paloalto TECHDOCS

Cloud NGFW for AWSの使用を開始する

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

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 documentation@paloaltonetworks.com.

Copyright

Last Revised

April 8, 2025

Table of Contents

Cloud NGFW for AWS の導入

どこで使用できますか?	何が必要ですか?
• Cloud NGFW for AWS	❑ Cloud NGFWサブスクリプション ❑ Palo Alto Networksカスタマー サポート アカウント (CSP) ❑ AWS Marketplaceアカウント ❑ ユーザーのロール（テナントまたは管理者）

AWS Marketplace でCloud NGFWを検出し、AWS仮想プライベート クラウド(VPC)で使用することができます。Cloud NGFWを使用すると、App-ID、URL カテゴリとジオロケーションに基づくURLフィルタリング、SSL/TLS復号化などの NGFW コア機能にアクセスできます。

Cloud NGFW コンポーネント

Cloud NGFW for AWS は、AWS 環境を保護するために連携して動作する多数のコンポーネントを作成します。

- **Cloud NGFW** テナント は、AWS ユーザーの 1 人がサービスをサブスクライブしたときに、AWS アカウントに関連付けられた Cloud NGFW サービスのインスタンス化です。Cloud NGFWは、サブスクライブしているAWSユーザーを、他のユーザーをテナントに招待できるCloud NGFWテナント(TenantAdminユーザーロール)の管理者として指定します。割り当てられた役割に基づいて、他のユーザーは Cloud NGFW リソースを作成し、テナントを使用してルールスタックを構成できます。
- **Cloud NGFW** リソース（または単に NGFW）は VPC に関連付けられており、複数のアベイラビリティゾーンにまたがることができます。このリソースには、回復性、スケーラビリティ、およびライフサイクル管理が組み込まれています。
- Cloud NGFW リソースを使用するには、目的の AWS アベイラビリティーゾーンごとに VPC に専用のサブネットを作成し、サブネット上に **NGFW** エンドポイントを作成し 、VPC ルートテーブルを更新して、これらの Cloud NGFW エンドポイントを介してトラフィックを送信します。
- ルールスタックは 、高度なアクセス制御（App-ID、URL フィルタリング）や脅威防止などの NGFW トラフィックフィルタリング動作を定義します。ルールスタックには、セキュリティ ルールのセットと、関連するオブジェクトおよびセキュリティ プロファイルが含まれます。

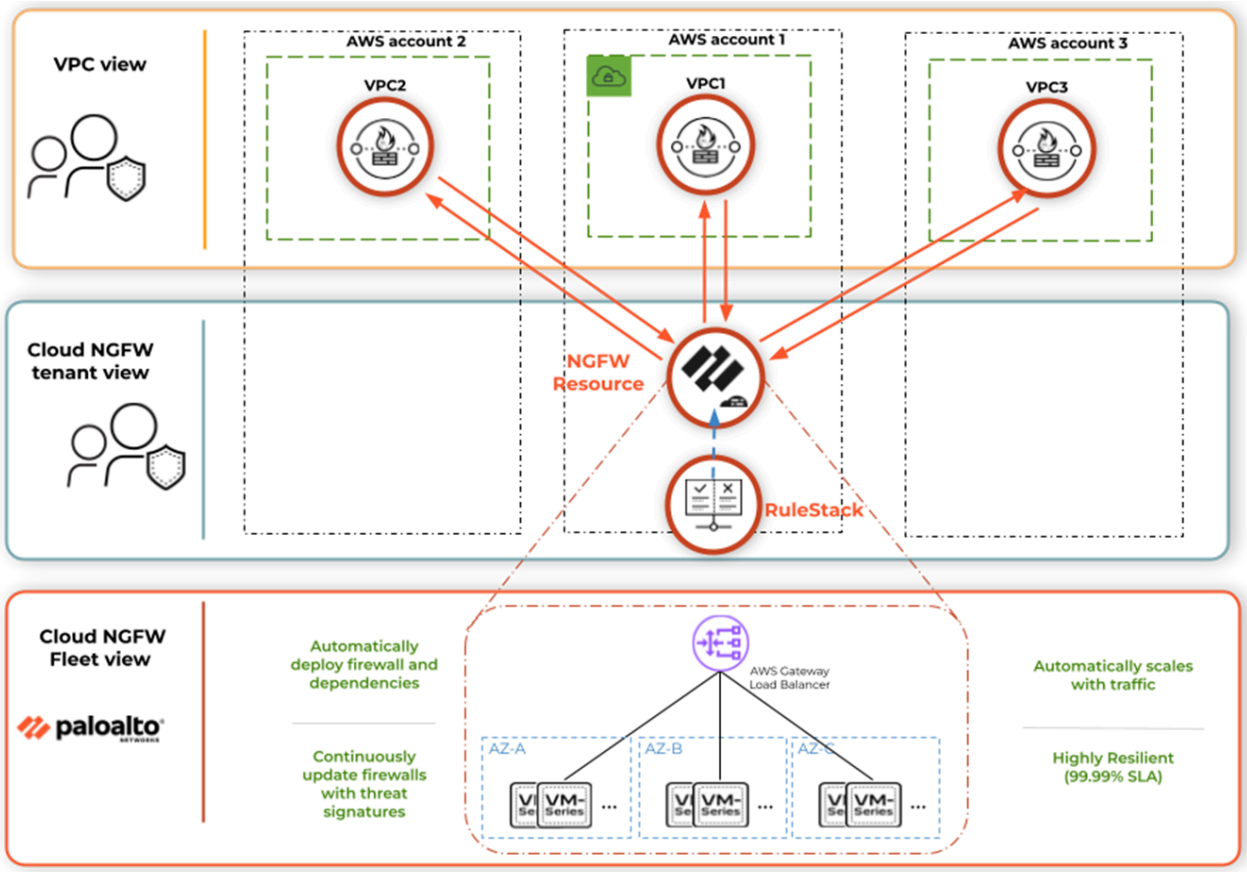
ルールスタックを使用するには、ルールスタックを 1 つ以上の NGFW リソースに関連付けます。Cloud NGFW には、2 種類のルールスタックが用意されています。

Cloud NGFW は、次の 2 種類のルールスタックをサポートしています。

- ローカルルールスタック:ローカル アカウント管理者は、ローカル ルール スタックをAWSアカウントのNGFWに関連付けることができます。ローカル ルール スタックにはローカル ルールが含まれます。
- グローバルルールスタック:AWSファイアウォール マネージャ管理者は、ファイアウォール マネージャ サービス(FMS)ポリシーを作成し、グローバル ルール スタックを関連付けることができます。AWS ファイアウォールマネージャは、AWS 組織のさまざまな AWS アカウントにあるこれらすべての NGFW にわたるグローバルルールスタックを管理します。グローバルルールスタックには、事前ルールと事後ルールが含まれます。

Cloud NGFWエンドポイントについて

NGFW は、指定した VPC 専用のファイアウォールリソースで、次世代のファイアウォール機能を提供します。作成時に、NGFWは1つ以上のVPCに関連付けられます。NGFWエンドポイントは、指定したVPCの各アベイラビリティゾーンに手動または自動で作成されるコンストラクトです。NGFWは、NGFWエンドポイントが受信するトラフィックにセキュリティ ポリシーを適用し、そのポリシーを適用します。NGFW を作成するときは、少なくとも1つのVPCとローカルルールスタックを指定する必要があります。さらに、関連付けられた NGFW エンドポイントをデプロイする方法と場所も指定する必要があります。



NGFW エンドポイントは、検査と適用のためにトラフィックを NGFW に送信する責任があります。NGFW エンドポイントはトラフィックをインターセプトし、検査とポリシー適用のために NGFW にルーティングします。2つの管理モードを使用して、エンドポイントを自動または手動で作成できます。

- サービス管理モードでは 、Cloud NGFW テナントは、指定したサブネットごとにエンドポイントを作成します。NGFW サービスは、指定した VPC 内のサブネットのリストを取得し、そのリストからエンドポイントを持つサブネットを選択します。
- カスタマー管理モードでは、指定したVPCでセキュリティ保護する必要がある既存のアベイラビリティ ゾーンを選択し、選択したアベイラビリティ ゾーンの既存のサブネットに NGFW エンドポイントを手動で作成します。NGFW を作成したら、AWS コンソールに移動して NGFW エンドポイントの作成プロセスを完了する必要があります。

NGFW エンドポイントと NGFW エンドポイントを作成したら、AWS ルートテーブルを更新して、トラフィックが NGFW に送信されるようにする必要があります。更新するルート表とその更新方法は、特定のデプロイメントによって異なります。詳細については、「トラフィックをCloud NGFWに転送」を参照してください。

Cloud NGFW の活動

1. **Cloud NGFW** サービスにサブスクライブする — まず、AWS マーケットプレイスを通じて Cloud NGFW for AWS サービスをサブスクライブします。サブスクライブ後、Cloud NGFW テナントを作成できます。サブスクライブしているAWS IAMユーザーはテナント管理者(TenantAdmin)で、そのユーザーは追加のユーザーを招待してロールを割り当てることができます。AWSアカウントをCloud NGFWテナントに追加します。アカウントを追加すると、ログの保存、NGFW エンドポイントの作成、および復号化に必要なキーへのアクセスに必要なアクセス許可が Cloud NGFW によって付与されます。
2. ルール スタックの作成 — Cloud NGFW テナント コンソールでユーザーを追加し、ロールを割り当てた後、ローカル ルール スタック管理者はローカル ルールとルール スタックを作成できます。
3. **NGFW** の作成 - NGFW ファイアウォールリソースを展開して VPC を保護します。NGFW の作成時に、以前に作成したローカルルールスタックを関連付けます。

   Cloud NGFW エンドポイントを作成するには、2 つのオプションがあります。最初の（サービス管理）オプションでは、VPC に目的の AWS アベイラビリティゾーンごとに専用のサブネットを作成し、Cloud NGFW リソースの作成時にそれらのサブネットを指定します。このオプションでは、Cloud NGFW はサブネット内に NGFW エンドポイントを作成します。または、2 番目の（顧客管理）オプションで、NGFW リソースがトラフィックを保護する目的の AWS アベイラビリティゾーンを指定します。このオプションでは、Cloud NGFW は、AWS アカウントで VPC エンドポイントリソースとして表示される Cloud NGFW リソースのみを作成します。その後、必要なAWSアベイラビリティゾーンごとにVPCに専用のサブネットを作成し、VPCエンドポイントも作成します。

4. **VPC**ルート テーブルの更新- Cloud NGFWリソースをデプロイした後、詳細についてはトラフィックをCloud NGFWに転送する必要があります。VPCルート テーブルを更新することで、トラフィックがNGFWファイアウォール リソースに送信され、検査と適用が行われます。

Cloud NGFW のユースケース

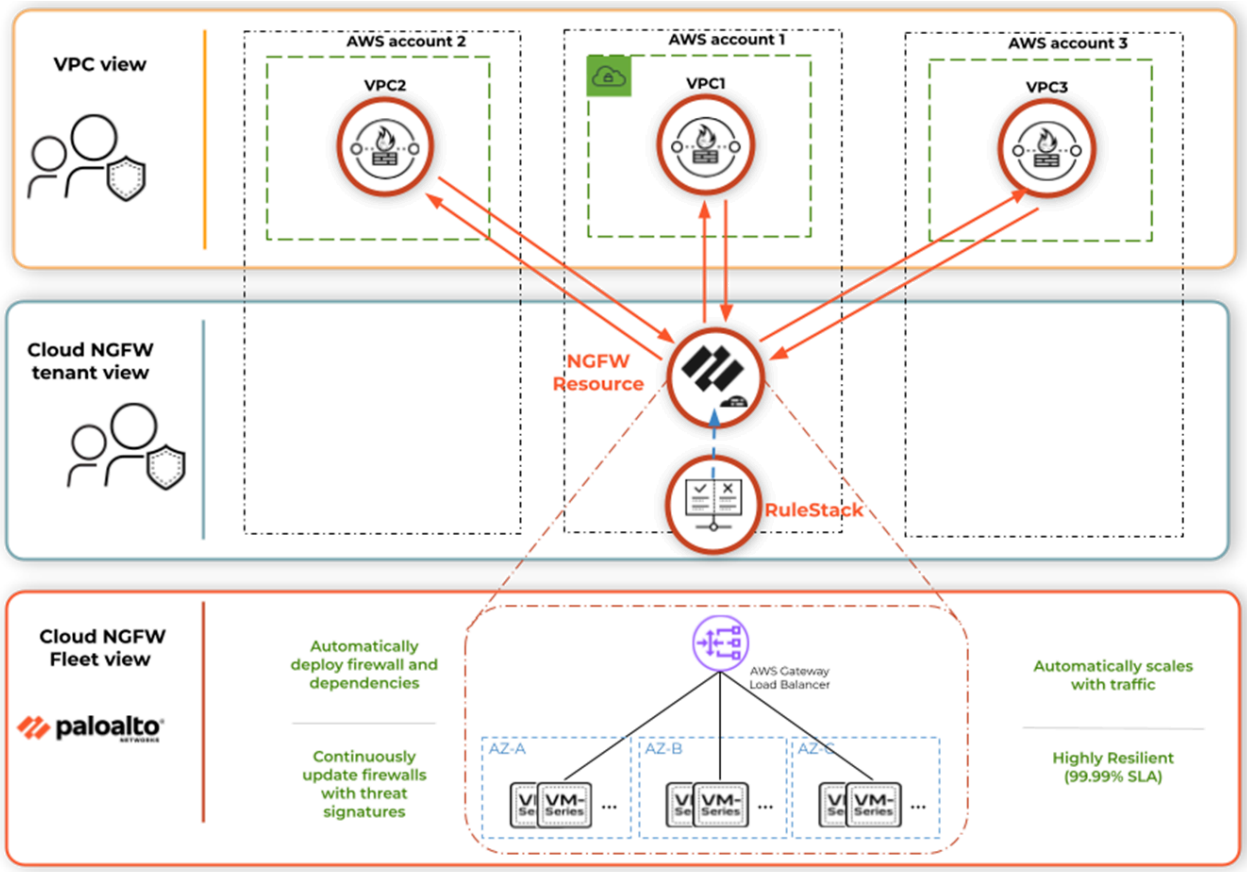
Cloud NGFW には、インバウンドトラフィック、アウトバウンドトラフィック、および East-West トラフィックを保護するためのツールと機能が用意されています。

- インバウンドトラフィックとは、AWS リージョンの外部から発信され、サーバーやロードバランサーなどのアプリケーション VPC 内のリソースにバインドされているトラフィックのことです。Cloud NGFWは、AWS セキュリティグループによって許可されたインバウンドトラフィックにマルウェアや脆弱性が VPC に入るのを防ぐことができます。
- アウトバウンド トラフィックとは、アプリケーションVPC内で発生するトラフィックを指します。このトラフィックをAWSリージョン外の宛先に転送します。Cloud NGFW は、アプリケーション VPC 内のリソースが許可されたサービスと許可された URL に接続されるようにすることで、機密データや情報の流出を防ぎ、アウトバウンドトラフィックフローを保護します。
- **East-West** トラフィックは、AWS リージョン内を移動するトラフィックです。具体的には、送信元と送信先の間のトラフィックが2つの異なるアプリケーションVPCまたは同じVPC内の2つの異なるサブネットにデプロイされます。Cloud NGFW は、AWS 環境内でのマルウェアの伝播を阻止できます。

Cloud NGFW リソースと NGFW エンドポイント

どこで使用できますか?	何が必要ですか?
• Cloud NGFW for AWS	❑ Cloud NGFWサブスクリプション ❑ Palo Alto Networksカスタマー サポート アカウント (CSP) ❑ AWS Marketplaceアカウント ❑ ユーザーのロール（テナントまたは管理者）

NGFW は、指定した VPC 専用のファイアウォールリソースで、次世代のファイアウォール機能を提供します。作成時に、NGFWは1つ以上のVPCに関連付けられます。NGFWエンドポイントは、指定したVPCの各アベイラビリティゾーンに手動または自動で作成されるコンストラクトです。NGFW は、NGFW エンドポイントが受信するトラフィックにセキュリティポリシーを適用し、そのポリシーを適用します。NGFW を作成するときは、少なくとも1つのVPCとローカルルールスタックを指定する必要があります。さらに、関連付けられた NGFW エンドポイントをデプロイする方法と場所も指定する必要があります。



NGFW エンドポイントは、検査と適用のためにトラフィックを NGFW に送信する責任があります。NGFW エンドポイントはトラフィックをインターセプトし、検査とポリシー適用のために NGFW にルーティングします。エンドポイントを自動または手動で作成するために使用できる管理モードは 2 つあります。

- サービス管理モードでは 、Cloud NGFW テナントは、指定したサブネットごとにエンドポイントを作成します。NGFW サービスは、指定した VPC 内のサブネットのリストを取得し、そのリストからエンドポイントを持つサブネットを選択します。
- カスタマー管理モードでは、指定した VPC でセキュリティ保護する必要がある既存のアベイラビリティゾーンを選択し、選択したアベイラビリティゾーンの既存のサブネットに NGFW エンドポイントを手動で作成します。NGFW を作成したら、AWS コンソールに移動して NGFW エンドポイントの作成プロセスを完了する必要があります。

NGFW エンドポイントと NGFW エンドポイントを作成したら、AWS ルートテーブルを更新して、トラフィックが NGFW に送信されるようにする必要があります。更新するルート表とその更新方法は、特定のデプロイメントによって異なります。ガイドとして役立つルート テーブルの例を含むデプロイメント例の詳細については、「トラフィックをCloud NGFWに転送」 を参照してください。

サポートされているCloud NGFWの管理およびデプロイメント機能

どこで使用できますか?	何が必要ですか?
• Cloud NGFW for AWS	❑ Cloud NGFWサブスクリプション ❑ Palo Alto Networksカスタマー サポート アカウント (CSP) ❑ AWS Marketplaceアカウント ❑ ユーザーのロール（テナントまたは管理者）

Palo Alto Networks Cloud NGFW for AWSは、以下の管理機能とデプロイメント機能をサポートしています。

NGFWのデプロイメントおよび管理	詳説	ネイティブNGFWのデプロイメント	AWSファイアウォール マネージャのデプロイメント
ツール	Cloud NGFWリソースをデプロイおよび管理するための複数の設定オプションがあります。	• Cloud NGFWコンソール • Cloud NGFW API • Cloud Formation • Terraform	• AWSコンソール • AWS API • Cloud Formation
AWSリージョン	Cloud NGFW for AWSはAWSの地域サービスです。導入するCloud NGFWは、そのAWSリージョンのVPC入出力トラフィックを保護します。	• 21	• 16
デプロイメント アーキテクチャ	Cloud NGFW for AWSには複数のデプロイメント モデルが用意されてい	• 集中型 • 分散	• 集中管理モデル • 分散モデル

NGFWのデプロイメントおよび管理	詳説	ネイティブNGFWのデプロイメント	AWSファイアウォール マネージャのデプロイメント
	ます。適切なモデルは、ユースケースと要件によって異なります。	• 結合 (マルチVPC NGFW リソース)	

サポート対象のセキュリティ ポリシー管理機能

Palo Alto Networks Cloud NGFW for AWSは、以下のセキュリティ機能をサポートしています。

セキュリティ ポリシーの管理、可視化、レポート	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
ツール	Cloud NGFWのポリシーを作成するための複数の設定オプションがあります。	• Cloud NGFWコンソール • Cloud NGFW API • Cloud Formation • Terraform	• Panoramaコンソール • Panorama API • Terraform	• SCMコンソール
ログ タイプ	Cloud NGFWは、ファイアウォールが監視するネットワーク トラフィック イベントの監査証跡となるタイムスタンプ付きのログを生成します。ログエントリには artifacts が含まれます。これはログされたイベントのプロパティ、アクティビティ、挙動です。つまり攻撃者のアプリケーションタイプや IP アドレスなどです。各ログタイプは	• トラフィック ログ • 脅威ログ • 復号化ログ • 監査ログ	• トラフィック ログ • Threat Logs（脅威ログ） • URL フィルタリング ログ • 復号化ログ	• ログ ビューアー • トラフィック ログ • Threat Logs（脅威ログ） • URL フィルタリング ログ • 復号化ログ

セキュリティ ポリシーの管理、可視化、レポート	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
	個別のイベントタイプの情報を記録します。たとえば、Cloud NGFWは、スパイウェア、脆弱性、またはウイルスのシグネチャに一致するトラフィックを記録するために脅威ログを生成します。			
ログ宛先	Cloud NGFWは、生成されたログを AWSの宛先とStrata Logging Serviceに配信できます。	• Amazon Simple Storage Service (S3) バケット • Amazon CloudWatchロググループ • Amazon Kinesis Data Firehose	• Amazon Simple Storage Service (S3) バケット • Amazon CloudWatchロググループ • Amazon Kinesis Data Firehose • Strata Logging Service • Strata Logging ServiceからSyslogサーバへのログの転送 • Strata Loggin ServiceからHTTPSサーバへのログの転送	• Amazon Simple Storage Service (S3) バケット • Amazon CloudWatchロググループ • Amazon Kinesis Data Firehose • Strata Logging Service • Strata Logging ServiceからSyslogサーバへのログの転送 • Strata Loging ServiceからHTTPSサーバへのログの転送

セキュリティ ポリシーの管理、可視化、レポート	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
ログの視覚化と分析	Cloud NGFWログを確認して、VPCトラフィックの豊富な情報を確認します。この情報の例としては、送信元、送信先、URL、ポート プロトコル、App-ID、脅威、国、URLなどがあります。	• Amazonの目的地のログを探索する	• Amazonの目的地のログを探索する • Strata Logging Serviceでログを探索する • Panoramaでログを監視する • Panoramaのアプリケーション コマンド センター (ACC) を監視する	• Amazonの目的地のログを探索する • Strata Logging Serviceでログを探索する • Strata Cloud Managerのアクティビティに関するインサイト • Strata Cloud Managerコマンド センター
レポート	VPCトラフィックのアプリケーション、脅威、URL アクティビティに関する事前定義済みレポートとカスタム レポートを生成します。	—	• スケジュールされたレポートとカスタム レポート	• スケジュールされたレポートとカスタム レポート
ポリシー分析と最適化	ルールの使用状況を監視することで、ポリシーの実装が施行ニーズに引き続き適合しているかどうかを評価することができます。 ポリシー アナライザーはCloud	—	• ルールの使用状況 • ポリシー オプティマイザー	• ルールの使用状況 • ポリシー オプティマイザー

セキュリティ ポリシーの管理、可視化、レポート	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
	NGFWルールを分析し、目的のセキュリティ態勢に合わせて特定のルールを統合または削除する方法を推奨します。また、ルールベースにシャドウ、冗長性、ジェネラライゼーション、相関関係、統合などの異常がないかチェックします。			
パケット キャプチャ	Palo Alto Networksファイアウォールを使用して、カスタム パケット キャプチャまたは脅威パケット キャプチャを実行します。	—	—	—

ポリシーとポリシー オブジェクト	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
セキュリティ ポリシー	セキュリティ ポリシーは、VPCトラフィックを脅威や中断から保護	• ローカル ルールスタック	• セキュリティ ポリシー • プレルール • ポストルール	• セキュリティ ポリシー • プレルール • ポストルール

ポリシーとポリシー オブジェクト	詳説	ネイティブポリシー管理（ルールスタック）	Panorama ポリシー管理 (クラウド デバイス グループ)	Strata Cloud Manager(SCM)ポリシー管理
	します。送信元と宛先のセキュリティ ゾーン、送信元と宛先のIPアドレス、アプリケーション、ユーザー、サービスなどのトラフィック属性に基づいて、個々のセキュリティ ポリシー ルールがセッションをブロックするか許可するかを決定します。	• グローバル ルールスタック	• デフォルトのルール	• デフォルトのルール
アドレス	IPv4アドレス、FQDN、またはワイルドカード アドレス (IPv4アドレスの後にスラッシュとワイルドカード マスクが続く) を含むアドレス オブジェクトを指定できます。	• プレフィックス リスト • FQDNリスト	• IPv4ネットマスク • IPv4範囲 • IPv4ワイルドカード マスク • FQDN	• IPv4ネットマスク • IPv4範囲 • IPv4ワイルドカード マスク • FQDN
アドレス グループ	同じポリシーを実施する必要のある特定の送信元アドレスまたは宛先アドレスをグループ化できます。	—	• アドレス グループ	• アドレス グループ

ポリシーとポリシー オブジェクト	詳説	ネイティブポリシー管理（ルールスタック）	Panorama ポリシー管理 (クラウド デバイス グループ)	Strata Cloud Manager(SCM)ポリシー管理
リージョン	郡などの地理的な場所に基づいて、IPアドレスからの (またはIPアドレスへの) トラフィックを許可またはブロックできます。リージョンは、ポリシーのソースと宛先を指定するときにオプションとして使用できます。国の標準リストから選択するか、カスタム地域/地理的位置とそれに関連するIPアドレスを指定できます。	• 国	• 事前定義された地域 • カスタム地域	• リージョン
サービス (ポートとプロトコル)	ネットワーク上の特定のポートへのVPCトラフィック セッションの使用を細かく制御できます (つまり、アプリケーションのデフォルト ポートを定義できます)。ファイアウォールには、service-httpとservice-httpsという 2 つ	• ポートとプロトコル	• サービス	• サービス

ポリシーとポリシー オブジェクト	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
	の事前定義サービスが含まれています。これらのサービスでは、TCPポート80および8080をHTTPに、ポート443をHTTPSに使用します。ただし、任意のTCP/UDPポートで任意のカスタム サービスを作成できます。	TCPポー		
サービス グループ	同じセキュリティ設定を持つサービスをサービス グループに結合して、セキュリティ ポリシーのルールの数を減らすことができます。	—	• サービス グループ	• サービス グループ
外部ダイナミック リスト	IPアドレス、ドメイン、またはURLの動的リストを使用して、VPCトラフィックを細かく制御できます。外部Webサーバーでホストされているファイルに保存されます。Palo Alto	• インテリジェンス フィード • 組み込みフィード • EDLホスティング サービス フィード	• 外部動的リスト • 内蔵EDL • EDLホスティング サービス リスト	• 外部動的リスト • 内蔵EDL • EDLホスティング サービス リスト

ポリシーとポリシー オブジェクト	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
	Networksは 、組み込みの (Bulletproof、High-Risk、Known Malicious、およびTor Exit IPアドレス) EDLも提供しています。さらに、Palo Alto Networksは、Microsoft 365、Azure、Amazon Web Services (AWS)、Google Cloud Platform (GCP) のIPアドレスの動的なリストを維持する無料の EDL ホスティング サービスを提供しています。これらのEDLを使用して、VPCのIngressおよびEgressトラフィックを制御できます。			
アプリケーション	アプリケーション シグネチャに基づいてネットワーク内のアプリケーションを正確に識別する Palo Alto Networks App-ID™ トラフィック分類シ	• アプリID	• アプリID • カスタム アプリケーション シグネチャ	• アプリID • カスタム アプリケーション シグネチャ

ポリシーとポリシー オブジェクト	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
	ステムを使用して、VPC トラフィックを細かく制御できます。			
アプリケーション グループ	同じポリシーの適用を必要とする一連のApp-IDをグループ化できます。	—	• アプリケーション グループ	• アプリケーション グループ
アプリケーション フィルタ	現在のApp-IDと特定の属性に一致する将来のApp-IDをグループ化するアプリケーション フィルターを定義することで、VPCトラフィックを細かく制御できます。たとえば、カテゴリ、サブカテゴリ、テクノロジー、リスク、特性など、1つ以上の属性ごとのアプリケーション フィルタの作成が可能です。今後は、コンテンツの更新に基づいて新しいApp-IDがCloud NGFWに導入さ	—	• アプリケーション フィルタ	• アプリケーション フィルタ

ポリシーとポリシー オブジェクト	詳説	ネイティブポリシー管理（ルールスタック）	Panorama ポリシー管理 (クラウド デバイス グループ)	Strata Cloud Manager(SCM)ポリシー管理
	れるたびに、フィルター条件に一致するすべての新しいアプリケーションが自動的にセットに追加されます。			
アプリケーション オーバーライド	ファイアウォールを通過する特定のトラフィックの通常のアプリケーション ID (App-ID) をオーバーライドするように Cloud NGFW を構成できます。アプリケーション オーバーライド ポリシーが有効になるとすぐに、トラフィックのそれ以降のすべての App-ID 検査が停止され、指定したカスタム アプリケーション シグネチャを使用してセッションが識別されます。	—	• アプリケーション オーバーライド	• アプリケーション オーバーライド
tags	タグを使用すると、キーワードまたは語句を使用してオブジェ	—	• tags	• tags

ポリシーとポリシー オブジェクト	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
	クトをグループ化できます。アドレス オブジェクト、アドレス グループ（静的および動的）、アプリケーション、ゾーン、サービス、サービス グループ、およびポリシー ルールにタグを適用できます。			
動的ユーザー グループ	ローカル データベース、外部データベースまたは一致条件からユーザーのリストを作成し、それらをグループ化できます。	—	—	—
デバイス	Device Dictionary（デバイス ディクショナリ）とも呼ばれるこのページには、デバイス オブジェクトのメタデータが含まれています。	—	—	—

証明書と復号化	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
証明書管理	Cloud NGFWは、証明書を使用してインテリジェントフィードにアクセスし、インバウンドおよびアウトバウンドの復号化を有効にします。各証明書には、平文を暗号化したり、暗号化テキストを復号化したりするための暗号化キーが含まれています。また、発行者の ID を認証するためのデジタル署名も含まれています。	• AWS Secrets ManagerのTLS/SSL 証明書	• 自己署名ルートCA証明書 • 証明書および秘密鍵のインポート • AWS Secrets ManagerのTLS/SSL 証明書 • 証明書の生成 • 外部CAからの証明書の取得 • オンライン証明書状態プロトコル (OCSP) レスポンダー • デフォルトの信頼されたCA • 証明書プロファイル	• 管理:証明書の管理 クラウド証明書は*Cloud NGFW*ではまだサポートされていません。
復号	Cloud NGFWは、ポリシーベースの決定として、VPCのIngressおよびEgressトラフィックを復号化、検査、再暗号化できます。どのVPCトラフィックを復号	• SSLアウトバウンド復号化 • SSL インバウンド インスペクション	• 復号ポリシー • 復号化プロファイル • SSLフォワード プロキシ (アウトバウンド復号化) • SSL インバウンド インスペクション	• 復号の管理

証明書と復号化	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
	化し、どのトラフィックを復号化できないか、および指定されたトラフィックに対して実行するSSL復号化のタイプを細かく制御できます。復号化を有効にするには、セッションに対して信頼できる第三者として機能するために必要な証明書をセットアップします。		• SSH プロキシ • サーバー証明書の確認 • 復号化の例外 • SSL 復号化を一時的に無効にする	

セキュリティ サービス	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
IPS脆弱性防御	脆弱性防御は、攻撃者がシステムの脆弱性を悪用してネットワークに侵入しようとするインバウンドの脅威から保護します。システムの脆弱性は、バッファ オーバーフロー、不正なコード実行などの形で現れる	• ベストプラクティス	• デフォルトのプロファイル • 厳格なプロファイル • カスタム プロファイル (脅威の例外) • カスタム脆弱性シグネチャ • Snort/ Suricataのシグネチャ	• 脆弱性防御

セキュリティサービス	詳説	ネイティブポリシー管理（ルールスタック）	Panorama ポリシー管理 (クラウド デバイス グループ)	Strata Cloud Manager(SCM)ポリシー管理
	可能性があります。			
アンチスパイウェア	アンチスパイウェアは、AWS VPC 内の (サイバー攻撃を利用した) マルウェアに感染したワークロードによって開始される、特にコマンド アンド コントロール (C2) アクティビティなどのアウトバウンドの脅威を検出してブロックします。スパイウェアのホーム電話通信を識別するためのカスタム正規表現パターンを定義することもできます。	• ベストプラクティス	• デフォルトのプロファイル • 厳格なプロファイル • カスタム プロファイル (脅威の例外) • カスタム スパイウェア シグネチャ • Snort/Suricataのシグネチャ	• アンチスパイウェア
ファイルブロッキング	ファイル ブロックを使用すると、指定された方向 (インバウンド/アウトバウンド/両方) のVPC トラフィック内のファイル タイプを細かく制御できます。脅威	• ベストプラクティスとカスタマイズ	• 基本プロファイル • 厳格なプロファイル • カスタム プロファイル	• ファイルブロッキング

セキュリティサービス	詳説	ネイティブポリシー管理（ルールスタック）	Panorama ポリシー管理 (クラウド デバイス グループ)	Strata Cloud Manager(SCM)ポリシー管理
	を含むことが知られているファイルや、アップロードやダウンロードに実際の使用例がないファイルを積極的にブロックできます。			
Antivirus（アンチウイルス）	アンチウイルスは、VPCトラフィック内の圧縮ファイル、実行ファイル、PDFファイル、HTMLおよびJavaScriptウイルスに隠されたマルウェアを検出し、保護します。	• ベストプラクティス	• デフォルトのプロファイル • カスタム プロファイル (脅威の例外)	• Anti-Virus:
WildFire分析	Cloud NGFWは、VPC トラフィック内のファイルと実行可能ファイルを検出し 、分析のためにWildFire™クラウド サービスに転送するほか、特定のファイルに対してインラインML分析も実行します。ファイルに脅	—	WildFire分析	WildFire分析

セキュリティサービス	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
	威が検出されると、WildFire はマルウェアをブロックする保護を作成し、5 分以内にその脅威に対する保護を世界中に配布します。			
URL フィルタリング	URLフィルタリングは、インライン分析を実行し、Palo Alto Networks が管理する URLカテゴリまたは指定したカスタム カテゴリと比較することで、VPCトラフィックを分析し、VPCワークロードによってアクセスされるURL (クリアテキストと暗号化されたトラフィックの両方) を制御します。	• Palo Alto Networksが管理するURLカテゴリのアクセス制御 • カスタム URL カテゴリ	• Palo Alto Network が管理するURLカテゴリとカスタムURLカテゴリのアクセス制御 • クラウドインライン分類	• Palo Alto Networkが管理するURLカテゴリとカスタムURLカテゴリのアクセス制御 • クラウドインライン分類
DNS セキュリティ	DNSセキュリティは、DNSトンネリング、ドメイン生成アルゴリズム (DGA) の検出、マルウェア ドメインなどの脅威	—	DNS セキュリティ	DNS セキュリティ

セキュリティ サービス	詳説	ネイティブポリシー管理（ルールスタック）	Panorama ポリシー管理 (クラウド デバイス グループ)	Strata Cloud Manager(SCM)ポリシー管理
	からVPCからのアウトバウンドDNS要求を保護します 。			
データ フィルタリングとエンタープライズDLP	データ フィルタリングは、VPCトラフィック内の機密情報（クレジットカード番号、社会保障番号、社内文書など）を検出し、このデータがAWS環境から出ないようにします。 Enterprise DLPを使用すると、クラウドベースの分析による事前定義されたデータ パターンのリストを使用して、VPCトラフィックで高度なデータ フィルタリングのメリットを享受できます。	—	• 事前定義済みパターン、正規表現、ファイル プロパティ • Enterprise DLP	*DLP*は現在*SCM*ではサポートされていません。
セキュリティ プロファイル グループ	セキュリティ プロファイル グループは、単位として扱われ、セキュリティ ポリシーに簡単に追加できるセ	—	• セキュリティ プロファイル グループ	• セキュリティ プロファイル グループ

セキュリティサービス	詳説	ネイティブポリシー管理（ルールスタック）	Panorama ポリシー管理 (クラウド デバイス グループ)	Strata Cloud Manager(SCM)ポリシー管理
	キュリティ プロファイルのセットです。			

セキュリティゾーンと保護	詳説	ネイティブポリシー管理（ルールスタック）	Panorama ポリシー管理 (クラウド デバイス グループ)	Strata Cloud Manager(SCM)ポリシー管理
セキュリティゾーン数	セキュリティゾーンは、ファイアウォール上のインターフェースと Cloud NGFW エンドポイントをグループ化して、VPC トラフィックを制御およびログに記録する論理的な方法です。	—	プライベートゾーンとパブリック ゾーン	—
ゾーン プロテクション	ゾーン プロテクションは、フラッド攻撃、偵察攻撃、パケットベースの攻撃からネットワーク セキュリティゾーンを防御します。	—	ゾーン プロテクション	—

ネットワークサービス	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
XFF	VPCワークロードへのトラフィックは、Cloud NGFWに到達する前に、複数のプロキシ サーバー (CDNやALB など) を通過する可能性があります。既存のXFFヘッダーがある場合、これらのプロキシはそれにIPアドレスを追加するか、IPアドレスを含むXFFヘッダーを追加します。したがって、XFF リクエスト ヘッダーには、カンマで区切られた複数のIPアドレスが含まれる場合があります。Cloud NGFWは、X-Forwarded-For (XFF) HTTPヘッダー フィールドを使用して、元のクライアントIPアドレスを識別します。NGFWは常に、XFF ヘッ	• ポリシーでのXF ヘッダーのサポート • ログ内の XFF 値を表示する	• XFF 値をポリシー内で使用する • ログ内の XFF 値を表示する • レポート内のXFF値を表示する	*XEF*は現在*SCM*ではサポートされていません。

ネットワークサービス	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
	ダーに最後に追加されたアドレスを使用してポリシーを適用します。			
NAT	Palo Alto Networksファイアウォールは、Ingress VPCトラフィックに送信元NATを適用し、Egress VPCトラフィックに宛先NATを適用できます。	出口NAT	出口NAT	—
DNS プロキシ	Cloud NGFWをDNS プロキシとして設定すると、ファイアウォールはクライアントとサーバー間の中継役として機能します。また、DNS キャッシュからのクエリを解決したり、クエリを別の DNS サーバーに送信したりすることで、DNS サーバーとしても機能します。このページは、ファイアウォールが	—	—	—

ネットワークサービス	詳説	ネイティブポリシー管理（ルールスタック）	Panorama ポリシー管理 (クラウド デバイス グループ)	Strata Cloud Manager(SCM)ポリシー管理
	どのような方法で DNS プロキシとして機能するかを設定する場合に使用します。			
インターフェース管理	Palo Alto Networksファイアウォールでは、VLAN、バーチャルワイヤ、Link Layer Discovery Protocol (リンクレイヤ ディスカバリ プロトコル - LLDP)、双方向転送検出（BFD）をインターフェース上で構成できます。	—	—	—
QoS	Palo Alto Networksファイアウォールを使用すると、優先処理または帯域幅制限を必要とするトラフィックを指定できます。QoSルールを使用すると、限られたネットワーク容量でも優先度の高いアプリケーション	—	—	—

ネットワーク サービス	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
	とトラフィックを確実に実行できます。			
ルーティング管理	Palo Alto Networksファイアウォールを使用すると、静的ルーティングとルーティング プロトコル (BGP、BFD、OSPF、OSPFv3、マルチキャスト、RIPv2、フィルター) を構成できます。	—	—	—
IPSecトンネル管理	Palo Alto Networksファイアウォールはは、IPSecトンネルを終了し、トンネルトラフィックを検査します。	—	—	—
GlobalProtect管理	Palo Alto Networksファイアウォールは、GlobalProtectゲートウェイ モジュールとクライアント間のVPNトンネルで認証と暗号化のアルゴリズムを指定することにより、モバイル	—	—	—

ネットワークサービス	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
	ワーカーを保護します。			
GREトンネル管理	Palo Alto Networksファイアウォールは、Generic Routing Encapsulation (GRE) トンネルを終了し、トンネル化されたトラフィックを検査します。	—	—	—
SD-WAN リンク管理	Palo Alto Networks ファイアウォールは、複数の WAN 接続 (ADSL/DSL、ケーブルモデム、イーサネット、ファイバー、LTE/3G/4G/5G、MPLS、マイクロ波/無線、衛星、Wi-Fi) を仮想インターフェースにバインドし、アプリケーションとサービス、および各アプリケーションまたはサービスが使用できるリンクの条件に基づいて、動的でインテリジェント	—	—	—

ネットワーク サービス	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
	なパス選択をサポートします。			
ポリシー ベース フォワーディング	Palo Alto Networksファイアウォールのポリシー ベース転送ルールにより、セキュリティまたはパフォーマンス上の理由からトラフィックが代替パスを取ることが可能になります。たとえば、本社と支店が、安価なインターネットと高価な専用線の 2 つのリンクで接続されているとします。セキュリティを高める場合は、PBF を使用して、FTP などのアプリケーションによって生成される非暗号化トラフィックは専用線を介して送信し、その他のトラフィックはインターネット経由で送信します。また、パフォーマンスを	—	—	—

ネットワーク サービス	詳説	ネイティブポリシー管理（ルールスタック）	**Panorama** ポリシー管理 **(**クラウド デバイス グループ**)**	**Strata Cloud Manager(SCM)**ポリシー管理
	高める場合は、基幹業務アプリケーションのトラフィックは専用線を通すようにルーティングし、Web ブラウジングなど、その他のすべてのトラフィックは安価なリンクを介して送信します。			

AWS Marketplaceからはじめる

どこで使用できますか?	何が必要ですか?
• Cloud NGFW for AWS	❑ Cloud NGFWサブスクリプション ❑ Palo Alto Networksカスタマー サポート アカウント (CSP) ❑ AWS Marketplaceアカウント ❑ ユーザーのロール（テナントまたは管理者）

AWS MarketplaceからCloud NGFWを利用するには、いくつかの方法があります。重要な判断基準は、AWSファイアウォールマネージャを使用してCloud NGFWと連携するかどうかです。

- **AWS**メンバーズ アカウントから—メンバーのAWSアカウントからPalo Alto Networks Cloud NGFW for AWS Marketplace SaaSリスティングを購読できます。サブスクリプションごとに固有のCloud NGFWテナントが作成されます。

  その後、他の複数のAWSアカウントをCloud NGFWテナントに追加して、Cloud NGFWリソース（NGFWとも呼ばれる）を作成し、AWSアカウントのVPCに関連付けることができます。これらのNGFWに関するセキュリティ ポリシールールを作成し、Cloud NGFWテナントの使用状況を監視して、計測レコードをAWS Marketplace Metering Serviceに送信します。AWSはこの情報を使用して顧客に請求書を発行します。

  次に、AWSアカウント内で、このリソースのNGFWエンドポイント（VPCエンドポイントとも呼ばれる）を追加します。次に、すべてのトラフィックを検査のためにNGFWエンドポイントにルーティングするVPCルートルールを追加します。AWSはNGFWエンドポイントに送信されたトラフィックを自動的にNGFWリソースにリダイレクトして検査します。NGFWエンドポイントに送信されたトラフィックは常に同じ NGFW エンドポイントに戻されます。NGFW は「ワイヤ内のバンプ」として動作します。

  この方法で開始すると、この*Cloud NGFW*テナントで*AWS*ファイアウォールマネージャを使用することはできません。

- **AWS**ファイアウォールマネージャ管理者アカウントから開始する—現在、AWSファイアウォールマネージャを使用してAWS組織全体のセキュリティグループやその他のネットワー

クセキュリティ機能を管理している場合、同じAWSファイアウォールマネージャを使用して、AWS組織全体の複数のアカウントやVPCにNGFWを展開できます。

Cloud NGFWリスティングのAWS Marketplaceサブスクリプションは、AWS組織の指定されたAWSファイアウォールマネージャ管理アカウントから開始します。

次に、AWSファイアウォールマネージャ ポリシー ワークフローを使用してグローバル ルールスタックを作成し、AWS Organization内の複数のAWSアカウントにNGFWをすばやく展開します。内部では、ファイアウォールマネージャがすべてのコンポーネントを調整します。これには、Cloud NGFW APIを呼び出してNGFWを作成したり、AWS APIを呼び出して顧客のVPCにNGFWエンドポイントを作成したりすることが含まれます。

AWSファイアウォールマネージャとCloud NGFW for AWSの統合の詳細については、AWSファイアウォールマネージャの統合ブログとビデオを参照してください。

この方法を開始したら、必ず*AWS*ファイアウォールマネージャを使用して*AWS*アカウントを*Cloud NGFW*テナントに追加する必要があります。

AWSメンバー アカウントのスタート ガイド

どこで使用できますか?	何が必要ですか?
• Cloud NGFW for AWS	❑ Cloud NGFWサブスクリプション ❑ Palo Alto Networksカスタマー サポート アカウント (CSP) ❑ AWS Marketplaceアカウント ❑ ユーザーのロール（テナントまたは管理者）

Cloud NGFWサービスに登録するには、以下のステップを完了します。Cloud NGFW SaaSサブスクリプションは、PAYG（従量課金制）で登録できます。

この手順では、最初のユーザー（テナント管理者）を作成するプロセスを開始します。テナント管理者は、Cloud NGFW サービスの最高レベルのユーザーです。Cloud NGFW サービスに AWS アカウントを追加し、追加のユーザーをオンボードする機能を提供します。

Cloud NGFW for AWS Credits 契約にサインアップする前に、*Cloud NGFW PAYG SaaS* サブスクリプションを作成します。

- Cloud NGFW PAYG SaaS サブスクリプション
- SSOとMFAを使用して現在のCloud NGFWアクセスを保護する
- 複数テナントでサポートされる単一ユーザーのマルチテナントユーザー
- 複数のAWSアカウントを追加する

Cloud NGFW PAYG SaaS サブスクリプション

AWS 環境で Cloud NGFW for AWS にサブスクライブしてデプロイする前に、次のことを考慮して作成する必要があります。サブスクリプション プロセス中に、CloudFormationテンプレート（CFT）で以下に説明するパラメーターを定義して、初期設定を完了します。

- エンドポイント設定（必須） — クロスアカウントIAMロールには、Cloud NGFWがVPCリソース情報を読み取ることを許可するアクセス許可が含まれています。これは、NGFWエンドポイントの構成に必要です。
- エンドポイントの作成（任意） — Cloud NGFWを設定して、AWS環境で NGFWエンドポイントを作成および管理できます。［はい］を選択すると、VPCで必要なエンドポイントを作成および管理するための Cloud NGFW 権限が付与されます。**[**いいえ**]**を選択した場合は、NGFWエンドポイントを手動で作成して表示する 必要があります。

- ロギングの権限（任意） — Cloud NGFW を使用すると、トラフィック、脅威、および復号化ログを S3 バケット、Cloudwatch ロググループ、または Kinesis Data Firehose に送信できます。Cloud NGFW がこれらのログを目的の宛先に送信するには、必要な権限を提供する必要があります。

  Cloud NGFW コンソールから AWS CloudFormation コンソールにリダイレクトされ、スタックの作成を求められます。このスタックは、クロスアカウントの IAM ロールを設定し、ロギング先を指定し（作成はしません）、Cloud NGFW が AWS アカウントの Secrets Manager にある証明書にアクセスして復号できるようにします。

  スタックは、CloudWatch ロググループと Kinesis Data Firehose 配信ストリームのロギング宛先に、**PaloAltoCloudNGFW** という宛先を事前設定します。S3 バケットフィールドは事前設定されていません。ログを別の宛先に送信する場合は、スタックの作成を完了する前に、その宛先を作成し、デフォルト値の名前を置き換える必要があります。

  S3 バケットのログ宛先には、宛先バケットの名前を指定する必要があります。

  Kinesis Data Firehose を使用している場合、その配信ストリームのソースは**Direct PUT** でなければなりません。

- 監査ログ（任意） — 管理者のアクティビティを追跡する監査ログを Cloudwatch ロググループに送信できます。CFT スタックには、**PaloAltoCloudNGFWAuditLog** という名前のデフォルトの Cloudwatch ロググループの宛先が含まれています。デフォルトの名前値で Cloudwatch ロググループを作成することも、デフォルト値を別の Cloudwatch ロググループの名前に置き換えることもできます。

- 復号化の権限（任意） — Cloud NGFW を使用して暗号化されたトラフィックフローを検査するには、Cloud NGFW が AWS シークレットマネージャから必要な証明書を取得できるようにする必要があります。CFT スタックの起動時にタグを指定して、Cloud NGFW が属性ベースのアクセス制御を使用できるようにする必要があります。

  デフォルトでは、CFT には **PaloAltoCloudNGFW** というタグが含まれます。デフォルトこのタグを変更するには、サービスで ARN を設定し、CFT でデフォルト値を置き換えます。

Cloud NGFW PAYG SaaS サブスクリプションでサブスクライブするには、この手順を完了します。

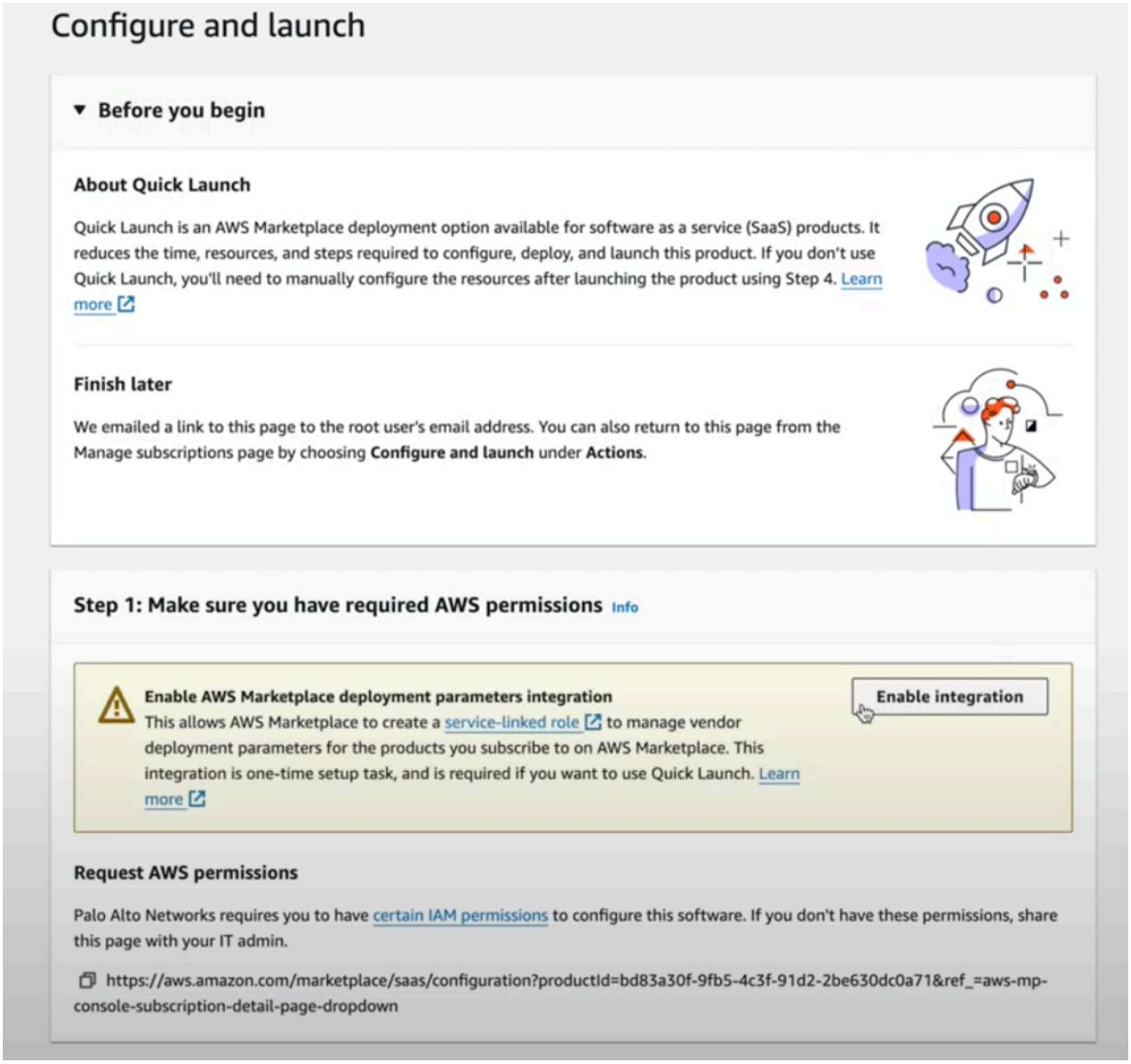
STEP 1 | AWS コンソールにログインします。

STEP 2 | AWS Marketplace で Cloud NGFW for AWS に移動します。

STEP 3 | ［登録]をクリックします。

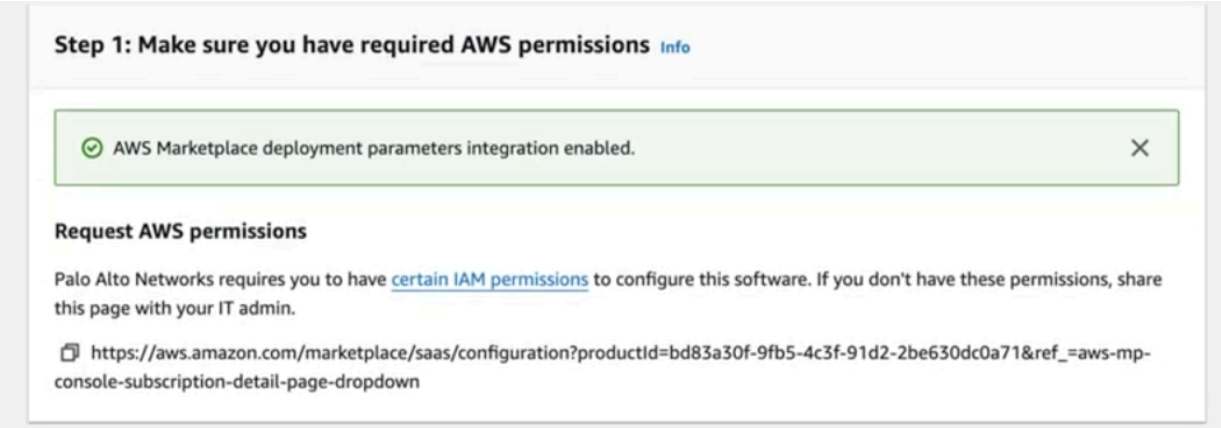
STEP 4 | ［製品のセットアップ]をクリックします。これにより、AWS Marketplaceの[Configure and Launch (SaaS Quick Launch)(設定して起動(SaaSクイック起動))]ページが起動します。Palo

Alto Networksは、クイック起動でCloud NGFW製品を有効にし、クイック起動を使用して新しいテナントを作成および展開できるようになりました。



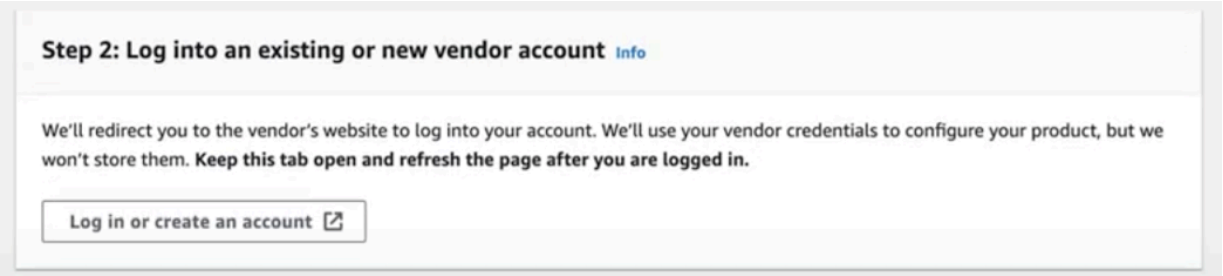
STEP 5 | クイック起動の［Configure and Launch(構成と起動)］ページで**[Enable integration(統合を有効にする)]**をクリックし、AWSから必要なIAM権限を持っていることを確認します。

新規ユーザーの場合は、*[Configure and Launch(構成と起動)]*ページのステップ*1*に*[Enable integration(統合を有効にする)]*ボタンが自動的に表示されます。



STEP 6 | **[Login or create an account(ログインまたはアカウントを作成する)]**ボタンをクリックして、既存のアカウントにサインインするか、ベンダーのウェブサイトで新しいアカウントを作

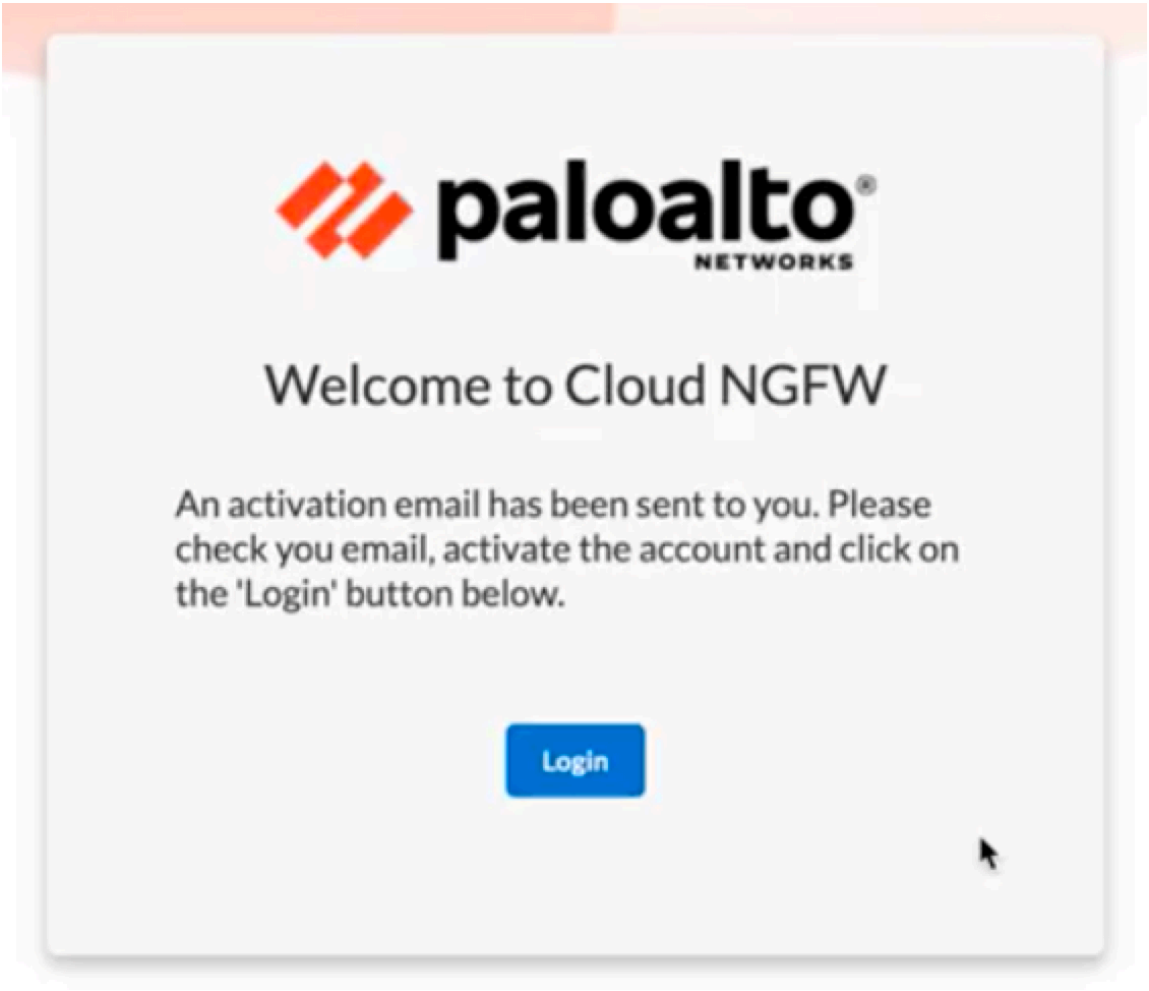
成します。これにより、Cloud NGFW for AWSテナントのテナント作成登録ページが表示されます。



1. 新規ユーザーの場合は、Cloud NGFWアカウントを作成する必要があります。電子メールアドレスを入力します。

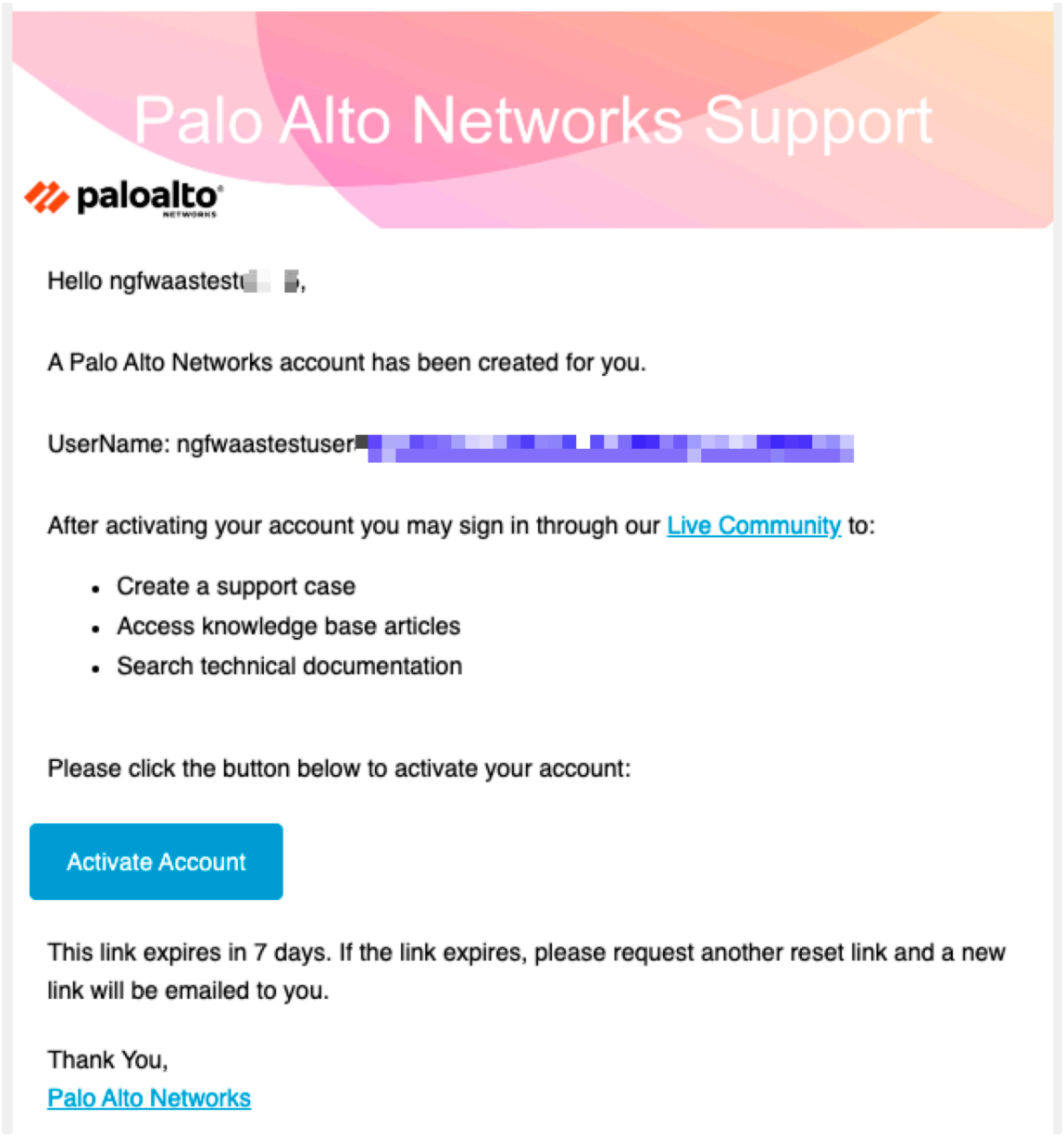
   Cloud NGFW サービスに初めてログインするときは、同じ電子メールを使用する必要があります。さらに、初回ログイン時に、この電子メール アドレスを使用して最初のユーザー（テナント管理者）が作成されます。さらに、テナント管理者によって招待されたユーザーの電子メールアドレスドメインは、テナント管理者のログイン資格情報の電子メールアドレスドメインと一致する必要があります。
2. 姓と名を入力します。
3. 作成をクリックします。

   ［**Create(作成)**］をクリックすると、上で入力した電子メールアドレスにアクティベーションボタン付きの電子メールが送信されます。

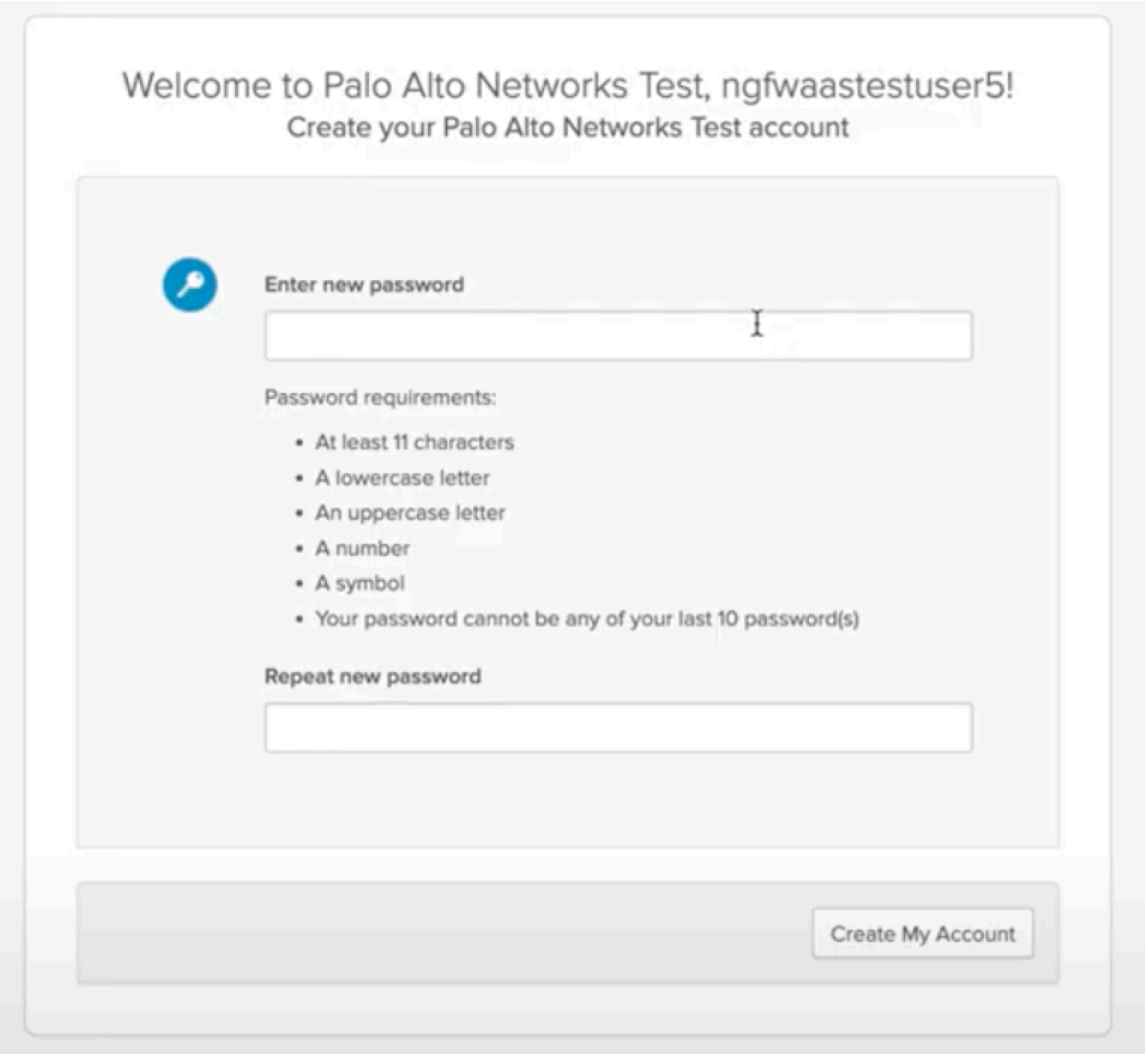


4. 届いたメールの**[Activate Account(アカウント有効化)]**ボタンをクリックします。

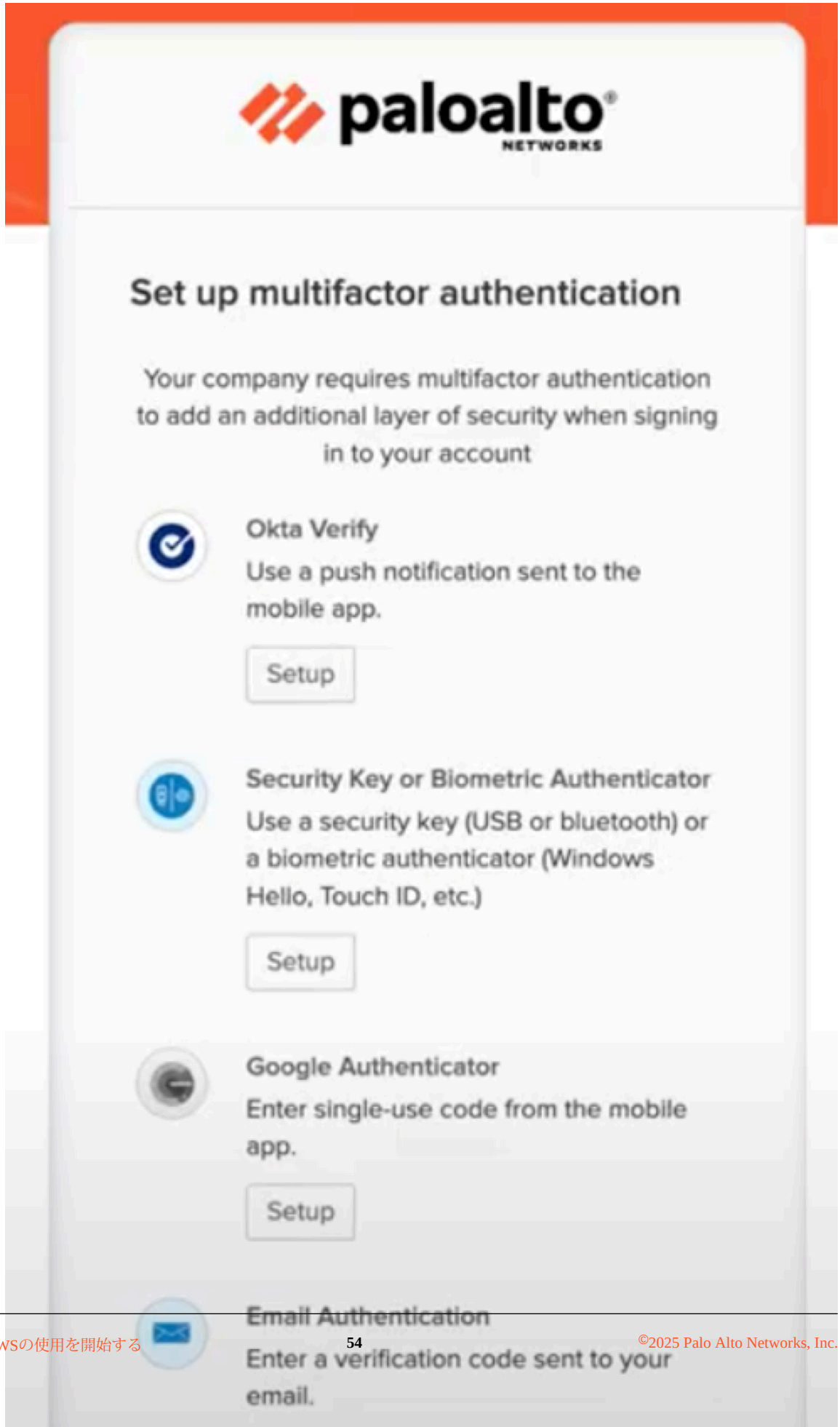
   リンクは7日間有効です。7日以内にリンクをクリックしない場合、アクティベーションメールを再送するようリクエストする必要があります。



5. 新しいパスワードを入力して再入力します。
6. **[Create My Account (**アカウントを作成**)]** をクリックします。



7. MFA（多要素認証）を設定します。

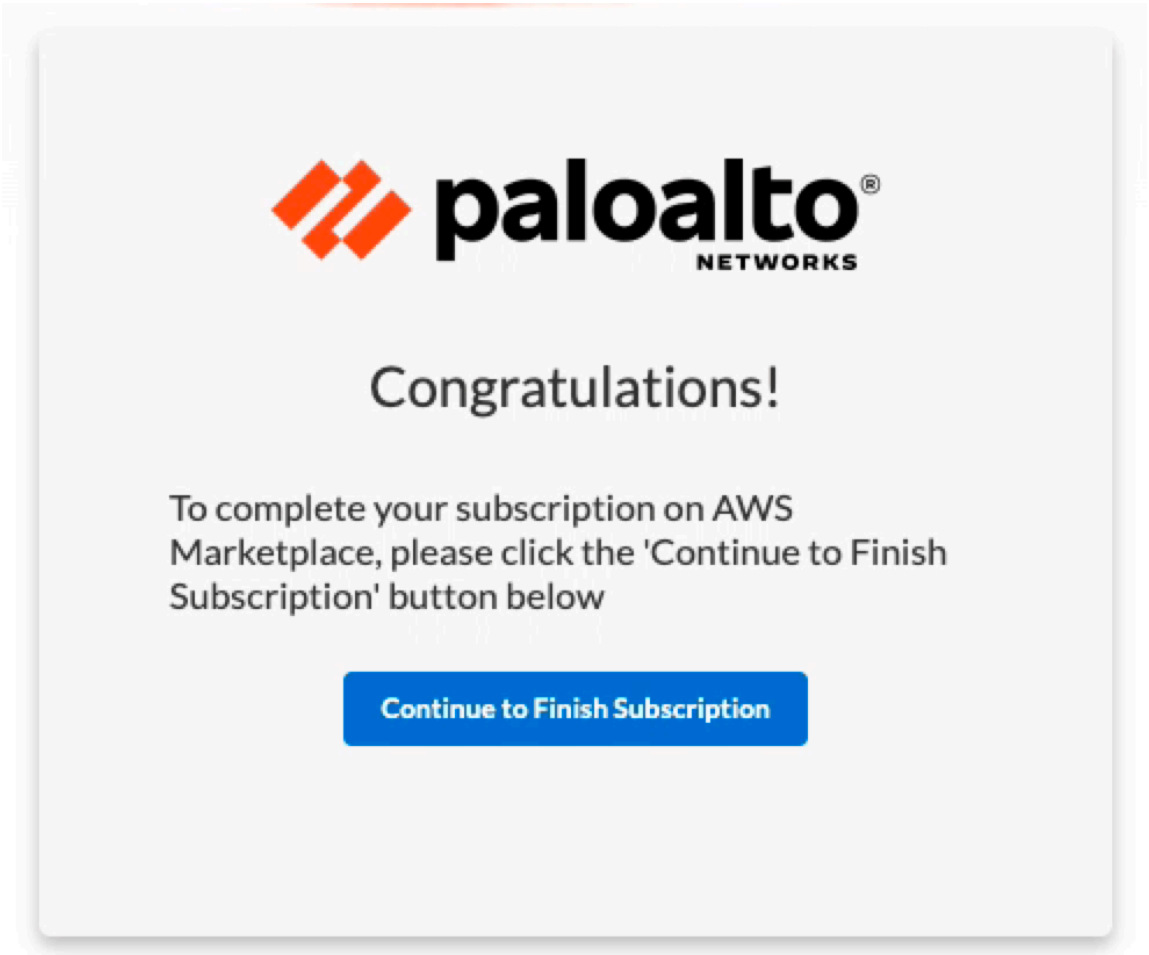


*MFA*に登録していないが*SSO*パスワードがわかっている場合は、いずれかのアプリケーションへの初回ログイン時に*MFA*への登録を求められます。*MFA*をリセットするには、サポートチケットを上げます。

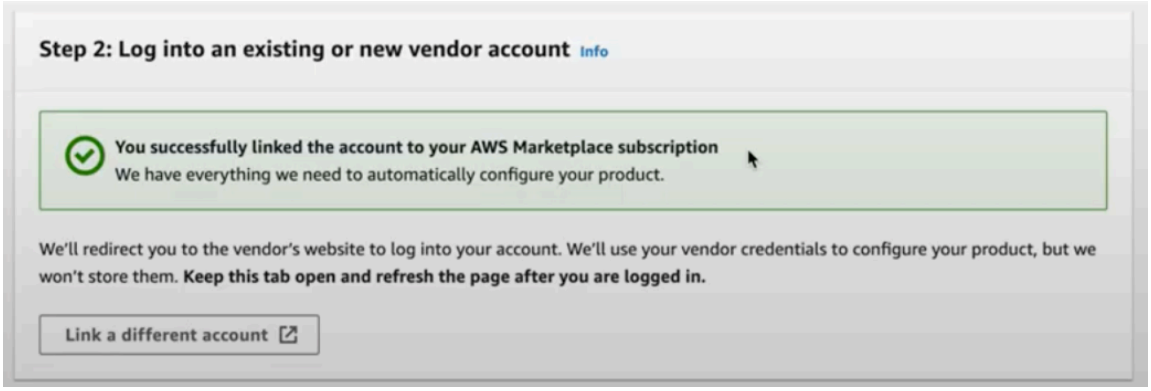
8. MFAのいずれかの方法を選択し、［**Setup(**セットアップ**)**］をクリックします。
9. MFAの確認プロセスを完了します。たとえば、[Email Authentication(電子メール認証)]の[Setup(セットアップ)]ボタンをクリックすると、[**Send me the code(**コードを送信**)**]ボタンをクリックするように求められます。クリックすると、認証コードが記載されたメールが届きます。確認コードを入力し、**[Verify(**確認**)]**をクリックします。また

は、Okta Verify、Security Key、Biometric Authenticator、またはGoogle Authenticatorを使用してMFA検証プロセスを完了することもできます。

10. 登録したメールアドレスとパスワードでテナントにサインインし、**[Continue to Finish Subscription(続行してサブスクリプションを終了する)]**をクリックします。



11. クイック起動ページに、アカウントをAWS Marketplaceサブスクリプションに正常にリンクしたことが示されました。



1. SSOに登録していない既存のユーザーで、同じメールIDを使用して新しいテナントを作成する場合は、テナントにログイン後にアクティベーションメールが届きます。手順6d～6kに従ってテナントを登録します。

   *Cloud NGFW*の既存ユーザーでテナント管理者ではない場合、*MFA*は現在利用できません。*MFA*登録を求めるメッセージは表示されずに、引き続きログインできます。

2. SSOに登録している既存のユーザーで、同じメールIDを使用して新しいテナントを作成する場合は、テナントを選択して**[Continue(**続行**)]**をクリックします。

STEP 7 | **[Launch Template(**テンプレートの起動**)]**をクリックしてCFTリージョンを選択し、テナントの役割と権限を作成します。

Cloud NGFW は、新しいブラウザタブで指定した AWS アカウントに関連付けられた AWS CloudFormation テンプレート（CFT）コンソールを開きます。ポップアップブロッカーがインストールされている場合、新しいタブがブロックされる可能性があります。この場合、Cloud NGFW コンソールで [AWS アカウント] を選択し、追加した AWS アカウントを見つけます。**[Status(**ステータス**)]**列で**[Pending(**保留中**)]**をクリックします。

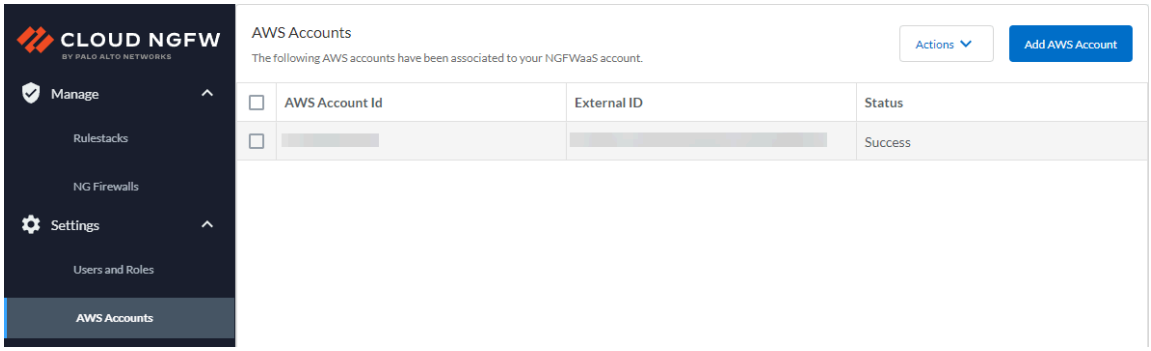
STEP 8 | CFT コンソールの下部にある [機能] セクションで、［私は、**AWS CloudFormation**が**IAM**リソースを作成する可能性があることを認めます**]**を確認します。

STEP 9 | ［スタックの作成］をクリックします。サブスクリプションに関連付けられたCFT（PaloAltoNetworksCrossAccountRoleSetup）が表示されます。

STEP 10 | ［製品の起動］をクリックします。

1. 電子メールアドレスとパスワードを入力し、［ログイン］をクリックします。
2. **AWS** アカウントを選択します。
3. ステータスが**Success**に変わったことを確認します。

AWS が *CFT* の起動を完了するまで、*Onboarding Status* は保留中状態のままです。

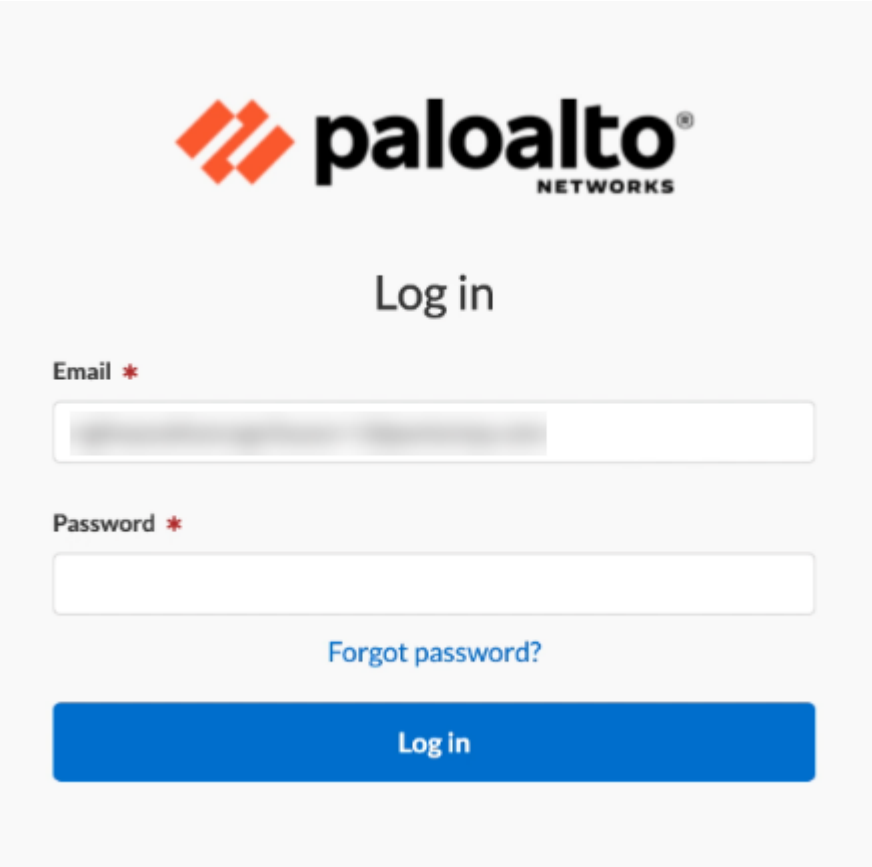


*SAML 2.0*は、*Cloud NGFW for AWS*の*ID*プロバイダーとして使用できます。詳細については、「Common Servicesによるサードパーティ アイデンティティ プロバイダの統合の管理」および「サードパーティ アイデンティティ プロバイダ(IDP)を有効にする方法」を参照してください。

SSOとMFAを使用して現在のCloud NGFWアクセスを保護する

このセクションの情報を使用して、既存の認知ユーザーをSSOに移行します。Cloud NGFW for AWSの既存ユーザーの場合、ログインや既存テナントへのアクセスには、既存テナントのSSOやMFA（SSO＋MFAでユーザーメールを有効化）などの追加セキュリティ対策の登録が必要です。

STEP 1 | AWS Cloud NGFWに登録したメールアドレスを入力し、［**Log in(ログイン)**］をクリックします。



STEP 2 | パスワードを入力して **[Log in(ログイン)]** をクリックします。

STEP 3 | Palo Alto Networksシングル サインオン（SSO）への登録を求められます。

STEP 4 | **[Continue(**続行**)**］をクリックしてSSOへの登録を続行します。または、**[Register Later(**後で登録**)]**をクリックして以前のログイン資格情報で続行することもできます。ただし、ログインを試みるたびにSSOへの登録が求められます。

STEP 5 | SSOに登録するための手順が記載されたメールが届きます。指示に従い、上記の方法でSSOとMFAへの登録を完了します。

STEP 6 | **Continue**（続行） をクリックします。

STEP 7 | 次回のログイン時に、SSOを使用してログインし直すための**[Enable and Log Out(**有効にしてログアウト**)]**ボタンが表示されます。

STEP 8 | メールアドレスを入力し、[Log in(ログイン)]をクリックします。[SSO Sign In(SSOサインイン)]ページが表示されます。

STEP 9 | メールアドレスを入力し、**[Mext(**次へ**)]**をクリックします。

STEP 10 | パスワードを入力して **[Log in(**ログイン**)]** をクリックします。

STEP 11 | MFAの検証プロセスを完了します。SSO認証情報でログイン後、Cloud NGFWテナントページにアクセスできるようになります。

複数テナントでサポートされる単一ユーザーのマルチテナントユーザー

Cloud NGFW for AWSは、複数のテナントの単一ログイン認証情報をサポートしています。Cloud NGFWコンソールにログインすると、ログイン資格情報を使用してユーザーを適切なテナントに

関連付けます。複数のテナントに同じログイン資格情報が使用されている場合、ログインページでは、設定するテナントを選択するように求められます。

Cloud NGFWにログインしたら、ドロップダウンメニューを使用して適切なテナントを選択し、［**Continue(**続行**)**］をクリックします。

次の表は、マルチテナント シナリオのユースケースを示しています。

ユースケース	手順
ユーザーAは既にテナントAに登録しており、ユーザーAはテナントBに招待されています。	アクティベーションメールは届きません。
ユーザーAはすでにテナントAに登録しており、AWS Marketplaceのサブスクリプションを通じて新しいテナントに登録します。	アクティベーションメールは届きません。

複数のAWSアカウントを追加する

同じテナントに複数のAWSアカウントをオンボードできます。オンボーディングすると、複数のアカウントでファイアウォール リソースを作成できます。さらに、任意のAWSアカウントのファイアウォール リソースのオンボードアカウント全体にCloud NGFWエンドポイントを展開できるようになります。

AWSアカウントのサブスクリプションは、AWS Marketplaceサービスの強化されたサブスクリプション エクスペリエンスと統合されます。この統合は、Cloud NGFWテナントを作成するときに行われます。AWSアカウントはCloud NGFWテナントにリンクします。

複数の*AWS*アカウントサブスクリプションをテナントに追加できます。*Cloud NGFW*は最大*200*アカウントまでサポートしています。

Cloud NGFWコンソールからテナントに複数のAWSアカウントをオンボードできます（新しいサブスクリプション要件はありません）。テナントのオンボーディング済みのすべてのAWSアカウントでファイアウォール リソースを作成します。

使いやすさを考慮して、テナントには存在する請求アカウントは1つだけです。請求アカウントがAWS Marketplaceから登録解除される場合、テナントの次の請求アカウントが動的に選択されます。追加のアカウント状態変更は、テナント内のAWSアカウントのライフサイクルをより適切に管理するために導入されています。最後のAWSアカウントがテナントから登録解除されると、テナントにアクティブな契約が添付されていない場合、テナントリソースのクリーンアップがトリガーされます。

テナントごとに*10*個の保留アカウントがサポートされます。

Cloud NGFWは、マルチアカウントテナントのサポートに加えて、マルチVPCファイアウォール リソースモデルをサポートしています。マルチVPCのサポートにより、Cloud NGFWを有効にして、複数のAWS VPCでトラフィックを保護できます。Cloud NGFWの使用量は、トラフィックを保護するためにNGFWがプロビジョニングされているAWS可用性ゾーンごとに支払います。

[Create Firewall(ファイアウォールの作成**)**］ページの**[Endpoint Management(**エンドポイントの管理**)**］セクションを使用して、これらの可用性ゾーンで NGFWのエンドポイントを作成する方

法を管理します。NGFW用に作成したVPC（ゲートウェイロードバランサー）エンドポイントごとにAWSに料金をお支払いいただきます。

マルチVPCファイアウォール リソースを使用する場合は、以下の点を考慮してください。

- マルチVPCファイアウォールは、お客様管理モードでのみサポートされます。
- 複数のVPCファイアウォールリソースのエンドポイントは、正常にオンボードされたアカウントの任意のVPCに存在する可能性があります。複数のVPCファイアウォール リソースに対して50のエンドポイントがサポートされます。
- ファイアウォール リソースのマルチVPC機能を無効にすると、エンドポイントはAnchor VPC（およびAnchorアカウント）にのみ存在できます。Anchorは、可用性ゾーンへの復元力のある接続を表します。Anchor VPCとAnchor Accountは、作成時にVPCとファイアウォール リソースに関連付けられたアカウントを参照します。Anchor Account とVPCの外部にエンドポイントが存在する場合、VPC との通信は失敗します。
- テナントからアカウントを削除する場合、マルチVPCファイアウォールのすべてのエンドポイントをアカウントから削除する必要があります。テナントから削除されたアカウントにエンドポイントが存在する場合、コールは失敗します。
- ファイアウォールリソースのアカウントをまたいでエンドポイントを作成する場合は、ファイアウォール構成で定義されたゾーンにマップされているゾーンIDのいずれかにエンドポイントを作成する必要があります。
- 0AWSではゾーンID名の扱いが異なります。個別のアカウントの場合は、同じゾーンIDを使用して、エンドポイントが正しいゾーンに表示されるようにします。
- アカウントIDは単一アカウントの場合は任意ですが、複数のアカウントではアカウントIDを使用する必要があります。

ゾーン名（例：*us-east-la*）は、アカウントごとに異なるゾーン*ID*（例：*use1-az4*）へのマッピングを持ちます。

AWS Marketplaceの拡張サブスクリプションエクスペリエンスを使用して、AWSアカウントからCloud NGFWテナントにクロスアカウントロールを追加できます。このプロセスでは、追加のIAM権限とリソース デプロイメントを追加する必要があります。Cloud NGFWコンソールを使用して、ロールARNを手動で追加することもできます。ロールの差分追加には、クロス アカウント ロール管理がサポートされています。

*Cloudformation*テンプレートの更新がサポートされています。

たとえば、account1の証明書とaccount2の証明書をaccount3のルールスタックにマップし、account4のファイアウォールリソースに関連付けることができます。このシナリオでは、すべてのアカウント（1-4）が正常にオンボーディングされている必要があります。

すでにオンボーディング済みのAWSアカウントの場合は、マルチアカウント テナントを使用してアカウントを追加できます。まず、Palo Alto NetworksのNGFWサブスクリプションのAWS Marketplaceサブスクリプションページにアクセスします。

STEP 1 | AWS Marketplaceでサブスクリプションにアクセスします。

STEP 2 | ステップ1で、サブスクリプションに必要なAWS管理者の権限があることを確認します。

STEP 3 | ステップ2で、新規または既存のベンダーアカウントをリンクします。**[Login or create vendor account(**ログインまたはベンダー アカウントを作成する**)**］をクリックして、既存のCloud NGFWアカウントにアクセスし、テナントをリンクしてAWSサービスとの通信を有効にします。**Palo Alto Networks Cloud NGFW**のログインページが表示されます。

STEP 4 | **[Welcome(**ようこそ**)]**画面で、**[Login with an Existing Account(**既存のアカウントでログイン**)]**をクリックします。

STEP 5 | Cloud NGFWテナントのログイン認証情報を入力します。ログインすると、AWS Marketplaceにベンダーアカウントが正常にリンクされたことが示されます。

アカウントにCloudFormationテンプレート（CFT）が存在しない場合、既存のCFTを構成する必要がある場合は、CloudFormationテンプレートを手動で追加するためのこの記事の最後にある情報を参照してください。

STEP 6 | CFTが存在する場合は、手順4に移動し、Cloud NGFWコンソールを起動して設定を続行します。**[Launch product(**製品の起動**)]**をクリックします。

STEP 7 | Cloud NGFWコンソールにログインします。

STEP 8 | **AWS** アカウントを選択します。

STEP 9 | マルチアカウント テナントとして追加する**AWS**アカウント**ID**を選択します。

STEP 10 | **[Add AWS Account(AWS**アカウントの追加**)]**をクリックします。

STEP 11 | 既存のアカウントに追加するアカウントの**AWS Accout ID**の名前を入力します。

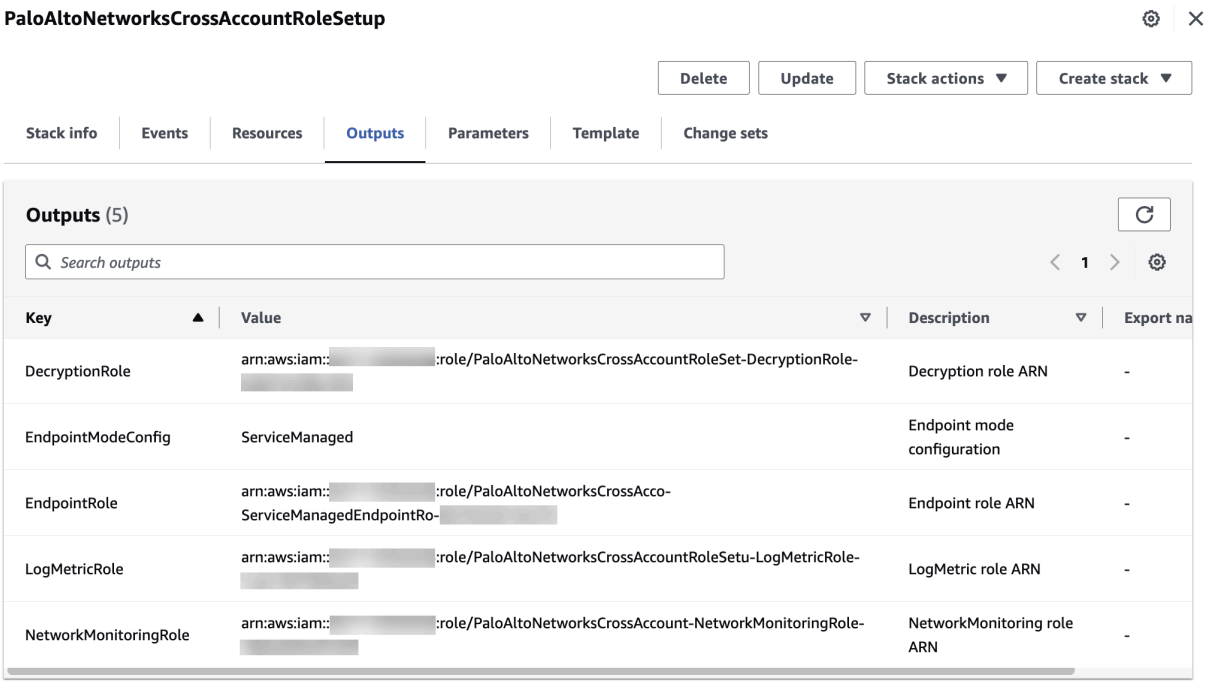
STEP 12 | AWSアカウントにログインします。

STEP 13 | AWSコンソールを使用してスタックを作成します。**[Create Stack on AWS(AWS**でスタックを作成**])**をクリックするか、AWS CLIを交互に使用します。

STEP 14 | **[I acknowledge that AWS Cloud Formation might create IAM resources with custom names(AWS CloudFormation**によって**IAM**リソースがカスタム名で作成される場合があることを承認します。**)]**を選択します

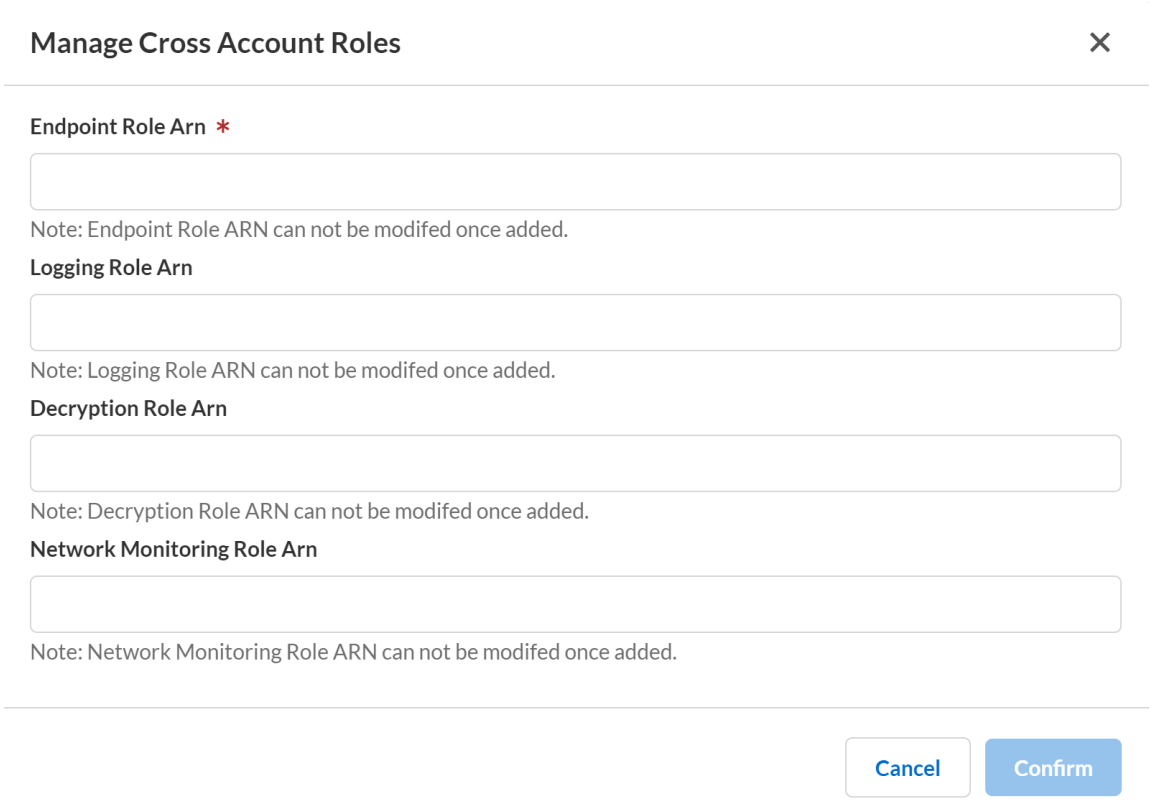
STEP 15 | ［スタックの作成］をクリックします。

STEP 16 | ステータスに**CREATE_COMPLETE**と表示されたら、AWSコンソールの**[Outputs(出力)]**タブからロールARNの値をコピーします。



STEP 17 | ロールARNの値をCloud NGFWテナントコンソールに追加します。

1. Cloud NGFWテナントコンソールを返します。
2. Cloud NGFWテナントコンソールで 、 **[[Settings(設定)]** > **[AWS Accounts(AWS**アカウント**)]**を選択します。
3. 追加するAWSアカウントのラジオボタンを選択し、**[Actions(**アクション**)]**ドロップダウンから**[Manage Cross Account Roles(**クロスアカウントロールの管理**)]**を選択します。
4. 前の手順で取得したRole ARNの値を対応するフィールドに貼り付けます。
5. **[Confirm(**確認**)]**をクリックします。



AWS Firewall Managerアカウントのスタート ガイド

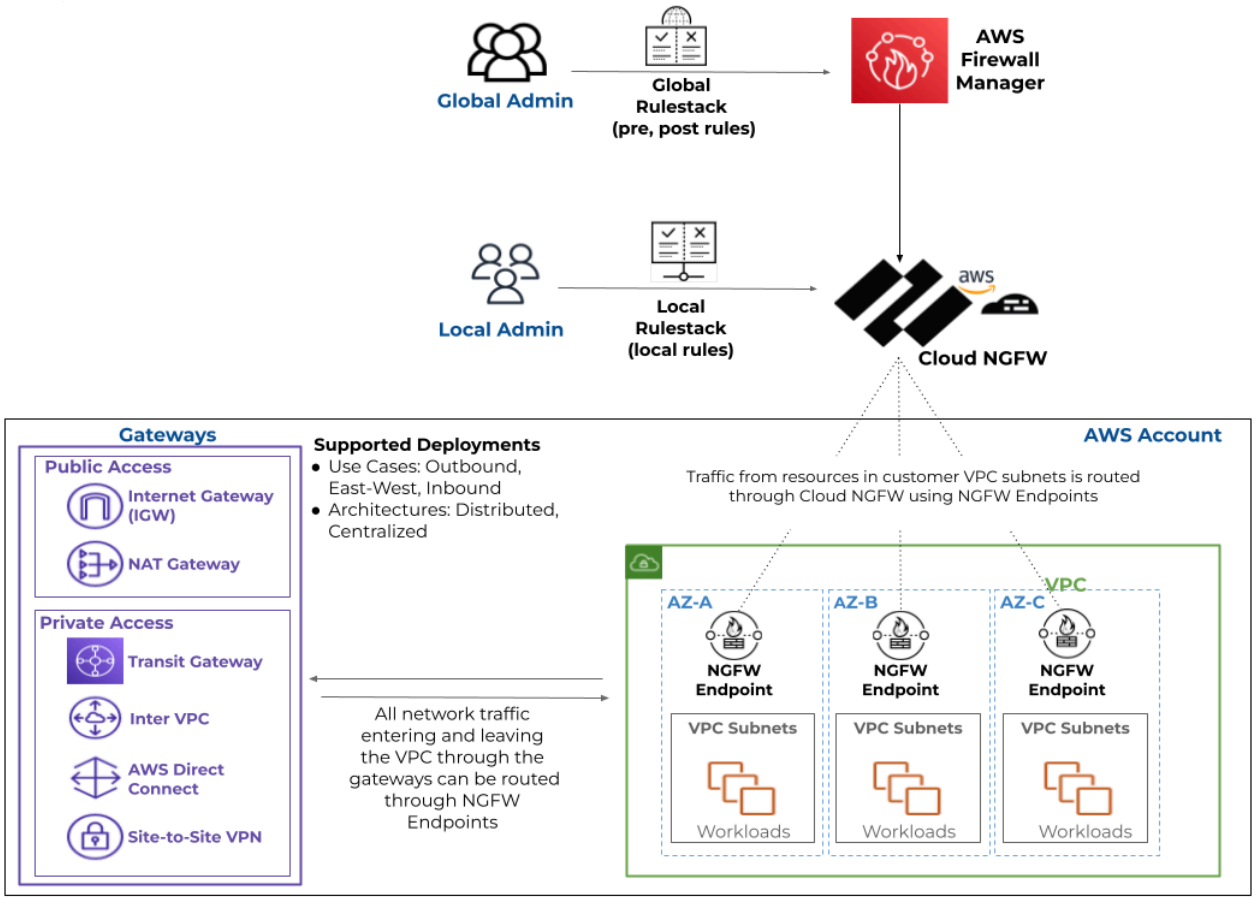
どこで使用できますか?	何が必要ですか?
• Cloud NGFW for AWS	❑ Cloud NGFWサブスクリプション ❑ Palo Alto Networksカスタマー サポート アカウント (CSP) ❑ AWS Marketplaceアカウント ❑ ユーザーのロール（テナントまたは管理者）

AWSファイアウォールマネージャ（FMS）は、AWS組織のすべてのメンバーアカウントにわたって、AWSウェブアプリケーションファイアウォール、セキュリティグループ、およびAWSネットワークファイアウォールのルールを一元管理できるサービスです。AWS ファイアウォールマネージャを使用して、Cloud NGFW リソースを一元的にデプロイし、AWS 組織のさまざまな AWS アカウントの VPC 間でルールを管理できるようになりました。AWS ファイアウォールマネージャダッシュボードでは、コンプライアンス通知を表示して応答することもできます。

AWS Firewall Manager には、

- FMS ポリシーとしての Cloud NGFW のデプロイ
- デプロイメントモードとリージョンの選択 、
- グローバルルールスタックの作成
- NGFW エンドポイントの設定
- 、および 組織全体での Cloud NGFW のスコープの定義を可能にするワークフローが用意されています。

詳細については、AWS ファイアウォールマネージャのドキュメントを参照してください。



Cloud NGFW は、*FMS* ポリシースコープ内でのみ *VPC* リソースをサポートします。

STEP 1 | Cloud NGFW for AWS サービスにサブスクライブします。Cloud NGFW サービスのサブスクライブに使用する AWS アカウントは、同じ AWS Firewall Manager 管理者アカウントである必要があります。

AWS ファイアウォールマネージャアカウントの IAM ユーザーとして、まず AWS マーケットプレイスを通じて Cloud NGFW サービスをサブスクライブします。初期設定が完了したら、AWS コンソールの FMS ダッシュボードに戻ります。この手順では、Cloud NGFW テナントを作成し、テナント管理者ロールとグローバルファイアウォール管理者ロールを（FMS 管理者）に自動的に割り当てます。

STEP 2 | Palo Alto Cloud NGFW サービスを Firewall Manager に関連付けます。

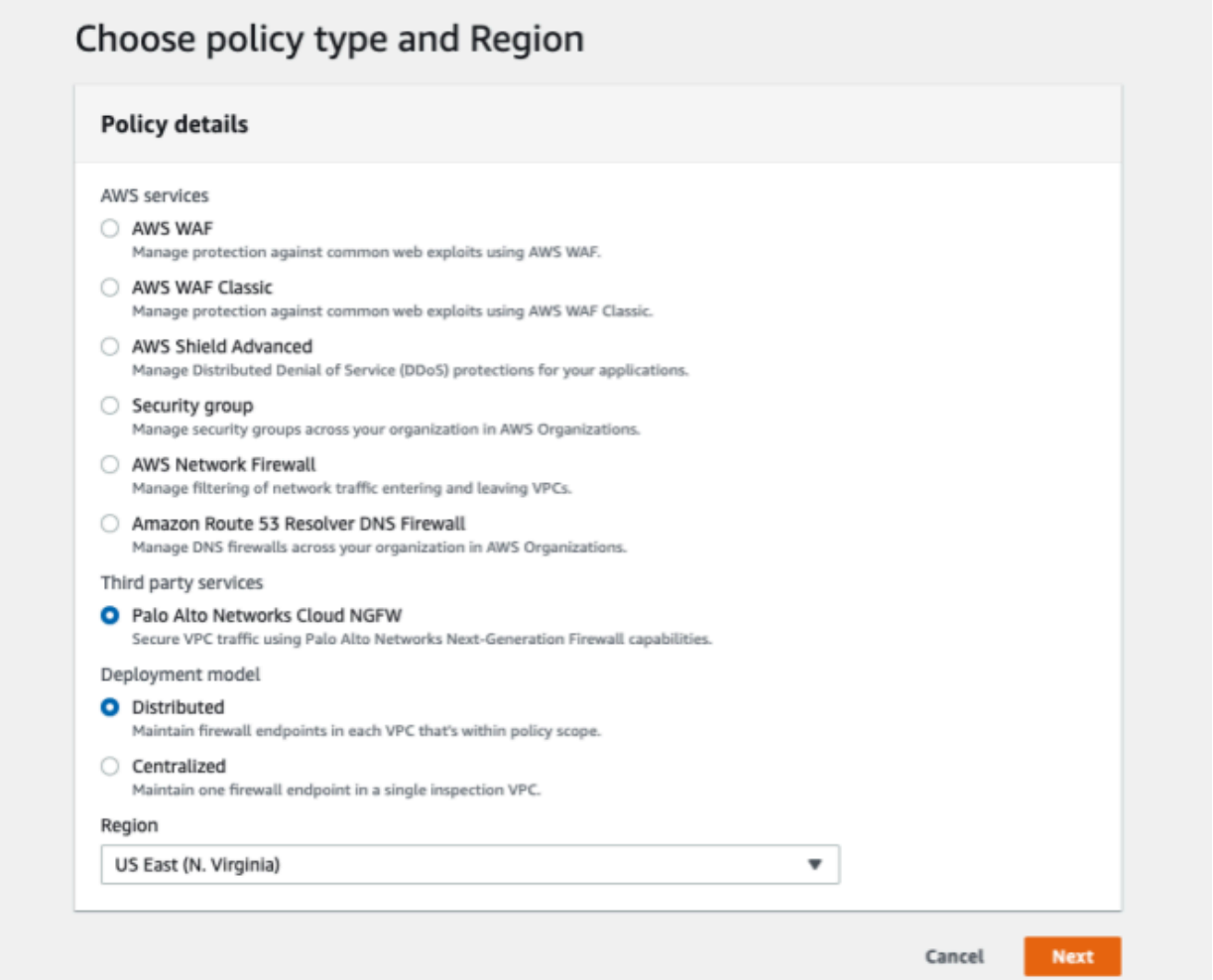
1. AWS コンソールにログインし、［サービス］ > ［**AWS Firewall Manager**］ > ［設定］を選択します。
2. [サードパーティファイアウォールの関連付けの状態] で、[Palo Alto Networks Cloud NGFW]を選択します。
3. **Associate**（関連付け）をクリックします。

STEP 3 | ［セキュリティポリシー > ［ポリシーの作成]を選択します。

STEP 4 | ポリシーの種類と地域を選択します。

1. [サードパーティサービス] で、［**Palo Alto Networks Cloud NGFW]**を選択します。
2. ［デプロイメントモード］（分散型または集中型）を選択します
3. 地域を選択します。

STEP 5 | **Next**（次へ）をクリックします。



STEP 6 | Cloud NGFW on AWS の FMS ポリシーについて説明します。

FMS ポリシーのわかりやすい名前を指定し、グローバルルールスタックを設定または FMS ポリシーに関連付け、ログ設定を行います。FMS は、既存のグローバルルールスタック（使用可能な場合）と、グローバルルールスタックを作成するために Cloud NGFW コンソー

ルに移動するリンクを表示します。サブスクライブしているユーザー（FMS 管理者）は GlobalRulestackAdmin であるため、ユーザーロールを変更する必要はありません。

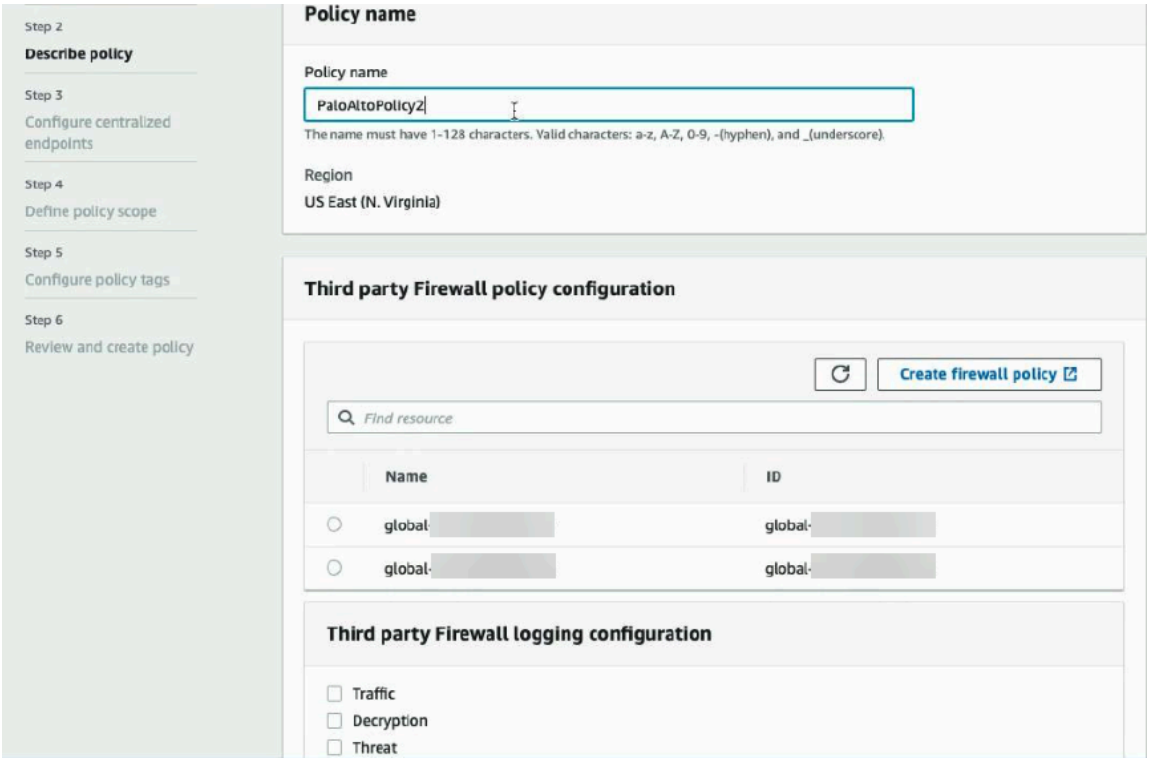
1. わかりやすいポリシー名を入力します。
2. サードパーティファイアウォールポリシー設定を選択または作成します。

   FMS コンソールでは、サードパーティファイアウォールポリシー設定は、Cloud NGFWのコンテキストにおけるグローバルルールスタックを参照します。すでに 1 つ以上のグローバルルールスタックを作成している場合は、ここにリストされます。グローバルルールスタックを作成していない場合は、［ファイアウォールポリシーの作成］をクリックして作成できます。これにより、Cloud NGFW コンソールにリダイレクトされます。ルールスタックとルールスタックの構成の詳細については、「rules」 および「rulestacks」を参照してください。
3. グローバルルールスタックを作成します。

   1. ルールスタックのわかりやすい名前を入力します。
   2. （任意）ルールスタックの説明を入力します。
   3. **[Save(保存)]**をクリックします。
   4. FMS コンソールに戻ります。
4. ログの設定。

   トラフィック、 復号化、または 脅威ログを選択できます。ログの種類ごとに、ドロップダウンから宛先（S3 バケット、CloudWatch ロググループ、または Kinesis Firehose 配信ストリーム）を指定する必要があります。ドロップダウンには、AWS 環境で以前に設定された宛先が表示されます。

5. **Next**（次へ）をクリックします。



STEP 7 | NGFWエンドポイントを設定します。

Cloud NGFWは、セキュリティで保護する必要があるアベイラビリティゾーンにエンドポイントを作成します。これらの NGFW エンドポイントは、検査と適用のためにトラフィックをインターセプトして Cloud NGFW にリダイレクトします。NGFW エンドポイントの数と場所は、デプロイメントモード（分散型または集中型）によって異なります。

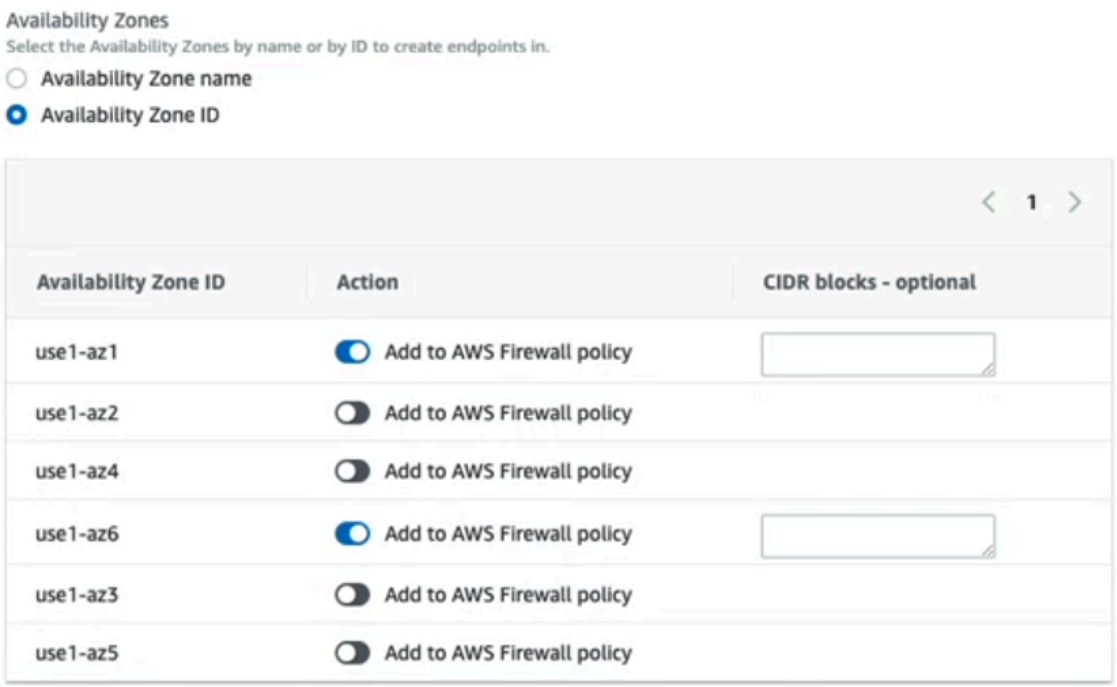
アベイラビリティゾーン名またはアベイラビリティゾーン ID を選択して、NGFW エンドポイントの場所を選択します。アベイラビリティゾーン名は AWS アカウント間で異なる場合が

ありますが、アベイラビリティゾーン ID はすべての AWS アカウントで一貫していることに注意してください。

1. **[**アベイラビリティゾーン名**]** または**[**アベイラビリティゾーン **ID]**を選択します。この選択によって、FMS コンソールがリストするオプション（名前または ID）が決まります。
2. 「アクション」列で、スライダーをクリックして、Cloud NFGW FMS ポリシーにアベイラビリティゾーンを追加します。
3. （任意）クラスレスドメイン間ルーティング（CIDR）ブロックを追加して、NGFW エンドポイントが使用するサブネットを指定します。

   選択したアベイラビリティゾーンごとに CIDR ブロックを指定するか、FMS の CIDR ブロックのリストを作成して、選択したアベイラビリティゾーンに割り当てることができます。各 CIDR ブロックは /28 CIDR ブロックでなければなりません。

   CIDRブロックを指定しない場合、FMSはベストエフォートアプローチを採用して、VPC内の割り当てられていないCIDRブロックを見つけて、NGFWエンドポイントのサブネットを作成します。VPCで使用可能な CIDR ブロックがない場合、FMSは非準拠エラーを表示します。
4. **Next**（次へ）をクリックします。



STEP 8 | Cloud NGFW FMS ポリシースコープを定義します。

ポリシースコープは、Cloud NGFW FMSポリシーの対象となるAWSアカウントまたは組織単位（OU）とリソースを定義します。組織内のすべてのAWSアカウントとVPCにCloud NGFW FMSポリシーを適用するか、アカウントやVPCのサブセットを指定できます。

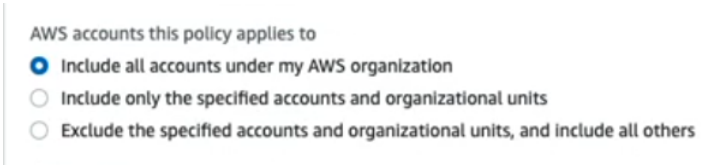
新しい AWS アカウントまたは VPC を組織に追加すると、FMS は Cloud NGFW ポリシーをそのアカウントまたは VPC に適用する必要があるかどうかを判断します。たとえば、除外された小さなサブセットを除くすべてのアカウントに Cloud NGFW ポリシーを適用できます。新

しいアカウントが組織に参加すると、除外リストにないため、Cloud NGFWポリシーが適用されます。

1. Cloud NGFW FMSポリシーに含めるまたは除外するアカウントを指定します。

   自分の **AWS** 組織の下にあるすべてのアカウントを含める、指定したアカウントと組織単位を含める、または特定のアカウントと組織単位を除外してその他すべてを含めるを選択できます。

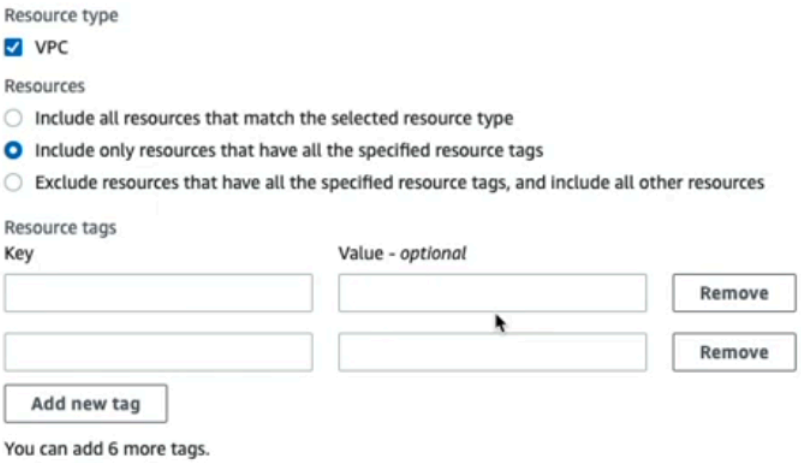
   アカウントとOUのサブセットを含めるか除外するかを選択すると、FMSコンソールには、それらのアカウントとOUを指定できるフィールドが表示されます。**[**リストの編集**]**をクリックして、包含リストまたは除外リストを作成します。

2. Cloud NGFW FMSポリシーに含めるか除外するVPCを指定します。

   アカウントと OU と同様に、選択したタイプに一致するすべてのリソースを含める、指定したすべてのリソースタグを持つリソースのみを含める、または指定したすべてのリソースタグを持つリソースを除外し、その他すべてを含めることができます。

   VPC のサブセットを含めるか除外するかを選択すると、FMS コンソールにオプションが表示され、最大 8 つのリソースタグと値のリストが表示されます。

3. サードパーティファイアウォール カスタマー **IAM** ロールで、Cloud NGFW IAM ロール CloudFormation テンプレート（CFT）のコピーをダウンロードできます。
4. **Next**（次へ）をクリックします。
5. （任意）ポリシータグを設定します。

   タグ（キーとオプションの値で構成される）を適用して、FMSを介して作成されたCloud NGFWリソースの検索とフィルタリングに役立てることができます。
6. **Next**（次へ）をクリックします。

7. Cloud NGFW ポリシーの設定を確認します。
8. **[**ポリシーの作成］をクリックして、Cloud NGFW をデプロイします。

Cloud NGFW for AWS 無料トライアル

どこで使用できますか?	何が必要ですか?
• Cloud NGFW for AWS	❑ Cloud NGFWサブスクリプション ❑ Palo Alto Networksカスタマー サポート アカウント (CSP) ❑ AWS Marketplaceアカウント ❑ ユーザーのロール（テナントまたは管理者）

AWS Marketplace を通じて Cloud NGFW を購読すると、自動的に無料トライアルに登録されます。サブスクリプション管理ページに移動して、Cloud NGFW テナントがAWS Marketplace **Palo Alto Networks**の**Cloud NGFW**従量課金制サブスクリプションリストにリンクされていること、および無料試用期間がクレジットで有効になっているなっていることを確認します。

この無料トライアルを有効にするには、Cloud NGFWは無料トライアル クレジットを新しく作成したテナントに関連付けます。これらのクレジットにより、最大100 GBのトラフィックを保護するファイアウォールを最大2つ作成できます。次の作業を行えます。

- AWSアカウントをテナントにオンボードします。
- AWS VPCに最大2つのNGFWリソースを作成します。
- ルールスタックを作成します。

無料体験期間が終了すると、使用量に対する支払いが始まります。サブスクリプション管理ページに移動して、Cloud NGFW テナントがまだ AWS Marketplace **Palo Alto Networks** の **Cloud NGFW** 従量課金制サブスクリプションリストにリンクされていること、および無料試用期間が無効になっていることを確認できます。以下を検討してください。

- 無料試用期間を一時停止することはできません。
- 無料トライアル期間が終了すると、Cloud NGFWの使用時に料金が発生し始めます。