paloalto TECHDOCS

AWS管理のためのCloud NGFW

docs.paloaltonetworks.com

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

管理 7

Cloud NGFW for AWS にユーザーを招待する 8

複数アカウントのユースケースに関する考慮事項 10

Cloud NGFW for AWS ユーザーを管理する 13

ユーザーロールの管理 13

ユーザーの削除 13

ユーザー情報の編集 14

ヘルプを受ける 15

初回ログイン時にCloud NGFWテナントを登録する 15

カスタマー サポート ポータルを使用したクラウドNGFWテナントの登録 16

Cloud NGFWコンソールを使用したカスタマー サポート ポータルへのCloud NGFWテナントの登録 19

Cloud NGFW for AWSのシリアルナンバーを見つける 27

使用量エクスプローラー 34

デプロイ 37

AWS で NGFW リソースを作成する 41

AWS エンドポイント用のクラウド NGFW を作成する 44

Cloud NGFWリソースの削除 45

Cloud NGFW for AWS にトラフィックを転送する 47

プライベートトラフィック範囲の設定 49

出口NATの設定 52

AWS NAT ゲートウェイ 52

Cloud NGFW Egress NAT 53

ハイブリッドNAT設定 54

Palo Alto Networks マネージド AWS EIP を使用して出口NAT を構成する 55

独自の IP の持ち込み (BYOIP) を使用して出口 NAT を構成する 56

クラウド NGFW リソースを作成し、出口 NAT を有効にして BYOIP を指定します 65

保護 69

CDSS（クラウド提供型セキュリティサービス）： 71

AWS 高度な脅威保護のためのクラウド NGFW 72

AWSのクラウドNGFW高度なURLフィルタリング 75
AWS WildFire Protection 上のCloud NGFW 78
AWS DNS セキュリティのためのクラウド NGFW 91
Cloud NGFW for AWSエンタープライズデータ損失防止（E-DLP）統合 103
クラウド NGFW ネイティブ ポリシー管理 123
Rulestacks and Rules on Cloud NGFW for AWS 124
Cloud NGFW for AWS での X-Forwarded-For 129
Cloud NGFW for AWS でプレフィックスリストを作成する 131
Cloud NGFW for AWS に証明書を追加する 132
Cloud NGFW on AWS の FQDN リストを作成する 139
Cloud NGFW for AWS のインテリジェントフィードを設定する 140
Cloud NGFW for AWS でセキュリティルールを作成する 142
Cloud NGFW for AWS セキュリティプロファイル 145
Cloud NGFW for AWSのルールの使用 175
Panoramaポリシー管理 183
Panama統合の準備 186
Cloud NGFWをPalo Alto Networks管理にリンク 188
リンクされたPanoramaをCloud NGFWリソースに関連付ける 199
Cloud NGFW を Panorama からリンク解除する 203
Cloud NGFW ポリシー管理に Panorama を使用する 206
タグベースのポリシーを構成する 245
ゾーンベースのポリシールールを構成する 278
Strata Cloud Managerポリシー管理 289
Cloud NGFWリソースをStrata Cloud Managerポリシー管理にリンクする 289
ファイアウォールをStrata Cloud Managerポリシー管理に関連付ける 297
Strata Cloud Managerでのファイアウォールの表示 305
Strata Cloud Managerを使用したCloud NGFWポリシー管理 311
Strata Cloud Managerを使用してCloud NGFWリソース用のフォルダを作成します 315
Strata Cloud Managerを使用した監視とトラブルシューティング 317
監視 319
AWS でネイティブにログを表示する 320
ログ タイプ 320
ログ宛先 322
Cloud NGFW for AWS トラフィックログフィールド 325

Cloud NGFW for AWS 脅威ログフィールド 328
Cloud NGFW for AWS 復号化ログフィールド 332
Panorama でトラフィックと脅威のログとアクティビティを表示する 335
Cloud NGFW ログをパノラマで表示する 335
ACCでCloud NGFWアクティビティを表示する 336
Strata Logging Service でトラフィックと脅威のログを表示する 338
Strata Logging Serviceへのログの転送 340
Strata Logging Serviceを使用せずにログを転送する 343
AWS のクラウド NGFW で監査ログを表示する 346
AWS CloudWatch でのカスタムメトリクスのパブリッシュと表示 349
Firewall-as-Code (ファイアウォール・アズ・コード) 353
プログラムによるアクセスを有効にする 355
Cloud NGFW AWS の Terraform サポート 363
アカウントの自動オンボーディングを設定する 365
Terraform ファイルの例 368
オンボード済みアカウントを削除する 368
オンボーディング済みアカウントを一覧表示する 368
Cloud NGFW リソースを AWS CFT にプロビジョニングする 369
Cloud NGFW のクロスアカウントロール CFT 権限 386

管理

どこで使用できますか?	何が必要ですか?
•	❑

AWS 向け Cloud NGFW は、セットアップとオンボードをシンプルかつ簡単にするサービスをサポートしています。包括的なデジタル サービス、テクニカル サポート、教育サービスは、Palo Alto Networks 導入の継続的な成功に向けた当社の取り組みを強調するものです。LIVE コミュニティとカスタマー サポート ポータルを通じてサポートを受けることができます。

AWS 向け Cloud NGFW は、すぐに稼働できるように設計されています。必須のルールスタックと自動化されたセキュリティ プロファイルを設定することで、時間のかかる導入プロセスを省略しながら、AWS のオンボーディング、監視、ログ記録などとの完全な統合など、AWS との連携方法を活用することができます。Cloud NGFW のデプロイメントの管理を支援する追加ユーザーを簡単に招待したり、既存のユーザーの役割を管理したりできます。

Cloud NGFW for AWS にユーザーを招待する

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）

テナント管理者は、追加のユーザーを招待して、Cloud NGFW デプロイメントの管理を支援することができます。次に、これらの新しいユーザーを、アクセスレベルに必要なロールに配置できます。ユーザーを Cloud NGFW テナントに招待するときは、ユーザーの電子メール アドレスを指定し、1 つ以上の Cloud NGFW ロールを割り当てます。Cloud NGFW テナントは、登録リンクと一時パスワードを含む電子メールをユーザーに送信します。初めてログインした後、新しいユーザーは新しいパスワードを作成します。招待されたユーザーが招待を受け入れてテナントにログインするまで、招待は保留中と見なされます。

Cloud NGFW のロール	許可
管理者	• AWS アカウントを追加します。 • ユーザーを招待し、ロールを割り当てます。 • NGFW を作成します。 • グローバルおよびローカルのルールスタックを作成および管理します。
テナント管理者	• AWS アカウントを追加します。 • ユーザーを招待し、ロールを割り当てます。
テナント リーダー	• すべてのファイアウォール リソースとその設定を読み取ります。 • すべてのグローバルおよびローカルのルールスタックを読み取ります。 • すべてのテナント ユーザーとテナント設定を読み取ります。

Cloud NGFW のロール	許可
グローバルルールスタック管理者	グローバルルールスタックを作成します。
ローカルファイアウォール管理者	• NGFW を作成します。 • ローカルルールスタックを NGFW に関連付ける ローカルファイアウォール管理者は、指定された *AWS* アカウント内でのみ *NGFW* を作成し、ルールスタックを関連付けることができます。
ローカルルールスタック管理者	• ローカルルールスタックを作成します。 • ローカルルールスタックを NGFW に関連付けます。 各ローカルルールスタック管理者には、関連付けられたアカウント ID があります。これにより、同じアカウント内の NGFW を使用してその管理者が作成したローカルルールスタックが許可されます。

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。

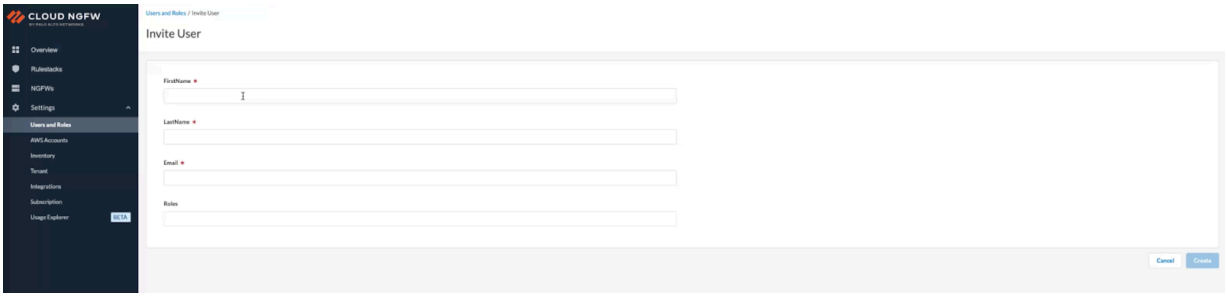
STEP 1 | Cloud NGFW テナントにログインします。

STEP 2 | ［設定］ > ［ユーザーとロール］ > ［ユーザーの招待］を選択します。

STEP 3 | 招待者の 名、姓、および電子メールアドレスを入力します。

STEP 4 | ［ロール] ドロップダウンから新しいユーザーのロールを選択します。既存のユーザーをCloud NGFWテナントに招待できるようになりました。

STEP 5 | 作成をクリックします。



ログイン後、テナントを選択して ***[Continue(***続行***)]***をクリックするように求められます。新規ユーザーの場合は、*SSO*に登録してテナントにログインできるアクティベーション メールが届きます。既存のユーザーは、*SSO*を使用してテナントに直接ログインできます。

複数アカウントのユースケースに関する考慮事項

AWSクライアント アカウントがCNGFWコンソールからテナントにすでに追加されている場合、サブスクリプション プロセス中に、ユーザーは既存のテナントでログインするか、新しいテナントを作成するかを選択できます。以下の表はこれらのユースケースを示しています。

ユースケース	手順
すでにSSOに登録されている場合。	アクティベーションメールは届きません

ユースケース	手順
SSO に登録されていない既存のユーザーの場合。	SSOへの登録を完了するためのアクティベーション メールが届きます。ただし、登録が完了するまでは、以前と同じようにサインインすることを選択できます。

[Login with an Existing Tenant(既存のテナントによるログイン**)]**オプションを使用して、単一の電子メールIDを使用してさまざまなテナントに登録します。

ログイン後、テナントを選択して **[Continue(**続行**)]**をクリックするように求められます。新規ユーザーの場合は、SSOに登録してテナントにログインできるアクティベーション メールが届きます。既存のユーザーは、SSOを使用してテナントに直接ログインできます。

Cloud NGFW for AWS ユーザーを管理する

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）

ユーザーのロールはいつでも変更して、アクセス権とアクセス許可を拡大または縮小できます。ユーザーを削除することもできます。また、個々のユーザーは、必要に応じて自分のロールを表示し、名前またはパスワードを変更できます。

ユーザーロールの管理

STEP 1 | **[**設定］ > ［ユーザーとロール**]**を選択します。

STEP 2 | ユーザーの名前をクリックします。

STEP 3 | 必要に応じて、名と姓を変更します。

STEP 4 | ユーザーのロールとスコープを変更します。

- ロールを追加するには:
  1. **[**ロールの追加**]**をクリックします。
  2. それぞれのドロップダウンからロールとスコープを選択します。
- ロールを削除するには:
  1. ルールの右側にある削除アイコン ( ) をクリックします。

STEP 5 | **[Save(**保存**)]**をクリックします。

ユーザーの削除

ユーザーのアクセス権とアクセス許可を完全に削除する必要がある場合は、そのユーザーを削除できます。

STEP 1 | **[**設定］ > ［ユーザーとロール**]**を選択します。

STEP 2 | ユーザー名の左側にあるチェックボックスをオンにします。

STEP 3 | ［アクション］ > ［削除］を選択します。

ユーザー情報の編集

テナント以外の管理者は、必要に応じて名前を変更したり、パスワードを変更したりできます。ただし、割り当てられたロールを変更することはできません。

STEP 1 | **[**設定］ > ［ユーザーとロール**]**を選択します。

STEP 2 | ユーザー名をクリックします。

STEP 3 | 必要に応じて、名と姓を変更します。

STEP 4 | パスワードを変更するには:

1. ［パスワードの変更］をクリックします。
2. ［現在のパスワード］を入力します。
3. 新しいパスワードを入力し、再入力します。
4. ［変更］をクリックします。

パスワードを変更すると、*Cloud NGFW* テナントからログアウトされます。新しいパスワードを使用してログインし直します。

STEP 5 | **[Save(**保存**)]**をクリックします。

ヘルプを受ける

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）

この情報を使用して、Cloud NGFW リソースをオンボードします。Cloud NGFW のシリアル番号を見つける方法とサポート ケースを作成する方法の情報も含まれています。

初回ログイン時にCloud NGFWテナントを登録する

Cloud NGFWは、パスワードを正常にリセットした後、Cloud NGFWテナントコンソールに初めてログインする前に、Cloud NGFWテナントのサポートアカウントを登録するように求めます。既存の 1 つ以上の Palo Alto Networks サポート アカウントの登録ユーザーの場合は、初回ログイン時に、そのうちの 1 つに Cloud NGFW テナントを登録することを選択できます。

Cloud NGFW へのサブスクライブに別のメール アドレスを使用し、Palo Alto Networks サポート アカウントにアクセスするために別のメール アドレスを使用している可能性があります。または、Cloud NGFW専用のPalo Alto Networksサポート アカウントを作成することもできます。どちらの場合も、初回ログイン時には登録オプションをスキップしますが、 **Cloud NGFW**テナントをカスタマー サポート ポータルに登録します.

次の手順を使用して、Cloud NGFW テナントを既存のサポート アカウントに登録します。

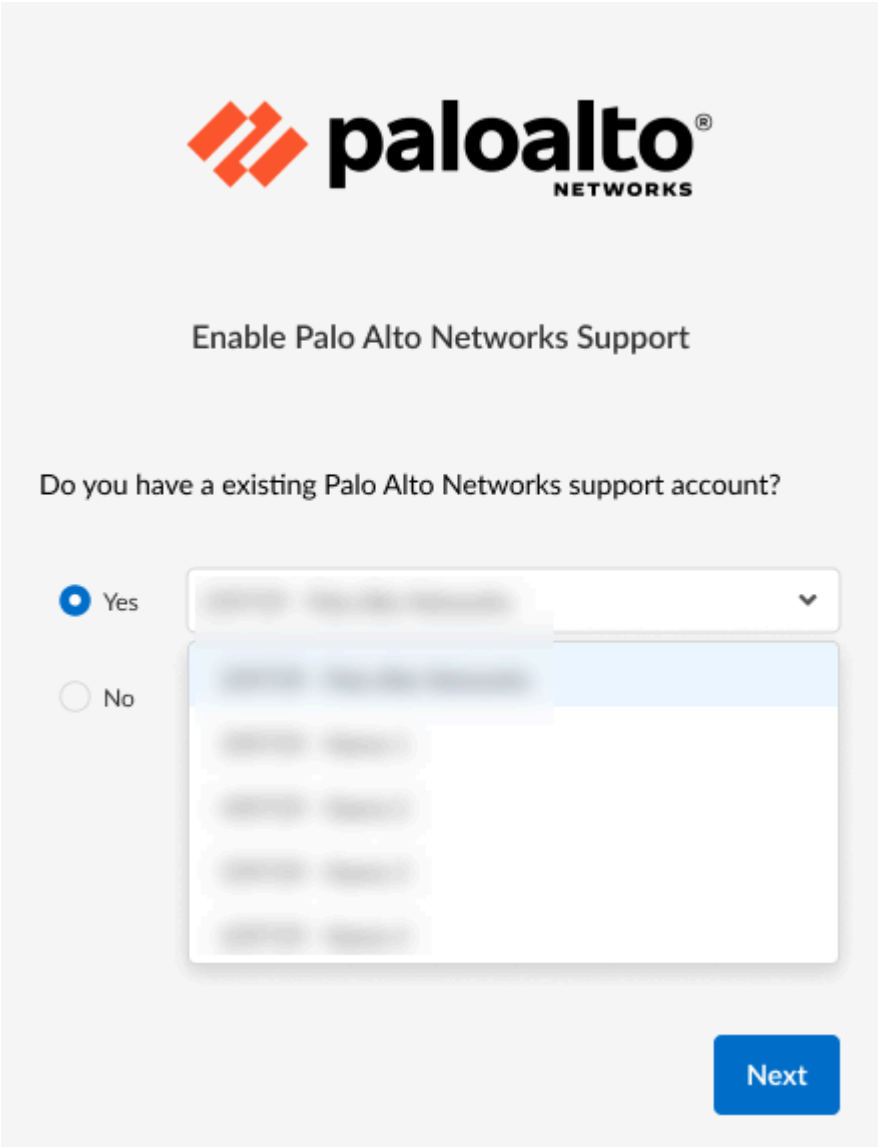
STEP 1 | Cloud NGFW コンソールにログインします。

STEP 2 | **[Enable Palo Alto Networks Support(Palo Alto Networks**のサポートを有効にする**)]**画面で、**[Yes(**はい**)]**を選択します。

> ***[Enable Palo Alto Networks(Palo Alto Networks**を有効にする**)]**画面で**[No(**いいえ**)]**を選択した場合、カスタマー サポート ポータル *(CSP)* を使用して *Cloud NGFW* テナントを登録するか、*Cloud NGFW* コンソールを使用して*CSP*に登録する必要があります。

STEP 3 | ドロップダウン メニューを使用して、サポート アカウントを選択します。

STEP 4 | **[Next（次へ）]**をクリックします。



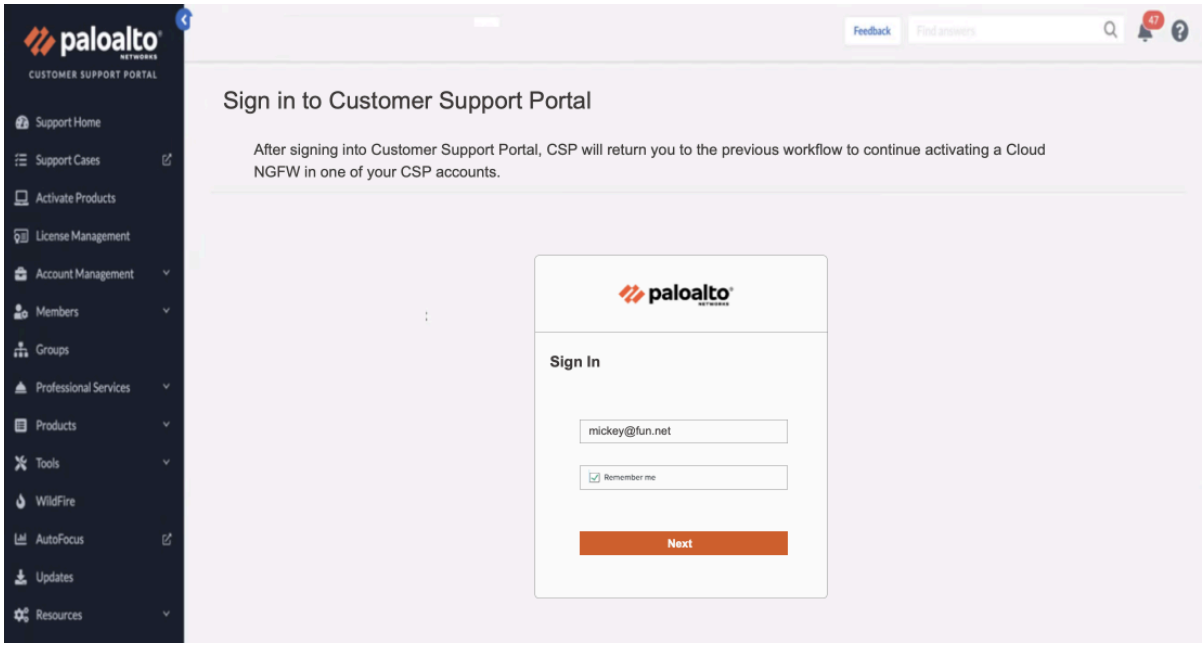
以前にカスタマーサポート*(CSP)*アカウントを登録したことがある場合、ドロップダウンには既存のアカウントが入力されます。ただし、新規ユーザーでまだアカウントをお持ちでない場合は、*CSP* ページを使用してアカウントを作成してください。「カスタマーサポートポータルを使用したCloud NGFWテナントの登録」と、「Cloud NGFWコンソールを使用したカスタマー サポート ポータルへのCloud NGFWテナントの登録」を参照します。

カスタマー サポート ポータルを使用したクラウドNGFWテナントの登録

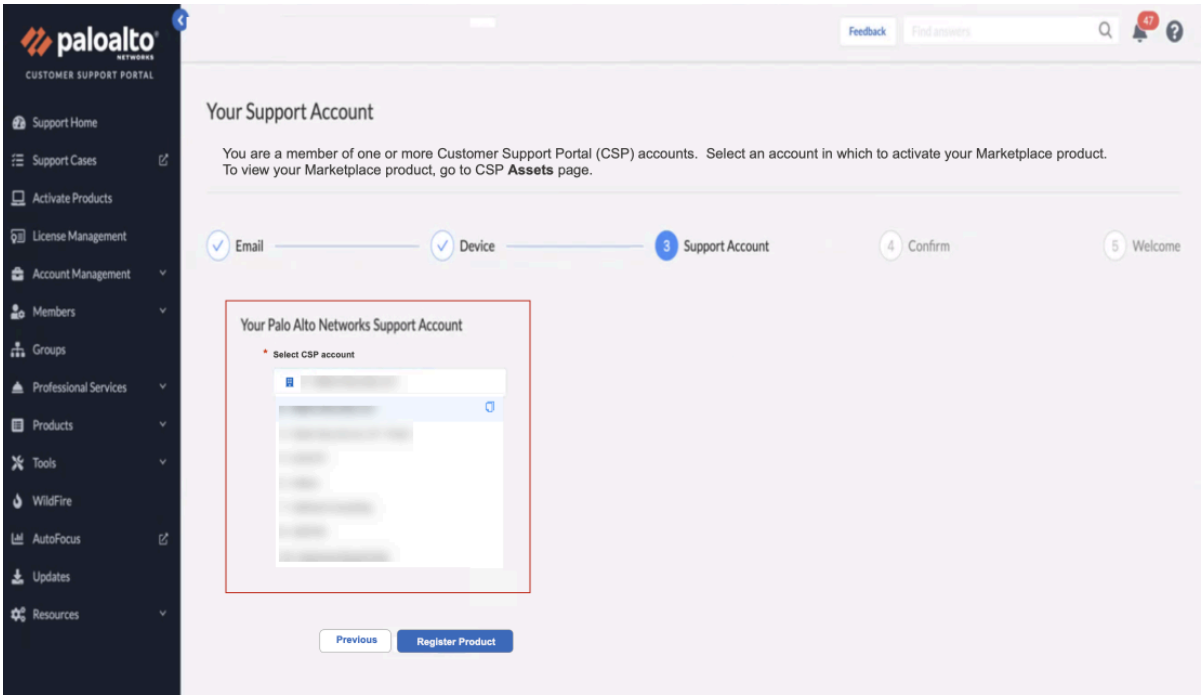
カスタマー サポート ポータルを使用して、Cloud NGFWテナントを登録できます。

*CSP*にログインするにはアカウントが必要です。詳細については、「カスタマー サポート アカウントの作成」をご覧ください。

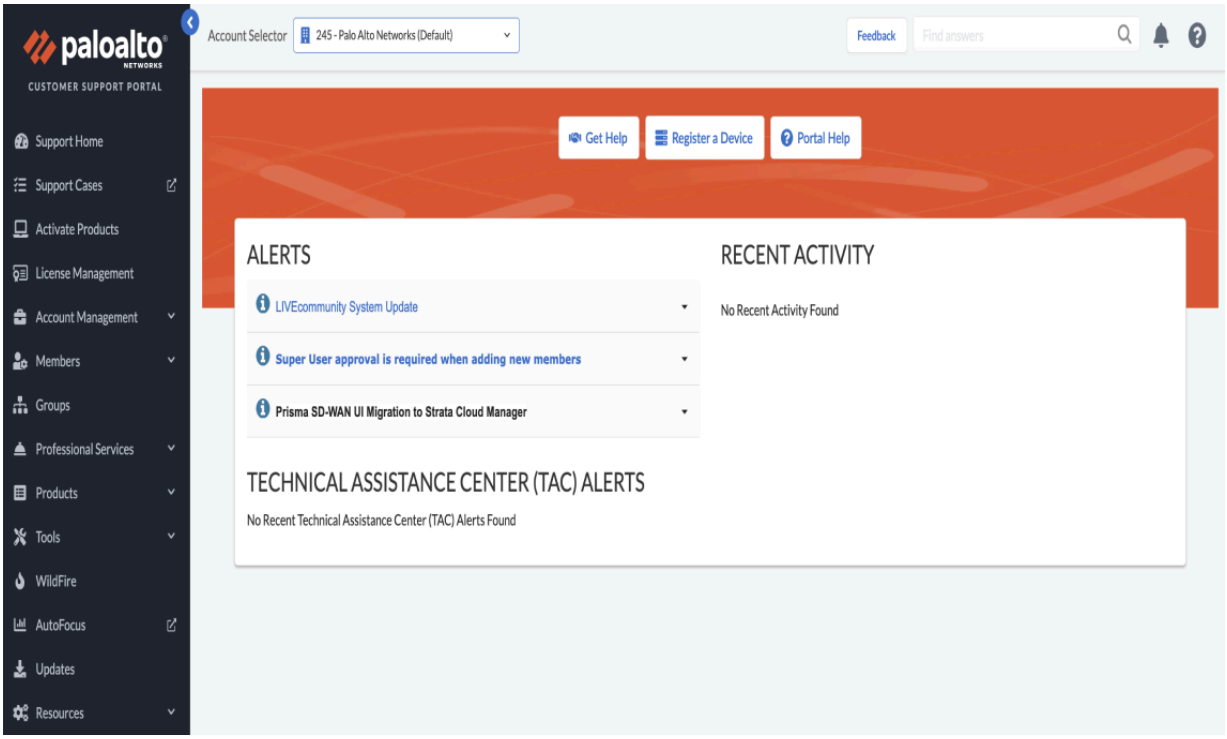
STEP 1 | [Customer Support Portal(カスタマーサポートポータル)]で、ログイン資格情報を入力してから、**[Next(次へ)]**をクリックします。



STEP 2 | お客様のサポートアカウントページには、ログイン資格情報に関連付けられた情報が表示されます。Palo Alto Networksのサポートアカウントを選択し、 **[Register Prpduct(製品の登録)]**をクリックします。



登録が完了すると、確認ウィンドウが表示され、続いてカスタマー サポート ポータル ページが表示されます。



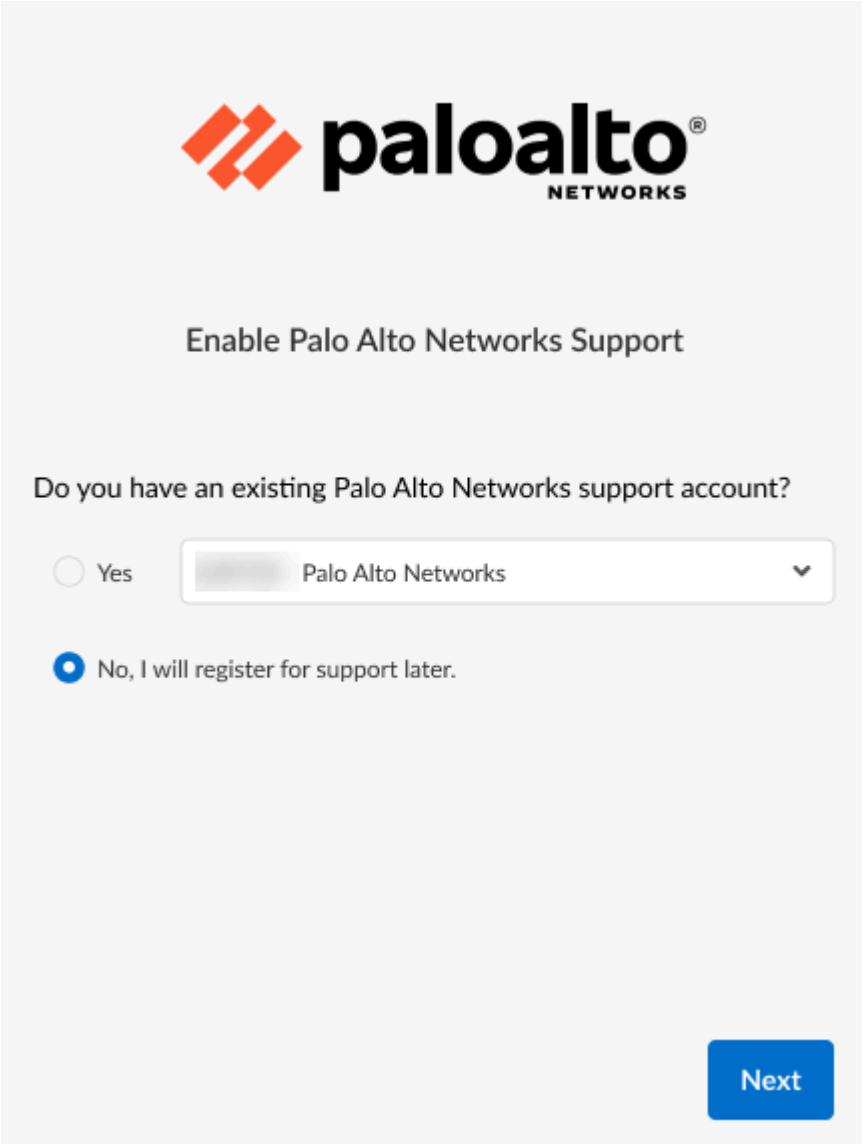
Cloud NGFWコンソールを使用したカスタマー サポート ポータルへのCloud NGFWテナントの登録

既存のPalo Alto Networksのサポート アカウントをお持ちでない場合は、Cloud NGFWテナントを使用する前にアカウントを保護するように求められます。

STEP 1 | Cloud NGFW リソースにログインします。

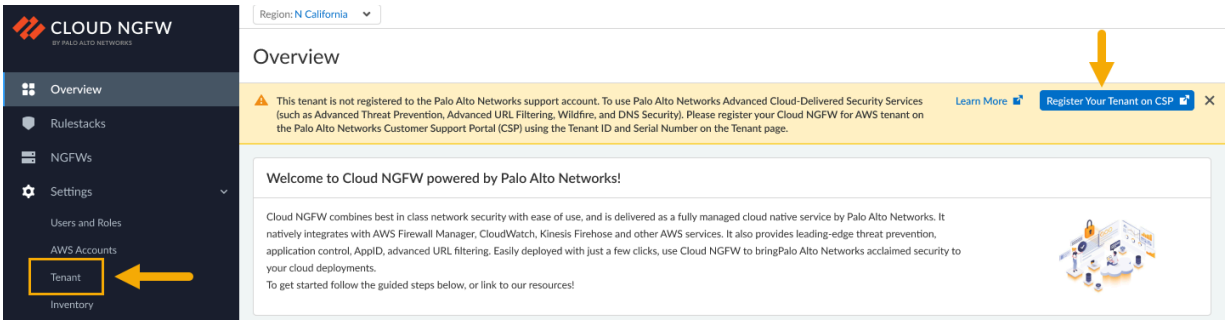
STEP 2 | **[Enable Palo Alto Networks Support(Palo Alto Networksのサポートの有効化)ページで、[No(いいえ)]を選択します。**

STEP 3 | **[Next（次へ）]をクリックします。**



STEP 4 | Cloud NGFW コンソールで、**[Register Your Tenant on CSP(CSP**にテナントを登録する**)]**をクリックします。

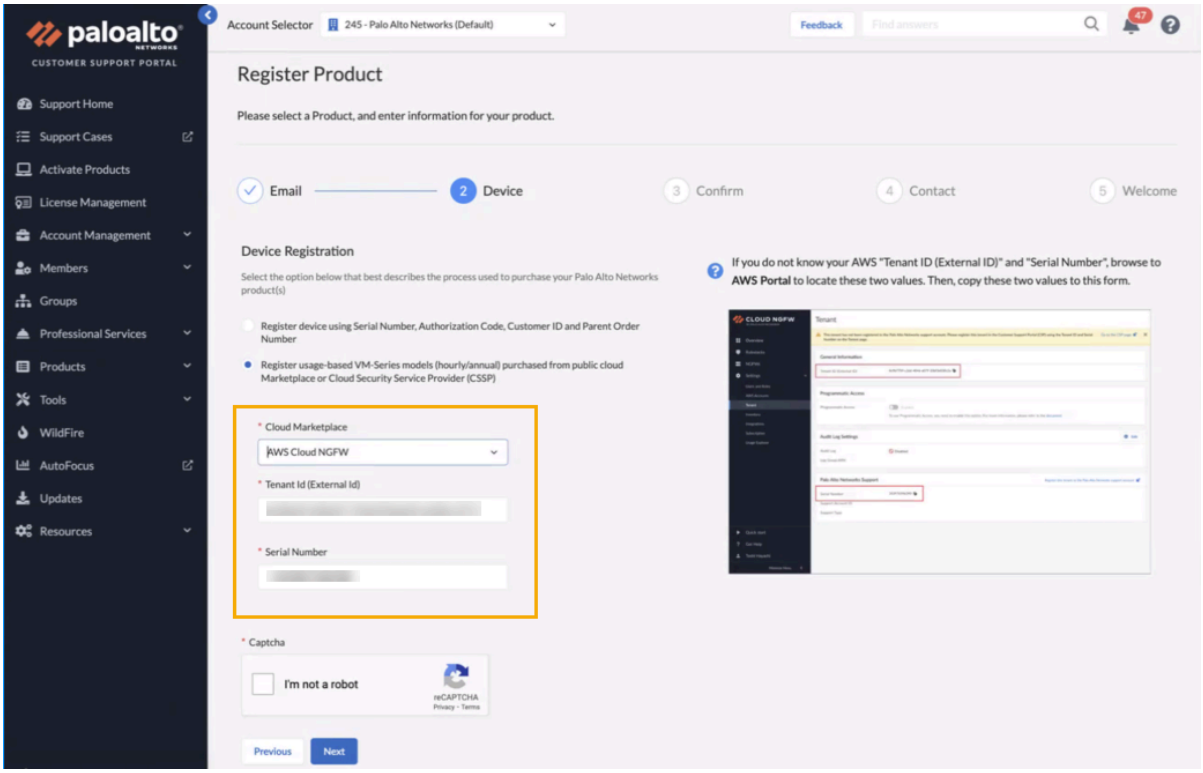
*Cloud NGFW*テナントをカスタマー サポート ポータル アカウントに関連付けるには、デバイス登録情報が必要です。テナント ***ID*** とシリアルナンバーを*Cloud NGFW* リソースに使用します。この情報は、*Cloud NGFW*コンソールの***[Tenant(***テナント***)]***ページにあります。[Create a Support Case(サポート ケースの作成)] ページに記載されている情報を参照してください。



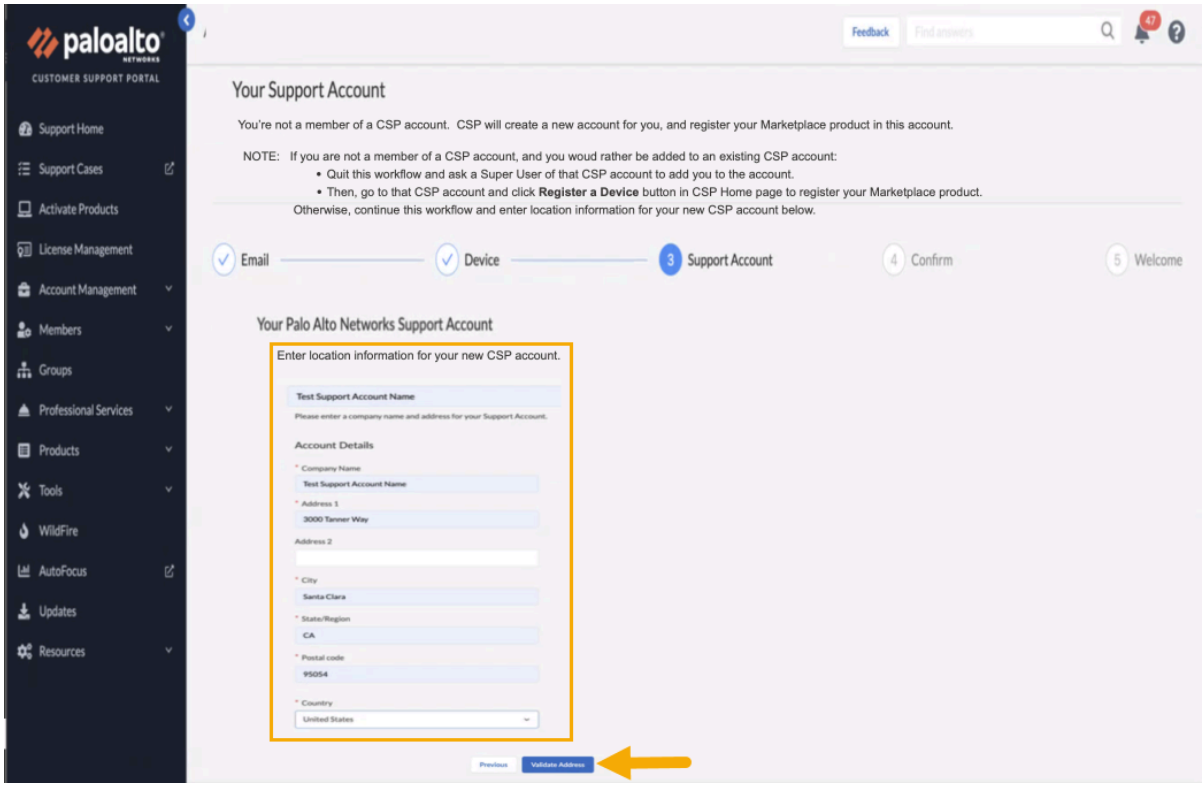
STEP 5 | カスタマー サポート ポータルの**[Register Product(**製品の登録**)]**ページで、ドロップダウン メニューを使用して**[Cloud Marketplace (**クラウド マーケットプレイス**)]**に**[AWS Cloud NGFW(AWS**クラウド**NGFW)]**を選択してください。テナント**ID**とシリアルナンバーを入力して、Captchaを解決します。

テナント*ID*とシリアルナンバーを見つけるには、[Create a Support Case(サポート ケースの作成)]ページをの情報を参照してください。

STEP 6 | **[Next（次へ）]をクリックします。**

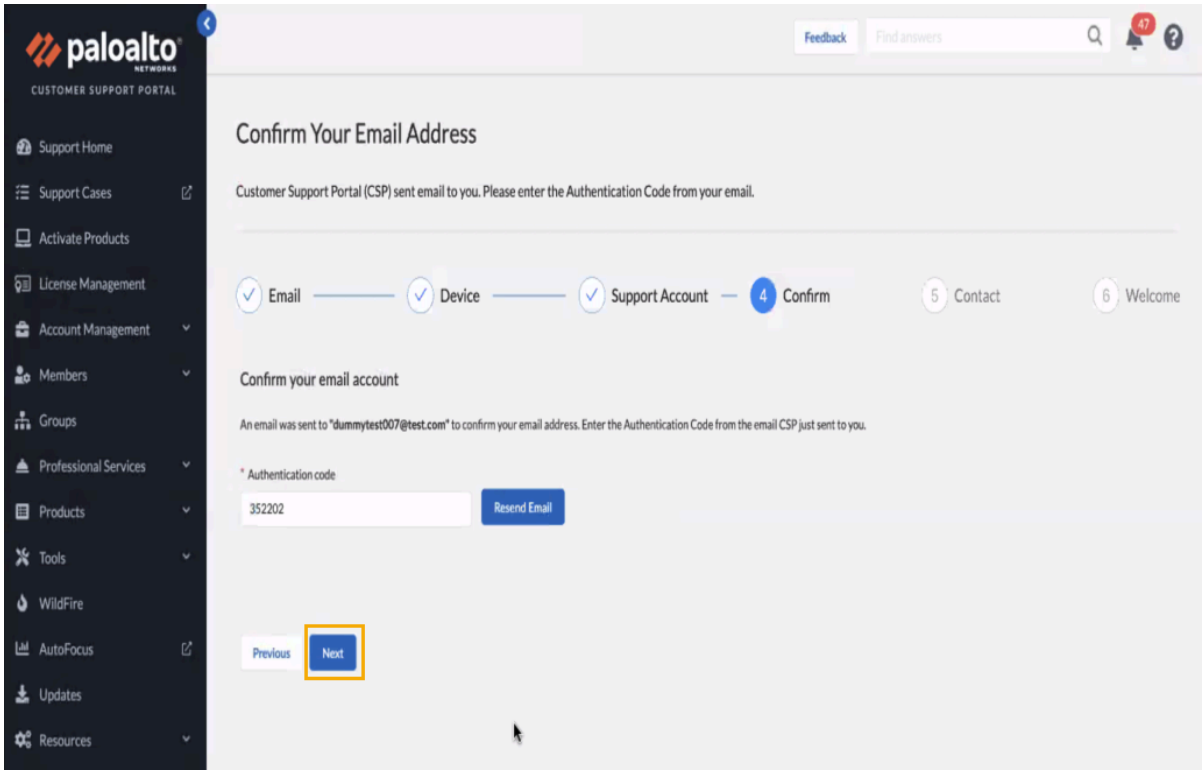


STEP 7 | サポート アカウントを作成します。**[Account Details(アカウントの詳細)]**に入り、 **[Validate Address(アドレスの検証)]**をクリックします。



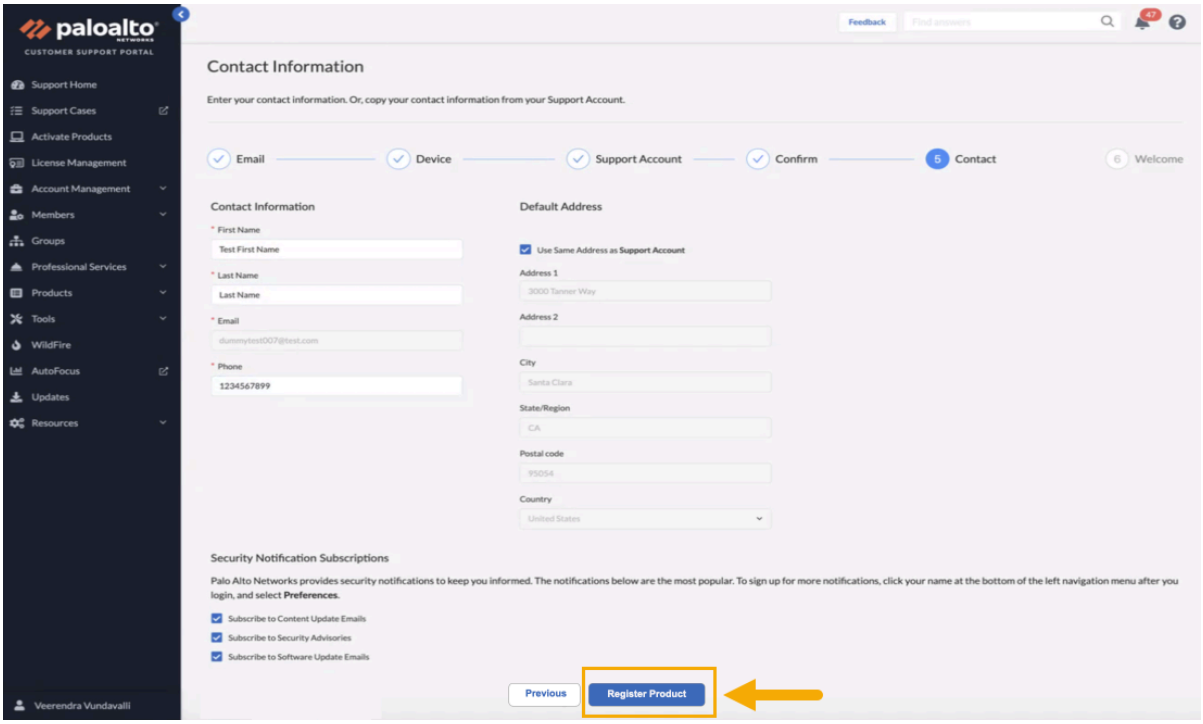
新しいサポート アカウントの住所を確認するように求められる場合があります。必要に応じて、住所を確認し、**[OK]**をクリックして、指定したメールアドレスに認証要求を送信します。

STEP 8 | 認証コードについてはメールを確認してください。**[Authentication code(認証コード)]**を入力し、**[Next(次へ)]**をクリックします。



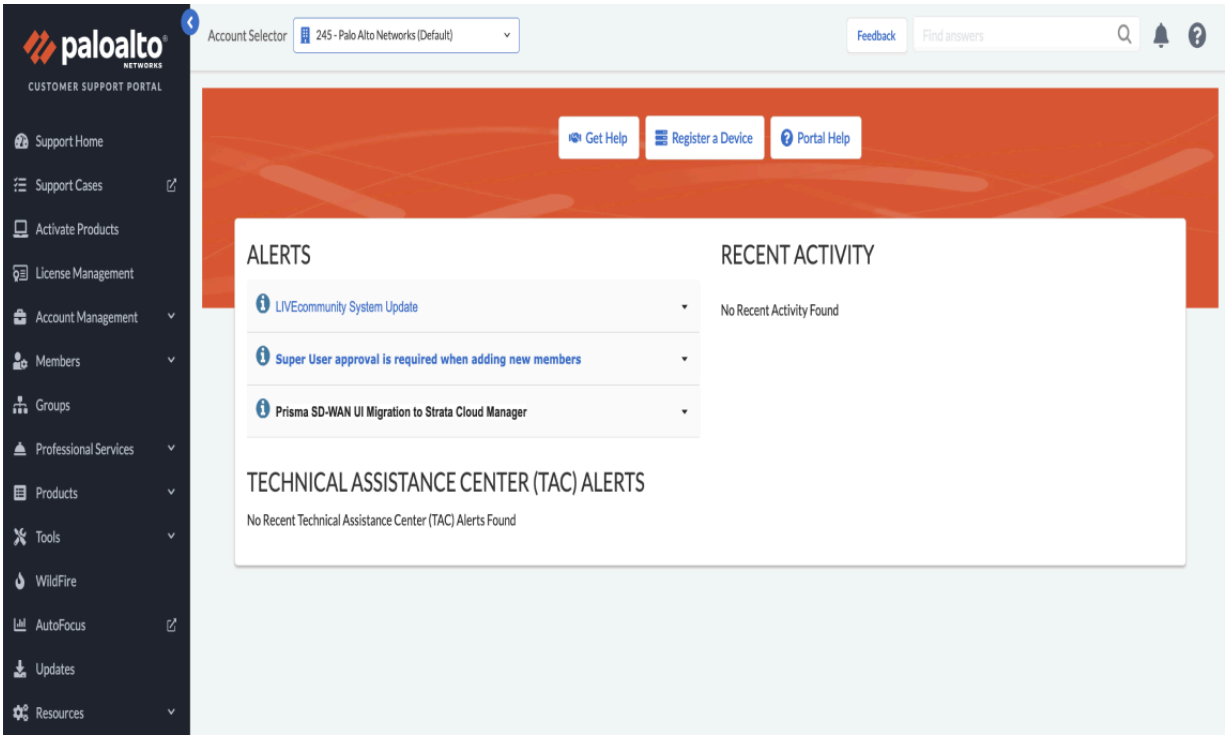
STEP 9 | カスタマー サポート ポータル アカウントのメール アドレスを確認し、**[Next(次へ)]**をクリックします。

STEP 10 | 連絡先情報を確認してください。**[Security Notification Subscriptions(**セキュリティ通知サブスクリプション**)]**を選択し、 **[Register Product(**製品の登録**)]**



をクリックします

登録が完了すると、確認ウィンドウが表示され、続いてカスタマー サポート ポータル ページが表示されます。

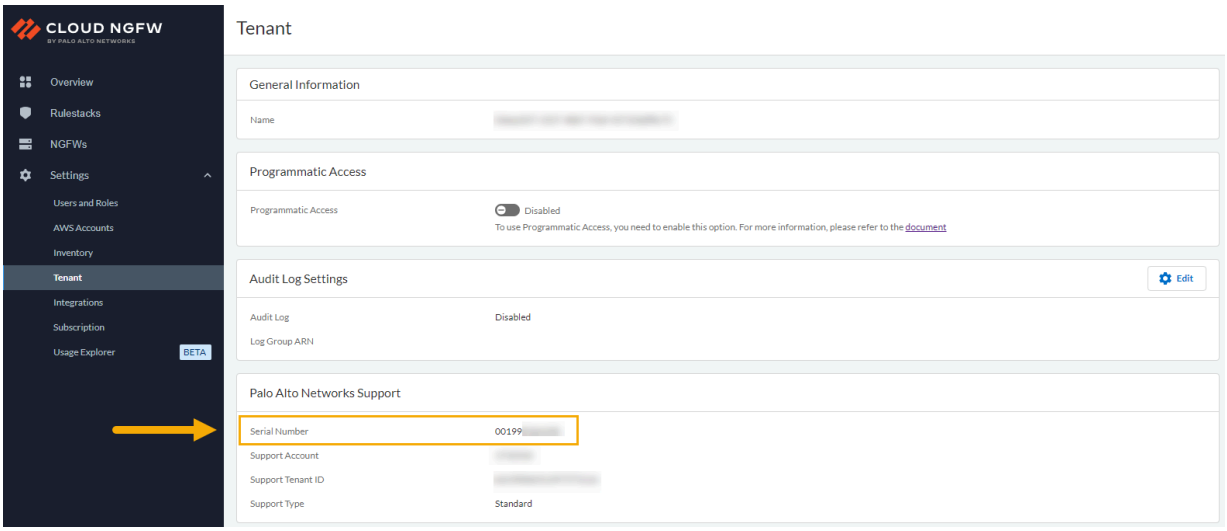


Cloud NGFW for AWSのシリアルナンバーを見つける

Cloud NGFWのシリアルナンバーを見つける方法:

STEP 1 | Cloud NGFW テナントにログインします。

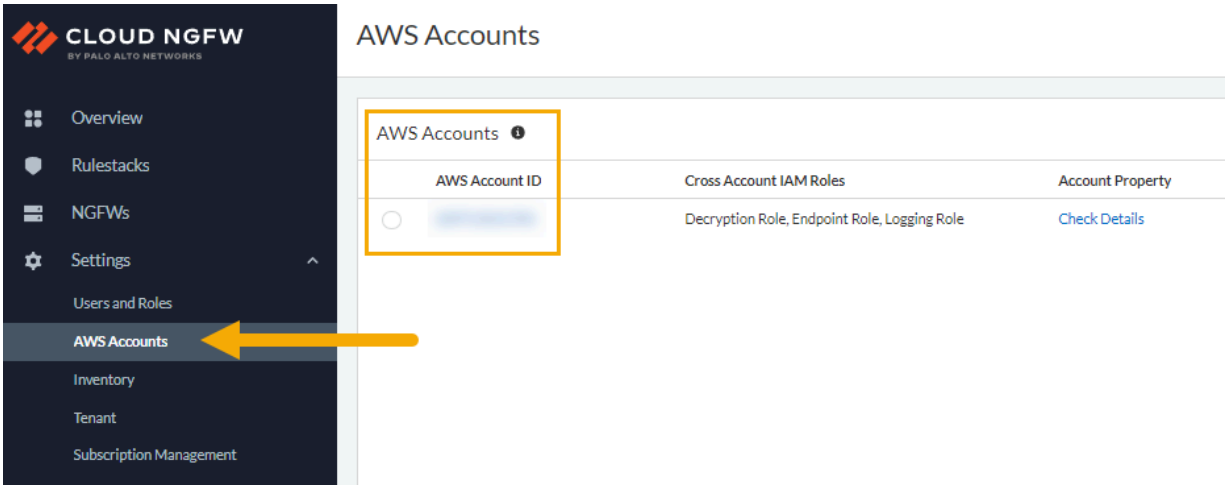
STEP 2 | **[Tenant(テナント)]**をクリックします。[Tenant(テナント)] ページには、シリアルナンバー、**Palo Alto Networks**のサポートセクションには追加情報が表示されます。



サポートケースの作成

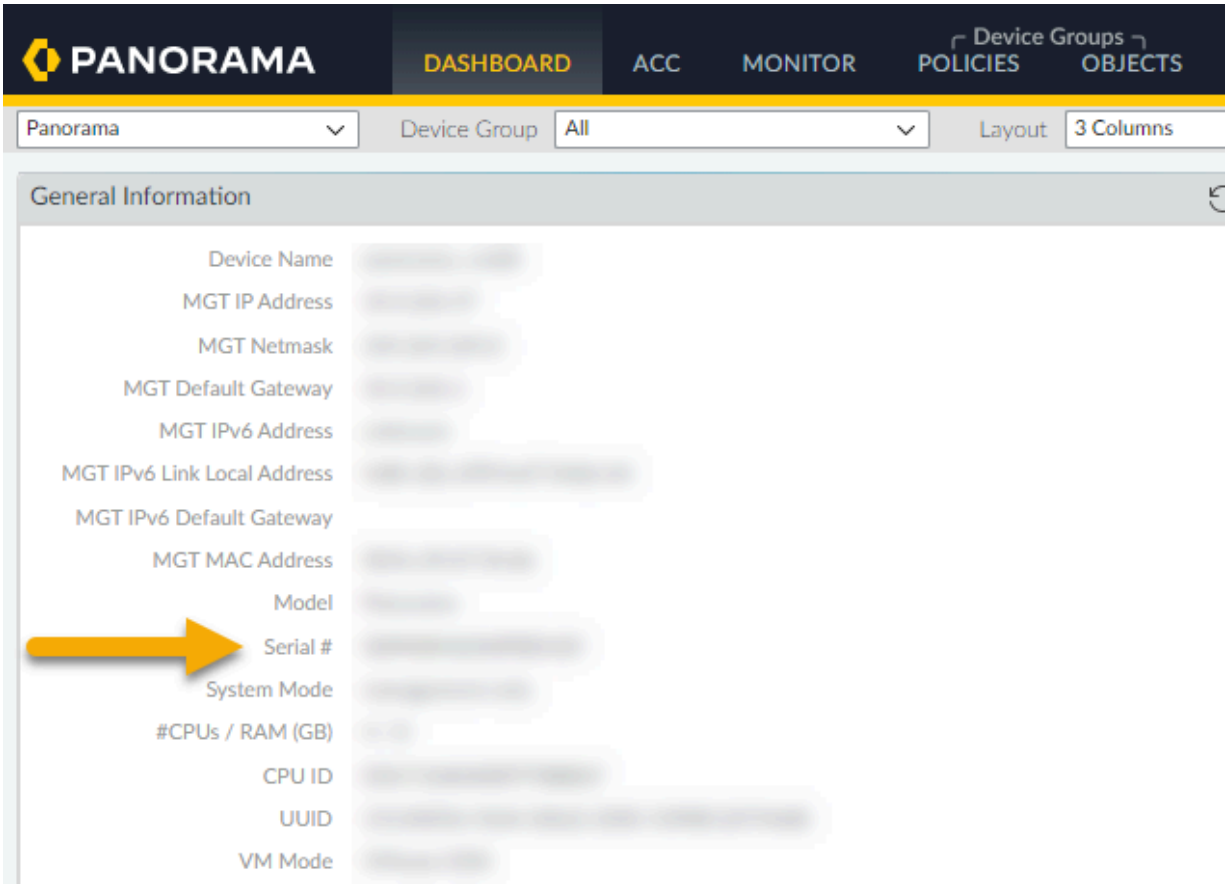
Cloud NGFWコンソールを使用してサポートケースを作成する方法:

STEP 1 | **AWS**アカウント**ID**を確認してください。**AWS** アカウントを選択します。

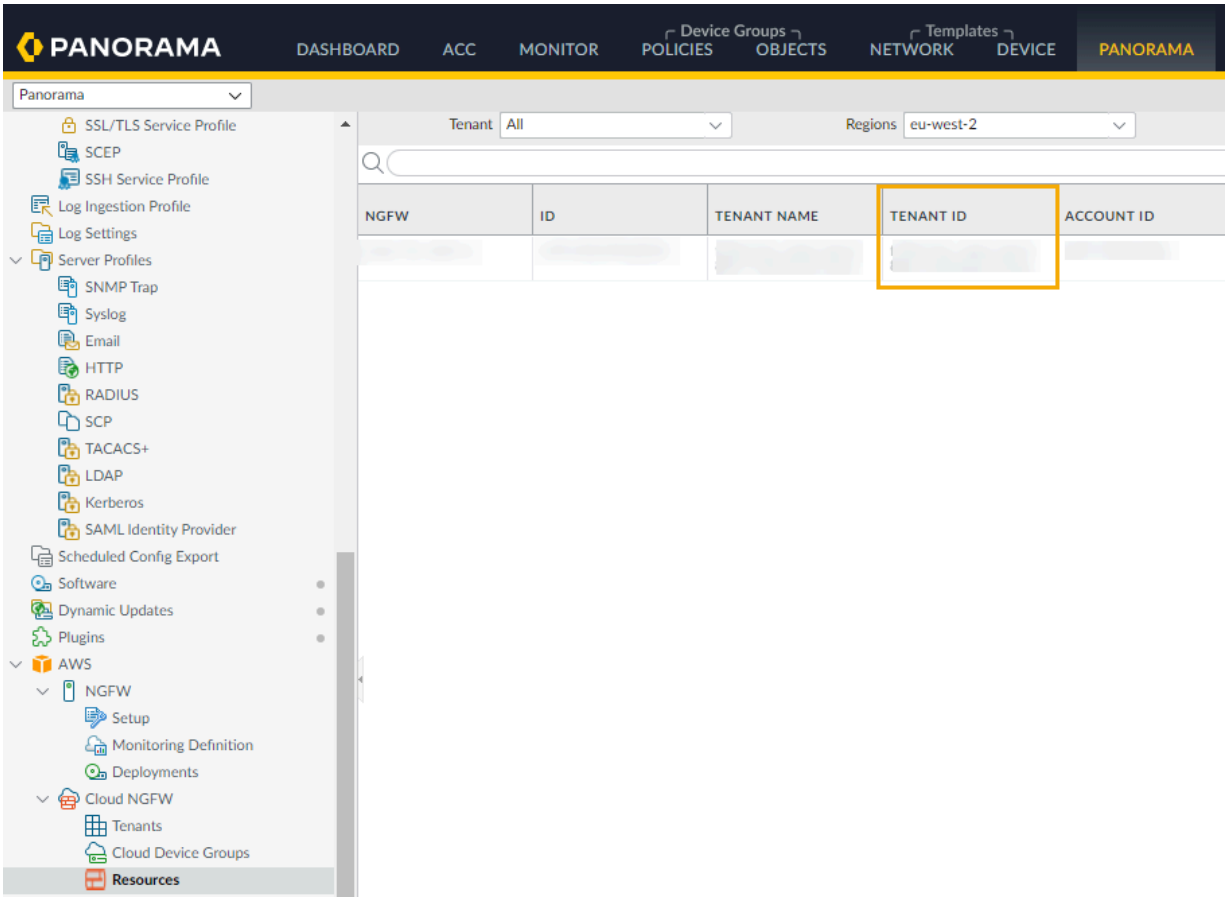


STEP 2 | 必要に応じて、Panoramaコンソールを使用して、テナントIDやPanoramaのシリアルナンバーなど、サポートケースに関する追加情報を確認してください。

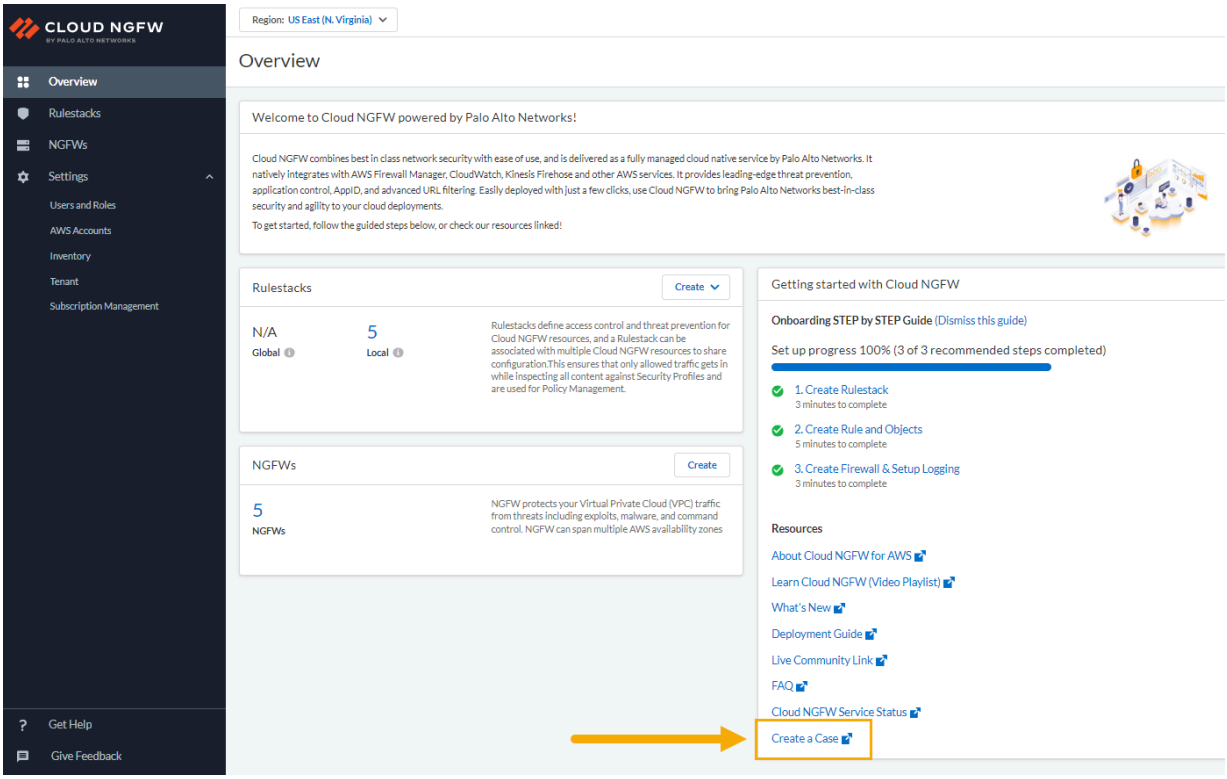
ダッシュボードを使用して**Panorama**のシリアルナンバーを確認してください。



Cloud NGFWリソースのテナント **ID**を確認します。



STEP 3 | Cloud NGFWコンソールの概要ページで、**[Create a case(ケースを作成)]**をクリックします。



使用量エクスプローラー

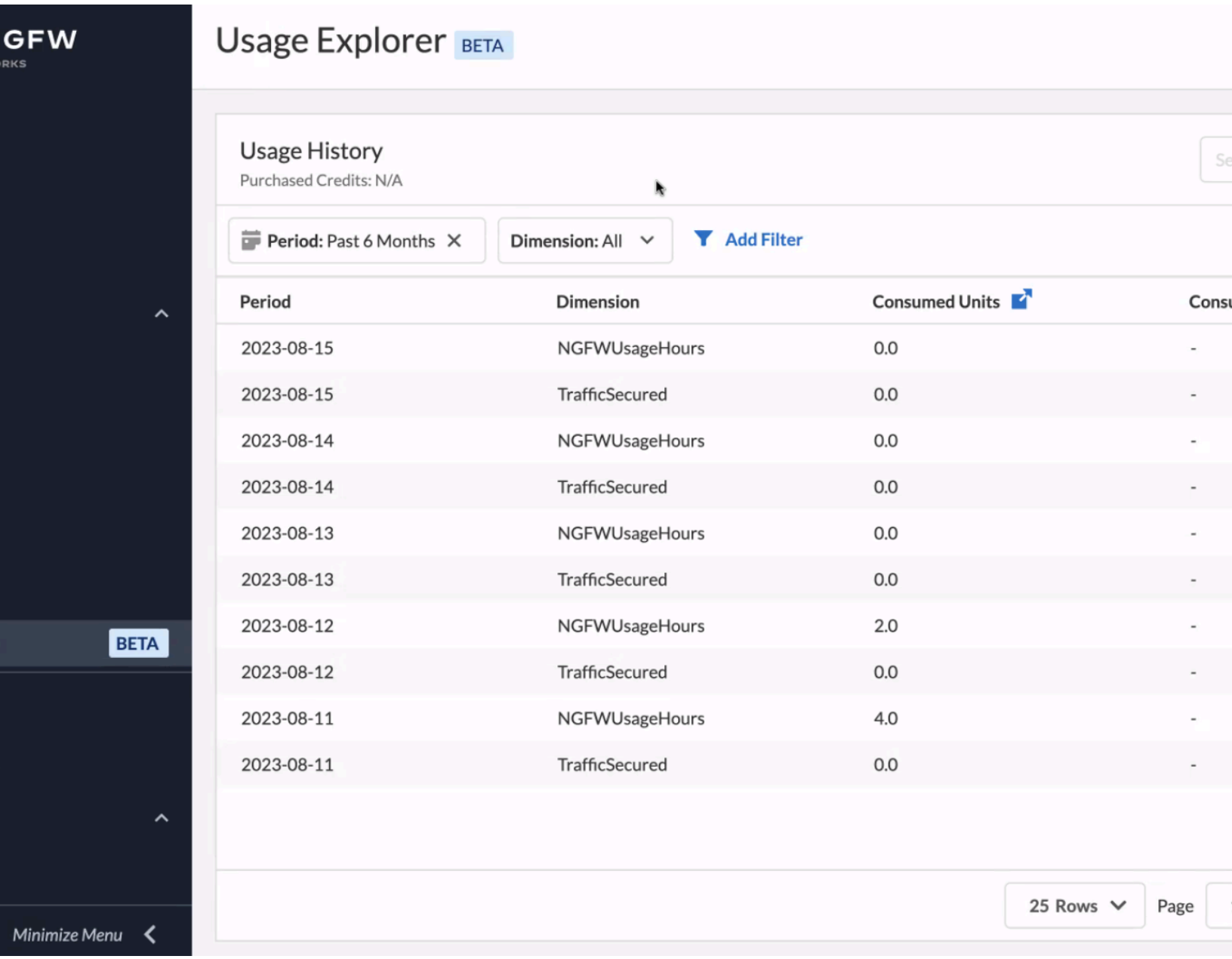
どこで使用できますか?	何が必要ですか?
• Cloud NGFW for AWS	❑ Cloud NGFWサブスクリプション ❑ Palo Alto Networksカスタマー サポート アカウント (CSP) ❑ AWS Marketplaceアカウント ❑ ユーザーのロール（テナントまたは管理者）

使用量エクスプローラーのダッシュボードでは、Pay-As-You-go（PAYG）(従量課金)とクレジットベースのサブスクリプション（契約を使用して購入）のテナントのCloud NGFW消費量を迅速かつ便利に判断できます。この情報には、平均消費量に関するインサイトや、テナントに関連付けられているCloud NGFWクレジットとの相関性など、日々の消費量が表示されます。

使用量エクスプローラー機能は、現在プレビュー版として提供されています。

使用量エクスプローラーにアクセスする方法:

1. Cloud NGFWコンソールに接続します。
2. コンソールで、**[Usage Explorer(**使用量エクスプローラー**)]**を選択します。



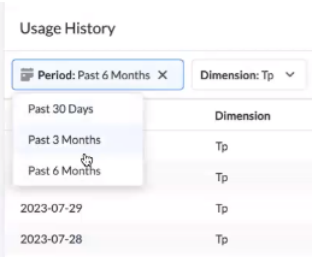
使用量エクスプローラーには、一定期間の消費量を表示するオプションがあり、CSVファイルをダウンロードして、今後の検査のために関連データをキャプチャできます。毎日の消費履歴は、以下のフィールドを含むテーブルで提供されます。

- [Period(期間)] - Cloud NGFWの消費期間を表します。
- [Dimension(ディメンション)] - Cloud NGFWの請求を識別するために使用されます。ディメンションとは、アドオン（脅威防御など）を指します。
- [Consumed Units(消費単位)] - 請求期間中にテナントが消費したリソースの量。このフィールドはPAYGサブスクリプションモデルに関連します。

- [Consumed as Credits(クレジットとして消費)] - 請求期間中にテナントが消費したリソースの量。PAYGサブスクリプション モデルに関連するフィールドです。

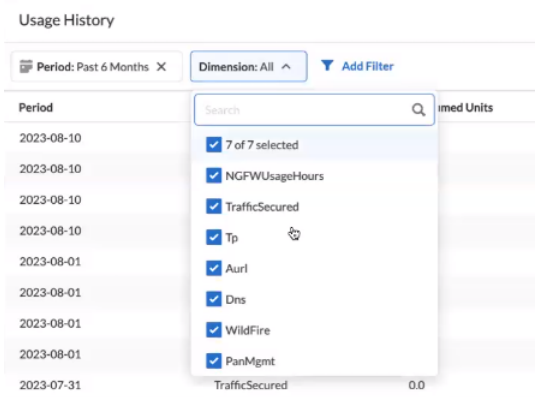
  サポートされているディメンションでのみフィルタリングできます。***[Add Filter(***フィルタの追加***)]***オプションは、現在このプレビュー リリースでは機能しません。

[Period(期間**)]**フィールドを使用して、指定した期間の消費量を表示します。このオプションを使用する場合は、消費を長期間フィルタリングすると、データを表示するときに遅延が発生する可能性があることを考慮してください。



デフォルトでは、使用量エクスプローラーには過去*30*日間の消費量データが表示されます。

[Dimensions(ディメンション**)]**フィールドを使用すると、使用量エクスプローラーの表示を変更して、契約に含まれるアドオン ディメンションのみを表示できます。

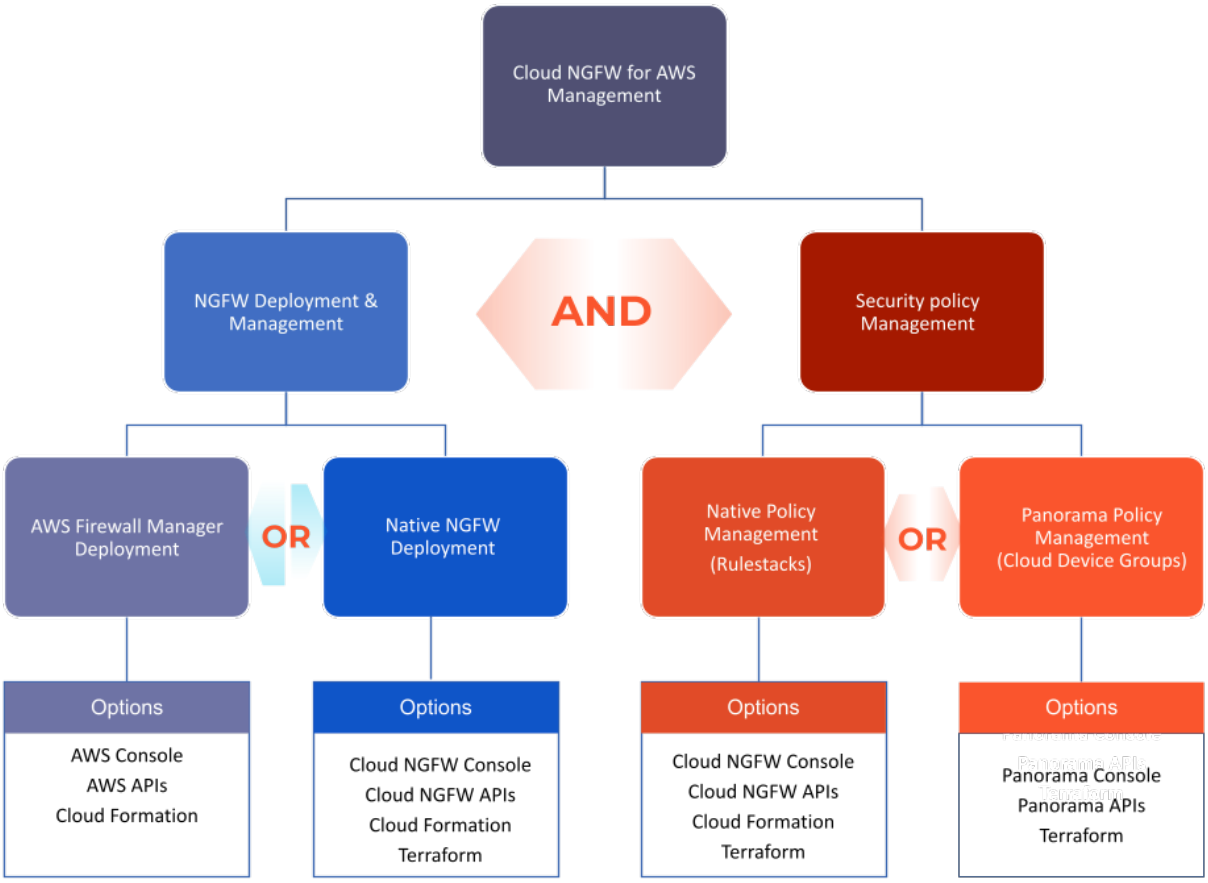


すべてのディメンションでフィルタリングすることも、ドロップダウン メニューからディメンションを選択することもできます。使用量エクスプローラーの表示は、*PAYG*または契約として、*Cloud NGFW*テナント サブスクリプション モデルによって異なります。

デプロイ

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 for AWSは、NGFWリソースのデプロイとセキュリティ ポリシー ルールの管理に複数のオプションを提供します。



NGFWのデプロイメントと管理

- ネイティブ**NGFW**デプロイメント—AWS Marketplace経由でCloud NGFWに登録すると、テナントを調達することになります。その後、Cloud NGFW コンソールを数回クリックするか、APIを使用すると、VPCのCloud NGFWリソースをデプロイできます。これらのリソースには、レジリエンス、スケーラビリティ、ライフサイクル管理が組み込まれています。また、これらのリソースを作成するための **Cloud Formation**またはTerraformのようなinfrastructure-as-codeツールを使用することもできます 。作成したセキュリティ ポリシーは、ネイティブ ポリシー管理(ルールスタック)または Panoramaポリシー管理(デバイス グループ)を使用して、これらのCloud NGFWリソースに対して作成できます。
- **AWS**ファイアウォールマネージャのデプロイメント— 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とVPCにNGFWをデプロイできます。AWSコンソール、AWSのAPIまたはCloud Formationを使用して、すべてのCloud NGFW設定をデプロイおよび管理するファイアウォールマネージャ ポリシー設定を作成します。

  AWSファイアウォールマネージャは、Cloud NGFWリソースがデプロイされているVPC 内のエンドポイント サブネット、ルート テーブル、およびゲートウェイ ロードバランサー エンドポイントも管理します。AWSファイアウォールマネージャを使用する場合、Cloud NGFWリソースは、セキュリティ設定とルールにCloud NGFW テナントのグローバル ルールスタックを使用します。以前にテナントでグローバル ルールスタックを設定していない場合(Panorama ポリシー管理を使用)、AWSファイアウォール マネージャは Cloud NGFW コンソールにリダイレクトし、ネイティブ ポリシー管理を使用してグローバル ルールスタックを作成および管理します。

セキュリティ ポリシー管理

- ネイティブ ポリシー管理— Cloud NGFW コンソールまたはAPIを使用してルールスタックをネイティブに作成して、Cloud NGFW リソースのセキュリティ ポリシー ルールを管理できます。また、これらのルールスタックを作成するためのCloud FormationまたはTerraformのような Infrastructure-as-codeツールを使用することもできます。ルールスタックは、NGFWの高度なアクセス制御(App-ID、URLフィルタリング)と脅威防御の動作を定義します。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。
- **Panorama**ポリシー管理- Cloud NGFWテナントをPanoramaアプライアンスにリンクして、Cloud NGFW リソースのポリシー ルールを作成および管理できます。Panoramaコンソール、API又は Terraformを使用して、これらのセキュリティ ポリシー ルールをクラウド デバイス グループで作成します。Panoramaクラウド デバイス グループで作成したポリシーは、Cloud NGFWテナントのグローバル ルールスタックとして現れます。
- **Strata Cloud Manager** ポリシー管理 — クラウド NGFW リソースを Strata Cloud Manager (SCM) にリンクしてポリシー管理を行うことができます。Strata Cloud Managerは、ネットワーク セキュリティ デプロイメント全体を統合管理するため、Palo Alto Networksのセキュリティ インフラストラクチャを単一の合理化されたWebインターフェースから簡単に管理でき

ます。このインターフェースを使用すると、すべてのネットワーク セキュリティ適用ポイントで、ユーザー、ブランチ サイト、アプリケーション、および脅威を包括的に可視化できます。この機能により、実用的な分析情報、セキュリティの向上、簡単なトラブルシューティングと問題解決が可能になります。

AWS で NGFW リソースを作成する

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）

ルールスタックとルールを作成したので、NGFW リソースを作成し、ローカルルールスタックをその NGFW に関連付けることができます。NGFW の構成中に、NGFW エンドポイントを自動または手動で作成する方法を選択する必要があります。NGFW エンドポイントを手動で作成することを選択した場合は、指定したアベイラビリティゾーンにNGFW エンドポイントを作成する必要があります。

NGFW を作成するには、次の手順を実行します。

STEP 1 | ［**NGFW**］を選択します。

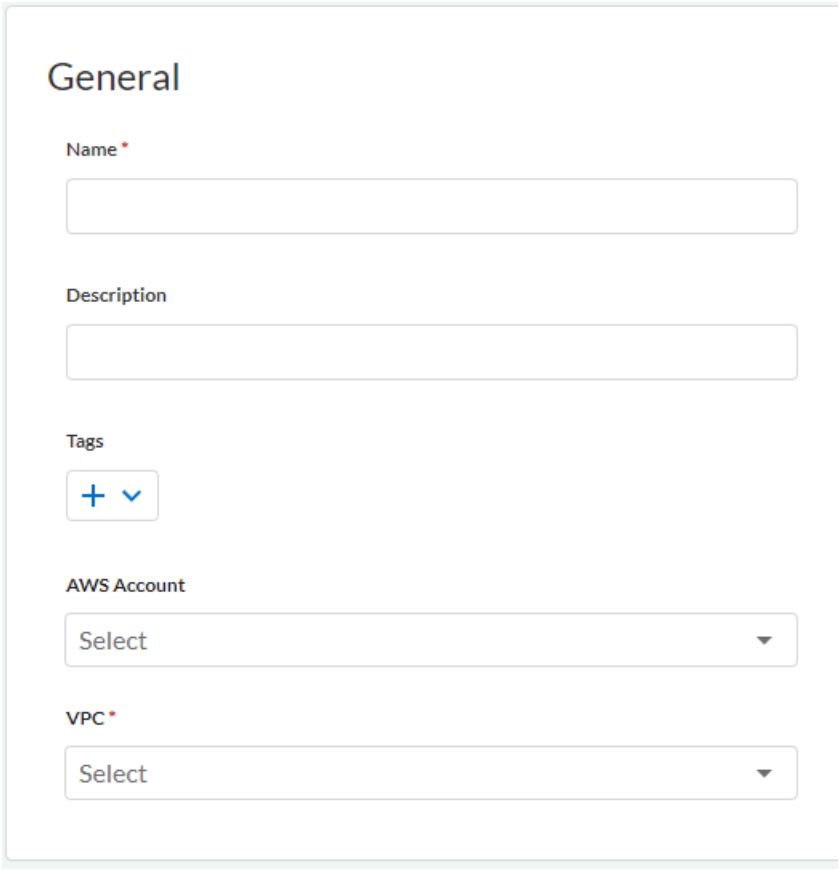
STEP 2 | ［ファイアウォールの追加]をクリックします。

STEP 3 | 分かりやすい **Name**（名前）を入力します。

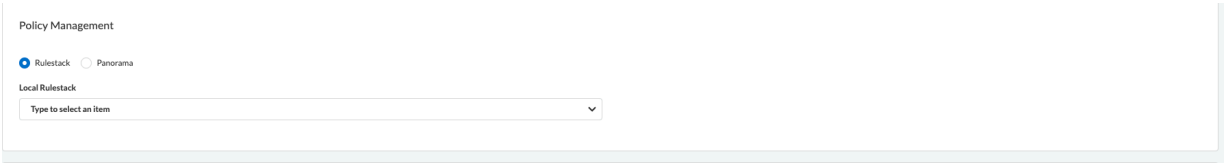
STEP 4 | （任意）**Description (**内容**)** を入力します。

STEP 5 | ドロップダウンから **AWS** アカウントを選択して、この NGFW に関連付けます。

STEP 6 | ドロップダウンから**VPC**を選択します。



STEP 7 | **[Policy Management(ポリシー管理)]**セクションで、ドロップダウンから **[Local Rulestack(ローカル ルールスタック)]**を選択します。

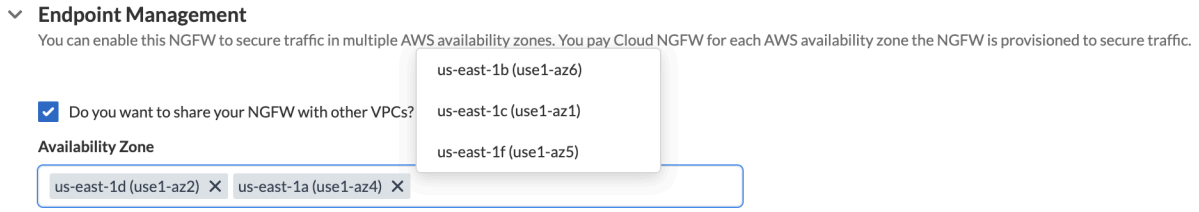


STEP 8 | AWS アベイラビリティ ゾーンまたはサブネットを指定します。Cloud NGFW テナントが NGFW エンドポイントを展開するかどうか (サービス管理モード)、または展開しないかどうか (顧客管理モード) を指定します。

- はい（サービス管理） - サービス管理モードでは、Cloud NGFW テナントは、指定した VPC サブネットに NGFW エンドポイントを自動的に作成します。サービス管理モードのエンドポイント管理は、Cloud NGFW コンソールからのみ実行します。サービス管理モードのエンドポイント管理は、サブネットの関連付けまたは関連付け解除によってのみ実行できます。サブネットを関連付けるとエンドポイントが作成され、サブネットの関連付けを解除するとエンドポイントが削除されます。
- いいえ（顧客管理） - 顧客管理モードでは、指定した各アベイラビリティゾーンに NGFW エンドポイントを手動で作成する必要があります。

> ***[Endpoint Management(***エンドポイント管理***)]***セクションでは、複数の*AWS*アベイラビリティーゾーンのトラフィックを保護するために*Cloud NGFW* を有効にすることができます。料金は、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*アベイラビリティー ゾーンごとにお支払いいただきます。これらのアベイラビリティー ゾーンで*NGFW*のエンドポイントを作成する方法を管理できます。*NGFW*用に作成する *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。

[Availability Zone(可用性ゾーン**)]**にはPalo Alto Networksアカウントの**[Zone ID(**ゾーン **ID)]** と対応する**[Availability Zone Name(**可用性ゾーン名**)]**が表示されます。可用性ゾーンをAWSアカウントにマッピングするときにこの情報を使用します。



STEP 9 | 作成をクリックします。

AWS エンドポイント用のクラウド NGFW を作成する

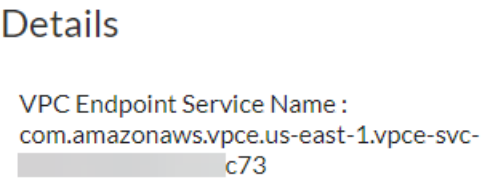
どこで使用できますか?	何が必要ですか?
• Cloud NGFW for AWS	❑ Cloud NGFWサブスクリプション ❑ Palo Alto Networksカスタマー サポート アカウント (CSP) ❑ AWS Marketplaceアカウント ❑ ユーザーのロール（テナントまたは管理者）

NGFW の作成時に顧客管理モードを選択した場合は、選択したサブネットの NGFW エンドポイントを手動で作成する必要があります。AWS コンソールでは、NGFW エンドポイントはゲートウェイロードバランサーエンドポイントとして表示されます。

NGFW エンドポイントを接続するサブネットは、NGFW の作成時に指定した仮想プライベートクラウド (VPC) 内にある必要があります。

STEP 1 | Cloud NGFW テナントから、**NGFW** を選択し、ファイアウォールをクリックします。

STEP 2 | ［エンドポイント］を選択し、VPC エンドポイントサービス名をメモします。



STEP 3 | AWS コンソールにログインします。

STEP 4 | ［サービス］ > ［ネットワーキングとコンテンツ配信］ > ［**VPC**］を選択します。

STEP 5 | VPC ダッシュボードから、 **[エンドポイント]** > **[エンドポイントの作成]**を選択します。

STEP 6 | 上記でメモした VPC エンドポイント サービス名に対応する名前でサービスを検索を選択します。

STEP 7 | ファイアウォールの作成時に指定した **VPC** をドロップダウンから選択します。

STEP 8 | NGFW エンドポイントを作成するサブネットを選択します。

STEP 9 | **[エンドポイントの作成]** をクリックします。

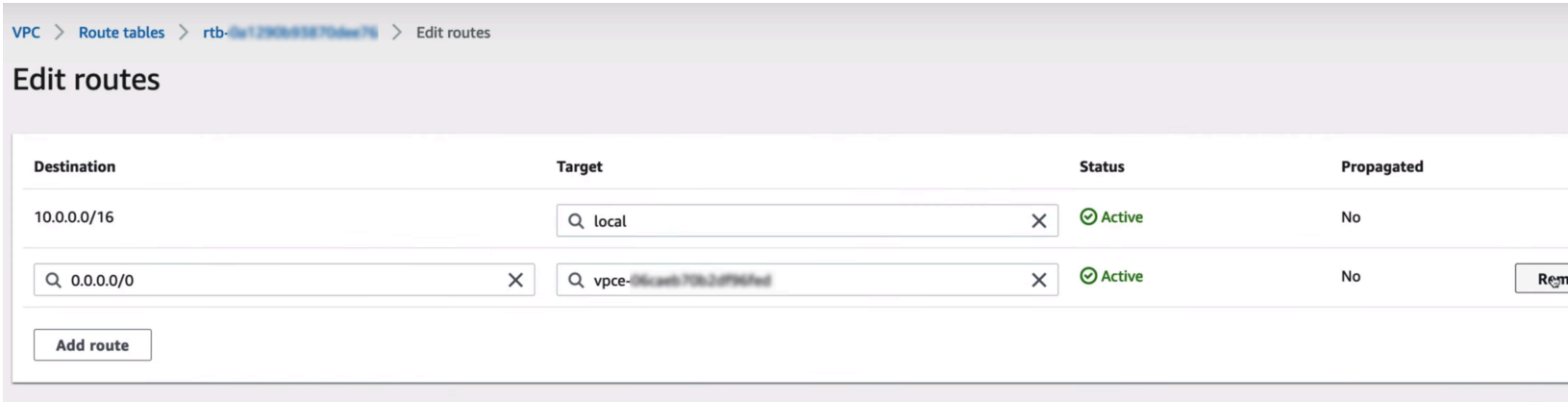
Cloud NGFWリソースの削除

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リソースが不要になった場合は、以下の手順を実行してAWSデプロイメントから削除します。

STEP 1 | ルートテーブルから関連するCloud NGFWエンドポイントを削除します。

1. AWS コンソールにログインします。
2. **VPC**を選択し、Cloud NGFWエンドポイントを含むVPCを探します。
3. **[Route Tables(**ルート テーブル**)**］を選択してから、削除するエンドポイントのルートテーブルを選択します。



4. **[Edit Routes(**ルートの編集**)**］をクリックします。
5. ルートテーブルからルートを削除するには、**[Remove(**削除**)]**をクリックします。
6. **[Save changes**（変更内容の保存）**]**をクリックします。

STEP 2 | (顧客管理エンドポイントのみ)独自のCloud NGFWエンドポイントを展開した場合は、AWSコンソールから削除する必要があります。

1. AWSコンソールから**[E**エンドポイント］を選択し、Cloud NGFWエンドポイントを選択します。
2. **[Actions(**アクション**)]** > **[Delete(**削除**)]**を選択し、削除を確認します。

STEP 3 | Cloud NGFWテナントからCloud NGFWリソースを削除します。

1. Cloud NGFWコンソールにログインし、**[NGFWs]**を選択します。
2. 削除するリソースを選択します。
3. **[Actions(アクション)]**ドロップダウンから、**[Delete(削除)]**をクリックします。
4. 削除を**[Confirm(確認)]**します。

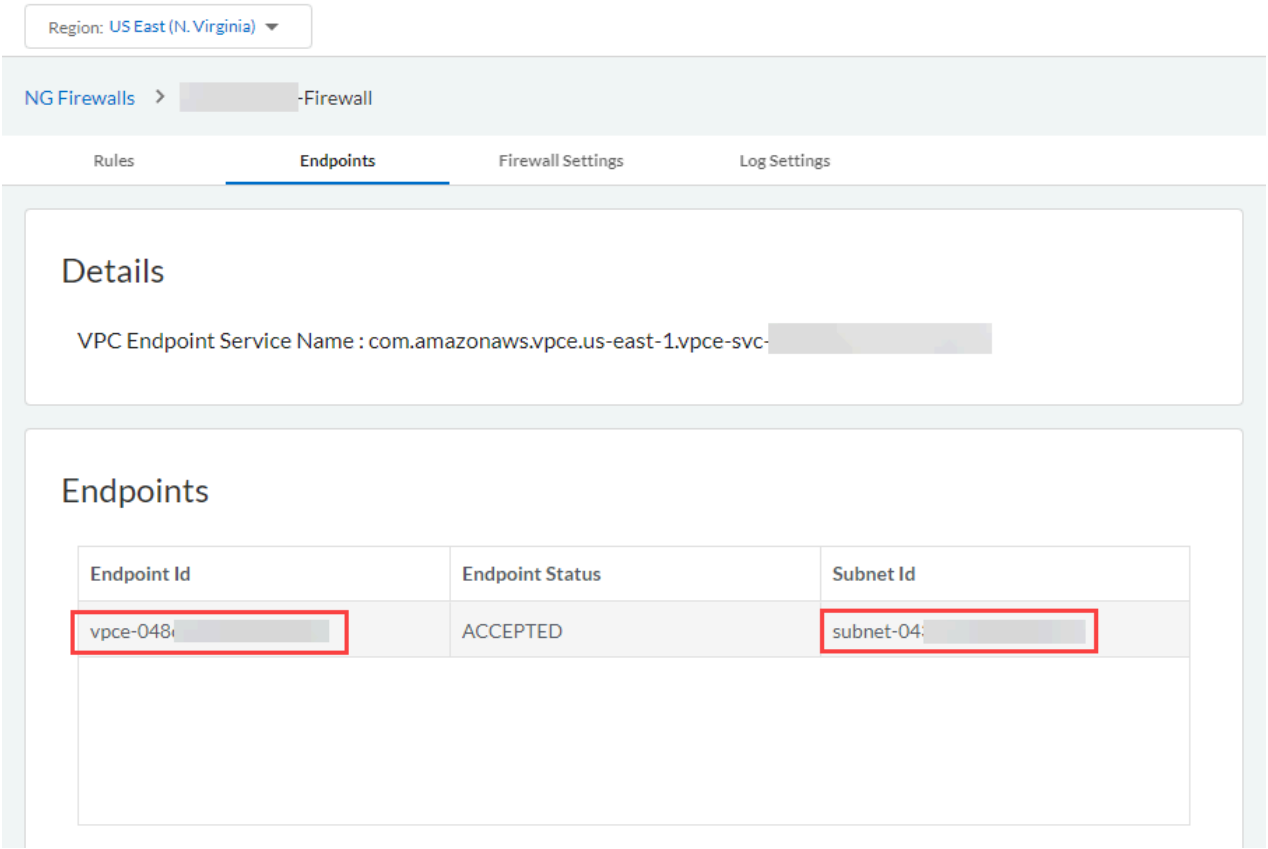
   数分後、Cloud NGFWリソースとそのすべてのエンドポイントがCloud NGFWデプロイメントから削除されます。

Cloud NGFW for AWS にトラフィックを転送する

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）

Cloud NGFW をデプロイしてエンドポイントを作成したら、ルートテーブルを更新してトラフィックをファイアウォールに送信する必要があります。どのルートテーブルを更新し、どのように更新するかは、特定の展開によって異なります。

AWS コンソールでは、NGFW エンドポイントは Gateway Load Balancer エンドポイントとして表示されます。エンドポイント ID によって、AWS コンソールで NGFW エンドポイントを識別できます。特定のファイアウォールのエンドポイント ID は、Cloud NGFW コンソールの **NGFWs** > **firewall-name** > **Endpoints**下にあります。



以下は、さまざまなデプロイメントモードでのパケット フローの例であり、それらのパケット フローの更新されたルートの例が含まれています。

- Cloud NGFW for AWS 集中型デプロイメント
- Cloud NGFW for AWS の分散型デプロイメント

プライベートトラフィック範囲の設定

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 を使用すると、エンドポイントごとにプライベート トラフィック範囲を指定できます。デフォルトでは、プライベート トラフィック範囲プレフィックスには、IANA RFC 1918で指定されている VPC 許可 IP アドレス範囲が含まれます。ただし、ハイブリッド クラウド ネットワークには、IANA RFC 6598 に準拠した共有アドレス空間や、プライベート トラフィック範囲プレフィックス内のパブリックにルーティング可能な CIDR ブロックの特定のセットが追加で含まれる場合があります。

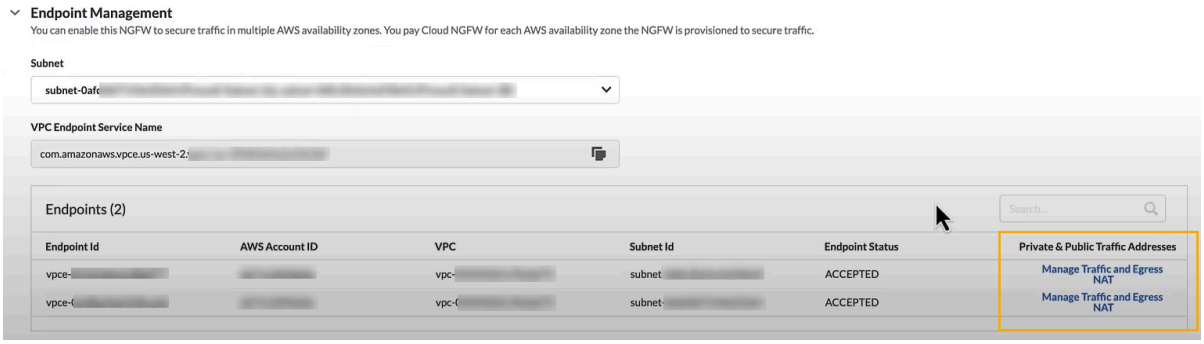
プライベート トラフィック範囲を構成するには:

STEP 1 | Cloud NGFW コンソールにログインします。

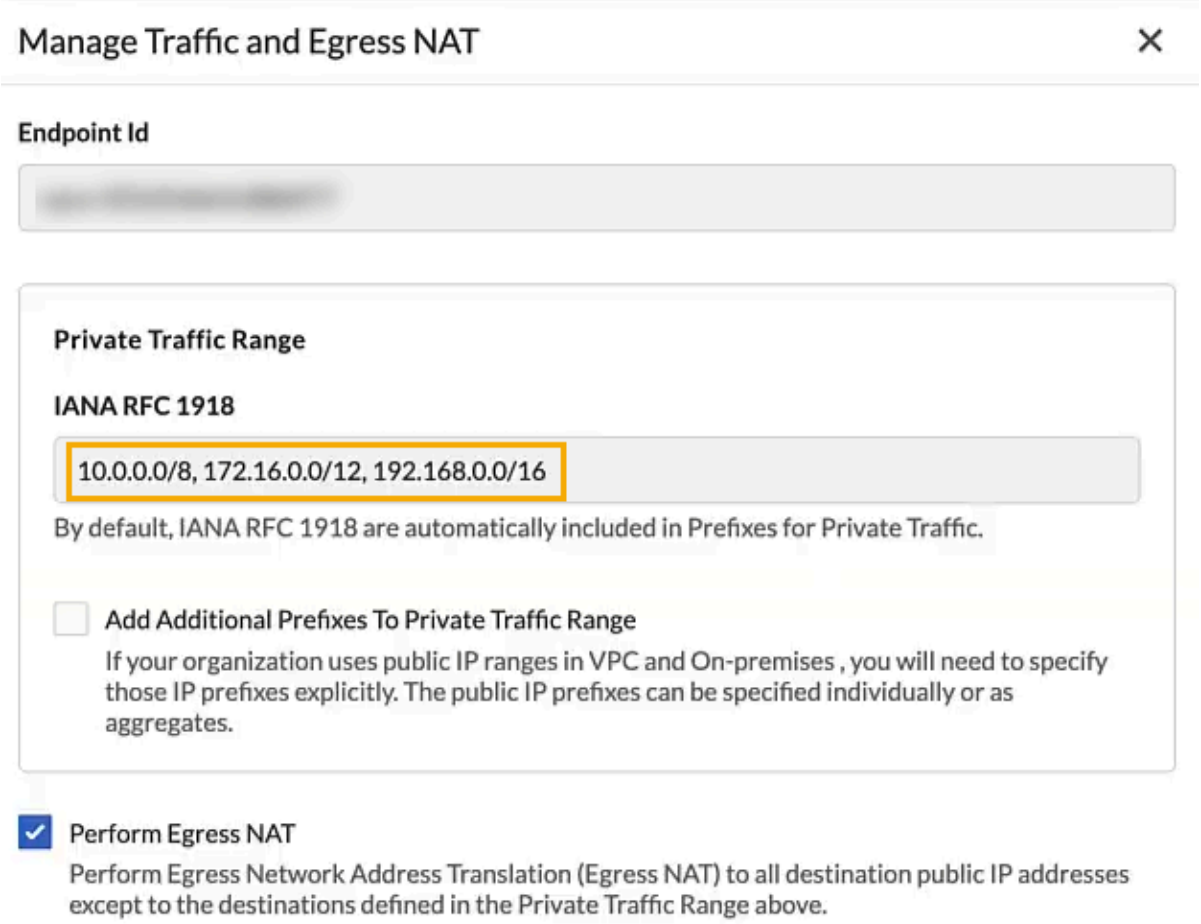
STEP 2 | **NGFW**をクリックします。

STEP 3 | エンドポイント管理セクションで、ドロップダウン メニューからサブネットを選択します。

STEP 4 | エンドポイント テーブルで適切なエンドポイントの トラフィックと出口 **NAT** の管理を 選択します。



STEP 5 | **[**トラフィックと出口 **NAT** の管理**]** 画面で、明示的に含める IP アドレス (またはアドレス群) を指定します。



STEP 6 | プライベート トラフィック範囲にプレフィックスを追加するには、チェック ボックスをオンにします。

STEP 7 | プライベート トラフィック範囲に記載されているものを除くすべてのパブリック IP アドレスの宛先に対してアドレス変換が行われるようにするには、**[**出口 **NAT** を実行する**]** チェック ボックスをオンにします。

STEP 8 | **[Save(**保存**)]**をクリックします。

出口NATの設定

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 は、パブリック インターネットの宛先への送信トラフィックに対してソース NAT を実行する 2 つの方法を提供します。AWS NAT ゲートウェイ と クラウド NGFW Egress NAT。

Egress NAT 機能は、既存のファイアウォール *(Cloud NGFW for AWS* のこのリリースより前に作成されたもの*)* ではサポートされていません。*Egress NAT* を使用するには新しいものを作成します。

AWS NAT ゲートウェイ

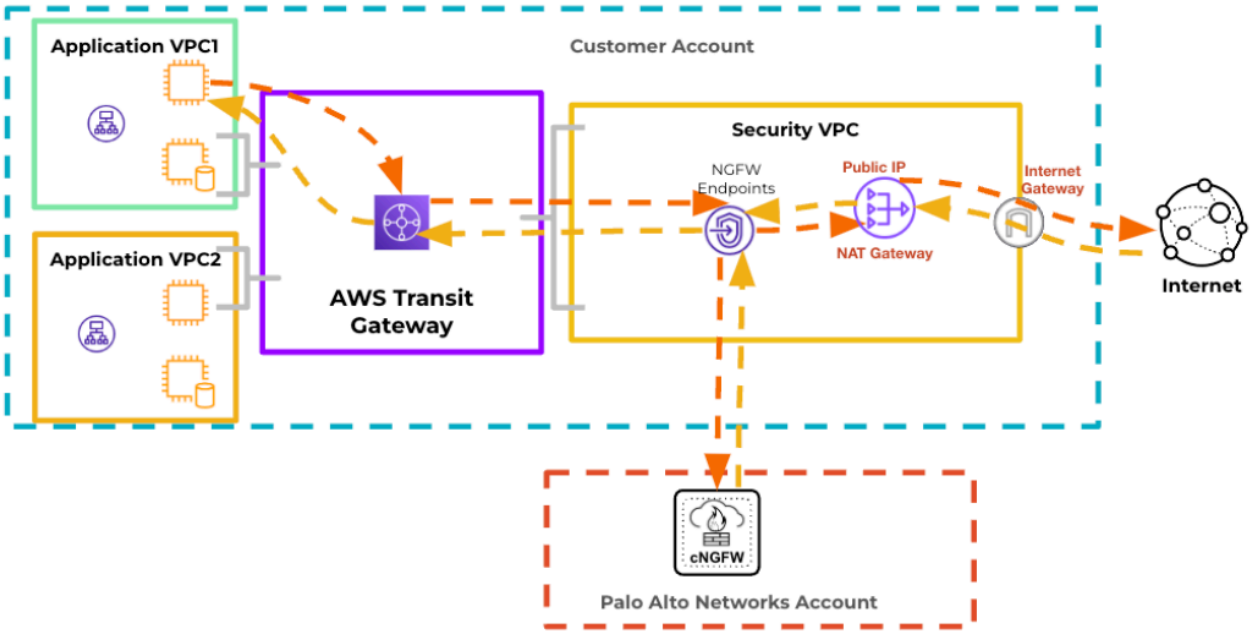
Amazon NAT ゲートウェイを使用 すると、プライベートサブネット内の VPC リソースは、パブリックインターネットを含むサブネット外のサービスに安全にアクセスでき、一方でプライベートリソースは未承諾トラフィックからアクセス可能になります。

VPC 内の AWS NAT ゲートウェイを引き続き使用できます。このシナリオでは、クラウド NGFW は Bump-In-The-Wire として機能し、検査されたすべてのトラフィックをエンドポイントに戻します。

NAT ゲートウェイと関連する *Egress* データ転送コストについては *AWS* にお支払いいただきます。*Egress*

NAT は、*Strata Cloud Manager (SCM)* ファイアウォールではサポートされていません。

以下の画像は、AWS NAT ゲートウェイを使用したインターネット向けトラフィックのソース NAT を示しています。



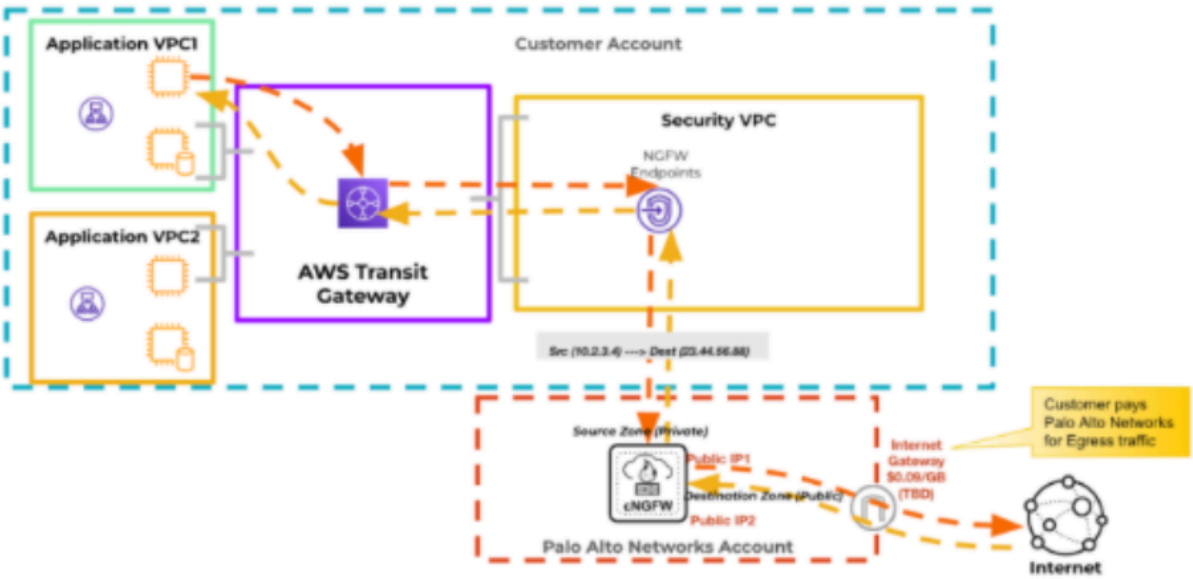
AWS を使用して *NAT* を設定する方法については、「NAT ゲートウェイの操作」を参照してください。

Cloud NGFW Egress NAT

または、Egress NAT 機能を設定します。この場合、Cloud NGFW は、トラフィックが Cloud NGFW リソースに入るエンドポイントに対して定義された プライベート トラフィック範囲 プレフィックス内の宛先 IP アドレスを持つセッションを除くすべての送信トラフィックに対してソース NAT を実行します。この場合、Cloud NGFW リソースは検査されたトラフィックをエンドポイントにリダイレクトしません。あるいは、検査された出口トラフィックはインターネットに直接送信されます。AWS NAT ゲートウェイのコストは発生しなくなりますが、出口トラフィックのデータ転送に対して Palo Alto Networks に料金を支払うことになります。ただし、パブリック IP アドレスを Cloud NGFW リソースに関連付けるには、次の 2 つの方法のいずれかを使用します。

1. Palo Alto Networks が管理する AWS Elastic IP Address (EIP) アドレスを使用して VPC のソース NAT を実行するように Cloud NGFW リソースを設定します。この場合、EIP 管理コストが時間単位で発生します。
2. 時間単位の EIP 管理コストを回避するには、BYOIP を AWS アカウントから Cloud NGFW に転送します。詳細については、「AWS IPAM を使用した BYOIP」を参照してください。

以下の画像は、Cloud NGFW Egress NAT を使用したインターネット バウンド トラフィックでのソース NAT の動作を示しています。Cloud NGFW Egress NAT を使用したインターネット バウンド トラフィックでのソース NAT は次のとおりです。

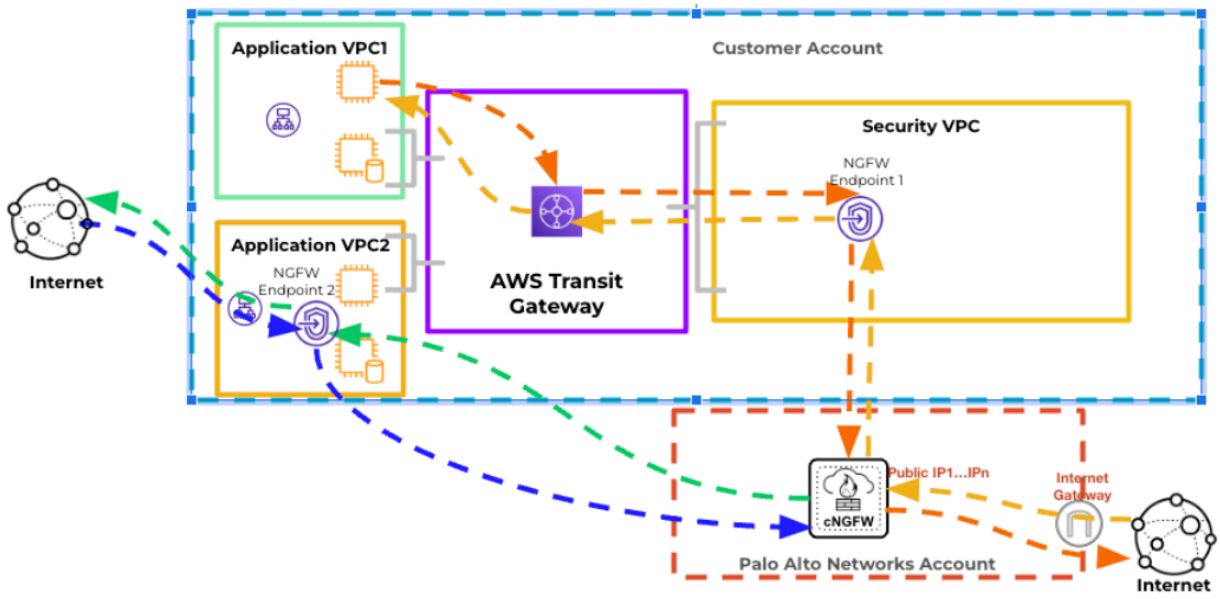


ハイブリッドNAT設定

NGFW リソースに対して Egress NAT を有効にすることはできますが、1 つ以上のエンドポイントで Egress NAT 設定を無効にするようにカスタマイズできます。この場合、Cloud NGFW は次のように動作します。

1. エンドポイントで Egress NAT を無効にすると、Cloud NGFW は Bump-In-The-Wire として機能し、検査されたすべてのトラフィックをエンドポイントに戻します。
2. エンドポイントで Egress NAT を有効にしたままにすると、Cloud NGFW は検査されたトラフィックを直接インターネットにリダイレクトします。

以下の画像は、エンドポイント 1 に対して Egress NAT が有効になっており、エンドポイント 2 に対して無効になっていることを示しています。



Palo Alto Networks マネージド AWS EIP を使用して出口NAT を構成する

AWS では、Elastic IP アドレス (EIP) は、動的なクラウド コンピューティングに使用される静的 IPv4 アドレスを表します。Elastic IP アドレスはパブリック インターネットからアクセスできますが、プライベート インスタンスに関連付けることでインターネットとの通信が可能になります。Egress NAT は、ルールスタックと Panorama ポリシー管理でのみサポートされます。

Palo Alto Networks が管理する AWS EIP を使用して Egress NAT を構成方法:

STEP 1 | Cloud NGFW コンソールにログインします。

STEP 2 | **NGFW**をクリックします。

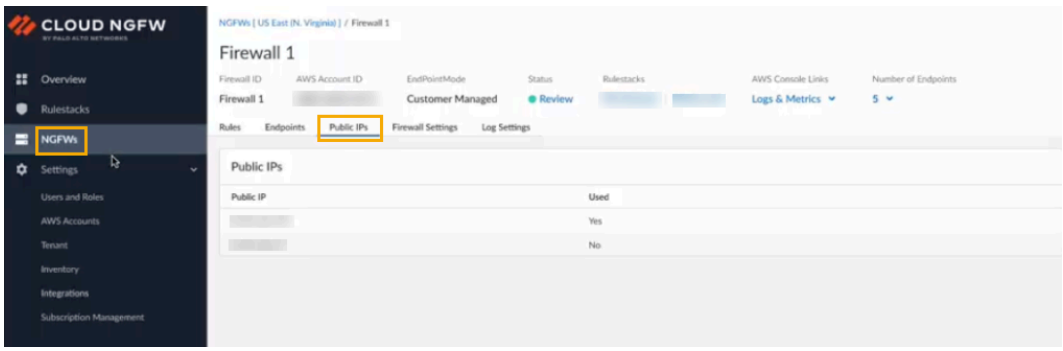
STEP 3 | 新しい NGFW リソースを作成します。

STEP 4 | ポリシー管理 セクションで、**Panorama**を選択します。ドロップダウン メニューを使用して、 統合されたPanoramaを選択します。

STEP 5 | **Egress NAT** セクションで、**Egress NAT** を有効にするを選択します。

STEP 6 | **[**パブリック **IP]** セクションで、**[AWS** サービス **IP]**を選択します。

ファイアウォール ページで *[*パブリック ***IP]*** タブを選択すると、出口 *NAT* トラフィックでサポートされている *IP* アドレスのリストが表示されます。



ファイアウォールが作成されたら、そのステータスを確認します。

独自の IP の持ち込み (BYOIP) を使用して出口 NAT を構成する

このシナリオでは、時間単位の EIP 管理コストが発生しないように、BYOIP アドレスを AWS アカウントから転送します。

BYOIP を使用するには、AWS アカウントに IP アドレス管理 (IPAM) プールを作成し、それを Cloud NGFW for AWS デプロイメント アカウントで共有する必要があります。IPAM は、セキュリティ要件を満たすために IP アドレス スキーマを管理するのに役立ちます。詳細については、AWS サイトの 「独自の IP アドレスを使用する」を 参照してください。Egress NAT は、ルールスタックと Panorama ポリシー管理でのみサポートされます。

*AWS で IPAM プールを作成するときは、Cloud NGFW データプレーンと AWS 間で IP アドレスを共有するために、Cloud NGFW の Palo Alto Networks AWS アカウント ID をホワイトリストに登録する必要があります。IPAM プールの作成プロセス中に、**Amazon VPC IP** アドレス マネージャーを許可する オプション (IPAM プールを作成するための必須の手順) を選択し、Cloud NGFW リソースの AWS データプレーン アカウント ID を指定します。010510656586.*

IPAM プールの作成には約 10 分かかる場合があります。

IPAMプールを作成する

IPAM プールを作成するには:

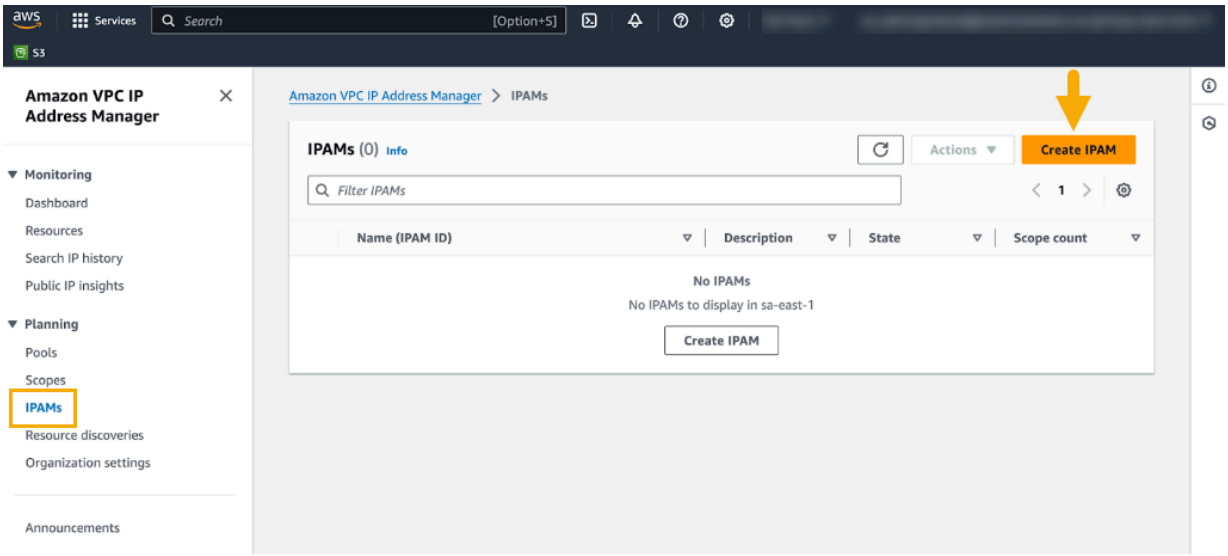
STEP 1 | AWS VPC IP アドレスマネージャーにログインします。

STEP 2 | **[計画] > [IPAM]**を選択します。

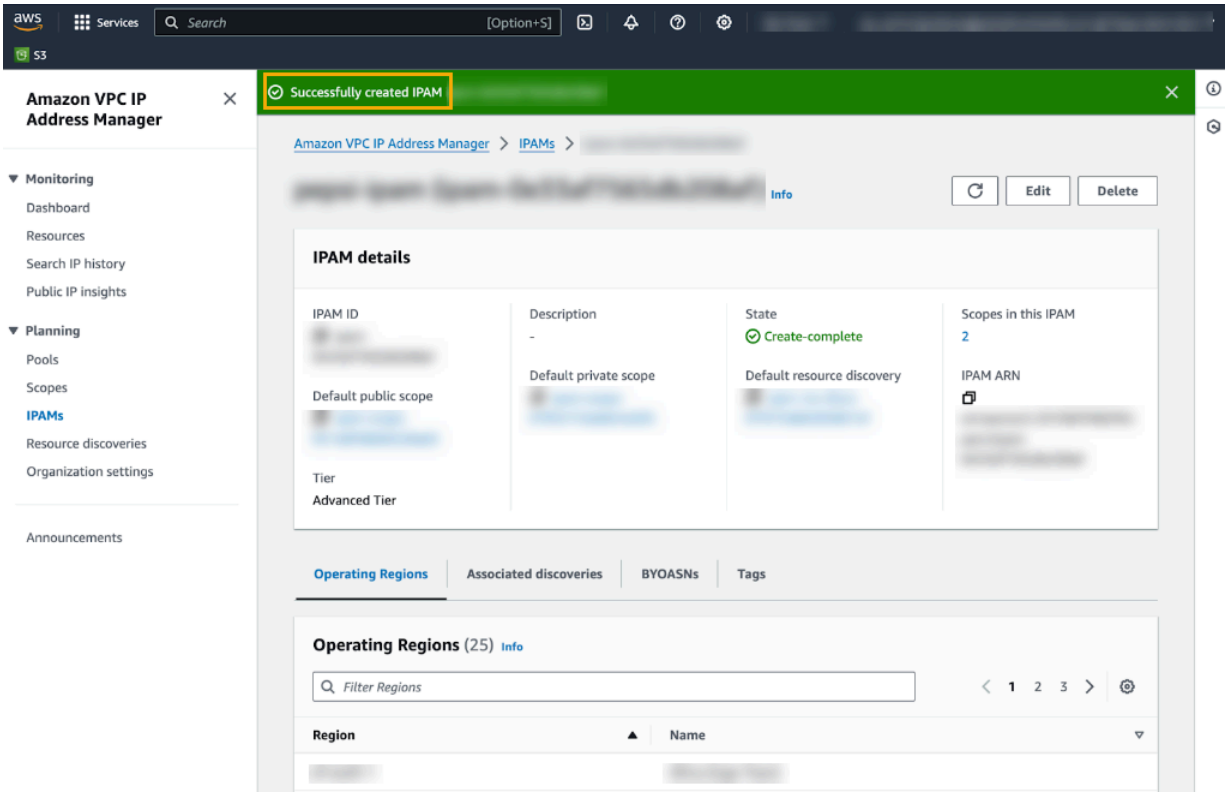
STEP 3 | **IPAM** ページで、「**IPAM** の作成」をクリックします。

詳細については、*AWS* ページの IPAM の作成手順を参照してください。

IPAM が正常に作成されると、**AWS VPC IP** アドレス マネージャーに IPAM の詳細が表示されます。

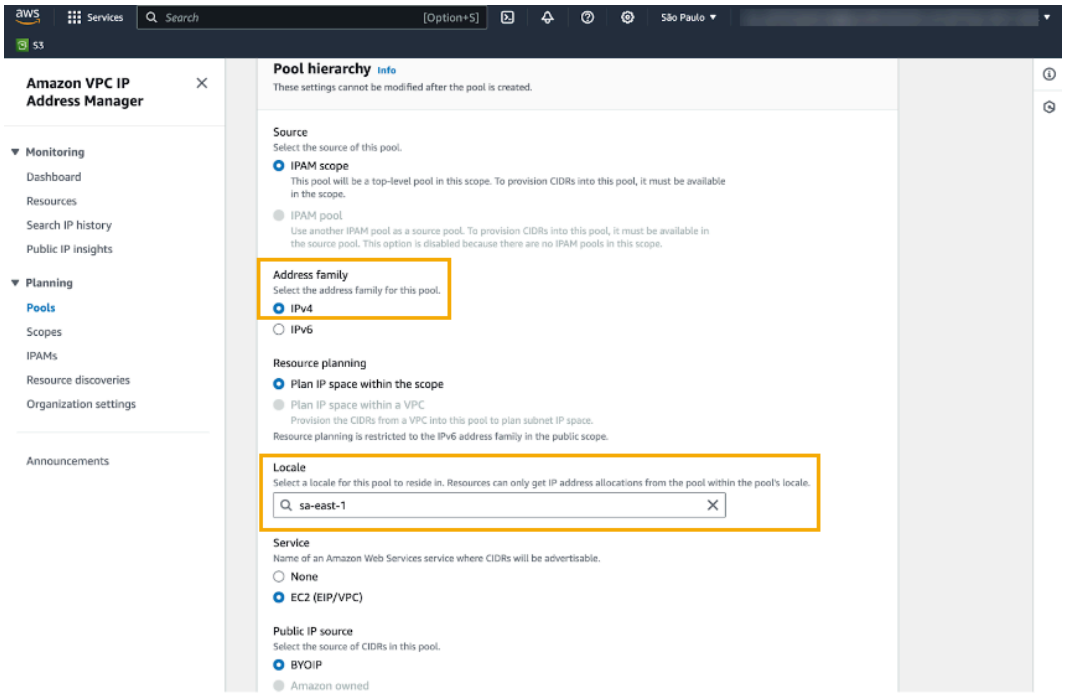


IPAM が正常に作成されると、**AWS VPC IP** アドレス マネージャーに IPAM の詳細が表示されます。

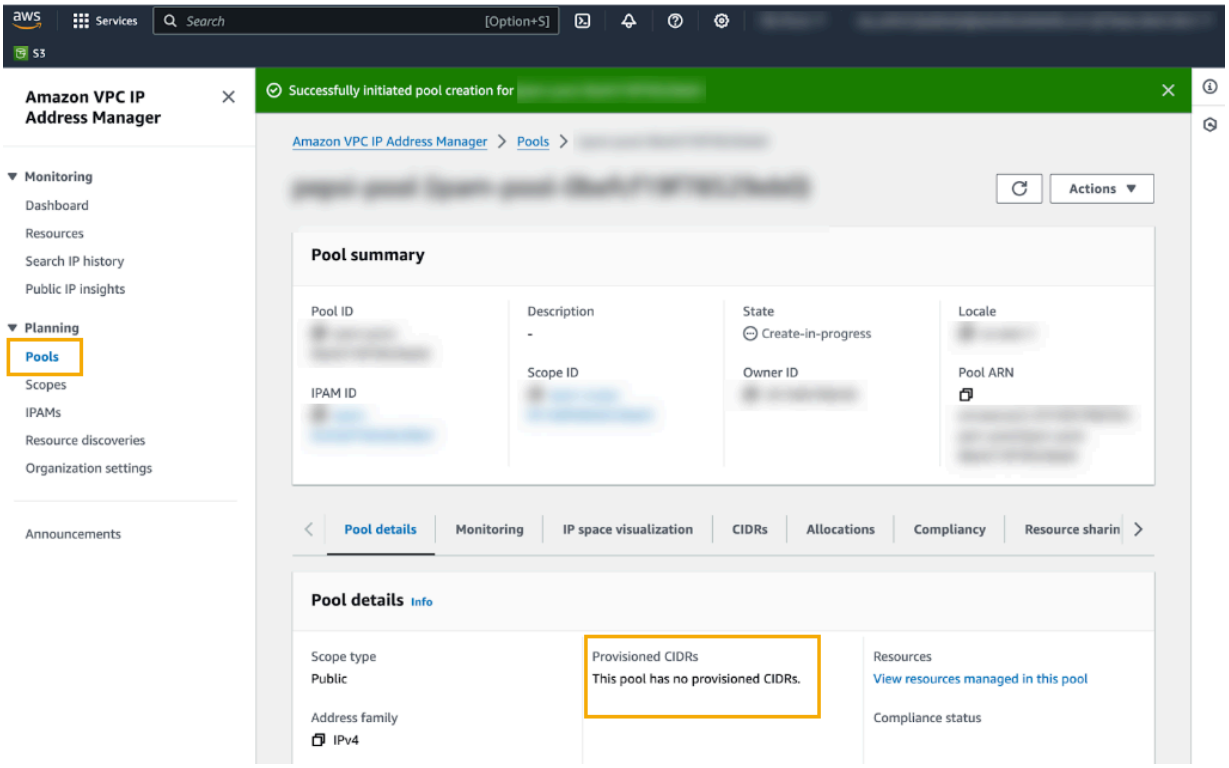


STEP 4 | IP アドレスのプロビジョニングを計画するために IPAM プール を作成します。**[計画] > [プール]** を選択し、**[プールの作成]**をクリックします。

IPAM プールを作成するときは、 プール階層 画面に示すように、 アドレス ファミリを***IPv4***に設定し、ロケールを *Cloud NGFW* リソースをデプロイする 場所に設定する必要があります。



IPAM が正常に作成されると、**AWS VPC IP** アドレス マネージャーに 新しいプールの詳細が表示されます。



新しく作成されたプールには *CIDR* がプロビジョニングされていません。パブリック *IP CIDR* 範囲と対応する証明書の秘密キーが必要になります。

STEP 5 | 前の手順で新しく作成したプールに CIDRS をプロビジョニングします。**[計画] > [プール]** を選択し、**[プールの概要]**の下の **[CIDR]** タブを選択します。

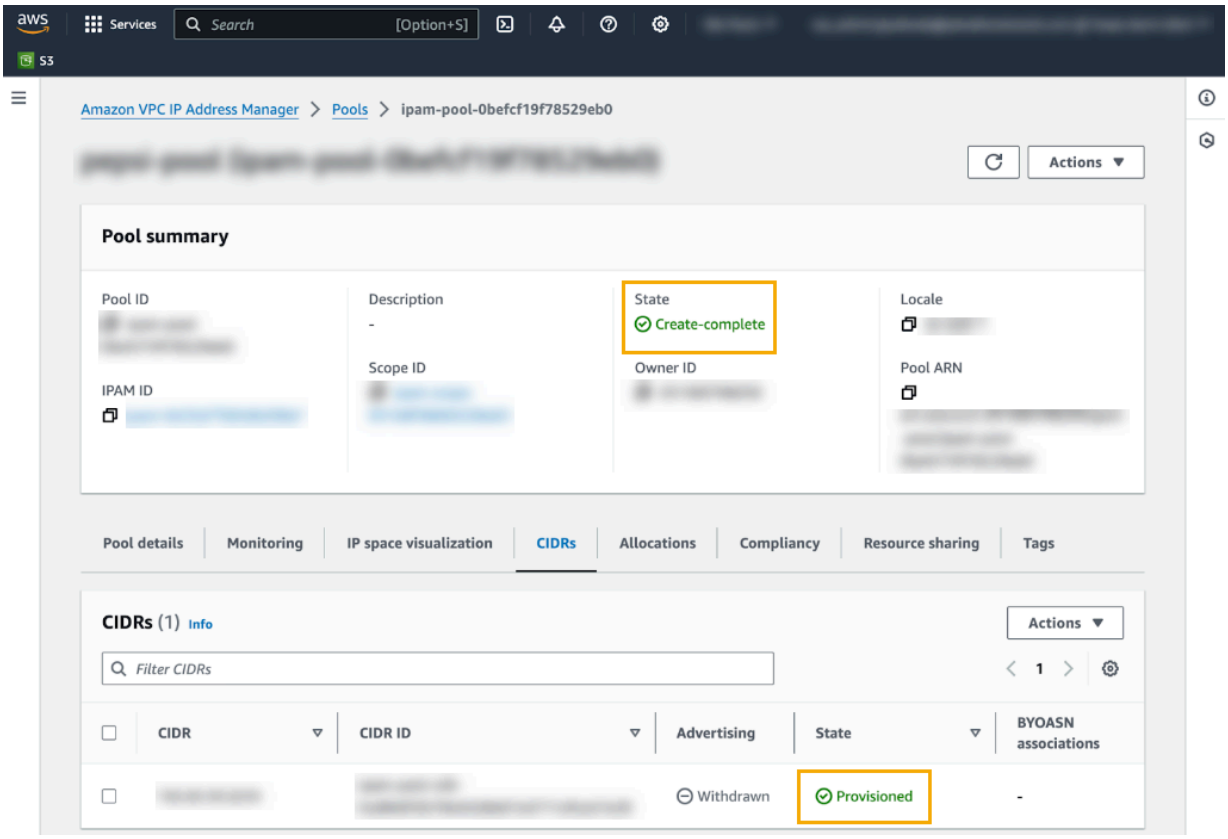
STEP 6 | 選択 アクション> **CIDR** をプロビジョニングします。このプロセスを使用して、パブリック IP CIDR 範囲と対応する証明書の秘密キーを取得します。詳細については、「プールへの CIDRS のプロビジョニング」 を参照してください。

STEP 7 | プロビジョニングする CIDR で、「**X.509** 証明書を使用して **CIDR** を入力」 をクリックします。

STEP 8 | シグネチャをコピーします。

STEP 9 | **[**プロビジョニング**]** をクリックします。

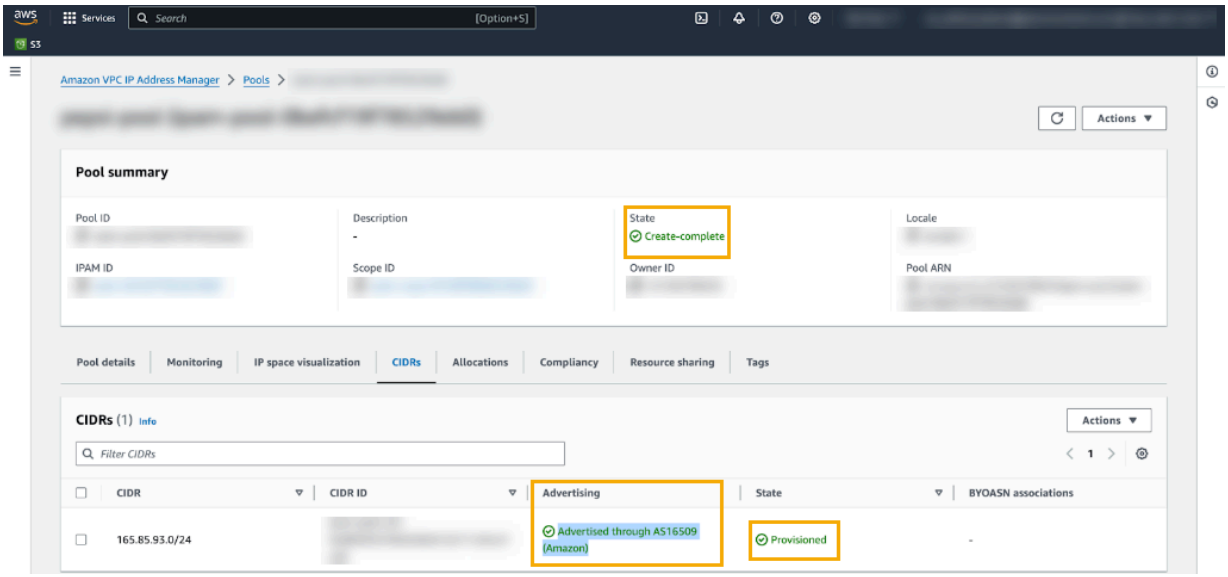
CIDR が正常にプロビジョニングされ、プールが正常に作成されたことを確認します。



STEP 10 | デフォルトでは、CIDR をプールに追加してもアドバタイズされません。それを宣伝して、インターネット上で一般公開できるようにします。CIDR をアドバタイズするには:

1. プールを選択します。
2. **CIDR** タブをクリックします。
3. **[アクション]** メニューで、**[広告]**を選択します。
4. **[CIDR** のアドバタイズ**]** メニューで、ドロップダウン メニューを使用して適切な ASN を選択し、**[CIDR** のアドバタイズ**]**をクリックします。詳細については、「CIDR のアドバタイズ」を参照してください。

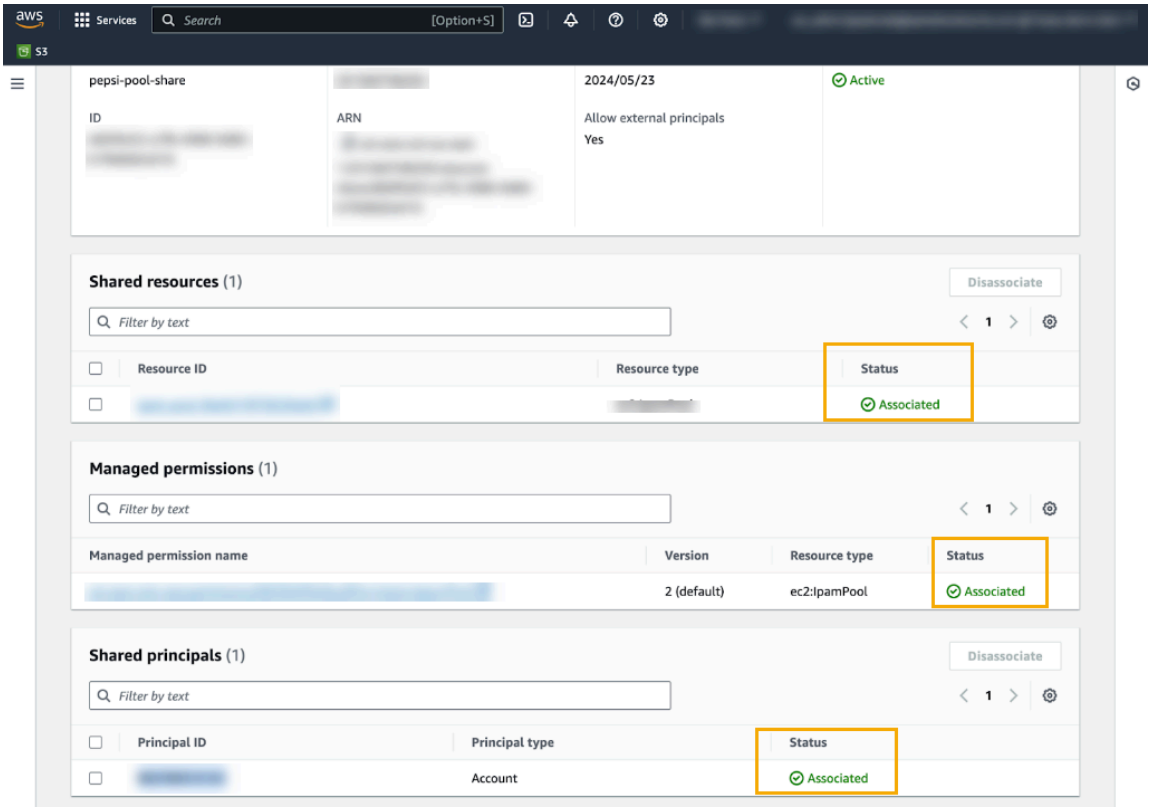
CIDR が正常にアドバタイズされたことを確認します。



STEP 11 | CIDR をアドバタイズした後、IPAM プールを Cloud NGFW デプロイメント アカウントと共有します。このために、次の作業を行います：

1. プールを選択します。
2. **[**リソース共有**]** タブをクリックします。
3. **[**リソース共有**]** メニューで、**[**リソース共有の作成**]**を選択します。
4. リソース共有名 メニューで、共有する IPAM プールの名前を入力します。
5. 必要に応じて、リソース共有名に **ARN** を追加します。
6. **Next**（次へ）をクリックします。
7. プリンシパルにアクセス権を付与します。
8. リソース共有オプションとプリンシパルを確認して、「作成」をクリックします。詳細については、「IPAM プールの共有」を参照してください。

   IPAM プールに関連付けられたリソースが正常に共有されたことを確認します。



クラウド NGFW リソースを作成し、出口 NAT を有効にして BYOIP を指定します

IPAM プールを作成する手順を完了したら、Cloud NGFW リソースを作成し、Egress NAT を有効にして、BYOIP を指定します。

BYOIP を使用して出口 NAT を構成するには:

STEP 1 | Cloud NGFW コンソールにログインします。

STEP 2 | **NGFW**をクリックします。

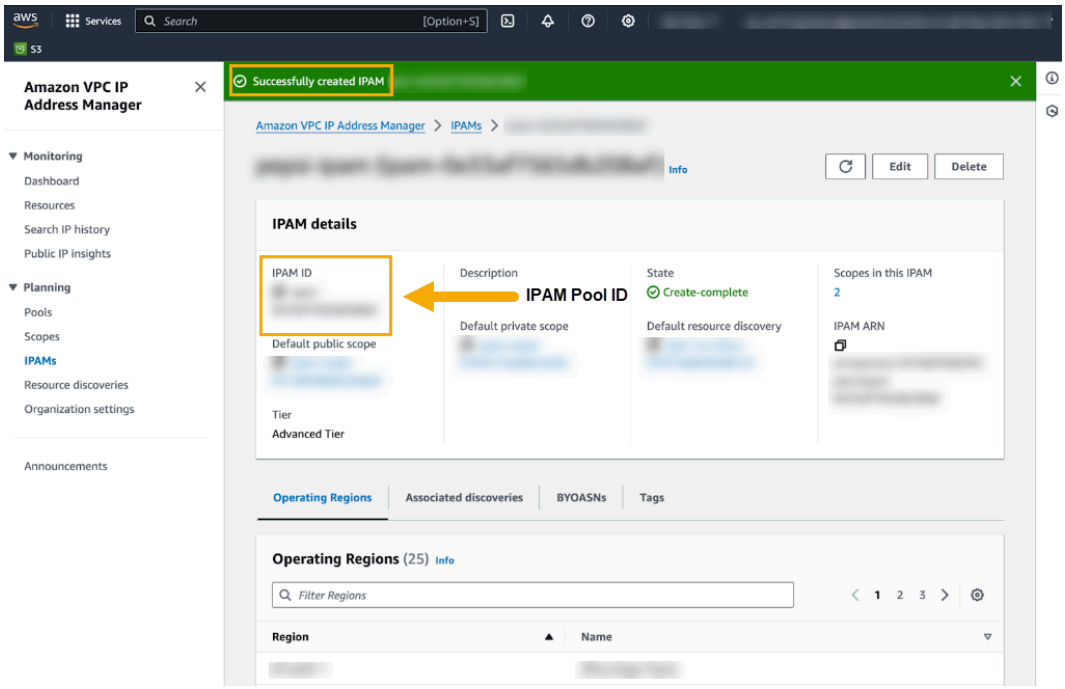
STEP 3 | 新しい NGFW リソースを作成します。

STEP 4 | ポリシー管理 セクションで、**Panorama**を選択します。ドロップダウン メニューを使用して、 統合されたPanoramaを選択します。

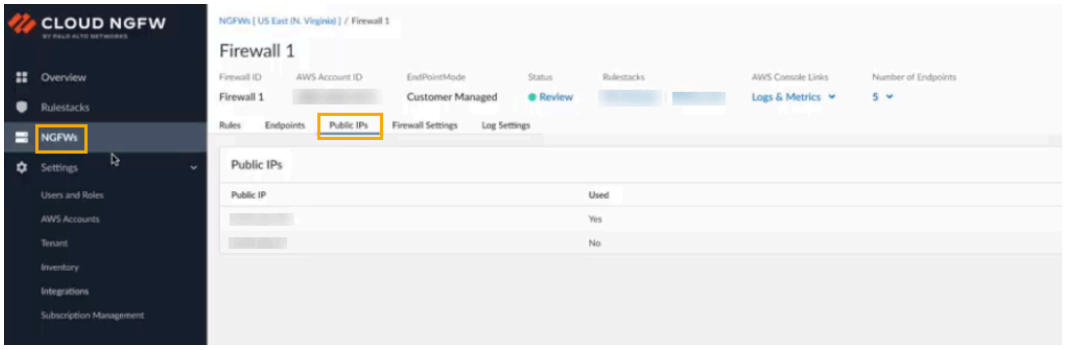
STEP 5 | **Egress NAT** セクションで、**Egress NAT** を有効にするを選択します。

STEP 6 | **[パブリック IP を使用する]** を選択し、手順 3 (上記) で作成した IPAM プール ID を入力します。

IPAM* プール *ID は、***IPAM*** プールの詳細 セクションにあります。



ファイアウォール ページで *[パブリック **IP**]* タブを選択すると、出口 *NAT* トラフィックでサポートされている *IP* アドレスのリストが表示されます。



ファイアウォールが作成されたら、そのステータスを確認します。

BYOIP を使用しない場合は、アドレスを *IPAM* プールに戻すために、*Palo Alto Networks* に連絡して サポート ケースを作成してください。

保護

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）

さまざまな種類のポリシー ルールを作成して、ネットワークを脅威や中断から保護できます。ネットワーク リソースの割り当てを最適化し、ポリシー ルールを管理してトラフィックの優先順位を付け、アプリケーションの分類を構成するのに役立ちます。

Cloud NGFW はルールを上から下へ評価し、トラフィックが定義されたルール基準に一致すると、後続のルールは評価されません。可能な限り最適な一致条件を適用するには、より一般的なポリシー ルールよりも、より具体的なポリシー ルールを優先する必要があります。ルールのログ記録が有効になっている場合、ポリシー ルールに一致するトラフィックのログが生成されます。ログ記録オプションはルールごとに設定可能です。

ベストプラクティス ポリシー ルールはほとんどのポリシー タイプで利用可能であり、迅速かつ安全に開始するのに役立ちます。これらのルールは、常に最低限のセキュリティ レベルを確保できるように編集することはできませんが、ポリシーをカスタマイズするための基盤として使用したい場合は、複製することができます。

AWS プラットフォーム向け Cloud NGFW は、規模や複雑さに関係なく、ビジネス全体を保護します。統合されたネットワーク セキュリティ アーキテクチャと、ディープラーニングをリアルタイムで活用する機能により、AWS 向け Cloud NGFW はすべてを把握し、保護するのに役立ちます。この保護は以下に適用されます。

- 支店。数千の支社のセキュリティを簡素化し、ゼロ トラスト ネットワーク セキュリティを実現します。
- キャンパス。統合された機能により、社内の資産と外部の世界が保護されるため、ユーザーはどこからでもデータやアプリケーションに接続できます。
- データセンター。クラウド環境全体にわたって詳細な可視性と一貫性のあるクラス最高のセキュリティ制御を実現します。
- パブリック クラウド。オンプレミス データ センターと同じレベルの保護で複数のパブリック クラウド環境を保護します。

- 5G セキュリティ。簡素化されたソリューションを活用して、独自のモバイル ネットワークのあらゆる側面を保護します。

AWS 向け Cloud NGFW を使用すると、インフラストラクチャを管理する必要がなくなります。この Palo Alto Networks 次世代ファイアウォールは、ルールスタック構成や自動化されたセキュリティ プロファイルにより、ストレスなく導入でき、ネットワーク セキュリティ要件を簡単に満たせるように設計されています。

CDSS（クラウド提供型セキュリティサービス）：

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のクラウド配信セキュリティ サービス (CDSS) スイートは、既知、未知、高度な回避型脅威から防御するために特別に設計された、特殊なサブスクリプションベースのセキュリティ ソリューションへのアクセスを提供します。高度な分析によって生成された脅威データは、Palo Alto Networks セキュリティ プラットフォーム全体で共有され、すべての脅威ベクトルを完全にカバーします。

CDSS を使用してトラフィックを安全に保護するために、Cloud NGFW for AWS は次のような Palo Alto Networks 保護を提供します。

- App-ID特許取得済みのレイヤー7 トラフィック分類テクノロジーに基づく App-ID サービスを使用すると、ネットワーク上のアプリケーションを確認し、その動作方法を把握し、その動作特性を観察し、相対的なリスクを理解することができます。AWS 向けクラウド NGFW は、アプリケーション シグネチャ、復号化、プロトコル デコード、ヒューリスティックなどの複数の手法を使用して、アプリケーションとアプリケーション機能を識別します。これらの機能は、ポートホッピングや暗号化を使用して正当なトラフィックを装って検出を回避しようとするアプリケーションも含め、ネットワークを通過するアプリケーションの正確な ID を特定します。
- Threat Prevention（脅威防御）。Palo Alto Networks の脅威防御サービスは、攻撃の各段階に対処するための複数の層の防止を提供することで、ネットワークを保護します。基本的な侵入防止サービス (IPS) 機能に加えて、脅威防御には、事前定義されたポートの限定されたセットに基づいてシグネチャを呼び出すだけでなく、任意のポート上の脅威を検出してブロックする独自の機能があります。
- 高度なURLフィルタリング。AWS の Cloud NGFW に組み込まれたこの重要なサービスは、業界唯一の ML を活用した高度な URL フィルタリングにより、未知の Webベースの攻撃をリアルタイムで阻止し、患者ゼロを防止します。高度な URLフィルタリングは、有名な Palo Alto Networks の悪意のある URL データベースと業界初のリアルタイム Web 保護エンジンを組み合わせ、組織が新しい悪意のある標的型 Web ベースの脅威を自動的かつ即座に検出して防止できるようにします。

- DNS。DNS セキュリティは、業界初の保護を適用して DNS を使用する攻撃を阻止し、リアルタイムの保護を提供します。Palo Alto Networks 次世代ファイアウォール (NGFW) との緊密な統合により、自動化された保護が提供され、攻撃者がセキュリティ対策を回避するのを防ぎ、独立したツールや DNS ルーティングの変更が不要になります。DNS セキュリティは、攻撃を阻止するための重要な新しい制御ポイントを組織に提供します。
- WildFire。Palo Alto Networks Advanced WildFire® は、特許取得済みの機械学習検出エンジンを使用して、ネットワーク、クラウド、エンドポイント全体で自動化された保護を可能にし、組織を非常に回避性の高い脅威から保護する、業界最大のクラウドベースのマルウェア防止エンジンです。高度な WildFire は、あらゆる未知のファイルを悪意のあるファイルとして分析し、最も近い競合製品よりも 60 倍速い記録的な速さで防御策を配布して、患者ゼロのリスクを軽減します。

AWS 高度な脅威保護のためのクラウド NGFW

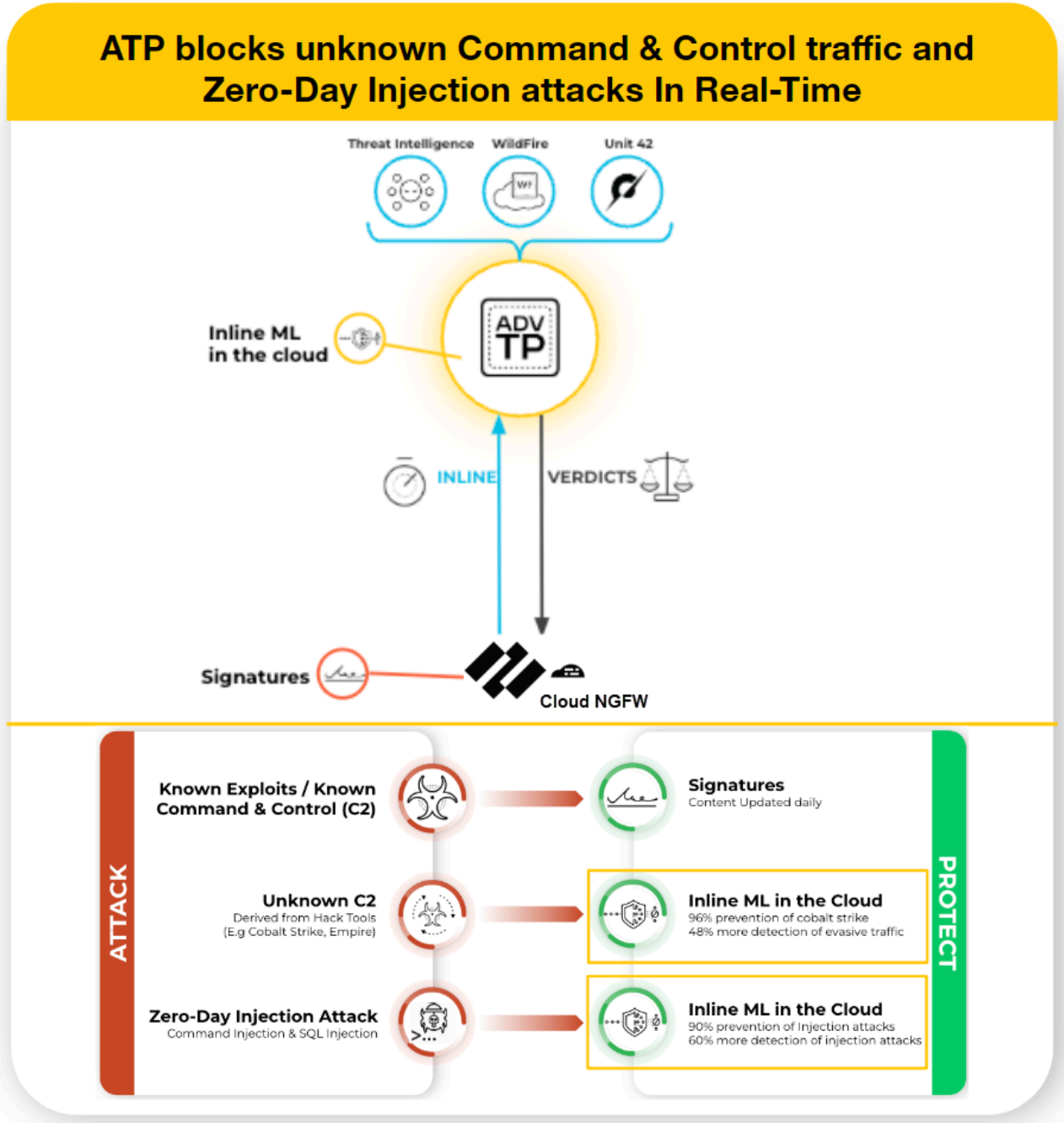
どこで使用できますか?	何が必要ですか?
• Cloud NGFW for AWS	❑ Cloud NGFWサブスクリプション ❑ Palo Alto Networksカスタマー サポート アカウント (CSP) ❑ AWS Marketplaceアカウント ❑ ユーザーのロール（テナントまたは管理者）

高度な脅威防御 (ATP) は、侵入防御システム (IPS) ソリューションで、 Cloud NGFW for AWSとクラウドで動作するコンポーネントを備えた多層防御システムを使用して、すべてのポートとプロトコルでマルウェア、脆弱性の悪用、およびコマンド アンド コントロール (C2) を検出してブロックできます。脅威防御クラウドは、Palo Alto Networksサービスからの脅威データを組み合わせて多数の検出サービスを実行し、それぞれが特定の識別可能なパターンを持つシグネチャを作成し、 Cloud NGFW for AWSによって、一致する脅威と悪意のある動作が検出されたときにセキュリティ ポリシー ルールを適用するために使用されます。これらのシグネチャは、脅威の種類に基づいて分類され、一意の識別子番号が割り当てられます。これらのシグネチャに対応する脅威を検出するために、 Cloud NGFW for AWSは、異常な特性を示すネットワーク トラフィックを検査および分類する分析エンジンを操作します。

高度な脅威防御を有効にした後は、*Panorama*を使用して、関連の高度な脅威防御ポリシーを設定します。

Advanced Threat Prevention（高度な脅威防御） クラウド のこれらのディープラーニング、MLベースの検出エンジンは、SQLインジェクションとコマンドインジェクションを利用する未知のC2 および脆弱性のトラフィックを分析し、ゼロデイ脅威からユーザーを保護します。Advanced Threat Prevention（高度な脅威防御） クラウドは、拡張可能なディープラーニング

モデルを運用し、要求ごとにCloud NGFW for AWSのインライン分析機能を有効にして、ゼロデイ脅威がネットワークに侵入するのを防具とともに、保護を分散させます。これにより、インライン検出器を使用したリアルタイムのトラフィック検査を使用して、未知の脅威を防ぐことができます。Advanced Threat Prevention（高度な脅威防御） クラウド のこれらのディープラーニング、MLベースの検出エンジンは、SQLインジェクションとコマンドインジェクションを利用する未知のC2 および脆弱性のトラフィックを分析し、ゼロデイ脅威からユーザーを保護します。脅威のコンテキストと包括的な検出の詳細を提供するために、レポートが生成されます。レポートには、攻撃者が使用したツールや手法、検出の範囲、影響のほか、MITRE ATT&CK®フレームワークで定義された対応するサイバー攻撃の分類が含まれます。



ネイティブポリシー管理

新しいローカル ルールスタックを作成すると、Advanced Threat Prevention（ATP、高度な脅威防御）が自動的に設定されます。2024年3月以前に作成したルールスタックの場合は、Cloud NGFW for AWSコンソールを使用してATPを手動で有効化します。

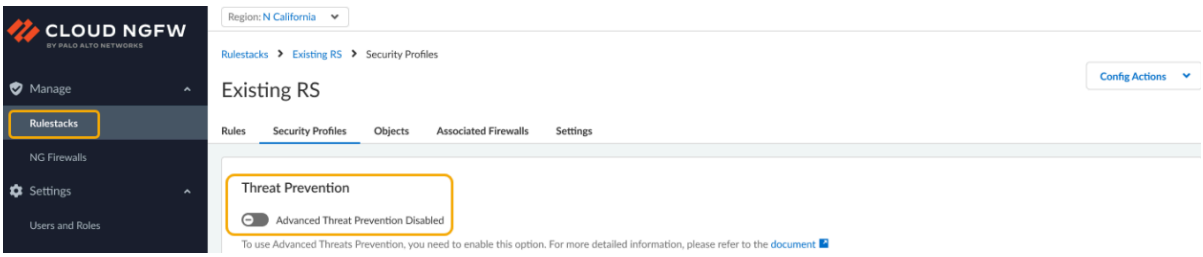
ルールスタックのATPを有効にする方法:

STEP 1 | Cloud NGFW コンソールにログインします。

STEP 2 | **[Rulestacks(ルールスタック)]**を選択します。

STEP 3 | **[Security Profiles(セキュリティ プロファイル)]**を選択します。

STEP 4 | **[Threat Prevention (脅威防御)]**セクションで、トグルを使用して**[Advanced Threat Prevention(高度な脅威防御)]**を有効にします。



STEP 5 | ATP機能によって料金が適用される場合があることを示す確認ダイアログが表示されます。**[Enable(有効にする)]**をクリックします。詳細はAWS課金サブスクリプションをご覧ください。

*Panorama*を使用して、ネットワーク セキュリティ デプロイメント内で*ATP*サブスクリプションを構成します。*ATP*を構成するすべてのプロセスを実装する必要はありませんが、デプロイメントを成功させるために、すべてのタスクを見直して利用可能なオプションに慣れることをお勧めします。

パノラマポリシー管理

高度な脅威防御（他のPalo Alto Networksのセキュリティ サービスと同様）は、セキュリティ プロファイルを通じて管理されます。セキュリティ プロファイルは、セキュリティ ポリシー ルールを通じて定義されたネットワーク適用ポリシーの構成に依存します。

*Cloud NGFW for AWS*を使用してルールスタックの高度な脅威防御を有効にしますが、セキュリティ サービスを構成するポリシーの設定には*Panorama*を使用する必要があります。

Panoramaを使用して高度なURLフィルタリング ポリシー ルールを設定するには、次の手順を実行します。

STEP 1 | Panorama にログインします。

STEP 2 | 高度なURLフィルタリングの適切なライセンス サブスクリプションがあることを確認します。Panoramaで、**[Device (デバイス)]>[Licenses (ライセンス)]**を選択します。ライセンスの有効期限が未来の日付であることを確認します。

STEP 3 | Panoramaを使用してAdvance Threat Prevention (高度な脅威防御)をセットアップします。

STEP 4 | 変更をコミットします。

*Palo Alto Networks*では、高度な脅威防御セキュリティサービスで処理されたアクティビティを監視するいくつかのオプションを提供しています。詳細については、「高度な脅威防御の監視」を参照してください。

AWSのクラウドNGFW高度なURLフィルタリング

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 は、事前定義された URL フィルタリングカテゴリのセットを提供します。顧客 URL カテゴリオブジェクトを使用して、独自の URL フィルタリングカテゴリを指定することもできます。たとえば、セキュリティポリシールールの一致基準として使用する URL のカスタムリストを作成します。これは、特定の URL をそれが属す URL カテゴリとは別に適用したい場合に、URL カテゴリに対する例外を指定する際に良い方法になります。

カスタムURLカテゴリの作成

STEP 1 | ［ルールスタック**]**を選択し、カスタム URL カテゴリを設定する、以前に作成したルールスタックを選択します。

STEP 2 | ［オブジェクト］ > ［カスタム **URL** カテゴリ］ > カスタム **URL** カテゴリを作成］を選択します。

STEP 3 | カスタム URL カテゴリのわかりやすい名前を入力します。

STEP 4 | （任意）カスタム URL カテゴリの説明を入力します。

STEP 5 | 1 行に 1 つずつ、複数の **URL** リストを入力します。

STEP 6 | **[Save(保存)]**をクリックします。

URL カテゴリ例外リストの基本的なガイドライン

- 関連する URL カテゴリとは別に実行する Web サイトの URL を入力します。
- リストのエントリは、完全一致である必要があり、大文字と小文字は区別されません。
- アクセスを制御するウェブサイト (場合によっては特定のサブドメイン) と完全に一致する文字列を入力するか、ワイルドカード文字を使用して複数の Web サイトのサブ ドメインに一致するエントリを入力します。ワイルドカード文字の使用の詳細については、を確認してください。
- URL エントリから `http` と `https` を省略します。
- 各 URL エントリの長さは最大255文字です。

URL カテゴリ例外リストのワイルドカードのガイドライン

URL カテゴリの例外リストでワイルドカードを使用すると、複数の Web サイトのサブドメインやページに一致するように 1 つのエントリを簡単に構成できます。

ワイルドカード エントリを作成するときは、次のガイドラインに従ってください：

- 以下の文字はトークン区切り文字とみなされます： . / ? & = ; +

  これらの文字の 1 つまたは 2 つで区切られたすべての文字列はトークンです。ワイルドカード文字をトークン プレースホルダとして使用すると、特定のトークンに任意の値を含めることができます。
- トークンの代わりに、アスタリスク（*）またはキャレット（^）を使用してワイルドカード値を示すことができます。
- ワイルドカード文字はトークン内の唯一の文字でなければなりません。たとえば、www.gmail*.com は、アスタリスクが他の文字の後に続くため無効になります。ただし、エントリには複数のワイルドカードを含めることができます。

アスタリスク（*）およびキャレット（^）ワイルドカードの使用方法

*	1 つ以上の変数サブドメインを示すために使用します。* を使用する場合、エントリは URL の先頭または末尾にかかわらず、追加のサブドメインと一致します。 例: • ***.paloaltonetworks.com** は、www.paloaltonetworks.com および www.paloaltonetworks.com.uk と一致します。 • ***.paloaltonetworks.com/** はwww.paloaltonetworks.com と一致します

	が、www.paloaltonetworks.com.uk とは一致しません。
^	1 つの変数サブドメインを示すために使用します。 例: **mail.^.com** は mail.company.com に一致しますが、mail.company.sso.com には一致しません。

連続するアスタリスク（*）ワイルドカードまたは *9* つ以上の連続したキャレット（^）ワイルドカードを含むエントリを作成しないでください。これらのエントリは、ファイアウォールのパフォーマンスに影響を与える可能性があります。

たとえば、***mail.*.*.com*** のようなエントリは追加せずに、アクセスを制御したい *Web* サイトの範囲に応じて、***mail.*.com*** または ***mail.^.^.com*** を入力します。***mail.*.com*** のようなエントリは、***mail.^.^.com*** よりも多くのサイトで一致します。***mail.*.com*** は、サブドメインを含むすべてのサイトに一致し、***mail.^.^.com*** は *2* つのサブドメインに正確に一致します。

URL カテゴリ例外リスト **-** ワイルドカードの例

次の表に、ワイルドカードを使用した URL リスト エントリの例と、これらのエントリに一致するサイトを示します。

URL 例外リストのエントリ	サイト一致
セット **1** の例	
*.company.com	eng.tools.company.com support.tools.company.com tools.company.com docs.company.com
^.company.com	tools.company.com docs.company.com
^.^.company.com	eng.tools.company.com support.tools.company.com

URL 例外リストのエントリ	サイト一致
セット2 の例	
mail.google.*	mail.google.com mail.google.co.uk mail.google.example.org
mail.google.^	mail.google.com mail.google.info
mail.google.^.^	mail.google.co.uk mail.google.example.info
セット3の例	
site.*.com	site.yourname.com site.abc.xyz.com
site.^.com	site.company.com site.example.com
site.^.^.com	site.a.b.com
site.com/*	site.com/photos site.com/blog/latest 任意の site.com サブディレクトリ

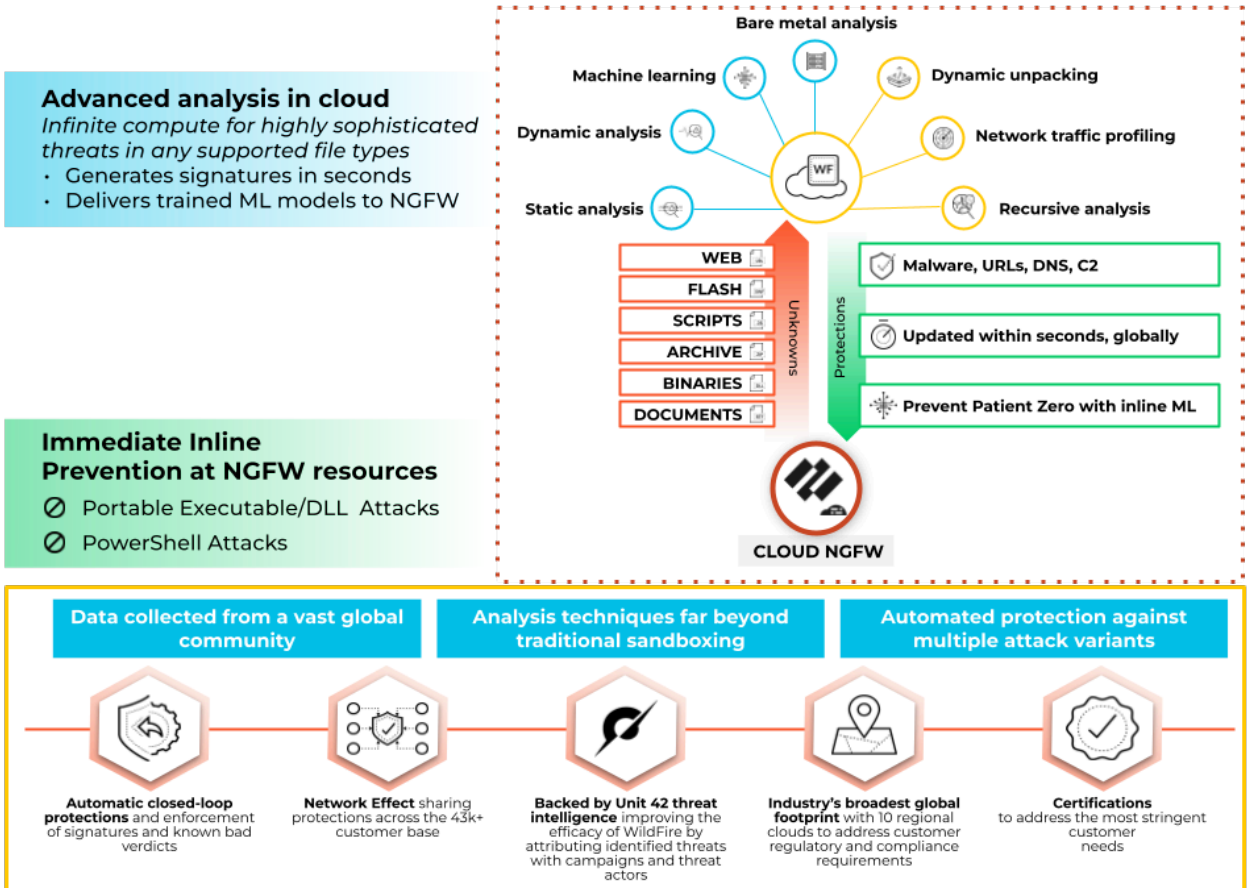
AWS WildFire Protection 上のCloud NGFW

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は、VPCトラフィック内のファイル、実行ファイル、および悪意のあるスクリプト (JScript や PowerShell など) を検出して WildFire™ クラウドサービスに転送して解析できるようになりました。次に、Wildfireは、転送されたファイル（実行可能ファイルまたはスクリプト）に脅威インテリジェンス、解析、および相関関係を適用し、分析に基づいて判断を下します。脅威が検出された場合、WildFireはマルウェアをブロックする保護機能を作成し、数分でその脅威に対する保護をグローバルに配布します。

WildFireは従来のサンドボックス型のアプローチにとどまらず、複数の手法を使用して悪意のある動作を起こす可能性があるファイルを特定します。これらの手法には以下が含まれます。

- 動的解析-回避に強い専用の仮想環境でファイルが実行されている様を観察し、何百もの動作特性を使用してこれまで知られていなかったマルウェアを検出できるようにします。
- 静的解析-マルウェアの効果的な検出によって動的解析を補完し、マルウェアの亜種をすばやく特定できます。静的解析では、動的な開梱をさらに活用して、パッキングツールセットを使用して検出を回避しようとする脅威を分析します。
- ネットワークトラフィックプロファイル-バックドアの作成、次段階のマルウェアのダウンロード、レピュテーションの低いドメインへのアクセス、ネットワークの偵察など、マルウェアの亜種に基づいて悪意のあるトラフィックパターンを検出します。
- 機械学習-各ファイルから何千もの固有の特徴を抽出し、予測機械学習モデルをトレーニングして新しいマルウェアを識別します。これは、静的解析や動的解析だけでは不可能です。
- カスタムビルドのハイパーバイザ-攻撃者がアクセスできるオープン ソース プロジェクトや独自のソフトウェアに依存しない堅牢な独自のハイパーバイザにより、攻撃者の回避手法を防ぎます。



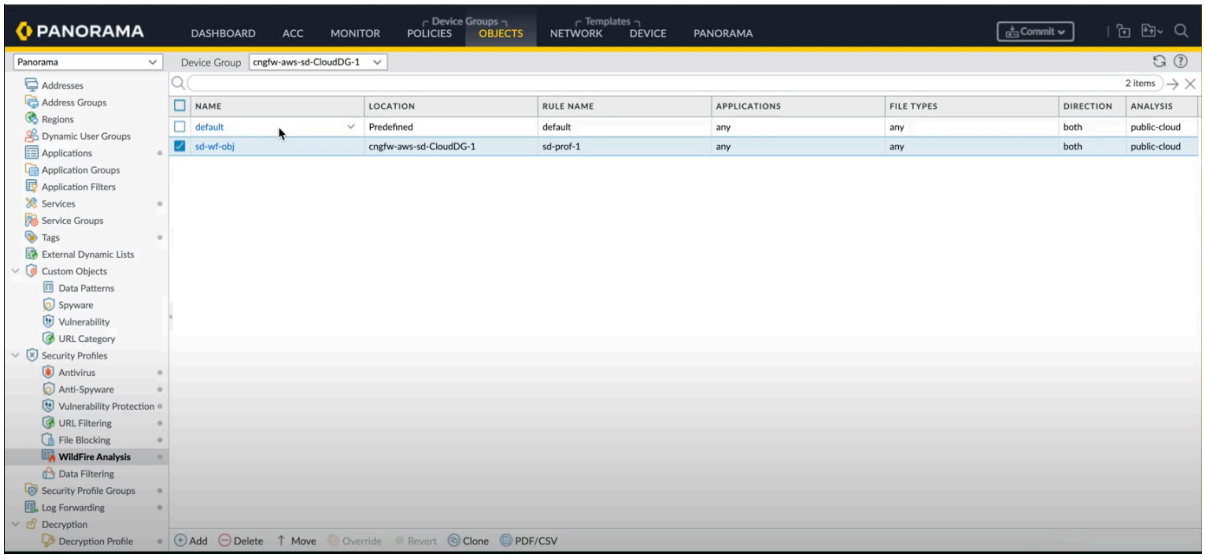
Cloud NGFW AWSリソースでWildfireを設定するには、以下を行う必要があります。

- Wildfireプロファイルを設定する
- Panoramaで作成したクラウド デバイス グループでセキュリティルールを定義する
- WildFire送信ログを表示する

Wildfireプロファイルを設定する

STEP 1 | **Panorama**にログインし、**[Object(オブジェクト)] > [WildFire Analysis(WildFire解析)]**をクリックします。[WildFire分析プロファイル]ウィンドウが表示されます。

STEP 2 | プロファイルを作成するデバイス グループをドロップダウン メニューから選択します。



STEP 3 | **[追加]** をクリックします。

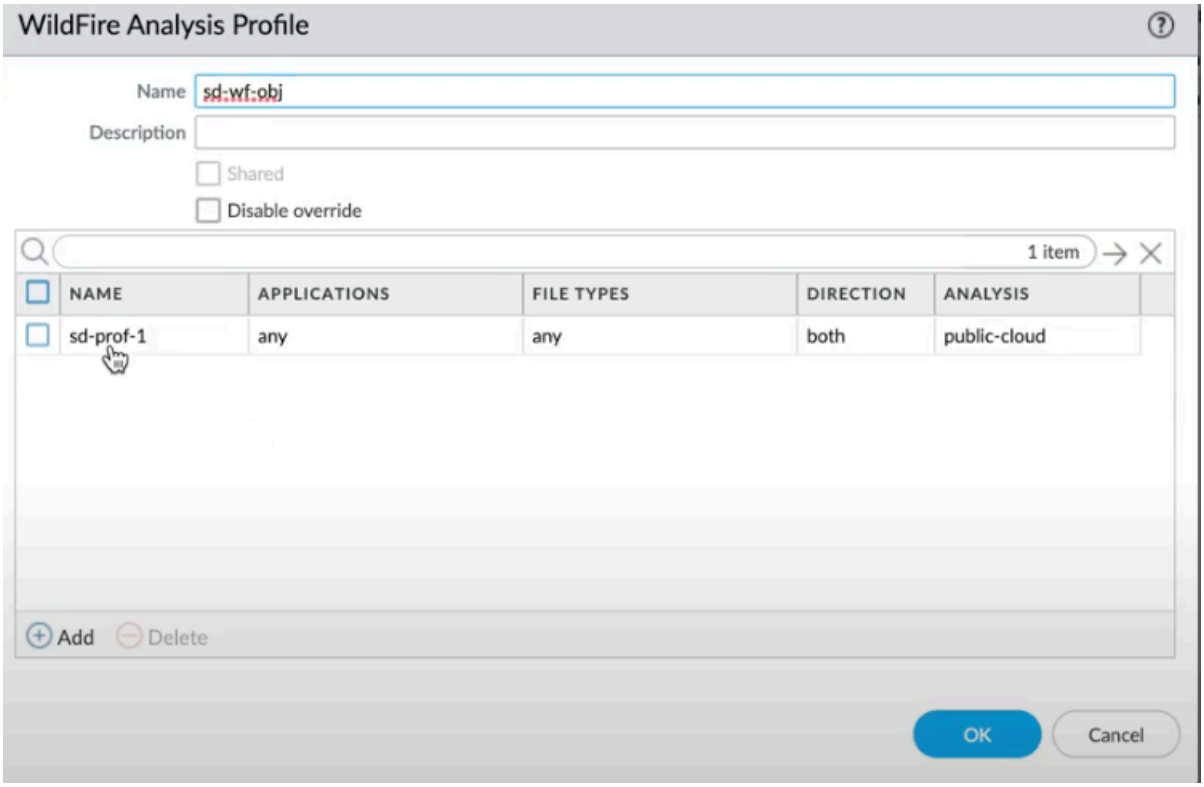
STEP 4 | WildFireプロファイルの名前を入力し、**[Add(追加)]**をクリックします。

STEP 5 | プロファイルに追加するルールの分かりやすい名前を入力します

STEP 6 | アプリケーションセクションで、**[Add(追加)]**をクリックして、Wildfireプロファイルからのアクセスを許可するアプリケーションのリストからアプリケーションを選択します。

STEP 7 | **[FileTypes]**をクリックして、許可するファイルタイプを選択します。

STEP 8 | ダウンロード/アップロード、または両方のオプションを許可するには、**[Direction(指示)]**をクリックします。



STEP 9 | トラフィックを転送して分析する **Destination**[宛先] を選択します。ルールに一致するすべてのトラフィックを分析のために WildFireパブリック クラウドに転送する場合は、 パブリック クラウド を選択します。

STEP 10 | ルールに一致するすべてのトラフィックをWildFireアプライアンスに転送して解析する場合は、**[private-cloud(プライベートクラウド)]**を選択します。

STEP 11 | **OK** をクリックします。

セキュリティルールの定義

STEP 1 | Panoramaにログインし、**[Policies(ポリシー)]**をクリックします。

STEP 2 | 必要なデバイス グループを選択し、事前設定済みのセキュリティ ルール ([Pre Rule(プレルール)] または [Post Rule(ポストルール)]) をクリックするか、新しいルールを作成します。

STEP 3 | **[Actions(アクション)]**をクリックします。

STEP 4 | プロファイル設定で、プロファイルタイプの下の **[**プロファイル**]**を選択します。

STEP 5 | **[WildFire Analysis(WildFire解析)]**ドロップダウンで、選択したいWildFireプロファイルを選択します。

STEP 6 | **OK** をクリックします。

デバイス グループをコミットしてCloud NGFW リソースにプッシュします。

詳細については、「WildFireクラウドの最新機能」を参照してください。

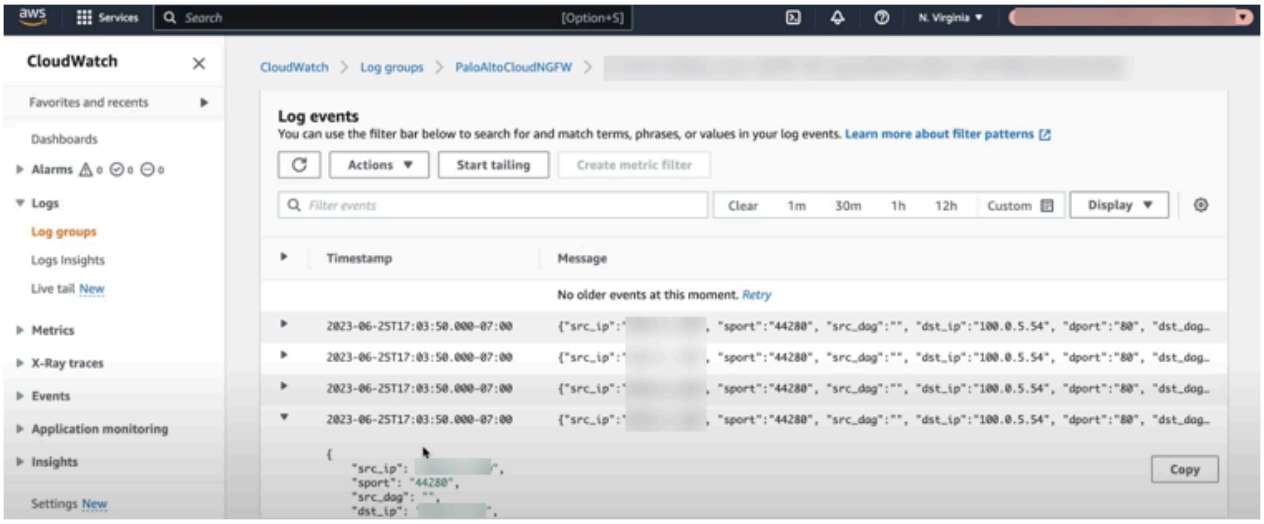
WildFire送信ログを表示する

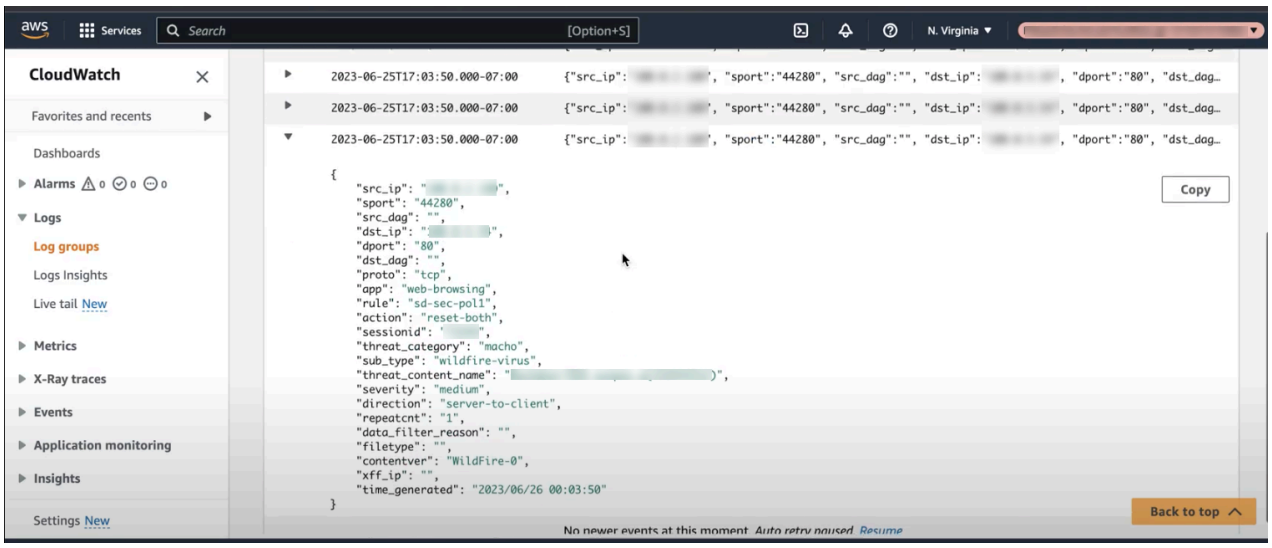
WildFire送信ログは次の場所で確認できます。

1. AWSログの宛先
2. Panorama
3. Strata Logging Service

AWSの宛先ログを表示する

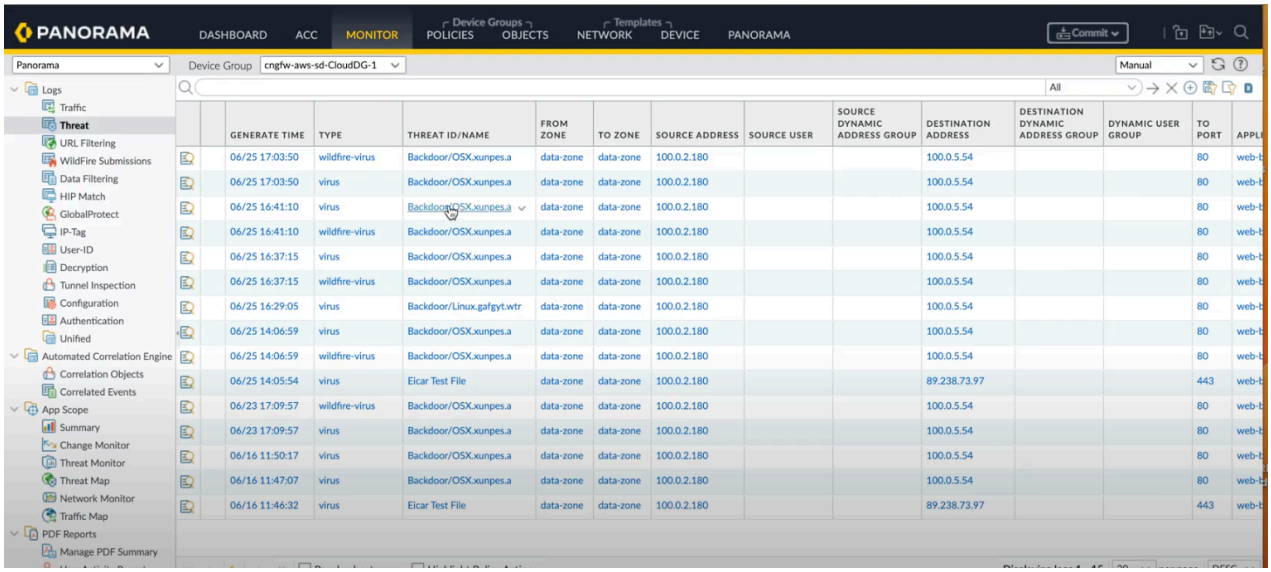
以前に Amazon Cloudwatch、Amazon S3、または Amazon Kinesis をログの保存先として設定している場合は、WildFire によって悪意のあるトラフィックがブロックされているかどうかを確認できます。





Panoramaでログを表示する

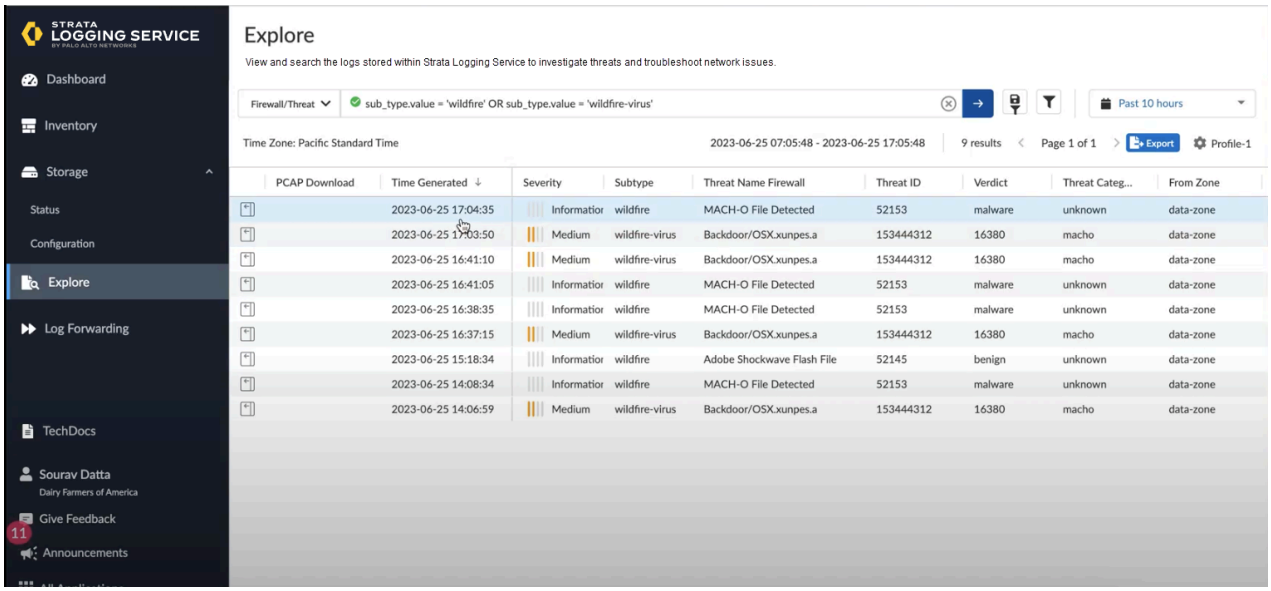
Panoramaでは、**[Monitor(監視)] > [Threats(脅威)]**を使用してデバイス ログのログを表示できます。



Strata Logging Serviceでログを表示する

Strata Logging ServiceインスタンスのWildFireログを表示することもできます。

1. **[Explore(探索)]**をクリックし、[Explore(探索)]ドロップダウンから**[Firewall(ファイアウォール)/Threat(脅威)]**を選択します。
2. `sub_typevalue =wildfire`または`wildfire-virus`と入力し、WildFireログをフィルタリングします。



AWS DNS セキュリティのためのクラウド NGFW

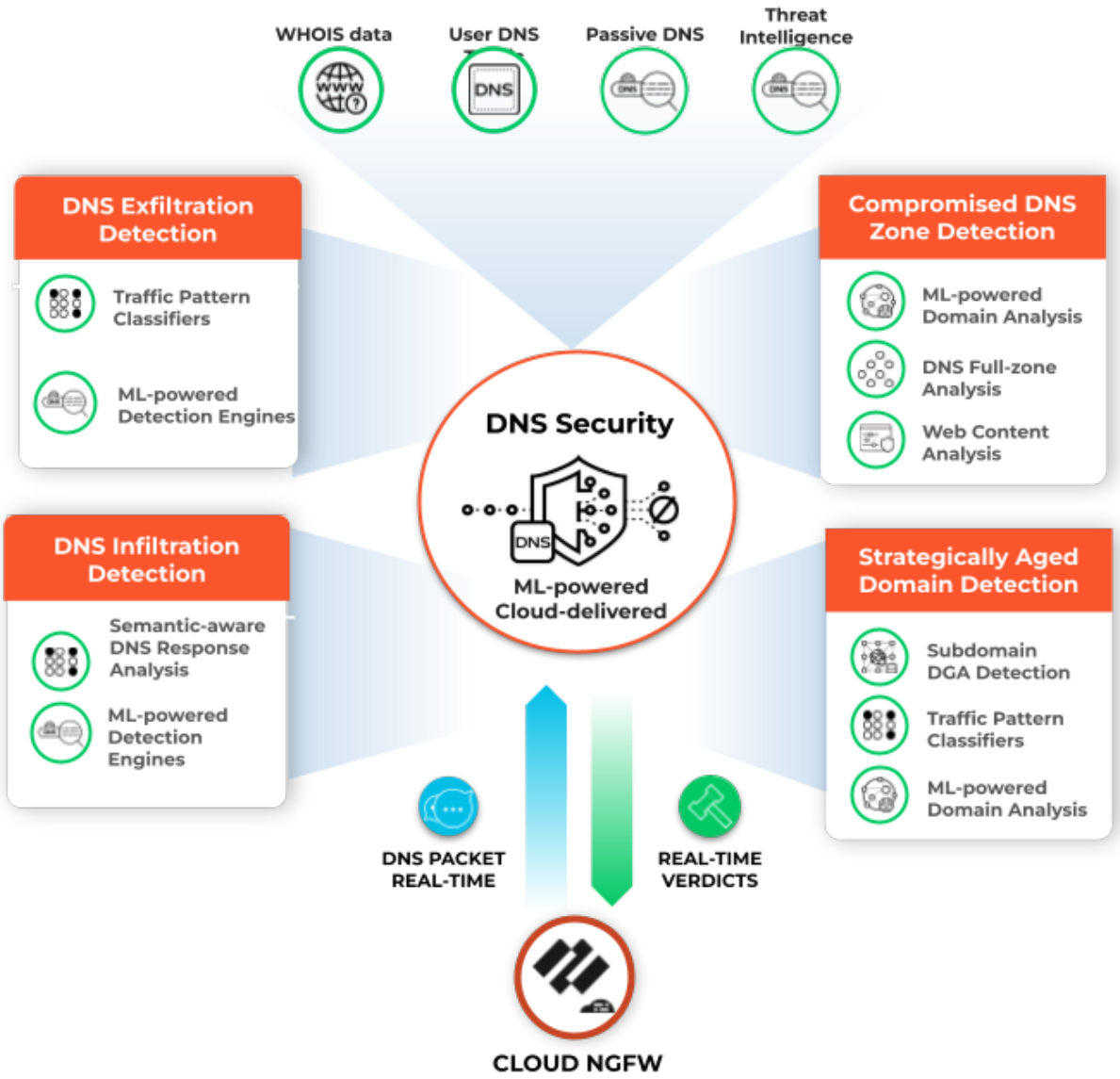
どこで使用できますか?	何が必要ですか?
• Cloud NGFW for AWS	❑ Cloud NGFWサブスクリプション ❑ Palo Alto Networksカスタマー サポート アカウント (CSP) ❑ AWS Marketplaceアカウント ❑ ユーザーのロール（テナントまたは管理者）

Domain Name Service（DNS； ドメイン ネーム サービス）は、プロトコルのコアRFC で説明されているように、インターネットの重要かつ基本的なプロトコルです。悪意のあるアクターは、DNSを介したコマンドアンドコントロール（C2）通信チャネルを利用し、場合によってはこのプロトコルを使用してデータを盗み出したこともあります。DNS流出は、悪意のあるアクターがVPC内のアプリケーションインスタンスを侵害した後に、DNS検索を使用してVPCから自身が管理するドメインにデータを送信することで発生する可能性があります。悪意のあるアクターは、DNSを介して悪意のあるデータやペイロードをVPCワークロードに侵入させることもできます。Palo Alto Networks Unit 42の調査では、発見されたさまざまなDNS不正利用について説明されています。

Cloud NGFW for AWSでは、VPCリソースが照会するドメインを監視および制御することで、DNSベースの高度な脅威からVPCトラフィックを保護できます。Cloud NGFW for AWSを利用する。Palo Alto Networksは不正または疑わしいと判断したドメインへのアクセスを拒否し、他のすべてのクエリを許可することができます。

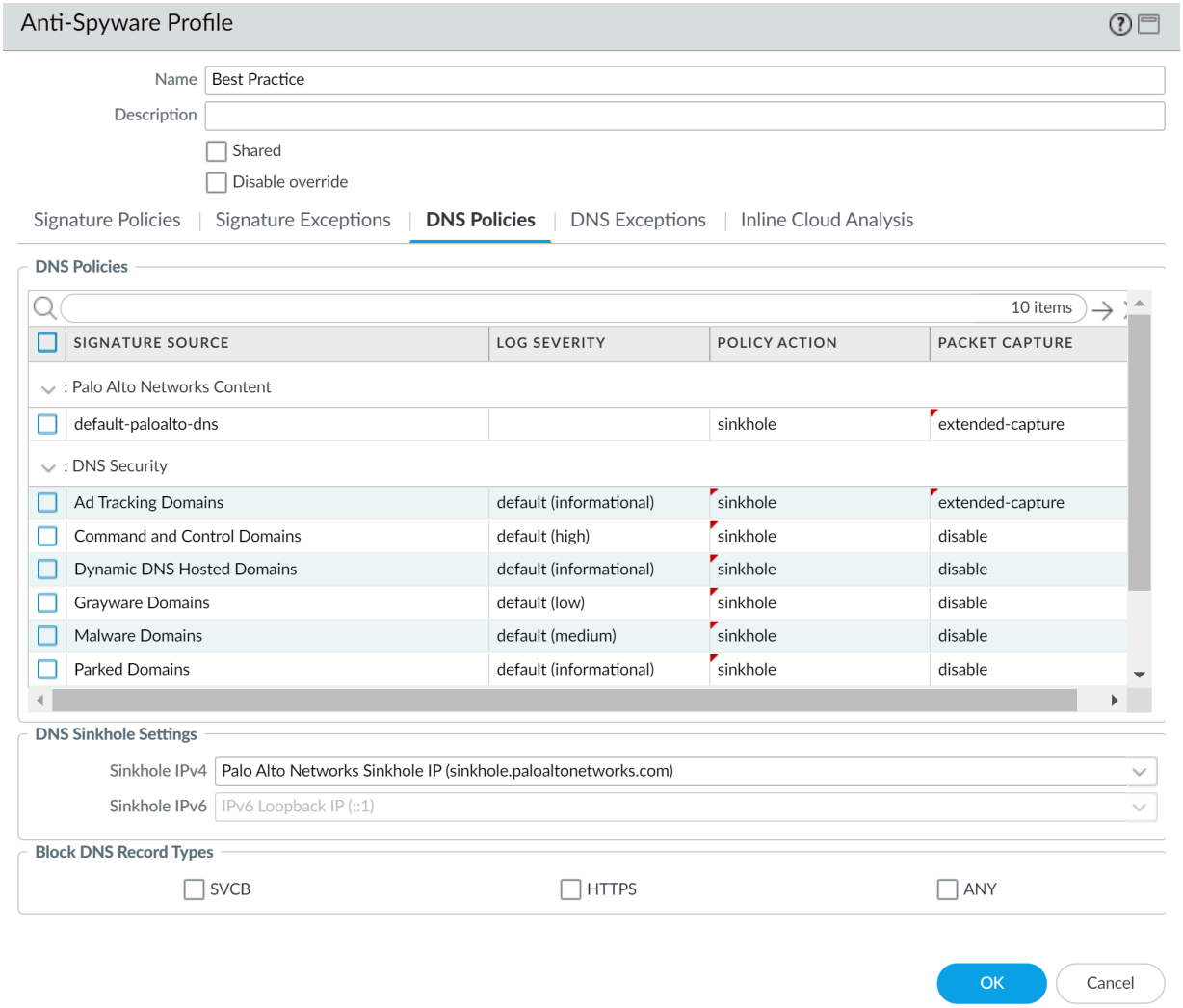
Cloud NGFWは、複数のソース（WildFireトラフィック分析、パッシブDNS、アクティブWebクロール＆悪意のあるWebコンテンツ分析、URLサンドボックス分析、Honeynet、DGAリバースエンジニアリング、テレメトリデータ、whois、Unit 42の研究組織、サイバー脅威アライアンス）のデータを使用して、高度な予測分析と機械学習を使用してDNSシグネチャを生成することで、悪意のあるドメインをプロアクティブに検出するPalo Alto Networks DNSセキュリティサービスを使用しています。その後、DNSセキュリティサービスは、これらのDNSシグネチャをCloud NGFWリソースに継続的に分配し、コマンドアンドコントロール（C2）とデータ盗難にDNSを使用するマルウェアからプロアクティブに防御します。

DNS Security for Cloud NGFWにはPanoramaが必要です。Panorama上ですべてのDNSセキュリティ関連のポリシー ルールを構成し、クラウド デバイス グループの一部としてCloud NGFWリソースにプッシュします。



Cloud NGFWリソースでDNSセキュリティを有効にするには—

STEP 1 | Cloud NGFWリソースに関連付けられたクラウド デバイス グループにアンチスパイウェア プロファイルを作成して、PanoramaでDNSセキュリティを有効にします。



STEP 2 | VPC内のDNSトラフィックをCloud NGFWリソースにリダイレクトします。トラフィック リダイレクションの設定方法は、DNSサーバのセットアップによって異なります。

- プライベート DNS サーバー
- Route 53 DNSサービス
- プライベートホストゾーンDNS

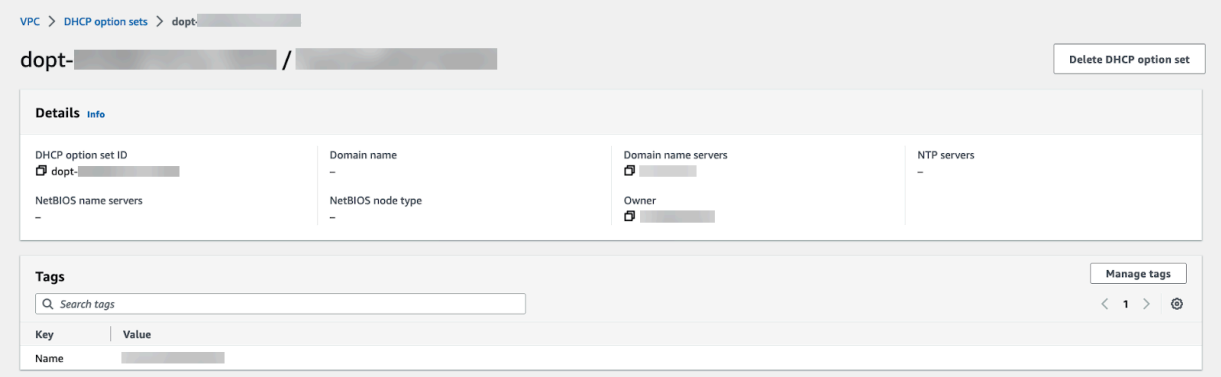
プライベート DNS サーバー

プライベートまたはオンプレミスのDNSサーバーを使用する場合、DNSトラフィックをCloud NGFWエンドポイントに転送するには、以下の手順を実行します。

STEP 1 | AWS コンソールにログインします。

STEP 2 | VPCを選択し、次に**DHCP**オプション セットを選択します。

STEP 3 | 新しいDHCPオプション セットを作成し、DNSサーバーのIPアドレスを追加できます。この例では、172.18.10.1がプライベートDNSサーバーのアドレスです。DNSサーバーが設定されている既存のDHCPオプションがある場合は、詳細を表示し、DNSサーバーのIPアドレスをメモします。



STEP 4 | **VPC**を選択し、保護するVPCを選択します。

STEP 5 | **[Actions(アクション)]**ドロップダウンから**[Edit VPC settings(VPC設定の編集)]**を選択します。

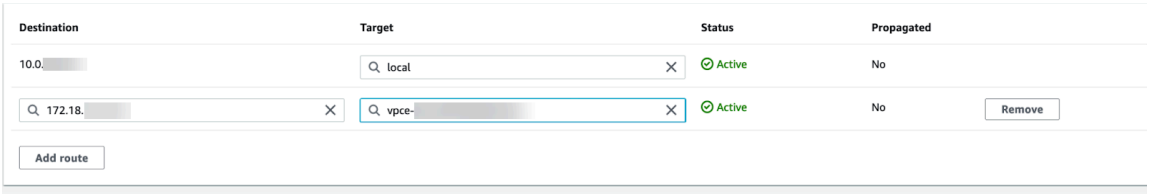
STEP 6 | **[DHCP settings(DHCP設定)]**で、**[DHCP option set(DHCPオプション セット)]**]ドロップダウンからプライベートDNSサーバーが設定されたDHCPオプション セットを選択します。

STEP 7 | **Save changes**（変更内容の保存）をクリックします。

選択したVPCは、すべてのDNSクエリを設定されたDNSサーバーに送信するようになりました。

STEP 8 | サブネット ルート テーブルを編集します。

1. **VPC** > **Route Tables**（ルートテーブル）を選択します。
2. セキュリティ保護するサブネットのルート テーブルを選択します。
3. ルートを追加し、接続先をDNSサーバのIPアドレスに設定します。



4. **[Save changes**（変更内容の保存）**]**をクリックします。

   保護されたサブネットからの DNSトラフィックはすべて、検査と適用のためにCloud NGFWエンドポイントを経由してCloud NGFWにルーティングされます。

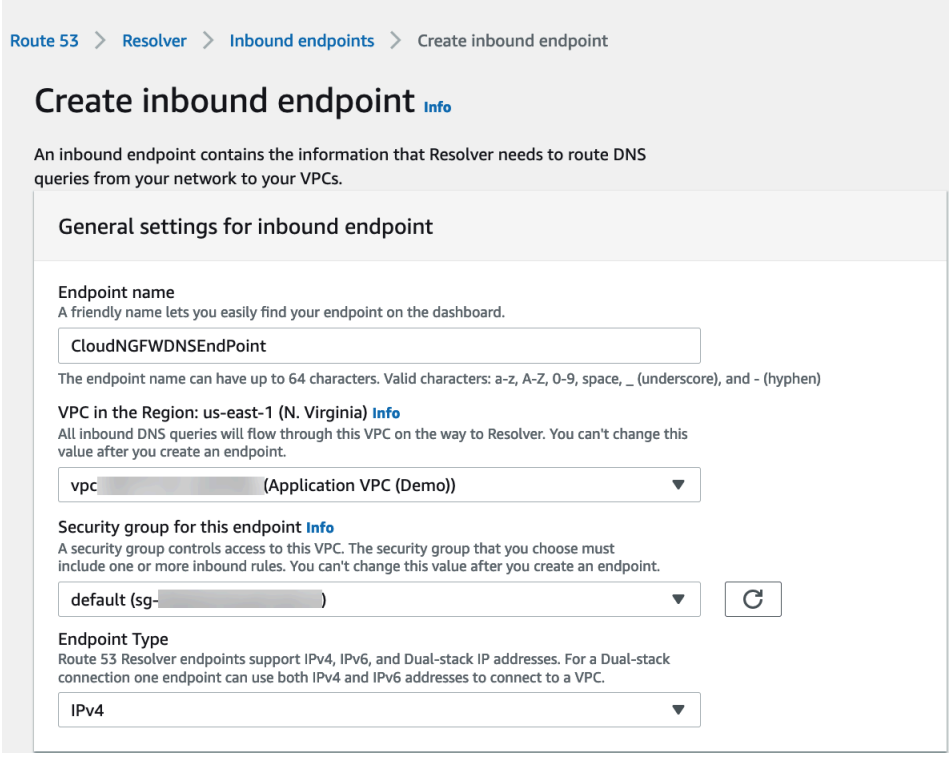
Route 53 DNSサービス

AmazonのRoute 53 DNSサービスを使用する場合、VPC内のDNSトラフィックを保護するには、以下の手順を実行します。リゾルバーの受信エンドポイントをデプロイするためのワークロードを含む各可用性ゾーンにサブネットを作成します 。

STEP 1 | AWS コンソールにログインします。

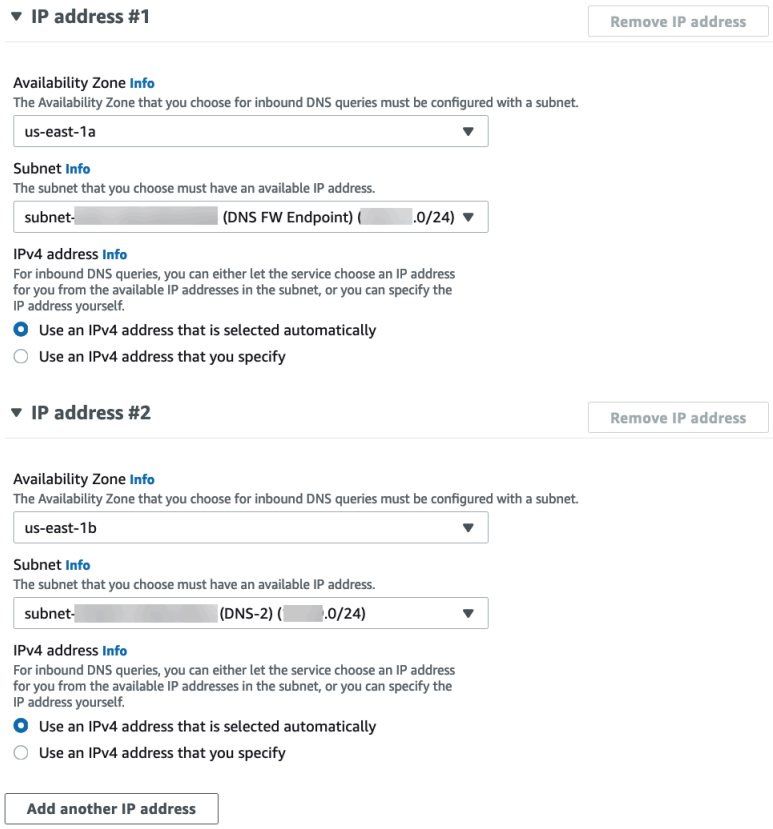
STEP 2 | 受信エンドポイントを作成します。

1. **[Services(サービス)]** > > **[Route 53** > **Resolver]** > > **[Inbound Endpoints(**インバウンド エンドポイント**)]**を選択します。
2. **[Create inbound endpoint(**受信エンドポイントの作成**)]** をクリックします。
3. 分かりやすい **Name**（名前）を入力します。
4. エンドポイントのVPCを選択します。
5. このエンドポイントにセキュリティ グループをアタッチします。
6. エンドポイント タイプをIPv4に設定します。



7. 可用性ゾーンを選択します。
8. 上記で作成したサブネットを選択します。

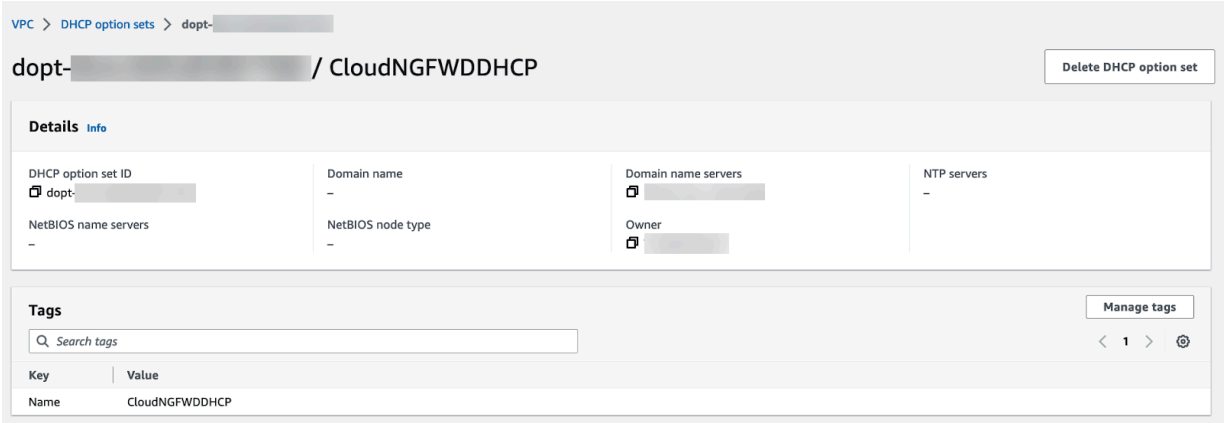
複数の可用性ゾーンがある場合は、それぞれの可用性ゾーンとサブネットを指定する必要があります。



9. **[Create inbound endpoint(受信エンドポイントの作成)]** をクリックします。
10. 受信エンドポイントに接続されている各サブネットに関連付けられているIPアドレスをメモします。以下の手順で**DHCP** オプション セットを構成するときに、これらのIPアドレスを使用します。

STEP 3 | **VPC** > **DHCP** オプション セットを選択します。

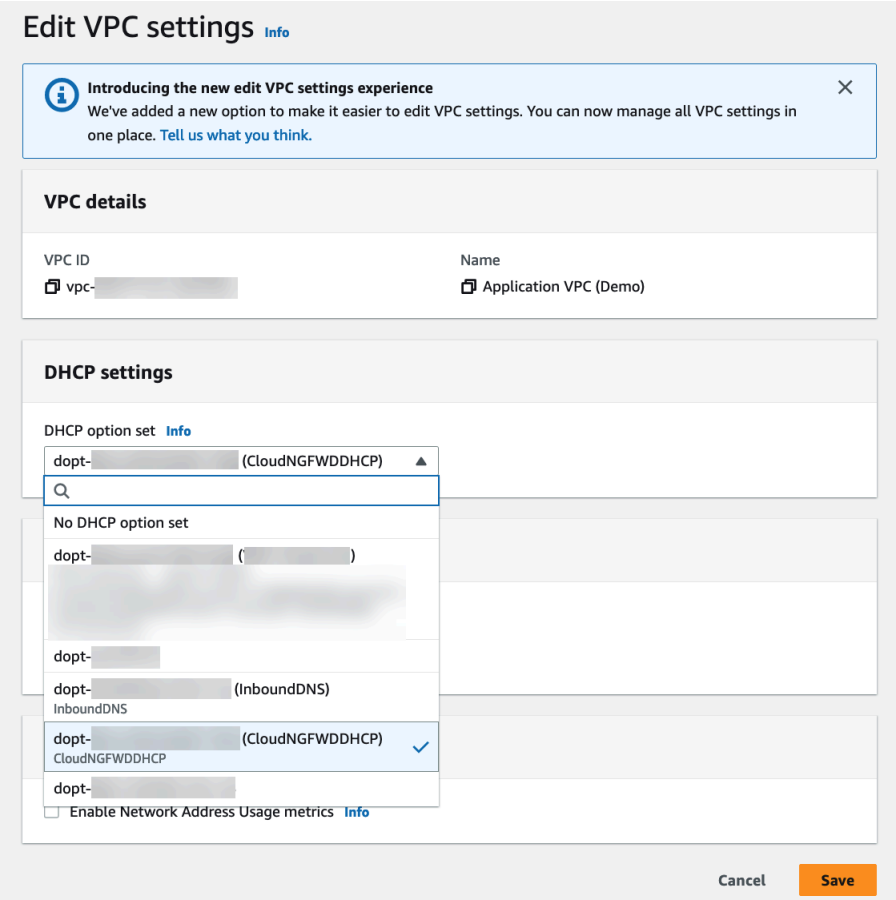
STEP 4 | 新しいDHCPオプション セットを作成し、各可用性ゾーンのIPアドレスを追加できます。複数の可用性ゾーンがある場合は、各IPアドレスをコンマ区切りのリストとして入力します。



STEP 5 | **VPC** を選択し、保護する VPC を選択します。

STEP 6 | **[Actions(アクション)]** ドロップダウンから、**[Edit VPC settings(VPC** 設定の編集**)]**を選択します。

STEP 7 | **[DHCP settings(DHCP** 設定**)]**で、**DHCP** オプション セット ドロップダウンから上記で作成したDHCPオプション セットを選択します。

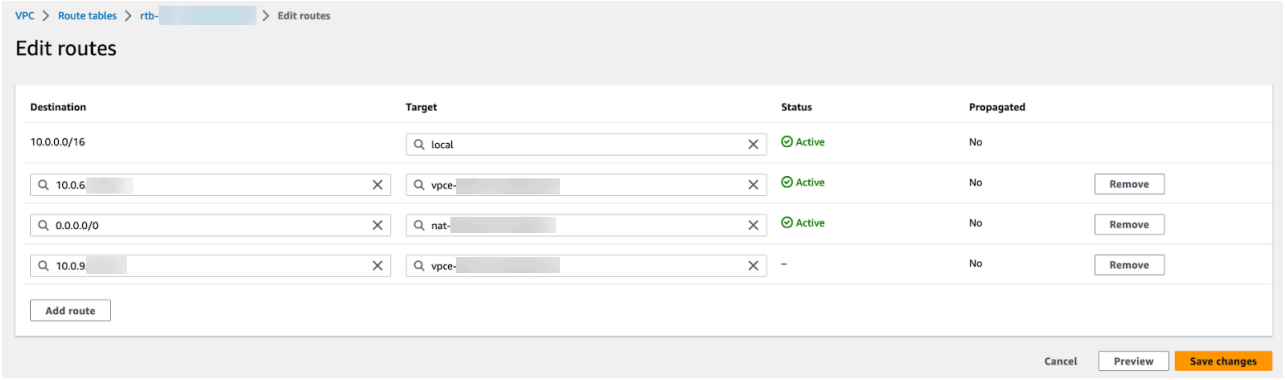


STEP 8 | **Save changes**（変更内容の保存）をクリックします。

選択したVPCは、すべてのDNSクエリを設定されたDNSサーバーに送信するようになりました。

STEP 9 | サブネット ルート テーブルを編集します。

1. **VPC** > **Route Tables**（ルートテーブル）を選択します。
2. 保護するサブネットのルート テーブルを選択します。
3. ルートを追加し、宛先をDNSサーバーのIPアドレスに設定し、ターゲットをCloud NGFW エンドポイントに設定します。



4. **Save changes**（変更内容の保存）をクリックします。

   保護されたサブネットからの DNSトラフィックはすべて、検査と適用のためにCloud NGFWエンドポイントを経由してCloud NGFWにルーティングされます。

プライベートホストゾーンDNS

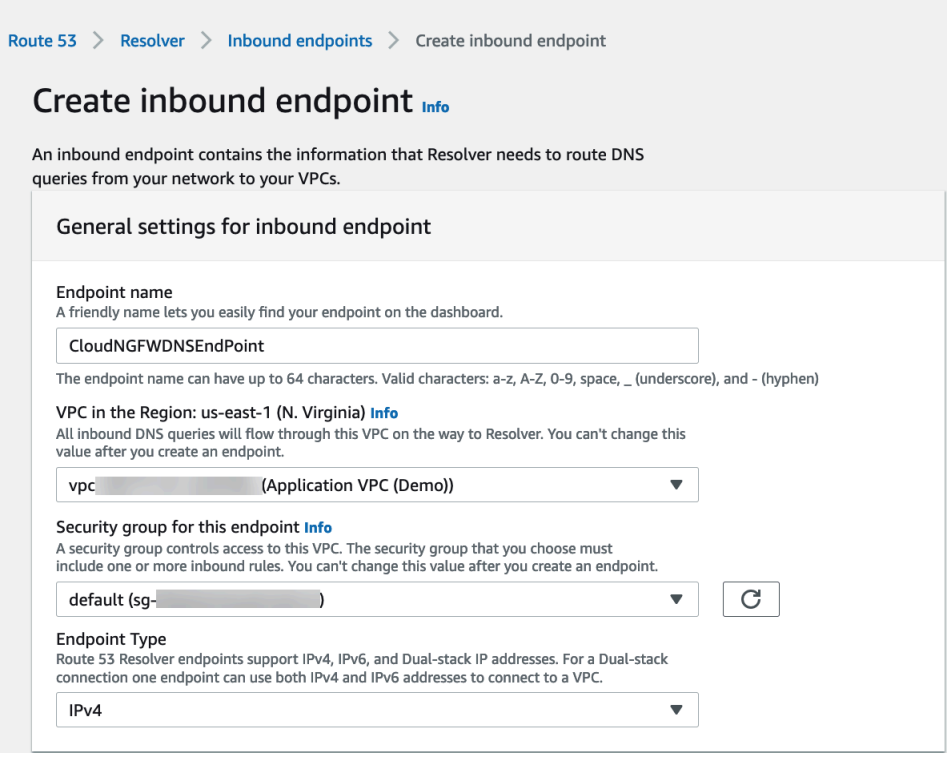
AWSでプライベートホストゾーンを作成するには、プライベートホストゾーンの作成を参照してください。

Cloud NGFWリソースがRoute 53 ResolverにRoute 53でホストされているDNSゾーン（プライベートゾーンなど）を照会できるようにするには、前述したようにRoute 53インバウンドエンドポイントを作成します。インバウンドエンドポイントは、他のサービスがRoute 53にドメイン名解決を問い合わせるためのブリッジです。インバウンド エンドポイントを作成すると、AWSはインバウンドDNSクエリを受信するように指定した各可用性ゾーン（AZ）に弾性ネットワークインターフェース（ENI）を作成します。

STEP 1 | Amazon VPCコンソールを開きます。

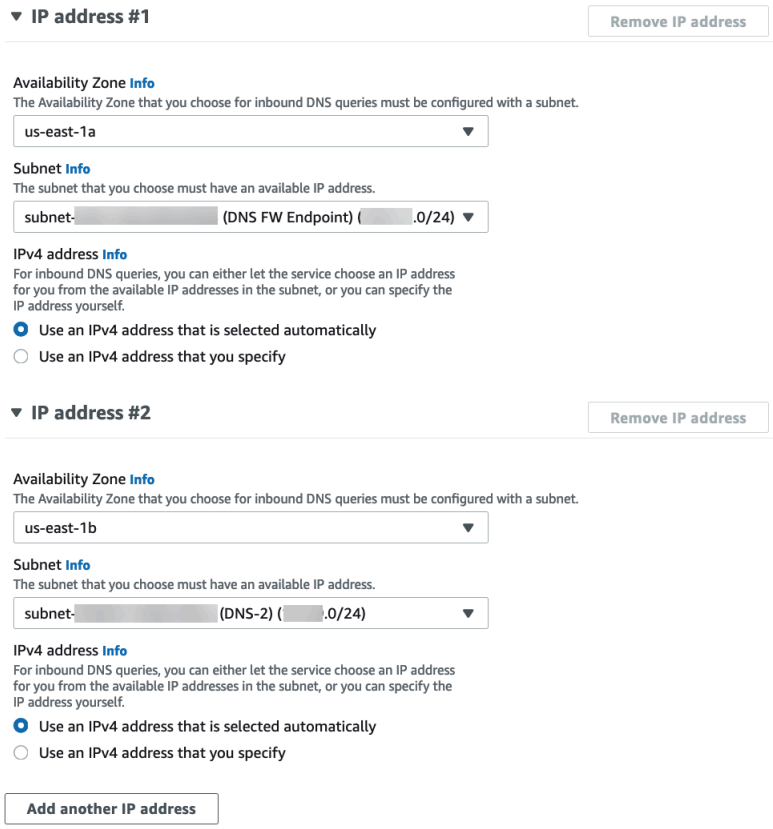
STEP 2 | インバウンド エンドポイントを作成します。

1. **[Services(サービス)]** > > **[Route 53** > **Resolver]** > > **[Inbound Endpoints(**インバウンド エンドポイント**)]**を選択します。
2. **[Create inbound endpoint(**受信エンドポイントの作成**)]** をクリックします。
3. 分かりやすい **Name**（名前）を入力します。
4. エンドポイントのVPCを選択します。
5. このエンドポイントにセキュリティ グループをアタッチします。
6. エンドポイント タイプをIPv4に設定します。



7. 可用性ゾーンを選択します。
8. 上記で作成したサブネットを選択します。

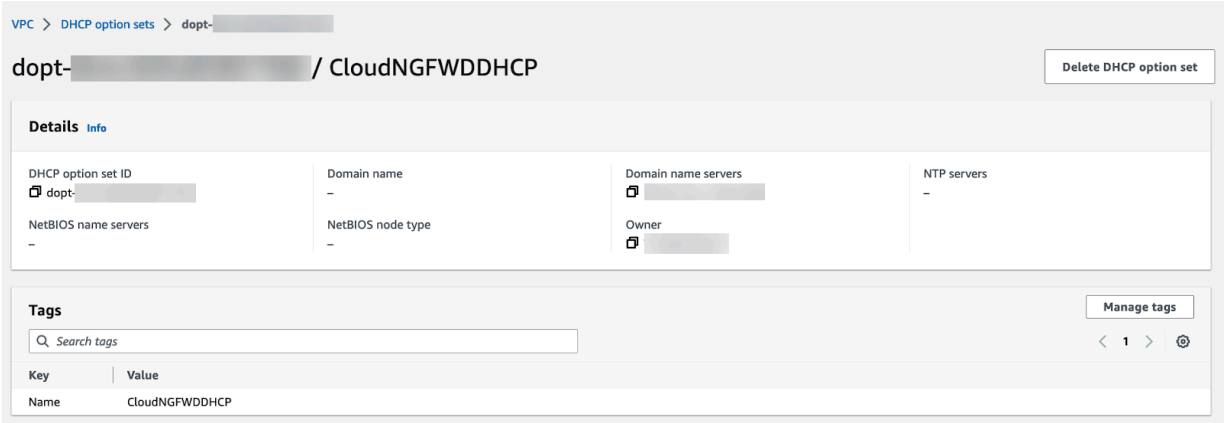
複数の可用性ゾーンがある場合は、それぞれの可用性ゾーンとサブネットを指定する必要があります。



9. **[Create inbound endpoint(受信エンドポイントの作成)]** をクリックします。
10. 受信エンドポイントに接続されている各サブネットに関連付けられているIPアドレスをメモします。以下の手順で**DHCP** オプション セットを構成するときに、これらのIPアドレスを使用します。

STEP 3 | **VPC** > **DHCP** オプション セットを選択します。

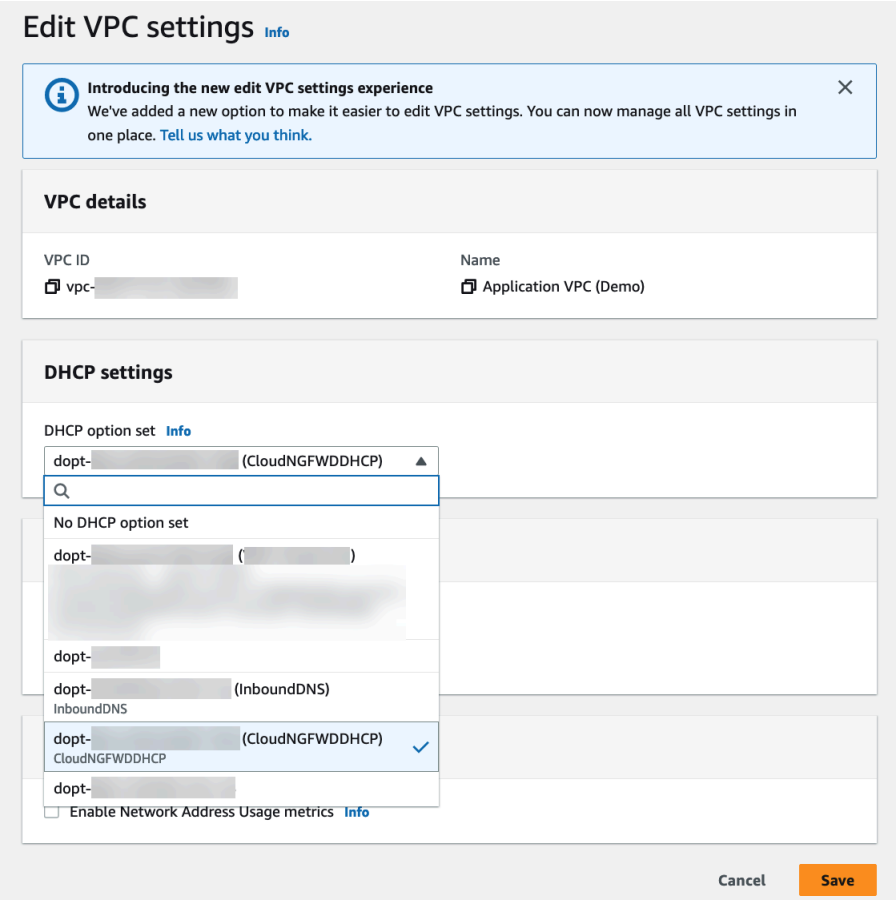
STEP 4 | 新しいDHCPオプション セットを作成し、各可用性ゾーンのIPアドレスを追加できます。複数の可用性ゾーンがある場合は、各IPアドレスをコンマ区切りのリストとして入力します。



STEP 5 | **VPC** を選択し、保護する VPC を選択します。

STEP 6 | **[Actions(アクション)]** ドロップダウンから、**[Edit VPC settings(VPC** 設定の編集**)]**を選択します。

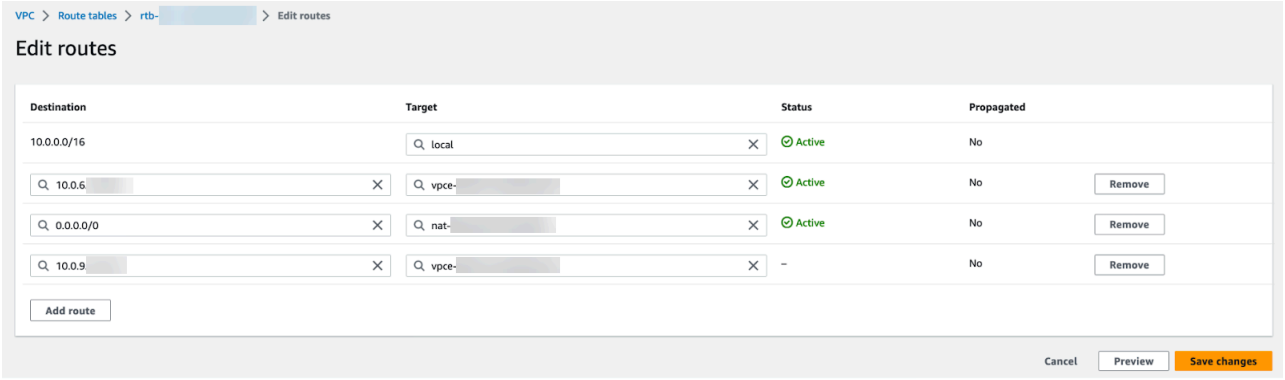
STEP 7 | **[DHCP settings(DHCP** 設定**)]**で、**DHCP** オプション セット ドロップダウンから上記で作成したDHCPオプション セットを選択します。



STEP 8 | **Save changes**（変更内容の保存）をクリックします。

STEP 9 | サブネット ルート テーブルを編集します。

1. **VPC** > **Route Tables**（ルートテーブル）を選択します。
2. 保護するサブネットのルート テーブルを選択します。
3. ルートを追加し、宛先をDNSサーバーのIPアドレスに設定し、ターゲットをCloud NGFW エンドポイントに設定します。



4. **Save changes**（変更内容の保存）をクリックします。

   保護されたサブネットからの DNSトラフィックはすべて、検査と適用のためにCloud NGFWエンドポイントを経由してCloud NGFWにルーティングされます。

Cloud NGFW for AWSエンタープライズデータ損失防止（E-DLP）統合

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）

エンタープライズデータ損失防止（E-DLP）は、機密情報を不正なアクセス、誤用、抽出、または共有から保護するための、一連のツールとプロセスです。詳細については、「エンタープライズDLPについて」を参照してください。

E-DLPとCloud NGFW for AWSを統合し、Panoramaコンソールを使用してセキュリティ ポリシー ルールにデータ フィルタリング プロファイルを追加できます。

最小要件

以下は、E-DLPをCloud NGFWサービスに統合するためのPanoramaとPanoramaプラグインのバージョン要件の組み合わせです。

Panoramaのバージョン (PAN-OS)	DLPプラグイン	AWS プラグイン
10.0.2以上	1.0.9	5.2.0
10.2.4以上	3.0.7	5.2.0
11.0.2以上	4.0.3	5.2.0
11.1.0以上	5.0.1	5.2.0

Cloud NGFW for AWSで新しいE-DLPテナントをプロビジョニングする

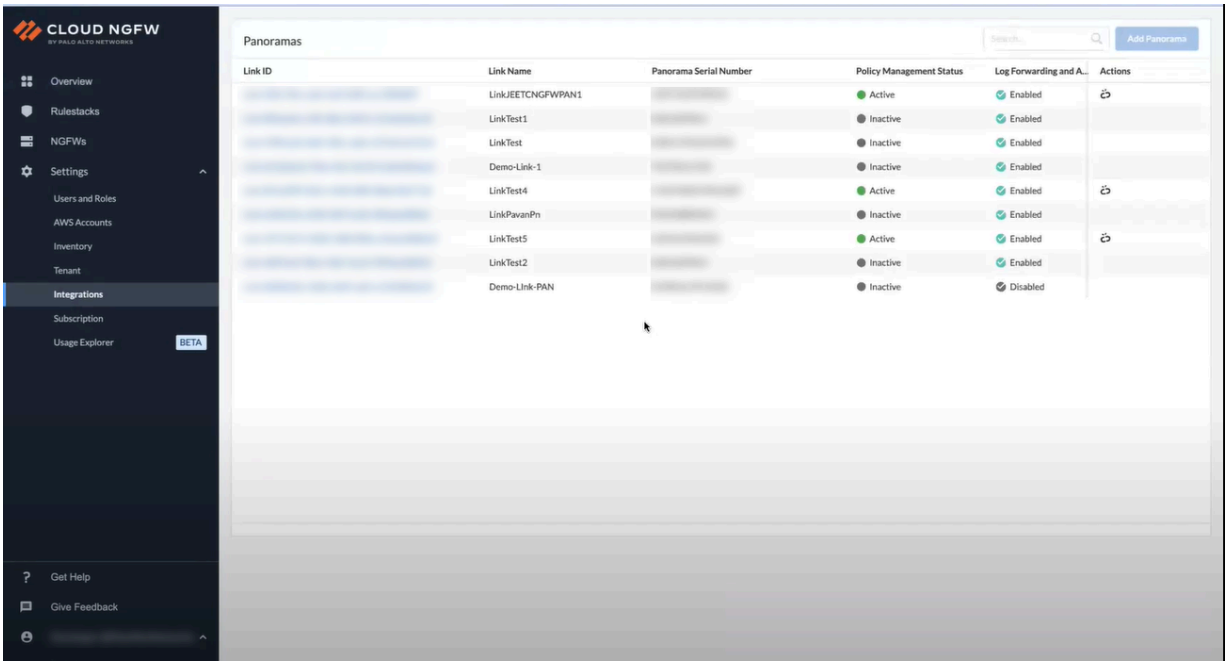
Panoramaでプロビジョニングされたカスタマーサポートポータル（CSP）アカウントに既存のDLPテナントがある場合、Cloud NGFWサービスはそのDLPテナントを使用してDLPとCloud NGFWを統合します。

カスタマーサポートポータルアカウントにDLPテナントがない場合、Cloud NGFWサービスは新しいDLPテナントを作成します。

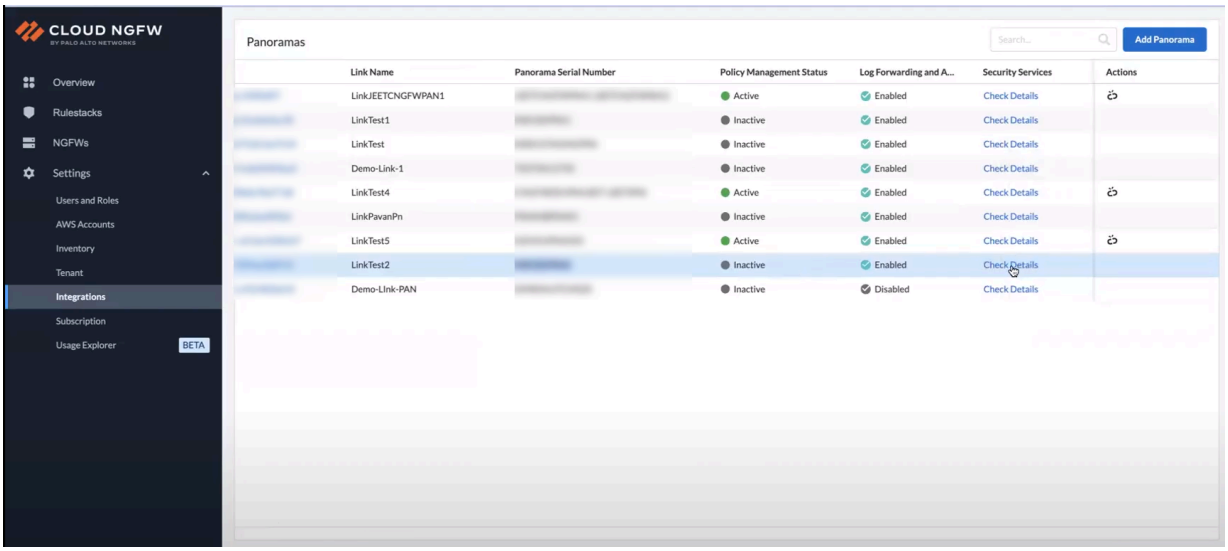
Cloud NGFWコンソールで新しいDLPテナントを有効にする手順は次のとおりです。

STEP 1 | Cloud NGFW コンソールにログインします。

STEP 2 | **[Integrations(統合)]**を選択します。

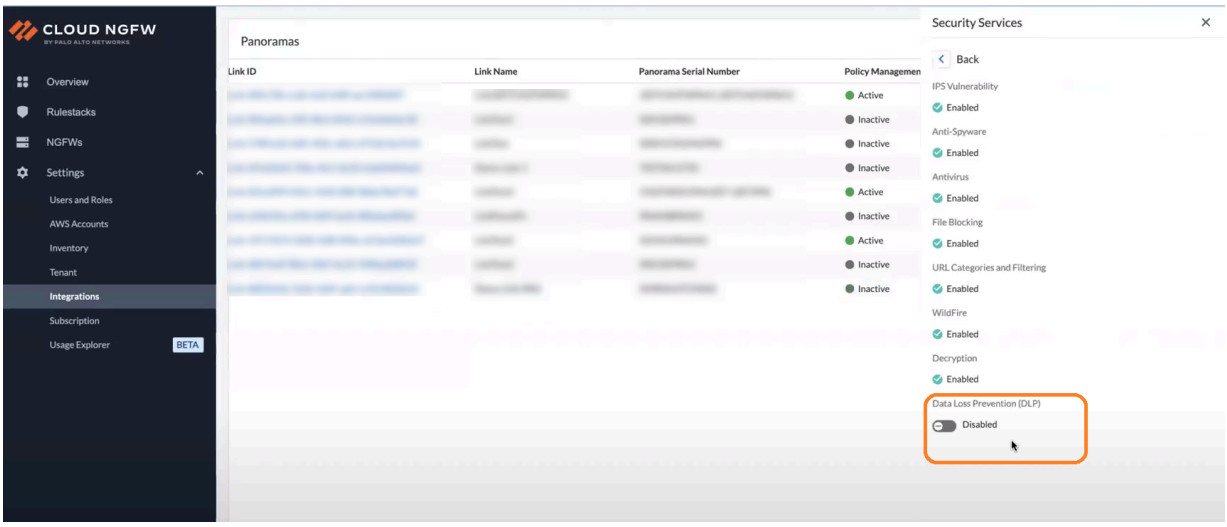


STEP 3 | [Security Service(セキュリティサービス)]列で、**[Check Details(詳細の確認)]**をクリックします

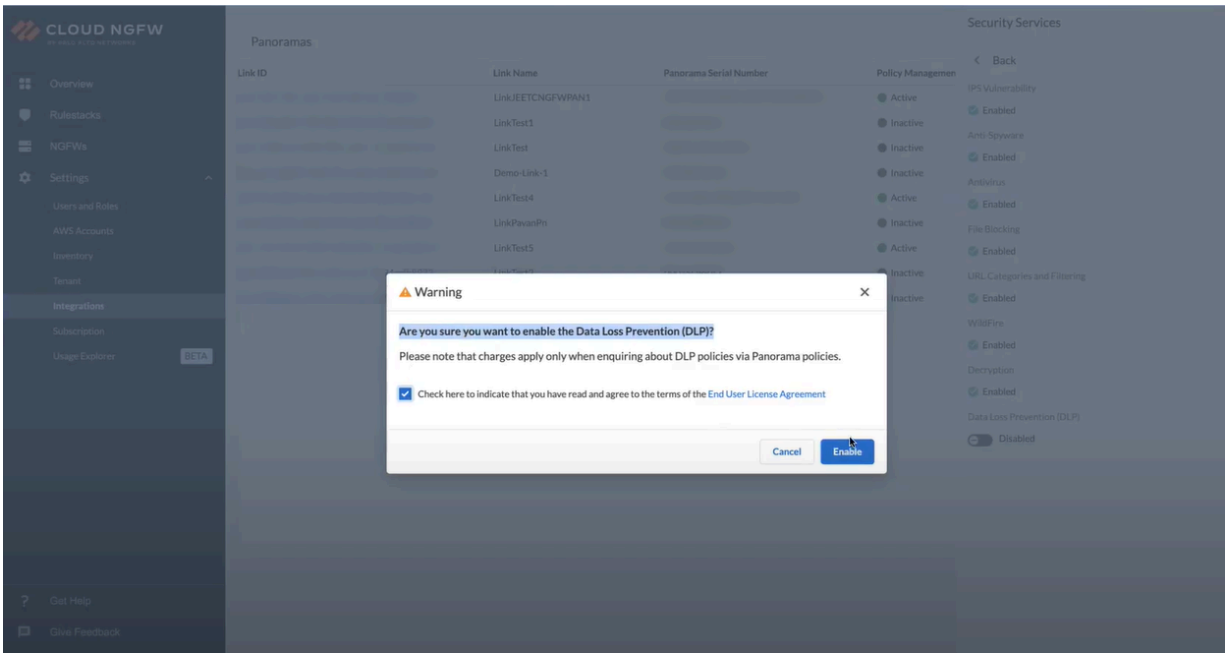


リンクされた*Panorama*のリンク***ID*** をクリックし、 ***[Check Details(詳細の確認)]***をクリックすることもできます。

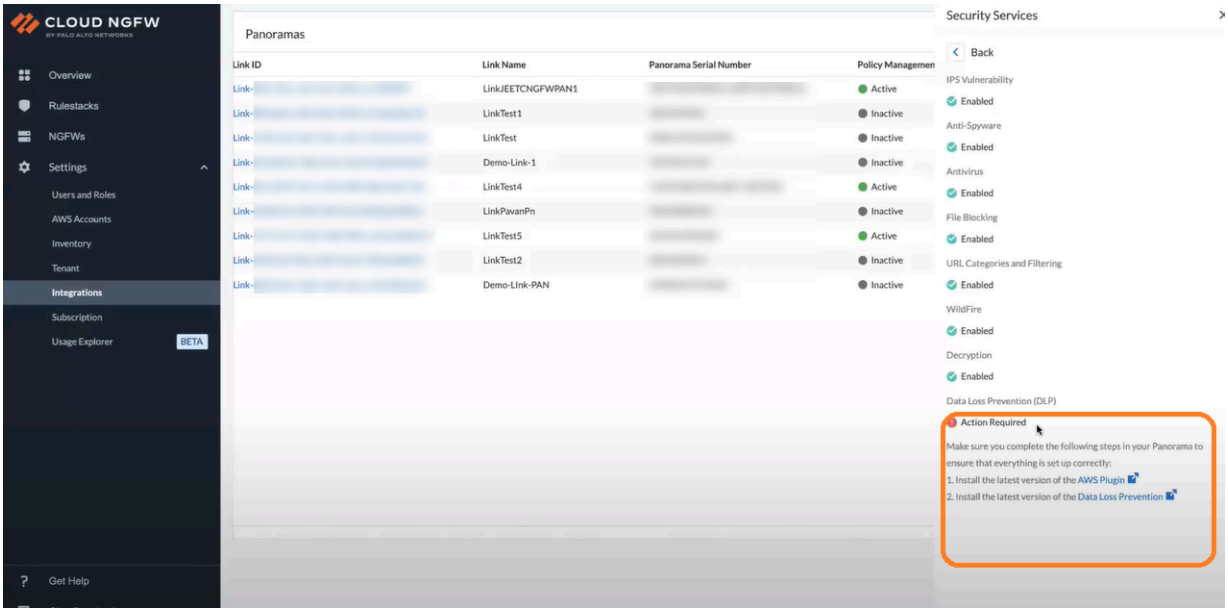
STEP 4 | ［セキュリティサービス]パネルで**[Data Loss Prevention (**データ損失防止（**DLP))]**トグルをクリックします。



STEP 5 | チェックボックスをオンにしてエンドユーザー使用許諾契約書に同意し、**[Enable(**有効にする**)]**をクリックします。



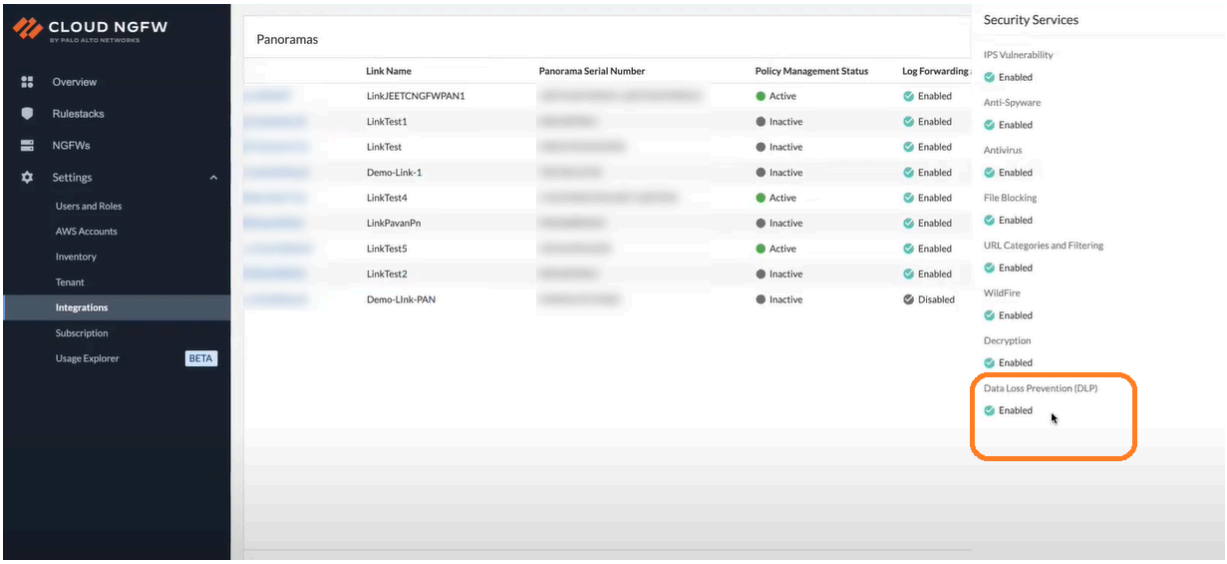
STEP 6 | リンク先のPanoramaの**[Action Required(必要な操作)]**を確認します。



DLPとCloud NGFWサービスを統合するために、リンクされたPanoramaがこのページで以前に記載された最小システム要件を満たしていることを確認します。

Panoramaに必要なAWSおよびDLPプラグインをインストールすると、Cloud NGFWコンソール上のDLPテナントが有効になります。

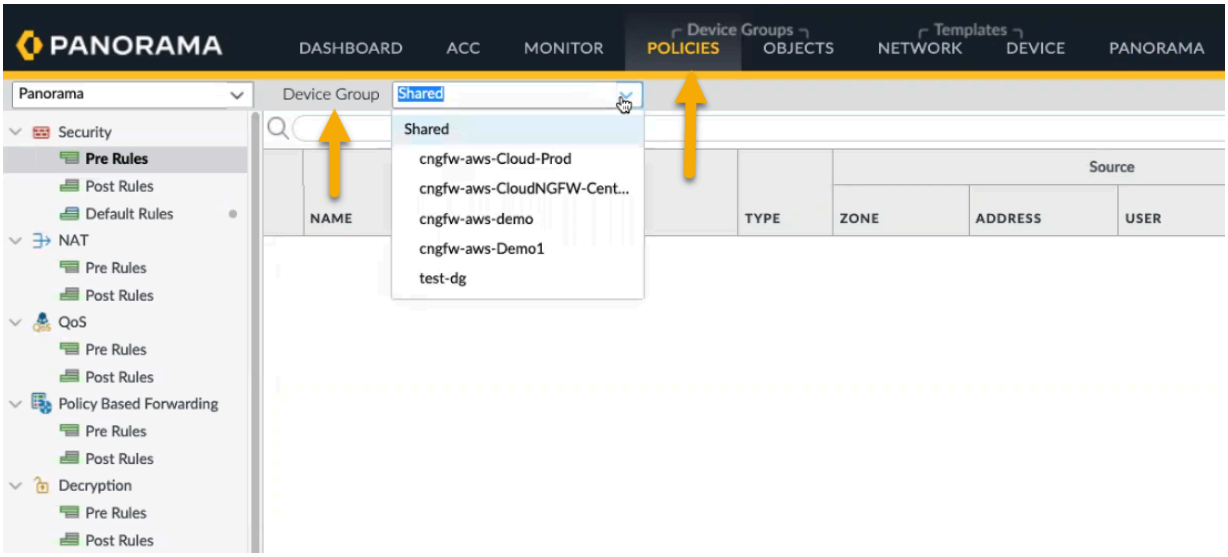
Cloud NGFWコンソールで、［**Integrations(統合)]**ページに移動し、リンクされたPanoramaを選択し、［セキュリティ サービス]列の下にある**[Check Details(詳細を確認)]**をクリックします。



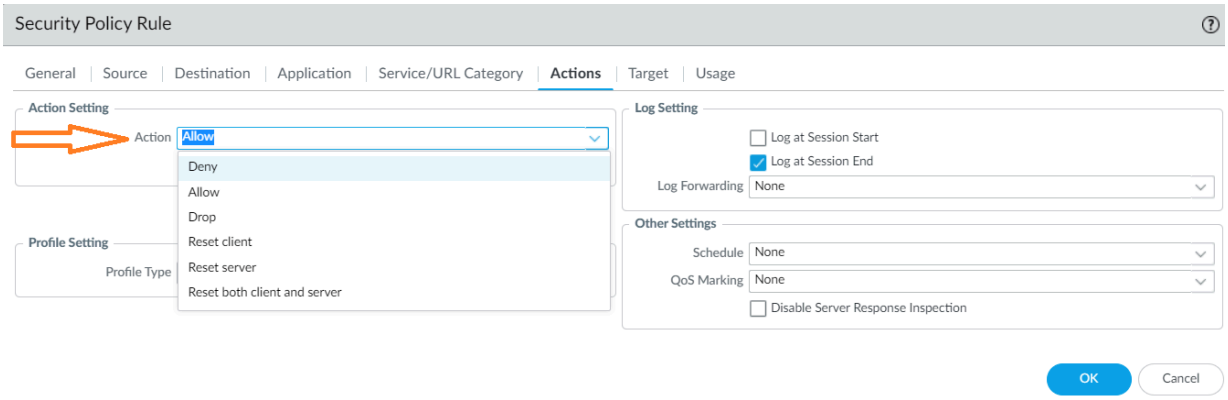
これで、有効になっているデータ損失防止**(DLP)**を確認できます。

Cloud NGFWコンソールでDLPテナントを正常に有効化すると、リンクされたPanoramaに関連付けられたファイアウォールがDLPサービスの使用を開始できるようになります。

Panoramaでファイアウォールのセキュリティ ポリシー ルールにDLPフィルタリング プロファイルを追加できます。

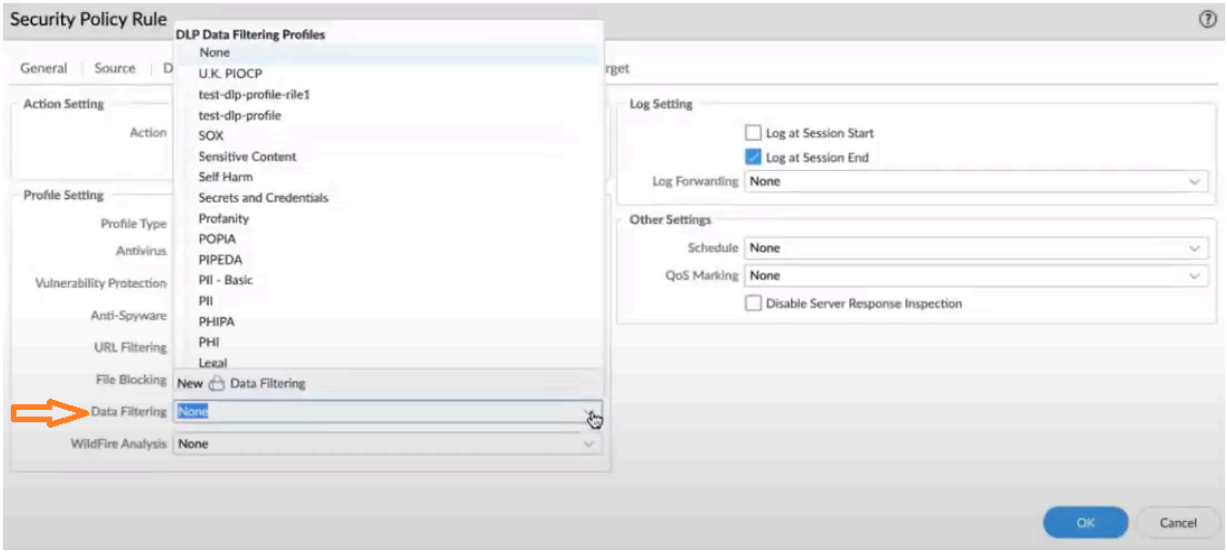


[セキュリティ ポリシー ルール]画面で、**[Actions(アクション)]**タブに移動し、実行するアクション(許可、拒否など)を選択します。

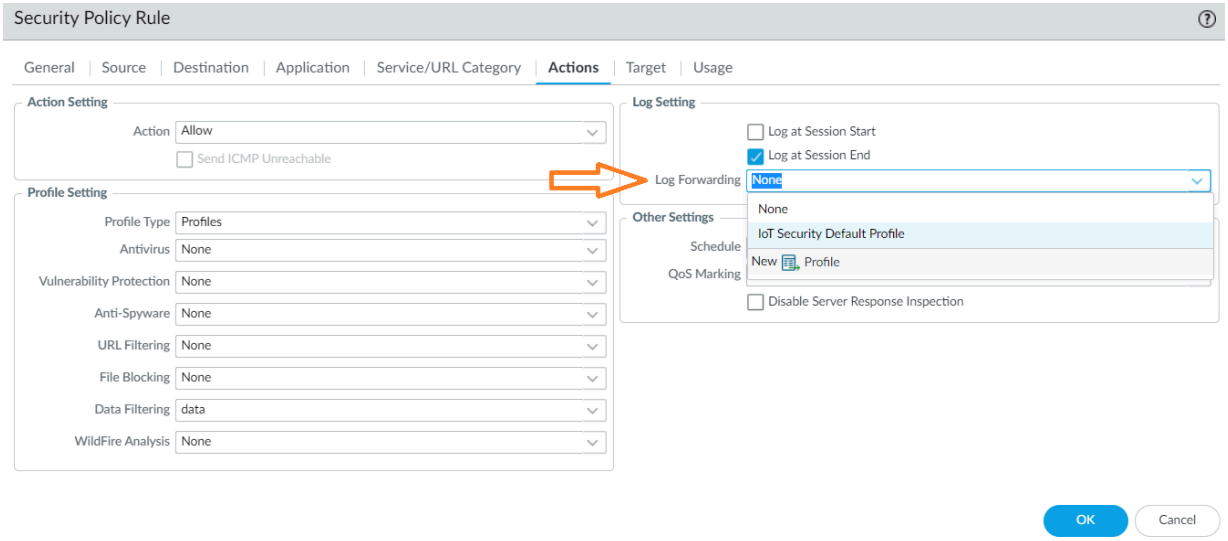


「プロファイル設定」を決定します。

[DLP data filtering profile(DLPデータ フィルタリング プロファイル**)]**を選択します。

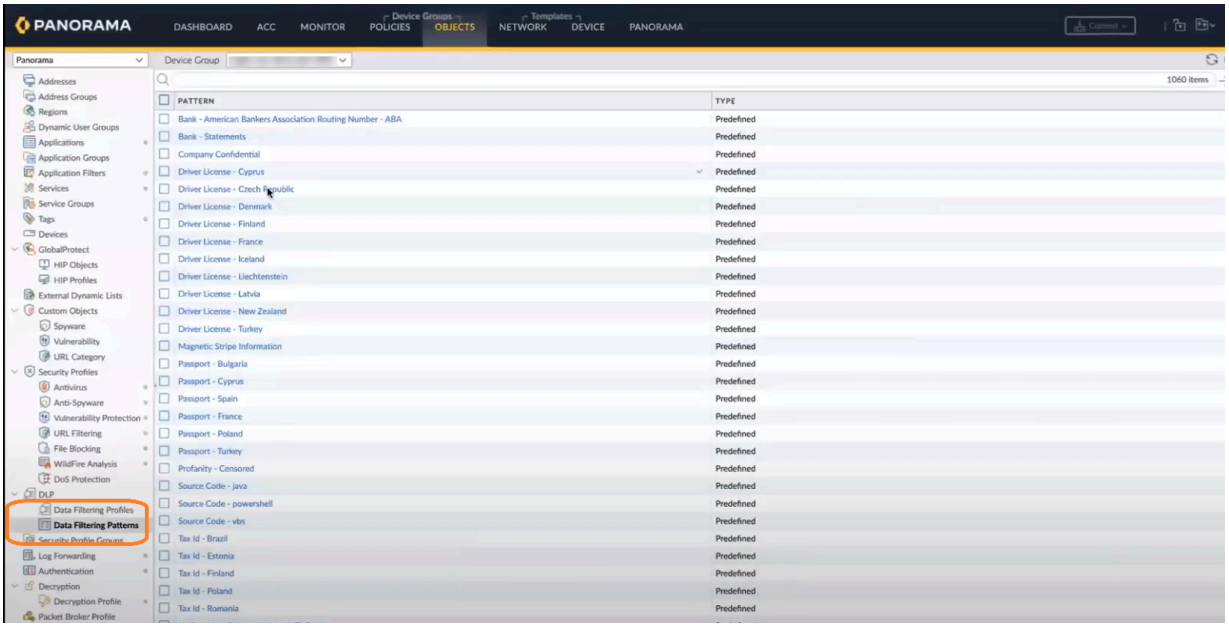


ログ設定などの設定を行います。



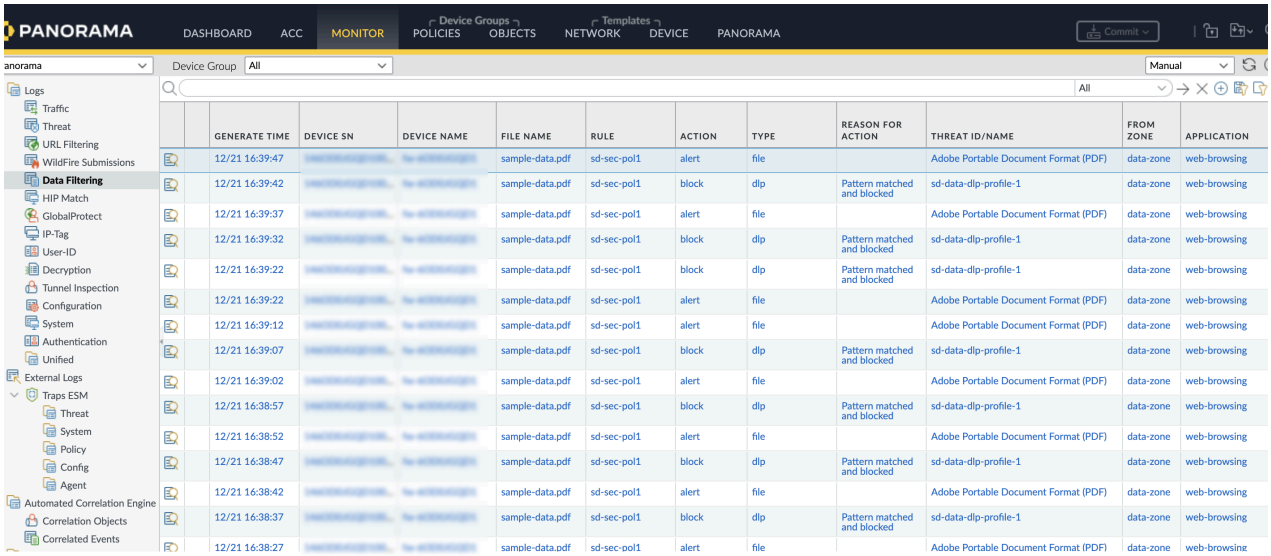
詳しくは、「Cloud NGFWポリシー管理にPanoramaを使用する」を参照してください。

セキュリティ ポリシー ルールをファイアウォールにプッシュすると、DLPテナントに使用できる既存のデータ フィルタリング プロファイルとデータ フィルタリング パターンを表示できます。

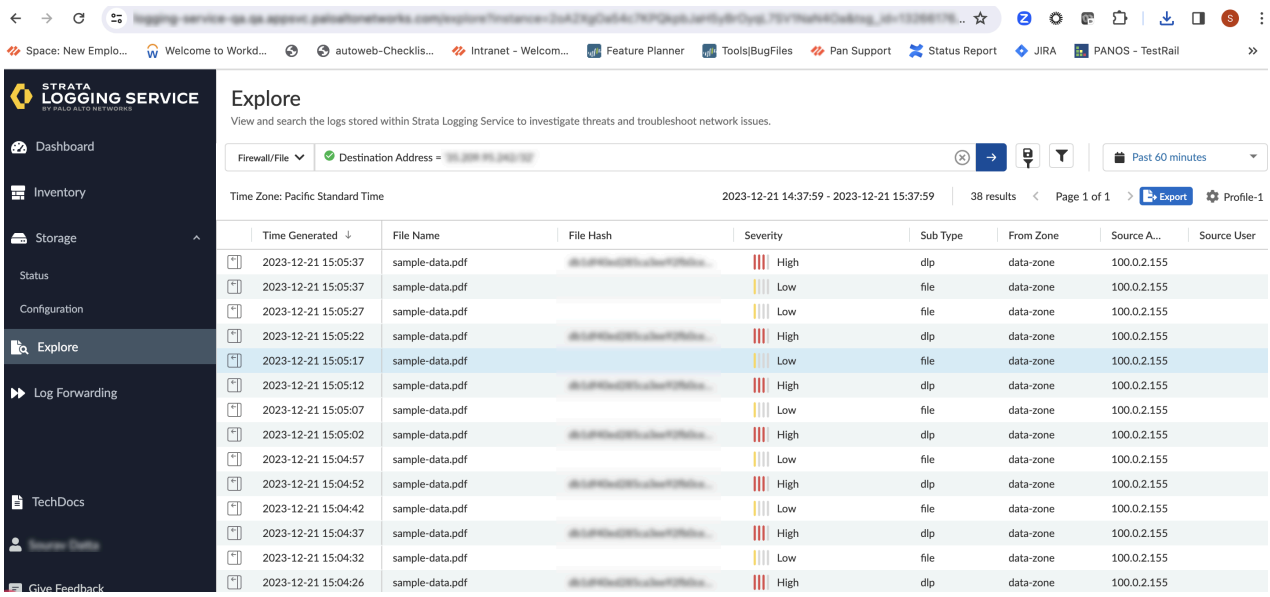


DLPログの詳細の監視

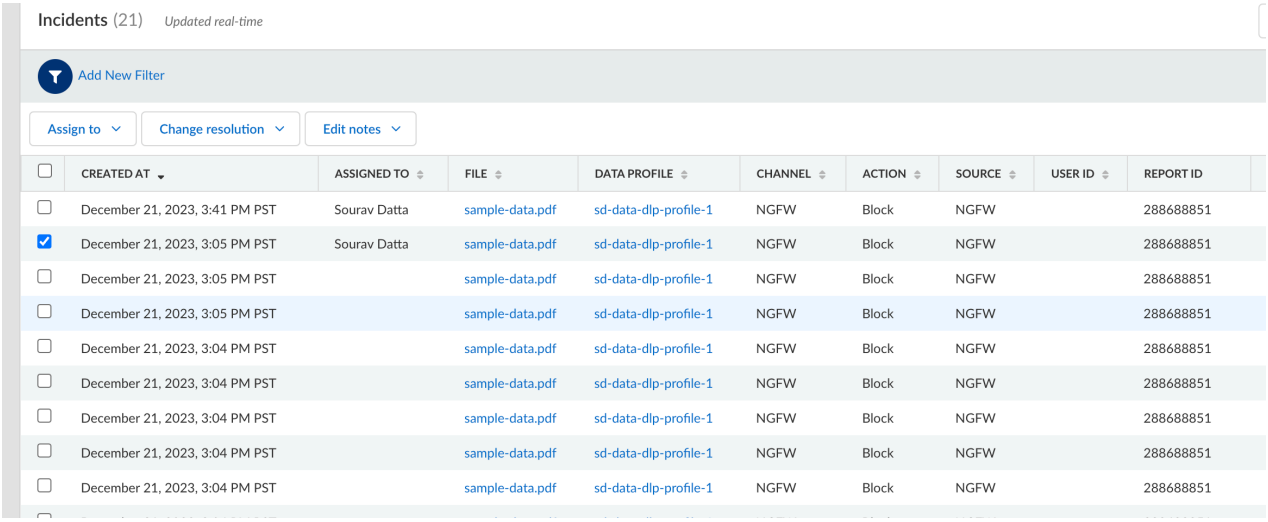
PanoramaでDLPログを表示するには、**[Monitor(**モニター**)**］タブをクリックし、**[Logs(**ログ**)**］＞［データ フィルタリング］を選択します。詳細については、「Panoramaでエンタープライズ DLPのログ詳細を表示する」を参照してください。



DLPのStrata Logging Serviceログを表示するには、**[Explore(探索)]**タブに移動し、**[Firewall or File(ファイアウォールまたはファイル)]**オプションを選択します。Strata Logging Serviceのログ詳細を表示するには、詳細情報をご覧ください。



SCMでDLPテナントインシデントログを表示するには、「Strata Cloud ManagerでエンタープライズDLPログ詳細を表示する」を参照してください。



DLPログのAWS宛先の詳細については、「Amazon CloudWatchログ」を参照してください。

クラウド NGFW ネイティブ ポリシー管理

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 では、セキュリティポリシールールを定義し、それらのルールを 1 つのルール スタックにグループ化します。

セキュリティ ポリシールールにより、ネットワーク上のトラフィックを許可またはブロックできますが、セキュリティ プロファイルを使用すると、許可するがスキャンを実施するルールを定義できます。このルールでは、許可されたアプリケーションにマルウェア、スパイウェア、DDOS 攻撃などの脅威が潜んでいないかスキャンされます。トラフィックがセキュリティ ポリシー ルールで定義した許可ルールと一致する場合、そのルールに添付されたセキュリティ プロファイルが、アンチウイルス チェックやデータ フィルタリングなどのコンテンツ検査ルールに追加適用されます。

セキュリティ プロファイルは、トラフィック フローの一致基準には使用されません。セキュリティプロファイルは、セキュリティポリシールールがアプリケーションまたはカテゴリを許可した後に、スキャントラフィックに適用される。

ファイアウォールでは、デフォルトのセキュリティ プロファイルをそのまま使用して、すぐにネットワークを脅威から保護できます。デフォルトのプロファイルをセキュリティ ポリシー ルールで使用する方法の詳細は、基本的なセキュリティ ポリシーのセットアップを参照してください。

セキュリティプロファイルのベストプラクティス設定に関する推奨事項については、セキュリティプロファイル作成のベストプラクティスを参照してください。

セキュリティ プロファイル グループの作成を行うことで、一緒に適用することが多いセキュリティ プロファイルをまとめておくことができます。このプロファイル グループは1つの単位として扱うことができるプロファイルのセットであり、セキュリティ ポリシー規則に 1 ステップで追加できます（デフォルトのセキュリティ プロファイル グループを設定した場合は、デフォルトでセキュリティ ポリシー規則に追加されます）。

ネットワーク上で許可するトラフィックに潜む脅威をスキャンすることで、基盤となる保護を提供するのがセキュリティ プロファイルです。セキュリティ プロファイルは、ピアツーピアのコマンド アンド コントロール（C2）アプリケーション トラフィック、危険なファイル形式、脆弱

性をエクスプロイトしようとする試み、アンチウイルス シグネチャをブロックし、新規および未知のマルウェアを特定する一連の連携する脅威防御ツール一式を提供します。

セキュリティポリシー許可ルールに追加するだけで良い事前定義済みのプロファイルを Palo Alto Networks が提供しているため、セキュリティ プロファイルは比較的簡単に適用できます。事前定義済みのプロファイルをクローンして編集すれば良いため、セキュリティ プロファイルは簡単にカスタマイズできます。ファイアウォールあるいは Panorama 上で一からセキュリティ プロファイルを作成することもできます。

ネットワーク トラフィック内の既知および未知の脅威を検出するために、ネットワーク上のトラフィックを許可するすべてのセキュリティポリシールールにSecurity Profiles（セキュリティ プロファイル）を付与し、許可されたすべてのトラフィックをファイアウォールに検査させます。ファイアウォールはセキュリティポリシー許可ルールにマッチしたトラフィックにセキュリティ プロファイルを適用し、セキュリティ プロファイルの設定に基づいてトラフィックをスキャンしてから、適切なアクションを実行してネットワークを保護します。ベストプラクティスのセキュリティプロファイルに関する推奨事項は、特に断りのない限り、データセンターの4つのトラフィックフローすべてに適用されます。

コンテンツ更新を自動的にダウンロードしてできるだけ早くインストールし、ファイアウォールの脅威防御シグネチャおよびコンテンツ（アンチウイルス、アンチスパイウェア、脆弱性、マルウェアなど）を最新に保ち、新しい脅威をブロックできるようにしてください。

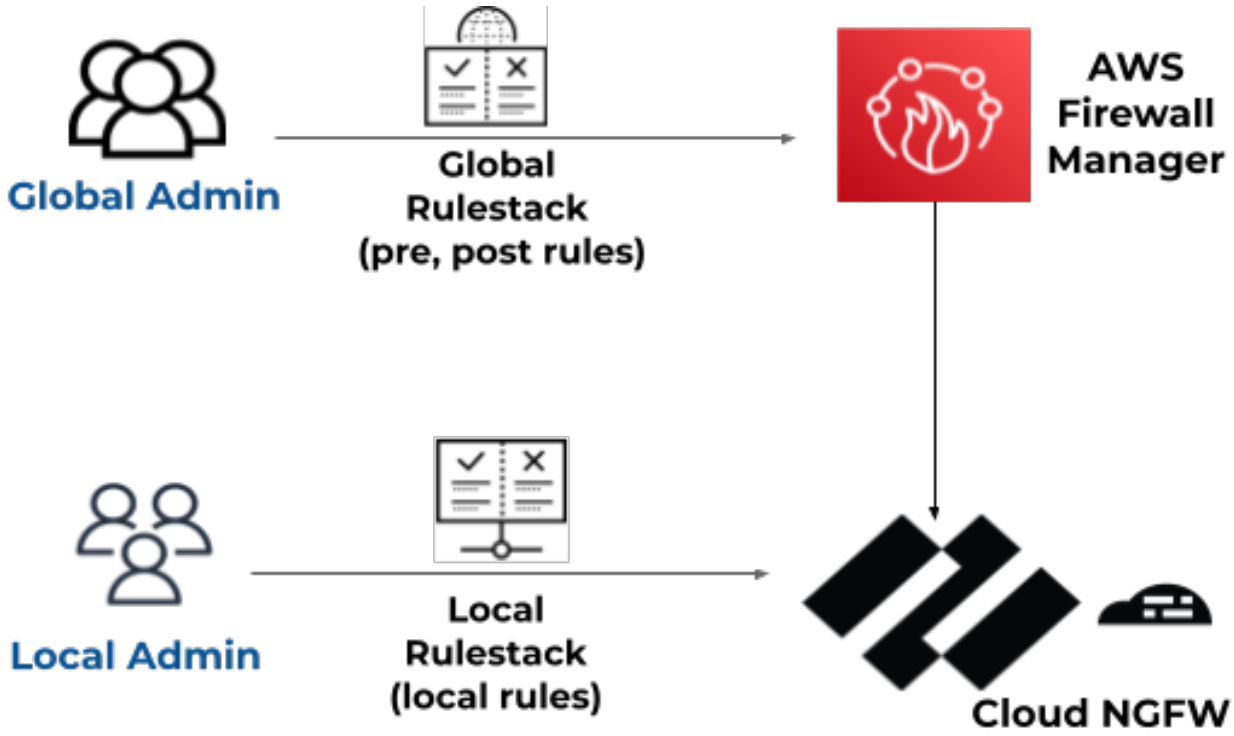
Rulestacks and Rules on Cloud NGFW for AWS

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）

ルールスタックは、Cloud NGFW リソースのアクセス制御（アプリ ID、URL フィルタリング）と脅威防止動作を定義します。Cloud NGFW リソースは、ルールスタック定義を使用して、2 段階のプロセスでトラフィックを保護します。まず、トラフィックを許可または拒否するルールを適用します。次に、セキュリティプロファイルで指定した内容に基づいて、許可されたトラフィックに対してコンテンツ検査を実行します。ルールスタックには、Panoramaのデバイスグループと同様のセキュリティルール、関連オブジェクト、およびプロファイルのセットが含まれます。ルールスタックには、次の 2 つのタイプがあります。

- ローカルルールスタック - ローカルルールスタックはローカルルールで構成され、ローカルルールを管理します。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を作成および管理するには、ローカルルールスタック管理者ロールが必要です。
- 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ーサービス（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は、各 NGFW の事前ルールと事後ルールを設定します。グローバルルールスタックを作成および管理するには、グローバルルールスタック管理者ロールが必要です。
  - 事前ルール- ルールの順序の先頭に追加されたルール。これらのルールは最初に評価されます。
  - ポストルール- ルールの順序の一番下に追加されたルール。これらのルールは、事前ルールとローカルルールスタックで定義されたルールが個々のNGFWに適用された後に評価されます。

AWSファイアウォールマネージャを使用する場合、ローカルルールスタックとグローバルルールスタックを組み合わせることで、階層ルールモデルを作成できます。グローバルルールスタックの事前ルールは、関連するすべてのファイアウォールのグローバルデフォルトルールとして機能します。その後、ローカルルールスタックを使用して、特定のアプリケーションまたはユーザーのルールを定義できます。ポストルールは、事前ルールまたはローカルルールスタックで定義されたルールに一致しないトラフィックを許可または拒否するために使用できます。



Region: US East (N. Virginia)

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

Name	Status	Type	Account Id
Application	Running	Local	
LocalFWRulestack1	Uncommitted	Local	
	Running	Local	
PerformanceRule	Running	Local	
Test	Uncommitted	Local	
	Uncommitted	Local	
-local-rulestack	Uncommitted	Local	

*1*つのグローバル ルールスタックと*1*つのローカル ルールスタックが各 *NGFW* に適用されます。

マルチアカウントテナントまたはマルチVPCを使用している場合は、ルールスタックの動作を次のように変更することを検討してください。

- ルールスタックが作成されると、特定のアカウントにマップされます。
- これで、任意のオンボーディング済みアカウントのファイアウォールリソースにルールスタックを関連付けることができます。
- アクセス権限は引き続きルールスタックに関連付けられているアカウントにマップされます。ルールスタックへの変更は、ルールスタックアカウントのLRA権限を持つユーザーが行います。

どのオンボーディング済みアカウントの証明書もルールスタックにマッピングされます。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られます。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。

Cloud NGFW for AWS でルールスタックを作成する

Cloud NGFW テナントでは、LocalRuleStackAdmin または GlobalRulestackAdmin ロールが割り当てられている場合、ルールスタックを作成できます。グローバル ルールスタックを作成するには、AWS Firewall Managerを使用してCloud NGFWテナントを作成しておく必要があります。

ローカル ルールスタックを作成するときは、AWSアカウントを指定する必要があります。ルールスタックは、そのAWSアカウントに関連付けられたNGFWにのみ適用します。ルールスタックを作成するには、次の手順を実行します。

STEP 1 | **[Rulestacks(**ルールスタック**)]** > **[Create Rulestack(**ルールスタックを作成**)]**を選択します。

STEP 2 | ドロップダウンから［ローカルルールスタック**]**または［グローバルルールスタック］（FMS デプロイメント）を選択します。

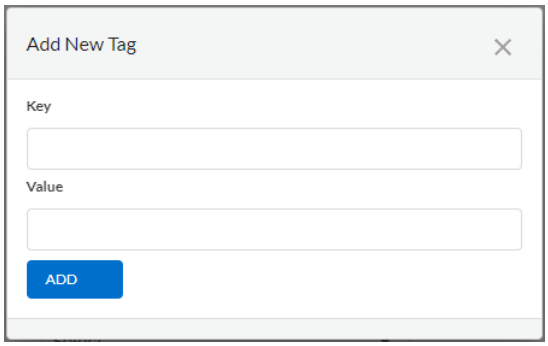
STEP 3 | ルールスタックのわかりやすい名前を入力します。

STEP 4 | （任意）ルールスタックの説明を入力します。

STEP 5 | （ローカルルールスタックのみ）ドロップダウンから**AWS**アカウントを選択します。

STEP 6 | （任意）タグを適用します。

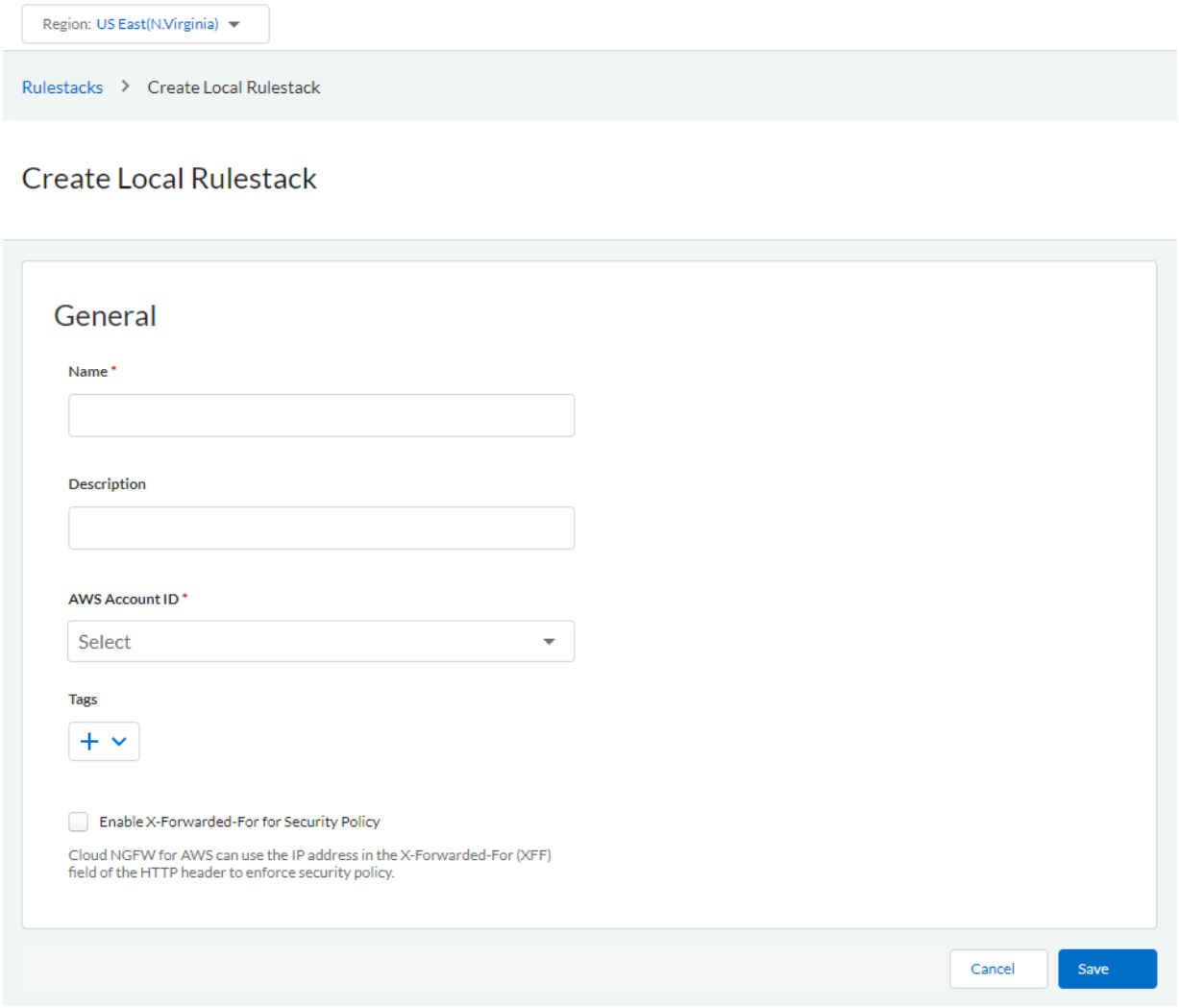
1. + アイコンをクリックし、［新規追加］を選択します。
2. キーと値を入力します。
3. **[追加]** をクリックします。



STEP 7 | （任意）セキュリティ ポリシーの X-Forwarded-For を有効にします。見る X-Forwarded の詳細については、こちらをご覧ください。

STEP 8 | **[Save(保存)]**をクリックします。

STEP 9 | ルールスタックを作成したら、ファイアウォールに展開します。



Cloud NGFW for AWS での X-Forwarded-For

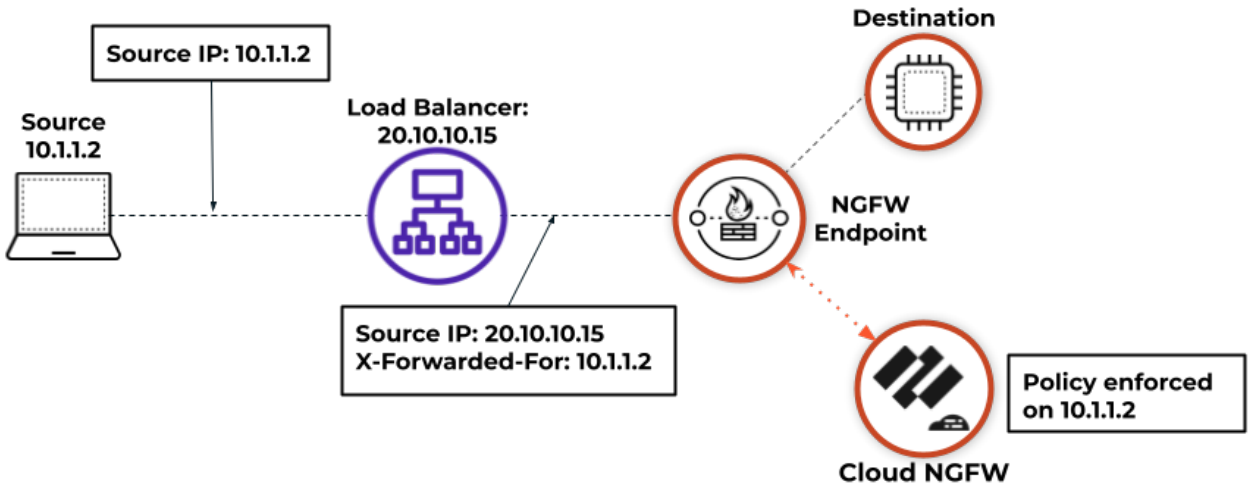
どこで使用できますか?	何が必要ですか?
• Cloud NGFW for AWS	❑ Cloud NGFWサブスクリプション ❑ Palo Alto Networksカスタマー サポート アカウント (CSP) ❑ AWS Marketplaceアカウント

どこで使用できますか?	何が必要ですか?
	❑ ユーザーのロール（テナントまたは管理者）

アプリケーションへのイングレストラフィックは、NGFW に到達する前に AWS ロードバランサーまたはプロキシサーバーを通過する場合があります。これらのデバイスは送信元と宛先の間のトラフィックをインターセプトするため、NGFW は送信元の IP アドレスではなく、ロードバランサーまたはプロキシサーバーの IP アドレスを認識します。これらのデバイスは、X-Forwarded-For（XFF）ヘッダーを HTTP リクエストに追加し、アプリケーションにアクセスするクライアントの実際の IPv4 または IPv6 アドレスを追加します。

アプリケーションへのトラフィックは、NGFW に到達する前に複数のプロキシサーバーを通過した可能性があります。XFF リクエストヘッダーには、コンマで区切られた複数の IP アドレスが含まれている場合があります。NGFW は常に、XFF ヘッ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。

ルールスタックを設定するときに、Cloud NGFW が XFF HTTP ヘッダーフィールドの送信元 IP アドレスを使用してセキュリティポリシーを適用できるようにすることができます。



Cloud NGFW for AWS でプレフィックスリストを作成する

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）

セキュリティールールオブジェクトは、IP アドレス、完全修飾ドメイン名（FQDN）、インテリジェントフィード、証明書などの個別の ID をグループ化する単一のオブジェクトまたは集合単位です。一般的にポリシー オブジェクトを作成する場合、ポリシーで同様のアクセス権限を必要とするオブジェクトをグループ化します。たとえば、組織でユーザーの認証にサーバー IP アドレスのセットを使用している場合、サーバー IP アドレスのセットをプレフィックスリストオブジェクトとしてグループ化し、そのプレフィックスリストを 1 つ以上のセキュリティルールで参照できます。グループオブジェクトを使用すると、ルールを作成する際の管理オーバーヘッドを大幅に削減できます。

プレフィックスリストを使用すると、同じポリシー適用を必要とする特定の IP アドレスをグループ化できます。プレフィックスリストには、CIDR 表記で 1 つ以上の IP アドレスまたは IP ネットマスクを含めることができます。タイプの IP Netmask のアドレスオブジェクトでは、IPv4 ネットワークを示すためにスラッシュ表記を使用して IP アドレスまたはネットワークを入力する必要があります。たとえば、192.168.18.0/24 です。

STEP 1 | ［ルールスタック］を選択し、接頭部リストを構成する前に作成したルールスタックを選択します。

STEP 2 | ［オブジェクト］ > ［プレフィックスリスト］ > ［プレフィックスの作成］を選択します。

STEP 3 | プレフィックスリストにわかりやすい名前を入力します。

STEP 4 | （任意）プレフィックスリストの説明を入力します。

STEP 5 | 1 つ以上の アドレスを入力します。IP アドレスまたは IP ネットマスクは、CIDR 形式で、1 行に 1 つの値を入力できます。

STEP 6 | **[Save(保存)]**をクリックします。

Cloud NGFW for AWS に証明書を追加する

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）

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。これらの証明書は AWS シークレットマネージャに保存されます。

一般的なデプロイメントで使用される証明書には3種類あります。

- 中間**CA**証明書 **(CA** 証明書**)**- 認証局 (CA) は、SSL 証明書を発行する信頼できる組織です。このデジタル証明書は、エンティティを公開キーにリンクするために使用されるファイルです。Webブラウザはこの証明書を使用して、Web サーバーから送信されたコンテンツを認証します。Webブラウザには通常、ホストを識別するために暗黙的に信頼する CA のリストが付属しています。CAの目的は、Webサイト、ドメイン、または組織の信頼性を検証することです。
- サーバー証明書- 特定のドメイン名に関連付けられた証明書。ウェブサイトに有効な証明書がある場合、それはウェブ アドレスが実際にその組織に属していることを確認する手順を認証局が踏んでいることを意味します。URL を入力すると、ブラウザは証明書をチェックし、Web サイトのアドレスが証明書のアドレスと一致することを確認します。また、証明書が信頼できる認証局によって署名されていることも確認します。

  信頼されていない証明書を持つサーバーに接続する場合があります。Cloud NGFW for AWSは、サーバーが接続を終了したかのように接続を切断します。
- ルート**CA**証明書- 認証局はツリー構造の形式で複数の証明書を発行できます。ルート証明書はツリーの最上位の証明書です。

Cloud NGFW で使用するために AWS シークレットマネージャに証明書を追加する場合、次の前提条件を満たす必要があります。

- **private-key** と **public-key**の 2 つのキーを使用して、キーまたは値のペアとして追加された証明書。秘密鍵の場合、値は実際の鍵である必要があり、公開鍵の場合、値は実際の証明書本体である必要があります。
- キーが **PaloAltoCloudNGFW** で値が **true**のタグ。
- ルート CA 証明書と中間 CA 証明書をクライアントの信頼ストアにインポートします。

- トラフィックの復号化にエンドエンティティ証明書を使用している場合は、エンドエンティティ証明書（秘密鍵と公開鍵の両方）のみを AWS Secrets Manager に保存する必要があります。
- PKCS8シークレット形式がサポートされています。PKCS1シークレット形式はサポートされていません。

サポートされている PKCS 形式:

```
-----BEGIN プライベートキー----- -----END プライベートキー-----
```

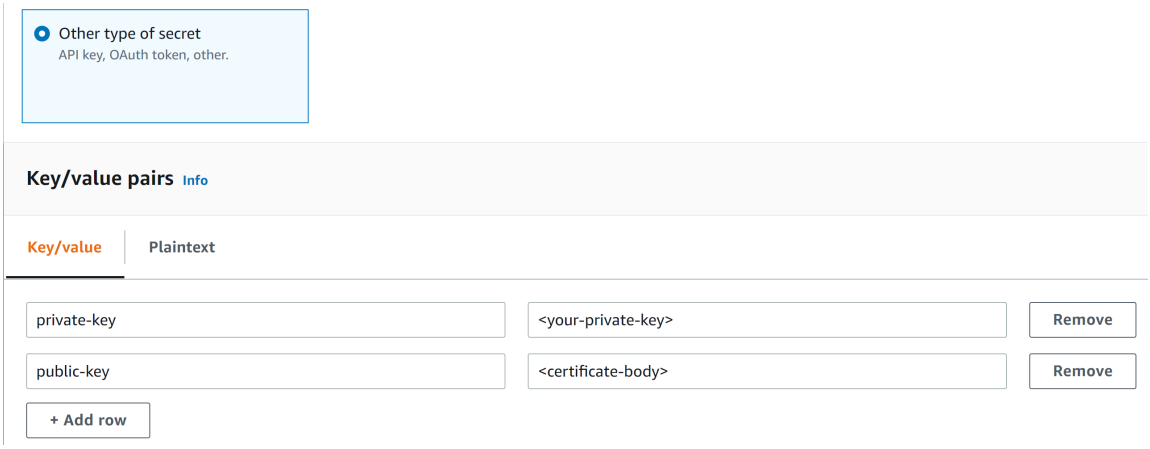
サポートされていない PKCS1 形式:

```
-----BEGIN RSA プライベートキー----- -----END RSA プライベートキー-----
```

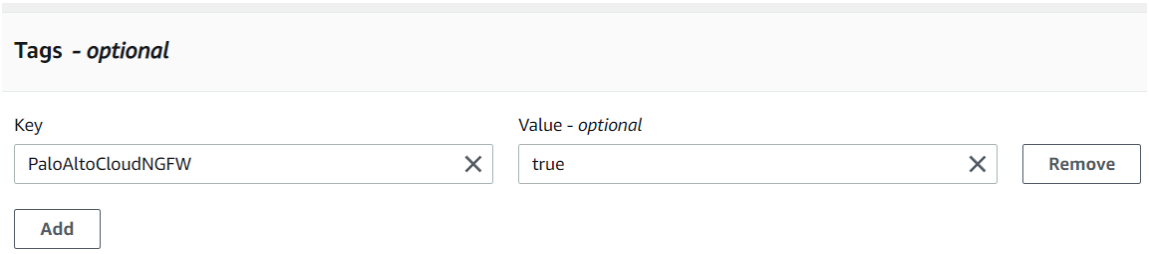
Cloud NGFW for AWS で使用する証明書を追加するには、次の手順を実行します。

STEP 1 | 証明書を AWSシークレットマネージャに追加します。

1. AWS コンソールにログインし、AWS シークレットマネージャに移動して、[**Store a new secret**]（新しいシークレットを保存）をクリックします。
2. **other type of secrets**（その他のタイプのシークレット）を選択します。
3. [キー/値のペア]で、**private-key** という名前のキーと **public-key**という名前の別のキーを作成します。
4. 対応するフィールドに秘密鍵全体と公開鍵全体を貼り付けます。



5. **Next**（次へ）をクリックします。
6. わかりやすいシークレット名を入力します。
7. キー **PaloAltoCloudNGFW** と値 **true**を持つタグを追加します。



8. [次へ]、[次へ]、[保存] の順にクリックして、 証明書の追加を完了します。

STEP 2 | **[**ルールスタック**]** を選択し、証明書を構成する前に作成したルールスタックを選択します。

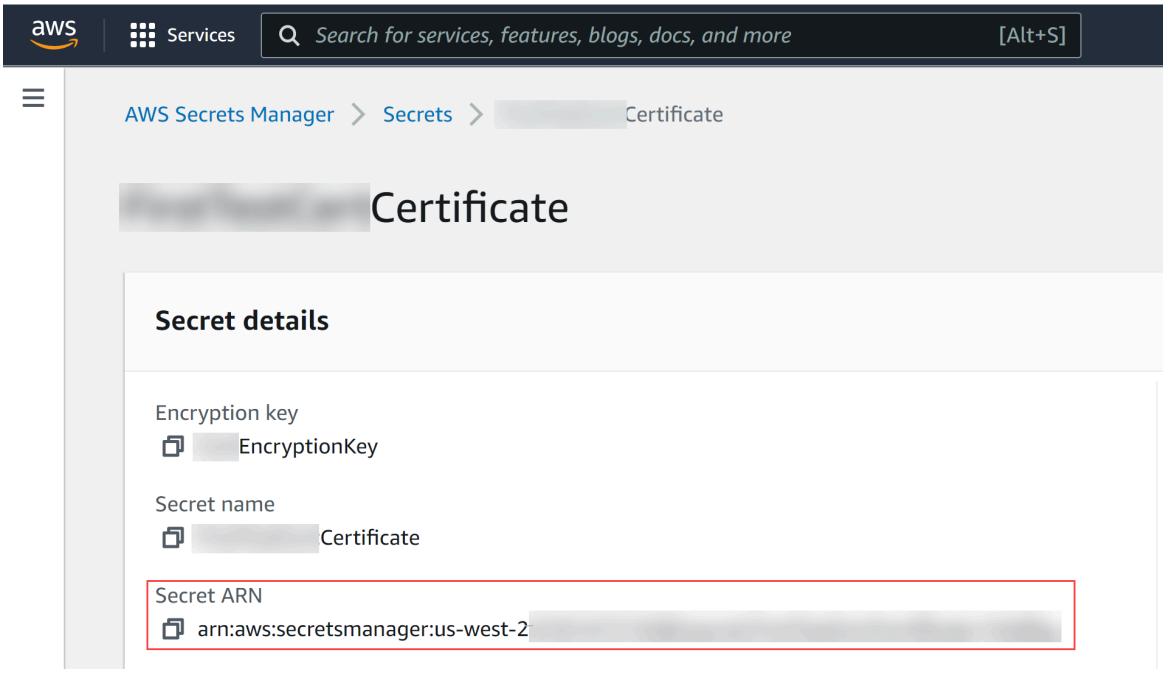
STEP 3 | ［オブジェクト］ > ［証明書リスト］ > ［証明書の追加］を選択します。

STEP 4 | 証明書にわかりやすい名前を入力します。

STEP 5 | （任意）証明書の説明を入力します。

STEP 6 | 証明書を選択します。

- Cloud NGFW で AWS シークレットマネージャから証明書をダウンロードする場合は、証明書 **ARN** を入力します。



- Cloud NGFW で自己署名証明書を作成する場合は、**[Self Signed Certificate (**自己署名証明書**)]**をオンにします。

STEP 7 | **[Save(**保存**)]**をクリックします。

Cloud NGFW on AWS の FQDN リストを作成する

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）

セキュリティールールオブジェクトは、IP アドレス、完全修飾ドメイン名（FQDN）、インテリジェントフィード、証明書などの個別の ID をグループ化する単一のオブジェクトまたは集合単位です。一般的にポリシー オブジェクトを作成する場合、ポリシーで同様のアクセス権限を必要とするオブジェクトをグループ化します。たとえば、組織でユーザーの認証にサーバー IP アドレスのセットを使用している場合、サーバー IP アドレスのセットをプレフィックスリストオブジェクトとしてグループ化し、そのプレフィックスリストを 1 つ以上のセキュリティルールで参照できます。グループオブジェクトを使用すると、ルールを作成する際の管理オーバーヘッドを大幅に削減できます。

ユーザーが IP アドレスを知り、FQDN が新しい IP アドレスに解決される度に手動で更新することなく、DNS が IP アドレスへの FQDN 解決を提供するため、使いやすいのが FQDN 型のアドレスオブジェクト（たとえば paloaltoneworks.com）です。

STEP 1 | ［ルールスタック**]** を選択し、FQDN リストを設定する、以前に作成したルールスタックを選択します。

STEP 2 | ［オブジェクト］ > ［**FQDN** リスト］ > ［**FQDN** の作成］を選択します。

STEP 3 | 画像のわかりやすい名前を入力します。

STEP 4 | （任意）FQDN リストの説明を入力します。

STEP 5 | 1 行に 1 つずつ、1 つ以上の **FQDN** を入力します。

STEP 6 | **[Save(**保存**)]**をクリックします。

Cloud NGFW for AWS のインテリジェントフィードを設定する

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）

セキュリティールールオブジェクトは、IP アドレス、完全修飾ドメイン名（FQDN）、インテリジェントフィード、証明書などの個別の ID をグループ化する単一のオブジェクトまたは集合単位です。一般的にポリシー オブジェクトを作成する場合、ポリシーで同様のアクセス権限を必要とするオブジェクトをグループ化します。たとえば、組織でユーザーの認証にサーバー IP アドレスのセットを使用している場合、サーバー IP アドレスのセットをプレフィックスリストオブジェクトとしてグループ化し、そのプレフィックスリストを 1 つ以上のセキュリティルールで参照できます。グループオブジェクトを使用すると、ルールを作成する際の管理オーバーヘッドを大幅に削減できます。

インテリジェントフィードは、外部動的リストとも呼ばれ、ユーザーまたはサードパーティが外部 Web サーバーでホストできるリストです。インテリジェンスフィードは、セキュリティルールのソースまたは宛先として指定できます。NGFW は、ホストされたリストを 1 時間ごとまたは 1 日ごとにチェックし、設定を変更することなく、リストの最新のエントリに基づいてセキュリティルールを適用します。

- インテリジェントフィード — 外部動的リスト（EDL）とも呼ばれるインテリジェントフィードは、組織のセキュリティに対する潜在的または現在の脅威に関連する継続的なデータストリームです。インテリジェントなフィードは、フィッシング詐欺、マルウェア、ボット、スパイウェア、ランサムウェアなどの脅威に関連する IP アドレスと URL を記録および追跡します。

  Cloud NGFW には、4 つの組み込みインテリジェントフィードが含まれています。

  - **Palo Alto Networks** バレットプルーフ **IP** アドレス—バレットプルーフ ホスティング プロバイダーが提供する IP アドレスが含まれます。バレットプルーフ ホスティング プロバイダーはコンテンツにほとんど (あるいは全く) 制約を設けないため、攻撃者は頻繁にこれらのサービスを使用して悪意のある、違法な、非倫理的なものをホストして配信します。
  - **Palo Alto Networks** 高リスク **IP** アドレス—信頼できるサードパーティの組織が発行した脅威アドバイザリーから得られる悪意のある IP アドレスを含みます。Palo Alto Networks は脅威アドバイザリーのリストに従いますが、それらの IP アドレスに悪意があるという証拠を直接持っているわけではありません。

- **Palo Alto Networks** 悪意のある既知の **IP** アドレス — WildFire 分析、Unit 42 リサーチ、テレメトリから収集されたデータに基づいて悪意があることが検証された IP アドレスを含みます。攻撃者はこれらの IP アドレスをほぼ独占的に使用してマルウェアを配布し、コマンド アンド コントロール アクティビティを開始し、攻撃を行います。
- **Palo Alto Networks Tor Exit IP** アドレス — 複数のプロバイダから提供され、Palo Alto Networks の脅威インテリジェンス データをアクティブな Tor 出口ノードとして検証した IP アドレスが含まれます。Tor 出口ノードからのトラフィックは正当な目的を果たすことができますが、特に企業環境では、悪意のあるアクティビティに不釣り合いに関連付けられます。

NGFW を Palo Alto Networks の組み込みインテリジェンスフィードやサードパーティのインテリジェントフィードに接続して、ネットワークへの脅威に関する最新情報を提供できます。接続で復号化証明書を指定する必要がある場合は、以下で説明する Cloud NGFW 証明書オブジェクトを使用するように Cloud NGFW を設定できます。

IP および URL リストの場合:

- **IP** リスト - ポリシールールの送信元または宛先アドレスオブジェクトとして IP アドレスタイプのインテリジェントフィードを使用して、アドホックに出現する送信元または宛先 IP アドレスのリストにポリシーを適用し、リストに含まれる IP アドレスへのアクセスを拒否または許可するように NGFW を設定します。NGFW は IP リストインテリジェントフィードをアドレスオブジェクトとして扱い、含まれるすべての IP アドレスは 1 つのアドレスオブジェクトとして処理されます。

  インテリジェントフィードは、個々のIPアドレス、サブネットアドレス（アドレス/マスク）、または IP アドレスの範囲を含むことができます。また、コメントや特殊文字も指定できます。例: *, :, ;, #、または /。リスト内の各行の構文は次のとおりです。**`[IP address, IP/Mask, or IP start range-IP end range] [space] [comment]`**

  1 行に 1 つの IP アドレス、IP 範囲、または IP サブネットを指定します。URL あるいはドメインは指定できません。「92.168.20.0/24」、「192.168.20.40-192.168.20.50」など、サブネットや IP アドレス範囲は 1 つの IP アドレス エントリとしてカウントされ、複数の IP アドレスとしてはカウントされません。コメントを追加する場合は、IP アドレス、IP 範囲、または IP サブネットと同じ行に指定する必要があります。IP アドレスの末尾のスペースは、IP アドレスとコメントを分ける区切り文字です

  IPアドレス リストの例：

  ```
  192.168.20.10/32 2001:db8:123:1::1 #test IPv6アドレス
   192.168.20.0/24 ;テスト内部サブネット 2001:db8:123:1::/64 内部 IPv6 範囲 192.168.20.40-192.168.20.50 をテストする
  ```

- **URL** リスト - URL を使用して、脅威やマルウェアの新しいソースからネットワークを保護します。NGFW は、カスタム URL カテゴリのような URL を持つインテリジェントフィードを処理します。URL リストのフォーマットの詳細については、AWSのクラウドNGFW高度なURLフィルタリングを参照してください。

NGFW では、インテリジェントフィードにアクセスするために証明書オブジェクトが必要です。詳細については、Cloud NGFW for AWS に証明書を追加するを参照してください。

STEP 1 | ［ルールスタック］を選択し、ファイルブロックを設定するために以前に作成したルールスタックを選択します。

STEP 2 | **[**オブジェクト］ > ［インテリジェントフィード**]** > ［インテリジェントフィードの作成］を選択します。

STEP 3 | インテリジェントフィードのわかりやすい名前を入力します。

STEP 4 | （任意）インテリジェントフィードの説明を入力します。

STEP 5 | インテリジェントフィードのタイプを選択します。

STEP 6 | ソース **URL**を入力します。

STEP 7 | 証明書プロファイルを設定します。

STEP 8 | 更新頻度（時間または日）を設定します。

STEP 9 | **[Save(**保存**)]**をクリックします。

Cloud NGFW for AWS でセキュリティルールを作成する

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）

セキュリティルールは、ネットワーク資産を脅威や障害から保護し、ネットワークリソースを最適に割り当てることで、ビジネスプロセスの生産性と効率性を向上させるのに役立ちます。Cloud NGFW for AWS では、送信元と宛先の IP アドレス、送信元と宛先の FQDN、またはアプリケーション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。

ファイアウォールを通過するすべてのトラフィックはセッションと照合され、各セッションはルールと照合されます。セッションが一致すると、NGFW は一致するルールをそのセッション（クライアントからサーバー、およびサーバーからクライアント）の双方向トラフィックに適

用します。定義されたルールに一致しないトラフィックには、デフォルトのルールが適用されます。

セキュリティ ポリシー ルールは、左から右に、および上から下の順に評価されます。定義済みの基準を満たす最初のルールとパケットが一致すると、それが引き金となり、それ以降のルールは評価されません。そのため、ベストマッチする基準を適用するには、個別のルールを一般的なルールよりも優先的に評価する必要があります。

ルールスタックを作成したら、ルールを作成してルールスタックに追加できます。

［ルールスタック］ > **<rulestack-name>** > ［セキュリティルール］ > **<rule-name>** > ［使用状況］に移動すると、トラフィックが特定のルールに一致した回数を表示できます。**[**使用状況**]**タブには、疑わしいルールが NGFW を通過するトラフィックによってトリガーされた回数が表示されます。ヒットカウンターは 15 秒ごとに更新されます。

さらに、［**NGFW**］ > **<firewall-name>** > ［ルール］ > **<rule-name>**を選択して、ルールヒットカウンターを表示できます。NGFW メニューからヒットカウンターを表示すると、ヒットカウンターは、選択したルールがその特定の NGFW でトリガーされた回数を示します。

STEP 1 | ［管理］ > ［ルールスタック］を選択し、新しいルールのターゲットルールスタックを選択します。

STEP 2 | ［新規作成］をクリックします。ルールをグローバル ルールスタックに追加する場合は、［事前ルール］また［事後ルール］を選択する必要があります。

STEP 3 | ルールにわかりやすい名前を入力します。

STEP 4 | （任意）ロールの説明を入力します。

STEP 5 | ルールの優先度を設定します。

ルールの優先度は、ルールが評価される順序を決定します。優先度の低いルールが最初に評価されます。さらに、ルールスタック内の各ルール。

STEP 6 | デフォルトでは、セキュリティ ルールは有効です。ルールを無効にするには、［有効］のチェックを外します。ルールはいつでも有効または無効にできます。

STEP 7 | ソースを設定します。

1. ［任意**]**または［一致**]**を選択します。

   ［任意］を選択すると、送信元に関係なく、トラフィックがルールに対して評価されます。

2. ［一致］を選択した場合は、追加アイコン（ ）少なくとも 1 つのソースオブジェクト（IP アドレス（CIDR）、プレフィックスリスト、国、またはインテリジェントフィード（IP タイプ）を指定します。

STEP 8 | 宛先を設定します。

1. ［任意]または［一致]を選択します。

   ［任意］を選択すると、宛先に関係なくトラフィックがルールに対して評価されます。

2. ［一致］を選択した場合は、追加アイコン（+ ⌄）を入力し、少なくとも 1 つの宛先オブジェクト（IP アドレス（CIDR）、プレフィックスリスト、FQDN リスト、国、またはインテリジェントフィード（IP タイプ）を指定します。

STEP 9 | アプリケーション（**App-ID**）の詳細な制御を設定します。

1. ［任意]または[選択］を選択します。

   ［任意］を選択すると、トラフィックはアプリケーションに関係なく評価されます。アプリケーションを指定することにより、トラフィックが指定されたアプリケーションと一致する場合、トラフィックはルールに対して評価されます。

2. [選択]を選択した場合は、追加アイコン（+ −）をクリックし、アプリケーションを指定します。

STEP 10 | **URL** カテゴリの詳細な制御を設定します。

1. ［任意］または［一致］を選択します。

   ［任意］を選択すると、トラフィックは URL に関係なく評価されます。アプリケーションを指定することにより、トラフィックが指定された URL カテゴリまたはインテリジェントフィード（URL タイプ）に一致する場合、トラフィックはルールに対して評価されます。

2. ［一致］を選択した場合は、［**URLCategoryNames**］または［フィード］を選択し、追加アイコン（+ ⌄ −）をクリックします。ドロップダウンから、URL カテゴリまたはインテリジェントフィードを選択します。

STEP 11 | ポートとプロトコルの詳細な制御を設定します。

1. **application-default**、［任意］または［選択］を選択します。

   ［任意］を選択すると、トラフィックはポートとプロトコルに関係なく評価されます。ポートとプロトコルを指定することにより、トラフィックが指定されたポートとプロトコルに一致する場合、トラフィックはルールに対して評価されます。

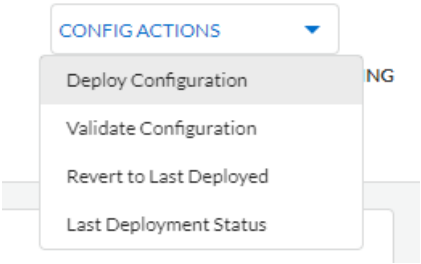
2. [選択]を選択した場合は、ドロップダウンからプロトコルを選択し、ポート番号を入力します。単一のポート番号を指定するか、コンマを使用して複数のポートを指定できます。以下に例を示します。80、8080。

STEP 12 | アクションを設定します。

1. トラフィックがルールに一致した場合にファイアウォールが実行するアクションを設定します（**[**許可**]**、［拒否］、［サーバーのリセット**]**、または**[**クライアントとサーバーの両方をリセット**]**）。
2. アウトバウンド **TLS** 復号化を有効にします。
3. ロギングを有効にします。

STEP 13 | 作成をクリックします。

STEP 14 | ルールスタックのルールを作成したら、設定を検証またはデプロイします。



Cloud NGFW for AWS セキュリティプロファイル

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）

Cloud NGFW は、ルールスタック定義を使用して、2 段階のプロセスで VPC トラフィックを保護します。まず、トラフィックを許可または拒否するルールを適用します。次に、セキュリティプロファイルで指定した内容に基づいて、許可されたトラフィック（URL、脅威、ファイル）に対してコンテンツインスペクションを実行します。さらに、Cloud NGFW が許可されたトラフィックをスキャンし、マルウェア、スパイウェア、DDOS 攻撃などの脅威をブロックする方法を定義するのに役立ちます。

IPS とスパイウェアの脅威からの保護

- **IPS** 脆弱性 — （デフォルトで有効になっており、ベストプラクティスに基づいて事前構成されています）侵入防止システム（IPS）脆弱性プロファイルは、システムの欠陥を悪用したり、システムへの不正アクセスを取得したりする試みを阻止します。アンチスパイウェアプロファイルは、トラフィックがネットワークから離れる際に感染したホストを特定するのに

役立ち、IPS 脆弱性プロファイルは、ネットワークに侵入する脅威から保護します。この機能は、たとえば、バッファ オーバーフロー、不正なコード実行、およびシステムの脆弱性を悪用するその他の試みからシステムを防御します。デフォルトの脆弱性防御プロファイルでは、重大度が「critical」、「high」、および「medium」のすべての既知の脅威からクライアントとサーバーを保護します。

以下の表は、デフォルトのベストプラクティスIPS脆弱性構成を示しています。

シグネチャの重大度	操作
極めて重大	Reset Both [両方のリセット]
高	Reset Both [両方のリセット]
中	Reset Both [両方のリセット]
情報	デフォルト
低	デフォルト

- アンチスパイウェア —（デフォルトで有効、ベストプラクティスに基づいて事前構成されています) アンチスパイウェアプロファイルは、侵害されたホスト上のスパイウェアが、外部のコマンドアンドコントロール（C2）サーバーに電話発信またはビーコン送信しようとするのをブロックします。感染したクライアントからネットワークを離れる悪意のあるトラフィック。

  以下の表は、デフォルトのベストプラクティスのアンチスパイウェア設定を示しています。

シグネチャの重大度	操作
極めて重大	Reset Both [両方のリセット]
高	Reset Both [両方のリセット]
中	Reset Both [両方のリセット]
情報	デフォルト

シグネチャの重大度	操作
低	デフォルト

次の表に、脆弱性とスパイウェアのカテゴリで考えられるすべてのシグネチャを示します。これらの署名は、NGFW で継続的に更新されます。

脅威カテゴリ	詳説
脆弱性シグネチャ	
ブルートフォース	ブルート フォース シグネチャは、一定期間に繰り返し生じる事象を検出します。正当なアクティビティが隔離される可能性もありますが、ブルート フォース シグネチャはアクティビティの正当性が疑わしくなるような頻度を示唆します。例えば、FTP ログインが一度失敗しても、悪意のあるアクティビティにはなりません。しかし、短期間に FTP ログインが多く失敗した場合、攻撃者が FTP サーバーへのアクセスを求めて組み合わせを変えながらパスワードを試していることが示唆されます。
code execution	攻撃者がログインしたユーザーの権限を使用してシステム上でコードを実行するために使用できるコード実行の脆弱性を検出します。
code-obfuscation	機能を維持したまま特定のデータを隠蔽するよう変更されたコードを検出します。難読化されたコードは読みづらい、あるいは判読不可能であるため、どのようなコマンドをコードが実行しているのか、どのプログラムとやり取りするよう設計されているのかをすぐに把握できません。最も多いのは、攻撃者がコードを難読化してマルウェアを隠蔽することです。それより頻度は落ちますが、プライバシー、知的財

脅威カテゴリ	詳説
	産を保護する、あるいはユーザーエクスペリエンスを向上させるために、正当な開発者がコードを難読化することもあります。例えば、ファイル サイズを減らしてウェブサイトの読み込み時間と帯域幅の消費量を減らす特定の難読化（ミニマイズ）があります。
Dos	攻撃者が目標のシステムを利用不可能にし、一時的にシステムおよびそれに従属するアプリケーションおよびサービスを中断させる、サービス拒否攻撃を検出します。DoS 攻撃を行うために、攻撃者は目標のシステムに大量のトラフィックを送ったり、エラーを発生させる情報を送信したりします。DoS 攻撃は、サービスの正当なユーザー（従業員、会員、アカウント所有者など）やユーザーがアクセスできるリソースなどを奪います。
exploit-kit	エクスプロイトキットのランディングページを検出します。エクスプロイトキットのランディングページには、複数のブラウザおよびプラグインに関して、一つあるいは多くの共通脆弱性識別子（CVE）をターゲットにする複数のエクスプロイトが含まれていることが多くあります。目標の CVE はすぐに変化するため、エクスプロイトキット シグネチャは CVE ではなくエクスプロイトキットのランディングページに基づいて発動します。 エクスプロイトキットを含むウェブサイトにユーザーがアクセスする際、エクスプロイトキットは目標の CVE をスキャンし、被害者のコンピューターに悪意のあるペイロードを密かに送り込もうとします。
info-leak	攻撃者がエクスプロイトしてセンシティブあるいは占有情報を盗む可能性があるソフトウェアの脆弱性を検出します。通常、データを保護する包括的なチェックは存在しないため、情報流出が発生する可能性があり、攻撃者は巧妙な要求を送信して情報流出をエクスプロイトできます。
insecure-credentials	ソフトウェア、ネットワークアプライアンス、および IoT デバイスの脆弱な、侵害された、製造元のデフォルトのパスワードの使用を検出します。
オーバーフロー	リクエストのチェックが不適切であり、攻撃者がエクスプロイトする可能性があるオーバーフローの脆弱性を検出します。攻撃が成功すると、アプリケーション、サーバー、あるいはオペレーティングシステムの権限でリモートからコードを実行できる可能性があります。
phishing	ユーザーがフィッシング キットのランディングページに接続しようとしているのを検出します（悪意のあるサイトへのリンクが記載され

脅威カテゴリ	詳説
	たメールの受信後が多い）。フィッシング サイトは、ユーザーをだまして認証情報を送信させ、攻撃者がその情報を盗んでネットワークへのアクセスを得られるようにします。
protocol-anomaly	プロトコルの挙動が通常の適切な用途から外れる、プロトコルの異常を検出します。例えば、不正な形式のパケット、プログラムが不適切なアプリケーション、標準的でないポート上で実行されているアプリケーションはすべて、異常なプロトコルとみなされ、回避ツールとして使用される可能性があります。
SQLインジェクション	攻撃者が SQL クエリをアプリケーションのリクエストに含め、データベースからデータを読み取る、あるいはデータを変更する、よくあるハッキング技術を検出します。このタイプのテクニックは、ユーザーの入力情報のサニタイズが不十分なウェブサイトに対してよく利用されます。
スパイウェア シグネチャ	
スパイウェア	アウトバウンド C2 通信を検出します。これらのシグネチャは自動生成されるか、Palo Alto Networks の調査員が手作業で作成します。 スパイウェアおよび自動生成シグネチャの両方がアウトバウンド *C2* 通信を検出しますが、自動生成シグネチャはペイロード ベースであり、未知、あるいは急速に変化する *C2* ホストとの *C2* 通信を一意に検出できます。
［Adware］	好ましくない広告を表示するおそれのあるプログラムを検出します。一部のアドウェアはブラウザに変更を加え、頻繁に検索されるキーワードを Web ページ上でハイライト表示し、ハイパーリンクを付与します。これらのリンクは、ユーザーを広告サイトにリダイレクトさせます。また、アドウェアはコマンド アンド コントロール（C2）サーバーからアップデートを取得し、それをブラウザやクライアント システムにインストールすることもできます。
autogen	このペイロード ベースのシグネチャは、コマンド アンド コントロール（C2）トラフィックを検出し、自動生成されます。自動生成されたシグネチャは C2 ホストが未知である場合、あるいは急速に変化する場合でも C2 トラフィックを検出できるというのが重要です。

脅威カテゴリ	詳説
バックドア	攻撃者がシステムへの不正なリモートアクセスを得られるようにするプログラムを検出します。
ボットネット	ボットネット アクティビティを示します。ボットネットとは、攻撃者が制御する、マルウェアに感染したコンピューター（ボット）のネットワークのことです。攻撃者はボットネットの全コンピューターに一元的に命令を出し、同時に一斉にアクション（例えば DoS 攻撃などを行う）を実行させます。
browser-hijack	ブラウザ設定を変更しているプラグインやソフトウェアを検出します。ブラウザを乗っ取った攻撃者は、自動検索をコントロールしたり、ユーザーのウェブ アクティビティを追跡したり、その情報を C2 サーバーに送信したりする可能性があります。
クリプトマイナー	(クリプトジャッキングまたはマイナーと呼ばれることもあります) ユーザーの知らないうちにコンピューティング リソースを使用して暗号通貨をマイニングするように設計された悪意のあるプログラムから生成されたダウンロードの試行またはネットワーク トラフィックを検出します。クリプトマイナー バイナリは、システム アーキテクチャを決定し、システム上の他のマイナー プロセスを強制終了しようとするシェル スクリプト ダウンローダーによって頻繁に配信されます。一部のマイナーは、悪意のある Web ページをレンダリングする Web ブラウザなど、他のプロセス内で実行します。
data-theft	情報を既知の C2 サーバーに送信しているシステムを検出します。
DNS	悪意のあるドメインに接続するための DNS リクエストを検出します。
ダウンローダー	（ドロッパー、ステージャー、ローダーとも呼ばれる） インターネット接続を使用してリモート サーバーに接続し、侵入先のシステムにマルウェアをダウンロードして実行するプログラムを検出します。最も一般的な使用例は、ダウンローダーがサイバー攻撃のステージ*1*の集大成として展開されることであり、ダウンローダーのフェッチされたペイロードの実行は、ステージ*2*と見なされます。シェル スクリプト (Bash、PowerShell など)、トロイの木馬、および PDFや Word ファイルなどの悪意のあるルアー ドキュメント (maldocs とも呼ばれます) は、一般的なダウンローダータイプです。
詐欺行為	(フォームジャッキング、フィッシング、詐欺を含む) ユーザーの機密情報を収集するために悪意のある JavaScript コードが挿入されている

脅威カテゴリ	詳説
	と判断された侵害された Web サイトへのアクセスを検出します。(例: 名前、住所、電子メール、クレジットカード番号、CVV、有効期限) を、電子商取引 Web サイトのチェックアウト ページでキャプチャされた支払いフォームから取得します。
hacktool	悪意のある攻撃者が偵察を行ったり、脆弱なシステムを攻撃またはアクセスしたり、データを盗み出したり、コマンドと制御チャネルを作成して許可なくコンピュー タシステムを密かに制御したりする目的でソフトウェア ツールを用いて生成したトラフィックを検出します。これらのプログラムはマルウェアやサイバー攻撃に関連しています。ハッキング ツールは、Red team および Blue team の運用、侵入テスト、ならびに R&D で使用される場合、良識ある方法で展開される可能性があります。これらのツールの使用または所持は、意図に関係なく、一部の国では違法である可能性があります。
networm	自己増殖し、システムからシステムへと広がるプログラムを検出します。ネットワームは、共有リソースを使用し、あるいはセキュリティの不備を利用して目標のシステムにアクセスする可能性があります。
phishing-kit	ユーザーがフィッシング キットのランディングページに接続しようとしているのを検出します（悪意のあるサイトへのリンクが記載されたメールの受信後が多い）。フィッシング サイトは、ユーザーをだまして認証情報を送信させ、攻撃者がその情報を盗んでネットワークへのアクセスを得られるようにします。
データ窃取被害後	攻撃者が侵入したシステムの価値を評価しようとするエクスプロイト後の段階を示唆するアクティビティを検出します。これには、システムに保存されているデータの重要性、さらにネットワークに侵入する上でそのシステムがどの程度重要かを評価することが含まれます。
Webshell	インプラントの検出やコマンドと制御の相互通信など、Web シェルと Web シェル トラフィックを検出します。悪意のある攻撃者は、侵害されたホストに Web Shellを埋め込み、ほとんどの場合、Webサーバーまたはフレームワークをターゲットにします。その後のWebシェルファイルとの通信により、悪意のある攻撃者がシステムに足場を確立し、Webサーバーユーザーのコンテキストでサービスとネットワークの列挙、データの漏えい、およびリモートコード実行を行うことができます。最も一般的な Web シェル タイプは、PHP、.NET、および Perl マークアップ スクリプトです。また、攻撃者はウェブシェルに感染した Web サーバー（インターネットに接続されたサーバー、内部

脅威カテゴリ	詳説
	システムの両方）を利用し、その他の内部システムもターゲットにします。
Keylogger	攻撃者がキー操作を記録し、スクリーンショットを撮影してユーザー アクティビティを密かに追跡できるようにするプログラムを検出します。 キーロガーは様々な C2 手法を使用し、定期的にログおよびレポートを事前定義済みのメールアドレスあるいは C2 サーバーに送信します。キーロガーによる監視を通じて、攻撃者がネットワーク アクセスを可能にする認証情報を入手する可能性もあります。

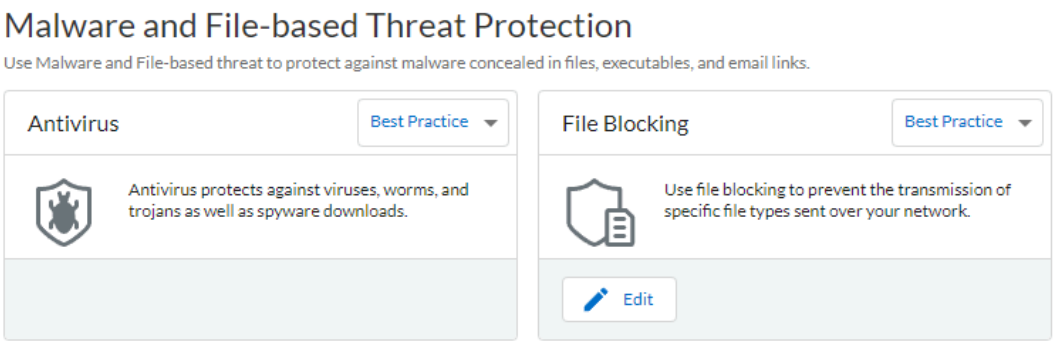
マルウェアおよびファイルベースの脅威からの保護

- アンチウイルス — （既定で有効になっており、ベストプラクティスに基づいて事前構成されています）ウイルス対策プロファイルは、マルウェア、ワーム、トロイの木馬、およびスパイウェアのダウンロードから保護します。Palo Alto Networks アンチウイルス ソリューションでは、パケットを最初に受信する瞬間にトラフィックを検査するストリームベースのマルウェア防御エンジンを使用して、ファイアウォールのパフォーマンスに大きな影響を与えることなくクライアントを保護することができます。このプロファイルは、実行ファイル、PDF ファイル、HTML、および JavaScriptマルウェアに含まれるさまざまなマルウェアをスキャンします。また、圧縮ファイルとデータ エンコード スキームの内部スキャンもサポートしています。

  以下の表は、デフォルトのベストプラクティスのアンチウイルス設定を示しています。

PROTOCOL	操作
FTP	Reset Both [両方のリセット]
HTTP	Reset Both [両方のリセット]
HTTP2	Reset Both [両方のリセット]
IMAP	Reset Both [両方のリセット]
POP3	アラート
SMB	Reset Both [両方のリセット]
SMTP	Reset Both [両方のリセット]

- ファイルブロッキング - ファイルブロッキングプロファイルは、ブロックまたは監視する特定のファイルタイプを識別することができます。ファイアウォールは、ファイルブロッキングプロファイルを使用して、特定のアプリケーション上および特定のセッションフロー方向（インバウンド/アウトバウンド/両方）で、特定のファイルタイプをブロックします。アップロードまたはダウンロードでアラート送信またはブロックするプロファイルを設定し、ファイル ブロッキング プロファイルの適用対象となるアプリケーションを指定できます。
  - **Alert** - 指定したファイルタイプが検出されると、データフィルタリングログでログが生成されます。
  - ブロック - 指定したファイルタイプが検出されると、ファイルがブロックされます。データ フィルタリング ログでログも生成されます。ファイル ブロック プロファイルの変更については、「ファイル ブロックのセットアップ」を参照してください。



以下の表は、デフォルトのベストプラクティス ファイル ブロック設定を示しています。

ファイル タイプ	アプリケーション	方向	操作
すべての危険なファイルタイプ: • 7z • bat • cab • chm • class • CPL • DLL • exe • flash • hip	任意	アップロードとダウンロードの両方	ブロック

ファイル タイプ	アプリケーション	方向	操作
• hta • msi • マルチレベルエンコーディング • ocx • PE • pif • rar • scr • tar • torrent • vbe • wsf • 暗号化rar • 暗号化zip			
残りのすべてのファイルタイプ	任意	アップロードとダウンロードの両方	アラート

次の表に、アンチウイルスカテゴリで使用可能なすべてのシグネチャを示します。これらの署名は、NGFW で継続的に更新されます。

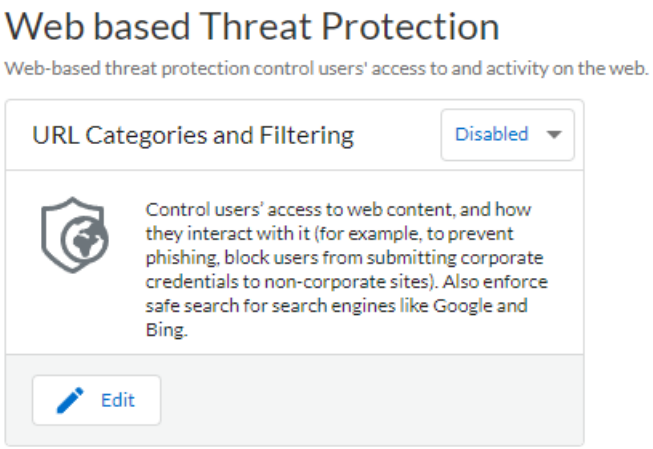
脅威カテゴリ	詳説
アンチウイルス シグネチャ	
APK	悪意のある Android Application（APK）ファイル。
Mac OS X	悪意のある Mac OS X ファイルには以下が含まれます: • Apple ディスク イメージ (DMG) ファイル • Machオブジェクトファイル(Mach-O)は、実行可能ファイル、ライブラリ、およびオブジェクトコード • Apple ソフトウェア インストーラー パッケージ (PKG)
Flash	Web ページに組み込まれている Adobe Flashアプレットおよびコンテンツ

脅威カテゴリ	詳説
jar	Java アプレット（JAR/クラス ファイル タイプ）。
ms-office	ドキュメント（DOC、DOCX、RTF）、ワークブック（XLS、XLSX）、PowerPoint プレゼンテーション（PPT、PPTX）を含む Microsoft Office ファイル。これには、Office Open XML (OOXML) 2007+ ドキュメントも含まれます。
pdf	ポータブルドキュメントフォーマット（PDF）ファイル。
PE	Portable executable（PE）ファイルは Microsoft Windows システムで自動的に実行され、身元が確認できる場合のみ許可できます。これには次のようなファイル形式があります： • オブジェクトコード。 • フォント（FON）。 • システムファイル（SYS）。 • ドライバーファイル（DRV）。 • Windows コントロールパネルのアイテム（CPL）。 • DLL（ダイナミック リンク ライブラリ）。 • OCX（OLE カスタムコントロール、あるいは ActiveX コントロール用ライブラリ）。 • Windows スクリーンセーバー ファイル (SCR)。 • デバイスの更新および起動操作をサポートする、OS およびファームウェアの間で実行される Extensible Firmware Interface（EFI）ファイル。 • プログラム情報ファイル（PIF）。
linux	実行可能およびリンク可能な形式（ELF）ファイル。
アーカイブ	Roshalアーカイブ（RAR）と7-Zip（7z）アーカイブファイル。

Web ベースの脅威対策

- **URL** フィルタリングとプロファイル - URL フィルタリングプロファイルは、ユーザーが HTTP および HTTPS で Web にアクセスする方法を監視および制御することができます。ファイアウォールには、既知のマルウェア サイト、フィッシング サイト、アダルト コンテンツ サイトなどの Web サイトをブロックするように設定されているデフォルト プロファイルが付属しています。URL フィルタリングプロファイルは、デフォルトでは有効になっていません。ルールスタックで URL フィルタリングプロファイルを有効にすると、Cloud NGFW はベ

ストプラクティスの URL フィルタリングプロファイルをトラフィックに適用します。必要に応じて、各カテゴリのデフォルトアクセスオプションを変更するオプションがあります。



以下の表は、デフォルトのベストプラクティスURLフィルタリング構成を示しています。

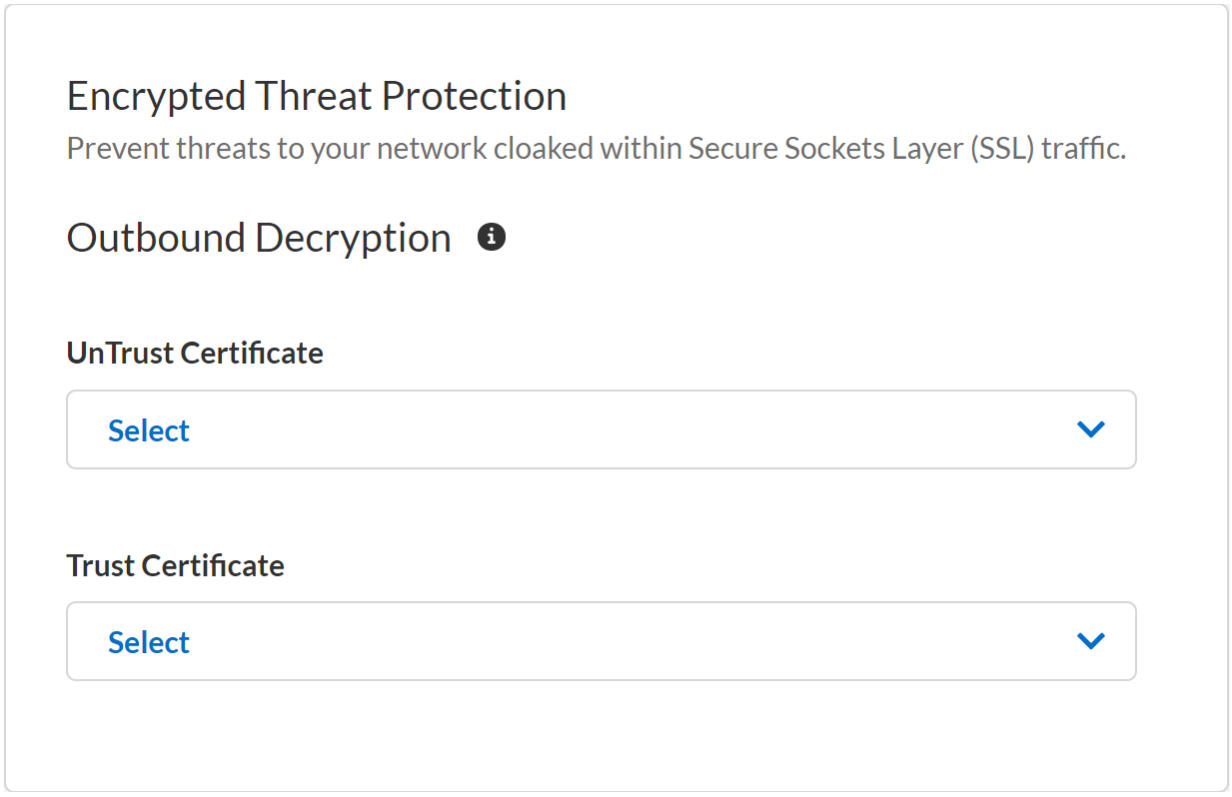
URL カテゴリ	サイト アクセス	資格証明書の提出
悪意のある、搾取的なカテゴリ: • 成人向け • コマンドアンドコントロール • 著作権侵害 • ダイナミックDNS • 過激主義 • マルウェア • パーク • phishing • プロキシ回避とアノニマイザ • unknown	ブロック	ブロック
その他すべてのURLカテゴリ	アラート	アラート

暗号化された脅威からの保護

- アウトバウンド復号化 — アウトバウンド復号化ポリシーでは、宛先、送信元、サービス、URL のカテゴリごとに復号化するトラフィックを指定し、関連する復号化プロファイルのセキュリティ設定に従って、指定したトラフィックをブロック、制限、転送することができます。アウトバウンド復号化プロファイルは、SSL プロトコル、証明書の検証、エラーチェックを制御し、弱いアルゴリズムやサポートされていないモードを使用するトラフィッ

クがネットワークにアクセスするのを防ぎます。Cloud NGFW リソースは証明書を使用してトラフィックをプレーンテキストに復号化します。次に、復号化、アンチウイルス、脆弱性、アンチスパイウェア、URLフィルタリング、ファイル ブロック プロファイルを含むApp-IDとセキュリティ プロファイルをプレーンテキスト トラフィックに適用します。トラフィックの復号化と検査を行った後、プレーンテキスト トラフィックはファイアウォールを出る

ときにファイアウォールによって再暗号化され、プライバシーとセキュリティが確保されます。



Cloud NGFW for AWS の定義済み URL カテゴリ

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）

次の表では、AWS 上の Cloud NGFW で使用できる定義済みの URL カテゴリについて説明します。これらのカテゴリをセキュリティルールで使用して、それらに分類される Web サイトへのアクセスをブロックまたは許可することができます。

URL カテゴリ	詳説
リスクカテゴリ	
高リスク	以前に悪意のあるサイトであることが確認されたが、少なくとも 30 日間は無害なアクティビティを表示しているサイト。防弾 ISP でホストされているサイト、または既知の悪意のあるコンテンツを含む ASN からの IP を使用しているサイト。既知の悪意のあるサイトとドメインを共有するサイト。「不明」カテゴリのすべてのサイトは高リスクになります。
中リスク	悪意のあるサイトであることが確認されたが、少なくとも 60 日間は無害なアクティビティを表示しているサイト。「オンラインストレージとバックアップ」カテゴリのすべてのサイトは、デフォルトで中程度のリスクになります。
低リスク	高リスクまたは中リスクではないサイト。これには、以前に悪意のあるサイトとして確認されたが、少なくとも 90 日間は無害なアクティビティを表示しているサイトが含まれます。
脅威カテゴリ	

URL カテゴリ	詳説
コマンドと制御	マルウェアや感染したホストが、密かに攻撃者のリモートサーバーと通信を行って悪意のあるコマンドを受信したりデータを盗んだりするために使用する、コマンドアンドコントロール URL およびドメイン。
マルウェア	マルウェアをホストしていることが分かっている、あるいはコマンドアンドコントロール（C2）トラフィックに使用されているサイト。エクスプロイトキットを使用する場合もあります。
脅威の隣接カテゴリ	
ダイナミックDNS	マルウェアのペイロードや C2 トラフィックの配信によく使われる、IP アドレスが動的に割り当てられるシステムのホスト名とドメイン名。また、動的DNSドメインは、信頼できるドメイン登録業者が登録したドメインとは違う検査プロセスを経ているため、信頼度が低くなります。
グレイウェア	直接的なセキュリティ上の脅威にはならないが、その他の目障りな動作を表示し、エンドユーザーにリモートアクセスの許可やその他の許可されていない操作の実行を促す Web コンテンツ。グレイウェアには、違法行為、犯罪行為、ローグウェア、アドウェア、その他、埋め込み型暗号マイナー、クリックジャック、ブラウザの要素を変更するハイジャッカーなどの不要なアプリケーションや未承認のアプリケーションが含まれます。悪質性を示さず、対象となるドメインが所有しないタイポスクワッティングドメインは、グレイウェアに分類されます。
ハッキング	通信機器・ソフトウェアへの違法または疑わしいアクセスまたは使用に関連するサイト。ネットワークやシステムの侵害につながる可能性のあるプログラム、ハウツー、ヒントを開発・配布すること。また、ライセンスとデジタル著作権システムのバイパスを容易にするサイトも含まれます。
フィッシング	これには、ログイン認証情報、クレジットカード情報（自発的または不本意な情報）、アカウント番号、PIN、およびソーシャルエンジニアリング技術を介して被害者から個人を特定できる情報（PII）と見なされる情報を含む、情報を収集するためにユーザーをだまそうとす

URL カテゴリ	詳説
	るWebコンテンツが含まれます。テクニカルサポート詐欺やスケアウェアもフィッシングとして含まれています。
疑わしい	
コンテンツが不十分	テストページを表示したり、コンテンツを表示しなかったり、エンドユーザが表示することを意図していない API アクセスを提供したり、別の分類を示唆している他のコンテンツを表示せずに認証を要求したりするウェブサイトやサービス。このカテゴリには、WebベースのVPNソリューション、Webベースのメールサービス、特定された認証情報のフィッシングページなど、リモートアクセスを提供するWebサイトを含めるべきではありません。
ドメインの新規登録	新しく登録されたドメインは、意図的にまたはドメイン生成アルゴリズムによってしばしば生成され、悪意のある活動に使用されます。
駐車	個人によって登録されたドメインであり、後に認証情報を盗むフィッシングに使用されていることが分かることがあります。フィッシングにより認証情報や個人のID情報を盗むために用意されたこれらのドメインは、正当なドメインに似通っている場合があります（例：pal0alto0netw0rks.com）。あるいはpanw.netなど、いつか価値が出ると期待させて不当な個人購入を行わせるドメインもあります。
プロキシ回避とアノニマイザ	コンテンツフィルター製品をバイパスするためによく使用されるURLとサービス。
未知	Palo Alto Networks によってまだ識別されていないサイトです。可用性がビジネスにとって重要であり、トラフィックを許可し、未知のサイトに警告し、トラフィックにベストプラクティスセキュリティプロファイルを適用し、アラートを調査する必要がある場合。
法律/ポリシー	
妊娠中絶	中絶に賛成または反対する情報またはグループに関連するサイト、中絶手順に関する詳細、中絶に賛成または反対するフォーラムの支援または支援、または中絶を追求

URL カテゴリ	詳説
	する（またはしない）結果/効果に関する情報を提供するサイト。
薬物乱用	合法薬物と違法薬物の乱用、薬物関連器具の使用と販売、薬物の製造および/または販売を促進するサイト。
adult	性的に露骨な素材、メディア（言語を含む）、アート、および/または製品、本質的に性的に露骨なオンライングループまたはフォーラム。テレビ/電話会議、エスコートサービス、ストリップクラブなどのアダルトサービスを宣伝するサイトアダルト コンテンツを含むもの（ゲームやコミックであっても）は、アダルト コンテンツとして分類されます。
アルコールとタバコ	アルコールおよび/またはタバコ製品および関連器具の販売、製造、または使用に関連するサイト。電子タバコに関連するサイトが含まれています。
オークション	個人間の商品販売を促進するサイト。
ビジネスと経済	マーケティング、管理、経済、および起業家精神または事業運営に関連するサイト。広告およびマーケティング会社を含みます。企業サイトは、その技術で分類されるべきものであるため、含めるべきではありません。また、fedex.comやups.com のような配送サイトも含まれます。
コンピュータとインターネット情報	コンピュータとインターネットに関する一般情報。コンピュータサイエンス、エンジニアリング、ハードウェア、ソフトウェア、セキュリティ、プログラミングなどに関するサイトを含める必要があります。プログラミングは参照と重複するかもしれませんが、主なカテゴリはコンピュータとインターネットの情報のままにする必要があります。
コンテンツデリバリーネットワーク	広告、メディア、ファイルなどの第三者にコンテンツを配信することを主な目的とするサイト。イメージサーバも含まれます。
著作権侵害	ソフトウェアまたはその他の知的財産の違法ダウンロードを許可するコンテンツなど、違法なコンテンツがあるドメインであり、潜在的な責任のリスクをもたらします。

URL カテゴリ	詳説
	教育業界で求められる児童保護法や、ユーザーがサービスを介して著作権で保護されたコンテンツを共有することをインターネットプロバイダーが防止しなければならない国の法律に準拠するために、このカテゴリーが導入されました。
仮想通貨	暗号通貨を宣伝するウェブサイト、暗号マイニングウェブサイト（ただし、埋め込まれた暗号マイナーではない）、暗号通貨取引所とベンダー、および暗号通貨ウォレットと元帳を管理するウェブサイト。このカテゴリには、暗号通貨を参照する従来の金融サービス Web サイト、暗号通貨とブロックチェーンの仕組みを説明および説明する Web サイト、または組み込みの暗号通貨マイナー（グレーウェア）を含む Web サイトは含まれません。
デート	オンライン出会い系サービス、アドバイス、その他の個人広告を提供する Web サイト。
教育機関	学校、カレッジ、大学、学区、オンラインクラス、およびその他の学術機関の公式 Web サイト。これらは、小学校、高校、大学などの大規模で確立された教育機関を指します。学習塾もここに入ることができます。
エンターテイメントとアート	映画、テレビ、ラジオ、ビデオ、番組ガイド/ツール、コミック、舞台芸術、美術館、アート ギャラリー、図書館のサイト。エンターテイメント、有名人、業界ニュースのサイトが含まれています。
過激主義	テロ、人種差別、ファシズムや、民族的な出自や宗教、その他の考え方が異なる人や集団を差別するその他の過激な思想を喧伝するウェブサイト。このカテゴリーは、教育業界で求められる児童保護法に準拠するために導入されました。地域によっては、法規制により過激派サイトへのアクセスが禁止されている場合があり、アクセスを許可すると責任を問われる可能性があります。
金融サービス	オンラインバンキング、ローン、住宅ローン、債務管理、クレジットカード会社、保険会社など、個人の財務情報またはアドバイスに関連する Web サイト。株式市場、証券会社、または取引サービスに関連するサイトは含まれ

URL カテゴリ	詳説
	ません。外貨両替のサイトが含まれています。外貨両替のサイトが含まれています。
gambling	リアルマネーおよび/またはバーチャルマネーの交換を容易にする宝くじまたはギャンブルのウェブサイト。賭博オッズやプールなど、ギャンブルに関する情報、チュートリアル、アドバイスを提供する関連ウェブサイト。ギャンブルに対応していないホテルやカジノの企業ウェブサイトは、旅行に分類されます。
ゲーム	ビデオおよび/またはコンピュータゲームのオンラインプレイまたはダウンロード、ゲームレビュー、ヒント、またはチートを提供するサイト、ならびに非電子ゲーム、ボードゲームの販売/取引、または関連する出版物/メディアの教育サイト。オンライン懸賞や景品をサポートまたはホストするサイトが含まれます。
政府	地方政府、州政府、および中央政府、ならびに関連機関、サービス、または法律の公式 Web サイト。
健康と医学	一般的な健康情報、問題、伝統的および非伝統的なヒント、救済策、治療法に関する情報を含むサイト。また、さまざまな医療専門分野、診療所、施設(ジムやフィットネスクラブなど)、専門家のためのサイトも含まれています。医療保険や美容整形に関連するサイトも含まれています。
ホーム＆ガーデン	住宅の修理とメンテナンス、建築、設計、建設、装飾、ガーデニングに関する情報、製品、およびサービス。
狩猟と釣り	狩猟・釣りに関する情報、説明、関連機器・用具の販売。
インターネット通信とテレフォニー	ビデオチャット、インスタントメッセージ、テレフォニー機能をサポートまたはサービスを提供するサイト。
インターネットポータル	ユーザーの出発点として機能するサイト（通常は、コンテンツとトピックの広範なセットを集約することによって）。

URL カテゴリ	詳説
求人検索	求人情報、雇用者のレビュー、面接のアドバイスやヒント、または雇用者と求職者双方のための関連サービスを提供するサイト。
法務	法律、法律サービス、法律事務所、またはその他の法的関連事項に関する情報、分析または助言
軍事	軍事部門、募集、現在または過去の作戦、または関連する道具に関する情報または解説。
自動車	自動車、オートバイ、ボート、トラック、RV のレビュー、販売および取引、修正、部品、およびその他の関連する議論に関する情報。
音楽	音楽の販売、配信、または情報。音楽アーティスト、グループ、レーベル、イベント、歌詞、および音楽ビジネスに関するその他の情報に関する Web サイトが含まれます。ストリーミング音楽は含まれません。
ニュース	オンライン出版物、ニュースワイヤーサービス、および現在の出来事、天気、またはその他の現代の問題を集約するその他のウェブサイト。新聞、ラジオ局、雑誌、ポッドキャストが含まれています。
未解決	Web サイトがローカル URL フィルタリングデータベースに見つからず、ファイアウォールがカテゴリを確認するためにクラウドデータベースに接続できなかったことを示します。URL カテゴリ検索が実行されると、ファイアウォールはまずデータプレーンキャッシュで URL をチェックし、一致するものが見つからない場合は管理プレーンキャッシュをチェックし、一致するものが見つからない場合はクラウド内の URL データベースにクエリを実行します。未解決として分類されるトラフィックに対して実行するアクションを決定するときは、アクションをブロックに設定すると、ユーザーにとって非常に混乱を招く可能性があることに注意してください。
裸体	アートワークなど、文脈や意図に関係なく、人体のヌードまたはセミヌードの描写を含むサイト。参加者の画像を含むヌーディストまたはナチュリストのサイトが含まれます。

URL カテゴリ	詳説
オンラインストレージとバックアップ	無料でサービスとしてファイルのオンラインストレージを提供するWebサイト。
ピアツーピア	トレント、ダウンロードプログラム、メディアファイル、またはその他のソフトウェアアプリケーションのピアツーピア共有のためのアクセスまたはクライアントを提供するサイト。主にビットトレントダウンロード機能を提供するサイトが対象です。シェアウェアやフリーウェアのサイトは含まれません。
個人サイトとブログ	個人またはグループによる個人のウェブサイトやブログ。最初にコンテンツに基づいて分類してみてください。たとえば、誰かが車に関するブログを持っている場合、サイトは「自動車」に分類されるべきです。ただし、サイトが純粋なブログの場合は、「個人用サイトとブログ」の下にとどまる必要があります。
哲学と政治的主張	哲学的または政治的見解に関する情報、見解、キャンペーンを含むサイト。
プライベート IP アドレス	このカテゴリには、RFC1918「プライベートイントラネットのためのアドレス割り当て」で定義された IP アドレスが含まれます。また、パブリックDNSシステムに登録されていないドメイン（*.localと*.onion）も含まれます。
疑わしい	個人やグループの特定の層を標的とした、悪趣味なユーモアや不快なコンテンツを含む Web サイト。
不動産	不動産の賃貸、販売、および関連するヒントや情報に関する情報。不動産業者、企業、賃貸サービス、リスティング（および集計）、不動産改善のためのサイトが含まれています。
レクリエーションと趣味	レクリエーションや趣味に関する情報、フォーラム、協会、グループ、出版物。
リファレンスとリサーチ	個人的、専門的、または学術的な参考ポータル、資料、またはサービス。オンライン辞書、地図、年鑑、国勢調査情報、図書館、系図、科学情報が含まれています。

URL カテゴリ	詳説
宗教	さまざまな宗教、関連する活動またはイベントに関する情報。宗教団体、役人、礼拝所のウェブサイトが含まれています。占いのためのサイトが含まれています。
検索エンジン	キーワード、フレーズ、またはその他のパラメータを使用した検索インターフェイスを提供し、結果として情報、ウェブサイト、画像またはファイルを返す可能性のあるサイト。
性教育	生殖、性的発達、安全な性行為、性感染症、避妊、より良いセックスのためのヒント、ならびに関連する製品または関連器具に関する情報。関連するグループ、フォーラム、または組織の Web サイトが含まれます。
シェアウェアとフリーウェア	ソフトウェア、スクリーンセーバー、アイコン、壁紙、ユーティリティ、着信音、テーマ、ウィジェットへのアクセスを無料および/または寄付で提供するサイト。オープンソースプロジェクトも含まれます。
ショッピング	商品やサービスの購入を容易にするサイト。オンラインマーチャント、百貨店の Web サイト、小売店、カタログ、および価格を集計および監視するサイトが含まれます。ここに掲載するサイトは、さまざまな商品を販売している（またはネット販売を主目的とする）オンラインマーチャントである必要があります。化粧品会社のホームページで、たまたまオンラインショッピングが可能な場合、ショッピングではなく、化粧品に分類する必要があります。
ソーシャル ネットワーキング	ユーザー同士がやり取りしたり、メッセージや画像を投稿したり、ユーザーのグループと通信したりするユーザーコミュニティやサイト。ブログや個人用サイトは含まれません。
社会	一般の人々に関連するトピック、ファッション、美容、慈善団体、社会、子供など、多種多様な人々に影響を与える問題。レストランのウェブサイトも含まれています。子供向けの Web サイトやレストランが含まれています。
スポーツ	スポーツイベント、アスリート、コーチ、役員、チームまたは組織、スポーツスコア、スケジュール、関連ニュー

URL カテゴリ	詳説
	ス、および関連する道具に関する情報。ファンタジースポーツやその他の仮想スポーツリーグに関するウェブサイトが含まれています。
株式投資アドバイスとツール	株式市場、株式またはオプションの取引、Palo Alto Networks製品のポートフォリオ管理、投資戦略、相場、または関連ニュースに関する情報。
ストリーミングメディア	オーディオまたはビデオコンテンツを無料でストリーミングおよび/または購入するサイト。オンラインラジオ局やその他のストリーミング音楽サービスが含まれます。
水着と下着・寝間着	水着、親密な服装、その他の挑発的な衣服に関する情報や画像を含むサイト
トレーニングとツール	オンラインの教育およびトレーニングおよび関連資料を提供するサイト。運転/交通学校、職場のトレーニングなどを含めることができます。
翻訳	ユーザー入力と URL 翻訳の両方を含む翻訳サービスを提供するサイト。これらのサイトでは、ターゲットページのコンテンツが翻訳者のURLのコンテキスト内に表示されるため、ユーザーはフィルタリングを回避できます。
トラベル	旅行のヒント、お得な情報、価格情報、目的地情報、観光、および関連サービスに関する情報。ホテル、地元のアトラクション、カジノ、航空会社、クルーズライン、旅行代理店、レンタカー、価格モニターなどの予約ツールを提供するサイトの Web サイトが含まれます。エッフェル塔、グランドキャニオンなどの地元の観光スポット/観光スポットのウェブサイトが含まれています。
兵器	兵器およびその使用に関する販売、レビュー、説明または指示。
ウェブ広告	広告、メディア、コンテンツ、バナー。
ウェブホスティング	Web 開発、出版、プロモーション、およびトラフィックを増やすためのその他の方法に関する情報を含む、Web ページのホスティングサービスを無料または有料で提供します。

URL カテゴリ	詳説
Web ベース電子メール	電子メールの受信トレイへのアクセスと電子メールの送受信機能を提供するすべての Web サイト。

Cloud NGFW for AWS でファイルブロッキングを設定する

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）

ファイルブロッキングプロファイルでは、ブロックまたはモニターする特定のファイルタイプを識別できます。ほとんどのトラフィックの場合 (内部ネットワークのトラフィックを含む)、脅威をもたらす既知のファイルや、アップロード/ダウンロードするメリットが無いファイルはブロックします。現在のところ、これにはバッチファイル、DLL、Java クラスファイル、ヘルプファイル、Windows ショートカット（.lnk）、BitTorrent ファイルが含まれます。

Cloud NGFW は、ネットワークを移動するファイルに対して次のアクションを実行できます。

- **alert** - 指定したファイル タイプが検出されると、データ フィルタリング ログでログが生成されます。
- **Block** [ブロック] - 指定したファイル タイプが検出されると、そのファイルはブロックされ、ユーザーに対してカスタマイズ可能なブロック ページが表示されます。データ フィルタリング ログでログも生成されます。
- **Continue** - 指定したファイルタイプが検出されると、ユーザーに対して応答ページが表示されます。ユーザーはページをクリックスルーしてファイルをダウンロードすることができます。データ フィルタリング ログでログも生成されます。このタイプの転送アクションは、ユーザーとのやり取りが必要になるため、Web トラフィックにのみ使用可能です。

さらに、ダウンロード、アップロード、またはアップロードとダウンロードの方向に基づいて、ファイルの種類を許可またはブロックできます。

STEP 1 | ［ルールスタック］を選択し、ファイルブロックを設定するために以前に作成したルールスタックを選択します。

STEP 2 | **[セキュリティ プロファイル]** > **[マルウェアおよびファイルベースの脅威防御]** > **[ファイルブロック]** > **[編集]**を選択します。

STEP 3 | 表示されたリストからファイルの種類を選択します。

STEP 4 | ドロップダウンから選択したファイルタイプのアクションとトラフィックの方向を設定します。

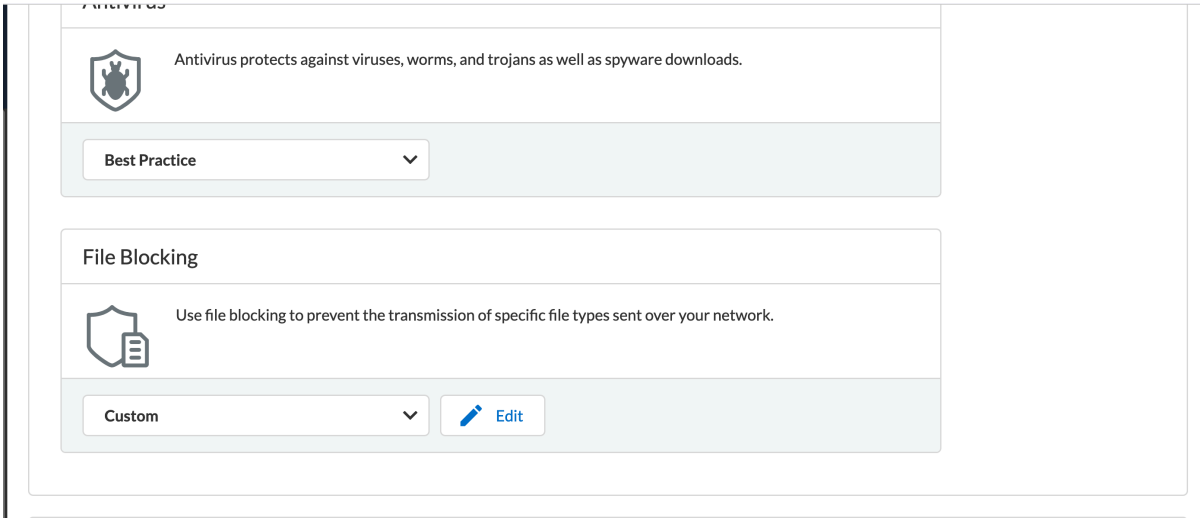
STEP 5 | **[Save(保存)]**をクリックします。

ファイル ブロック プロファイルを変更する

デフォルトでは、ファイル ブロック プロファイルはベストプラクティスに設定されています。ファイル ブロック プロファイルを変更する方法:

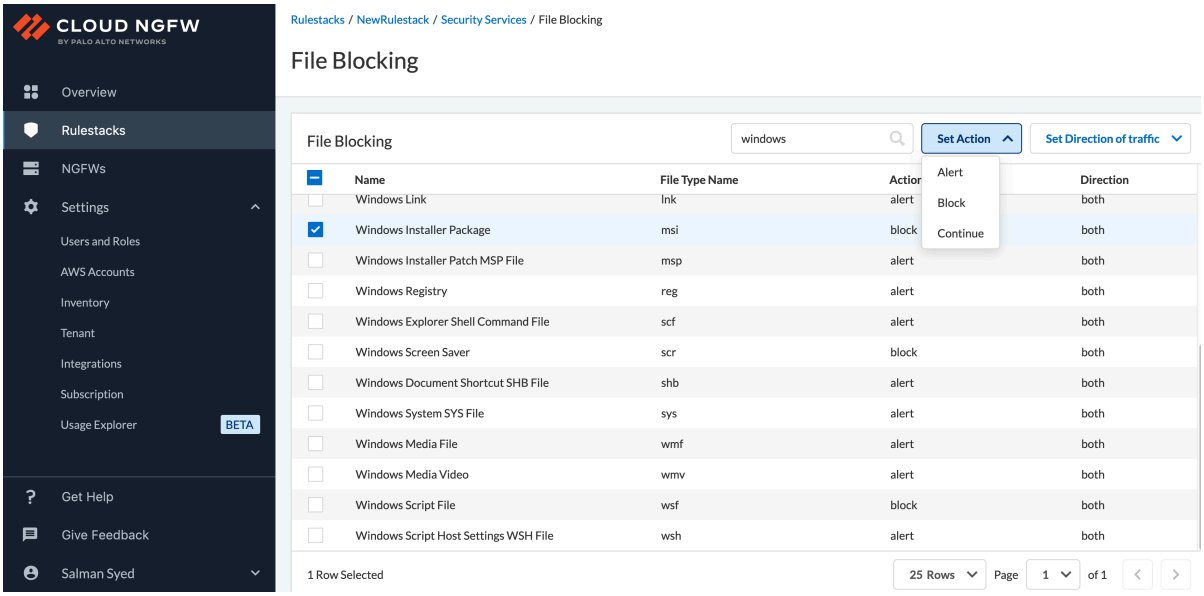
STEP 1 | **[Malware and File-based Threat Protection(マルウェアとファイルベース脅威保護(]**画面で、**[File Blocking(ファイル ブロック)]**に移動します。

STEP 2 | ドロップダウンを使用して「カスタム」を選択します。



STEP 3 | Cloud NGFW コンソールを開きます。**[Rulestacks(ルールスタック)] > [Rulestack name(ルールスタック名)] > [Security Services(セキュリティ サービス)] > [File Blocking(ファイル ブロック)]**の順に進みます。

STEP 4 | **[Set Action(アクションを設定)]**ドロップダウンで、アクションを**[Alert(アラート)]**または**[Contnue(続行)]**に変更します。



Cloud NGFW for AWS でのアウトバウンド復号化の設定

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）

アウトバウンド復号化では、Cloud NGFW は SSL フォワードプロキシのように動作し、関連する証明書を使用して、クライアント/サーバーセッションの信頼できるサードパーティ（中間者）としての地位を確立します。ただし、Cloud NGFW はトラフィックパケットヘッダーとペイロードをそのまま保持し、送信元の ID を宛先に完全に可視化します。

アウトバウンド復号化では、信頼と不信頼の 2 つの証明書オブジェクトが使用されます。NGFW は、クライアントが信頼された認証局（CA）によって署名された証明書を持つサーバーに接続しようとしている場合、SSL 暗号化解除中にクライアントに信頼証明書を提示します。あるいは。NGFW は、NGFW が信頼していない CA によって署名された証明書を持つサーバーに接続しようとしているクライアントに信頼できない証明書を提示します。

NGFW リソースを設定して、VPC またはサブネットから送信される SSL トラフィックを復号化できます。その後、ウイルス対策、脆弱性、スパイウェア対策、URL フィルタリング、ファイルブロックプロファイルなど、プレーンテキストトラフィックに App-ID とセキュリティ設定を適

用できます。トラフィックの復号化と検査を行った後、プレーンテキスト トラフィックはファイアウォールを出るときにファイアウォールによって再暗号化され、プライバシーとセキュリティが確保されます。

この手順では、ファイアウォールがアウトバウンド TLS 復号化に使用する証明書のみを定義します。ルール作成中に送信 TLS 復号化を有効にします。

STEP 1 | ［ルールスタック］を選択し、証明書を適用する以前に作成したルールスタックを選択します。

STEP 2 | セキュリティサービス > アウトバウンド復号化を選択します。

CA 証明書のBasic ConstraintsのCA値を **true**に設定する必要があります。

STEP 3 | 証明書を選択します。

- 信頼できない証明書を選択します。
- 信頼証明書を選択します。

まだ証明書を作成していない場合は作成します。

証明書とプライベートキーはAWS Secrets Manager (ASM)に保存され、ワークロードはこれらの情報を使用してトラフィックを復号します。

証明書はCA証明書である必要があります。[Basic Constraints(基本制約)]のCA値をTRUEに設定する必要があります。次に、プライベートCA証明書の例を示します。

```
証明書：データ：バージョン：3 (0x2) シリアルナンバー:4121 (0x1019) シ
グネチャ アルゴリズム: sha256WithRSAEncryption発行者:C=米
国、ST=ワシントン、L=シアトル、O=サンプル会社、ルートCA、OU=Corp、
 CN=www.example.com/emailAddress=corp@www.example.com 有
効期限 これより前は無効:2018年2月26日20:27:56 GMT これよ
り後は無効:2028年2月24日 20:27:56 GMT 件名:C=米国、ST=ワ
シントン、L=シアトル、O=サンプル会社、下位CA、OU=Corporate
 Office、CN=www.example.com Subject サブジェクト公開鍵情報:公開鍵アルゴリ
ズム:rsaEncryption パブリックキー:(2048ビット)係数:00:c0: ...a3:4a:51 指
数:65537 (0x10001) X509v3 拡張:X509v3 サブジェクト キー識別
子:F8:84:EE:37:21:F2:5E:0B:6C:40:C2:9D:C6:FE:7E:49:53:67:34:D9
 X509v3 認証キー識別子:
 keyid:0D:CE:76:F2:E3:3B:93:2D:36:05:41:41:16:36:C8:82:BC:CB:F8:A0
 X509v3 基本的な制約: 重要なCA:TRUE X509v3 キーの使用法: 重要なデジタ
```

```
ル シグネチャ、CRL署名シグネチャ ルゴリズム: sha256WithRSAEncryption
 6:bb:94: ...80:D8
```

証明書がチェーンの場合は、リーフ証明書とキーを使用します。ルートCA証明書と中間CA証明書をクライアント トラストストアにインポートします。次に、ルートCA証明書と中間CA証明書をUbuntu OSのトラストストアにインポートする方法の例を示します。

```
$ sudo apt-get install -y ca-certificates $ sudo cp root-ca.crt /
usr/local/share/ca-certificates $ sudo cp intermediate-ca.crt /usr/
local/share/ca-certificates $ sudo update-ca-certificates
```

トラフィックの復号化にエンドエンティティ証明書を使用している場合は、公開鍵と秘密鍵を持つエンド エンティティ証明書のみをASMに保存する必要があります。

*PKCS8*はサポートされている証明書形式です。

アウトバウンド トラスト復号化は、自己署名証明書をサポートしていません。

STEP 4 | **[Save(保存)]**をクリックします。

Cloud NGFW for AWS で受信復号化を設定する

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）

Cloud NGFWは、SSL インバウンド復号化を使用して、クライアントから対象のネットワーク サーバー（証明書があり、ファイアウォールにインポートできる任意のサーバー）へのインバウンド SSL/TLS トラフィックを検査および復号化し、疑わしいセッションをブロックすることができます。ファイアウォールは外部クライアントと内部サーバーの間のプロキシとして機能し、安全なセッションごとに新しいセッションキーを生成します。ファイアウォールは、クライアントとファイアウォールの間に安全なセッションを作成し、ファイアウォールとサーバーの間に別の安全なセッションを作成して、トラフィックを暗号化解除して検査します。ただし、Cloud NGFW はトラフィックパケットのヘッダーとペイロードをそのまま保持し、VPC 内のアプリケーションに対してソースの ID を完全に可視化します。

証明書 とセッション キーは AWS シークレットマネージャ に保存され、SSL インバウンド検査を実行します。ファイアウォールは、SSL/TLS ハンドシェイク中に対象のサーバーから送信され

た証明書が、復号化ポリシールールにある証明書と一致することを検証します。一致するものがある場合、ファイアウォールはサーバーの証明書をサーバー・アクセスを要求するクライアントに転送し、セキュア接続を確立します。

STEP 1 | ［ルールスタック］を選択し、証明書を適用する以前に作成したルールスタックを選択します。

STEP 2 | ［ルール**]**、復号化用の新しい［セキュリティルールの作成］を選択 します。

STEP 3 | ［一般］の下に次の詳細を入力します。

- 名前 — ルールの名前。
- 説明 — ルールの説明。
- ルール優先順位 — ルールの一意の優先順位。
- 有効— フィールドを有効にして、ルールスタックをルールに関連付けます。このフィールドはデフォルトで有効になっています。

STEP 4 | 送信元および宛先 IP アドレスフィールドの一致基準を定義します。

STEP 5 | 詳細な制御を設定します。

- ルールで許可またはブロックするアプリケーション（**App-ID™**） を指定します。

  *TLS*復号化ルールは、***[Applications(***アプリケーション***)]***（***App-ID™***）—***[Any(***任意***)]*** または ***SSL—[Match*** *only(*一致のみ*)]*で作成できます。
- そのルールの一致条件として **URL** カテゴリを指定します。
- ルールで許可またはブロックするプロトコルとポートを指定します。

STEP 6 | 作成したルールのいずれかにトラフィックが一致したときにファイアウォールが実行するアクションを指定します。

- 許可 — トラフィックを許可します。
- 拒否 — トラフィックをブロックし、拒否されるアプリケーションについて定義されたデフォルトの拒否アクションを実行します。
- サーバーのリセット — サーバー側デバイスに TCP リセットを送信します。
- 両方のリセット — クライアント側とサーバー側の両方のデバイスに TCP リセットを送信します。

STEP 7 | ［**TLS** 復号化**]**で［インバウンド**]**を選択し、［インバウンドインスペクション証明書］を選択します。

まだ証明書を作成していない場合は作成します。証明書オブジェクトを作成するときに、シークレットの *Amazon* リソース名（*ARN*）を証明書 *ARN* で使用する必要があります。

証明書と秘密鍵はAWS Secrets Manager（ASM）に格納され、Application Load Balancer（ALB）はこれらの情報を使用してトラフィックを復号化します。証明書はCA証明書である必要はありません。証明書がチェーンの場合は、リーフ証明書とキーを使用します。

*PKCS8*はサポートされている証明書形式です。

インバウンド復号化は、自己署名証明書をサポートしていません。

TLS 復号化の復号化プロファイルは、ベストプラクティスセキュリティポリシーに設定されています。詳細については、完全な可視性と脅威検査のためのトラフィックの復号化を参照してください。

STEP 8 | ［有効**]**をクリックしてログを有効にします。

STEP 9 | **[Save(**保存**)]**をクリックします。

STEP 10 | ［アクションの設定］ > ［設定のデプロイ］ > ［コミット］をクリックして、ファイアウォールの実行中の設定にルールを保存します。

Cloud NGFW for AWSのルールの使用

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）

Panoramaを使用してCloud NGFWリソース上のルールを管理し、運用やトラブルシューティングタスクのルール使用状況を追跡および監視します。Panoramaコンソールで、クラウド デバイス

グループでルールの使用状況を表示し、Cloud NGFWリソースのすべてが一致するか、一部に一致するか、まったく一致しないかを判断できます。

Panorama では、ポリシー ルール ヒット カウントが有効（デフォルト）であり 、デバイス グループを使用してポリシー ルールを定義およびプッシュした管理対象ファイアウォールのルール使用の詳細を表示できます。Panorama ではファイアウォールでローカルに設定されたポリシー ルールのルール使用状況の詳細を取得できないため、ローカルに設定されたルールのルール使用情報を表示するには、ファイアウォールにログインしなければなりません。詳細については、「ポリシー ルール使用状況の監視」を参照してください。

ルールの使用方法: ルールヒットとポリシーオプティマイザ

システム要件

次に、セキュリティ ポリシー ルールの使用状況を監視するための最小システム要件を示します。

- Panorama（PAN-OS）バージョン10.2.8以上
- AWSプラグインのバージョン5.2.0以上
- Cloud Servicesプラグインのバージョン5.0.0以上
- クラウド コネクタ プラグインのバージョン2.0.1以上

クラウド デバイス グループのルール ヒット数の表示

Panoramaコンソールで、クラウド デバイス グループをCloud NGFWリソースに関連付け、クラウド デバイスグループのポリシーを設定した後、以下の手順を実行してPanoramaでクラウド デバイス グループのルール ヒット数を表示します。

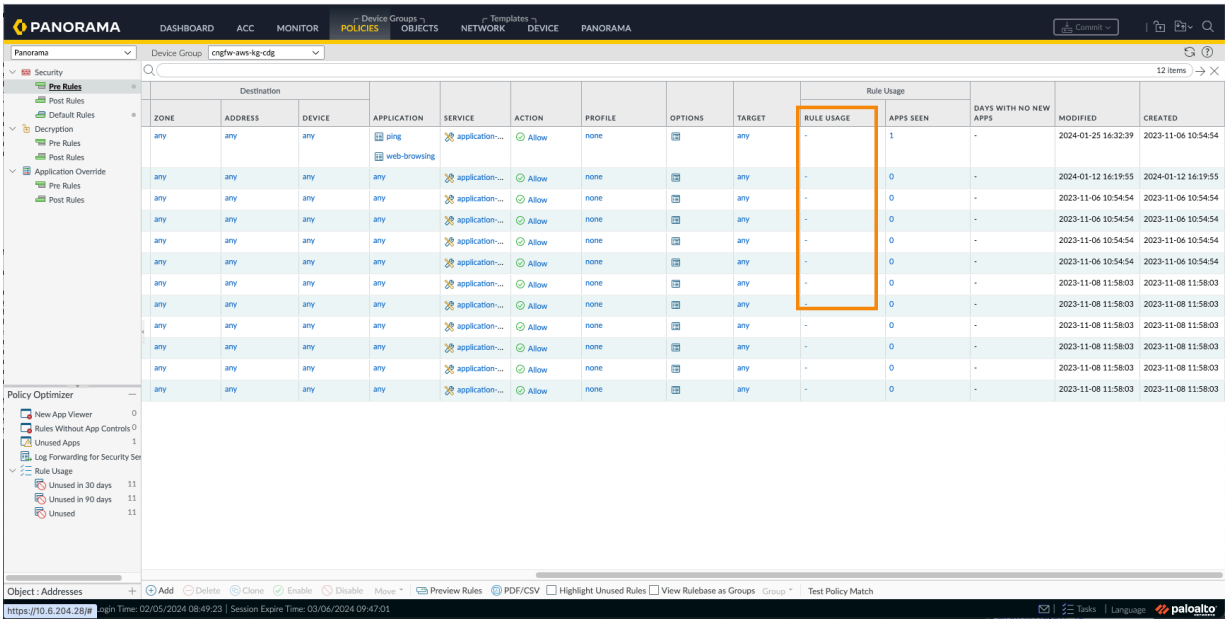
*NGFW*ファイアウォール リソースは、*2*分ごとにルールヒット データをクラウド*NGFW*サービスに報告します。その後、クラウド*NGFW*サービスは、ファイアウォール リソースからデータをポーリングするために最大*2*分間のレイテンシーを持ちます。これにより、*Panorama*コンソールでのルール ヒット数データ表示に最大*4*分間の遅延が発生します。

STEP 1 | **Policies (**ポリシー**)**を選択します。

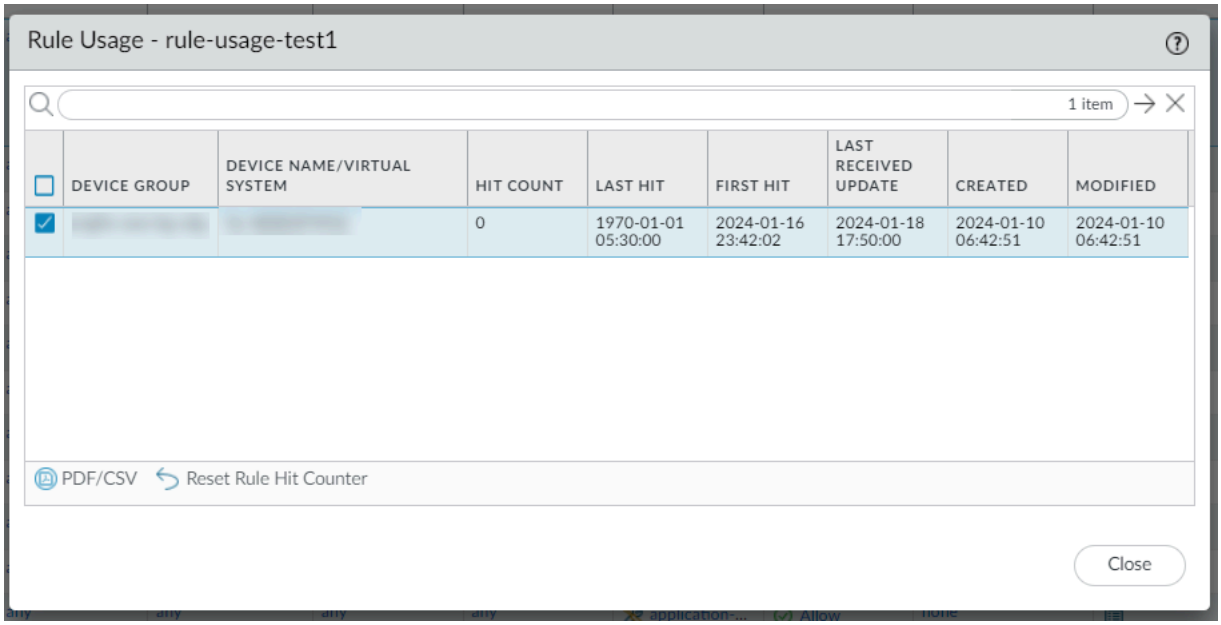
STEP 2 | **[Device Group(**デバイス グループ**)]**セクションで、ドロップダウンを使用してクラウド デバイス グループを選択します。

STEP 3 | ルールを選択し、**[Rule Usage(**ルールの使用**)]**をクリックします。

セキュリティ、復号化、およびアプリケーションオーバーライド ポリシー タイプの事前ルール、事後ルール、およびデフォルト ルールの使用状況を監視できます。



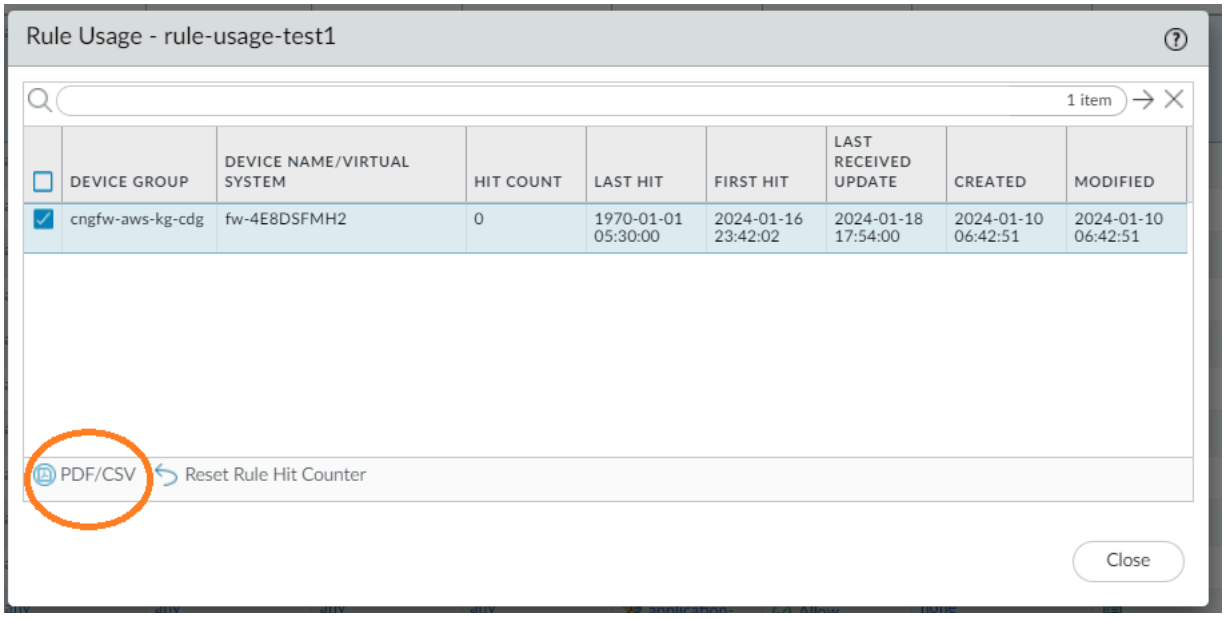
選択したルールのヒット数が表示されるようになりました。



*Panorama*コンソールでは、ルール ヒット数はデフォルトで*4*分間隔ごとに更新されます。

選択したルールのヒット数を更新するには、**[Reset Rule Hit Counter(**ルール ヒット数カウンタ**)**] をクリックします。

[PDF/CSV]をクリックして、選択したルールのルール使用の詳細をCSVまたはPDFファイルとしてエクスポートします。

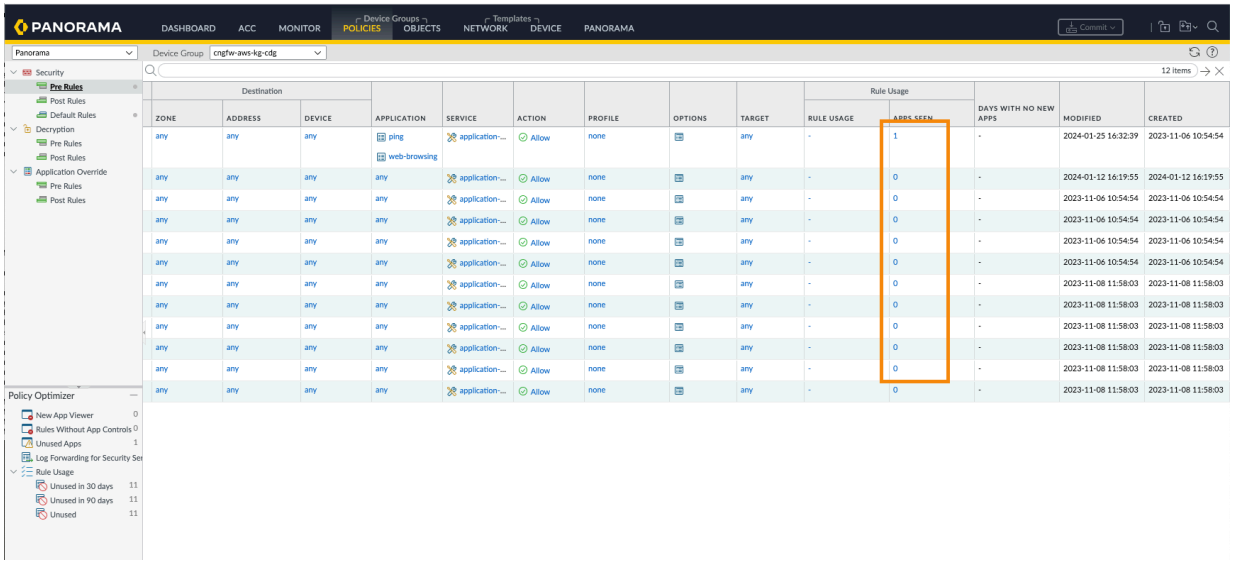


ルールの使い方 - 表示されるアプリとポリシー オプティマイザー

セキュリティ ポリシー ルールに一致するファイアウォールで表示および許可されているすべてのアプリケーションを表示できます。**[Apps Seen(表示アプリ)]** の横の数字は、ルールで見られたアプリケーションの数を示します。

- Panoramaコンソールで、**[Policies(ポリシー)]**タブに移動します。
- **[Device Group(デバイス グループ)]**セクションで、ドロップダウンを使用してクラウド デバイス グループを選択します。

- [Rule(ルール)]を選択し、**[Apps seen(表示アプリ)]**をクリックします。



これで、セキュリティ ポリシー ルールで設定および表示されるアプリケーションを確認できます。

ルールのアプリケーション、表示されるアプリケーション、およびアプリケーションの表示アクションの詳細については、「アプリケーションおよび使用状況」を参照してください。

[Policy Optimizer(ポリシーオプティマイザー**)]**セクションでは、Panorama上で設定したすべてのクラウド デバイス グループのルールヒット数を表示することもできます。Policy Optimizer は、従来のセキュリティポリシールールベースを App-ID ベースのルールベースに移行するための簡単なワークフローを提供します。これにより、攻撃の入り口を減らし、アプリケーションを可視化して安全に有効にできるため、セキュリティが向上します。詳細については、「セキュリティポリシー ルールの最適化」および「アプリケーションおよび使用状況」を参照してください。

Panoramaポリシー管理

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は、AWS 上のクラウドネイティブ サービスとして提供される、業界で唯一の機械学習 (ML) 搭載NGFWです。Cloud NGFWを使用すると、実際のクラウド ネイティブ エクスペリエンスにより、クラウドの速度とクラウド規模で、より多くのアプリを安全に実行できます。AWSのサービスとして提供されるネイティブに統合されたネットワーク セキュリティにより、両方の長所を体験できます。

このページでは、Cloud NGFW for AWSを Palo Alto Networks Panorama と構成して統合する方法について説明します。

Panoramaアプライアンスを使用すると、物理ファイアウォール アプライアンスや仮想ファイアウォール アプライアンスとともに、Cloud NGFWリソース上で共有セキュリティ ルール セットを集中管理できます。また、共有オブジェクトとプロファイル構成のあらゆる側面を管理し、これらのルールをプッシュし、Cloud NGFWリソースのトラフィック パターンやセキュリティ インシデントに関するレポートを生成することも、すべて単一のPanoramaコンソールから行うことができます。

Panoramaは、ハードウェア ファイアウォール、仮想ファイアウォール、クラウド ファイアウォールにわたるポリシーとファイアウォールの一元管理を単一の場所で実行できるため、ファイアウォールのハイブリッド ネットワークの管理と保守における運用効率が向上します。

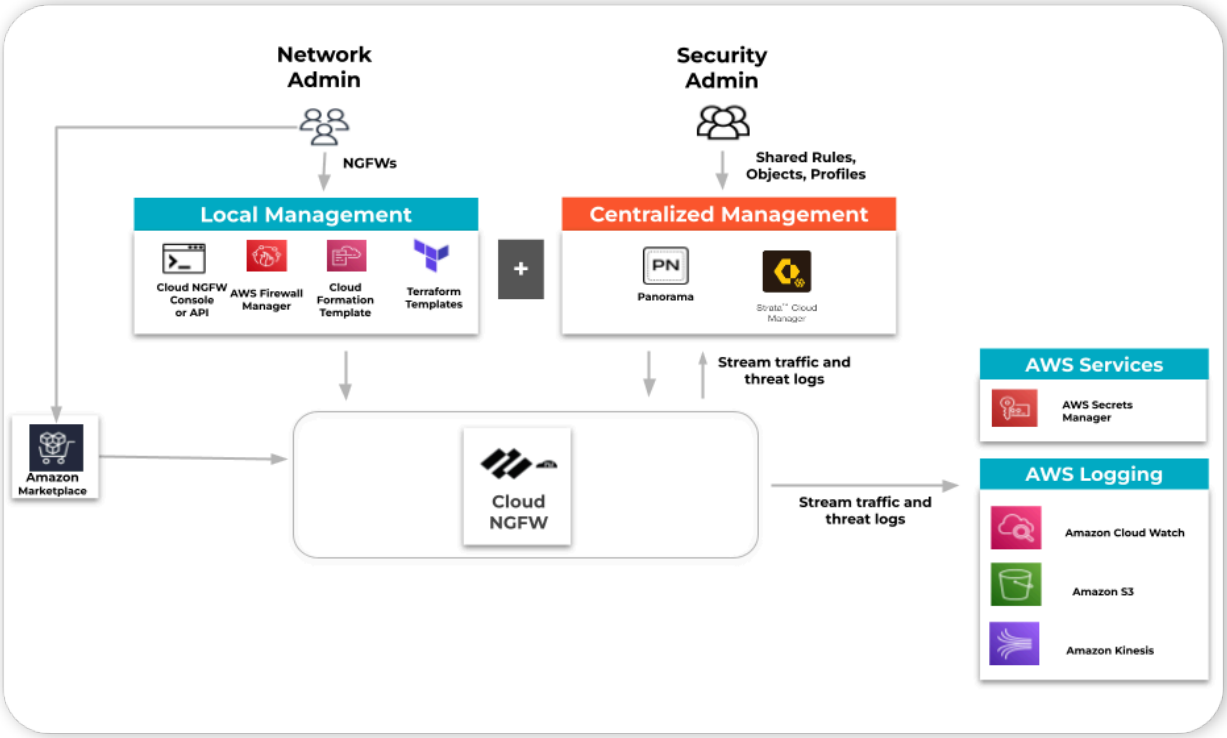
統合はどのように機能しますか?

引き続きAWS Marketplaceを使用してCloud NGFW サービスに登録し、テナントを作成します。その後、Cloud NGFW テナントをPanoramaアプライアンスにリンクできます。その後、このテナント上に作成した Cloud NGFW リソース上で、物理および仮想ファイアウォール アプライアンスとともに共有のセキュリティ ルール セットを一元的に管理し、 ログ記録、レポート作成、ログ分析をすべてPanoramaコンソールから使用できるようになります。

Panoramaアプライアンスは、任意のクラウド リージョンまたはオンプレミス環境に配置できます。PanoramaはAWSプラグインを使用して、ポリシーとオブジェクトをAWSリージョンのNGFWリソースにプッシュします。

Cloud NGFWとPanoramaアプライアンスの統合により、オプションでCloud NGFWリソースから Strata Logging Service(CDL) アカウントにログをストリーミングできるようになります。その後、CDL UI、Panoramaログ ビューア、またはアプリケーション コマンド センター (ACC) を使用して、CDLからのログを表示および分析できます。Panoramaは、クラウド サービス プラグインを使用して、CDLアカウントからログを照会します。

また、S3、Cloudwatch、KinesisストリームなどのAWSログの送信先にログをストリーミングするようにCloud NGFWリソースを構成することもできます。



複数の*Panorama*、*Strata Logging Service*ペアを*Cloud NGFW*テナントにリンクできます。

統合コンポーネント

下の画像は、Cloud NGFWがPanoramaと統合される様子を示しています。これらの各コンポーネントについては、次のセクションで説明します。

Palo Alto Networksのポリシー管理は、ソリューションの主要かつ必須のコンポーネントです。Cloud NGFWリソースのポリシーを作成および管理するには、**Panorama**アプライアンスを使用する必要があります。ポリシー管理コンポーネントは、作成したポリシーとオブジェクトを、異なるAWSリージョンの複数のCloud NGFWリソースに関連付けるのにも役立ちます。

Palo Alto Networksのログ管理は、このソリューションの必須コンポーネントではありません。Panorama コンソールでログを表示する場合や、Panorama コンソールのアプリケーション コマンド センター (ACC) を使用して Cloud NGFW トラフィックに関する洞察を得たり、Panoramaでレポートを生成したりする場合は、Strata Logging Service を使用できます。このためには、Panorama のクラウド サービス プラグインを使用して、Panorama を Strata Logging Service アカウントにリンクする必要があります。Cloud NGFWリソースを設定して、ログをStrata Logging ServiceとAWS ログ送信先 (S3、Cloudwatch、またはKinesis ストリーム)の1つに同時に送信できます。

1) Panorama を*Cortex Data Lake*にリンクしてから、*Cloud NGFW*テナントにリンクします。*2)* 同じ *Cloud NGFW*テナントで複数の*Panorama*を使用している場合は、各*Panorama*が個別の*Cortex Data Lake*インスタンスにリンクされていることを確認します。

Panorama AWS プラグインは 、このソリューションの必須コンポーネントです。Panorama AWSプラグインを使用すると、Panoramaにリンクされた Cloud NGFWテナントのNGFWリソース上のポリシーとオブジェクトを管理するのに役立つクラウド デバイス グループとクラウド テンプレート スタックを作成できます。Panorama AWSプラグインは、内部的にCloud Connectorプラグインを使用してCloud NGFWリソースと通信します。

クラウド デバイス グループは 、クラウドNGFW リソースのルールとオブジェクトを作成できる特別な目的のPanoramaデバイス グループです。Cloud NGFWテナントおよびAWSリージョン情報を指定して、Panorama AWSプラグイン UI/APIを使用してCloud DGを作成できます。クラウド デバイス グループは、そのテナントまたはリージョン内のグローバル ルール スタックとして表示されます。

- Panorama AWSプラグインを使用して、複数のクラウド デバイス グループを作成できます。
- ネイティブPanorama Webインターフェースのデバイス グループ ページを使用して、クラウド デバイス グループのポリシーとオブジェクトの構成、およびそれらに関連付けられたオブジェクトとセキュリティ プロファイルを管理できます。

- また、クラウド デバイス グループで作成したセキュリティ ルールで既存の Panoramaデバイス グループ内の既存の共有オブジェクトとプロファイルを参照することで、それらを活用することもできます。
- あるいは、これらのCloud DGをPanoramaで管理するデバイス グループ階層に追加して、デバイス グループルールとオブジェクトを継承することもできます。ただし、Cloud NGFWは現在、セキュリティ ゾーンやユーザーを使用するルールなど、クラウド デバイス グループによって継承されたすべてのルールを適用することはできません。
- 同じCloudデバイス グループをCloud NGFW テナントの複数のリージョンに関連付けることができます。このCloudデバイス グループは、Cloud NGFWテナントの各AWS リージョンで専用のグローバル ルールスタックとして表示されます。

クラウド テンプレート スタック **(Cloud TS)** は、特別な目的のPanoramaテンプレート スタックであり、これを使用すると、クラウド デバイス グループのセキュリティ ルールで、Panoramaでテンプレートを使用して管理できるオブジェクト設定を参照できます。Cloudデバイス グループを作成するときに、Panorama AWSプラグインを使用すると、クラウド テンプレート スタックを作成または指定できます。プラグインは、このCloud TSを自動的に作成し、参照テンプレート スタックとしてクラウドデバイスグループに追加します。今後は、ネイティブPanorama Webインターフェースのテンプレート スタック ページを使用してテンプレートを構成し、これらのCloud TSに追加できるようになります。

- Palo Alto Networks Cloud NGFWサービスは、Cloud NGFWリソース内のほとんどのデバイスとネットワーク構成を管理します。したがって、Cloud TSに追加されたテンプレートでインターフェース、ゾーン、ルーティング プロトコルなどのインフラストラクチャ設定を構成している場合、Cloud NGFWはそれらの設定を無視します。
- Cloud NGFWは現在、Cloudデバイス グループ構成で参照されるテンプレート内の証明書管理とログ設定を尊重します。他のすべての設定は無視されます。

管理対象デバイスをクラウド デバイス グループおよびクラウド テンプレート スタックに割り当てることはできません。

Cloud NGFWをPanoramaと統合するには、いくつかの手順が必要です。Panoramaバーチャル アプライアンスをセットアップし、プラグインをインストールしたら、AWS Marketplaceを使用してCloud NGFWに楼六し、テナントを作成する必要があります。Cloud NGFWテナントを作成したら、それをPanorama仮想アプライアンスにリンクします。Cloud NGFWを正常にリンクしたら、Panoramaを使用してセキュリティ オブジェクトとルールを管理し、ログと分析を監視します。

Panama統合の準備

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

どこで使用できますか?	何が必要ですか?
	❑ 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サービスをPanoramaバーチャル アプライアンスと統合する方法:

- 登録済みの Panorama がライセンスとともにインストールされ、カスタマー サポート ポータル (CSP)の サポート ライセンスを使用してアクティブ化され 、ソフトウェア バージョン10.2.3 (またはそれ以降) を使用していることを確認します。

  *Palo Alto Networks*カスタマー サポート ポータル *(CSP)* で正常に認証し、*1*つ以上のクラウド サービスを活用するには、*Panorama*管理サーバーに デバイス証明書をインストールする必要があります。

- Palo Alto Log Management を使用する場合は、必ず Panorama を Strata Logging Service 用に構成して ください。
- Cloud NGFWテナントを作成するには、Cloud NGFWに正常に登録していることを確認してください。Cloud NGFW サブスクリプションを使用して、Panorama と正常に統合します。
- Cloud NGFWテナントにテナント管理者ロールがあることを確認します。
- PanoramaにPanorama管理者ロールがあることを確認します。
- 組織がPanoramaアプライアンスを登録したPalo Alto Networksカスタマー サポート ポータル (CSP) アカウントのメンバーであることを確認します。

  CSP アカウントの登録に使用したメール アドレスは、*Cloud NGFW* テナント サブスクリプションに使用する必要があります。このメールが異なる場合、*Cloud NGFW* を構成して *Panorama* と統合することはできません。

- ドメインhttps://storage.googleapis.comへのアクセスを許可します。このドメインは、地理的な場所に関係なく、Cloud NGFW アプリケーションのAIOpsにアクセスするために使用されます。

その他の要件

PanoramaをCloud NGFWにリンクできるように準備する方法:

- Cloud Connectorプラグイン バージョン2.0.1以降をインストールします

  PAN-OSバージョン11.1.xには、Cloud Connectorプラグイン (バージョン 2.1.0-c98) が事前にパッケージ化されています。このプラグイン バージョンでは、*PAN-OSバージョン11.1.x*にリンクされている*Cloud NGFW*リソースの管理に問題が発生します。*PAN-OSバージョン11.1.x*を使用している場合、*Palo Alto Networks*では*Cloud Connector*プラグインをバージョン*2.0.1*にダウングレードすることをお勧めします。
- AWSプラグインバージョン5.1.1以降をインストールします。
- Cloud ConnectorとAWSプラグインをインストールした後、Panorama CLIを使用してコマンド`request plugins cloudconnector enable cloudngfw`を実行します。
- ダッシュボードを使用して、Panoramaにインストールされているプラグインを表示します。
- Panorama CLIを使用して、Panoramaプラグインのステータスを表示します。たとえば、`show plugins aws cngfw-status`です。

  `show plugins aws cngfw-status` `CloudConnector`プラグインが有効になっています。`Cloud NGFW` 機能が有効になっています。

重要な考慮事項

AWSプラグインでは、PanoramaでCloud NGFW機能を開始するために設定変更をコミットする必要があります。AWS プラグインをアップグレードする場合、このコミットは必要ありません。

Panorama HAデプロイメントでは、設定の変更 (たとえば、クラウド デバイス グループの変更) をプッシュすると、Panoramaバーチャル アプライアンスがハングする可能性があります。次のようなエラーメッセージが表示されます。「プッシュを処理できません。構成のアップロードが完了していません。後で再試行してください。」この問題を解決するには、`commit-force`を使用し、次に`commit-all`を使用します。

Cloud NGFWをPalo Alto Networks管理にリンク

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）

リンクには次の2つのオプションがあります。

1. ポリシー管理のみを目的として、Cloud NGFWをPanoramaでPalo Alto Networksにリンクします。
2. Cloud NGFWテナントをPanoramaとリンクしてポリシー管理を行い、Strata Logging Serviceをログ管理用にリンクします。

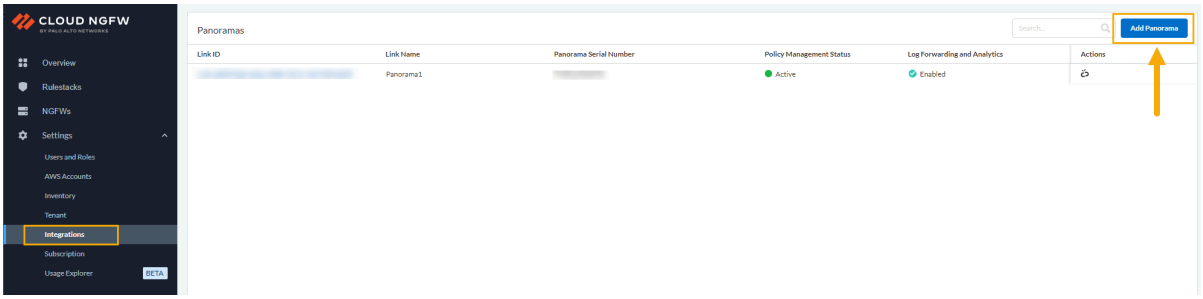
*Cloud NGFW*を*Panorama*と統合するには、*AWS Marketplace*を使用して*Cloud NGFW*サービスに登録する必要があります。*Cloud NGFW*テナントを*Panorama*にリンクすると、*AWS*プラグインの*Panorama*コンソールでテナントとリソースとそのステータスを確認できます。

既存の *Panorama* バーチャル アプライアンスを *Cloud NGFW* リソースから削除するには、「Panorama からのリンク解除」 を参照してください。*AWS* ファイアウォールマネージャを使用している場合、*Cloud NGFW* リソースから*Panorama*のリンクを解除することはできません。詳細については 「AWS ファイアウォールマネージャの使用時に Panorama と Cloud NGFW のリンクを解除するためのサポートケースを作成する」 を参照してください。

Cloud NGFW を使用してCloud NGFW テナントをPanoramaにリンクする方法:

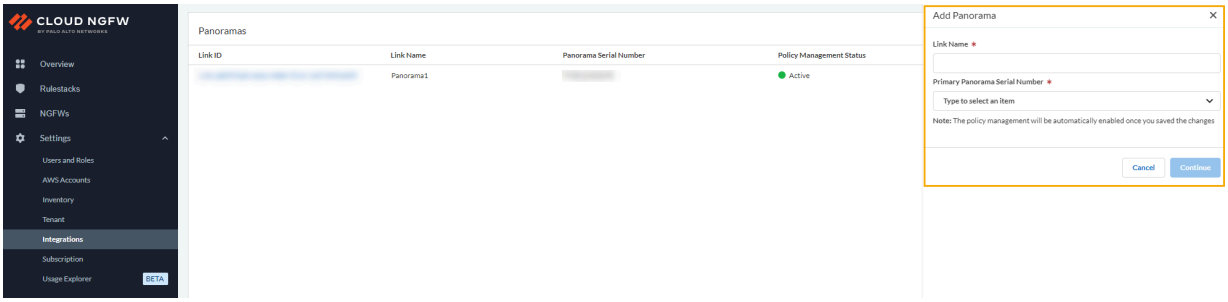
STEP 1 | **[Integrations (統合)]**選択します。

STEP 2 | **[Integrations(統合)]**ページで、**[Add Panorama(Panoramaを追加)]**をクリックします。

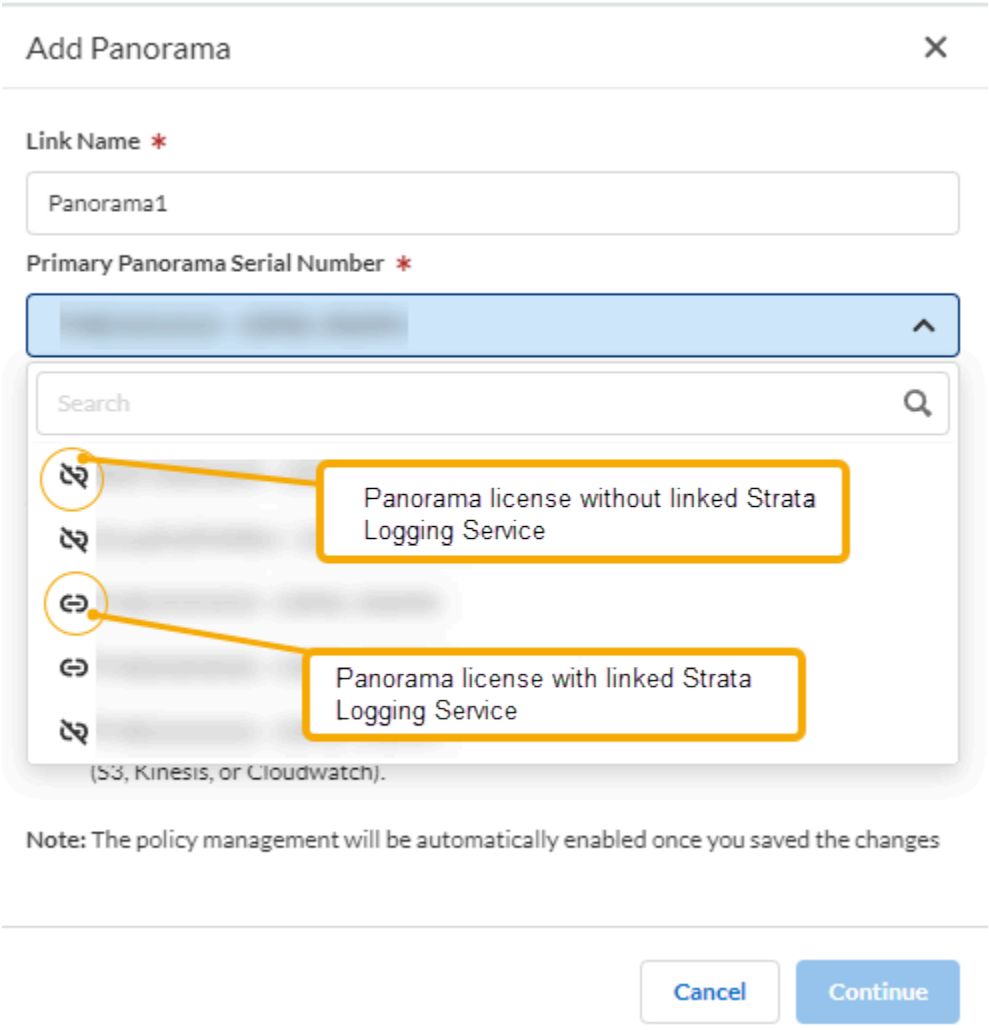


AWSファイアウォールマネージャを使用して作成されたPanoramaにリンクされたテナントを使用している場合、Cloud NGFW リソースのリンクを解除することはできません。

STEP 3 | **[Add Panorama (Panoramaの追加)]**画面で、リンク名を入力します。ドロップダウンからプライマリ**Panorama**のシリアルナンバーを選択します。HA環境では、ドロップダウンからセカンダリ**Panorama**のシリアルナンバーを選択します。



この画面には、Panoramaライセンスの状態を示す2つの異なるアイコンが表示されます。1つはCDLにリンクされたPanorama、もう1つはStrata Logging Serviceにリンクされていないpanoramaです。以下の画像は、これらのアイコンを示しています。

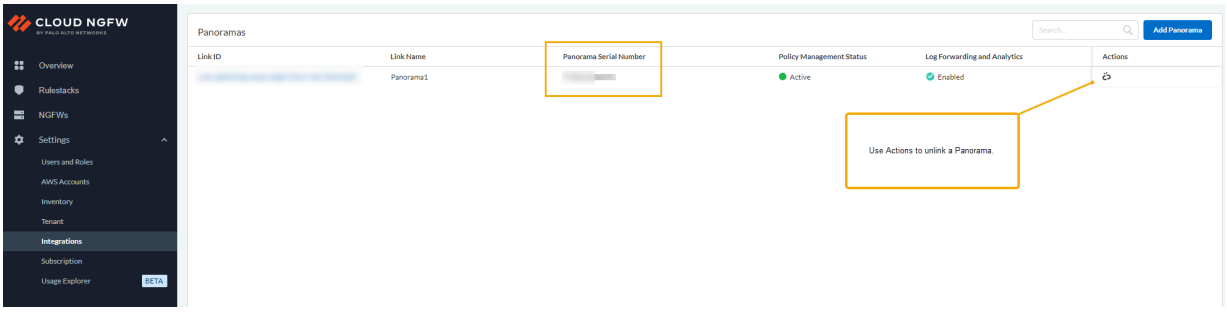


Strata Logging Serviceにリンクされていないpanoramaシリアルナンバーを選択した場合は、リンク処理をキャンセルするオプションを指定する必要があります。この場合は、CDLライセ

ンスを調達してPanoramaアプライアンスと関連付けることに同意するか、ポリシー管理にのみPanoramaを使用し続けることに同意します。

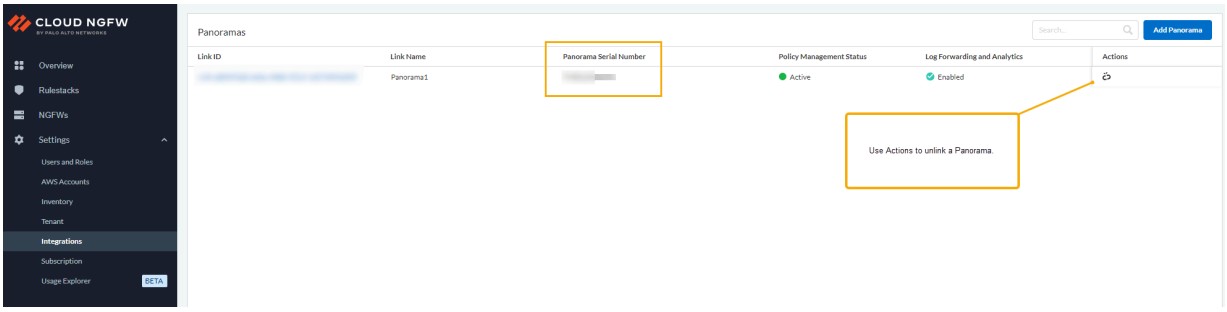
Strata Logging Serviceにすでに接続されているPanoramaライセンスを選択した場合は、統合プロセスを続行する前に関連付けを確認するメッセージが表示されます。

Panoramaライセンスを選択したら、**[Continue(**続行**)]**をクリックします。**[Integrations (**統合**)]**ページに切り替わり、リンク**ID**とリンクされた**Panorama**シリアルナンバーが表示されます。

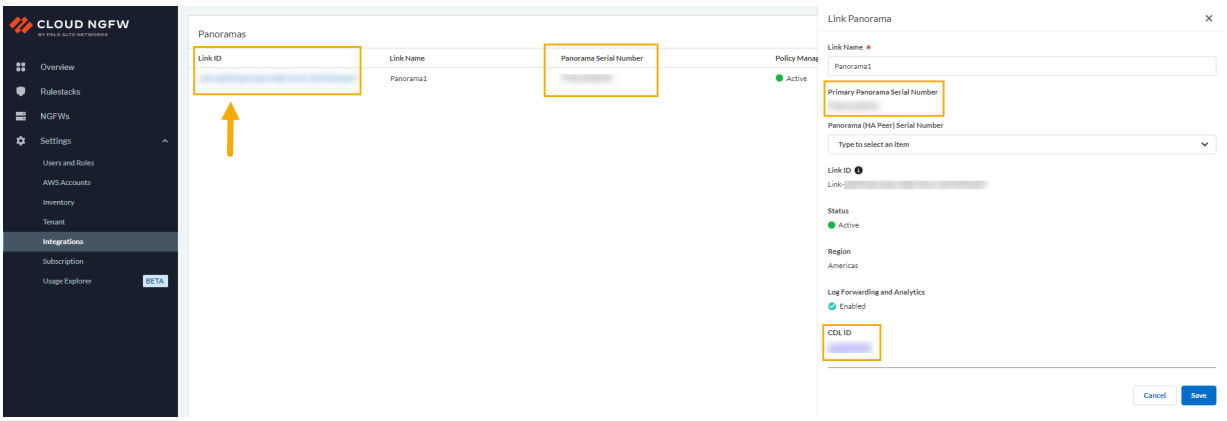


Cloud NGFW テナントは、Panorama から Strata Logging Service 情報を自動的に取得します。Strata Logging Serviceを使用する予定がない場合は、ログを AWS に送信できます。詳細については、「Cloud NGFW on AWS用のロギングの設定」を参照してください。

[Integrations (統合**)]**ページに切り替わり、リンク**ID**とリンクされた**Panorama**シリアルナンバーが表示されます。



リンクされた Panorama に関連付けられている Strata Logging Service ID などの追加情報については、 統合 ページのリンク **ID** をクリックしてください。**[Link Panorama(Panorama**のリンク**)]**ウィンドウが表示されます。



AWS MarketplaceからCloud NGFW テナントを登録解除する

Cloud NGFW テナントをAWS Marketplaceから登録解除するには:

STEP 1 | AWS管理コンソールにログインします。

STEP 2 | **[My Subscriptions(マイサブスクリプション)]**ページへ移動します。

STEP 3 | キャンセルする製品のサブスクリプションを選択します。

STEP 4 | **[Cancel subscription(サブスクリプションをキャンセル)]**を選択します。サブスクリプションをキャンセルすると、アプリケーションを起動できなくなります。

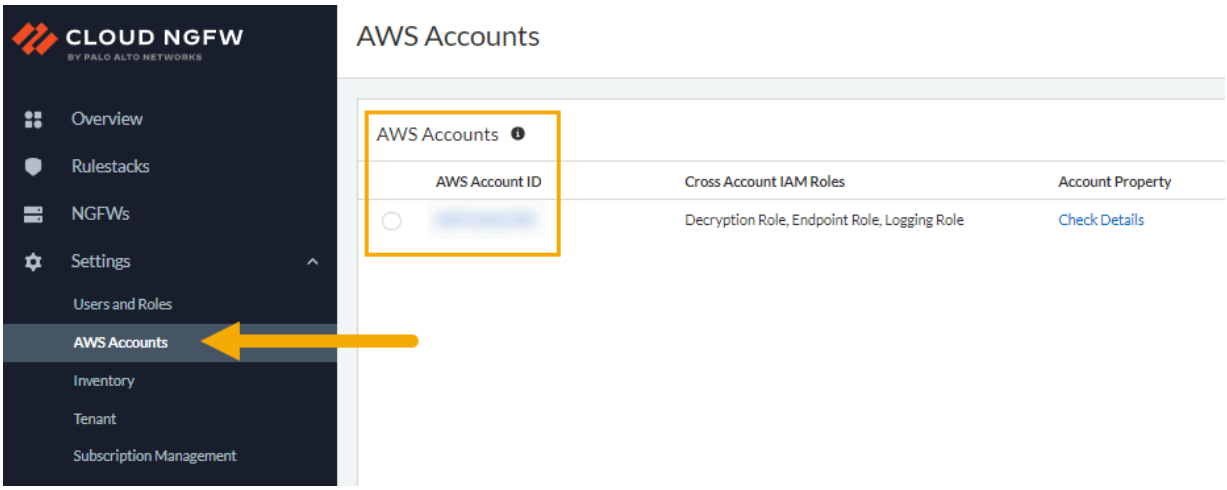
詳細については、「サブスクリプションをキャンセルする」を参照してください。

AWSファイアウォールマネージャを使用する際にPanoramaをCloud NGFW からリンク解除するためのサポートケースを作成する

AWSファイアウォールマネージャを使用していて、Cloud NGFW リソースをPanoramaにリンクしている場合は、Palo Alto Networksのサポートに連絡して、Cloud NGFWリソースをPanoramaからリンク解除する必要があります。サポートケースを作成する際に、AWSアカウントIDやリソースのテナントIDなどの追加情報の提供を求められる場合があります。

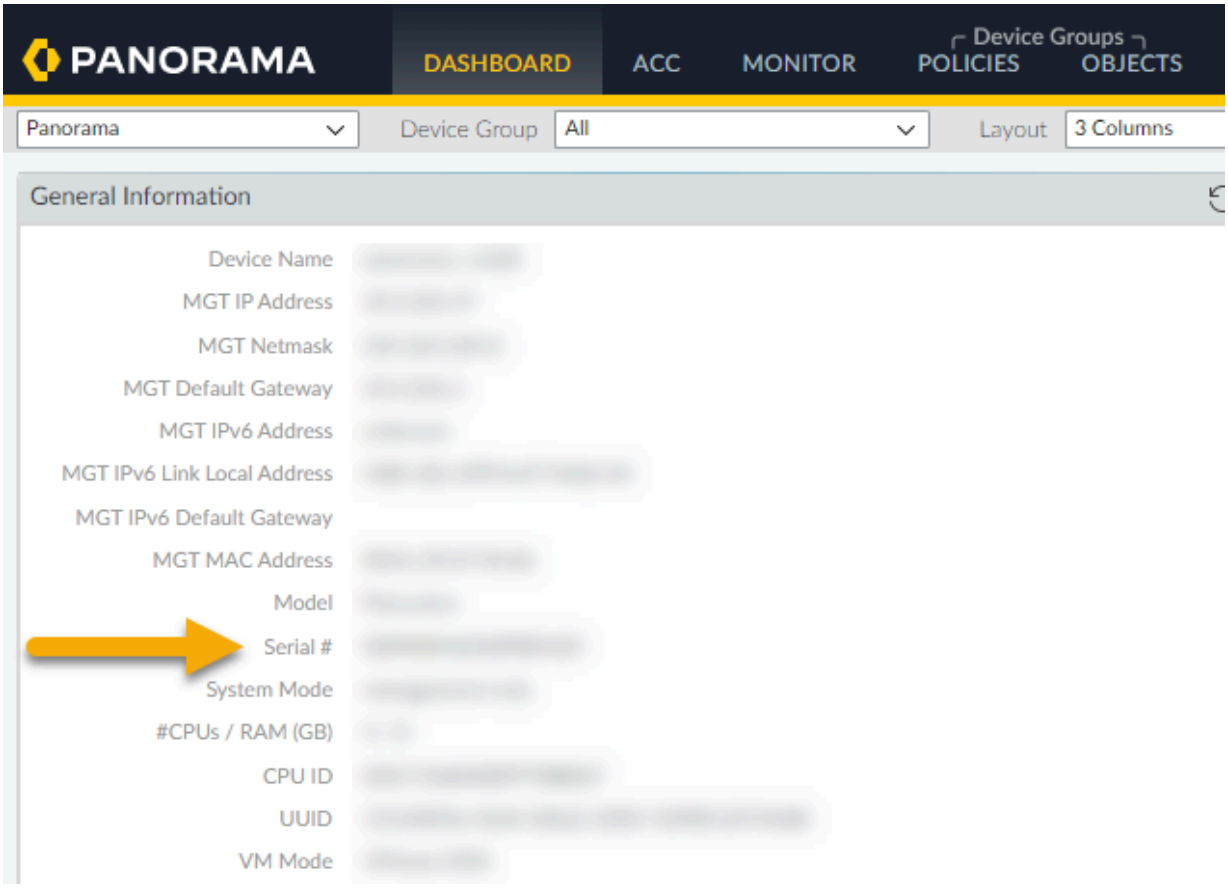
Cloud NGFWコンソールを使用してサポートケースを作成する方法:

STEP 1 | **AWS**アカウント**ID**を確認してください。**AWS** アカウントを選択します。

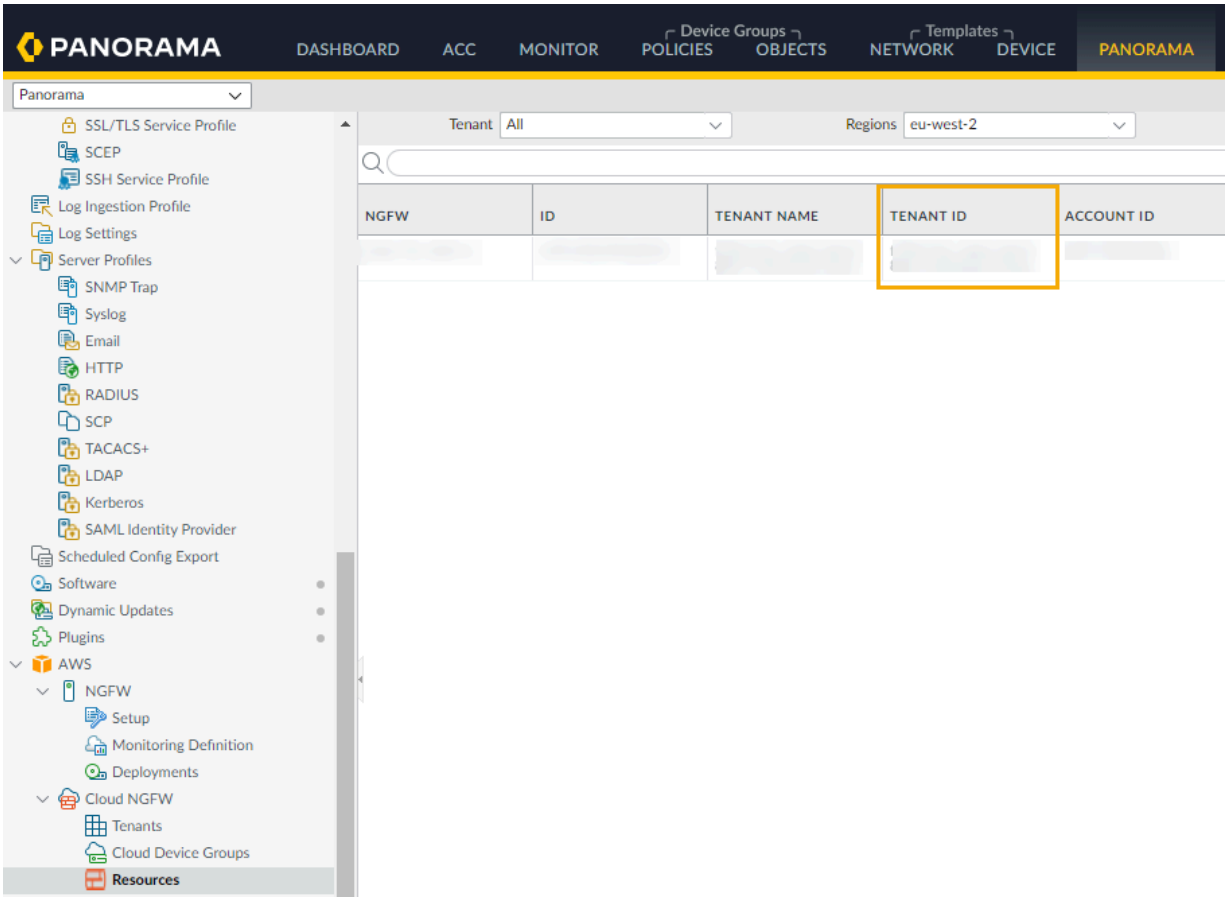


STEP 2 | 必要に応じて、Panoramaコンソールを使用して、テナントIDやPanoramaのシリアルナンバーなど、サポートケースに関する追加情報を確認してください。

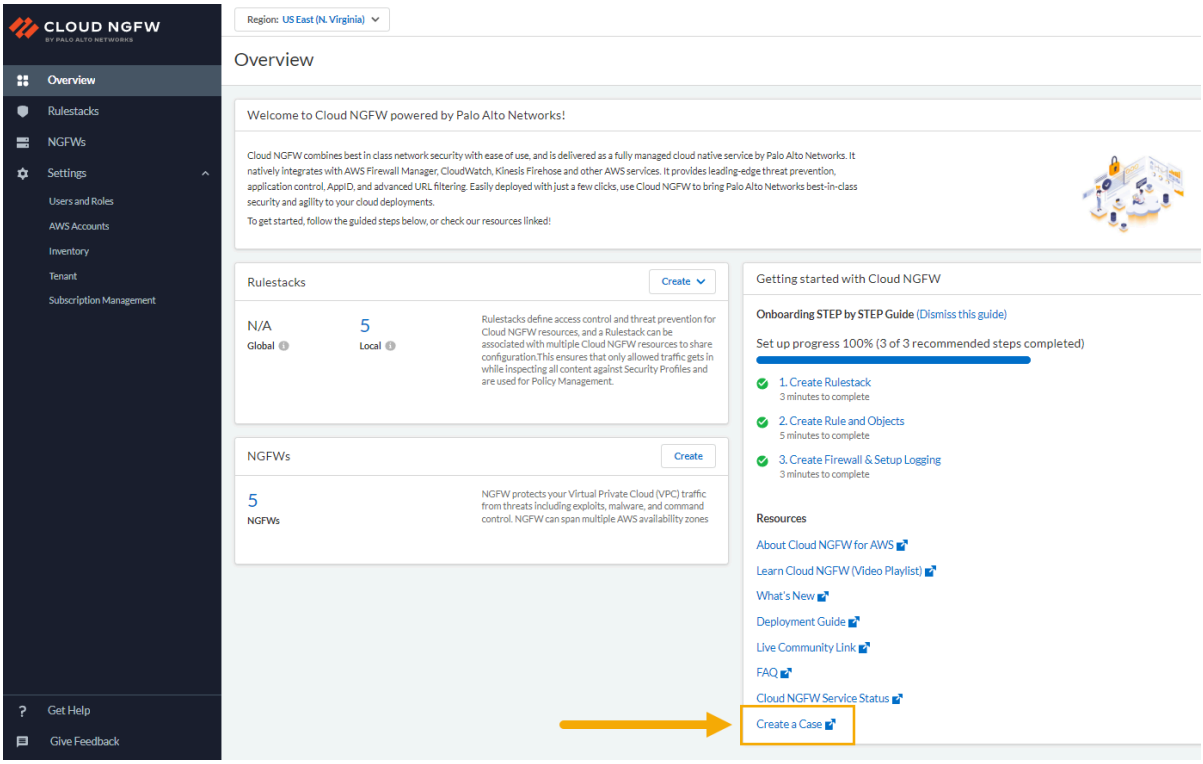
ダッシュボードを使用して**Panorama**のシリアルナンバーを確認してください。



Cloud NGFWリソースのテナント **ID**を確認します。



STEP 3 | Cloud NGFWコンソールの概要ページで、**[Create a case(ケースを作成)]**をクリックします。



リンクされたPanoramaをCloud NGFWリソースに関連付ける

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）

複数のPanoramaをCloud NGFWテナントにリンクする前に、Cloud NGFWリソースをPanoramaバーチャル アプライアンスに統合する必要があります。この統合のために、まずプラグインをインストールしてPanoramaアプライアンスを準備します。その後、Cloud NGFWコンソールを使用してPanoramaアプライアンスと連携する必要があります。Cloud NGFWとの連携に成功したら、Panoramaを使ってセキュリティ オブジェクトとルールを管理し、ログと分析を監視します。

STEP 1 | Panoramaを準備します。

STEP 2 | Panoramaをリンクします。

PanoramaをCloud NGFWリソースにリンクしたら、別のCloud NGFWテナントに関連付けることができます。

複数の**Panorama**を**Cloud NGFW**テナントにリンクする

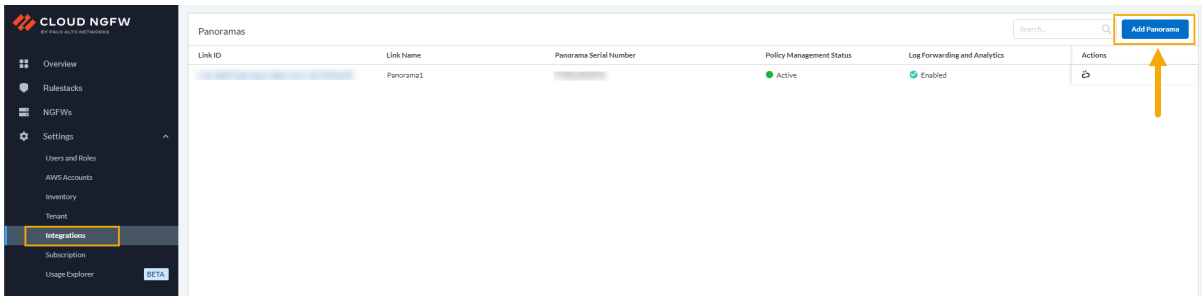
複数のPanoramaを同じCloud NGFWテナントにリンクする方法:

STEP 1 | Cloud NGFW コンソールにログインします。

STEP 2 | **[Integrations (統合)]**選択します。

[Integrations (統合)]ページには、現在リンクされているPanoramaに関する情報が表示されます。現在PanoramaがCloud NGFWテナントにリンクされていない場合、このページは空です。

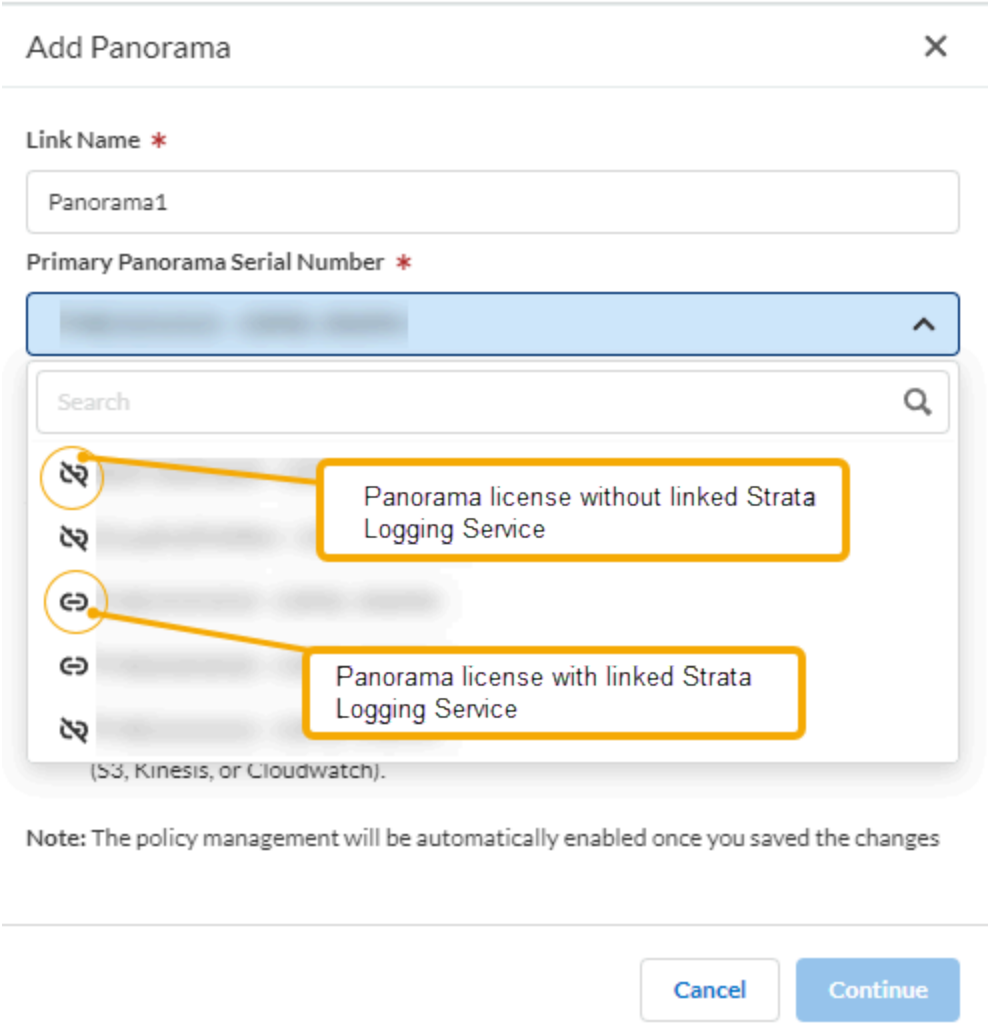
STEP 3 | **[Integrations (統合)]**ページを使用してPanoramaを追加します。**[Add Panorama (パノラマを追加)]**をクリックします。



STEP 4 | **[Add Panorama (パノラマの追加)]**画面で、リンク名を入力します。**[Primary Panorama Serial Number(プライマリPanoramaシリアルナンバー)]**ドロップダウンから現在リンクされ

ているPanoramaを選択します。HA環境では、ドロップダウンからセカンダリ**Panorama**のシリアルナンバーを選択します。

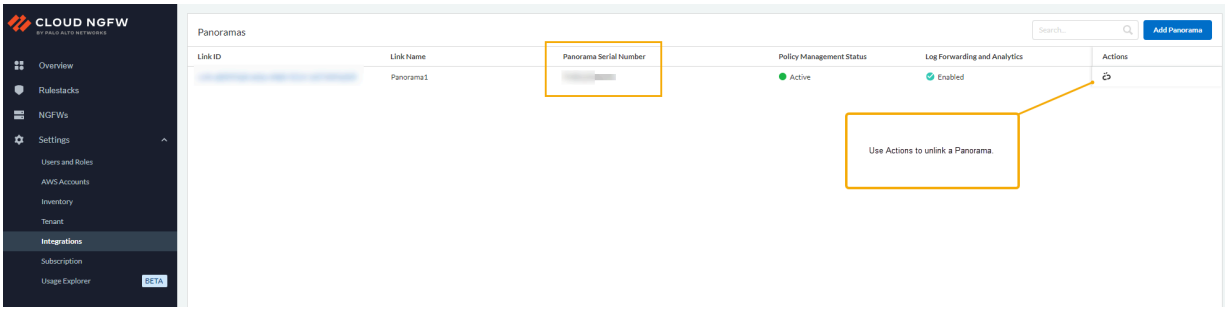
この画面には、Panoramaライセンスの状態を示す2つの異なるアイコンが表示されます。1つはCDLにリンクされたPanorama、もう1つはStrata Logging Serviceにリンクされていないpanoramaです。以下の画像は、これらのアイコンを示しています。



Strata Logging Serviceにリンクされていないpanoramaシリアルナンバーを選択した場合は、リンク処理をキャンセルするオプションを指定する必要があります。この場合は、CDLライセンスを調達してPanoramaアプライアンスと関連付けることに同意するか、ポリシー管理にのみPanoramaを使用し続けることに同意します。

Strata Logging Serviceにすでに接続されているPanoramaライセンスを選択した場合は、統合プロセスを続行する前に関連付けを確認するメッセージが表示されます。

STEP 5 | Panoramaライセンスを選択したら、**[Continue(続行)]**をクリックします。**[Integrations (統合)]**ページに切り替わり、リンク**ID**とリンクされた**Panorama**シリアルナンバーが表示されます。



STEP 6 | Cloud NGFWにPanoramaを追加したら、**[NGFWs]**をクリックし、Panoramaに関連付けるファイアウォールを選択します。

STEP 7 | **[Firewall Settings(ファイアウォール設定)]**タブを選択します。

STEP 8 | **[Policy Management (ポリシー管理)]**セクションまでスクロールします。**Panorama** を選択します。

STEP 9 | ドロップダウンメニューを使用して、ファイアウォールに関連付けるリンク**Panorama**を選択します。

STEP 10 | **[Save(保存)]**をクリックします。

STEP 11 | 手順6～10を繰り返して、別のPanoramaをリソースに含めます。

Cloud NGFW を Panorama からリンク解除する

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）

Palo Alto Networksは、Cloud NGFWリソースを Panoramaバーチャル アプライアンスからリンク解除する前に、Cloud NGFW リソースまたはリージョンに関連付けられているクラウド デバイス グループを削除するか、関連付けを解除することを推奨しています。詳細については、「クラウド デバイス グループを削除する」または「クラウド デバイス グループをリソースから関連付け解除する」を参照してください。

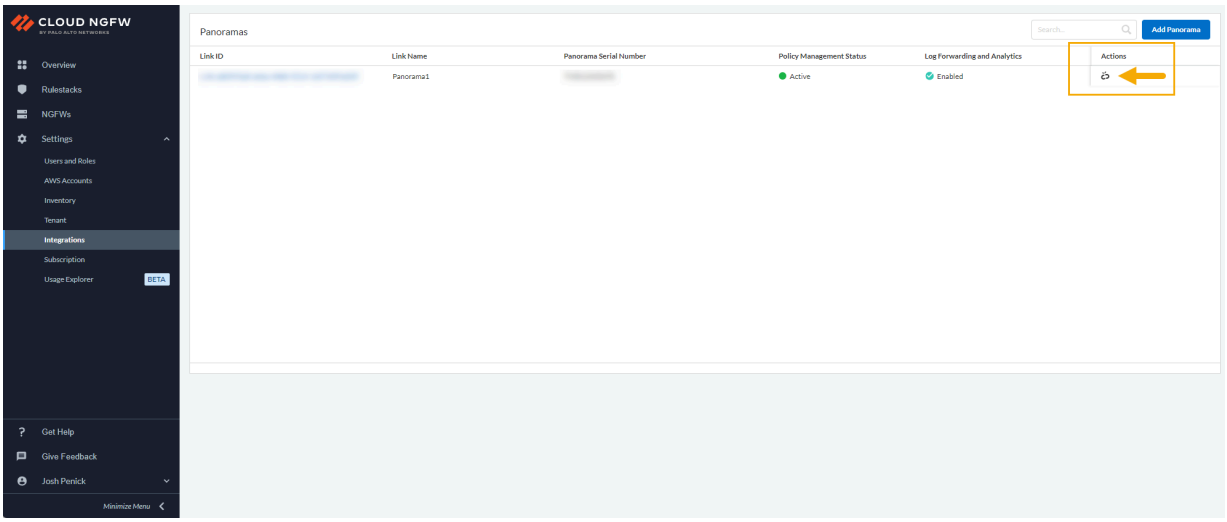
Panoramaバーチャル アプライアンスをCloud NGFW リソースからリンク解除する方法：

STEP 1 | ファイアウォールまたはルールスタック ページで、リージョン (たとえば **us-east-1**) を選択します。

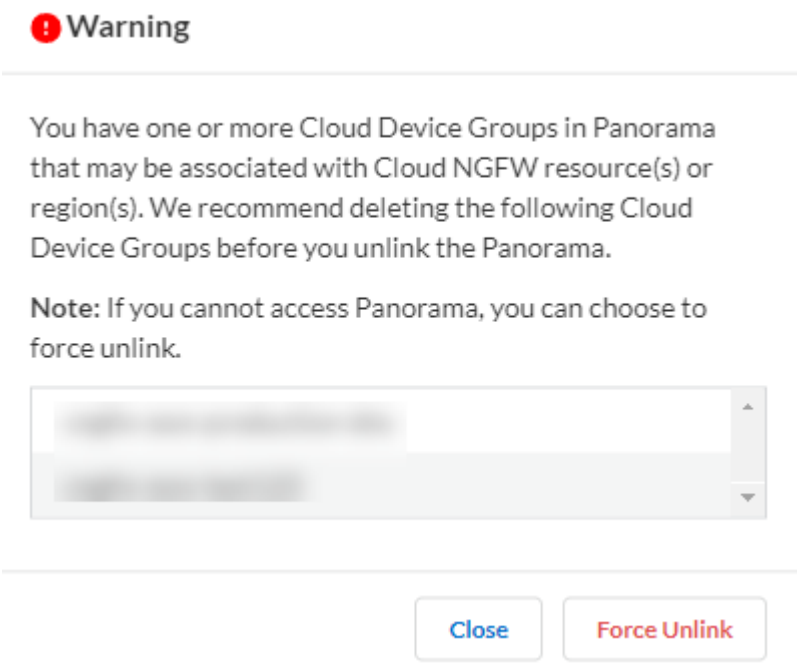
STEP 2 | Cloud NGFWコンソールで、**[Integrations(統合)]**を選択します。

STEP 3 | **[Integrations(統合)]**ページで、**[Actions(アクション)]**セクションを探します。。以前にリンクされたPanoramaはグレー表示されます。

STEP 4 | **[Unlink(リンク解除)]**アイコンをクリックして、リンク解除プロセスを開始します。HAペアが設定されている場合、両方のペアがリンク解除されます。



STEP 5 | Panoramaバーチャル アプライアンスをCloud NGFW テナントからリンク解除すると、リンクを解除するCloud NGFW リソースまたはリージョンに関連付けられている1つ以上のクラウド デバイス グループを削除するように求められる場合があります。このような場合、Panoramaにリンクされているリソースに関連付けられているクラウド デバイス グループを一覧表示するエラー メッセージが表示されます。リンクを解除する前に、クラウド デバイス グループを削除するか、クラウド デバイス グループをリソースから関連付け解除してください。Panoramaにアクセスしてこれらのクラウド デバイス グループを削除できない場合は、**[Force Unlink(**リンクを強制解除**)]**をクリックします。



STEP 6 | リンク解除プロセスを確認してください。PanoramaがStrata Logging Serviceアカウントに関連付けられている場合、保持期間が過ぎると、その関連付けは解除され、ログは削除されます。

リンク解除リクエストを確認すると、統合ページが変わり、Cloud NGFWリソースのステータスが表示されます。

Palo Alto Networksは、Panoramaに設定されているモニタリング定義を削除することを推奨しています。

強制リンク解除オプションを使用しても、モニタリング定義はPanoramaから自動的に削除されません。

CLIでのみ次のコマンドを実行して、テナント モニタリング定義を表示して削除できます。

```
request plugins dau plugin-name cloud_services unblock-device-push
 yes request plugins dau plugin-name cloudconnector unblock-device-
push yes request plugins dau plugin-name vm_series unblock-device-
push yes request plugins dau plugin-name aws unblock-device-push
 yes
```

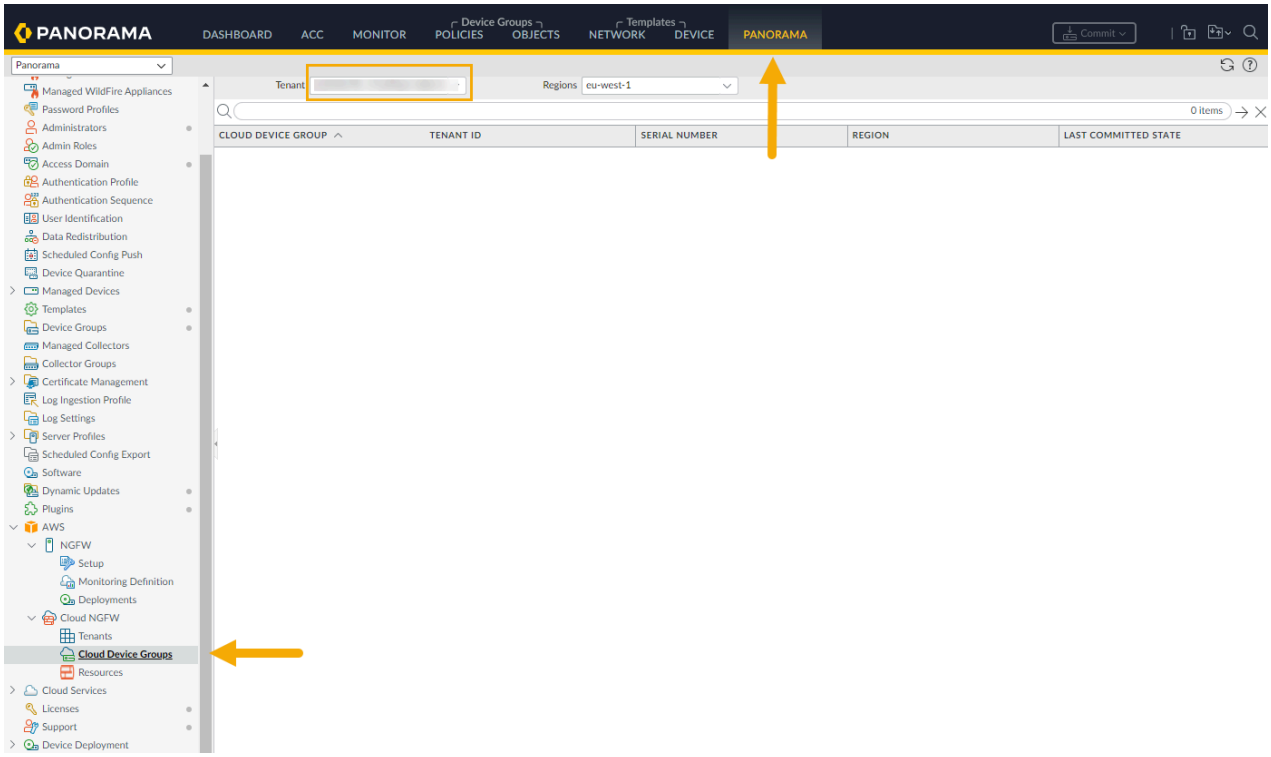
Cloud NGFW ポリシー管理に Panorama を使用する

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）

Cloud NGFWテナントをPanoramaバーチャル アプライアンスにリンクしたら、Panoramaコンソールを使用して、デバイス グループの追加やCloud NGFWテナントのデバイス グループへのポリシーの適用など、ポリシー管理タスクの統合の使用を開始できます。

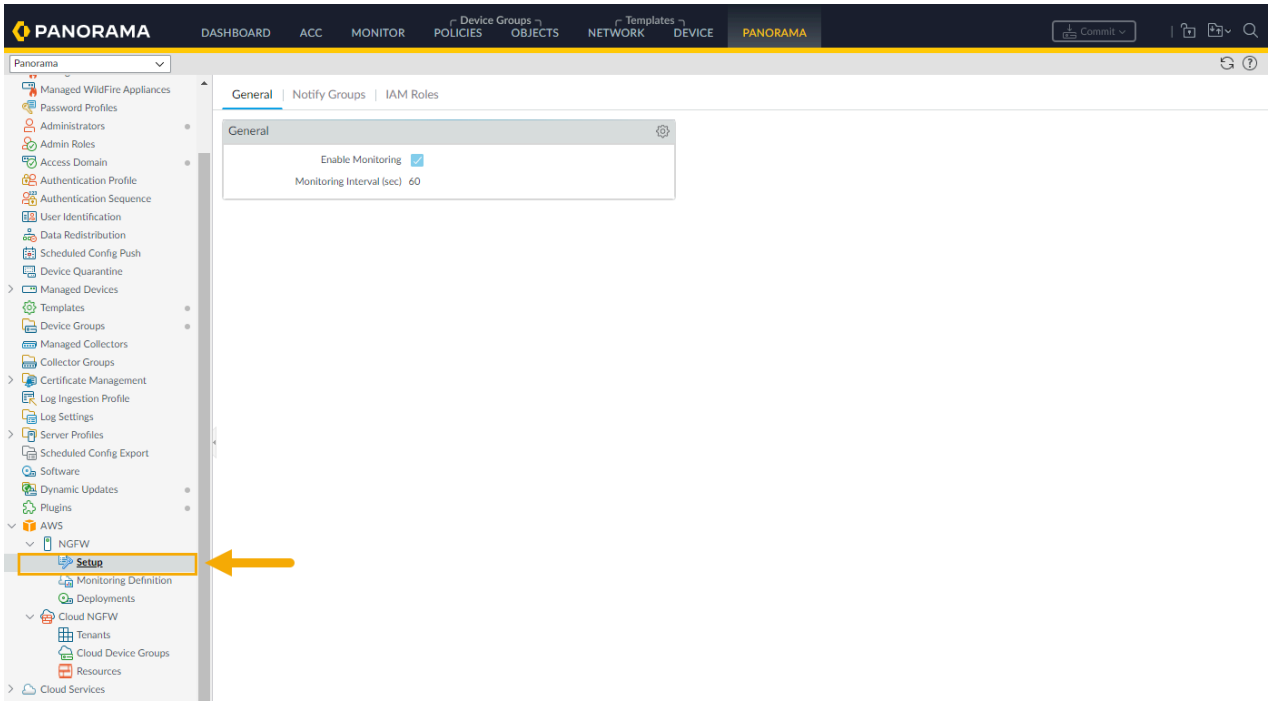
Panoramaコンソールを使用してCloud NGFWを設定すると、ブラウザはクラウド デバイス グループ、テンプレート スタック、リージョンなどのローカル情報をキャッシュするため、Panoramaタスクを切り替えると、キャッシュされたCloud NGFW情報がPanoramaコンソールに表示されます。

[クラウド デバイス グループ**]]**ノードからテナントを選択し、Panoramaで別の設定オプションに移動しても、**[Resources(**リソース**)]**ノードに戻ると、以前に選択したテナント ビューが保持されます。たとえば、リージョン内の単一のテナントを選択すると、そのテナントに設定されているクラウド デバイス グループが表示されます。

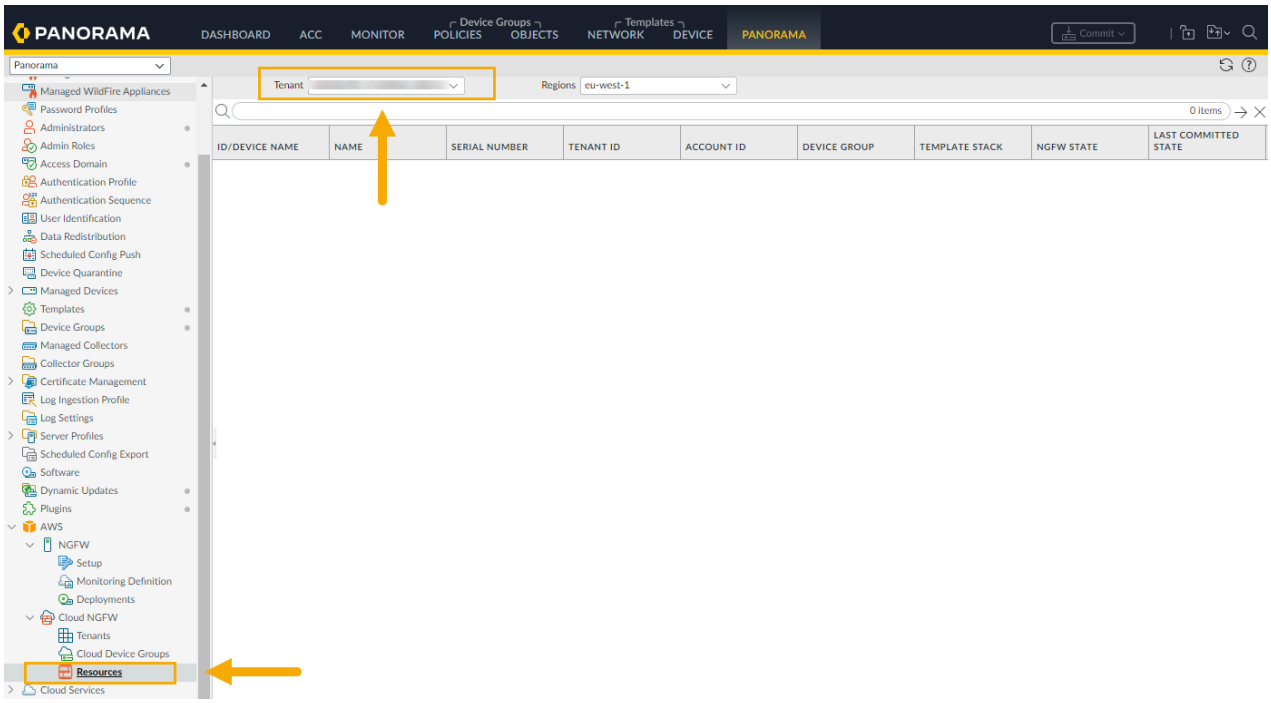


Panoramaコンソールで別の領域に移動してから［**Cloud NGFW**］ > ［**Cloud Device Groups(**クラウド デバイス グループ**)]**］に戻ると、以前に選択したシングル テナントがコンソールに

表示されます。たとえば、テナントのクラウド デバイス グループを表示したら、**[AWS]** > ［**Setup(セットアップ)]**を選択します。

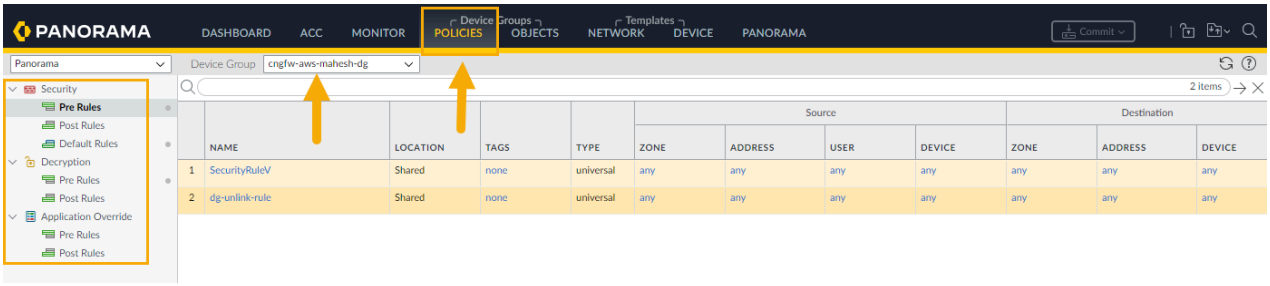


[Cloud NGFW] > [Resources(リソース)]画面に戻ると、Panoramaコンソールは**Cloud NGFW**リソースに関連付けられているすべてのテナントを表示するのではなく、以前に選択したテナントを記憶しています。



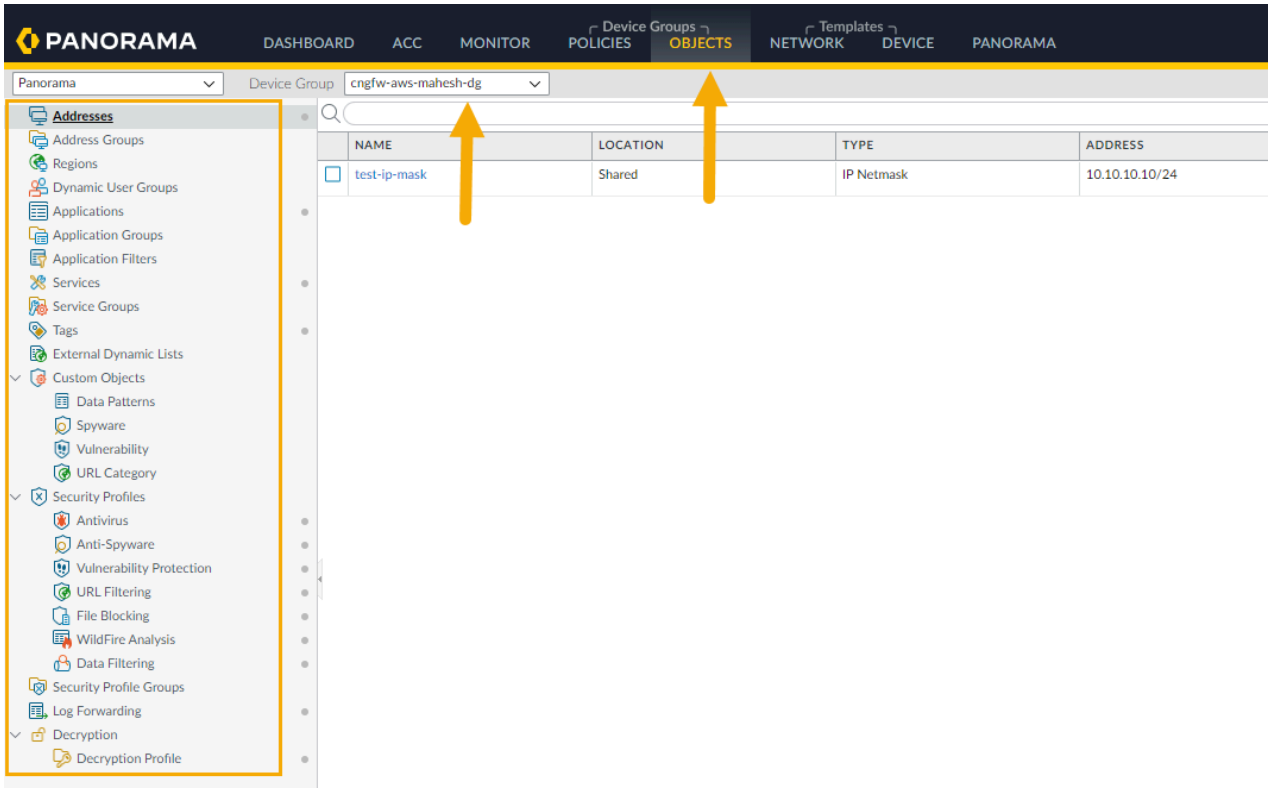
ブラウザを更新して表示をダイナミック更新します。

Panorama統合では、Cloud NGFWリソースで使用できる設定オプションのみが表示されます。たとえば、Cloud NGFWリソースで使用できるポリシー オプションを表示するには、**[Policies(**ポリシー**)]**を選択します。Panoramaコンソールには、Cloud NGFWクラウド デバイス グループで使用できるポリシーのみが表示されます。

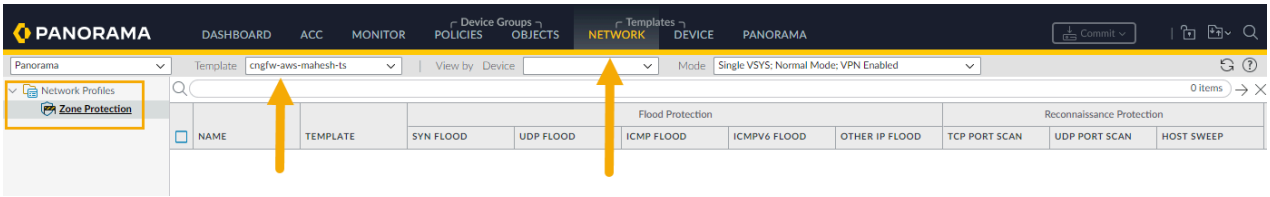


デバイス グループ名の先頭に *cngfw-aws* が付きます。

Cloud NGFWリソースでサポートされているデバイス グループ オブジェクトを表示するには、**[Objects(**オブジェクト**)]**を選択します。Cloud NGFWでサポートされているオブジェクトのみがPanoramaコンソールに表示されます。



Cloud NGFWリソースでサポートされているテンプレートを表示するには、［**Network(**ネットワーク**)**］を選択します。Cloud NGFWでサポートされているクラウド テンプレートのみが表示されます。



ルールスタックに関する考慮事項

ローカル ルールスタックでCloud NGFWリソースをプロビジョニングする場合、Panoramaのクラウド デバイス グループと関連付けることはできません。ファイアウォールはPanoramaコンソールでグレーで表示されます。この問題を解決するには、Cloud NGFWコンソールを使用してローカル ルールスタックの関連付けを解除するか、ローカル ルールスタックなしで新しいファイアウォール リソースをプロビジョニングし、Panoramaでクラウド デバイス グループに関連付けることができます。または、グローバル ルールスタックを使用します。

AWS Firewall Manager Service（FMS）を使用して作成されたファイアウォールの場合、Panoramaコンソールでルールスタックの選択を解除することはできません。FMSコンソールからPanoramaでプッシュされたグローバル ルールスタックを選択します。このプロセスは関連するルールスタックを削除し、Panoramaでプッシュされたグローバル ルールスタックでファイアウォールを更新します。詳細については、AWS FMSのドキュメントを参照してください。

クラウド デバイス グループを追加する

Panoramaでは、ネットワーク内のファイアウォールをデバイス グループと呼ばれる論理ユニットにグループ化します。デバイス グループを使用すれば、ネットワークのセグメント化、地理的なロケーション、組織の役割、あるいは類似のポリシー設定を必要とするファイアウォールに共通するその他の要素に基づいてグループ化を行うことができます。

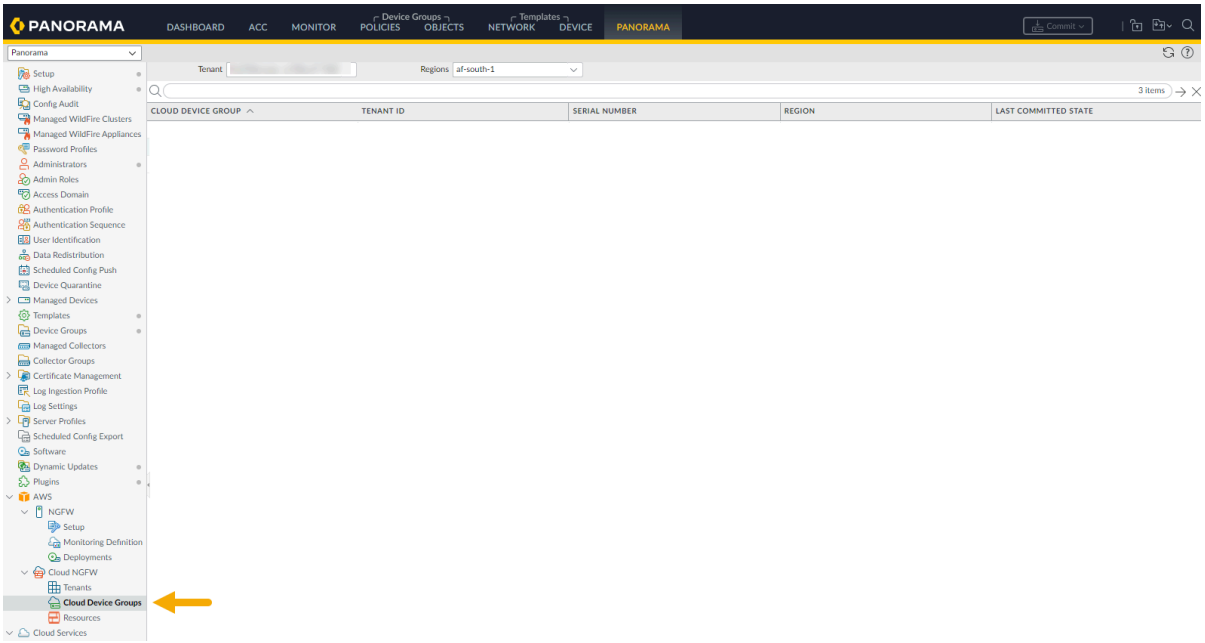
デバイスグループを使用し、ポリシールールやそれらが参照するオブジェクトを設定することができます。共有ルールおよびオブジェクトを最上層に、デバイス グループ固有のルールおよびオブジェクトをその配下に置くことで、デバイス グループを階層化することができます。これにより、ファイアウォールによるトラフィックの処理方法を強制するルールの階層を作成できます。詳細については、

「デバイス グループの管理」を参照してください。

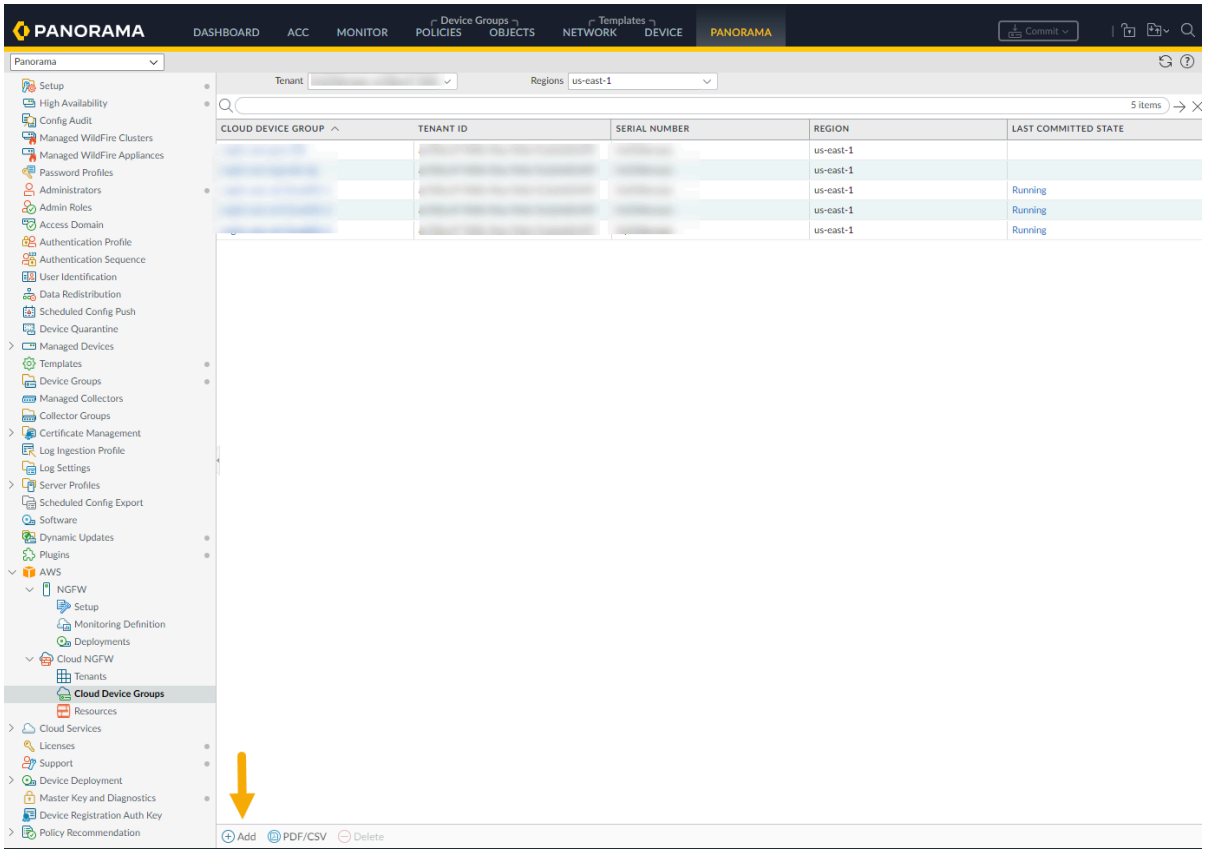
Panoramaコンソールを使用してクラウド デバイス グループを追加する方法:

STEP 1 | **AWS**プラグインで**[Cloud Device Groups(**クラウド デバイス グループ**)]**を選択します。最初に選択したときは、［Cloud Device Group(クラウド デバイス グループ)］テーブルは空で

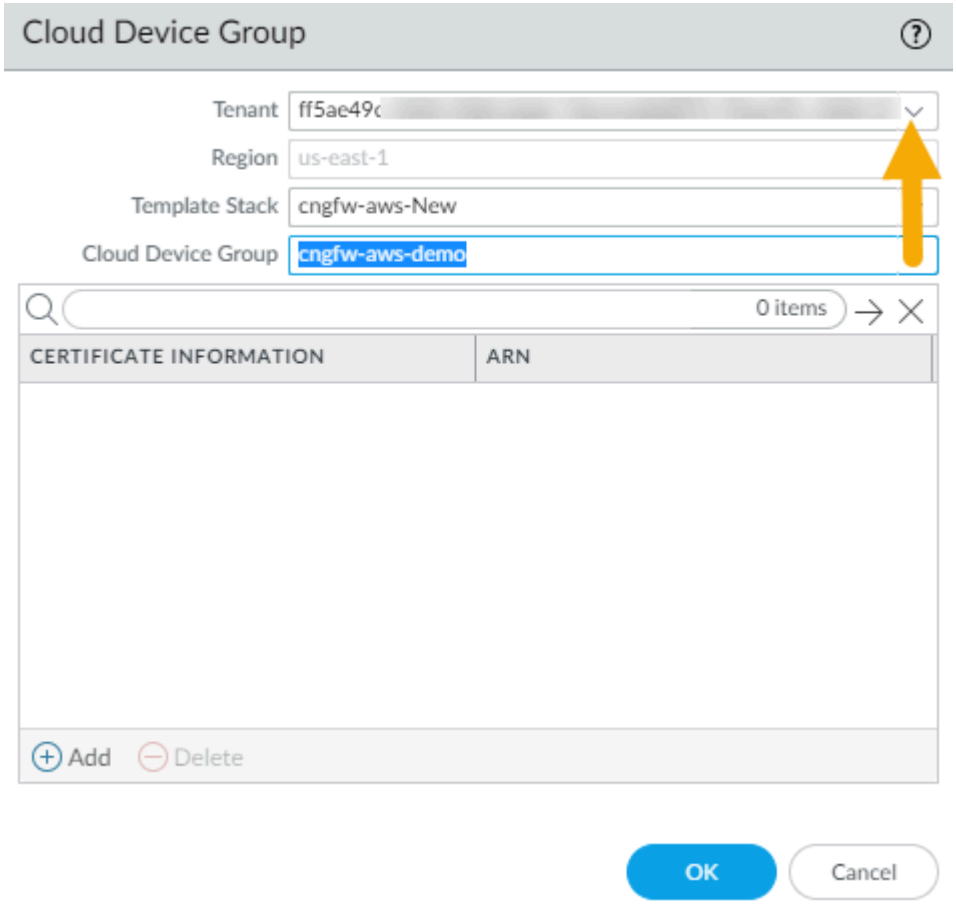
す。以前に作成したクラウド デバイス グループは、AWSを使用してCloud NGFWテナント用に確立されている場合に表示されます。



STEP 2 | 左下の**[Add(追加)]**をクリックします。



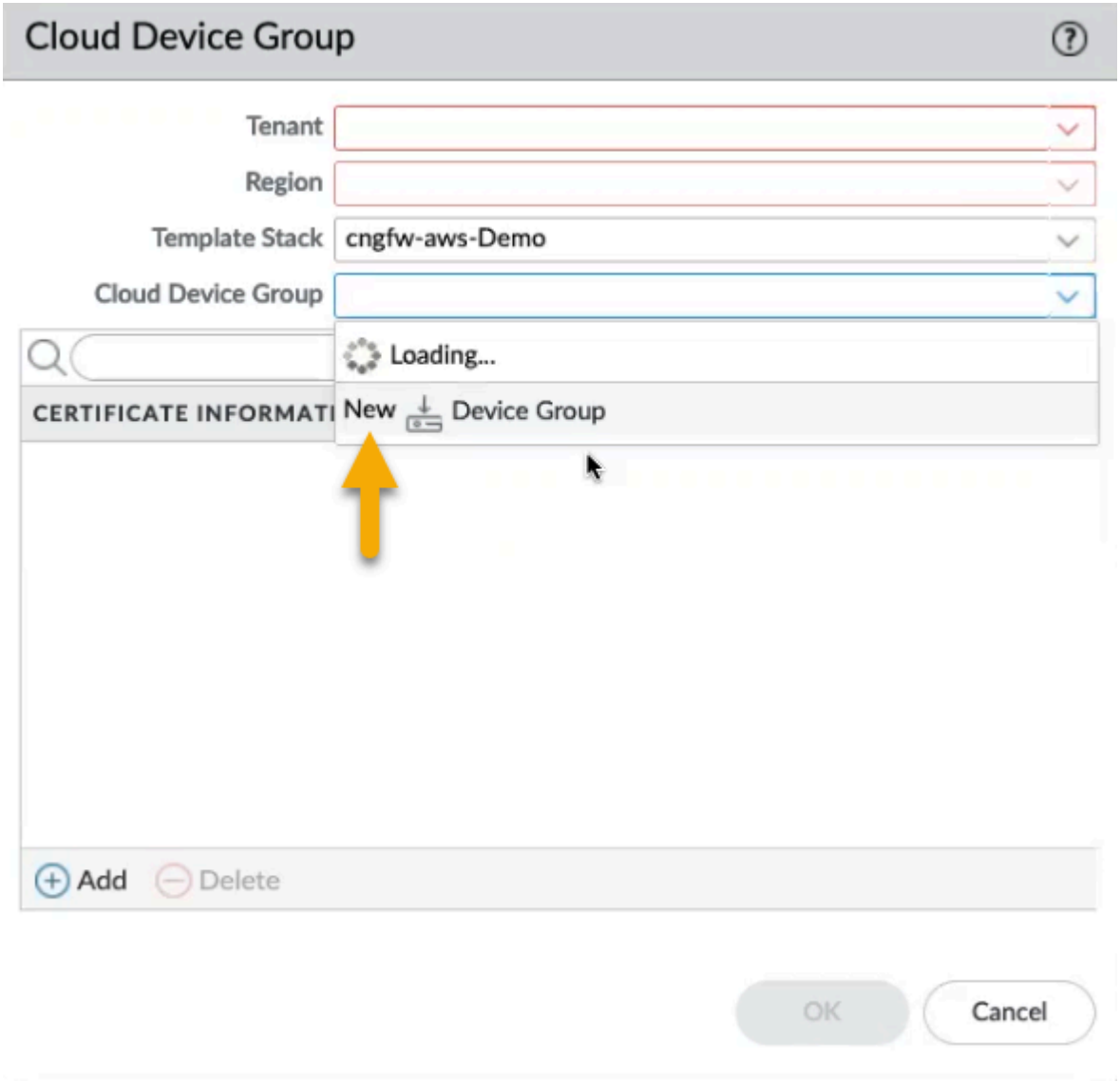
STEP 3 | **[Cloud Device Group(クラウド デバイス グループ)]**画面で、ドロップダウン メニューを使用して使用するテナントを選択します。



[Region(リージョン)]には、テナントが存在する地域が自動的に入力されます。

STEP 4 | 新しい**[Template Stack(テンプレートスタック)]**を作成するか、ドロップダウン メニューを使用して既存のテンプレート スタックを選択します。

STEP 5 | **[Cloud Device Group(クラウド デバイス グループ)]]**ドロップダウン メニューを選択し、**[New(新規)]**を選択します。



STEP 6 | デバイス グループのデバイス グループ名を入力し、**[Create(作成)]**をクリックします。

STEP 7 | **[OK]**をクリックして、クラウド デバイス グループをテナントに適用します。

STEP 8 | Panoramaネイティブ証明書を関連付けることも、ARNマッピングを指定することもできます。Cloud NGFW for AWSに証明書を追加したら、証明書の名前を入力し、ARNマッピングを交互に指定します。

STEP 9 | 変更をコミットします。

リソースからクラウド デバイス グループを削除する

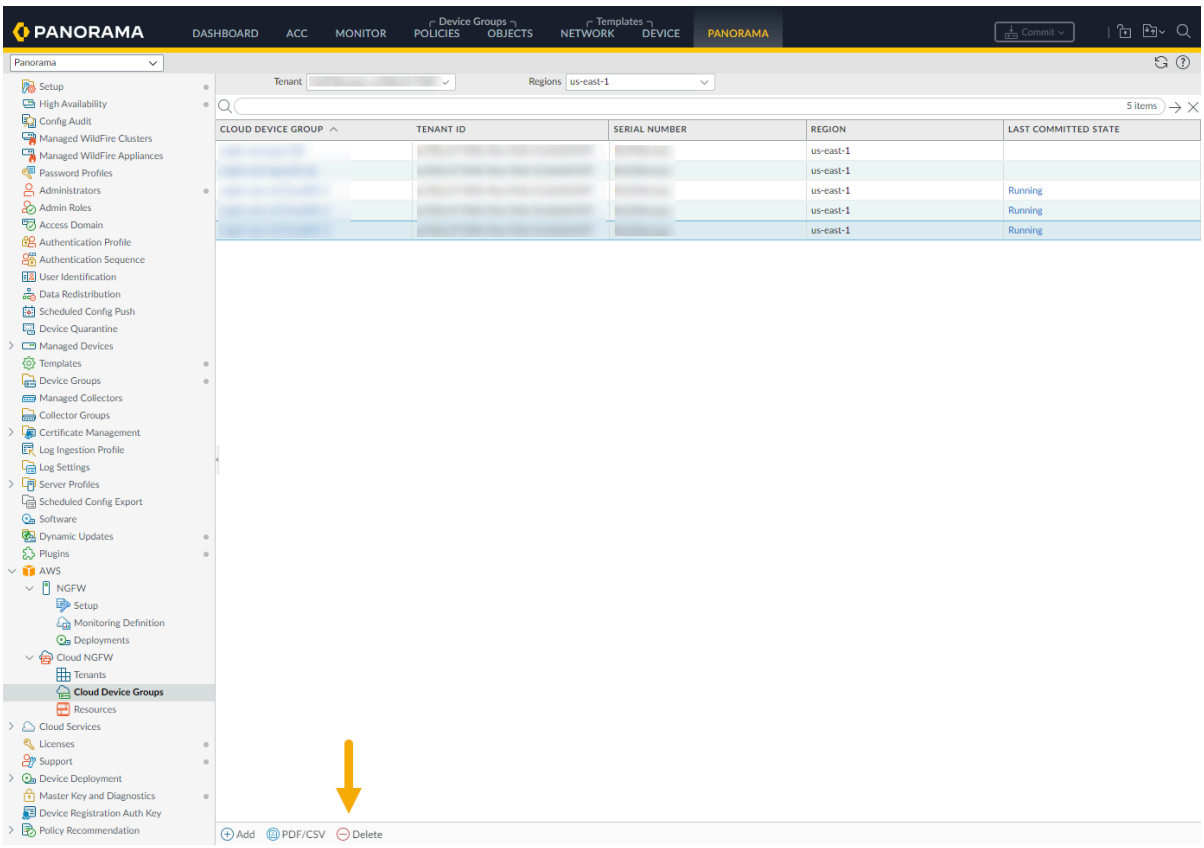
Panoramaコンソールを使用してクラウド デバイス グループを削除します。クラウド デバイス グループを削除できるのは、そのグループにファイアウォールが接続されていない場合のみです。

Panoramaコンソールを使用してクラウド デバイス グループを削除する方法:

STEP 1 | **Panorama**で**[Cloud Device Groups(**クラウド デバイス グループ**)]**を選択します。

STEP 2 | 削除するクラウド デバイス グループを選択します。

STEP 3 | Panoramaコンソールの下部にある**[Delete(削除)]**をクリックします。



STEP 4 | **[Yes(はい)]**をクリックして、削除を確認します。

STEP 5 | 変更をコミットします。

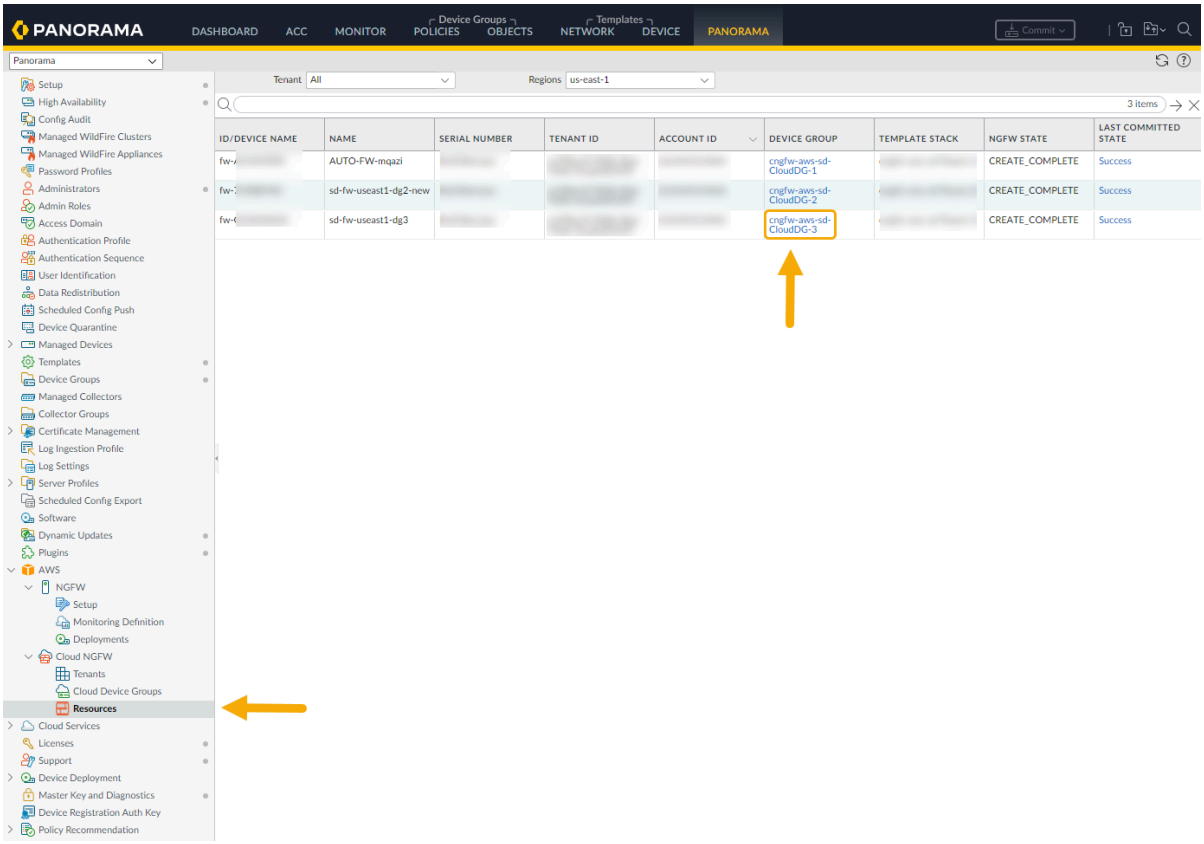
リソースへのクラウド デバイス グループの関連付け

Panoramaコンソールを使用して、クラウド デバイス グループをCloud NGFWリソースに関連付けます。リソースに関連付けずにクラウド デバイス グループをプッシュできます。ただし、リソースでクラウド デバイス グループ設定を使用する場合は、クラウド デバイス グループを関連付ける必要があります

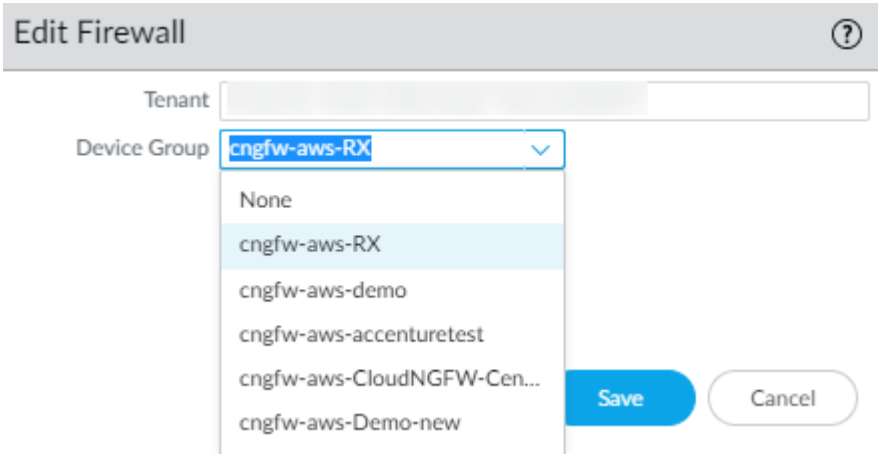
Panoramaコンソールを使用してクラウド デバイス グループをCloud NGFWリソースに関連付けるには、次の手順を実行します。

STEP 1 | **Panorama**で**[Resources(**リソース**)]**を選択します。

STEP 2 | デバイス グループを選択します。



STEP 3 | **[Edit Firewall(ファイアウォールの編集)]**画面でドロップダウン メニューを使用して、Cloud NGFWリソースに関連付けるクラウド デバイス グループを選択します。



STEP 4 | **[Save(保存)]**をクリックします。

STEP 5 | 変更を **Commit**（コミット）します。

STEP 6 | 変更をデバイスにプッシュします。

リソースからのクラウド デバイス グループの関連付けの解除

Panoramaコンソールを使用してCloud NGFWリソースからクラウド デバイス グループの関連付けを解除するには、次の手順を実行します。

STEP 1 | **Panorama**で**[Resources(リソース)]**を選択します。

STEP 2 | NGFWリソースのデバイス グループを選択します。

STEP 3 | **[Edit Firewall(ファイアウォールの編集)]**画面で、**[Device Group(デバイス グループ)]**ドロップダウンから**[None(なし)]**を選択します。[Save（保存）]をクリックします。

ポリシーの適用

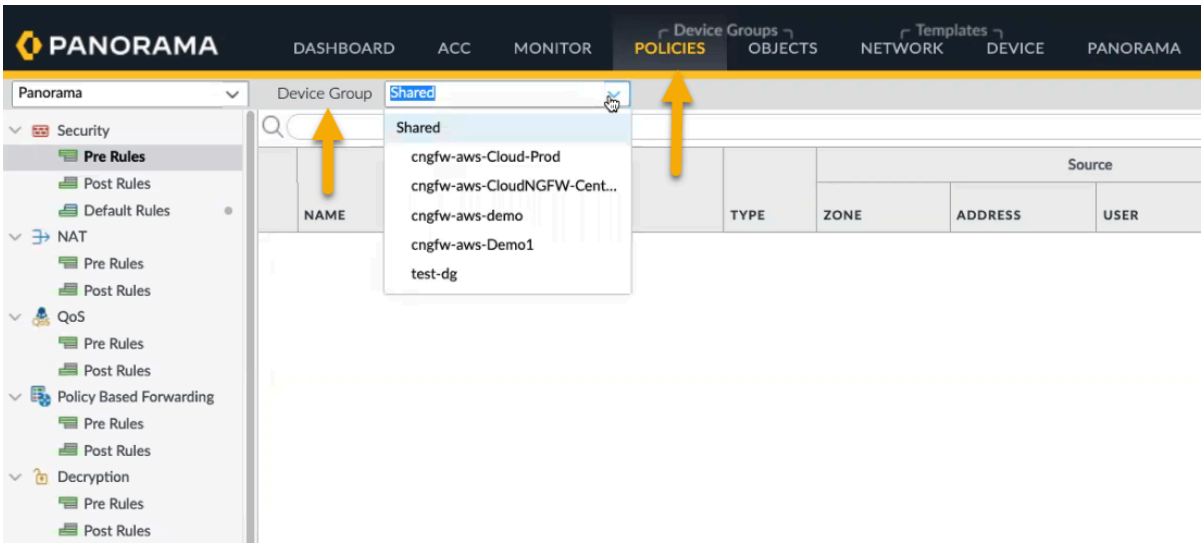
Panorama™のDevice Groups（デバイス グループ）を使用すると、ファイアウォール ポリシーを一元的に管理できます。Panorama 上に定義されるポリシーは、プレ ルールまたはポスト ルールとして作成されます。プレ ルールとポスト ルールにより、階層的な方法でポリシーを実装できます。詳細は、「Panoramaのポリシーの定義」を参照してください。

*Panorama*上で作成されたポリシーは、グローバルなルールスタックを作成します。ファイアウォールは*Panorama*で生成されたルールとテナントで生成されたルールを持つことはできません。ルールは*Cloud NGFW*または*Panorama*で作成する必要があります。

Panoramaでクラウド デバイス グループのポリシーを設定する方法:

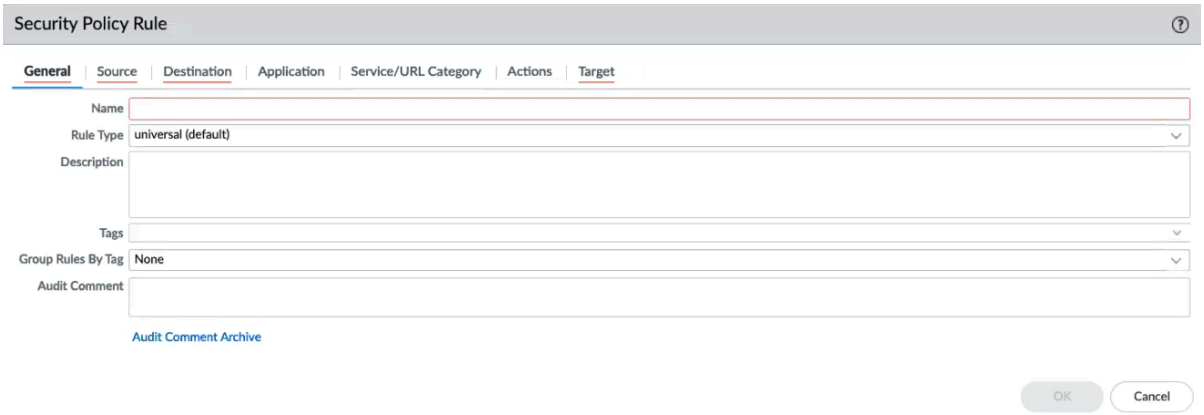
STEP 1 | **Policies (**ポリシー**)**を選択します。

STEP 2 | **[Device Group(**デバイスグループ**)]**セクションで、ドロップダウン メニューを使用して、以前に作成した**[Cloud Device Group(**クラウド デバイス グループ**)]**を選択します。Cloud NGFWのデバイス グループを作成すると、名前は*cngfw*で始まります。たとえば、*cngfw-aws-demo*となります。



STEP 3 | コンソールの左下にある**[Add(**追加**)]**をクリックします。

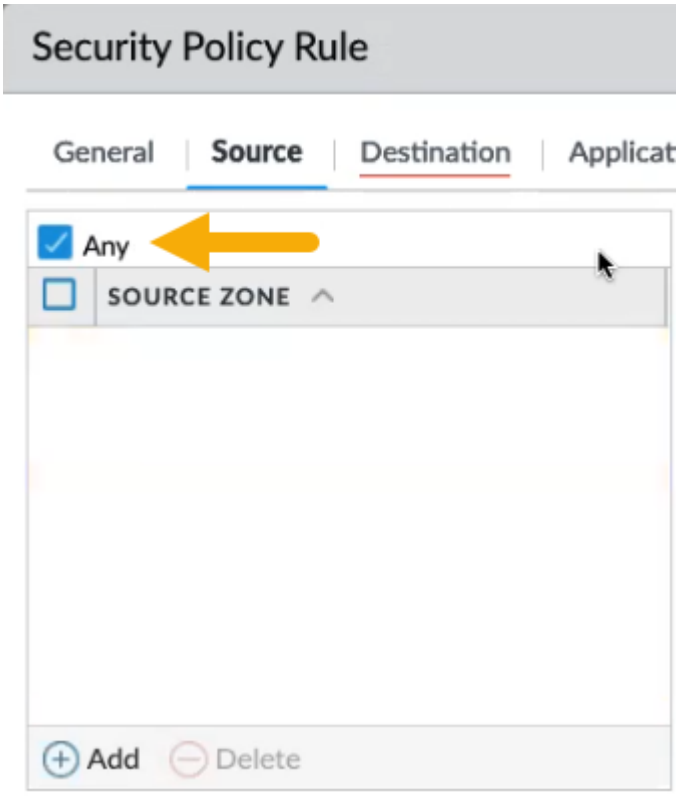
STEP 4 | [Security Policy Rule(セキュリティ ポリシー ルール)]画面で、デバイス グループに適用するポリシーの要素を設定します。



STEP 5 | **[General(全般)]**タブで、ポリシーの名前を含めます。

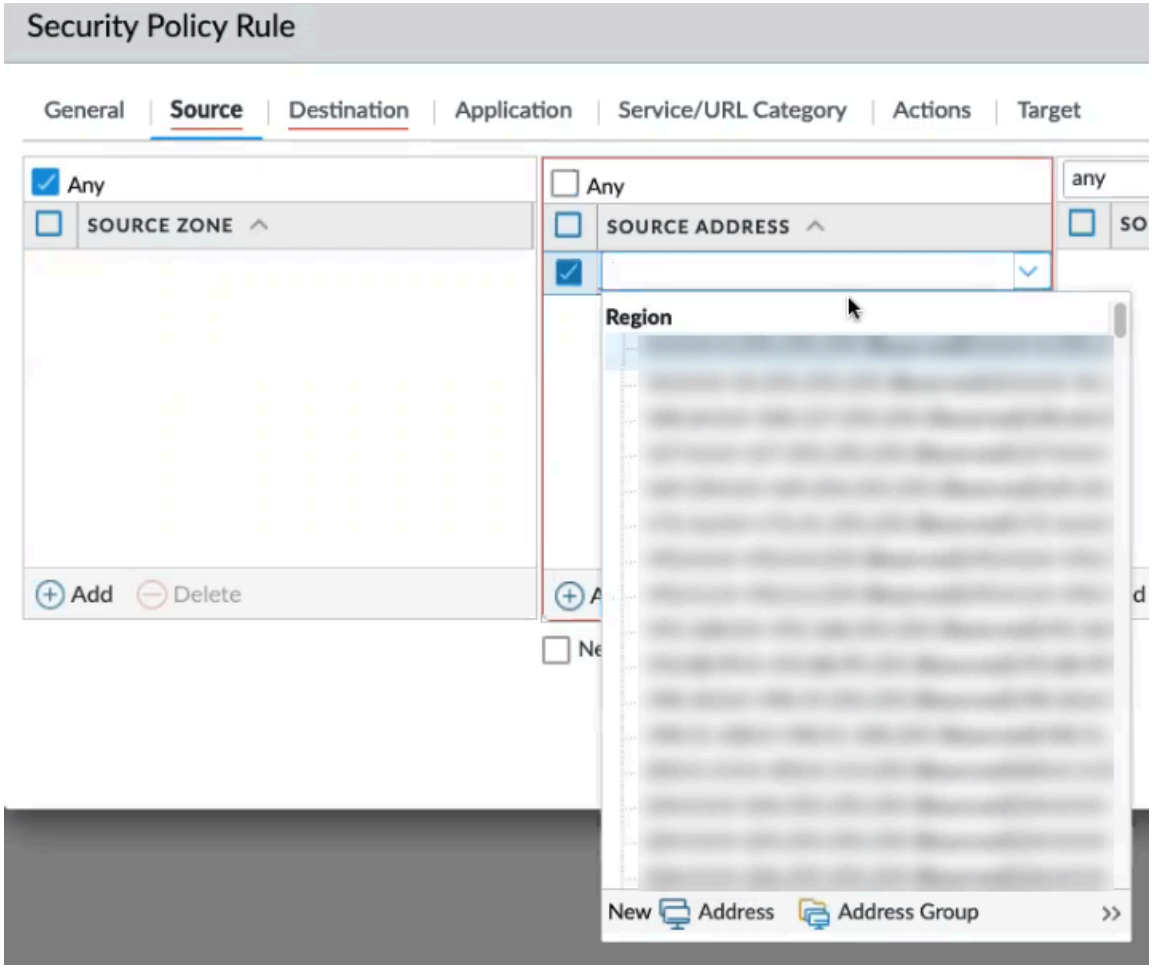
STEP 6 | **[Source(送信元)]**ポリシーを設定します。**[Source(送信元)]**ポリシーは、トラフィックの送信元となる送信元ゾーンまたは送信元アドレスを定義します。**[Source Zone(送信元ゾーン)]**」

については、**[Any(任意)]**をクリックします。特定の送信元アドレスを追加することはできません。



1. **[Source Address(送信元アドレス)]**を含めて、**[Source(送信元)]**の適用を続行します。**[Any(任意)]**をクリックするか、ドロップダウン メニューを使用して既存のアドレ

スを選択するか、オプションを使用して新しいアドレスまたはアドレス グループを追加します。

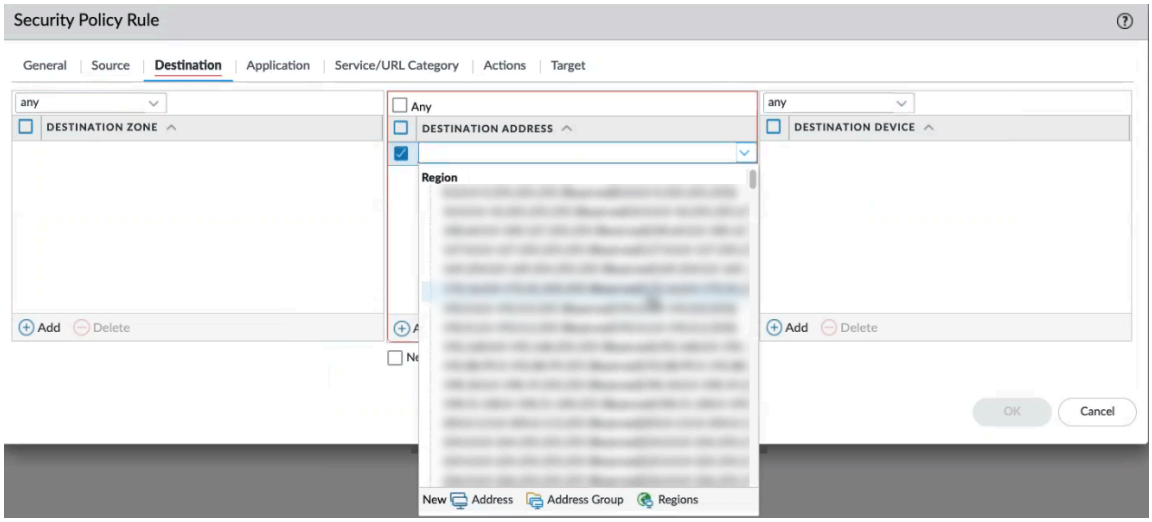


2. ［**Source User(送信元ユーザー)]**および**[Source Device(送信元デバイス)]**ポリシーの場合は、［**Any(任意)**］をクリックします。Cloud NGFWは特定の送信元ユーザーや送信元デバイスの指定をサポートしていない

STEP 7 | 宛先ポリシーは、トラフィックの宛先ゾーンまたは宛先アドレスを定義します。ドロップダウンメニューを使用して既存のアドレスを選択するか、オプションを使用して新しいアドレスまたはアドレス グループを追加します。宛先ポリシーには、ゾーン、アドレス、およびデバイスのフィールドが含まれます。

1. **[Destination Zone(宛先ゾーン)]**で、**[Any(任意)]**をクリックします。Cloud NGFWは個別の宛先ゾーンの追加をサポートしていません。

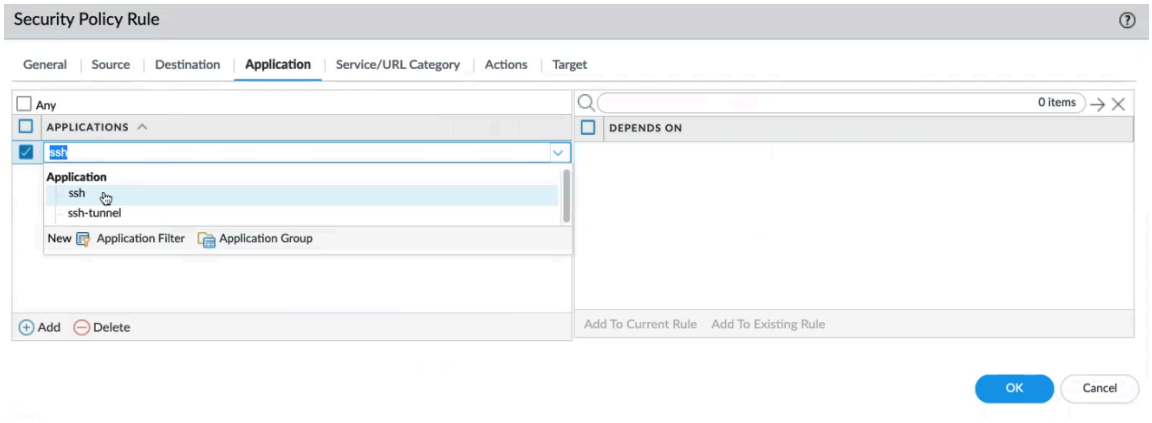
2. **[Destination Address(宛先アドレス)]**で、**[Any(任意)]**をクリックするか、ドロップダウンメニューを使用して既存のゾーンを選択します。［**New(新規)**］をクリックして、新しいアドレス、アドレス グループ、または地域を追加します。
3. **[Destination Device(宛先デバイス)]**で、**[Any(任意)]**をクリックします。Cloud NGFWは、個別の宛先デバイスの追加をサポートしていません。



STEP 8 | **Application**ポリシーを設定して、アプリケーションまたはアプリケーション グループに基づいて、ポリシーがアクションを実行するように設定します。管理者は、既存の App-ID™ シグネチャを使用し、カスタマイズして、独自のアプリケーションや、既存のア

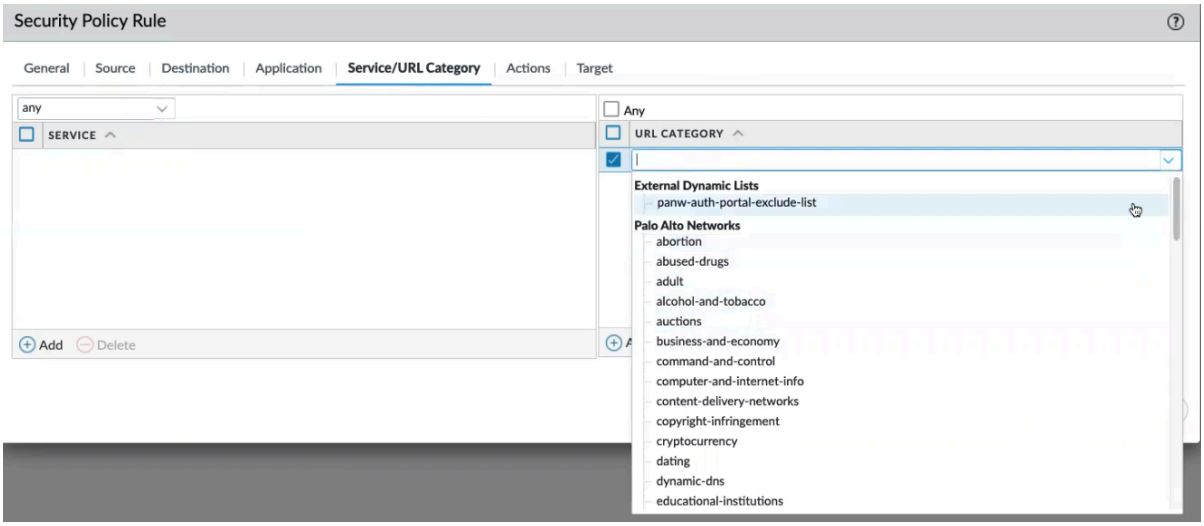
プリケーションの特定の属性を検出することもできます。カスタム アプリケーションは**ObjectsApplications**で定義されます。

1. **[Application(アプリケーション)]**画面で**[Any(任意)]**をクリックするか、SSHなどの特定のアプリケーションを指定します。新しいアプリケーションポリシーを含めるには**[Add(追加)]**をクリックします。



STEP 9 | ファイアウォール用に**[Service/URL Category**（サービス/**URL** カテゴリ）**]**を設定して特定のTCPやUDPのポート番号またはURLカテゴリをポリシーの一致条件として設定します。**[Any(任意)**］を選択してサービス レベル ポリシーまたは**URL**カテゴリー ポリシーを指定するか、ドロップダウン オプションを使用して適用するポリシー要素を個別に選択しま

す。**[Add(追加)]**をクリックして、サービスまたはURL/カテゴリの新しいポリシーを作成します。



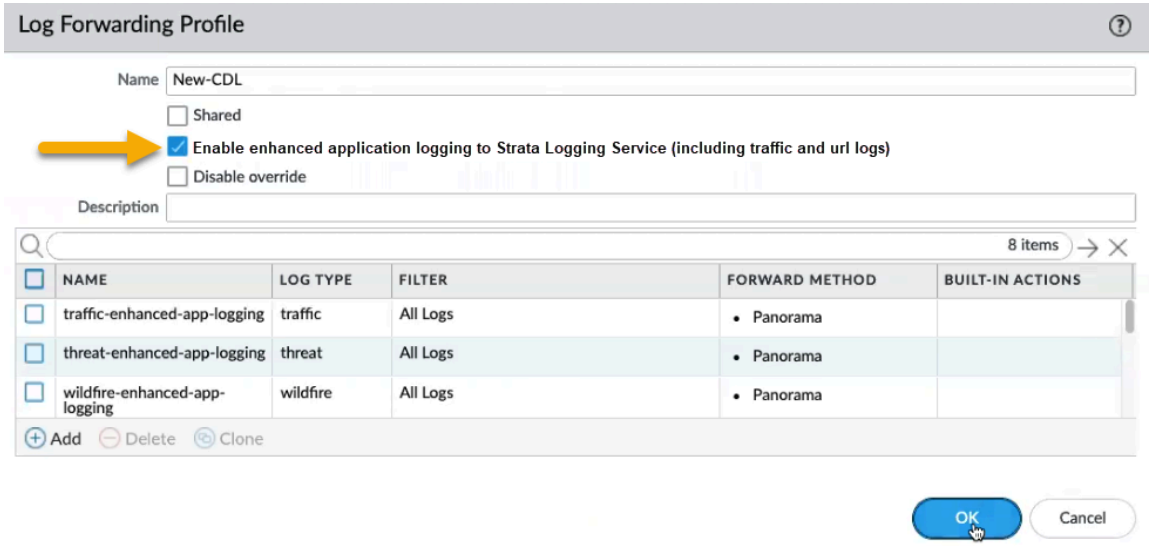
STEP 10 | 定義されたポリシー属性に一致するトラフィックに基づいて実行されるアクションを決定するアクションポリシーを設定します。

1. **[Actions(アクション)]**画面で、実行するアクション(許可や拒否など)を選択し、**[Profile Setting(プロファイル設定)]**を決定し、**[Log Setting(ログ設定)]**などの設定を行います。

   Panoramaログの使用方法については、「集中型ロギングおよびレポート」および「ログの表示」を参照してください。

2. オプションで、セキュリティ ポリシー ルール画面を使用してログをStrate Logging Serviceに転送することができます。**[Log Setting(ログ設定)]**フィールドで、**[Log Forwarding(ログ転送)]**ドロップダウンを選択し、**[New Profile(新しいプロファイル)]**をクリックします。ログ転送プロファイルで、ログの名前を入力し、**[Enable enhanced application logging to Strata Logging Service (including traffic and url logs)(Strata Loggin**

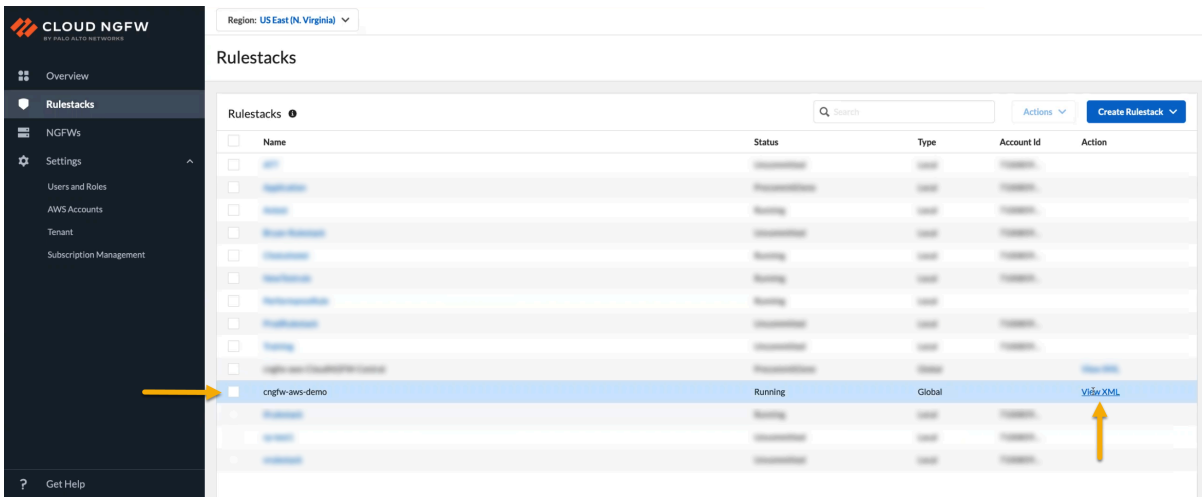
Serviceへの高度なアプリケーションロギングを有効にする(トラフィックと**URL**ログを含む))]を選択します。**[OK]**をクリックします。



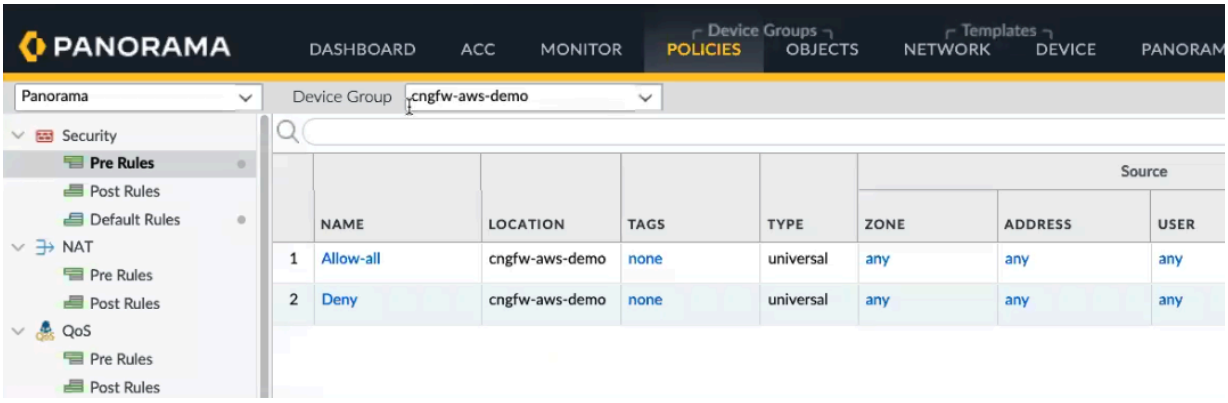
Strata Logging Serviceの詳細については、「ログの調査」を参照してください。

STEP 11 | Cloud NGFWコンソールに戻り、Panoramaで作成したルールを表示します。**[View XML(XML**の表示**)]**をクリックすると、Panoramaからクラウド デバイス グループに適用さ

れているグローバル ルールスタックにプッシュされたルールに関する情報が表示されます。

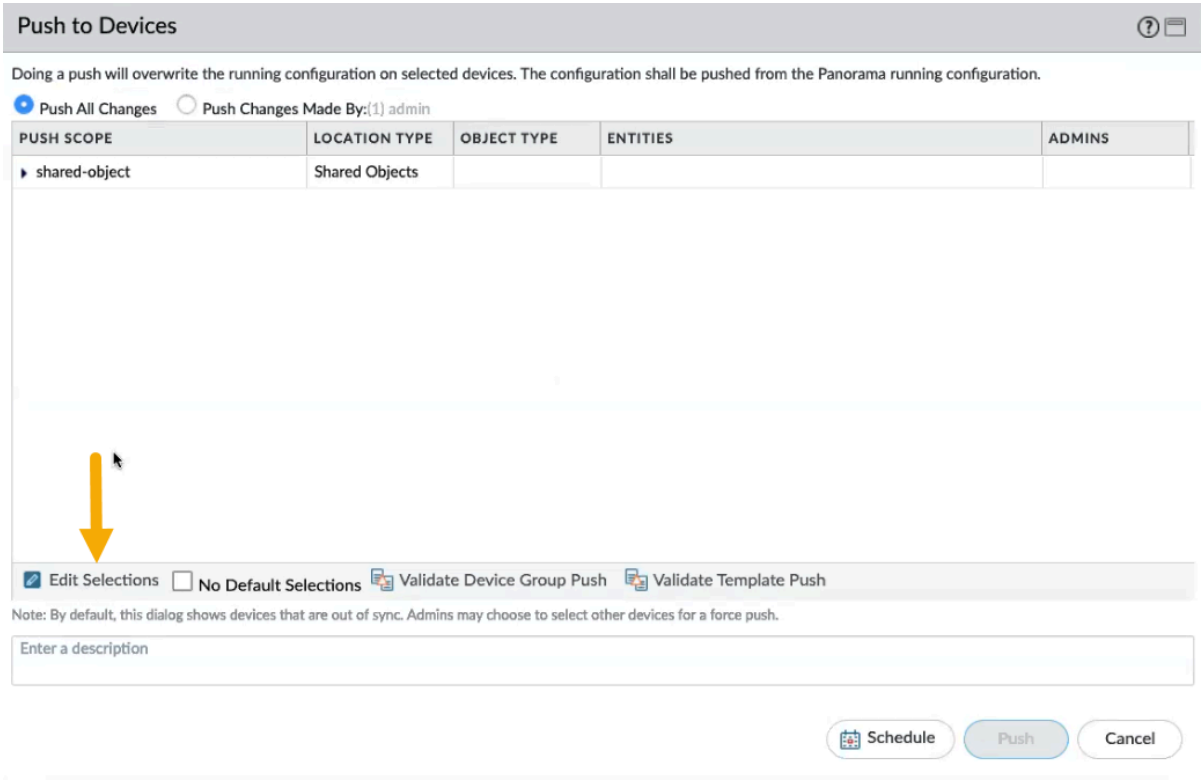


これで、ルールスタックはPanoramaで作成したクラウド デバイス グループに適用されるポリシーに関連付けられました。

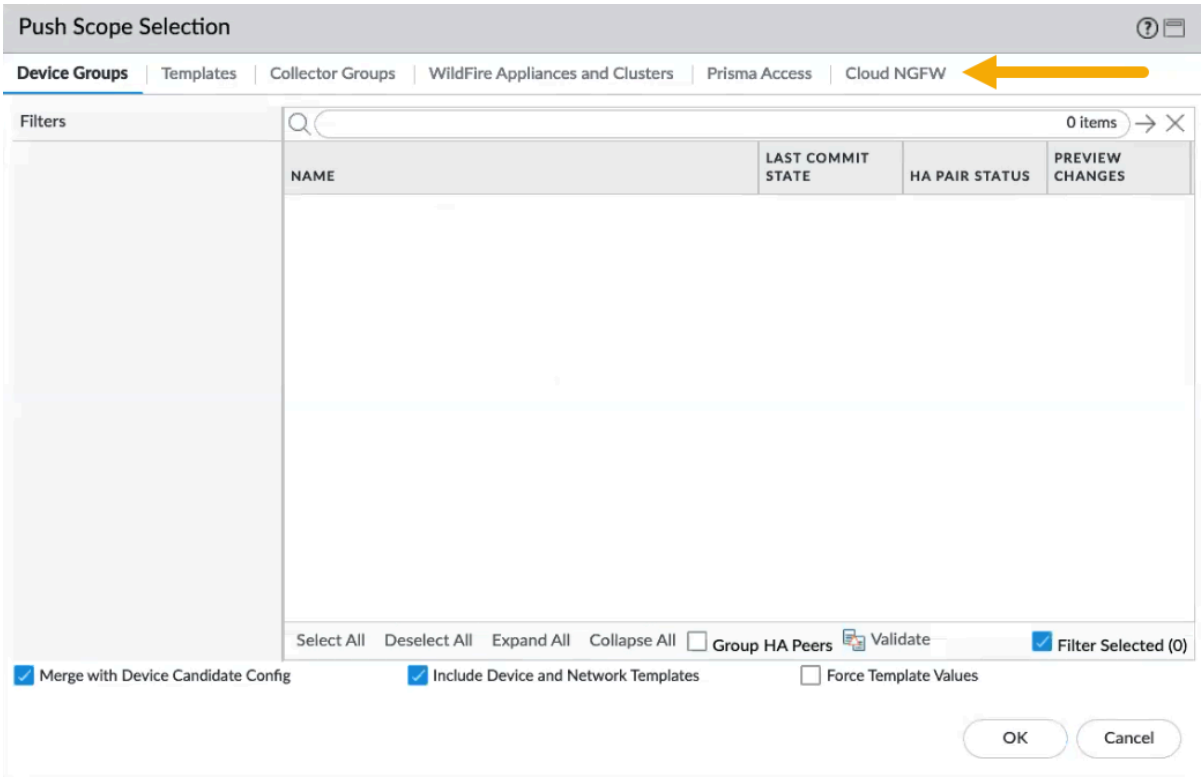


STEP 12 | Cloud NGFWテナントのクラウド デバイス グループにポリシーを適用したら、Panoramaコンソールで変更をプッシュします。

STEP 13 | **[Push to Devices(デバイスにプッシュ)]**画面で、**[Edit Selections(選択項目の編集)]**をクリックします。



STEP 14 | **[Push Scope Selection(プッシュスコープ選択)]**画面で、**[Cloud NGFW]**をクリックします。**[Push Scope Selection(プッシュスコープ選択)]**画面に**Cloud NGFW**ノードが追加され、Cloud NGFWとPanoramaの統合が容易になりました。



STEP 15 | リソースにプッシュするクラウド デバイス グループを選択し、**[OK]**をクリックしてから、**[Push(プッシュ)]**をクリックします。

Panoramaからプッシュされたデバイス グループを使用する

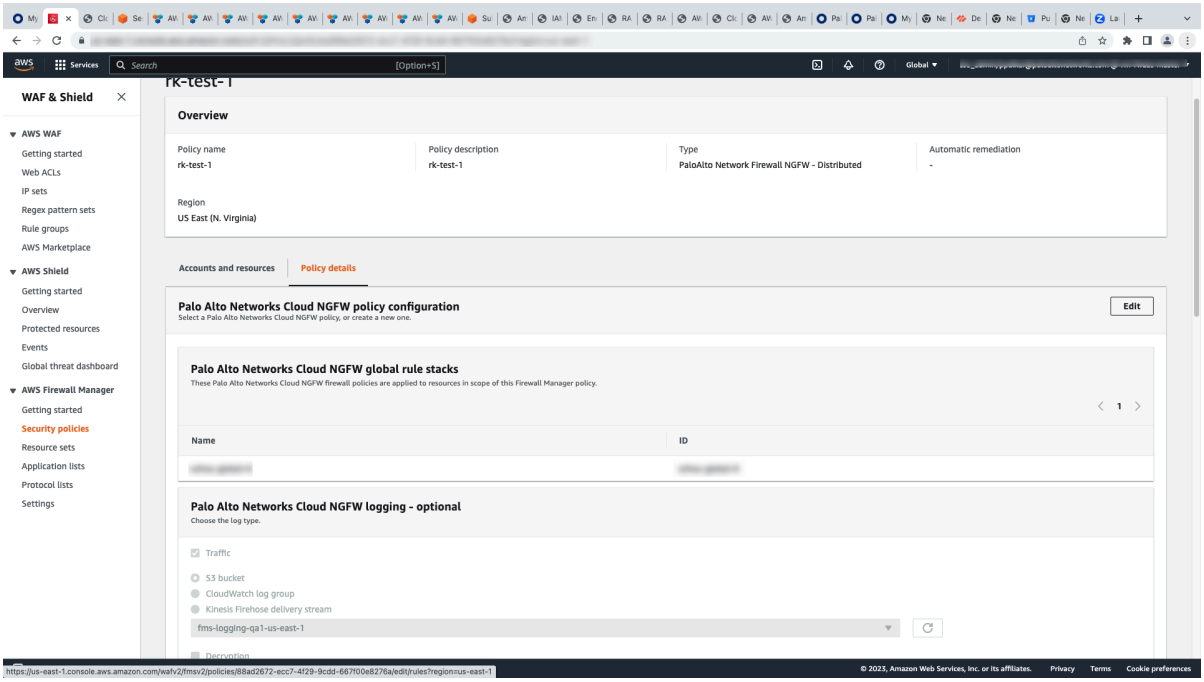
このセクションの情報は、AWS Firewall Manager Service（FMS）を使用してPanoramaからプッシュされたデバイス グループを構成するユーザーを対象としています。

*FMS*を使用している場合、クラウド デバイス グループを*Panorama*から*Cloud NGFW*に関連付けることはできません。このオプションは*Panorama*コンソールでグレー表示されます。*FMS AWS*コンソールを使用して、この関連付けを作成します。

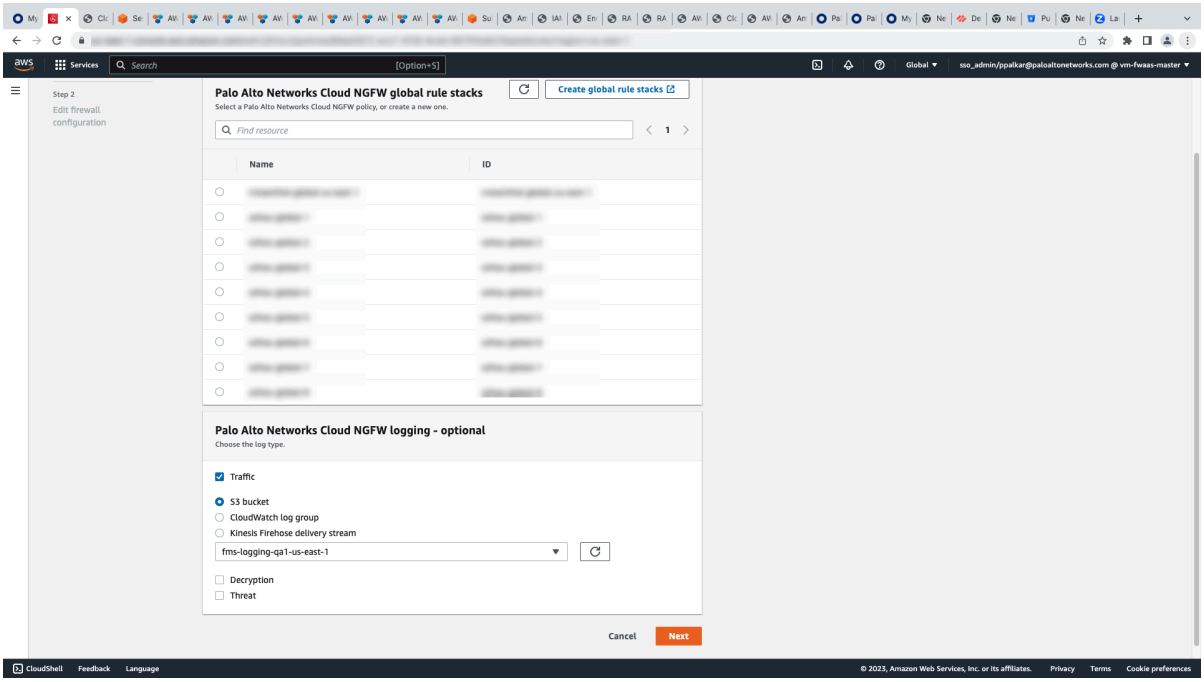
STEP 1 | テナントをPanoramaにリンクします。

STEP 2 | クラウド デバイス グループを作成し、Cloud NGFWにプッシュします。この手順は、FMSを使用していないユーザーでも同じです。

STEP 3 | FMS AWSコンソールに移動し、ポリシーを編集します。



STEP 4 | Panoramaからプッシュされたグローバル ルールスタックを選択します。



STEP 5 | 変更を保存します。

Cloud NGFWリソースで複数のPanoramaを使用する

同じCloud NGFWリソースで複数のPanoramaを使用する方法

STEP 1 | Cloud NGFW コンソールにログインします。

STEP 2 | **[Integrations(統合)]**を選択します。**[Integrations(統合)]**ページには、現在リンクされているPanoramaに関する情報が表示されます。現在PanoramaがCloud NGFWテナントにリンクされていない場合、このページは空です。

STEP 3 | **[Panorama]**ページで、**[Add Panorama(パノラマの追加)]**をクリックします。

STEP 4 | **[Add Panorama(パノラマの追加)]**ウィンドウで、リンク名を入力します。ドロップダウンメニューから**[Primary Panorama Serial Number(プライマリPanoramaシリアルナンバー)]**を選択します。

[Add Panorama(パノラマの追加)]ウィンドウには、Cloud NGFWテナントにアクセス可能な各Panoramaの横にアイコンが表示されます。これらのアイコンは、PanoramaライセンスがStrata Logging Serviceにリンクされているかどうかを示します。詳細については、「Cloud NGFWをPalo Alto Networks管理にリンク」を参照してください。

STEP 5 | HAペアのセカンダリ**Panorama**シリアルナンバーを選択します。

STEP 6 | **Continue**（続行） をクリックします。

STEP 7 | リンク処理が完了したことを示す通知が表示されます。**[Confirm(確認)]**をクリックします。

[Integrations(統合)]ページに、Cloud NGFWテナントにリンクされたPanoramaが表示されるようになりました。**Link ID**をクリックすると、情報が表示されます。また、リンク名を変更することもできます。リンクの名前を変更した場合は、**[Save(保存)]**をクリックします。

STEP 8 | Cloud NGFWコンソールで、**[NGFWs**］を選択して、展開されたファイアウォールを表示します。

Cloud NGFWコンソールの左上にあるドロップダウンを使用して、ファイアウォールが存在するリージョンを選択します。

STEP 9 | Panoramaで管理するファイアウォールを選択します。

STEP 10 | ［**Firewall Settings(ファイアウォール設定)]**タブをクリックします。

STEP 11 | **[Policy Management(ポリシー管理)]**セクションまでスクロールし、**Panorama**を選択します。

STEP 12 | ドロップダウン メニューを使用して、**[Linked Panorama(リンクPanorama)]**を選択します。

STEP 13 | **[Save(保存)]**をクリックします。

STEP 14 | 手順8～13を繰り返して、別のパノラマを別のNGFWテナントに管理します。

STEP 15 | **[Integrations(統合)]**をクリックして別のPanoramaをリンクします。

STEP 16 | **[Panorama]**ページで、**[Add Panorama(パノラマの追加)]**をクリックします。

STEP 17 | **[Add Panorama(Panoramaの追加)]**]ウィンドウで、新しいリンク名を入力します。ドロップダウンメニューから**[Primary Panorama Serial Number(プライマリPanoramaシリアルナンバー)]**を選択します。

STEP 18 | HAペアのセカンダリ**Panorama**シリアルナンバーを選択します。

STEP 19 | **Continue**（続行） をクリックします。

STEP 20 | リンク処理が完了したことを示す通知が表示されます。**[Confirm(確認)]**をクリックします。

複数のPanoramaをCloud NGFWテナントにリンクする場合、ルールスタックは関連付けられません。Panoramaを使用してクラウド デバイス グループをファイアウォールにプッシュすると 、［NGFWs］ページの**[Rulestacks(ルールスタック)**］セクションが変更し、NGFWに関連付けられたポリシー管理が反映されます。

STEP 21 | リンク処理が完了したことを示す通知が表示されます。**[Confirm(確認)]**をクリックします。

タグベースのポリシーを構成する

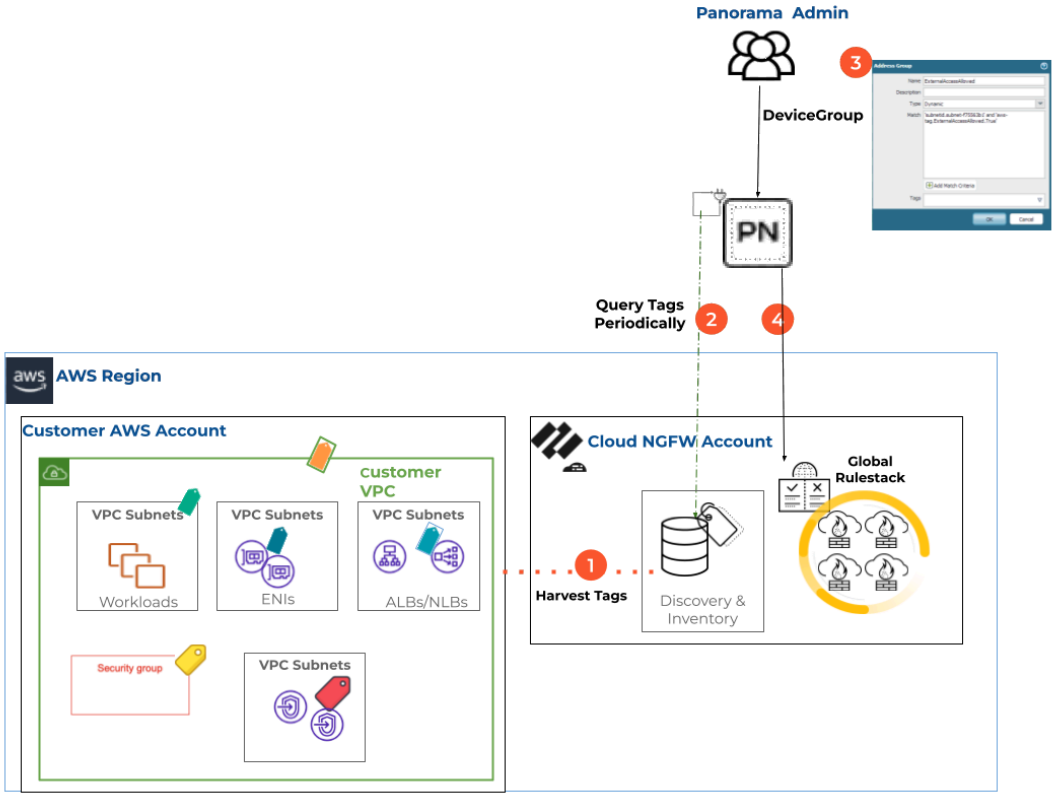
どこで使用できますか?	何が必要ですか?
• Cloud NGFW for AWS	❑ Cloud NGFWサブスクリプション ❑ Palo Alto Networksカスタマー サポート アカウント (CSP) ❑ AWS Marketplaceアカウント ❑ ユーザーのロール（テナントまたは管理者）

Palo Alto Networks® Cloud NGFWリソースのセキュリティ ポリシーを自動的に更新できるため、AWSパブリッククラウドにAWSアセット（EC2インスタンスなど）を導入または終了する際に、これらのAWSアセットへのトラフィックを保護できます。

Panoramaからこの機能を有効にするには、追加したAWSアカウントからCloud NGFWテナントが収集するIP/タグを取得するようにPanorama AWSプラグインを設定する必要があります。次に、AWS Panoramaプラグインを使用して、監視定義を設定することでこれらのタグをCloud

NGFWリソースにプッシュし、これらのPalo Alto Networksファイアウォールに対応するデバイス グループに通知します。

その後、AWSリソース タグを使用して、それらのデバイス グループにPanoramaダイナミック アドレス グループ オブジェクトを作成できます。ダイナミック アドレス グループ内でこれらのタグを参照してセキュリティポリシー ルール内の項目にマッチさせる際、AWS アカウント内にデプロイしたすべてのアセットに対して一貫した形でポリシーを適用できます。



前提条件

Cloud NGFW for AWSリソースのタグベースのポリシーを有効にするには、以下の最小システム要件が必要です。

- PanoramaにAWSプラグイン5.1.0バージョン以上 をインストールします。詳細については、「AWSプラグインのインストールまたはアップグレード」を参照してください。
- Cloud NGFW コンソールを使用して 、AWS アカウントを Cloud NGFW テナントに追加し、そこからタグを収集します。
- Panoramaプラグインを使用してタグを照会し、Panoramaデバイス グループに追加します。
- デバイス グループでタグを使用してダイナミック アドレス グループ（DAG）オブジェクトを設定します。

キーコンセプト

用語	定義
クラウド アセット タグ	AWSリソースに設定されたAWSタグ。
VPCグループ	1つ以上のAWSアカウントのAWS VPCのセット。
モニタリングの定義	VPCグループを通知グループに関連付けます。
グループに通知	同じタグセットを必要とするPanoramaデバイス グループのセットをグループ化できます。

Cloud NGFW for AWSリソースのタグベースのポリシーを有効にするには、AWSプラグイン5.1.0バージョン以降をインストールして、この統合のためにPanoramaアプライアンスを準備する必要があります。Cloud NGFWコンソールを使用して、AWSアカウントを追加し、AWSリソースからタグを収穫します。次に、Panoramaプラグインを使用してCloud NGFWテナントからタグを定期的にクエリし、Panoramaデバイス グループに追加してダイナミック アドレス グループ オブジェクトとルールを管理します。

PanoramaアプライアンスでCloud NGFWタグベースのポリシーを有効にするには、次の手順を実行します。

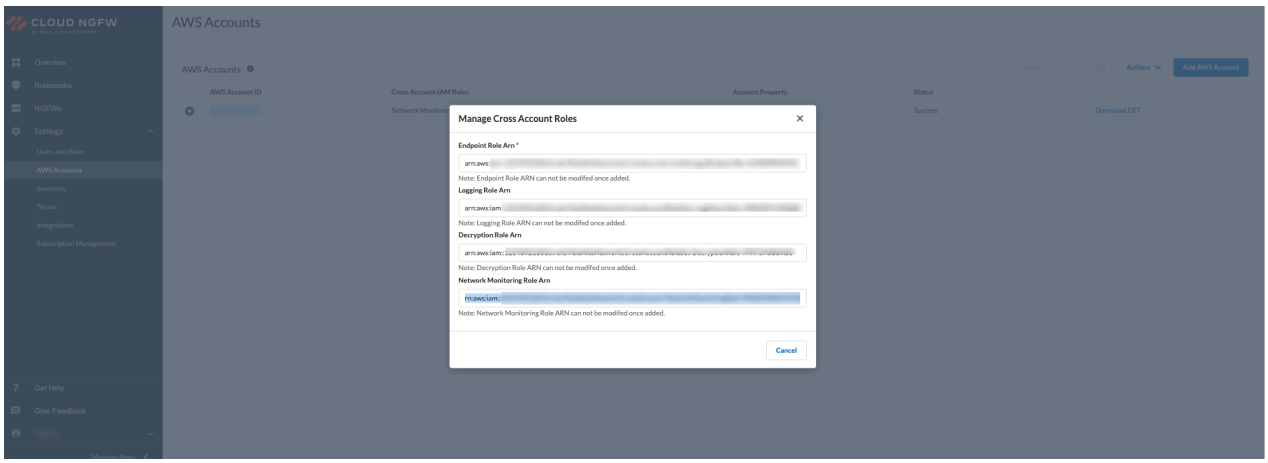
1. AWSアカウントをCloud NGFWテナントに追加し、そこからタグを収集する。
2. Panoramaプラグインを使用してタグを照会し、Panoramaデバイス グループに追加します。
3. デバイス グループでタグを使用してダイナミック アドレス グループ（DAG）オブジェクトを設定します。

AWSアカウントをCloud NGFWテナントに追加し、そこからタグを収集する。

AWSアカウントをCloud NGFWテナントにオンボードします。詳しくは、Cloud NGFW PAYG SaaSサブスクリプションの手順**10**を参照してください。

AWSアカウントをCloud NGFWテナントですでにオンボードしている場合は、タグハーベスティングを直接開始できます。

オンボーディング済みのAWSアカウントの既存のCloudFormationテンプレート（CFT）に、`Network MonitoringRole Arn`ロールを追加する必要があります。ネットワーク モニタリング ロールは、AWSがホストするアプリケーションを接続するネットワーク パフォーマンスを可視化します。詳細については、「CloudFormationテンプレートを手動で追加する」を参照してください。



モニタリングを有効にする

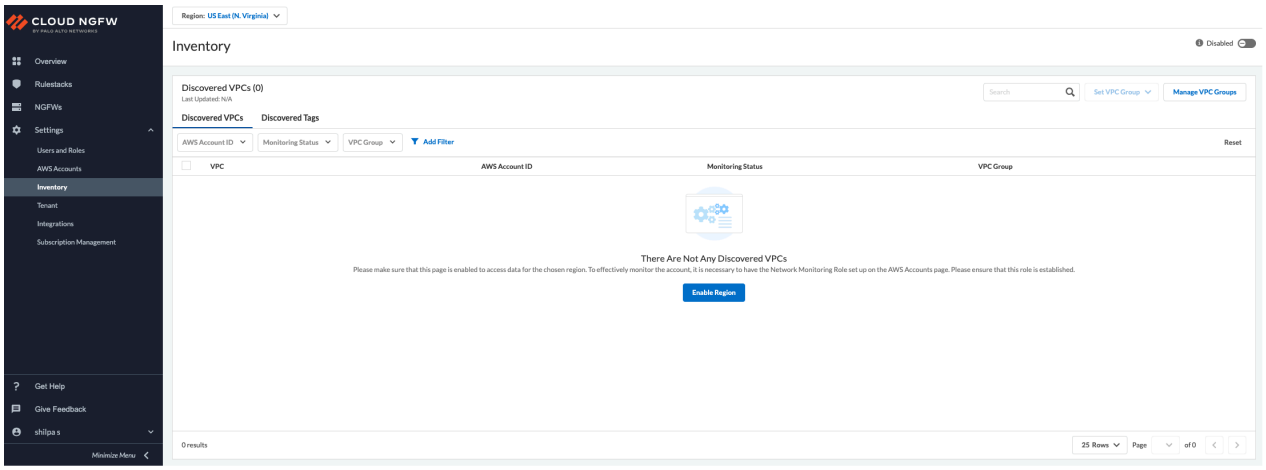
Cloud NGFWコンソールで、目的のリージョンのAWSリソースタグの検出を有効にできます。Cloud NGFWは、AWSリソースのこれらのタグを定期的に収集します。(例:異なるAWSア

カウントに収集し（例：EC2、SG、LB）、情報をCloud NGFWテナントに登録します。Cloud NGFWは、各AWSアカウントのVPCによって整理されたリソース上のリソースタグを表示します。

このためには、**[Inventory(**インベントリ**)]**ページでモニタリングを有効にして各AWSリージョンのデータにアクセスし、タグの検出をトリガーする必要があります。

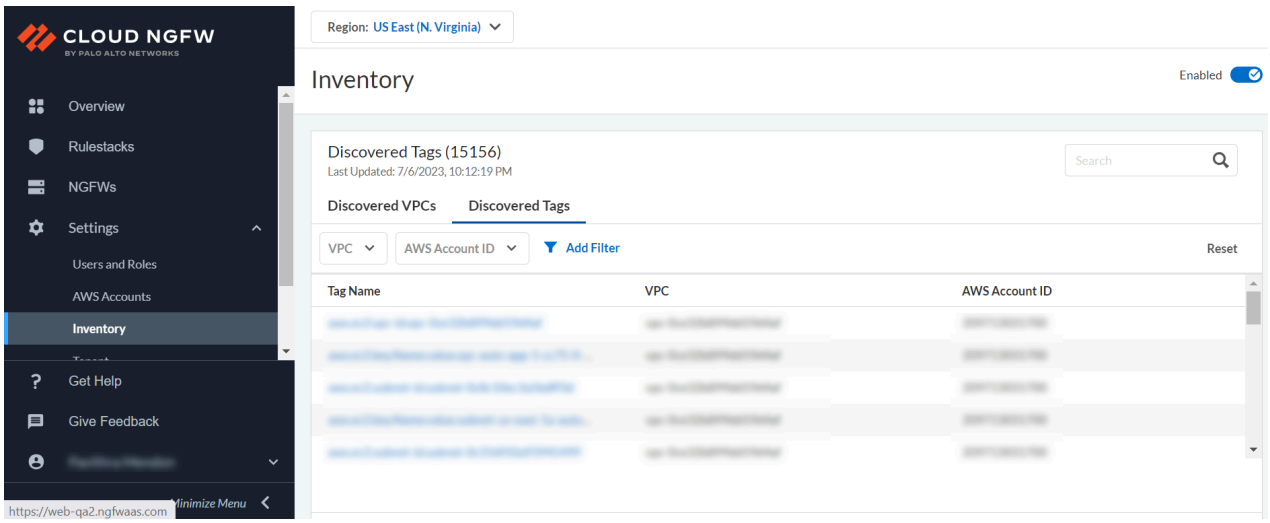
[Discovered VPCs(検出された**VPC)]**タブの**[Enable Region(**リージョンを有効にする**)]**ボタンは、AWSアカウントを初めてオンボードしたときにのみ表示されます。ドロップダウンから**[Region(**地域**)]**を選択し、**[Enable Region(**地域にする**)]**をクリックしてタグのモニタリングを有効にします。

または、ドロップダウンから**[Region(**地域**)]**を選択し、［**Enable(**有効**)**］トグルをクリックしてタグのモニタリングを有効にすることもできます。

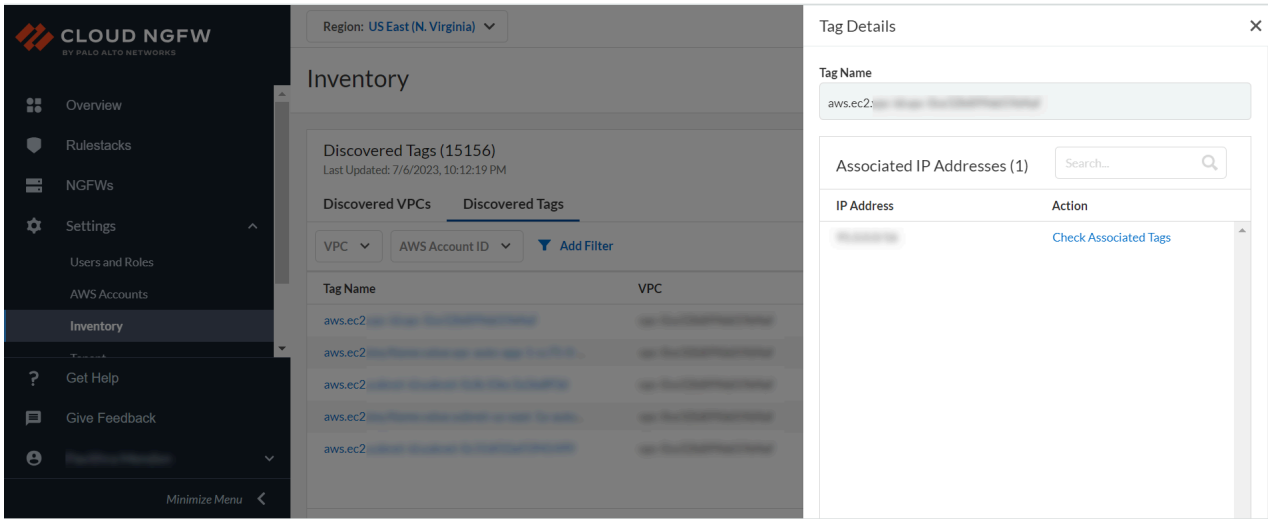


Cloud NGFWコンソールで収集されたタグを表示する

検出されたタグの総数は、**[Discovered Tags(**検出されたタグ**)]**タブの**[Inventory(**インベントリ**)**ページで確認できます。



[Tag Name(タグ名)]をクリックすると、各タグに関連付けられているIPが一覧表示されます。



[Check Associated Tags(関連付けられたタグを確認する)]をクリックして、IPアドレスに関連付けられているさまざまなタグを一覧表示します。

NGFWコンソールでは、任意のAWSリソースタイプ（キーまたは値の組み合わせ）のタグ文字数制限は**127**文字です。キーと値が **127** より大きい タグは **DiscoveredTags** リストに追加されません。詳細は、「タグの制限」を参照してください。

インベントリ管理者権限がない場合、***VPC*** グループの設定 や 新しい ***VPC*** グループの作成 はできません。

*Panorama*プラグインを使用してタグを照会し、*Panorama*デバイス グループに追加します。

Panorama AWSプラグインを使用して、以下を実行します。

STEP 1 | VPCグループを作成および管理します。

STEP 2 | モニタリング定義を使用してタグをデバイス グループに追加し、グループに通知します。

> *Panorama*に*AWS Plugin 5.1.0*プラグイン（またはそれ以降）をインストールして設定すると、*Cloud NGFW*テナントに収集された*AWS*アセット タグをクエリし、クラウド デバイス グループに追加できます。

VPCグループの作成と管理

モニタリングを有効にすると、デフォルトのVPCグループが自動的に作成されます。デフォルトの VPC グループは 削除 できません。新しく検出されたVPCは常にデフォルト VPCグループに入れられます。必要に応じて、別のVPCグループに移動できます。

> リージョンで作成された*VPC*グループのスコープは、そのリージョンにのみ適用されます。たとえば、リージョン*X*で作成した*VPC*グループ*A*は、リージョン*Y*ではアクセスできません。

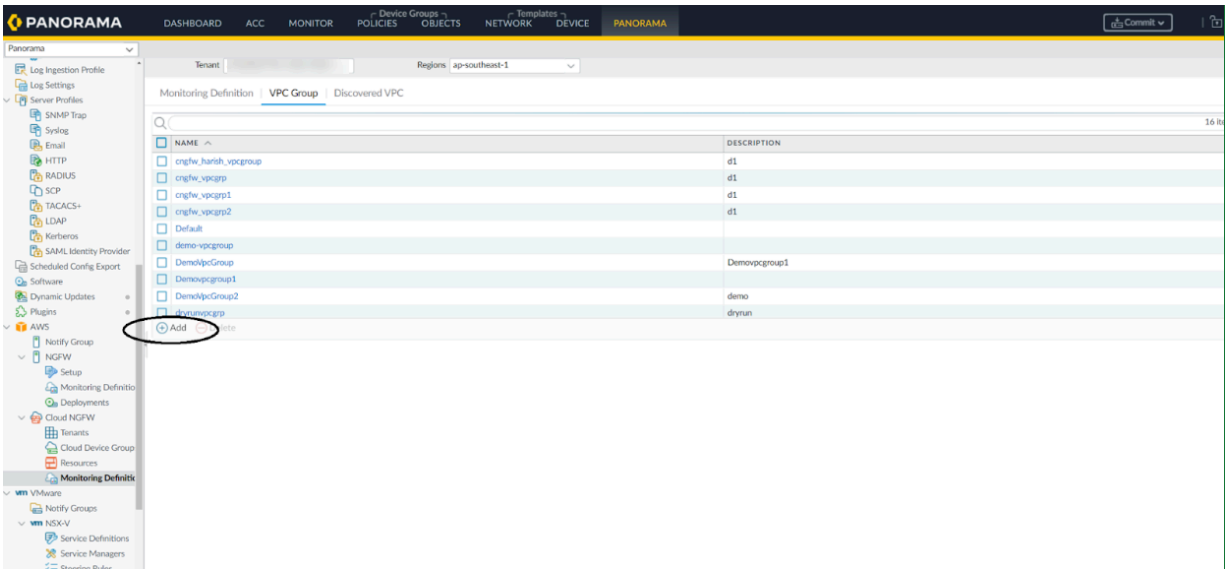
または、次の手順を使用して、新しいVPCグループを作成し、これらのVPCを他の VPC グループに移動できます。

Panoramaで新しいデフォルト以外の**VPC**グループを作成する場合は、以下の手順でカバーされている手順に従ってください。

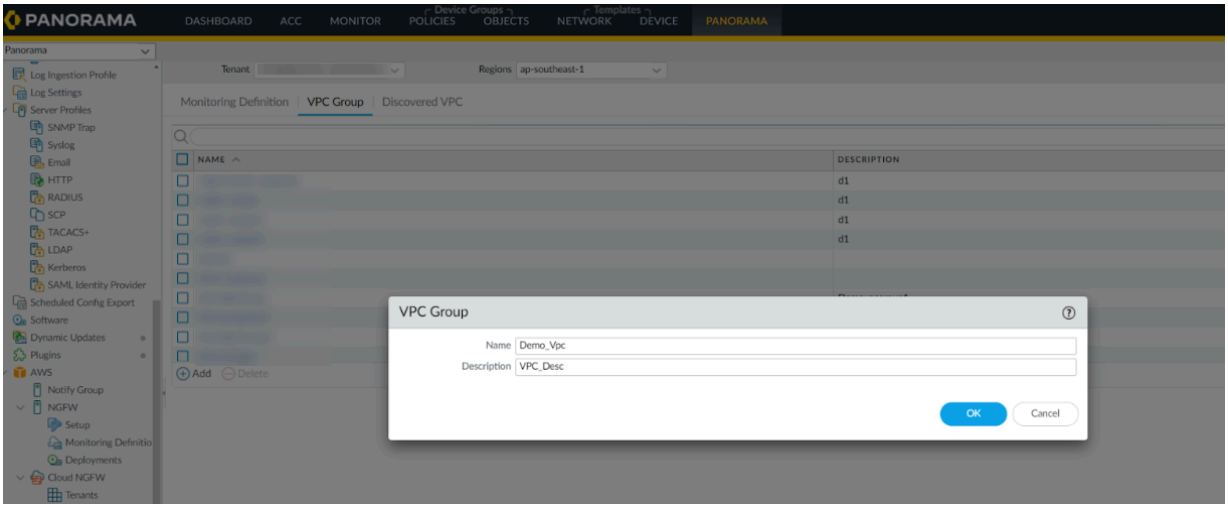
STEP 1 | **Panorama**コンソールの**[Panorama]**タブに移動し、**[AWS]**をクリックします。

STEP 2 | **[Tenant(テナント)]**と**[Region(地域)]**を選択します。

STEP 3 | ［**AWS**］ > ［**Cloud NGFW**］ > **[Monitoring Definition(**モニタリングの定義**)**］ > **[VPC Group(VPC**グループ**)**］ > **[Add(**追加**)**］の順に進みます。

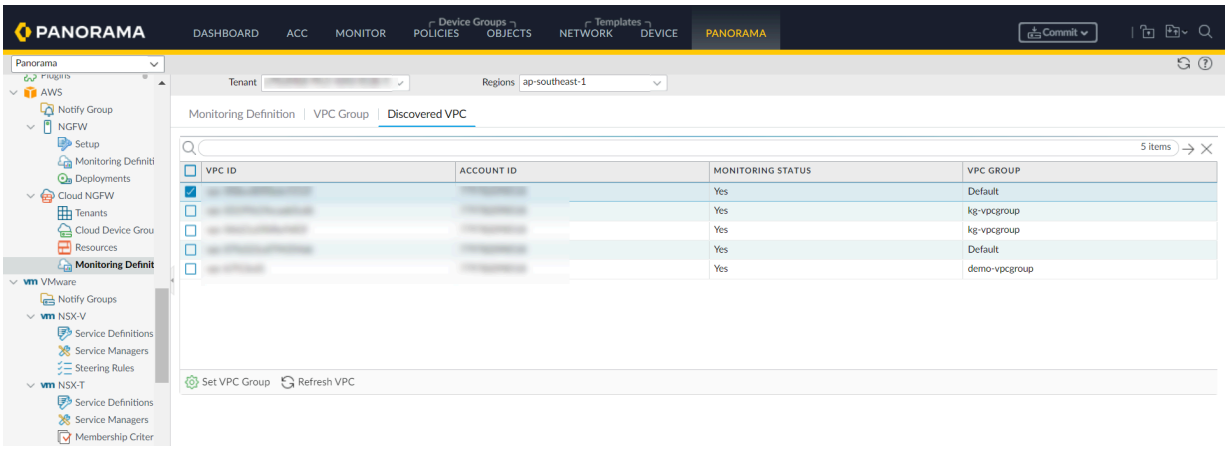


STEP 4 | VPCグループ名と説明を入力します。



STEP 5 | **OK** をクリックします。

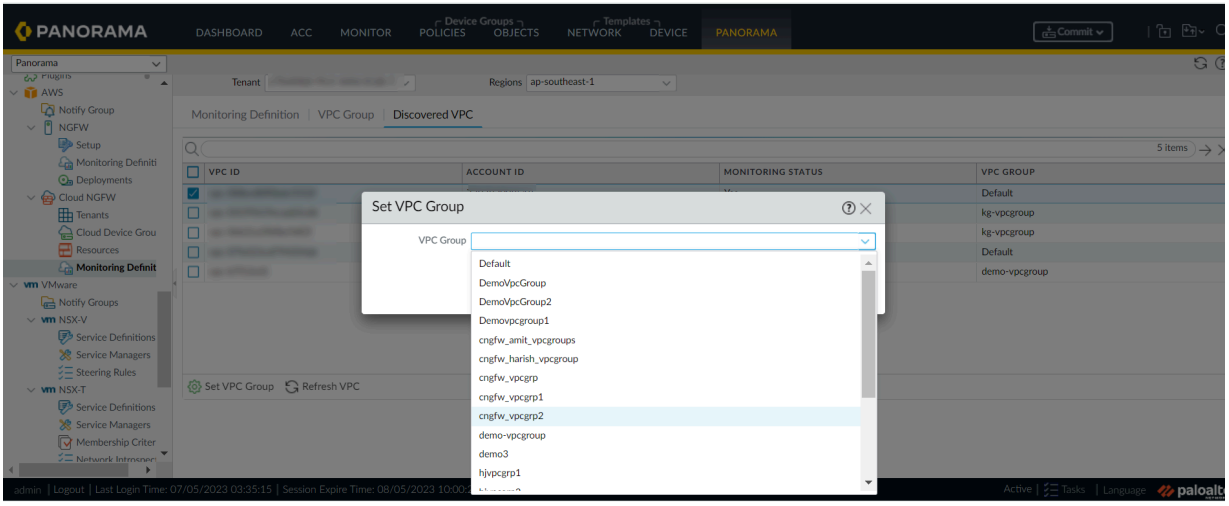
STEP 6 | **[AWS] > [Cloud NGFW] > [Monitoring Definition(モニタリング定義)] > [Discovered VPC(発見したVPC)]**に移動します。



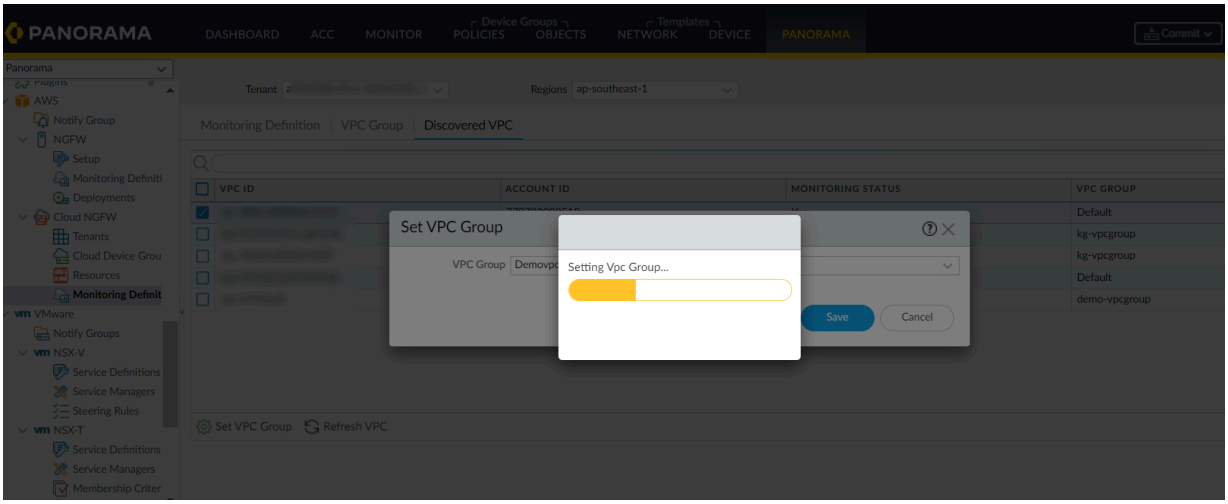
- ***VPC** グループを 8 個を超えるデバイス グループにマップすることはできません。特定の*VPC*グループが *([Notify Groups(*グループに通知*)]*を介して*) 8*つのデバイス グループしかマップされないように*VPC*グループでモニタリング定義を設定し、パフォーマンスを向上させます。*
- *デフォルトの*VPC*グループが自動的に作成されます。デフォルトの VPC グループは 削除 できません。新しく検出された*VPC*は、常にデフォルトの*VPC*グループに入れられます。必要に応じて、*VPC*を別の*VPC*グループの下に移動できます。*

STEP 7 | **[Set VPC Group(VPCグループの設定)]**をクリックします。

STEP 8 | **[VPC Group(VPCグループ)]** を選択します。



STEP 9 | **[Save(保存)]**をクリックします。



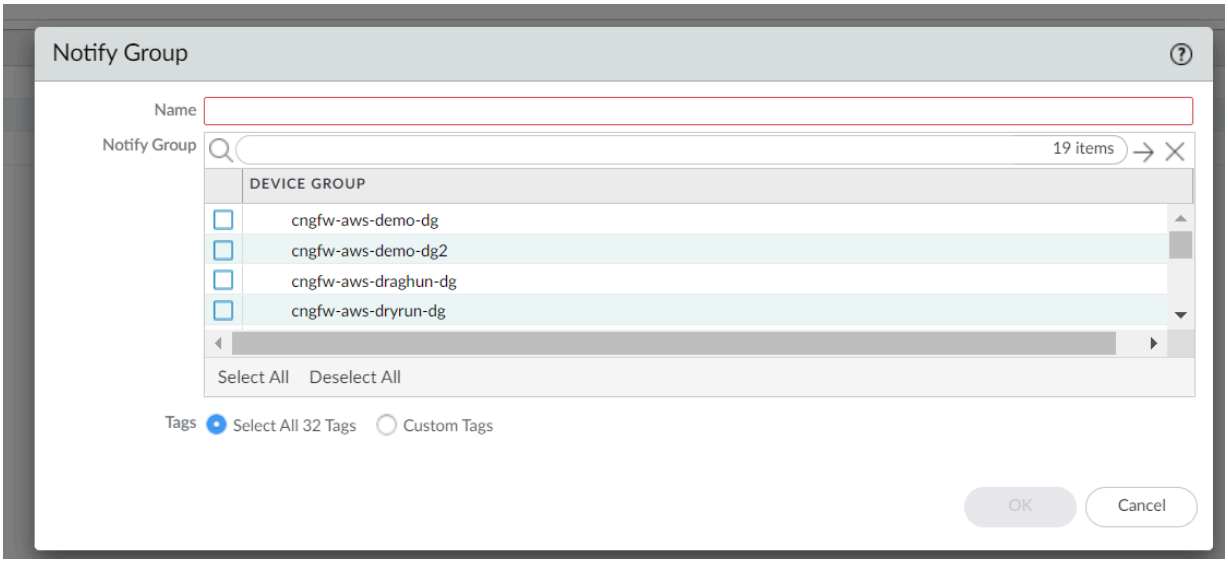
モニタリング定義とデバイス グループを使用したデバイス グループへのタグの追加

Cloud NGFWテナントから学習したタグをCloud NGFWリソースにプッシュするには、これらのPalo Alto Networksファイアウォールに対応する対応するデバイス グループに**[Notify Groups(**グループに通知**)**と**[Monitoring definitions(**モニタリング定義**)]**を設定していることを確認します。その後、Cloud NGFWテナントから収集されたAWSアカウントタグをPanoramaで表示できます。

次の手順で、クラウド デバイス グループの通知グループを作成します。

STEP 1 | **Panorama**プラグインのコンソールで 、**[AWS**］ **>[Notify Group(**グループに通知**)]**に移動します。

STEP 2 | **Add**（追加）を選択します。



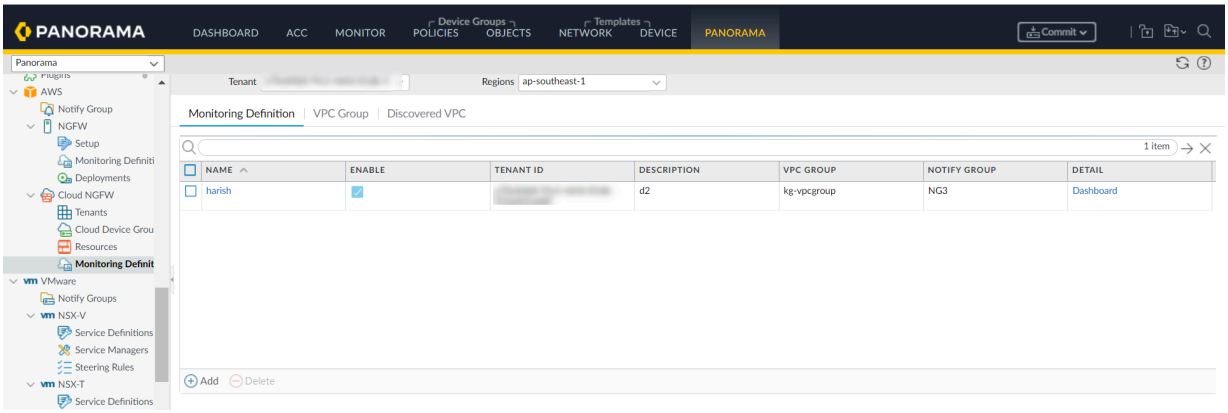
STEP 3 | 名前を入力します。

STEP 4 | デバイス グループとタグを選択します。

STEP 5 | **[OK]** をクリックします。

必要な**VPC**グループと、Cloud NGFWから学習したタグの通知グループを関連付けるクラウドモニタリング定義を作成します。

STEP 6 | **Panorama**で、**[AWS] > [Cloud NGFW] > [**モニタリング定義**]**に移動します。

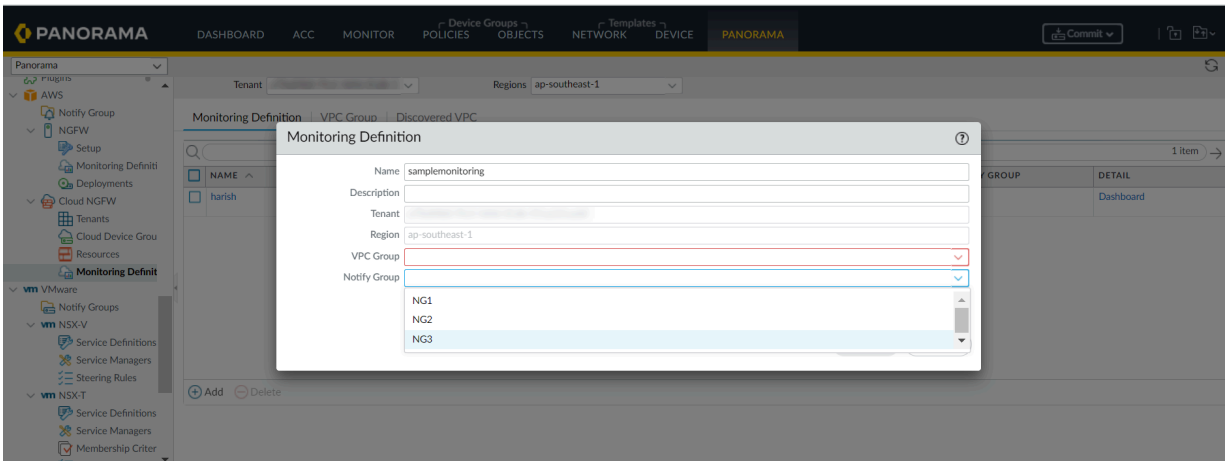


STEP 7 | **[**追加**]** をクリックします。

STEP 8 | **[Name(**名前**)]**と**[Description(**説明**)]**を入力します。

STEP 9 | **[VPC Group]**ドロップダウンメニューから必要なVPCグループを選択します。

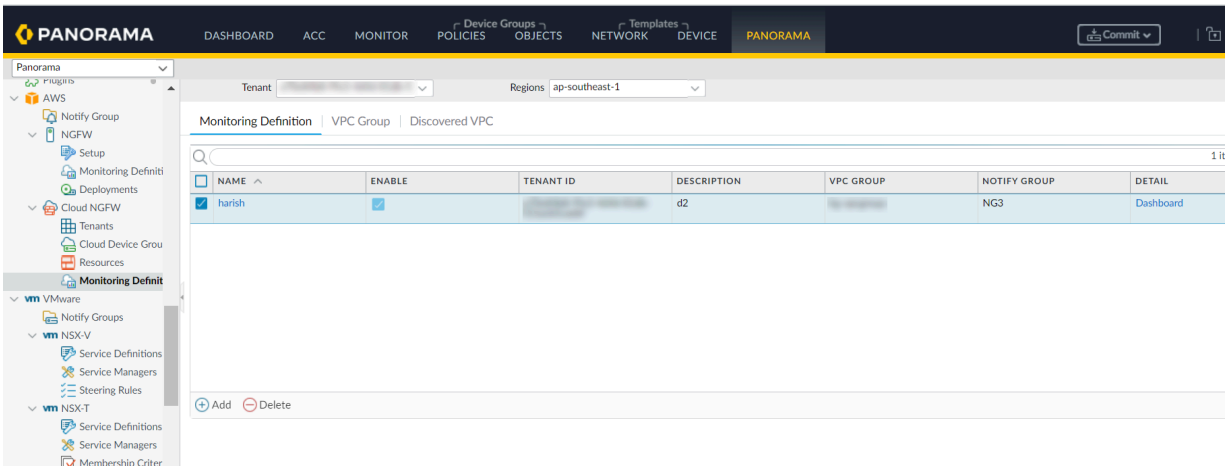
STEP 10 | **[Notify Group(通知グループ)]**ドロップダウンメニューから必要な通知グループを選択します。



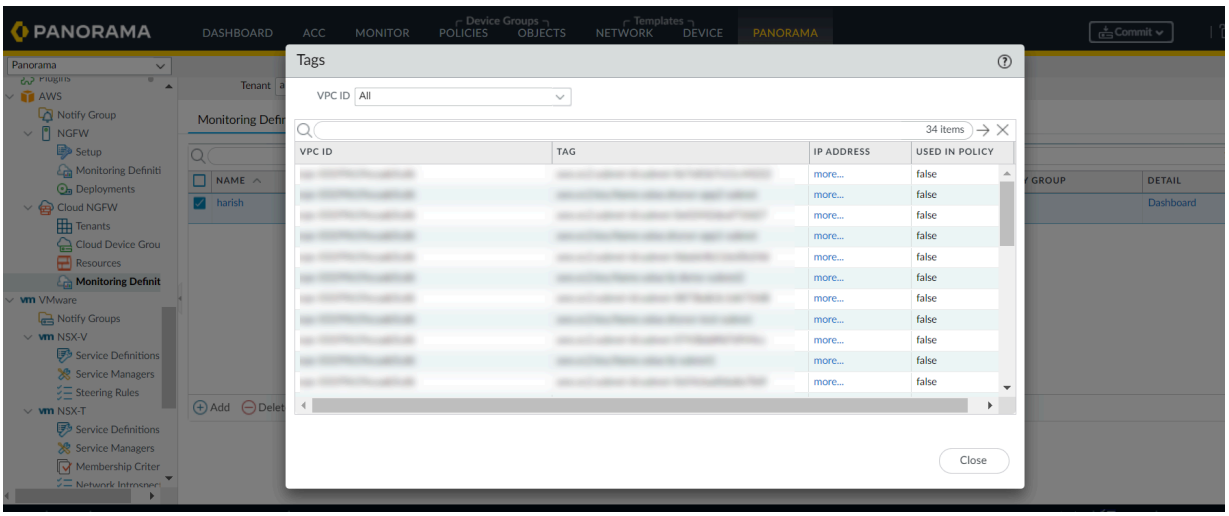
STEP 11 | **OK** をクリックします。

STEP 12 | Panoramaで変更をコミットし、プッシュします。

STEP 13 | **[Monitoring Definition(モニタリング定義)]**を選択し、**[Dashboard(ダッシュボード)]**をクリックすると、Cloud NGFWテナントから収集されたタグが表示されます。



Cloud NGFWテナントで収穫したタグを表示できるようになりました。



デバイス グループでタグを使用してダイナミック アドレス グループ オブジェクトを設定します。

収集されたCloud NGFWタグを使用して、クラウド デバイス グループのダイナミック アドレス グループを作成できます。詳細については、「ダイナミック アドレス グループの作成」を参照してください。

ダイナミック アドレス グループの一致条件を追加する手順は次のとおりです。

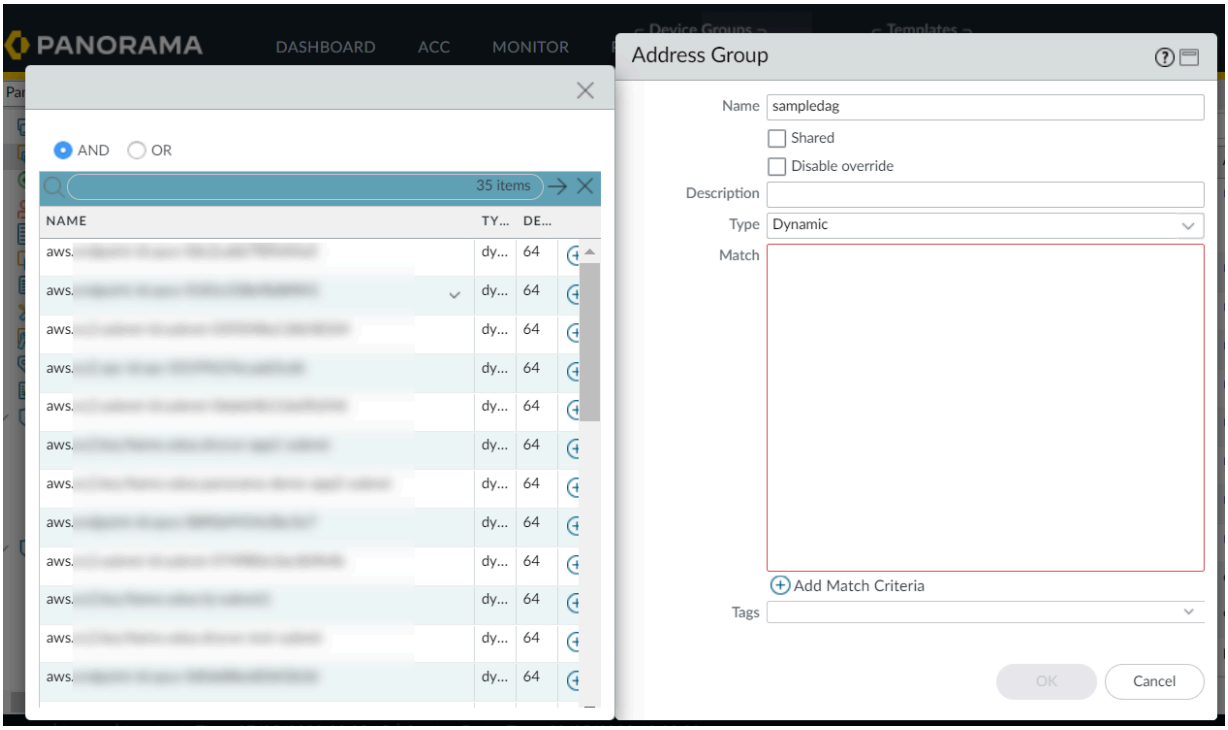
STEP 1 | **Panorama**で、**[**オブジェクト**]** タブを選択します。

STEP 2 | 左側のペインで、**[Address Groups(**アドレス グループ**)]**に移動します。

STEP 3 | **[**追加**]** をクリックします。

STEP 4 | アドレス グループの名前を入力し、タイプ**[Dynamic(**ダイナミック**)]**を選択します。

STEP 5 | **[Add match Criteria（一致条件の追加）]**をクリックします。

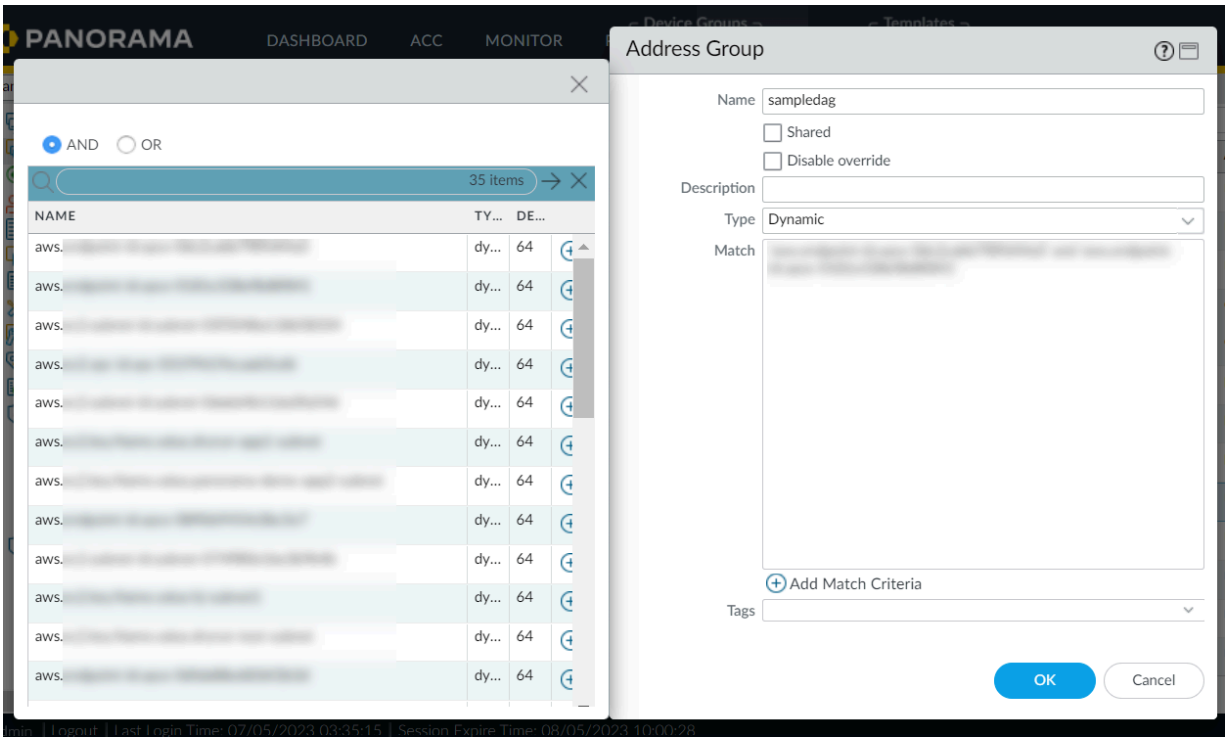


これで、クラウド デバイス グループの作成されたDAGを参照して、ダイナミック アドレス グループ ポリシーを作成できます。

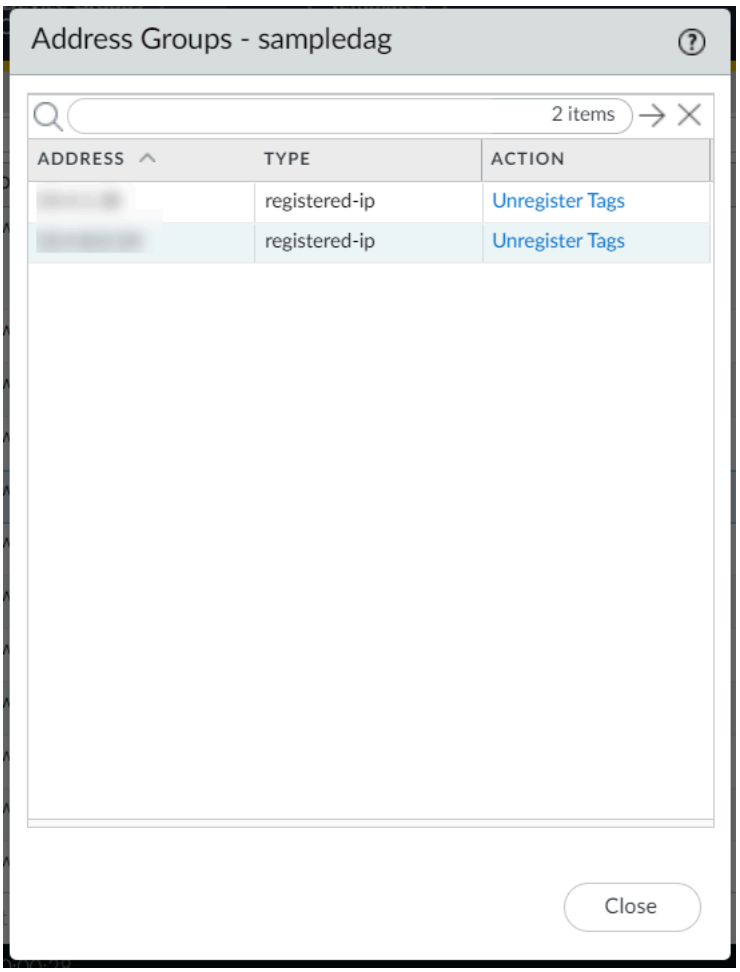
動的アドレス グループ オブジェクトに、さまざまなリージョンのタグを追加できます。異なるリージョンのタグを使用するには、他のリージョンに同じ名前のクラウド デバイス グループを作成する必要があります。また、通知グループをそのリージョンのVPCグループに

マッピングするモニタリング定義を他のリージョンに作成する必要があります。詳細については、「クロスリージョン タグ ベース ポリシー」を参照してください。

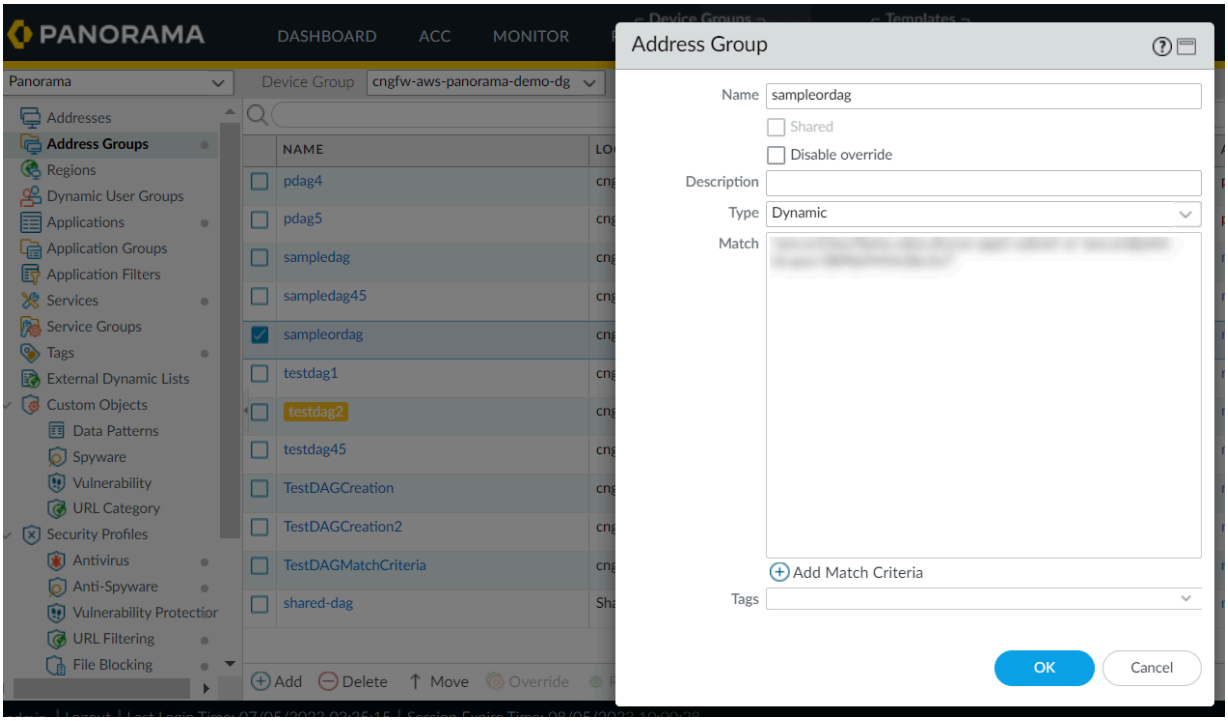
次に、**AND**演算子を使用してDAGを作成する例を示します。



アドレス グループには、両方の一致条件に一致するアドレスのリストが表示されます。

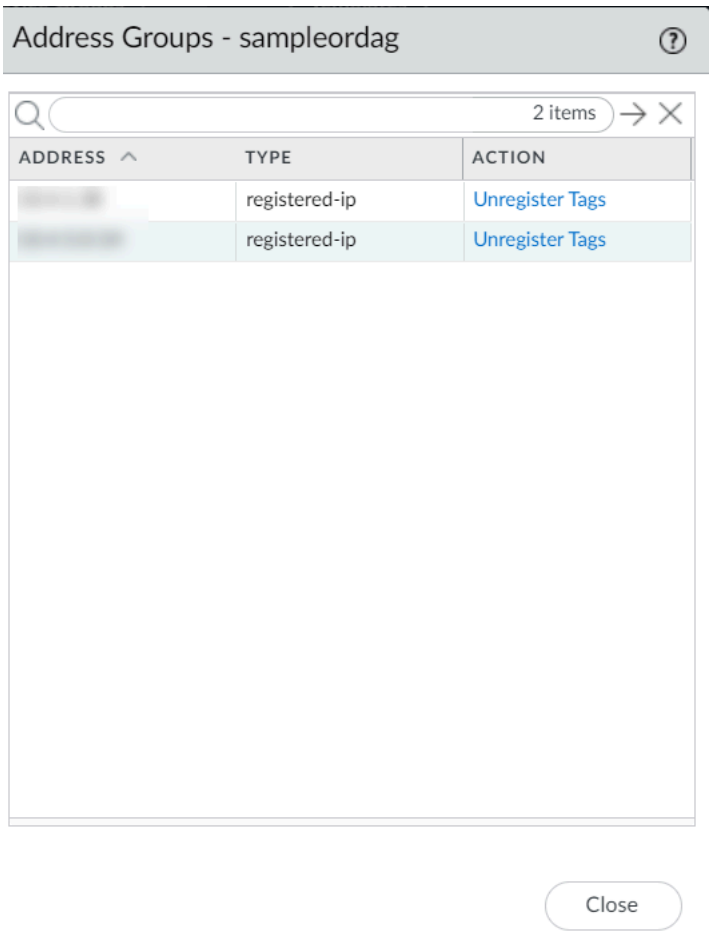


次に、**OR**演算子



を使用してDAGを作成する例を示します。

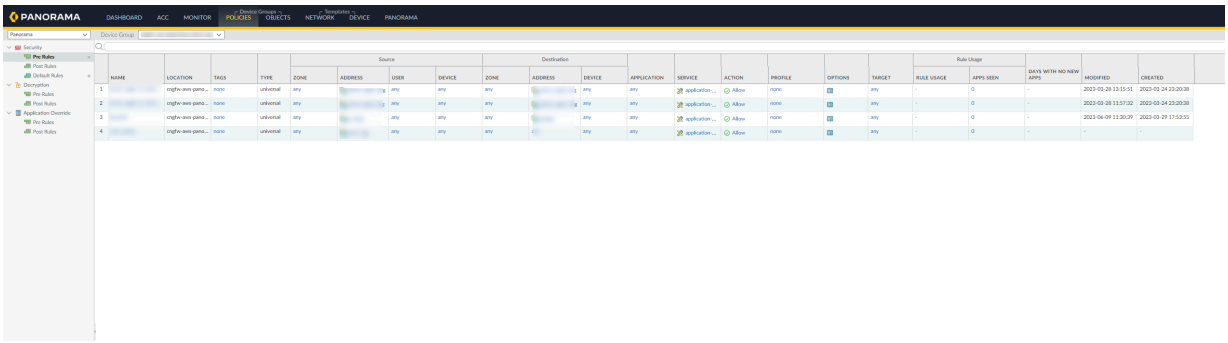
アドレス グループは、指定された一致条件のいずれかに一致するアドレスのリストを表示します。



クラウド デバイス グループの DAG を参照する動的アドレス ポリシー ルールを作成するには、次の手順に従います。

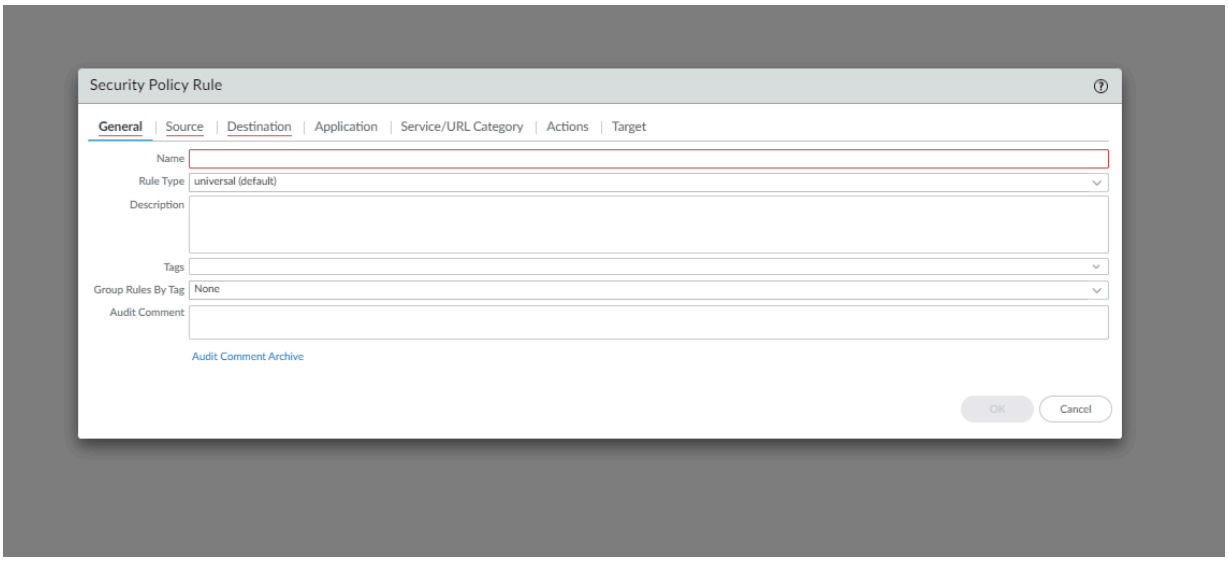
STEP 6 | **Panorama**コンソールで、**[Policies(**ポリシー**)]**タブに移動します。

STEP 7 | **[Security(セキュリティ)]>[Pre/Post/Default Rules(事前/投稿/デフォルト ルール)]**に移動します。

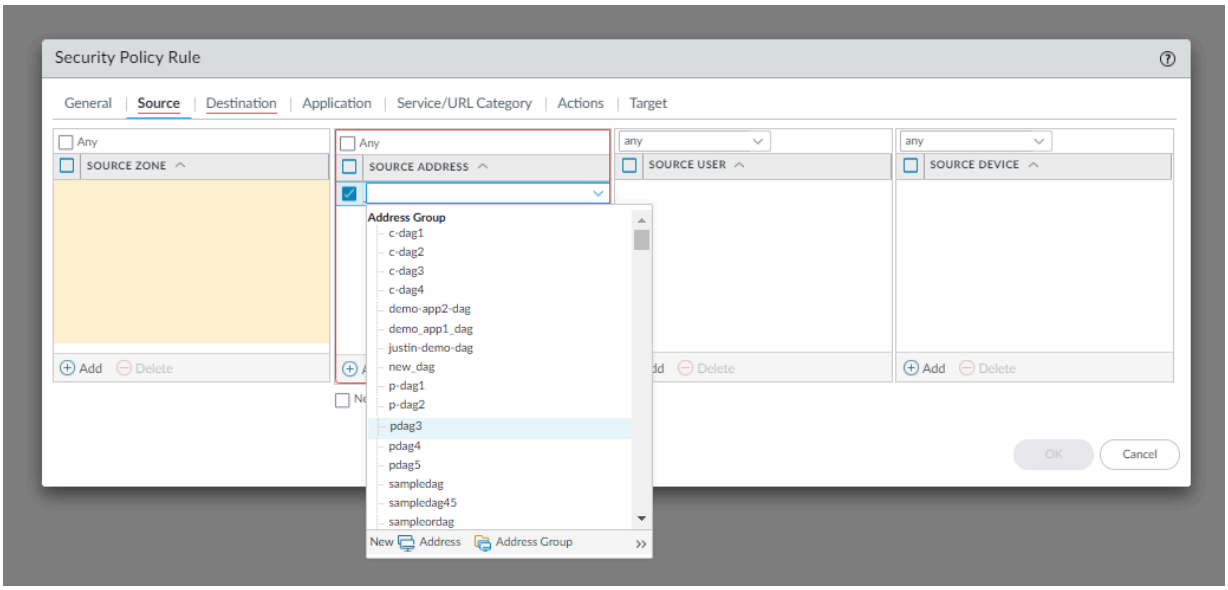


STEP 8 | **[追加]** をクリックします。

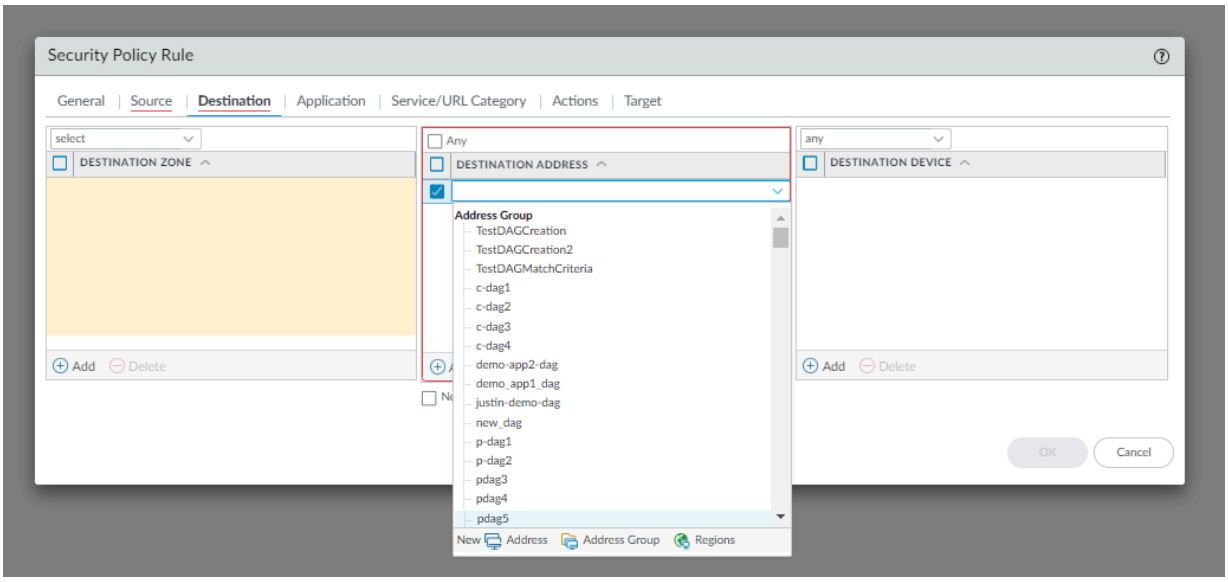
STEP 9 | [Security Policy Rule(セキュリティ ポリシー ルール)]ダイアログボックスで、セキュリティポリシールールの名前を入力します。



STEP 10 | **[Source(送信元)]**タブで、**[Source Address(送信元アドレス)]**フィールドのダイナミック アドレス グループを選択し、**[Add(追加)]**をクリックします。



STEP 11 | **[Destination(宛先)]**タブで、**[Destination Address(通知先アドレス)]**フィールドのダイナミック アドレス グループを選択し、**[Add(追加)]**をクリックします。



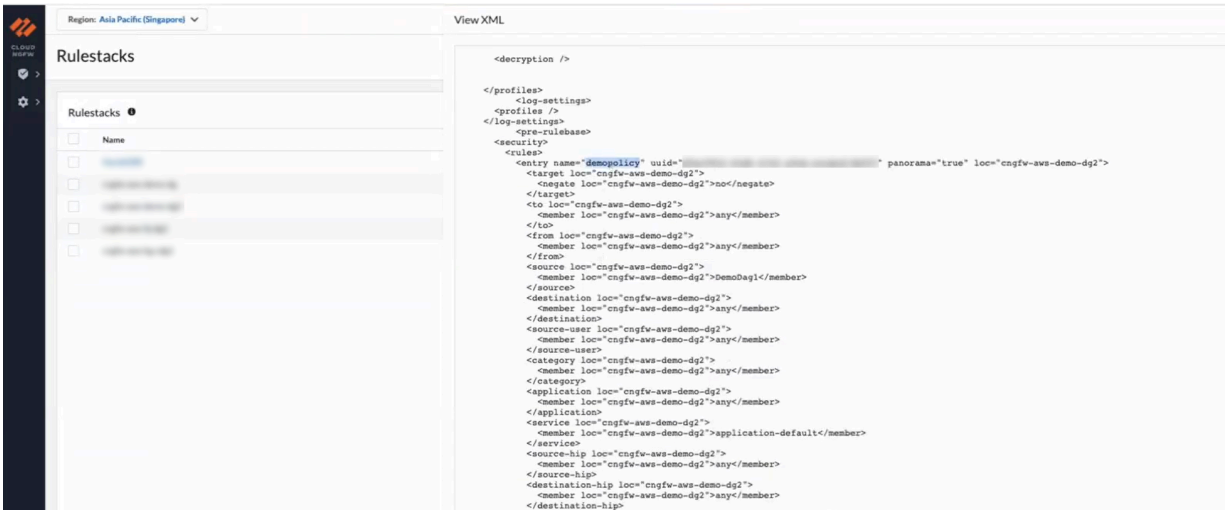
STEP 12 | **OK** をクリックします。

STEP 13 | Cloud NGFWデバイス グループに変更をコミットしてプッシュします。

ファイアウォールへの設定変更のコミットとプッシュの詳細については、「プレビュー、検証、または設定変更のコミット」を参照してください。

Cloud NGFWコンソールに戻り、Panoramaからそれぞれのクラウド デバイス グループにプッシュされたダイナミック アドレス ポリシー ルールを含むXMLファイルを確認します。クリック

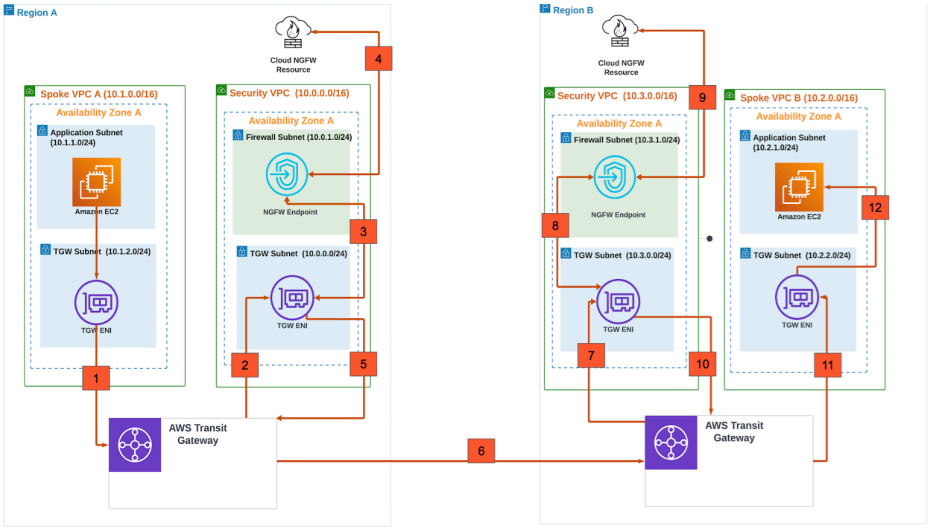
XMLを表示して、クラウド デバイス グループに新しく追加されたダイナミック アドレス ポリシー ルールの情報を表示します。



クライアント アカウントに新しいサブネットを追加します。詳細については、「AWSコンソールのサブネットの作成」を参照してください。

クロスリージョン タグ ベースのポリシー

2つの異なるリージョンのタグをクラウド デバイス グループに入力できます。



以下に例を示します。

リージョンXとリージョンYは、AWSリソースタグの検出を有効にするために希望するリージョンです。リージョンYからタグを学習する必要があるリージョンXにCNGFW リソースが存在し、それをリージョン X のCloud デバイス グループに使用する場合は、次の手順を実行します。

STEP 1 | AWSアカウントをCloud NGFWテナントに追加し、そこからタグを収集する。

STEP 2 | Panoramaプラグインを使用してタグを照会し、Panoramaデバイス グループに追加します。

STEP 3 | デバイス グループでタグを使用してダイナミック アドレス グループ オブジェクトを設定します。

ダイナミック アドレス グループ オブジェクトの設定に使用できるリージョン*X*タグのみが表示されます。

STEP 4 | リージョンYにリージョンXと同じ名前のクラウド デバイス グループを作成します。Panorama上で変更をコミットしてプッシュします。必要に応じて、VPCグループを作成して適切なVPCを割り当てるか、リージョンYのデフォルトVPCグループを使用します。

STEP 5 | リージョンYにモニタリング定義を作成し、VPCグループと通知グループ（Cloud デバイス グループがすでにマッピングされている場所）を選択します。

STEP 6 | デバイス グループでタグを使用してダイナミック アドレス グループ オブジェクトを設定します。ダイナミック アドレス グループ オブジェクトの設定にリージョンXタグとリージョンYタグの両方が使用できることが確認できます。

STEP 7 | Panoramaで設定をコミットします。

クラウド デバイス グループでは、設定するリージョンYのタグが表示され、ダイナミック アドレス グループを作成できます。

ゾーンベースのポリシールールを構成する

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）

ネットワークを機能ゾーンと組織ゾーンに分割すると、攻撃対象領域（潜在的な攻撃者にさらされる部分）が減ります。セキュリティ ゾーンは、ネットワークをより小さく管理しやすい領域に分割し、それらの領域へのトラフィック アクセスを制御することでネットワークを保護します。

自己管理型 Palo Alto Networks ファイアウォール (VM シリーズなど) では、セキュリティ ゾーンは 1 つ以上の物理または仮想ファイアウォール インターフェースと、ゾーンのインターフェースに接続されたネットワーク セグメントで構成されます。まずゾーンを定義し、次に物理インターフェースと仮想インターフェースをそれらのゾーンに関連付けます。最後に、作成したセキュリティ ポリシー ルールでこれらのゾーンを使用します。

ただし、Cloud NGFW はネットワーク構造を自動的に設定します。インターフェースの設定や、作成したゾーンへの関連付けについて心配する必要がなくなりました。Panorama でゾーンベースのポリシー ルールを作成し、Cloud NGFW に適用できます。

Cloud NGFWゾーン

Cloud NGFW を使用すると、 プライベート ゾーンと パブリック ゾーンを使用して VPC トラフィックを分類し、ポリシーの適用を簡素化できます。

- プライベート ゾーン には、 プライベート トラフィック範囲プレフィックスによって定義されたハイブリッド クラウド ネットワークが含まれます。このネットワークには、AWS 上の VPC とオンプレミス ネットワーク (Direct Connect または VPN 経由で接続) が含まれます。
- パブリック ゾーンは 、ハイブリッド クラウド ネットワーク (パブリック インターネット) の外部にあるすべてのプレフィックスで構成されます。

この分類を制御するには、トラフィックが Cloud NGFW リソースに入るエンドポイントのプライベート トラフィック範囲プレフィックスを適切に指定します。

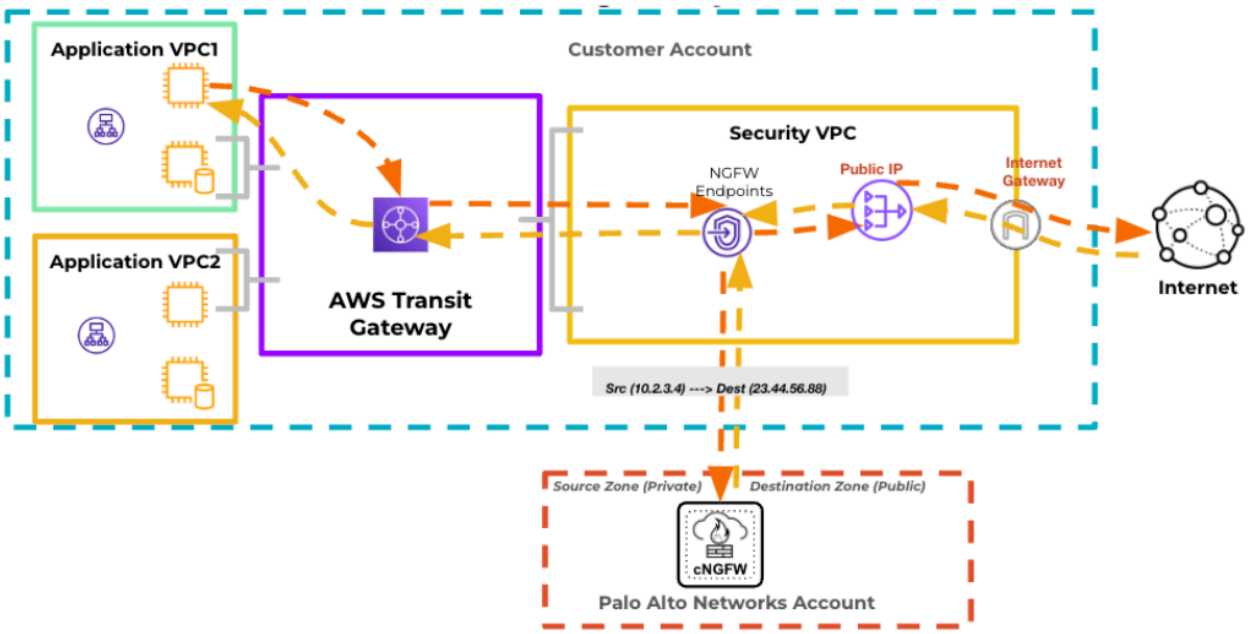
送信元ゾーンと送信先ゾーン

トラフィック セッションの送信元 IP アドレスが、トラフィックが Cloud NGFW リソースに入るエンドポイントに対して定義された プライベート トラフィック範囲 プレフィックス内にある場合、Cloud NGFW は自動的に ソース ゾーンを プライベート として割り当てます。それ以外の場合、Cloud NGFW はソースゾーンを **Public**として割り当てます。

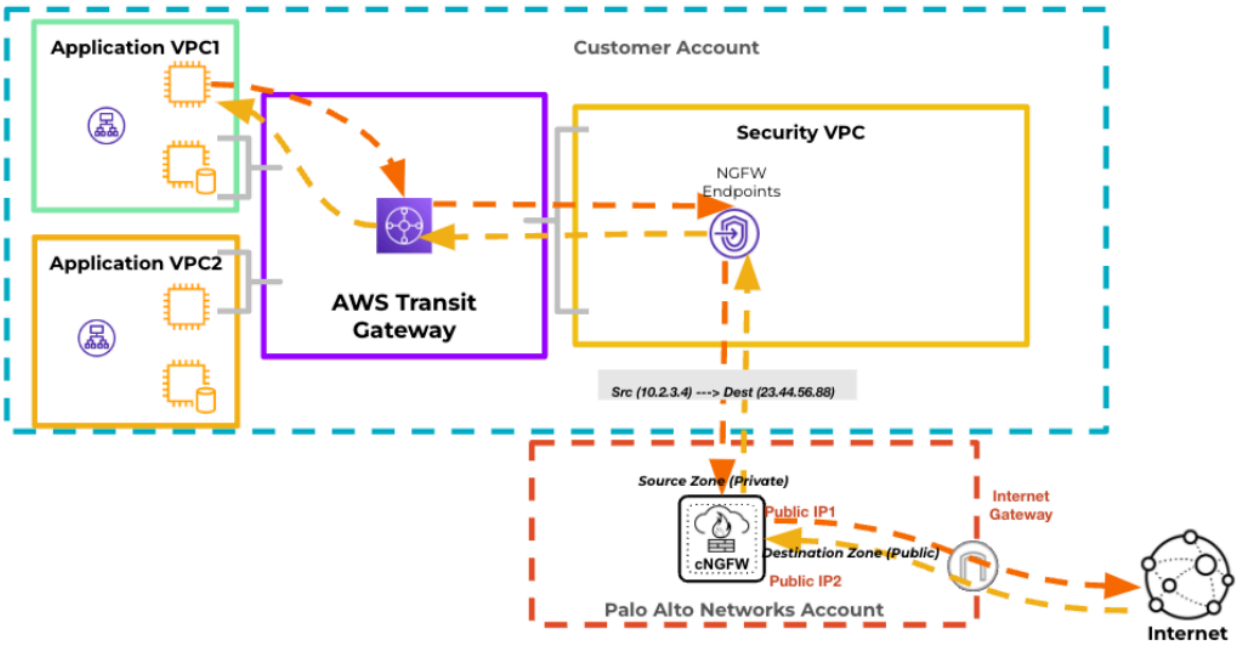
同様に、トラフィック セッションの宛先 IP アドレスが、トラフィックが Cloud NGFW リソースに入るエンドポイントに対して定義された プライベート トラフィック範囲 プレフィックス内にある場合、Cloud NGFW は 宛先ゾーンをプライベート として自動的に割り当てます。それ以外の場合、Cloud NGFW は宛先ゾーンを **Public**として割り当てます。

たとえば、Cloud NGFW は、送信元 IP アドレスが 10.2.3.4、宛先 IP アドレスが 23.44.55.66 のセッションに対して、送信元 (Ingress) ゾーンをプライベート、宛先ゾーンをパブリックに割り当てます。

次の図は、Egress NAT が無効になっているエンドポイント経由のトラフィックの送信元ゾーンと宛先ゾーンを示しています。



次の図は、Egress NAT が有効になっているエンドポイント経由のトラフィックの送信元ゾーンと宛先ゾーンを示しています。



ゾーン プロテクション

DoS 攻撃を効果的に防ぐには、レイヤーアプローチが必要になります。最初の防御層は、セッションベースのファイアウォールが処理するように設計されていないボリューム攻撃から防御するための、AWS Shield などの専用の大容量 DDoS 保護サービスである必要があります。ただし、クラウド NGFW は、ゾーン プロテクション プロファイルを使用して、より細かい DoS 攻撃防御レイヤーを追加し、専用の DDoS サービスでは提供されないアプリケーション トラフィックの可視性を提供します。

トラフィックが専用の DDoS サービス (AWS Shield など) を通過して VPC に入ると、Ingress (ソース) ゾーンに Zone Protection プロファイルが添付されている場合は、Cloud NGFW によってそれが適用されます。Cloud NGFW は、パケットの送信元 IP アドレスから Ingress (送信元) ゾーンを決定します。ゾーン プロテクション プロファイルは、ゾーンに入る集約トラフィックに基づいて、DoS 攻撃に対する広範な防御を提供します。ゾーン プロテクション プロファイルがパケットを拒否した場合、Cloud NGFW はパケットを破棄し、セキュリティ ポリシーの検索をスキップします。Cloud NGFW は、新しいセッション (既存のセッションと一致しないパケット) にのみゾーン プロテクション プロファイルを適用します。セッションが確立されると、クラウド NGFW パケット処理エンジンは、そのセッション内の後続のパケットに対してゾーン プロテクション プロファイルの検索をバイパスします。

Panorama Cloud デバイス グループ テンプレートを使用して、プライベート ゾーンとパブリック ゾーンにゾーン プロテクション プロファイルを添付できます。ゾーン プロテクション プロファイルは、最も一般的なフラッド攻撃、偵察攻撃、パケットベースの攻撃から入口 (またはソース) ゾーンを保護します。

- フラッド防御。フラッド防御を設定したゾーン プロテクション プロファイルは、入力ゾーン全体を SYN、ICMP、ICMPv6、UDP、およびその他の IP フラッド攻撃から保護します。

- 偵察行為防御。軍における定義と同様に、ネットワーク セキュリティにおける偵察行為の定義は、攻撃者が秘密裏にネットワークを調査して弱点を探り、ネットワークの脆弱性についての情報を得ようと試みることです。偵察行為はしばしば、ネットワークへの攻撃の前触れになります。ポートスキャンとホストスイープから防御するには、プライベートゾーンとパブリックゾーンの両方で偵察保護を有効にします 。
- パケット ベースの攻撃防御。パケット ベースの攻撃には様々な形態があります。ゾーン プロテクション プロファイルは、IP、TCP、ICMP、IPv6、および ICMPv6 パケット ヘッダーをチェックし、ゾーンにパケットを許可する前に、望ましくない特性を持つパケットをドロップしたり、パケットから望ましくないオプションを削除したりすることで、ゾーンを保護します。

Cloud NGFW ゾーンマッピング

ゾーンは、VM シリーズなどの自己管理型ファイアウォールのインターフェースに関連付けられます。ただし、Cloud NGFW 内では、ネットワーク インフラストラクチャが自動的に設定されます。つまり、インターフェースの設定や、作成したゾーンへの関連付けについて心配する必要がなくなります (また、Panorama Cloud NGFW テンプレート スタックとテンプレートでは、インターフェースを設定するための Web インターフェースが Panorama から削除され、不要な Panorama Web インターフェース要素は Panorama Managed Cloud Device Groups から削除されます)。

ただし、一貫したセキュリティ ポリシーの適用を有効にするには、クラウド デバイス グループにゾーン マッピングを作成し、クラウド NGFW が Panorama 内のセキュリティ ゾーンをクラウド NGFW のプライベート (内部) ゾーンとパブリック (外部) ゾーンのどちらに関連付けるかを認識できるようにする必要があります。これらのマッピングにより、Cloud NGFW はセキュリティ ポリシー ルールを適切に適用できるようになります。

最新バージョンの *AWS* プラグイン *(*バージョン *5.3.0)* を実行していない場合、ゾーン マッピングが失敗することがあります。*Palo Alto Networks* では、*AWS* プラグイン バージョン *5.3.0* 以降を使用して新しい *Egress NAT AMI* にアップグレードされていない既存のファイアウォールに対しては、ゾーンベースのポリシーを有効にしないことをお勧めします。

Panorama Cloud デバイス グループでゾーン マッピングを構成する

ゾーンベースのポリシー ルールには、次の最小システム要件が必要です。

- AWS プラグイン バージョン 5.3.0 以上、
- PAN-OS バージョン 10.2.8 以上、
- Cloud Connector プラグイン バージョン 2.0.1 以上

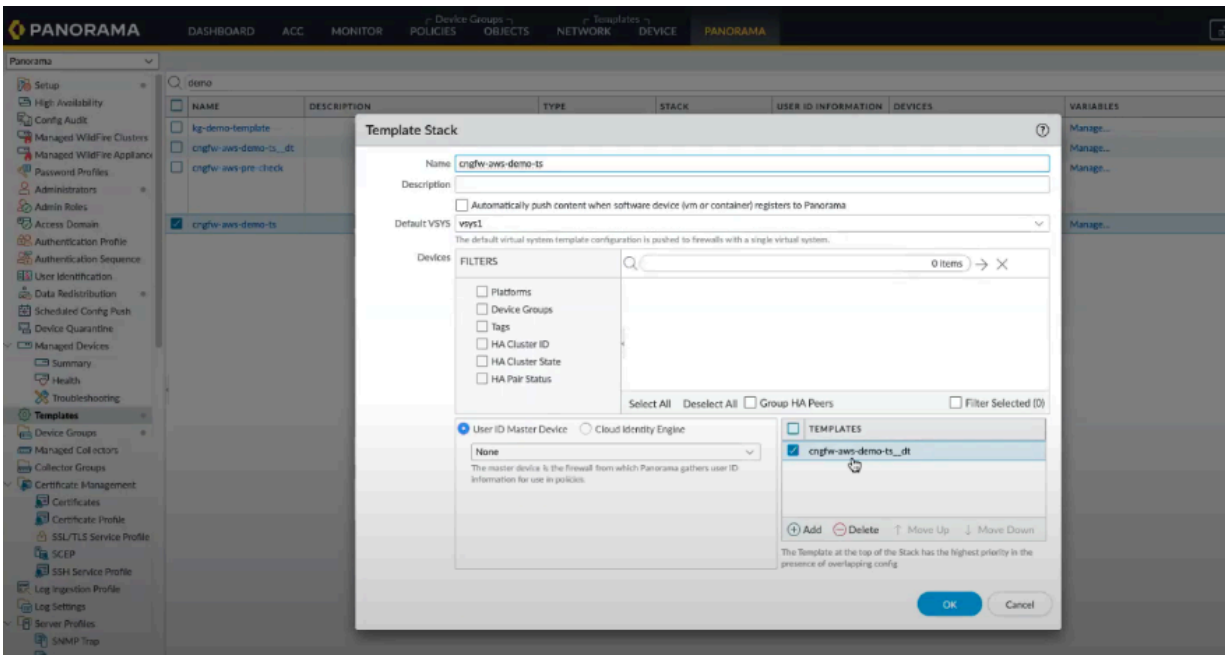
Panorama コンソールを使用してゾーン マッピングを構成するには:

STEP 1 | Panoramaコンソールを使用してクラウド デバイス グループを追加する方法。

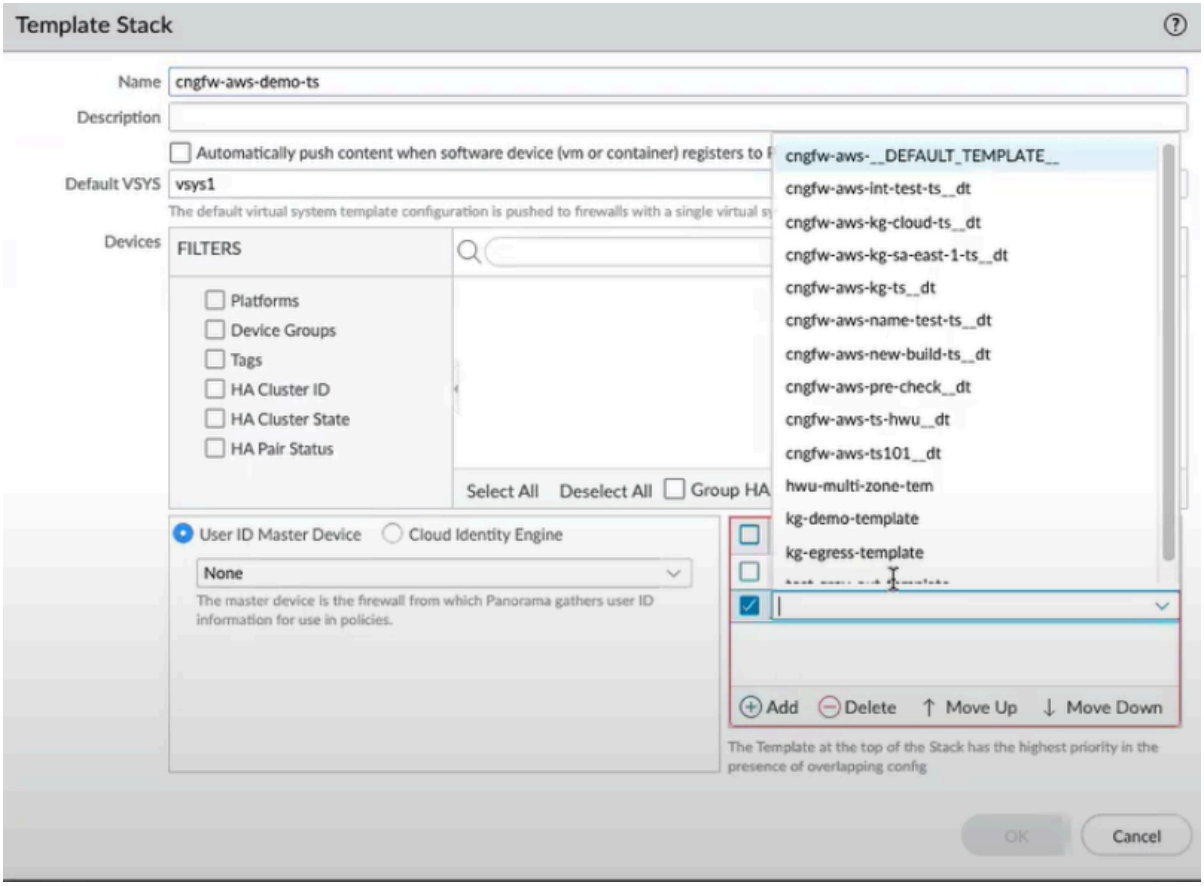
STEP 2 | **Panorama** > テンプレート を選択し、 テンプレートスタックを選択します。

AWS プラグインは、テンプレート スタックをクラウド デバイス グループに関連付けます。AWS プラグインはデフォルトのテンプレートを作成し、デフォルトでこのテンプレートに パブリック ゾーン と プライベート ゾーンを追加します。

テンプレート セクションでは、AWS プラグインによって作成されたデフォルトのテンプレートを確認できます。このテンプレートの名前は、テンプレートスタックと同じ名前で、その名前にサフィックス `__dt` が追加されます。



STEP 3 | 他の Panorama テンプレートをテンプレート スタック リストに参照し、**[追加]** をクリックしてテンプレートを選択することもできます。



STEP 4 | ゾーン プロテクション プロファイルを作成し、それをデフォルト テンプレートのデフォルトの プライベート ゾーンと パブリック ゾーンに関連付けます。ゾーン プロテクション プロファイルを作成するには:

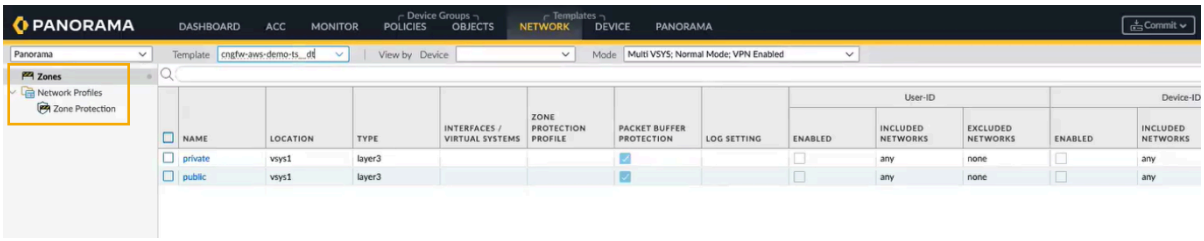
1. Panorama コンソールで、**[ネットワーク] >[ゾーン プロテクション]**に移動します。
2. **[追加]** をクリックします。
3. ゾーン プロテクション プロファイルの 名前 と 説明 を入力します。
4. ゾーン プロテクションサービスを選択します。
5. **OK** をクリックします。

ゾーン プロテクション プロファイルを作成した後、次の手順を実行して、デフォルト テンプレートの プライベート ゾーンと パブリック ゾーンを関連付けます。

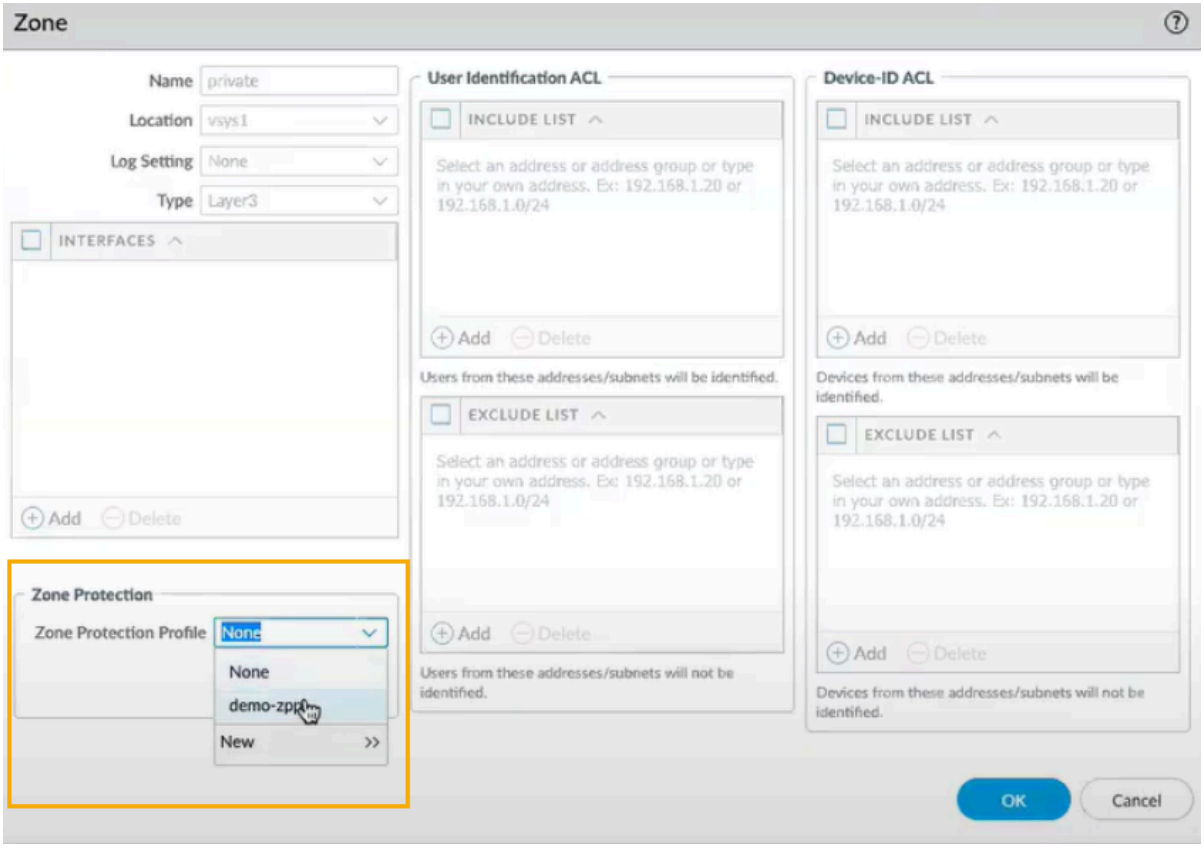
STEP 5 | Panorama コンソールで、**[ネットワーク]** タブを選択します。

STEP 6 | **Template**（テンプレート）を選択します。

STEP 7 | ゾーンに移動します。



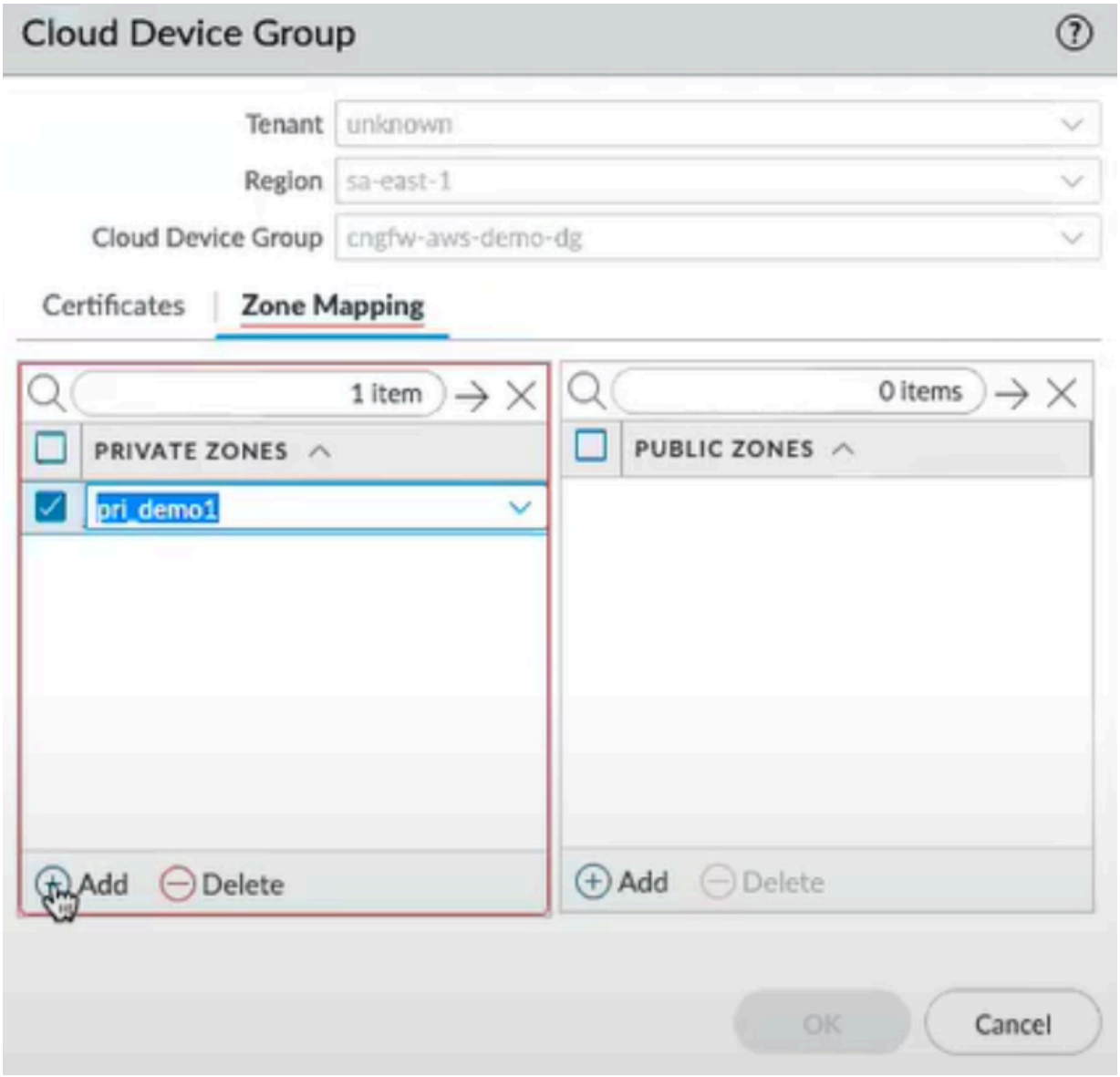
STEP 8 | **[プライベート]** をクリックし、 プライベート ゾーンの ゾーン プロテクション プロファイル を選択します。



STEP 9 | **[パブリック]** をクリックし、 パブリック ゾーンの ゾーン プロテクション プロファイル を選択します。

STEP 10 | クラウド デバイス グループに戻ります。ゾーン マッピング タブに移動します。

テンプレート スタック リストに参照した Panorama テンプレートのリストが表示されます。Panorama ゾーンを、AWS プラグインによって作成されたデフォルトの プライベート ゾーンと パブリック ゾーンにマップできます。



STEP 11 | Panorama でクラウド デバイス グループのセキュリティ ポリシー ルールを構成します。その後、上記でマップされた Panorama セキュリティ ゾーン、セキュリティ ポリシー内の

デフォルトの プライベート ゾーンまたは パブリック ゾーンを、送信元ゾーンまたは宛先ゾーンとして使用できます。詳細については、「ポリシーの適用」 セクションを参照してください。

プライベートからパブリック、パブリックからプライベート、プライベートからプライベート、*any-to-any*、プライベートから*any* は、*Panorama Cloud* デバイス グループで許可されるゾーンベースのポリシー ルールです。セキュリティ ルールでは、送信元セキュリティ ゾーンと宛先セキュリティ ゾーンのその他の組み合わせはサポートされていません。

STEP 12 | Panoramaで変更をコミットし、プッシュします。

STEP 13 | Cloud NGFW コンソールにログインして、Panorama からそれぞれのクラウド デバイス グループにプッシュされた プライベート ゾーン と パブリック ゾーンのマッピングを含む XML ファイルを確認します。

STEP 14 | 「**Rulestacks**」に移動し、 クラウド デバイス グループを選択して、「**XML** の表示」 をクリックすると、Panorama からクラウド デバイス グループに新しく追加された プライベート ゾーン とパブリック ゾーンの情報が表示されます。

上記の手順を使用して、テンプレート スタックから既存のテンプレートを追加して既存のクラウド デバイス グループにゾーンベースのポリシー ルールを設定し、*Panorama* でそれらのクラウド デバイス グループのセキュリティ ポリシー ルールを設定することもできます。

Strata Cloud Managerポリシー管理

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リソースを Strata Cloud Manager(SCM) ポリシー管理用にリンクします。Strata Cloud Managerは、ネットワーク セキュリティ デプロイメント全体を統合管理するため、Palo Alto Networksのセキュリティ インフラストラクチャを単一の合理化されたWebインターフェースから簡単に管理できます。このインターフェースを使用すると、すべてのネットワーク セキュリティ適用ポイントで、ユーザー、ブランチ サイト、アプリケーション、および脅威を包括的に可視化できます。この機能により、実用的な分析情報、セキュリティの向上、簡単なトラブルシューティングと問題解決が可能になります。

Cloud NGFWポリシー管理にSCMを使用する場合は、以下の点を考慮してください。

- SCMに初めて接続すると、Cloud NGFWリソース(リソースIDなど)が表示されないことがあります。これらのリソースは、根本的な接続の問題がない場合、しばらくすると表示されます。
- Cloud NGFW SCM ポリシー管理のベストプラクティスは、Cloud NGFWリソースで Panoramaポリシー管理を使用する場合とは異なります。たとえば、Panorama管理環境の一部のパススルー トラフィックは、SCM管理のCloud NGFWリソースでドロップされる場合があります。
- X転送機能は、Cloud NGFWリソースの SCM ポリシー管理ではサポートされていません。
- クラウド証明書はサポートされていません。
- DLP はサポートされていません。
- SCMで管理されているCloud NGFWリソースのセキュリティ ルールを設定するときは、セキュリティルールの場合**ANY**を指定する必要があります。しかし**from/to**ゾーンはStrata Logging Service でデータゾーンとして表示されます。

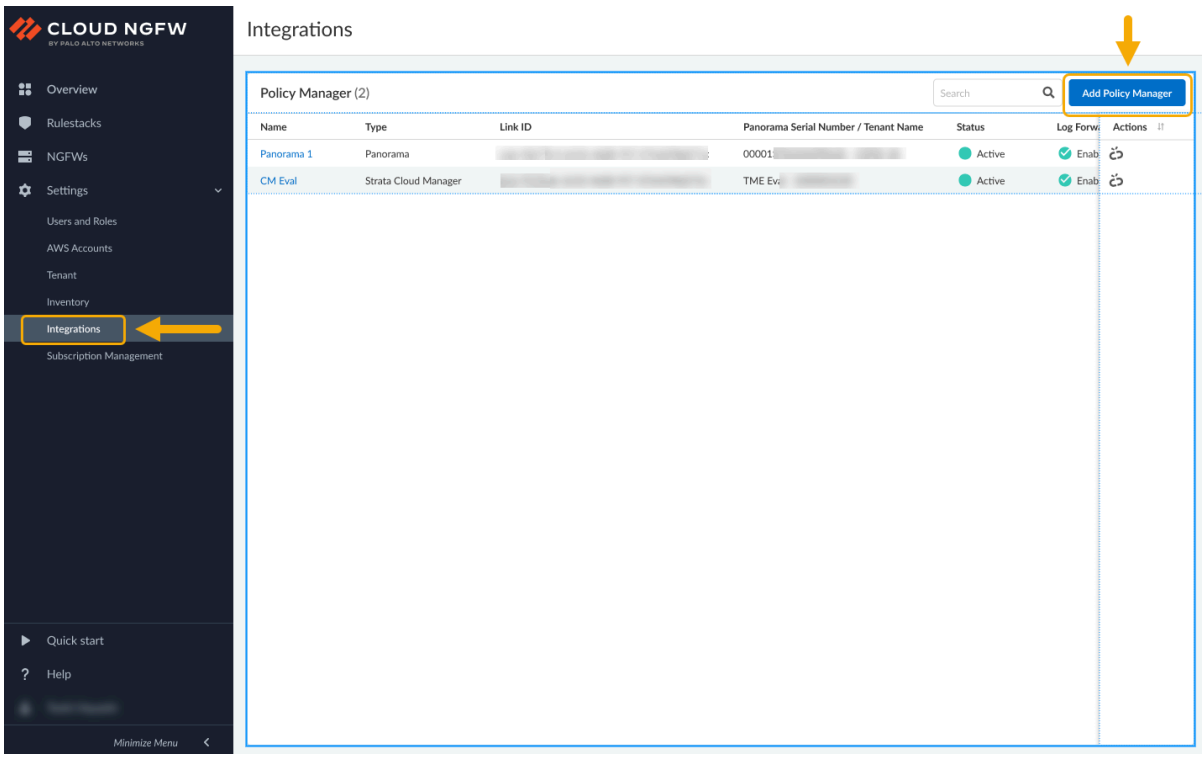
Cloud NGFWリソースをStrata Cloud Managerポリシー管理にリンクする

Cloud NGFW リソースを Strata Cloud Manager Policy Managementと統合する方法:

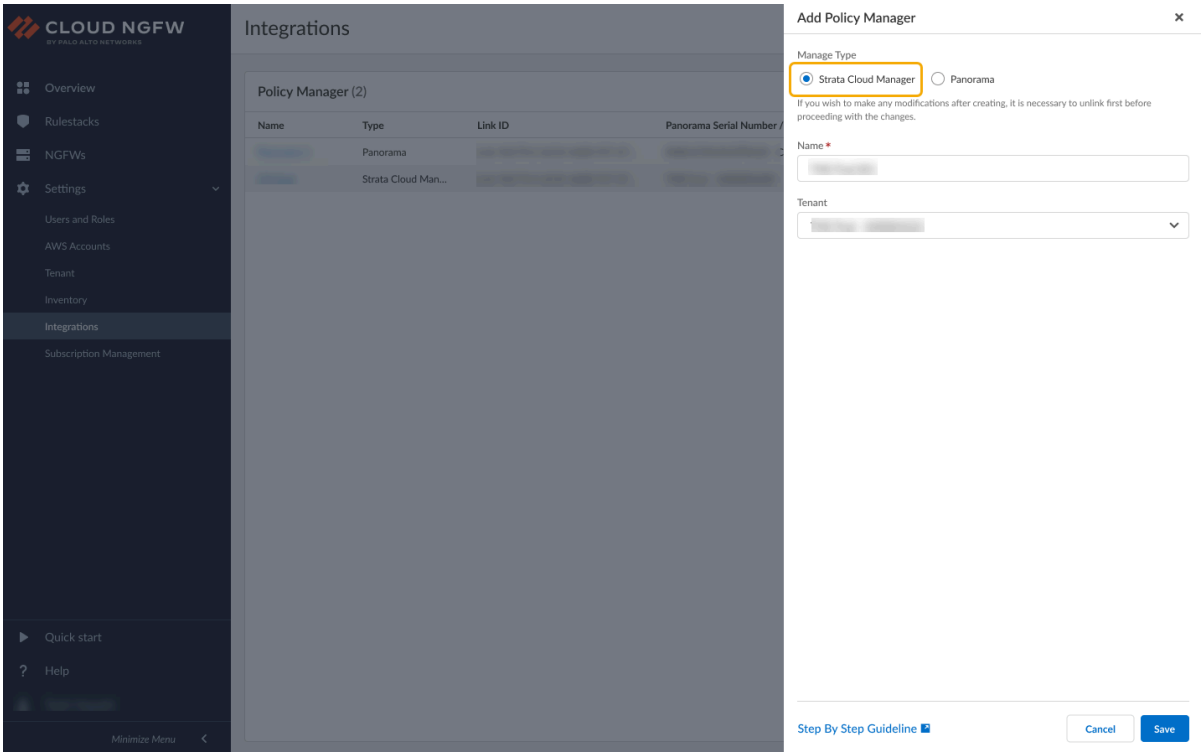
STEP 1 | Cloud NGFW コンソールにログインします。

STEP 2 | **[Integrations (統合)]**を選択します。

STEP 3 | **[Policy Manager(ポリシー マネージャ)]** 画面で、 **[Add Policy Manager(ポリシーマネージャを追加)]**をクリックします。



STEP 4 | **[Add Policy Manager(**ポリシーマネージャを追加**)]**セクションで、 **[Manage Type(**管理タイプ**)]**に**[Strata Cloud Manager]**を選択します。



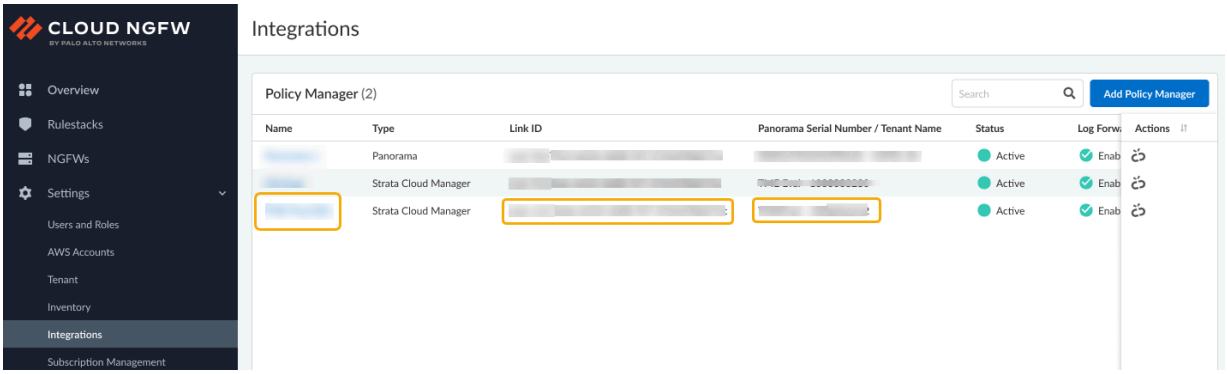
STEP 5 | 分かりやすい名前を入力します。

STEP 6 | ドロップダウンメニューを使用してリソースに関連付けるSCMテナントを選択します。

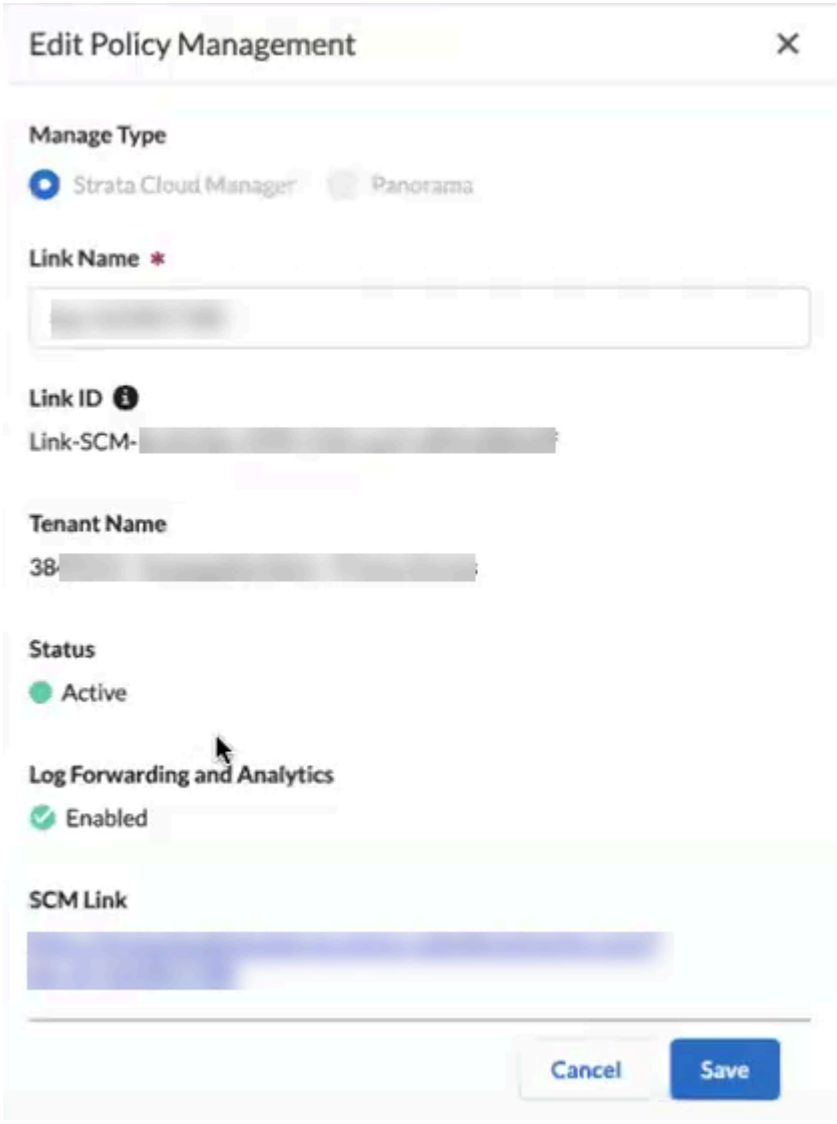
カスタマー サポート ポータル*(CSP)*アカウントは、*SCM*と*CNGFW*の両方で同じである必要があります。

STEP 7 | **[Save(保存)]**をクリックします。これにより、Cloud NGFWリソースがSCMテナントに効果的にリンクされます。

設定を保存した後、**[Integrations(統合)]**ページが更新され、新しいポリシー管理パラダイムが、関連するリンクIDとSCMシリアルナンバー/テナント名とともに反映されます。



リンクされた個々のSCMテナントに関する情報を表示するには、ポリシー マネージャ画面のリンク**ID**をクリックします。**[Edit Policy Management(ポリシー管理の編集)]**画面を仕様して**[Link Name(リンク名)]**を変更し、情報を表示します。



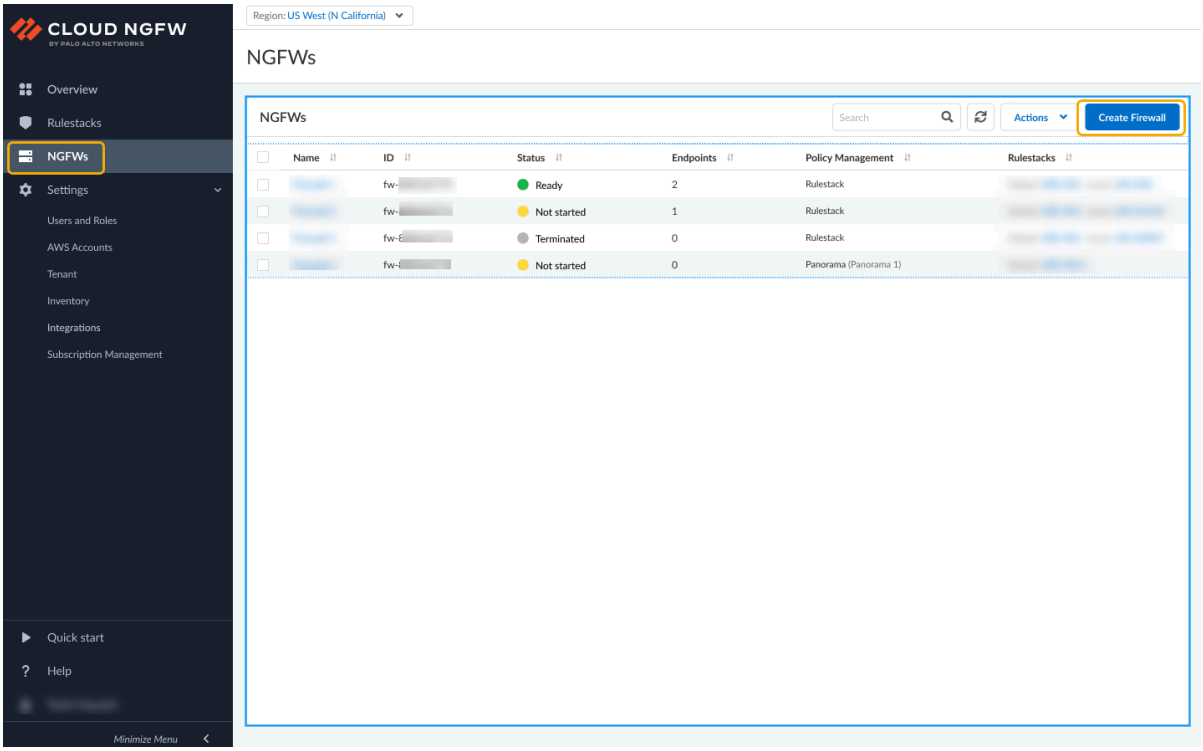
ファイアウォールをStrata Cloud Managerポリシー管理に関連付ける

Strata Cloudポリシー管理へのリンクを確立したら、リンクされたSCMテナントに新しいファイアウォールを関連付けることができます。

STEP 1 | Cloud NGFW コンソールにログインします。

STEP 2 | ［**NGFW**］を選択します。

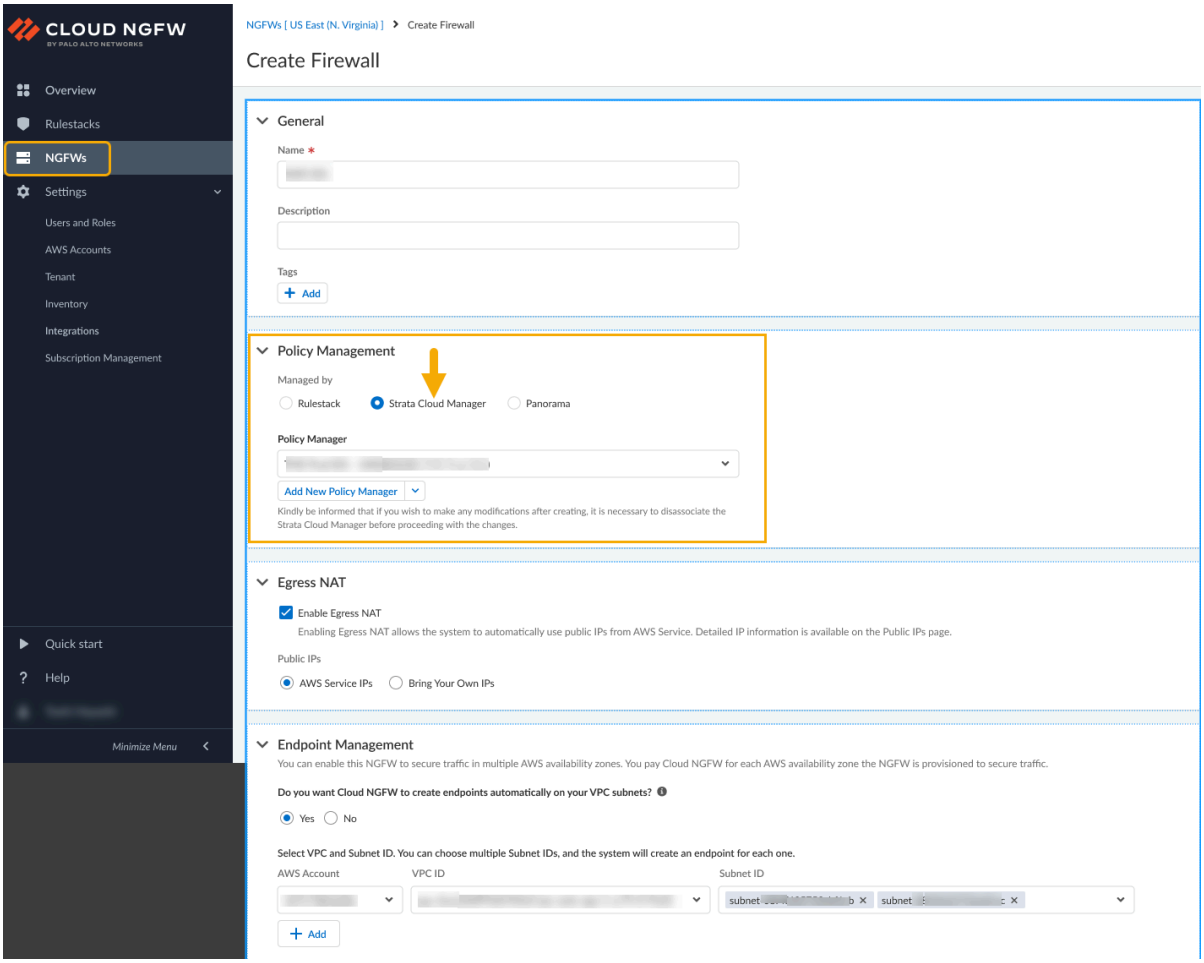
STEP 3 | **[Create Firewall(ファイアウォールの作成)]**をクリックします。



STEP 4 | **[Create Firewall(ファイアウォールの作成)]**画面で、ファイアウォールの名前を入力します。

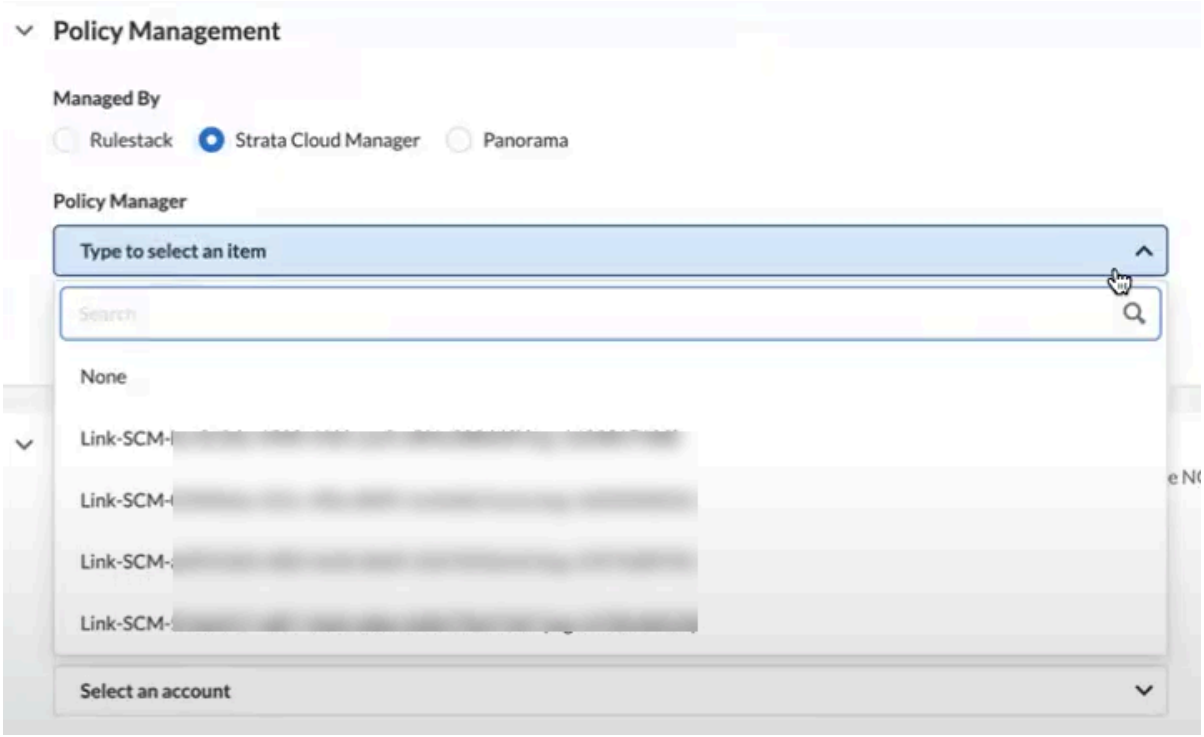
STEP 5 | 必要に応じて、説明を含めます。

STEP 6 | **[Policy Managment(ポリシー管理)]**セクションで、 **Strata Cloud Manager**.



を選択します。

STEP 7 | **[Policy Manager(ポリシーマネージャ)]**ドロップダウン メニューで、ファイアウォールに関連付けるリンクされたSCMテナントを選択します。



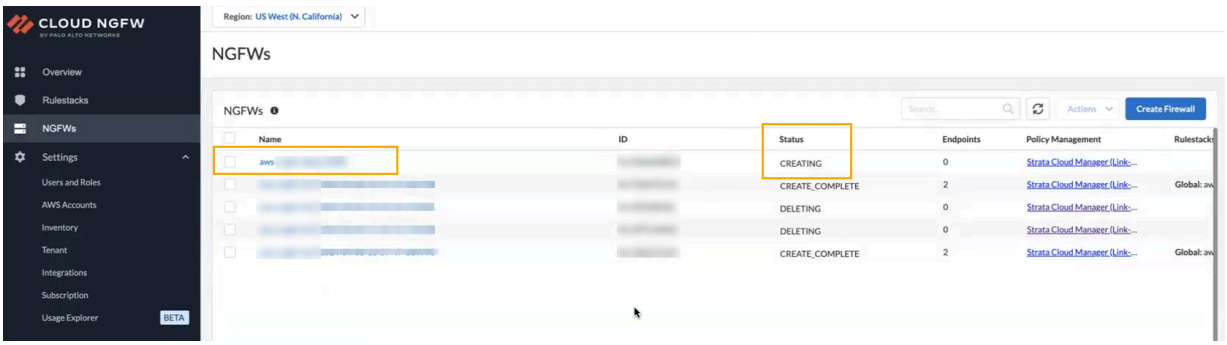
STEP 8 | **[Endpoint Management(**エンドポイント管理**)]**を設定して、複数のAWS可用性ゾーンのトラフィックをセキュリティで保護します。

1. Cloud NGFWでVPC サブネット上にエンドポイントを自動的に作成するかどうかを決定します。サービス管理エンドポイントの場合**[Yes(**はい**)]** を選択します。

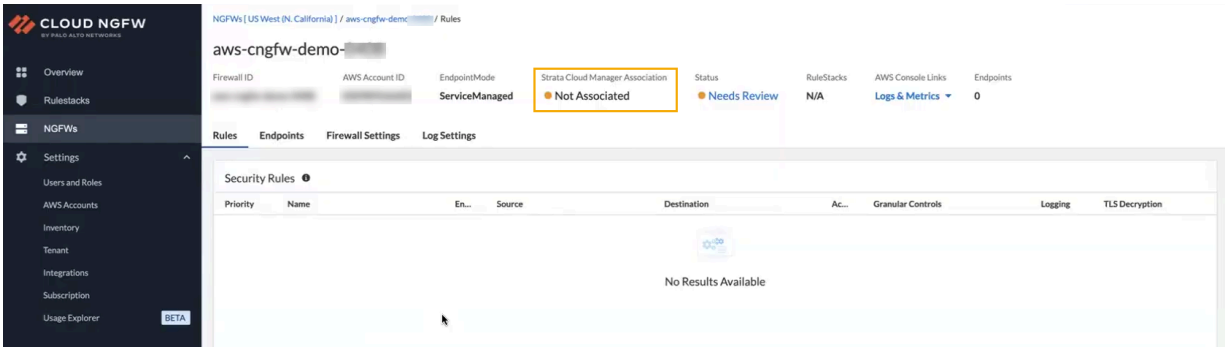
   デフォルトでは、*Cloud NGFW*リソースはこれらのエンドポイントを自動的に作成しません。ラジオボタンは***[No(***いいえ***)]***に設定されています。

2. ドロップダウンを使用して、**AWS**アカウント**ID**を選択します。
3. ドロップダウンを使用して、**VPC**を選択します。
4. サブネット フィールドを使用して、使用可能なサブネットを選択します。
5. **[Save(**保存**)]**をクリックします。

NGFW画面が、新しく作成されたファイアウォールを反映して変更されます。新しいファイアウォールを作成するプロセスを完了するには、約6～10分かかります。 ステータスは**[CREATING(**作成中**)]**と表示されます。



NGFW名をクリックして、ファイアウォールに関する詳細情報を表示します。ファイアウォールの作成中は、表示される情報は限定されます。



Strata Cloud Managerでのファイアウォールの表示

Cloud NGFW リソースをSCMテナントにリンクし、ファイアウォールを作成したら、SCMをポリシー管理に使用できます。

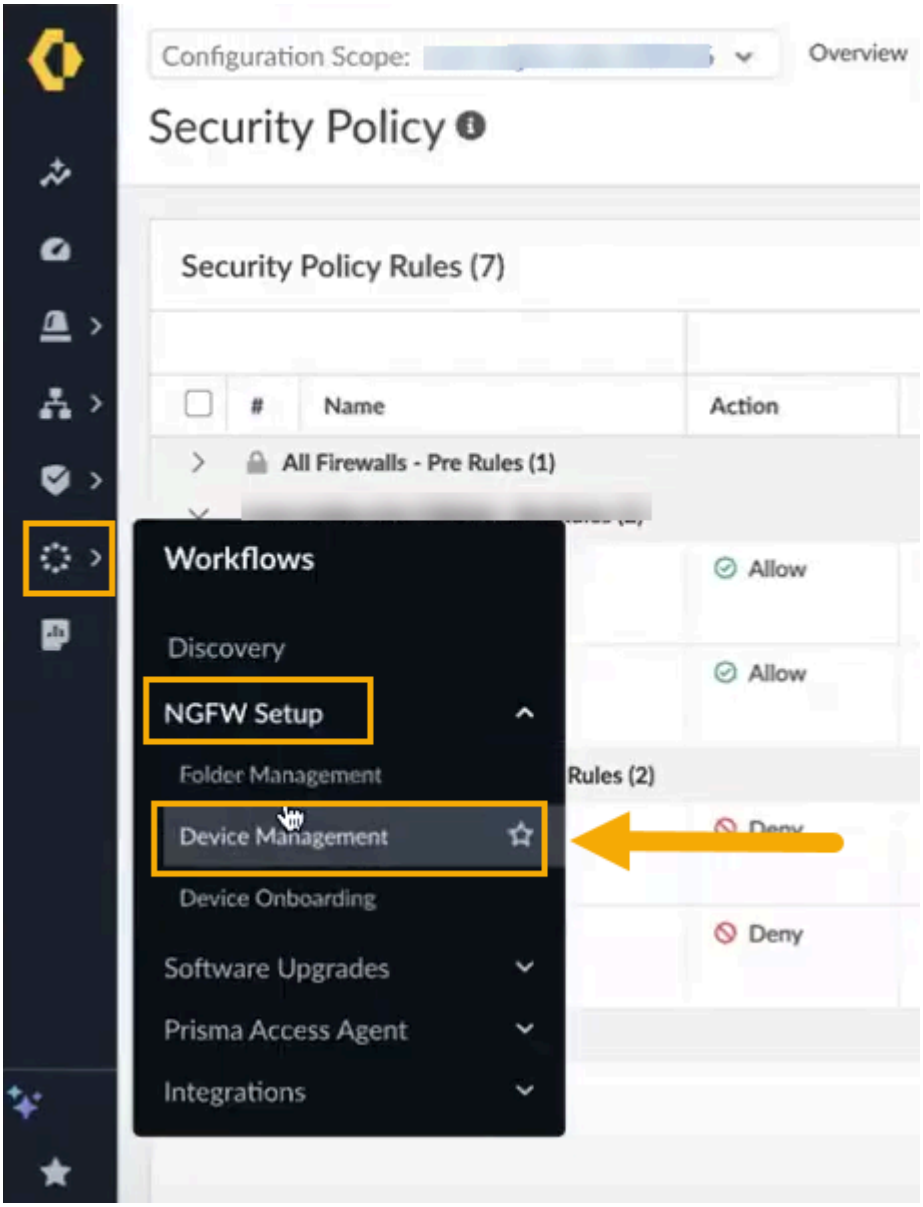
*Strata Cloud Managerにログインすると、ダッシュボードの**NGFW >[**ソフトウェア**]**にCloud NGFWカウントが表示されません。*

STEP 1 | stratacloudmanager.paloaltonetworks.comで直接、Palo Alto Networksハブから Strata Cloud Managerアプリにログインします。

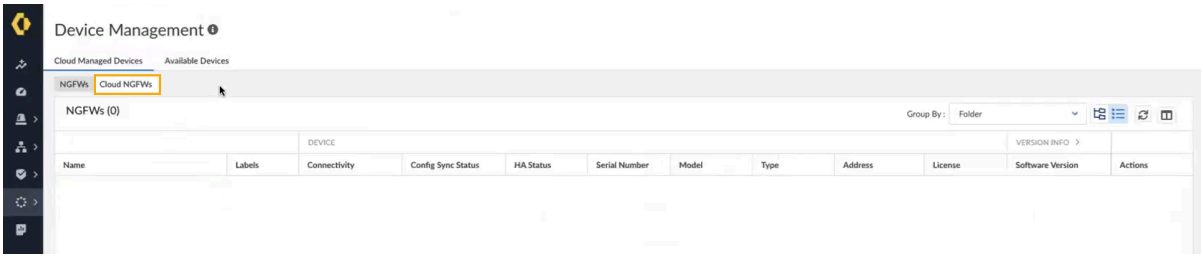
STEP 2 | Strata Cloud Managerインターフェースで、左側のナビゲーション オプションを使用してCloud NGFWテナントを見つけます。

これにより、Cloud NGFW リソースにリンクされている使用可能なテナントが公開されます。または、テナント名又は*ID*でテナントを検索できます。

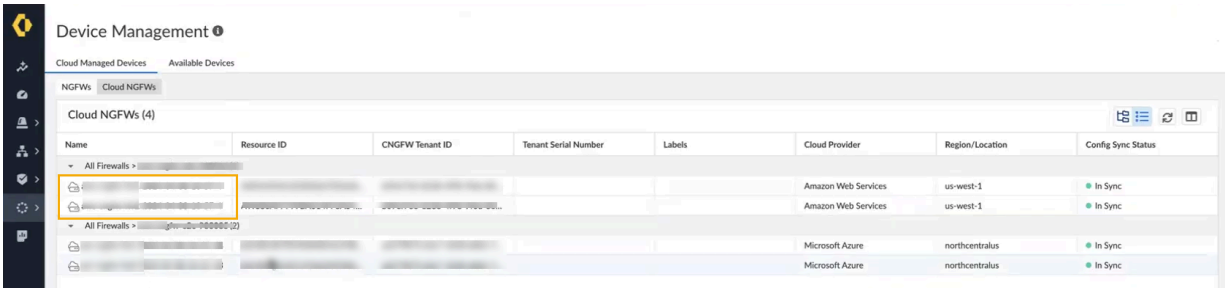
STEP 3 | **[Workflows(ワークフロー)] > [NGFW Setup(NGFWセットアップ)] >[Device Management(デバイス管理)]**を選択します。



STEP 4 | [Device Management(デバイス管理)]画面には、 **NGFWs**と**Cloud NGFW**が表示されます。SCM テナントに関連付けられているファイアウォールを表示するには、**Cloud NGFW**をクリックします。



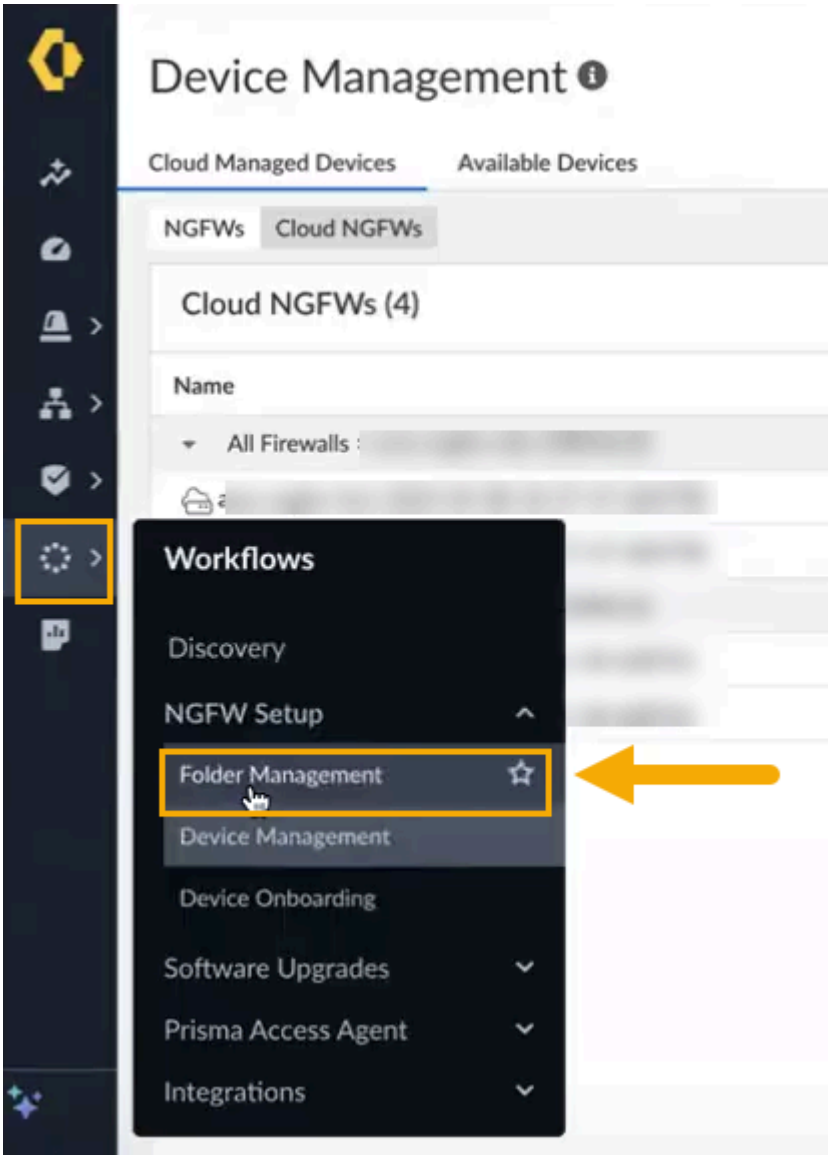
[Device Management(デバイス管理)]画面には、現在SCMによって管理されているCloud NGFWリソースが表示されます。



[Device Management(デバイス管理)] 画面には、以下のフィールドが表示されます。

- [Name(名前)]。Cloud NGFW リソースの名前を表します。
- [Resource ID(リソースID)]。NGFWリソースに関連付けられているリソースIDを示します。
- [CNGFW Tenant ID(CNGFWテナントID)]。SCMにリンクされている Cloud NGFW テナントに関連付けられている ID。
- [CNGFW Tenant Serial Number(CNGFWテナントのシリアルナンバー)]Cloud NGFW テナントに関連付けられたシリアルナンバー。
- [Labels(ラベル)]。Cloud NGFWに付与された任意のラベル。
- [Cloud Provider(クラウド プロバイダ)]。Cloud NGFWリソースに関連付けられているクラウド プロバイダを示します。
- リージョンとロケーション。Cloud NGFWリソースが配置されているリージョン。
- [Config Sync Status(設定同期ステータス)]。Cloud NGFWリソースのステータス。

STEP 5 | **[Device Management(デバイス管理)]**画面は、Cloud NGFWリソースをフォルダ 1 にグループ化します。これらのフォルダの構造を表示するには、 **[Workflows(ワークフロー)] > [Folder Management(フォルダ管理)**を選択します。



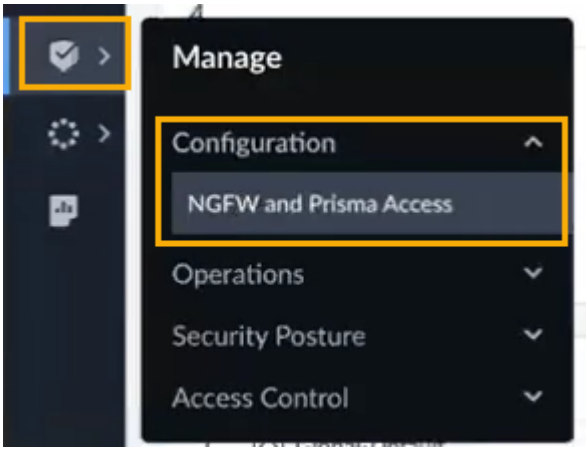
[Folder Management(フォルダ管理)]画面には、SCMテナントに関連付けられた Cloud NGFWリソースが表示されます。

フォルダの作成については、以下を参照してください。 Strata Cloud Managerを使用してCloud NGFWリソース用のフォルダを作成する。

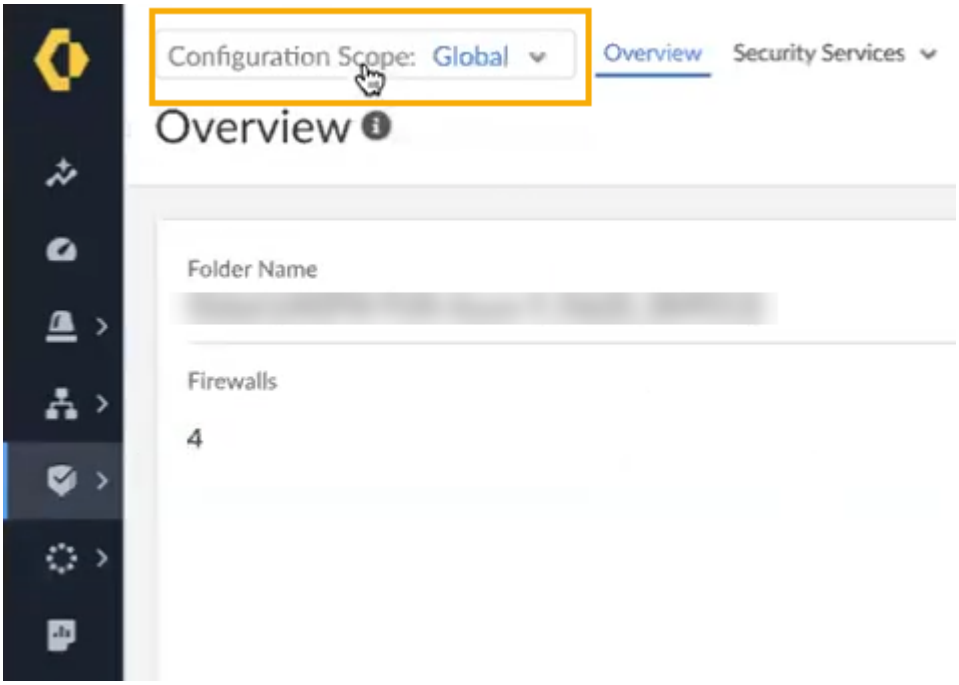
Strata Cloud Managerを使用したCloud NGFWポリシー管理

Strata Cloud Managerを使用して、フォルダを構成するCloud NGFWリソースにセキュリティ ポリシーをグローバルに適用できます。

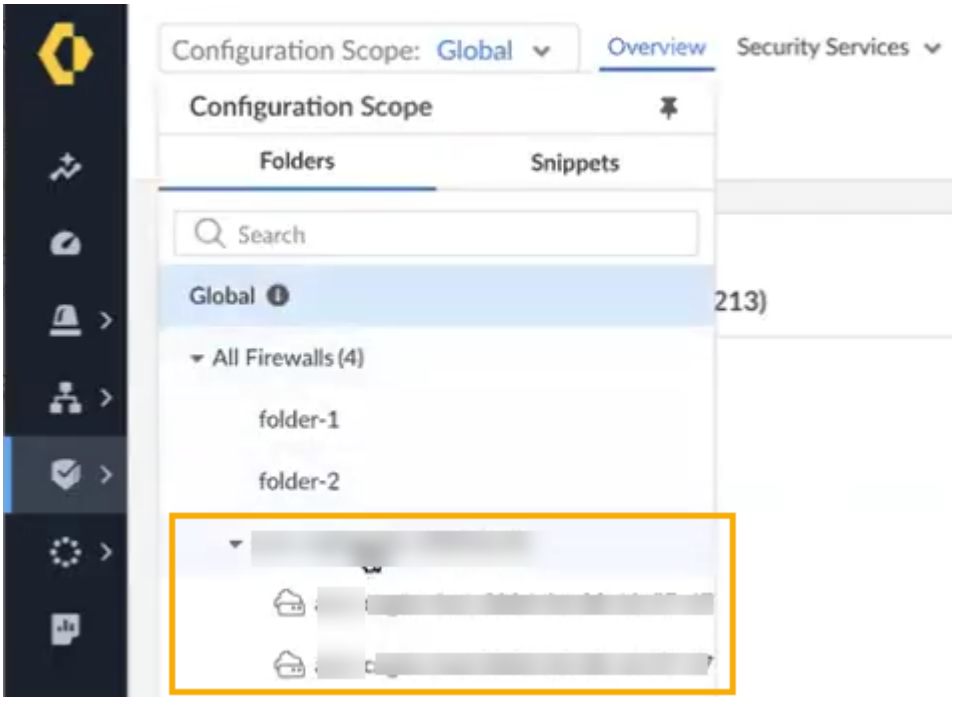
STEP 1 | Strata Cloud Managerで、**[Manage(管理)] > [Configuration(設定)] > [NGFW and Prisma Access(NGFWとPrisma Access)]**を選択します。



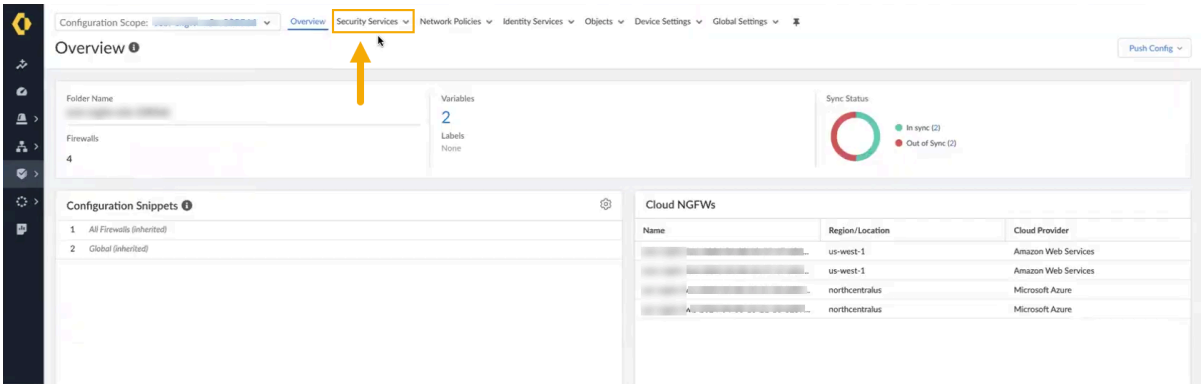
STEP 2 | 設定スコープを選択します。



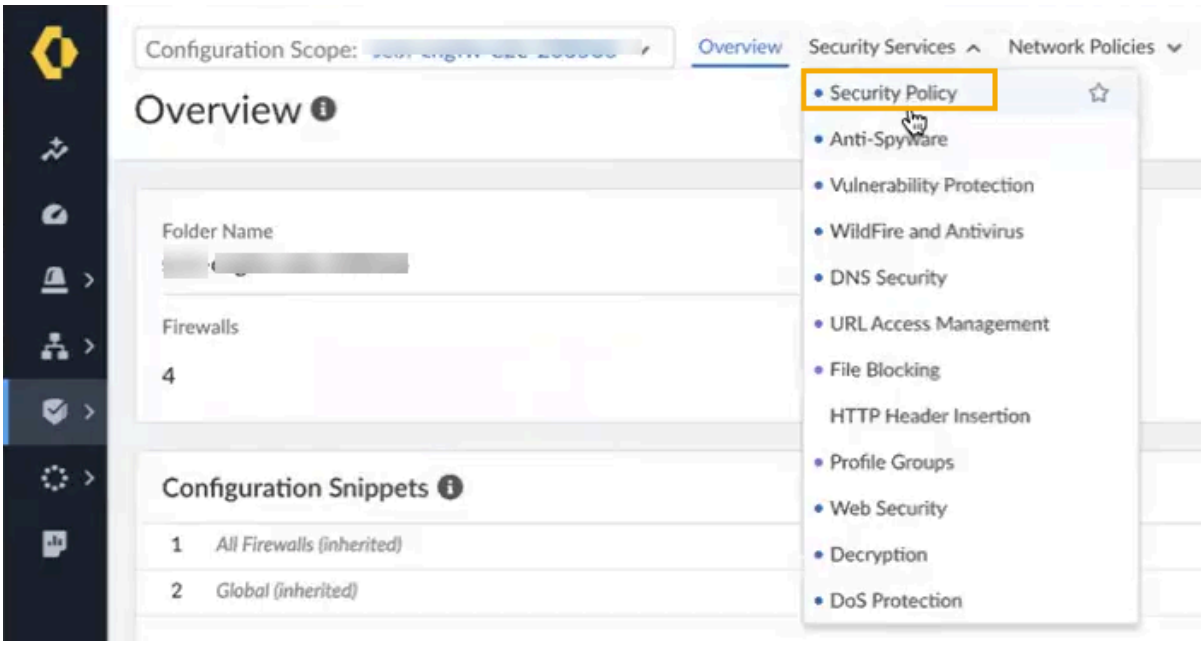
STEP 3 | ドロップダウンリストで、 **Cloud NGFW AWS**リソースを含むフォルダを探します:



STEP 4 | **[Overviewe(概要)]**ページで、**[Security Services(**セキュリティ サービス**)**を選択します。



STEP 5 | **[Security Services(セキュリティサービス)]** ドロップダウンリストで、**[Security Policy (セキュリティ ポリシー)**を選択します。



Strata Cloud Managerを使用したセキュリティ ポリシーの設定の詳細については、次を参照してください。 セキュリティポリシーの管理。

Strata Cloud Managerを使用してCloud NGFWリソース用のフォルダを作成します

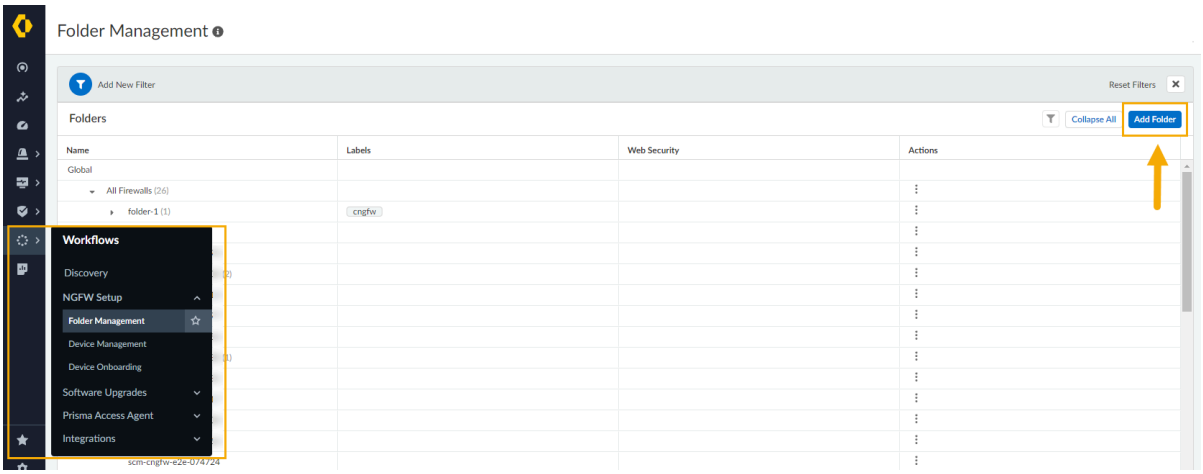
Cloud NGFW リソースにStrata Cloud Managerサービスを使用するように適切なサブスクリプションを設定したら、ファイアウォールに関連付けられたデータを表示するためのフォルダを作成します。フォルダは、ファイアウォールやデプロイメントタイプ(Cloud NGFWリソースのサービス接続など)を論理的にグループ化し、設定管理を簡素化するために使用されます。複数のネストされたフォルダを含むフォルダを作成して、同様の設定を必要とするファイアウォールとデプロイメントをグループ化できます。すでにネストされているフォルダには、複数のネストされたフォルダを含めることもできます。

他の*Palo Alto Networks*アプリケーション*(Prisma Access*など*)*と*NGFW*のフォルダは別々です。*Prisma Access*のデプロイメントを含むフォルダ内の*NGFW*をグループ化することはできません。ただし、共有設定をすべてのフォルダにグローバルに適用したり、 [Manage(管理)]:[Snippet(スニペット)] を使用して、標準設定とポリシー要件を複数のフォルダに簡単に適用できます。

Cloud NGFWリソース用のフォルダを作成するには:

STEP 1 | stratacloudmanager.paloaltonetworks.comで直接、Palo Alto Networksハブから Strata Cloud Managerアプリにログインします。

STEP 2 | Strata Cloud Managerインターフェースで、 **[Workflow(ワークフロー)]** > **[NGFW Setup(NGFWセットアップ)]** > **[Folder Management(フォルダ管理)]** を選択し、 **[Add Folder(フォルダを追加)]**をクリックします。



STEP 3 | **[Create Folder(フォルダ作成)]**画面:

1. フォルダの分かりやすい名前を入力します。
2. 必要に応じて、フォルダの説明を入力します。
3. 必要に応じて、1つ以上のラベルを割り当てます。既存のラベルを選択するか、作成するラベルを入力して新しいラベルを作成できます。たとえば、**[Labels(ラベル)]**ドロップダウンを選択して**[cngfw]**を選択します。
4. ドロップダウン メニューを使用して、フォルダを作成する場所を指定します。**[All Firewalls(すべてのファイアウォール)]**を選択するか、既存のフォルダを選択して、その下にフォルダをネストします。これは必須フィールドです。
5. 作成をクリックします。

フォルダの分かりやすい名前を入力します。

Strata Cloud Managerを使用した監視とトラブルシューティング

Strata Cloud Managerを使用して、Cloud NGFWリソースのステータスについて知ることができます。SCM が提供する**Monitor(モニター)**機能では、次の内容について説明します。

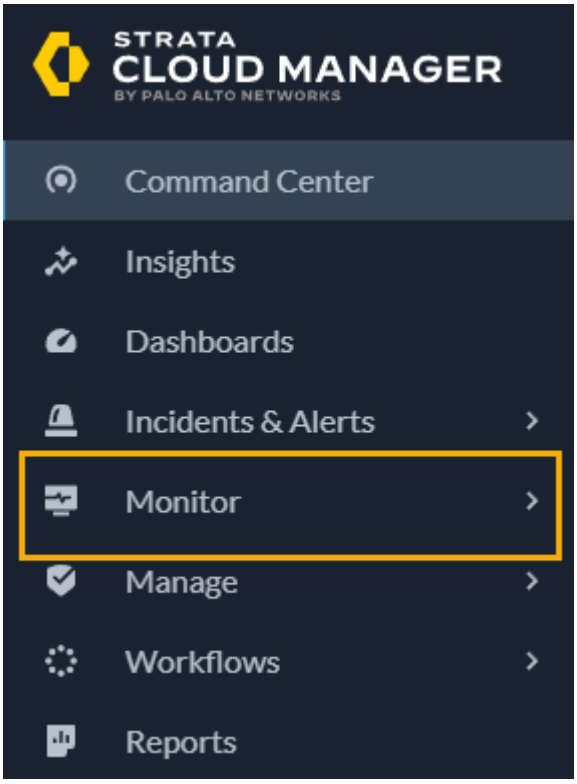
- Strata Cloud Managerで管理している製品とサブスクリプション。
- Cloud NGFWデバイスの正常性と接続ステータス。

詳細については、Strata Cloud Managerでの監視を参照してください。

Strata Cloud Managerを使用してCloud NGFWリソースを監視する方法:

STEP 1 | stratacloudmanager.paloaltonetworks.comで直接、Palo Alto Networksハブから Strata Cloud Managerアプリにログインします。

STEP 2 | インターフェースで、**[Monitor(モニター)]**:



監視

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）

ネットワークトラフィック全体、およびStrata Cloud Managerで管理している製品やサブスクリプションを包括的に可視化できます。Prisma Access では、リモート ネットワーク、アプリケーション、NGFW デバイス、モバイル ユーザーの健全性と接続状態を保護的に監視できます。Strata Cloud Manager には、共通ネットワーク サービスのパフォーマンス、サブスクリプション ライセンスの消費量の詳細を監視し、接続の問題を分析するために使用されるツールを管理する機能も用意されています。

潜在的な問題を未然に防止し、問題が発生した場合の対応を促進するために、このファイアウォールは有益な情報を含むカスタマイズ可能なレポートを使用し、トラフィックとユーザーパターンに関するインテリジェンスを提供します。ファイアウォールのダッシュボード、アプリケーション コマンド センター（ACC）、レポート、およびログを使用してネットワーク上のアクティビティをモニターできます。ログをモニタリングして情報をフィルタリングし、事前定義されたビューまたはカスタマイズされたビューで構成されるレポートを生成できます。たとえば、事前定義されたテンプレートを使用してユーザーのアクティビティに関するレポートを生成したり、レポートとログを分析して、ネットワーク上での異常な振る舞いの意味を解釈したり、トラフィックのパターンに関するカスタム レポートを生成したりすることができます。視覚的に訴求する方法でネットワーク アクティビティを表示するために、ダッシュボードと ACC にはウィジット、グラフ、および表が含まれており、操作して関心のある情報を見つけることができます。さらに、モニターした情報を電子メール通知、Syslog メッセージ、SNMP トラップ、NetFlow レコードとして外部システムに転送するようにファイアウォールを設定できます。

AWS でネイティブにログを表示する

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）

ログが自動的に生成されます。これはタイムスタンプされたファイルで、ファイアウォールのシステムイベントまたはファイアウォールがモニターするネットワークトラフィックイベントの監査証跡を提残します。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。各ログタイプは個別のイベントタイプの情報を記録します。例えば、ファイアウォールは、スパイウェア、脆弱性、マルウェア シグネチャに一致するトラフィックを記録するための脅威ログまたはポートスキャンやファイアウォールのホストスイープアクティビティに設定されたしきい値に一致するDoS攻撃を生成します。

Cloud NGFW は、トラフィック、脅威、および復号化ログを S3 バケット、CloudWatch Log Group、または Kinesis Data Firehose に送信できます。これらのログ送信先の名前は、Tenet Admin AWS アカウントを Cloud NGFW に追加するときに起動される Cloud NGFW CloudFormation テンプレート(CFT)に含める必要があります。CloudWatch Log Group と Kinesis Data Firehose のデフォルト値は CFT の **PaloAltoCloudNGFW** です。S3 バケットにはデフォルトがありません。Cloud NGFW は、AWS 環境でこれらのリソースを作成しません。CFT は、Cloud NGFW にログを宛先に書き込むためのアクセス許可を与えます。NGFW ログを正常にキャプチャするには、CFT で指定した名前の宛先がデプロイメントに存在する必要があります。

CloudWatch ロググループ、*S3* バケット、*CloudWatch* 名前空間、および *Kinesis* ストリームは、*CloudFormation* テンプレート *(CFT)* で事前に作成する必要があります。

ログ タイプ

Cloud NGFW は、3 種類のログをキャプチャして保存できます。

- トラフィック — トラフィックログは、各セッションの開始と終了のエントリを表示します。詳細については Cloud NGFW for AWS トラフィックログフィールドを参照してください。
- 脅威 — トラフィックがファイアウォールのセキュリティルールに関連付けられているセキュリティプロファイルの 1 つと一致すると、脅威ログはエントリを表示します。各エントリには、日付と時刻の情報が含まれます。脅威の種類（マルウェアやスパイウェアなど）脅威の

説明または URL（名前列）。アラームアクション（許可やブロックなど）。と重大度レベル。

詳細については Cloud NGFW for AWS 脅威ログフィールドを参照してください。

重要度	説明
極めて重大	広範囲にデプロイされたソフトウェアのデフォルト インストールに影響するような深刻な脅威。サーバーの root が悪用され、弱点のあるコードが広範囲の攻撃者の手に渡ることになります。攻撃者は通常、特殊な認証資格証明や個々の被害者に関する知識を必要としません。また、標的がなんらかの特殊な機能を実行するように操作する必要もありません。
高	重大度が Critical に変わる可能性があるものの、軽減要因が存在する脅威。たとえば、悪用するのが困難であったり、上位の特権が与えられることがなかったり、被害サーバー数が多くなかったりする場合です。
中	影響が最小限に抑えられる小さな脅威。たとえば、標的に侵入することのない DoS 攻撃や、攻撃者が被害サーバーと同じ LAN 上に存在する必要があり、標準以外の設定や隠れたアプリケーションにのみ影響するか、アクセスがごく限られている悪用などです。
低	組織のインフラストラクチャへの影響がわずかな警告レベルの脅威。通常、ローカルまたは物理的なシステムへのアクセスが必要であり、被害者のプライバシーや DoS の問題、情報漏洩などが発生することがあります。
情報	直ちに脅威とはならなくても、存在する可能性がある深層の問題に注意を引くために報告される、疑わしいイベント。URL フィルタリング ログ エントリは Informational（通知）としてログに記録されます。何らかの判定をを含むログ エントリおよびブロックするよう設定されたアクションも、Informational（通知）としてログに記録されます。

- **Decryption Logs** - 復号化ログには、デフォルトで失敗した TLS ハンドシェークのエントリが表示され、復号ポリシーで有効にすると、成功した TLS ハンドシェークのエントリを表示できます。成功したハンドシェークのエントリを有効にする場合は、ログ用のシステム リソー

ス (ログ スペース) があることを確認してください。詳細については Cloud NGFW for AWS 復号化ログフィールドを参照してください。

ログ宛先

Cloud NGFW ログの宛先には 3 つの選択肢があります。これらの宛先はすべて、Cloud NGFW サービスの外部にありますが、AWS アカウント（S3 バケット、Cloudwatch ロググループ、または Kinesis データファイアホース）内にあります。各ログファイルは JSON ファイルとして生成されます。

Cloud NGFW for AWS にサブスクライブすると、AWS CloudFormation テンプレートスタックを設定するように求められます。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 フィールドは事前に入力されていません。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。

各 NGFW リソース（ログストリーム名に NGFW 名として表示される）は、そのログを複数のストリームに出力します（ログ・ストリーム名のランダムな文字ストリングによって区別されます）。したがって、特定の Cloud NGFW リソースのログが複数のストリームに分散している可能性があります。

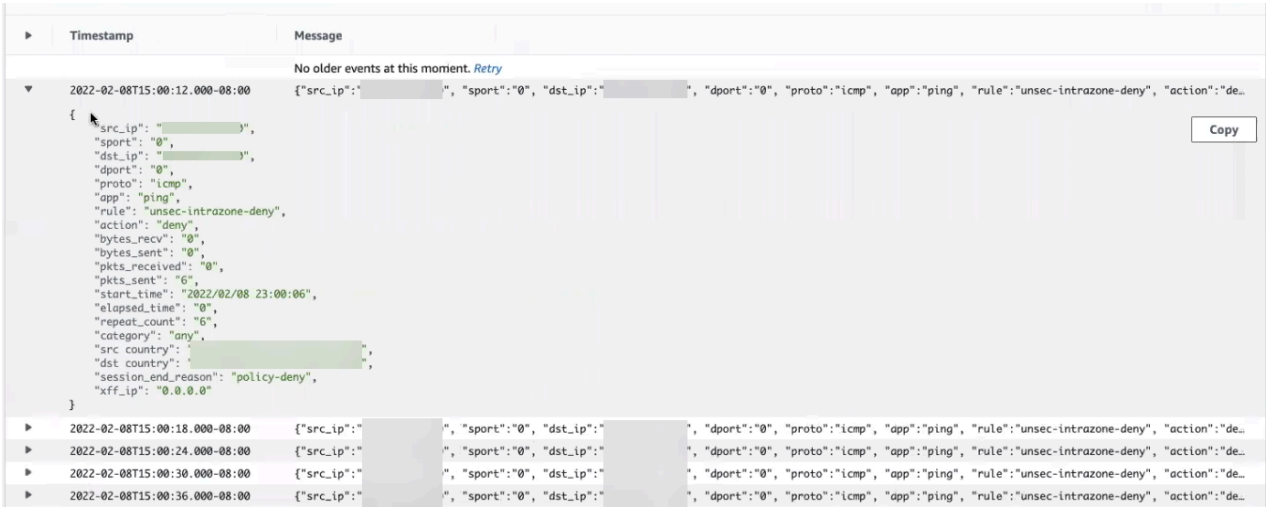
ログを CloudWatch ロググループに送信すると、AWS CloudWatch コンソールでログエントリを直接表示できます。ロギングの設定時に指定する CloudWatch ロググループに、ログストリームのリストが表示されます。ログ ストリーム名は次のように表示されます。

`/<aws-account-id>/<region>/<NGFW-name>/<random-string>/<log-type>。<year>。<month>。<day>。<hour>`

たとえば、/account123/us-west-1/firewall-1/qadd232312345dea/TRAFFIC.2022.02.10.Twenty-three

の <*random string*> ログを生成した個々の *NGFW* リソースを参照します。

ストリーム名をクリックすると、次の例に示すようにログ エントリが表示されます。



ログを S3 バケットに送信すると、ログ ファイルは JSON ファイルとして保存されます。NGFW は、ファイアウォールが 256 MB のログを生成したか、最後のログファイルが生成されてから 10 分が経過したという条件のいずれかが満たされると、新しいログファイルを送信します。指定した S3 バケット内のファイルを見つけるには、AWS の S3 コンソールにアクセスし、指定したバケットを見つけます。次に、***AWS*** アカウント ***ID***、 > リージョン、 > ***NGFW*** 名、 > ログ タイプ、 > 年、 > 月 > 、日 > 、時間を選択します。S3 バケットのログファイル名は次の形式に従います。

```
<aws-account-id>-<region>-<NGFW-name>-<log-type>-<year>-<month>-<day>-<hour>-<random-string>
```

の *<random string>* ログを生成した個々の *NGFW* リソースを参照します。

その後、ファイルをダウンロードし、JSON リーダーを使用して、より読みやすい形式でログを表示できます。ログ情報に加えて、各ログ エントリには、日付、優先度、時刻、ファイアウォールのホスト名、ログの種類、年、月、日、時、分、秒を記録するヘッダーも含まれています。

ログファイルを Kinesis ファイアホースに送信すると、ログは指定したストリーム名に送信され、次に最終宛先に送信されます。S3 バケット、Datadog、Splunk などです。Kinesis ファイアホースのソースは、**Direct PUT**またはその他のソースである必要があります。ログ情報に加えて、各ログエントリには、日付、優先度、時刻、ファイアウォールホスト名、ログタイプ、年、月、日、時、分、秒、リージョン、ファイアウォール名、AWS アカウント ID を記録するヘッダーも含まれています。NGFW は、リージョン、ファイアウォール名、AWS アカウント ID をログに追加して、ログファイル名にこの情報が含まれていないため、ログが生成された場所を識別できるようにします。その後、表示用に JSON ファイルをダウンロードできます。

ログエントリとログファイル名に記録された時刻と日付は、*UTC* 時間で表示されます。ただし、*AWS* コンソールに表示されるログ日付は、ローカル時刻と日付で表示されます。

STEP 1 | Cloud NGFW コンソールから、［**NGFW**］を選択し、 ロギングを設定するファイアウォールを選択します。

STEP 2 | **[**ログ設定**]**を選択します。

STEP 3 | **[**ログの種類**]**で 、キャプチャする 1 つ以上のオプションログの種類を選択します。

すべてのログを同じ宛先に送信するか、ログ・タイプごとに異なる宛先を選択するかを選択できます。

STEP 4 | ログ宛先を選択します。複数のログタイプを選択する場合は、ログタイプごとに宛先を個別に選択する必要があります。

STEP 5 | ログ宛先名を入力します。ログ宛先名は、

STEP 6 | **[Save(**保存**)]**をクリックします。

Cloud NGFW for AWS トラフィックログフィールド

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）

以下の表では、Cloud NGFW for AWSトラフィック ログ フィールドについて説明します。

フィールド名	詳説
生成時間 (time_generated または cef-formatted-time_generated)	データプレーンでログが生成された日時。
送信元アドレス（src）	元のセッション送信元 IP アドレス。
送信元ポート（sport）	セッションで使用された送信元ポート。
セッション ID (sessionid)	各セッションには内部の数値識別子が適用されます。
宛先アドレス (dst_ip)	元のセッション宛先 IP アドレス。
宛先ポート（dport）	セッションで使用された宛先ポート。
IP プロトコル（proto）	セッションに関連付けられた IP プロトコル。
アプリケーション (app)	セッションに関連付けられたアプリケーション。
ルール名（rule）	セッションで一致したルールの名前。
アクション（action）	セッションで実行されたアクション。値は以下のいずれかです。 • allow —セッションはポリシーによって許可されました • deny — セッションはポリシーによって拒否されました • reset both — セッションは終了し、TCP リセットが接続の両端に送信されました

フィールド名	詳説
	• reset client — セッションは終了し、TCP リセットがクライアントに送信されました • reset server — セッションは終了し、TCP リセットがサーバーに送信されました
受信バイト数 (bytes_recv)	セッションのサーバーからクライアント方向へのバイト数。
送信済バイト (bytes_sent)	セッションのクライアントからサーバー方向へのバイト数。
受信したパケット（pkts_received）	セッションのサーバーからクライアントへのパケット数。
送信されたパケット（pkts_sent）	セッションのクライアントからサーバーへのパケット数。
開始時間 (start_time)	セッションの開始時刻とディスク使用量。
経過時間 (elapsed_time)	セッションの経過時間。
リピート回数 (repeat_count)	5秒以内に開始された、送信元 IP、宛先 IP、アプリケーション、サブタイプが同じになっているセッションの数。
カテゴリ（category）	セッションに関連付けられた URL カテゴリ (該当する場合)。
ソース国 (src country)	プライベート アドレスの送信元の国または内部領域。最大長は 32 バイトです。
宛先国 （dst country）	プライベート アドレスの宛先の国または国内地域。最大長は 32 バイトです。
セッション終了理由（session_end_reason）	セッションが終了したためです。複数の原因で終了した場合、このフィールドには優先度が最も高い理由のみが表示されます。有効なセッション終了理由の値は、優先度の高い順に以下のとおりです。 • threat — ファイアウォールが、リセット、ドロップ、またはブロック（IP アドレス）アクションに関連付けられた脅威を検出しました。

フィールド名	詳説
	• policy-deny — セッションが、拒否またはドロップ アクションが指定されたセキュリティ ルールと一致しました。 • decrypt-cert-validation — 失効、信用されていない発行者、未知の状態、状態検証タイムアウトなどの状況によりセッションがクライアント認証を実施またはセッションがサーバー証明書を実施する時に、ブロックするようにファイアウォールを設定したのでセッションが終了しました。サーバー証明書が type bad_certificate、unsupported_certificate、certificate_revoked、access_den または no_certificate_RESERVED (SSLv3 のみ)の致命的エラー アラートを生成する時にもこのセッションの終了理由が表示されます。 • decrypt-unsupport-param—セッションがサポートしていないプロトコルバージョン、暗号鍵またはSSHアルゴリズムを使用している場合、SSL送信プロキシ複合またはSSLインバウンドインスペクションをブロックするようにファイアウォールを設定したのでセッションは終了しました。unsupported_extension、unexpected_message、または handshake_failureのタイプの致命的エラーアラートをセッションが発生すると、このセッション終了理由が表示されます。 • decrypt-error：ファイアウォール リソースが利用できないときに、SSL フォワード プロキシ復号化または SSL 受信検査をブロックするようにファイアウォールを設定したため、セッションが終了しました。このセッション終了理由は、SSL エラーが発生した SSL トラフィックをブロックするようにファイアウォールを設定した場合、または復号化証明書検証および非サポート の終了理由にリストされている以外の致命的なエラー アラートを生成した場合にも表示されます。 • tcp-rst-from-client — クライアントが TCP リセットをサーバーに送信しました。 • tcp-rst-from-server — サーバーが TCP リセットをクライアントに送信しました。 • resources-unavailable — システム リソース制限が原因でセッションがドロップしました。たとえば、セッションの順序外パケット数が、フローまたはグローバル順

フィールド名	詳説
	序外パケット キューごとに許容される数を超えた場合などが考えられます。 • tcp-fin — 接続中の両ホストが TCP FIN メッセージを送信してセッションを閉じました。 • tcp-reuse — セッションが再利用され、ファイアウォールが前のセッションを閉じました。 • decoder — デコーダがプロトコル内で新しい接続を検出し（HTTP-Proxy など）、前の接続を終了しました。 • aged-out — セッションがエージアウトしました。 • n/a — この値は、トラフィック ログのタイプが **end** 以外の場合に適用されます。
XFF アドレス (xff_ip)	Webページをリクエストしたユーザーの IPアドレス、またはリクエストが通過した最後から2番目のデバイスのIPアドレス。リクエストが1つ以上のプロキシ、ロード バランサー、またはその他のアップストリーム デバイスを通過する場合、ファイアウォールは最も新しいデバイスの IP アドレスを表示します。

Cloud NGFW for AWS 脅威ログフィールド

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）

フィールド名	詳説
生成時間 (time_generated または cef-formatted-time_generated)	データプレーンでログが生成された日時。

フィールド名	詳説
送信元アドレス（src_ip）	元のセッション送信元 IP アドレス。
送信元ポート（sport）	セッションで使用された送信元ポート。
セッション ID (sessionid)	各セッションには内部の数値識別子が適用されます。
宛先アドレス (dst_ip)	元のセッション宛先 IP アドレス。
宛先ポート（dport）	セッションで使用された宛先ポート。
IP プロトコル（proto）	セッションに関連付けられた IP プロトコル。
アプリケーション (app)	セッションに関連付けられたアプリケーション。
ルール名（rule）	セッションで一致したルールの名前。
アクション（action）	セッションに対して実行されたアクション。値は、「alert」、「allow」、「deny」、「drop」、「drop-all-packets」、「reset-client」、「reset-server」、「reset-both」、「block-url」です。 • alert — 脅威または URL が検出されましたが、ブロックされていません • allow— フラッド検出アラート • deny — フラッド検出メカニズムがアクティブにされ、設定に基づいてトラフィックを拒否します • drop— 脅威が検出され、関連付けられたセッションが廃棄されました • reset-client — 脅威が検出され、TCP RST がクライアントに送信されました • reset-server — 脅威が検出され、TCP RST がサーバーに送信されました • reset-both — 脅威が検出され、TCP RST がクライアントとサーバーの両方に送信されました • block-url — ブロックするように設定された URL カテゴリで照合が行われたため、URL 要求がブロックされました • block-ip—脅威が検出され、クライアント IP がブロックされます • random-drop—フラッドが検出され、パケットがランダムにドロップされました

フィールド名	詳説
	• sinkhole—DNS シンクホール起動 • syncookie-sent—syncookie アラート • block-continue（URL サブタイプのみ）—HTTP リクエストがブロックされ、続行確認のためのボタンが付いた Continue（続行）ページにリダイレクトされます • continue（URL サブタイプのみ）—継続要求が続行されたことを示す、block-continue URL 続行ページへの応答ブロック • block-override（URL サブタイプのみ）—HTTP リクエストがブロックされ、ファイアウォール管理者からのパスコードが必要な管理オーバーライド ページにリダイレクトされます • override-lockout（URLサブタイプのみ）—送信元 IP からの管理上のオーバーライドパスコードの試行に失敗しました。IP が block-override リダイレクト ページからブロックされるようになりました • override（URLサブタイプのみ）—正しいパスコードが提供され、リクエストが許可されている block-override ページへの応答 • block（WildFire® のみ）—ファイルはファイアウォールでブロックされ、WildFire® にアップロードされました
脅威カテゴリ（threat_category）	異なる種類の脅威シグネチャを分類化するのに使用する脅威カテゴリを示します。
脅威/コンテンツの種類（threat_content_type）	脅威ログのサブタイプ値は以下を含みます。 • data — データ フィルタリング プロファイルと一致するデータ パターン • file—ファイルブロッキングプロファイルと一致するファイルタイプ • flood — ゾーン プロテクション プロファイルによって検出されたフラッド • packet—ゾーンプロテクションプロファイルでトリガーされたパケットベース攻撃防御 • scan — ゾーン プロテクション プロファイルによって検出されたスキャン • Spyware —アンチスパイウェアプロファイルで検出したスパイウェア

フィールド名	詳説
	• url — URL フィルタリング ログ • ml-マルウェア —ウイルス対策プロファイルを介して WildFire インライン ML によって検出されたマルウェア。 • マルウェア—アンチウイルスプロファイルを介して検出されたマルウェア。 • Vulnerability —脆弱性防御プロファイルで検出した脆弱性バグ • 山火事 — ファイアウォールが WildFire 分析プロファイルごとにファイルを WildFire に送信し、その結果に基づいて判定 (マルウェア、フィッシング、グレーウェア、無害な情報) を WildFire の送信ログに記録すると、WildFire の判定が生成されます。 • wildFire®マルウェア—アンチウイルスプロファイルを介して検出されたマルウェア。
脅威/コンテンツ名（threat_content_name）	既知およびカスタム脅威に対する Palo Alto Networksの識別子。一部のサブタイプでは、説明の文字列にかっこで囲んだ 64 ビットの数値識別子が続きます。 • 8000 ～ 8099 — スキャン検出 • 8500 ～ 8599 — フラッド検出 • 9999— URL フィルタリング ログ • 10000 ～ 19999 — スパイウェア フォンホーム検出 • 20000 ～ 29999 — スパイウェア ダウンロード検出 • 30000 ～ 44999 — 脆弱性悪用検出 • 52000 ～ 52999 — ファイルタイプ検出 • 60000 ～ 69999 — データ フィルタリング検出 以前のリリースで使用されていたマルウェア検出、*WildFire* シグネチャ フィード、および *DNS C2* シグネチャの 脅威 *ID* 範囲は、永続的かつ グローバルな一意の ID に置き換えられています。脅威/コンテンツ タイプ *(subtype)* および脅威カテゴリ *(thr_category)* フィールド名を参照し、更新されたレポート、フィルタ、脅威ログ、*ACC* アクティビティを作成します。

フィールド名	詳説
重大度 (severity)	脅威に関連付けられた重大度。値は、「informational」、「low」、「medium」、「high」、「critical」です。
方向 (direction)	攻撃の方向（「クライアントからサーバーへ」、または「サーバーからクライアントへ」）を示します。 • 0 — 脅威の方向はクライアントからサーバーへ • 1 — 脅威の方向はサーバーからクライアントへ
リピートカウント（repeatcnt）	5 秒以内に開始された、送信元 IP、宛先 IP、アプリケーション、コンテンツ/脅威タイプが同じになっているセッションの数。
理由（data_filter_reason）	データ フィルタリング アクションの理由。
XFF アドレス (xff_ip)	WebページをリクエストしたユーザーのIPアドレス、またはリクエストが通過した最後から2番目のデバイスのIPアドレス。リクエストが1つ以上のプロキシ、ロード バランサー、またはその他のアップストリーム デバイスを通過する場合、ファイアウォールは最も新しいデバイスの IP アドレスを表示します。
コンテンツ バージョン（contentver）	ログが生成される際の、ファイアウォール上のアプリケーションおよび脅威のバージョンです。

Cloud NGFW for AWS 復号化ログフィールド

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）

次の表には、復号化ログ フィールドに関する情報が含まれています。

フィールド名	詳説
生成時間 (time_generated または cef-formatted-time_generated)	データプレーンでログが生成された日時。
送信元 IP アドレス（src_ip）	元のセッション送信元 IP アドレス。
送信元ポート（sport）	セッションで使用された送信元ポート。
セッション ID (sessionid)	各セッションには内部の数値識別子が適用されます。
宛先アドレス (dst_ip)	元のセッション宛先 IP アドレス。
宛先ポート（dport）	セッションで使用された宛先ポート。
IP プロトコル（proto）	セッションに関連付けられた IP プロトコル。
アプリケーション (app)	セッションに関連付けられたアプリケーション。
ルール(rule)	セッション トラフィックを制御するセキュリティ ポリシー ルール。
アクション（action）	セッションで実行されたアクション。値は以下のいずれかです。 • allow —セッションはポリシーによって許可されました • deny — セッションはポリシーによって拒否されました • reset both — セッションは終了し、TCP リセットが接続の両端に送信されました • reset client — セッションは終了し、TCP リセットがクライアントに送信されました • reset server — セッションは終了し、TCP リセットがサーバーに送信されました
TLS バージョン (tls_version)	セッションに使用される TLS プロトコルのバージョン。
鍵交換アルゴリズム(key_exchange_algorithm)	セッションに使用される鍵交換アルゴリズム。

フィールド名	詳説
暗号アルゴリズム (tls_enc)	AES-128-CBC、AES-256-GCM、等のセッション データの暗号化に使用されるアルゴリズム。
ハッシュアルゴリズム(hash_algorithm)	SHA, SHA256、SHA384 等のセッションに使用される認証アルゴリズム。
楕円曲線 (elliptic_curve)	クライアントとサーバーがネゴシエートし、ECDHE 暗号スイートを使用する接続に使用する楕円暗号曲線。
サーバー名の表示（server_name_indication）	サーバー名の表示。
サーバー名表示の長さ（server_name_indication_length）	サーバー名表示の長さ (hostname)。
プロキシタイプ (proxy_type)	転送プロキシの転送、インバウンド検査の着信、復号化されていないトラフィックの復号化なし、GlobalProtect などの復号化プロキシの種類。 ***None***ではなく ***No Decrypt*** を選択すると、トラフィックがドロップされます。
チェーン ステータス (chain_status)	チェーンが信頼されているかどうか。値を以下に示します。 • 未検査 • 信頼されていない • 信頼されている • 不完全

Panorama でトラフィックと脅威のログとアクティビティを表示する

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）

Cloud NGFW ログをパノラマで表示する

Cloud NGFWリソースがPanoramaおよびStrata Logging Serviceと統合されている場合、ログとアクティビティはPanoramaの [Monitoring and Application Command Center(ACC)(モニタリング・アプリケーション コマンド センター(ACC))]タブにキャプチャされて表示されます。PanoramaはCloud NGFWによって生成されたログを収集し、モニター タブに表示します。トラフィック、脅威、URLフィルタリング、および復号化ログから選択し、IDまたは名前でフィルタリングできます。ログフィールドの説明については、Cloud NGFWロギングのドキュメントをご覧ください。

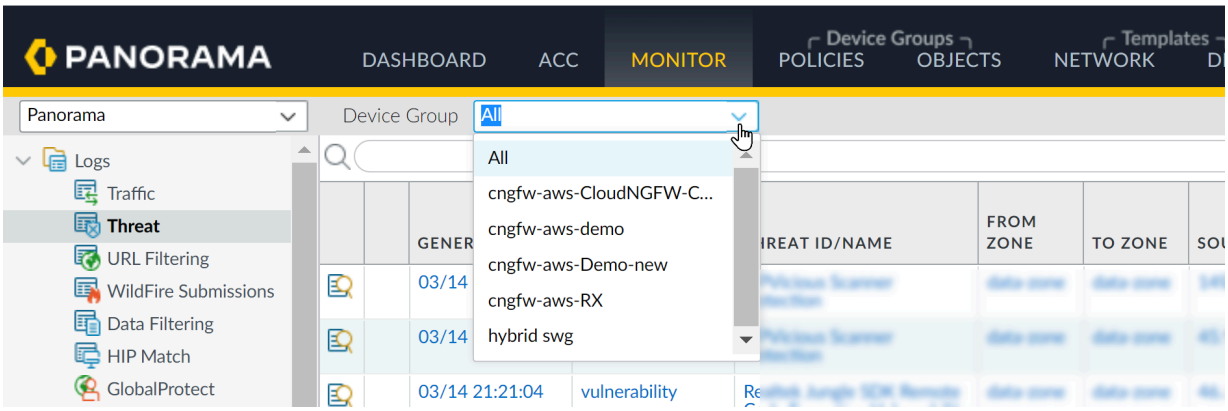
STEP 1 | Panorama にログインします。

STEP 2 | **Monitor(**監視**)**を選択します。

STEP 3 | **[Device Group(**デバイス グループ**)]** ドロップダウンで、**[Cloud Device Group(**クラウド デバイス グループ**)** をクリックしてアクティビティを表示します。

STEP 4 | Panoramaフィルターを使用して、個々のクラウド デバイス グループのログを表示します。デバイス名を見つけます。Panoramaインターフェースの右上の+アイコンをクリックして、新しいフィルターを追加します。フィルターの名前を入力し、**[Save(**保存**)]**をクリックします。**[Load Filter(**フィルタをロードする**)]**アイコンをクリックします。新しく作成したフィルターを選択して、個々のクラウド デバイス グループのログを表示します。

STEP 5 | Panoramaコンソールの左側の**[Logs(ログ)]**メニューから、表示する特定のログの種類を選択できます。



ACCでCloud NGFWアクティビティを表示する

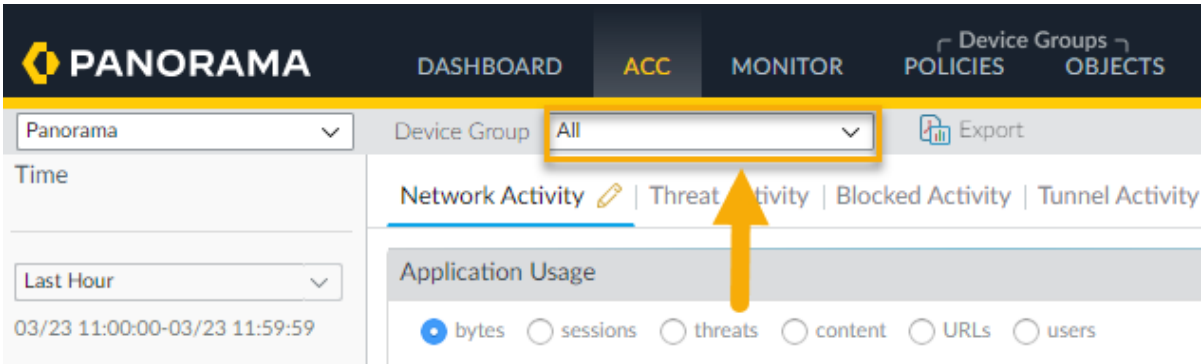
ACCは、ネットワーク内のアクティビティに関する実用的なインテリジェンスを提供する分析ツールです。ACCは、Cloud NGFWログを使用してネットワーク上のトラフィック トレンドをグラフィカルに表現します。このグラフィカル表現を使用して、データにアクセスし、ネットワークの使用パターン、トラフィック パターン、疑わしいアクティビティ、異常を含め、ネットワーク上のイベント間の関係を視覚化できます。

Panoramaでは、クラウド デバイス グループに基づいてACCコンテンツをフィルタリングできます。Cloud NGFWリソースのアクティビティに関する特定の情報をフィルタリングして表示する方法については、PAN-OSのACC ドキュメントを参照してください。

STEP 1 | Panorama にログインします。

STEP 2 | **ACC** を選択します。

STEP 3 | **[Device Group(デバイス グループ)]**ドロップダウンで、**[Cloud Device Group(クラウド デバイス グループ)]**をクリックしてアクティビティを表示します。



STEP 4 | Panoramaフィルターを使用して、個々のクラウド デバイス グループのログを表示します。デバイス名を見つけます。Panoramaインターフェースの右上の+アイコンをクリックして、新しいフィルターを追加します。フィルターの名前を入力し、**[Save(保存)]**をクリックします。**[Load Filter(フィルタをロードする)]**アイコンをクリックします。新しく作成したフィルターを選択して、個々のクラウド デバイス グループのログを表示します。

Strata Logging Service でトラフィックと脅威のログを表示する

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）

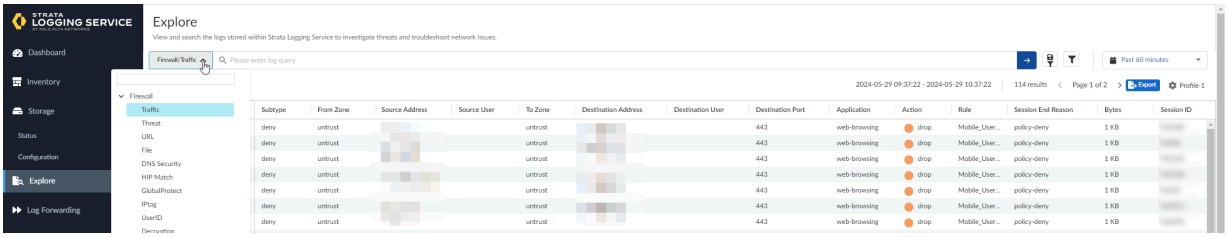
Cloud NGFWをPanoramaおよびStrata Logging Serviceと統合すると、Cloud NGFW リソースによって作成されたログを転送し、Strata Logging Serviceで表示できるようになります。Strata Logging Service Webインターフェースでは、Cloud NGFWリソースによって生成されたトラフィック、脅威、復号化のログを表示できます。Panoramaを使用していて、ログ収集にStrata Logging Serviceを使用していない場合、ログを別のエンティティに転送することができます。ただし、ログ プロファイルでStrata Logging Serviceを有効にする必要があります。

ログ フィールドの詳細については、「Strata Logging Service Schema Reference:Traffic, Threat, and Decryption」を参照してください。

STEP 1 | Strata Logging Serviceインスタンスにログインします。

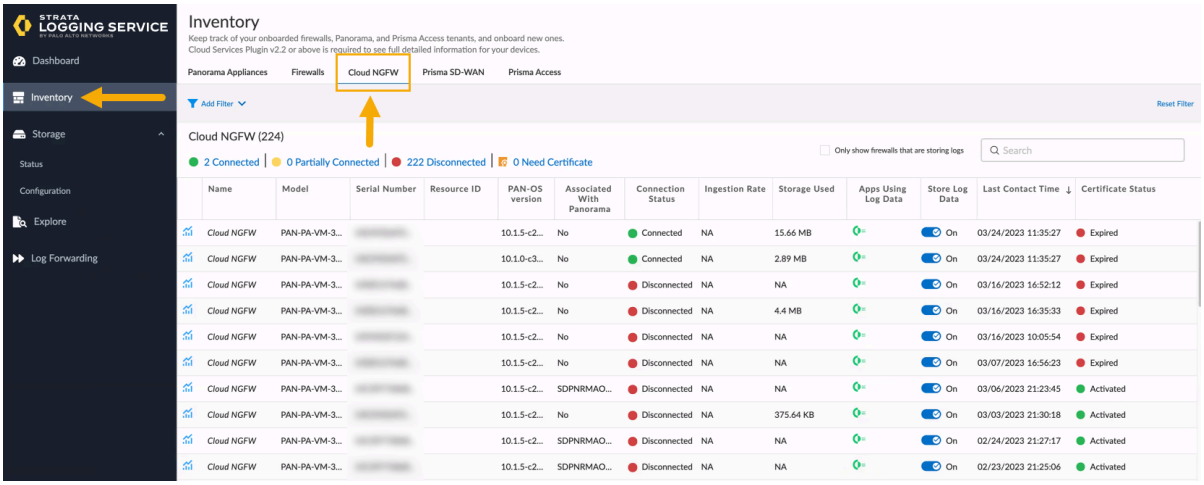
STEP 2 | **[Explore(探索)]**を選択します。

STEP 3 | クエリのドロップダウンから、ログの種類を選択できます。各ページに100件のログが表示されます。ただし、Strata Logging Serviceクエリを使用して、表示される情報を絞り込むことができます。



STEP 4 | **[Inventory(インベントリ)]**を選択すると、オンボーディング済みのファイアウォールに関する情報が表示されます。

STEP 5 | **[Inventory(インベントリ)]**ページで、**[Cloud NGFW]**を選択します。



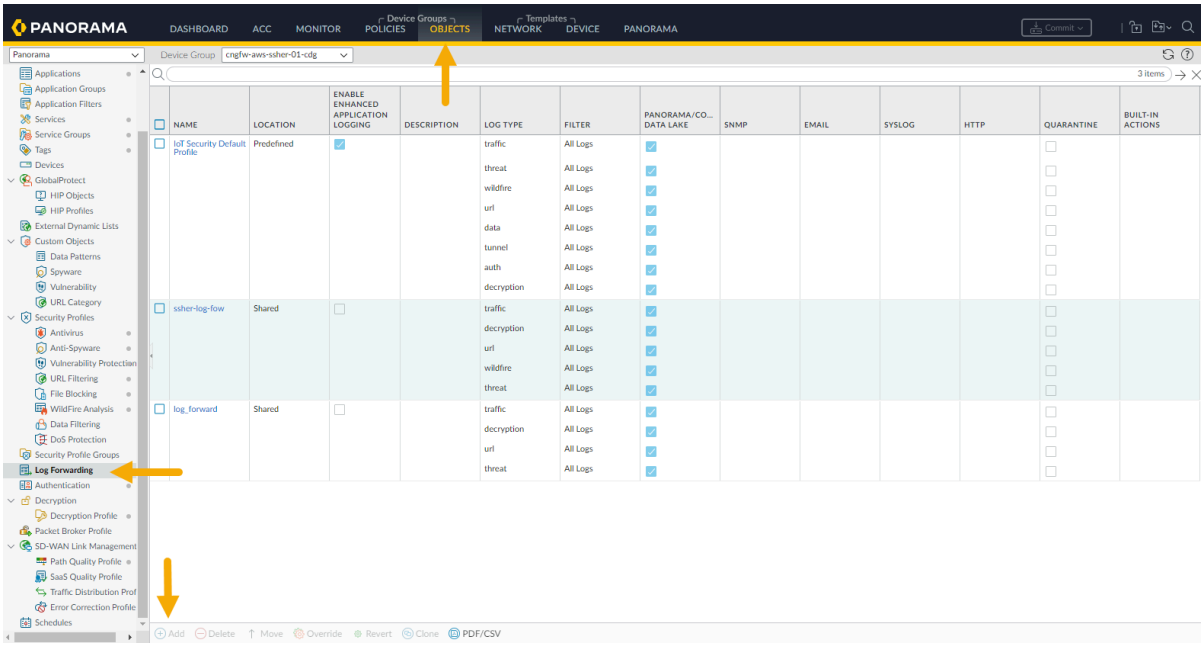
Strata Logging Serviceへのログの転送

Strata Logging Serviceにログを転送する方法:

STEP 1 | Panoramaコンソールで、**[Device Groups(デバイス グループ)]**の**[Objects(オブジェクト):]**を選択します。

STEP 2 | **[Log Forwarding(ログ転送)]**を選択します。

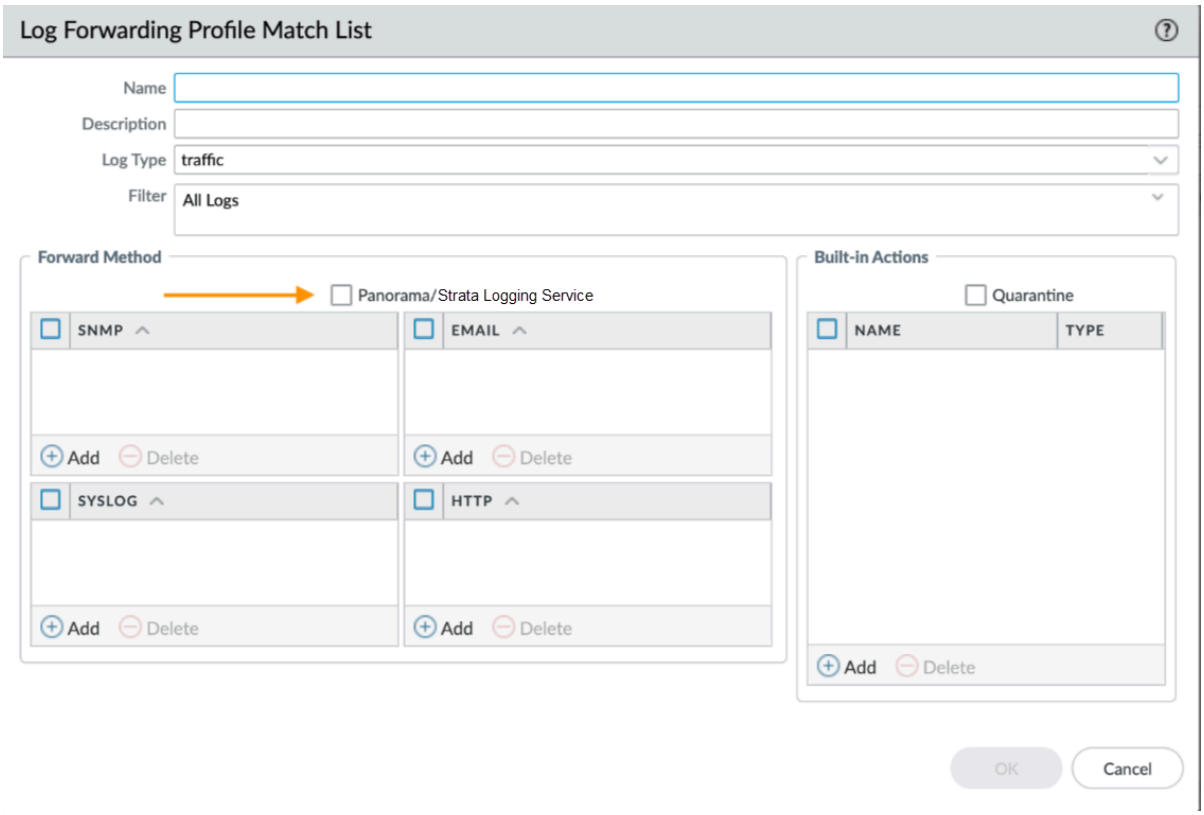
STEP 3 | **[Add(追加)]** をクリックして、新しいログ転送一致リスト プロファイルを作成します。



STEP 4 | **[Log Forwarding Profile Match List(ログ転送プロファイル一致リスト)]**画面で、ログの名前を指定します。

STEP 5 | ドロップダウンから**[Log Type(ログタイプ)]**を選択します。

STEP 6 | **[Forward Method(（転送方法）)]**として、**[Panorama/Strata Logging Service]**を選択します。



STEP 7 | **OK** をクリックします。

STEP 8 | 変更をコミットしてプッシュします。

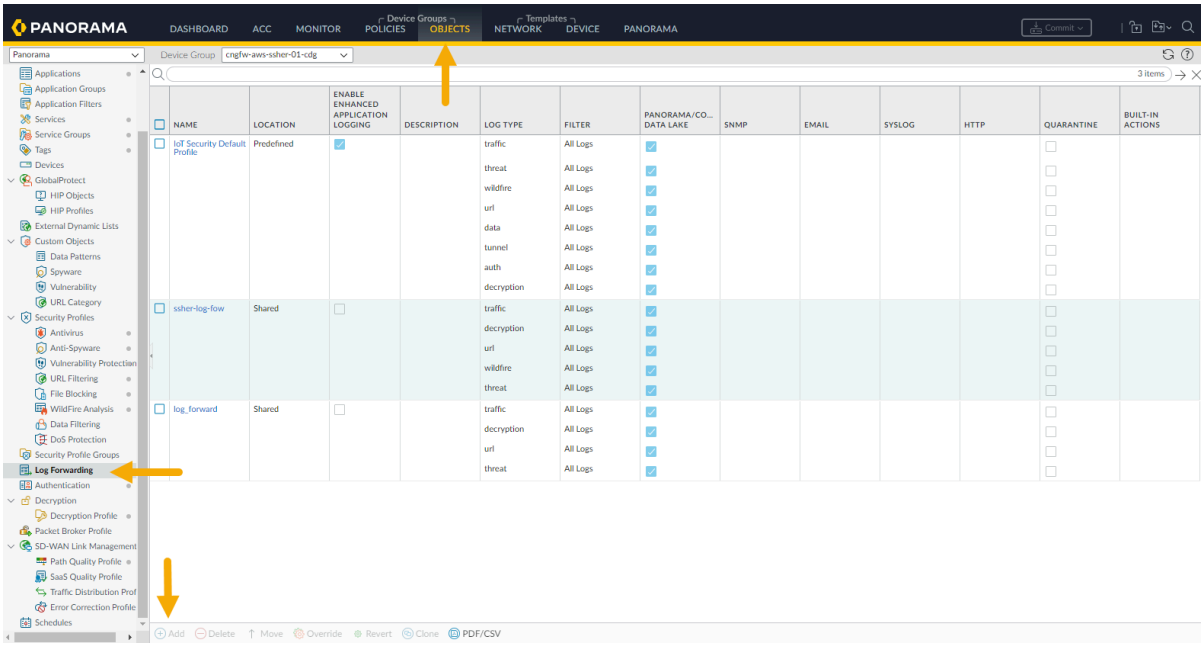
Strata Logging Serviceを使用せずにログを転送する

Panoramaを使用していて、ログ収集にStrata Logging Serviceを使用していない場合は、AWS Cloudwatch、Amazon S3、Amazon Kinesisなどの別のエンティティにログを転送できます

STEP 1 | Panoramaコンソールで、**[Device Groups(デバイス グループ)]**の**[Objects(オブジェクト):**を選択します。

STEP 2 | **[Log Forwarding(ログ転送)]**を選択します。

STEP 3 | **[Add(追加)]**をクリックして、新しいログ転送一致リスト プロファイルを作成します。



STEP 4 | **[Log Forwarding Profile Match List(**ログ転送プロファイル一致リスト**)]**画面で、ログの名前を指定します。

STEP 5 | ドロップダウンから**[Log Type(**ログタイプ**)]**を選択します。

PanoramaがStrata Logging Serviceにリンクされていない場合、ログはPanoramaコンソールに転送されず、Cloud watch、S3、Kinesisなどの別のアプリケーションで表示できます。Cloud NGFWコンソールを使用して、これらの他のロギング方法を設定します。

ログを直接送信するつもりがなくても、ロギングプロファイルで*Strata Logging Service*を有効にします。

STEP 6 | **OK** をクリックします。

STEP 7 | 変更をコミットしてプッシュします。

AWS のクラウド NGFW で監査ログを表示する

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）

Cloud NGFW for AWS で管理者のアクティビティを追跡して、デプロイメント全体のアクティビティのリアルタイムレポートを実現します。管理者アカウントが侵害されたと信じるに足る理由がある場合、監査ログは、管理者が Cloud NGFW テナント全体をナビゲートした場所と、管理者が行った構成変更の完全な履歴を提供するため、詳細に分析し、実行されたすべてのアクションに対応できます。侵害されたアカウントになります。

Cloud NGFW for AWS をすでにデプロイしている場合は、CFT を更新する必要がある場合があります。現在の CFT に [監査ログ] フィールドが含まれていない場合。

ロググループは、*Cloud NGFW CFT* がデプロイされたのと同じリージョンの *AWS* コンソールで作成する必要があります。

イベントが発生すると、監査ログが生成され、指定した CloudWatch ロググループに転送されます。

STEP 1 | 必要に応じて、CFT を更新して、監査ログ CloudWatch ロググループへの書き込みに必要なアクセス許可を追加します。

1. Cloud NGFW コンソールにログインします。
2. ［**AWS Accounts** > **Download CFT**］ を選択して、CFT を yaml ファイルとしてダウンロードします。
3. CFT を AWS コンソールにアップロード、編集、適用します。
   1. AWS コンソールにログインし、［**CloudFormation**］ > ［スタック］を選択します。
   2. Cloud NGFW スタック - **PaloAltoNetworksCrossAccountRoleSetup** を見つけます。
   3. ［更新]を選択します。
   4. 現在のテンプレートを置き換えとテンプレートファイルをアップロードを選択します。
   5. CFT yaml ファイルを選択し、［次へ］をクリックします。
   6. CFT スタックの設定を確認し、［次へ］をクリックします。
   7. CFT スタックオプションを確認し、［次へ］をクリックします。
   8. CFT スタックを確認し、［更新］をクリックします。

STEP 2 | Cloud NGFW テナントコンソールにログインします。

STEP 3 | ［テナント］を選択します。

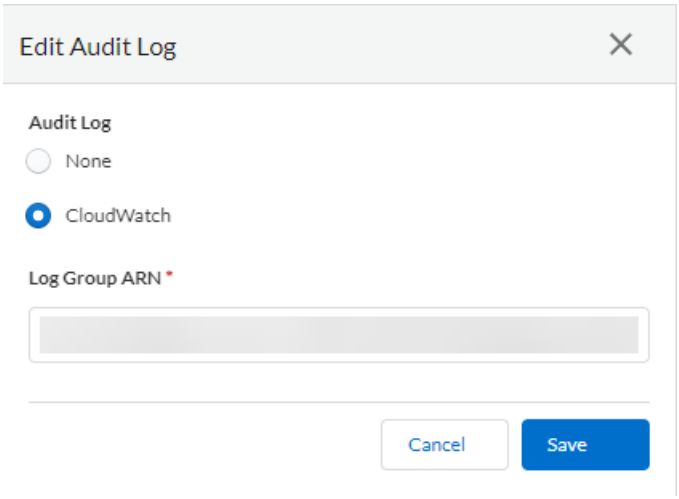
STEP 4 | 監査ログ設定編集アイコンをクリックします  。

STEP 5 | CloudWatch ラジオボタンを選択します。

STEP 6 | ターゲット CloudWatch ログ グループの Amazon リソース名（ARN）を入力します。

ここで入力する ARN が、CFT スタックで指定した CloudWatch ログ グループに対応していることを確認してください。

STEP 7 | **[Save(保存)]**をクリックします。



AWS CloudWatch でのカスタムメトリクスのパブリッシュと表示

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 for AWSは、Cloud NGFWの健全性、パフォーマンス、使用パターンを監視するのに役立つカスタム メトリックをAWS CloudWatch に公開します。これらの追加メトリックを使用すると、クラウドNGFWリソースの全体的な健全性を評価し、パフォーマンスのボトルネックを特定し、異常を検出できます。これらのメトリックは、特定の時点でのCloud NGFWの側面を表す数値です。メトリックは5分ごとに収集され、頻繁にサンプリングされるため、アラートに役立ちます。

CloudWatch ロググループ、*S3* バケット、*CloudWatch* 名前空間、および *Kinesis* ストリームは、*CloudFormation* テンプレート *(CFT)* で事前に作成する必要があります。

メトリックは *5* 分ごとに収集されます。すべてのメトリックは*1*つの名前空間に公開されます。*CloudWatch*はメトリックを保存するため、履歴情報にアクセスして、*Cloud NGFW*リソースのパフォーマンスに関する追加の視点を得ることができます。また、特定のしきい値を監視するアラームを設定し、そのしきい値に達したときに通知を送信したり、アクションを実行したりすることもできます。詳細については、Amazon CloudWatchのドキュメントを参照してください。

Cloud NGFWリソースでは、以下のCloudWatchメトリックがサポートされています。

フィールド名	詳説
データプレーン CPU 使用率（%）	Cloud NGFWリソースのデータプレーンCPU使用率を監視してトラフィック ロードを測定します。
データプレーン パケット バッファ使用率（%）	データプレーン バッファの使用状況を監視し、バッファ使用率を測定します。トラフィックが突発的に増加することがある場合は、バッファ利用率を監視することによ

フィールド名	詳説
	り、ファイアウォールがデータプレーン バッファを使い果たした結果パケットが破棄されてしまうことを防止できます。
1秒あたりの接続数	同時TCP接続の合計数を表します。
セッション スループットKbps	セッション スループットは Kbps 単位で測定されます。
セッションスループット Pps	セッション スループットは Kbps 単位で測定されます。
アクティブなセッション	Cloud NGFWリソース上でアクティブなセッションの合計数を監視します。アクティブなセッションとは、ポリシーで必要とされる場合に、パケットが検査および転送されるフロー ルックアップ テーブルにあるセッションのことです。
セッション使用率（%）	現在アクティブなTCP、UDP、ICMP、および SSL のセッション、ならびにパケット レート、新しい接続確立レート、およびファイアウォール スループットを監視して、セッション使用率を判断します。
BytesIn	セッションのサーバーからクライアント方向へのバイト数。
BytesOut	セッションのクライアントからサーバー方向へのバイト数。
PktsIn	セッションのサーバーからクライアントへのパケット数。
PktsOut	セッションのクライアントからサーバーへのパケット数。

CloudWatchメトリックを公開する方法:

STEP 1 | Cloud NGFW リソースにログインします。

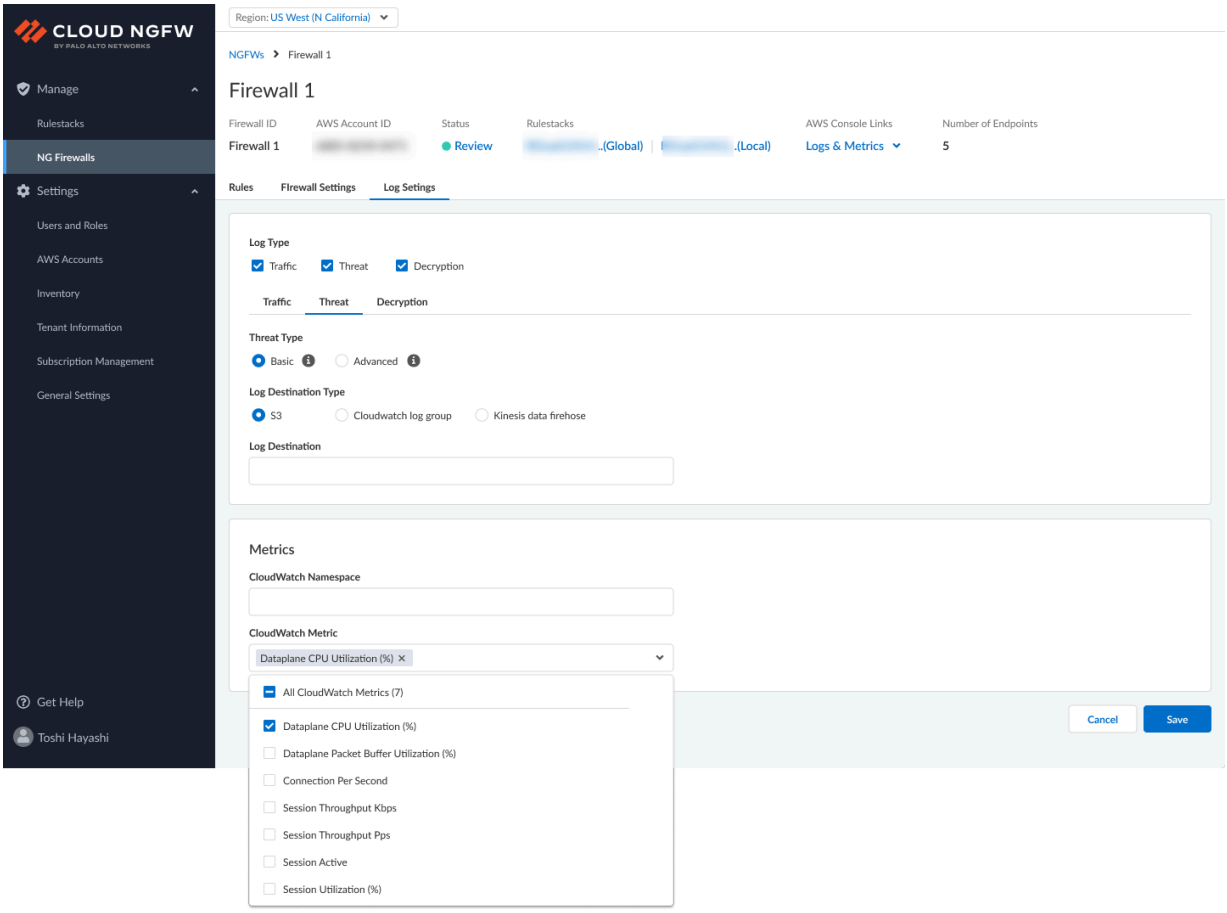
STEP 2 | **[NG Firewalls(NG**ファイアウォール**)]**を選択します。

STEP 3 | **[**ログ設定**]**を選択します。

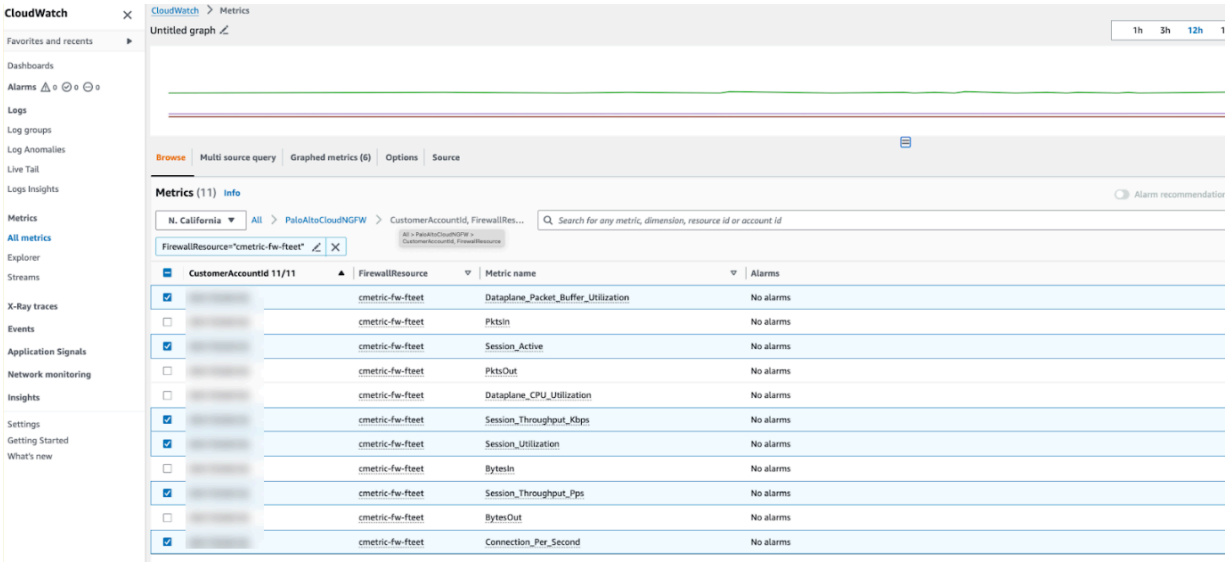
STEP 4 | **[Metrics(メトリック)]**で、以下を指定します。

1. **CloudWatch**名前空間。このフィールドは、メトリックが収集されるAWS上の場所を表します。
2. **CloudWatch** メトリック。監視するメトリックを選択します。サポートされているメトリックについては、上記の表を参照してください。

STEP 5 | **[Save(保存)]をクリックします。**



アカウントに表示されるメトリックのサンプル出力は次のようになります。



Firewall-as-Code (ファイアウォール・アズ・コード)

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 の Cloud NGFW は、コードとしてのファイアウォールをサポートします。これには、構成ファイルを使用してインフラストラクチャ リソースを定義、管理、バージョン管理できるオープンソース ツールである Terraform のサポートが含まれます。インフラストラクチャ アズ コード ツールである Terraform を使用すると、再利用、共有、バージョン管理が可能な構成ファイルでリソースを定義して、クラウドおよびオンプレミスのリソースを自動化できます。

- 冗長なワークフローを最小限に抑えることでコストを削減します。
- インフラストラクチャをコード化して再利用する方法を標準化することでリスクを軽減します。
- 自動化を使用して、クラウド NGFW リソースのデプロイにかかる時間を短縮します。
- Cloud NGFW リソースが Terraform 構成ファイルで宣言されているとおりにプロビジョニングおよび構成されていることを確認することで、信頼性が向上します。

Terraform のサポートに加えて、Cloud NGFW リソースは AWS CloudFormation もサポートします。CloudFormation は、AWS が提供するサービスであり、使用するすべての AWS リソース (Amazon EC2 インスタンスなど) を記述するテンプレートを作成することで、AWS リソースをモデル化および構成するのに役立ちます。CloudFormation テンプレートを使用すると、AWS リソースを個別に作成して構成する必要がありません。テンプレートがあなたの代わりに作業を行います。具体的には、次のようになります。

- テンプレートを使用してすべてのリソース (自動スケーリング グループや Elastic Load Balancer など) とそのプロパティを記述することで、インフラストラクチャ管理を簡素化します。
- インフラストラクチャを複製し、CloudFormation テンプレートを一貫性のある繰り返し可能な方法で再利用できるようにします。テンプレートを使用してリソースを一度記述し、同じリソースを複数のリージョンにわたって繰り返しプロビジョニングします。

- 増分アップグレードなどの状況をサポートすることで、デプロイメントの変更を制御および追跡します。たとえば、アップグレードによって予期しないパフォーマンスの問題が発生する可能性があります。インフラストラクチャを手動で元の設定にロールバックするには、変更されたリソースと元の設定をよく理解している必要があります。読みやすいテキスト ファイルとして記述された CloudFormation テンプレートは、リビジョンを明確に識別することでインフラストラクチャの変更を識別するのに役立ちます。さらに、バージョン管理システムと組み合わせると、いつ、どこで、誰が変更を加えたかを正確に把握できます。

プログラムによるアクセスを有効にする

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）

Cloud NGFWプログラムによるアクセスにより、REST APIを使用してNGFW とルールスタックを作成および管理できます。これらの API を使用すると、アプリケーションまたはサードパーティツールを介して Cloud NGFW リソース（NGFW およびルールスタック）でアクションを呼び出すことができます。これらのAPIを使用すると、Cloud Formation Templates（CFT）やTerraformテンプレートなどのInfrastructure-as-Code（IAC）ツールを使用することもできます。これらのIaCツールをAWS環境の内外のワークロードにインストールして実行できます。

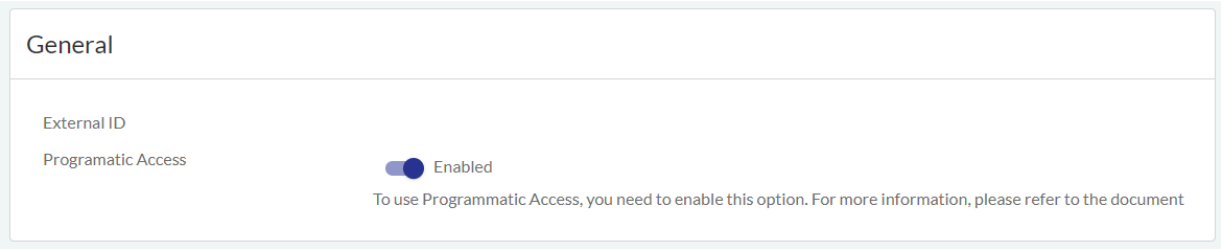
プログラムによるアクセスは強力であるため、Cloud NGFW は、認証要求に署名するための別のアクセスキーまたは秘密鍵を提供しません。代わりに、AWS アカウントで IAM ロールを使用して Cloud NGFW API にアクセスし、どの IAM リソースがこのロールを引き受けることができるかを設定できます。このアプローチは、一時的な認証情報を使用してそれらを自動的にローテーションすることにより、一般的なセキュリティ体制を改善します。

Cloud NGFW のプログラムによるアクセスは、デフォルトで無効になっています。

API リファレンスマテリアルの詳細については、Cloud NGFW API ドキュメントを参照してください。

STEP 1 | プログラムによるアクセスを有効にします。

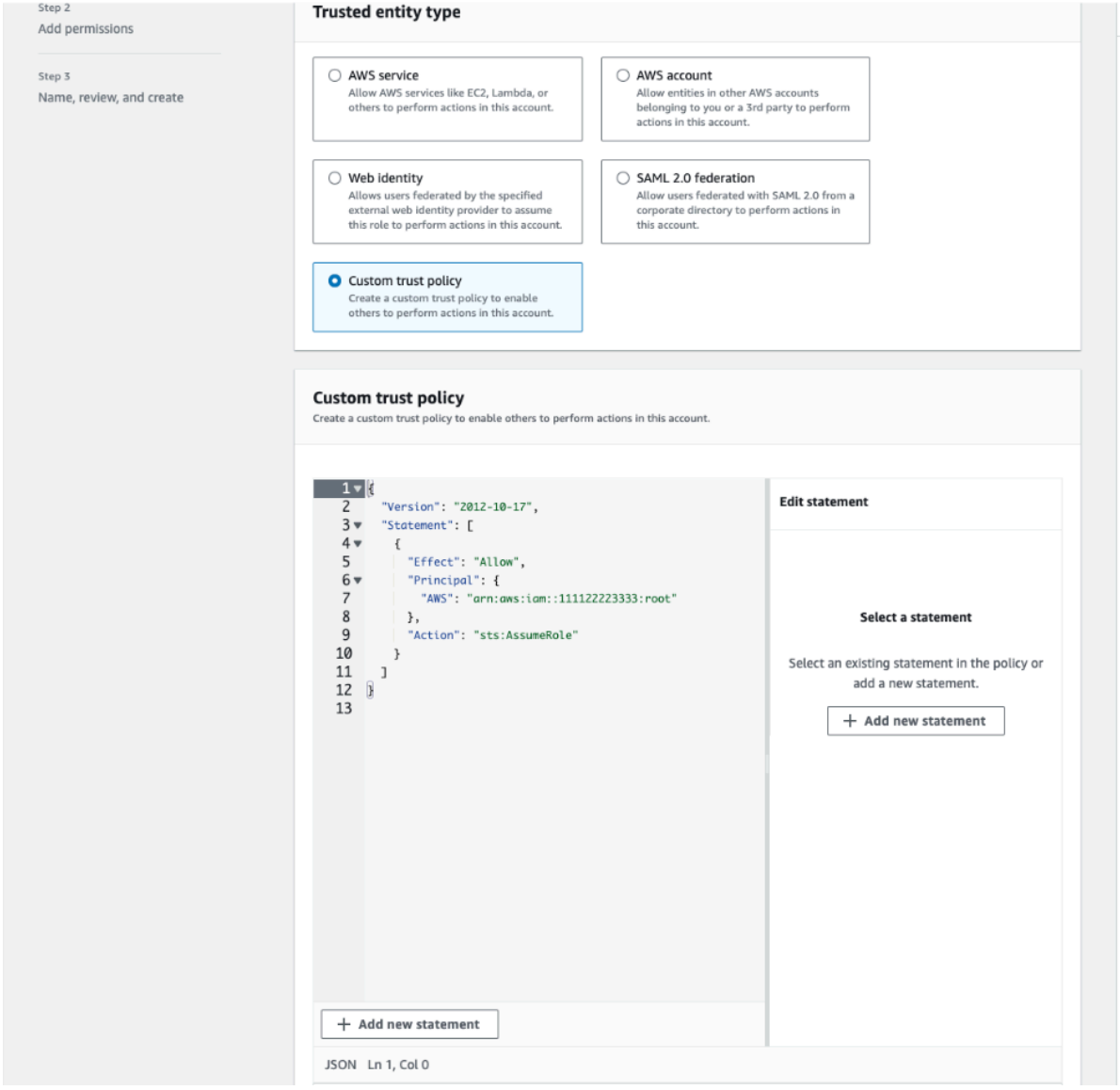
- **Cloud NGFW** テナントコンソールで［テナント］を選択します。
- ［全般］で、［プログラムによるアクセス］スライダーをクリックします。
- ［有効にする]をクリックして確定します。



STEP 2 | カスタム信頼ポリシーを使用して新しいロールを作成します。

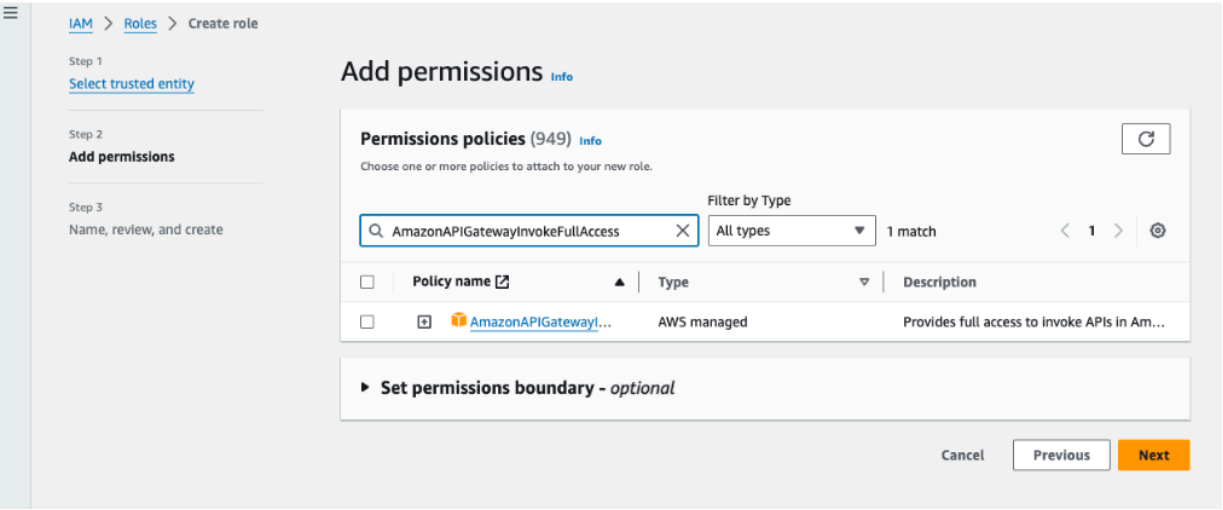
以下はカスタム信頼ポリシーの例です。

```
{ "Version":"2012-10-17", "Statement": [ { "Effect":"Allow",
 "Principal": { "AWS": "arn:aws:iam::111122223333:root" },
 "Action": "sts:AssumeRole" } ] }
```



上記のプリンシパル ルートを使用した信頼関係の例では、意図したよりも多くのプリンシパルへのアクセスが提供される場合があります。*Principal* 要素と *Condition* 要素を使用して、特定のプリンシパルのロールへのアクセスを制限できます。詳細については、「IAM ロールで信頼ポリシーを使用する方法」を参照してください。また、このロールを *1* つの *AWS* アカウントで作成し、クロスアカウントアクセスを使用して特定のアクセス許可を別のアカウントに委任することもできます。クロスアカウント アクセスで信頼ポリシーを定義するには、の例をこちらより参照してください。

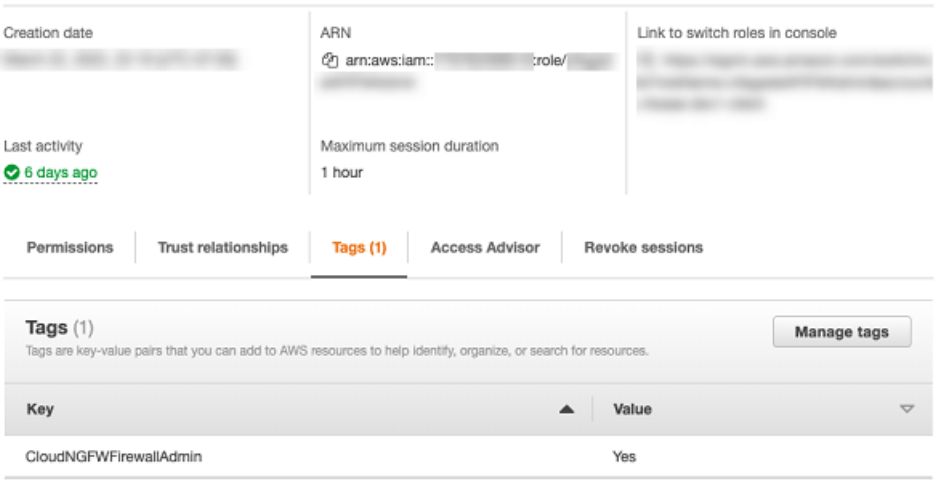
STEP 3 | API を呼び出すための Amazon**APIGatewayInvokeFullAccess** アクセス許可ポリシーを追加します。詳細については ここをクリック してください。



STEP 4 | 次のタグ（キーと値で構成される）を IAM ロールに追加して、必要に応じてアクセス許可ポリシーを提供します。

使用率	TagKey	TagValue
ファイアウォールの作成と管理	**CloudNGFW**ファイアウォール管理者	あり

使用率	TagKey	TagValue
ローカルルールスタックの作成と管理	**CloudNGFWRulestackAdmin**	あり
グローバルルールスタックの作成と管理	**CloudNGFWGlobalRulestackAdmin**	あり
AWSアカウントのオンボード	CloudNGFWAccountAdmin	あり



同じロールに複数のタグを割り当てることができます。これらのタグは、さまざまなCloud NGFWプログラム アクセス ロール トークンにアクセスするために使用できます。

STEP 5 | （Cloud NGFW Programmatic Access の例を使用することを選択した場合は、ステップ7から9をスキップします） Gitリポジトリの下のAPIフォルダーとCFTフォルダーの例を使用して、それぞれプログラムアクセスツールとCFTにアクセスします。

*Palo Alto Networks*が提供する例を実行するには、*programmatic_access*ディレクトリ全体をダウンロードします。

ツールは内部的にロールを引き受け、ロールのアクセス キーとシークレット キーを生成し、SigV4ヘッダーを生成します。また、特定のエンドポイント ロールを呼び出して、Cloud NGFW のプログラムアクセストークンを取得します。

STEP 6 | AWS CLIを使用して、必要に応じてステップ5で説明したタグキー ペアの値を持つロールを引き受けます。

```
$ aws sts assume-role --role-arn arn:aws:iam::<AWS-ACCOUNT-
ID>:role/<ROLE-NAME> --profile <AWS-PROFILE-TO-ASSUME> --role-
session-name <SESSION-NAME> { "Credentials": { "AccessKeyId":
 "<ACCESS-KEY>", "SecretAccessKey": "<SECRET-ACCESS-KEY>",
 "SessionToken": "<SESSION-TOKEN>", "Expiration": "<CREDENTIALS-
```



```
EXPIRATION>" }, "AssumedRoleUser": { "AssumedRoleId": "<ROLE-
ID>:<SESSION-NAME>", "Arn": "arn:aws:iam::<AWS-ACCOUNT-ID>:role/
<ROLE-NAME>/<SESSION-NAME>" } }
```

ロールを引き受けると、一時的なアクセスキーとシークレットキーがアカウント用に生成されます。詳細については、特定のタグを持つ役割を引き受けるを参照してください。

STEP 7 | ステップ7で取得した一時的な資格情報を使用して、SigV4(署名バージョン4)ヘッダーを生成します。詳細については、SigV4 を使用した AWS リクエストへの署名を参照してください。

以下は、AWS SigV4署名付きヘッダーの例です。

```
AWS4-HMAC-SHA256 Credential=<ACCESS-KEY>/20220421/<REGION>/execute-
api/aws4_request, SignedHeaders=host;x-amz-date;x-amz-security-
token, Signature=<SIGNATURE>
```

STEP 8 | `SubcriptionKey` と `TokenID`を生成します。

REST API を使用して Cloud NGFW にアクセスするには、API 呼び出しの前にこのパスを使用します —`api.<region-name>.aws.cloudngfw.paloaltonetworks.com`.詳細は、Azure ドキュメントを参照してください。

- クラウドファイアウォール管理者ロールの場合 — `https://api.<region-name>.aws.cloudngfw.paloaltonetworks.com/v1/mgmt/tokens/cloudfirewalladmin` を取得
- クラウドルールスタック管理者ロールの場合 — `https://api.<region-name>.aws.cloudngfw.paloaltonetworks.com/v1/mgmt/tokens/cloudrulestackadmin` を取得
- クラウドグローバルルールスタック管理者ロールの場合 — `https://api.<region-name>.aws.cloudngfw.paloaltonetworks.com/v1/mgmt/tokens/cloudglobalrulestackadmin` を取得

トークンを取得する

以下は、トークンを取得するためのcURLコマンドの例です。

```
$ curl --location --request GET 'https://api.us-
east-1.aws.cloudngfw.paloaltonetworks.com/v1/mgmt/tokens/
cloudfirewalladmin' \ > --header 'X-Amz-Security-Token: <SESSION-
TOKEN>' \ > --header 'X-Amz-Date: <CREDENTIALS-EXPIRATION-AMZ-DATE-
FORMAT>' \ > --header 'Authorization: <AWS-V4-SIGNED-HEADER>'
```

応答

```
{"Response": {"TokenId": "<CLOUD-NGFW-PROGRAMMATIC-ACCESS-TOKEN>",
 "SubscriptionKey": "<SUBSCRIPTION-KEY>", "ExpiryTime":30,
 "Enabled": true}, "ResponseStatus": {"ErrorCode":0}}
```

STEP 9 | Cloud NGFW コンソールの ヘッダーセクションに応答データを追加します。

ヘッダー	値
承認:	<TokenID>
x-api-key	<SubscriptionKey>

以下は、Cloud NGFW API呼び出しのサンプルです。

```
curl --location --request GET 'https://api.us-
east-1.aws.cloudngfw.paloaltonetworks.com/v1/config/rulestacks/
rs-1' \ > --header 'Authorization: <CLOUD-NGFW-PROGRAMMATIC-ACCESS-
TOKEN>' \ > --data-raw ''
```

応答

```
{"Response": {"RuleStackName": "rs-1", "RuleStackCandidate":
 {"Scope":"Local", "MinAppIdVersion":"8433-6838", "Profiles":
 {"AntiSpywareProfile":"BestPractice"、"AntiVirusProfile":"BestPractice"、"Vul
 "FileBlockingProfile":"BestPractice"}, "UpdateToken":"1"},
 "RuleStackState":"Uncommitted"}, "ResponseStatus":
 {"ErrorCode":0}}
```

STEP 10 | プログラムによるアクセスを取り消すには、アクセスキー、シークレットキー、およびサブスクリプションキーを使用してトークン API を呼び出します — `DELETE https://:<region-name>.aws.cloudngfw.paloaltonetworks.comv1/mgmt/tokens/{TokenID}`。

アクセスキーとシークレットキーは一時的なものです。有効期限が切れた場合は、新しいアクセスキーとシークレットキーを生成します。

Cloud NGFW AWS の Terraform サポート

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）

HashiCorp Terraform は、マルチクラウド環境を管理するチーム向けのオープンソースインフラストラクチャとしてのコードツールです。これにより、クラウドインフラストラクチャのターゲット状態を説明する設定を定義し、それを使用して、クラウドインフラストラクチャのプロビジョニングと管理に関連する変更を実行しながら、定義されたターゲットに到達するために必要なステップを自動的に計算できます。これらの Terraform 設定では、プロバイダーと呼ばれるプラグインを使用します。プラグインは、AWSなどのプロバイダーと連携して、クラウドインフラストラクチャの構築と維持のための繰り返し可能なステップを作成することで再利用を促進し、CI/CDパイプラインへの簡単な追加を保証します。

パロアルトネットワークスは、セキュリティインフラストラクチャの構築プロセスを自動化し、NGFWルールスタックを使用してネットワークセキュリティポスチャを維持するために、cloudngfwawsプロバイダーを追加しました。このプロバイダーは、クライアント (Terraform を実行しているデバイス) と Cloud NGFW for AWS サービスが提供する API 間の通信を容易にする翻訳レイヤーとして機能します。

Palo Alto Networksの開発者向けドキュメントで、Terraformを使用したCloud NGFW on AWSのデプロイについて詳細を確認し、Terraformの参照情報を表示します。

次への構成ではTerraformプロバイダーを使用できます:

- Cloud NGFWを起動します。
- Cloud NGFW がポリシー情報を取得するために使用するルールスタックを設定します。ルールスタックには、セキュリティ ルール、インテリジェント フィード、さまざまなオブジェクトなど、関連するポリシー情報が含まれています。

cloudngfwaws Terraformプロバイダーを使用して、Cloud NGFW for AWSを管理するためのリソースにアクセスします。**cloudngfwaws** プロバイダーは、一時的な認証情報を生成する STS の引き受けロールを使用して AWS への認証を行います。これらの一時的な認証情報は、最初の認証シーケンスで簡単に使用され、アクセスキー、シークレットキー、セッショントークンが含まれます。このシーケンスでは、次のようになります:

1. 認証では AWS API を使用してAWS STSがロールを引き受けます。API アクセスを有効にする必要があります。
2. STS 認証情報は、Cloud NGFW for AWS API を使用して Cloud NGFW 管理者トークンを更新するために使用されます。これらの認証情報は、ルールスタックの管理者トークンを更新するためにも使用されます。
3. Cloud NGFW 管理者トークンとルールスタック管理者トークンは、Cloud NGFW for AWS APIを使用した構成管理に使用されます。

以下を検討してください。

- AWS への認証が成功すると、プロバイダーはファイアウォールとルールスタックの管理用に JWT を取得します。
- プロバイダーブロックで AWS アクセスとシークレットキーを静的に指定できます。これらの認証情報を指定しない場合、共有認証情報ファイルから自動的に取得されます。access_key と secret_key のパラメータを使用して、AWS 認証情報を静的に提供します。
- プロバイダーをセットアップするとき、AWS 認証ワークフローはAWS Go SDKを使用して認証に関連する変数を制御します。AWS 環境変数を使用して、AWS 認証に使用される認証情報を設定できます。
- プロバイダーはAPI アクセスが必要です。

プロバイダー パラメーターは、さまざまな方法で優先順位が付けられます。値が重複している場合、これらのパラメーターは以下の順序で処理されます。

1. プロバイダー ブロックで静的に設定されます。
2. 環境変数。
3. JSON 設定ファイルから取得します。

クラウド **NGFW** の例の **Terraform** プロバイダー

Terraform 0.13以降:

```
テラフォーム { required_providers { cloudngfwaws = { source =
 "paloaltonetworks/terraform-provider-cloudngfwaws" version
 = "1.0.0" } } } provider "cloudngfwaws" { json_config_file =
 "~/.cloudngfwaws_creds.json" }
```

JSON 設定ファイル:

```
{ "host": "api.us-east-1.aws.cloudngfw.paloaltonetworks.com",
 "region": "us-east-1", "arn": "arn:aws:iam::123456789:role/MyRole" }
```

アカウントの自動オンボーディングを設定する

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）

Cloud NGFW for AWSは、大量のAWSアカウントを扱う環境向けに、アカウントの自動オンボーディングをサポートするようになりました。この機能により、個々のアカウントを手動でオンボードする必要がなくなりました。アカウントの自動オンボーディングを使用する場合は、次の点を考慮してください。

- 一度に100アカウントまでオンボードできます。100個を超えるアカウントをオンボードするには、複数のモジュールを定義する必要があり、それぞれに100個のアカウントが含まれます。詳細については、Terraformのマニュアルを参照してください。
- アカウントの自動オンボーディングは、完了までに約10分かかります。
- AUTH に AWS プロファイルを使用している場合は、アカウントのオンボーディングに `CloudNGFWGAccountAdmin` プロファイルを使用します。
- CloudFormation テンプレート (CFT) を使用してロールを作成し、オンボードする各アカウントに 権限を適用します 。
- マーケットプレイス経由で Cloud NGFW にサブスクライブすると、アカウントが正常にオンボードされるはずです。
- 必要な役割は 2 つあります。
  - 管理者アカウントに `CloudNGFWAccountAdmin` ロールを作成します。
  - Terraform を使用してオンボードする各アカウントで CFT を実行できるロールを作成します。

これらの役割については、以下の手順で説明します。

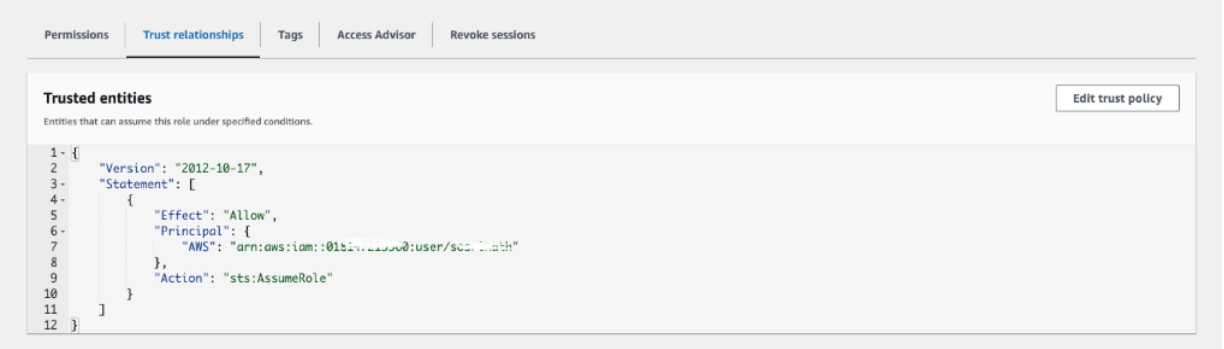
自動アカウントオンボーディング機能にアクセスするには、最新のTerraformテンプレートをダウンロードして、プログラムによるアクセスを有効にする必要があります。

アカウントの自動オンボーディングの設定方法:

STEP 1 | 現在オンボーディング済みのアカウントのAccountAdminプログラムによるアクセスロールを作成します。「プログラムによるアクセスを有効にする」の手順 1 ～ 4 に従って、 タグ CloudNGFWAccountAdminを持つロールを作成します。

STEP 2 | オンボードする各アカウントで、CloudFormation テンプレート (CFT) を実行するロールを作成します。

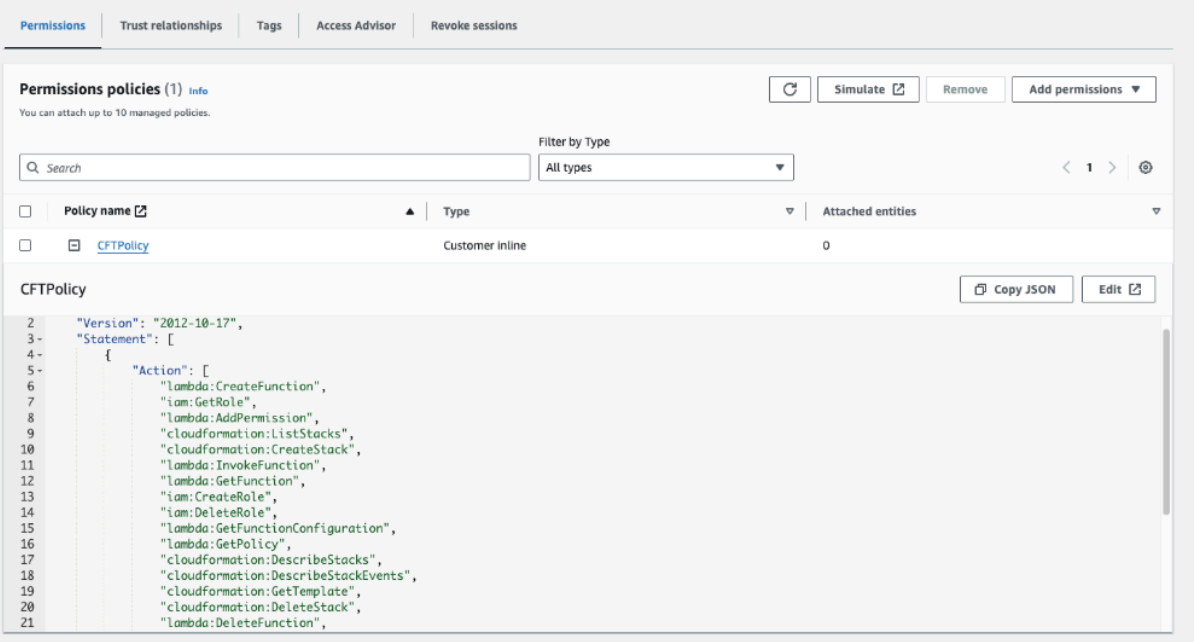
```
{ "Version":"2012-10-17", "Statement": [ { "Effect":"Allow",
 "Principal": { "AWS": "arn:aws:iam::ACCOUNT_ID:user/USERNAME" },
 "Action": "sts:AssumeRole" } ] }
```



ロールの権限ポリシーは 、インライン ポリシーの作成を使用して定義されます。例:

```
"Statement": [ { "Action": [ "lambda:CreateFunction",
 "iam:GetRole", "lambda:AddPermission",
 "cloudformation:ListStacks", "cloudformation:CreateStack",
 "lambda:InvokeFunction", "lambda:GetFunction", "iam:CreateRole",
 "iam:DeleteRole", "lambda:GetFunctionConfiguration",
 "lambda:GetPolicy", "cloudformation:DescribeStacks",
 "cloudformation:DescribeStackEvents",
 "cloudformation:GetTemplate", "cloudformation:DeleteStack",
 "lambda:DeleteFunction", "iam:DeleteRolePolicy",
 "iam:DetachRolePolicy", "iam:AttachRolePolicy",
```

```
"iam:PutRolePolicy", "iam:PassRole" ], "Resource": "*",
"Effect":"Allow", "Sid":"VisualEditor1" } ] }
```



信頼関係の例 (上記) は、*CFT* を実行する権限が与えられた特定のアカウント内の特定のユーザーを表しています。独自の信頼ポリシーを定義する方法の詳細については、「IAM ロールで信頼ポリシーを使用する方法」を参照してください。

STEP 3 | Terraform Applyを実行します。

CFTに変更を適用した後、Cloud NGFWリソースは各アカウントをオンボードします。

- アカウント オンボーディング モジュールは、アカウントでアカウント ロール セットアップCFTを実行します。
- クロス アカウント ロールCFTは、ロールARNをCloud NGFWリソースに送信します。

アカウント オンボーディング モジュールは時間を待機します。すべてのアカウントのオンボーディングが完了するまでに 10 分以上かかる場合があります。

Terraform ファイルの例

次の例は、プロバイダーとモジュールの定義を含む Terraform ファイルを示しています。この例では、account_admin_arn は手順 1 で作成されたプログラム アクセス ロールを参照します。フィールド **account_ids** は、 オンボードする必要がある AWS アカウントのリストを表します。フィールド **cft_role_name** は、 オンボードされた各アカウントの手順 2 で作成されたロールを表します。

```
terraform { required_providers { cloudngfwaws = { source
 = "paloaltonetworks/cloudngfwaws" } } } provider
 "cloudngfwaws" { account_admin_arn = "arn:aws:iam::11222333344:role/
fwaas_prog_onboard" json_config_file = "./.cloudngfwaws_creds.json" }
 module "account_onboarding1" { source = “github.com/
PaloAltoNetworks/terraform-provider-cloudngfwaws/modules/
account_onboarding" account_ids = ["ACCOUNT_1", "ACCOUNT_2"....,
 “ACCOUNT_100”] cft_role_name = "cft_apply_role" } module
 "account_onboarding2" { source = “github.com/PaloAltoNetworks/
terraform-provider-cloudngfwaws/modules/account_onboarding"
 account_ids = ["ACCOUNT_101", "ACCOUNT_102"...., “ACCOUNT_200”]
 cft_role_name = "cft_apply_role" }
```

オンボード済みアカウントを削除する

Terraform **destroy**を使用します。詳細については、Terraform のドキュメントを参照してください。

オンボーディング済みアカウントを一覧表示する

Terraform リストを使用します。詳細については、Terraform のドキュメントを参照してください。

Cloud NGFW リソースを AWS CFT にプロビジョニングする

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）

Cloud NGFW では、独自のリソースを作成できるため、AWS CloudFormation テンプレート（CFT）にリソースを柔軟にプロビジョニングできます。

Cloud NGFW で *CloudFormation* レジストリを使用する前に、プログラムによるアクセスを有効にする必要があります。

PaloAltoNetworks::CloudNGFW::RuleStack と **PaloAltoNetworks::CloudNGFW::NGFW** スキーマを使用して、Cloud NGFW を AWS CloudFormation テンプレートに統合します。このドキュメントに記載されている構文を使用して、AWS CloudFormation レジストリと統合できる Cloud NGFW ファイアウォールの設定を定義します。

PaloAltoNetworks::CloudNGFW::RuleStack スキーマ

- JSON

```
{ "Type" :"PaloAltoNetworks::CloudNGFW::RuleStack", "Properties" :
 { "RuleStackName" :String, "RuleStack" :RuleStack, "RuleList" :
 [ Rule, ... ], "SecurityObjects" :SecurityObjects,
 "CustomSecurityProfiles":CustomSecurityProfiles, } }
```

- YAML

```
Type:PaloAltoNetworks::CloudNGFW::RuleStack プロ
パティ:RuleStackName:String RuleStack:RuleStack
 RuleList: - Rule SecurityObjects:SecurityObjects
 CustomSecurityProfiles:CustomSecurityProfiles
 ProgrammaticAccessToken:文字列
```

要素	詳説

RuleStackName	ルールスタックのわかりやすい名前を入力します。
	JSON
	`“RuleStackName” :String,`
	YAML
	`RuleStackName:String`

RuleStack	ルールスタックの説明を入力します。説明には以下が含まれます:
	JSON
	`{ "Scope" :String, "Profiles" :RuleStackProfiles, "Description" :String "Deploy" :String }`
	YAML
	`Scope:String Profiles:RuleStackProfiles Description:String Deploy:String`

RuleStackProfiles	指定されたルールスタックのプロファイルを識別します。プロファイルには以下が含まれます:
	JSON
	`{ "AntiSpywareProfile" :String, "AntiVirusProfile" :String, "VulnerabilityProfile" :String, "URLFilteringProfile" :String, "FileBlockingProfile" :String, "OutboundTrustCertificate" :String, "OutboundUntrustCertificate" :String }`
	YAML
	`AntiSpywareProfile:String AntiVirusProfile:String VulnerabilityProfile:String URLFilteringProfile:String FileBlockingProfile:String OutboundTrustCertificate:String OutboundUntrustCertificate:String`

rule	ルールスタックのルールを確立します。ルールには以下が含まれます:

要素	詳説
	JSON `{ "RuleName" :String, "Description" :String, "RuleListType" :String, "Priority" :Integer, "Enabled" :Boolean, "Source" :RuleSource, "NegateSource" :Boolean, "Destination" :RuleDestination, "NegateDestination" :Boolean, "Applications" : [String, ...], "Category" :UrlCategory, "Protocol" :String, "AuditComment" :String, "Action" :String, "Logging" :Boolean, "DecryptionRuleType" :String, "Tags" : [Tag, ...] }` **YAML** `RuleName:String Description:String RuleListType:String Priority:Integer Enabled:Boolean Source:RuleSource NegateSource:Boolean Destination:ルール宛先無効化宛先:Boolean Applications: - String Category:UrlCategory Protocol:String AuditComment:String Action:String Logging:Boolean DecryptionRuleType:String Tags: - Tag`

RuleSource	**RuleSource** を使用してルールのコレクションを設定します。RuleSource には以下が含まれます:
	JSON
	`{ "Cidrs" : [ String, ... ], "PrefixLists" : [ String, ... ], "Countries" : [ String, ... ], "Feeds" : [ String, ... ] // RuleStackname? }`
	YAML
	`cidrs: - String PrefixLists: - String Countries: - String Feeds: - String`

RuleDestination	確認 URL と 1 つ以上のデータ収集 URL をサポートする Web サービスの **RuleDestination** を設定します。RuleDestination には以下が含まれます: **JSON** `{ "Cidrs" : [ String, ... ], "FqdnLists" : [ String, ... ], "PrefixLists" :`

要素	詳説
	<pre>[String, ...], "Countries" : [String, ...], "Feeds" : [String, ...] // RuleStackname? }</pre> **YAML** <pre>Cidrs: - String FqdnLists: - String PrefixLists: - String Countries: - String Feeds: - String</pre>
タグ	ルールスタックのタグを指定します。タグには以下が含まれます: **JSON** <pre>{ "Key" :String, "Value" :String }</pre> **YAML** <pre>Key:String Value:String</pre>
UrlCategory	**URLCategory** を使用して、認証、復号化、QoS、およびセキュリティポリシールールの条件を照合します。UrlCategory には以下が含まれます: **JSON** <pre>{ "URLCategoryNames" : [String, ...], "Feeds" : [String, ...] }</pre> **YAML** <pre>URLCategoryNames: - String Feeds: - String</pre>

SecurityObjects	ルールスタックの **SecurityObjects** を設定します。SecurityObjectsには以下が含まれます:
	
	JSON
	<pre>{ "PrefixList" :PrefixList,
	"FqdnLists" :FqdnList,
	"CustomUrlCategories" :CustomUrlCategory,
	"IntelligentFeeds" :IntelligentFeed,
	"CertificateLists" :CertificateList }</pre>
	YAML
	<pre>PrefixList:PrefixList FqdnList:FqdnList CustomUrlCategory:CustomUrlCategory</pre>

要素	詳説
	IntelligentFeed:IntelligentFeed CertificateList:CertificateList
CustomSecurityProfiles	**CustomSecurityProfiles** を使用して、信頼されたセキュリティゾーン間のトラフィックに対するアンチウイルスの検査を最小限に抑え、インターネットなどの信頼されていないゾーンから受信したトラフィックや、サーバーファームなどの機密性の高い宛先に送信されるトラフィックの検査を最大化できます。CustomSecurityProfiles には以下が含まれます: **JSON** { "FileBlocking" :FileBlocking } **YAML** FileBlocking:FileBlocking
PrefixLists	**PrefixList** を使用して、プレフィックスに基づいてルートをフィルタリングします。注文番号と IP プレフィックスを定義することで、支店またはデータセンターの ION デバイスはルートを許可または拒否できます。動的で自動生成されるプレフィックスリストは、ION デバイスがアドバタイズする内容に基づいています。プレフィックスは分割することも、分割しないこともできます。PrefixList には以下が含まれます: **JSON** { "Name" :String, "PrefixList" : [String, ...], "AuditComment" :String, "Description" :String } **YAML** Name:String PrefixList: - String AuditComment:String Description:String
FqdnLists	**FqdnList**オブジェクトを使用すると、DNSはIPアドレスのFQDN解決を行うため、IPアドレスを知る必要がなくなり、FQDNが新しいIPアドレスに解決されるたびに手動で更新できます。FqdnListsには以下が含まれます:

要素	詳説

	JSON
	`{ "Name" :String, "Description" :String, "FqdnList" : [ String, ... ], "AuditComment" :String }`
	YAML
	`Name:String Description:String FqdnList: - String AuditComment:String`

CustomUrlCategories	**CustomURLCategories**を使用して、カスタムURLフィルタリングオブジェクトを作成して、URLカテゴリの適用に対する例外を指定し、複数のURLカテゴリに基づいてカスタムURLカテゴリを作成できます。
	• URL カテゴリの強制に対する例外を定義する - セキュリティポリシールールで一致条件として使用する URL のカスタムリストを作成します。これは、特定の URL をそれが属す URL カテゴリとは別に適用したい場合に、URL カテゴリに対する例外を指定する際に良い方法になります。
	• 複数の PAN-DB に基づいてカスタム URL カテゴリを定義 — 一連のカテゴリにマッチするウェブサイトに絞って適用させることができます。ウェブサイトあるいはページは、カスタム カテゴリの一部として定義されたすべてのカテゴリにマッチしなければなりません。
	CustomURLCategoriesには次のものが含まれます:
	JSON
	`{ "URLTargets": [String, ...]、 "Name":String, "Description" :String, "Action" :String, "AuditComment" :String }`
	YAML
	`URLTargets: - String Name:String Description:String Action:String AuditComment:String`

IntelligentFeeds	**IntelligentFeeds**を使用して、最新の脅威インテリジェンスデータを継続的にフィードします。IntelligentFeedsには以下が含まれます:

要素	詳説

	JSON
	`{ "Name" ：String, "Description" :String, "Certificate" :String, "FeedURL" :String, "Type" :String, "Frequency" :String, "Time" :Integer, "AuditComment" :String }`
	YAML
	`Name:String Description:String Certificate:String FeedURL:String Type:String Frequency:String Time:Integer AuditComment:String`

CertificateObjects	**CertificateObjects**を使用して証明書の要素を定義します。CertificateObjectsには以下が含まれます:
	JSON
	`{ "Name" :String, "Description" :String, "CertificateSignerArn" :String, "CertificateSelfSigned" :Boolean, "AuditComment" :String }`
	YAML
	`Name:String Description:String CertificateSignerArn:String CertificateSelfSigned:Boolean AuditComment:String`

FileBlocking	**FileBlocking** を使用して、ブロックまたは監視したい特定のファイルタイプを識別します。ほとんどのトラフィックの場合（内部ネットワークのトラフィックを含む）、脅威をもたらす既知のファイルや、アップロード/ダウンロードするメリットが無いファイルはブロックします。FileBlocking には以下が含まれます:
	JSON
	`{ "Direction" :String, "FileType" :String, "Description" :String, "Action" :String, "AuditComment" :String }`
	YAML
	`Direction:String FileType:String Description:String Action:String AuditComment:String`

PaloAltoNetworks::CloudNGFW::NGFW Schema

- JSON

```
{ "Type":"PaloAltoNetworks::CloudNGFW::NGFW", "Properties" :
 { "Description" :String, "EndpointMode" :String,
 "FirewallName" :String, "RuleStackName" :String,
 "RuleStackName" :String, "SubnetMappings" : [ String, ... ],
 "Tags" : [ Map, ... ], "VpcId" :String, "UpdateToken" :String,
 "LogDestinationConfigs" : [ LogProfileConfig, ... ],
 "CloudWatchMetricNamespace" :String, }
```

- YAML

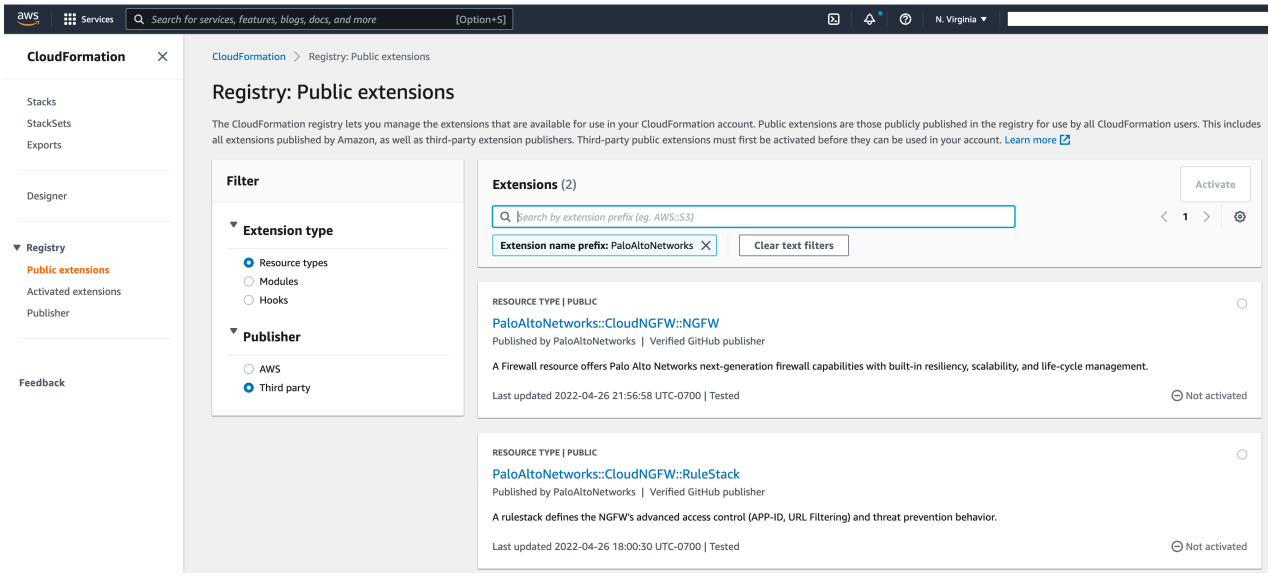
```
type:PaloAltoNetworks::CloudNGFW::NGFWProperties:AppIdVersion:String
 AutomaticUpgradeAppIdVersion:Boolean Description:String
 EndpointMode:String FirewallName:String RuleStackName:String
 RuleStackName:String SubnetMappings: - String Tags: - Map
 VpcId:String UpdateToken:String LogDestinationConfigs:
 - LogProfileConfig CloudWatchMetricNamespace:String
 ProgrammaticAccessToken:文字列
```

要素	詳説

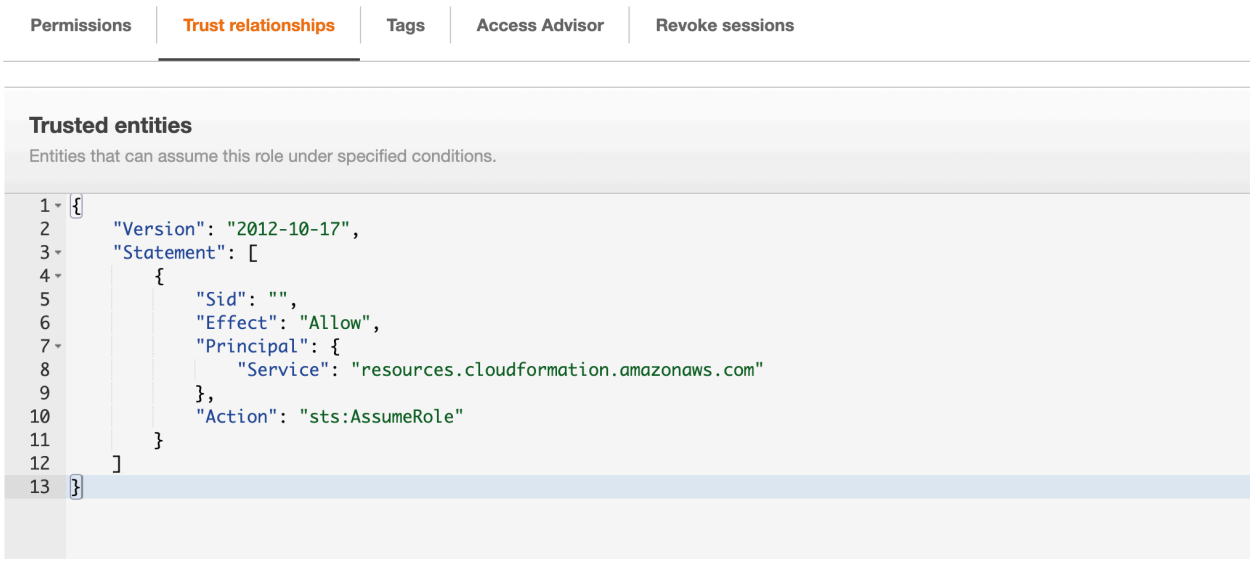
LogProfileConfig	**LogProfileConfig** を使用すると、ファイアウォール構成を変更するためのエントリを表示できます。
	
	JSON
	
	`{ "LogDestination" :String, "LogDestinationType" :String, "LogType" :String}`
	
	YAML
	
	`LogDestination:String LogDestinationType:String LogType:String`

パブリックエクステンションを有効にする

アカウントの **PaloAltoNetworks::CloudNGFW::NGFW**と**PaloAltoNetworks::CloudNGFW::RuleStack** パブリックエクステンションの両方をアクティベートする:



エクステンションの実行ロール ARN を作成します。どちらのエクステンションも同じロールを使用できます。CloudFormationテンプレートを消費するロールで信頼関係を確立します:



信頼関係を確立したら、拡張機能をアクティブ化します:

AWS CloudWatchでログを出荷する

には、または Cloud NGFW for AWSを使用します。

スタック出力

スタック出力として次のリソース属性にアクセスできます。

```
FirewallResource: "/properties/ReadFirewall", "/properties/
ReadFirewall/AccountId", "/properties/ReadFirewall/AppIdVersion",
 "/properties/ReadFirewall/AutomaticUpgradeAppIdVersion", "/
properties/ReadFirewall/EndpointMode", "/properties/ReadFirewall/
FirewallName", "/properties/ReadFirewall/MultiVpcEnable", "/
properties/ReadFirewall/Description", "/properties/ReadFirewall/
VpcId", "/properties/ReadFirewall/SubnetMappings", "/properties/
ReadFirewall/LinkId", "/properties/ReadFirewall/Attachments", "/
properties/ReadFirewall/LinkStatus", "/properties/ReadFirewall/
FirewallStatus", "/properties/ReadFirewall/RuleStackStatus",
```

```
 "/properties/ReadFirewall/FailureReason", "/properties/
ReadFirewall/EndpointServiceName", "/properties/ReadFirewall/
Tags", "/properties/ReadFirewall/RuleStackName", "/properties/
ReadFirewall/GlobalRuleStackName" RuleStackResource: "/properties/
RuleStackCandidate", "/properties/RuleStackRunning", "/properties/
RuleStackCandidate/AccountId", "/properties/RuleStackRunning/
AccountId", "/properties/RuleStackCandidate/Scope", "/properties/
RuleStackRunning/Scope", "/properties/RuleStackCandidate/
MinAppIdVersion", "/properties/RuleStackRunning/MinAppIdVersion",
 "/properties/RuleStackCandidate/Description", "/properties/
RuleStackRunning/Description", "/properties/RuleStackRunning/
Profiles/AntiSpywareProfile", "/properties/RuleStackCandidate/
Profiles/AntiSpywareProfile", "/properties/RuleStackRunning/
Profiles/AntiVirusProfile", "/properties/RuleStackCandidate/
Profiles/AntiVirusProfile", "/properties/RuleStackCandidate/Profiles/
VulnerabilityProfile", "/properties/RuleStackRunning/Profiles/
VulnerabilityProfile", "/properties/RuleStackCandidate/Profiles/
URLFilteringProfile", "/properties/RuleStackRunning/Profiles/
URLFilteringProfile", "/properties/RuleStackCandidate/Profiles/
FileBlockingProfile", "/properties/RuleStackRunning/Profiles/
FileBlockingProfile
```

実行ロール

実行ロールには以下を使用します。

信頼関係:

```
{ "Version":"2012-10-17", "Statement": [ { "Effect":"Allow",
 "Principal": { "Service":
 "resources.cloudformation.amazonaws.com" }, "Action":
 "sts:AssumeRole", "Condition": { "StringEquals":
 { "aws:SourceAccount": "{customer-account-id}" },
 "StringLike": { "aws:SourceArn": "arn:aws:cloudformation:*:
{customer-account-id}":type/resource/PaloAltoNetworks-
CloudNGFW-NGFW/*" } } }, { "Effect":"Allow", "Principal":
 { "Service": "resources.cloudformation.amazonaws.com" },
 "Action": "sts:AssumeRole", "Condition": { "StringEquals":
 { "aws:SourceAccount": {customer-account-id}" }, "StringLike":
 { "aws:SourceArn": "arn:aws:cloudformation:*:{customer-
account-id}":type/resource/PaloAltoNetworks-CloudNGFW-RuleStack/
*" } } } ] }タグ:CloudNGFWRulestackAdmin:CloudNGFWFirewallAdminあ
り:CloudNGFWGlobalRulestackAdminあり:アクセス権限あ
り:AmazonAPIGatewayInvokeFullAccess
```

ロールを作成し、ロール*ARN*を使用してアクティベーション中に実行ロール*ARN*を設定します。アクティベーション中に実行ロールを構成せずにリソースを作成することはできません。

CloudFormationファイアウォール リソース スキーマの例

ルールスタック スキーマの例として以下を使用します。

```
{ "typeName":"PaloAltoNetworks::CloudNGFW::NGFW", "description":"ファ
イアウォール リソースは、耐障害性、拡張性、ライフサイクル管理が組み込まれた パロ
アルトネットワークスの次世代ファイアウォール機能を提供します。", "sourceUrl":
 "https://github.com/aws-cloudformation/aws-cloudformation-rpdk.git",
 "definitions" : { "LogProfileConfig": { "title":"LogProfileConfig",
 "description":"ログ プロファイル設定の追加", "type": "object",
 "properties": { "LogDestination": { "title":"Logdestination",
 "minLength":1, "maxLength":128, "type": "string" },
 "LogDestinationType": { "title":"Logdestinationtype", "enum":
 ["S3", "CloudWatchLogs", "KinesisDataFirehose"], "type": "string" },
 "LogType": { "title":"Logtype", "enum": ["TRAFFIC", "DECRYPTION",
 "THREAT"], "type": "string" } }, "required": ["LogDestination",
 "LogDestinationType", "LogType"], "additionalProperties": false },
 "SubnetMappings": { "type": "array", "items": { "type": "object",
 "properties": { "AvailabilityZone": { "title": "availabilityZone",
 "type": "string" }, "SubnetId": { "title": "subnetId", "type":
 "string" } }, "additionalProperties": false } } }, "properties":
 { "AccountId": { "title":"Accountid", "pattern": "^[0-9]+$", "type":
 "string", "minLength":1 }, "AppIdVersion": { "title":"Appidversion",
 "minLength":1, "maxLength":64, "pattern": "^[0-9]+-[0-9]+
$", "type": "string" }, "AutomaticUpgradeAppIdVersion":
 { "title":"Automaticupgradeappidversion", "default": true,
 "type": "boolean" }, "Description": { "title":"Description",
 "type": "string", "minLength":1 }, "EndpointMode":
 { "title":"Endpointmode:CustomerManaged Or ServiceManaged",
 "enum": ["ServiceManaged", "CustomerManaged"], "type": "string" },
 "FirewallName": { "title":"Firewallname", "minLength":1,
 "maxLength":128, "pattern": "^[a-zA-Z0-9-]+$", "type": "string" },
 "MultiVpcEnable": { "title":"MultiVpcEnable", "type": "boolean" },
 "RuleStackName": { "title":"Rulestackname", "type": "string",
 "minLength":1 }, "SubnetMappings": { "$ref": "#/definitions/
SubnetMappings" }, "AssociateSubnetMappings": { "$ref": "#/
definitions/SubnetMappings" }, "DisassociateSubnetMappings":
 { "$ref": "#/definitions/SubnetMappings" }, "Tags":
 { "title":"Tags", "type": "array", "items": { "type": "object" } },
 "VpcId": { "title":"Vpcid", "type": "string", "minLength":1 },
 "LinkId": { "title":"LinkId", "type": "string", "minLength":1 },
 "LogDestinationConfigs": { "title":"Logdestinationconfigs", "type":
 "array", "items": { "$ref": "#/definitions/LogProfileConfig" } },
 "CloudWatchMetricNamespace": { "title":"Cloudwatchmetricnamespace",
 "type": "string", "minLength":1 } }, "additionalProperties":
 false, "required": [ "FirewallName" ], "createOnlyProperties": [ "/
properties/FirewallName" ], "primaryIdentifier": [ "/properties/
FirewallName" ], "handlers": { "create": { "permissions": [ "execute-
api:Invoke" ] }, "read": { "permissions": [ "execute-api:Invoke" ] },
 "update": { "permissions": [ "execute-api:Invoke" ] }, "delete":
 { "permissions": [ "execute-api:Invoke" ] } } }
```

ルールスタック スキーマの例

ルールスタック スキーマの例として以下を使用します。

```
{ "typeName":"PaloAltoNetworks::CloudNGFW::RuleStack",
 "description":"ルールスタックはNGFWの高度なアクセス制御 (APP-ID、URLフィ
ルタリング) と脅威防御動作を定義します。", "sourceUrl": "https://
github.com/aws-cloudformation/aws-cloudformation-rpdk.git",
 "definitions": { "RuleStack": { "title":"RuleStack", "type":
 "object", "properties": { "AccountId": { "title":"Accountid",
 "pattern": "^[0-9]+$", "type": "string", "minLength":1 },
 "Scope": { "title":"Scope", "default":"Local", "enum":
 ["Local", "Global"], "type": "string" }, "LookupXForwardedFor":
 { "title":"LookupXForwardedFor", "default":"None", "enum":
 ["SecurityPolicy", "None"], "type": "string" }, "MinAppIdVersion":
 { "title":"Minappidversion", "default":"8433-6838", "pattern":"8\
\d\\d\\d\\-\\d\\d\\d\\d", "type": "string" }, "Profiles": { "$ref":
 "#/definitions/RuleStackProfiles" }, "Description": { "title":"説明",
 "maxLength":512, "type": "string" }, "Deploy": { "title":"Deploy",
 "description":"Deploy RuleStack YES/NO", "default":"YES", "type":
 "string" } }, "additionalProperties": false }, "RuleStackProfiles":
 { "title":"RuleStackProfiles", "type": "object", "properties":
 { "AntiSpywareProfile": { "title":"Antispywareprofile",
 "default":"BestPractice", "enum": ["BestPractice", "None"], "type":
 "string" }, "AntiVirusProfile": { "title":"Antivirusprofile",
 "default":"BestPractice", "enum": ["BestPractice",
 "None"], "type": "string" }, "VulnerabilityProfile":
 { "title":"Vulnerabilityprofile", "default":"BestPractice", "enum":
 ["BestPractice", "None"], "type": "string" }, "URLFilteringProfile":
 { "title":"Urlfilteringprofile", "default":"None", "enum":
 ["BestPractice", "None"], "type": "string" }, "FileBlockingProfile":
 { "title":"Fileblockingprofile", "default":"BestPractice",
 "enum": ["Custom", "BestPractice", "None"], "type": "string" },
 "OutboundTrustCertificate": { "title":"Outboundtrustcertificate",
 "maxLength":63, "type": "string" }, "OutboundUntrustCertificate":
 { "title":"Outbounduntrustcertificate", "maxLength":63,
 "type": "string" } }, "additionalProperties": false },
 "Tag": { "title":"タグ", "type": "object", "properties":
 { "Key": { "title":"キー", "minLength":1, "maxLength":128,
 "type": "string" }, "Value": { "title":"値", "minLength":1,
 "maxLength":128, "type": "string" } }, "required": ["Key", "Value"],
 "additionalProperties": false }, "Rule" : { "title":"Rule",
 "type": "object", "properties": { "RuleName": { "title":"Rulename",
 "minLength":1, "maxLength":48, "pattern": "^[a-zA-Z0-9-]+$", "type":
 "string" }, "Description": { "title":"説明", "maxLength":512,
 "type": "string" }, "RuleListType": { "title":"RuleListType",
 "description":"RuleList type:LocalRule, PreRule, PostRule", "type":
 "string" }, "Priority": { "title":"優先順位", "description":"ルー
ルの優先順位", "type": "integer" }, "Enabled": { "title":"有効",
 "default": true, "type": "boolean" }, "Source": { "$ref": "#/
definitions/RuleSource" }, "NegateSource": { "title":"Negatesource",
 "default": false, "type": "boolean" }, "Destination": { "$ref":
 "#/definitions/RuleDestination" }, "NegateDestination":
 { "title":"Negatedestination", "default": false, "type":
 "boolean" }, "Applications": { "title":"アプリケーション",
```

```
 "default": ["any"], "type": "array", "items": { "type": "string",
 "maxLength":63 } }, "Category": { "$ref": "#/definitions/
UrlCategory" }, "Protocol": { "title":"プロトコル", "default":
 "application-default", "maxLength":63, "type": "string" },
 "ProtPortList": { "title":"ProtPortList", "type": "array",
 "items": { "type": "string", "maxLength":63 } }, "AuditComment":
 { "title":"監査コメント", "maxLength":512, "type": "string" },
 "Action": { "title":"アクション", "default":"Allow", "enum":
 ["Allow", "DenySilent", "DenyResetServer", "DenyResetBoth"], "type":
 "string" }, "Logging": { "title":"ロギング", "default": false, "type":
 "boolean" }, "DecryptionRuleType": { "title":"Decryptionruletype",
 "enum": ["SSLOutboundInspection", "SSLInboundInspection",
 "SSLOutboundNoInspection", "SSLInboundNoInspection"],
 "type": "string" }, "InboundInspectionCertificate":
 { "title":"InboundInspectionCertificate", "type": "string",
 "maxLength":63 }, "Tags": { "title":"タグ", "maxItems":200, "type":
 "array", "items": { "$ref": "#/definitions/Tag" } } }, "required":
 ["RuleName", "RuleListType", "Priority"], "additionalProperties":
 false }, "RuleSource": { "title":"RuleSource", "type":
 "object", "properties": { "Cidrs": { "title":"Cidrs", "type":
 "array", "items": { "type": "string", "maxLength":24 } },
 "PrefixLists": { "title":"Prefixlists", "type": "array",
 "items": { "type": "string", "maxLength":63 } }, "Countries":
 { "title":"国", "description":"国コード", "type": "array",
 "items": { "type": "string", "maxLength":2 } }, "Feeds":
 { "title":"フィード", "type": "array", "items": { "type":
 "string", "maxLength":63 } } }, "additionalProperties": false },
 "RuleDestination": { "title":"RuleDestination", "type": "object",
 "properties": { "Cidrs": { "title":"Cidrs", "type": "array",
 "items": { "type": "string", "maxLength":24 } }, "FqdnLists":
 { "title":"Fqdnlists", "type": "array", "items": { "type": "string",
 "maxLength":63 } }, "PrefixLists": { "title":"Prefixlists",
 "type": "array", "items": { "type": "string", "maxLength":63 } },
 "Countries": { "title":"国", "description":"国コード", "type":
 "array", "items": { "type": "string", "maxLength":2 } },
 "Feeds": { "title":"フィード", "type": "array", "items": { "type":
 "string", "maxLength":63 } } }, "additionalProperties": false },
 "UrlCategory": { "title":"UrlCategory", "type": "object",
 "properties": { "URLCategoryNames": { "title":"Urlcategorynames",
 "type": "array", "items": { "type": "string", "maxLength":128 } },
 "Feeds": { "title":"フィード", "type": "array", "items": { "type":
 "string", "maxLength":63 } } }, "additionalProperties": false },
 "CustomSecurityProfiles":{ "description":"カスタム セキュリティ プロファ
イル オブジェクト", "type": "object", "properties": { "FileBlocking":
 { "$ref": "#/definitions/FileBlocking" } }, "additionalProperties":
 false }, "FileBlocking":{ "title":"FileBlocking", "type": "object",
 "properties": { "Direction": { "title":"指示", "default": "both",
 "enum": ["upload", "download", "both"], "type": "string" },
 "FileType": { "title":"FileType", "type": "string" }, "Description":
 { "title":"説明", "minLength":1, "maxLength":255, "type": "string" },
 "Action": { "title":"アクション", "default": "alert", "enum":
 ["alert", "block", "continue"], "type": "string" }, "AuditComment":
 { "title":"監査コメント", "type": "string" } }, "required":
 ["FileType"], "additionalProperties": false }, "SecurityObjects":
 { "description":"セキュリティ オブジェクト", "type": "object",
```



```
 "properties": { "PrefixLists": { "type": "array", "uniqueItems":
 false, "items": { "$ref": "#/definitions/PrefixList" } },
 "FqdnLists": { "type": "array", "uniqueItems": false, "items":
 { "$ref": "#/definitions/FqdnList" } }, "CustomUrlCategories":
 { "type": "array", "uniqueItems": false, "items": { "$ref":
 "#/definitions/CustomUrlCategory" } }, "IntelligentFeeds":
 { "type": "array", "uniqueItems": false, "items": { "$ref":
 "#/definitions/IntelligentFeed" } }, "CertificateObjects":
{ "type": "array", "uniqueItems": false, "items": { "$ref":
 "#/definitions/CertObject" } } }, "additionalProperties":
 false }, "PrefixList": { "title":"PrefixList", "description":"セ
キュリティ オブジェクトのプレフィックス リスト", "type": "object",
 "properties": { "Name": { "title":"Name", "minLength":1,
 "maxLength":58, "pattern": "^[a-zA-Z0-9-]+$", "type": "string" },
 "PrefixList": { "title":"Prefixlist", "type": "array", "items":
 { "type": "string" } }, "AuditComment": { "title":"監査コメ
ント", "maxLength":512, "type": "string" }, "Description":
 { "title":"説明", "maxLength":512, "type": "string" } }, "required":
 ["Name", "PrefixList"], "additionalProperties": false },
 "FqdnList":{ "title":"FqdnList", "type": "object", "properties":
 { "Name": { "title":"Name", "minLength":1, "maxLength":58,
 "pattern": "^[a-zA-Z0-9-]+$", "type": "string" }, "Description":
 { "title":"説明", "maxLength":512, "type": "string" }, "FqdnList":
 { "title":"Fqdnlist", "type": "array", "items": { "type":
 "string", "minLength":1, "maxLength":255, "pattern": "^[a-
zA-Z0-9._-]+$" } }, "AuditComment": { "title":"監査コメント",
 "maxLength":512, "type": "string" } }, "required": ["Name",
 "FqdnList"], "additionalProperties": false }, "CustomUrlCategory":
{ "title":"CustomURLCategory", "type": "object", "properties":
 { "URLTargets": { "title":"Urltargets", "type": "array",
 "items": { "type": "string", "minLength":1, "maxLength":255 } },
 "Name": { "title":"Name", "minLength":1, "maxLength":58,
 "pattern": "^[a-zA-Z0-9-]+$", "type": "string" }, "Description":
 { "title":"説明", "minLength":1, "maxLength":255, "type":
 "string" }, "Action": { "title":"Action", "type": "string",
 "default": "none", "enum": ["none", "allow", "alert", "block"] },
 "AuditComment": { "title":"監査コメント", "type": "string" } },
 "required": ["URLTargets"], "additionalProperties": false },
 "IntelligentFeed":{ "title":"IntelligentFeed", "type": "object",
 "properties": { "Name": { "title":"Name", "minLength":1,
 "maxLength":63, "pattern": "^[a-zA-Z0-9-]+$", "type": "string" },
 "Description": { "title":"説明", "maxLength":512, "type":
 "string" }, "Certificate": { "title":"証明書", "type": "string" },
 "FeedURL": { "title":"Feedurl", "minLength":1, "maxLength":255,
 "pattern": "^(http|https)://.+$", "type": "string" }, "Type":
 { "title":"Type", "enum": ["IP_LIST", "URL_LIST"], "type":
 "string" }, "Frequency": { "title":"Frequency", "enum":
 ["HOURLY", "DAILY"], "type": "string" }, "Time": { "title":"時
間", "default":3, "minimum":0, "maximum":23, "type": "integer" },
 "AuditComment": { "title":"監査コメント", "maxLength":512, "type":
 "string" } }, "required": ["Name", "FeedURL", "Type", "Frequency"],
 "additionalProperties": false }, "CertObject":{ "title":"Certificate
 Object", "type": "object", "properties": { "Name": { "title":"Name",
 "minLength":1, "maxLength":63, "pattern": "^[a-zA-Z0-9-]+
$", "type": "string" }, "Description": { "title":"説明",
```



```
 "maxLength":512, "type": "string" }, "CertificateSignerArn":
 { "title":"Certificatesignerarn", "type": "string" },
 "CertificateSelfSigned": { "title":"Certificateselfsigned",
 "default": false, "type": "boolean" }, "AuditComment":
 { "title":"監査コメント", "maxLength":512, "type": "string" } },
 "required": ["Name"], "additionalProperties": false } },
 "properties": { "RuleStackName": { "description":"ルール スタック
名", "minLength":1, "maxLength":128, "pattern": "^[a-zA-Z0-9-]+
$", "type": "string" }, "RuleStack": { "$ref": "#/definitions/
RuleStack" }, "RuleList": { "description": "list of rules",
 "type": "array", "uniqueItems": false, "items": { "$ref": "#/
definitions/Rule" } }, "SecurityObjects": { "$ref": "#/definitions/
SecurityObjects" }, "CustomSecurityProfiles": { "$ref": "#/
definitions/CustomSecurityProfiles" } }, "additionalProperties":
 false, "required": [ "RuleStackName" ], "createOnlyProperties":
 [ "/properties/RuleStackName" ], "primaryIdentifier": [ "/
properties/RuleStackName" ], "handlers": { "create": { "permissions":
 [ "execute-api:Invoke" ] }, "read": { "permissions": [ "execute-
api:Invoke" ] }, "update": { "permissions": [ "execute-
api:Invoke" ] }, "delete": { "permissions": [ "execute-
api:Invoke" ] } } }
```


Cloud NGFW のクロスアカウントロール CFT 権限

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 には、AWS アカウントに関連付けられた情報とリソースにアクセスするためのアクセス許可が必要です。AWS アカウントをオンボードすると、アクセス許可を有効にするのに役立つ CloudFormation テンプレート（CFT）が提供されます。CFT をデプロイすると、AWS アカウントにクロスアカウント IAM ロールが作成されます。この IAM ロールは、エンドポイントの作成と管理、ログ記録の宛先へのログの送信、およびトラフィック復号化のための AWS シークレットマネージャ での証明書へのアクセスに必要な VPC 情報の読み取りに必要なアクセス許可を Cloud NGFW に付与します。

エンドポイント設定

クロスアカウント IAM ロールには、VPC リソースに関する情報を読み取るためのアクセス許可が必要であり、AWS 環境で NGFW エンドポイントを設定できます。

```
{ "Sid":"Cloud NGFW に VPC リソースの読み込みを許可する",
 "Effect":"Allow", "Action": [ # 最初の 4 つのアクセス許可
は、最低限必要な "ec2:DescribeVpcs", "ec2:DescribeSubnets",
 "ec2:DescribeAvailabilityZones "ec2:DescribeVpcEndpoints",
 "Resource": "*" }
```

エンドポイントの作成

（任意）AWS アカウントで NGFW エンドポイントを作成および管理するように Cloud NGFW を設定できます。アクセス許可を設定しない場合は、NGFW を展開した後に NGFW エンドポイントを手動で作成する必要があります。

```
{ "Sid":"Cloud NGFW に NGFW エンドポイントの管理を許可する",
 "Effect":"Allow", "Action": [ "ec2:deleleVpcEndpoints"
 "ec2:CreateVpcEndpoints" ], "Resource": "*" }
```

ロギングとメトリック管理

（任意）クロスアカウントロールには、ログ記録とメトリックの管理に必要なアクセス許可が含まれます。テンプレートはロギング宛先を作成しません。代わりに、指定されたログ記録先にアクセスするために必要なアクセス許可を提供します。テンプレートで指定するロギング宛先を作成する必要があります。

このテンプレートは、Cloudwatch名前空間とKinesis Date Firehoseの初期値**PaloAltoCloudNGFW**を提供します。テンプレートは、S3 バケットのデフォルト値を提供しません。デフォルト値を、AWS アカウントの対応するロギング宛先の値に置き換えることができます。

```
{ "Sid":"Cloud NGFW が 1 つの Cloudwatch 名前空間にアクセスできるようにする", "Effect":"Allow", "Resource": "*", "Action":
 "cloudwatch:PutMetricData", "Condition": { "StringEquals":
 { "cloudwatch:namespace":"PaloAltoCloudNGFW" } } }
{ "Sid":"Cloud NGFW のアクセスが 1 つの LogGroup にログを書き込めるようにする", "Action": [ "logs:CreateLogStream",
 "logs:DescribeLogStreams", "logs:PutLogEvents", ], "Effect":"Allow",
 "Resource": [ "arn:aws:logs:*:*:log-group:PaloAltoCloudNGFW"
 "arn:aws:logs:*:*:log-group:PaloAltoCloudNGFW:log-stream:*" ], }
{ "Sid":"オプションで、Cloud NGFW が 1 つの S3 バケットにログを書き込めるようにする"、"Effect":"Allow", "Action": [ "s3:putObject" ], "Resource":
 [ # これは提案 #1 です - 名前は externalid に基づいてコーディングされます"arn:aws:s3:::<PaloAltoCloudNGFW-ExternalD>/*" # これは提案 #2 です - 名前は CFT で顧客によって提供されます。'arn:aws:s3:::${S3Bucket}/*' ] }{ "Sid":" 必要に応じて、Cloud NGFW がログをストリームに書き込めるようにする"、"Effect":"Allow", "Action": [ "firehose:putRecordBatch" ],
 "Resource": [ "arn:aws:kinesis:region:account:deliveryStream/PaloAltoCloudNGFW*" ], }
```

復号

（任意）クロスアカウントロールには、Cloud NGFW が AWS アカウントのシークレットマネージャから証明書を取得し、それを使用して NGFW を通過するトラフィックを復号化する権限が含まれています。これらのアクセス許可は、アクセス用のタグを指定することによって、属性ベースのアクセス制御（ABAC）メカニズムを使用します。これらのアクセス許可はオプションであり、テンプレートのデプロイ時に設定しないことを選択できます。

```
{ "Sid":"Cloud NGFW が証明書を取得できるようにする", "Effect":"Allow",
 "Action": [ "secretsmanager:GetSecretValue" ], "Resource":
 "*", "Condition": { "StringEquals": { "aws:ResourceTag/PaloAltoCloudNGFW": "true" } } }
```

アカウントのモニタリング

（オプション）オンボーディング済みのAWSアカウントの既存のCloudFormationテンプレート（CFT）に、アカウント監視権限を追加できます。

```
{ "Version":"2012-10-17", "Statement": [ { "Action":
 [ "ec2:DescribeVpcs", "ec2:DescribeNetworkInterfaces",
 "ec2:DescribeSecurityGroups", "ec2:DescribeInstances",
 "ec2:DescribeVpcEndpoints", "ec2:DescribeSubnets",
 "ec2:DescribeManagedPrefixLists",
 "elasticloadbalancing:DescribeLoadBalancers",
 "elasticloadbalancing:DescribeTags" ], "Resource": "*",
 "Effect":"Allow" }, { "Action":
 [ "ec2:GetManagedPrefixListAssociations",
 "ec2:GetManagedPrefixListEntries" ], "Resource":
 [ "arn:aws:ec2:*:*:prefix-list/*" ], "Effect":"Allow" } ] }
```