paloalto TECHDOCS

Cloud NGFW for Azure

1.0

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

May 31, 2024

Table of Contents

Cloud NGFW for Azure の使用を開始する

AzureネイティブISVサービスであるPalo Alto NetworksのCloud Next-Generation Firewallは、Microsoft Azureプラットフォーム上でPalo Alto Networksのフルマネージドクラウドネイティブサービスとして提供されるMLベースの次世代ファイアウォール（NGFW）です。このデプロイメントモデルは、Palo Alto NGFW の機能と使いやすさを兼ね備えています。Cloud NGFW サービスは、Palo Alto Networks の App-ID および URL フィルタリングテクノロジーを使用して、高度なアプリケーションの可視性とアクセス制御を提供します。クラウドで提供されるセキュリティサービスと脅威防止シグネチャを通じて、脅威の防止と検出を提供します。

Cloud NGFW for Azure

Cloud NGFWは、クラウドネイティブサービスとして提供される機械学習（ML）次世代ファイアウォールです。Cloud NGFWを使用すると、複数のアプリケーションをクラウド速度で安全に実行でき、真のクラウドネイティブエクスペリエンスで拡張できます。Cloud NGFWは、クラス最高のネットワークセキュリティと使いやすさを兼ね備え、フルマネージドのクラウドネイティブサービスを提供します。Palo Alto Networksの脅威防止機能をクラウドプロバイダーに拡張するとともに、クラウドプロバイダーのさまざまなサービスにネイティブに統合されています。Cloud NGFW：

- インフラストラクチャの管理を最小限に抑えます。
- Webベースのゼロデイ脅威をリアルタイムで阻止します。
- アプリケーションが正当なWebベースのサービスに接続する際にセキュリティを確保します。
- 複数のアカウントにわたるシンプルで一貫性のあるファイアウォールポリシー管理により、ネイティブクラウドプロバイダーのエクスペリエンスをシンプルにします。
- API、ARMテンプレート、Terraformのサポートにより、エンドツーエンドのワークフローを自動化します。

Cloud NGFWは、特許取得済みのApp-IDトラフィック分類技術を使用して、Webベースの攻撃、脆弱性、エクスプロイト、および高度なファイルベースの攻撃を含むその他の既知の回避を阻止します。Cloud NGFW：

- Azure VNetやvWANのように、信頼の境界を越えてトラフィックを保護します。Cloud NGFWが提供するマネージドサービスは、攻撃者がリソースにアクセスするのをブロックし、データの窃取やコマンドアンドコントロール（C2）トラフィックを阻止します。無許可または東西の横方向の移動を阻止する目的で構築されています。
- 自動化を念頭に置いて設計されています。ルールスタック構成と自動化されたセキュリティプロファイルにより、Cloud NGFWは、ネットワークトラフィックに応じて拡張できる耐障害性の高いファイアウォールリソースの作成を簡素化する直感的なユーザーインターフェイスを使用して、ネットワークセキュリティ要件を簡単に満たすように設計されています。
- ネットワークトラフィックに応じて動的に拡張する自動化されたクラウドファイアウォールモデルを組み込み、GWLB（ゲートウェイ負荷分散）によって予測不可能なスループット要求を満たし、オンデマンドの高可用性と柔軟な拡張を実現します。必要な容量だけアクセスでき、必要に応じてスケールアップとスケールダウンが可能です。
- クラウドプロバイダーが管理するワークフローにセキュリティを統合します。クラウドプロバイダーと統合された初の次世代ファイアウォールであるCloud NGFWを使用すると、必要なルールスタックや自動化されたセキュリティプロファイルを設定する場合でも、長い導入サイクルを回避し、迅速に運用を開始できます。選択したクラウド プロバイダーが提供するセキュリティ モデルを活用しながら、プロバイダーのオンボーディング、モニタリング、ログ機能と統合できます。Cloud NGFWは、クラウドプロバイダーとの統合時に独自のメリットを

提供します。メンテナンス不要の自動スケーリングと高可用性を活用できます。この統合により、複数のクラウドプロバイダーアカウントで一貫したファイアウォールポリシー管理が可能になります。

Cloud NGFW for Azureを利用することができます。Cloud NGFW を使用すると、App-ID、URL カテゴリとジオロケーションに基づく URL フィルタリング、SSL/TLS 復号化などの NGFW コア機能にアクセスできます。

サポートされている機能

Cloud NGFW for Azureは、以下の機能を提供します。

- クラウドネイティブのデプロメールと管理。他のAzureサービスと同様に、Cloud NGFWリソースの0日目とN日目の運用をシームレスに管理しながら、Azure環境で次世代ファイアウォール機能を有効にします。権限については、[Azure role-based access control (RBAC) (ロールベースアクセス制御（RBAC）)]を使用してCloud NGFWリソースを制御します。
- 高度なアプリケーションの可視性と制御。Cloud NGFWは、App-IDとURLフィルタリング技術による
- 次世代脅威防御機能を使用した高度なアプリケーション認識とアクセス制御を提供します。クラウドで提供されるセキュリティサービスと脅威防止シグネチャを備えたPalo Alto NetworksのNGFW機能は、物理およびソフトウェアのインストールベース全体で提供されます。

Cloud NGFW for Azure モデル

Cloud NGFWは、Azure Native ISV Service (AzureネイティブISVサービス)です。このアプローチにより、Palo Alto Networksは、Azureサービスが提供するフックを使用して、Azure UIとAPIを通じてFWaaSをネイティブに活用することで、FWaaSを開発および管理できるようになります。Cloud NGFW for Azureは、Azure Marketplace (Azure マーケットプレイス)からアクセスできます。AzureのVNetやvWANには、パPalo Alto Networksが提供するNGFWのメリットをすべて活用できます。

Cloud NGFW コンポーネント

Cloud NGFW for Azureの主なコンポーネントは次のとおりです。

- **Cloud NGFW**。Cloud NGFWはマネージドAzureのリージョナルサービスで、Azureの主要地域の一部で利用できます。
- **NGFW**。Palo Alto Networksは、NGFWを顧客のvNETまたはvWANハブに関連するリソースとして使用します。耐障害性、拡張性、ライフサイクル管理を提供します。NGFW は、ユーザが指定した NGFW サブネット内のプライベート IP アドレスとして現れます。NGFW リソースを使用するには、プライベート IP アドレスを介してトラフィックを送信するように VNet UDR を更新します。
- **NGFW**ルールスタック。このリソースには、App-IDとURLフィルタリング、脅威防止機能を使用して、高度なアクセス制御を可能にする一連のセキュリティルール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ています。ローカルルールスタックを1つ以上のNGFWに関連付けることができます。

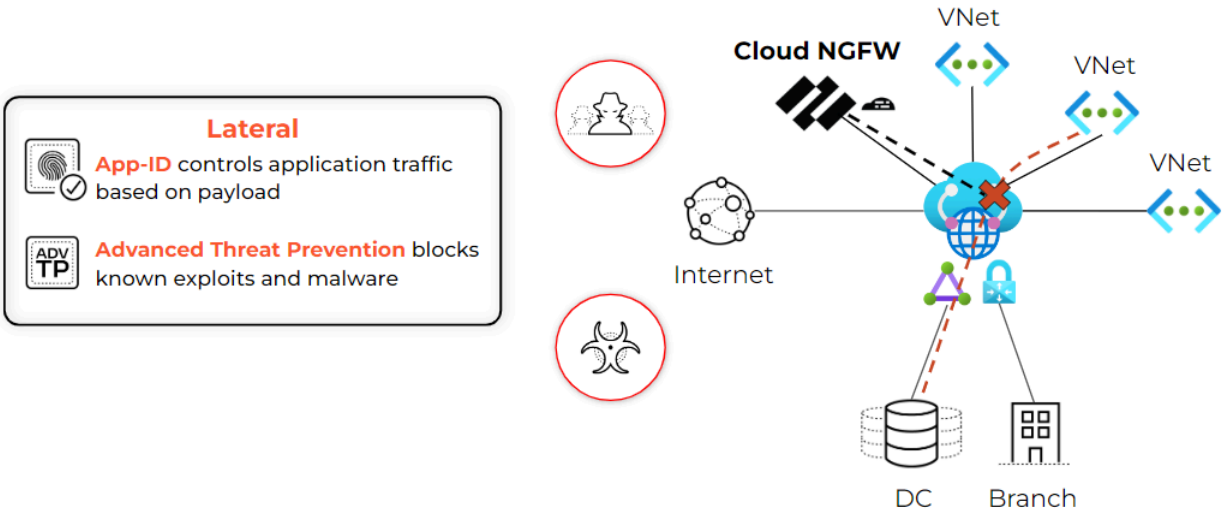
Cloud NGFWによるトラフィックの保護

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

インバウンドトラフィックとは、Azure リージョンの外部から発信され、サーバーやロードバランサーなどのアプリケーション VPC 内のリソースにバインドされているトラフィックのことです。Cloud NGFWは、Azure セキュリティグループによって許可されたインバウンドトラフィックにマルウェアや脆弱性が VNet に入るのを防ぐことができます。

アウトバウンドトラフィックとは、アプリケーション VNet 内で発信されるトラフィックのことで、Azure リージョン外の宛先にバインドされます。Cloud NGFW は、アプリケーション VNet 内のリソースが許可されたサービスと許可された URL に接続されるようにすることで、機密データや情報の流出を防ぎ、アウトバウンドトラフィックフローを保護します。

East-WestトラフィックはAzureリージョン内を移動します。具体的には、送信元と送信先の間のトラフィックが 2 つの異なるアプリケーション VNet または同じ VNet 内の 2 つの異なるサブネットにデプロイされます。Cloud NGFW は、Azure 環境内でのマルウェアの伝播を阻止できます。



Cloud NGFW コンポーネント

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

- **Cloud NGFW** リソース（または単に NGFW）はVNetもしくはvWANハブに関連付けられており、複数のアベイラビリティゾーンにまたがることができます。このリソースには、回復性、スケーラビリティ、およびライフサイクル管理が組み込まれています。
- ルールスタックは 、高度なアクセス制御（App-ID、URL フィルタリング）や脅威防止などの NGFW トラフィックフィルタリング動作を定義します。ルールスタックには、セキュリティルールのセットと、関連するオブジェクトおよびセキュリティプロファイルが含まれます。ルールスタックを使用するには、ルールスタックを1つ以上のNGFWリソースに関連付けます。

Cloud NGFW for Azure サポート対応リージョン

Azureリージョンは最大3つの可用性ゾーンをサポートし、各ゾーンに必要な割り当て済みVMは1つだけです。各ゾーン間のトラフィックはVNetを使用するため、クロスゾーンの課金は一切不要です。次の表は、特定のリージョンのゾーン可用性を示しています。

リージョン名	リージョンコード
オーストラリア東部	australiaeast
オーストラリア南東部	australiasoutheast
ブラジル南部	brazilsouth
カナダ中部	canadacentral
カナダ東部	canadaeast
中央インド	centralindia
米国中部	centralus
東アジア	eastasia
米国東部	eastus
米国東部 2	eastus2
フランス中部	francecentral
ドイツ西中部	germanywestcentral
イスラエル中央	israelcentral
イタリア北部 (ミラノ)	italynorth
東日本	japaneast
西日本	japanwest
北中部米国	northcentralus
北ヨーロッパ	northeurope

リージョン名	リージョンコード
ノルウェー東部	norwayeast
南アフリカ北部(ヨハネスブルグ)	southafricanorth
南中部米国	southcentralus
東南アジア	southeastasia
スウェーデン中央 (ガヴレ)	swedencentral
スイス北部	switzerlandnorth
UAE北部(ドバイ)	uaenorth
UK南部	uksouth
UK西部	ukwest
西ヨーロッパ	westeurope
米国中西部 (ワイオミング州)	westcentralus
米国西部	westus
米国西部 2	westus2
米国西部 3	westus3

Cloud NGFW for Azureの制限と割り当て

次の表は、Cloud NGFW テナントの制限とパフォーマンスデータを示したものです。特に明記されていない限り、これらの制限の引き上げをリクエストできます。

Cloud NGFW for Azure pricing estimator (Cloud NGFW for Azure価格見積もり)を使用して、*Cloud NGFW*サブスクリプションの*Azure*制限と割り当ての決定にお役立ていただけます。

ローカル ルールスタック ポリシー管理

氏名	**Cloud NGFW** テナントごとのデフォルト制限
テナント内のクラウド (Azure) アカウントの数	200

ネイティブポリシー管理(ルールスタック)

属性	**Cloud NGFW**リソースあたりの上限数
セキュリティ ルール	1,000
オブジェクト（FQDNリストおよびIPプレフィクスリスト）に対応	1,000
IPプレフィックスリストの数	1,000
すべてのFQDNリストにわたるFQDNオブジェクト	2,000
各IPプレフィクスリストのプレフィクス オブジェクト	2,500
カスタムURLカテゴリ	500
すべてのURLカテゴリのURL	25,000
インテリジェント フィード（事前定義された5つのフィードを含む）	30
すべてのフィードのIPアドレス	50,000

属性	Cloud NGFWリソースあたりの上限数
証明書オブジェクト	100

Panoramaポリシー管理

属性	Cloud NGFWリソースあたりの上限数*
Policy（ポリシー）	
セキュリティ ルール	10,000
復号化ルール	1,000
オブジェクト	
アドレスオブジェクト	10,000
アドレスグループ	1,000
メンバー/アドレス グループ	2,500
FQDNアドレス グループ	2,000
サービス オブジェクト	2,000
サービスグループ	500
メンバー/サービス グループ	500
EDL	
ドメイン システムあたりのDNSの最大数	500,000
システムあたりのIPの最大数	50,000
システムあたりの URL の最大数	100,000
カスタムリストの最大数	30

属性	**Cloud NGFW**リソースあたりの上限数*
URL フィルタリング	
許可リスト、ブロック リスト、およびカスタム カテゴリの合計エンティティ数	25,000
最大カスタム カテゴリ	500

#指定するポリシーとオブジェクトの制限は一次元最大値です。Palo Alto Networksは、ポリシーオーサリングの目的を確実に満たすために、お客様の環境内で追加のテストを行うことをお勧めします。

Azure PerformanceのためのCloud NGFW

次の表に、Cloud NGFW for Azureテナントのパフォーマンス情報を示します。

次の表に示す情報は、最大*40*インスタンスを想定しています。

属性	パフォーマンス メトリック
ファイアウォール スループット(App-ID有効)	最大スループット:100Gbps。インスタンスあたり2.92Gbps コールドスタート:8.55Gbps コールドスタート トラフィックでは、コンテンツ脅威検出が有効になります。コンテンツ脅威保護を使用しない場合、各ファイアウォール インスタンスはインスタンス タイプにより*3.00 Gbps*で制限されます。これは*Azure*の制限です。
脅威防止スループット	最大スループット:92 Gbps、1インスタンスあたり2.31 Gbps
暗号化トラフィックスループット	44 Gbps(コンテンツ脅威検出あり)、1インスタンスあたり1.11 Gbps

属性	パフォーマンス メトリック
	60 Gbps(コンテンツ脅威検出なし) 1インスタンスあたり1.52 Gbps

Cloud NGFW for Azureの価格

Cloud NGFW は、Azure Marketplace (Azure マーケットプレイス) で従量課金制（PAYG）サブスクリプションとして利用できます。このモデルでは、毎月使用した分だけ支払い、統合請求や組織の Microsoft Azure 使用量コミットメント (MACC) に対するクレジットなどの Azure Marketplace の特典も利用できます。

Cloud NGFW for Azure は、Azure Marketplace メータリング サービスを使用して使用量に応じて課金します。このモデルでは、すべてのCloud NGFW の展開時間、処理されるトラフィックの総量、使用されているセキュリティ機能に基づいて柔軟な価格設定をお求めいただけます。基本 **NGFW** リソース の課金は、次のディメンションと単位を使用して行われます。

寸法	価格	同等の**Cloud NGFW** クレジット
基本 NGFW リソースの使用	デプロイメント時間あたり 1.50 ドル	125
テナントあたりのトラフィック保護（最初15TB/月）	処理量 1GB あたり 0.065 ドル	5.416666667
テナントあたりの保護されたトラフィック（次回15TB/月）	処理量 1GB あたり 0.045 ドル	3.75
テナントあたりのトラフィック保護（30TB/月以上）	処理量 1GB あたり 0.030 ドル	2.5
アドオン	10 個あたり 0.12 ドル	各アドオンの具体的な請求情報については以下を参照してください。
Azureネットワーク料金	処理量 1GB あたり 0.01 ドル	

Cloud NGFW for Azure は、*Azure* ネットワーク料金ディメンションでエグレス使用量 *(*受信、送信、東西トラフィック*)* を課金し、その後、消費量の詳細が *Azure Marketplace* で共有されます。これらの料金は、*Azure* 仮想ネットワークの価格によって決まります。詳細については、「Virtual Network Pricing (仮想ネットワークの料金)」を参照してください。

高度な脅威保護、高度な URL フィルタリング、高度な Wildfire アドオン

これらのセキュリティ サービスの使用料は アドオン ディメンションを使用して課金されます。使用量は、次の表に示すように、$/時間および $/GB で測定されます。

保護されたトラフィック	時間あたりの料金	GB あたりの料金	Cloud NGFW クレジット相当
使用時間	$0.450	-	37.5
最初15 TB/月		$0.020	1.6
次回 15 TB/月		$0.014	1.125
30 TB/月以上		$0.009	0.75

WildFire と DNS セキュリティ アドオン

これらのセキュリティ サービスの使用料は アドオン ディメンションを使用して課金されます。使用量は、次の表に示すように、$/時間および $/GB で測定されます。

トラフィック保護	時間あたりの料金	GBあたりの料金	CloudNGFWクレジット相当
使用時間	$0.300	-	25
最初の15 TB/月		$0.013	1.083333333
次回15 TB/月		$0.009	0.75
30 TB/月以上		$0.006	0.5

Panorama 集中管理アドオン

このセキュリティ サービスの使用料は アドオン ディメンションを使用して課金されます。使用量は、次の表に示すように、$/時間および $/GB で測定されます。

トラフィック保護	時間あたりの料金	GBあたりの料金	クラウドNGFWクレジット相当
使用時間	$0.300	-	25

トラフィック保護	時間あたりの料金	GBあたりの料金	クラウドNGFWクレジット相当
最初15 TB/月		$0.003	0.2166666667
次回15TB/月		$0.002	0.15
30 TB/月以上		$0.001	0.1

Azureネットワーク料金

Palo Alto Networks は、顧客のサブスクリプションで Cloud NGFW リソースを公開するために使用されるネットワーク インターフェイスに関連する VNet ピアリング コストを負担します。これらのコストは Azure 仮想ネットワーク ピアリングの価格に基づいて顧客に転嫁されます。

クレジット使用量と使用状況の可視性

長期契約の Cloud NGFW 使用量に NGFW クレジットを使用できるようになりました。このクレジットは、テナント レベルで Azure クラウド環境全体のファイアウォール リソースに割り当てることができます。Cloud NGFW クレジットは、標準の Palo Alto Networks 販売チャネルとプロセスを通じて購入できます。

クレジットを購読するには、*PAYG* サブスクリプションが必要です。詳細については、営業チームにお問い合わせください。

次の点を考慮してください。

- クレジット プールには開始時間と終了時間があります。値の単位はクレジット/時間 (容量とも呼ばれます) です。
- 容量は、サービスと、時間の経過に伴って処理されるトラフィックの量 (例: 1 時間あたり) の組み合わせに基づいて計算されます。
- Azure の Cloud NGFW ファイアウォールに必要なクレジットを見積もるには、Azure 向け Cloud NGFW の価格見積もりツールを使用してください。見積もりツールは、入力されたリソース、サービス、トラフィックの量に応じて必要なクレジット数を提供します。クレジットのドル金額も表示されます。
- クレジットが購入され、請求されると、テナント レベルで Azure アカウントに追加されます。
  - テナント内に展開されたすべてのリソースは、同じプールのクレジットを消費します。
  - 使用量が割り当てられたクレジットの金額を超えた場合、超過分は PAYG (デフォルトの支払い方法) として請求されます。
  - これらの料金は、Azure の月額請求書に Marketplace パートナー料金として反映されます。

x 容量にサインアップした場合、 *x * 24 (*時間*) * 30 (*月の日数*)* のクレジット数がクレジット バケット内のアカウントに毎月追加されます。クレジットは、契約終了日までの月間使用量に応じてクレジット バケットから差し引かれます。販売チャネルを通じてクレジットの容量を増やすことができます。クレジットの有効期限が切れた後は、異なる容量と終了日でクレジットを更新できます。

クレジットの請求方法

クレジットを請求するには、Cloud NGFW 製品のシリアルナンバーと CSP (Palo Alto Network のカスタマー サポート ポータル) サポート アカウント ID が必要です。Cloud NGFW 製品のシリアルナンバーは、次の 2 つの方法で生成できます。

- ファイアウォールを作成します。
- ルールスタックを作成します。

その後、製品シリアルナンバー (テナントの CSP シリアルナンバー) を使用して 新しい CSP シリアル アカウントを作成する か、[新しいサポート リクエスト] セクションの *[Azure* テナントを新規または既存の *Palo Alto Networks* サポート アカウントに登録する*]* リンクを使用して既存の CSP アカウントをリンクすることができます。

テナント登録後、30日間は無料トライアルとしてご利用いただけます。30 日間の無料トライアルが終了する前に無料クレジットを利用した場合、追加の使用には PAYG レートで課金されます。

無料トライアル期間中に *Cloud NGFW* クレジットを追加すると、契約が直ちに開始され、無料トライアルが上書きされます。

クレジットの使用状況情報は、Azure Marketplace の **[New Support (**新しいサポート**)]** 要求セクションで確認できます。

月間平均使用量が購入したクレジットを超えた場合、超過分は PAYG 料金で請求されます。

クレジットは毎月 *1* 日にリセットされます。クレジットの有効期限が切れると、アカウントは *PAYG* レートに戻ります。未使用のクレジットは翌月に繰り越されません。Cloud NGFW for Azure の価格見積もりを 使用すると、*Cloud NGFW* テナントの *Azure* の価格を判断できます。

Cloud NGFW for Azure 無料トライアル

Azure ADテナントで最初のCloud NGFWまたはルールスタックを作成すると、自動的に30日間の無料トライアルに登録されます。無料トライアル期間は、Azureリソース用の最初のCloud NGFWの作成時に開始されます。

無料トライアルは、*Azure AD*テナントのすべてのサブスクリプションで有効です。

無料トライアル期間中は、以下の機能を無料でご利用いただけます。

- 2つのクラウドNGFWリソース
- 合計1TBのトラフィック検査(Cloud NGFWリソースあたり平均500GB)
- Panorama統合
- 脅威防御とURLフィルタリングクラウド配信セキュリティサービス（CDSS）対応

無料トライアル期間が終了するか、無料トライアルの制限を超えると、Azureマーケットプレイス「**Palo Alto Networks Cloud NGFW Pay-As-You-Go (**従量課金**)**」サブスクリプション リストに記載された条件に基づいて料金が発生します。無料トライアルを利用する際は、以下の点を考慮してください。

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

Cloud NGFW for Azure を始める

まず、**Resource Provider (**リソース プロバイダ**)**として Palo Alto Networks を登録します。Azure コンソールの **Settings (**設定**)**セクションで、 **Resource providers (**リソースプロバイダー**)**を選択します。Palo Alto Networks Cloud NGFWを検索し、 **PaloAltoNetworksCloudngfw**をクリックし、**Register (**登録**)**をクリックします。

次に、Azure ポータルにログインして、Cloud NGFW とそのポリシー ルールを作成します。NGFW を作成するときは、Azure VNet または vWAN と、セキュリティで保護する必要があるサブネットを指定します。NGFW を作成したら、ゲートウェイとサブネットのルート テーブルを更新して、すべてのトラフィックを検査のために NGFW にルーティングする必要があります。

AzureユーザーのCloud NGFWロールの管理

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。ここで提供される情報は、ファイアウォールの読み取り専用ユーザの作成など、カスタムロールの作成に役立ちます。既定では、Cloud NGFWは、サブスクリプション上のオーナーまたはコントリビュータロールがリソースプロバイダーに加入し、Cloud NGFWリソースを使用する必要がある。

*Cloud NGFW*ロールの管理については、「Assign Azure roles using the Azure portal (Azureポータルを使用したAzureロールの割り当て)」を参照してください。

シングルサインオンの統合

組織のSSOログインフローを、Azure Cloud NGFWサブスクリプションのPalo Alto Networks カスタマーサポートポータル（CSP）アカウントと統合できます。

サードパーティIDプロバイダ(IDP)を有効にする

カスタマーサポートポータル（CSP）でサードパーティの識別子プロバイダー（IDP）を有効にすると、独自の企業ログイン資格情報を使用してPalo Alto Networks のカスタマーサポートポータル（CSP）にログインできます。IDPはドメインレベルで設定するため、ドメイン内のメンバーは企業のSSOログイン資格情報を使用して複数のCSPアカウントにログインできます。ただし、ドメイン管理者アカウントは引き続きPalo Alto Networks のログイン資格情報を使用する必要があります。

ドメインのサードパーティIDPを有効にするには、次の手順を実行します。

- アカウントにサードパーティのIDPアクセスを設定するには、CSPでドメイン管理者ロールを持っている必要があります。
- Palo Alto Networks が提供するSSO構成の詳細を更新するには、識別子プロバイダーに対する管理者アクセス権が必要です。
- 検証にはドメイン以外の管理者アカウントが1つ必要です。

STEP 1 | Azureポータルにログインし、**[Active Directory (アクティブディレクトリ)]**を検索します。

STEP 2 | Active Directoryで、**[Enterprise Application (エンタープライズアプリケーション)]**を選択し、**[New Application (新規アプリケーション)]**を選択します。

STEP 3 | SSOアプリケーションの名前（panorama-ssoなど）を入力し、［**Create (作成)**］をクリックします。

STEP 4 | **[Create your own application (独自のアプリケーションを作成)]**ウィンドウで、**[Integrate any other application not found in the gallery (Non-gallery) (ギャラリーにない他のアプリケーションを統合する（非ギャラリー）)]**を選択します。

STEP 5 | 作成をクリックします。

STEP 6 | **[Manage (管理)]**セクションで、**[Single sign-on (シングルサインオン)]**をクリックします。

STEP 7 | **SAML**シングルサインオン方式を選択します。SAMLベースのサインオンページには、新しいSSOエンタープライズアプリケーションをPalo Alto Networks のCSPアカウントにリンクするのに必要な情報が含まれています。

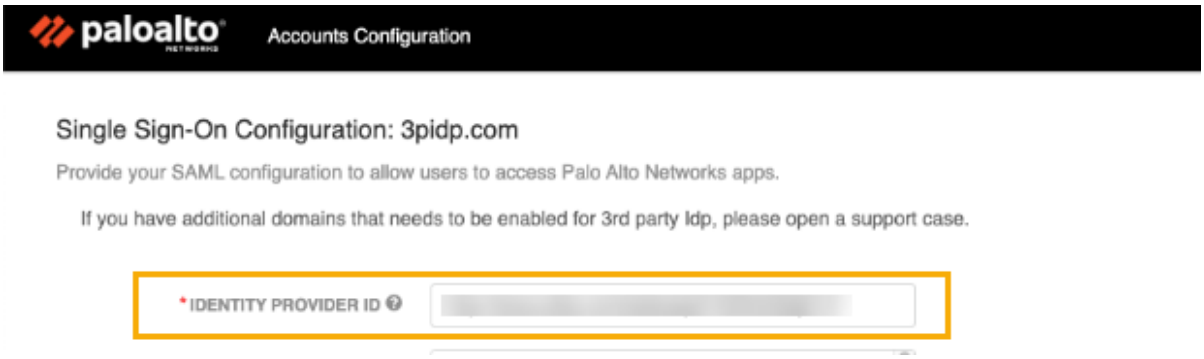
STEP 8 | SAMLベースのサインオンページで、下にスクロールして［**Set up ［your SSO application name (SSOアプリケーション名の設定)**］セクションのURLを見つけます。**Azure AD**識別子をコピーします。

STEP 9 | CSPにログインします。

STEP 10 | CSPで、**[Account Management (アカウントの管理)] > [Account Details (アカウントの詳細)]**を選択します。

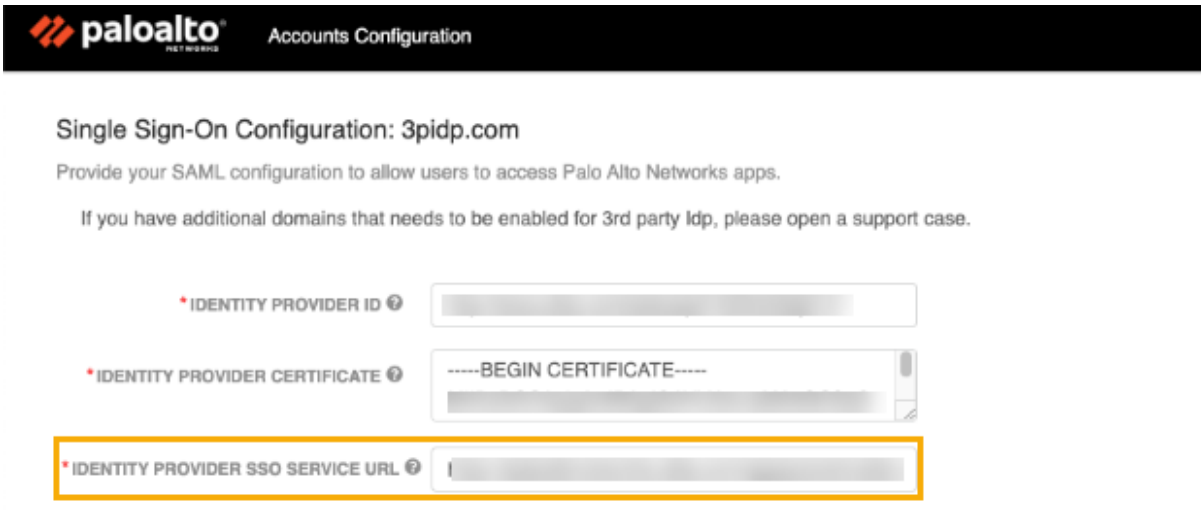
STEP 11 | **[SSO]**セクションで、［**View Single Sign-On settings for your domain (シングルサインオン設定の表示)**］をクリックします。

STEP 12 | **[Accounts Configuration (アカウント構成)]**で、手順8でコピーした**Azure AD**識別子を**[Identifier Provider ID (識別子プロバイダーID)]**フィールドにペーストします。



STEP 13 | Azureポータルの**SAML**ベースサインオン画面に戻ります。下にスクロールして、［**Set up ［your SSO application name ([SSOアプリケーション名]を設定する)**］セクションのURLを見つけます。ログイン**URL**をコピーします。

STEP 14 | CSPの**Accounts Configuration (アカウント設定)**ページに戻ります。コピーした［**Login URL (ログイン URL)**］（前のステップから）を［**Identity Provider SSO Service URL (識別子プロバイダー SSOサービス URL)**］フィールドに貼り付けます。

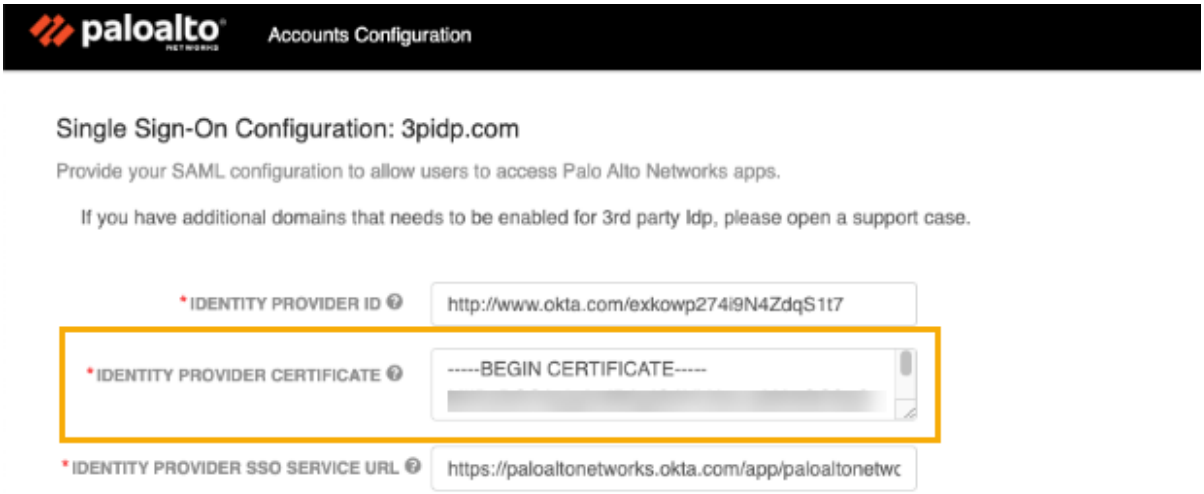


STEP 15 | 「識別子プロバイダ宛先**URL**」フィールドには同じ識別子プロバイダ**SSO**サービス**URL**アドレスを使用します。

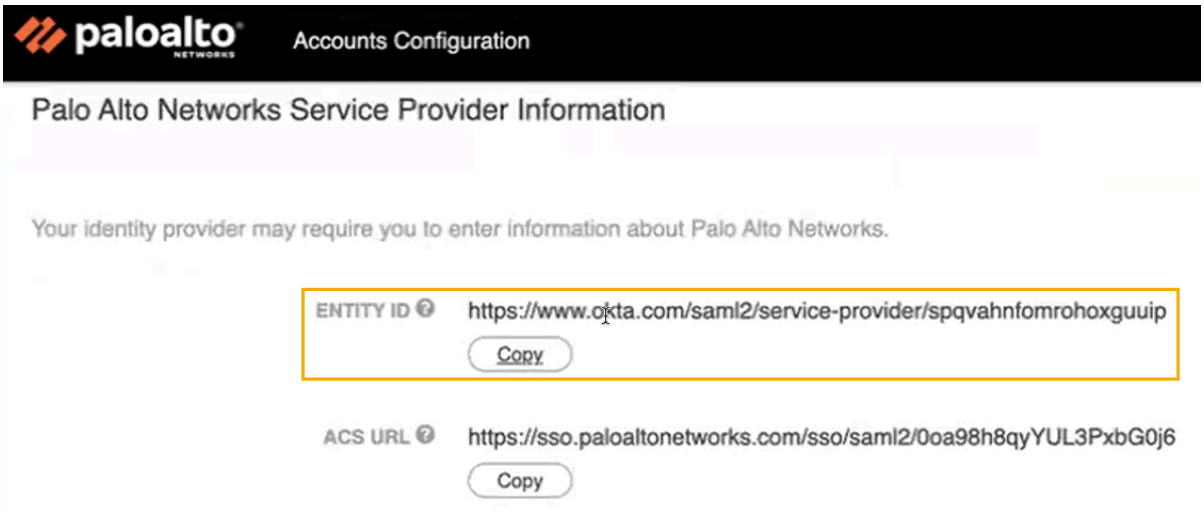
STEP 16 | Azureポータルの**SAML**ベースのサインオン画面に戻ります。下にスクロールして、**[SAML Certificates (SAML**証明書**)]**セクションを探します。

STEP 17 | [SAML証明書]セクションで、**[**証明書**(Base64)]**をダウンロードします。

STEP 18 | CSPの**[Account Management (**アカウント管理**)] > [Account Details (**アカウント詳細**)]**ページに戻ります。ダウンロードした証明書（前の手順で取得したもの）を識別子プロバイダ証明書フィールドに貼り付けます。



STEP 19 | **[Accounts Configuration (アカウント設定)]**ページが切り替わり、**Palo Alto Networks**サービスプロバイダ情報が表示されます。エンティティ**ID**のURLをコピーします。



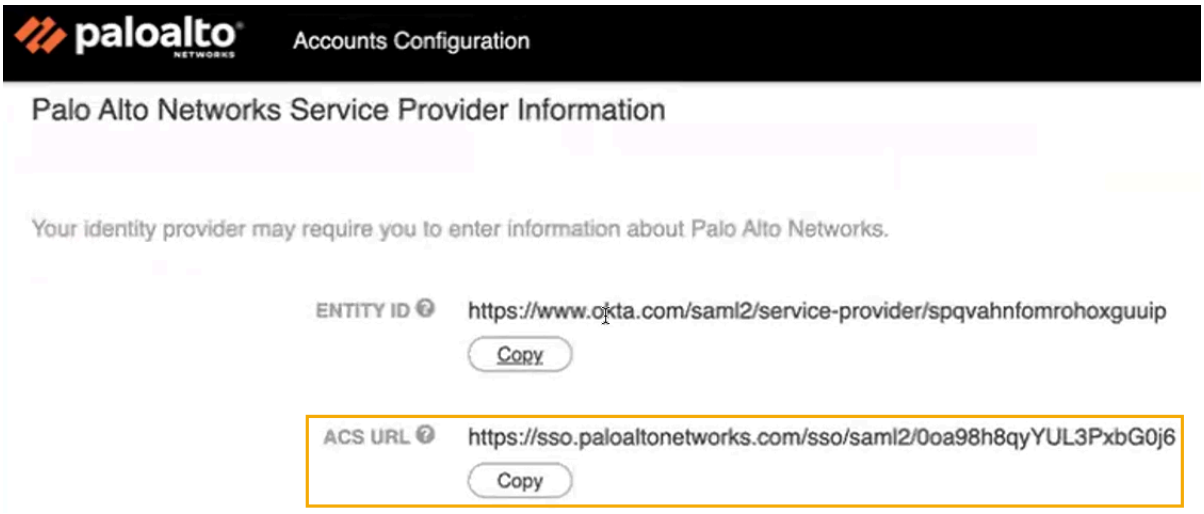
STEP 20 | Azureポータルの**SAML**ベースサインオン画面に戻ります。

STEP 21 | **[Basic SAML Configuration (SAML基本構成)]**画面で、**[Edit (編集)]**をクリックします。

STEP 22 | **[Identifier (Entity ID) (識別子(エンティティID))]**フィールドで、**[Add Identifier (識別子の追加)]**をクリックします。

STEP 23 | **[Identifier (識別子)]**フィールドにPalo Alto Networks の**Entity ID (エンティティID)**(手順21)を貼り付けます。

STEP 24 | CSPの**[Account Management (アカウント管理)] > [Account Details (アカウント詳細)]**ページに戻ります。**ACS URL** をコピーします。



STEP 25 | Azureポータルの**SAML**ベースサインオン画面に戻ります。

STEP 26 | **[Basic SAML Configuration (SAML基本構成)]**画面で、**[Edit (編集)]**をクリックします。

STEP 27 | ［**Reply URL** （**Assertion Consumer Service URL**）**(返信URL** （アサーション コンシューマ サービス**URL)**］ に ACS URL（手順 24 からコピー）を入力します。

STEP 28 | CSP**[Accounts Configuration (アカウント設定)]**ページに戻ります。トグルボタンを使用して、識別子プロバイダを有効にします。

STEP 29 | **Save**（保存）をクリックします。

STEP 30 | Azure ポータルに戻ります。SSOアプリケーションの**[Manage (管理)]**セクションで、**[Users and groups (ユーザーとグループ)]**をクリックします。

STEP 31 | ［**Add user/group (ユーザー/グループの追加)**］ オプションを使用して、指定した各ユーザの SSO ログインの使用を有効にします。

SSOログインの確認

IDプロバイダを有効にすると、すべてのユーザー（ドメイン管理者を除く）が強制的にSSOを使用してログインします。SSOログインが正しく設定されていることを確認するには、次の手順を実行します。

- ログインページでメールアドレスを指定します。ドメイン管理者のログイン資格情報は使用しないでください。
- 認証のためにIDPログインページにリダイレクトされていることを確認します。
- 認証後、Palo Alto Networks のカスタマーサポートポータルページが表示されます。

Azure Marketplaceを使用して、ドメイン以外のユーザー向けにSSOとCSPを統合する

Azure Marketplaceを使用してCSPアカウントにユーザーを統合するには、次の手順を実行します。

STEP 1 | Azureアカウントにログインします。

STEP 2 | [**Azure Services**]で[**Cloud NGFWs by Palo Alto Networks**]を選択します。

STEP 3 | CSPアカウントと統合するファイアウォールを選択します。

STEP 4 | **[Support + Troubleshooting(サポート+トラブルシューティング)]**セクションで、**[New Support Request(新しいサポート要求)]**をクリックします。[Palo Alto Networks Support]画面が表示され、テナント**ID**と製品シリアルナンバーが表示されます。

STEP 5 | **[Register User account(ユーザーアカウント登録)]**をクリックし、カスタマサポートポータルでケースを作成します。

STEP 6 | **[Create New Account / Use Existing Account (新規アカウント作成/既存アカウントの使用)]**ページで、メールアドレスを入力して認証手順を完了し、**[Next (次へ)]**をクリックします。

STEP 7 | **[Device Registration (デバイス登録)]**セクションで、ドロップダウンメニューから**[Cloud Marketplace (クラウドマーケットプレイス)]**サブスクリプションを選択します。たとえば、*Azure Cloud NGFW*が該当します。

STEP 8 | Azure Marketplaceサブスクリプションのテナント**ID**とシリアルナンバーを入力します。この情報は、手順4のPalo Alto Networksサポートページからコピーできます。**Next**（次へ）をクリックします。

STEP 9 | メールアドレスに送信された認証コードを入力します。**Next**（次へ）をクリックします。

STEP 10 | SSOを使用して認証すると、CSPログインページが表示されます。メールアドレスを入力し、**[Mext(次へ)]**をクリックします。

Azure Marketplaceを使用して、ドメインユーザー向けにSSOとCSPを統合する

Azure Marketplaceを使用してドメインユーザーとCSPアカウントを統合するには、Palo Alto Networks のログイン資格情報が必要です。

STEP 1 | ドメインユーザー資格情報を使用してAzureアカウントにログインします。

STEP 2 | [**Azure Services**]で[**Cloud NGFWs by Palo Alto Networks**]を選択します。

STEP 3 | CSPアカウントと統合するファイアウォールを選択します。

STEP 4 | **[Support + Troubleshooting(サポート+トラブルシューティング)]**セクションで、**[New Support Request(新しいサポート要求)]**をクリックします。[Palo Alto Networks Support (Palo Alto Networksサポート)]画面が表示され、テナント**ID**と製品シリアルナンバーが表示されます。

STEP 5 | **[Register User account(ユーザーアカウント登録)]**をクリックし、カスタマサポートポータルでケースを作成します。

STEP 6 | **[Create New Account / Use Existing Account (新規アカウント作成/既存アカウントの使用)]**ページで、メールアドレスを入力して認証手順を完了し、**[Next (次へ)]**をクリックします。

STEP 7 | **[Device Registration (デバイス登録)]**セクションで、ドロップダウンメニューから**[Cloud Marketplace (クラウドマーケットプレイス)]**サブスクリプションを選択します。たとえば、*Azure Cloud NGFW*が該当します。

STEP 8 | Azure Marketplaceサブスクリプションのテナント**ID**とシリアルナンバーを入力します。この情報は、手順4のPalo Alto Networksサポートページからコピーできます。**Next**（次へ）をクリックします。

STEP 9 | メールアドレスに送信された認証コードを入力します。**Next**（次へ）をクリックします。

STEP 10 | SSOを使用して認証すると、CSPログインページが表示されます。メールアドレスを入力し、**[Mext(次へ)]**をクリックします。

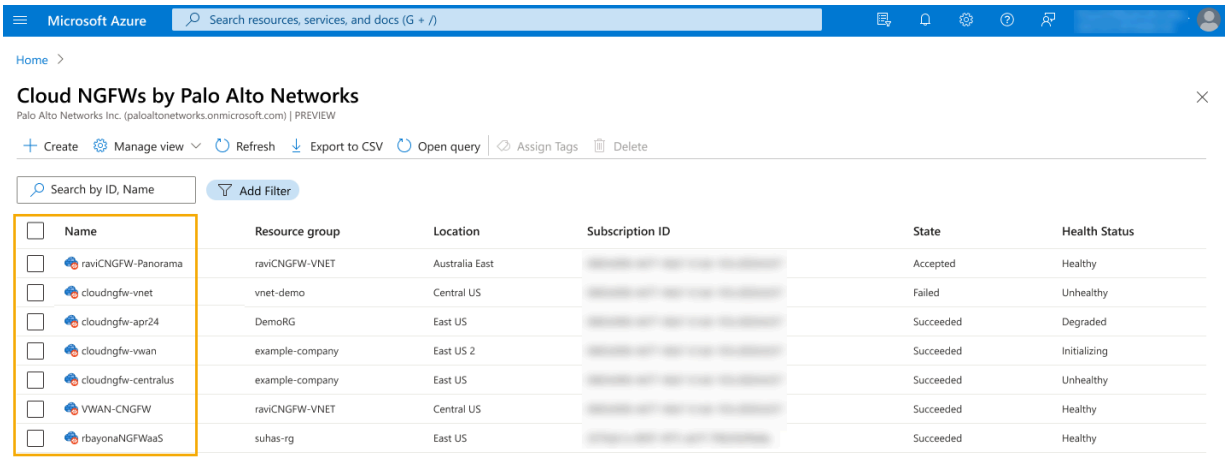
Cloud NGFWの状態を監視

Cloud NGFWは、Azureポータルを使用したヘルスモニタリングに対応しています。ファイアウォールの全体的なヘルスステータス、接続ステータス、およびファイアウォールの状態が正常でない原因の特定に使用できる診断情報を表示します。

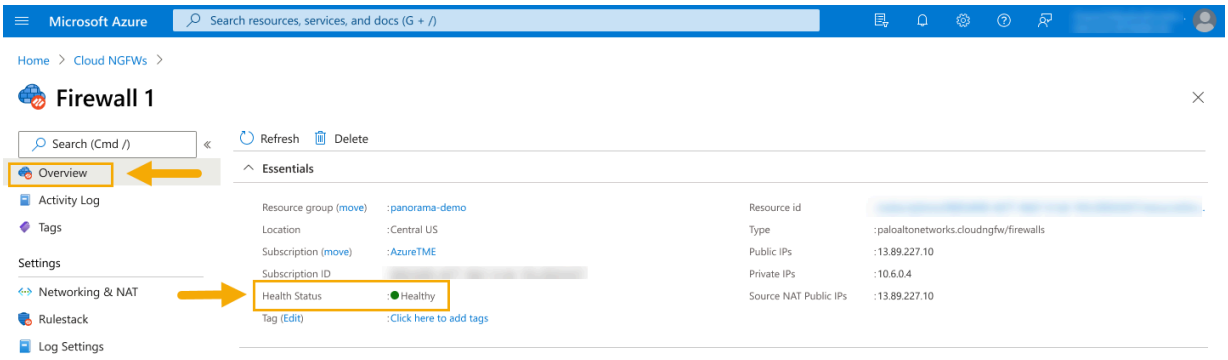
Cloud NGFWの状態を監視する方法：

STEP 1 | Azureポータルにログインし、**Cloud NGFW by Palo Alto Networks**を検索します。Azureに登録したCloud NGFWが表示されます。

STEP 2 | 監視するCloud NGFWを選択します。



STEP 3 | **[Overview (概要)]**ページで、**[Essentials (エッセンシャル)]**を展開します。Essentialsセクションには、選択したCloud NGFWの稼働状態が表示されます。



ヘルスモニタの状態

稼働状態は色分けされたアイコンで表示され、ネットワークセキュリティとクラウドセキュリティの両方で表示されます。

ネットワークセキュリティの稼働状態:

- 正常(緑のアイコン)。プライマリとセカンダリのPanoramaが、ネットワークセキュリティアプリケーション用のCloud NGFWリソースに接続されていることを示します。
- 機能低下(黄色いアイコン)。Cloud NGFWリソースのネットワークセキュリティが低下します。
- 不正常(赤いアイコン)。Cloud NGFWがPanorama仮想アプライアンスに接続できないことを示します。Cloud NGFW が Panorama に登録されていることを確認します。

クラウドセキュリティの稼働状態は、ファイアウォールの作成と更新に適用されます。

- 正常(緑のアイコン)。Cloud NGFWリソースに接続されたプライマリおよびセカンダリPanorama仮想アプライアンスの状態を示す、Cloud NGFWリソースに関連付けられたルールスタックの個々のステータスを示します。この情報は「関連するルールスタック」セクションに表示され、**[Connected (接続済み)]**または**[Not Connected (未接続)]**と表示されます。

- 機能低下(黄色いアイコン)。クラウドのセキュリティが低下している。
- 不正常(赤いアイコン)。Cloud NGFWルールスタックがどのインスタンスでも正常にコミットされなかったことを示します。問題を解決すると、ヘルスモニタが正常状態（緑のアイコン）に変わります。
- 初期化中青いアイコン)。Cloud NGFWリソースが初期化中であることを示します。

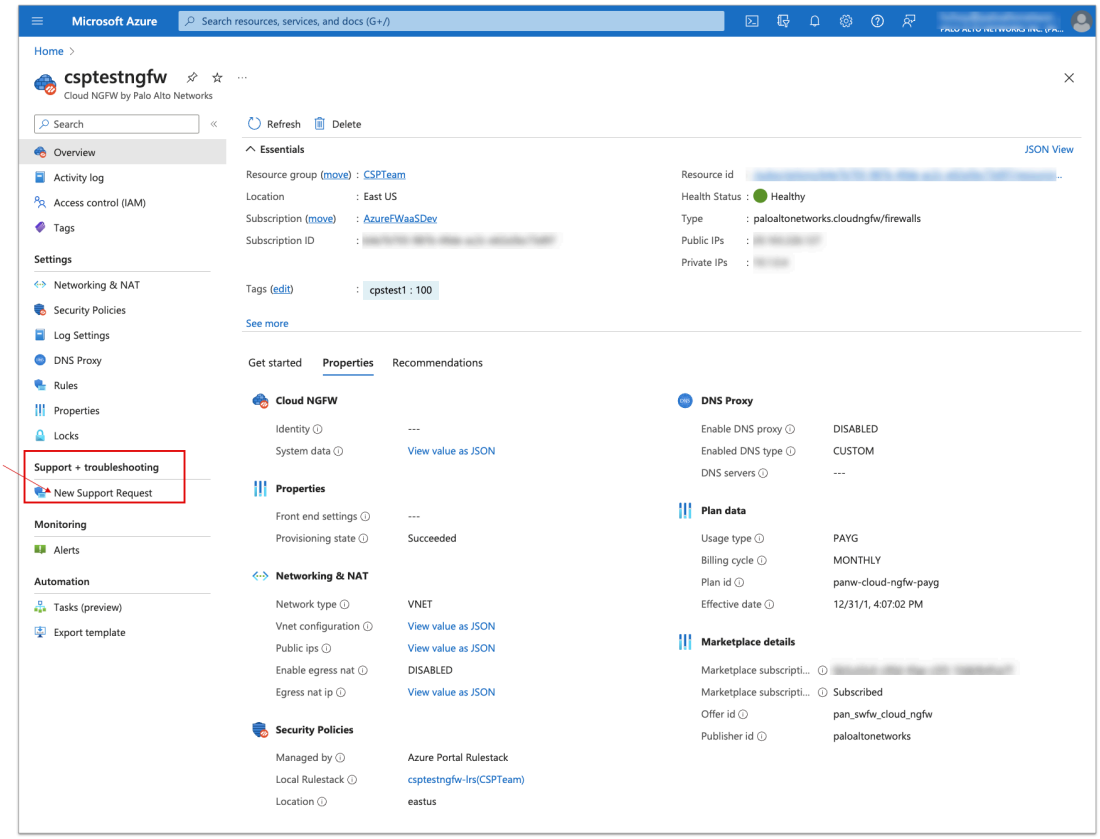
サポートケースの作成

Azureポータルを使用してサポートケースを作成するには、次の手順に従います。

STEP 1 | Azureポータルにログインします。

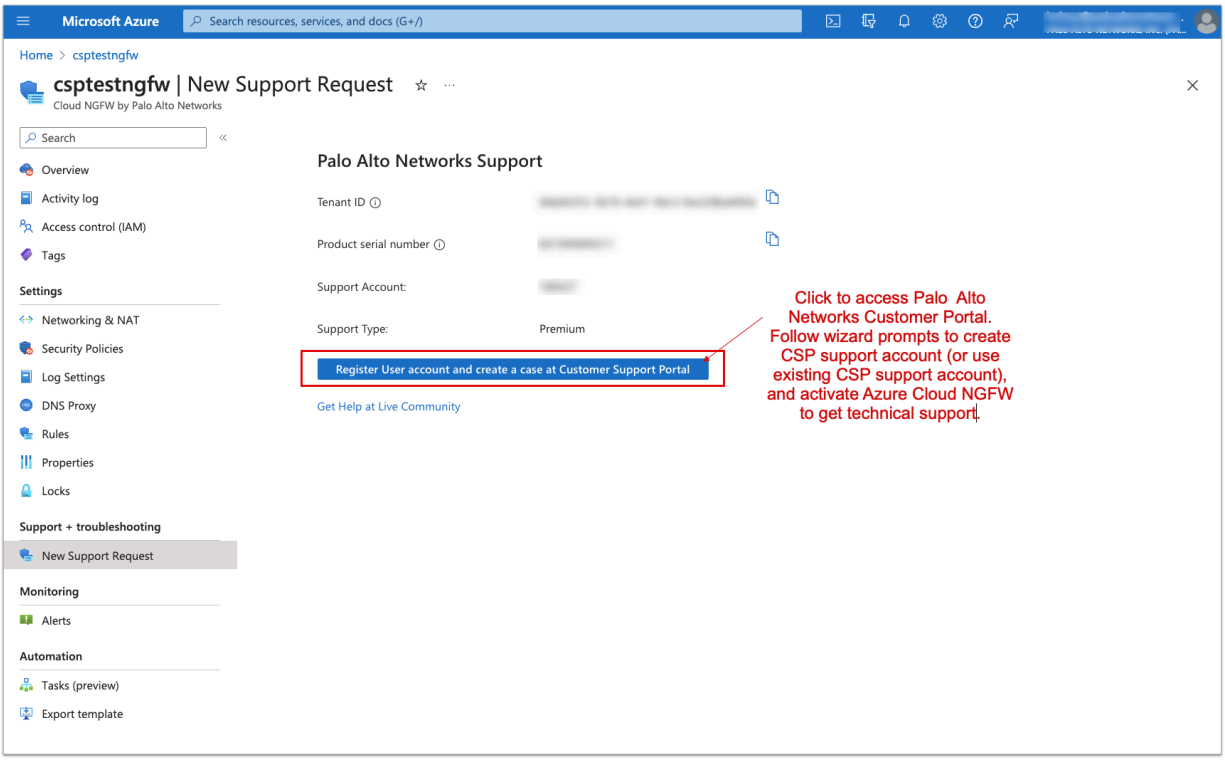
STEP 2 | **[Support + Troubleshooting(**サポート+トラブルシューティング**)]**セクションで、**[New Support Request(**新しいサポート要求**)]**をクリックします。

1.



STEP 3 | **[New Support request(新しいサポート要求)]**ページで**[Register User account(ユーザーアカウント登録)]**をクリックし、カスタマサポートポータルでケースを作成します。

2.



STEP 4 | 指示に従って、Palo Alto Networksのカスタマーサポートポータル（CSP）アカウントを作成します。すでにCSPアカウントを持っている場合は、既存のログイン資格情報を使用します。

Cloud NGFW for Azureをデプロイする

このセクションの情報は、Azureポータルを使用してCloud NGFWを導入する際の参考資料となります。Azureポータルを使用して、複数のAzureアカウントにCloud NGFWを展開できます。Azureポータルは、Cloud NGFWコンソールを使用してローカルルールスタックを作成します。

Azure VNetとAzure vWANの2つのデプロイメント方法がサポートされています。Azure vNETは、他のAzureリソース、インターネット、オンプレミスネットワークとの安全な通信を可能にします。Azure vWANは、ネットワーキング、セキュリティ、ルーティングの各機能を組み合わせて単一の運用インターフェイスを提供するネットワーキングサービスを表します。Azure環境にデプロイするには、Cloud NGFWコンソールとAzureポータルが必要です。

*vNET*または*vWAN*のスループットは*100Gbps*に制限されます。

- vNETにCloud NGFWをデプロイする
- vWANにCloud NGFWをデプロイする

vNETにCloud NGFWをデプロイする

Cloud NGFWは、vNETに2つのプライベートIPアドレス（パブリックとプライベート）として表示されます。ユーザー定義ルート（Cloud NGFWのプライベートIPアドレスをネクストホップとする）を使用して、トラフィックをCloud NGFWにリダイレクトし、パケット検査と脅威防止を行うことができます。Azure Cloud NGFW

は、Cloud NGFWと通信してルールスタックを追加します。Cloud NGFWはCloud NGFWリソースの使用状況を継続的に測定し、Azureサブスクリプションごとの使用状況記録をAzure測定サービスに送信します。このサービスは課金を担当します。

vNETにCloud NGFWを導入後、詳細については設定例のページを参照してください。

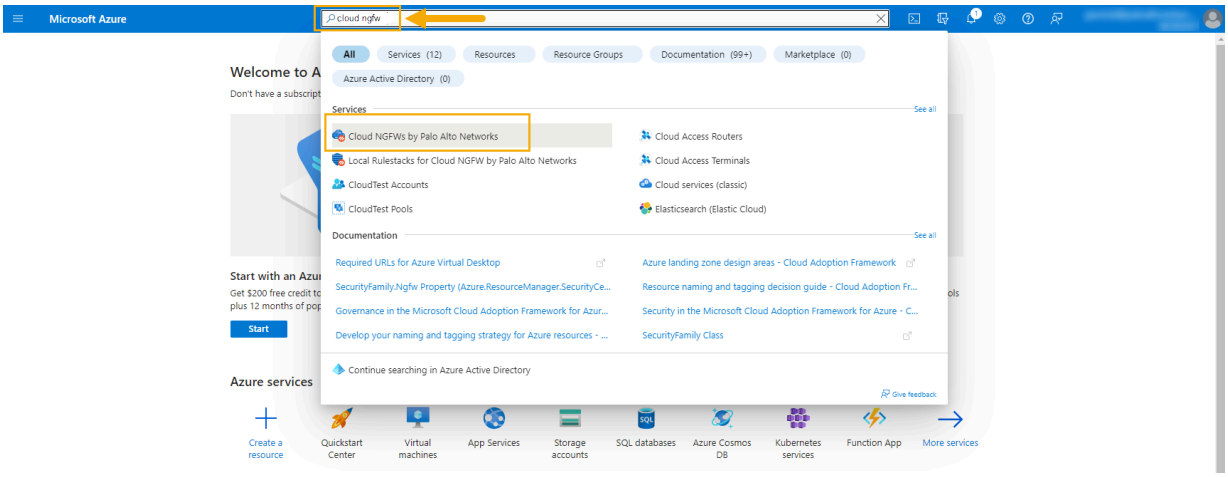
前提条件

vNETにCloud NGFWを導入するには、Azureサブスクリプションが必要です。このサブスクリプションにはオーナーまたはコントリビューターの役割が必要です。

既存の*vNETハブを使用してvNETにCloud NGFWを導入する場合、最小サイズは/25にする必要があります。最小サイズ/26のサブネットが2つ必要です。これらのサブネットは **PaloAltoNetworks.Cloudngfw/firewalls** サービスに委任する必要があります。*

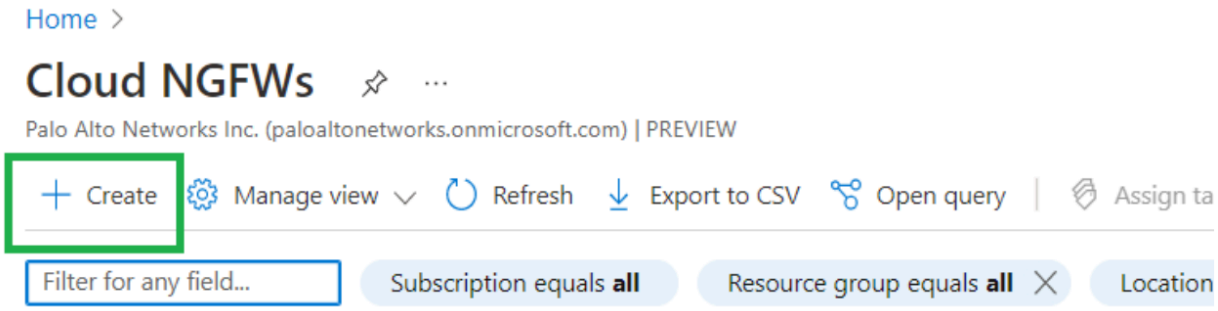
100Gbpsをサポートする導入の場合、合計80個の空きIPアドレスが必要です。 パブリック 用に40個、 プライベート用に40個のIPアドレスが使用されます。

STEP 1 | Azureポータルにログインし、**Cloud NGFW**を検索します。この検索では、Cloud NGFWサービス「**Cloud NGFW by Palo Alto Networks**」を表示します。



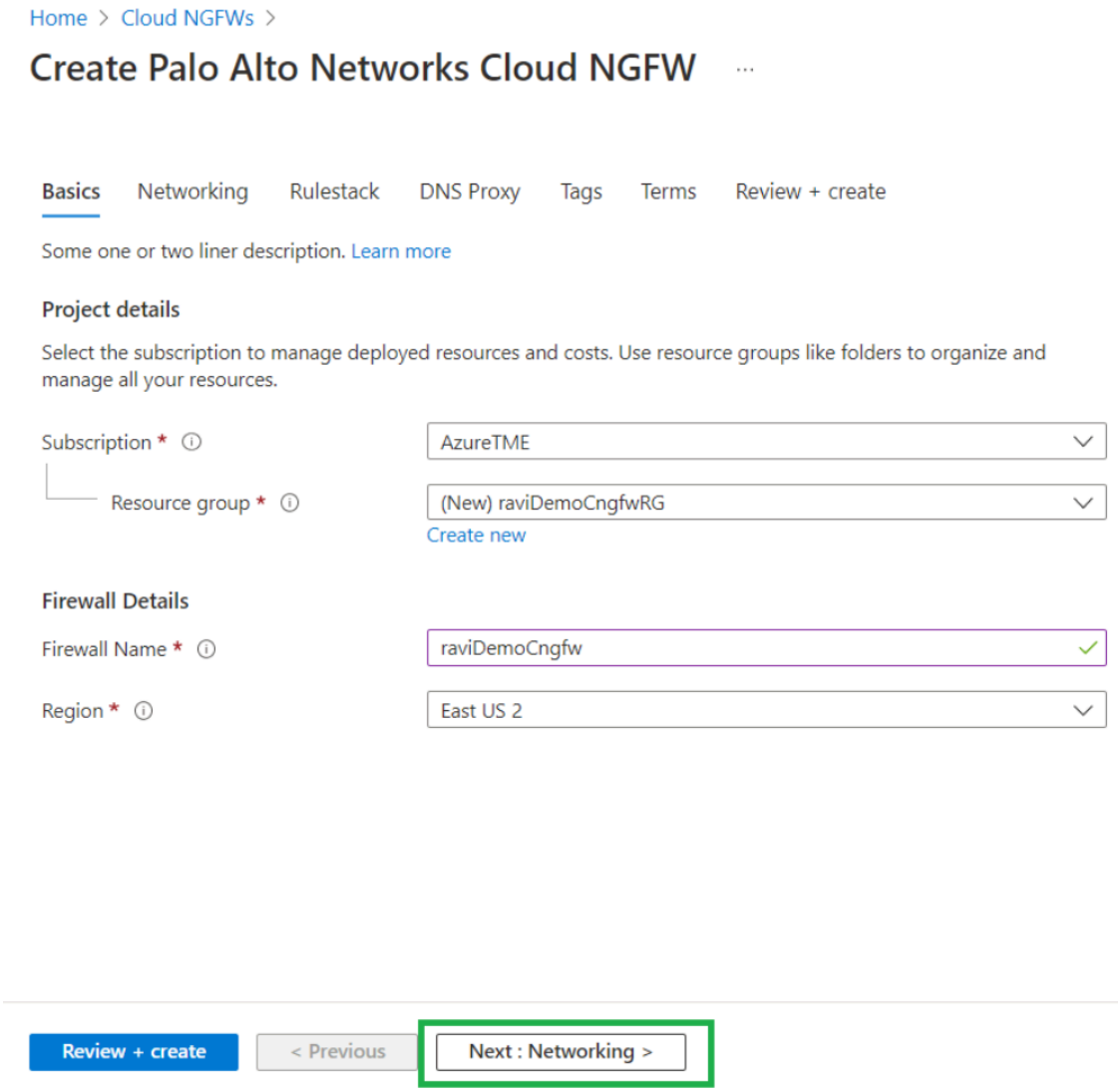
STEP 2 | ［**Cloud NGFWs**］をクリックして、Azure向けのPalo Alto Networks Cloud NGFWサービスの作成を開始します。

STEP 3 | Cloud NGFWリソースの待ち受け画面で、［**Create (作成)**］をクリックしてCloud NGFWリソースの作成を開始します。



サブスクリプションが以前に作成されている場合、ランディングページにはCloud NGFWリソースに関する情報が含まれています。

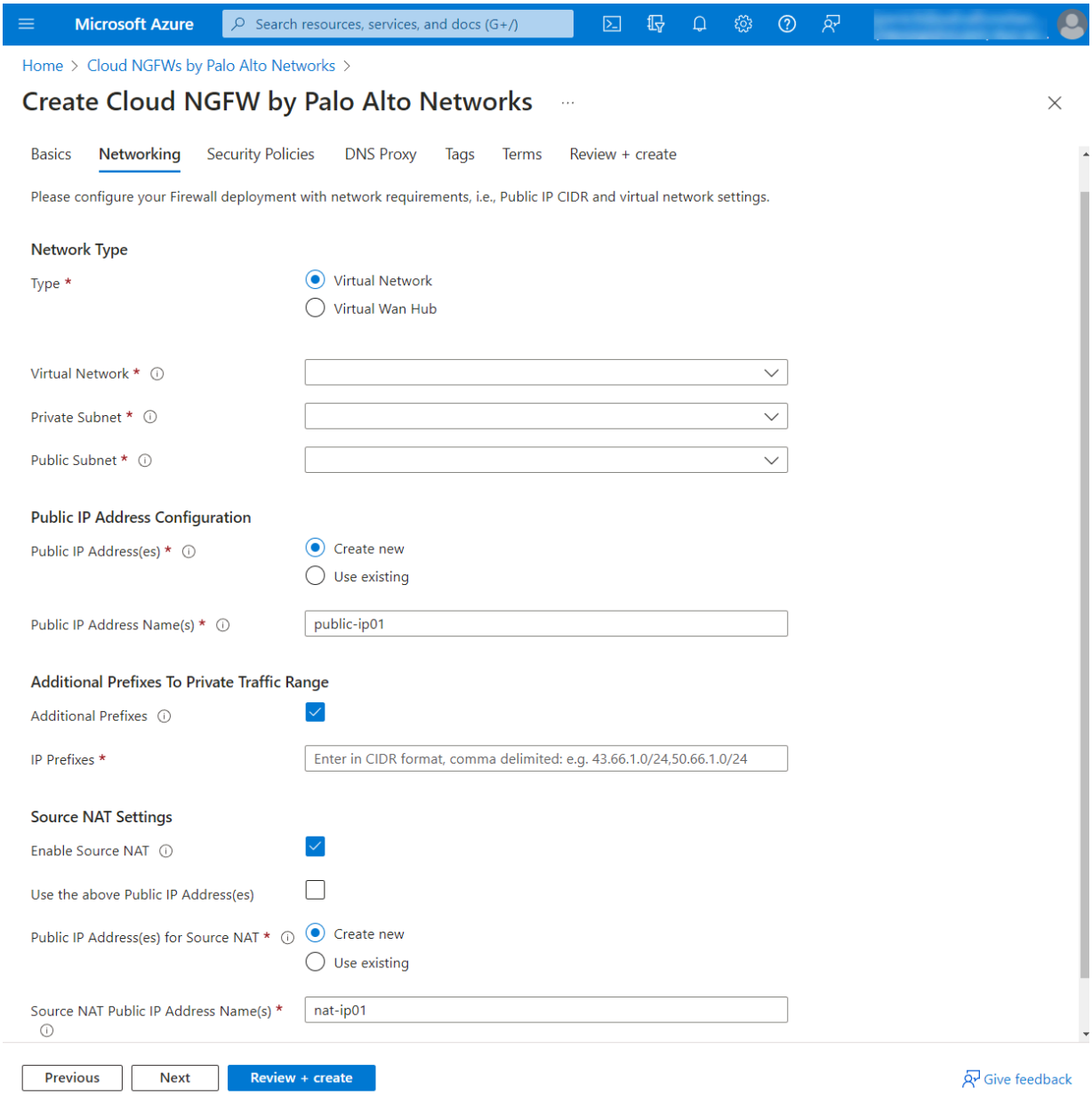
STEP 4 | **[Create (**作成**)]**をクリックすると、**[Create Palo Alto Networks Cloud NGFW (Palo Alto Networks Cloud NGFW**の作成**)]**画面が表示されます。



次の表の情報を使用して**[Basic (基本)]**情報を入力し、[**Next:Networking (次へ:**ネットワーク**)]**をクリックします。

項目	の意味
サブスクリプション	ログイン中に使用されたサブスクリプションに基づいて自動的に選択されます。
リソースグループ	既存のリソースグループのいずれかを使用するか、Cloud NGFWリソースが作成される新しいリソースグループを作成します([**Create New (**新規作成**)**]オプションを使用)。
ファイアウォール名	Cloud NGFWファイアウォールリソースの名前。  *Panorama*管理ファイアウォールの場合、ファイアウォール名にはすべて大文字を使用しないでください。
リージョン	Cloud NGFWがプロビジョニングされるリージョン。

STEP 5 | ［**Networking (**ネットワーク**)**］画面で、ファイアウォールの導入に関する情報を入力します。



［**Networking (**ネットワーク**)**］画面には、次の表のフィールドがあります。

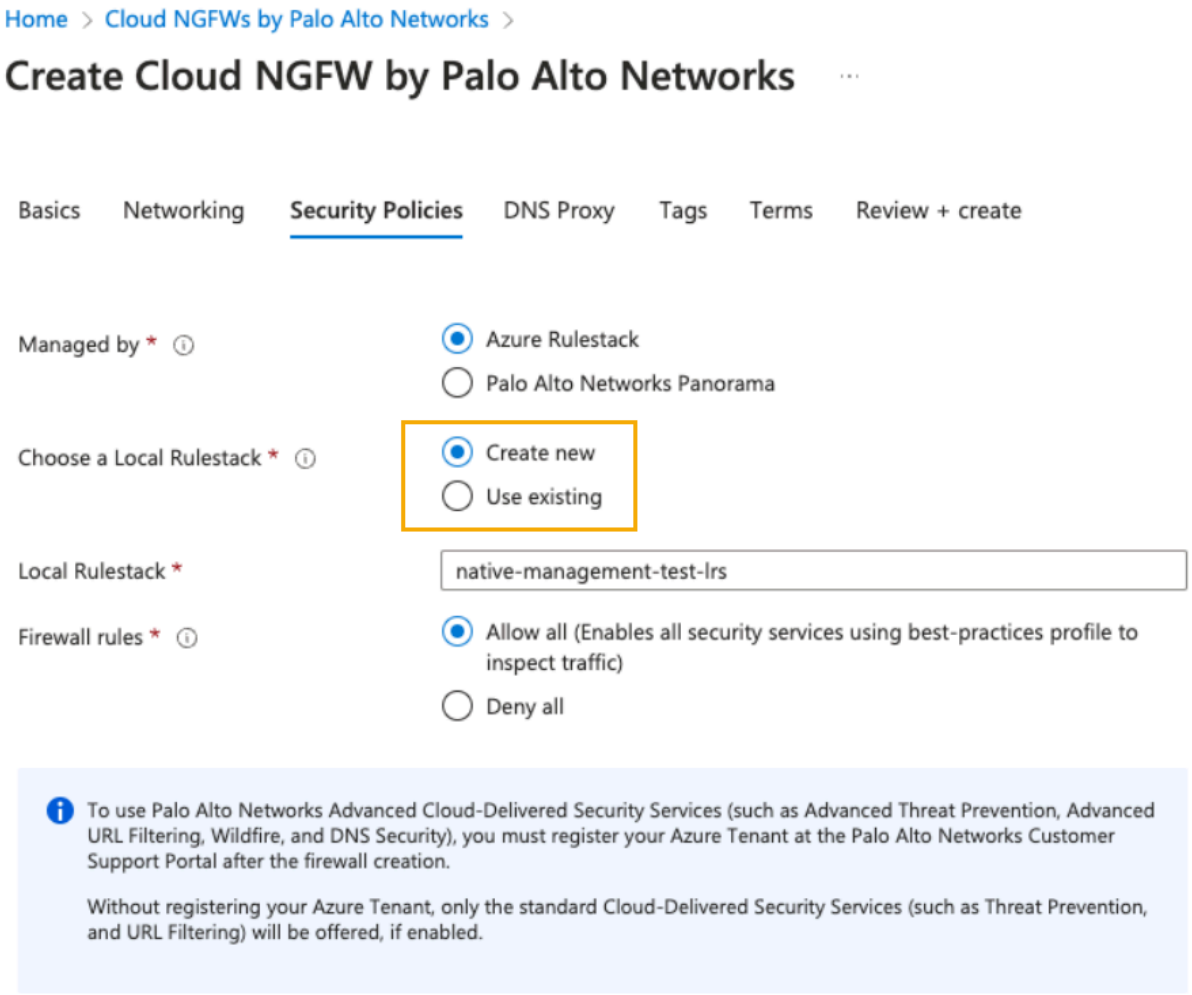
項目	の意味
タイプ	ログイン中に使用されたサブスクリプションに基づいて自動的に選択されます。
仮想ネットワーク	［**Virtual network (**仮想ネットワーク**)**］ を選択します。新しい仮想ネットワークを作成するか、既存の仮想ネットワークを選択します。
プライベートサブネット	プライベートサブネットを選択します。
パブリックサブネット	パブリックサブネットを選択します。
パブリックIPアドレスの設定	パブリック**IP**アドレスを指定します。**[Create new (**新規作成**)]**をクリックして新しいアドレスを確立するか、**[Use existing (**既存を使用**)]**をクリックして既存のアドレスを指定します。
プライベートトラフィック範囲への追加のプレフィクス	RFC 1918 で指定された範囲以外の追加のプライベート IP アドレス範囲をサポートする場合は、**[Additional Prefixs to Private Traffic Range (**プライベート トラフィック レンジへの追加のプリフィックス**)]** のオプションを使用します。このサポートにより、トラフィックをインターネットにルーティングすることなく、プライベートネットワークでパブリックIPアドレスブロックを使用できます。 ［**Additional Prefixes (**追加のプレフィックス**)**］チェックボックスをクリックします。CIDR形式でアドレスを入力します（例：40.0.0.0/24）。複数のアドレスを含めるには、カンマ区切りリストを使用します。 デフォルトでは、*RFC 1918* プレフィクスは自動的にプライベート トラフィック範囲に含まれます。組織がパブリック*IP*範囲を使用している場合は、それらの*IP*プレフィックスを明示的に指定します。これらのパブリック *IP* プレフィクスは個別に指定することも、集約として指定することもできます。

項目	の意味
	ファイアウォールの導入後に追加のプレフィクスを追加する方法については、「Edit an Existing Firewall to Add Additional Private Addresses for Non-RFC 1918 Support (RFC 1918 以外のサポート用の追加のプライベートアドレスを追加する既存のファイアウォールを編集する)」セクションを参照してください。
送信元 NAT の設定	インターネットに出るトラフィックで Network Address Translation（NAT； ネットワーク アドレス変換）を使用する場合は、送信元 **NAT** オプションを含めます。

STEP 6 | 「**Next:Security Policies (**次へ**:**セキュリティポリシー**)**」をクリックします。

STEP 7 | [**Security Policies (セキュリティポリシー)**]ページで、ローカルルールスタックを作成するか、既存のルールスタックを選択します。新しいルールスタックにはルールが含まれていません。Cloud NGFWリソースの導入後にセキュリティルールを定義できます。

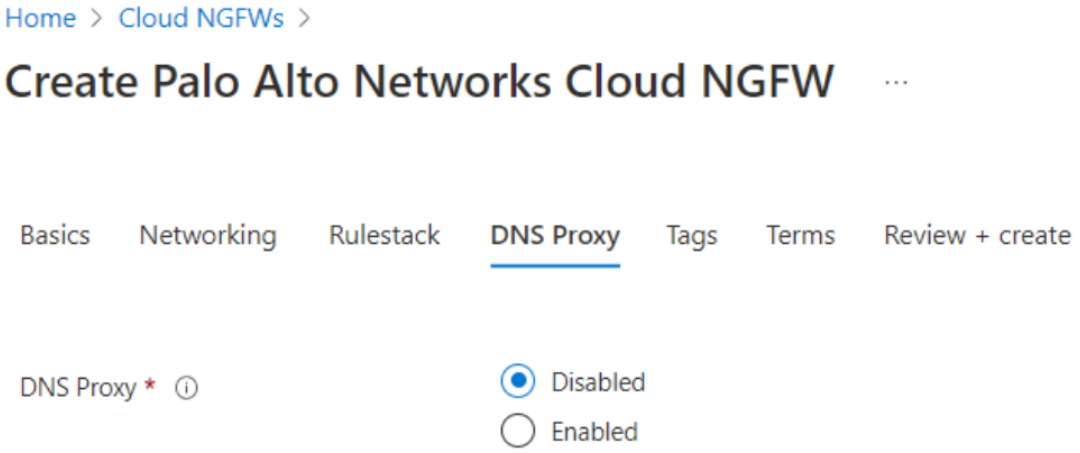
管理者は、ネイティブの*Azure*ルールスタックを使用してセキュリティポリシーを管理することも、*Palo Alto Networks Panorama*を使用してポリシーを管理することもできます。詳細については、「Link the Cloud NGFW to Palo Alto Networks Management (Cloud NGFW を Palo Alto Networks 管理にリンクする)」を参照してください。



*Palo Alto Networks*の高度なセキュリティサービス（高度な脅威防止や高度な*URL*フィルタリングなど）を使用する場合は、ファイアウォールの作成後にPalo Alto Networksカスタマーサポートポータルで*Azure*テナントを登録する必要があります。テナントの登録の詳細については、[Start with Cloud NGFW for Azure (Cloud NGFW for Azureを始める)]を参照してください。

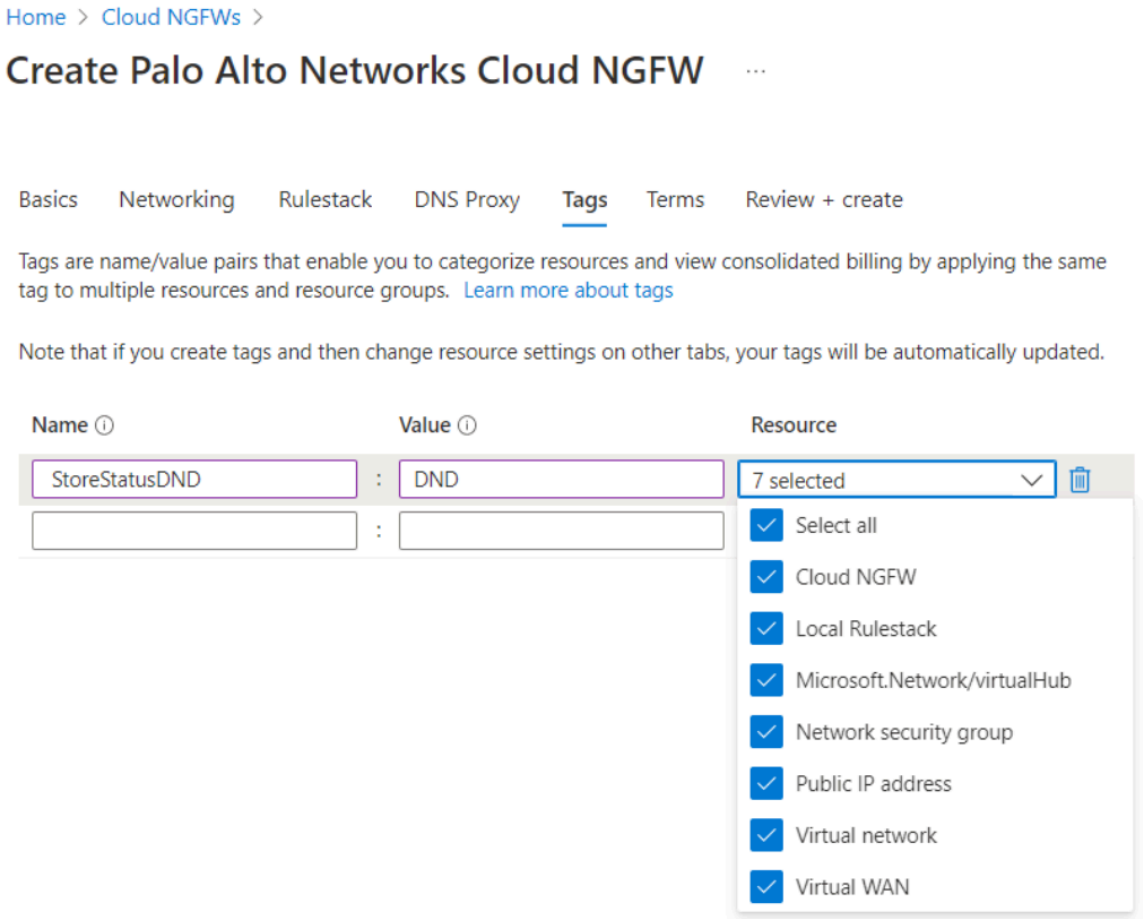
1.

STEP 8 | **NEXT (次へ)** をクリックします。**Cloud NGFW**リソースを**DNS**プロキシとして構成するための**DNS**プロキシ。vNETリソースのプロキシとして機能することで、すべてのDNSトラフィックを検査するようにCloud NGFWを設定できます。設定すると、DNSプロキシはDNSリクエストをデフォルトのAzure DNSサーバー、または指定したDNSサーバーに転送します。デフォルトでは、DNSプロキシは無効になっています。



STEP 9 | **[Next:Tags (次へ:タグ)]**をクリックして、Azure要件のタグを指定します。タグは、環境内の脆弱性を管理したり、Azureアカウントに関連する統合課金を表示したりするのに役立つ事

前定義されたラベルです。タグは、一元的に定義され、脆弱性やポリシー例外として設定できます。



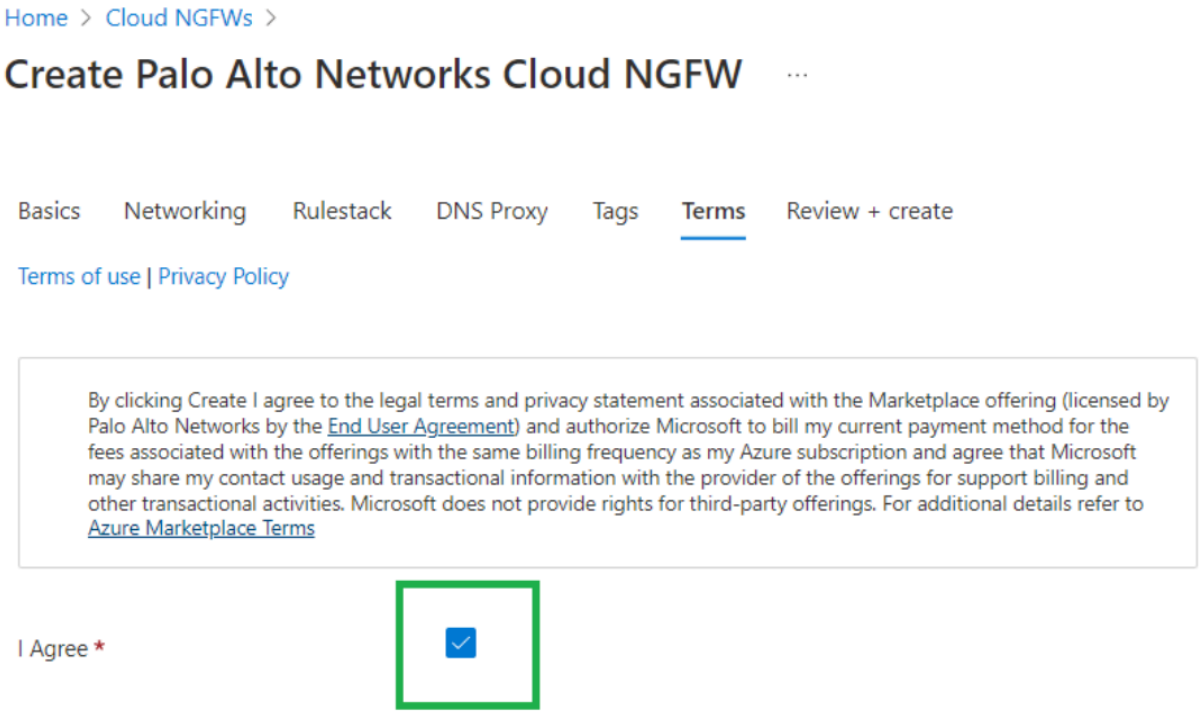
タグは次のように使用されます。

- 脆弱性ラベル。環境内の脆弱性を分類する便利な方法を提供します。
- ポリシーの例外。タグ付けされた脆弱性に特定の影響を与えるために、これらのルールを各自のルールに組み入れることができます。
- Azureアカウントの統合請求を表示します。

  タグは、複数のチームが同じ環境で作業する大規模なコンテナ展開がある場合に便利です。たとえば、様々な種類の脆弱性を処理する様々なチームがいる場合があります。その場合、タグを設定して、脆弱性に対する責任を定義できます。他の用途としては、脆弱性の修正ステータスを設定したり、近い将来修正できない既知の問題であれば無視される脆弱性とマークしたりすることができます。

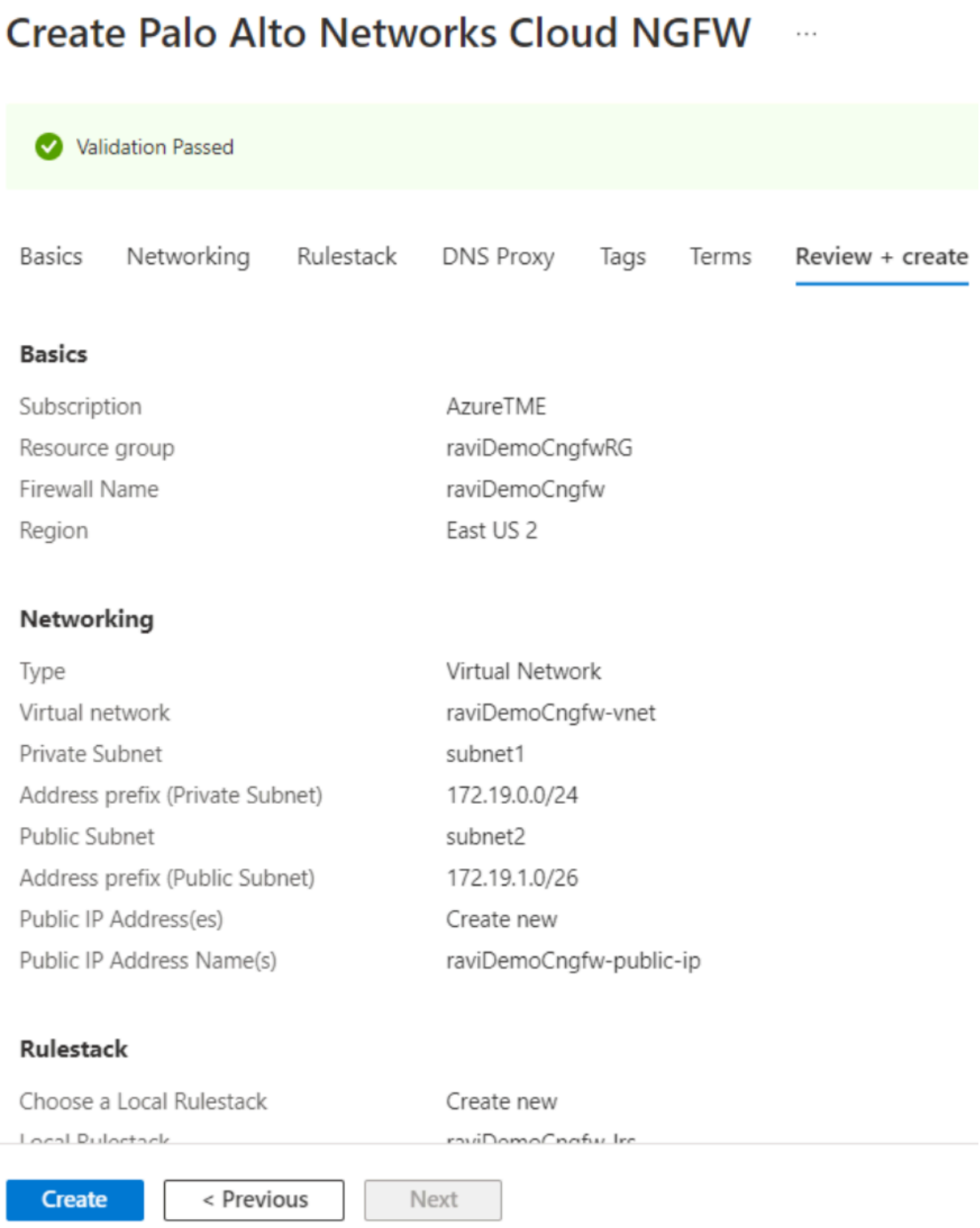
タグはいくつでも定義できます。*Azure*アカウントのタグの作成については、「Use tags to organize your Azure resources and management hierarchy (タグを使用してAzureリソースと管理階層を整理する)」を参照してください。

STEP 10 | **[Next:Terms (次へ:条件)]**をクリックし、デプロイメント条件に同意する



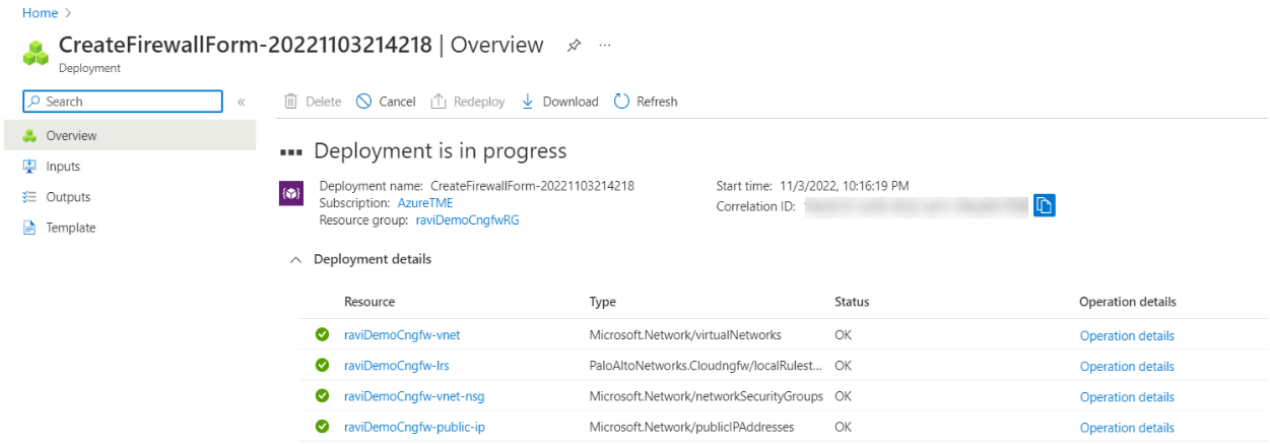
STEP 11 | **[Next:Review + create (次ページ：レビュー＋作成)]**をクリックして、Cloud NGFWリソースのAzureサブスクリプションの検証を確認します。リソースはまず検証され、次に作成され

ます。画面に**[Validation Passed (**検証に合格しました**)]**と表示されます。**[Create (**作成**)]**をクリックして、Cloud NGFW サービスをデプロイします。



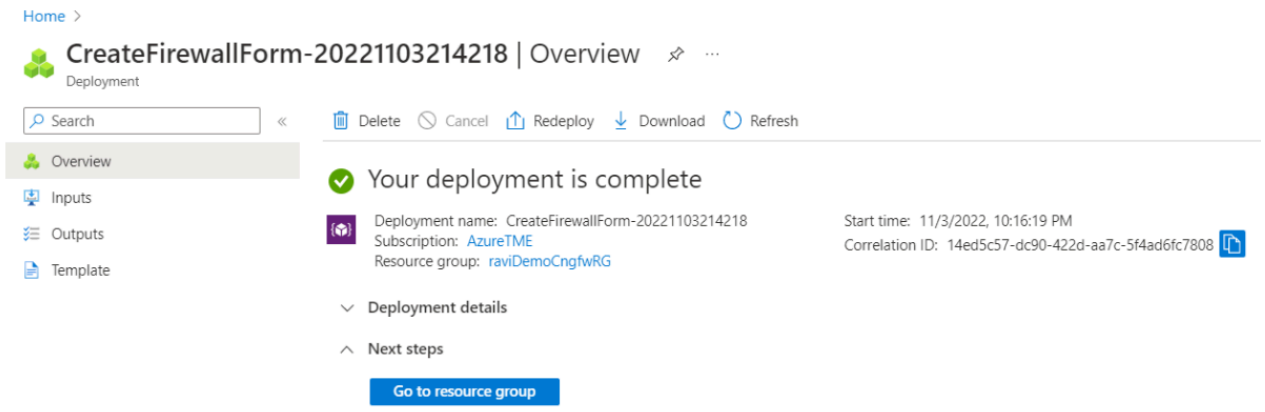
vNETへのCloud NGFWのデプロイメントを確認

Cloud NGFWサービスを作成すると、デプロイメントの進行状況が表示されます。

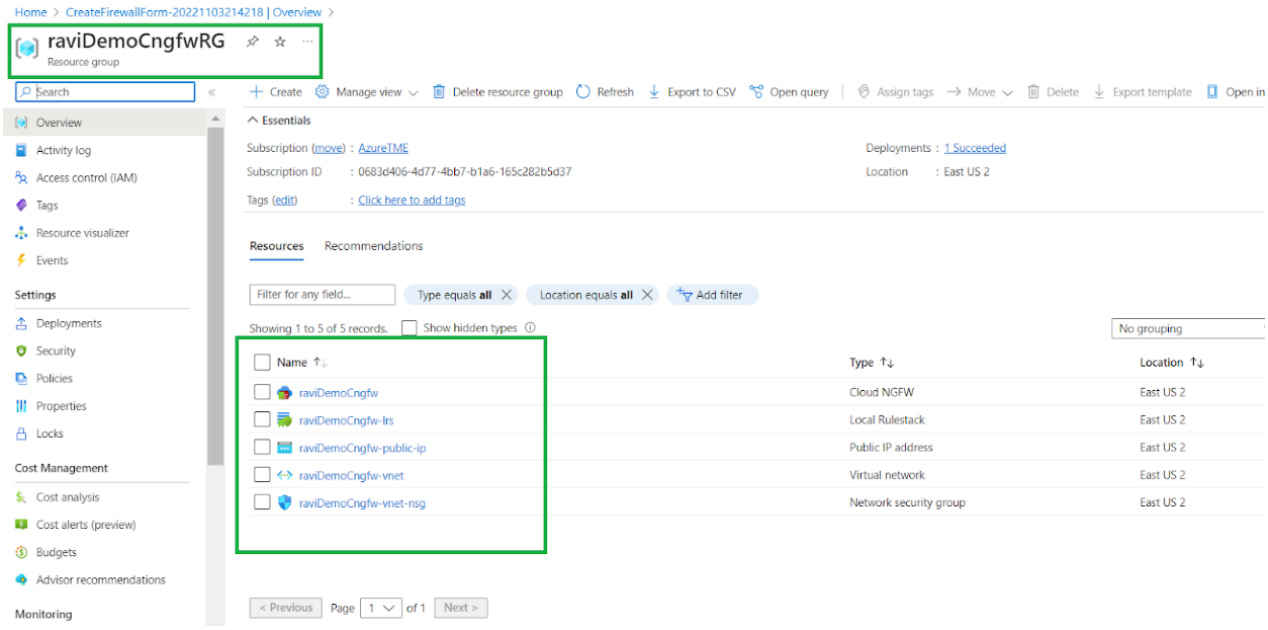


*Cloud NGFW*リソースの導入にかかる時間は約*30*分です。

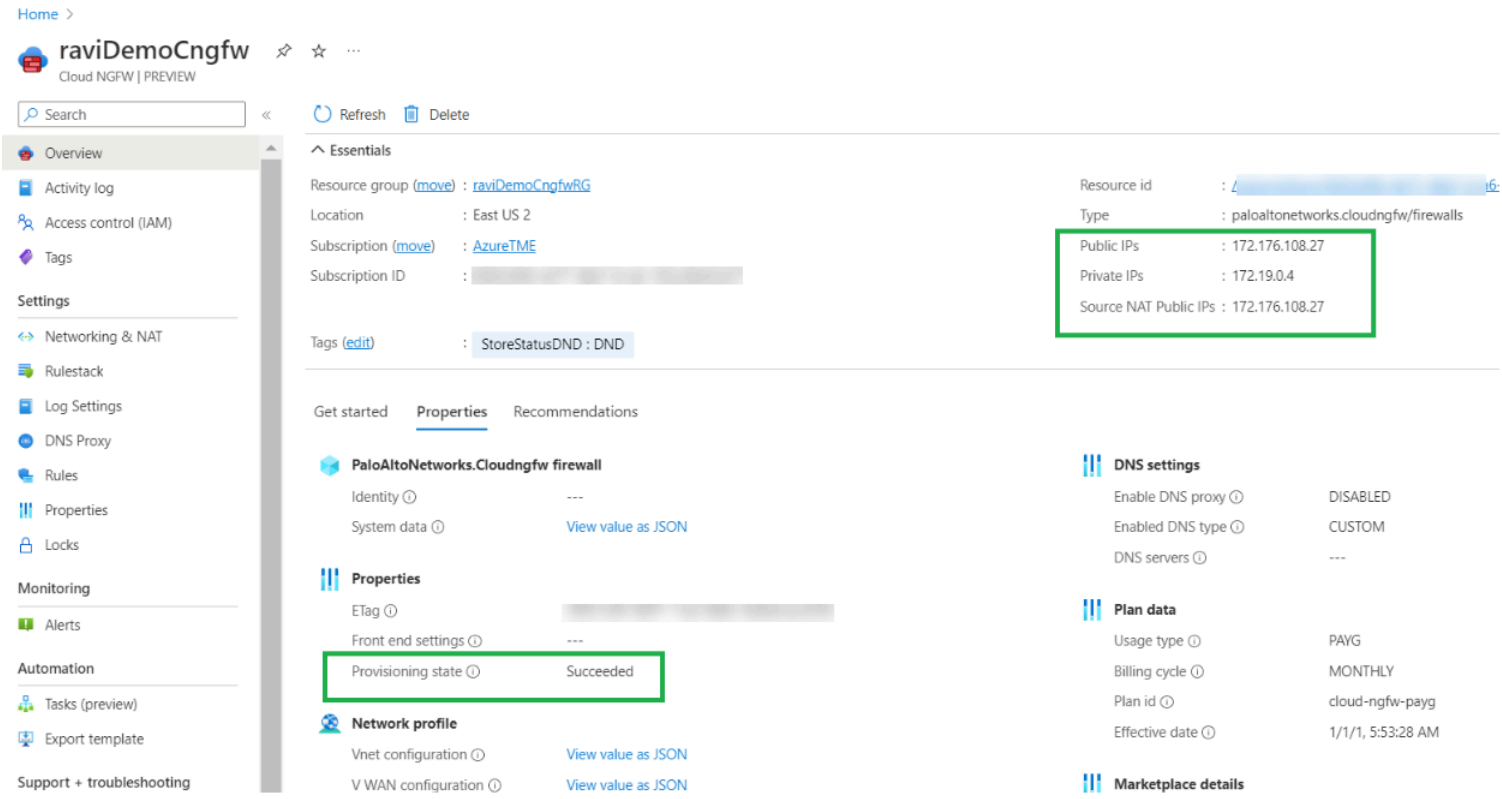
正常にデプロイされると、次の画面が表示されます。**]Go to resource group (**リソースグループに移動**)]**をクリックして、この導入用に作成されたリソースを確認します。



5つのリソースが作成されます。Cloud NGFW、ローカルルールスタック、パブリックIPアドレス、仮想ネットワーク、セキュリティグループが含まれます。



Cloud NGFWリソースが作成されたら、それを選択してプロビジョニング状態が**[Succeeded (**成功**)]**になっていることを確認します。この画面には、Cloud NGFWサービスに関連付けられているパブリックIPアドレスとプライベートIPアドレスも表示されます。



vNETにCloud NGFWを展開したら、詳細については[設定例]を参照してください。

既存のファイアウォールを編集して、RFC 1918 以外のサポート用のプライベートアドレスを追加する

既存のファイアウォールを編集してプライベートアドレスを追加します。

STEP 1 | Azure PortalでCloud NGFWを探します。

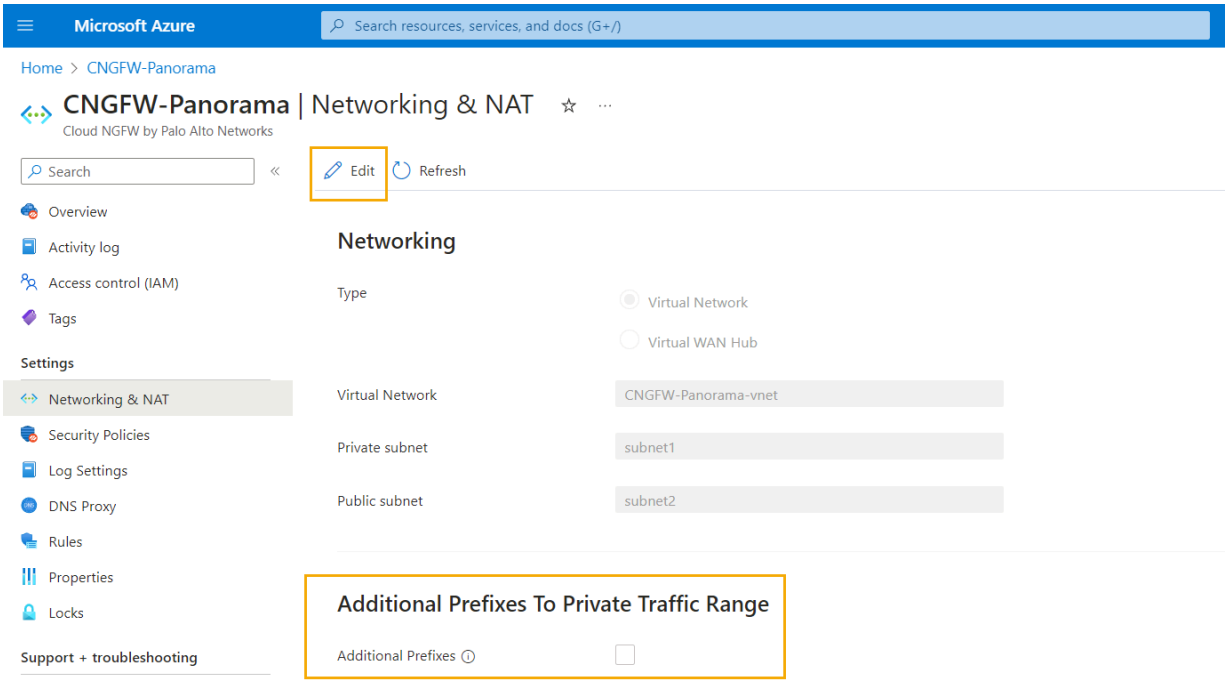
STEP 2 | **[Settings (設定)]**セクションで**[Networking & NAT (ネットワークとNAT)]**を選択します。

STEP 3 | **Edit**（編集）をクリックします。

STEP 4 | **[Additional Prefixes to Private Traffic Range (プライベート トラフィック レンジへのプレフィックス追加)]**セクションで、**[Additional Prefixs (追加のプレフィックス)**］ のチェックボックスをオンにします。

STEP 5 | CIDR形式でアドレスを入力します（例：40.0.0.0/24）。複数のアドレスを含めるには、カンマ区切りリストを使用します。

STEP 6 | **Save**（保存）をクリックします。



既存のファイアウォールを編集してプライベート送信元 NAT を有効にする

ルーティング不可能なサブネット内のインスタンスからの要求に対して送信元ネットワークアドレス変換を実行する場合は、プライベート送信元 **NAT** オプションを使用します。このオプションを使用すると、アプリケーションロードバランサ（ALB）に割り当てられたルーティング可能なIPアドレスにトラフィックを送信できます。プライベート送信元 NAT を有効にしたら、宛先 IP アドレスを含めます。

*Cloud NGFWのEast-West*トラフィックは、ユーザー定義ルート（*UDR*）に依存してファイアウォールにトラフィックを転送します。この依存関係は、ネットワークの両端がプライベートネットワークの一部である場合、一般的な東西方向のトラフィックによってサポートされます。しかし、これは新しいタイプのトラフィックにとって課題となります。導入の片側はプライベートネットワークであり、もう片側は仮想ネットワーク内のプライベートエンドポイントを介してアクセス可能なパートナーまたは*PaaS*サービスをサポートします。そのような環境では、*UDR* を設定するために（他の）ネットワーク全体への管理アクセス権を持っていない場合があります。トラフィックは*UDR*によって*Cloud NGFW*に向けられますが、リターントラフィックは*Cloud NGFW*を通過せずにクライアントの送信元*IP*に送信されます。その結果、非対称ルートの問題が発生し、結果として生じる*TCP*ハンドシェイクをファイアウォールで完了できなくなります。*Cloud NGFW*は、プライベート送信元***NAT***を使用してソース*IP*アドレスをファイアウォールのインスタンスのプライベートインターフェイス*IP*に変換します。これにより、リターントラフィックが*Cloud NGFW*によって適切なインターフェイスに確実に処理されます。

STEP 1 | Azure PortalでCloud NGFWを探します。

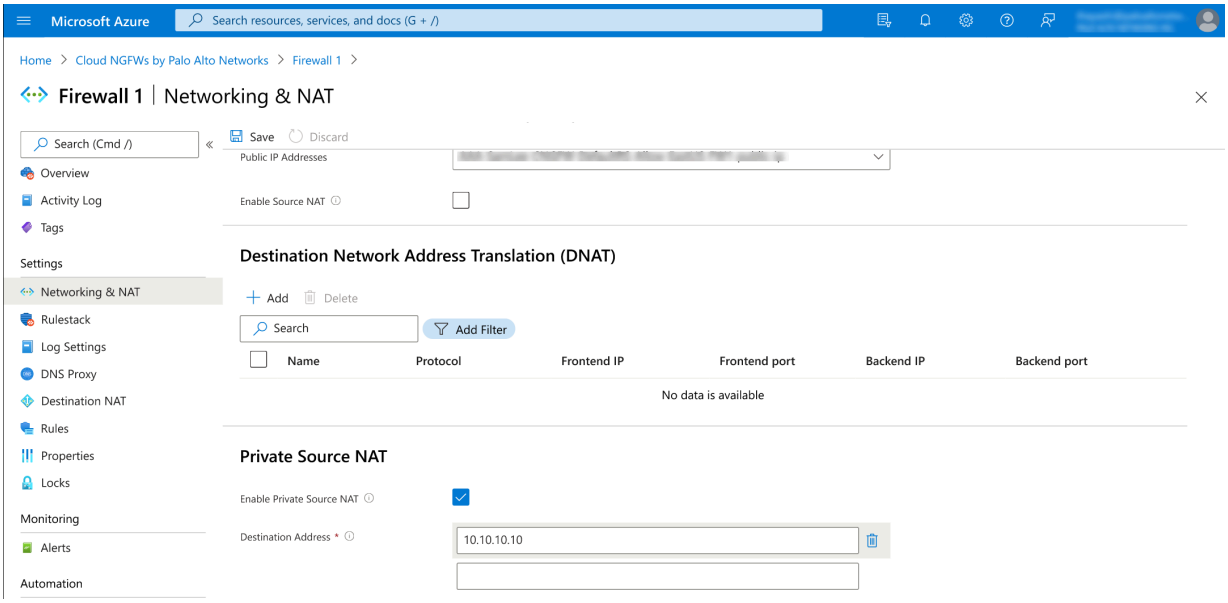
STEP 2 | **[Settings (**設定**)]**セクションで**[Networking & NAT (**ネットワークと**NAT)]**を選択します。

STEP 3 | **Edit**（編集）をクリックします。

STEP 4 | **[Private Source NAT (**プライベート送信元**NAT)]** セクションで、**[Enable Private Source NAT (**プライベート送信元**NAT**の有効化**)]** のチェックボックスをオンにします。

STEP 5 | 送信先アドレスを入力します。

STEP 6 | **Save**（保存）をクリックします。



vNETデプロイメント後の設定例

Azure vNETにCloud NGFWを正常にデプロイしたら、Cloud NGFWサービスの構成を開始できます。このセクションで提供される情報は、Azure環境でCloud NGFWを実行するための一般的なタスクを示しています。

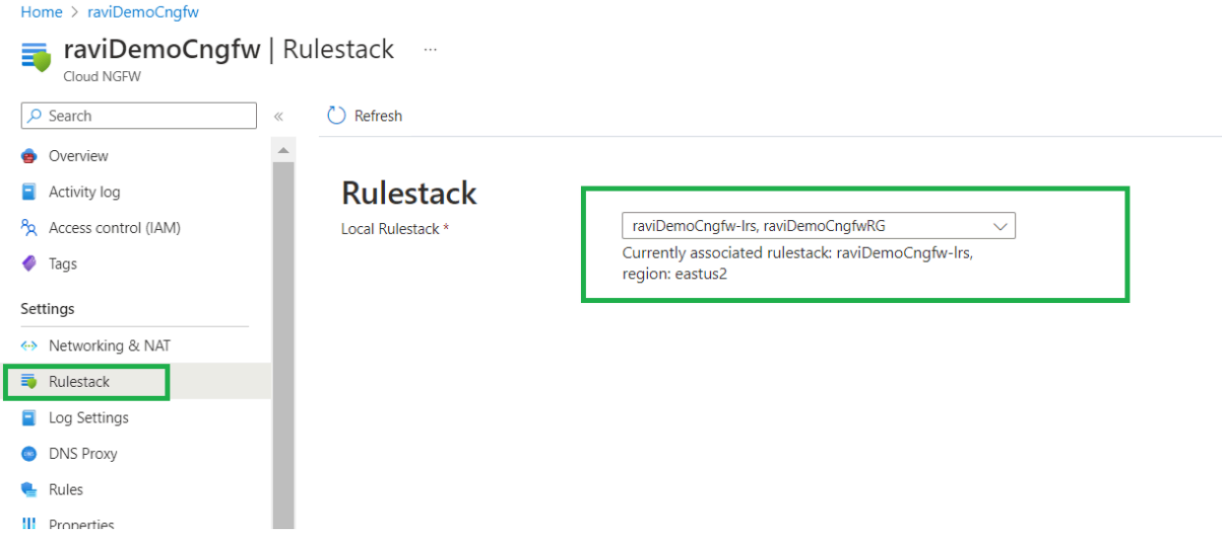
- ルーレスタックを作成または更新する
- FQDN リストの追加
- ルールの追加
- 送信元と宛先のNATルールを設定する
- ロギングの設定
- ネットワークセキュリティグループを更新する
- vNETピアリングの設定
- ルートテーブルを追加する

ルールスタックを作成または更新する

この節では、ローカルルールスタックを更新するために、ルールを追加し、ロギングを有効にします。

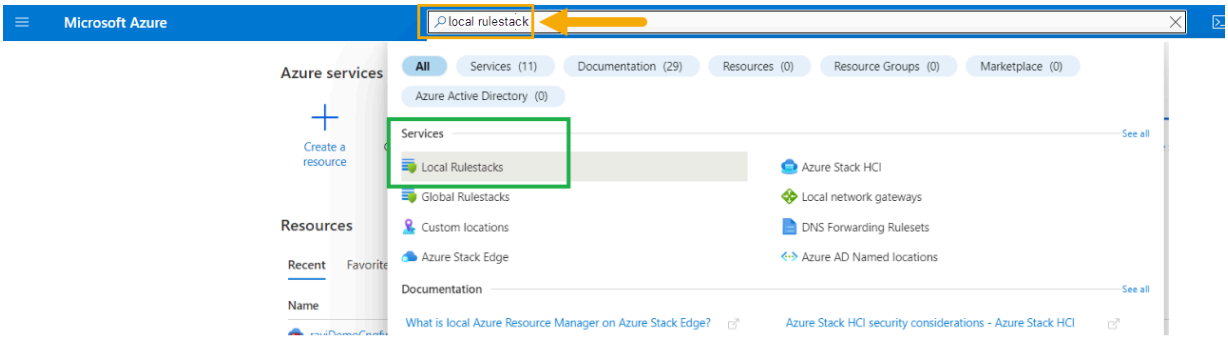
既存のルールスタックを更新する方法：

STEP 1 | Azure Resource Manager（ARM）コンソールで、構成するCloud NGFWリソースの［**Rulestacks (**ルールスタック**)**］をクリックします。Cloud NGFWサービスに関連付けられているルールスタックが、リソースグループとともに表示されます。

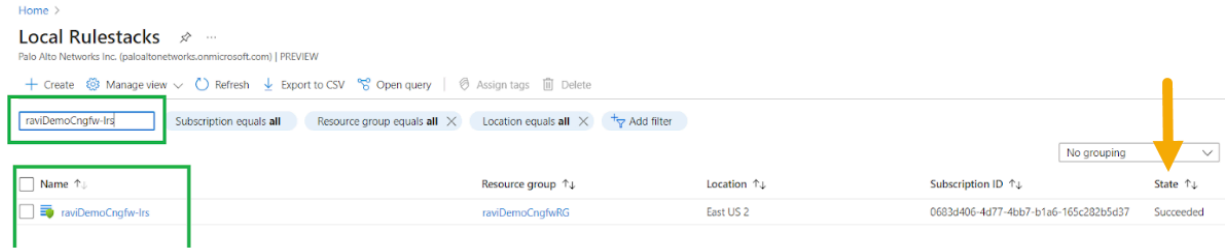


STEP 2 | ルールスタックを変更してファイアウォールルールを追加します。これらのルールは、特定のトラフィックをブロックしながら一部のトラフィックを許可します。デフォルトで

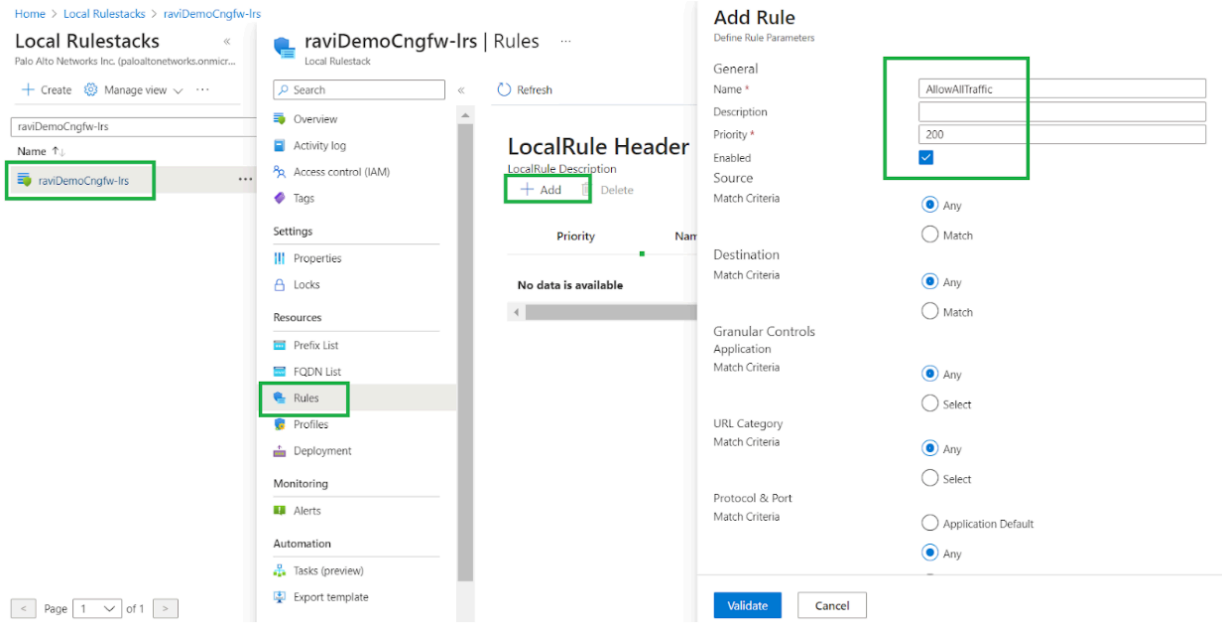
は、Cloud NGFWはすべてのトラフィックをブロックします。Azureポータルが提供するグローバル検索オプションを使用して、ローカルルールスタックを検索します。



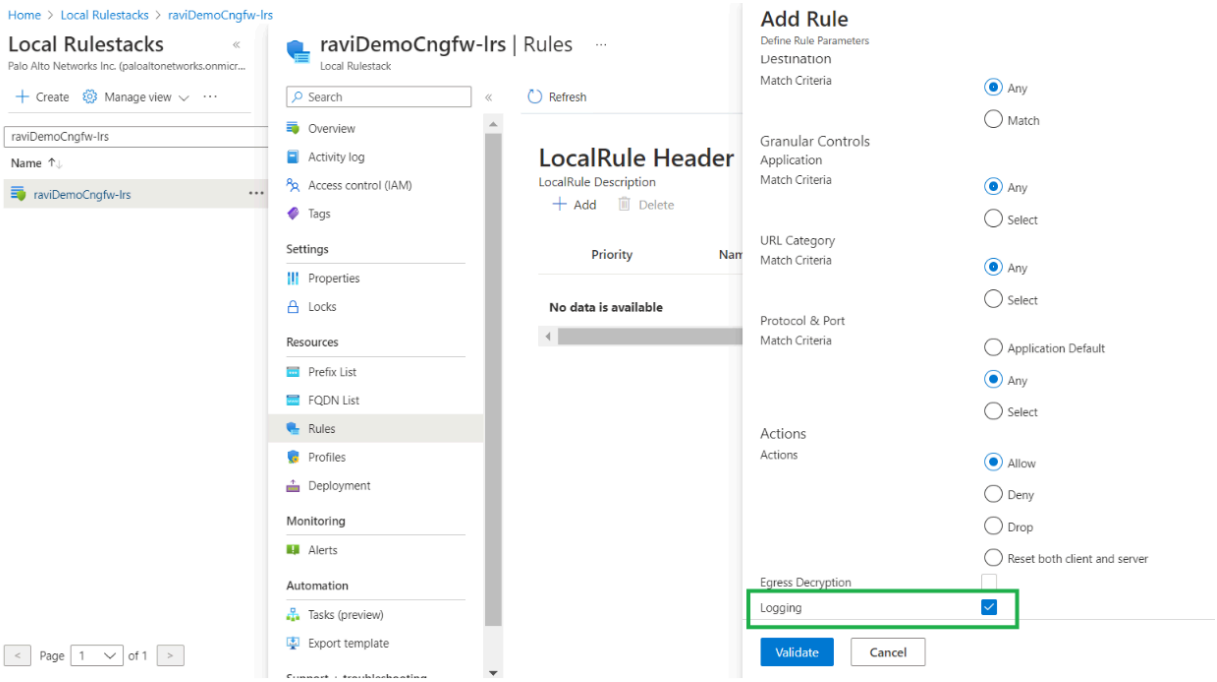
STEP 3 | ローカルルールスタックサービスを選択して、Cloud NGFWサブスクリプションに関連付けられているローカルルールスタックのリストに移動します。ローカルルールスタックを検索し、状態が成功であることを確認します。



STEP 4 | ルールスタックをクリックしてルールを追加します。**[Add Rule (**ルールの追加**)]**ウィンドウで、ルールを変更します。たとえば、トラフィックを許可するルールを追加します。必須フィールドに入力し、残りのフィールドにはデフォルト設定を使用します。



STEP 5 | ルールのロギングを有効にします。[Add Rule (ルールの追加)]ウィンドウで、**[Logging (ロギング)]**を選択します。



STEP 6 | **[Validate (検証)]**をクリックし、**[Add (追加)]**をクリックしてルールスタックにルールを追加します。

FQDNリストを追加する

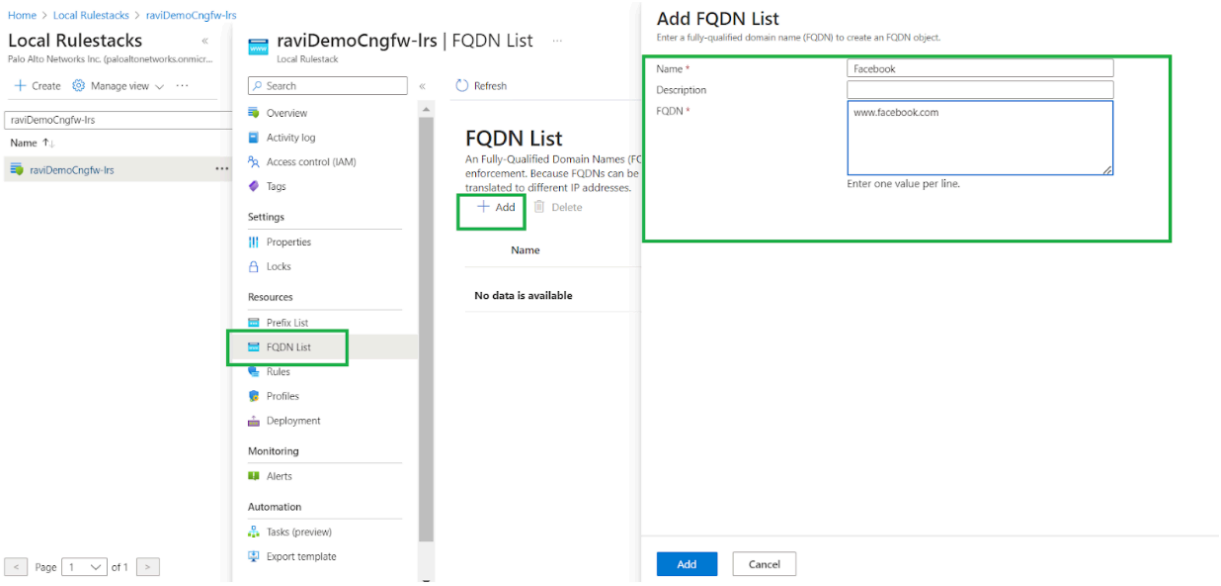
Facebookを含むローカルルールスタックにFQDNリストを追加します。このリストを使用して、facebook.comへのトラフィックをブロックするルールを追加します

STEP 1 | クラウドNGFWリソースのローカルルールスタックページで、［**FQDN List (FQDN**リスト**)**］をクリックします。

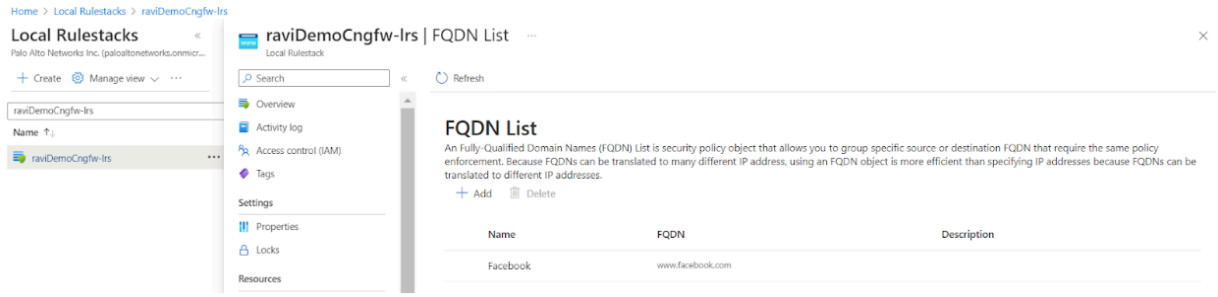
STEP 2 | **[**追加**]** をクリックします。

STEP 3 | **[Add FQDN List (FQDN**リストを追加**)]**画面で、名前と説明を入力します。［FQDN］フィールドに、www.facebook.comなどのURLを1つ以上入力します。FQDNフィールドの1行に存在できるFQDN URLは1つだけです。

STEP 4 | **[**追加**]** をクリックします。



STEP 5 | 指定したURLがFQDNリストに表示されていることを確認します。



ルールを追加する

以前に作成したFQDNリストと一致するルールをローカルルールスタックに追加します。ルールでは、トラフィックのドロップなどのアクションを設定できます。たとえば、URL www.facebook.com にアクセスしようとするトラフィックをドロップするアクションを FQDN ルールに適用できます。

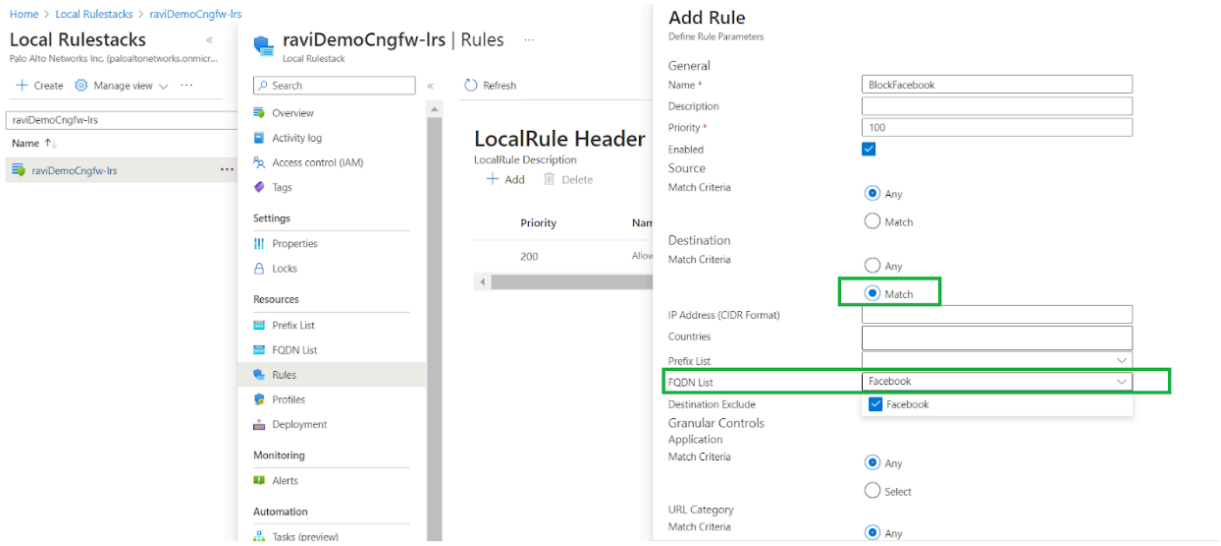
STEP 1 | クラウドNGFWリソースのローカルルールスタックページで、［**Rules (ルール)**］をクリックします。

STEP 2 | **[追加]** をクリックします。

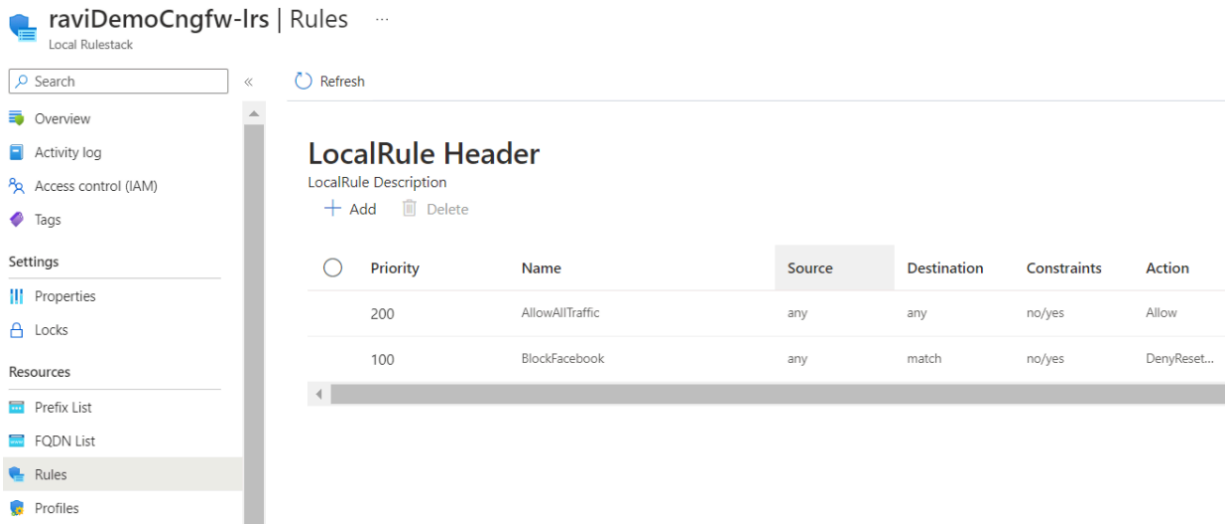
STEP 3 | **[Add Rule (ルールの追加)]**画面で、「一致条件」を「一致」に設定します。**[FQDNリスト (FQDN List)]**フィールドで、ドロップダウンメニューを使用してFacebook

STEP 4 | **[Actions (アクション)]**フィールドで、[ドロップ]を選択します。

STEP 5 | **[追加]** をクリックします。

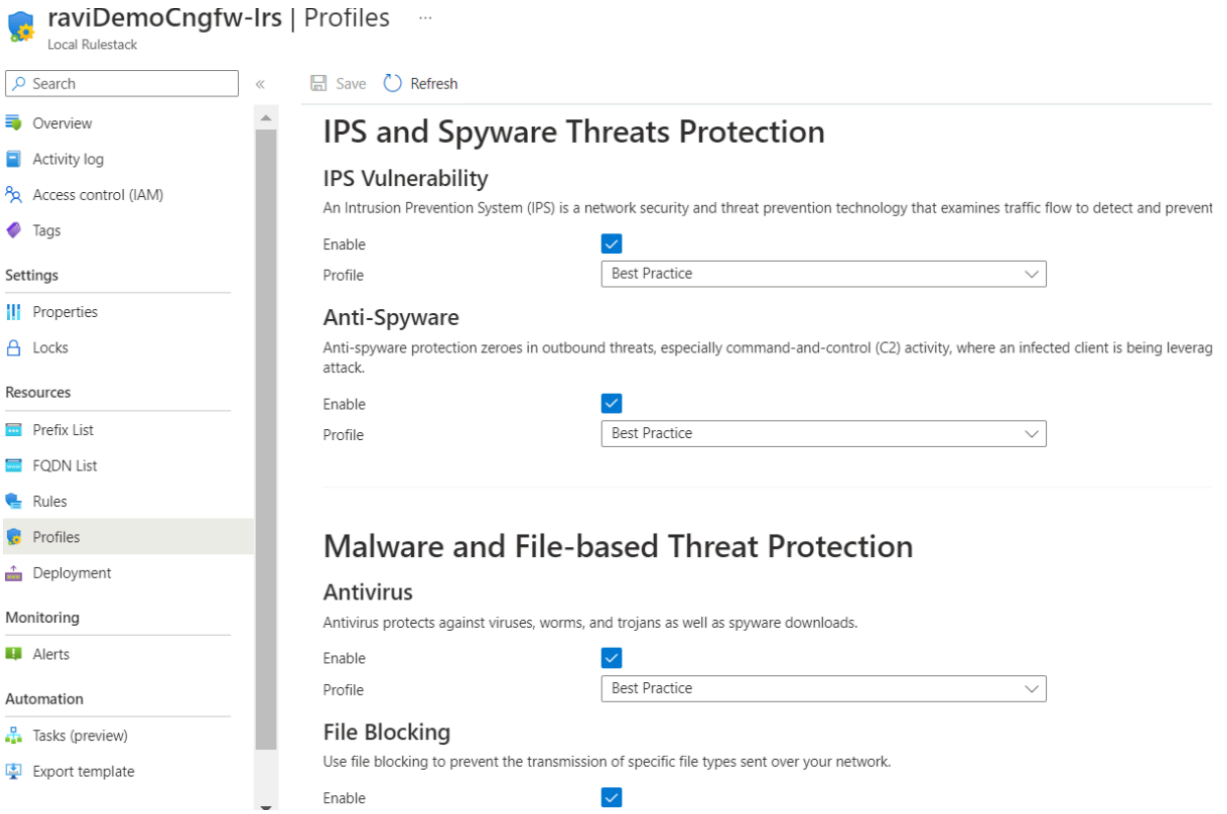


両方のルールがローカルのルールスタックヘッダーページに表示されます。



このCloud NGFWサービスの一環として、セキュリティプロファイルはデフォルトでベストプラクティス構成で有効化されます。Cloud NGFWがネットワークに導入されると、トラフィッ

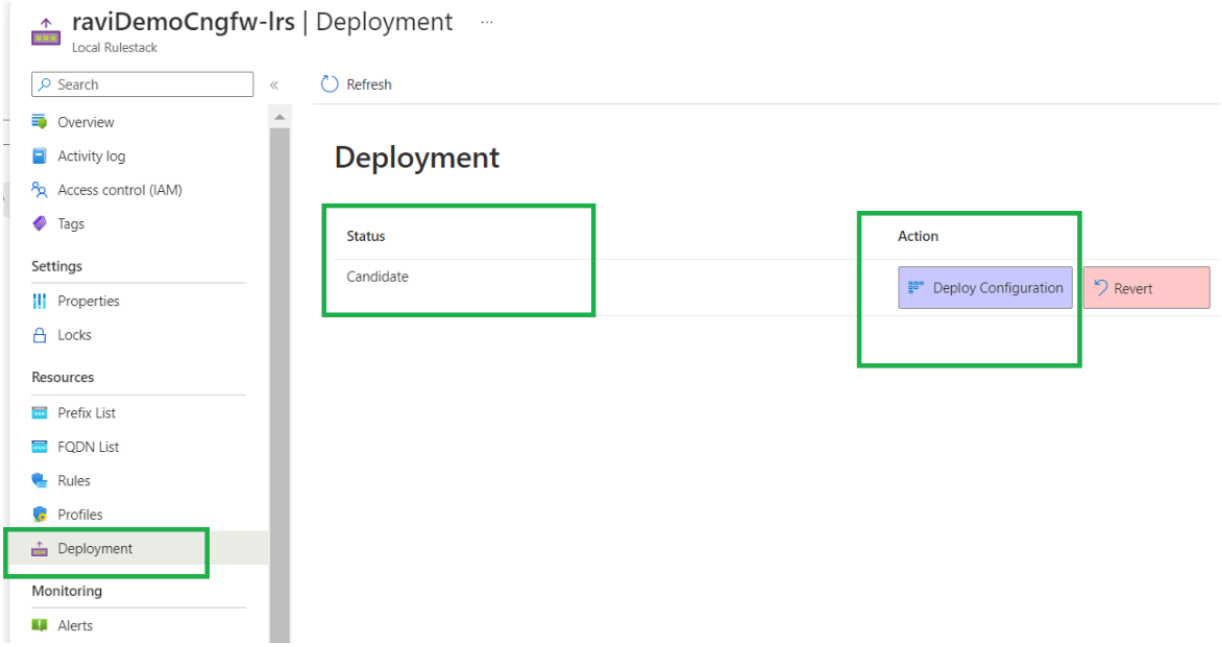
クは最適なセキュリティプロファイルで保護されます。ローカルルールスタックの**Profiles (プロファイル)**ページを使用してこれらを表示します。



ルールを変更したら、Cloud NGFWサービスに関連付けられたローカルルールスタックに展開します。

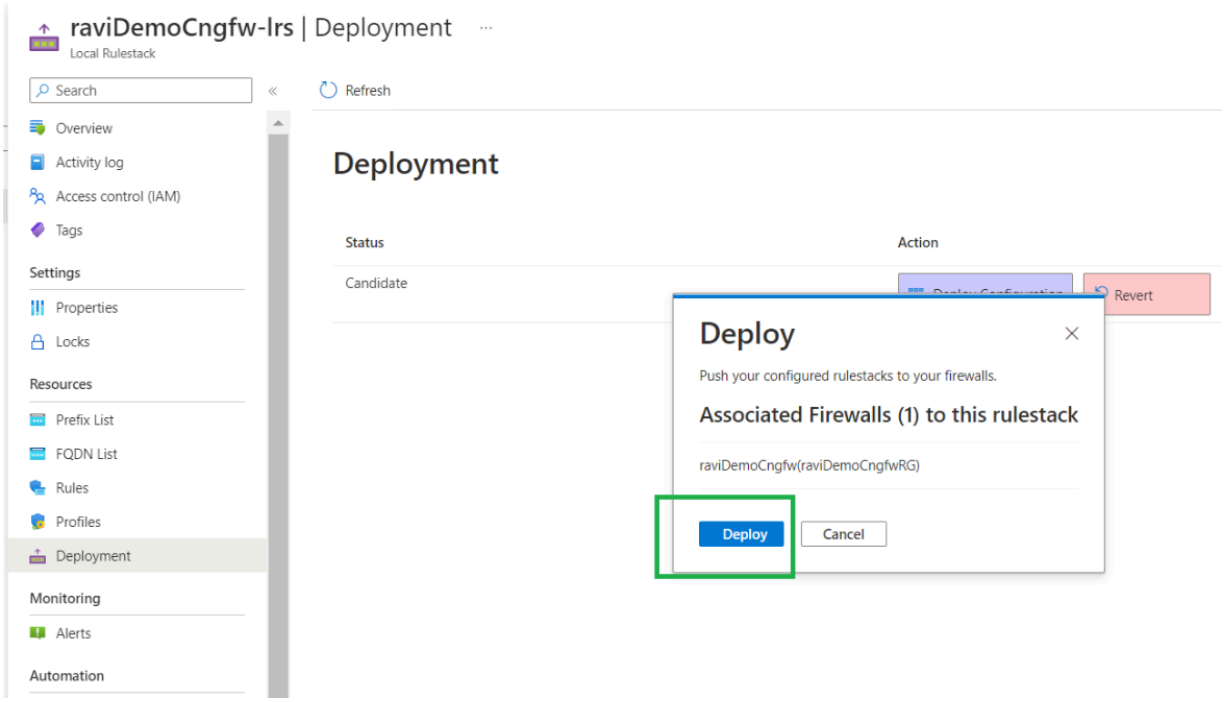
STEP 6 | ローカルルールスタックで、**[Deployment (展開)]**をクリックします。デプロイメントステータスページが[Candidate (候補)]と表示されます。これは、設定が構築されたがまだデプロイされていないことを意味します。

STEP 7 | **[Deploy Configuration (設定のデプロイ)]**をクリックして、設定をCloud NGFWサービスに展開します。ルールスタックにルールを展開するには、この手順を実行する必要があります。

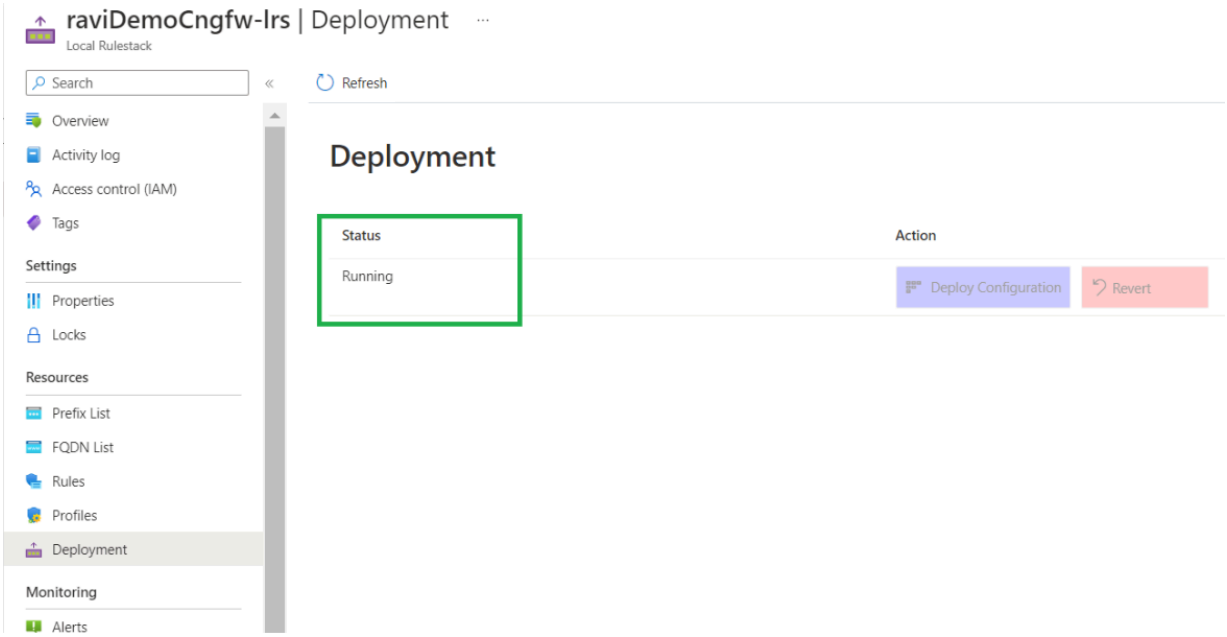


STEP 8 | **[Deploy Configuration (設定のデプロイメント)]**をクリックすると、ルールスタックに関連付けられているファイアウォールを示すポップアップメッセージが表示されま

す。［**Deploy (デプロイ)**］をクリックして、関連するすべてのファイアウォールにこのルールスタックを設定します。



STEP 9 | 設定のデプロイに成功すると、**[Deployment (デプロイメント)]**ステータスは**[Running (実行中)]**になります。

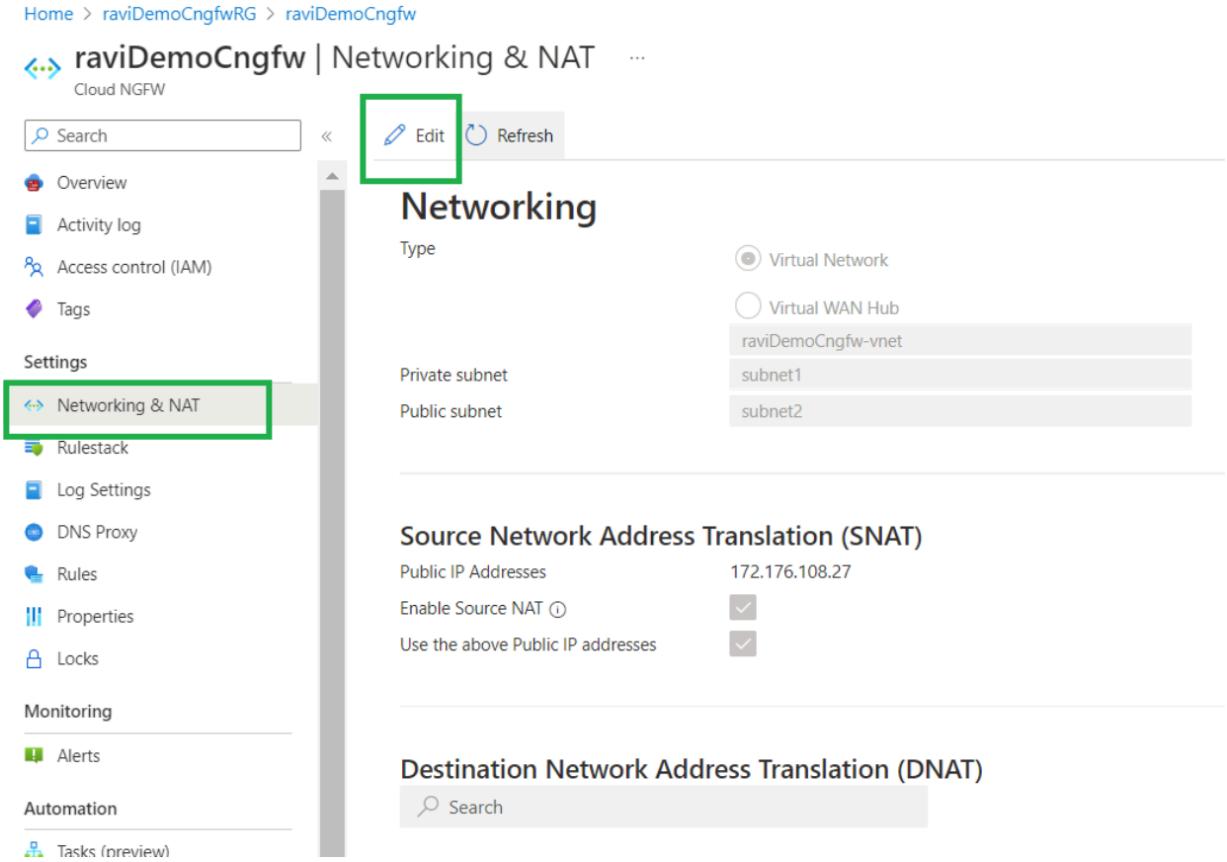


送信元および宛先の NAT ルールの設定

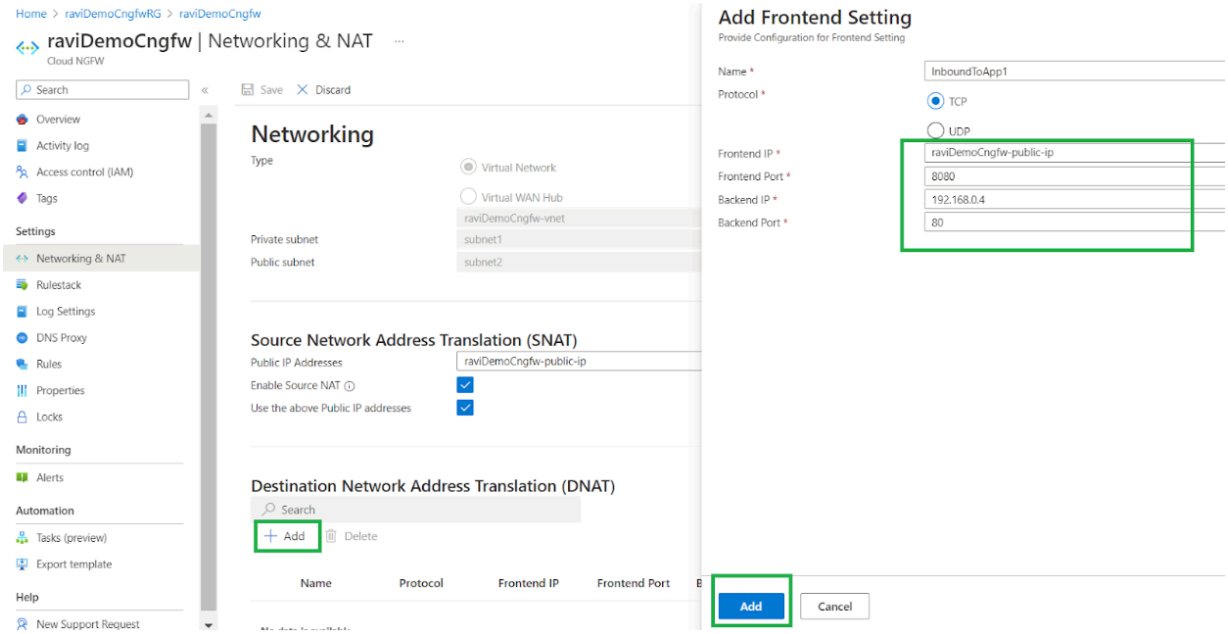
インバウンド トラフィックに対応する宛先 NAT ルールを設定できます。

STEP 1 | Cloud NGFWリソースの**[Networking and NAT (ネットワーキングとNAT)]**設定にアクセスします。送信元NAT設定が有効になっているかどうかを確認する。

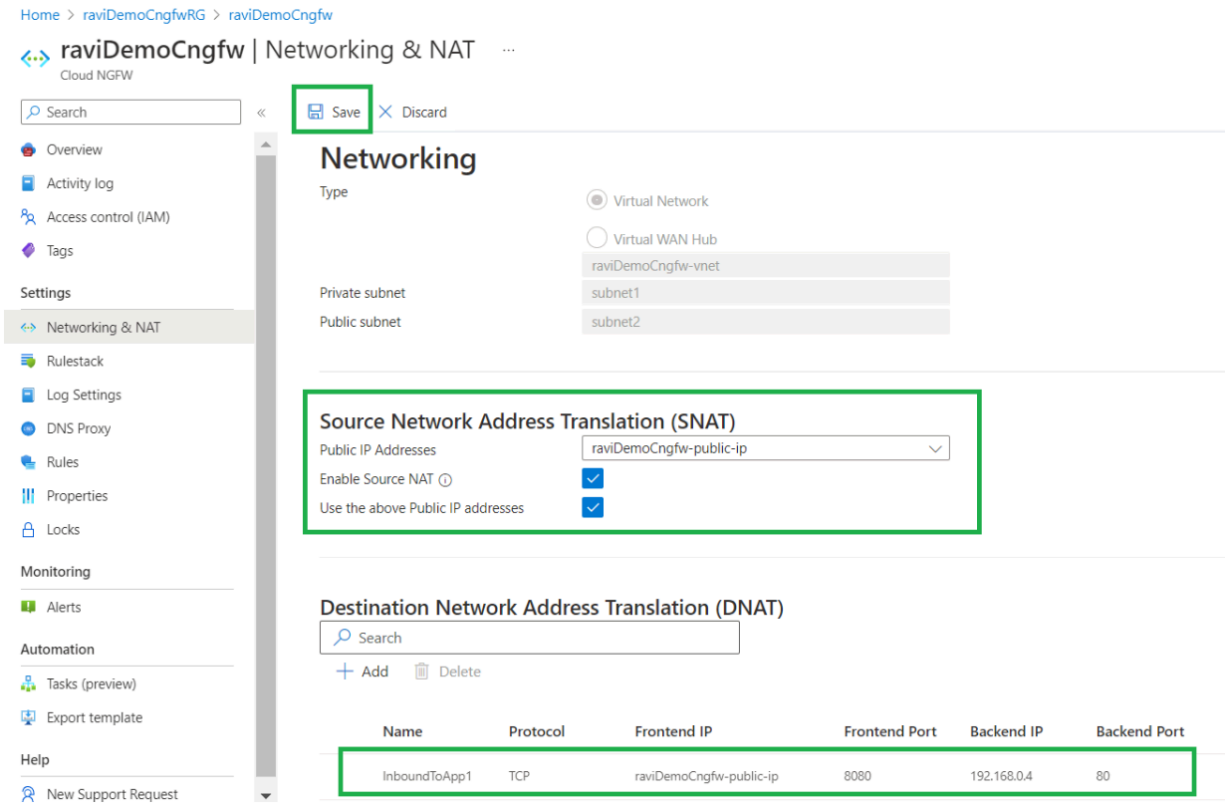
STEP 2 | **[Edit (編集)]** をクリックして、宛先 NAT ルールを追加します。



STEP 3 | 宛先 NAT ルールを追加します。フロントエンドIPは、Cloud NGFWに関連付けられたパブリックIPアドレスを表します。フロントエンドのポート番号を入力し、［**Add (追加)**］をクリックします。



STEP 4 | 宛先NATルールを追加したら、［**Save (保存)**］をクリックしてクラウドNGFWリソースに設定を展開します。



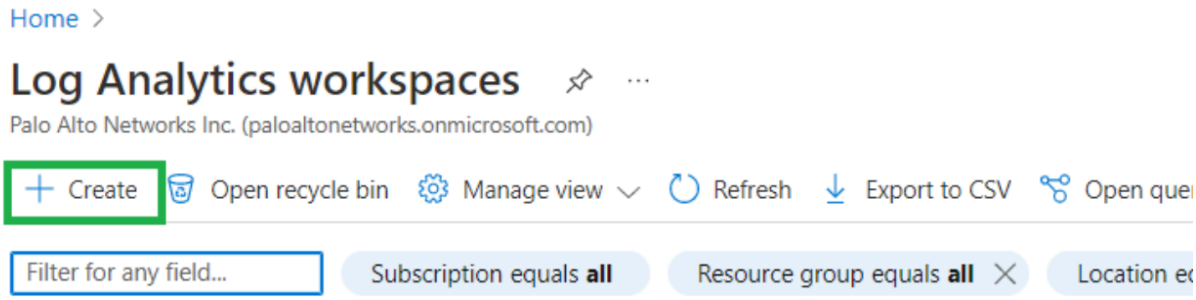
フロントエンドアドレスは、Cloud NGFWを通じて設定されたポートを通じてリダイレクトされるようになりました。インバウンドトラフィックがCloud NGFWを経由するようになりました。

ログの設定。

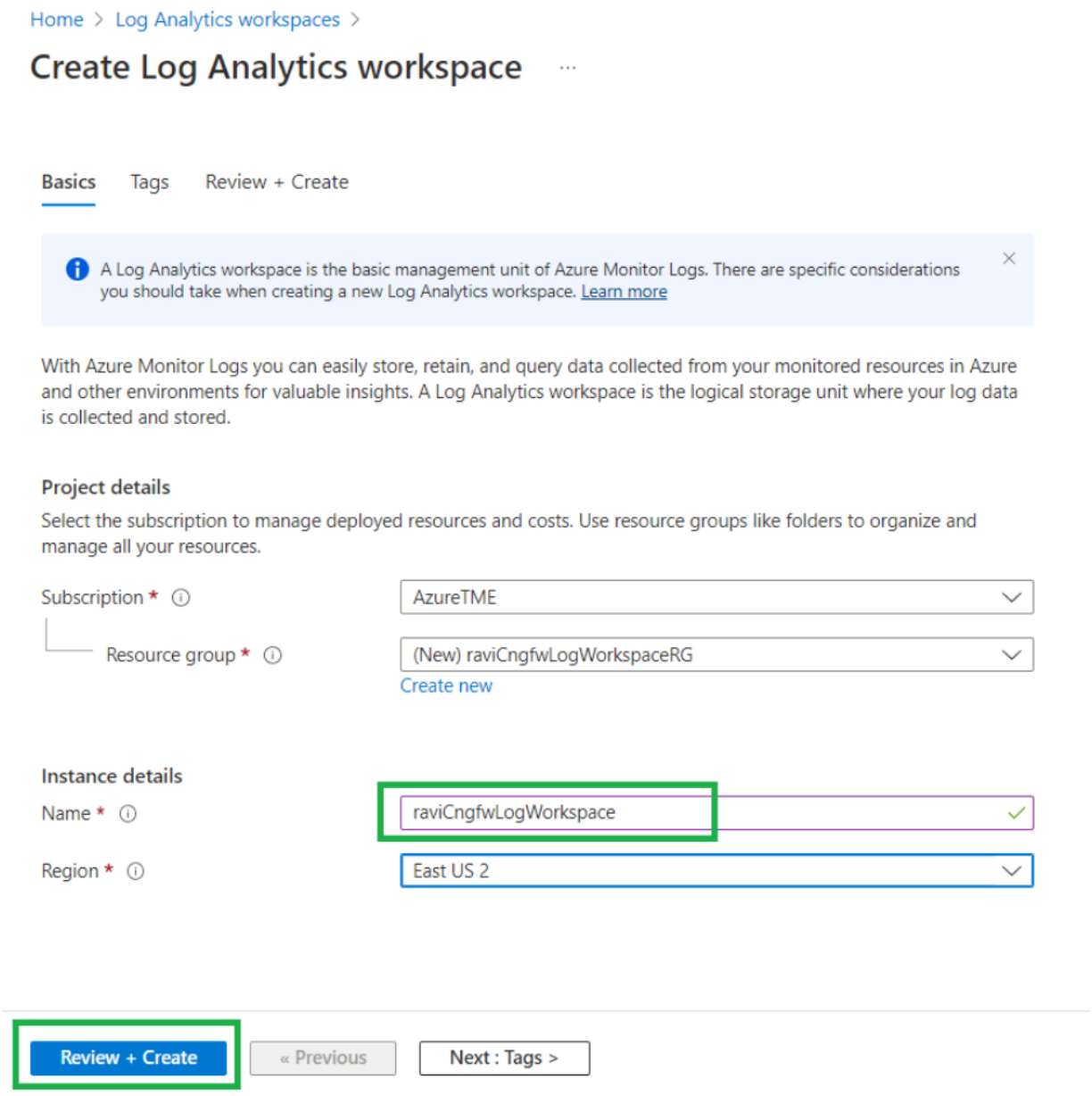
Cloud NGFWでロギングを構成する前に、AzureでLog Analyticsワークスペースを作成します。

STEP 1 | Azureポータルで、**Azure Log Analytics workspace (Azure**ログ分析ワークスペース**)**を検索します。**[Log Analytics Workspaces (**ログ分析ワークスペース**)**］をクリックして、サービスとして追加します。

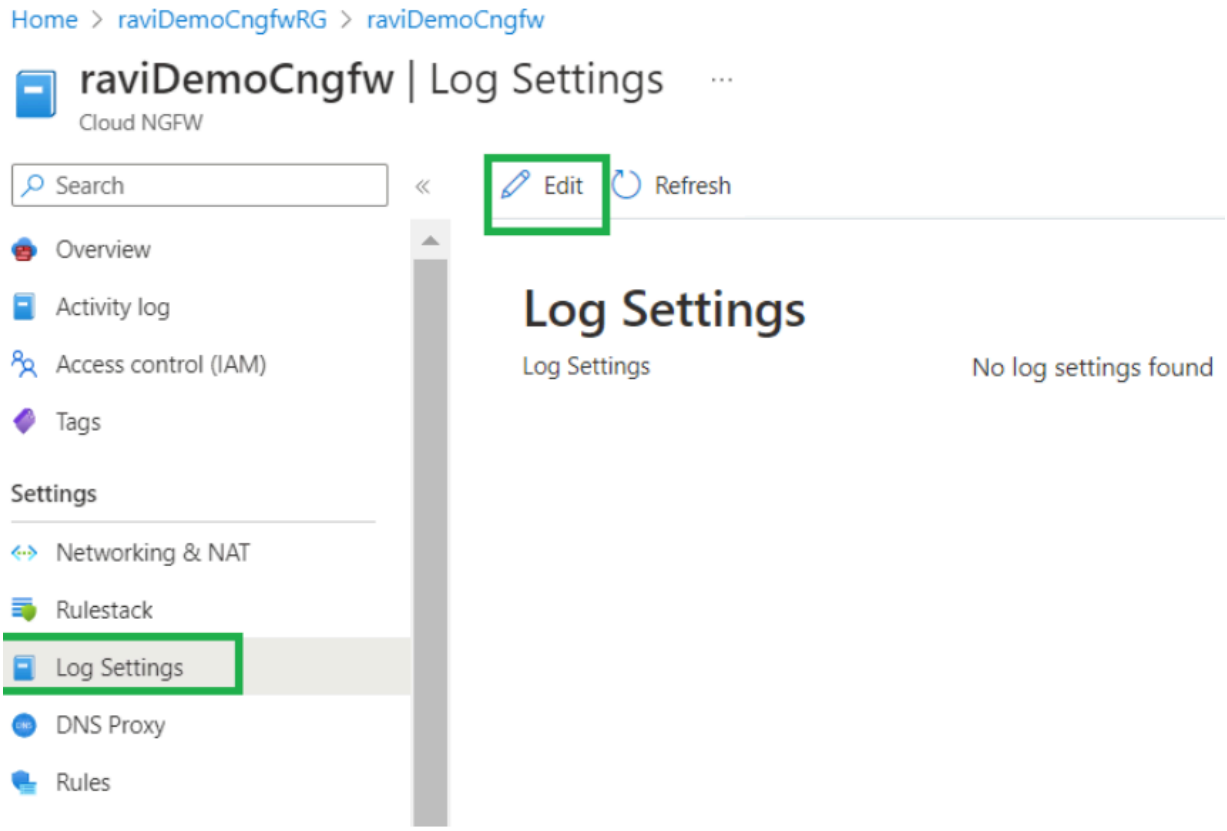
STEP 2 | **[Create (**作成**)]**をクリックして、新しいログ分析ワークスペースを確立します。



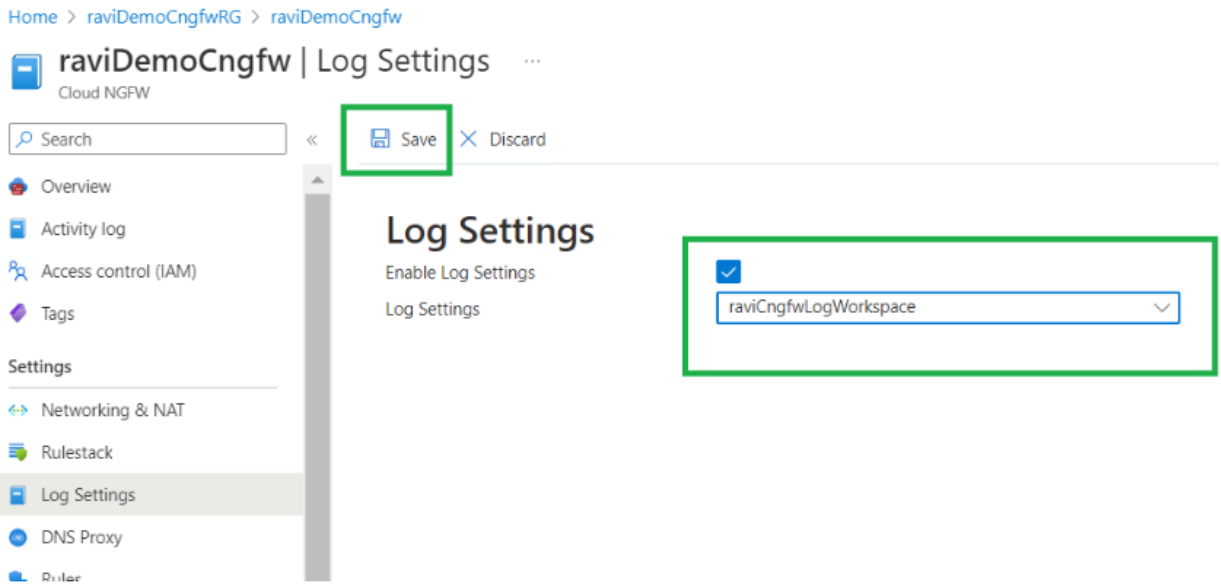
STEP 3 | [ログ分析の作成]ワークスペースで、インスタンスの詳細を指定します。ドロップダウンメニューから作業スペースの名前を選択し、地域を指定します。



STEP 4 | Cloud NGFWリソースのログ設定を行います。**[ログ設定]**を選択します。**Edit**（編集）をクリックします。



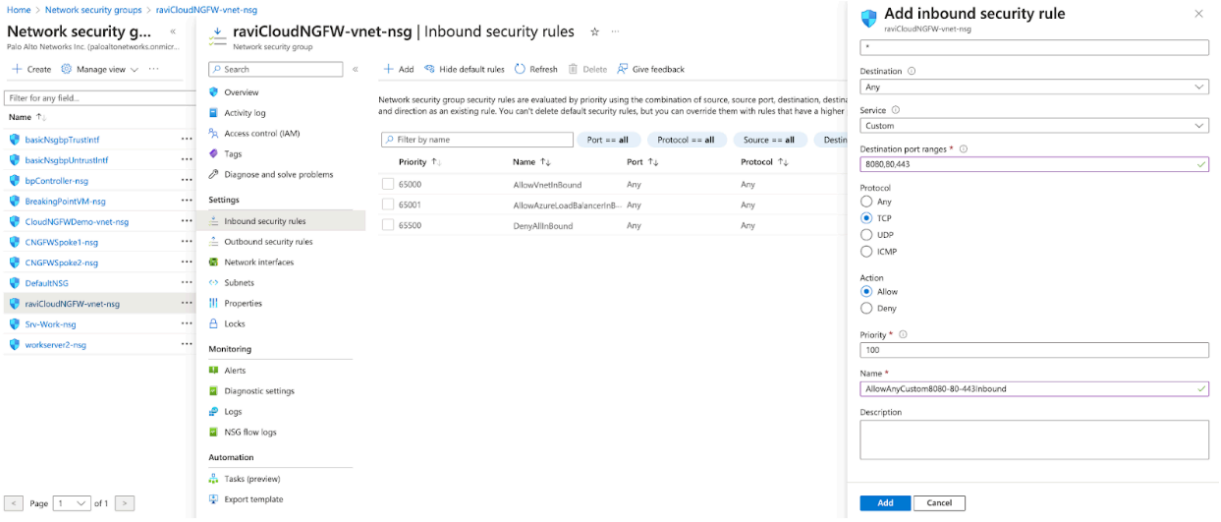
STEP 5 | **[Log Settings (ログ設定)]**フィールドで、以前に作成したログ分析ワークスペースを選択し、**[Save (保存)]**をクリックします。



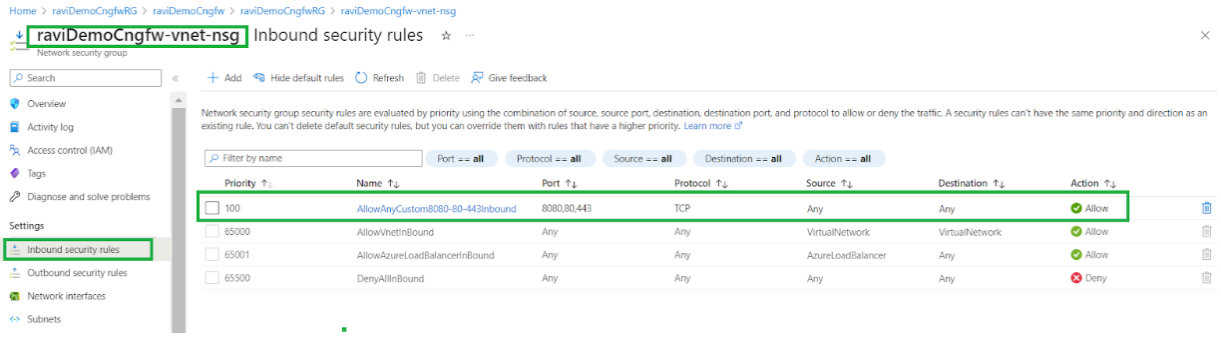
ネットワークセキュリティグループの更新

Cloud NGFWの導入の一環として作成されたネットワークセキュリティグループを更新します。このセキュリティグループは、Cloud NGFWサブスクリプションのvNETの一部としてプライベートサブネットとパブリックサブネットの両方に関連付けられます。

STEP 1 | フロントエンド（宛先）NATルール設定の一部としてトラフィックを許可します。クラウドNGFWを介してアプリケーションvNETからインターネットにアクセスできるように、HTTPおよびHTTPSトラフィックを許可する。



STEP 2 | **[Add (追加)]**をクリックして、次のインバウンドセキュリティルールを組み込みます。



vNETピアリングを構成する

vNETピアリングを設定するには、次の手順を実行します。

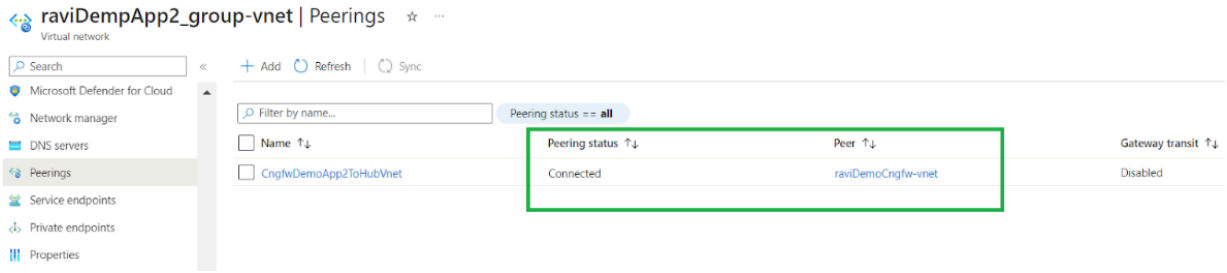
STEP 1 | vNETを探し、**[Peerings (ピアリング)]**を選択します。

STEP 2 | ［**Add (追加)**］をクリックして新しいピアリングを作成します。

STEP 3 | ピアリングの名前を指定し、デフォルト設定のままにします。

STEP 4 | ピアにするハブvNETを選択します。既存のvNETハブを使用してvNETにCloud NGFWを導入する場合、最小サイズは/25にする必要があります。最小サイズ/26のサブネットが2つ必

要です。これらのサブネットは**PaloAltoNetworks.Cloudngfw/firewalls**サービスに委任する必要があります。



STEP 5 | このセクションで概説する手順を繰り返して、追加のvNET間のvNETピアリングを設定します。

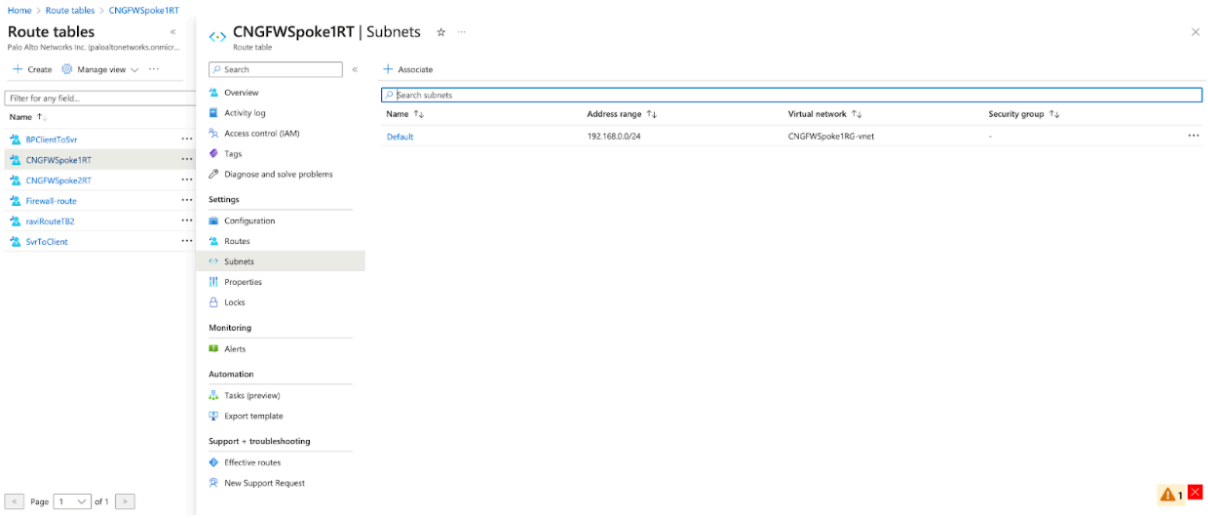
クラウドNGFWを介してトラフィックをルーティングするルートテーブルを追加する

STEP 1 | Azureポータルの検索バーで**[Route table (**ルートテーブル**)]**を検索します。

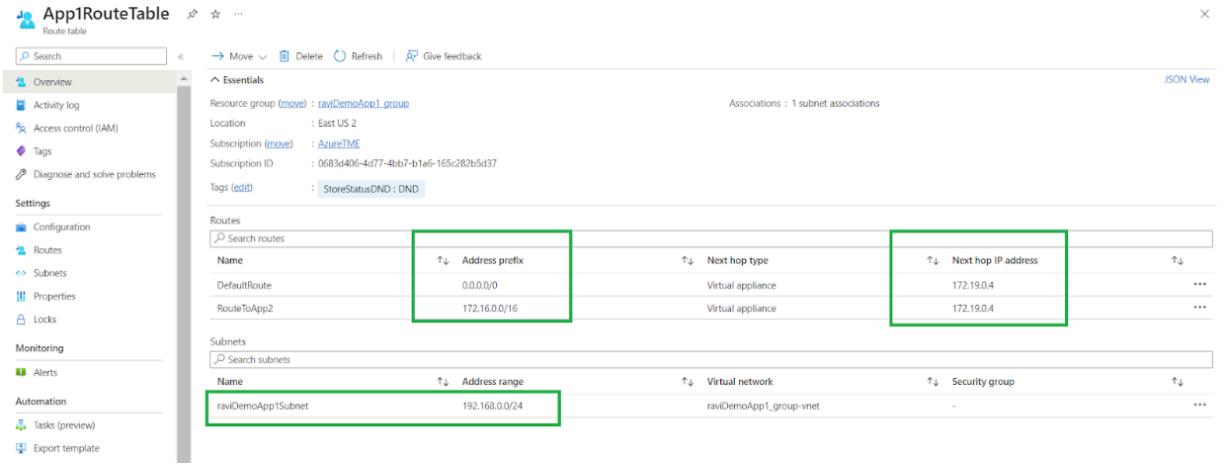
STEP 2 | **[Create (**作成**)]** をクリックして、新しいルート テーブルを確立します。

STEP 3 | ルートテーブルのフィールドに入力し、［**Review+create (**レビュー+作成**)**］ をクリックします。

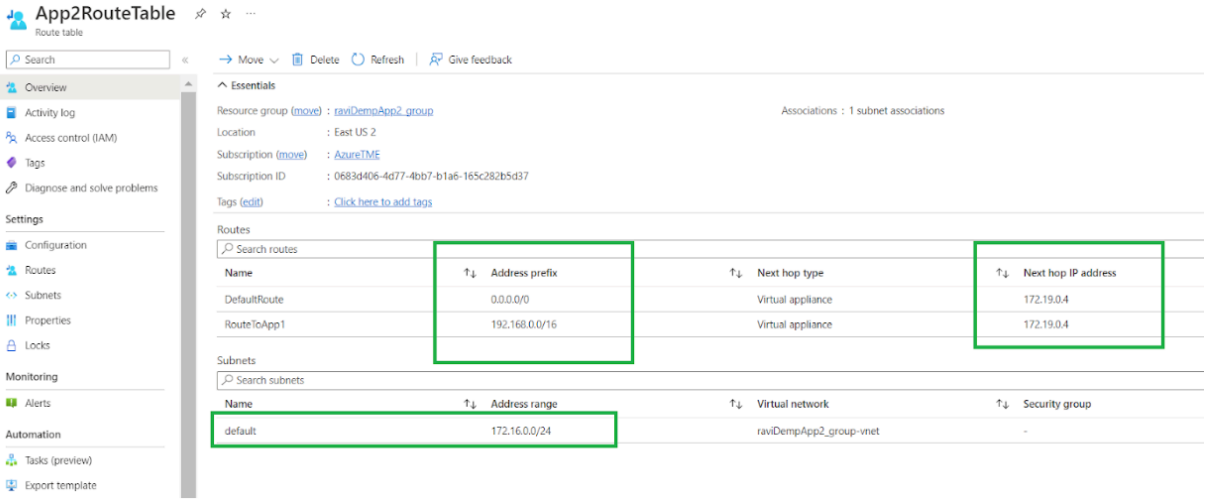
STEP 4 | ルートテーブルを作成したら、**[Subnets (サブネット)]**セクションを選択し、テーブルをサブネットに関連付けます。



STEP 5 | アウトバウンドトラフィックのデフォルトルートを設定し、ネクストホップをCloud NGFWプライベートIPアドレスとしてサブネットに向かってルーティングします（East-Westトラフィックの場合）。



STEP 6 | 1つ以上のルートテーブルをvNETから別のサブネットに関連付けます。デフォルトルート(アウトバウンドトラフィック用)を設定し、ネクストホップをCloud NGFWプライベートIPアドレスとして別のサブネット(East-Westトラフィック用)にルーティングします。



vWANにCloud NGFWをデプロイする

Cloud NGFWは、拡張性の高いファイアウォールソリューションとしてvWANハブにシームレスに展開し、Azureとオンプレミス間のグローバルハイブリッドネットワークでホストされている重要なワークロード間のトラフィックを保護できます。Azure vWANと利用可能な機能の詳細については、[Azure Virtual WAN documentation (Azure仮想WANのマニュアル)]を参照してください。

vWANにCloud NGFWを導入する場合は、次の点を考慮してください。

- NGFWリソースには1つのプライベートIPアドレスが使用されます。vWAN 環境の場合は、vWAN ハブ ルーティング ポリシーを設定して、サービスのトラフィックをヘアピンします。つまり、トラフィックはインターフェイスから出て、インターネットに出る前に戻ってきます。
- 新しいvWANハブのプロビジョニングに約30分かかる場合があります。新しく作成されたvWANハブのステータスは、**[Overview (概要)]**ページの**[Essentials (エッセンシャル)]**セクションの**[Routing Status (ルーティングステータス)]**フィールドで確認できます。

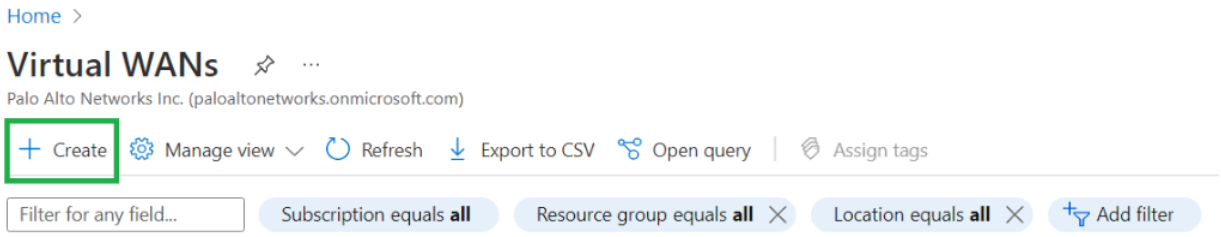
Cloud NGFW for Azure vWAN デプロイメント：

- SaaSフレームワークを使用してAzure Virtual WANに完全に統合されています。
- vWAN仮想ハブに直接展開されます。
- ルーティングインテントとポリシーを利用して、Cloud NGFWサービスによって検査されるトラフィックを制御します。
- ハブ間およびリージョン間のトラフィックに一貫したセキュリティポリシーを適用可能

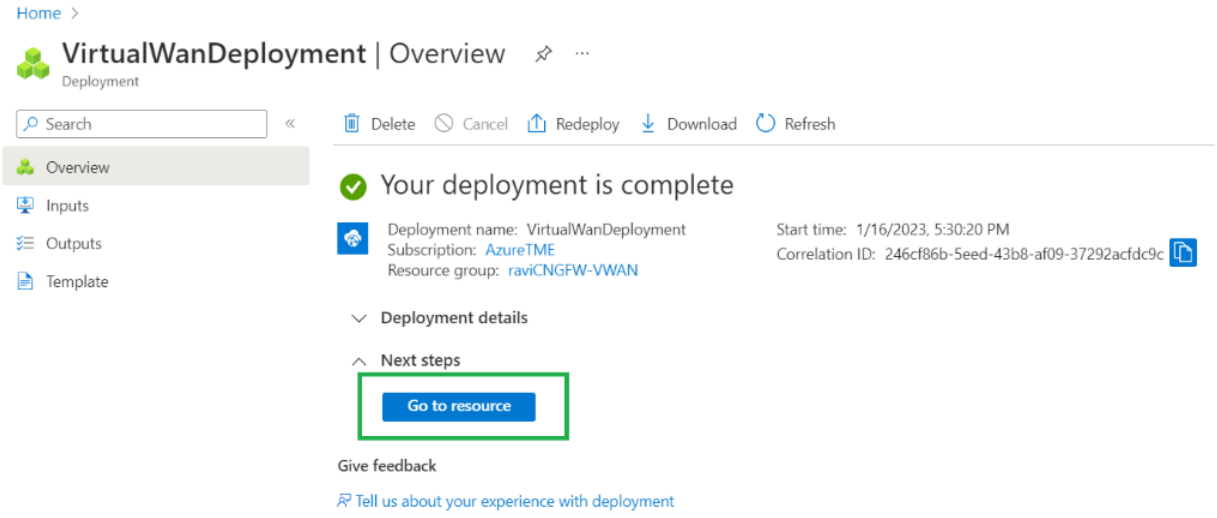
前提条件

vWANにCloud NGFWをデプロイするには、Azureサブスクリプションが必要です。このサブスクリプションには、**owner (所有者)**または**contributor (貢献者)**のロールが必要です。

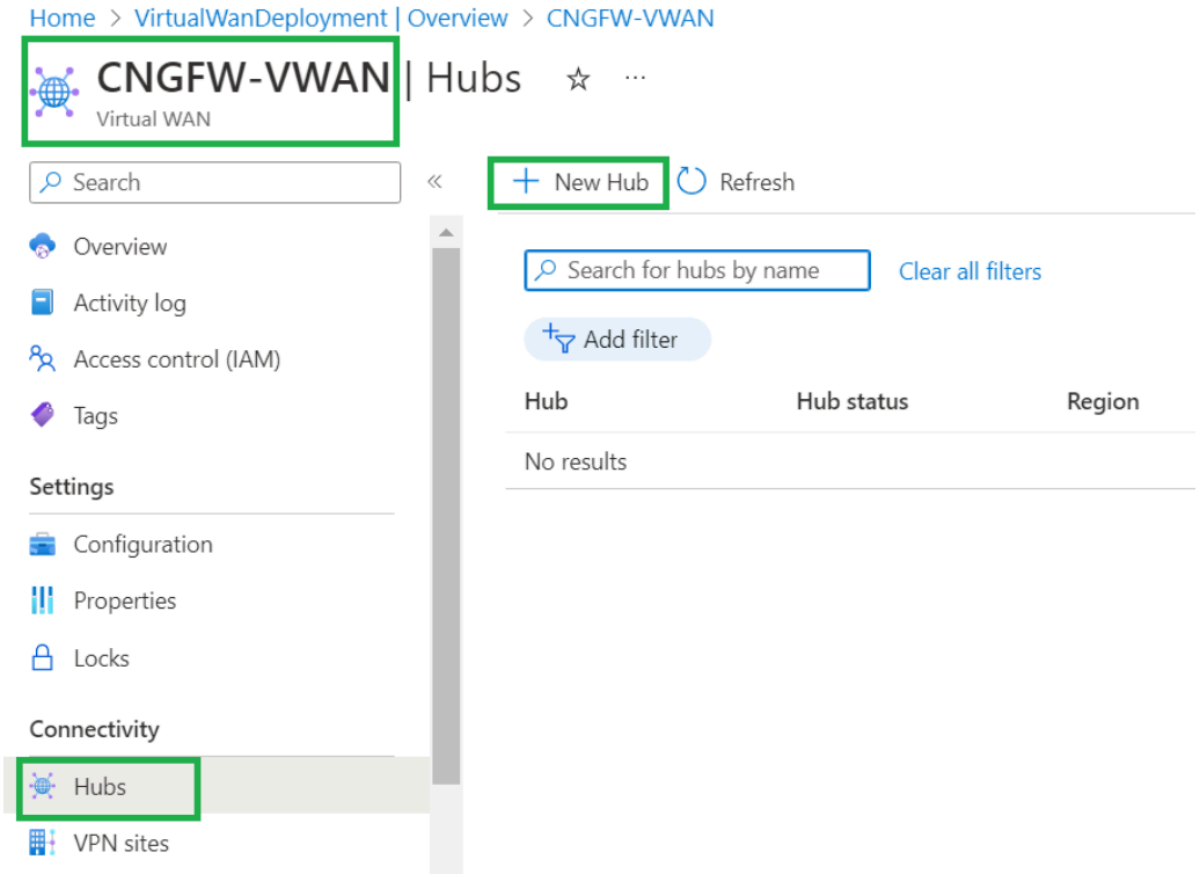
STEP 1 | Azureポータルにログインし、**Virtual WAN (仮想WAN)**を検索します。**[Create (作成)]**をクリックして仮想WANサービスを作成します。



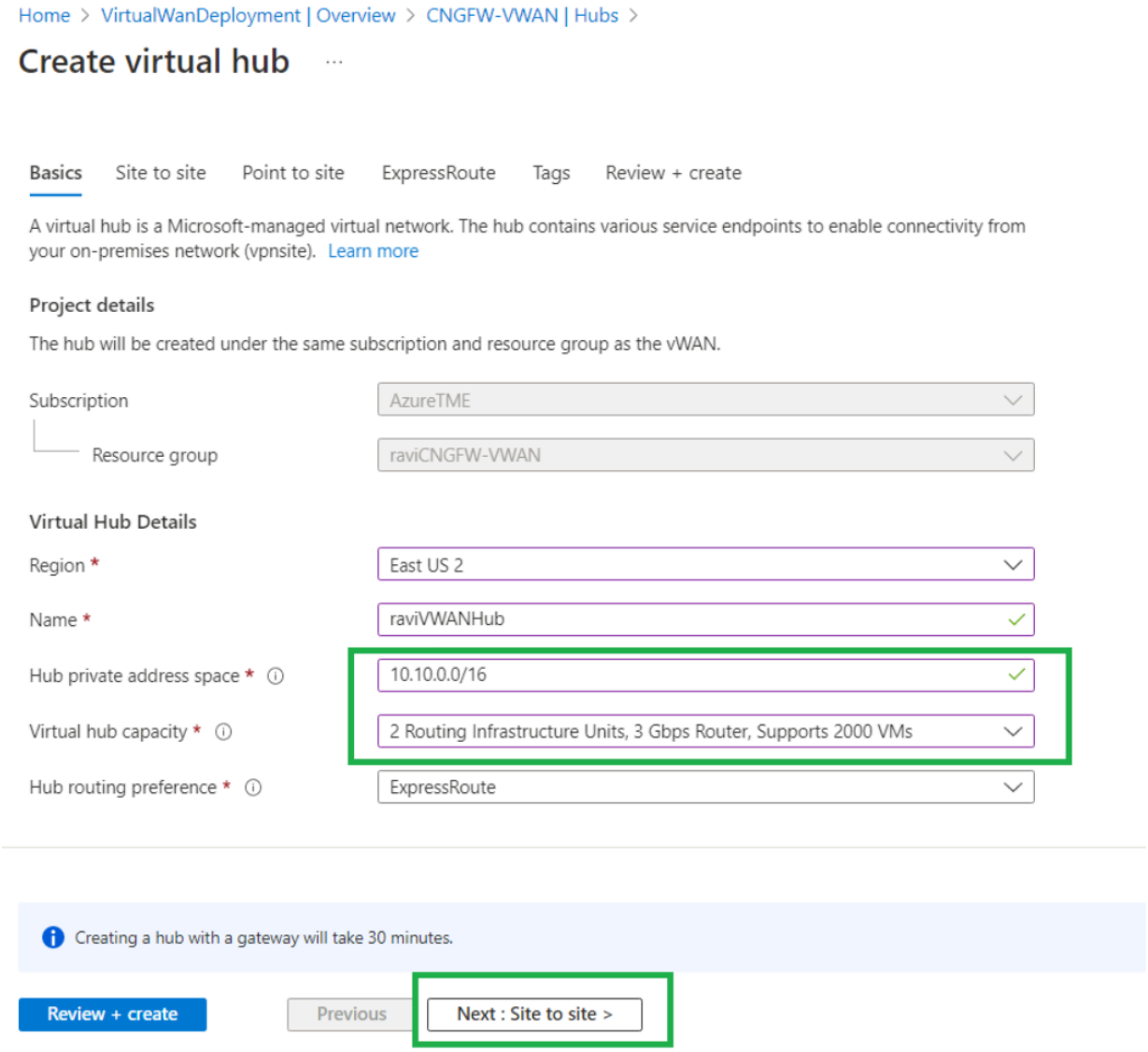
STEP 2 | 仮想WANサービスが正常に作成されたら、[**Go to resource (リソースに移動)**]をクリックします。



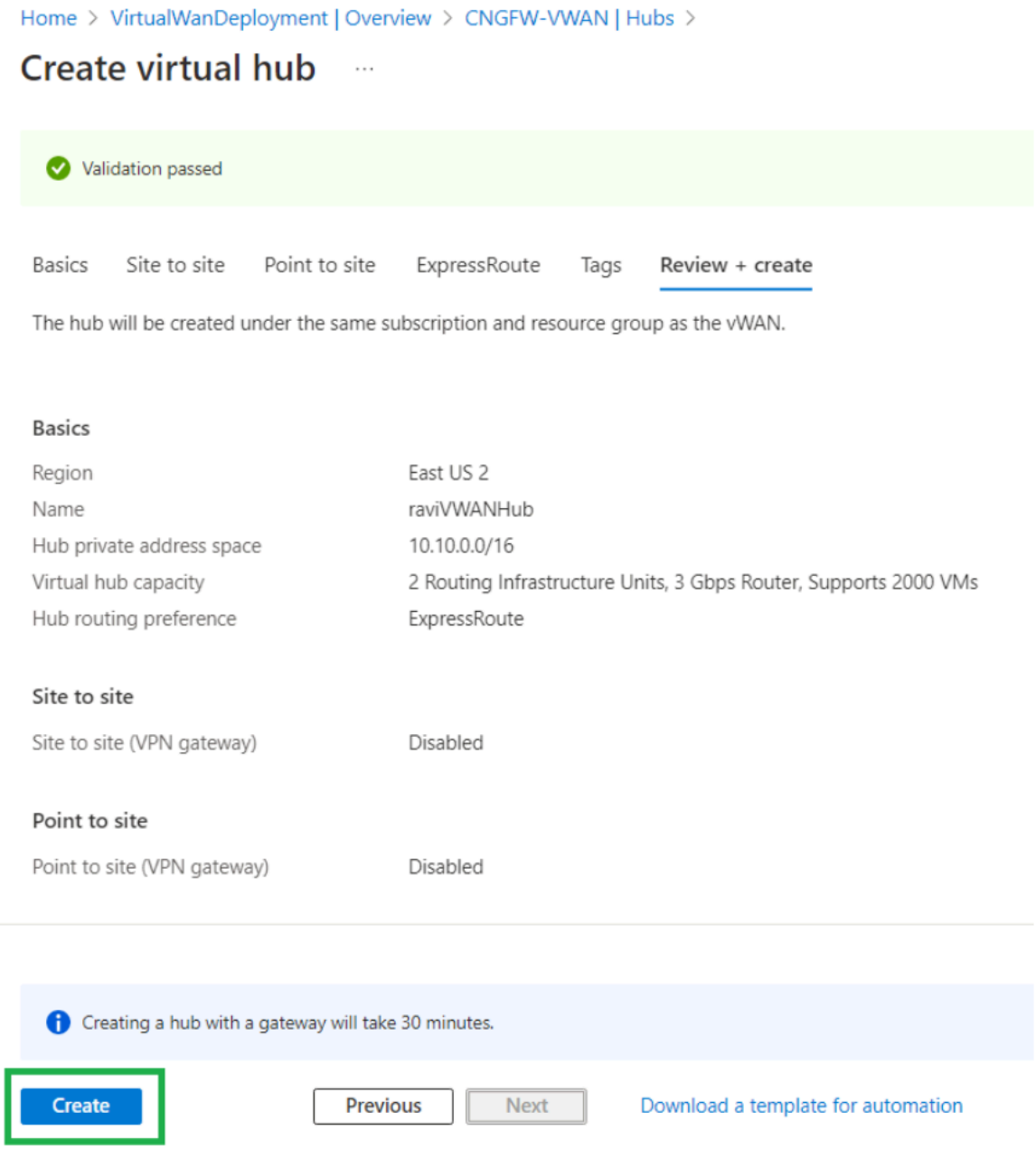
STEP 3 | 作成した仮想WANにハブを追加します。**[Connectivity (接続)] >[Hubs (ハブ)]**を選択します。**[New Hub (新しいハブ)]**をクリックします。



STEP 4 | **[Virtual Hub Details (仮想ハブの詳細)]**を設定します。ハブプライベートアドレスと仮想ハブ容量を指定し、**[Next (次へ)]**をクリックします。サイト間。

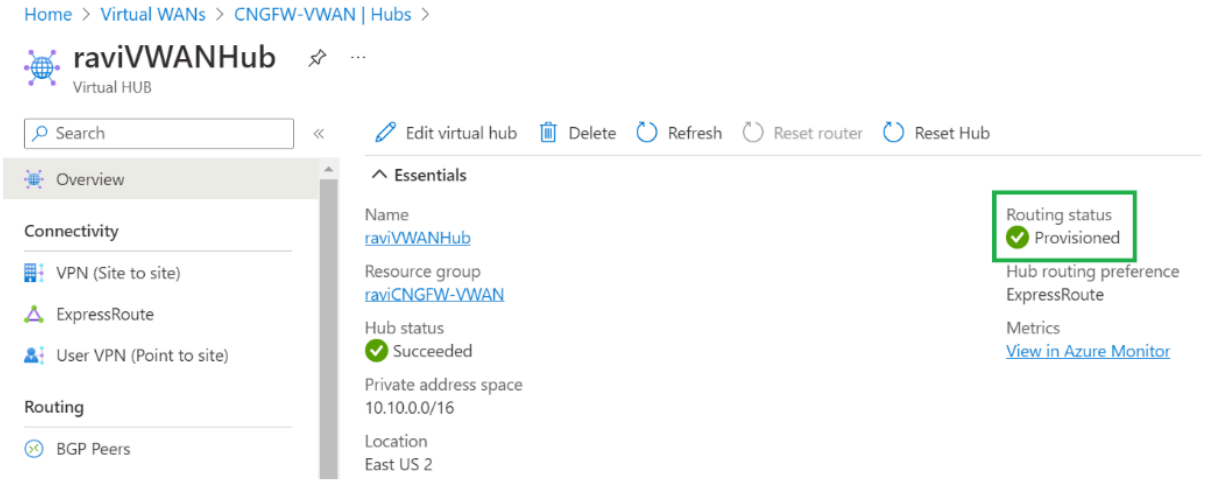


STEP 5 | 設定を確認したら、**[Create (作成)]**をクリックして仮想WANハブを作成します。



STEP 6 | **[Routing status (ルーティング ステータス)]**が**[Provisioned (プロビジョニング済み)]**となっていることを確認します。

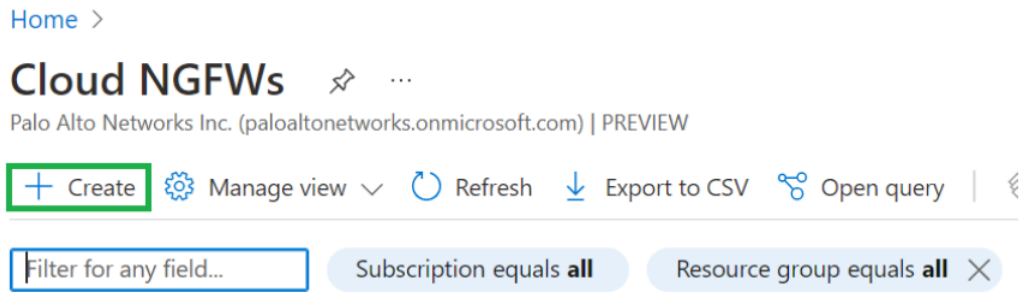
新しい*vWAN*ハブのプロビジョニングには約*30*分かかる場合があります。***[Overview (概要)]***ページを使用して、ルーティングステータスを表示します。



STEP 7 | Azureポータルにログインし、**Palo Alto Networks**の**Cloud NGFW**を検索します。

STEP 8 | **[Cloud NGFWs by Palo Alto Networks]**をクリックして、Azure向けのPalo Alto Networks Cloud NGFWサービスの作成を開始します。

STEP 9 | [**Cloud NGFWs**]画面で、[**Create (**作成**)**]をクリックします。このランディングページには、事前にリソースを作成している場合は、Cloud NGFWインスタンスがあらかじめ入力されています。

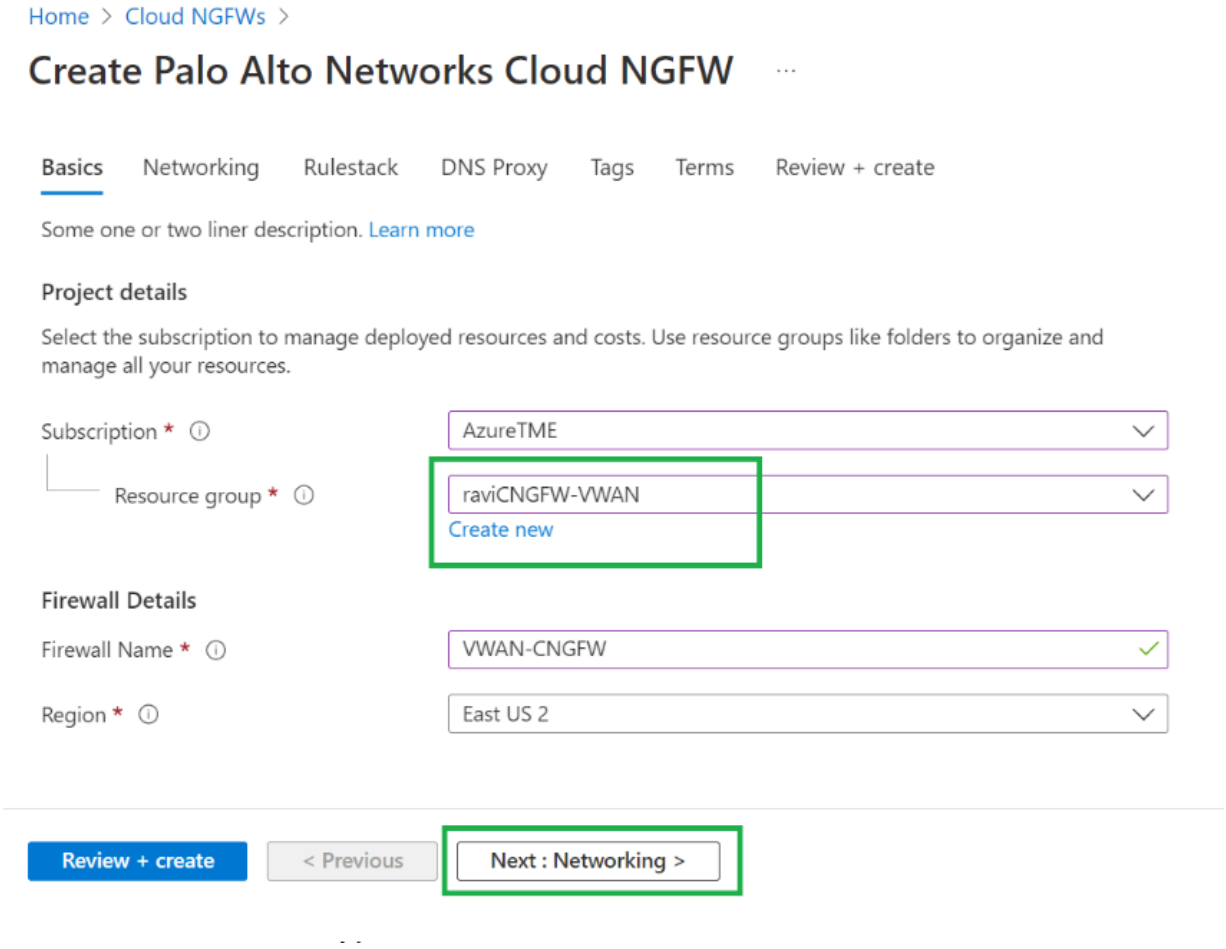


STEP 10 | [**Create Palo Alto Networks Cloud NGFW**]画面で、プロジェクトの詳細セクションに基本構成情報を入力します。

次の表の情報を使用して、プロジェクトの詳細を提供します。

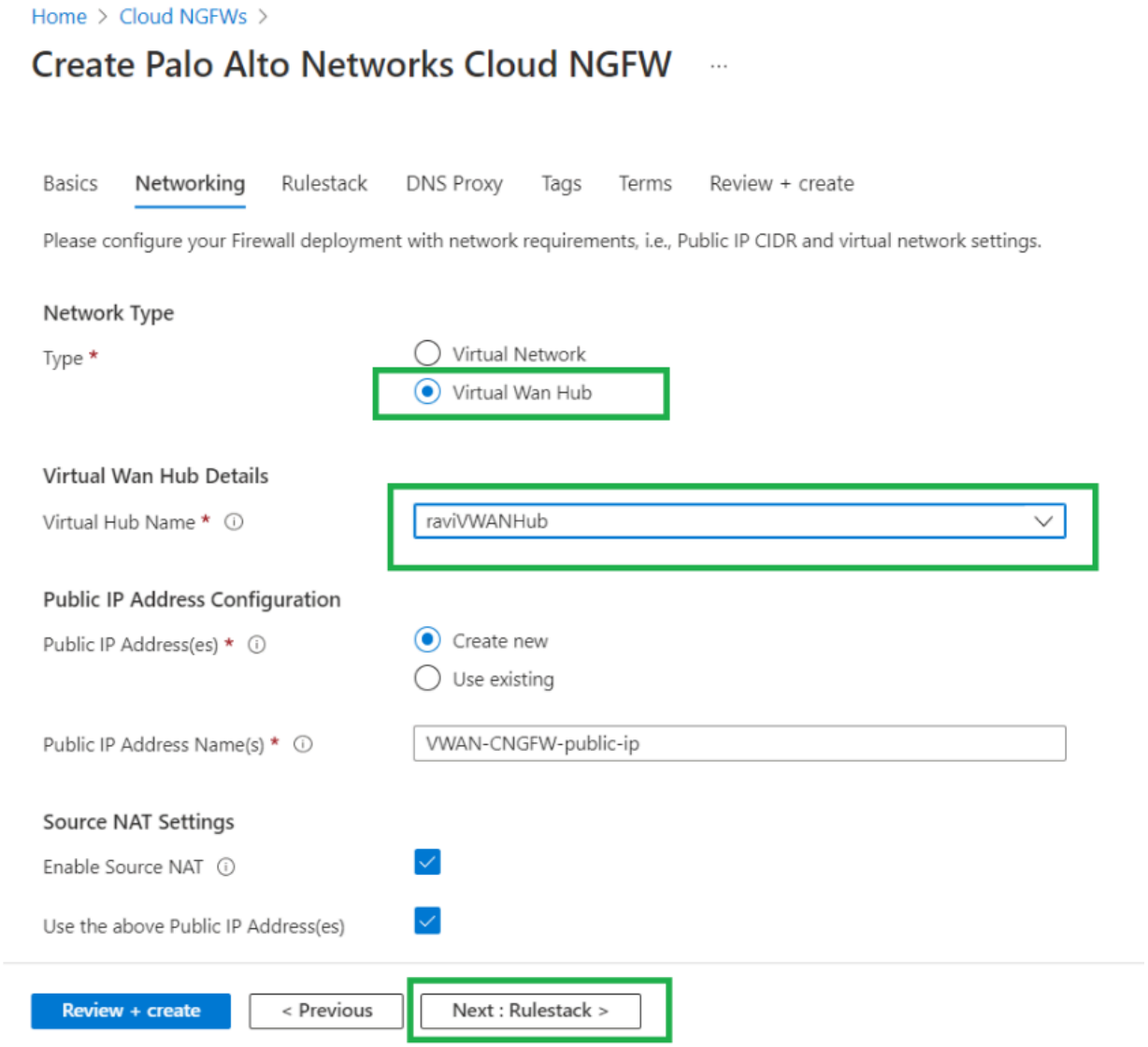
項目	の意味
サブスクリプション	ログイン中に使用されたサブスクリプションに基づいて自動的に選択されます。
リソースグループ	既存のリソースグループのいずれかを使用するか、Cloud NGFWリソースが作成される新しいリソースグループを作成します([**Create New (**新規作成**)**]オプションを使用)。
ファイアウォール名	Cloud NGFW ファイアウォール リソースの名前。

項目	の意味
リージョン	Cloud NGFWがプロビジョニングされるリージョン。

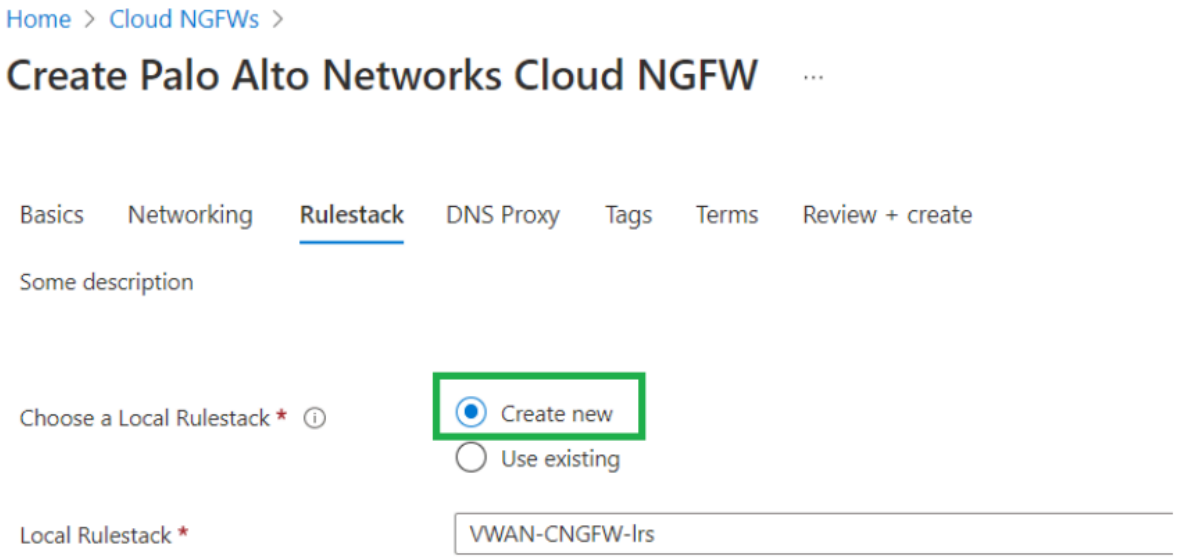


STEP 11 | **NEXT (次へ)** をクリックします。ネットワーク。ネットワーク環境に関する情報を提供します。**[Network Type (ネットワークタイプ)]**に**[Virtual WAN Hub (仮想WANハブ)]**を選択します。**[Virtual WAN Hub Details (仮想WANハブ詳細)]**セクションで、ドロップダウンメニューから以前に作成した仮想ハブ名を選択します。パブリック**IP**アドレスを指定し、イ

ンターネットに出るトラフィックでアドレス変換を使用する場合は送信元**NAT**オプションを指定します。

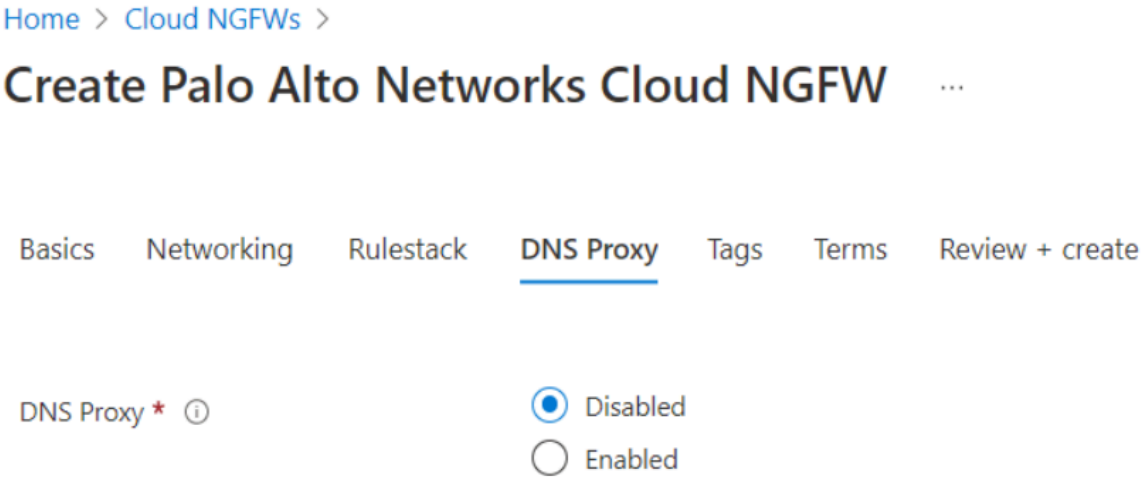


STEP 12 | **NEXT (次へ)** をクリックします。ルールスタック:ルールが定義されているローカルルールスタックを作成します。これはローカルルールスタック作成用のプレースホルダです。**[Create new (新規作成)]**または**[Use existing (既存の使用)]**をクリックします(ローカルルールスタックがすでに存在する場合は、ドロップダウンメニューから選択します)。Cloud NGFWリソースを作成した後、このルールスタックを変更して、ルール、FQDN、プレフィックスリストを追加または編集できます。



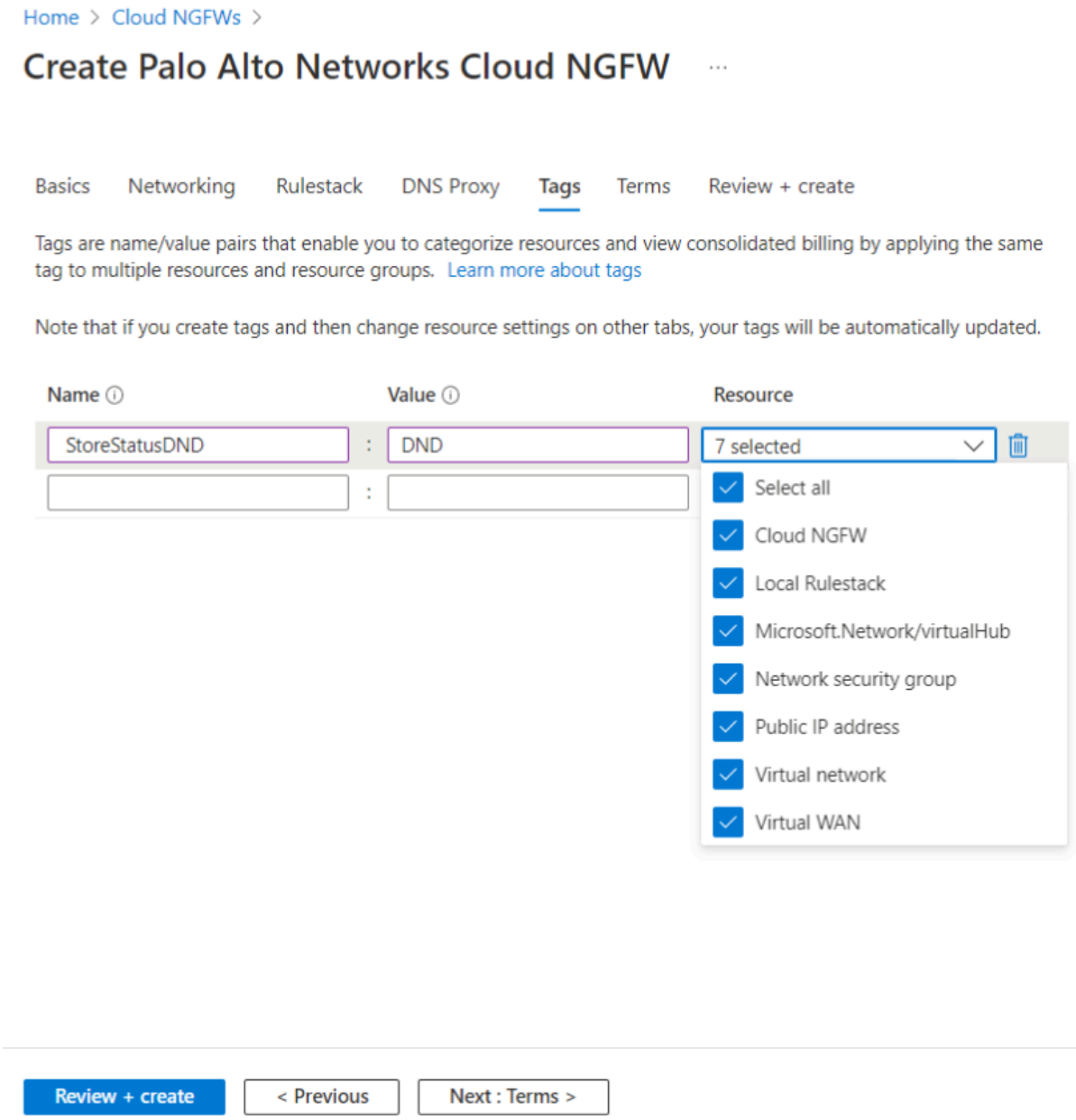
STEP 13 | **NEXT (次へ)** をクリックします。**DNS** プロキシ。デフォルトでは、DNSプロキシは無効になっています。vWANリソースのプロキシとして機能することで、すべてのDNSトラフィッ

クを検査するようにCloud NGFWを設定できます。設定すると、DNSプロキシはDNSリクエストをデフォルトのAzure DNSサーバー、または指定したDNSサーバーに転送します。



STEP 14 | **[Next:Tags (次へ:タグ)]**をクリックして、Azure要件のタグを指定します。タグは、環境内の脆弱性を管理したり、Azureアカウントに関連する統合課金を表示したりするのに役立つ事

前定義されたラベルです。タグは、一元的に定義され、脆弱性やポリシー例外として設定できます。



タグは次のように使用されます。

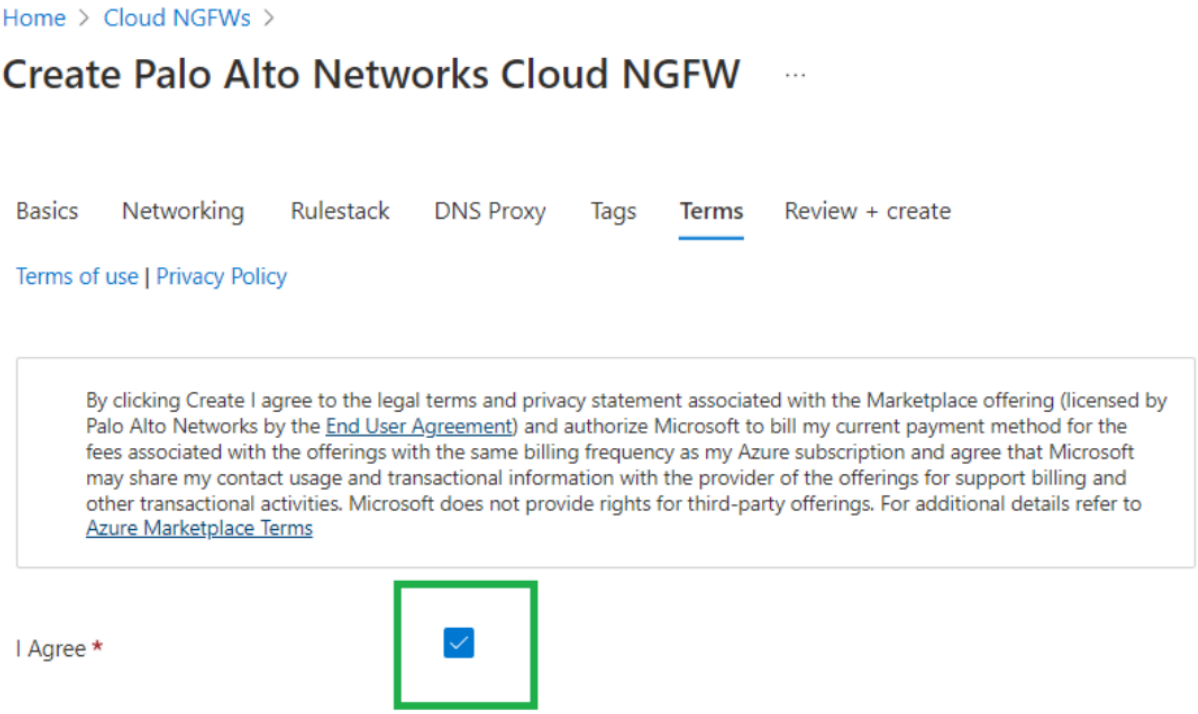
- 脆弱性ラベル。環境内の脆弱性を分類する便利な方法を提供します。
- ポリシーの例外。タグ付けされた脆弱性に特定の影響を与えるために、これらのルールを各自のルールに組み入れることができます。
- Azureアカウントの統合請求を表示します。

  タグは、複数のチームが同じ環境で作業する大規模なコンテナ展開がある場合に便利です。たとえば、様々な種類の脆弱性を処理する様々なチームがいる場合があります。その場合、タグを設定して、脆弱性に対する責任を定義できます。他の用途としては、脆弱性の修正ステータスを設定したり、近い将来修正できない既知の問題であれば無視される脆弱性とマークしたりすることができます。

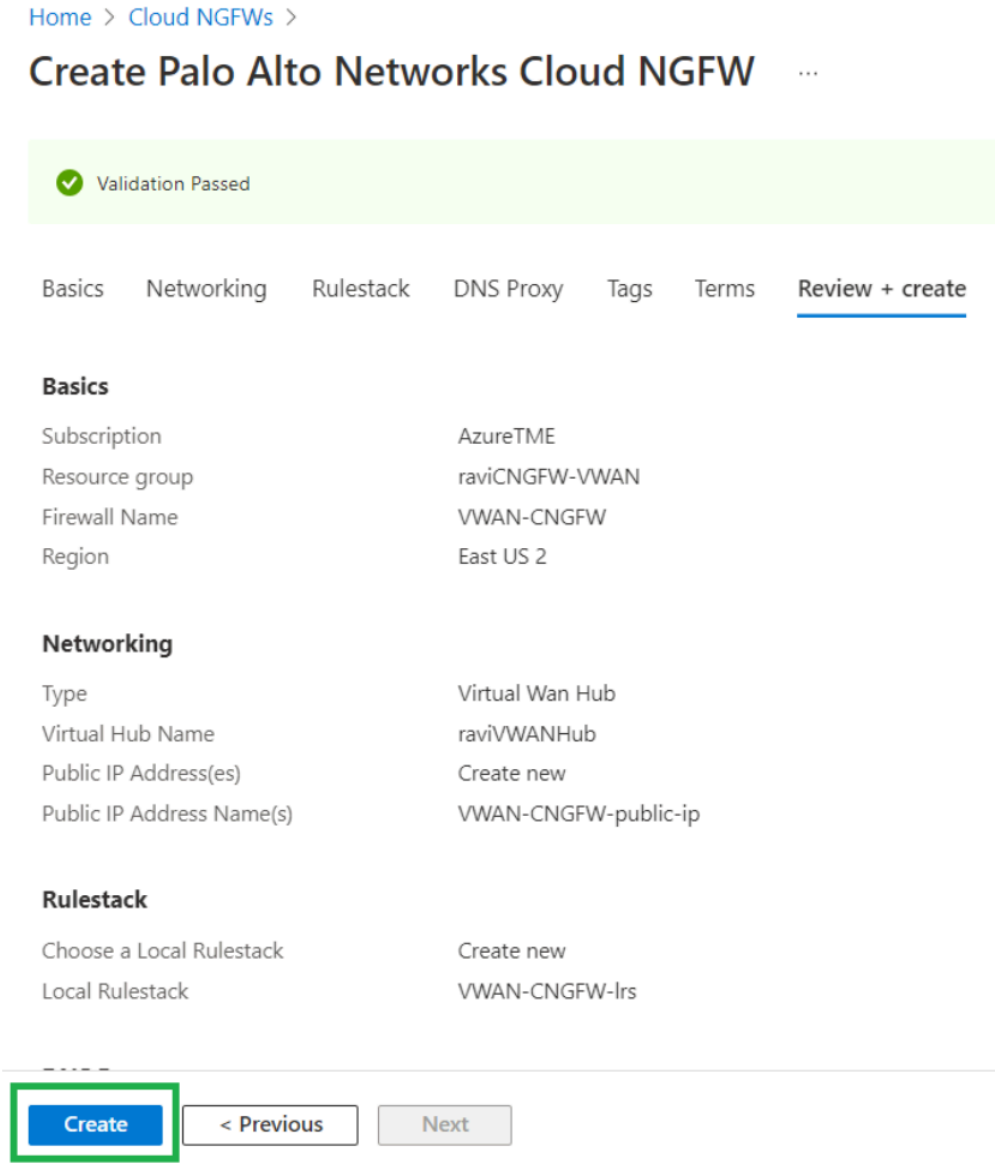
  タグはいくつでも定義できます。*Azure*アカウントのタグの作成については、「Use tags to organize your Azure resources and management hierarchy (タグを使用してAzureリソースと管理階層を整理する)」を参照してください。

STEP 15 | **[Next:Terms (次へ:条件)]**をクリックし、デプロイメント条件に同意します。

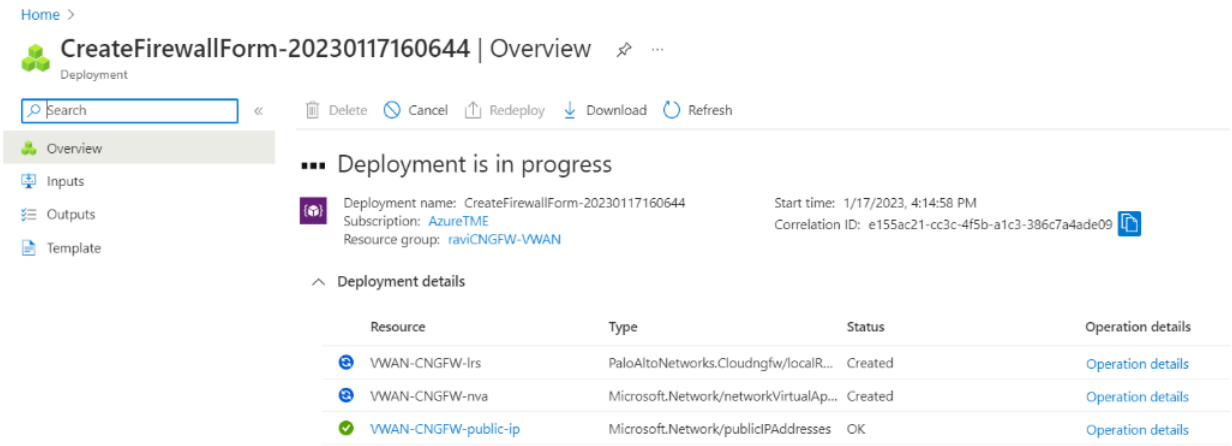


STEP 16 | **[Review + create (レビュー＋作成)]**をクリックして、Cloud NGFWリソースのAzureサブスクリプションの検証を確認します。リソースはまず検証され、次に作成されます。画面

に**[Validation Passed (**検証に合格しました**)]**と表示されます。**[Create (**作成**)]**をクリックして、Cloud NGFW サービスをデプロイします。

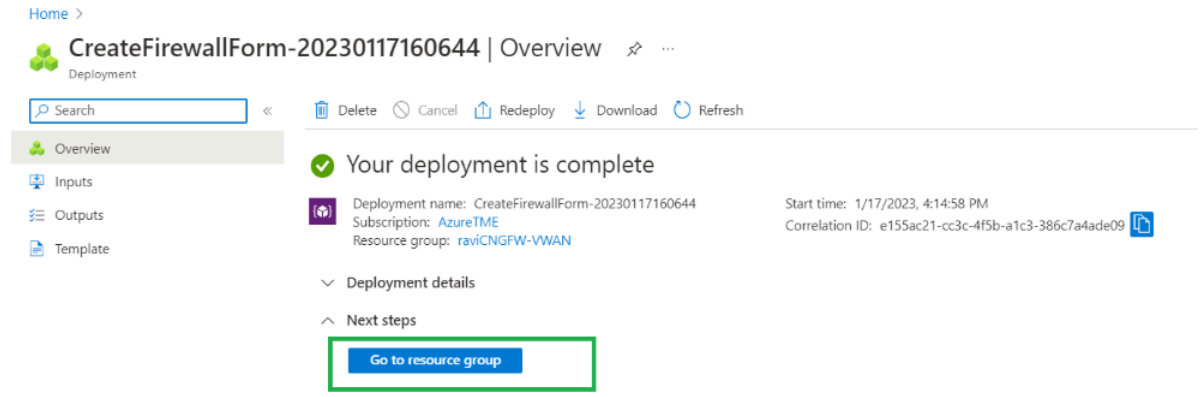


Cloud NGFWサービスの作成後、導入の進行状況が表示されます。

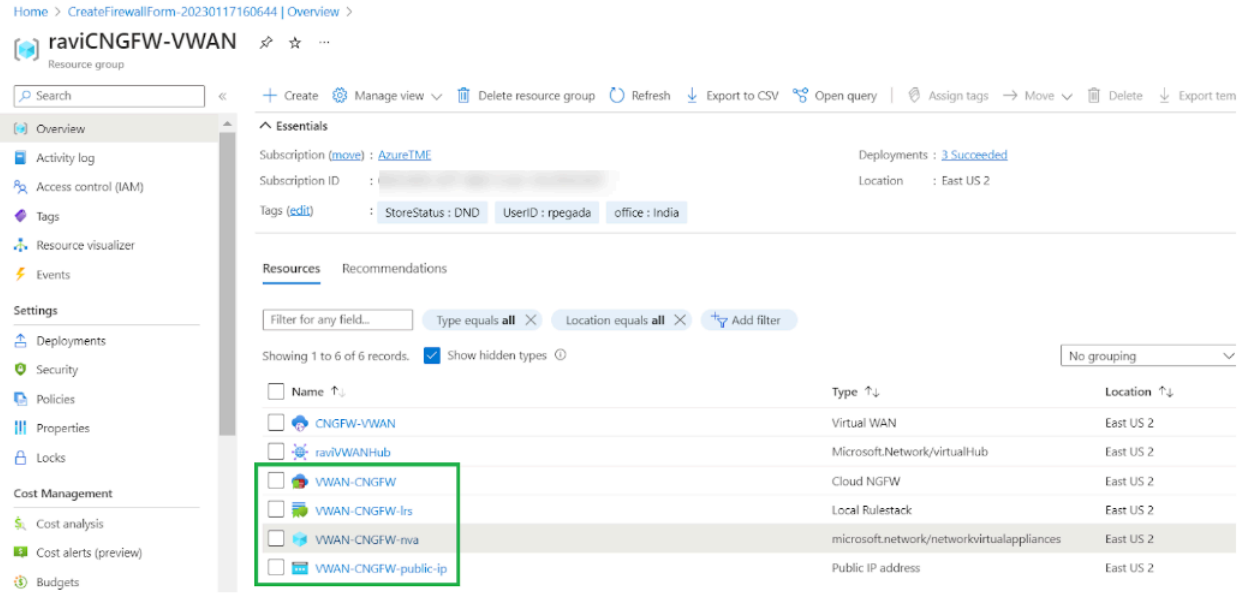


*Cloud NGFW*リソースの完了には約*30*分かかります。

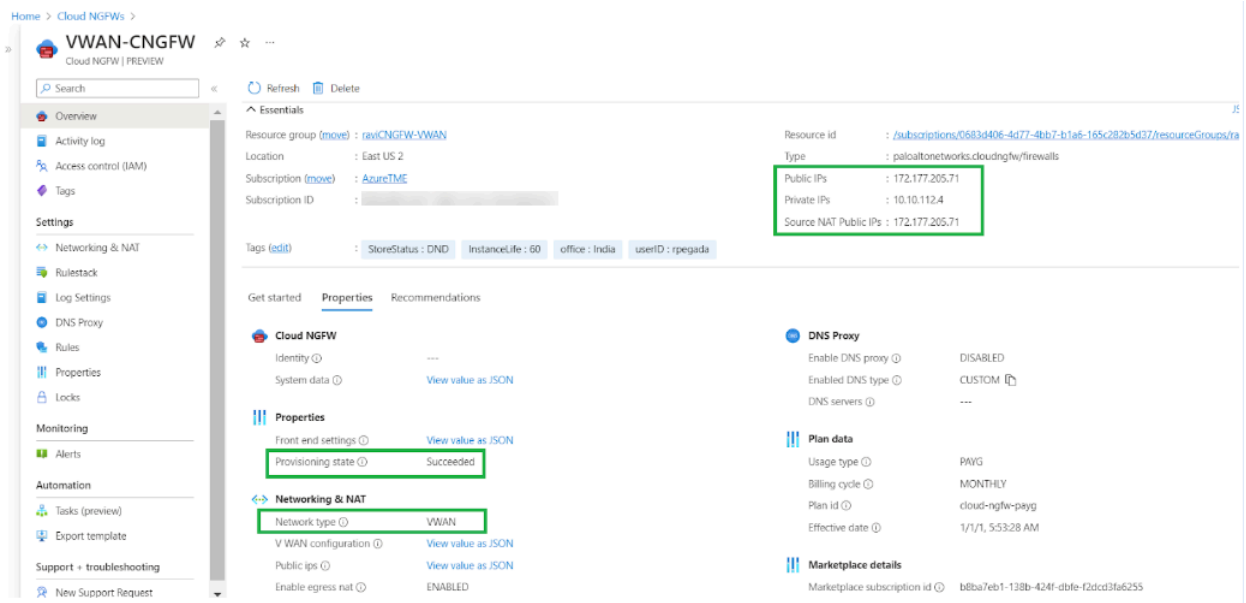
正常にデプロイされると、次の画面が表示されます。



STEP 17 | Cloud NGFW、ローカルルールスタック、パブリックIPアドレス、Cloud-nvaを含む4つのリソースが作成されます。



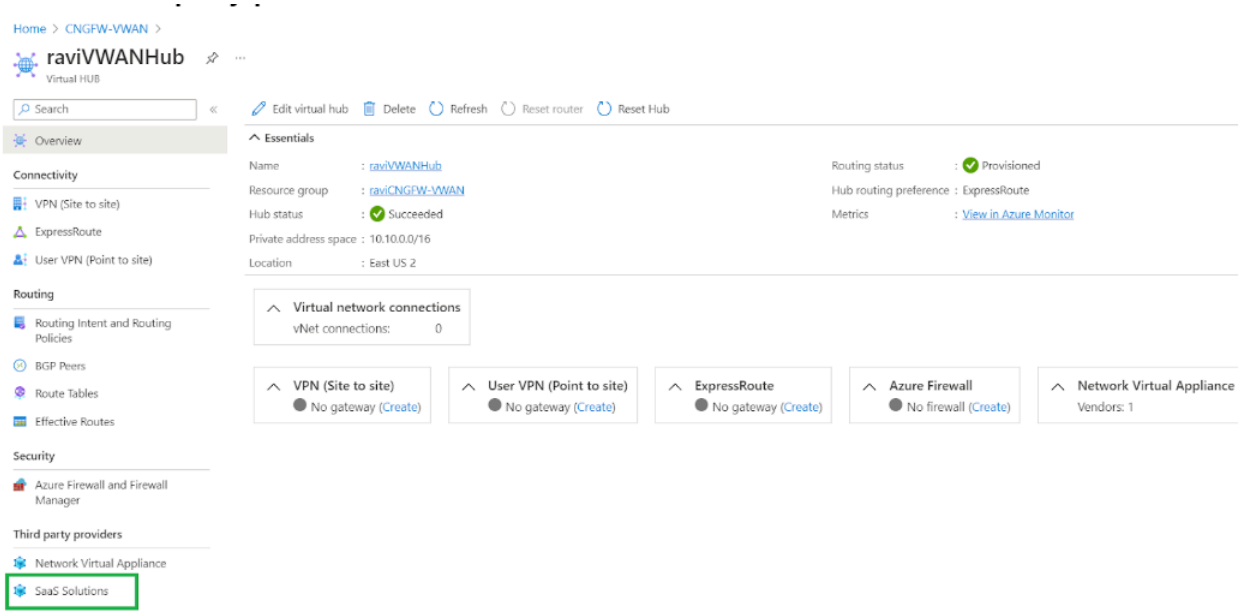
STEP 18 | Cloud NGFWリソースを作成したら、それを選択してプロビジョニング状態がSucceededであることを確認します。このページでは、Cloud NGFWサービスに関連付けられているパブリックIPアドレスとプライベートIPアドレスも表示されます。ネットワークの種類がvWANであることを確認します。



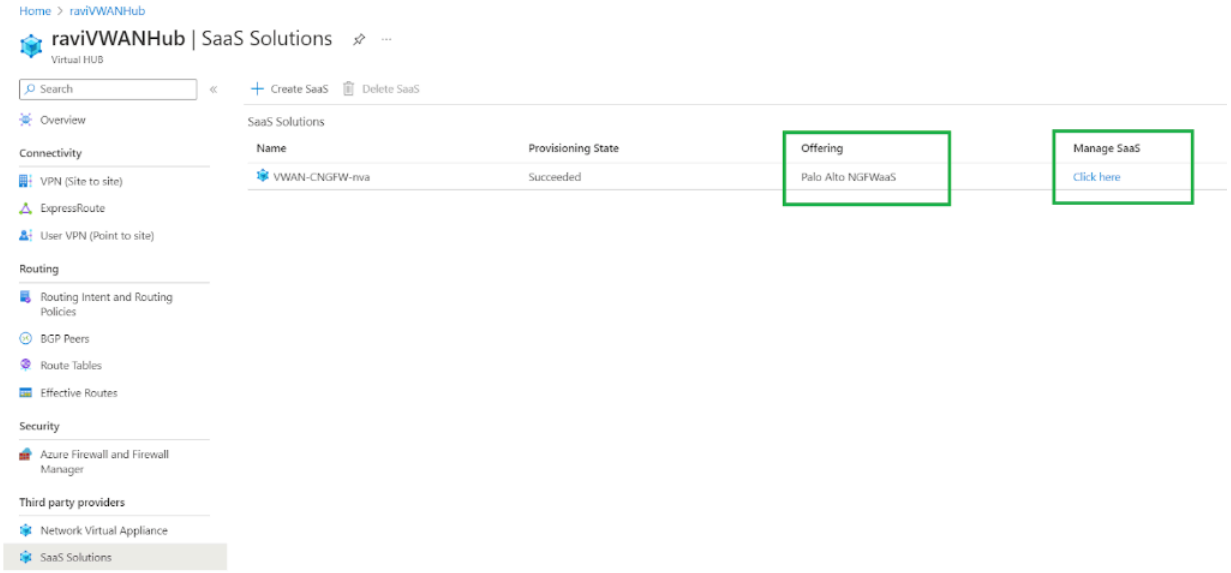
vWANへのCloud NGFWのデプロイを確認

vWANネットワークタイプのCloud NGFWサービスが正常に作成されたら、Cloud NGFWがvWANのSaaSソリューションとして追加されたことを確認します。

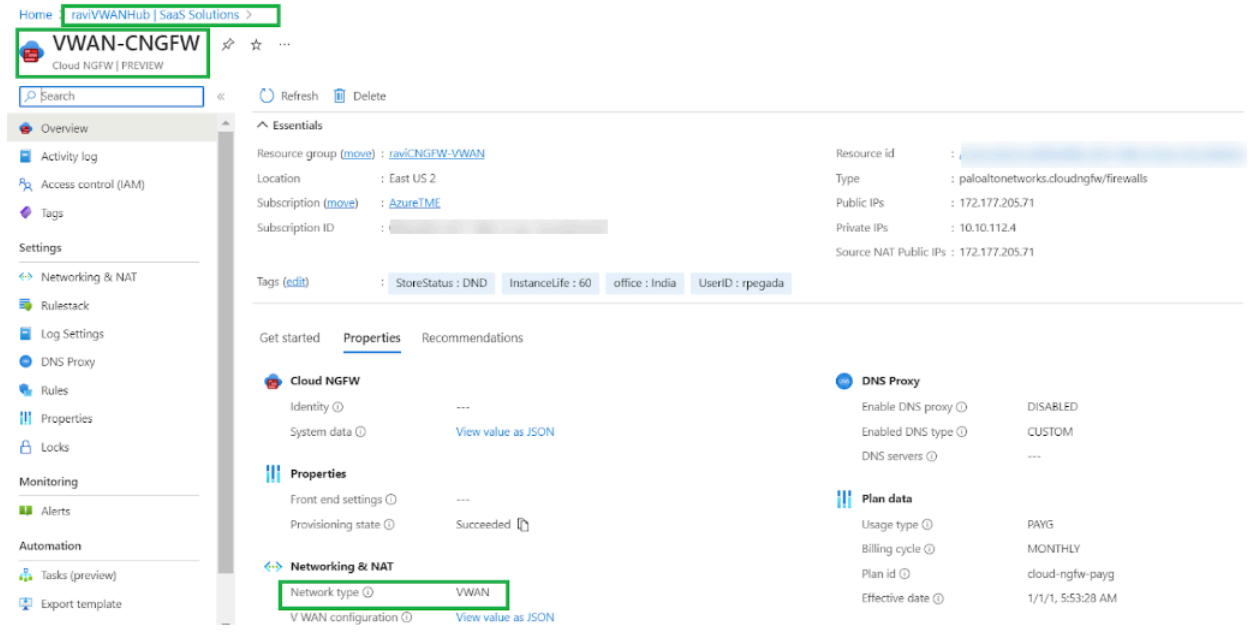
STEP 1 | Cloud NGFWサービスの作成時に使用したVirtual Hubに移動します。**[Third party providers (第三者プロバイダ)]**セクションで、**[SaaS Solutions (SaaSソリューション)]**をクリックします。



STEP 2 | Cloud NGFWが作成されたことを確認します。このハブにSaaSソリューションとして追加されます。**[SaaS Solutions (SaaSソリューション)]**セクションで**[Click here (**ここをクリック**)]**を選択します。



vWANの展開に関連する情報が表示されます。



vWANデプロイメント後の設定例

デプロイメント後

デプロイメントを確認したら、デプロイメント後の次のタスクを実行します。

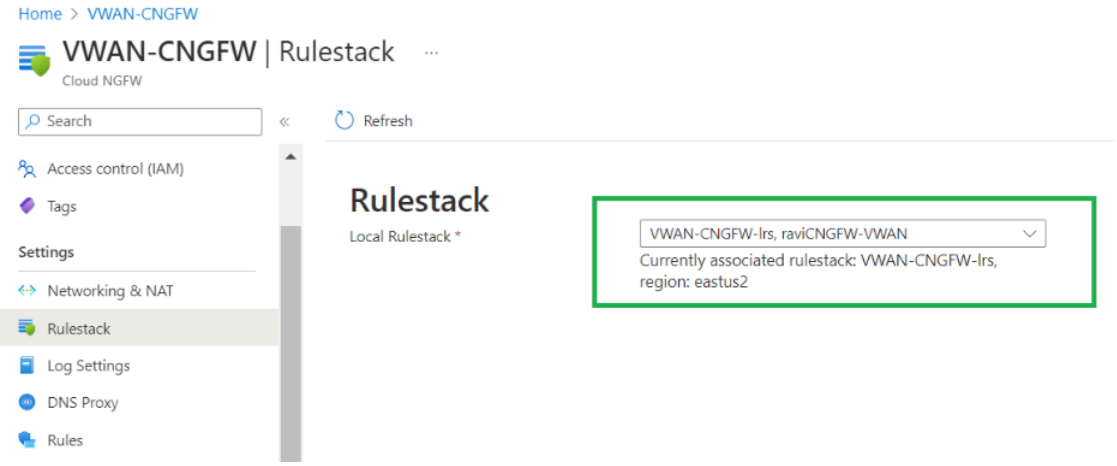
- ルールスタックを作成または更新する

- Cloud NGFW上の送信元/宛先NATルール
- ロギングの設定
- 仮想WANへの仮想ネットワーク接続としてのアプリケーションvNETの追加
- vWANハブのルーティングインテントとルーティングポリシーの設定

ルールスタックを作成または更新する

既存のルールスタックを更新する方法：

STEP 1 | Azure Resource Manager（ARM）コンソールで、構成するCloud NGFWリソースの［**Rulestacks (**ルールスタック**)**］をクリックします。Cloud NGFWサービスに関連付けられているルールスタックが、リソースグループとともに表示されます。

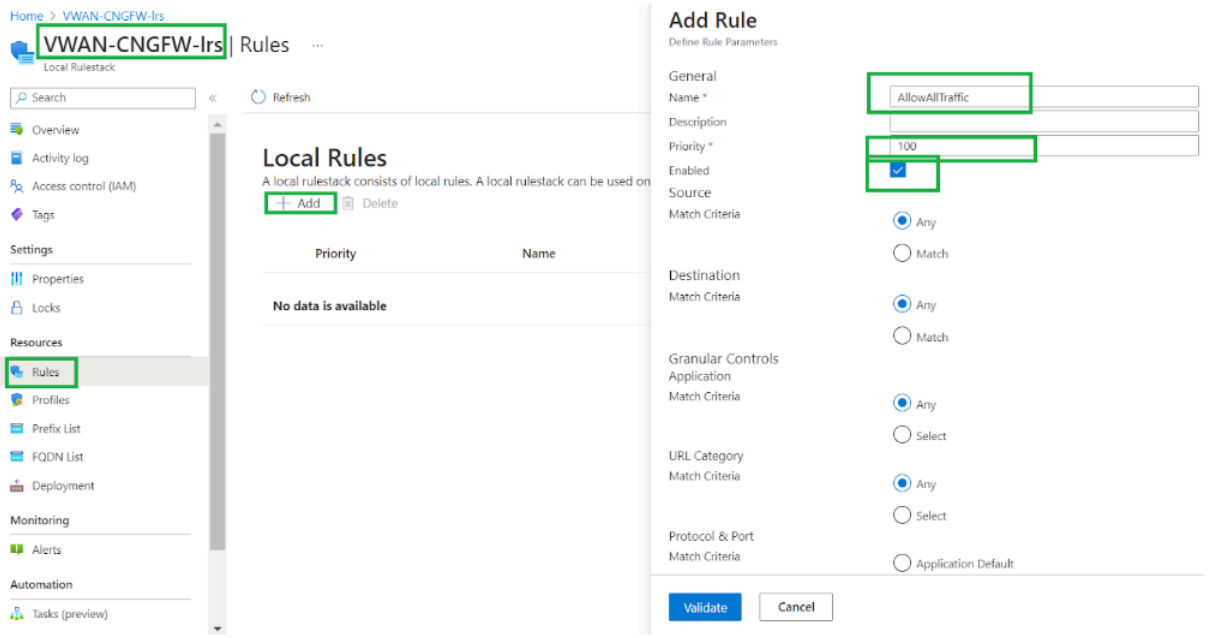


STEP 2 | ルールスタックを変更してファイアウォールルールを追加します。これらのルールは、特定のトラフィックをブロックしながら一部のトラフィックを許可します。デフォルトでは、Cloud NGFWはすべてのトラフィックをブロックします。Azureポータルが提供するグローバル検索オプションを使用して、以前に作成したローカルルールスタックを検索します。

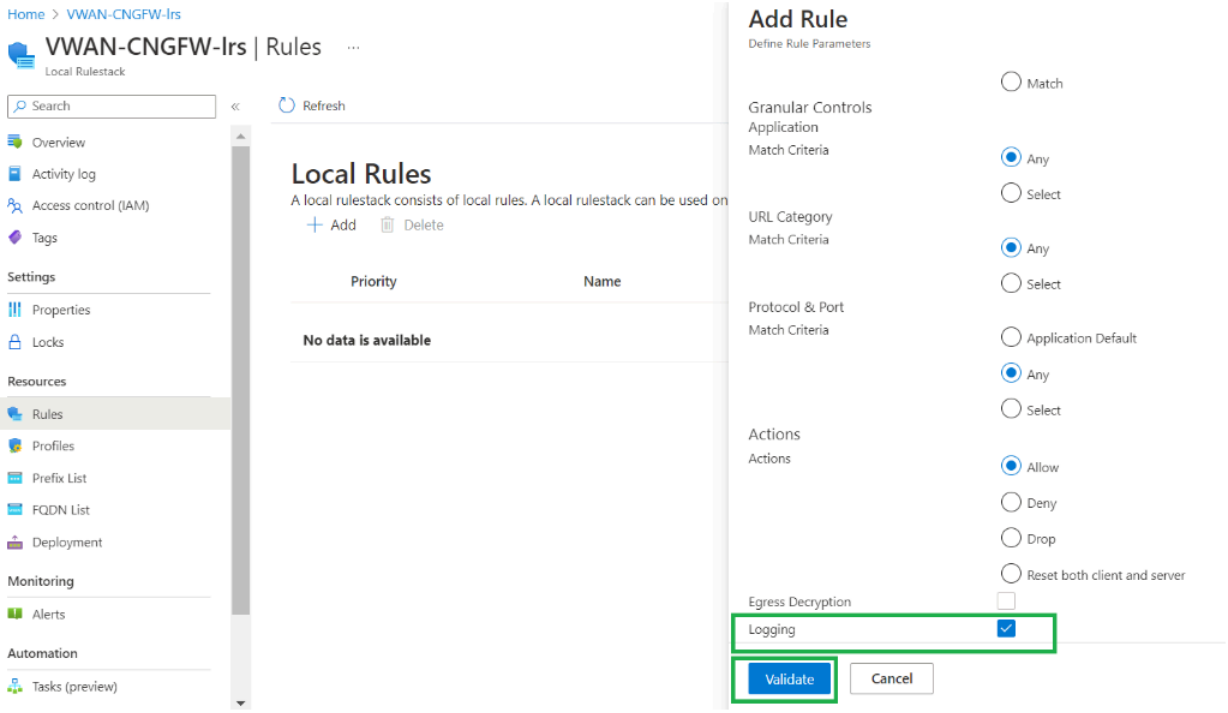
STEP 3 | Cloud NGFWサブスクリプションに関連付けられている以前に作成したローカルルールスタックを選択し、［**Rules (**ルール**)**］を選択します。

STEP 4 | **[Local Rules (**ローカルルール**)]**セクションで、**[Add (**追加**)]**をクリックします。**[Add Rule (**ルールの追加**)]**ウィンドウで、ルールを変更します。たとえば、トラフィックを許可する

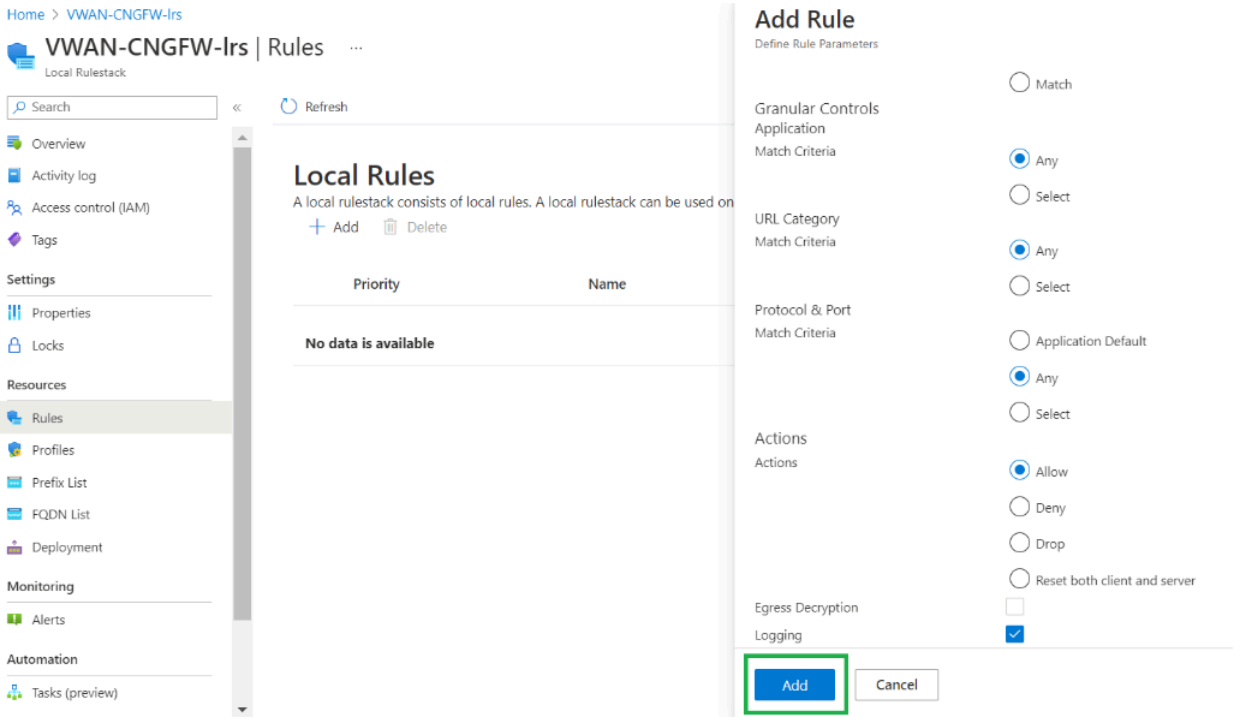
ルールを追加します。必須フィールドに入力し、残りのフィールドにはデフォルト設定を使用します。



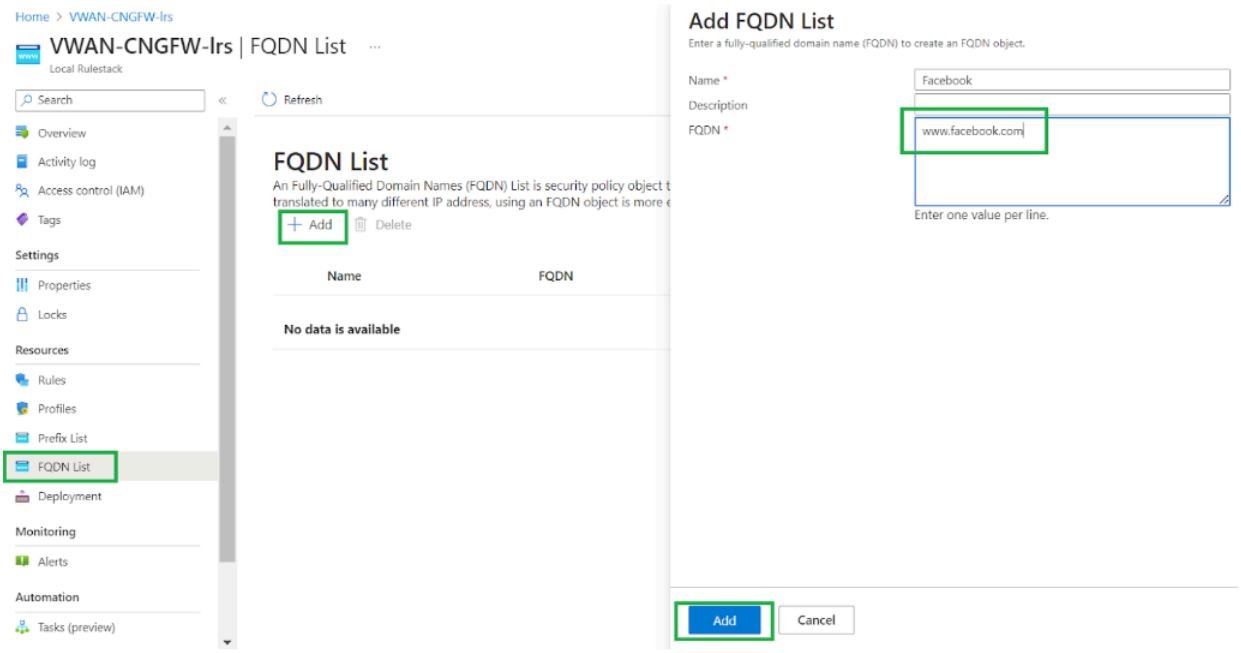
STEP 5 | ルールのロギングを有効にします。[Add Rule (ルールの追加)]ウィンドウで、**[Logging (ロギング)]**を選択します。



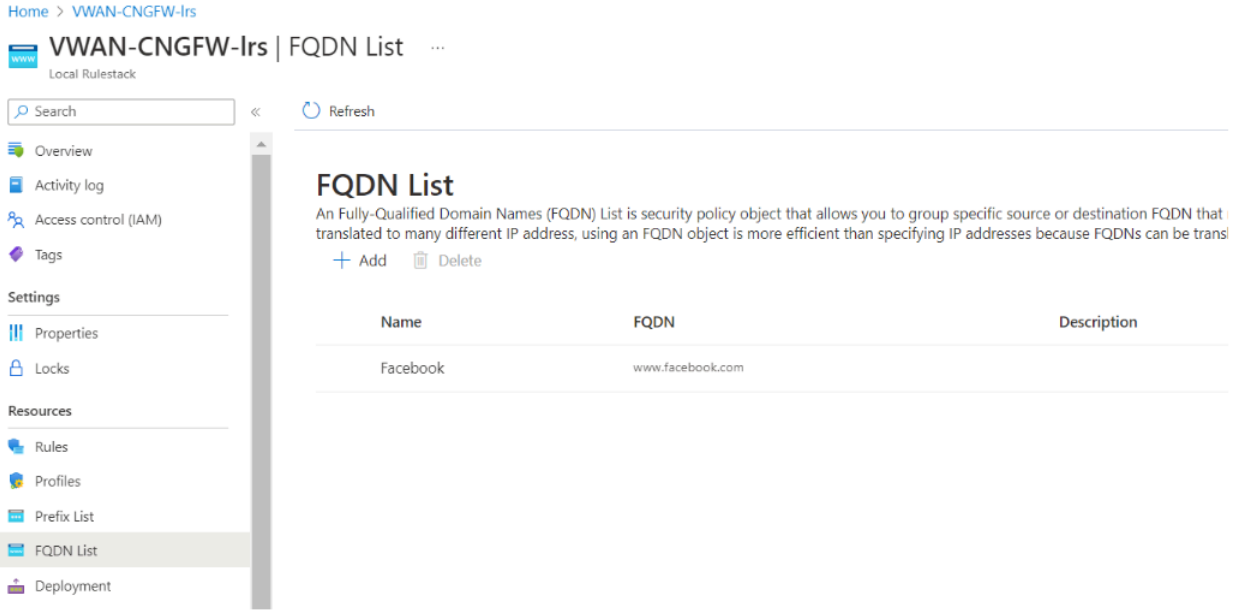
STEP 6 | **[Validate (検証)]**をクリックし、**[Add (追加)]**をクリックしてルールスタックにルールを追加します。



STEP 7 | URLを指定する**FQDN**リストを追加してから、実行するアクションを指定します。たとえば、URL www.facebook.com にアクセスしようとするトラフィックをドロップするアクションを FQDN ルールに適用できます。



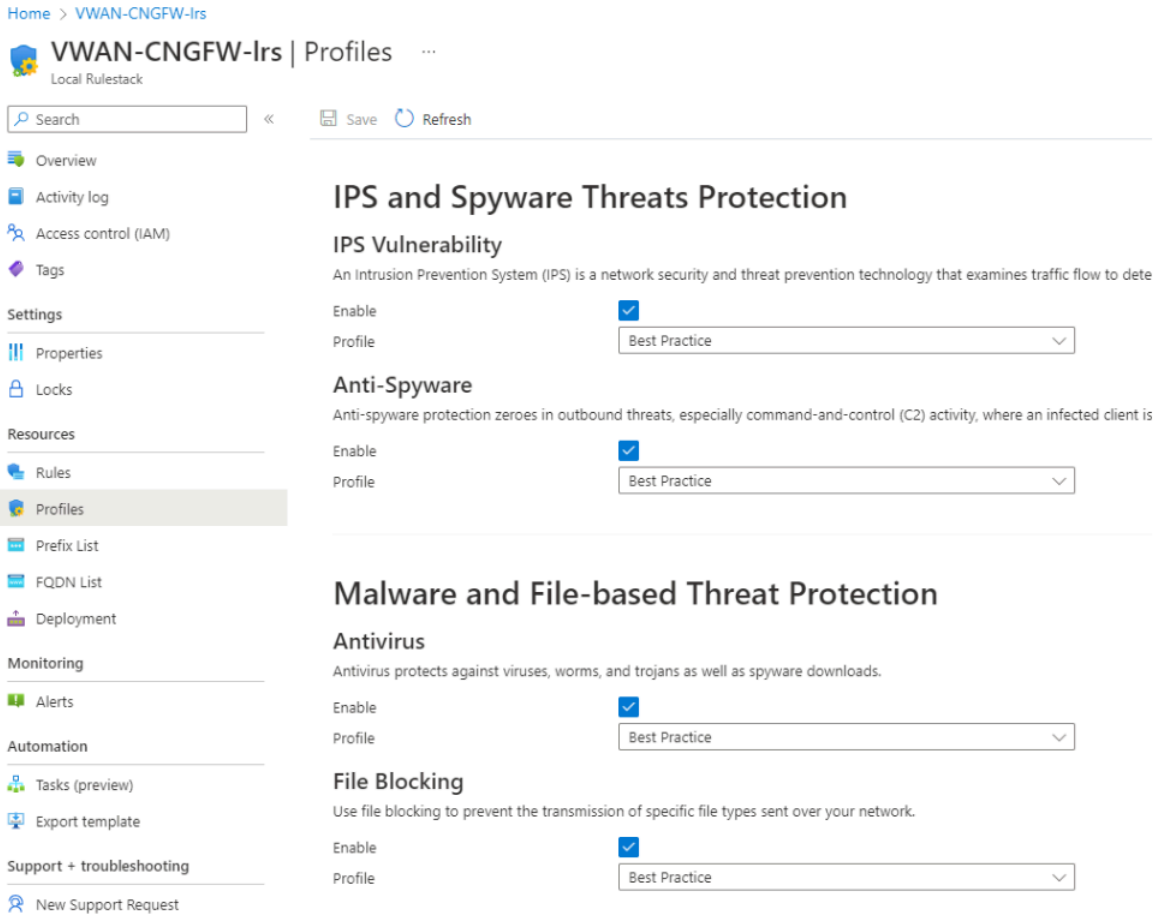
入力したURLがFQDNリストに表示されていることを確認します。



STEP 8 | ルール設定ページに戻り、新しく作成したFQDNリストに一致するルールを追加します。アクションを**[Drop (ドロップ)]** トラフィックに設定します。

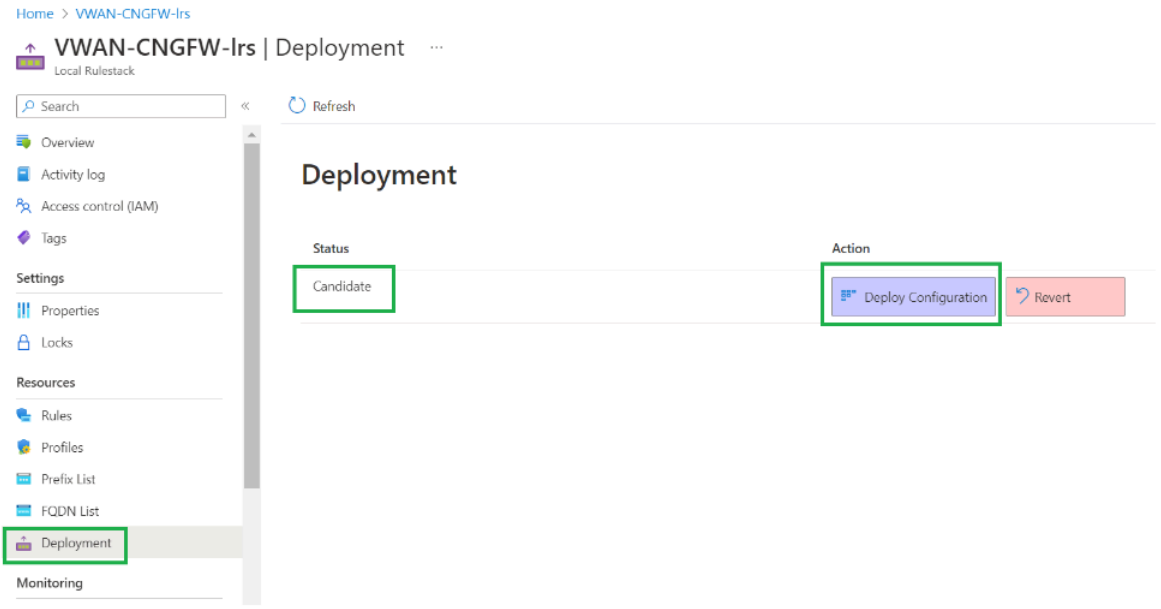
両方のルールが［Local Rules (ローカルルール)］ページに表示されます。

STEP 9 | Cloud NGFWサービスの一部として、セキュリティプロファイルはデフォルトでベストプラクティス設定で有効化されます。サービスを開始およびデプロイすると、トラフィックは最適なセキュリティプロファイルで保護されます。［**Profiles (**プロファイル**)**］を選択すると、これらのセキュリティプロファイルが表示されます。

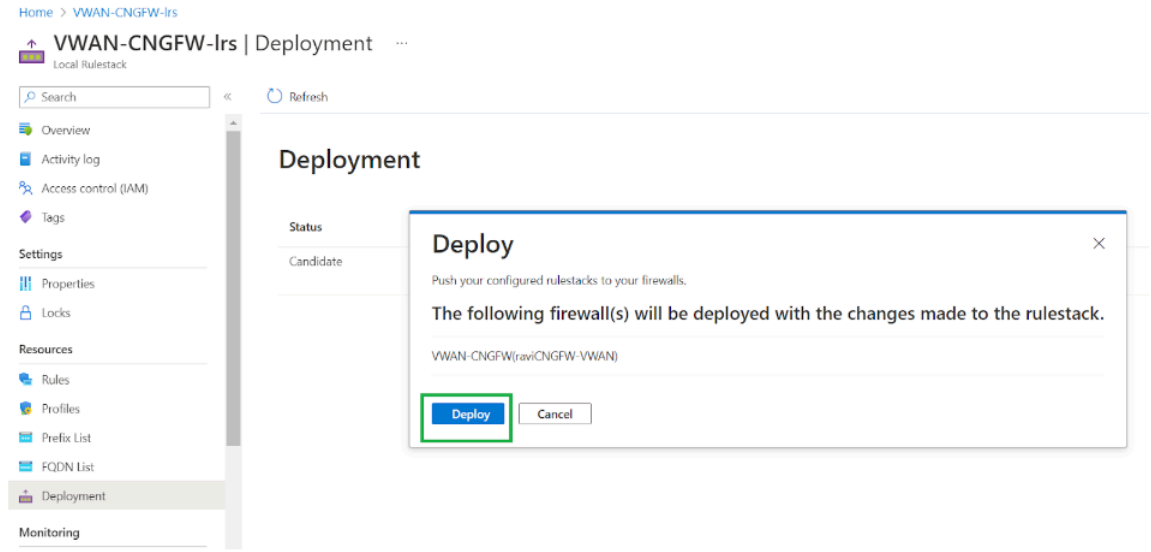


STEP 10 | ルールを変更したら、Cloud NGFWサービスに関連付けられたローカルルールスタックに展開します。**[Deployment**デプロイメント**]**をクリックします。デプロイメントステータスが**[Candidate (**候補**)]**と表示されます。これは、設定が構築されたがまだデプロイされていないことを意味します。**[Deploy Configuration (**設定のデプロイ**)]**をクリックして、設定

をCloud NGFWサービスに展開します。ルールスタックを導入するには、この手順を完了する必要があります。



STEP 11 | **[Deploy Configuration (**設定のデプロイメント**)]**をクリックすると、ルールスタックに関連付けられているファイアウォールを示すメッセージが表示されます。［**Deploy (**デプロイ**)**］をクリックして、ルールスタックを使用するすべての関連するファイアウォールにこのルールスタックを構成します。



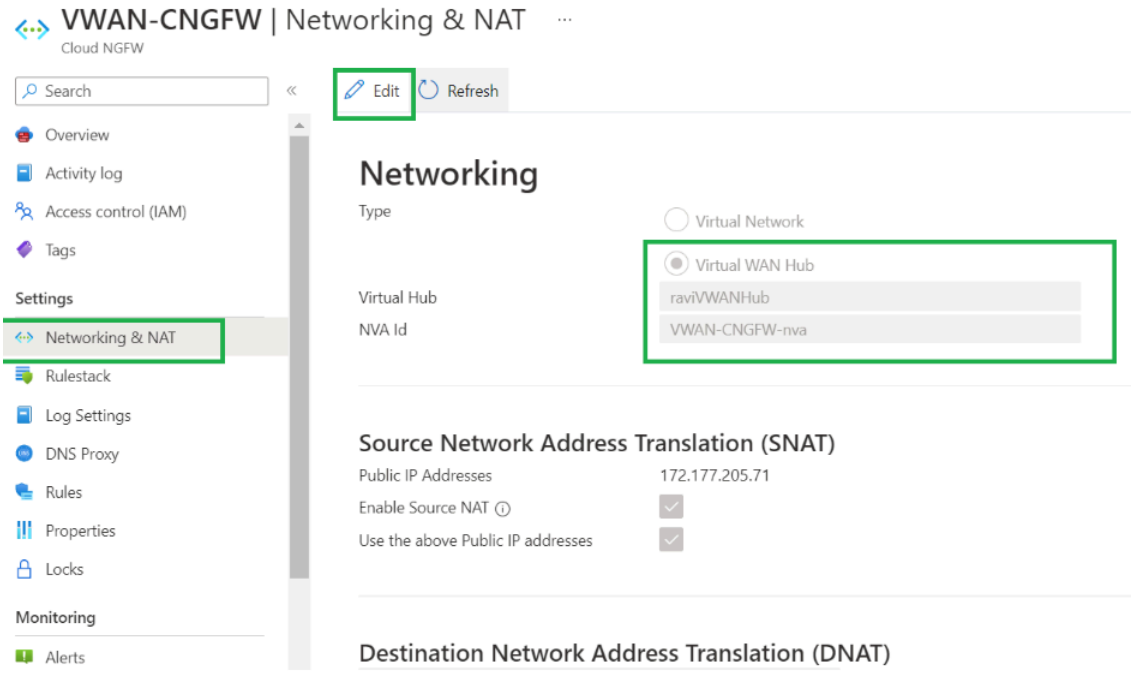
設定が正常にデプロイされると、画面にデプロイステータスが「実行中」と表示されます（Cloud NGFWとローカルルールスタックが正常にデプロイされています）。

Cloud NGFW上の送信元/宛先NATルール

Cloud NGFW上のフロントエンド構成で宛先NATルールを設定し、インバウンドトラフィックをvWAN上のアプリケーションに向けます。

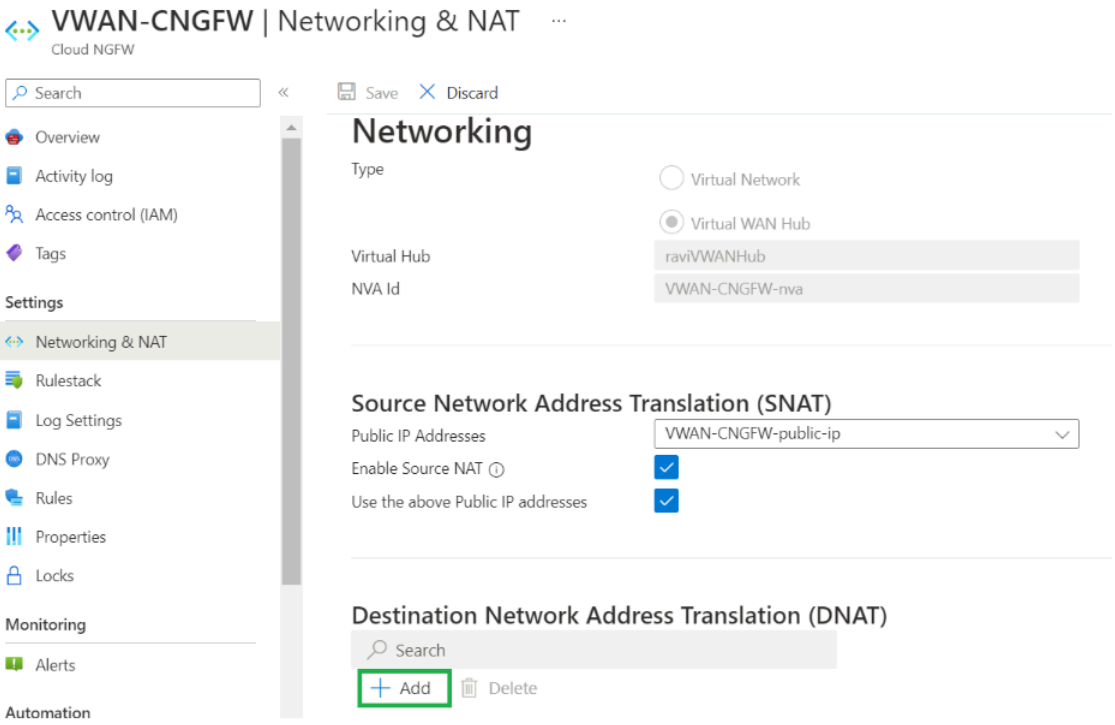
STEP 1 | Cloud NGFWリソースの［**Networking & NAT (ネットワークとNAT)**］設定画面にアクセスします。この画面で、ネットワークタイプが**Virtual WAN Hub (仮想WANハブ)**かどうか、および**Source NAT (送信元NAT)**フィールドのステータス（有効または無効）を確認します。送信元NATが有効だった場合は、この画面に表示されます。

STEP 2 | **[Edit (編集)**］ をクリックして、宛先 NAT ルールを追加します。



STEP 3 | フロントエンド設定の宛先 NAT ルールを追加します。フロントエンドIPアドレスは、Cloud NGFWに関連付けられたパブリックIPアドレスを表します。ドロップダウンメニューを使用してアドレスを選択します。

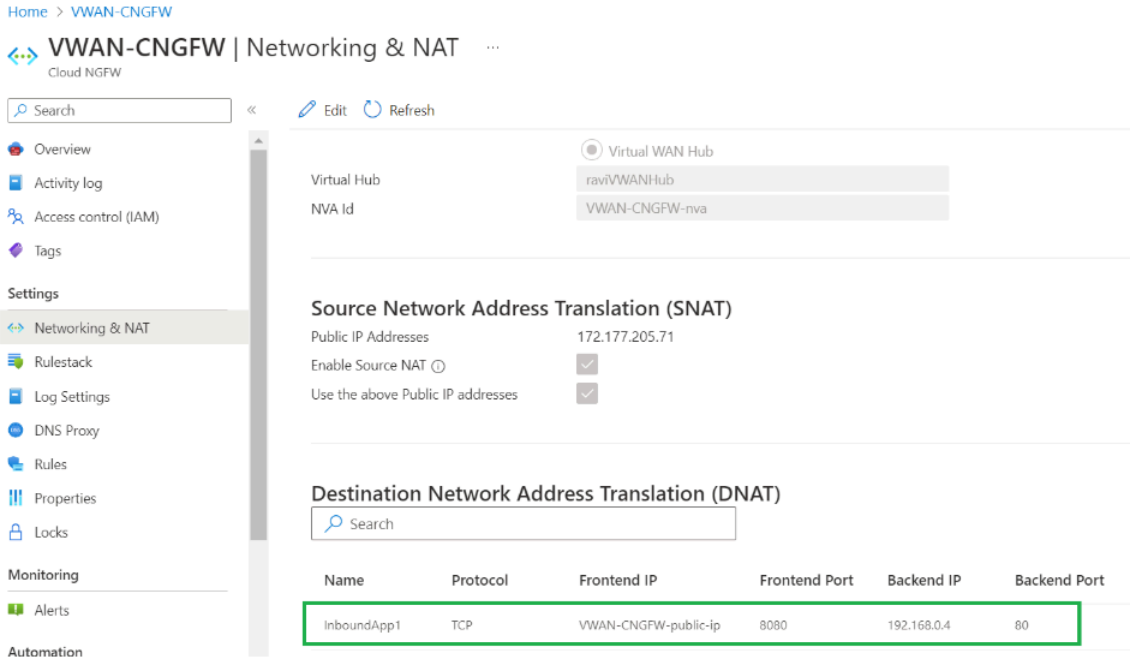
STEP 4 | フロントエンドの設定情報をルールに追加し、**[Add (追加)]**をクリックします。



宛先NATルールを追加したら、［保存］をクリックしてCloud NGFWリソースに設定をデプロイします。

設定が正常に保存されると、［Destination Network Address Translation（DNAT）］フィールドに更新内容が表示されます。アドレスhttp://frontendIP:8080は、Cloud NGFWを介して指定さ

れたポート上の注目アプリケーションにリダイレクトされます。これで、インバウンドトラフィックはCloud NGFWを通過しています。



ロギングの設定

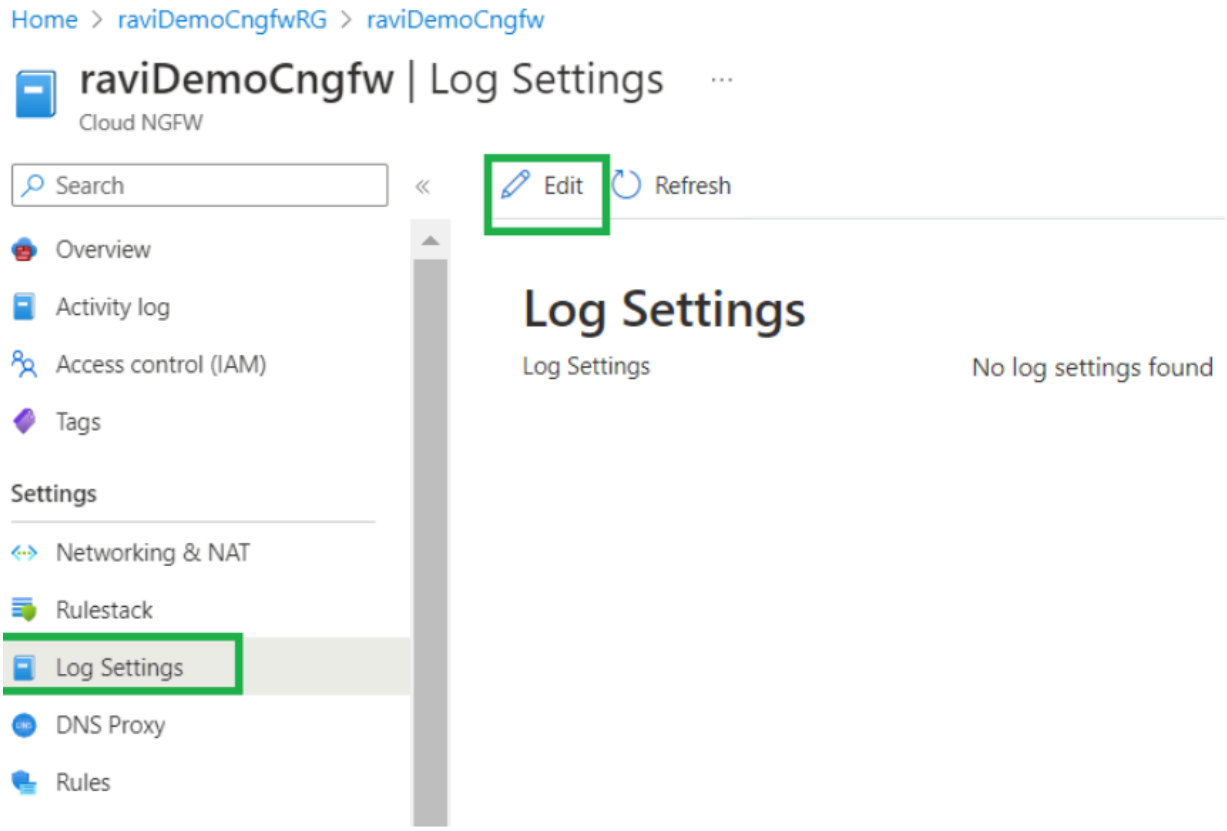
Cloud NGFWでロギングを構成する前に、Azureで**Log Analytics (**ログ分析**)**ワークスペースを作成します。

STEP 1 | Azureポータルで、**Azure Log Analytics workspace (Azure**ログ分析ワークスペース**)**を検索します。**[Log Analytics Workspaces (**ログ分析ワークスペース**)**］をクリックして、サービスとして追加します。

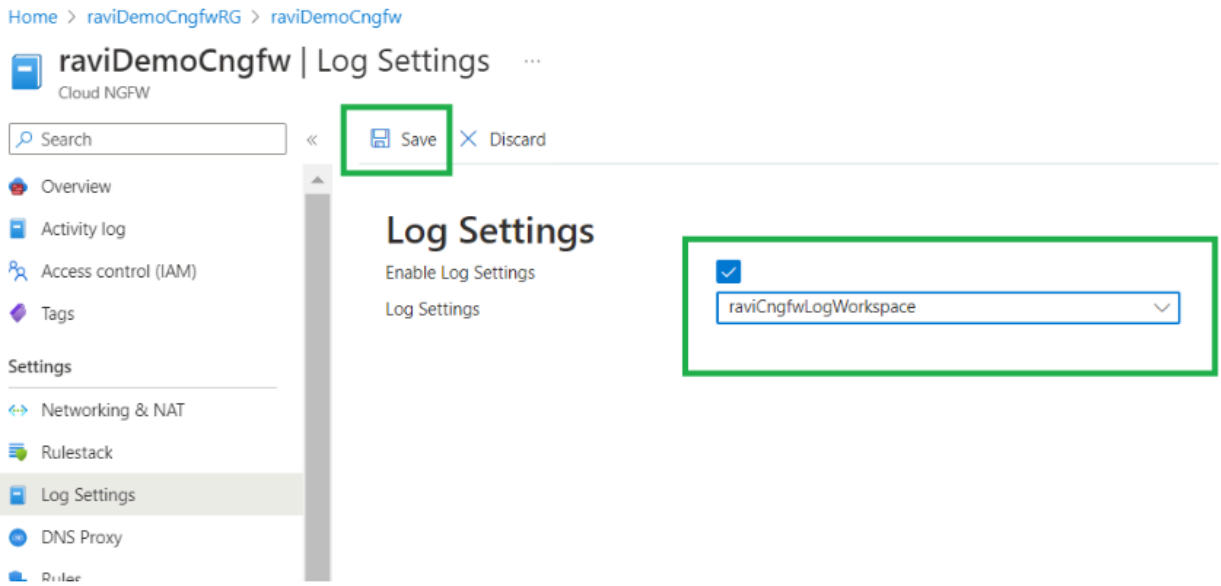
STEP 2 | **[Create (**作成**)]**をクリックして、新しいログ分析ワークスペースを確立します。

STEP 3 | [ログ分析の作成]ワークスペースで、インスタンスの詳細を指定します。ドロップダウンメニューから作業スペースの名前を選択し、地域を指定します。

STEP 4 | Cloud NGFWリソースのログ設定を行います。**[ログ設定]**を選択します。**Edit**（編集）をクリックします。



STEP 5 | **[Log Settings (ログ設定)]**フィールドで、以前に作成したログ分析ワークスペースを選択し、**[Save (保存)]**をクリックします。

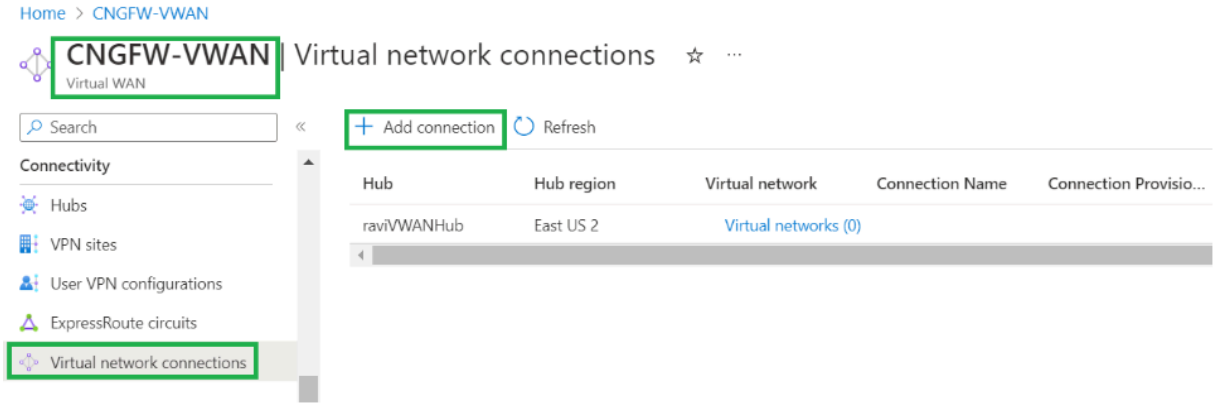


仮想**WAN**への仮想ネットワーク接続としてのアプリケーション**vNET**の追加

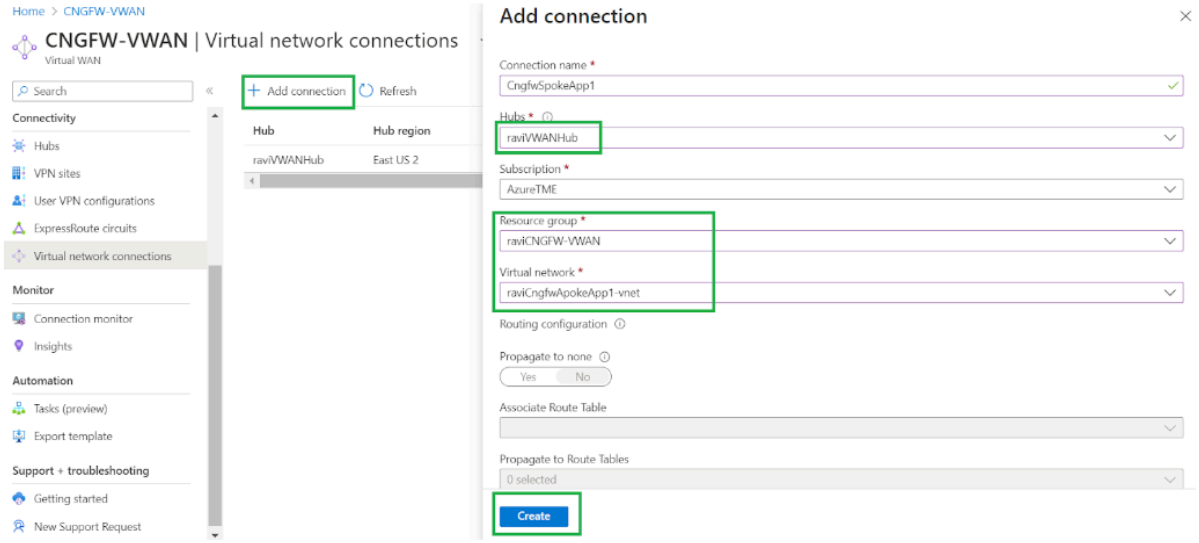
アプリケーションvNETを仮想ネットワーク接続として仮想WANハブに追加します。

STEP 1 | vWANリソースで、**[Virtual Network Connections (仮想ネットワーク接続)]**を選択します。

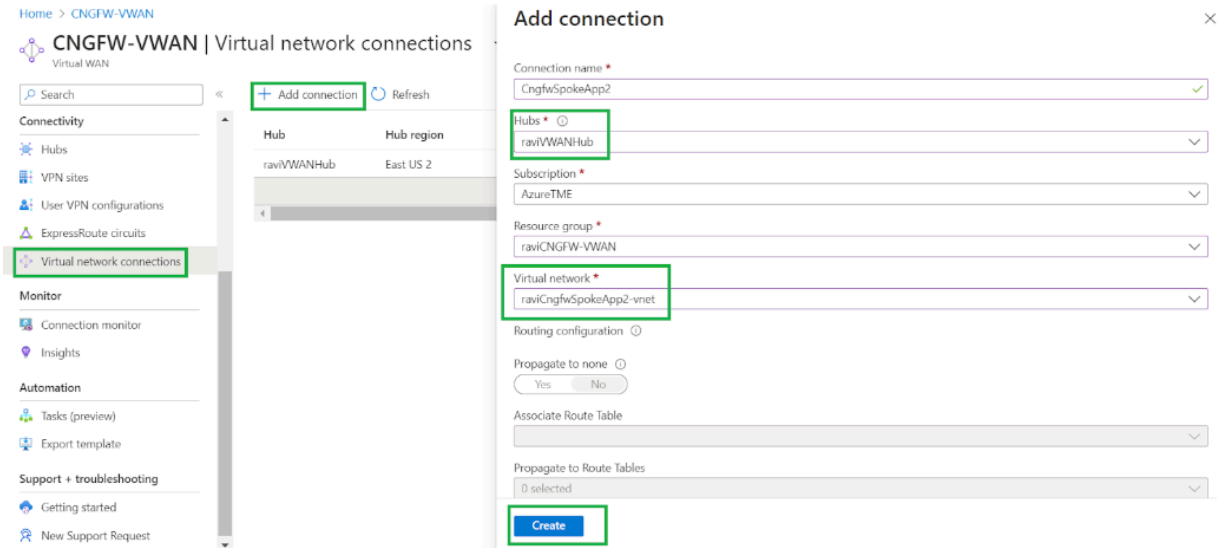
STEP 2 | **[Add connection (接続の追加)]**をクリックします。



STEP 3 | 仮想ネットワークとして設定するvNETを選択し、［**Create (**作成**)**］をクリックします。



STEP 4 | 2つ目の仮想ネットワークに別のvNETを選択し、**[Create (作成)]**をクリックします。



STEP 5 | 仮想ネットワークとvHubの接続に成功したら、ステータスが**[Connected (接続済み)]**であることを確認します。

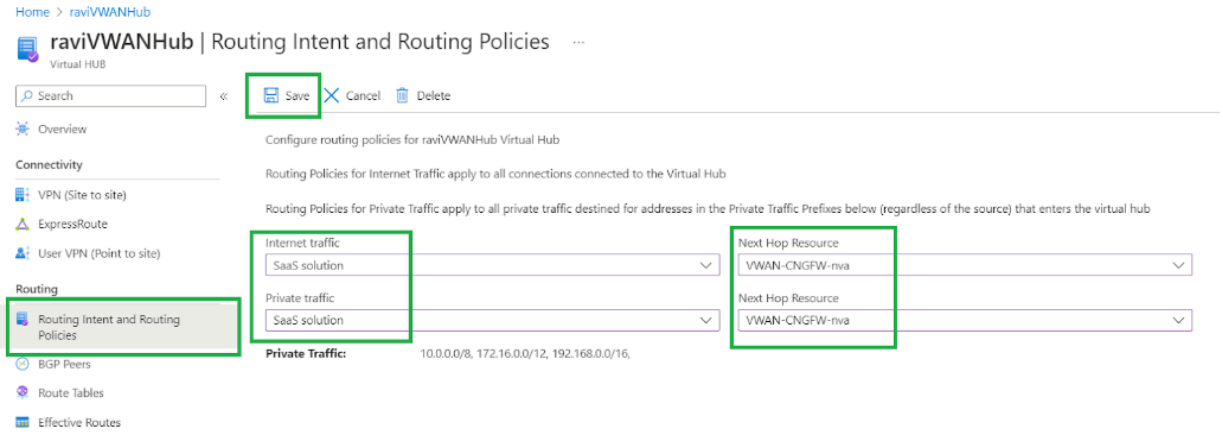
vWANハブのルーティングインテントとルーティングポリシーの設定

仮想WANハブ内のルーティングポリシーは、Cloud NGFWサービスを介してトラフィックをルーティングするために使用されます。インターネットに向かうトラフィックとプライベートトラフィック（スポークツースポーク）をルーティングするには、ネクストホップをvWAN Cloud NGFWとして設定する必要があります。

*vWANのルーティングインテント、ルーティングポリシー、SaaS機能は現在、Microsoftによって*Azure Portal*向けに開発されています。Cloud NGFWを利用できるすべてのリージョンの目標提供日は2023年5月9日（火）です。*

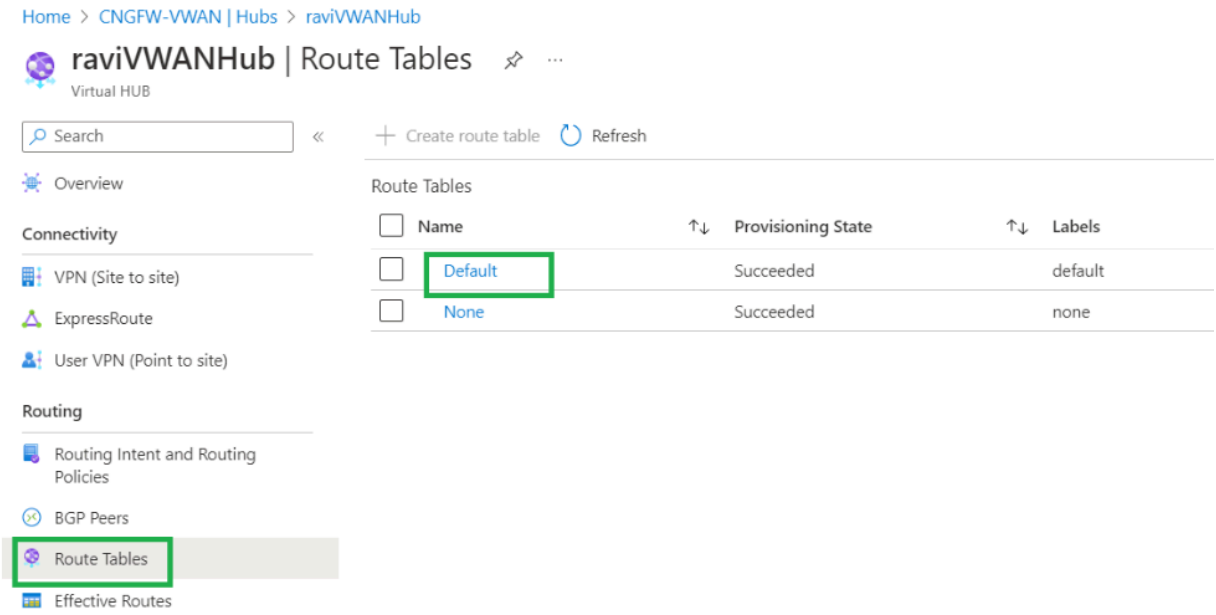
STEP 1 | vWANリソースで、ルーティングインテントとルーティングポリシーを選択します。

STEP 2 | ドロップダウンメニューからインターネットトラフィックとネクストホップリソースを選択し、［**Save (保存)**］をクリックします。

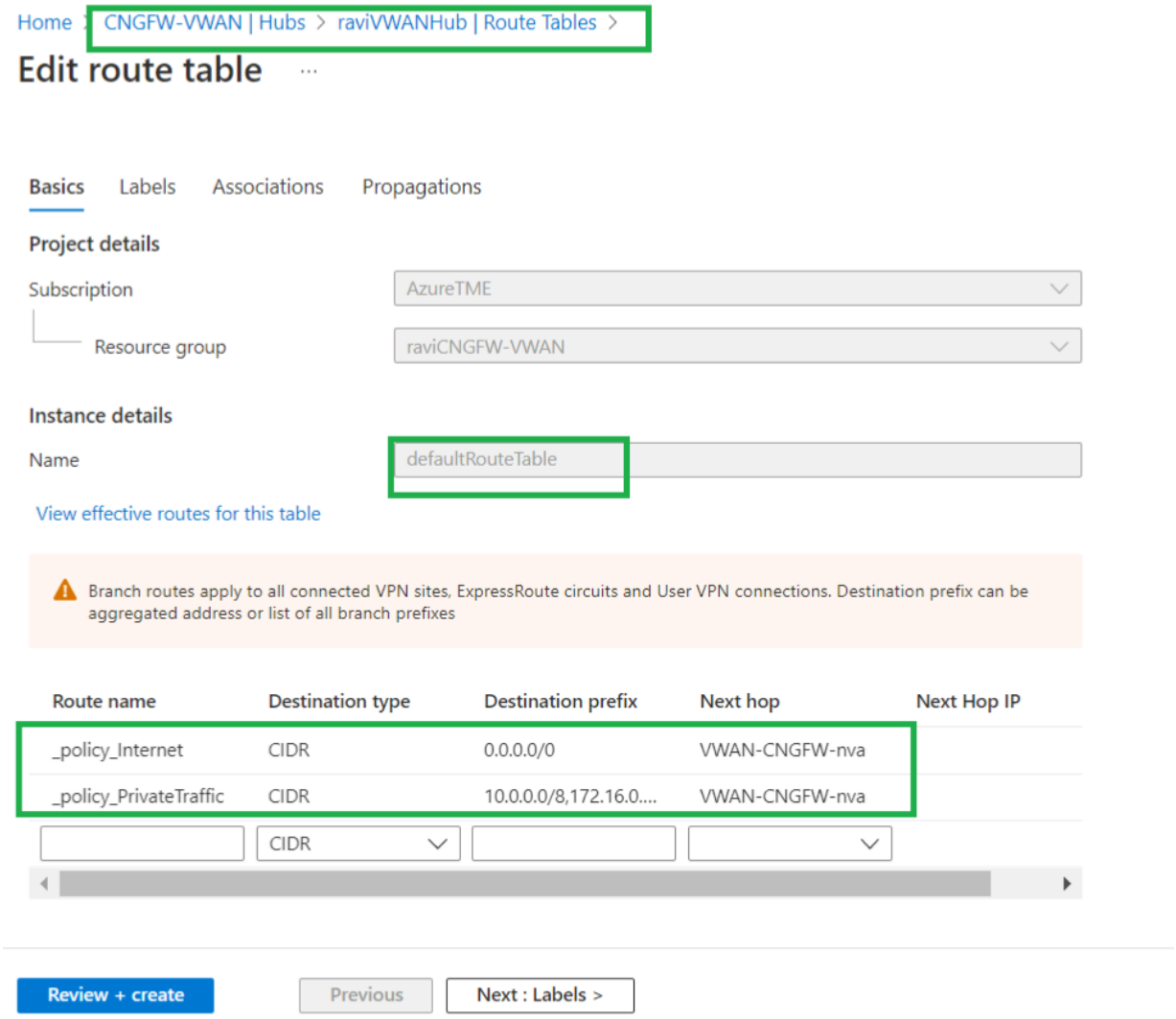


STEP 3 | ルーティングポリシーを設定したら、Cloud NGFWを介してトラフィックをルーティングするようにルーティングテーブルが更新されたことを確認します。**[Route Tables (**ルートテー

ブル)]をクリックし、**[Route Tables (ルートテーブル)]**セクションで**[Default (デフォルト)]**を選択します。



ルートテーブルを編集して、デフォルトルーティングテーブルに関連付けられたルートに関する詳細を表示できます。インターネットや他のvNETに送信されるトラフィックは、Cloud NGFWを介してルーティングされます。



STEP 4 | 2つ目の仮想ネットワークに別のvNETを選択し、**[Create (作成)]**をクリックします。

STEP 5 | 仮想ネットワークを仮想WANハブに正常に接続したら、ステータスが**[Connected (接続済み)]**となっていることを確認します。

ルールスタックを使用したCloud NGFW ネイティブ ポリシー管理

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。

- Azure 向け Cloud NGFW のルールスタックとルールについて
- Azure 向けCloud NGFW のルールスタックを作成する
- Azure 向けCloud NGFW のセキュリティ ルール オブジェクト
- Cloud NGFW for Azure のセキュリティ サービス

Cloud NGFW for Azure のルールスタックとルールについて

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、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。

ローカル ルールスタックは、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するために使用されるローカル ルールで構成されます。アカウント管理者は、これらのルールをAzureアカウントのNGFWリソースに関連付けることができます。

Cloud NGFW for Azure でルールスタックを作成する

Cloud NGFW では、**LocalRuleStackAdmin** ロールが割り当てられていれば、ルールスタックを作成できます。

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 | Microsoft Azure ホームページの**Local Rulestack (**ローカルルールスタック**)**アイコンをクリックします。または、ホームページの検索バーで目的のルールスタックを検索してアクセスすることもできます。

STEP 2 | 作成をクリックします。

STEP 3 | **[Basics (**基本**)]**タブの「プロジェクト詳細」セクションにあるそれぞれのドロップダウンから**[Subscription (**サブスクリプション**)]**と**[Resource Group (**リソースグループ**)]**を選択します。

STEP 4 | ルールスタックのわかりやすい**[Name (**名前**)]**を入力します。

STEP 5 | ルールスタックでサポートされる**[Region (**リージョン**)]**を入力します。

STEP 6 | **[Tags (**タグ**)]** タブをクリックします。

1. **[Name (**名前**)]** と **[Value (**値**)]** を入力します。
2. **[Review+create (**レビュー+作成**)]**をクリックします。

STEP 7 | 選択したルールスタックオプションを確認し、**[Create (**作成**)]**をクリックします。

Cloud NGFW for Azure のセキュリティルールオブジェクト

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)、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と **FQDN** リスト- プレフィックスリストと FQDN リストを使用すると、同じポリシーの適用を必要とする特定の送信元または宛先の IP アドレスまたは FQDN 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 インターネット プロトコル ネットマスクを含めることができます。インターネット プロトコル ネットマスク タイプのアドレスオブジェクトでは、IPv4ネットワークを示すスラッシュ表記を使って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。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。
- **Certificate (**証明書**)**：証明書オブジェクトは、AzureアカウントのAzure Key Vaultに格納されているTLS証明書への参照であり、アウトバウンド復号化で使用されます。

  アウトバウンド復号化に *Azure Key Vault* を使用する場合は、*PAN-OS* バージョン *11.0.x* が必要です。

Cloud NGFW for Azure でプレフィックスリストを作成する

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 | ホームページから**[Local Rulestacks (**ローカルルールスタック**)]**アイコンをクリックし、プレフィックスリストを構成する以前に作成したルールスタックを選択します。

STEP 2 | 左ペインの**[Prefix List (**プレフィックスリスト**)]**をクリックし、[Add (追加)]をクリックします。[プレフィックス リストの追加] ウィンドウが開きます。

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 | **[**追加**]** をクリックします。

Cloud NGFW on Azure の FQDN リストを作成する

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 | ホームページから**[Local Rulestacks (**ローカルルールスタック**)]**アイコンをクリックし、FQDNリストを構成する以前に作成したルールスタックを選択します。

STEP 2 | 左ペインの**[FQDN**リスト**]**をクリックし、**[Add (**追加**)]**をクリックします。［Add FQDN List (FQDNリストの追加)］ ペインが開きます。

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 | **[**追加**]** をクリックします。

Cloud NGFW for Azure に証明書を追加する

Cloud NGFW は証明書を使用してアウトバウンド復号化を有効にします。これらの証明書は Azure Key Vault に保存されます。

現在、復号化には自己署名証明書とルート *CA* 署名証明書のみがサポートされています。チェーン証明書はサポートされていません。

アウトバウンド復号化に *Azure Key Vault* を使用する場合は、*PAN-OS* バージョン *11.0.x* が必要です。

STEP 1 | ホームページから **[Local Rulestacks (**ローカル ルールスタック**)]** アイコンをクリックし、証明書を作成する以前に作成したルールスタックを選択します。

STEP 2 | 左側のペインで **[Certificates (**証明書**)]** をクリックし、**[Add (**追加**)]**をクリックします。[Add Certificate List (証明書リストの追加)] ペインが開きます。

STEP 3 | 証明書にわかりやすい名前を入力します。

STEP 4 | （任意）証明書の説明を入力します。

STEP 5 | 証明書が自己署名されている場合は、**[Self Signed Certificate (**自己署名証明書**)]**をチェックします。

STEP 6 | 証明書が自己署名されていない場合は、**[Azure Key Vault]** > **[Certificates (**証明書**)]** に移動して証明書 URI を取得し、 **[Certificate URI (**証明書 **URI)]**にシークレット識別子 URI をコピーして貼り付けます。

STEP 7 | (任意) **[Certificate source (**証明書ソース**)]** フィールドで、それぞれのオプションを選択します。**[Key vault (**キーコンテナ**)]** または **[Paste URI (URI** の貼り付け**)]**から選択します。

STEP 8 | **[**追加**]** をクリックします。

STEP 9 | key vault (キー コンテナ)と同じリソース グループにマネージド ID を作成します。「ユーザー割り当てマネージド ID を作成する」を参照してください。

STEP 10 | **[Azure Key Vault]**> **[Access Policies (**アクセス ポリシー**)]**に移動します。

STEP 11 | **[Create (**作成**)]** を クリックして、 手順 **9**で作成したマネージド ID に **[Key Vault Certificates Officer (**キーコンテナ 証明書担当者**)]** と **[Key Vault Secrets User (**キーコンテナ シークレット ユーザー**)]** を割り当てるアクセス ポリシーを構成します。

Cloud NGFW for Azure でセキュリティルールを作成する

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 Azure 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。定義されたルールのいずれとも一致しないトラフィックには、デフォルト 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。

STEP 1 | ホームページから**[Local Rulestacks (**ローカルルール**)]**スタックアイコンをクリックし、ルールを追加したい以前に作成したルールスタックを選択します。

STEP 2 | **[Rules (**ルール**)]** をクリックし、**[Add (**追加**)]** をクリックします。

STEP 3 | 一般セクションで、ルールの説明的な**[**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. **[Any (任意)]**、**[Match (一致)]**または **[Exclude (除外)]**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. **[Match (一致)]**を選択した場合、[IP アドレス (CIDR)]、[プレフィックス リスト]、[国]、[インテリジェント フィード]、または [動的プレフィックス リスト] を指定します。

STEP 8 | 宛先を設定します。

1. **[Any (任意)]**、**[Match (一致)]**または **[Exclude (除外)]**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. 選択した場合 **[Match (一致)]**で、[プレフィックス リスト]、[FQDN リスト]、[国] を指定します。

STEP 9 | [Granular Control (きめ細かい制御)]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. **[Select (選ぶ)]**を選択した場合、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[選択］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。

2. **[[Select (選ぶ)]**を選択した場合、 **[Predefined Categories (事前定義されたカテゴリ)]** ドロップダウンから一つを選択します。

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 (アプリケーション デフォルト)]**、［**any (任意)**］または［**Select (選択)**］を選択します。

   [Select (選ぶ)]を選択した場合、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. **[[Select (選ぶ)]**を選択した場合、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。1 つのポート番号を指定できます。

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（**[Allow (**許可**)]**、［**Deny (**拒否**)**］、［**Drop (**ドロップ**)]**、または**Reset both client and server ([**クライアントとサーバー の両方をリセット**)]**）。
2. **[Egress Decryption (**出力復号化**)]**を有効化します。
3. ロギングを有効にします。

STEP 13 | **[**追加**]** 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 Azure のセキュリティ サービス

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 Azure Virtual Network（VNet）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、ウイルス、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。

  ベストプラクティスの設定

  Cloud NGFW for Azureでは、以下の脆弱性のベストプラクティス構成がデフォルトで有効になっています。

Signature Severity (シグネチャの重大度)	Action (アクション)
Critical (重大)	Reset both (両方リセット)
High (高)	Reset both (両方リセット)
Medium (中)	Reset both (両方リセット)
Informational (情報)	Default (デフォルト)
Low (低)	Default (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。

ベストプラクティスの設定

Cloud NGFW for Azureでは、以下のアンチスパイウェアのベストプラクティス構成がデフォルトで有効になっています。

Signature Severity (シグネチャの重大度)	**Action (アクション)**
Critical (重大)	Reset both (両方リセット)
High (高)	Reset both (両方リセット)
Medium (中)	Reset both (両方リセット)
Informational (情報)	Default (デフォルト)
Low (低)	Default (デフォルト)

IPSの脆弱性とアンチスパイウェア シグネチャ

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	の意味
脆弱性シグネチャ	
brute force	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	攻撃者が悪用し、ログイン済みのユーザーの権限でシステム上でコードを実行できるようにする、コード実行時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、

脅威カテゴリ	の意味
	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（DoS）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、攻撃者は巧妙なリクエスト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

脅威カテゴリ	の意味
	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。
backdoor	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。

脅威カテゴリ	の意味
［Botnet］	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	(フォームジャック、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悪意のある JavaScript コードが挿入されている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。(例えば：名前、住所、メール アドレス、クレジットカード番号、CVV、有効

脅威カテゴリ	の意味
	期限等) eコマース Web サイトの決済ページにある支払いフォームから。
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との関連度が高いです。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。
post-exploitation	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。Web シェルは、最初に悪意のある攻撃者によって侵害されたホストに埋め込まれる必要があり、ほとんどの場合、Web サーバーまたはフレームワークを標的にします。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。

脅威カテゴリ	の意味
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、ウイルス、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 ウイルス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。

  ベストプラクティスの設定

  Cloud NGFW for Azureでは、以下のアンチウイルスのベストプラクティス設定がデフォルトで有効になっています。

Protocol (プロトコル)	**Action (アクション)**
FTP	Reset both (両方リセット)
HTTP	Reset both (両方リセット)
HTTP2	Reset both (両方リセット)
IMAP	Reset both (両方リセット)
POP3	Alert (アラート)
SMB	Reset both (両方リセット)
SMTP	Reset both (両方リセット)

- ファイルブロック：（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に設定されています）ファイルブロックプロファイルを使用すると、ブロックまたは監視する特定のファイルタイプを指定できます。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。

ベストプラクティスの設定

Cloud NGFW for Azureでは、以下のファイルブロックのベストプラクティス構成がデフォルトで有効になっています。

File Types (ファイルタイプ)	Application (アプリケーション)	Direction (ディレクション)	Action (アクション)
All risky file types (すべてのリスクのあるファイルタイプ)： • 7z • bat • cab • chm • class • cpl • dll • exe • flash • hip • hta • msi • Multi-Level-Encoding • ocx • PE • pif	Any	Both (upload and download)	Block

File Types (ファイルタイプ)	Application (アプリケーション)	Direction (ディレクション)	Action (アクション)
• rar • scr • tar • torrent • vbe • wsf • encrypted-rar • encrypted-zip			
All remaining file types (残りのすべてのファイルタイプ)	Any (任意)	Both (upload and download) (両方（アップロードとダウンロード）)	Alert (アラート)

アンチウイルス シグネチャ

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	の意味
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。
MacOSX	次のような悪意のある MacOSX ファイル: • 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
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）

脅威カテゴリ	の意味
	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 Categories and Filtering (URL**カテゴリーとフィルタリング**)**］—（デフォルトで有効で、ベストプラクティスに基づいて事前設定済み）URL Filtering プロファイルを使用すると、HTTP および HTTPS 経由でユーザが Web にアクセスする方法を監視および制御できます。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。

ベストプラクティスの設定

URLフィルタリングは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たセキュリティポリシーが使用されます。

URL Categories (URLカテゴリー)	Site Access (サイトへのアクセス)	Credential Submissions (クレデンシャル提出)
Malicious and exploitative categories (悪意ある悪用カテゴリー)： • adult (アダルト) • command-and-control (コマンド＆コントロール) • copyright-infringement (著作権侵害) • dynamic-dns (動的DNS) • extremism (過激思想) • malware (マルウェア) • parked (パークド) • phishing (フィッシング) • proxy-avoidance-and-anonymizers (プロキシ回避と匿名化ツール) • unknown (不明)	Block (ブロック)	Block (ブロック)
All other URL categories (その他すべてのURLカテゴリー)	Alert (アラート)	Alert (アラート)

Cloud NGFW for Azure の定義済み **URL** カテゴリ

次の表では、Azure 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	の意味
リスクカテゴリ	

URL カテゴリ	の意味
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	
コマンドアンドコントロール	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

URL カテゴリ	の意味
	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。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

URL カテゴリ	の意味
	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。

URL カテゴリ	の意味
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。企業のウェブサイトは、自社の技術で分類する必要があるため、含めるべきではありません。feedex.comやups.comなどの発送サイトもこれに該当します。
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。
コンテンツ配信ネットワーク	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。画像サーバーも含まれます。
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。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。

URL カテゴリ	の意味
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、個人の財務情報やアドバイスに関するサイト。株式市場、証券会社、取引サービスに関するサイトは含まれません。外貨両替サイトが含まれます。外貨両替サイトが含まれます。
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。賭け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サイト。ギャンブルができないホテルやカジノの企業サイトは「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。オンライン懸賞および/または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。

URL カテゴリ	の意味
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ヒント、救済策、治療法に関する情報を含むサイト。また、専門家だけでなく、さまざまな医療の専門、プラクティス、施設（ジムやフィットネスクラブなど）のサイトが含まれています。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）。
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

URL カテゴリ	の意味
	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。
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。これは主にbittorrentのダウンロード機能を提供するサイトです。シェアウェアまたは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。

URL カテゴリ	の意味
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。
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を含みます。占いサイトも含まれます。
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

URL カテゴリ	の意味
	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、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	オンライン教育訓練および関連資料を提供するサイト。自動車/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

URL カテゴリ	の意味
	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。
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 AzureでDNSセキュリティを有効にする

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、重要かつ基本的なインターネット プロトコルです。悪意のあるアクターは、DNSを介してCommand & Control（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抜き取ることさえあります。DNS窃取は、悪意のあるアクターがネットワーク内のアプリケーションインスタンスを侵害した後に、DNSルックアップを使用してネットワークから自分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を介してネットワークワークロードに悪意のあるデータ/ペイロードを侵入させることもできます。長年にわたり、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してきました。

Cloud NGFW for Azureでは、ネットワーク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vNetおよびvWANトラフィックを保護できます。Cloud NGFW for Azureでは、Palo Alto Networksが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通過させることができます。

この目的のために、Cloud NGFWは、複数のソースからのデータ（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、ユニット42の研究組織、サイバー脅威アライアンス）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のDNS（ドメインネームシステム）セキュリティサービスを活用しています。その後、DNSセキュリティサービスは、Cloud NGFWリソースにこれらのシグネチャを配布し、DNSを使用してマルウェアからC2（コマンドアンドコントロール）とデータ盗難をプロアクティブに防御します。

DNSセキュリティを有効にすると、Cloud NGFWはDNSセキュリティカテゴリごとに以下のアクションを実行します。

カテゴリ	ログ重大度	操作
広告追跡ドメイン	情報	Allow [許可]
コマンドアンドコントロール（C2）ドメイン	高	ブロック
ダイナミックDNS(DDNS)ドメイン	情報	Allow [許可]
グレイウェアドメイン	低	ブロック

カテゴリ	ログ重大度	操作
マルウェアドメイン	中	ブロック
新しく登録されたドメイン	情報	Allow [許可]
パークドメイン	情報	Allow [許可]
フィッシングドメイン	低	ブロック
プロキシ回避とアノニマイザ	低	ブロック

DNSトラフィックを検査するには、Cloud NGFW for AzureでDNSプロキシを有効にする必要があります。

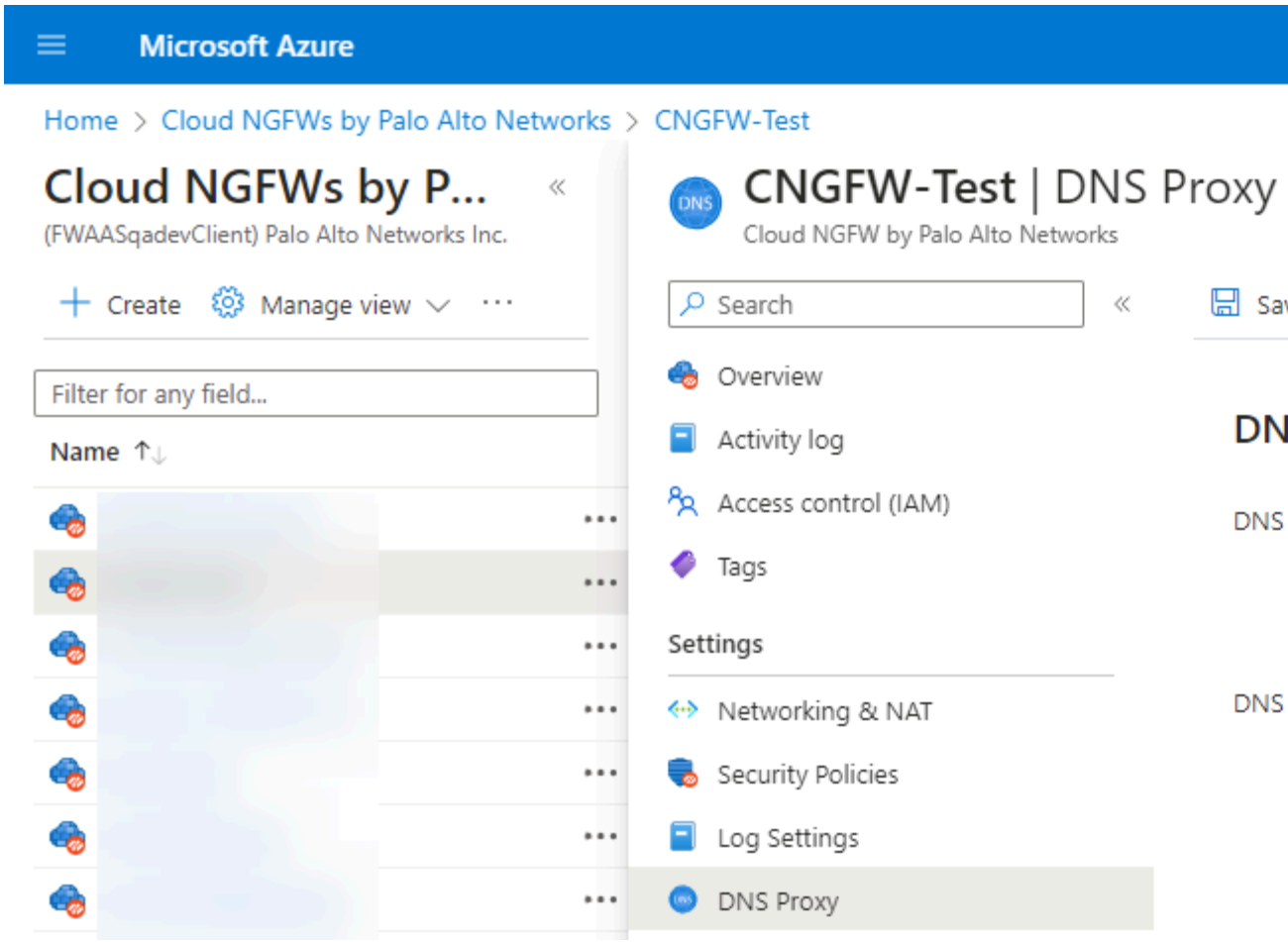
STEP 1 | Azure ポータルにログインします。

STEP 2 | [Azure Services]の[Cloud NGFWs]アイコンをクリックします。

STEP 3 | Cloud NGFWインスタンスを選択します。

STEP 4 | DNSプロキシを有効にします。

1. **[Settings (設定)]** > **DNS Proxy (DNSプロキシ)]**を選択します。
2. **[Enabled (有効)]**ラジオボタンを選択します。
3. デフォルトのDNSサーバーを使用するか、［**Custom (カスタム)**］を選択し、仮想ネットワークで以前に構成したDNSサーバーを指定します。
4. **Save**（保存）をクリックします。

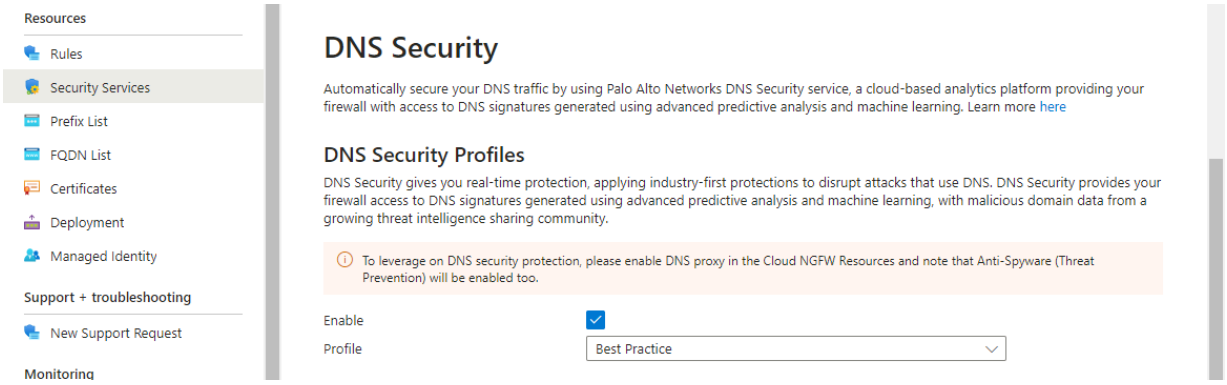


STEP 5 | Cloud NGFWインスタンスに関連付けられたローカルルールスタックに移動します。

STEP 6 | **[Security Services (セキュリティサービス)]**を選択します。

STEP 7 | **DNS** セキュリティを有効化します。

*DNS*セキュリティを有効にするには、アンチスパイウェアも有効にする必要があります。さらに、「*DNS Security (DNS*セキュリティ*)*」と「*Anti-Spyware (*アンチスパイウェア*)*」の両方が「ベストプラクティス」に設定されている必要があります。



Cloud NGFW for Azure でのアウトバウンド復号化の設定

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。

*Azure Key Vault*を送信復号化に使用する場合は、*PAN-OS*バージョン*11.0.x*が必要です。

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。また。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、VNet 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。ルールの作成時にアウトバウンド TLS 復号化を有効にする必要があります 。

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 | ［**Security Profiles (**セキュリティプロファイル**)**］ > **Egress Decryption ([**出力暗号化解除**)**］を選択します。

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。

Cloud NGFW for Azure に証明書を追加するまだ行っていない場合は行ってください。

証明書と秘密鍵はAzure Key Vaultに格納され、ワークロードはこ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
```

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Azure Key Vault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。

信頼証明書は自己署名できませんが、信頼できない証明書は自己署名または*ca*署名が可能です。

STEP 4 | 以前に作成した**[Rulestack (**ルールスタック**)]**に移動し、「**Managed Identity (**管理対象アイデンティティ**)**」ページに移動します。

STEP 5 | **[Enable MI (MI**を有効にする**)]**ドロップダウンメニューから、鍵保管庫に関連付けられた管理対象IDを選択します。

STEP 6 | **Save**（保存）をクリックします。

Cloud NGFW for Azure でインバウンド復号化を設定する

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、VNets 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。

Web 証明書と秘密キーを 1 つのキーとして連結する必要があります `pem` 又は `PFX` のファイルを作成し、 Azure Key Vault を使用して 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。

証明書とキーを別々に *Azure Key Vault* にアップロードしないでください。

-

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。
- 優先権- ルールの一意の優先度。
- 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 **Match Criteria** を指定します。

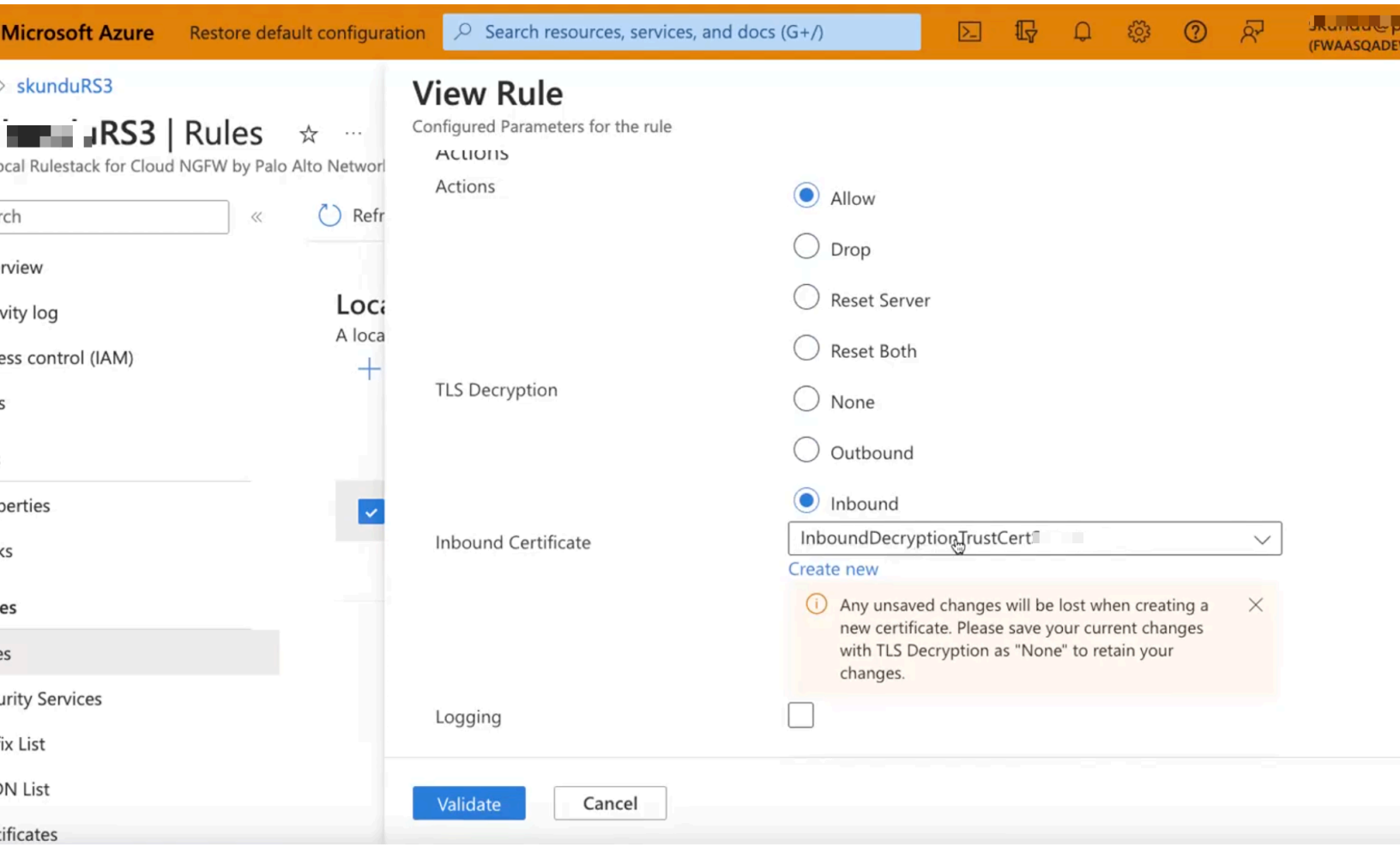
  TLS 復号化ルールは、次のようにして作成できます。 アプリケーション—任意 又は ***SSL***について—***Match (***一致***)***のみ。

- そのルールの一致条件として **URL** カテゴリを指定します。
- ルールを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。

  ステップ 6 **A**を指定します。

- 許可 — トラフィックを許可します。
- ドロップ — 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ドロップ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 6 | ［**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、証明書の作成を行います。証明書オブジェクトを作成するときに、シークレットの *Azure* リソース名（*ARN*）を証明書 *ARN* で使用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。
- インバウンド復号化は、自己署名証明書とルート *CA* 署名付き証明書をサポートし、チェーン証明書はサポートしません。
- *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 7 | **Logging (**ロギング**)** を選択してログ記録を有効にします。

STEP 8 | **[**検証**]**をクリックします。

STEP 9 | ［**Config ActionsDeploy (**アクションの設定**)**］ ［**Deploy Configuration (**設定のデプロイ**)**］ ［**Commit (**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。

Panoramaポリシー管理

このセクションの情報を使用して、Cloud NGFW for Azure を Palo Alto Networks Panorama 仮想アプライアンスと統合します。

Panorama統合

Cloud NGFWは、Azure上のクラウドネイティブサービスとして提供されている業界唯一の機械学習（ML）対応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。Azure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 Azure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?

Azure Portalを使用してCloud NGFWリソースを作成する場合、Palo Alto Networks Panoramaを使用してセキュリティポリシーを管理するオプションがあります。その後、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 、ログ分析をすべて単一のPanoramaコンソールから使用できるようになります。

ファイアウォールが正常でない状態に達して切断されると、一定時間（通常は3日間）後に*Panorama*から削除されます。これにより、ファイアウォールが途中で削除されることはありません。

統合コンポーネント

Cloud NGFWリソースをPanoramaに統合するには、以下のPalo Alto Networksコンポーネントを使用します。

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Azure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。

Panorama Azure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 Azureプラグインを使用すると、PanoramaにリンクされたCloud 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。

クラウド デバイス グループ **(Cloud DG)** 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 DGは、Panorama Azure Plugin UIを使用して、Cloud NGFWリソースとAzureリージョン情報を指定して作成します。クラウドDGはその地域でグローバルなルールスタックとして現れます。

- Panorama Azure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 UI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、DG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 DG をCloud NGFW リソース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 DGは、Cloud NGFWリソースの各Azure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 DGを作成するときに、Panorama Azure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、ネイティブ Panorama UI 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、これらのクラウド テンプレート スタックに追加できます。

Cloud NGFW をデプロイした後にテンプレート スタック名を変更することはできません。

- 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 DG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。

統合の手順

Cloud NGFWをPanoramaと統合するには、いくつかの手順が必要です。この統合のためには、まずAzureプラグインをインストールしてPanorama仮想アプライアンスを準備します。Cloud NGFWのリンクに成功したら、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ます。

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:

- PanoramaがPanorama統合の前提条件を満たしていることを確認します。
- PanoramaをCloud NGFWに リンクします。
- Cloud NGFWポリシー管理にPanoramaを使用します。

*Cloud NGFW*リソースを*Panorama*と統合する場合は、次の点を考慮してください。

- *Cloud NGFW*リソースを別の*Panorama*に移動するには、再デプロイする必要があります。
- *Cloud NGFW*リソースのデプロイ後にログコレクタを追加した場合は、再デプロイする必要があります。
- *Panorama*IPアドレスを変更した場合は、*IP*アドレスも再展開する必要があります。

Panorama統合の前提条件

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には、次の手順を実行します。

- Panoramaをセットアップします。
  - ソフトウェアバージョン11.0.1-h1以降または10.2.4-h2以降を実行している Panoramaをデプロイします。
  - 登録済みの Panorama がライセンスとともにインストールされ、Cloud NGFW for Azure の展開をサポートするために必要な容量を持ち、Customer Support Portal (CSP) (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

    。
  - 組織でPanoramaアプライアンスを登録しているPalo Alto Networks Customer Support Portal（CSP）アカウントのメンバーであることを確認します。

    *CSP*アカウントへの登録に使用する電子メールは、*Cloud NGFW*と*Panorama*の統合に使用する必要があります。このメールが異なると、*Cloud NGFW*の設定や*Panorama*との連携ができなくなります。
- Azure プラグインバージョン 5.0.0のインストール
- PanoramaにPanorama管理者の役割があることを確認します。
- Cloud NGFWとPanorama間の通信を確保するために、ネットワークで次のポートをターゲットとするトラフィックがPanorama仮想アプライアンスに許可されていることを確認します。3978, 28443, 28270.

接続シナリオ

上記の項目に加えて、Cloud NGFWリソースがPanoramaに接続する方法も考慮する必要があります。Panoramaを使用してCloud NGFWポリシーを管理するには、PanoramaがVNetに接続されている必要があります。ただし、ネットワークトポロジによっては、PanoramaとVNetの接続が有効になる方法が異なります。

- **Private Network Access with Panorama Private IP**—PanoramaをハブVNetプライベートサブネットに直接展開することも、Cloud NGFW VNetとピア接続された別のVNetに展開することもできます。

  ハブVNetプライベートサブネットに直接展開した場合、Panoramaは同じサブネット内にあるため、Cloud NGFWリソースと直接接続できます。Cloud NGFWに関連付けられたハブVNetの

プライベートサブネットとピアリングされたVNetにPanoramaを展開すると、VNetピアリングによってCloud NGFWリソースがPanoramaプライベートIPアドレスに到達できるようになります。

- **VPN**経由のオンプレミス**Panorama**アクセス—Panoramaインスタンスがオンプレミスにデプロイされている場合、Cloud NGFWリソースはVPN経由でPanoramaのプライベートIPアドレスに到達できます。さらに、このシナリオは VNet ピアリングをサポートします。

  このシナリオでは、Panoramaはオンプレミスネットワークにデプロイされ、Cloud NGFWハブVNetまたはCloud NGFWハブVNetとピアリングされたハブVNetへのVPNゲートウェイ接続を直接使用します。いずれの場合も、ハブ VNet には、Panorama のプライベート IP アドレスを宛先として VPN トンネルを指すルートが必要です。この設定の詳細については、「Configure VPN gateway transit for virtual network peering (仮想ネットワークピアリング用のVPNゲートウェイ中継の設定)」を参照してください。

- インターネット経由**Panorama**パブリック**IP**アクセス—PanoramaとCloud NGFWハブVNetの間にVNetピアリング、VPN、またはVWAN接続がない場合、Cloud NGFWリソースはインターネット経由でPanoramaのパブリックIPアドレスに接続できます。この接続を許可するには、Azureでネットワークセキュリティグループのルールを作成し、Cloud NGFWパブリックIPアドレスからPanoramaが使用するポートへのインバウンドトラフィックを許可する必要があります。

- **Access Panorama from Anywhere**（**VWAN**）—Cloud NGFW for Azureは、Azure VWANにマネージドSaaSサービスとして展開されるため、VWANハブを通過するすべてのトラフィックを保護できます。Cloud NGFWリソースは、VWANハブに接続されている任意の場所に展開されたPanoramaインスタンスのプライベートIPアドレスに接続できます。

  *Azure VWAN*導入環境に*East-West*トラフィックのネットワークセキュリティグループがある場合、*Cloud NGFW*リソースのプライベート*IP*アドレスから*Panorama*プライベート*IP*アドレスへのインバウンドトラフィックを許可するネットワークセキュリティグループルールを作成する必要があります。

Cloud NGFWをPalo Alto Networks管理にリンク

クラウドデバイスグループの作成

統合のための環境を準備したら、Cloud NGFWをPanorama仮想アプライアンスにリンクし、ポリシー管理の使用を開始できます。まず、クラウドデバイスグループを作成します。

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。

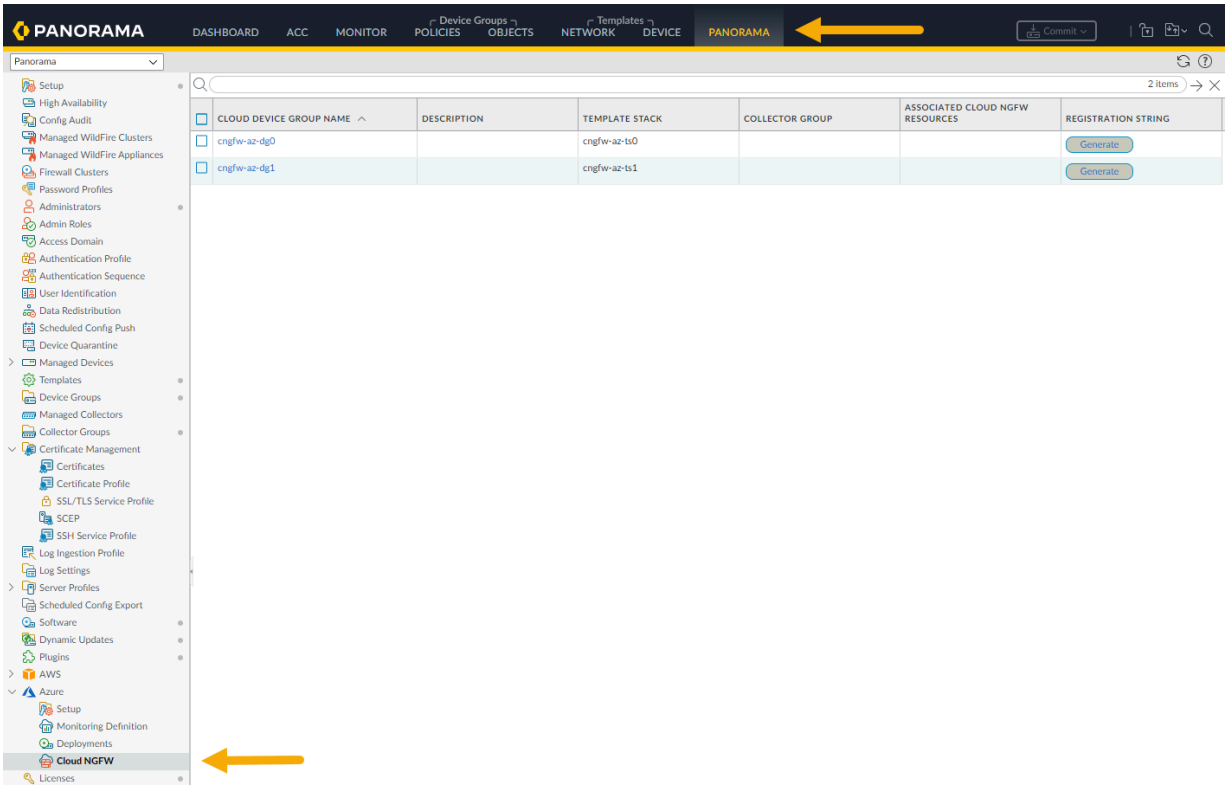
Panoramaコンソールを使用してクラウドデバイスグループとテンプレートスタックを追加するには

STEP 1 | Panoramaコンソールで、**Panorama**を選択します。

STEP 2 | ナビゲーションツリーで、**Azure**プラグインを選択します。

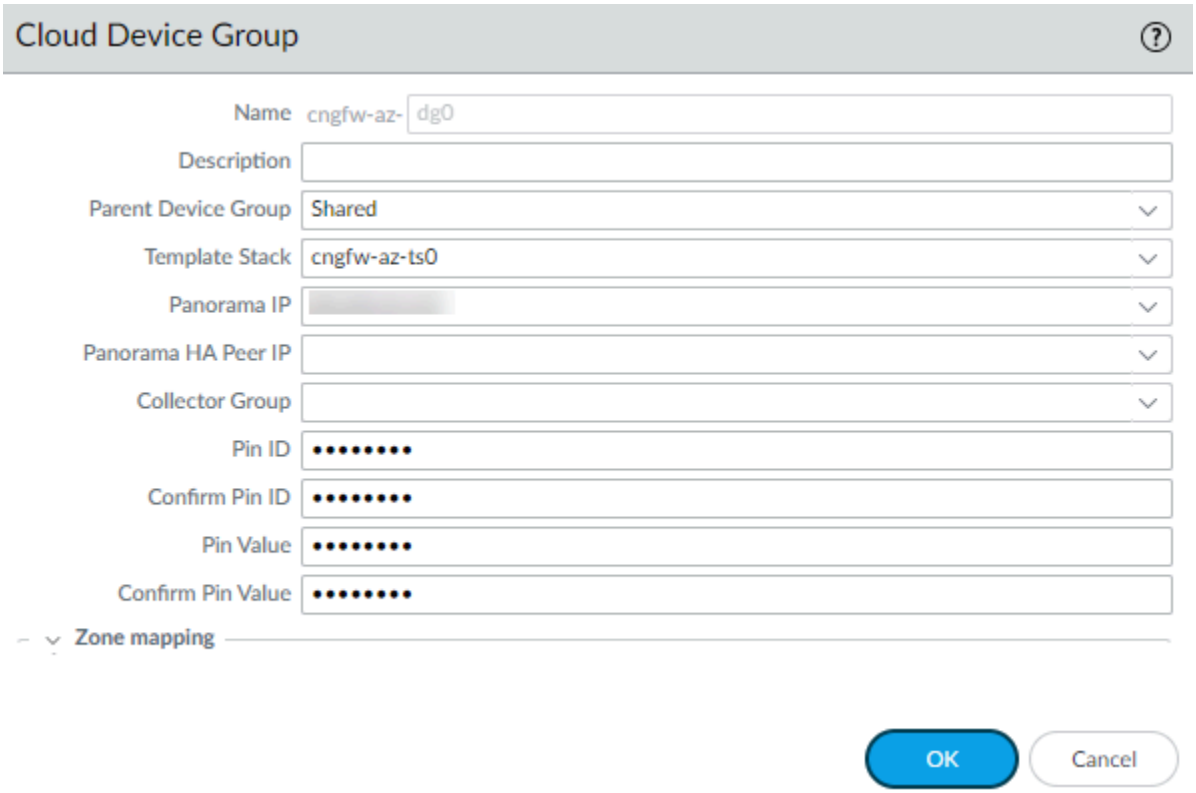
STEP 3 | Azureプラグインを展開し、設定オプションを表示します。[**Cloud NGFW**]を選択し、[Cloud Device Group (クラウド デバイス グループ)]画面を表示します。［Cloud NGFW］オプションが表示されない場合は、Azureプラグインが正常にインストールされていることを確認し

ます。**[Panorama]** > **[Plugins (プラグイン)**] を選択すると、インストールされているプラグインのリストが表示されます。



STEP 4 | Panoramaコンソールの左下部分で、［追加 **(**追加**)**］をクリックして新しいクラウドデバイスグループを作成します。

STEP 5 | Device Group (クラウドデバイスグループ)]画面で、次の手順を実行します。

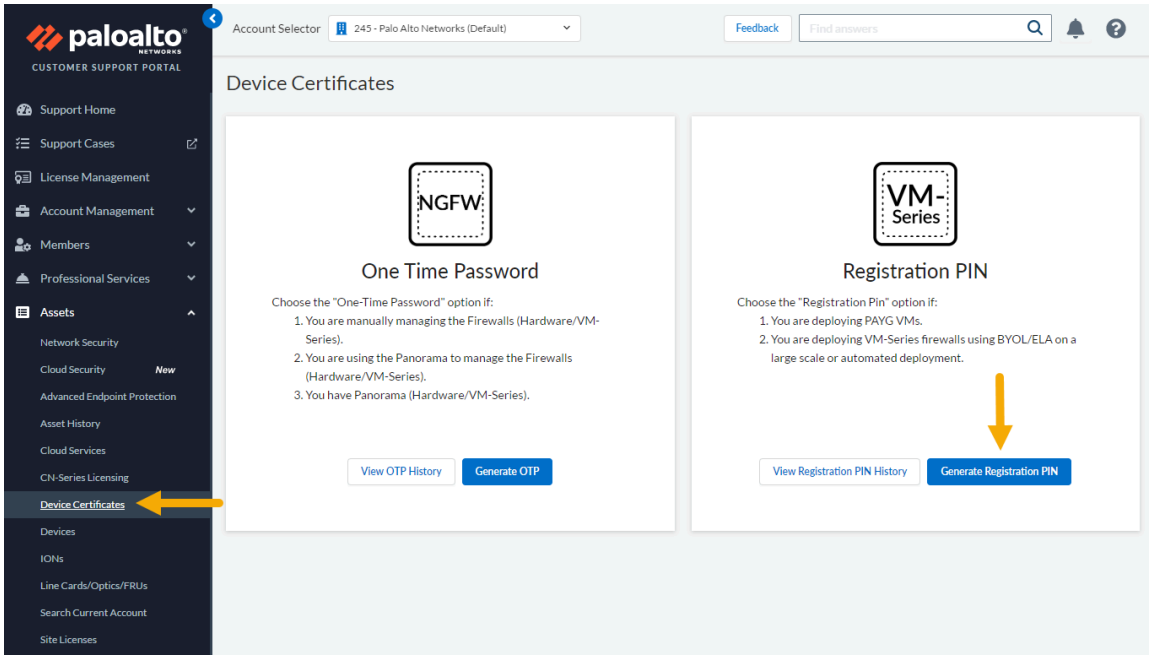


1. クラウドデバイスグループの一意の名前を入力します。
2. **Description (**説明**)** を入力します。
3. ドロップダウンメニューを使用して、親デバイスグループを選択します。デフォルトでは、この値は共有されます。
4. ドロップダウンメニューからTemplate Stack (テンプレートスタック)を選択します。または、**[Add (**追加**)]**をクリックして新規作成します。Cloud NGFWの導入後にテンプレートスタック名を変更することはできません。
5. 展開で使用する**PanoramaIP**アドレスを選択します。ドロップダウンメニューでプライベートまたはパブリックのIPアドレスを選択できます。
6. オプションでPanorama HAピア**IP**アドレスを選択します。
7. オプションでドロップダウンメニューを使用して、Collector Group (コレクタグループ)を選択します。
8. **PIN ID**を入力します。この値は、カスタマーサポートポータルによって提供されます。

   PINを取得するには、Palo Alto Networksのカスタマーサポートポータル(CSP)アカウントが必要です。

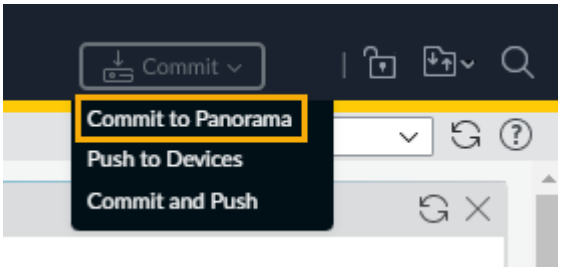
*PIN ID*の有効期限は*1*年間です。すでに*Cloud NGFW*のシリアル番号を登録している場合は省略可能です。まだ登録されていない場合は、*Panorama*仮想アプライアンスを登録したのと同じ*CSP*アカウントに対して、 のシリアル番号を使用して*Cloud NGFW*を登録します。

9. 暗証番号と暗証番号を取得するには、カスタマーサポートポータルに登録ユーザとしてログインします。
10. [カスタマーサポートポータル]ページで、**[Assests (**アセット**)]** > **[Device Certificates (**デバイス証明書**)]**を選択します。
11. [**Device Certificate (**デバイス証明書**)**]ページで、[VMシリーズ用のファイアウォールに**[Generate Registration PIN (**登録**PIN**生成**)]**を選択します。



12. 新しく作成した登録IDをコピーし 、 クラウドデバイスグループ画面の「**PIN ID** 」 「**PIN Value (PIN値)**」欄に貼り付けます。
13. PIN IDとPIN値の値を確認します。

14. オプションで、クラウドデバイスグループのゾーンマッピングを設定します。パブリック/プライベートの2つのゾーンのみがサポートされています。
15. **OK** をクリックします。
16. Panoramaコンソールで変更をコミットしてクラウドデバイスグループを作成します。次に、Cloud NGFWリソースを作成するための登録文字列を生成し、Azureにデプロイします。



場合によっては、クラウドデバイスグループを構成する際に検証エラーが発生することがあります。この問題を解決するには、管理者の資格情報を使用して、*Azure Plugin for Panorama*が正しくインストールされていることを確認します。*HA*環境の場合は、セカンダリノードにプラグインをインストールしてから、プライマリノードにプラグインをインストールします。

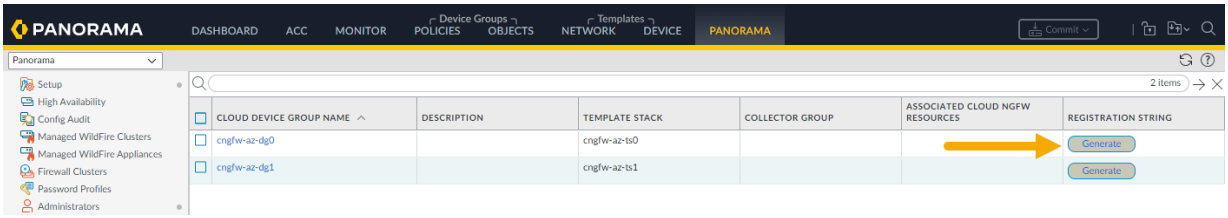
Cloud NGFWを作成する登録文字列を生成し、Azureにデプロイする

変更をコミットしてクラウドデバイスグループを作成すると、登録文字列を生成できます。この文字列は、AzureでCloud NGFWを作成およびデプロイするために使用します。

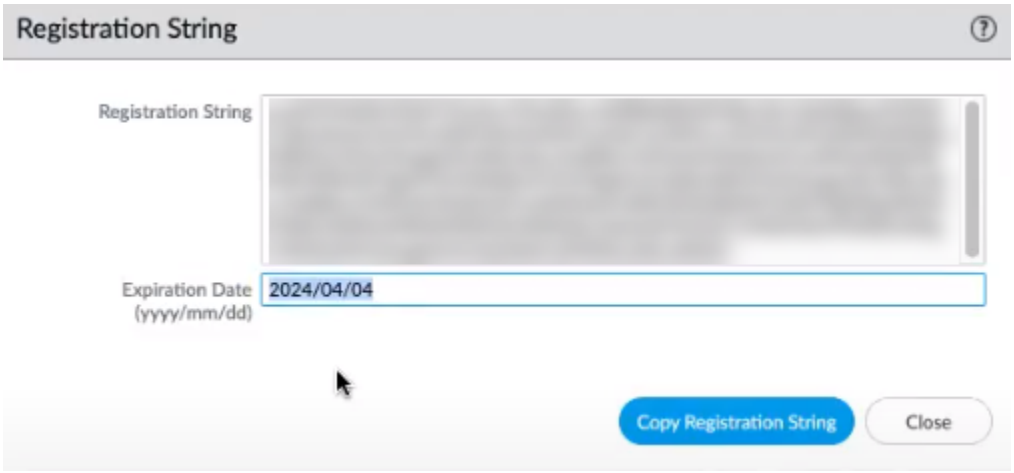
PINを取得するには

STEP 1 | Panoramaコンソールで、前のセクションで作成したクラウドデバイスグループを探します。

STEP 2 | [登録文字列]フィールドで、**[Generate (生成)]**をクリックします。

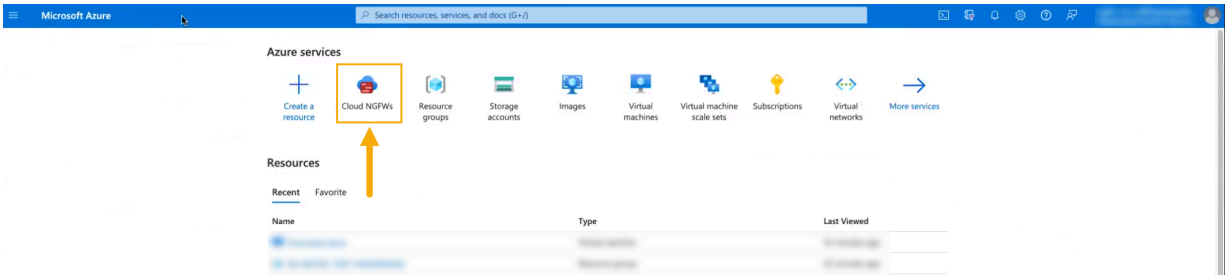


STEP 3 | **[Copy Registration String (登録文字列をコピー)]**を選択します。

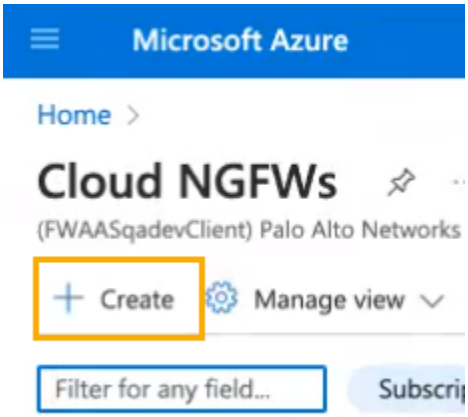


登録文字列をコピーしたら、Azure Marketplaceにアクセスして Cloud NGFWリソースを作成します。

STEP 4 | Azure Marketplaceで、**Cloud NGFWs**を選択します。

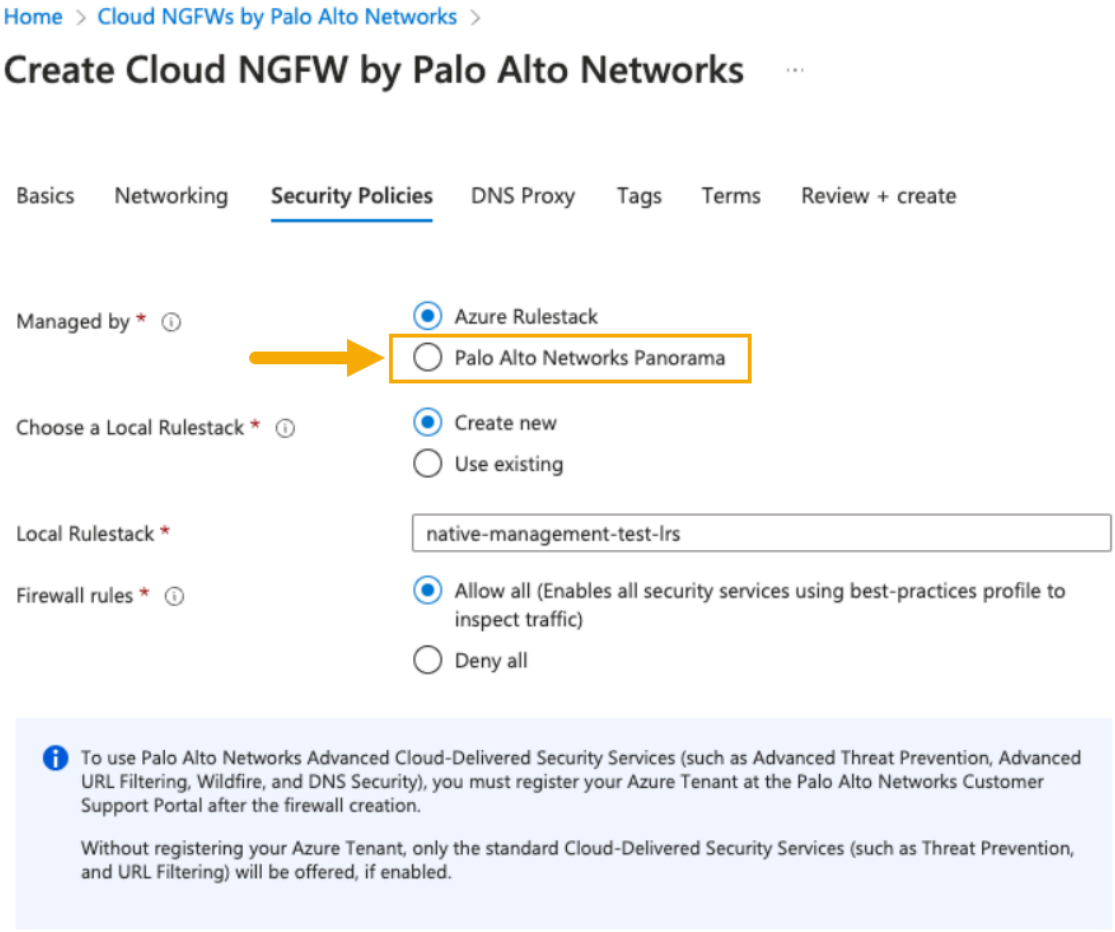


STEP 5 | **[+ Create (+作成)]**をクリックして、新しいCloud NGFWリソースを作成します。

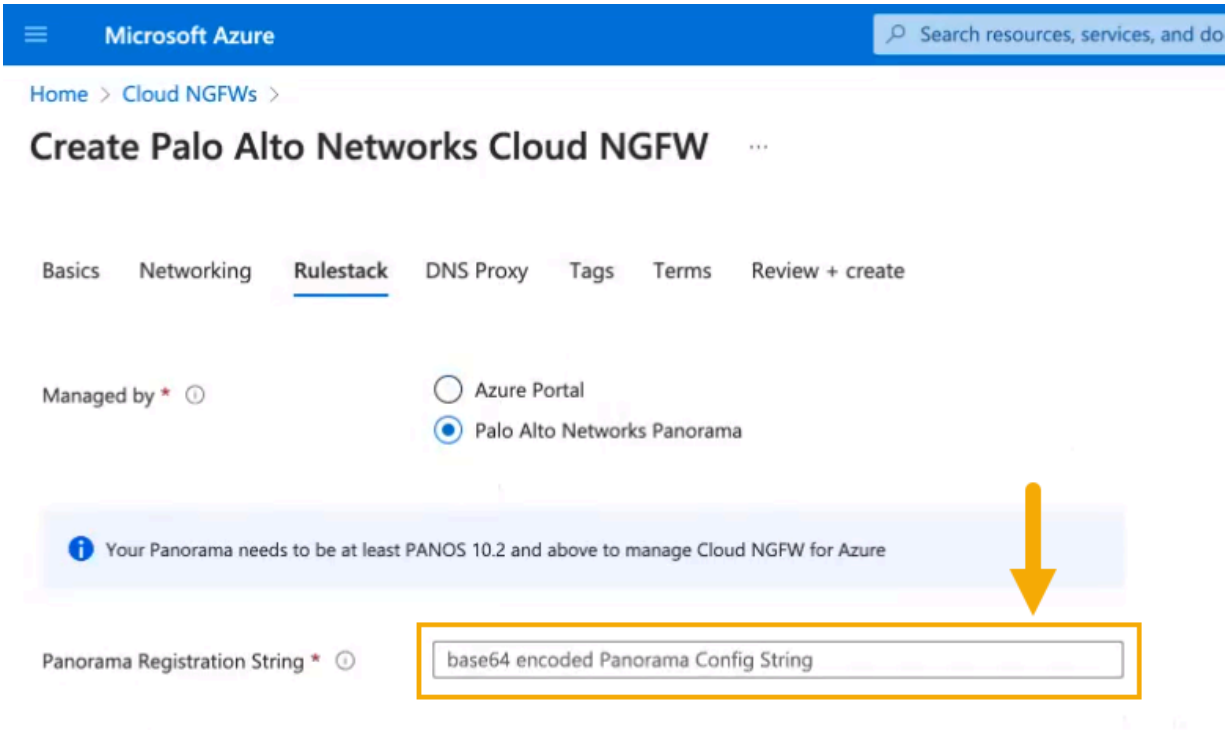


STEP 6 | セットアップ手順に従って、**[Create Palo Alto Networks Cloud NGFW (Palo Alto Networks Cloud NGFWを作成)]**に進みます。

1. Basic情報を設定します。
2. ネットワーキングを構成します。
3. セキュリティポリシーを設定します。**[Manged by (管理者)]**セクションで、**[Palo Alto Networks Panorama]**を選択します。



STEP 7 | [**Managed by Palo Alto Networks Panorama**]を選択すると、[Security Policies (セキュリティポリシー)]ページが変わり、[**Panorama Registration String (Panorama** 登録ストリング**)**]フィールドが表示されます。上記の手順3でコピーした登録文字列を入力します。



STEP 8 | DNSプロキシ、タグ、用語の情報を指定して、Cloud NGFWリソースの作成を続行します。設定を確認し、［**Create (**作成**)**］をクリックします。

Cloud NGFWリソースの作成には、約10~15分かかる場合があります。

PanoramaコンソールがCloud NGFWリソースにリンクされるようになりました。

Cloud NGFW ポリシー管理に Panorama を使用する

クラウドデバイスグループの追加

後 リンクに Cloud NGFWリソースをPanorama仮想アプライアンスに追加すると、デバイスグループの追加やデバイスグループへのポリシールールの適用など、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。

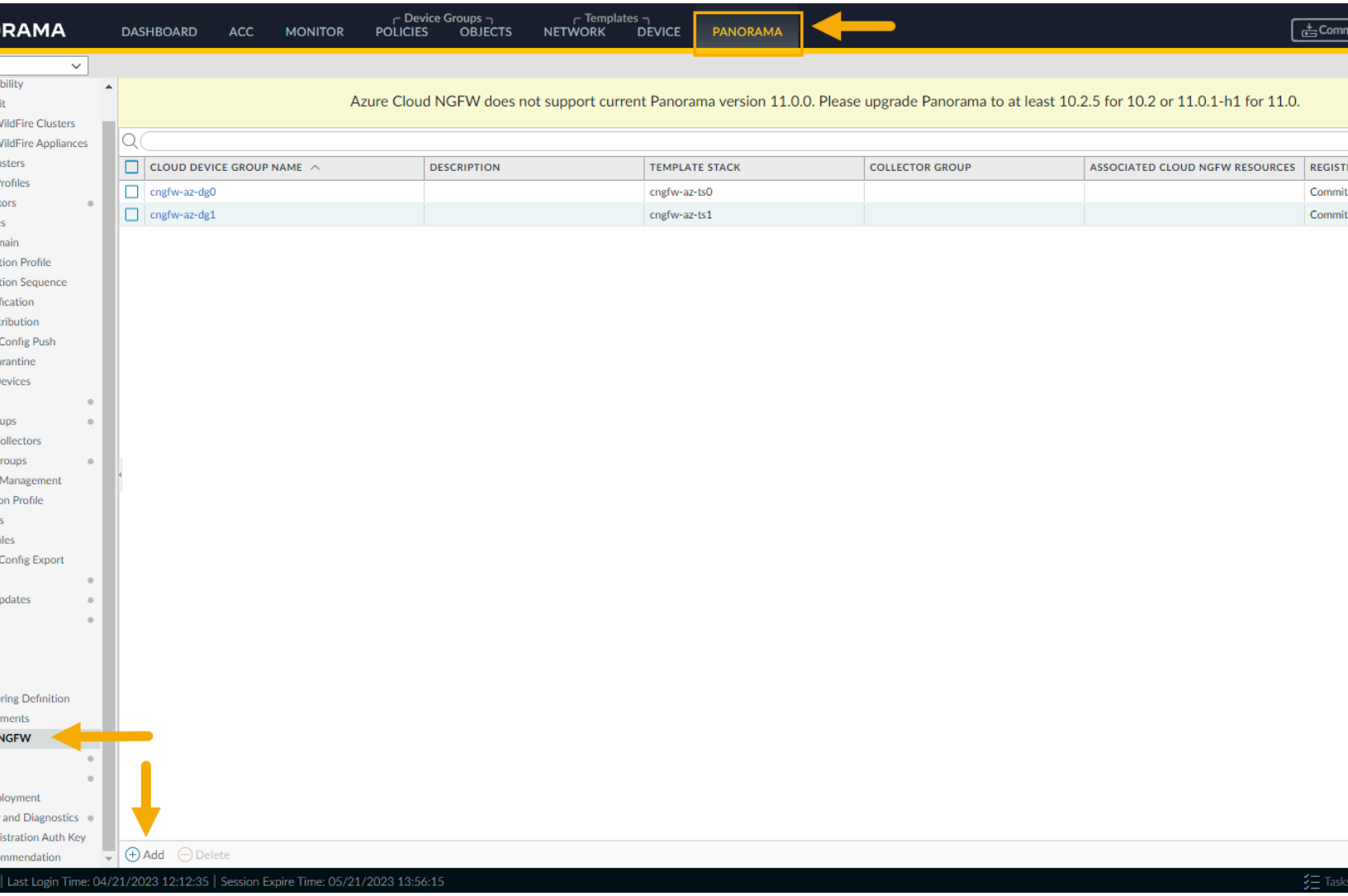
デバイスグループを使用し、ポリシールールやそれらが参照するオブジェクトを設定することができます。共有ルールおよびオブジェクトを最上層に、デバイス グループ固有のルールおよびオブジェクトをその配下に置くことで、デバイス グループを階層化することができます。これにより、ファイアウォールによるトラフィックの処理方法を強制するルールの階層を作成できます。詳細については、「デバイス グループの管理」を

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:

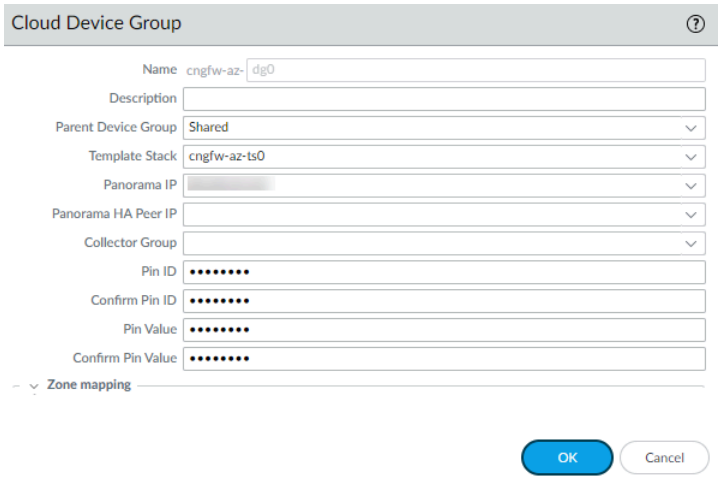
STEP 1 | **Azure** プラグインで、**Cloud NGFW** を選択します。

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、Azure を使用してCloud NGFW リソースに対して確立された場合に表示されます。

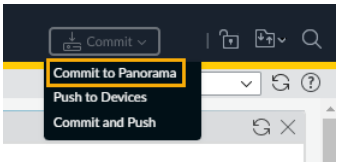


STEP 2 | 左下の**[Add(追加)]**をクリックします。

STEP 3 | **Device Group (クラウドデバイスグループ)]**画面で、次の手順を実行します。



1. 一意の 名前 クラウドデバイスグループの場合。
2. **Description (説明)** を入力します。
3. ドロップダウンを使用して、親デバイスグループを選択します。デフォルトでは、この値は共有されます。
4. ドロップダウンからTemplate Stack (テンプレートスタック)を選択します。または、**[Add (追加)]**をクリックして新規作成します。
5. 展開で使用する**Panorama IP**アドレスを選択します。ドロップダウンでプライベートまたはパブリックのIPアドレスを選択できます。
6. オプションでPanorama HAピア**IP**アドレスを選択します。
7. オプションでドロップダウンを使用して、Collector Group (コレクタグループ)を選択します。
8. オプションで、クラウドデバイスグループのゾーンマッピングを設定します。次の 2 つのゾーンのみがサポートされています。 パブリックまたはプライベート.
9. **OK** をクリックします。
10. Panoramaコンソールで変更をコミットしてクラウドデバイスグループを作成します。次に、Cloud NGFWリソースを作成するための登録文字列を生成し、Azureにデプロイします。



クラウドデバイスグループの削除

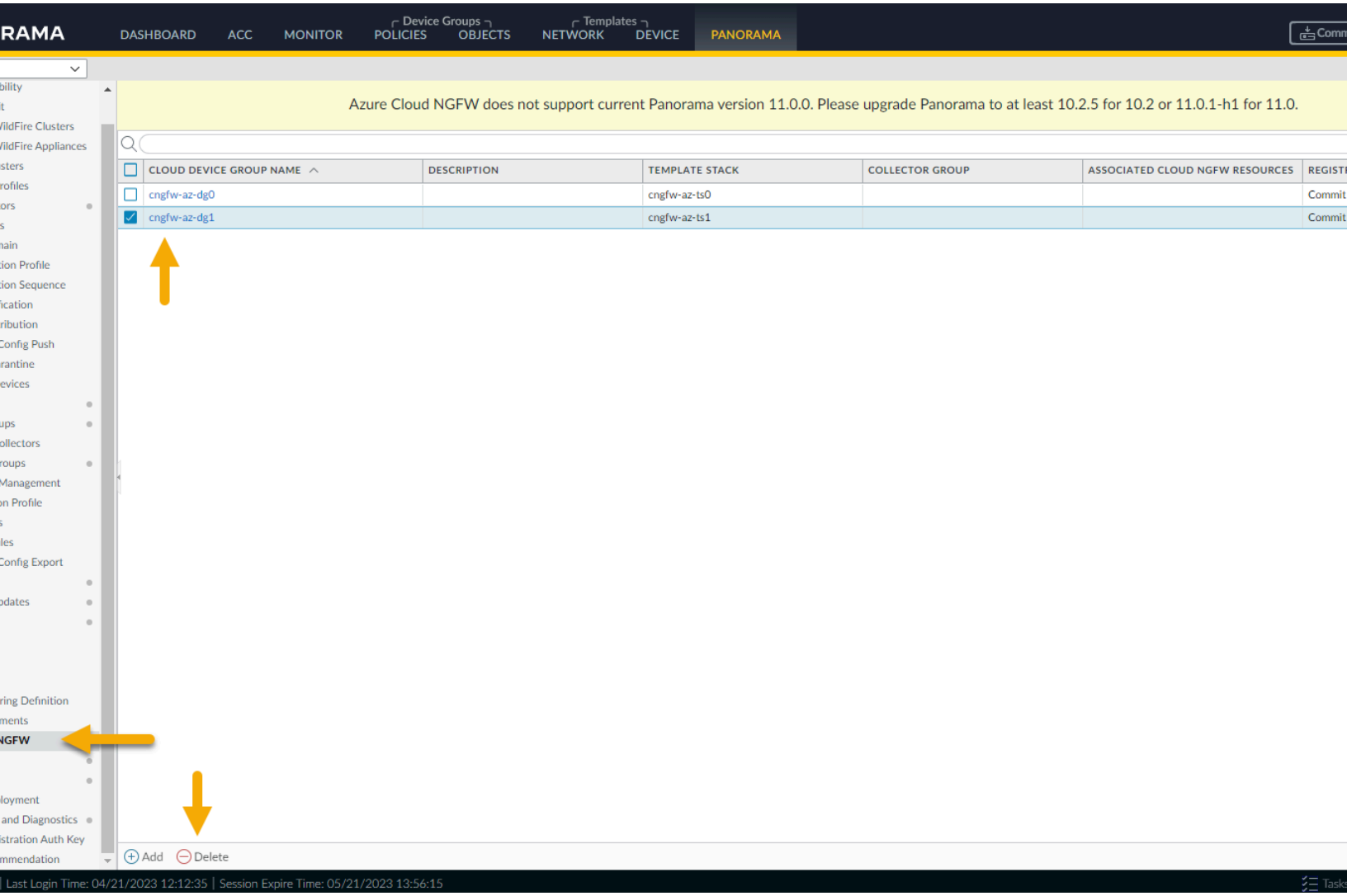
Panoramaコンソールを使用してクラウド デバイス グループを削除します。クラウド デバイス グループを削除できるのは、そのグループにファイアウォールが接続されていない場合のみです。

Panorama コンソールを使用してリソースから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。

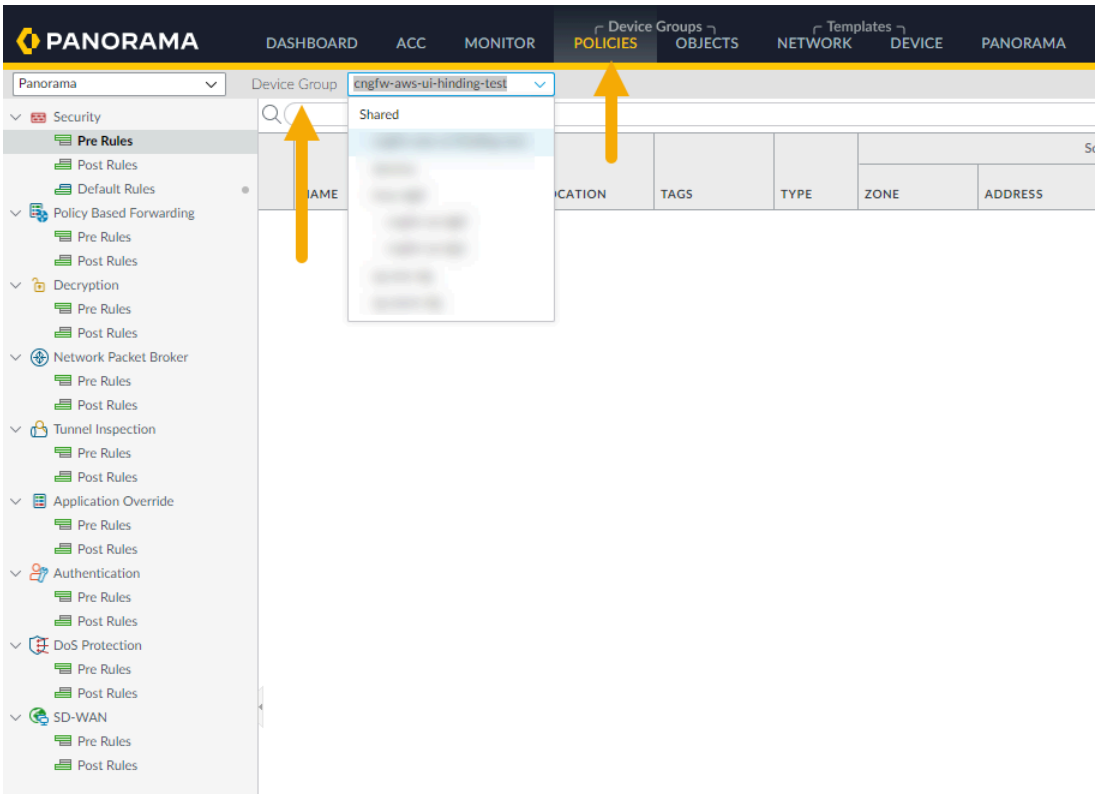
ポリシーの適用

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 ルールを一元的に管理できます。Panorama でポリシー ルールは、事前ルールまたは事後ルールとして作成します。これらのルールを使用すると、ポリシーを実装するための階層化されたアプローチを作成できます。詳細は、「Panoramaのポリシーの定義」を参照してください。

Panorama でクラウド デバイス グループのポリシー ルールを設定する方法:

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。

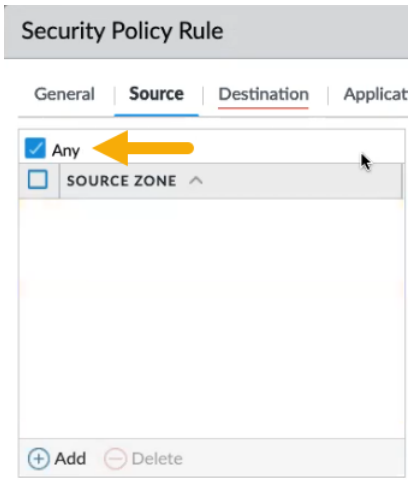


Cloud NGFWのデバイス グループを作成すると、名前は*cngfw*で始まります。例えば *cngfw-azure-demo*となります。

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

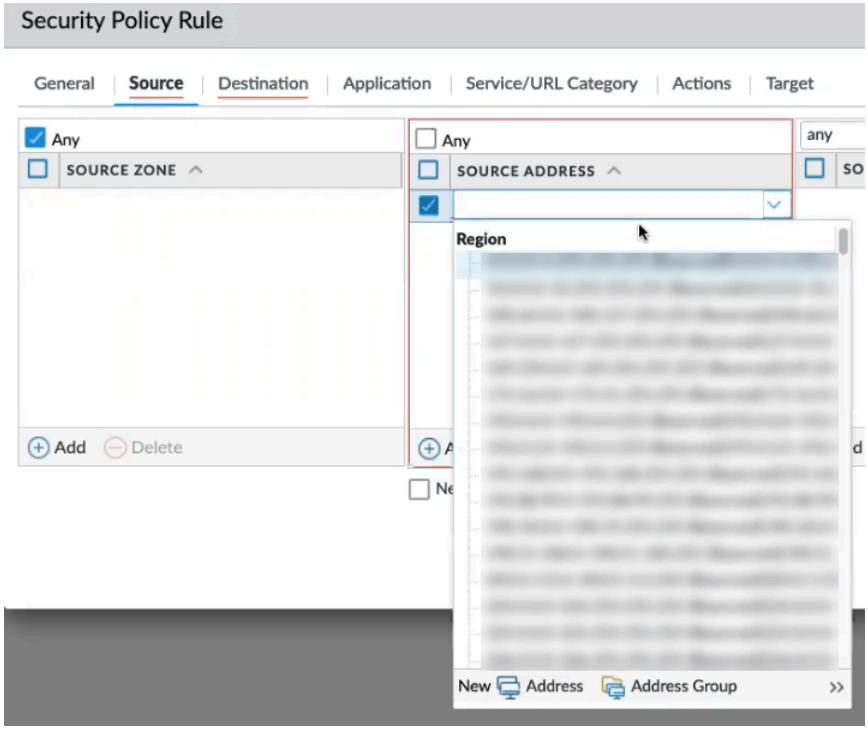
STEP 4 | [Security Policy Rule(セキュリティ ポリシー ルール)]画面で、デバイス　グループに適用するポリシーの要素を設定します。

1. **[General(全般)]**タブで、ポリシーの名前を含めます。必要に応じて、追加情報を入力します。
2. **[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。特定のソースゾーンを追加することはできません。



[Source Address(送信元アドレス)]を含めて、**[Source(送信元)]**ポリシールール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。



［**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ません。

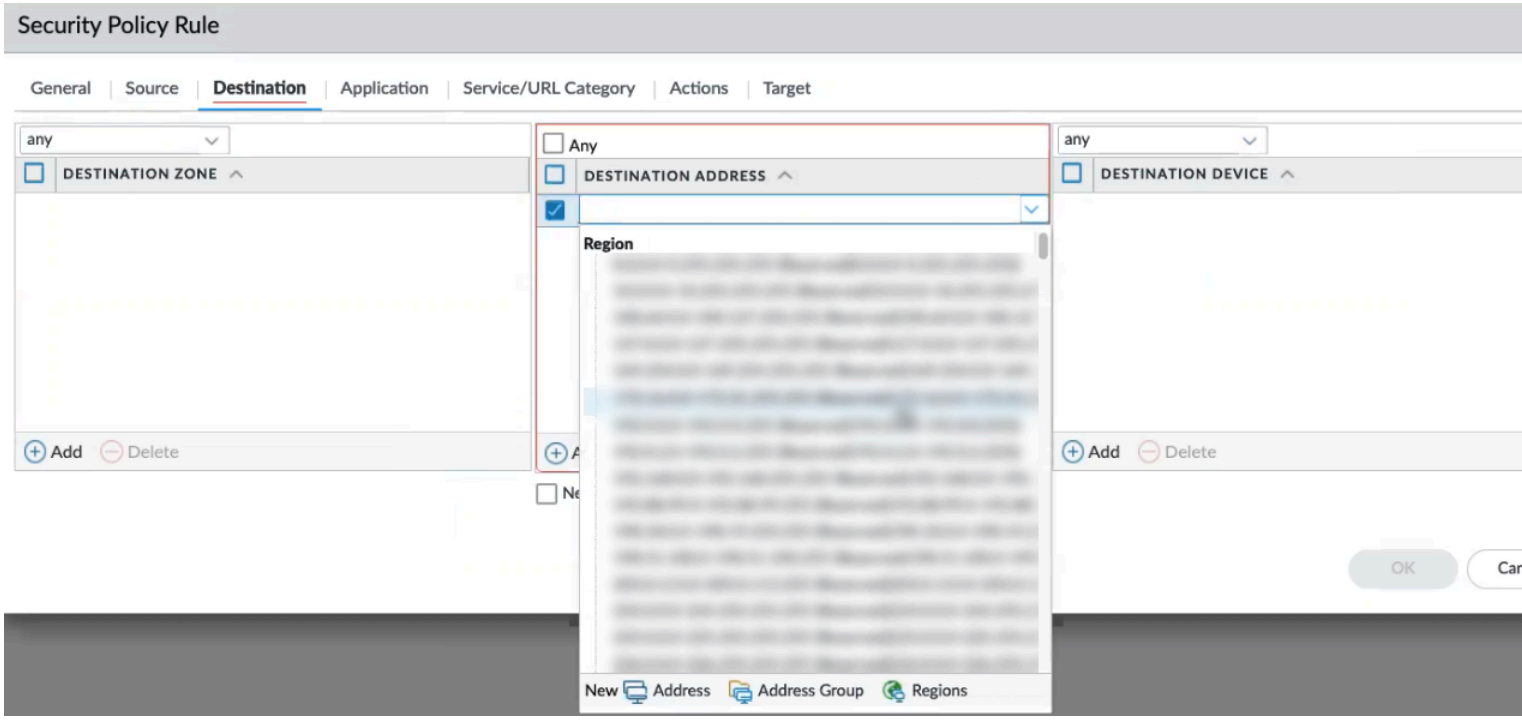
3. 宛先ポリシーは、トラフィックの宛先ゾーンまたは宛先アドレスを定義します。ドロップダウンを使用して既存のアドレスを選択するか、オプションを使用して新しいアドレ

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。

[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。

[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。

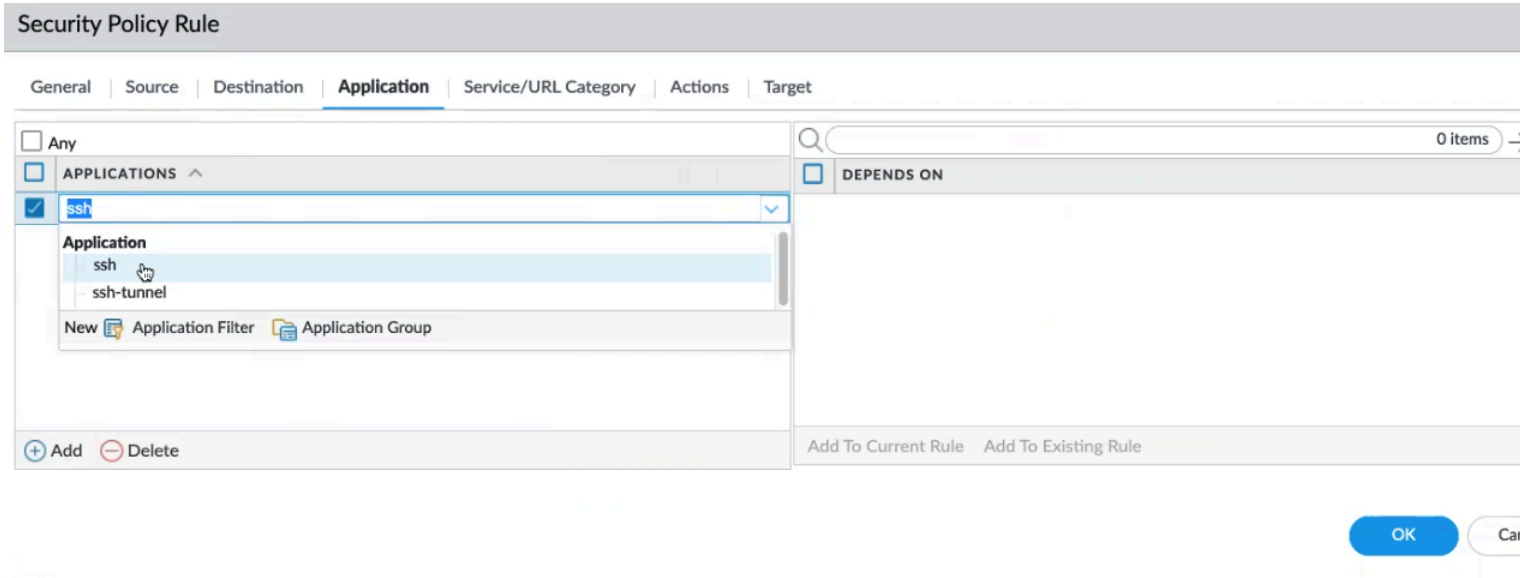
[Destination Device(宛先デバイス)]で、**[Any(任意)]**をクリックします。Cloud NGFWは、個別の宛先デバイスの追加をサポートしていません。



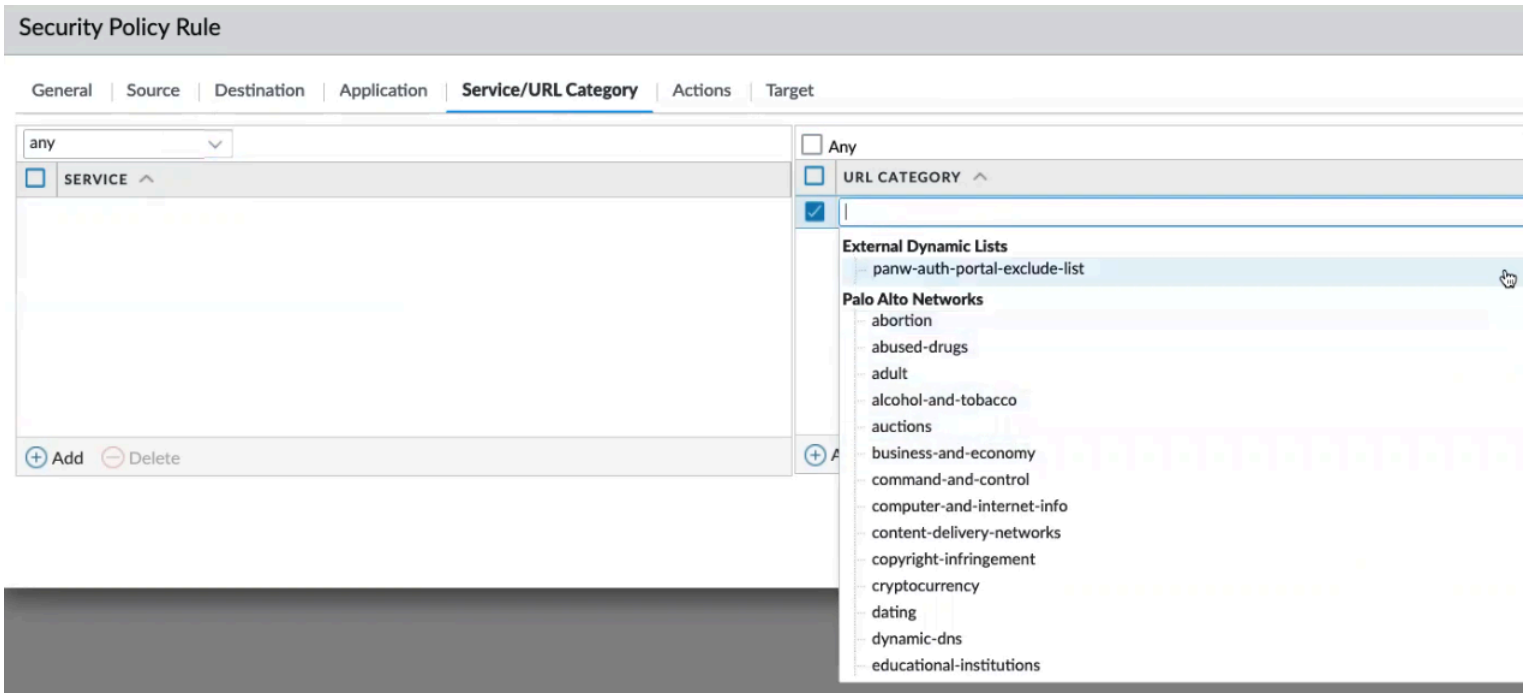
4. **Application**ポリシーを設定して、アプリケーションまたはアプリケーション グループに基づいて、ポリシーがアクションを実行するように設定します。管理者は、既存のApp-ID シグネチャを使用し、カスタマイズして、独自のアプリケーションや、既存の

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。

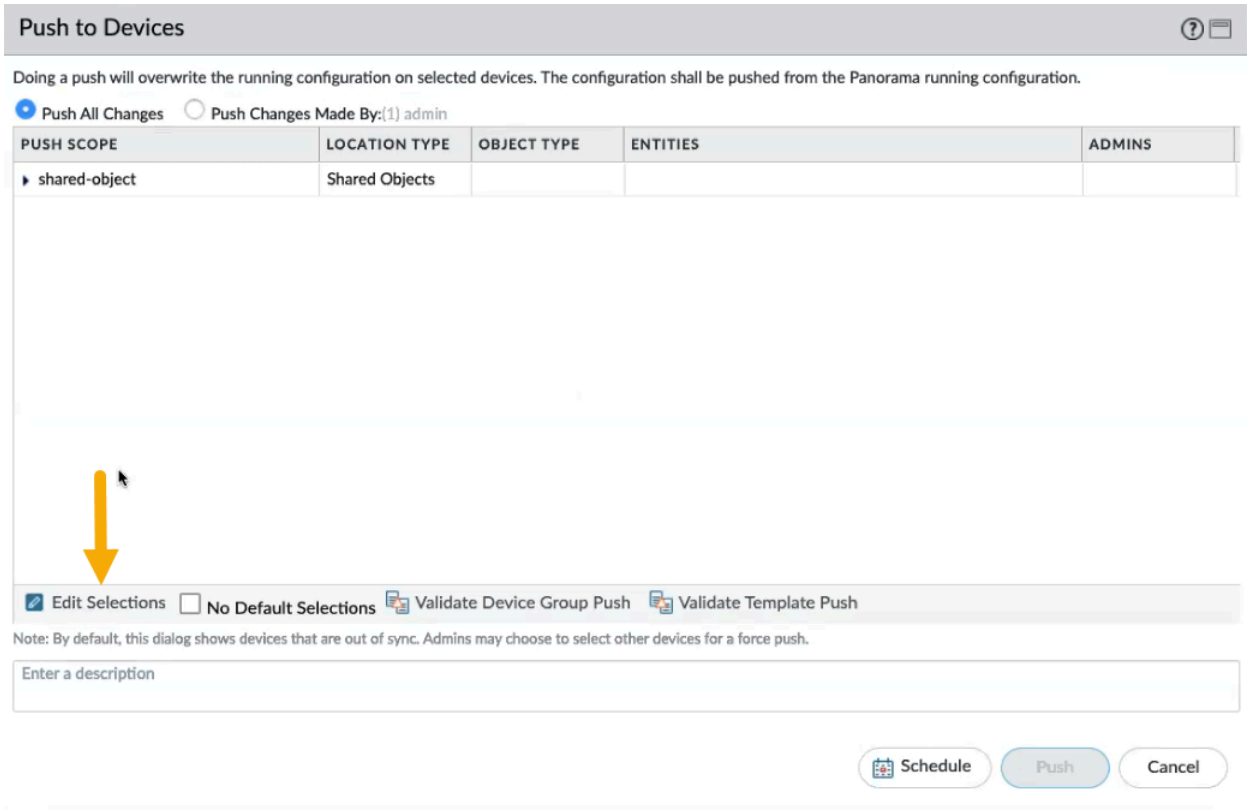
[Application(アプリケーション)]画面で[Any(任意)]をクリックするか、SSHなどの特定のアプリケーションを指定します。新しいアプリケーションポリシーを含めるには**[Add(追加)]**をクリックします。



5. 構成 サービス/**URL** カテゴリ ファイアウォールのポリシールールで、特定の TCP または UDP 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指定します。**[Service (サービス)]**レベルポリシールールまたは **[URL Category (URL**カテゴリ**)]** ポリシールールを **[Any (任意)]**を選択するか、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 5 | Cloud NGFW リソースのクラウドデバイスグループにポリシールールを適用した後、Panorama コンソールで変更をプッシュします。**[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 6 | 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。

Cloud NGFW for AzureでユーザーIDを有効化する

IP アドレスとは対照的に、ユーザーの識別は効果の高いセキュリティ インフラに欠かせない要素です。誰がネットワーク上の各アプリケーションを使い、誰が脅威を伝搬した可能性があり、誰がファイルを転送中であるのか把握することで、セキュリティポリシーを強固なものにして、インシデントに素早く対応できるようになります。Palo Alto Networks のファイアウォールの標準機能である User-ID™ により、多彩なレポジトリに保存されているユーザー情報を活用できるようになります。User-IDの概念の詳細については、[PAN-OS documentation (PAN-OSドキュメント)]を参照してください。

ユーザーIDまたはグループからポリシーを適用するには

- ファイアウォールは、IPアドレスをユーザ名にマッピングできる必要があります。
- ユーザーIDは、ユーザーマッピング情報を収集するためのさまざまなメカニズムを提供します。詳細については、こちらをクリックしてください。
- マッピング方法でマッピングをキャプチャできない場合は、ユーザーを認証ポータルログインにリダイレクトするように認証ポリシーを構成できます。ユーザーは、IDプロバイダーと照合される資格情報を提供し、それに応じてアクセスを強制できます。認証ポリシーの詳細については、こちらをご覧ください。

*Cloud NGFW*は現在、エージェントのインストールによるサーバー監視マッピングのみをサポートしています。

ユーザーとグループベースのポリシーを有効にするには

- ファイアウォールでは、使用可能なすべてのユーザと対応するグループメンバシップのリストが必要です。
- PanoramaはLDAPサーバーに直接接続してグループマッピング情報を収集し、Cloud NGFWに配信します。

Cloud NGFWの導入には、Palo Alto Networks Terminal Server Agentまたはネットワーク内のドメインサーバーで実行されるWindowsベースのエージェントを使用したサーバー監視の使用をお勧めします。

STEP 1 | ユーザ ID を有効化

1. Panorama にログインします。
2. **Network** > **Zones** の順に選択し、ゾーンの **Name** (名前) をクリックします。
3. **Enable User Identification** (ユーザー **ID** の有効化) を行って **OK** をクリックします。

STEP 2 | ユーザーID エージェントの専用サービス アカウントを作成します。

STEP 3 | ユーザー対グループのマッピング。

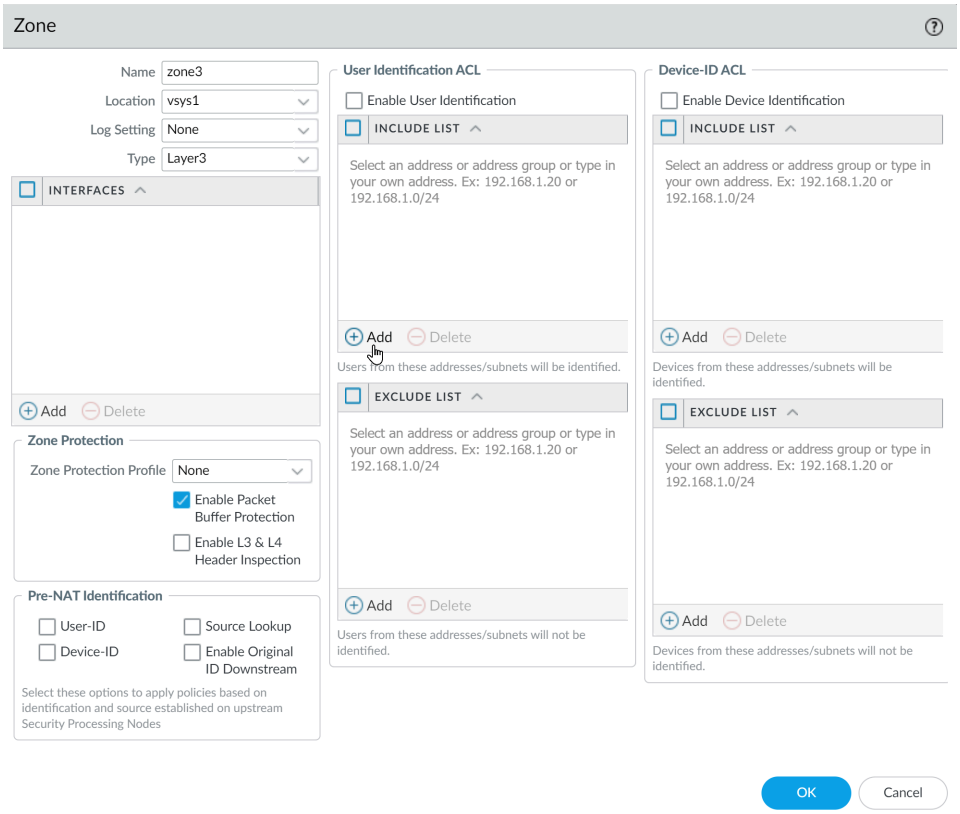
STEP 4 | UsersへのIPアドレスマッピングを設定します。Cloud NGFW for Azureは、Windows User-IDエージェントまたはターミナルサーバエージェントを使用したIPとユーザーのマッピングをサポートしています。

- Windows ユーザー ID エージェント を使用してユーザー マッピングを構成する
- Terminal Server Users (ターミナル サーバー ユーザー)向けのユーザー マッピングの設定

STEP 5 | ユーザーマッピングに含めるネットワーク、除外するネットワークを指定します。

ベストプラクティスとして、必ず *User-ID* に含める、あるいは除外するネットワークを指定してください。これにより、信頼できるアセットだけがプロービングされるようになり、不要なユーザーマッピングが意図せず作成されなくなります。

1. **[Network (ネットワーク)]** > **[Zones (ゾーン)]**を選択し、ユーザーIDを設定しているゾーンを選択します。
2. 必要に応じて、ネットワークを**[Include (含む)]**リストと**[Exclude (除外)]**リストに追加します。
3. **OK** をクリックします。



STEP 6 | ユーザーおよびグループ ベースのポリシーを有効化します。

Cloud NGFWでUser-IDを有効にしたら、セキュリティポリシールールの送信元または送信先としてユーザー名またはグループ名を使用できます。

1. **[Policies (ポリシー)]** > **[Security (セキュリティ)]**を選択し、**[Add (追加)]**をクリックして新しいセキュリティポリシー規則を作成するか、セキュリティポリシー名をクリックして既存の規則を変更します。
2. [User (ユーザー)] を選択し、次のいずれかの方法で、ルールでマッチさせるユーザーおよびグループを指定します。
   - 一致基準としてユーザー/グループを選択する場合は、Source User (送信元ユーザー) セクションで **Add (追加)** をクリックすると、ファイアウォールのグループ マッピング機能により検出されたユーザーおよびグループのリストが表示されます。ルールに追加するユーザーあるいはグループを選択します。
   - 正常に認証されたかどうかに関係なく任意のユーザーと一致し、特定のユーザー名またはグループ名を把握する必要がない場合は、Source User [送信元ユーザー]リストの上にあるドロップダウンから **known-user** [既知のユーザー]または **unknown** [不明]を選択します。
3. 必要に応じてルールのその他の部分を設定し、**OK** をクリックして設定を保存します。セキュリティ ルールのその他のフィールドの詳細は、「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。

できる限りユーザーではなくグループに基づいてルールを作成します。これにより、ユーザー ベースが変更するたびにルールを更新(コミットが必要)し続ける必要がなくなります。

STEP 7 | セキュリティポリシールールを作成して信頼できるゾーン内で User-ID を安全に有効化し、User-ID トラフィックがネットワーク外に出ないようにします。

「インターネット ゲートウェイのセキュリティポリシーの推奨設定 」に従い、必ずエージェント（Windows エージェントおよび PAN-OS 統合エージェントの両方）がサービスを監視してファイアウォールにマッピングを配信しているゾーン内でのみ User-ID アプリケーション（`paloalto-userid-agent`）が許可されるようにします。具体的な内容は次のとおりです。

- エージェントが存在するゾーンおよび監視されているサービスが存在するゾーンの間（あるいは、エージェントをホストしている特定のシステムおよび監視されているサーバーの間の方がより好ましい）で `paloalto-userid-agent` アプリケーションを許可します。

- ユーザーマッピングを必要とするファイアウォールおよびエージェントの間、ユーザーマッピングを再配信しているファイアウォールおよびその情報を再配信しているファイアウォールの間で `paloalto-userid-agent` アプリケーションを許可します。

インターネットゾーンなどの外部ゾーンへの`paloalto-userid-agent`アプリケーションを拒否します。

ベストプラクティスとして、*HA*構成の***Enable Config Sync***オプションを常に有効にして、グループマッピングとユーザーマッピングがアクティブファイアウォールとパッシブファイアウォールの間で同期されるようにします。

STEP 8 | 変更を **Commit (**コミット**)** します。

制限事項

- 大規模なネットワークでは、すべてのファイアウォールがマッピング情報ソースに直にクエリを送るよう設定する代わりに、再配信を通じて一部のファイアウォールだけがマッピング情報を収集するよう設定することで、リソースを合理的に使用できます。AzureのCloud NGFWでは、ユーザーマッピング情報機能の再配布はサポートされていません。
- 認証および認可ポリシーはサポートされていません。
- User-IDマッピングのためのPAN-OSベースのエージェント方式はサポートされていません。
- User-IDマッピングのXML-API方式はサポートされていません。

オンプレミスサービスのサービスルートの設定

Cloud NGFW for Azureを構成して、DNSサーバー、外部動的リスト、ログコレクター、syslog、動的コンテンツ更新、LDAP、MFAなどのオンプレミスのホスト型サービスにアクセスできます。デフォルトでは、Cloud NGFWファイアウォールは管理インターフェイスを使用してこれらのタイプのサービスにアクセスします。ただし、管理インターフェイスの使用は推奨されない場合もあります。代わりに、Palo Alto Networksは、これらのサービスにアクセスするためにファイアウォールにサービスルートを設定することをお勧めします。サービスルートを使用する場合、サービスパケットは各サービスに割り当てたデータポートを使用してファイアウォールから出ます。その代わり、サービスは設定された送信元 IP および送信元インターフェイスに応答を送信します。

*Cloud NGFW for Azure*でサービスルートを構成するには、*Panorama*および*Panorama plugin for Azure 5.1.1*以降が必要です。

次のシナリオでは、サービスルートを使用する必要があります。

- プライベートIPアドレスを使用してオンプレミスネットワークでホストされるサービス。Cloud NGFW管理インターフェイスはオンプレミスネットワークに接続されていないため、サービスのプライベートIPアドレスにアクセスできません。
- サービスはインターネット経由でパブリックIPアドレスを介してアクセスできますが、許可リスト構成では静的送信元IPが必要です。Cloud NGFW管理インターフェイスは、SNAT変換されたソースIPを使用してインターネットにアクセスします。パブリックデータインターフェイスを使用してオンプレミスサービスにアクセスするサービスルートを構成することができ、トラフィックソースIPアドレスはクラウドNGFWパブリックIPアドレスにSNAT変換されます。

デフォルトでは、各Cloud NGFW Panoramaテンプレートには、プライベート、パブリック、ループバックの3つのゾーンが含まれています。ループバックゾーンは、サービスルートに使用されるインターフェイス loopback.3 を使用します。

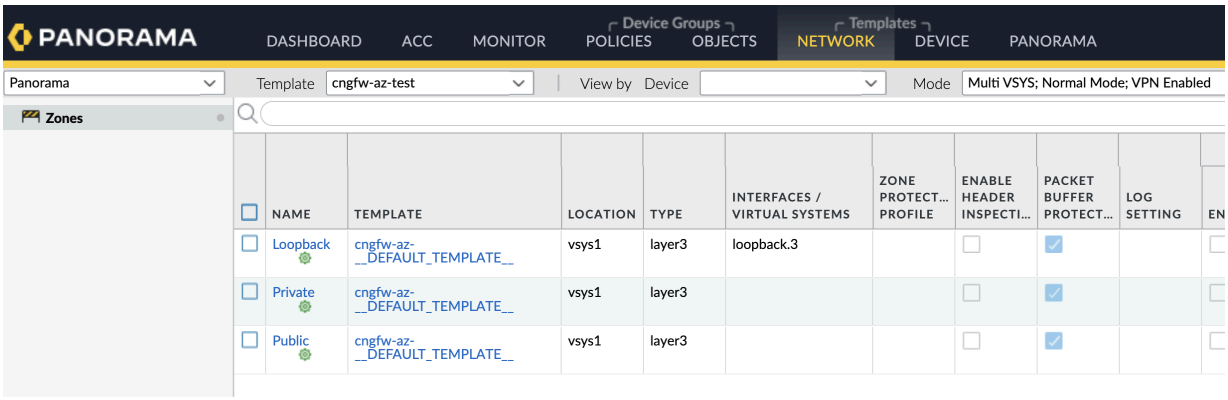
Cloud NGFW for Azureでサービスルートを構成するには、次の手順を実行します。

STEP 1 | Panorama にログインします。

STEP 2 | Azure 5.1.1以降のPanoramaプラグインがインストールされていることを確認します。

STEP 3 | **[Templates (テンプレート)]** > **[Device (デバイス)]**に移動し、[Template (テンプレート)]のドロップダウンからクラウドNGFWテンプレートを選択します。

cngfw-az - _DEFAULT_TEMPLATE_ は、*Cloud NGFW* の下の *Panorama plugin for Azure* でテンプレートスタックを作成した後にのみ表示されます。



STEP 4 | **[Setup (セットアップ)]** > **[Services (サービス)]** を選択して **[Service Route Configuration (サービスルートの設定)]** をクリックします。

STEP 5 | **Customize (**カスタマイズ**)** を選択し、次のいずれかを選択してサービスルートを作成します。

- 事前定義済みのサービスの場合：

  1. **IPv4** あるいは **IPv6** を選択し、サービスルートをカスタマイズしたいサービスのリンクをクリックします。

     複数のサービスに同じ送信元アドレスを簡単に使用するには、サービスのチェックボックスをオンにして、***[Set Selected Routes (***選択したルートを設定***)]***をクリックして、次の手順に進みます。

  2. 送信元アドレスのリストを制限するには、 送信元インターフェイスとして loopback.3 を選択します。次に、サービスルートとして（そのインターフェイスから）送信元アドレスを 選択します。アドレス オブジェクトは、選択したインターフェイスで既に設定されている場合は、送信元アドレスとして参照することもできます。**Any (**すべての**)** Source Interface (ソース インターフェイス) を選択すると、アドレスを選択する Source Address (送信元アドレス) リストで、あらゆるインターフェイスのすべての IP アドレスを利用できるようになります。ではサービスルートに管理インターフェイスを使用するようにファイアウォールに指示されるため、**[Use default (**デフォルトを使用**)]**を選択しないでください。

     サービス ルートの送信元アドレスは、参照先インターフェイスから構成の変更を継承しません。別の *IP* アドレスまたはアドレス オブジェクトにインターフェイス *IP* アドレスを変更しても、対応するサービス ルート 送信元アドレスは更新されません。これにより、コミットエラーが発生し、サービス ルートを有効な送信元アドレス値に更新する必要があります。

  3. **OK** をクリックして設定を保存します。

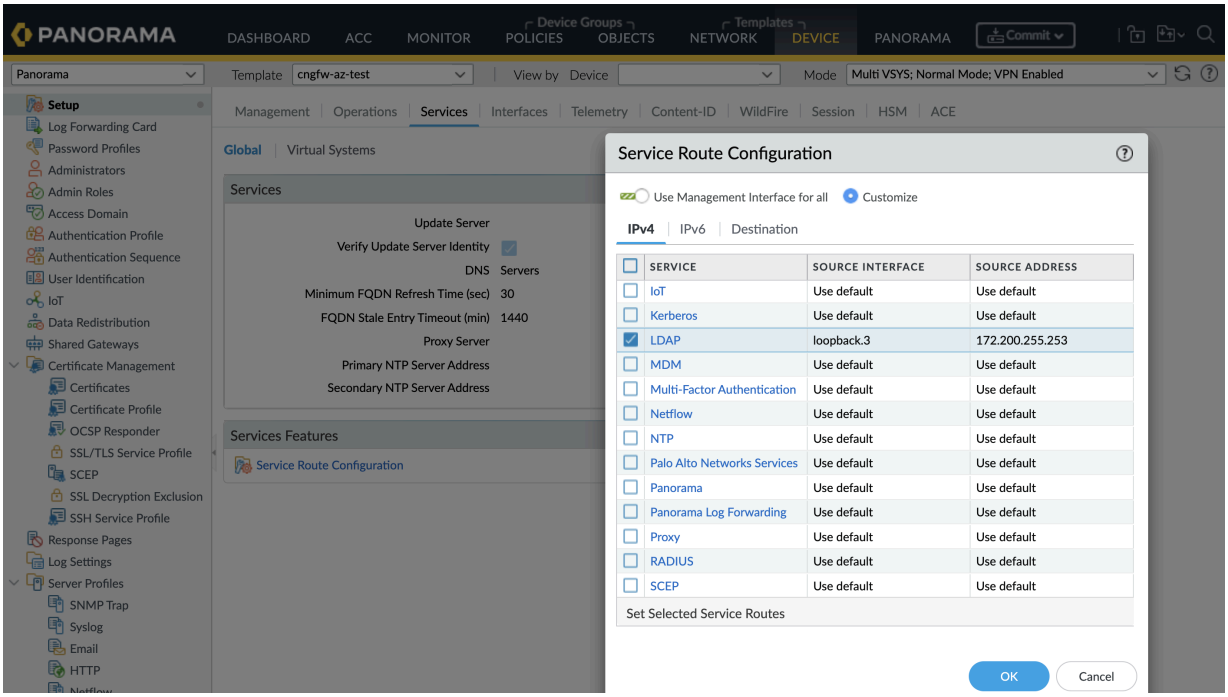
  4. サービス用に **IPv4** および **IPv6** アドレスの両方を指定したい場合はこのステップを繰り返します。

- サービスがリストにない場合は、[Destination (宛先)]タブを選択して、IPアドレスでターゲットサービスを指定します。

  1. **Destination (**宛先**)** を選択し、**Destination (**宛先**) IP** アドレス を **Add (**追加**)** します。このケースでは、この設定済みの **Destination (**宛先**)** アドレスにマッチする宛先 IP アドレスと共にパケットが到達した場合、そのパケットの送信元 IP アドレスが、次のステップで設定する **Source Address (**送信元アドレス**)** にセットされます。

  2. 送信元アドレスのリストを制限するためには、**loopback.3** インターフェイスを選択し、(インターフェイスから) Source Address (送信元アドレス) をサービスルートとして選択します。**Any (**すべての**)** Source Interface (ソース インターフェイス) を選択すると、アドレスを選択する Source Address (送信元アドレス) リストで、あらゆるインターフェイスのすべての IP アドレスを利用できるようになります。[MGT]を選択すると、ファイアウォールはサービスルートに MGT インターフェイスを使用します。

3. **OK** をクリックして設定を保存します。



STEP 6 | 変更を **Commit (**コミット**)** します。

STEP 7 | クラウドNGFWがオンプレミスサービスに到達できるようにするセキュリティポリシールールを追加します。

セキュリティポリシールールは、次のようにサービスルートトラフィックを照合できます。

- ［Any (任意)］ ゾーンから ［Public (パブリック)］ ゾーンまたは ［Private (プライベート)］ ゾーン（サーバにパブリックまたはプライベートの IP アドレスが設定されているかどうかによって異なる）。
- 送信元 IP アドレス（172.200.255.253）から宛先 IP アドレス（サービスの IP アドレス）。

ポリシーでのXFF IPアドレス値の使用

ネットワーク上のユーザーとの間にロード バランスなどのアップストリーム デバイスを有する場合、 Cloud NGFW インスタンスと Cloud NGFWは、アップストリーム デバイスの IPアドレスを、コンテンツを要求したクライアントの IPアドレスではなく、プロキシが転送する HTTP/HTTPS トラフィックの送信元 IPアドレスと見なすことがあります。多くの場合、アップストリーム デバイスは、コンテンツを要求したクライアントまたは要求の送信元クライアントの実際の IPv4 または IPv6 アドレスが含まれている HTTP リクエストに、X-Forwarded-For (X-Forwarded-For - XFF)ヘッダーを追加します。

Microsoft Azure では、デフォルトで、アプリケーション ゲートウェイが元の送信元 IPアドレスとポートを XFF ヘッダーに挿入します。ファイアウォールのポリシーで XFF ヘッダーを使用するには、XFF ヘッダーからポートを省略するようにアプリケーション ゲートウェイを設定する必要があります。アプリケーションゲートウェイの構成方法については、Azureのドキュメントを参照してください。

この機能は、*Panorama*が管理する*Cloud NGFW for Azure*でのみサポートされます。

Panoramaでセキュリティポリシールールを設定するときに、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。パケットがファイアウォールに到達する前に単一のプロキシ サーバーを通過する場合、XFF フィールドには発信元エンドポイントの IP アドレスが入ります。ただし、パケットが複数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後に追加された IP アドレスを使用してポリシーを適用したり、IP 情報に依存する他の機能を使用することができます。

STEP 1 | Panorama にログインします。

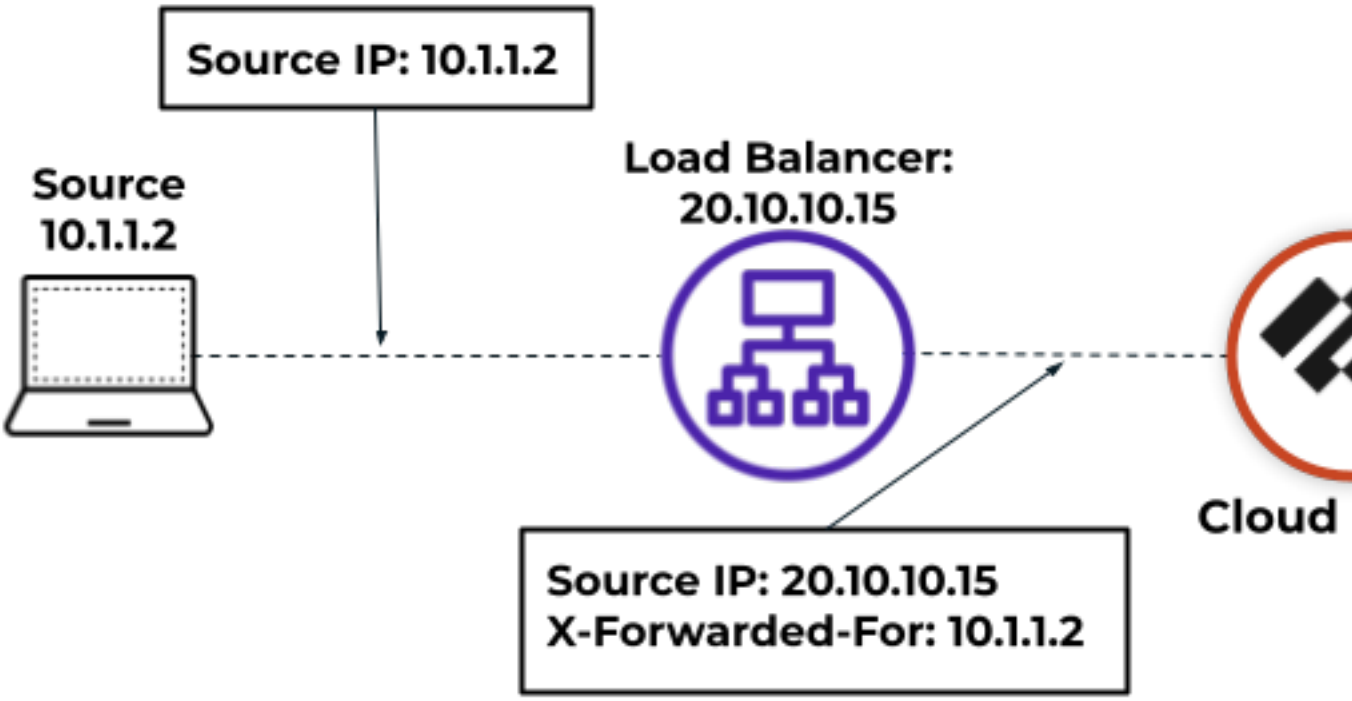
STEP 2 | Cloud NGFW for Azureクラウドデバイスグループを選択します。

STEP 3 | **[Device (デバイス)]** > **[Setup (セットアップ)]** > **[Content ID (コンテンツID)]** > **[X-Forwarded-For Headers （XFFヘッダー）]**を選択します。

STEP 4 | 編集アイコンをクリックします。

STEP 5 | **Use X-Forwarded-For (XFF)** ヘッダードロップダウンから、**Enabled for Security Policy (**セキュリティ ポリシーに対して有効化**)** を選択します。

セキュリティポリシー用の***X-Forwarded-For Header (XFF*ヘッダー)** と *User-ID* を同時に有効にすることはできません。



STEP 6 | (任意) **Strip X-Forwarded-For Header (XFF**ヘッダー**)** を選択して、発信 HTTP 要求から XFF フィールドを削除します。

このオプションを選択しても、ポリシーでの XFF ヘッダーの使用は無効になりません。Cloud NGFW for Azureは、XFFフィールドを使用してポリシーを適用した後、クライアント要求からXFFフィールドを除去します。

STEP 7 | **OK** をクリックします。

STEP 8 | 変更を **Commit (**コミット**)**します。

Cloud NGFWのログとアクティビティをPanoramaで表示する

Cloud NGFW ログをパノラマで表示する

Cloud NGFWリソースがPanorama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。

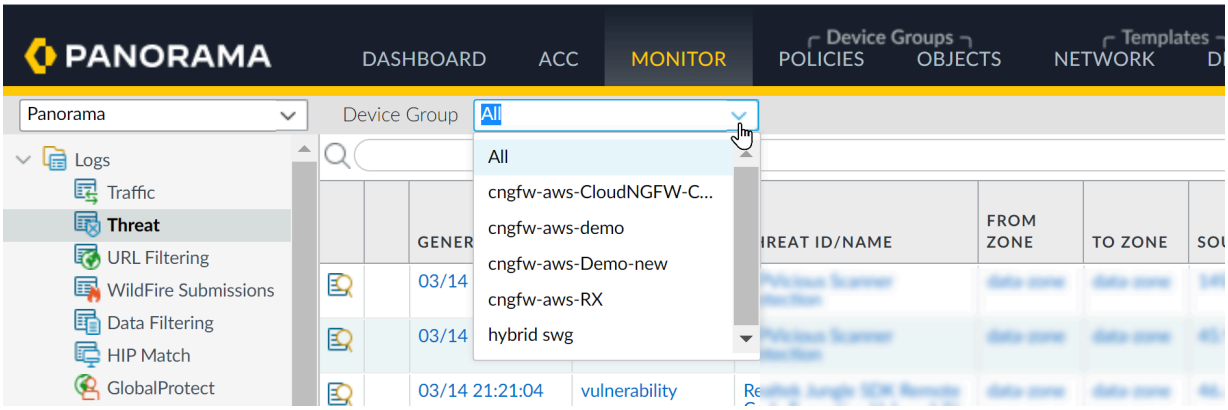
STEP 1 | Panorama にログインします。

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

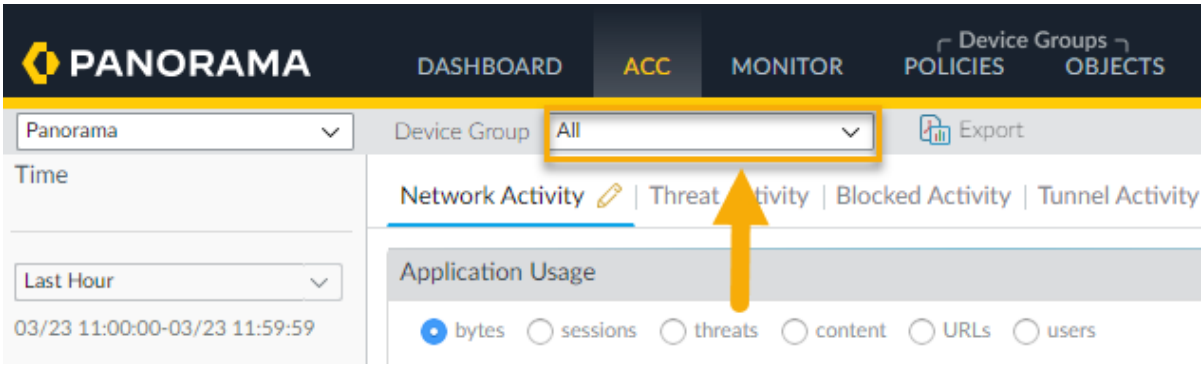
ACCは、ネットワーク内のアクティビティに関する実用的なインテリジェンスを提供する分析ツールです。ACCは、Cloud NGFWログを使用してネットワーク上のトラフィック トレンドをグラフィカルに表現します。このグラフィカル表現を使用して、データにアクセスし、ネットワークの使用パターン、トラフィック パターン、疑わしいアクティビティ、異常を含め、ネットワーク上のイベント間の関係を視覚化できます。

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。

ロギング

Cloud NGFWは、Azureポータルに作成するAzure Log Analytics Workspaceにトラフィック、脅威、復号化のログを送信できます。

Cloud NGFW on Azure のロギングの設定

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、ウイルス 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、Azureポータルに作成するAzure Log Analytics Workspaceにトラフィック、脅威、復号化のログを送信できます。ログ分析ワークスペースは、ワークスペースID、プライマリキー、およびコントロールプレーンによってロギングAPIを通じて取得されるセカンダリキーに関連付けられます。

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 Azure 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（ウイルス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 Azure 脅威ログフィールドを参照してください。

重要度	説明
Critical (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。
High（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。

重要度	説明
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 Azure 復号化ログフィールドを参照してください。

Cloud NGFW for Azure トラフィック ログ フィールド

フィールド名	の意味
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。
宛先アドレス (dst)	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 • 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
受信済バイト (bytes_received)	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。

フィールド名	の意味
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）	セッションの開始時間。
経過時間 (elapsed)	セッションの経過時間。
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、サブタイプが同じになっているセッションの数です。
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)。
送信元（srcloc）	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（dstloc）	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理由。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。 • 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。

フィールド名	の意味
	• 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時に、 SSL 送信プロキシ暗号化または 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。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。

フィールド名	の意味
XFF アドレス（xff）	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 Azure 脅威ログフィールド

フィールド名	の意味
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。
宛先アドレス (dst)	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

フィールド名	の意味
	• 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 • 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

フィールド名	の意味
	• 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 • url — URL フィルタリング ログ • ml-ウイルス —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ウイルス。 • virus—アンチウィルスプロファイルで検出したウィルス • 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-virus—アンチウィルスプロファイルで検出したウィルス
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ウイルス検出、*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脅威 *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	の意味
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です。
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）	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 Azure 復号化ログフィールド

フィールド名	の意味
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。
宛先アドレス (dst)	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 (tls_keyxchg)	セッションに使用される鍵交換アルゴリズム。
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。

フィールド名	の意味
ハッシュ アルゴリズム (tls_auth)	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 (ec_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。
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

ログ設定を有効にする

ログ設定を有効にするには

STEP 1 | ホームページから、ログ設定を有効にするCloud NGFWファイアウォールに移動します。

STEP 2 | **[Log Settings (ログ設定)]**をクリックします。

STEP 3 | **[Enable Log Settings (ログ設定を有効にする)]**をチェックします。

STEP 4 | ログ設定を有効にするログ分析ワークスペースを、**[Log Settings (ログ設定)]**ドロップダウンから選択します。

STEP 5 | **Save**（保存）をクリックします。

ログ設定を無効にする

ログ設定を無効にする方法：

STEP 1 | ホームページから、ログ設定を有効にするCloud NGFWファイアウォールに移動します。

STEP 2 | **[Log Settings (ログ設定)]**をクリックします。

STEP 3 | **[ログ設定を無効にする]**をチェックします。

STEP 4 | ログ設定を無効にするログ分析ワークスペースを、**[Log Settings (ログ設定)]**ドロップダウンから選択します。

STEP 5 | **Save**（保存）をクリックします。

Cloud NGFW for Azureでアクティビティログを有効にする

Cloud NGFW for Azure 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。

クラウド上の複数のロギング宛先 NGFW for Azure

Cloud NGFWリソースのログを管理し、クラウドセキュリティに関するインサイトを得ることができます。Cloud NGFW for Azureから生成したログをAzure Log Analyticsのワークスペースやに同時に複数の宛先に送信できます。これらのログには、トラフィックログと脅威ログの両方が含まれます（URLフィルタリング、WildFireの提出、ファイルブロック、データブロック、復号化から）

ログ分析ワークスペースとPanoramaでトラフィックログを有効にする

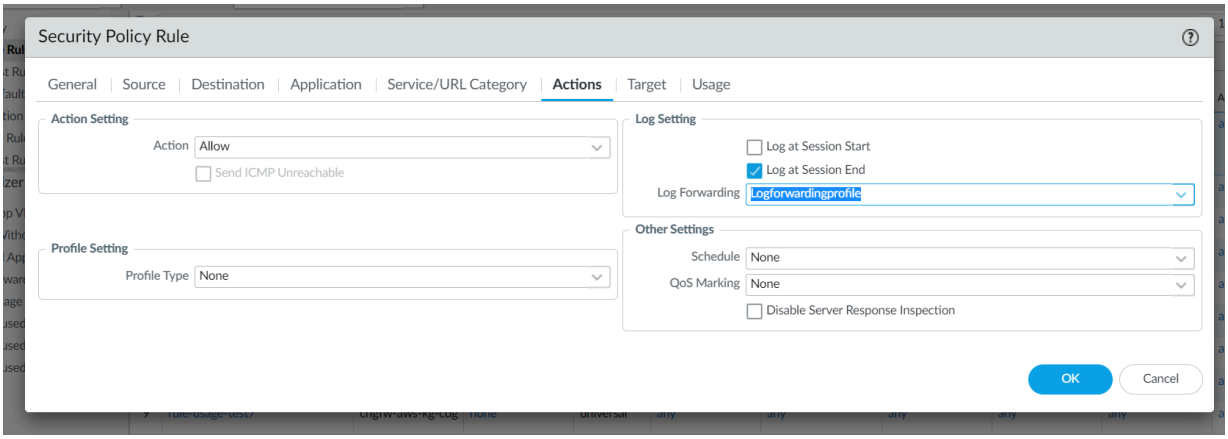
ログ分析ワークスペースとPanoramaでトラフィックログを有効にする手順は次のとおりです。

STEP 1 | Cloud NGFW for Azureコンソールでログ設定を有効にする。

STEP 2 | 「Panorama」で、**[Policies (ポリシー)]**に移動します。

STEP 3 | クラウドデバイスグループのポリシールールを選択します。

STEP 4 | **[Actions (アクション)]**タブを開き、**[Log Forwarding (ログ転送)]**プロファイルを選択します。



STEP 5 | **OK** をクリックします。

STEP 6 | Panoramaコンソールで変更を**Commit and Push (**コミットしてプッシュ**)**します。

トラフィックが送信されると、Log Analytics WorkspaceとPanoramaでCloud NGFWログを表示できます。詳しくは、[View the Logs (ログの表示)]と[View Cloud NGFW Logs in Panorama (Cloud NGFWログのPanoramaでの表示)]を参照してください。

ログ分析ワークスペースでトラフィックログを有効にし、Panoramaで無効にする

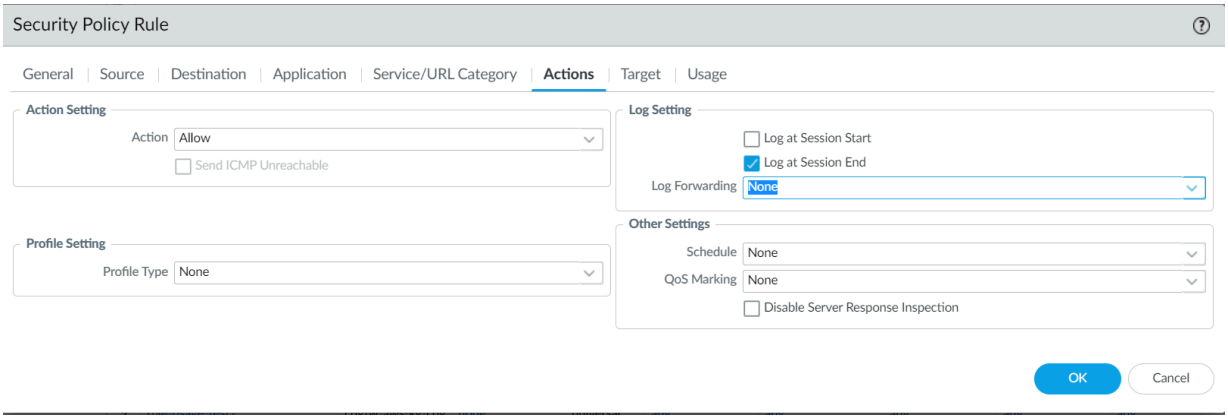
Log Analyticsワークスペースでトラフィックログを有効にし、Panoramaでログを無効にする手順は次のとおりです。

STEP 1 | Cloud NGFW for Azureコンソールでログ設定を有効にする。

STEP 2 | 「Panorama」で、**[Policies (**ポリシー**)]**に移動します。

STEP 3 | クラウドデバイスグループのポリシールールを選択します。

STEP 4 | 「**Actions (**アクション**)**」タブに移動し、ログ転送プロファイルで**[None (**なし**)]**を選択します。



STEP 5 | **OK** をクリックします。

STEP 6 | Panoramaコンソールで変更を**Commit and Push (コミットしてプッシュ)**します。

トラフィックが送信されると、Log Analytics WorkspaceとPanoramaでCloud NGFWログを表示できます。詳しくは、[View the Logs (ログの表示)]と[View Cloud NGFW Logs in Panorama (Cloud NGFWログのPanoramaでの表示)]を参照してください。

ログ分析ワークスペースでトラフィックログを無効にし、Panoramaで有効にする

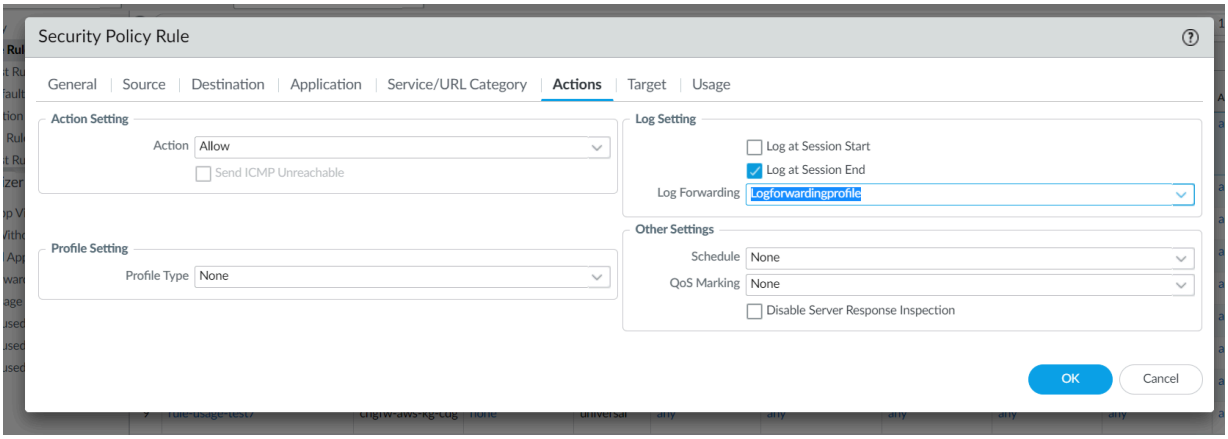
ログ分析ワークスペースでログを無効にし、Panoramaでログを有効にする手順は次のとおりです。

STEP 1 | Cloud NGFW for Azureコンソールのログ設定を無効にする。

STEP 2 | 「Panorama」で、**[Policies (ポリシー)]**に移動します。

STEP 3 | クラウドデバイスグループのポリシールールを選択します。

STEP 4 | **[Actions (アクション)]**タブを開き、**[Log Forwarding (ログ転送)]**プロファイルを選択します。



STEP 5 | **OK** をクリックします。

STEP 6 | Panoramaコンソールで変更を**Commit and Push (コミットしてプッシュ)**します。

トラフィックが送信されると、Log Analytics WorkspaceとPanoramaでCloud NGFWログを表示できます。詳しくは、[View the Logs (ログの表示)]と[View Cloud NGFW Logs in Panorama (Cloud NGFWログのPanoramaでの表示)]を参照してください。

ログ分析ワークスペースとPanoramaでトラフィックログを無効にする

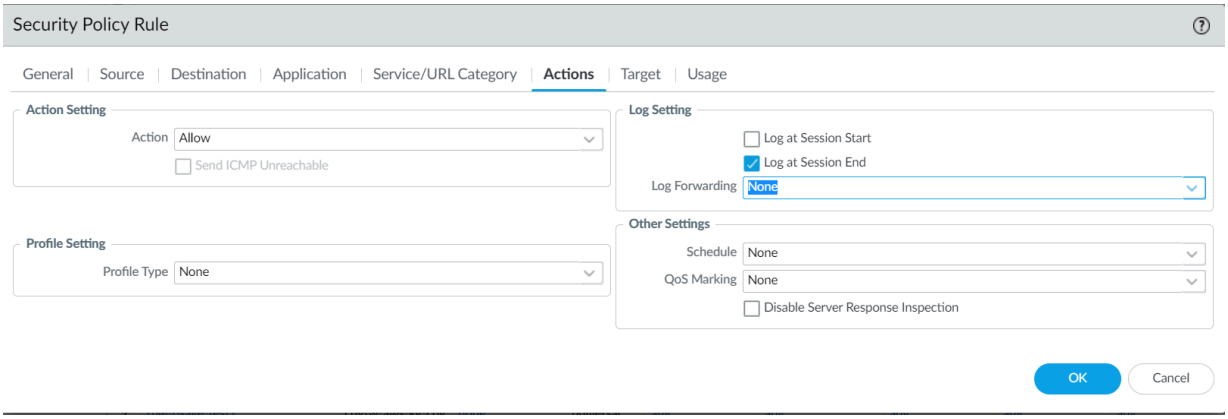
ログ分析ワークスペースとPanoramaでログを無効にする手順は次のとおりです。

STEP 1 | Cloud NGFW for Azureコンソールのログ設定を無効にする。

STEP 2 | 「Panorama」で、**[Policies (ポリシー)]**に移動します。

STEP 3 | クラウドデバイスグループのポリシールールを選択します。

STEP 4 | **[Actions (アクション)]**タブに移動し、ログ転送プロファイルで**[None (なし)]**を選択します。



STEP 5 | **OK** をクリックします。

STEP 6 | Panoramaコンソールで変更を**Commit and Push (コミットしてプッシュ)**します。

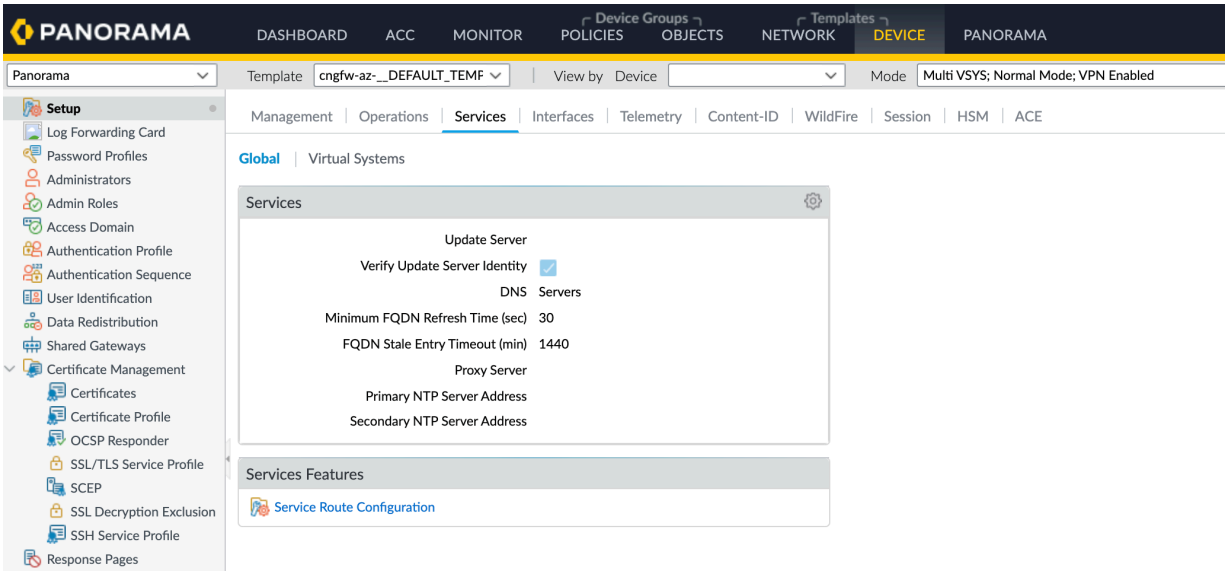
Cloud NGFWログは、ログ分析ワークスペースとPanoramaに反映されなくなります。

ログ分析ワークスペースでトラフィックログを無効にし、PanoramaとSyslogで有効にする

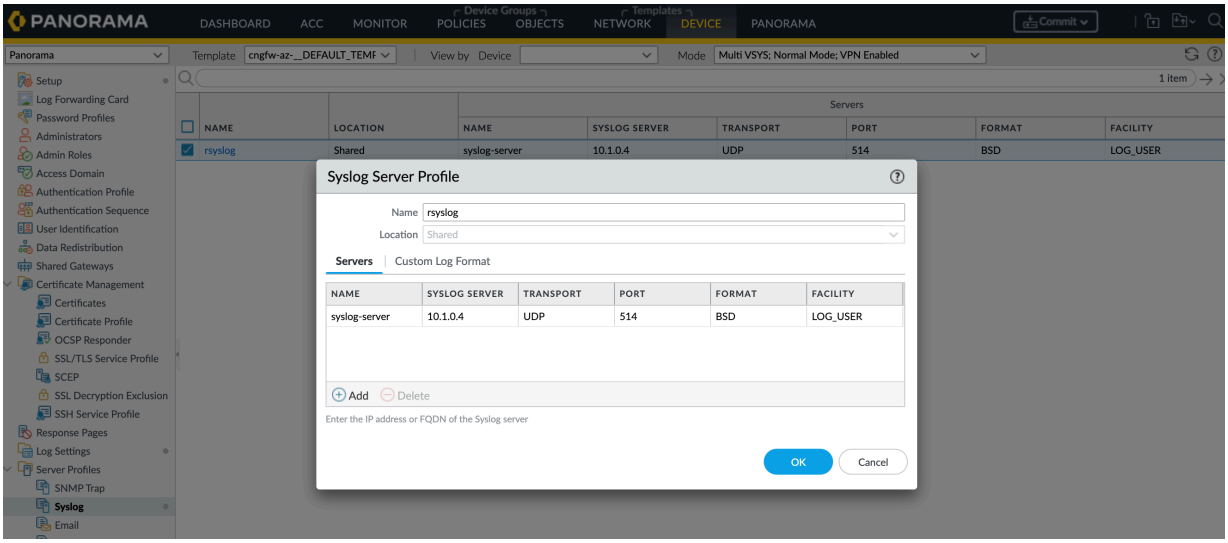
Log Analyticsワークスペースでログを無効にし、PanoramaとSyslogサーバーでログを有効にする手順は次のとおりです。

STEP 1 | Cloud NGFW for Azureコンソールのログ設定を無効にする。

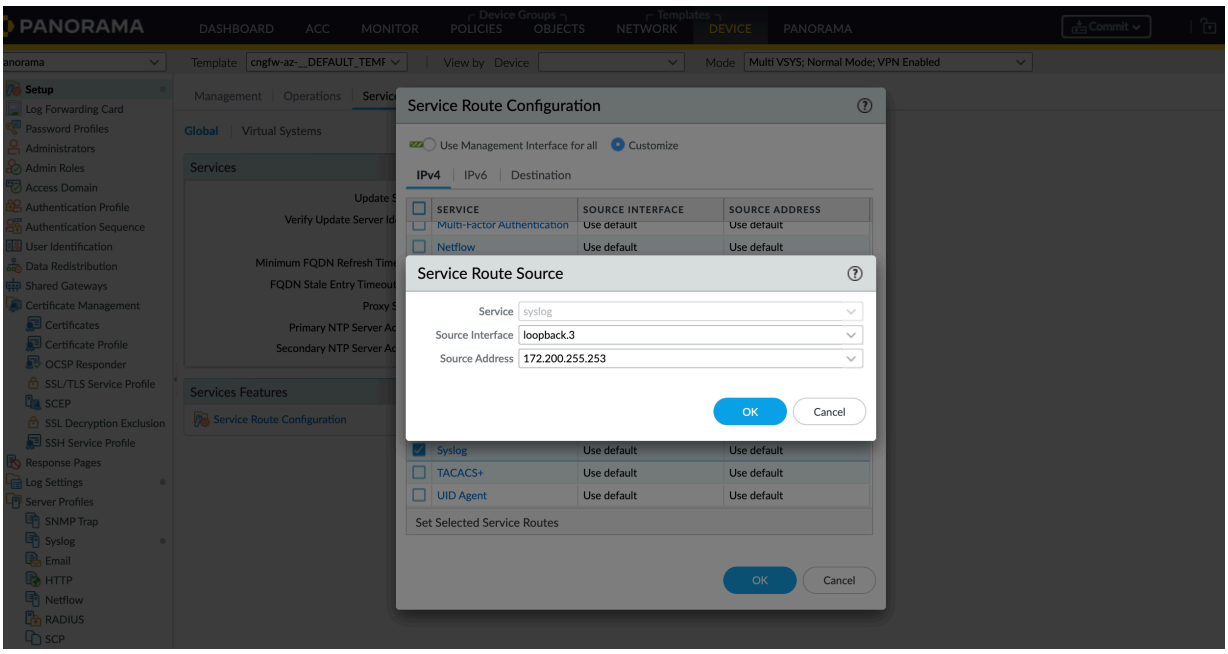
STEP 2 | Panoramaの**[Device (デバイス)]**タブを開き、azure NGFWAASのデフォルトテンプレート（`cngfw-az - _ _DEFAULT_TEMPLATE _ _`）を選択します。



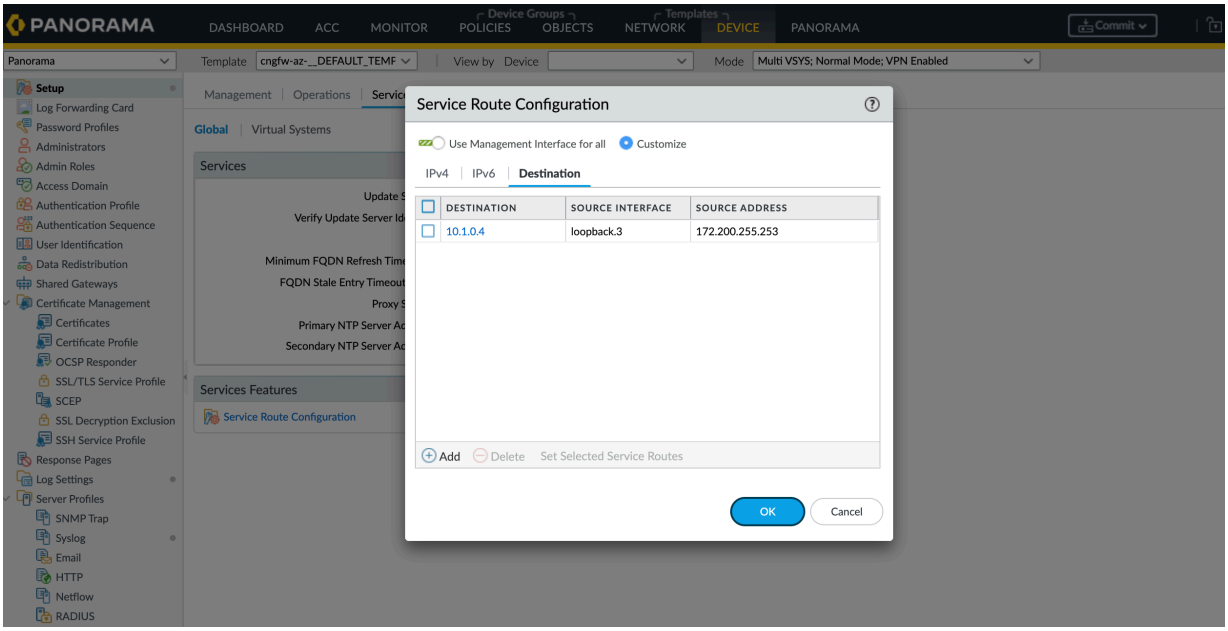
STEP 3 | **Server profiles**-> **Syslog**と進み、syslogサーバのプライベートIPを追加します。



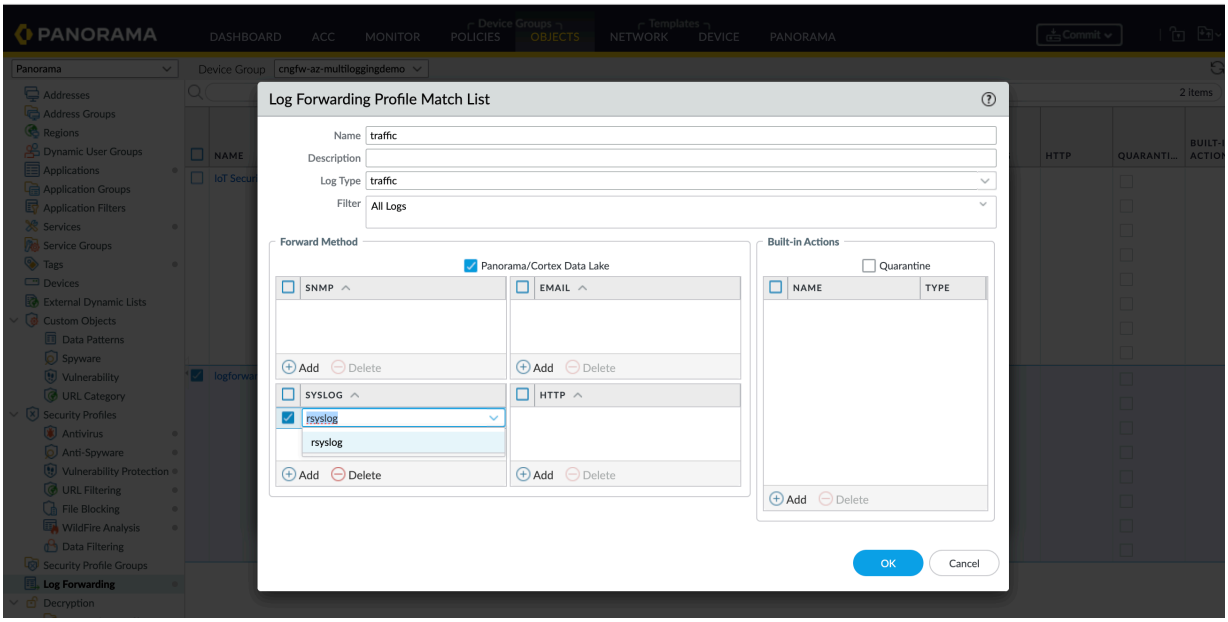
STEP 4 | [Device (デバイス)]タブに移動し、**[Setup (セットアップ)]**をクリックしてから、**[Service Route Configuration (サービスルート構成)]**をクリックします。



- サービスベースルーティングの設定では、**IPv4**と**Syslog**サービスを選択します。送信元インターフェイスとして**loopback.3**を選択することを確認する必要があります。
- 宛先ベースルーティングの設定では、宛先を選択してsyslogサーバのプライベートIPを追加し、送信元インターフェイスとして**loopback.3**を選択します。



STEP 5 | ログ転送プロファイルで、syslogサーバを追加します。



STEP 6 | Panoramaで**[Policies (**ポリシー**)**］タブに移動し、クラウドデバイスグループのポリシールールを選択します。

STEP 7 | **[Actions (**アクション**)]**タブに移動し、**[Log Forwarding profile (**ログ転送プロファイル**)]**を選択します。

STEP 8 | **OK** をクリックします。

STEP 9 | Panoramaコンソールで変更をコミットしてプッシュします。

syslog サーバでトラフィックを受信するには、*Syslog Server VNET* と *Firewall Hub VNET* の間で *VNET* ピアリングを完了する必要があります。トラフィック送信後、*Panorama*と*Syslog*サーバーで*Cloud NGFW*ログを表示できます。

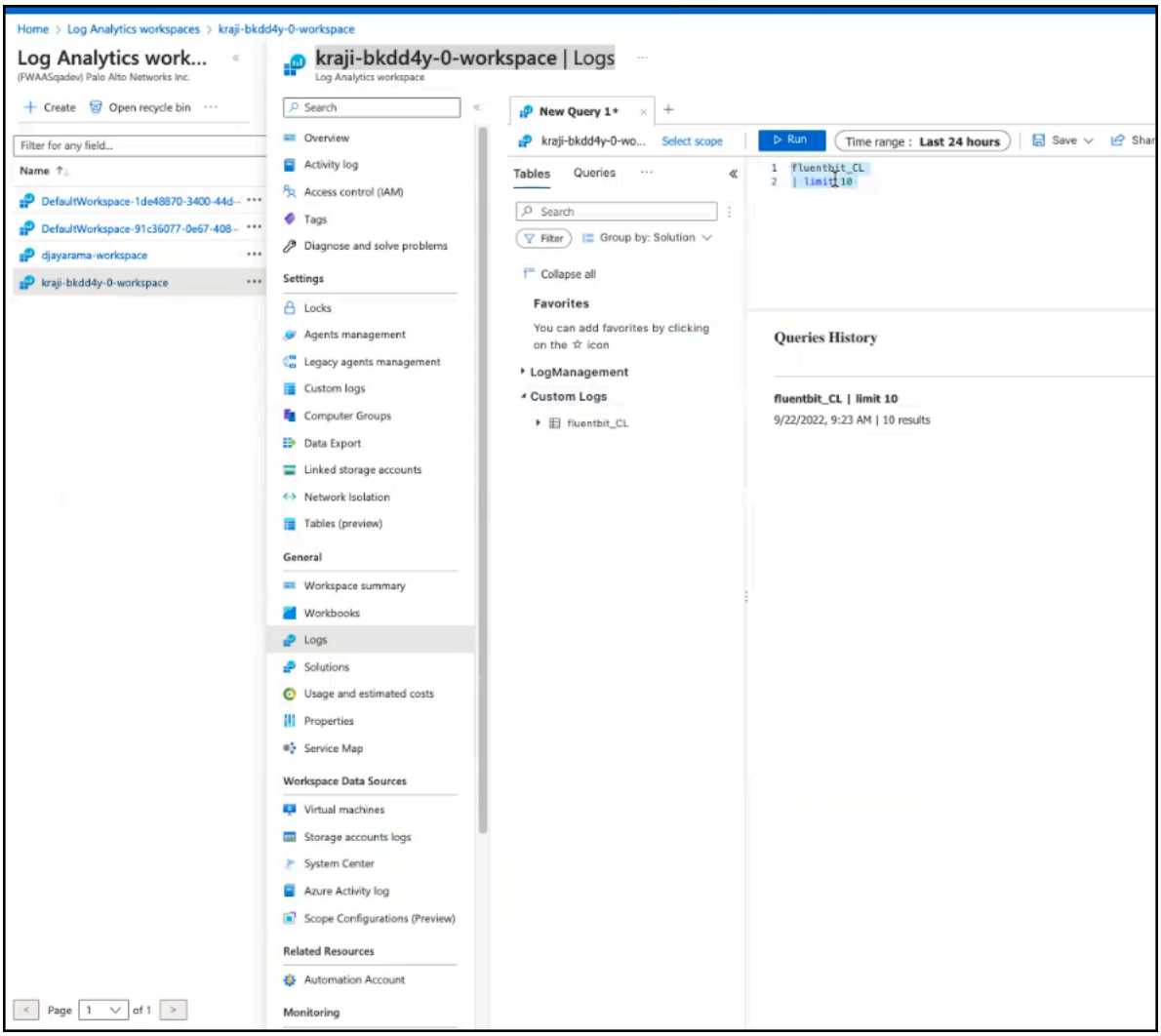
ログを表示する

Log Analytics Workspace (ログ分析ワークスペース)を作成したら、ファイアウォールの下のログ設定を更新し、トラフィックの送信を開始します。トラフィックが送信されると、以下の手順に従ってログを表示できます。

STEP 1 | ログを表示する必要がある **[Log Analytics Workspace (ログ分析ワークスペース)]** をクリックします。

STEP 2 | **[Logs (ログイン)]**をクリックします。

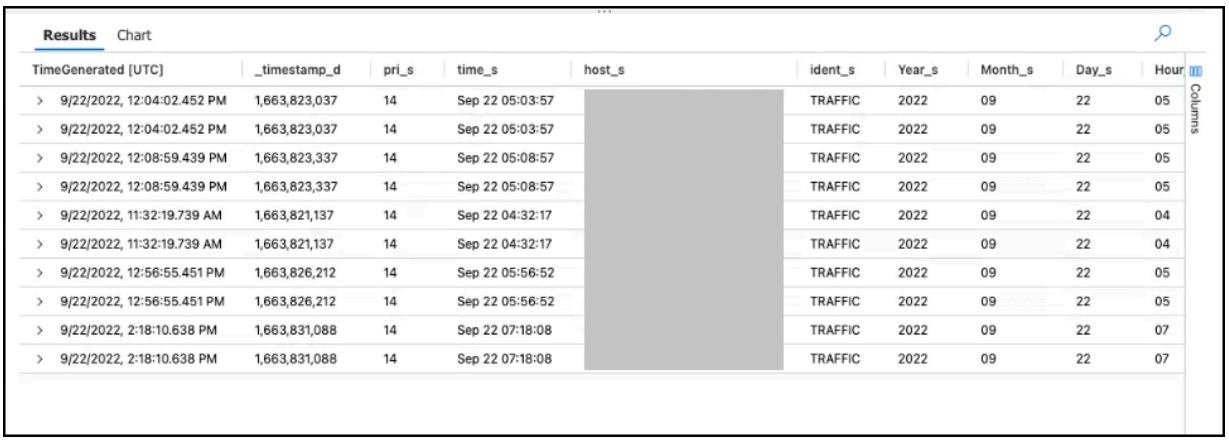
STEP 3 | クエリ ウィンドウで **[Custom Logs (カスタム ログ)]** をクリックし、作成したクエリ を**Run (実行)**します 。



ログの数、時間範囲などのパラメータを使用してカスタマイズされたクエリを作成できます。たとえば、単純なクエリ

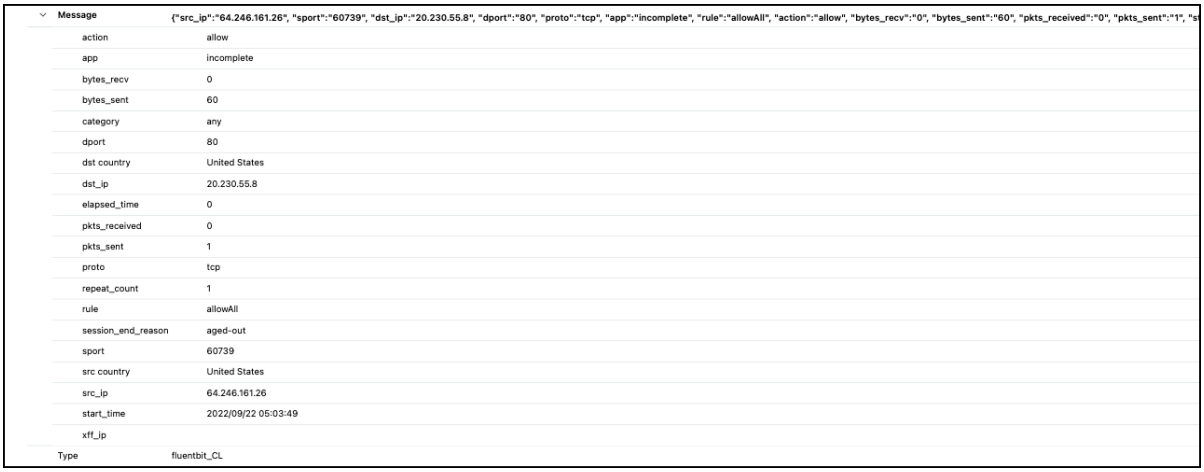
```
fluentbit_CL | limit 10
```

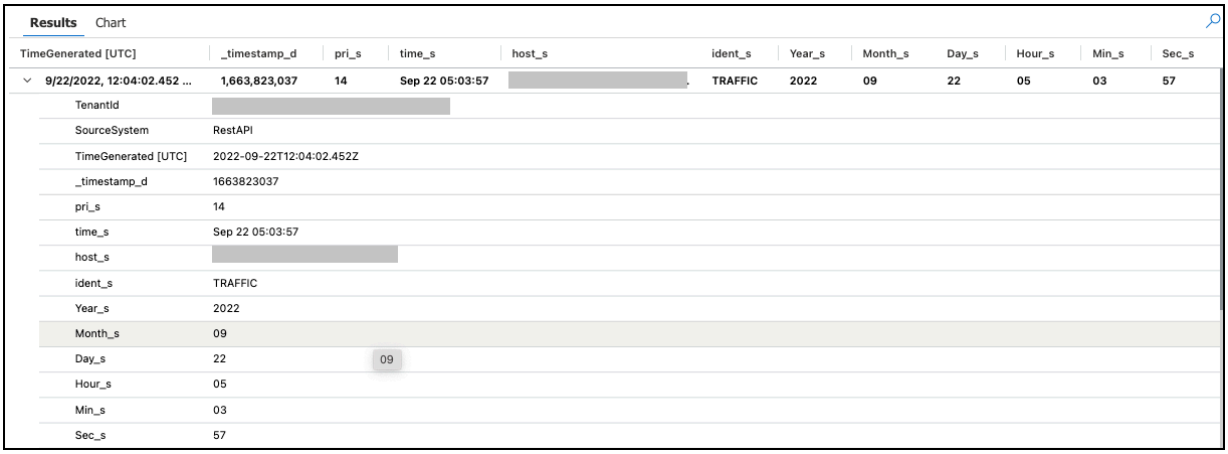
があります



TimeGenerated [UTC]	_timestamp_d	pri_s	time_s	host_s	ident_s	Year_s	Month_s	Day_s	Hour
9/22/2022, 12:04:02.452 PM	1,663,823,037	14	Sep 22 05:03:57		TRAFFIC	2022	09	22	05
9/22/2022, 12:04:02.452 PM	1,663,823,037	14	Sep 22 05:03:57		TRAFFIC	2022	09	22	05
9/22/2022, 12:08:59.439 PM	1,663,823,337	14	Sep 22 05:08:57		TRAFFIC	2022	09	22	05
9/22/2022, 12:08:59.439 PM	1,663,823,337	14	Sep 22 05:08:57		TRAFFIC	2022	09	22	05
9/22/2022, 11:32:19.739 AM	1,663,821,137	14	Sep 22 04:32:17		TRAFFIC	2022	09	22	04
9/22/2022, 11:32:19.739 AM	1,663,821,137	14	Sep 22 04:32:17		TRAFFIC	2022	09	22	04
9/22/2022, 12:56:55.451 PM	1,663,826,212	14	Sep 22 05:56:52		TRAFFIC	2022	09	22	05
9/22/2022, 12:56:55.451 PM	1,663,826,212	14	Sep 22 05:56:52		TRAFFIC	2022	09	22	05
9/22/2022, 2:18:10.638 PM	1,663,831,088	14	Sep 22 07:18:08		TRAFFIC	2022	09	22	07
9/22/2022, 2:18:10.638 PM	1,663,831,088	14	Sep 22 07:18:08		TRAFFIC	2022	09	22	07

STEP 4 | 詳細なログを表示したいクエリ結果項目をクリックします。





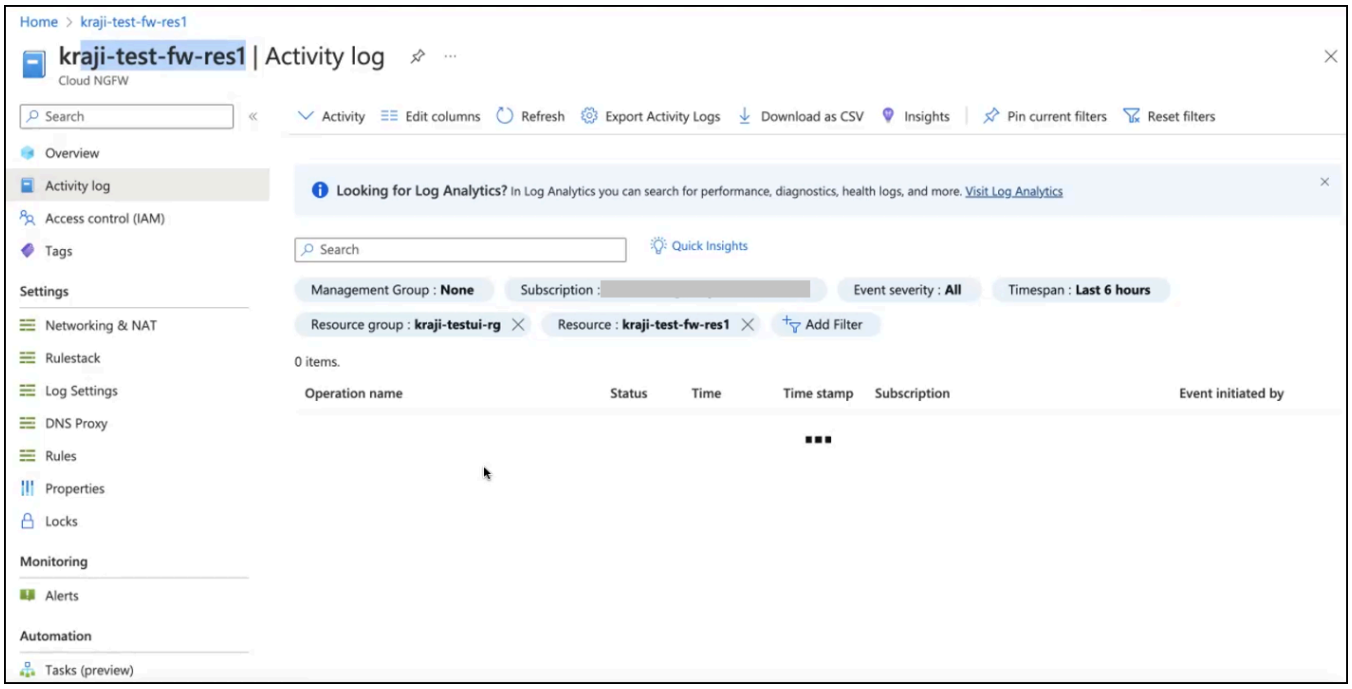
ファイアウォールリソースの監査ログの表示

リソースグループに導入されているファイアウォールリソースの監査ログを表示する方法：

STEP 1 | ホームページから、ログを表示するCloud NGFWファイアウォールリソースに移動します。

STEP 2 | 左ペインの**[Activity Log (アクティビティログ)]**をクリックし、ログを表示する目的の**[Timespan (タイムスパン)]**を選択して、**[Apply (適用)]**をクリックします。選択したタイムスパンのログの一覧が表示されます。

STEP 3 | 目的のログをクリックすると、ログの**[Summary (サマリー)]**と**JSON**が表示されます。



リソースグループの監査ログを表示する

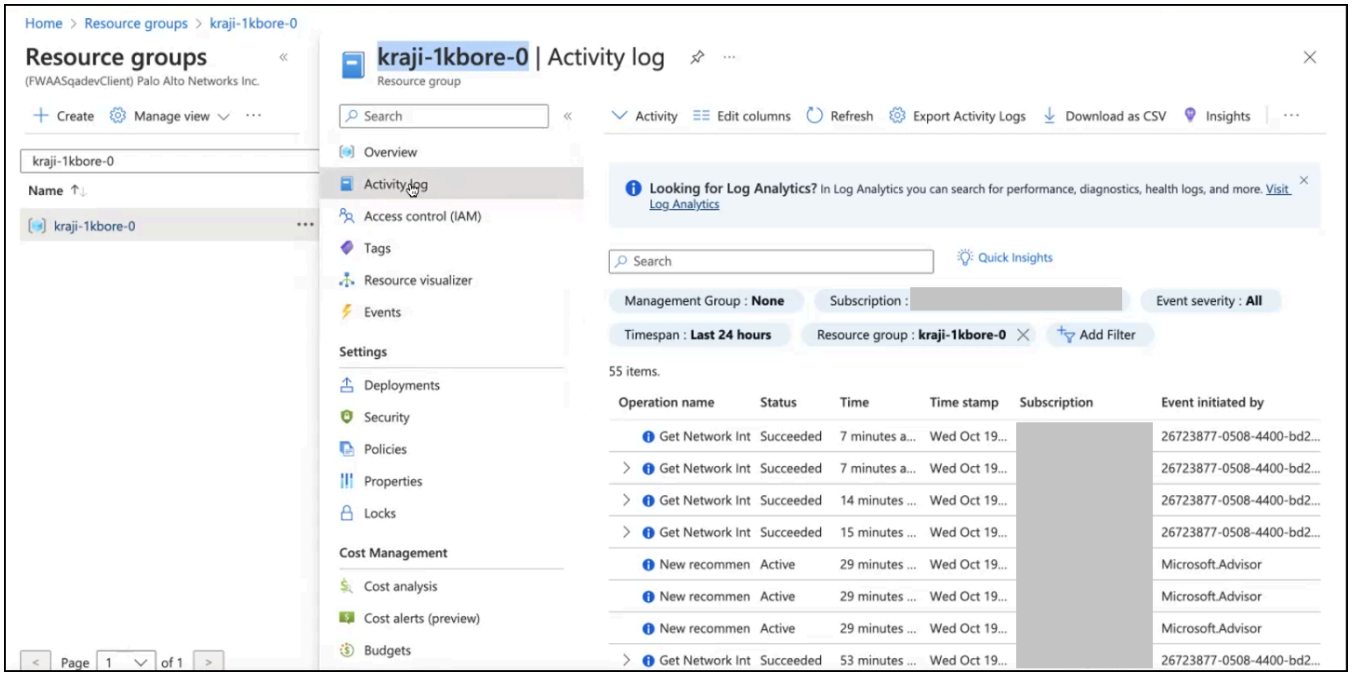
リソースグループの監査ログを表示する方法:

STEP 1 | ホームページから [**Resource groups (**リソースグループ**)**] に移動します。

STEP 2 | アクティビティログを収集したいリソースグループをクリックします。

STEP 3 | 左ペインの**[Activity Log (**アクティビティログ**)]**をクリックし、ログを表示する目的の**[Timespan (**タイムスパン**)]**を選択して、**[Apply (**適用**)]**をクリックします。選択したタイムスパンのログの一覧が表示されます。

STEP 4 | 目的のログをクリックすると、ログの**[Summary (**サマリー**)]**と**JSON**が表示されます。



新着情報

Cloud NGFW for Azure の新機能は次のとおりです。

2024年6月の最新情報

新規	の意味
追加の Azure リージョンのサポート	Cloud NGFW for Azure が次の Azure リージョンで利用できるようになりました。 • 西日本(大阪) • スウェーデン中央部(ガブレ) • イタリア北部(ミラノ) • 南アフリカ北部(ヨハネスブルグ) • イスラエル中央部 • 米国中西部 (ワイオミング州) • アラブ首長国連邦北部(ドバイ) サポートされるリージョンの完全なリストについては、Cloud NGFW for Azure Supported Regions and Zones (Cloud NGFW for Azure がサポートするリージョンとゾーン)を参照してください。

2024年5月の最新情報

新規	の意味
XFF ヘッダー値を使用してセキュリティ ポリシーを適用する	Cloud NGFW for AzureX-Forwarded-For (XFF) ヘッダーに IP アドレスを使用して、Panorama で作成したセキュリティ ポリシーを適用できるようになりました。
追加の Azure リージョンのサポート	Cloud NGFW for Azure が次の Azure リージョンで利用できるようになりました。 • カナダ東部 サポートされるリージョンの完全なリストについては、Cloud NGFW for Azure Supported Regions and Zones (Cloud NGFW for Azure がサポートするリージョンとゾーン)を参照してください。
クレジット使用量と使用状況の可視性	長期契約の Cloud NGFW 使用量にクレジットを使用できるようになりました。このクレジットは、テナント レベルで Azure クラウド環境全体のファイアウォール リソースに割り当てることができます。詳細については、Credit Usage Visibility (クレジット使用量の可視性)を参照してください。

2024年3月の最新情報

新規	の意味
追加の Azure リージョンのサポート	Cloud NGFW for Azure が次の Azure リージョンで利用できるようになりました。 • ノルウェー東部 • ドイツ 西中部 • 中央インド • スイス北部 サポートされるリージョンの完全なリストについては、Cloud NGFW for Azure Supported Regions and Zones (Cloud NGFW for Azure がサポートするリージョンとゾーン)を参照してください。
Azureネットワーク料金	Cloud NGFW for Azure では、仮想ネットワーク ピアリング料金が Azure ネットワーク料金ディメンションで課金されます。使用量の詳細は Azure Marketplace で共有されます。使用状況は、インバウンドトラフィック (インターネットから VNET へ)、アウトバウンドトラフィック (VNET からインターネットへ)、および東西トラフィック (VNET 間) で追跡されます。料金の詳細については、以下を参照してください。 Cloud NGFW for Azureの価格.
インバウンド復号化のサポート	Azure の Cloud NGFW は、 SSL インバウンド復号化 クライアントからターゲットのネットワーク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します。詳細については、以下を参照してください。 Azure の Cloud NGFW でのインバウンド復号化の設定.

2024年2月の最新情報

新規	の意味
複数のログ宛先	Panorama で管理されている Cloud NGFW for Azure リソースから、Azure Log Analytics Workspace、Syslog Servers、Panorama にログを送信できるようになりました。見る Cloud NGFW for Azure上の複数のログ宛先 詳細情報。
追加の Azure リージョンのサポート	Cloud NGFW for Azure が次の Azure リージョンで利用できるようになりました。 • フランス中部 • 米国中南部 サポートされるリージョンの完全なリストについてはCloud NGFW for Azure Supported Regions and Zones (Cloud NGFW for Azureがサポートするリージョンとゾーン)を参照してください。

2024年1月の新機能

新規	の意味
100Gbpsに対応	このリリースにより、Cloud NGFW for Azure は、vNET と vWAN の両方のデプロイで最大 100Gbps まで自動的にスケールアップできます。詳細については、「Deploy the Cloud NGFW in a vNET (vNET でのクラウド NGFW のデプロイ)」および「Deploy the Cloud NGFW in a vWAN (vWAN でのクラウド NGFW のデプロイ)」を参照してください。

2023年12月の新機能

新規	の意味
追加の Azure リージョンのサポート	Cloud NGFW for Azure が次の Azure リージョンで利用できるようになりました。 • 米国中北部 • 東南アジア サポートされるリージョンの完全なリストについては、「Cloud NGFW for Azure Supported Regions and Zones (Cloud NGFW for Azureがサポートするリージョンとゾーン)」を参照してください。
プライベートソース NAT のサポート	このリリースでは、プライベート ソース NAT のサポートが追加されています。このサポートにより、ネットワークアドレス変換 (NAT) を実行するためのプライベート NAT ゲートウェイを作成できます。詳細については、「Edit an Existing Firewall to Enable Private Source NAT (既存のファイアウォールを編集してプライベートソース NAT を有効にする)」を参照してください。

2023年11月の新機能

新規	の意味
追加の Azure リージョンのサポート	Cloud NGFW for Azure が次の Azure リージョンで利用できるようになりました。 • 東日本 • ブラジル南部 サポートされるリージョンの完全なリストについては、Cloud NGFW for Azure Supported Regions and Zones (Cloud NGFW for Azureがサポートするリージョンとゾーン)を参照してください。
ルールスタックの機能拡張	このリリースでは、ルールスタックでの暗黙的なルール削除がサポートされています。この機能強化により、次のことが可能になります。 • ルールやオブジェクトを削除せずに、空でない関連付けられていないルールスタックを削除できます。 • リソース グループは、空または空でない関連付けられていないルールスタックを保持したまま削除できます。 • Azure CLI、CDK、PowerShell、Terraform を使用して、空でない関連付けられていないルールスタックを削除できます。 この削除機能は、コミットされていないルールスタックと空でない実行中のルールスタックに適用されます。
DNSセキュリティサービスのサポート	Cloud NGFW for Azureは、Palo Alto Networks DNS Securityサービスのサポートを追加します。このサービスを使用すると、ネットワーク リソースがクエリを実行するドメインを監視および制御することで、vNET および vWAN トラフィックを高度な DNS ベースの脅威から保護できます。詳細については、「Enable DNS Security on Cloud NGFW for Azure (Azure のCloud NGFW で DNS セキュリティを有効にする) 」を参照してください。
非RFC 1918のサポート	このリリースでは、vNET および vWAN デプロイメントの RFC 1918 で指定されているアドレス以外の追加のプライベート IP 範囲のサポートが追加されています。このサポートにより、トラフィックをインターネットにルーティングせずに、パブリック IP アドレス ブロック (40.0.0.0/24 など) をプライベート ネットワークとして使用できます。vNET デプロイメントでのこの機能の詳細については、「**Networking Section (**ネットワーキングセクション**)**」 (ステップ5)

新規	の意味
	「dditional Prefixes to Private Traffic Range (プライベートトラフィック範囲への追加のプレフィックス)」を参照してください。。

2023年10月の新機能

<table>
<tr><th>新規</th><th>の意味</th></tr>
<tr><td>追加の Azure リージョンのサポート</td><td>Cloud NGFW for Azure が次の Azure リージョンで利用できるようになりました。
米国西部 2
北ヨーロッパ
サポートされるリージョンの完全なリストについては、「Cloud NGFW for Azure Supported Regions and Zones (Cloud NGFW for Azureがサポートするリージョンとゾーン)」を参照してください。</td></tr>
<tr><td>プログラムによるアクセス</td><td>プログラムによるアクセスにより、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のツールを通じて Cloud NGFW リソースに対するアクションを呼び出すことができます。次の表はサポートされているツールに関する情報を示したものです。<table><tr><td>テラフォーム</td><td>Azure プロバイダーを使用して、Azure Resource Manager API を使用してインフラストラクチャを構成します。</td></tr><tr><td>PowerShell</td><td>Microsoft Azure PowerShell コマンドレットを使用して、Azure のCloud NGFW を設定します。</td></tr><tr><td>CLI</td><td>これらのコマンドを使用して、Cloud NGFW for Azure リソースを管理します。</td></tr><tr><td>SDK</td><td>Python 用のSDK パッケージがサポートされています。</td></tr></table></td></tr>
</table>

2023年9月の新機能

新規	の意味
SSOログインフローをサポートポータルアカウントと統合する	組織のSSOログインフローを、Cloud NGFWのAzureサブスクリプションのPalo Alto Networks カスタマーサポートポータルアカウントと統合します。詳細については、Integrate Single Sign-on (シングルサインオンの統合)を参照してください。
パブリックドメインのメールアドレスのサポート	このリリースでは、次のパブリックドメインのメールアドレスのサポートが追加されています。 カスタマーサポートポータル アカウント。以前は、Cloud NGFW アセットと関連するサポート ケースを管理するユーザーは、アカウントにログインするために企業のメール アドレスが必要でした。この追加機能により、次のようになります。 • パブリックドメインのユーザーは、自分がメンバーであるアカウントのアセットとサポートケースにアクセスします。 • RBAC アクセス制御は、パブリック ドメインのメールを持つユーザーに割り当てて適用できます。 • あるアカウントで公開ドメインのメールアドレスを持つユーザーは、別のアカウントのアセットやサポートケースにアクセスできません。この問題を解決するには、パブリック ドメインのメール アドレスを持つユーザーを、アクセスする必要があるアカウントに追加します。 • パブリックドメインのメールアドレスを持つユーザーには、スーパーユーザーやドメイン管理者など、任意のロールが割り当てられます。 • アカウントには、パブリックドメインのメールアドレスを持つユーザーが1人以上含めることができます。パブリックドメインのメールアドレスを持つユーザーによってアカウントが作成された場合、そのアカウントはパブリックであるとされます。 アカウントに、会社のメールアドレスと公開のメールアドレスを持つユーザーを混在させることはできません。 次のパブリックドメインのメールアドレスがサポートされています。 gmail.com　yahoo.*　hotmail.*

新規	の意味		
	live.*	outlook.com	aol.com
	gms.* (gmx.de, gmx.net, gmx.us)	icloud.com	msn.com
	comcast.net**	att.net	

2023年8月の新機能

新規	の意味
一般提供	Cloud NGFW for Azure が一般提供になりました。このリリースには、多数の修正、追加の リージョン、および従量課金制 (PAYG) サブスクリプションモデルの強化が含まれています。

2023年6月の最新情報

新規	の意味
ヘルスモニタリング	Cloud NGFW ファイアウォールの全体的なヘルスステータス、接続ステータス、診断情報を表示します。この情報を使用して、ファイアウォールの状態が正常でない原因を特定します。詳細については、「Monitor Cloud NGFW Health (Cloud NGFWのヘルスの監視)」を参照してください。

2023年5月の最新情報

新規	の意味
Cloud NGFW for Azure の初期リリース	Cloud NGFW for Azure の初期リリースには、次の機能が含まれています。 • vNET およびvWAN -ベースのファイアウォールデプロイメント • vWAN 用のシングルハブとマルチハブ。詳細については、「Configure Palo Alto Networks Cloud NGFW in Virtual WAN (仮想 WAN での Palo Alto Networks Cloud NGFW の設定)」を参照してください。 • インバウンド、アウトバウンド、および東西トラフィックの使用例 • ポリシー管理 ルールスタック、プレフィックスオブジェクト、FQDN オブジェクト、および証明書オブジェクトの場合 • ロギングは以下をサポートしています。 • 自動スケールのサポート • アウトバウンド復号化 • コンテンツとアンチウイルスのアップグレード • ファイアウォールリソースのローリングアップグレード • サポート提供元 カスタマーサポートポータル • 組み込みロールのサポート (LocalNGFirewall と LocalRuleStacksAdministrator)

Cloud NGFW for Azure の既知の問題

Palo Alto NetworksのAzure Cloud NGFWでは、以下の既知の問題が確認されています。

ID	の意味
FWAAS-10519	マルチロギング宛先を有効にすると、Panoramaとsyslogサーバにログは表示されますが、ログ分析ワークスペースにはログは表示されません。 回避策:ログ分析ワークスペースとともにsyslogを使用する場合は、サービスルートをサービスベースルートではなくデスティネーションベースに変更します。 宛先ベースルーティングの設定では、宛先を選択し、syslogサーバのプライベートIPを追加してから、送信元インターフェイスとして**loopback.3**を選択します。
FWAAS-9688	Panoramaのデフォルトルールは、Cloud NGFWリソースによって上書きされます。**[Profile (**プロファイル**)]**や**[Action (**アクション**)]**などのパラメータは保持されません。たとえば、アクションを**[Allow (**許可**)]**に設定すると、**[Deny (**拒否**)]**に戻ります。ロギングプロファイルを設定すると、**[None (**なし**)]**に戻ります。
FWAAS-7531	自己署名証明書は、リソース名がないにもかかわらず、誤ってルールスタックに関連付けられる可能性があります。
FWAAS-7542	Panoramaは、新しく作成されたCloud NGFW for Azureリソースにコンテンツやウイルス対策のアップデートを自動的にプッシュするとは限りません。
FWAAS-7547	（デバイステンプレートによって提供される）QoSプロファイルは、Panorama仮想アプライアンスに表示されるときに削除されません。
FWAAS-7956	ルールスタックがファイアウォールと同じ名前を共有している場合、誤った情報が表示されます。
FWAAS-8642	ローカルルールを大量に作成すると、HTTPエラー（503サーバエラー：サービス利用不可

ID	の意味
FWAAS-9086	Azureポータルのデプロイメントステータス情報は、完全な情報が表示されずに切り捨てられます。
FWAAS-10195	DNSプロキシを有効にせずにRFC 1918以外のアドレスを有効にすると、ファイアウォールの作成に失敗します。
PAN-217954	Cloud NGFW for Azureリソースが初めてPanoramaに接続すると、リソースのCloud Device Groupに関連付けられたテンプレートスタックが同期しなくなります。
PAN-217459	Panorama HAペアによって管理されるCloud NGFWリソースは、セカンダリPanorama上のシリアル番号（デバイス名ではなく）によってクラウドデバイスグループに表示されることがあります。ただし、プライマリPanoramaでは、Cloud NGFWリソースはデバイス名でリストされます。
PAN-217966	親デバイスグループにダイナミックアドレスグループが設定されていない場合、設定されたダイナミックアドレスグループのタグとIPアドレスは子クラウドデバイスグループには表示されません。

Cloud NGFW for Azure で解決された問題

Cloud NGFW for Azure のこのリリースでは、次の問題が修正されました。

ID	詳説
FWAAS-3919	ローカルルールスタックで無効なルール名が生成され、コミットが失敗する可能性があることが確認されています。
FWAAS-4546	ルールヒットカウンターのDBエントリがルールを削除しても削除されないため、同じ名前でルールを再度作成すると古い値になります。
FWAAS-4767	DNSプロキシは、ファイアウォールの更新呼び出しの後、ファイアウォール上で同時に更新されません。
FWAAS-4805	ファイアウォールのホスト名が誤ってログに表示されます。
FWAAS-7430	作成が完了する前に新しいCloud NGFWリソースを削除しようとすると、削除は失敗します。
FWAAS-7542	Panoramaは、新しく作成されたCloud NGFW for Azureリソースに、コンテンツやウイルス対策の更新を常に自動的にプッシュするわけではありません。
FWAAS-8696	Panorama仮想アプライアンスへのログ転送が完了するまでに時間がかかる場合があります。
FWAAS-9041	CNGFW デバイスに使用されるPanoramaテンプレートで、デバイス サーバ プロファイル（LDAP、Syslog など）が誤って無効と表示される。
FWAAS-9050	場合によっては、VMシリーズファイアウォールのライセンスがPanorama仮想アプライアンスから削除されることがあります。
FWAAS-9055	クラウドデバイスグループ名が変更されると、CNGFWは異常な状態になり、Panoramaへの接続が失われます。
PAN-217460	Panorama HAペアによって管理されているクラウド NGFW リソースは、セカンダリPanoramaで切断されているように見えることがあります。ただ

ID	詳説
	し、プライマリPanoramaでは、クラウド NGFW リソースは接続済みと表示されます。

