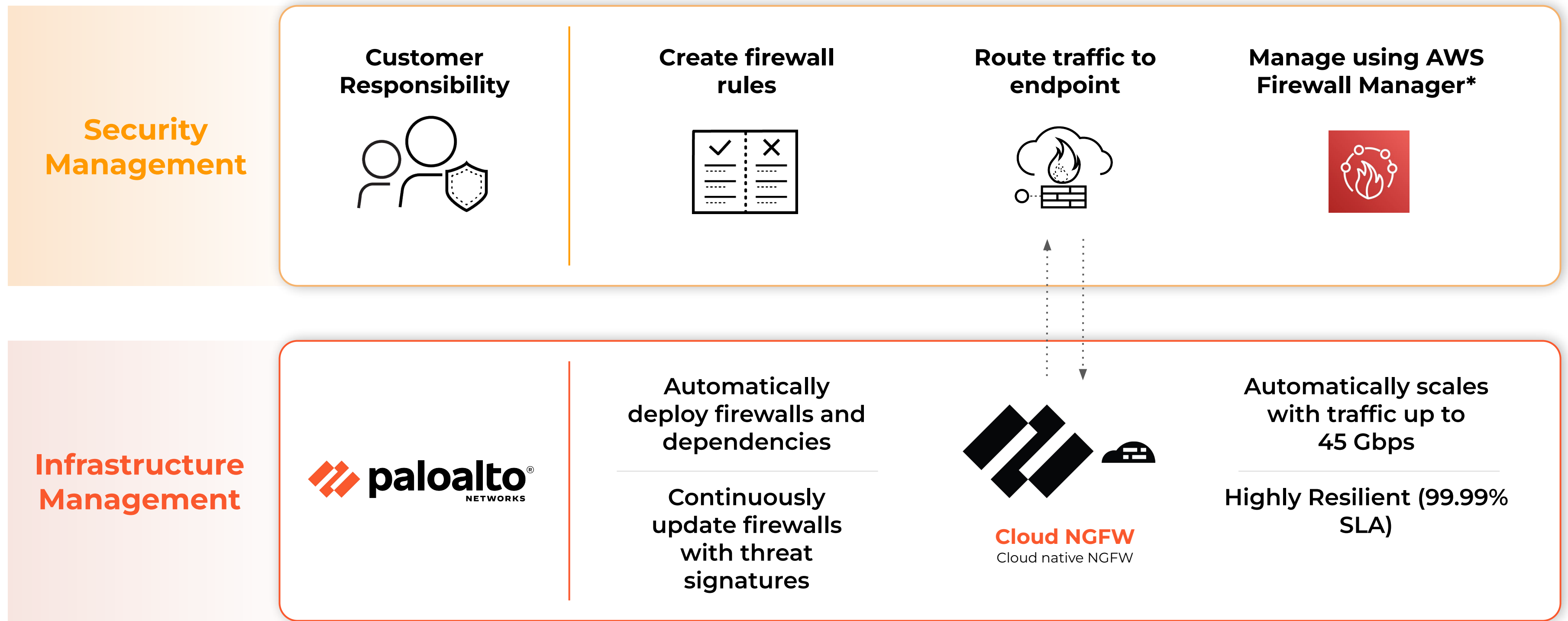
Command
Line
Interface*



Software
Development
Kit*

* AWS Firewall Manager only

Cloud NGFW | Delivered as a Managed Cloud Native Service



*Optional. All customers must use Cloud NGFW management

Cloud NGFW for AWS | Region Availability

Latest updates [here](#)

Available Now:

- us-east-1 (N. Virginia)
- us-east-2 (Ohio)
- us-west-1 (N. California)
- us-west-2 (Oregon)
- ca-central-19 (Canada Central)
- eu-central-1 (Frankfurt)
- eu-north-1 (Stockholm)
- eu-west-1 (Ireland)
- eu-west-2 (London)
- eu-west-3 (Paris)
- eu-south-1 (Milan)
- ap-southeast-1 (Singapore)
- ap-southeast-2 (Sydney)
- ap-northeast-1 (Tokyo)
- ap-northeast-3 (Osaka)
- ap-northeast-2 (Seoul)
- ap-south-1 (Mumbai)
- sa-east-1 (São Paulo)
- af-south-1 (Cape Town)
- ap-east-1 (Hong Kong)
- ap-southeast-3 (Jakarta)
- me-south-1 (Bahrain)




Cloud NGFW for AWS | Marketplace Listings

1 SaaS Subscription (Pay-As-You-Go)

Palo Alto Networks Cloud NGFW (Next-Generation Firewall) Pay-As-You-Go	
Overview	Pricing
Usage	
Support	
This software is priced along a consumption dimension. Your bill will be determined by the number of units you use. Additional taxes or fees may apply.	
Palo Alto Networks Cloud NGFW (Next-Generation Firewall) Pay-As-You-Go	
Units	Cost
Base Firewall Usage Hours (1 unit = 1 usage hour per AZ)	\$1.637 / unit
Traffic Secured (1 unit = 1 GB secured)	\$0.043 / unit
Threat Prevention Usage Hours (1 unit = 1 usage hour per AZ)	\$0.327 / unit
Advanced URL Filtering Usage Hours (1 unit = 1 usage hour per AZ)	\$0.491 / unit
Enhanced Support (1 unit = 18% of total usage hour consumption)	\$0.295 / unit
Cloud NGFW Overages	\$0.016 / unit

GET STARTED HERE!
Provides 15 day free trial and pay-as-you-go pricing

2 SaaS Contract (Credits) NEW



Overview

Pricing

Usage

Su

Pricing Information

Below are the total costs for these different subscription durations. Additional taxes or fees may apply.

Palo Alto Networks Cloud NGFW for AWS Credits				
Units	Description	12 MONTHS	24 MONTHS	36 MONTHS
Cloud NGFW Credits_100	Cloud NGFW Credits (1unit = 100 Credits)	\$11,469	\$22,939	\$34,408

Additional usage fees

You will be billed monthly for additional usage costs if your usage exceeds your contract. Your additional usage costs will be determined by the number of units you use above your contract.

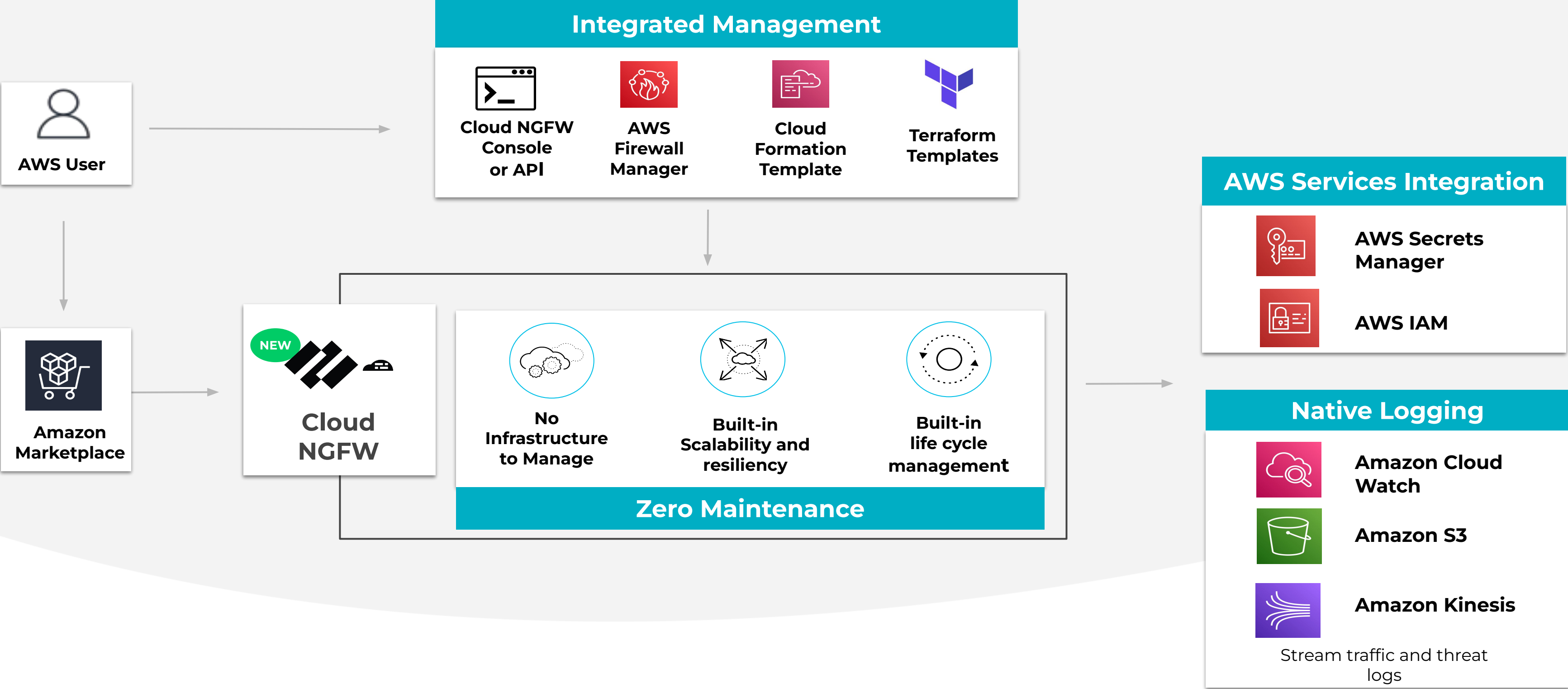
Description	Fees
Cloud NGFW Overages	\$0.016/unit

SAVE MONEY!
Get discounted pricing on a long-term commitment

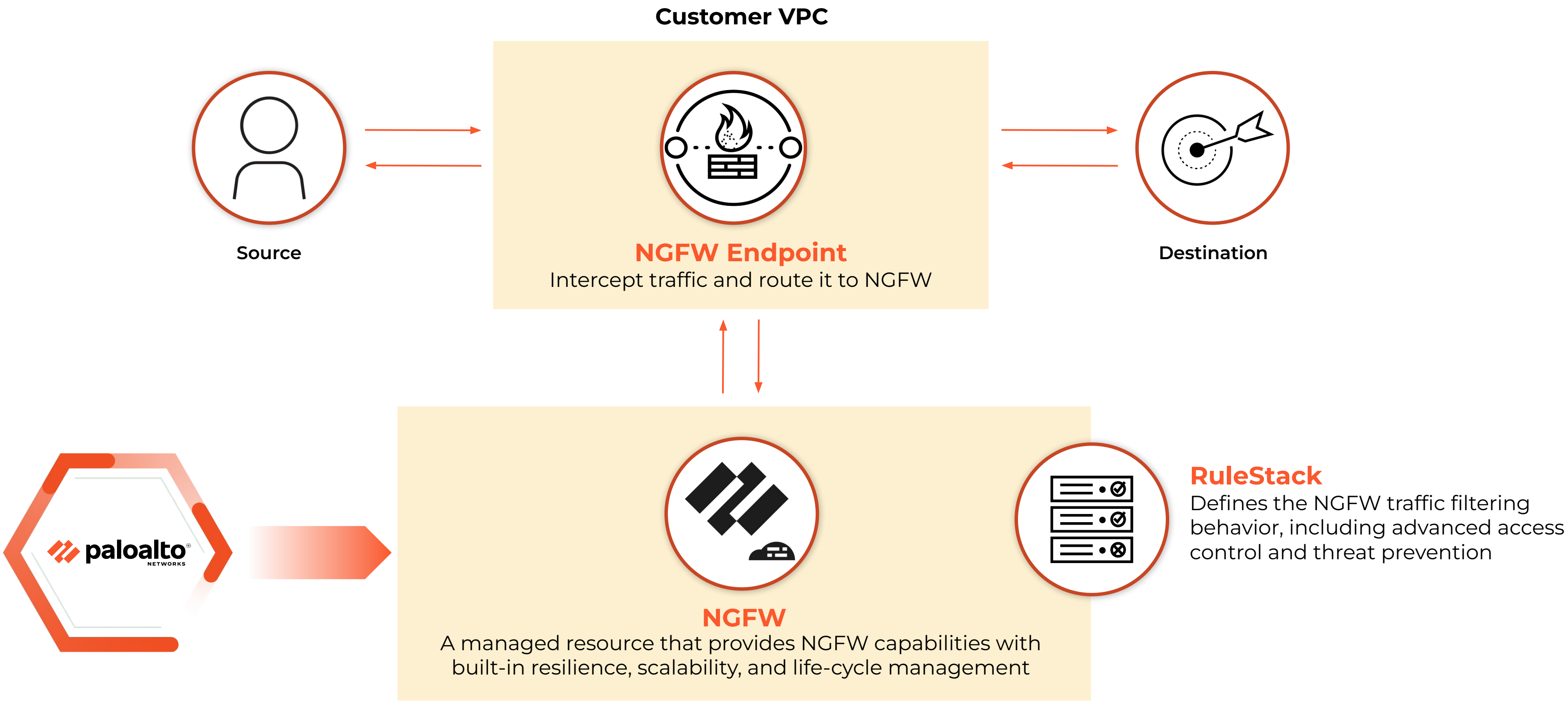
*Contact your sales and partner teams for private Offers

Fundamentals

Cloud NGFW | Fits in with the way you work with AWS



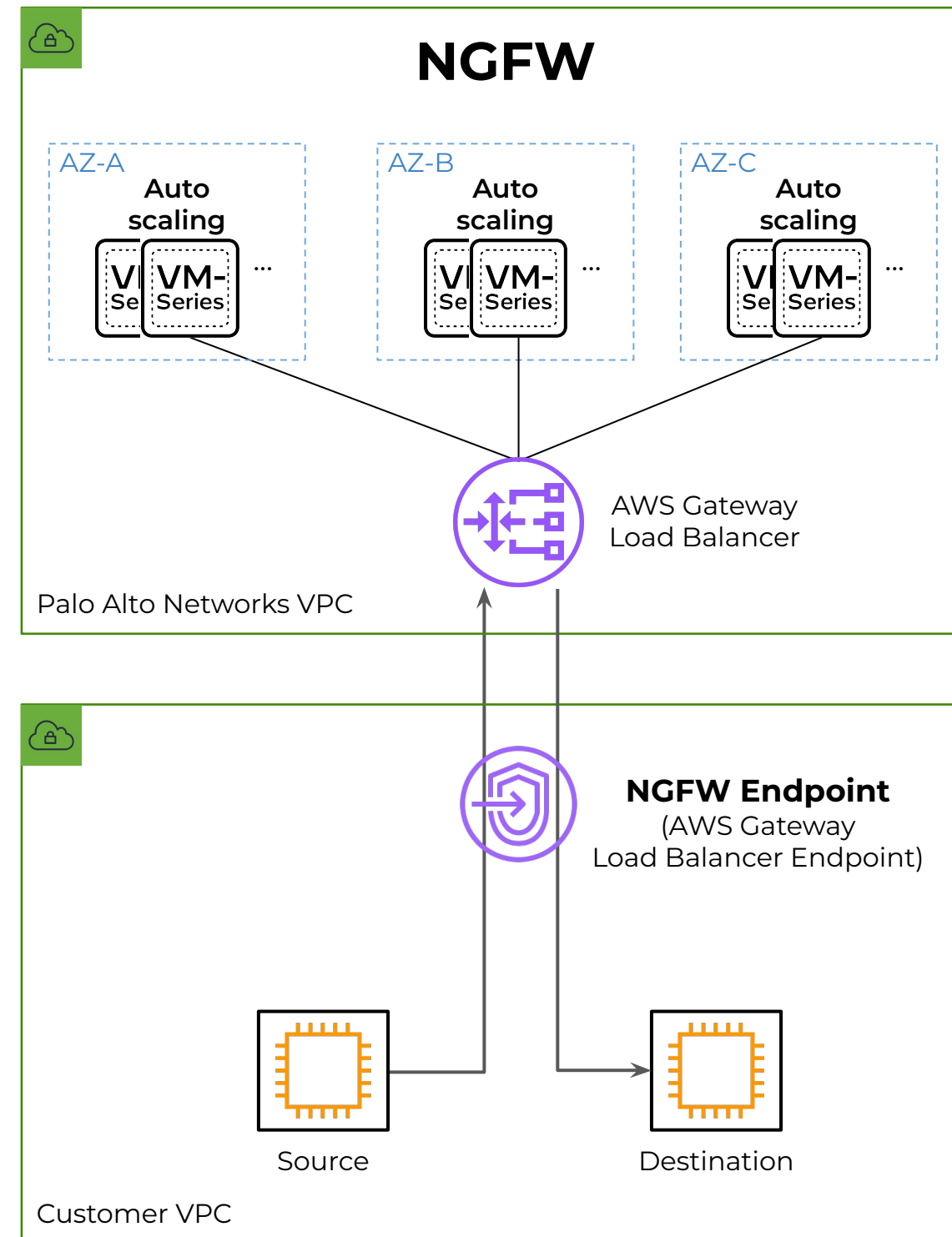
Cloud NGFW | Components



Cloud NGFW | Delivered using AWS Gateway Load Balancer

NGFW

A fully managed cluster of VM-Series front ended by AWS Gateway Load Balancer and provided to customers as a resource



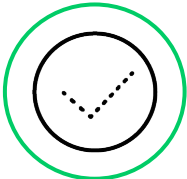
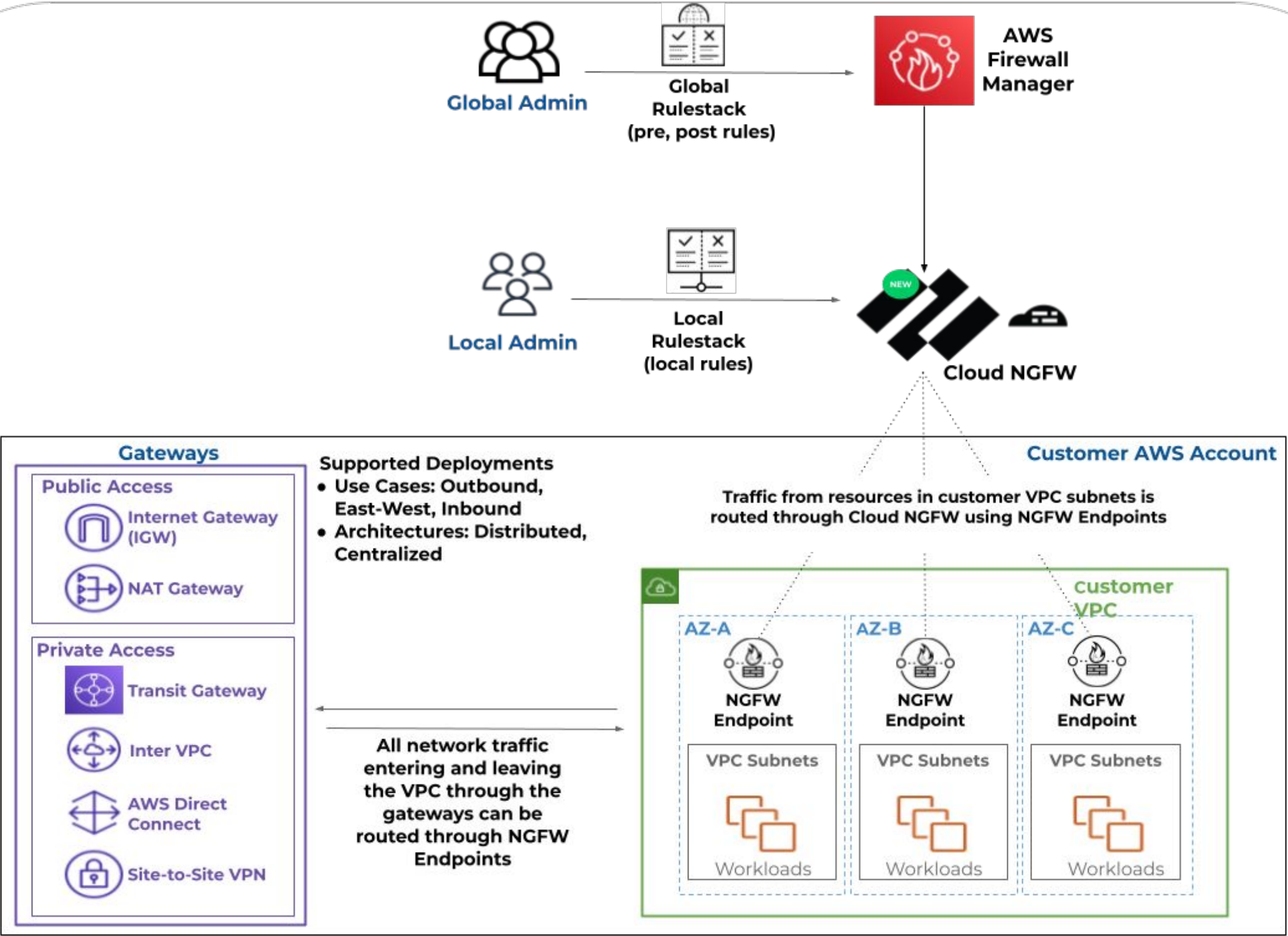
NGFW Features

- Auto scaling
- Fault tolerance
- Transparent insertion into customer VPC
- Cost of GWLB is included in the Cloud NGFW price

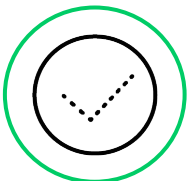
Built

Note: Customers have to pay AWS for each Cloud NGFW (a.k.a GWLB) endpoint that they would use in their AWS account(s).

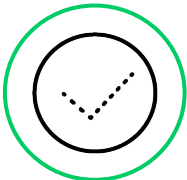
AWS Firewall Manager and Cloud NGFW integration



Centrally deploy Cloud NGFWs across VPCs and AWS accounts



Hierarchical Rule enforcement

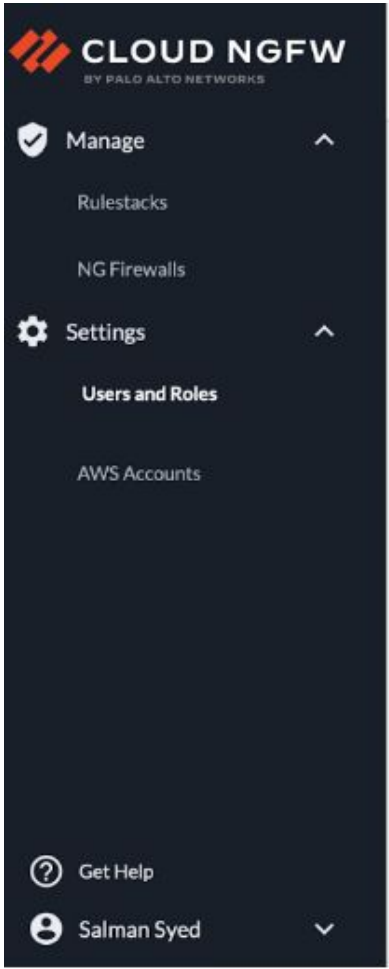


Dashboard with Compliance notifications

Roles and Permissions

Cloud NGFW | Roles and Permissions

Roles	Permissions
Tenant Administrator	<ul style="list-style-type: none">• Add AWS Accounts• Invite users and assign roles
Global Firewall Administrator	<ul style="list-style-type: none">• Create NGFW resources
Global Rulestack Administrator	<ul style="list-style-type: none">• Create a global rulestack
Local Firewall Administrator	<ul style="list-style-type: none">• Create NGFW resources
Local RuleStack Administrator	<ul style="list-style-type: none">• Create Local rulestacks



Users and Roles

As a Tenant Administrator you can invite users in your email domain to use the tenant. A user who joins, is added to the table with Active status. Click a user name to add or remove previously defined AWS roles. You can deactivate an account and reactivate it later, or delete it.

Users

Actions

Invite User

<input type="checkbox"/>	Name	Email	Status	Roles
<input type="checkbox"/>	Bry	bpell	CONFIRMED	710085992487/LocalRuleStackAdmin, ...
<input type="checkbox"/>	cha	cbrar	CONFIRMED	710085992487/LocalRuleStackAdmin, ...
<input type="checkbox"/>	Dav	dmor	CONFIRMED	TenantAdmin, 710085992487/LocalRul...
<input type="checkbox"/>	Joh	jcone	FORCE_CHANGE_PASSWORD	710085992487/LocalRuleStackAdmin, ...
<input type="checkbox"/>	Mai	mani	CONFIRMED	710085992487/LocalRuleStackAdmin, ...
<input type="checkbox"/>	Mej	mmu	FORCE_CHANGE_PASSWORD	710085992487/LocalRuleStackAdmin, ...
<input type="checkbox"/>	Mul	mugu	CONFIRMED	710085992487/LocalRuleStackAdmin, ...
<input type="checkbox"/>	Nid	npan	FORCE_CHANGE_PASSWORD	710085992487/LocalRuleStackAdmin, ...
<input type="checkbox"/>	Phil	pbai	CONFIRMED	710085992487/LocalRuleStackAdmin, ...
<input type="checkbox"/>	Prak	prnai	CONFIRMED	710085992487/LocalRuleStackAdmin, ...

Cloud NGFW Console

Configure using Cloud NGFW Console

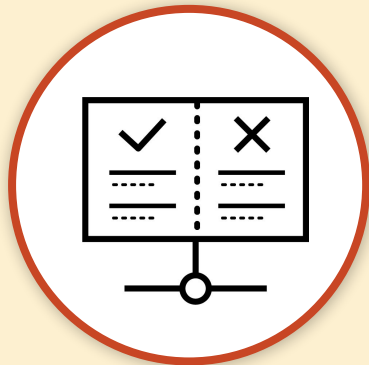
1

Onboard AWS account to the Cloud NGFW tenant



2

Create RuleStacks with Rules



RuleStack

3

Create NGFW and Endpoints



NGFW



NGFW Endpoint

4

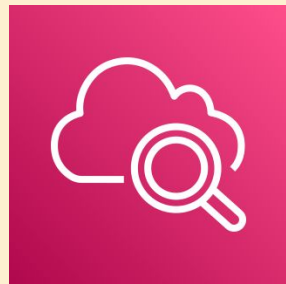
Specify Logging Options



Amazon S3




Amazon Kinesis



Amazon CloudWatch

Cloud NGFW Console

2 Create Rule Stacks and Rues



CLOUD NGFW
BY PALO ALTO NETWORKS

Manage

Rulestacks

NGFWs

Settings

Users and Roles

AWS Accounts

Tenant

Region: US West (N. California) ▼

Rulestacks

A Rulestack is a set of security rules, and associated objects and security profiles, used for enabling advanced access control (APP-ID™,, URL filtering) and threat prevention features. A Rulestack can be associated with one or more Firewalls. You can create two types of rulestacks-global and local. Global rulestacks apply to all firewalls in your deployment and local rulestacks apply to specific firewalls.

Rulestacks

Action ▼

Create Rulestack ▼

<input type="checkbox"/>	Name	Status	Type	Account Id
<input type="checkbox"/>	Development-Rulestack		Local	
<input type="checkbox"/>	Production-Rulestack		Local	

3 Deploy Cloud Firewalls and Endpoints

1 Add AWS Accounts

Firewall Manager

Deploy and Manage Cloud NGFW

- Subscribe to Cloud NGFW Service from AWS Firewall Manager

Choose policy type and Region

Policy details

AWS services

- ☐ AWS WAF
Manage protection against common web exploits using AWS WAF.
- ☐ AWS WAF Classic
Manage protection against common web exploits using AWS WAF Classic.
- ☐ AWS Shield Advanced
Manage Distributed Denial of Service (DDoS) protections for your applications.
- ☐ Security group
Manage security groups across your organization in AWS Organizations.
- ☐ AWS Network Firewall
Manage filtering of network traffic entering and leaving VPCs.
- ☐ Amazon Route 53 Resolver DNS Firewall
Manage DNS firewalls across your organization in AWS Organizations.

Third-party services

- ☒ Palo Alto Networks Cloud NGFW
Secure VPC traffic using the Palo Alto Networks Next-Generation Firewall (NGFW) capabilities.

Deployment model

- ☒ PaloAlto Network Firewall NGFW - Distributed
Maintain firewall endpoints in each VPC that's within policy scope.
- ☐ PaloAlto Network Firewall NGFW - Centralized
Maintain one firewall endpoint in a single inspection VPC.

Region

US East (N. Virginia)

Third-party services

- ☒ Palo Alto Networks Cloud NGFW
Secure VPC traffic using the Palo Alto Networks Next-Generation Firewall (NGFW) capabilities.

Deployment model

- ☒ PaloAlto Network Firewall NGFW - Distributed
Maintain firewall endpoints in each VPC that's within policy scope.
- ☐ PaloAlto Network Firewall NGFW - Centralized
Maintain one firewall endpoint in a single inspection VPC.

Cancel

Next

Choose Policy Type and Region

Step 1

Choose policy type and Region

Step 2

Describe policy

Step 3

Configure distributed endpoints

Step 4

Define policy scope

Step 5

Configure policy tags

Step 6

Review and create policy

Choose policy type and Region

Policy details

AWS services

☐ AWS WAF

Manage protection against common web exploits using AWS WAF.

☐ AWS WAF Classic

Manage protection against common web exploits using AWS WAF Classic.

☐ AWS Shield Advanced

Manage Distributed Denial of Service (DDoS) protections for your applications.

☐ Security group

Manage security groups across your organization in AWS Organizations.

☐ AWS Network Firewall

Manage filtering of network traffic entering and leaving VPCs.

☐ Amazon Route 53 Resolver DNS Firewall

Manage DNS firewalls across your organization in AWS Organizations.

Third party services

☒ Palo Alto Networks Cloud NGFW

Manage network firewall resources in Palo Alto Networks platform.

Deployment model

☒ Distributed

Maintain firewall endpoints in each VPC that's within policy scope.

☐ Centralized

Maintain one firewall endpoint in a single inspection VPC.

Region

US East (N. Virginia)

Cancel

Next

Describe Policy In FMS

Step 2

Describe policy

Step 3

Configure centralized endpoints

Step 4

Define policy scope

Step 5

Configure policy tags

Step 6

Review and create policy

Policy name

Policy name

PaloAltoPolicy2

The name must have 1-128 characters. Valid characters: a-z, A-Z, 0-9, -(hyphen), and _(underscore).

Region

US East (N. Virginia)

Third party Firewall policy configuration

Create firewall policy

Find resource

	Name	ID
<input type="radio"/>	global-	global-
<input type="radio"/>	global-	global-

Third party Firewall logging configuration

☐ Traffic

☐ Decryption

☐ Threat

Configure Distributed Endpoints

AWS Firewall Manager > Security policies > Create security policy

Step 1

Choose policy type and Region

Step 2

Describe policy

Step 3

Configure distributed endpoints

Step 4

Define policy scope

Step 5

Configure policy tags

Step 6

Review and create policy

Configure distributed endpoints

Configure AWS Network Firewall endpoint

Availability Zones

Select the Availability Zones by name or by ID to create endpoints in.

☒ Availability Zone name

☐ Availability Zone ID


< 1 >

Availability Zone	Action	CIDR blocks - optional
us-east-1a	<input checked="" type="radio"/> Add to AWS Firewall policy	
us-east-1b	<input checked="" type="radio"/> Add to AWS Firewall policy	
us-east-1c	<input checked="" type="radio"/> Add to AWS Firewall policy	
us-east-1d	<input checked="" type="radio"/> Add to AWS Firewall policy	
us-east-1e	<input checked="" type="radio"/> Add to AWS Firewall policy	
us-east-1f	<input checked="" type="radio"/> Add to AWS Firewall policy	

CIDR blocks for firewall subnets - optional

Firewall Manager creates subnets for your firewall endpoints. You can provide up to 50 CIDR blocks to use for the subnets. Firewall Manager uses the CIDR blocks in the order that they are listed.

© 2023 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

 paloalto
NETWORKS

Define Policy Scope

Step 1

Choose policy type and Region

Step 2

Describe policy

Step 3

Configure distributed endpoints

Step 4

Define policy scope

Step 5

Configure policy tags

Step 6

Review and create policy

Define policy scope

Policy scope

Policy scope defines the accounts and resources covered by this policy.

AWS accounts this policy applies to

☐ Include all accounts under my AWS organization

☒ Include only the specified accounts and organizational units

☐ Exclude the specified accounts and organizational units, and include all others

Included AWS accounts

Delete selection

Edit list

☐

AWS accounts

No Accounts added

Included organizational units

Delete selection

Edit list

☐

Name


ID

No OUs added

Resource type

☒ VPC

© 2023 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

 paloalto
NETWORKS

Security Model

Rulestack

A Rulestack includes a set of security rules, associated objects, and profiles

- **Objects**

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. Objects can only be applied to a single rulestack

- **Security Rules**

Security rules determine whether to block or allow a session based on traffic attributes, such as the source and destination IP address, source and destination FQDNs, or the application

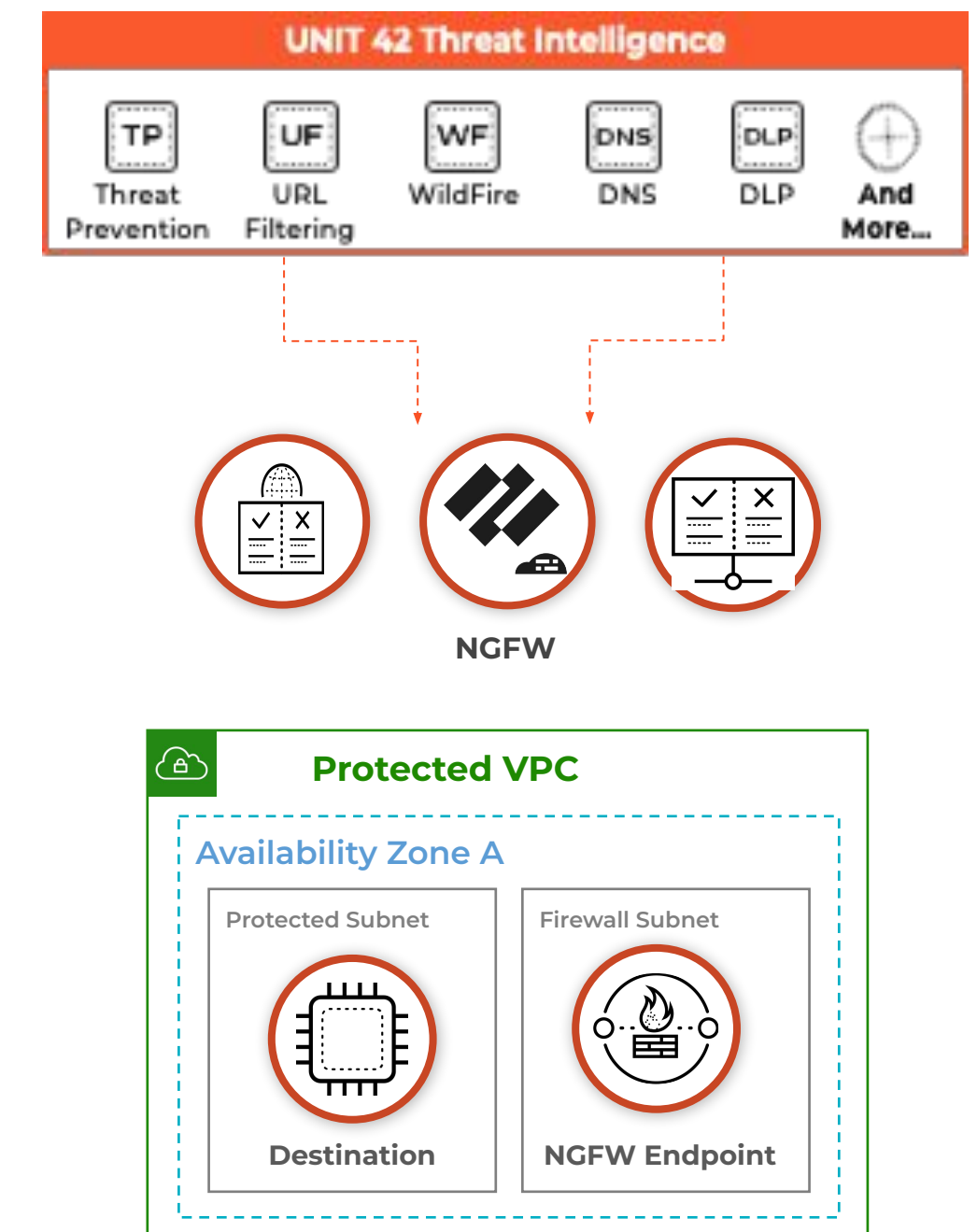
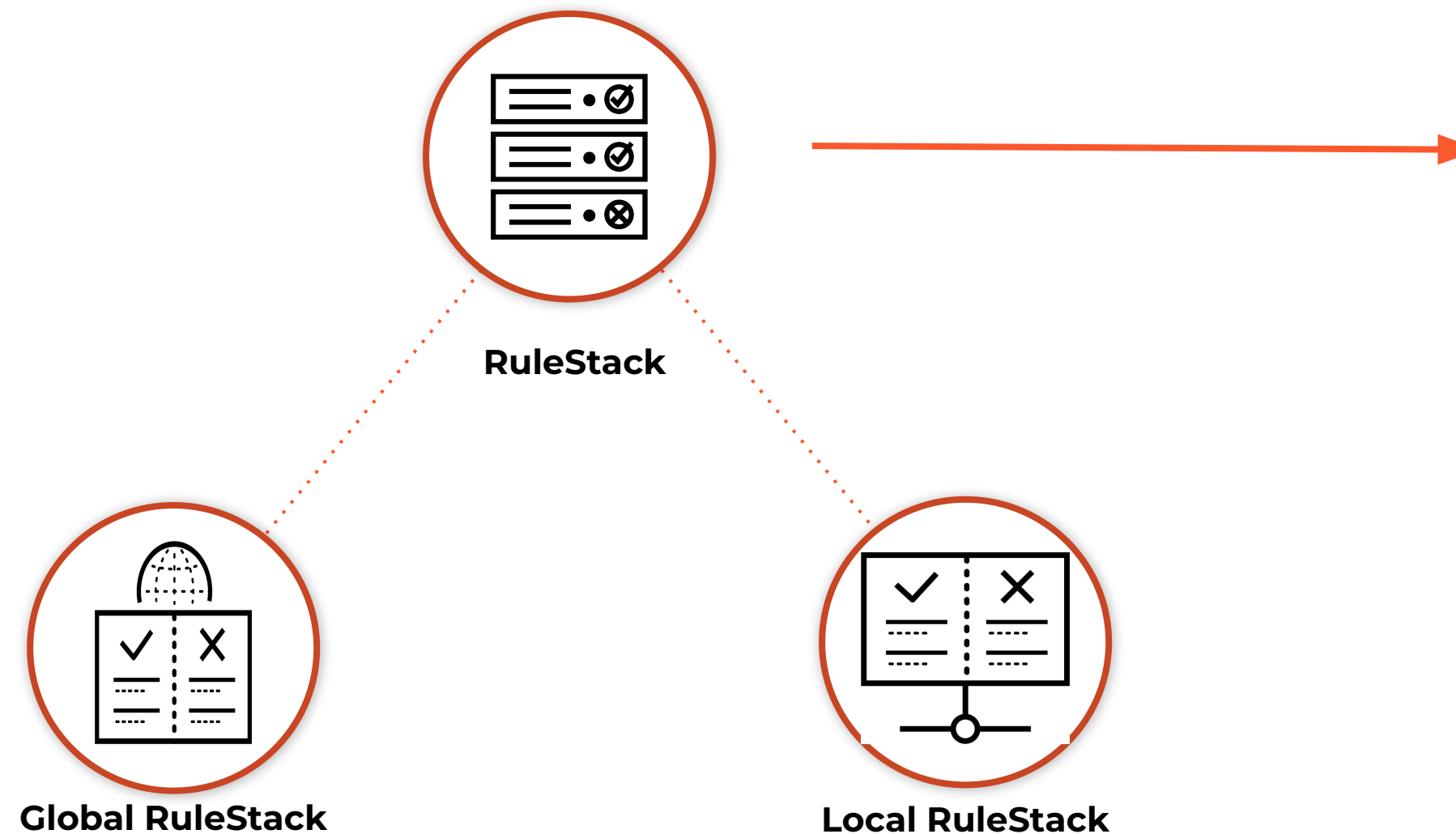
- **Security profiles**

Security profiles help you define an allow but scan rule, which scans allowed traffic for threats, such as viruses, malware, spyware, and DDOS attacks.

*** Rulestacks cannot be shared between multiple AWS regions**

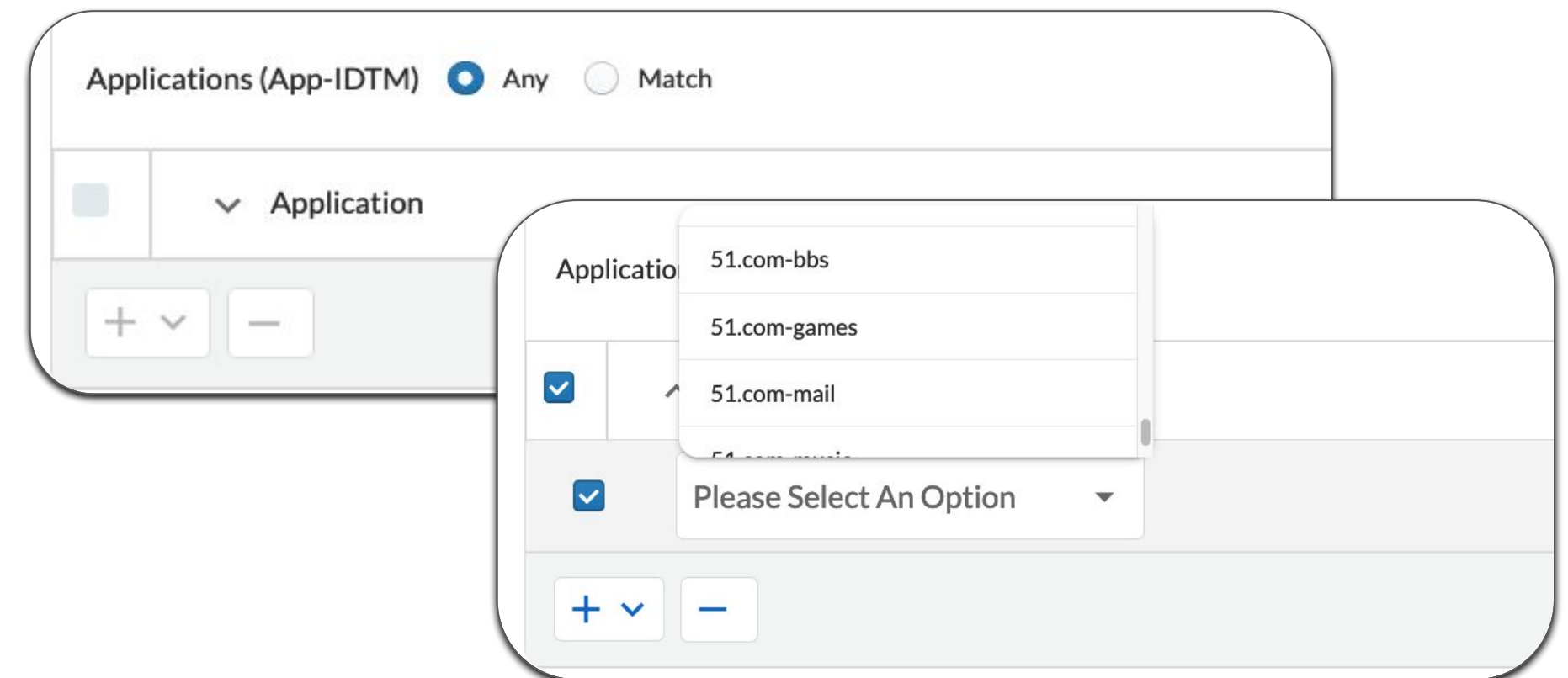
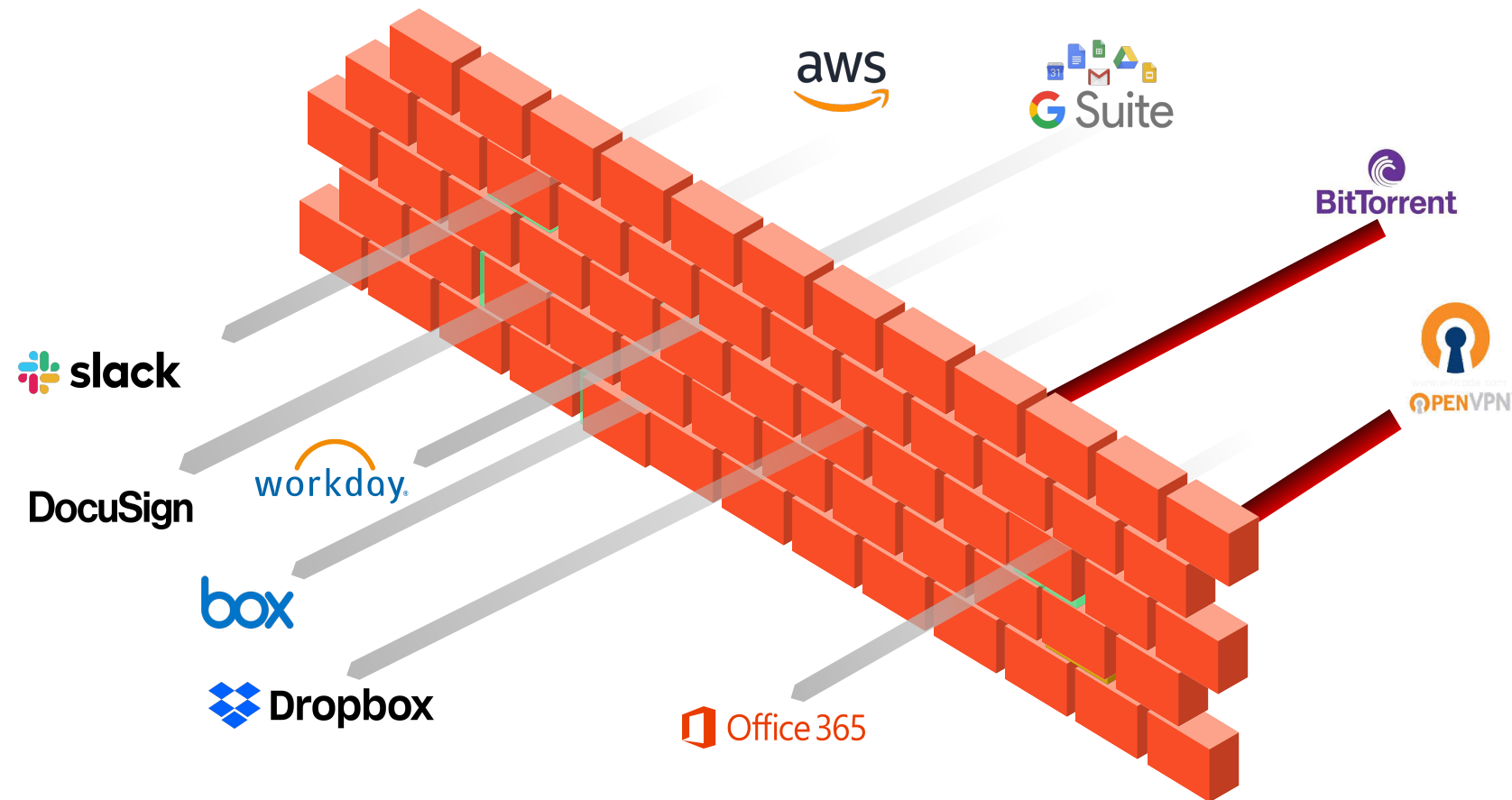
Security Components

- Local Rulestack
 - A Local Rulestack consists of local rules. As a local AWS account administrator, you can associate a local rulestack (with local rules) to an NGFW resource in your AWS account
- Global Rulestack
 - As an AWS Firewall Manager administrator, you can author and enforce a global rulestack on all NGFW resources in your AWS organization



Secure Traffic With Application-Based Control

- Move from port to application based policy
- Gain Unprecedented Application Visibility
- Reduce the surface area of cyber attacks



Programmatic Access

Enable Programmatic Access

General

External ID ff5ae49c-4

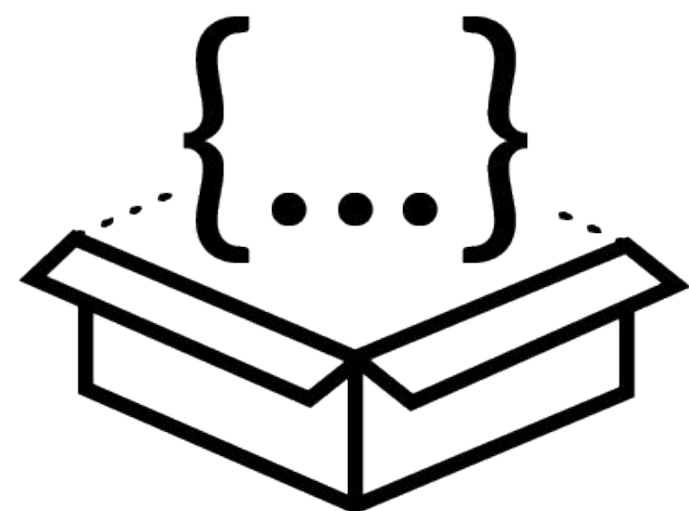
CloudNGFW Account ID 12

SNS Topic ARN arn:aws:sns:us-east-1

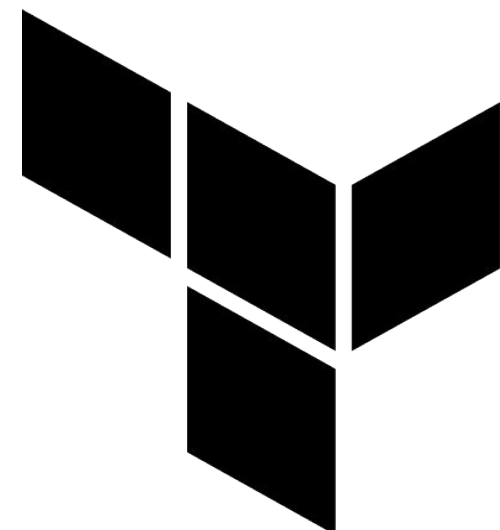
Programatic Access ☐ Disabled

To use Programmatic Access, you need to enable this option. For more information, please refer to the document [Programmatic Access](#)

Infrastructure as Code (IaC) Capabilities



Application Programming Interface



Terraform Provider



Cloud Formation Templates



Command Line Interface*

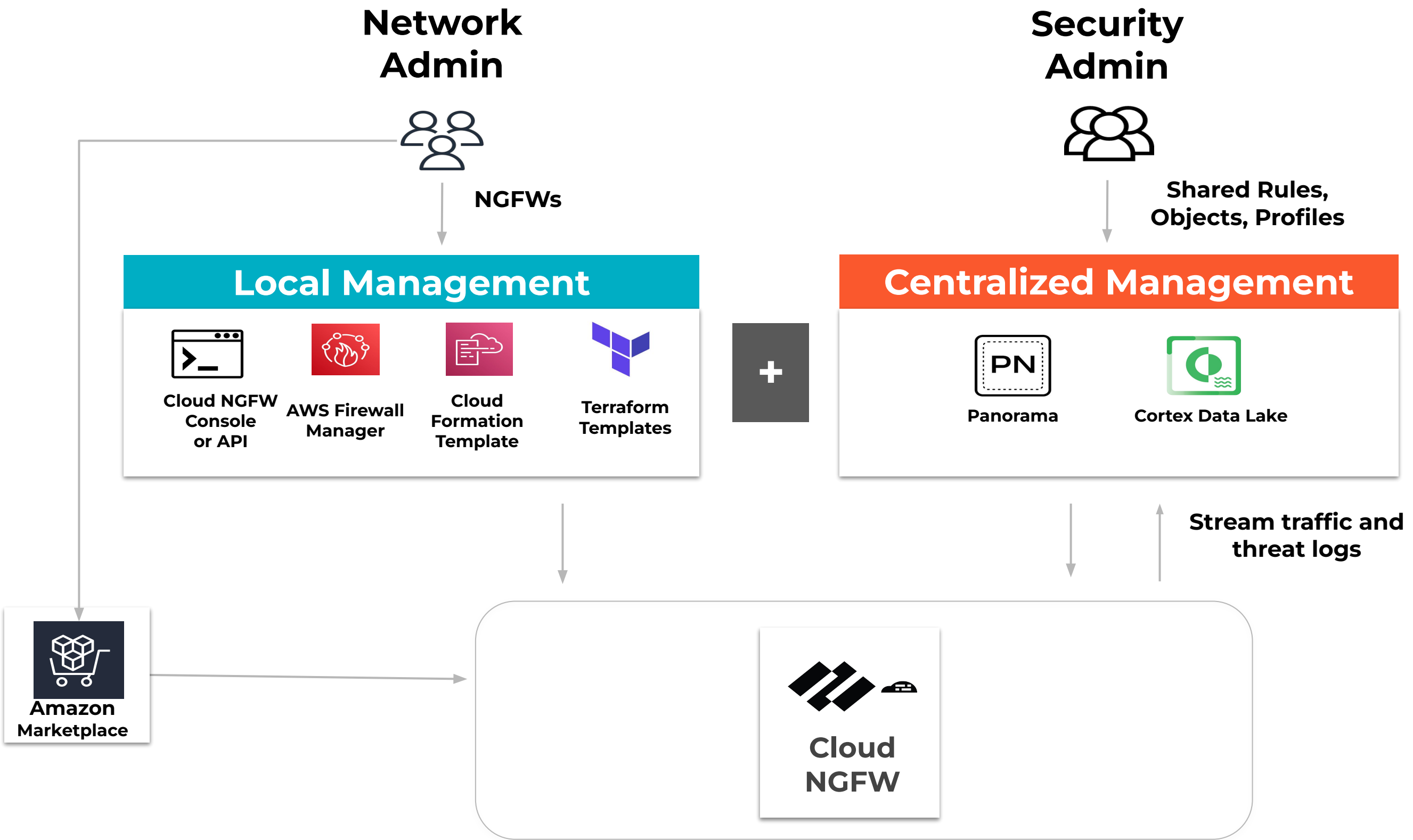


Software Development Kit*

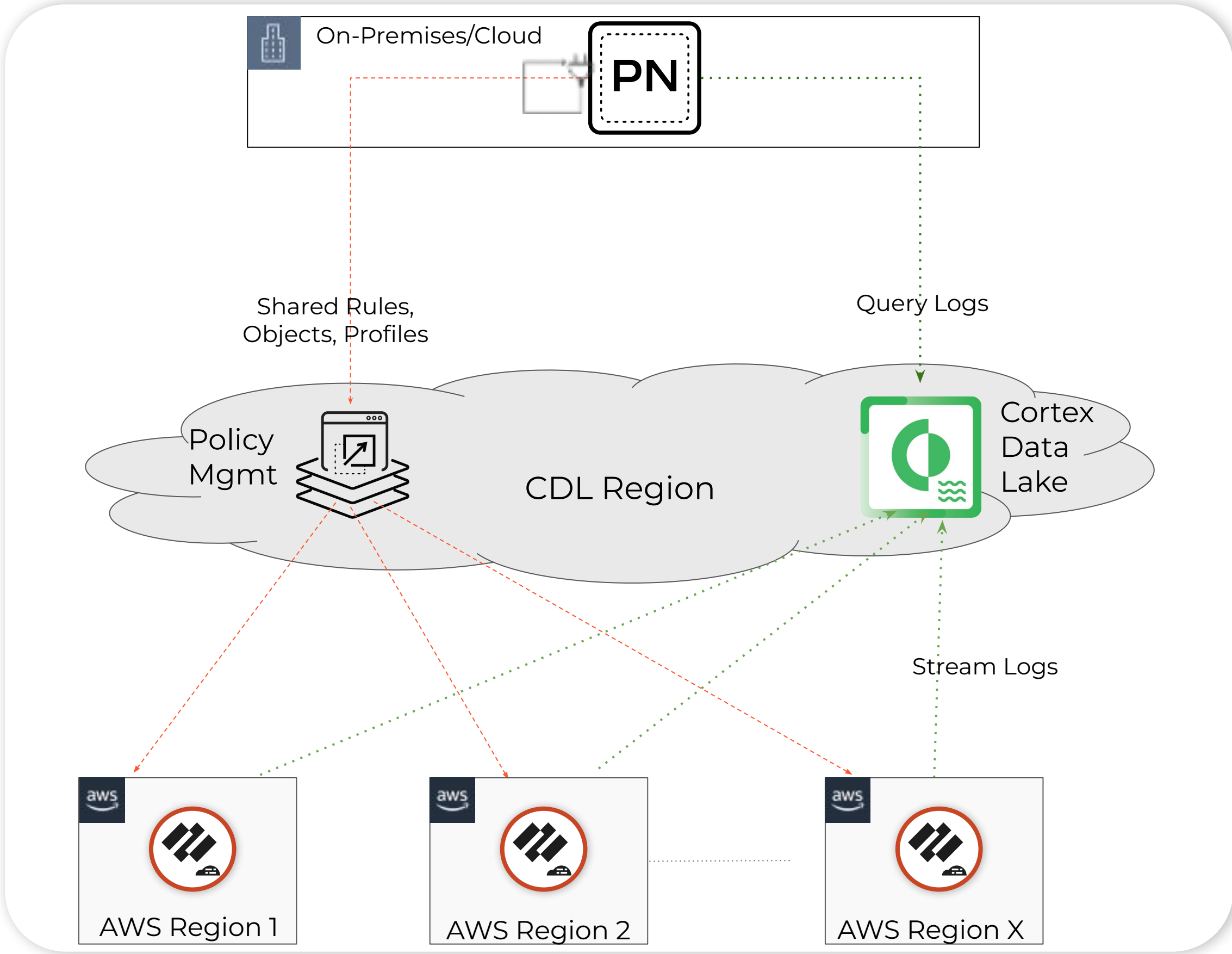
* AWS Firewall Manager only

Panorama Integration

Cloud NGFW | Fits the Way Your NetSec Teams Work



Cloud NGFW for AWS | Panorama Integration



Thank You

paloaltonetworks.com