paloalto
TECHDOCS

Strata Cloud Manager AIOps

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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2023-2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

February 3, 2025

Table of Contents

©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

AIOps for NGFW

PAN-OSデバイステレメトリを通じて収集されたデータを利用して、 AIOps for NGFW 次世代ファイアウォール展開の正常性とセキュリティの概要を示し、改善点を特定し、セキュリティギャップを埋めるのに役立ちます。 AIOps for NGFWは、デバイスの動作状態に関連するデバイス テレメトリー メトリクスから正常性に関する情報を導き出します。セキュリティ情報については、 AIOps for NGFWはPalo Alto Networksのベストプラクティスに照らしてデバイスの構成を分析し、セキュリティ体制の潜在的なギャップを指摘します。

AIOps for NGFW Premium & Strata Cloud Manager

Strata Cloud Manager は、*AIOps for NGFW Premium*ライセンスを使用する*NGFW*のみに統合された管理と運用を提供します。

- ***NGFW(PAN-OS***および***Panorama***管理*)* → *AIOps for NGFW Premium*ライセンスを持つ*PAN-OS*および*Panorama Managed NGFW*の場合は、*Strata Cloud Manager*を使用して、デプロイメントの正常性とセキュリティ体制を監視します。
- ***NGFW(***クラウド管理*)* → *AIOps for NGFW*ライセンスを使用すると、*Strata Cloud Manager*をNGFW のクラウド管理にも使用できます。

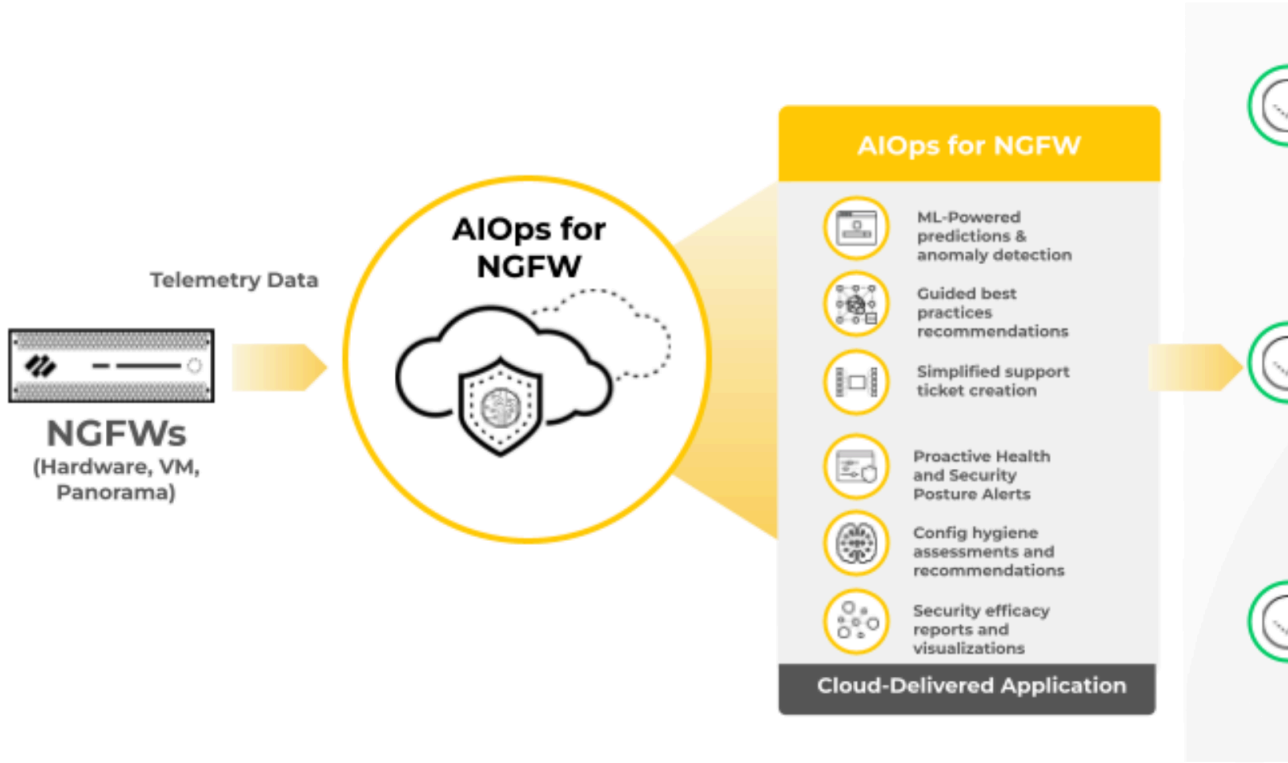
*2024*年*10*月以降、*Strata Cloud Manager*には*2*つのライセンス階層があります。*Strata Cloud Manager Essentials* および *Strata Cloud Manager Pro*。この統一された構造により、*NGFW*の*AIOps*、*Autonomous Digital Experience Management(ADEM)*、クラウド管理機能、*Strata Logging Service*などのネットワークセキュリティ製品の導入が効率化されます。Strata Cloud Manager ライセンスを確認する。

NGFW無料のための***AIOps*** アプリまたは *Strata Cloud Manager* を ***NGFW***プレミアムの***AIOps*** ライセンスをすでに使用している場合、既存のライセンスは影響を受けず、引き続き修正、延長、または更新できます。

始めましょう：

- NGFWの無料およびプレミアムAIOps
- NGFWのAIOpsのアクティブ化
- NGFWのAIOpsへのデバイス テレメトリの送信を開始する
- 新機能
- オンデマンド BPA レポート

- NGFWインシデントとアラートのためのAIOps



 ©2025 Palo Alto Networks, Inc.

AIOps for NGFWのリージョン

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	次のいずれか: ☐ AIOps for NGFW Free または Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium または Strata Cloud Manager Pro

AIOps for NGFW をアクティベートするときに選択するリージョンによって、AIOps がデータを処理する物理的な場所が決まります。

AIOps for NGFWは、Strata Logging Service（SLS）インフラストラクチャがサポートされているすべての地域で提供されるわけではありません。AIOps for NGFWの導入は、テレメトリデータの送信先に合わせて、まもなく追加リージョンに拡大される予定です。現在、AIOpsアプリケーションがサポートされていない地域にテレメトリデータを送信した場合、データは米州地域のAIOps for NGFWインスタンスによって処理されます。

AIOps for NGFWをアクティブにすると、これらの制限が自動的に適用されます。たとえば、AIOps for NGFWのインスタンスをアクティブ化するリージョンとしてドイツを選択した場合、ドイツを拠点とするSLSテナントのみをそのインスタンスに接続できます。

*AIOps for NGFW*をサポートするのと同じリージョンが、*Strata Cloud Manager*で*NGFW*をサポートしています。

次の表を参照して、さまざまなテレメトリ先リージョンのAIOpsデータ処理を理解してください。

Strata Logging Serviceリージョン	**AIOps for NGFW**インスタンスがデータを処理するためにサポートされるリージョン
ドイツ	ドイツ
英国	英国
オランダ - ヨーロッパ	オランダ - ヨーロッパ
イタリア - ヨーロッパ	イタリア - ヨーロッパ
スペイン - ヨーロッパ	スペイン - ヨーロッパ
スイス - ヨーロッパ	スイス - ヨーロッパ

©2025 Palo Alto Networks, Inc.

Strata Logging Serviceリージョン	AIOps for NGFWインスタンスがデータを処理するためにサポートされるリージョン
フランス - ヨーロッパ	フランス - ヨーロッパ
ポーランド - ヨーロッパ	ポーランド - ヨーロッパ
韓国	韓国
インドネシア	インドネシア
イスラエル	イスラエル
台湾	台湾
カタール	カタール
シンガポール	シンガポール
オーストラリア	オーストラリア
インド	インド
日本	日本
カナダ	カナダ
残りのSLSリージョン	米国 - アメリカ

©2025 Palo Alto Networks, Inc.

無料機能とプレミアム機能

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	次のいずれか： ❑ AIOps for NGFW Free または Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium または Strata Cloud Manager Pro

AIOps for NGFWには、無料とプレミアムの2つのライセンス階層があります。

無料のAIOps for NGFW機能により、ファイアウォールの導入に関する理解を深めることができます。

無料機能：

- ファイアウォールの構成を評価し、改善点を特定する
- ファイアウォールからランタイムおよび履歴テレメトリデータに簡単にアクセスできるようにする
- システムの問題を検出します(検出方法とは無関係)
- アラート/通知ワークフローによる解決までの時間の短縮
- いくつかのセキュリティサブスクリプションの動的なダッシュボードと視覚化を提供する

プレミアムティアライセンスでは、無料とプレミアムの両方の機能を利用できます。プレミアム機能は、ファイアウォールのフル活用と最大限のセキュリティ成果の実現に焦点を当てています。

プレミアム機能

- NGFWのためのクラウド管理

  *Strata Cloud Manager*を使用してCloud Management for NGFWを有効にするには、アカウントチームにお問い合わせください。
- 高度なML技術を使用して、変化する脅威とネットワーク環境に対応する常に最適なセキュリティ態勢を推進し、アタックサーフェスを縮小する
- WildFireとIOC Searchの動的なダッシュボードと可視化を提供する
- Strata Cloud Managerコマンドセンターでデータとやり取りし、ネットワーク上のイベント間の関係を視覚化して、異常を発見したり、ネットワークセキュリティを強化する方法を見つける

©2025 Palo Alto Networks, Inc.

*Strata Cloud Manager*には、次の2つのライセンス階層があります。*Strata Cloud Manager Essentials*と*Strata Cloud Manager Pro*です。この統一された構造により、*NGFW*の*AIOps*、*Autonomous Digital Experience Management(ADEM)*、クラウド管理機能、*Strata Logging Service*などのネットワークセキュリティ製品の導入が効率化されます。Strata Cloud Manager ライセンスを確認する。

NGFW無料のための***AIOps*** アプリまたは *Strata Cloud Manager* を ***NGFW***プレミアムの***AIOps*** ライセンスをすでに使用している場合、既存のライセンスは影響を受けず、引き続き修正、延長、または更新できます。

機能セット	無料	Premium(Strata Cloud Managerを使用)
セキュリティ体制の強化	一部	あり
• セキュリティ体制インサイト	あり	あり
• 機能の導入状況	あり	あり
• セキュリティ体制の設定	いいえ	あり
• ソフトウェアアップグレードの推奨事項	いいえ	あり
• CDSS の採用	あり	あり
• ポリシーアナライザー	いいえ	あり
• オンデマンド BPA レポート	あり	あり
• Panorama CloudConnectorプラグイン	いいえ	あり
• 容量アナライザー	いいえ	あり
• NGFW SDWANダッシュボード	いいえ	あり
• コンプライアンス概要ダッシュボード	いいえ	あり
ファイアウォールの障害をプロアクティブに解決	一部	あり
• アラートとインシデント	一部	あり
• PAN-OS CVEダッシュボード	あり	あり
• アラートの考えられる原因分析	いいえ	あり

©2025 Palo Alto Networks, Inc.

機能セット	無料	Premium(Strata Cloud Managerを使用)
ログによるトラブルシューティング	あり	あり
• ログビューアでログを表示、照会、エクスポートログビューアを使用するためのライセンスおよびその他の要件を  確認します。	あり	あり
• トラブルシューティングのためのメタデータのエクスポート	あり	あり
• 監査ログの表示	あり	あり
セキュリティ投資の最適化	一部	あり
• 正常性とセキュリティ体制に基づくデバイスのランク付け	あり	あり
• 脅威インサイトダッシュボードを除くすべてのダッシュボードとレポート	あり	あり
• 脅威インサイトのダッシュボードとレポート	いいえ	あり
• セキュリティアーティファクトの検索	いいえ	あり
• カスタムダッシュボードの構築	いいえ	あり
• Strata Cloud Managerコマンドセンター	いいえ	あり
通知	一部	あり
• 電子メール通知	あり	あり
• ServiceNowとの連携	いいえ	あり
エンゲージメントとサポート	いいえ	あり

©2025 Palo Alto Networks, Inc.

機能セット	無料	Premium(Strata Cloud Managerを使用)
• 運用上の問題に対する製品内サポートチケットの作成機能には、 ファイアウォールでのプラチナ層サポートが必要 です(電源障害アラートを除く)。	いいえ	あり

製品の新機能は、すべての機能カテゴリにわたって、*Palo Alto Networks*の判断のみに基づいて、フリーおよびプレミアム階層に割り当てられます。

©2025 Palo Alto Networks, Inc.

AIOps for NGFWをアクティブにする方法

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	次のいずれか： ☐ AIOps for NGFW Free または Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium または Strata Cloud Manager Pro

AIOps for NGFWをアクティブ化するためのさまざまなシナリオを次に示します。

シナリオ	計画
AIOps for NGFWフリーのアクティブ化	AIOps for NGFWの有効化(無料)
AIOps for NGFW Premiumの有効化（Strata Cloud Managerアプリを使用）	Common Servicesを介したAIOps for NGFWのアクティブ化
アクティブ化されたAIOps for NGFW Freeインスタンスへの新規デバイスのオンボード	デバイスをテナントに関連付ける デバイスで遠隔測定を有効にする
アクティブ化されたAIOps for NGFW Premiumへの新規デバイスのオンボード（Strata Cloud Managerアプリを使用）	デバイスをテナントに関連付ける テナント内のデバイスをアプリに関連付ける デバイスで遠隔測定を有効にする
ELAAIOps for NGFWプレミアムの有効化	AIOps for NGFW PremiumのELA（エンタープライズライセンス契約）を有効化
Strata Cloud Manager（AIOps for NGFW Premium）を使用したVM-Seriesの管理	ソフトウェアNGFWクレジットライセンス契約の有効化
Panorama Managed VM-SeriesにStrata Cloud Manager（AIOps for NGFW Premium）を使用する	PanoramaマネージドVM-Series用ソフトウェアNGFWクレジットライセンスの有効化
AIOps for NGFW Premiumトライアルライセンスの本番環境への変換	試用版ライセンスを製品版に変換
Strata Cloud Manager Essentials および Strata Cloud Manager Proを有効化する。	• Strata Cloud Manager Essentialsの有効化 • Strata Cloud Manager Proの有効化

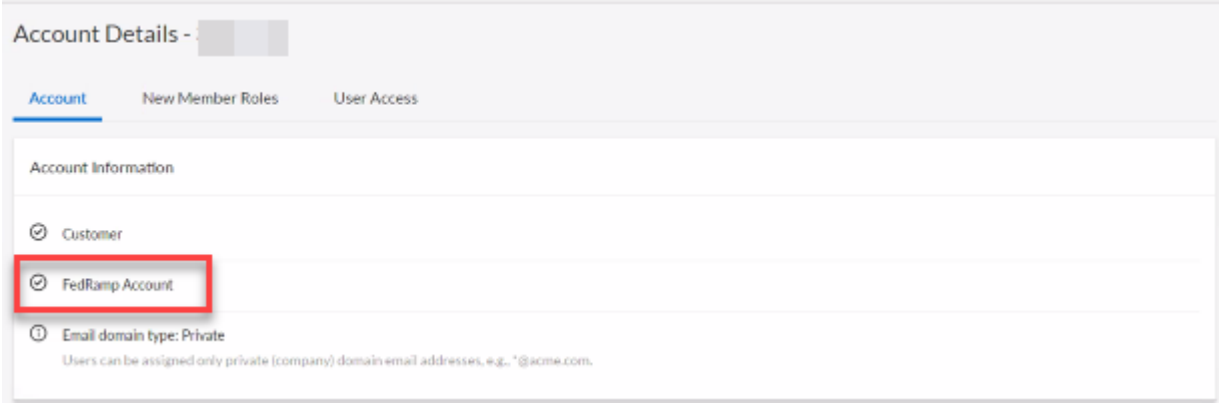
©2025 Palo Alto Networks, Inc.

シナリオ	計画
*Strata Cloud Manager Essentials*と*Strata Cloud Manager Pro*は、以下の機能を持たないカスタマーサポートポータル（*CSP*）アカウントでアクティベートできます。サイズのストレージを備えた*Strata Logging Service*、*NGFW Free*または*Premium*用の*AIOps*、*Prisma Access*のいずれか。	

Strata Cloud Manager は、AIOps for NGFW Premiumライセンスを使用するNGFWのみに統合された管理と運用を提供します。AIOps for NGFW Freeにオンボードされ ているNGFWについては、引き続きAIOps for NGFW Freeアプリを使用してください。

Strata Cloud Managerは、次の2つのライセンス階層を備えています。Strata Cloud Manager Essentials および Strata Cloud Manager Pro。この統一された構造により、NGFWのAIOps、Autonomous Digital Experience Management(ADEM)、クラウド管理機能、Strata Logging Serviceなどのネットワークセキュリティ製品の導入が効率化されます。これらの新しいライセンス階層の導入前にStrata Cloud Managerを使用していた場合、既存のAIOps for NGFW PremiumとAIOps for NGFW Freeのライセンスはサポートされたままです。これらのライセンスは、引き続き修正、延長、または更新することができます。

*FedRAMP*アカウントは*AIOps for NGFW*を使えません。該当するかどうかを確認するには、カスタマーサポートポータルアカウントにサインインし、***[Account Management (**アカウント管理**)]*** > ***[Account Details (**アカウントの詳細**)]***を選択します。***FedRamp***アカウントが表示されている場合は、*AIOps for NGFW*を使用できません。



AIOps for NGFWの有効化(無料)

アクティベーションにはアカウント管理者またはアプリ管理者ロールが必要です。

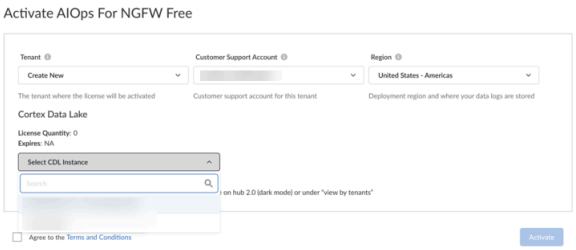
 ©2025 Palo Alto Networks, Inc.

1. テナント中心のビューでハブにログインします。

   サポートアカウントビューを表示している場合は、**[View by Support Account (サポートアカウント別表示)]**をオフに切り替えます。

   既存のテナントがない場合は、サポートアカウントビューでハブにログインします。

2. AIOps for NGFW Freeを見つけ、**[Activate (アクティベート)]**を選択します。
3. フォームに入力します。

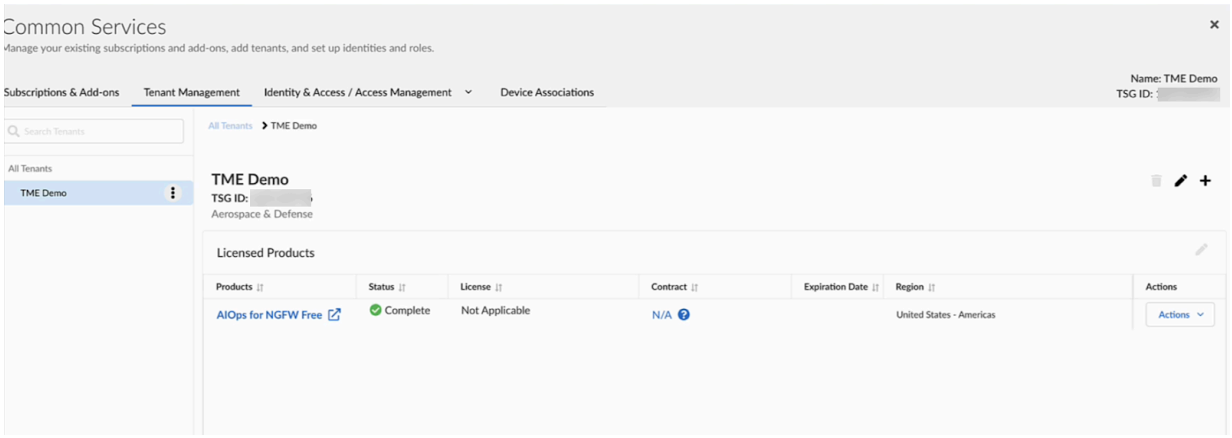


テナント	AIOps for NGFW Freeインスタンスをアクティブにするテナントを選択します。既存のテナントがない場合は、**[Create New (新規作成)]**を選択します。
カスタマーサポートアカウント	カスタマーサポートポータルのアカウントID。
リージョン	デプロイメントリージョンとデータログが格納されるリージョン。「Regions for AIOps for NGFW」を参照してください。
Strata Logging Service	AIOps for NGFW Freeにデータを送信するStrata Logging Service。ロギングSLSがある場合は、AIOps for NGFW Freeに関連付けることができます。それ以外の場合はスキップできます。

4. 利用規約に同意し、アクティベートします。

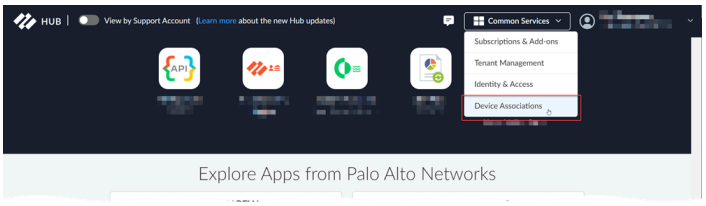
©2025 Palo Alto Networks, Inc.

5. NGFW Free の AIOps は、**[Status (ステータス)]** に **[Complete (完了)]** と表示されたら準備完了です。



 ©2025 Palo Alto Networks, Inc.

6. AIOps for NGFW Freeインスタンスを含むテナントにデバイスを関連付けます。
   1. ハブにログインします。
   2. **[Common Services (**共通サービス**)]** > **[Device Associations (**デバイス アソシエーション**)]**を選択します。



   3. **[Add Device (**デバイスの追加**)]**を選択します。
   4. ファイアウォールまたはPanoramaアプライアンスを1つ以上選択して保存します。

Panoramaマネージド導入をオンボードする場合は、AIOps for NGFW Freeを含むテナントにPanoramaを関連付ける必要があります。Panoramaで管理されているファイアウォールはすべて個別にテナントに関連付けてください。

テナントに関連付けたデバイスは、自動的にAIOps for NGFW Freeに追加されます。詳細については、「デバイスとテナントの関連付け」を参照してください。

- *AIOps for NGFW Free*のアクティベーションでは、アプリとデバイスの関連付けは必要ありません。
- すでに既存のテナントがある場合は、アクティベーションの開始時にデバイスをテナントに関連付けることができます。
- デバイスの関連付けの消去は、たとえば、ファイアウォールやパノラマアプライアンスを廃棄または返却する場合、または別のテナントサービスグループ（*TSG*）と関連付ける場合に実施できます。

©2025 Palo Alto Networks, Inc.

7. デバイスでテレメトリを有効にします。
   1. support.paloaltonetworks.comにログインして、デバイスがカスタマー・サポート・ポータルに登録されていることを確認し、アカウントに切り替え（必要な場合）、**[Assets (アセット)]** > **[Devices (デバイス)]**でデバイスを確認します。
   2. デバイス証明書をインストールする オンボードするデバイスで。
   3. デバイス上でテレメトリ共有を有効にします 。

   デバイスをオンボードしてテレメトリを有効にした後、最初の分析情報セットが*AIOps for NGFW*ダッシュボードに表示されるまでに約2時間かかります。デバイス側でテレメトリを生成して送信するプロセスはバッチで行われ、各メトリックは、メトリックが使用されるユースケースに最適化された頻度でサンプリングおよび収集されます。このバッチ プロセスにより、ファイアウォールのオンボードと分析情報の可用性の間に遅延が発生する可能性があります。新しくオンボードされたデバイスに関連付けられているすべての分析情報が*AIOps for NGFW*のダッシュボードに表示されるまでに、数時間かかる場合があります。
8. ハブ内のアイコンをクリックして、AIOps for NGFW Freeにログインします。

©2025 Palo Alto Networks, Inc.

NGFW機能のAIOpsはどこにありますか？

本コンテンツは、*AIOps for NGFW*と*Strata Cloud Manager*を備えた次世代ファイアウォールのクラウド管理のためのものです。*PAN-OS*による次世代ファイアウォールの管理を開始するには、ここをクリックしてください。

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	次のいずれか: ❑ AIOps for NGFW Free または Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium または Strata Cloud Manager Pro

Palo Alto Networks Strata Cloud Managerは、AIを活用した新しい統合ネットワークセキュリティ管理プラットフォームです。Strata Cloud Managerを使用して、他のPalo Alto Networks製品やサブスクリプションとAIOps for NGFWを連動させ、管理することができます。

Strata Cloud Managerを起動するには：

- ハブに移動してStrata Cloud Managerアプリを起動
- Strata Cloud ManagerURLに直接移動します

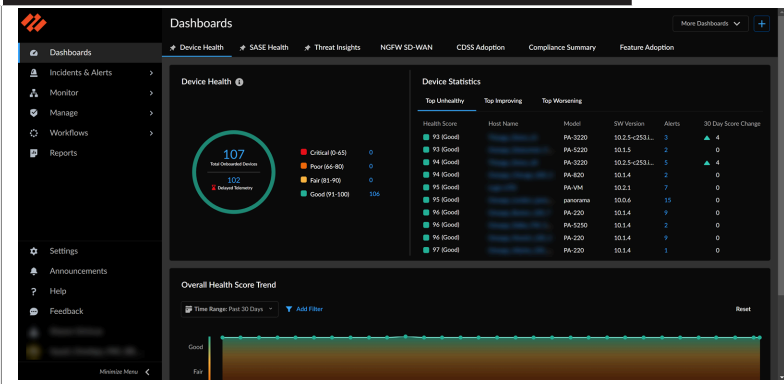
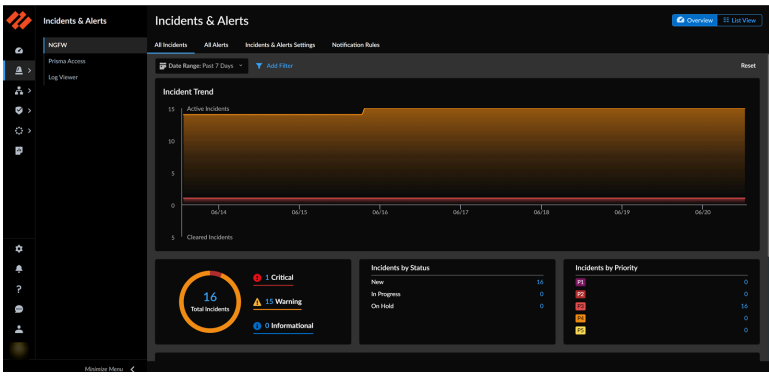
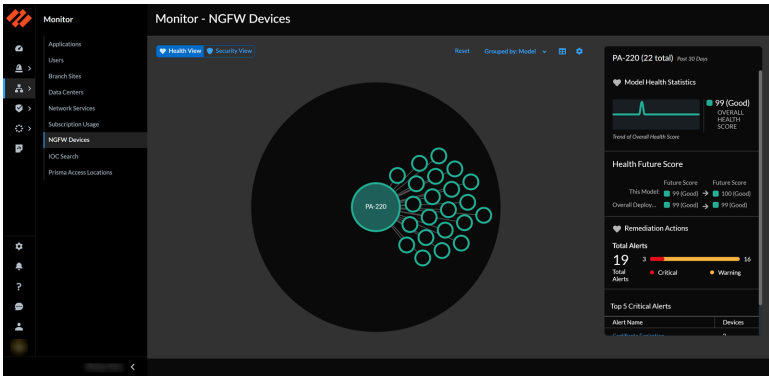
- Strata Cloud Manager は、*AIOps for NGFW Premium*ライセンスを使用する*NGFW*のみに統合された管理と運用を提供します。*AIOps for NGFW*（プレミアムアプリのみ）のハブ上のアプリケーションタイル名が*Strata Cloud Manager*に変更されました。今回のアップデートでは、アプリケーションの*URL*もstratacloudmanager.paloaltonetworks.comに変更され、左側のナビゲーションペインにも*Strata Cloud Manager*のロゴが表示されるようになりました。*AIOps for NGFW Free*にオンボードされている*NGFW*については、引き続き*AIOps for NGFW Free*アプリを使用してください。
- *Strata Cloud Manager*を使用してCloud Management for NGFWを有効にするには、アカウントチームにお問い合わせください。

以前にAIOps for NGFWアプリを使用したことのある方は、Strata Cloud Managerで以下の機能を利用できます。

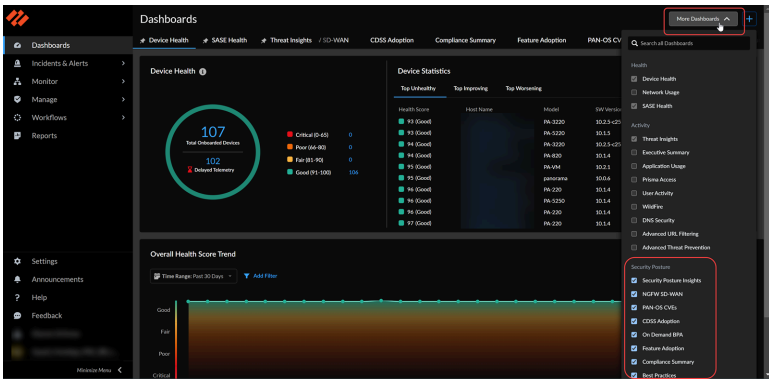
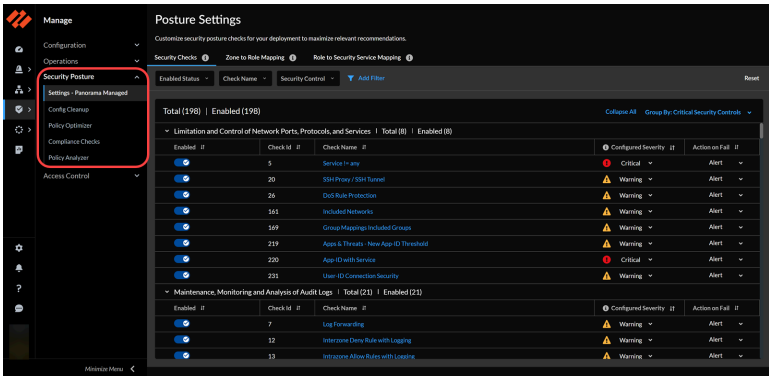
表 **1 :**

AIOps for NGFWアプリケーション	**Strata Cloud Manager**でこれらの同じ機能を見つける場所:
ダッシュボード	→[Dashboards (ダッシュボード)]→[Device Health(デバイスの正常性)]に移動

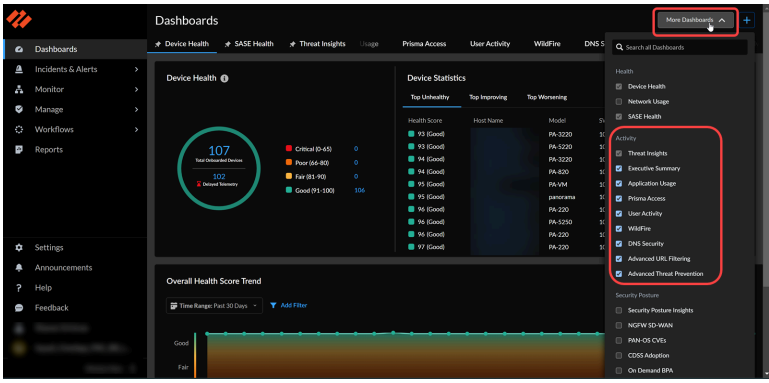
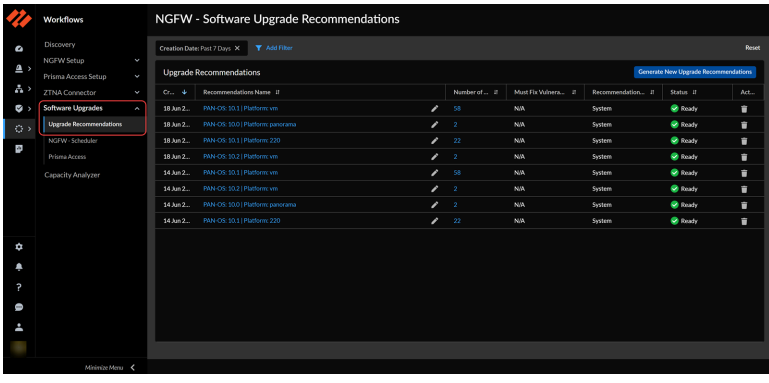
©2025 Palo Alto Networks, Inc.

AIOps for NGFWアプリケーション	Strata Cloud Managerでこれらの同じ機能を見つける場所:
	
アラート	→[Incidents & Alerts (インシデントとアラート)]→[NGFW]に移動 
監視	→[Monitor(監視)]→[Devices(デバイス)]→[NGFW]と進む 
姿勢	→[Dashboards (ダッシュボード)]に移動して、以下を確認します。 • ベストプラクティスダッシュボード • セキュリティ体制インサイトダッシュボード

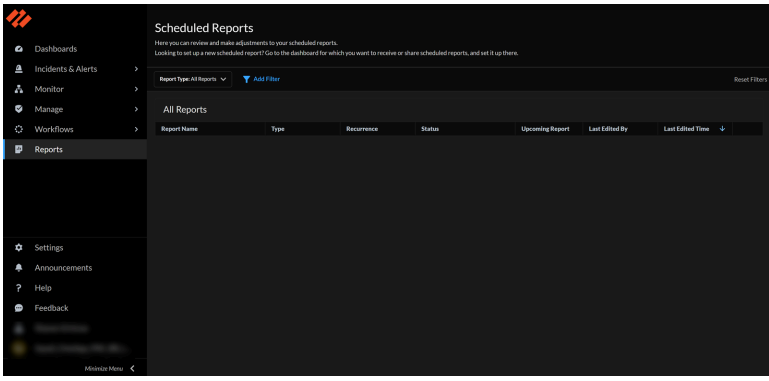
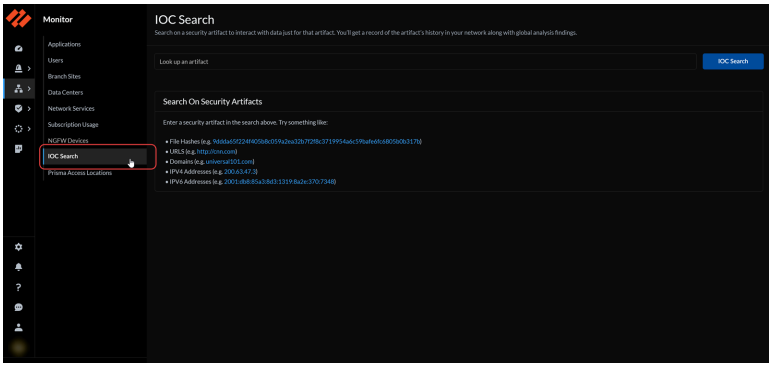
©2025 Palo Alto Networks, Inc.

AIOps for NGFWアプリケーション	Strata Cloud Managerでこれらの同じ機能を見つける場所:
	• NGFW SD-WANダッシュボード • セキュリティアドバイザリダッシュボード（PAN-OS CVE） • CDSS導入状況ダッシュボード • オンデマンドBPAダッシュボード • 機能の導入状況ダッシュボード • コンプライアンス概要ダッシュボード  →[Manage (管理)]→[Security Posture (セキュリティ体制)]で次の項目を見つけます。 • 設定 - Panorama 管理 • 構成のクリーンアップ • ポリシー オプティマイザー • コンプライアンスのチェック • ポリシーアナライザー 
アクティビティ	→[Dashboards (ダッシュボード)]に移動して、以下を確認します。 • ネットワークの使用状況

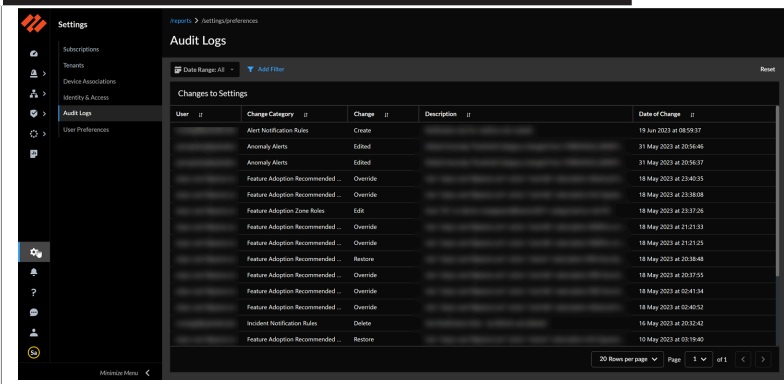
 ©2025 Palo Alto Networks, Inc.

AIOps for NGFWアプリケーション	Strata Cloud Managerでこれらの同じ機能を見つける場所:
	• 脅威のインサイト • アプリケーションの使用状況 • アドバンスド WildFire • DNS セキュリティ • エグゼクティブ概要 • ユーザーアクティビティ  →[Reports (レポート)]に移動し、サポートされているダッシュボードのレポートを生成します。 →[Log Viewer (ログビューア)]の[Incidents & Alerts (インシデントとアラート)]に移動します。
ワークフロー	→[Upgrade Recommendations (アップグレード推奨事項)]を使用するには、「Workflows (ワークフロー) > [Software Upgrades (ソフトウェアアップグレード)]に移動します。 

©2025 Palo Alto Networks, Inc.

AIOps for NGFWアプリケーション	Strata Cloud Managerでこれらの同じ機能を見つける場所:
レポート	→**[Reports (**レポート**)]**に移動し、サポートされているダッシュボードのレポートをスケジュールします。 
検索	→ [IoC Search (IoC検索)]の**[Monitor (**モニター**)]**に移動します。 
設定	→ **[Incidents & Alerts (**インシデントとアラート**)]** > **[NGFW]** > **[Incidents & Alerts Settings (**インシデントとアラート設定**)]** を開き、**[Forecast and Anomaly Incidents & Alerts (**予測、異常インシデント、アラート**)]**を表示します。 →**[Incidents & Alerts (**インシデントとアラート**)]** > **[NGFW]**で**[Notification Rules (**通知ルール**)]**を設定します。 →**[Settings (**設定**)]**で次の項目を確認します。 • 監査ログ • ユーザー設定

 ©2025 Palo Alto Networks, Inc.

AIOps for NGFWアプリケーション	Strata Cloud Managerでこれらの同じ機能を見つける場所:
	 → **[Security Posture (セキュリティ体制)]** > **[Manage (管理)]** から **Settings - Panorama Managed (設定-パノラマ管理)**をカスタマイズします。 →**[Help (ヘルプ)]**→**[Export Tenant Metadata (テナントメタデータのエクスポート)]**に移動します。
–	**Strata Cloud ManagerでNGFWを管理する**方法をお探しですか？ これはAIOps for NGFW Premium付きのStrata Cloud Managerでのみサポートされ、AIOps for NGFWアプリでは利用できません。 → **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWs and Prisma Access (NGFWとPrisma Access)]** および**[Workflows (ワークフロー)]** > **[NGFW Setup (NGFWセットアップ)]**へと移動します。

©2025 Palo Alto Networks, Inc.

Panorama CloudConnectorプラグイン

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	☐ AIOps for NGFW Premium または Strata Cloud Manager Pro

ポリシールールがベストプラクティスに準拠しているかプロアクティブにチェックしたいポリシールールをプッシュした後にアラートを取得して問題を修正するまで待つ必要はありません。AIOps for NGFWまたはStrata Cloud ManagerをPanoramaに接続し、管理対象のファイアウォールにプッシュする前に、特定のベストプラクティスチェックに照らして構成を評価します。セキュリティチェックのプロアクティブな実施を参照してください。

セキュリティポリシールールの更新は、時間的制約を伴うことが多く、迅速な対応が求められます。ただし、セキュリティポリシーのルールベースに対して行う更新は、要件に適合し、エラーや設定ミス（ルールの重複や矛盾を招くような変更）が発生しないようにする必要があります。

これを実現するために、Strata Cloud ManagerのPolicy Analyzerを使用すると、変更要求を実装するときに時間とリソースを最適化できます。Policy Analyzerは、特定のルールを分析して、意図に沿った統合や削除の可能性を提案するだけでなく、ルールベースのシャドウ、冗長性、汎化、相関、統合などの異常もチェックします。

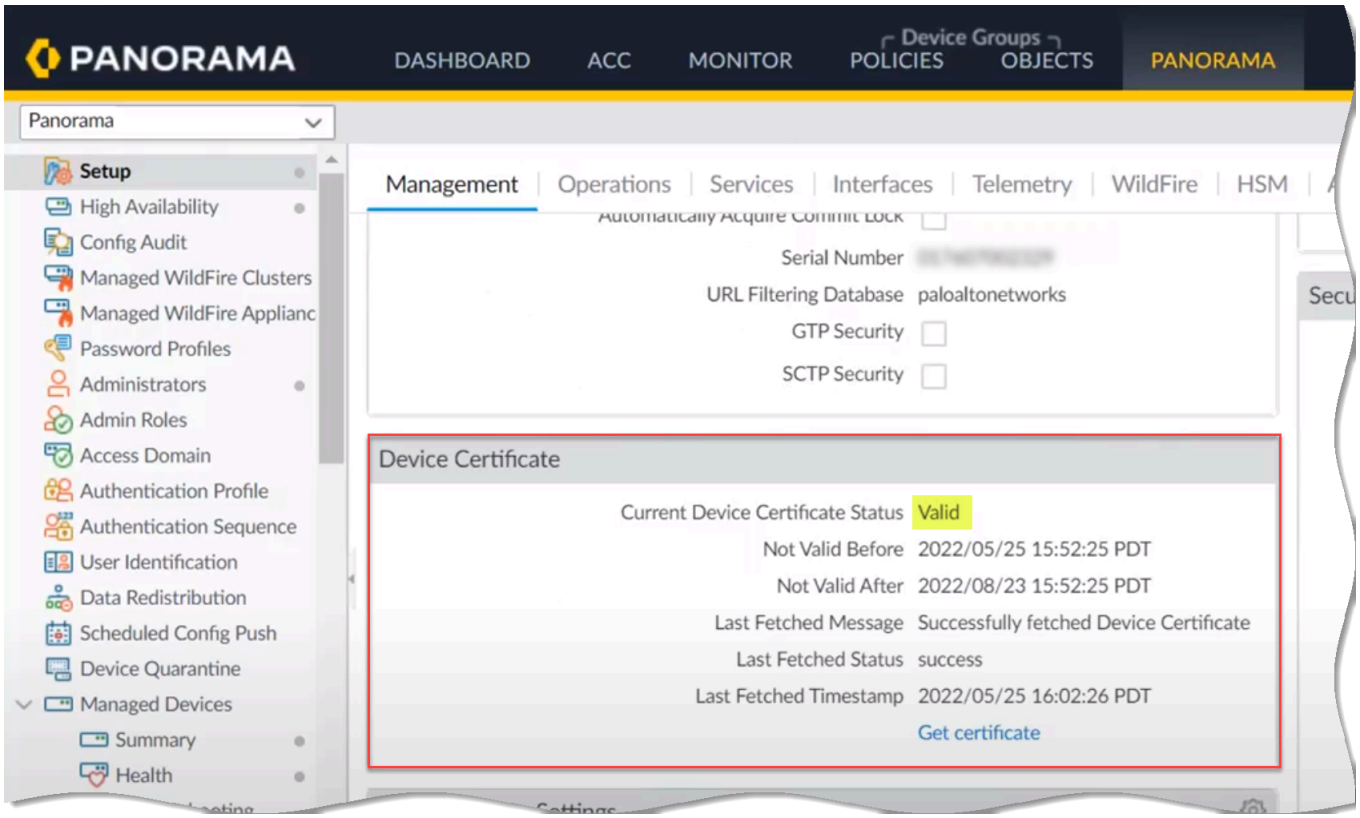
AIOps for NGFWまたはStrata Cloud Manager を Panoramaに接続し、Policy Analyzerを使用してセキュリティポリシールールベースを追加または最適化します。「Policy Analyzer (ポリシーアナライザ)」を参照してください。

AIOps for NGFWとPanoramaを繋ぐには、次のものが必要です。

NGFWまたはStrata Cloud ManagerインスタンスのAIOps:Panorama CloudConnectorプラグインのインストールにAIOps for NGFW Premiumライセンスは必要ありません。ただし、ポリシーアナライザやプロアクティブベストプラクティス評価（BPA）などのプレミアム機能を利用するには、プレミアムライセンスが必要です。

©2025 Palo Alto Networks, Inc.

デバイス証明書がインストールされたPanorama。

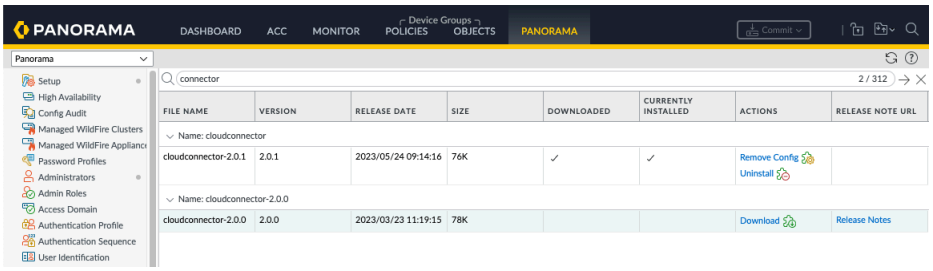


©2025 Palo Alto Networks, Inc.

PAN OS 10.2.3以降を実行しているPanoramaにインストールされているPanorama CloudConnectorプラグイン。

コマンドを使ってこのプラグインを有効にする必要があります。

```
> request plugins cloudconnector enable basic
```



- お客様を支援するため、このプラグインを新しいバージョンの*Panorama*（*11.0.1*以降）にプリインストールしました。
- *AIOps*プラグインと*CloudConnector*プラグインの両方がすでにインストールされている場合は、*AIOps*プラグインをアンインストールします。これらは同一であり、名前だけが変更されているためです。インストールされているプラグインが*1*つだけであることを確認します。こ*CloudConnector*プラグインの最新バージョンである必要があります。

AIOpsプラグインをPAN-OS 10.2.3にインストールした後、PAN-OS 11.0.1以降にアップグレードした場合、プラグインのデフォルトバージョンが新しいPAN-OSバージョンでインストールされます。これにより、両方のプラグインがPanorama上に存在することになります。この場合、次の手順に従います。

1. Panoramaウェブインターフェースで 、 「**[Panorama]>[Plugins]**を選択し、AIOpsプラグインをアンインストールします。
2. CloudConnectorプラグインを有効にします。

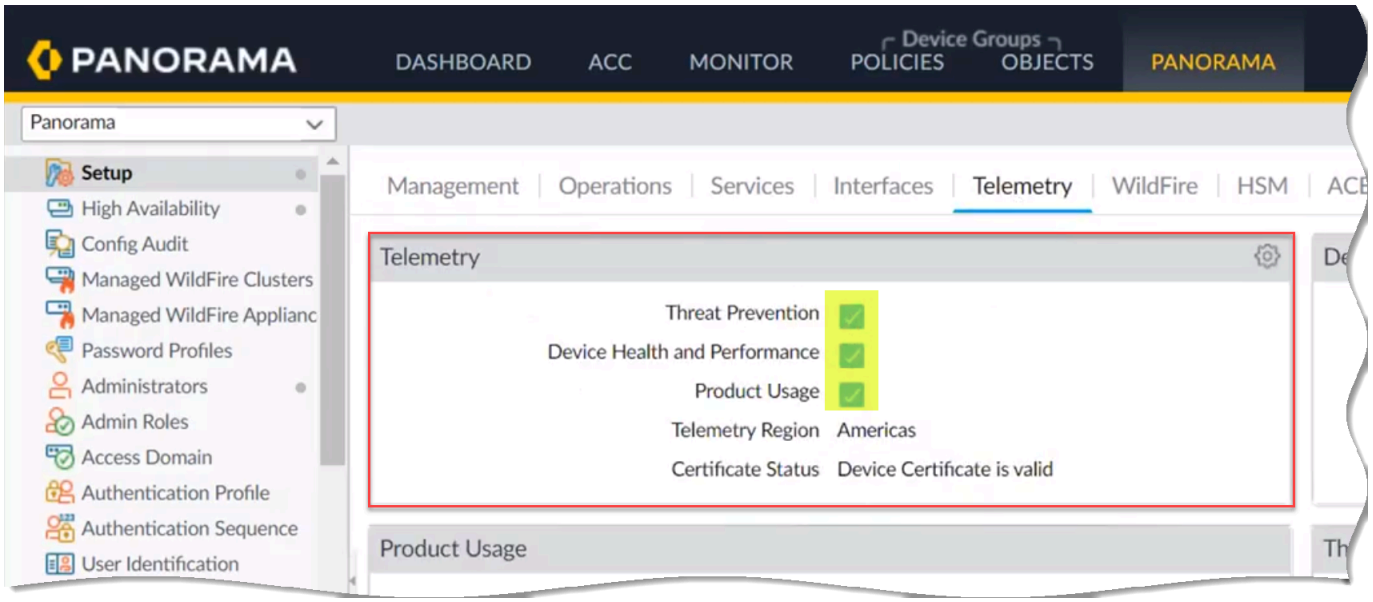
   ```
   > request plugins cloudconnector enable basic
   ```

CloudConnectorプラグイン2.2.0はPanoramaからのプロキシ設定に対応しています。これらの設定はコミット後にのみ有効になります。シナリオは次のとおりです。

- プロキシ設定の構成:プロキシ設定を構成してコミットを実行すると、CloudConnectorプラグインはこのコミット中に新しいプロキシ設定を認識しません。コミット後、プラグインはプロキシ設定を使用して、今後のクラウドとのやり取りを行います。
- プロキシ設定の削除：プロキシ設定を削除してコミットを実行すると、CloudConnectorプラグインはコミット中に削除されたプロキシ設定を認識しません。コミット後、プラグインはクラウドとの今後の対話にプロキシ設定を使用しなくなります。

 ©2025 Palo Alto Networks, Inc.

Panoramaでデバイステレメトリが有効になっています。



PanoramaとStrata Logging Serviceホストリージョンに対応するFQDN間の通信を許可するセキュリティポリシールール：

アメリカ (アメリカ)	https://prod.us.secure-policy.cloudmgmt.paloaltonetworks.com/
オーストラリア（AU）	https://prod.au.secure-policy.cloudmgmt.paloaltonetworks.com/
カナダ（CA）	https://prod.ca.secure-policy.cloudmgmt.paloaltonetworks.com/
ヨーロッパ (ヨーロッパ)	https://prod.eu.secure-policy.cloudmgmt.paloaltonetworks.com/
FedRAMP (政府)	https://prod.gov.secure-policy.cloudmgmt.paloaltonetworks.com/
ドイツ (DE)	https://prod.de.secure-policy.cloudmgmt.paloaltonetworks.com/
インド (IN)	https://prod.in.secure-policy.cloudmgmt.paloaltonetworks.com/
日本（JP）	https: / /prod.jp.secure-policy.cloudmgmt.paloaltonetworks.com/
シンガポール (SG)	https://prod.sg.secure-policy.cloudmgmt.paloaltonetworks.com/
英国（UK）	https://prod.uk.secure-policy.cloudmgmt.paloaltonetworks.com/

©2025 Palo Alto Networks, Inc.

アラート通知を取得する

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	次のいずれか: ❑ AIOps for NGFW Free または Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium または Strata Cloud Manager Pro

Strata Cloud Managerを既存の運用に統合するには、プロアクティブなアラートの設定が必要です。これにより、深刻な複雑さにエスカレートする前に、潜在的な問題を検出し、管理できます。これらのアラートは、一般的に使用されるP1やP2など、運用チームのケース管理プロトコルに合わせて調整できます。

たとえば、最も重大な問題を示す重要なアラートが瞬時にセキュリティチームにエスカレーションされ、すぐに対処できるアラートシステムを設定するとします。一方、緊急度は低いものの、それでも重要な警告アラートは、毎日確認できるようにアレンジできます。このような配置により、円滑な業務運営を維持しながら、効率的なインシデント管理を実現します。

チームに基づいてアラートをルーティングする方法もあります。特定のカテゴリのアラート、さらには特定のアラートを、そのアラートを処理するのに最適な設備を備えたさまざまなチームにルーティングできます。通知をトリガーするアラート、通知の受信方法、受信頻度など、通知の環境設定を定義し、通知ルールを作成できます。

通知ルールの作成方法を紹介する動画です。

STEP 1 | **[Incidents & Alerts (インシデントとアラート)]** > **[Incident & Alert Settings (インシデントとアラートの設定)]** > **[Notification Rules (通知ルール)]** > **[+ Add Notification Rule (通知ルールを追加)]**を選択します。

STEP 2 | `[Name (名前)]`と`[Description (説明)]`を入力します。

STEP 3 | **[Add New Condition (新しい条件を追加)]**をクリックして、通知をトリガーする`[Rule Conditions (規則条件)]`を指定します。

たとえば、ハードウェアアラートの通知を作成するには、**[subCategory (サブカテゴリ)]**、**[Equals (イコール)]**、**[Hardware (ハードウェア)]**を選択します。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | 通知の[Notification Type and Recipients (通知タイプと受信者)]を選択します。

1. [電子メール]を選択する場合は、電子メール通知を受け取るユーザーのグループである電子メールグループを選択するか、または「**Create a New Email Group (**新しい電子メールグループの作成**)**」を選択します。
   1. 新しい電子メールグループを作成する場合は、「電子メールグループ名」を入力し、グループに追加する電子メールアドレスの入力を開始します。各メールアドレスの入力が終わったらリターンキーを押します。
   2. **Next**（次へ）を選択します。
   3. これらの通知を送信する頻度を選択します。
      - 直ちに
      - グループ化して4時間ごとに送信
      - グループ化して1日1回送信
2. **ServiceNow**を選択する場合は、ServiceNow URL、クライアント認証情報、ServiceNow認証情報、ServiceNow APIバージョンを入力します。
   1. 接続をテストして、連動が機能していることを確認します。
   2. **Next**（次へ）を選択します。

STEP 5 | ルールを保存します。

 ©2025 Palo Alto Networks, Inc.

NGFW接続およびポリシー適用の異常のトラブルシューティング

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ AIOps for NGFW Premium または Strata Cloud Manager Pro ❑ ロギングにはStrata Logging Serviceライセンスが必要です ❑ Prisma Accessライセンスをお持ちの場合は、フォルダ管理を使用して定義済みフォルダを表示し、フォルダのウェブセキュリティを有効にすることができます

Strata Cloud ManagerからNGFWのトラブルシューティングを実行でき、さまざまなファイアウォールインターフェース間を移動する必要はありません。NGFW を展開して設定した後に接続の問題が発生した場合は、ルーティングおよびトンネルの状態を集約的に把握できます。詳細をドリルダウンして、異常や問題のある設定を発見できます。

IDベースのポリシールールと動的に定義されたエンドポイントのトラブルシューティングを行います。特定のNGFWのステータスをチェックし、ポリシーの動作を期待する方法と実際の適用動作のミスマッチの可能性を明らかにすることができます。

トラブルシューティングを行うことで、これらのネットワーキングおよびアイデンティティ機能内で発生する可能性のある問題をドリルダウンできます。接続の問題やポリシー適用の異常を追跡して解決できます。

ネットワークのトラブルシューティング

- NAT
- DNS プロキシ

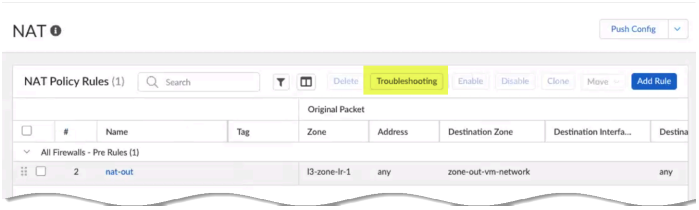
IDとポリシーのトラブルシューティング

- ユーザー グループ
- ダイナミック アドレス グループ
- ダイナミックユーザー グループ
- ユーザーID

ファイアウォールのトラブルシューティング

- セッションブラウザ

©2025 Palo Alto Networks, Inc.



ファイアウォールのトラブルシューティングを開始するには、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW and Prisma Access (NGFWとPrisma Access)]** > **[Operations (オペレーション)]** > > **[Troubleshooting (トラブルシューティング)]** > **[Session Browser (セッションブラウザ)]** の順に進みます。

または、トラブルシューティングを行う機能に移動して、［**Troubleshooting (トラブルシューティング)]**ボタンを選択して開始できます。

実行したトラブルシューティングジョブをステータス、アクション、検索対象、タイムスタンプ別に表示およびソートできます。

機能	機能の場所	利用可能なアクション	アクションスコープ	ジョブ出力の整理者:
セッションブラウザ(ファイアウォール)	管理 > 設定 > **NGFW** と **Prisma** のアクセス > 業務 > トラブルシューティング > セッションブラウザ	フィルタ条件： • Firewalls (ファイアウォール) • Rule Name (ルール名) • Source Zone (送信元ゾーン) • Source Address (送信元アドレス) • Source User (送信元ユーザー) • Source Port (送信元ポート) • Destination Zone (宛先ゾーン) • Destination Address (宛先アドレス)	指定したファイアウォール	• セッション ID • 開始時間 • ゾーン • 送信元 • 宛先 • ポート • PROTOCOL • アプリケーション • 入口 • 出口 • バイト数

 ©2025 Palo Alto Networks, Inc.

機能	機能の場所	利用可能なアクション	アクションスコープ	ジョブ出力の整理者:
		• Destination Port (宛先ポート) • App-ID		
DNSプロキシ(ネットワーク)	構成の管理 > **NGFW** と **Prisma** のアクセス > デバイス設定 > **DNS** プロキシ	• DNS プロキシキャッシュを表示 • DNS プロキシキャッシュを検索	指定したファイアウォール	• ドメイン名 • IP アドレス • Type–IPv4 Address Record (A)、IPv6 Address Record (AAAA)、Canonical Name Record (CNAME)、Mail Exchange Record (MX)、Pointer to a canonical Name (PTR) • クラス:インターネット（IN TCP/IP）、カオス（CH）、ヘシオド（HS） • TTL（存続可能時間）（秒） • ヒット数：最後のリブート以降にレコードが要求された回数
NAT (ネットワーク)	構成の管理 > **NGFW** と **Prisma** のアクセス > ネットワークポリシー > **NAT**	NATルールのIPプールを表示する	指定したファイアウォール	• rule • タイプ • 使用中 • 使用可能

©2025 Palo Alto Networks, Inc.

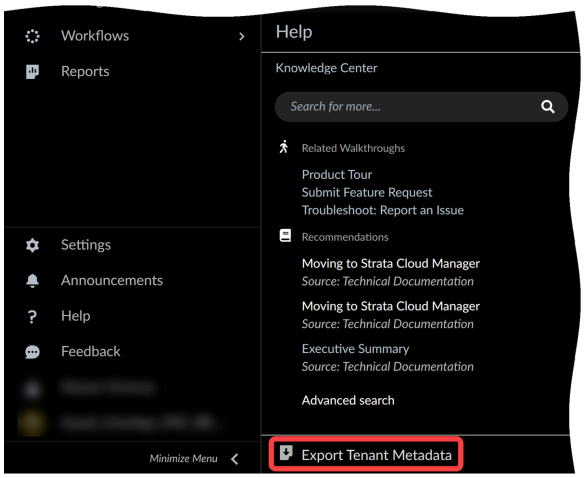
機能	機能の場所	利用可能なアクション	アクションスコープ	ジョブ出力の整理者:
				• メモリサイズ比
ユーザーグループ(アイデンティティ)	構成の管理 > **NGFW** と **Prisma** のアクセス > **ID** サービス > **Cloud Identity Engine**	• ユーザーグループを表示 • ユーザーグループの検索	指定したファイアウォール	• username • グループ
Dynamic Address Group (ダイナミックアドレス グループ)(アイデンティティ)	構成の管理 > **NGFW** と **Prisma** のアクセス > オブジェクト > アドレス > アドレス グループ	• すべてのダイナミック アドレスグループを表示 • ダイナミックアドレスグループの検索（リストから選択）	指定したファイアウォール	• 氏名 • フィルタ • メンバー
Dynamic User Groups Column (ダイナミックユーザー グループ列)	構成の管理 > **NGFW** と **Prisma** のアクセス > オブジェクト > ダイナミックユーザー グループ	• ダイナミックユーザーグループで検索 • ユーザー名で検索	指定したファイアウォール	• メンバー(ユーザー名)および/またはダイナミックユーザーグループ
ユーザーID(アイデンティティ)	構成の管理 > **NGFW** と **Prisma** のアクセス > **ID** サービス > アイデンティティ情報再配信	• すべてのユーザーのIPマッピングを表示 • ユーザーIPマッピングを検索	指定したファイアウォール	• IP • ユーザー • 開始日時 • アイドル タイムアウト • 最大タイムアウト

トラブルシューティングのためのメタデータのエクスポート

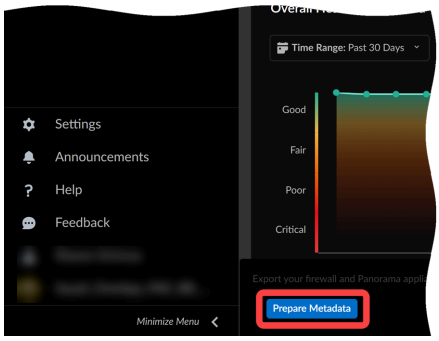
AIOps for NGFWでは、テクニカルサポートがお客様をより適切に支援するために必要な情報を提供するため、展開データをローカルマシンにエクスポートできます。このデータは、gzip形式で圧縮されたJSONファイルで届きます。

©2025 Palo Alto Networks, Inc.

1. [ヘルプ]>[テナントメタデータのエクスポート]を選択します。



2. メタデータを準備します。



3. メタデータファイルをダウンロード します。

   メタデータファイル名には、カスタマーサポートポータル（CSP）ID、NGFWテナントIDのAIOps、およびエクスポートのタイムスタンプが含まれます :<*csp-tenant-timestamp*>.gzip。

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

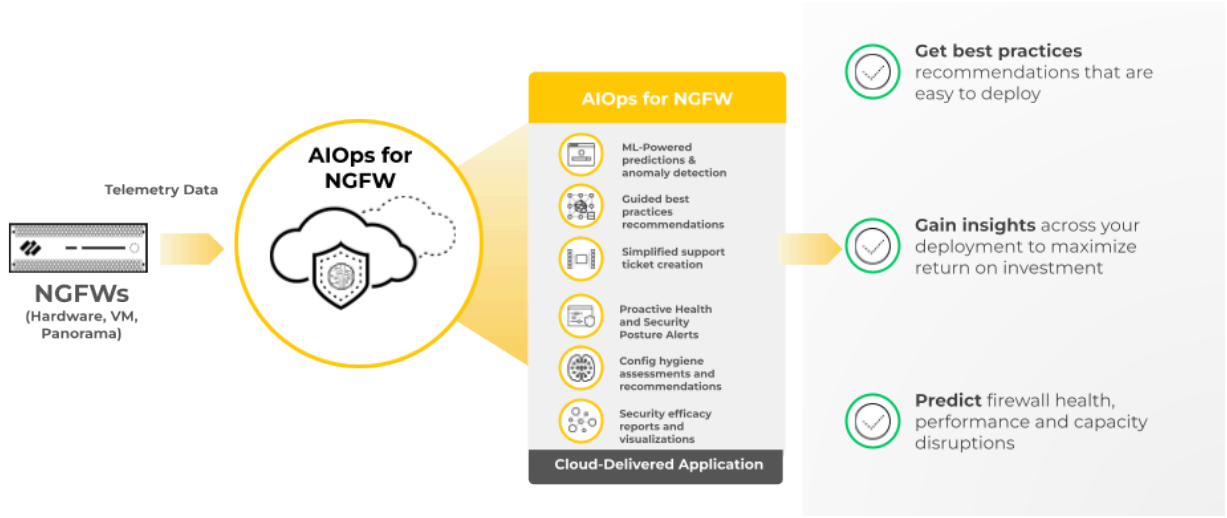
AIOps for NGFWのデバイスのテレメトリ

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	次のいずれか ❑ または ❑ または

AIOps for NGFWは、PAN-OSデバイスがStrata Logging Serviceに送信するテレメトリデータを分析することで、導入したファイアウォールの健全性を評価します。このデータを送信するには、デバイスのテレメトリーを有効にする必要があります。

テレメトリーが設定されると、次世代ファイアウォールは一定の間隔で生のテレメトリーデータをStrata Logging Serviceに送信します。Strata Logging Serviceはこの生データを解析・変換し、AIOps for NGFWがデバイスのステータス、視覚化、アラートを提供できるようにします。

デバイスをオンボードし、AIOps for NGFWにデバイスのテレメトリを送信します。



デバイスでのテレメトリの有効化

PAN-OSデバイスでAIOps for NGFWを使用するには、以下の手順に従ってください。

アウトバウンド トラフィックがプロキシを通過する場合、AIOps for NGFWに必要なドメインを許可していることを確認します。

*Panorama*で管理されるデプロイをオンボードする場合は、*NGFW*の*AIOps*で*Panorama*をオンボードする必要があります。

1. support.paloaltonetworks.comにログインして、デバイスがカスタマー・サポート・ポータルに登録されていることを確認し、アカウントに切り替え（必要な場合）、**[Assets (アセット)]** > **[Devices (デバイス)]**でデバイスを確認します。
2. デバイス証明書をインストールする オンボードするデバイスで。
3. デバイス上でテレメトリ共有を有効にします 。

デバイスをオンボードしてテレメトリを有効にした後、最初の分析情報セットが*AIOps for NGFW*ダッシュボードに表示されるまでに約*2*時間かかります。デバイス側でテレメトリを生成して送信するプロセスはバッチで行われ、各メトリックは、メトリックが使用されるユースケースに最適化された頻度でサンプリングおよび収集されます。このバッチ プロセスにより、ファイアウォールのオンボードと分析情報の可用性の間に遅延が発生する可能性があります。新しくオンボードされたデバイスに関連付けられているすべての分析情報が*AIOps for NGFW*のダッシュボードに表示されるまでに、数時間かかる場合があります。

©2025 Palo Alto Networks, Inc.

AIOps for NGFWに必要なドメイン

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	次のいずれか ❑ または ❑ または

デバイスからの送信トラフィックがプロキシを通過する場合、AIOps for NGFWを正常に使用するために、以下のFQDNを許可していることを確認する。

AIOps for NGFWにアクセスするためのドメイン

AIOps for NGFWアプリケーションにアクセスするには、地域に関係なく、これらのドメインを許可してください。

- *.prod.di.paloaltonetworks.cloud
- *.paloaltonetworks.com
- *.prod.di.paloaltonetworks.com
- *.prod.reporting.paloaltonetworks.com
- *.receiver.telemetry.paloaltonetworks.com
- https://storage.googleapis.com

テレメトリを送信するための**App-ID**とドメイン

テレメトリデータをAIOps for NGFWに正常に送信するためにPalo Alto Networksファイアウォールで許可する必要があるApp-IDとポートについては、「Strata Logging Serviceに必要なTCPポートとFQDN」を参照してください。

プロキシサーバーでは、必要なポートとFQDNを許可することに加えて、デバイスがAIOps for NGFWにテレメトリデータを送信できるように、地理的な地域に対応するドメインを許可します。

リージョン	ドメイン
米国	http://br-prd1.us.cdl.paloaltonetworks.com/
ヨーロッパ	http://br-prd1.nl.cdl.paloaltonetworks.com/
イギリス	http://br-prd1.uk.cdl.paloaltonetworks.com/
カナダ	http://br-prd1.ca1.ne1.cdl.paloaltonetworks.com/

©2025 Palo Alto Networks, Inc.

リージョン	ドメイン
シンガポール	http://br-prd1.sg1.se1.cdl.paloaltonetworks.com/
日本	http://br-prd1.jp1.ne1.cdl.paloaltonetworks.com/
オーストラリア	http://br-prd1.au1.se1.cdl.paloaltonetworks.com/
ドイツ	http://br-prd1.de1.ew3.cdl.paloaltonetworks.com/
インド	http://br-prd1.in1.as1.cdl.paloaltonetworks.com/

©2025 Palo Alto Networks, Inc.

セキュリティ体制を最適化

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	次のいずれか □ または □ または

AIOps for NGFWは、ファイアウォールを機能的に正常な状態に維持するだけでなく、ファイアウォールがセキュリティの脅威に対して効果的な保護を提供していることを確認するのに役立ちます。

現在、セキュリティ体制の評価では複数の仮想システムをサポートしていません。設定処理中に考慮されるのは、デフォルトの仮想システム*(vsys1)*のみです。

- セキュリティ体制インサイトを監視する:オンボードのNGFWデバイスのセキュリティ体制に基づいて、デプロイメントのセキュリティ ステータスと傾向を可視化できます。
- モニタ機能の導入状況:デプロイメント環境で使用しているセキュリティ機能を表示します。
- セキュリティサブスクリプションの監視:推奨されるクラウド配信セキュリティサービス（CDSS）サブスクリプションと、デバイスでのその使用状況を確認できます。
- 脆弱性の評価:特定のファイアウォールやPAN-OSのバージョンに影響を与える脆弱性を表示し、アップグレードが必要かどうかの意思決定プロセスに役立てることができます。
- コンプライアンスのサマリーを監視する:インターネット セキュリティ センター (CIS) および国立標準技術研究所 (NIST) のフレームワークごとにグループ化された、過去12か月までのセキュリティチェックの変更履歴を表示します。
- セキュリティチェックをプロアクティブに実施:特定のベストプラクティス チェックに合格しないコミットをブロックすることで、最適でない構成に対するプロアクティブな対策を実施します。
- ポリシーアナライザー:特定のポリシールールの統合や削除の可能性を解析し、提案することで、お客様の意図するセキュリティ体制を満たすことができます。また、ルールベース内のシャドー、冗長、一般化、相関、統合などの異常をチェックすることもできます。

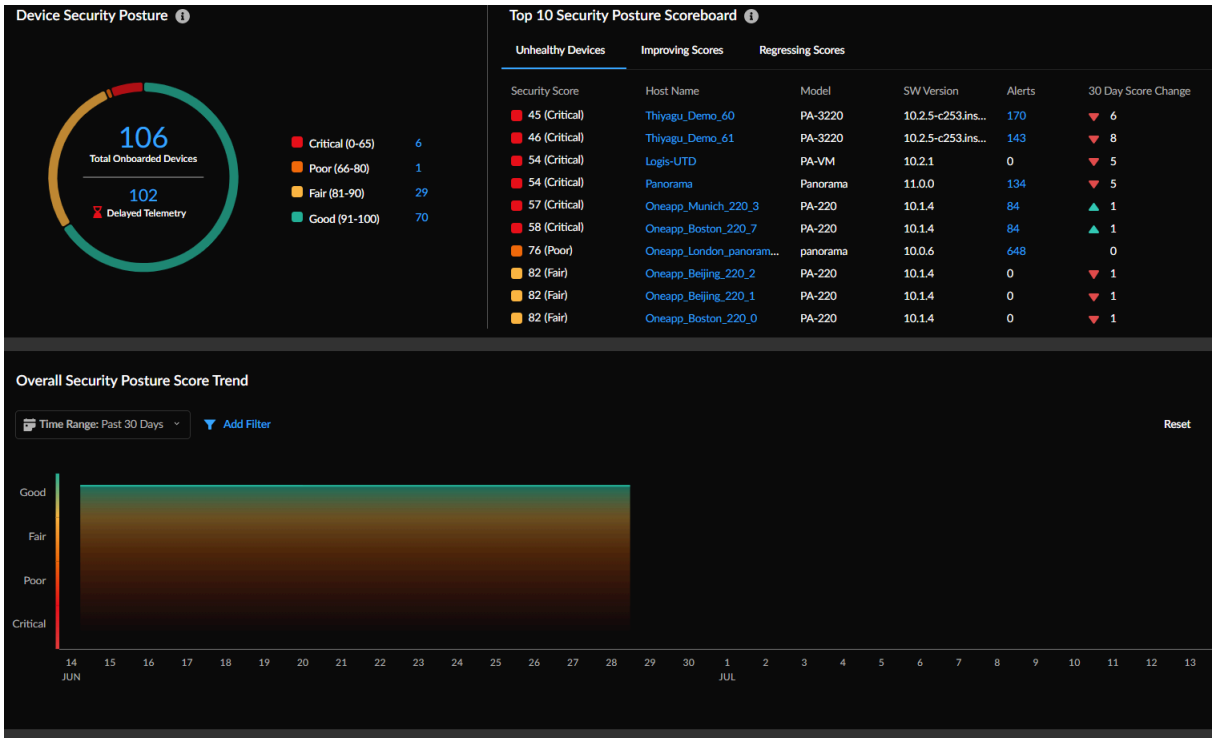
セキュリティ体制インサイトを監視する

どこで使用できますか?	何が必要ですか?

• Software NGFW Creditsによって資金提供されたものを含む	• 次のいずれか
	  ❑ または
	  ❑ または
	• ダッシュボードを表示する権限を持つロール

[Security Posture Insights (セキュリティ体制インサイト)] ダッシュボードを使用すると、オンボードのNGFWデバイスのセキュリティ体制に基づいて、展開のセキュリティ ステータスと傾向を可視化できます。セキュリティスコアの重大度（0～100）と、それに対応するセキュリティグレード（良好、普通、不良、重大）によって、デバイスのセキュリティ体制が決定されます。セキュリティスコアは、未解決のアラートの優先度、数量、種類、ステータスに基づいて計算されます。

1. **[Dashboards (ダッシュボード)]** > **[Security Posture Insights (セキュリティ体制インサイト)]**に移動して、作業を開始します。

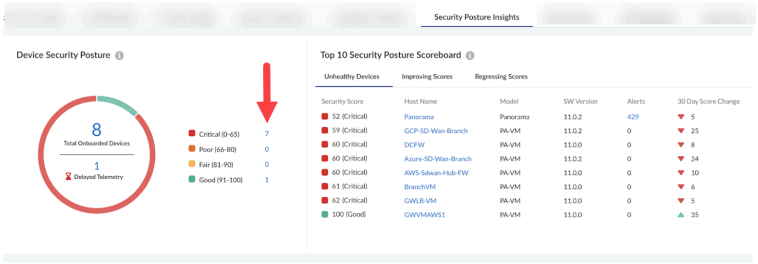


 ©2025 Palo Alto Networks, Inc.

2. **[Device Security Posture (**デバイスのセキュリティ体制**)]**を使用してデバイスの正常性を表示します。次のものを表示できます。

   - オンボードNGFWの総数。
   - 12時間以上テレメトリデータを送信していないデバイスの数。
   - 配置内のオンボードデバイスのセキュリティスコアの優先順位。番号リンクをクリックすると、デバイスの詳細とセキュリティ統計を知ることができます。

   たとえば、すべてのデバイスについて7つの重大なリスクを表示できます。



   この場合、重要なアラートをクリックすると、アラートを生成したデバイスを確認できます。さらに掘り下げると、ファイアウォールで「ユーザー資格情報の保護」が有効になっていないことがわかります。すべてのデバイスでこの問題に対処することで、フィッシング攻撃を回避できます。

3. 過去30日間で最も不健全で退行しているセキュリティスコアのデバイスを確認します。デバイスの動作ステータス、ソフトウェアのバージョン、その他の重要なメトリックなど、デバイスの正常性を表示できます。

   また、一部のデバイスが古いソフトウェアバージョンを実行しているかどうかも確認できます。この場合、最新の推奨バージョンへのアップグレードを計画できます。最新の推奨バージョンは、「アップグレード推奨事項」で確認できます。

4. 選択した期間におけるデプロイメントのセキュリティ体制の傾向を確認します。トリガーポイントにカーソルを合わせると、セキュリティ体制の傾向に貢献しているデバイスとアクティブなアラートを確認できます。ホスト名、モデル、またはソフトウェアバージョンでフィルタリングされた1つ以上のデバイスの傾向を表示できます。

詳細については、「ダッシュボード:セキュリティ体制インサイト」をご確認ください。

 ©2025 Palo Alto Networks, Inc.

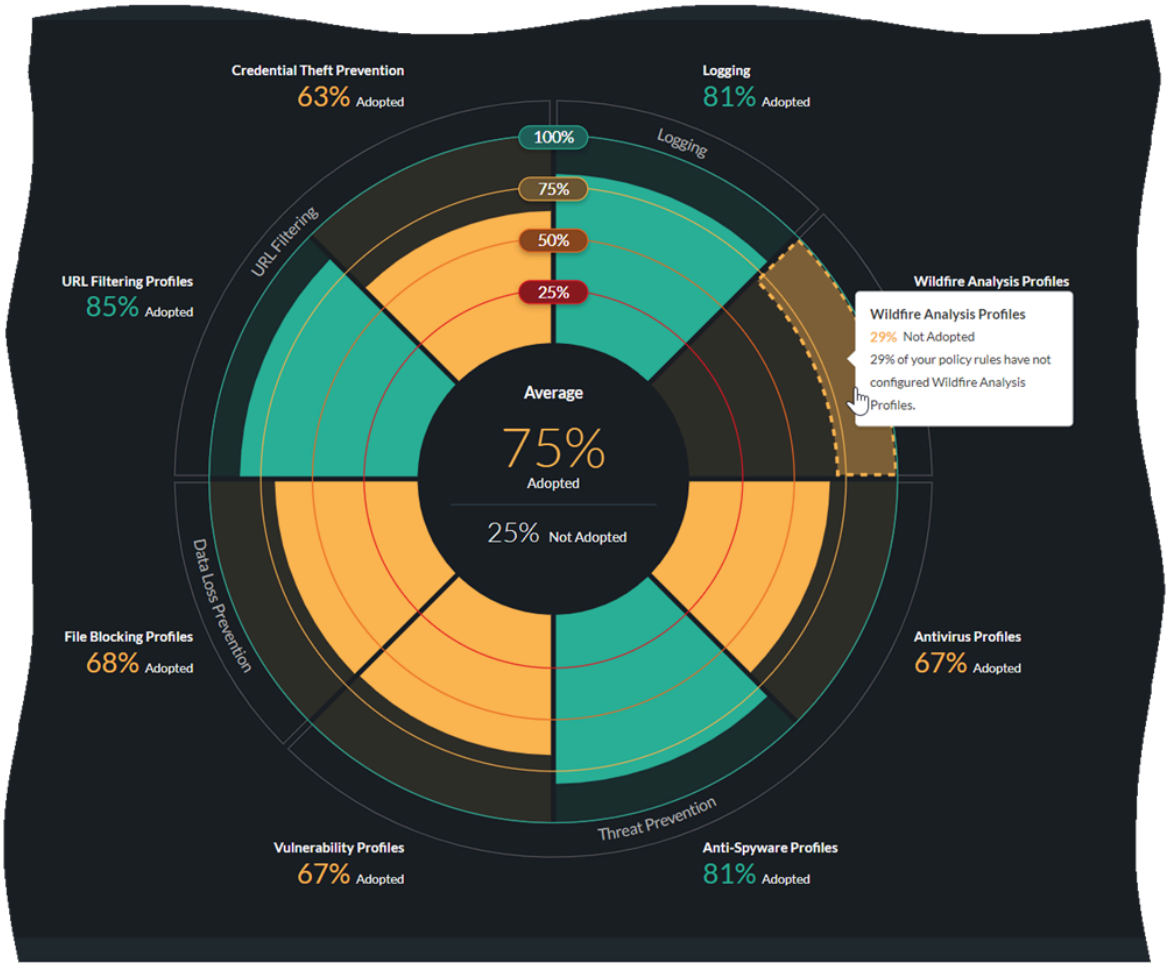
モニタ機能の導入状況

[Dashboards (ダッシュボード)] > [Feature Adoption (機能の導入状況)]

どこで使用できますか?	何が必要ですか?

• Software NGFW Creditsによって資金提供されたものを含む	• 次のいずれか
	  ◻ または
	  ◻ または
	• ダッシュボードを表示する権限を持つロール

では、デプロイメントで使用しているセキュリティ機能を確認できます。これにより、Palo Alto Networksのセキュリティ サブスクリプションとファイアウォール機能を最大限に活用することができます。



このダッシュボードは、ユーザーのセキュリティポリシーがどの点で強いが、どこにセキュリティポリシー機能適用のギャップがあるか—したがって改善の努力をすべきかを示してくれま

©2025 Palo Alto Networks, Inc.

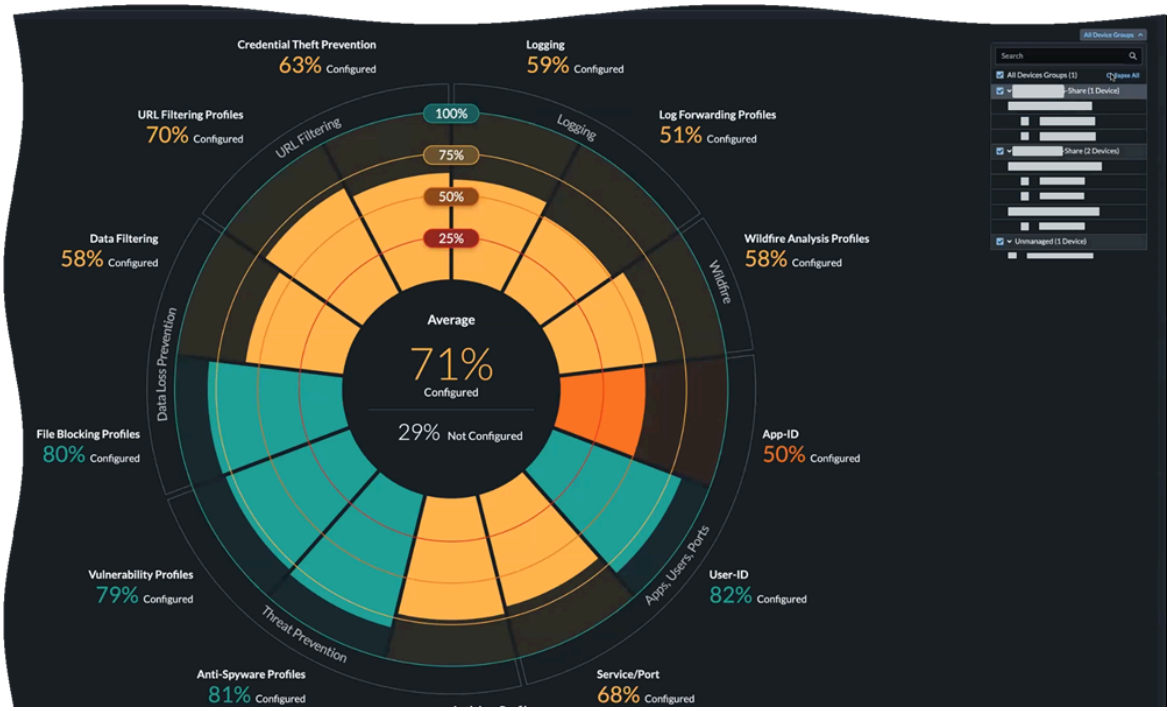
す。トラフィックの可視性を最大化し攻撃に対する最大の保護を実現するには、セキュリティ機能適用の目標を設定し、ベストプラクティス ベースラインとして以下の推奨事項を適用します。ベースラインに照らして現在の姿勢を評価し、セキュリティポリシー機能の採用のギャップを特定します。

導入状況の概要は、セキュリティポリシー機能の採用を改善できるデバイス、ゾーン、および領域を特定するのに役立ちます。適用情報は、Device Group（デバイスグループ）、Serial Number & Vsys（シリアル番号とVSYS）、Zones（ゾーン）、Areas of Architecture（アーキテクチャのエリア）、Tags（タグ）、Rule Details（ルール詳細）、およびZone Mappings（ゾーンマッピング）別に確認できます。デバイスグループでフィルタリングして範囲を狭め、ギャップを特定します。

[Feature Adoption (機能の導入状況**)]**では、**[Best Practices (**ベストプラクティス**)]**を選択することで、

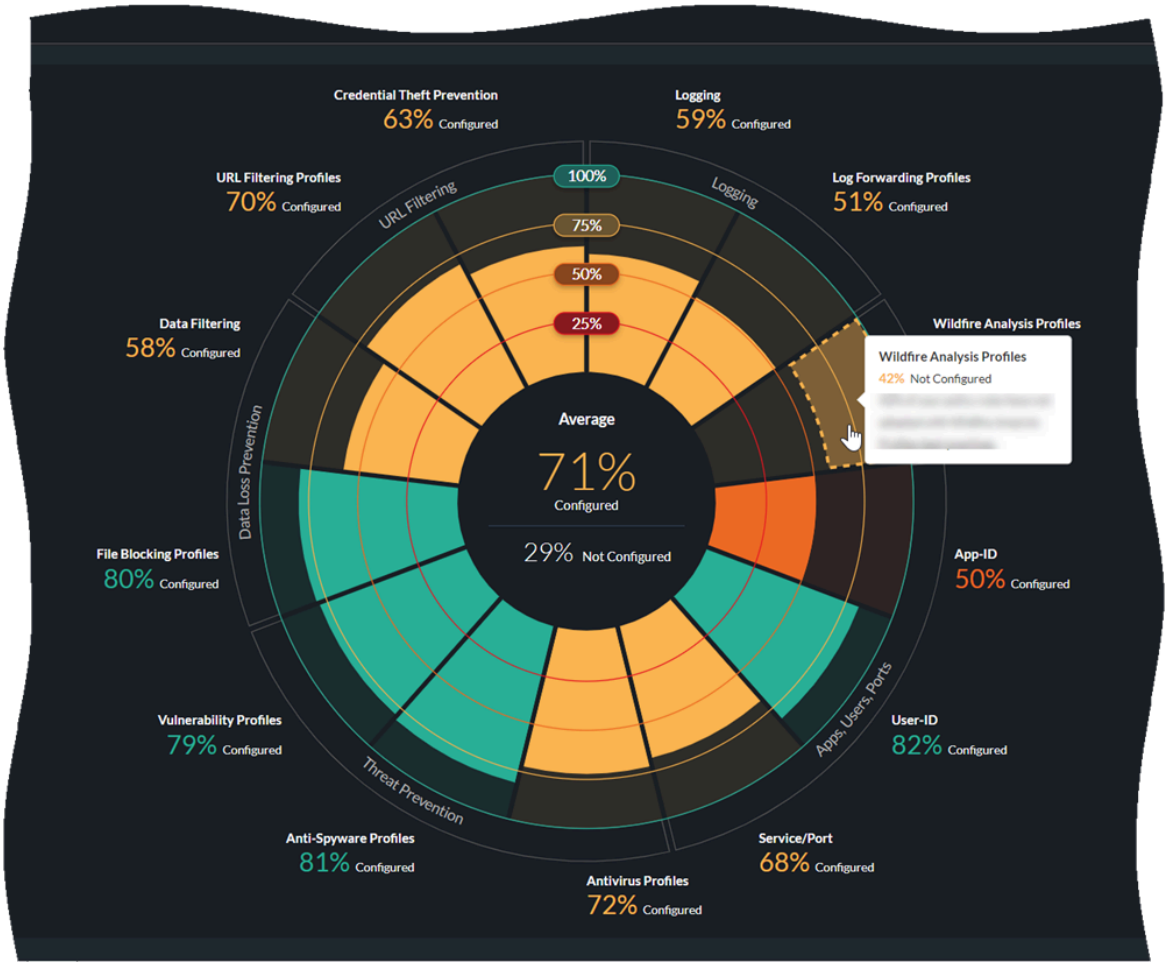
セキュリティ機能がPalo Alto Networksのベストプラクティスに従って設定されているかどうかも表示できます。

特定のファイアウォールセットのベストプラクティスへの準拠に焦点を当てるために、デバイスグループに基づいてチャートをフィルタリングできます。



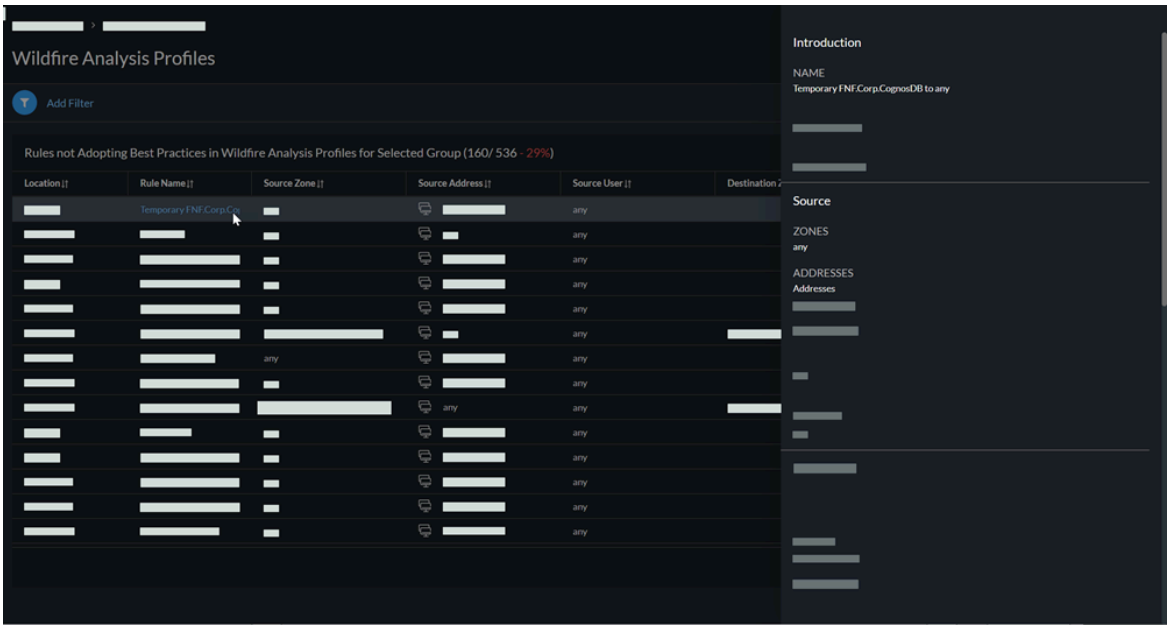
 ©2025 Palo Alto Networks, Inc.

チャート上の機能のセクションを選択すると、どのポリシー規則を改善できるかが表示されます。



©2025 Palo Alto Networks, Inc.

ルールを選択すると、アプリを終了せずにルールの詳細を表示できます。



詳細については、「ダッシュボード:機能の導入状況」を確認してください。

©2025 Palo Alto Networks, Inc.

セキュリティサブスクリプションの監視

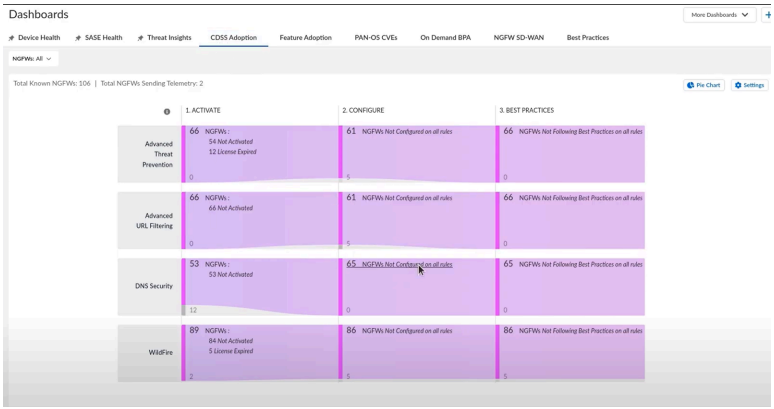
どこで使用できますか?	何が必要ですか?

• Software NGFW Creditsによって資金提供されたものを含む	• 次のいずれか
	  ❑ または
	  ❑ または
	• ダッシュボードを表示する権限を持つロール

[Dashboard (ダッシュボード)] > **[Posture (体制)]** > **[CDSS Adoption (CDSS導入状況)]**では、推奨されるクラウド配信セキュリティサービス（CDSS）サブスクリプションと、デバイスでのその使用状況を確認できます。これにより、セキュリティギャップを特定し、企業のセキュリティ体制を強化するのに役立ちます。このページに移動すると、NGFWでゾーンの役割を確認または更新するように求めるポップアップが表示され、セキュリティサービスの推奨事項を正確に取得できます。このポップアップウィンドウのリンクをたどると、ゾーンをロールにマップできます。

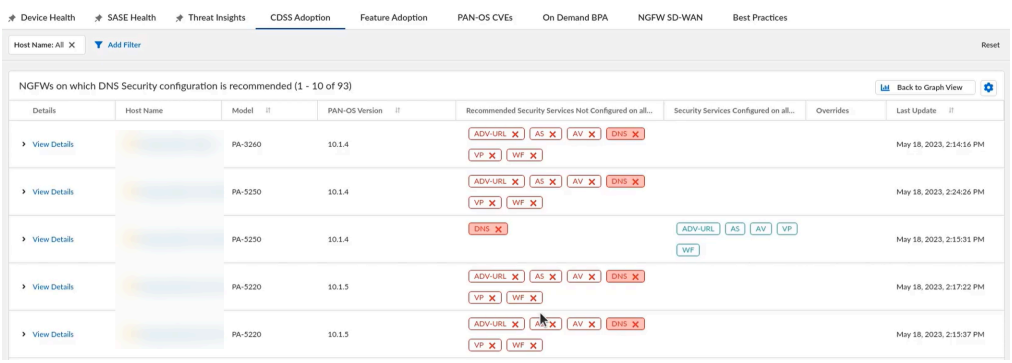
現在、このダッシュボードは、次の4つのセキュリティサブスクリプションのみをサポートしています。高度な脅威防御、高度な*URL*フィルタリング、*DNS*セキュリティ、*Wildfire*。

1. **CDSS Adoption (CDSS**の導入状況**)**ページの上部に、既知のNGFWの総数と、インスタンスでテレメトリを送信しているNGFWの数が表示されます。
2. CDSSの導入は、アクティベーション、設定、ベストプラクティスの遵守を通じて進行します。各サブスクリプションの進捗状況を追跡するには、グラフの数字をクリックするだけで、このプロセスでアップデートが必要なデバイスのリストが表示されます。この場合、DNSセキュリティが設定されていないNGFWを確認してみましょう。



 ©2025 Palo Alto Networks, Inc.

3. DNSセキュリティ設定が推奨されているが、設定されていないNGFWをチェックします。詳細を表示して、コピー元ロールとコピー先ロールを確認します。

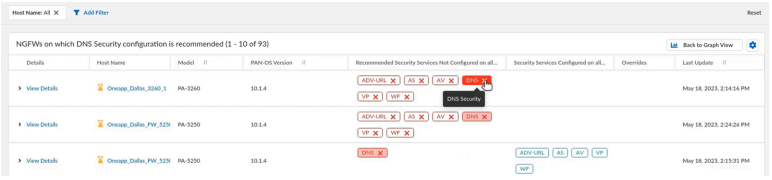


4. ［**View Policies (**ポリシーの表示**)**］をクリックすると、ルールの詳細と対応するソースおよび宛先ゾーンが表示されます。

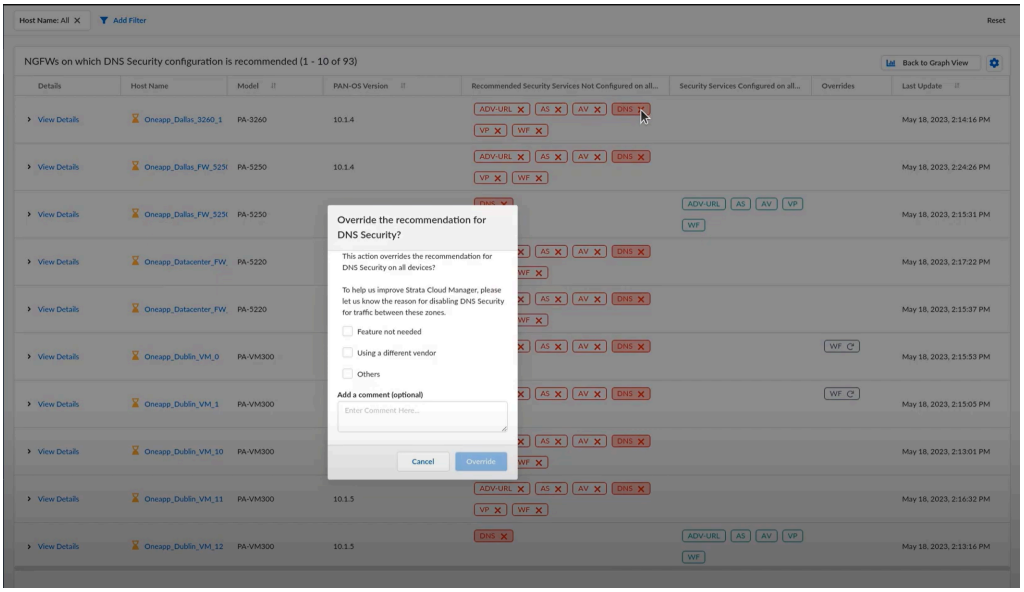
   さらに、ルール名をクリックすると、その詳細を表示できます。

5. ファネルグラフに戻ります。同じ情報を円グラフ形式でも表示できます。

6. 何らかの理由で推奨されるセキュリティサービスが必要ない場合は、それを上書きできます。この場合、DNSセキュリティサービスは必要ありません。**DNS**の横にあるキャンセルアイコンをクリックします。



7. 推奨事項を上書きする理由を1つ選択します。



©2025 Palo Alto Networks, Inc.

8. **[Override (オーバーライド)]**をクリックします。

以上、推奨するCDSSサブスクリプションの表示方法と、お使いのデバイスでの使用状況について説明しました。

詳細については、「ダッシュボード:CDSSの導入状況」をご確認ください。

©2025 Palo Alto Networks, Inc.

脆弱性の評価

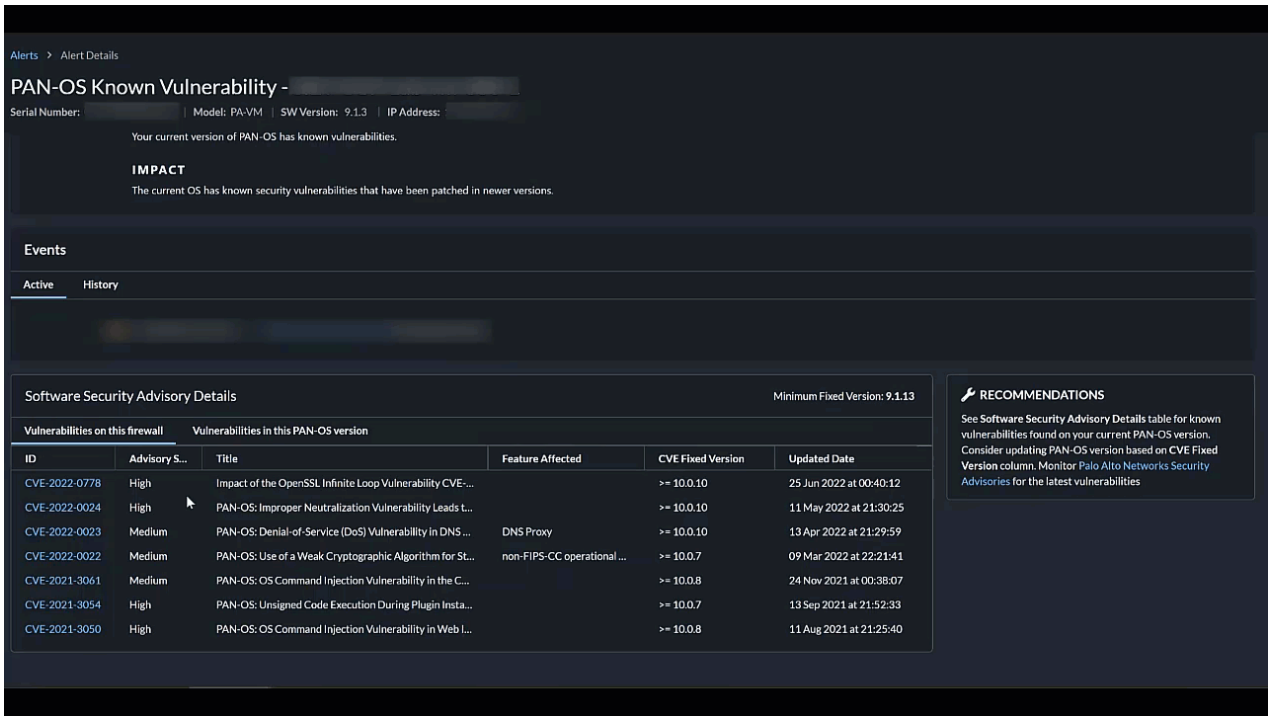
どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	次のいずれか ❑ または ❑ または

Strata Cloud Managerは特定のファイアウォールと PAN-OS バージョンに影響を与える脆弱性を示し、アップグレードする必要があるかどうかの判断に役立てることができます。**[Incidents & Alerts (**インシデント&アラート**)]** > **[NGFW]** > **[All Alerts (**すべてのアラート**)]**に移動します 。**[PAN-OS Known Vulnerability (PAN-OS** の既知の脆弱性**)]** アラートを選択し、アラートを発生させたファイアウォールに影響する最新のセキュリティ勧告を確認します。

[Vulnerabilities in this PAN-OS version (この**PAN-OS**バージョンの脆弱性**)]**を選び、**[Feature Affected (**影響を受ける機能**)]**コラムの脆弱性の影響を受ける機能を表示します。これにより、脆弱性と有効な機能への影響に基づいてファイアウォールをアップグレードするかどうかを決定できます。CVE がフィーチャに関連付けられていない場合、 **Feature Affected (**影響を受ける機能**)**は空白です。このタイプのCVEは、指定されたモデルまたはバージョンのファイアウォールに影響を与えます。

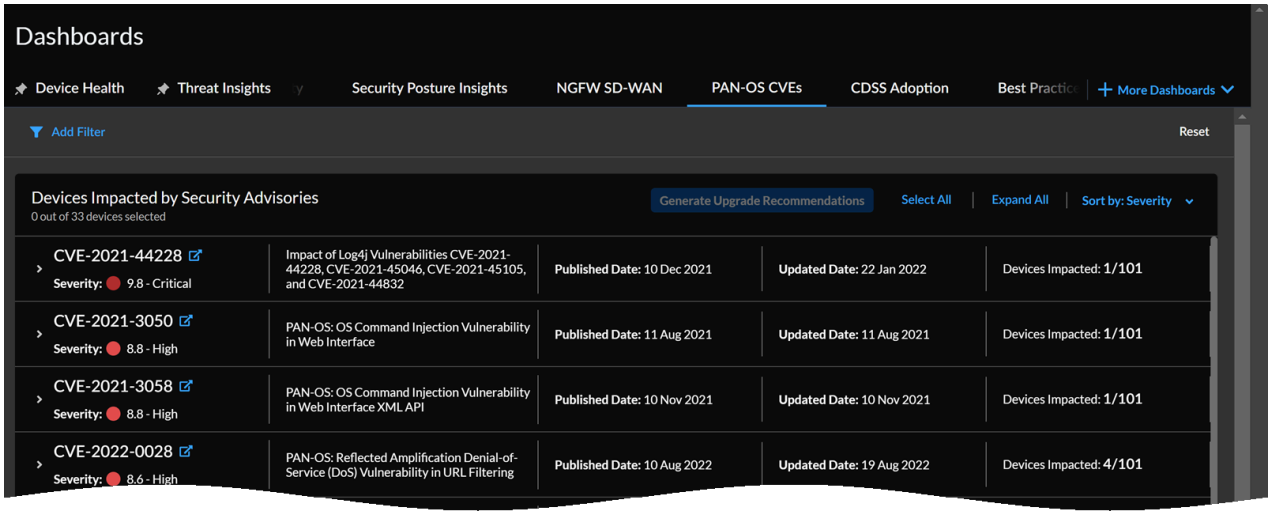
デフォルトでは、 **PAN-OS Known Vulnerability (PAN-OS** の既知の脆弱性**)** アラートは、デバイス上のPAN-OSバージョンのすべての脆弱性を表示します。ただし、 ファイアウォール上での製品使用状況テレメトリを実行した場合、特定のファイアウォールに影響する脆弱性のみを、その有効な機能に基づいて表示することを選択できます。これにより、ファイアウォールにとって懸念事項となる脆弱性をよりよく理解し、アップグレードするかどうかについてより多くの情報に基づいた決定を下すことができます。

©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

また、**PAN-OS CVE**ダッシュボードを使用すると、デバイスで有効になっている機能に基づいて、特定の脆弱性の影響を受けるデバイスの数を表示できます。Strata Cloud Managerは、有効になっている機能を分析して、CVEの影響を受けるデバイスを特定します。次のタスクでは、デバイスに影響を与える脆弱性を評価し、脆弱性を修正するためのアップグレードの推奨事項を生成する方法を示します。



このタスクでは、デバイスに影響を与える脆弱性を評価し、脆弱性を修正するためのアップグレードの推奨事項を生成する方法を示します。

STEP 1 | Strata Cloud Managerから、 **[Dashboards (ダッシュボード)]** > **[PAN-OS CVE]**を選択します。

STEP 2 | CVEを展開して、その影響を受けるデバイスを表示します。

STEP 3 | 脆弱性を修正するためにアップグレードするデバイスを選択します。

STEP 4 | ソフトウェアアップグレードの推奨事項。

STEP 5 | デバイス用に新しく生成されたレポートをクリックします。

STEP 6 | アップグレード オプションのいずれかを選択して、詳細を表示します。 表示できる詳細は、**[New Features (新機能)]**、**PAN-OS Known Vulnerabilities (PAN-OS** の既知の脆弱性)、**Changes of Behavior (**振る舞いの変化)そして **PAN-OS Known Issues (PAN-OS** の既知の問題)が含まれます。

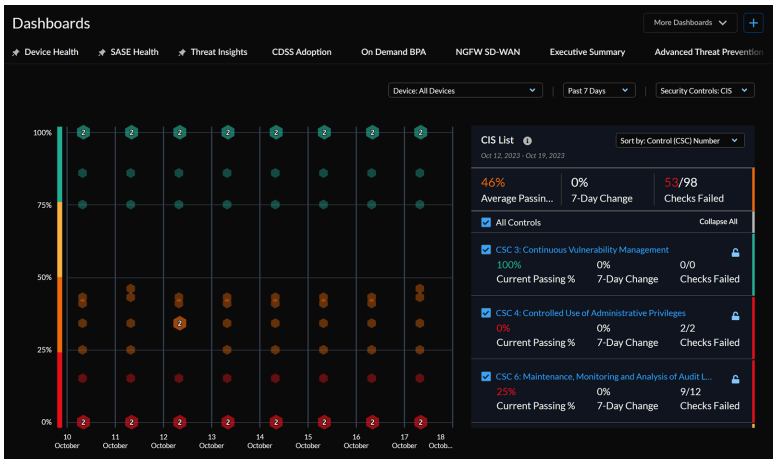
詳細をCSVファイルにエクスポートし、ダウンロードすることができます。

©2025 Palo Alto Networks, Inc.

コンプライアンスのサマリーを監視する

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	❑ または ❑ サポート対象製品のデータをダッシュボードに表示するライセンス:Prisma Access

[Compliance Summary Dashboard (コンプライアンス概要ダッシュボード)]にアクセスするには、**[Dashboards (ダッシュボード)]**に移動し、**[Compliance Summary (コンプライアンス概要)]**タブを選択します。インターネット セキュリティ センター (CIS) および 国立標準技術研究所 (NIST) のフレームワークごとにグループ化された、過去12か月までのセキュリティチェックの変更履歴を表示できます。各フレームワークごとに、コントロールのリストと、各コントロールの現在および平均順守率、ベストプラクティスチェックの合計数、失敗したチェックの数が表示されます。チャートとリストを操作し、コントロールとその履歴統計の関係を確認します。個々のコントロールとそれに関連するチェックの詳細を表示し、ベストプラクティスのチェックを選択すると、チェックで不合格となったファイアウォール構成が表示されます。**CIS**重要セキュリティコントロールフレームワークは、既知のサイバー攻撃ベクトルから組織とそのデータを保護するのに役立つ推奨処置とベストプラクティスの優先順位セットです。



CISコントロールの基本および基礎となる16種類のうち、11種類のチェック概要を表示できます。

- CSC 3:継続的な脆弱性管理
- CSC 4:管理者権限の制御された使用
- CSC 6:監査ログの保守、モニタリング、および分析
- CSC 7:メールと Web ブラウザの保護
- CSC 8:マルウェア防御
- CSC 9:ネットワーク ポート、プロトコル、およびサービスの制限と制御
- CSC 11:ファイアウォール、ルーター、スイッチなどネットワークデバイスの安全な設定

©2025 Palo Alto Networks, Inc.

- CSC 12:境界防御
- CSC 13:データ保護
- CSC 14:Need to Knowに基づいて制御されているアクセス
- CSC 16:アカウントのモニタリングと制御

NISTサイバーセキュリティフレームワーク **SP 800-53** コントロールのフレームワークは、連邦政府機関やその他の組織が情報システムのセキュリティとプライバシーの管理を実装し、維持管理するためのガイダンスです。NISTコントロールの8つのファミリーのチェック概要を表示できます。

- SCアクセス制御
- AU:監査と説明責任
- CM：設定の管理
- CP:緊急時対応計画
- IA:識別と認証
- RA:リスク アセスメント
- SCシステムと通信の保護
- SI:システムと情報の完全性

詳細については、「ダッシュボード:コンプライアンス概要」をご確認ください。

 ©2025 Palo Alto Networks, Inc.

セキュリティチェックをプロアクティブに実施

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	☐ または

デプロイメントのセキュリティ体制チェックをカスタマイズして、次の機能を使用して、関連する推奨事項を最大限に高めます。

- セキュリティチェック

  AIOps for NGFW が設定を評価するために使用するベストプラクティスチェックのリスト。ファイアウォールとPanoramaの構成をPalo Alto Networksのベストプラクティスチェックと比較し、デバイスのセキュリティ態勢を評価し、セキュリティ警告を生成します。設定を評価するために使用するベストプラクティスチェックのリストを確認できます。

  ここでは、次のことができます。

  1. 展開に最も重要なチェックを特定するために、チェックの重大度レベルを設定します。
  2. チェックを一時的に無効にします。

     チェックを無効にする場合は、無効のままにする期間を指定し、無効にする理由を説明するコメントを残すことができます。
  3. チェックに失敗したときのレスポンスを設定します。
- ゾーンとロールのマッピング

  カスタマイズされた推奨事項を取得するには、NGFW のゾーンをロールにマップします。
- ロールとセキュリティサービスのマッピング

  すべての NGFW のゾーンとロール間のトラフィックに必要なセキュリティサービスを管理します。

Panorama CloudConnectorプラグインは、特定のベストプラクティスチェックに合格しないコミットをブロックすることで、最適でない構成に対してプロアクティブな対策を講じることができます。AIOps for NGFWでコミットを失敗させるチェックを指定すると、Panoramaは自動的にそのチェッ クに合格しないコンフィギュレーションのコミットをブロックします。失敗したベストプラクティスチェックに関するアラートを受け取るのを待つのではなく、プラグインを使用して、構成の問題をそもそも導入環境から排除します。

STEP 1 | すべての前提条件を満たしていることを確認し、プラグインをインストールします。

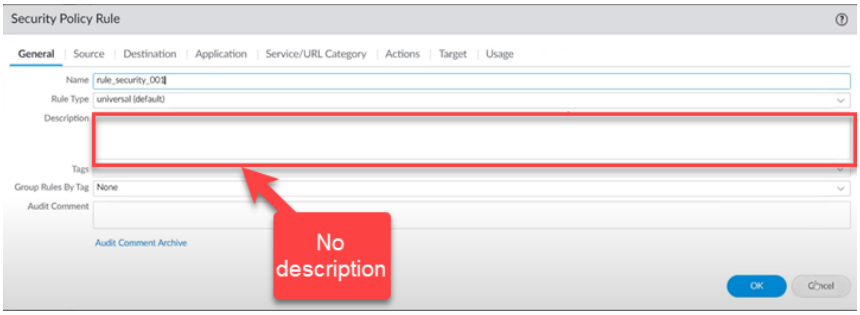
STEP 2 | 失敗時にコミットをブロックするベストプラクティスチェックを指定します。

1. **[Manage (管理)] > [Security Posture (セキュリティ体制)] > [Settings (設定)]**を選択します
2. コミットをブロックするチェックを見つけます。
3. **[Action on Fail (失敗時のアクション)]** を**[Fail Commit (コミット失敗)]**に設定します

©2025 Palo Alto Networks, Inc.

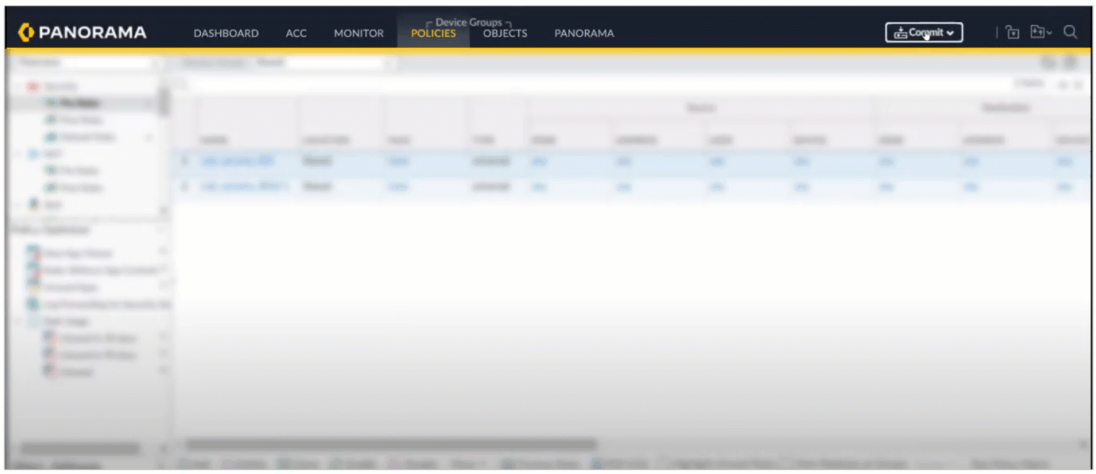
STEP 3 | チェックに合格しないコンフィギュレーションをコミットして確認します。

1. Panorama にログインします。
2. **[Fail Commit (コミット失敗)]**に指定したベストプラクティスチェックに違反します。



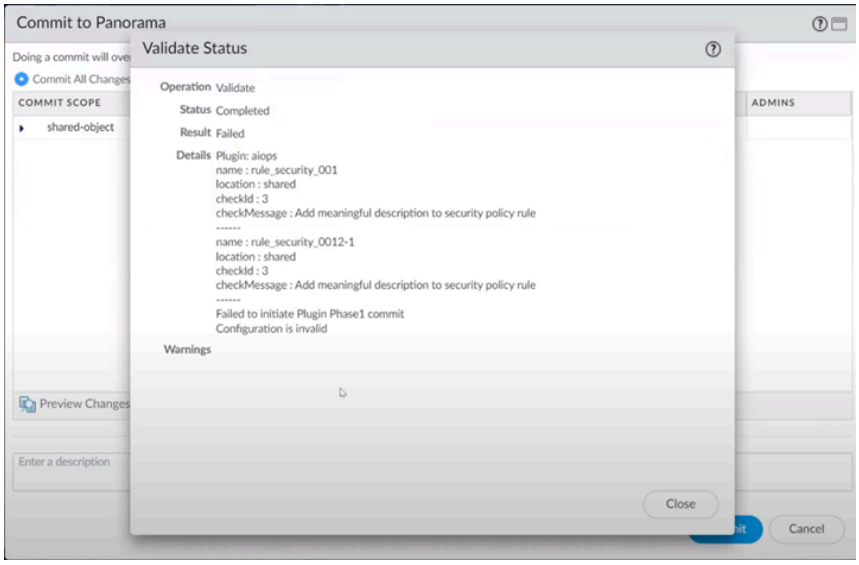
3. **[Commit (コミット)]** > **[Commit to Panorama (Panoramaにコミット)]** > **[Validate Configuration (設定の検証)]**を選択します。

©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

構成がベストプラクティスのチェックに合格しなかったために検証に失敗したことを示すダイアログが表示されます。



チェックを***[Fail Commit (***コミット失敗***)]***に設定すると、検証と実際のコミット操作の両方でチェックが失敗します。

詳細については、「管理:セキュリティ体制の設定」を参照してください。

 ©2025 Palo Alto Networks, Inc.

ポリシーアナライザー

どこで使用できますか?	何が必要ですか?
• NGFW (Panorama管理) • (Panorama管理) •	❑ または ❑ Panorama管理デプロイメント用Panorama CloudConnectorプラグイン

セキュリティポリシールールの更新は、時間的制約を伴うことが多く、迅速な対応が求められます。ただし、セキュリティポリシーのルールベースに対して行う更新は、要件に適合し、エラーや設定ミス（ルールの重複や矛盾を招くような変更）が発生しないようにする必要があります。

Strata Cloud Managerのポリシーアナライザーを使用すると、変更要求を実装するときに時間とリソースを最適化できます。Policy Analyzer (ポリシーアナライザー)は、特定のルールを分析して、意図に沿った統合や削除の可能性を提案するだけでなく、ルールベースのシャドウ、冗長性、汎化、相関、統合などの異常もチェックします。

ポリシーアナライザーを使用して、セキュリティポリシールールベースを追加または最適化します。

- 新しいルールを追加する前に：新しいルールを追加する必要があるかどうかを確認します。ポリシーアナライザーは、可能であれば別のルールを追加せずに、要件を満たすために既存のセキュリティポリシールールを変更する最善の方法を推奨します。
- 既存のルールベースの合理化と最適化：肥大化を最小限に抑え、競合を排除するために、また、トラフィックの実施がセキュリティポリシーのルールベースの意図と一致するように、ルールをアップデートできる場所を確認できます。

変更をコミットする前と後の両方でセキュリティポリシールールを分析します。

- 変更前ポリシー分析：新しいルールの影響を評価し、既存のルールに対して新しいルールの意図を分析して、その意図に最も適合する方法を推奨できます。
- 変更後ポリシー分析：時間の経過とともに蓄積されたシャドウ、冗長性、およびその他の異常を特定することで、既存のルールベースをクリーンアップできます。

- *Policy Analyzer (ポリシーアナライザー)*を使用するには、*Panorama*アプライアンスにCloudConnectorプラグイン*1.1.0*以降が必要です。コマンドを使ってこのプラグインを有効にする必要があります。

  ```
  > request plugins cloudconnector enable basic
  ```

- *Policy Analyzer(ポリシーアナライザー)*は、*Panorama*を*PAN-OS*バージョン*10.2.3*以降にアップデートする必要があります。

Policy Analyzer (ポリシーアナライザー)が検出する異常の種類

Policy Analyzer (ポリシーアナライザー)は、セキュリティポリシールールベース全体で次のタイプの異常を検出します。

©2025 Palo Alto Networks, Inc.

- シャドウ：ルールベースの上位のルールが同じトラフィックをカバーするため、ヒットしないルール。

  セキュリティ ポリシー ルールは、ルール ベースの上位にあるルールが、下位にあるルールが一致する同じトラフィックと一致し、ルールが別のアクションで設定されている場合にシャドウが作成されるように、ルール・ベース内で上から下に向かって評価されます。下位のルールを順番に削除しても、セキュリティポリシーは変更されません。
- 冗長性：同じトラフィックに一致し、同じアクションで設定されている複数のルール。
- 汎化：ルールベースの下位にあるルールが、ルールベースの上位にあるルールのトラフィックと一致するが、その逆ではない場合。ルールが異なるアクションを実行する。2つのポリシー規則の順序が逆の場合、セキュリティポリシーに影響します。
- 相関：一方のルールが他方のルールの一部のパケットに一致するが、結果として異なるアクションが発生する場合に、別のルールと相関するルール。2つの規則の順序が逆の場合、セキュリティ ポリシーに影響します。
- 統合：アクションは同じで、1つのアトリビュートだけが異なるため、1つのルールに統合できるルール。いずれかのルールの属性を変更し、他のルールを削除することで、ルールを1つのルールにマージできます。

変更前のポリシー分析

どこで使用できますか?	何が必要ですか?
• NGFW (Panorama管理) • (Panorama管理) •	❑ または ❑ Panorama管理デプロイメント用Panorama CloudConnectorプラグイン

セキュリティポリシールールの変更前分析では、新しい意図満足度分析が実行されます。

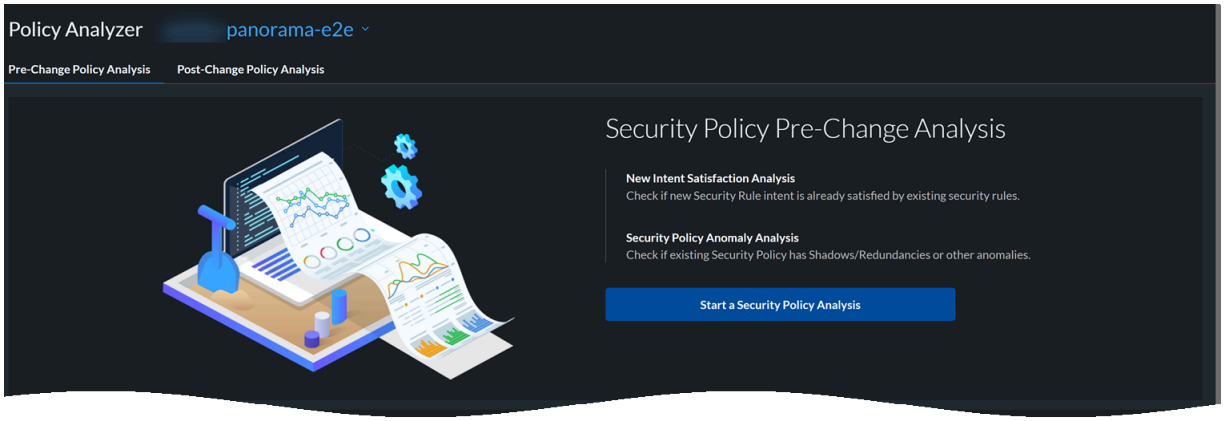
- 新しいインテント満足度分析：新しいセキュリティ ポリシー ルールの意図がすでに既存のルールでカバーされているかどうかをチェックします。

開始する前に：

1. **[Manage (管理)]** > **[Security Posture (セキュリティ体制)]** > **[Policy Analyzer (ポリシーアナライザー)]** > **[Pre-change Policy Analysis (変更前のポリシー分析)]**に順に移動します。

©2025 Palo Alto Networks, Inc.

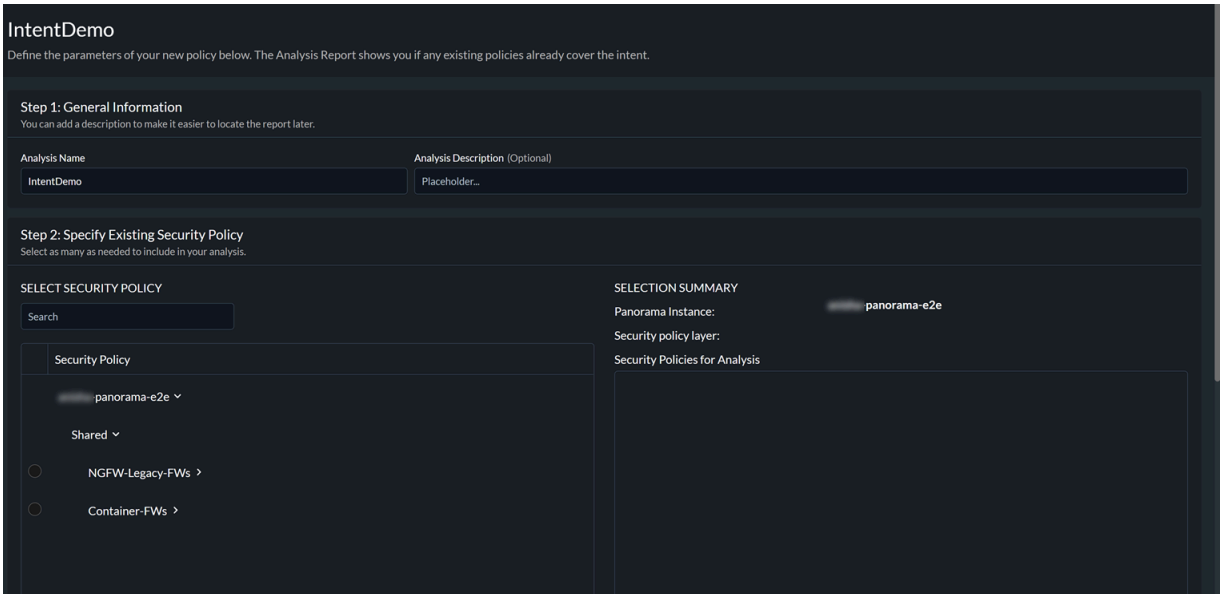
2. [Policy Analyzer (ポリシーアナライザ)]ページの最上部で、分析する必要があるポリシー規則を含むパノラマインスタンスを選択します。



3. セキュリティポリシー分析を開始します。

新しい分析を開始するには、次の手順を実行します。

STEP 1 | 「**Analysis Name (解析名)**」と「**Analysis Description (解析の説明)**」を入力します。



Panoramaアプライアンスでは、デバイスグループは階層構造になっています。作成できるデバイスグループには4つのレベルがあり、階層の最下位のデバイスグループにNGFWを割り当てます。上位レベルで作成したポリシーは、その下位のすべてのデバイスグループに継承されます。

NGFWが直接割り当てられた最大10個のデバイス グループに対して分析を実行できます。これにより、直接割り当てられたNGFWのセットにプッシュされるすべてのポリシー規則を分析できます。

STEP 2 | 分析する既存のセキュリティポリシーセットを選択します。

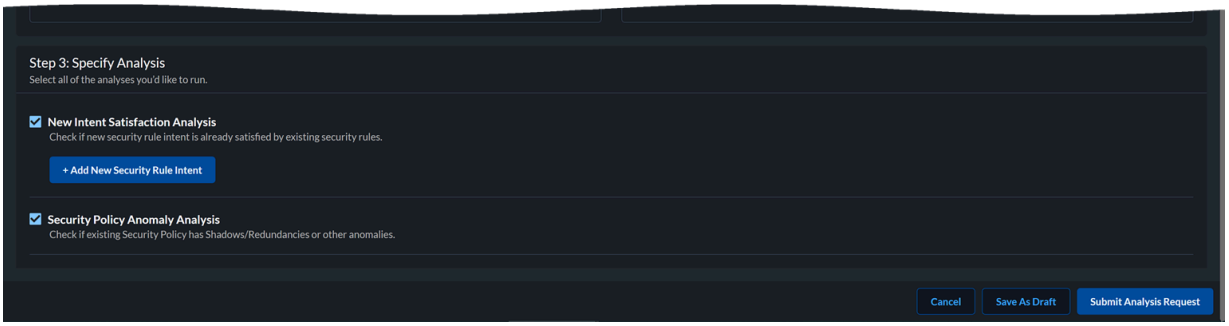
分析ごとに最大10個のデバイスグループを選択できます。

©2025 Palo Alto Networks, Inc.

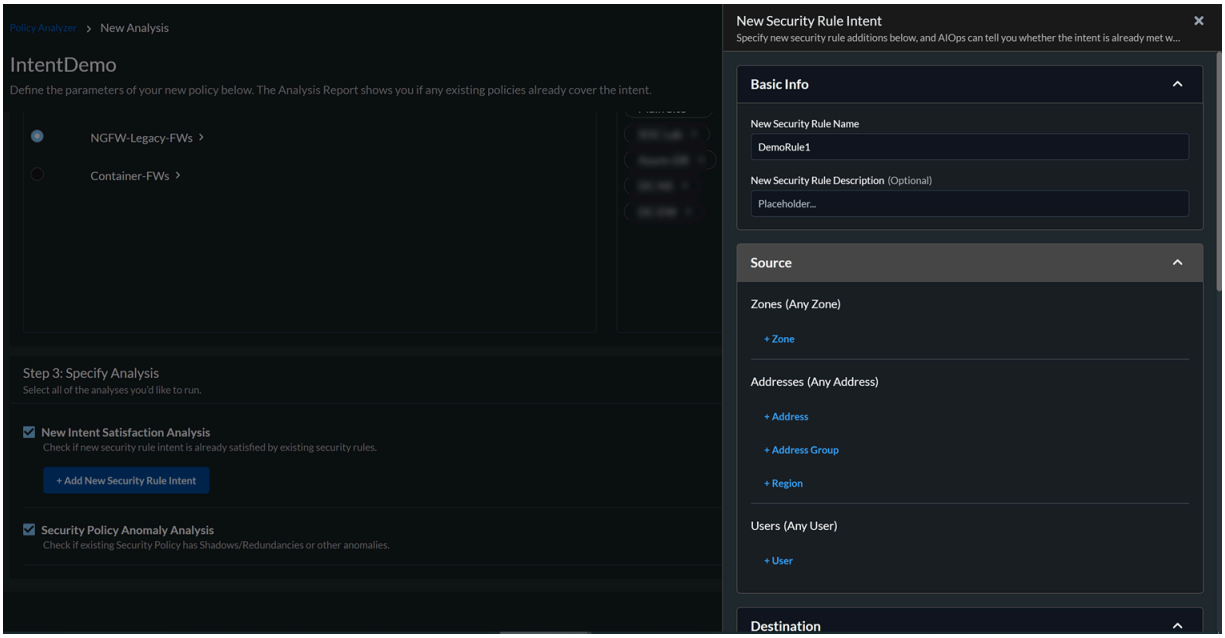
STEP 3 | 1つ以上の分析タイプを選択して、分析タイプを指定します。

- 新しいインテント満足度分析

分析用に新しいセキュリティルールインテントを追加します。



新しいセキュリティルールに関する情報を指定します。AIOps for NGFWは、既存のルールがその意図をカバーしているかどうかを確認できます。

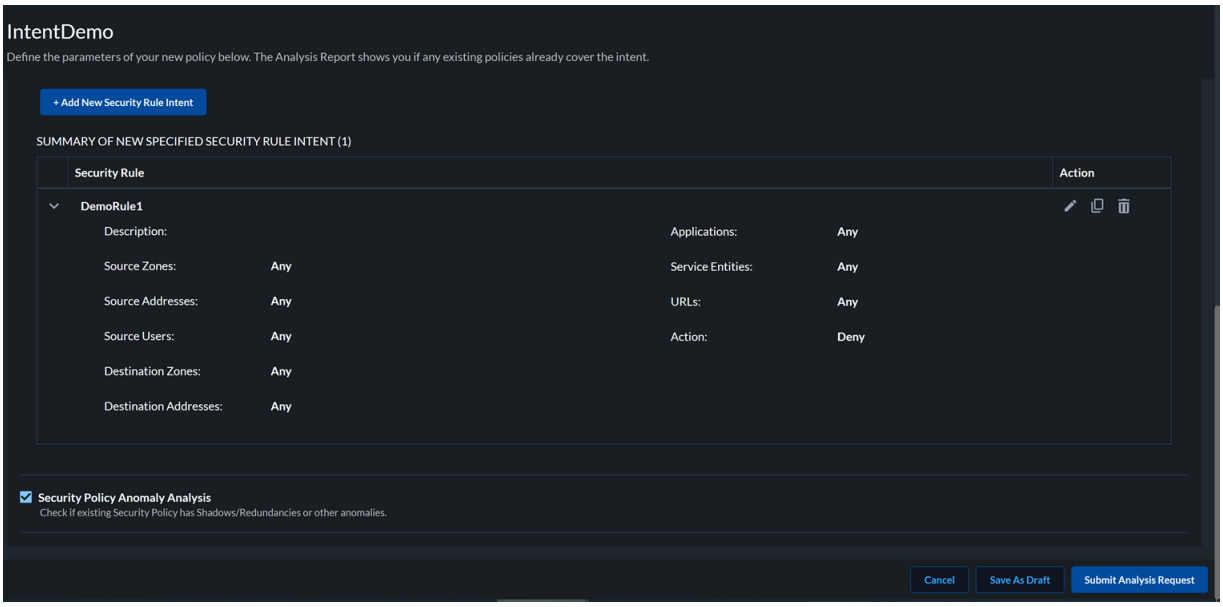


セキュリティポリシー規則のコンポーネントの値を入力します。。セキュリティ規則に関連するフィールドのデフォルト値は「任意」です。

設定を保存します。

新しいセキュリティルールの意図の概要を確認します。

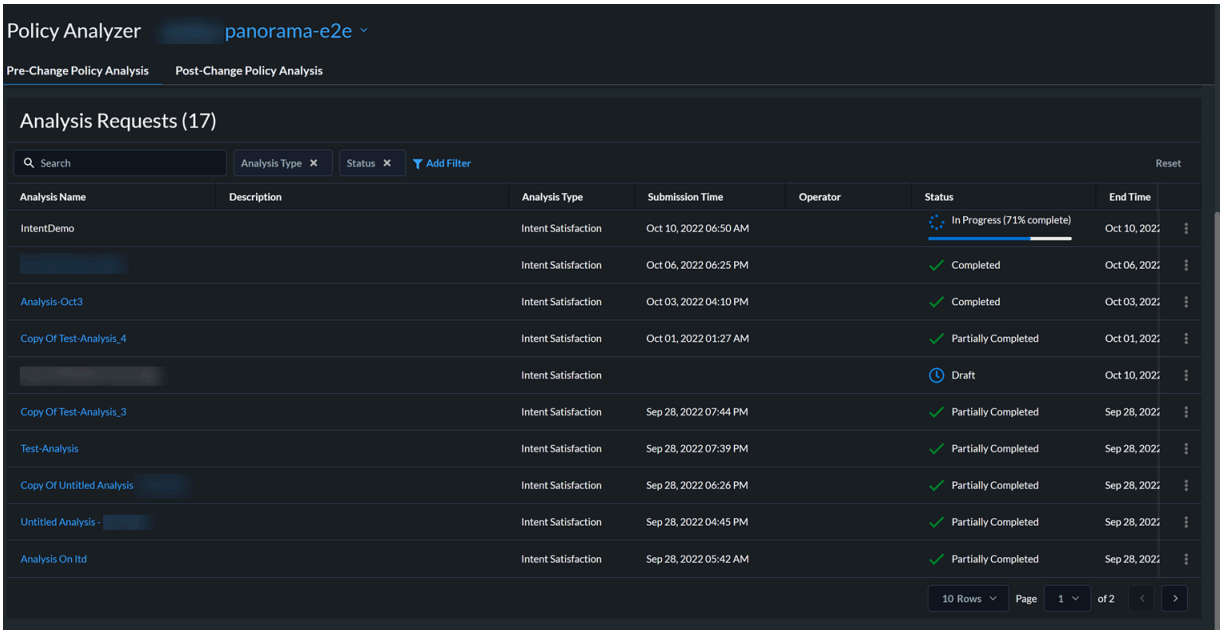
 ©2025 Palo Alto Networks, Inc.



新しいセキュリティルールは10個まで作成できます。また、ルールをコピーして編集することもできます。

STEP 4 | **[Submit Analysis Request or Save As Draft (**分析リクエスト送信またはドラフトとして保存**)]**を選択して、後でルールを編集します。

[Policy Analyzer (ポリシーアナライザー)]ページの[Analysis Requests (分析リクエスト)]で分析のステータスを表示します。



ステータスが実行中であるルールをキャンセルできます。キャンセル済みと表示されます。

分析が完了したら、分析レポートを表示します。

 ©2025 Palo Alto Networks, Inc.

変更前のポリシー分析レポート

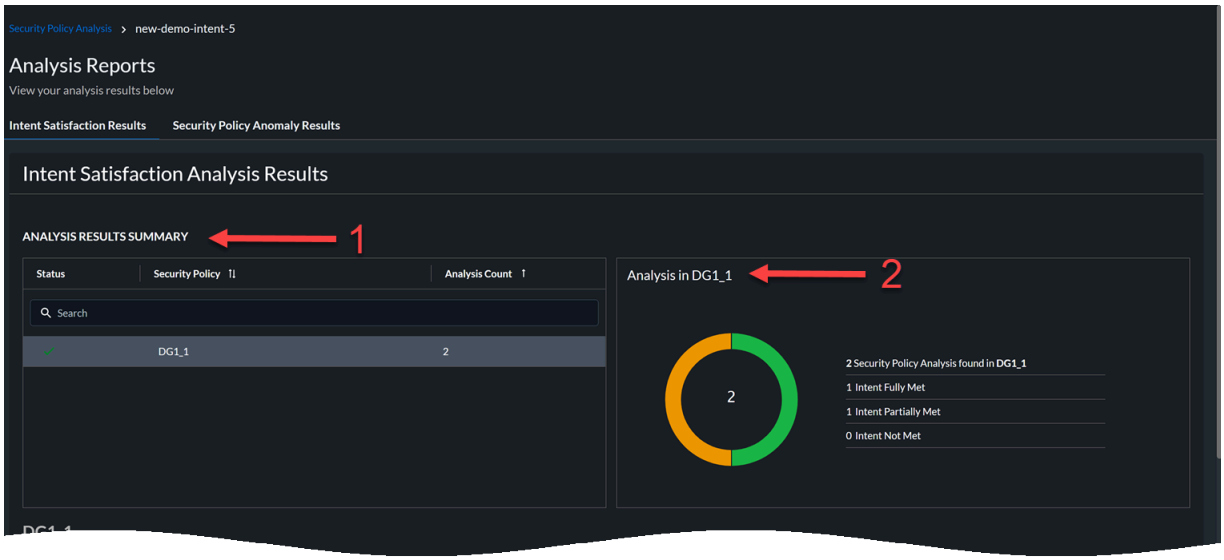
どこで使用できますか?	何が必要ですか?
• NGFW (Panorama管理) • (Panorama管理) •	❑ または ❑ Panorama管理デプロイメント用Panorama CloudConnectorプラグイン

ステータスが完了した分析レポートを選択すると、ポリシー分析の結果が表示されます。解析結果を表示できます。

インテント満足度の結果

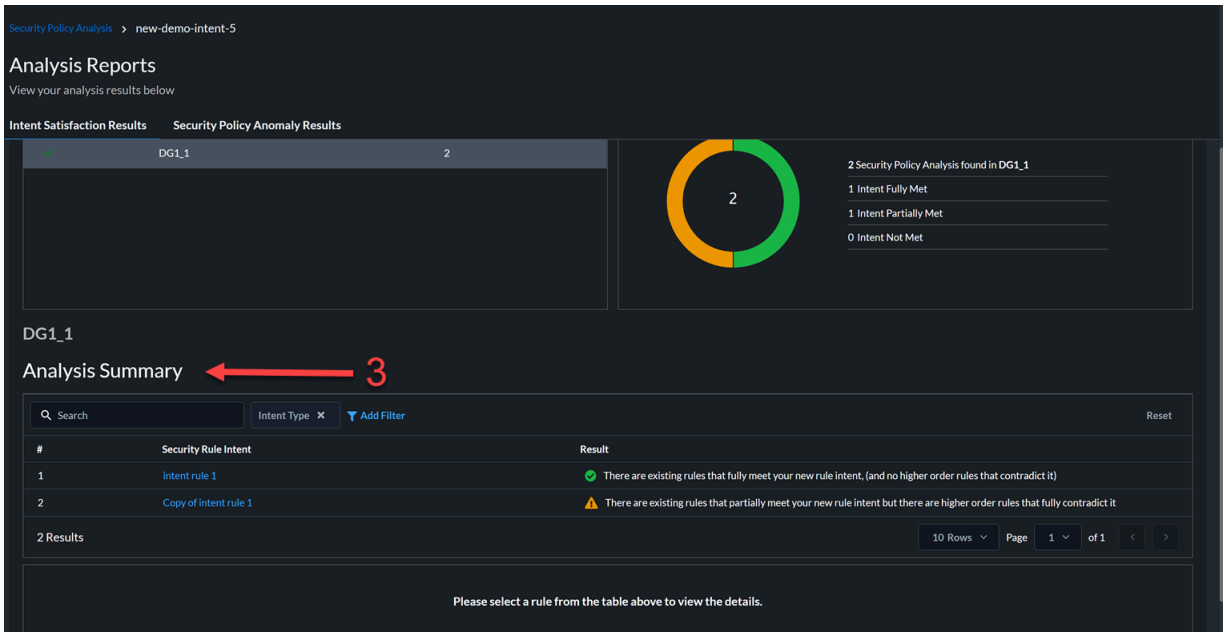
[Analysis Requests (分析リクエスト)]の下にある分析リストから、分析をクリックすると、分析結果が表示されます。これらの結果は次のとおりです。

1. デバイスグループと異常カウントに関する詳細を含む分析の概要。
2. デバイスグループの名前をクリックすると、意図満足度分析の結果が表示されます。
   - ［Intent Fully Met (意図を完全に満たす)］：セキュリティ規則がデバイス グループの既存の規則のいずれかと重複しています。
   - ［Intent Partially Met (意図を部分的に満たす)］：セキュリティ規則が、デバイス グループ内の既存の規則の1つの意図を部分的に満たしている。
   - [Intent not met (意図を満たしていない)]：セキュリティ規則は、デバイス グループには存在しない固有の規則です。このルールをデバイスグループに追加できます。



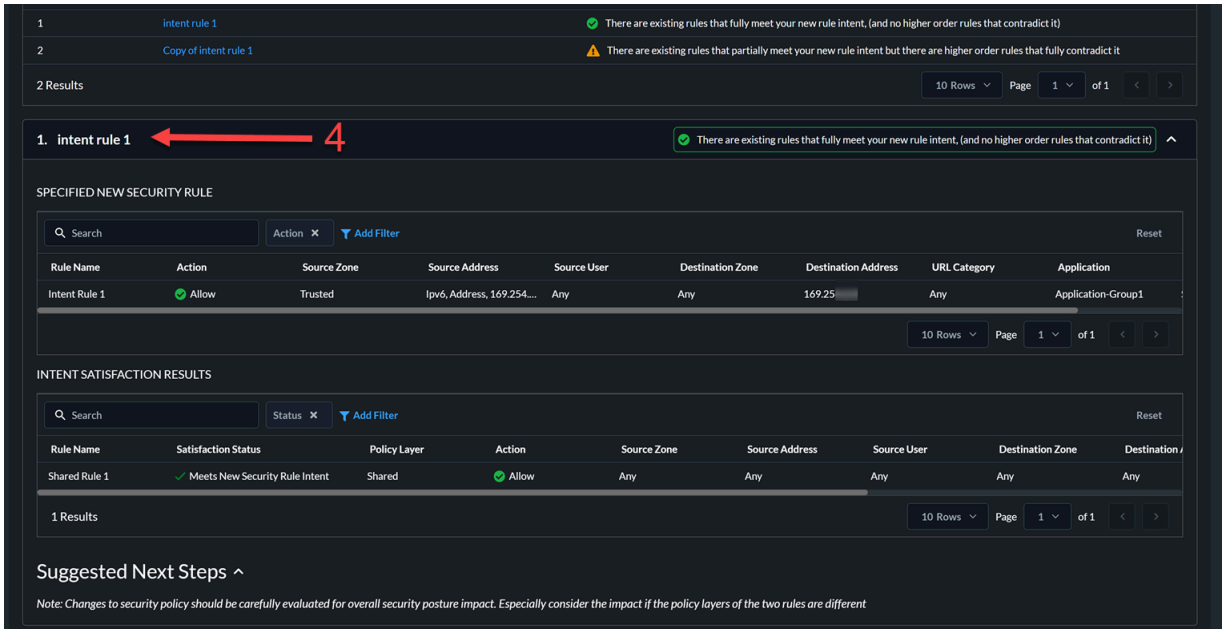
 ©2025 Palo Alto Networks, Inc.

3. 新しいセキュリティルールの意図に関する分析結果を表示します。



この例では、2つのルールがあります。最初のルールの意図は既存のルールと完全に一致し、2番目のルールの意図は既存のルールと部分的に一致します。

4. 新しいセキュリティルールの詳細を表示し、意図満足の結果を確認します。



この例では、新しいルールインテントルール1のすべての属性が、既存のルール共有ルール1の属性と一致します。新しいルールの意図は、既存のルールの意図と完全に一致します。したがって、この新しいルールを設定に追加する必要はありません。

 ©2025 Palo Alto Networks, Inc.

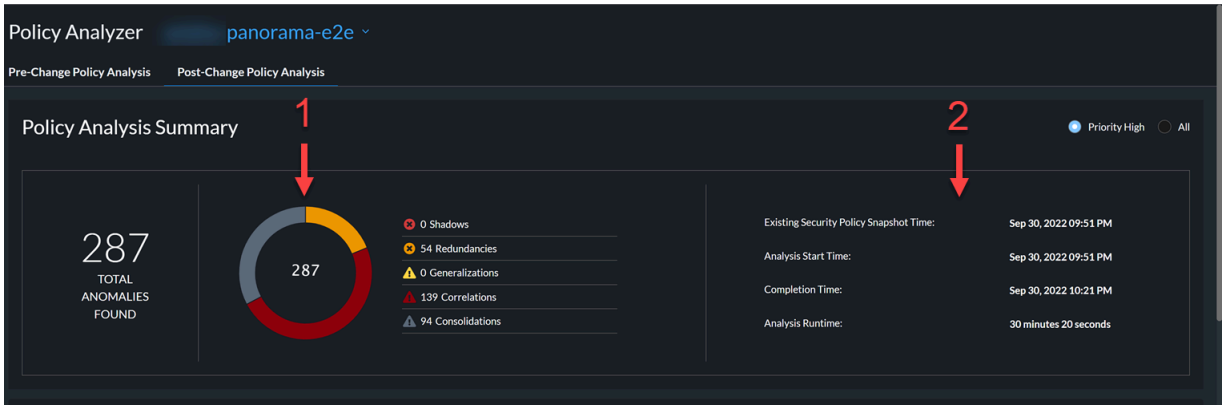
変更後のポリシー分析

どこで使用できますか?	何が必要ですか?
• NGFW (Panorama管理) • (Panorama管理) •	❑ または ❑ Panorama管理デプロイメント用Panorama CloudConnectorプラグイン

Panorama上で構成をコミットすると、プラグインを通じてStrata Cloud Managerに分析できるようになります。Policy Analyzerは、この設定をシャドウ、冗長性、その他の異常について分析します。その結果は、 **[Manage (管理)] > [Security Posture (セキュリティ体制)] > [Policy Analyzer (ポリシーアナライザー)] > [Post-change Policy Analysis (変更後のポリシー分析)]**で確認できます。

次の情報を表示できます。

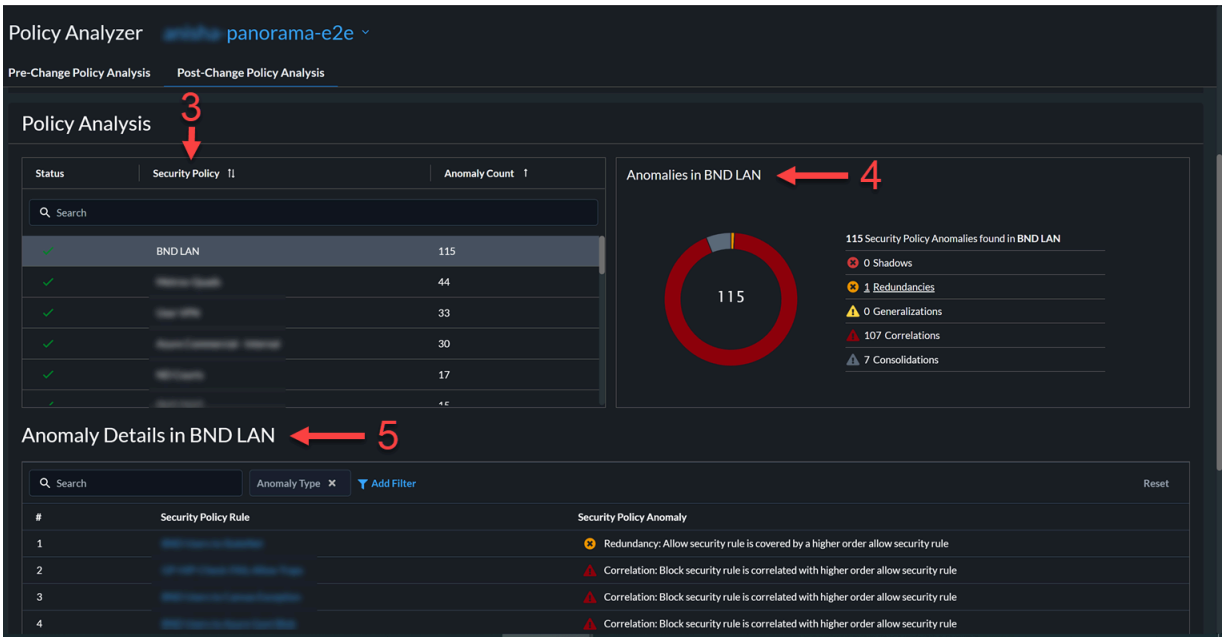
1. すべてのポリシー セット（NGFWが直接割り当てられたすべてのデバイス グループ）にわたる分析の要約を表示します。異常値または優先度の高い値に基づいて異常値を表示できます。このレポートの値は、すべてのデバイスグループで見つかった固有の異常数を示します。チャート内の色は、さまざまなタイプの異常を示します。



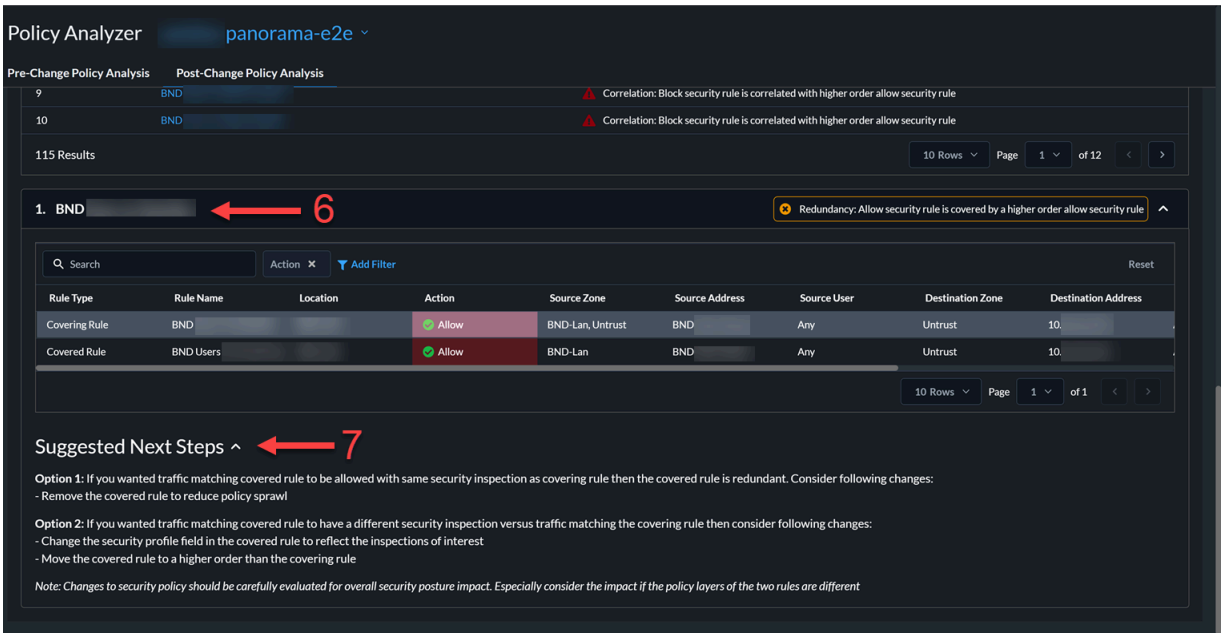
2. 以下を含む分析のタイムスタンプ
   - 既存のセキュリティポリシースナップショット-構成がコミット後にPanoramaで実行中としてマークされたときのタイムスタンプ。
   - 分析が開始された時刻
   - 時間分析が終了した時刻
   - 分析が完了するまでにかかった時間
3. セキュリティポリシーのステータスと各ポリシーの異常数を表示します。
4. 選択したセキュリティポリシーの異常の内訳を表示します。

©2025 Palo Alto Networks, Inc.

5. セキュリティポリシーのすべてのルールの異常の詳細を表示します。



6. 選択したルールの属性と異常の詳細を表示します。



この画像は冗長性異常の一例です。この例では、BNDルールはすでに別のBND Usersルールの対象になっています。そのため、BNDルールを削除できます。

7. 異常を修復するための次のステップの候補を表示します。

 ©2025 Palo Alto Networks, Inc.

NGFWの正常性とソフトウェア管理

この章では、NGFWの正常性とソフトウェアのアップグレードを管理する方法について説明します。

- デバイスの正常性の表示 - オンボードされたNGFWの正常性スコアに基づいて、展開の累積的なヘルス ステータスとパフォーマンスを表示します。
- アップグレードの推奨事項 - アップグレード可能なデバイスに最適なソフトウェア バージョンを決定するための推奨事項を作成します。
- メトリック容量の分析 - モデル タイプに基づいてメトリックの使用状況を追跡することにより、デバイスのリソース容量を分析および監視します。

デバイスの正常性を表示

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	次のいずれか ❑ または ❑ または

[Device Health (デバイスの正常性)] ダッシュボードには、オンボードされたNGFWの正常性スコアに基づいて、展開の累積的な正常性ステータスとパフォーマンスが表示されます。デバイスの正常性は、正常性スコアの重大度（0～100）と、それに対応する正常性グレード（良好、普通、不良、重大）によって決定されます。稼働状態スコアは、未解決のアラートの優先度、数量、種類、ステータスに基づいて計算されます。

このダッシュボードは、次のことに役立ちます。

- 稼働状態スコアの履歴データを見ることで、ある期間に行った導入の改善点を把握できます。
- 展開で注意が必要なデバイスを絞り込み、問題を解決するために問題の優先順位を付けます。

詳細については、「ダッシュボード:デバイスの正常性」を確認してください。

©2025 Palo Alto Networks, Inc.

アップグレードに関する推奨事項

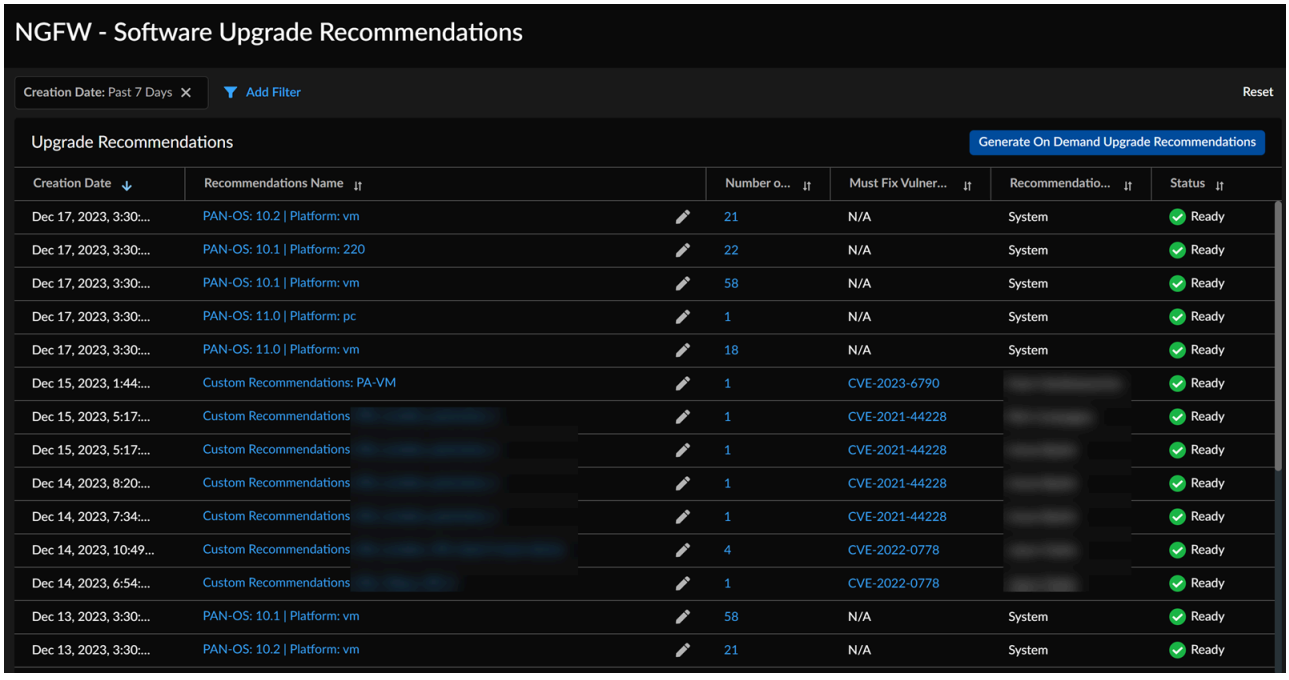
どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	☐ または

[ワークフロー] > [ソフトウェアアップグレード] > [アップグレードの推奨事項]を選択すると、Strata Cloud Managerを使用してファイアウォールで有効になっている機能を分析し、ネットワークに固有の情報を提供するカスタマイズされた推奨事項を作成できます。

- デバイスで実行するのに最適なソフトウェアバージョン。
- 各推奨ソフトウェアバージョンの新機能、動作の変更、脆弱性、ソフトウェアの問題に関する情報。

アップグレードの推奨事項の種類:

- デバイステレメトリデータから毎週2回生成されるシステム生成レコメンデーション。
- 特定のPAN-OS CVEのデバイスを選択すると生成される、ユーザー生成のカスタム推奨事項。
- ファイアウォールのテクニカルサポートファイル（TSF）をアップロードして生成する、ユーザ生成の推奨事項。



すべてのレコメンデーションに対して以下のタスクを実行できます。

- アップグレードが必要なデバイスの数と、対処が必要な脆弱性を表示します。
- カスタム推奨事項を区別するために、推奨事項の名前を編集します。

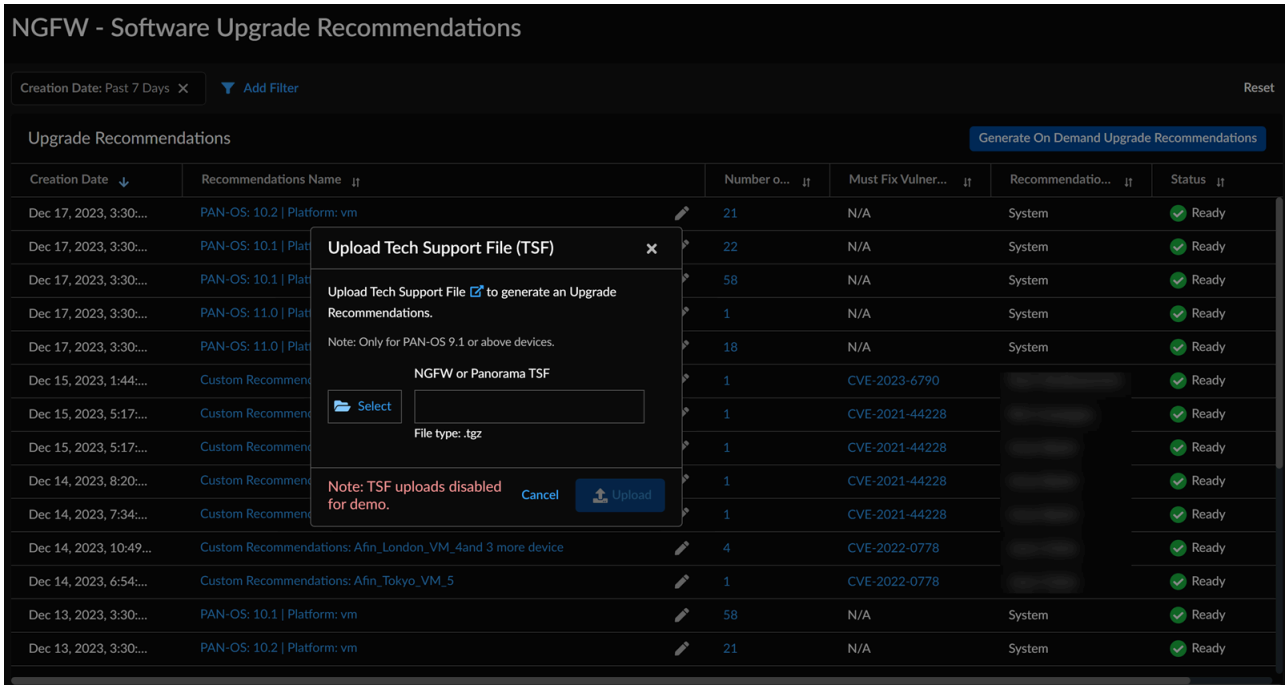
©2025 Palo Alto Networks, Inc.

- [作成日]、[推奨事項名]、[生成者]で推奨事項をフィルタリングします。
- 失敗した、または適切でなくなった推奨事項を削除します。

オンデマンドアップグレード推奨事項の生成

1. オンデマンドアップグレード推奨事項の生成。
2. テクニカルサポートファイル（TSF）を選択し、アップロードします。

- 一度にアップロードできるデバイスの*TSF*は*1*つだけで、*TSF*は*.tgz*形式である必要があります。
- ソフトウェアアップグレードの推奨事項を生成できるのは、*PAN-OS 9.1*以降の*PAN-OS*バージョンを実行しているファイアウォールに対して生成し、ファイアウォールからアップロードする*TSF*からのみです。



3. ステータスが[Ready (準備完了)]になったら、ソフトウェアアップグレードの推奨事項を表示します。

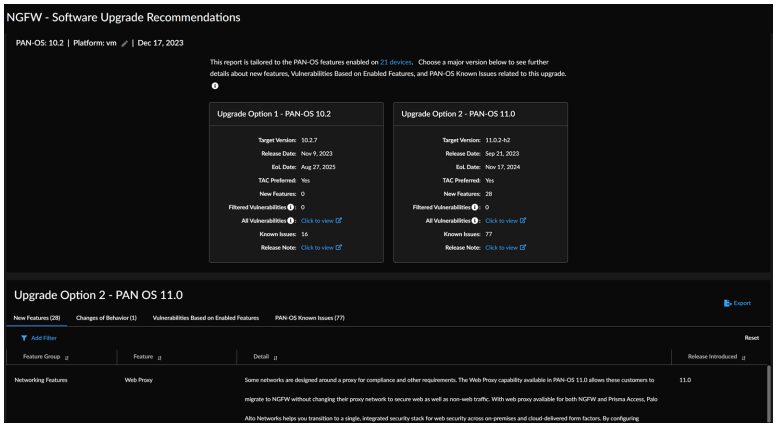
   また、[Status (ステータス)]をチェックして、TSFのアップロード、ファイル形式、または処理に関連するエラーがあるかどうかを確認できます。

ソフトウェアアップグレードの推奨事項レポートの表示

推奨事項をクリックすると、デバイスのアップグレードオプションを含む詳細レポートが表示されます。アップグレードオプションを選択すると、**[New Features (新機能)]**、**[Changes of Behavior (振る舞いの変更)]**、**[Vulnerabilities Based on Enabled Features (有効な機能に基づく脆弱性)]**、および**[PAN-OS Known Issues (PAN-OS既知の問題)]**に関する詳細が表示されます。このレポートはCSV形式でエクスポートすることもできます。

 ©2025 Palo Alto Networks, Inc.

- 推奨レポートには、デバイスで有効になっている機能に固有の情報が含まれています。
- ***PAN-OS***既知の問題の場合、*Associated Case Count* (関連するケース数)は問題を報告したお客様の数を表します。



 ©2025 Palo Alto Networks, Inc.

メトリック容量の分析

どこで使用できますか?	何が必要ですか?
•	❑ または

Strata Cloud Managerから**[Monitor (監視)]** > **[Capacity Analyzer (容量アナライザ)]**に移動し、モデルタイプに基づいてメトリックの使用状況を追跡して、デバイスのリソース容量を分析および監視します。以下の方法でメトリックを分析できます。

- メトリック、モデル、デバイスに基づいてメトリック容量を分析する
- デバイスモデルに基づくメトリック容量の分析
- メトリックに基づいてメトリック容量を分析する

Capacity Analyzerは、最大容量に近づいたリソースの消費を予測してアラートを発生させるのに役立つアラートをサポートするように拡張されています。「Manage Capacity Analyzer Alerts (容量アナライザアラートの管理)」を参照してください。

*VM*シリーズのファイアウォールでは、容量アナライザ機能はサポートされていません。

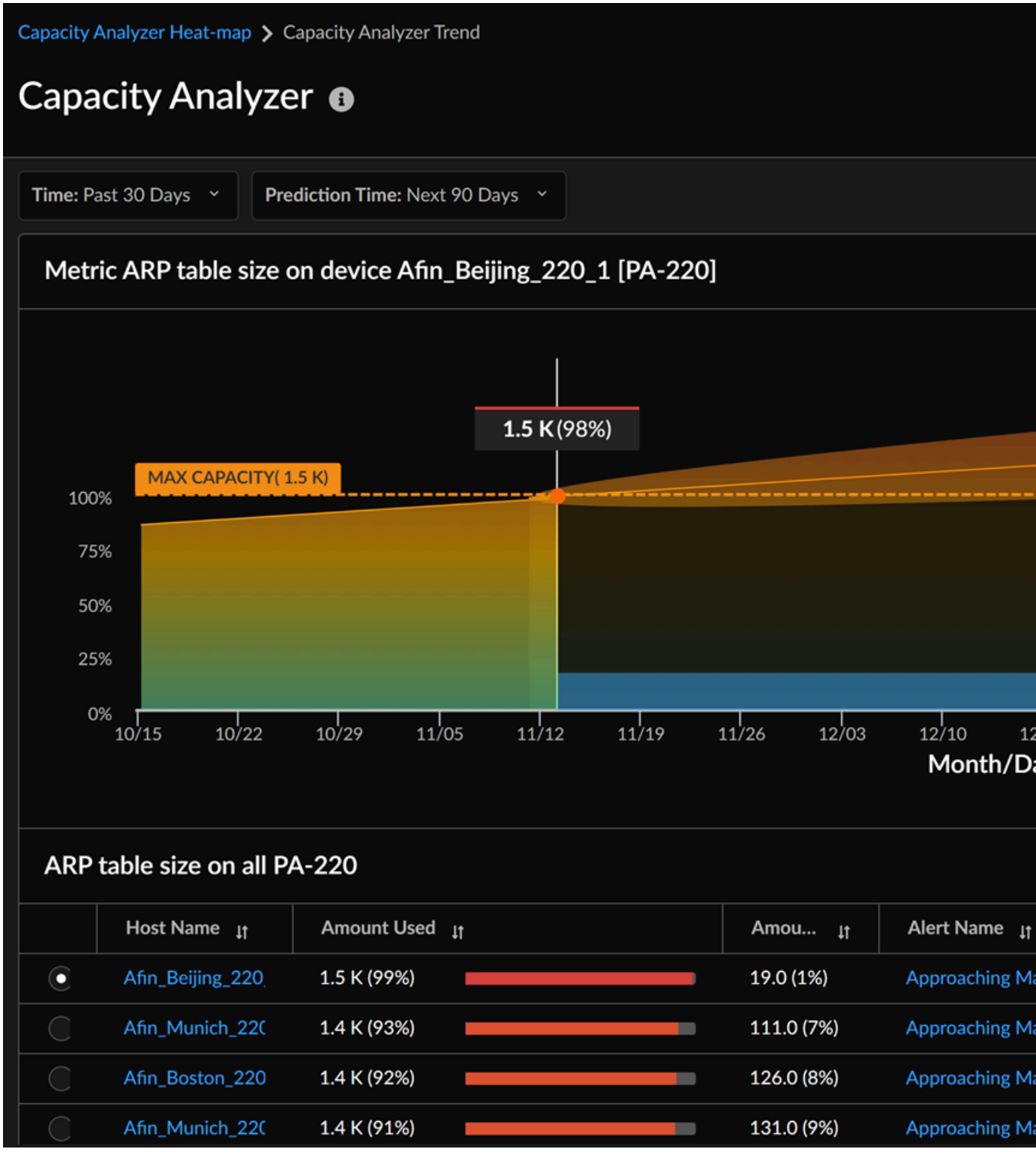
メトリック、モデル、デバイスに基づいてメトリック容量を分析する

1. 容量アナライザのヒートマップで、セルの上にカーソルを置くと、対応するデバイスモデルに属するすべてのデバイスのメトリック容量使用状況が表示されます。

   この例では、ポップアップ ウィンドウに、**PA-220** モデルに属するすべてのデバイスの **ARP** テーブル サイズのメトリック容量が表示されます。

 ©2025 Palo Alto Networks, Inc.

2. デバイスモデルとメトリックに対応するセルをクリックして、容量の使用状況を確認します。この例では、**PA-220**デバイスモデルのARPテーブルサイズをクリックしています。



次のものを表示できます。

- **PA-220** モデルに属するすべてのデバイスの ARP テーブル サイズ メトリック容量。

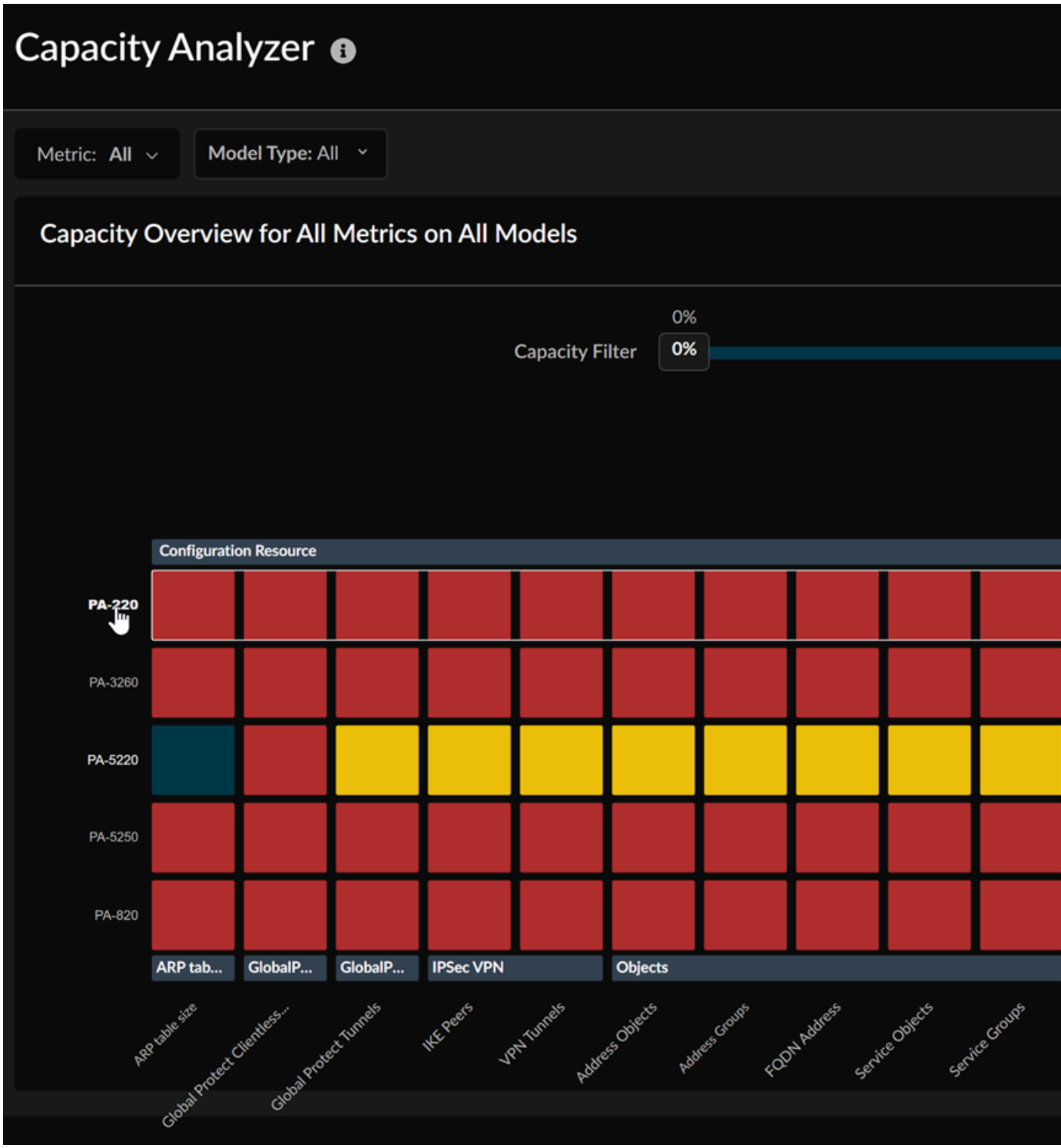
©2025 Palo Alto Networks, Inc.

- いずれかのホスト名を選択すると、メトリック容量の傾向が表示されます。
- メトリックおよびメトリックが最大容量に達する予測日に対して発生したアラート。
- メトリックの予測トレンド。Strata Cloud Managerは、メトリックが最大容量に達する日付を予測します。グラフの上にカーソルを置くと、任意の時点のメトリック容量を確認できます。

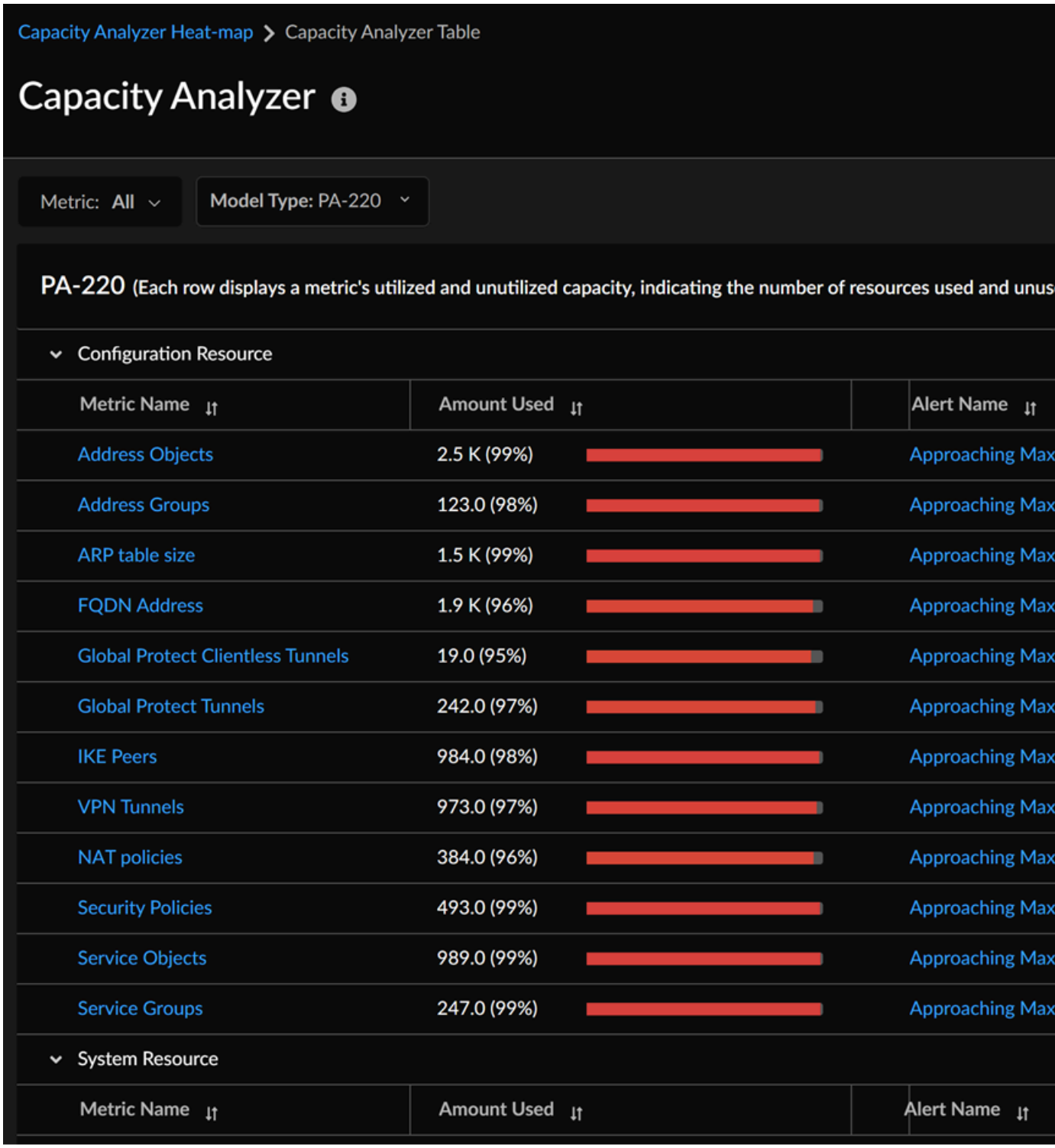
©2025 Palo Alto Networks, Inc.

デバイスモデルに基づくメトリック容量の分析

1. 容量アナライザヒートマップからデバイスモデルを選択すると、関連するすべてのメトリックが表示されます。



 ©2025 Palo Alto Networks, Inc.



各行にはメトリックの使用容量が表示され、デバイス内のそのメトリックで使用しているリソースの数が示されます。さらに、メトリックとそのメトリックが最大容量に達する予測日に発生するアラートを表示できます。

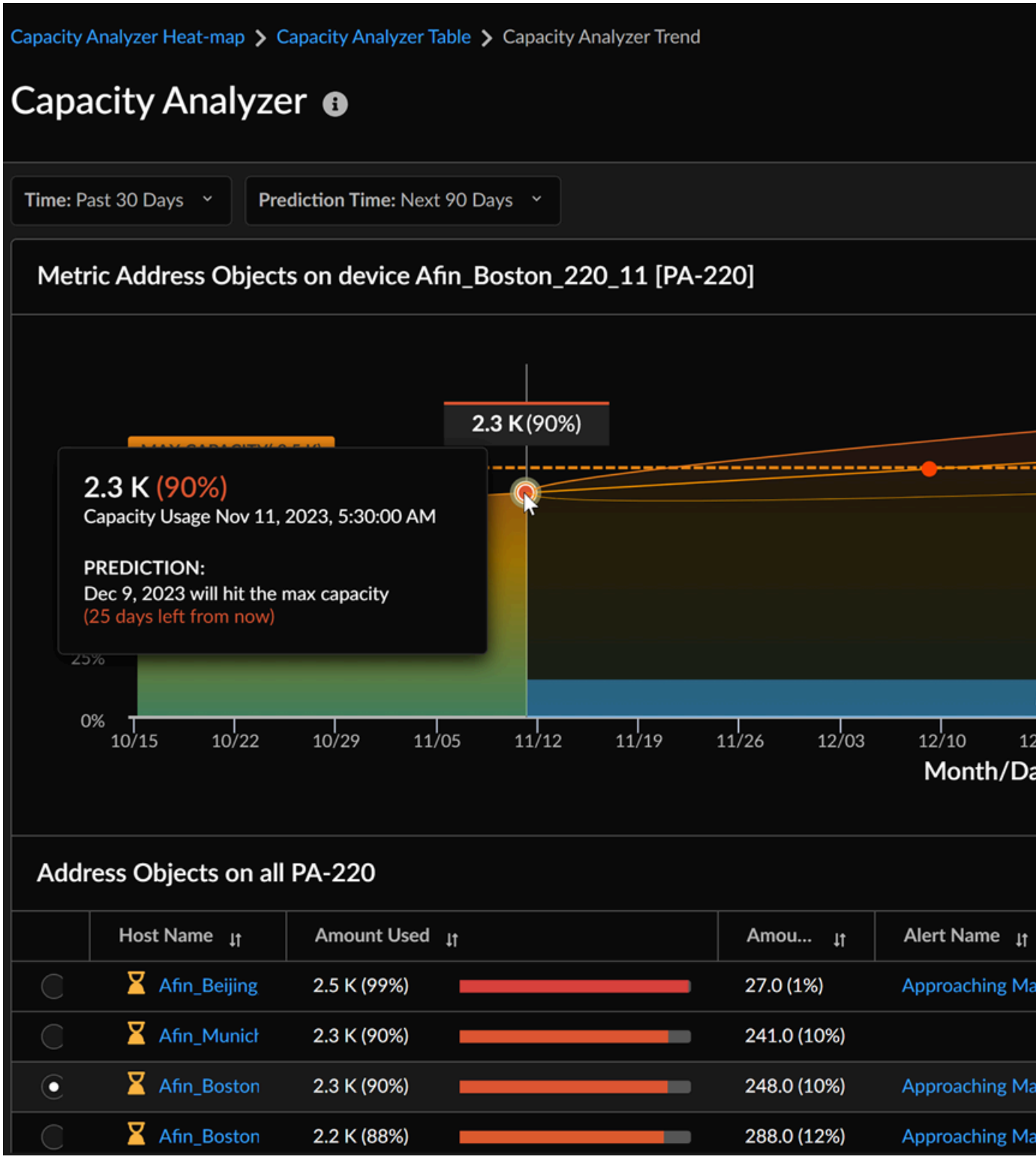
2. ［Capacity Analyzer (容量アナライザ)］ テーブルで、デバイスの傾向を表示するメトリックを選択します。

 ©2025 Palo Alto Networks, Inc.

3. デバイスを選択すると、そのデバイスのメトリックの傾向が表示されます。

   [Prediction Time (予測時間)]を選択すると、指標の予測トレンドを確認できます。Strata Cloud Managerは、メトリックが最大容量に達する日付を予測します。

   グラフの上にカーソルを置くと、任意の時点のメトリック容量を確認できます。



 ©2025 Palo Alto Networks, Inc.

[**Alert Name (アラート名)**]では、ホスト名に対応するアドレスオブジェクトメトリックに対して発生したアラートを表示できます。

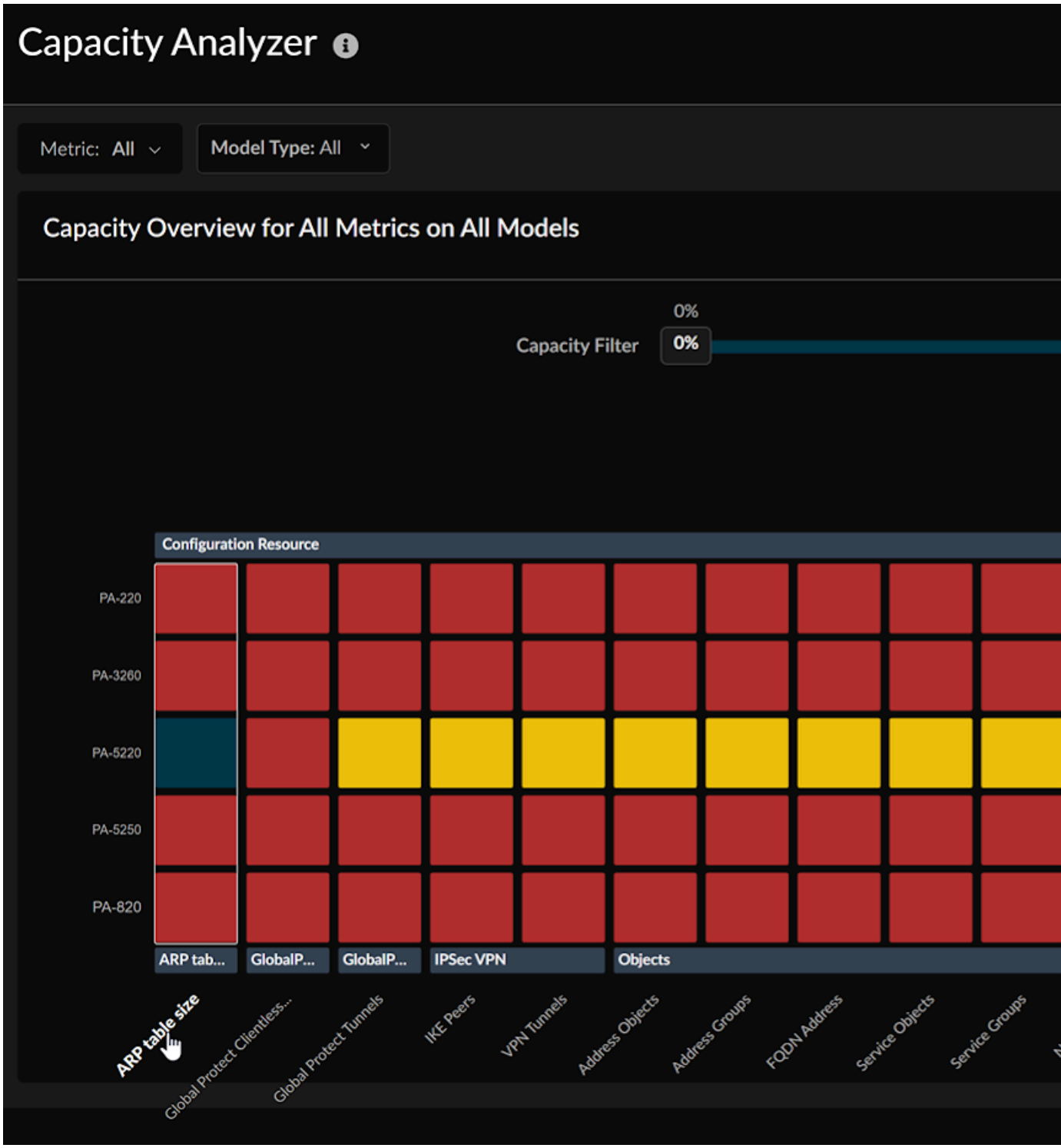
©2025 Palo Alto Networks, Inc.

メトリックに基づいてメトリック容量を分析する

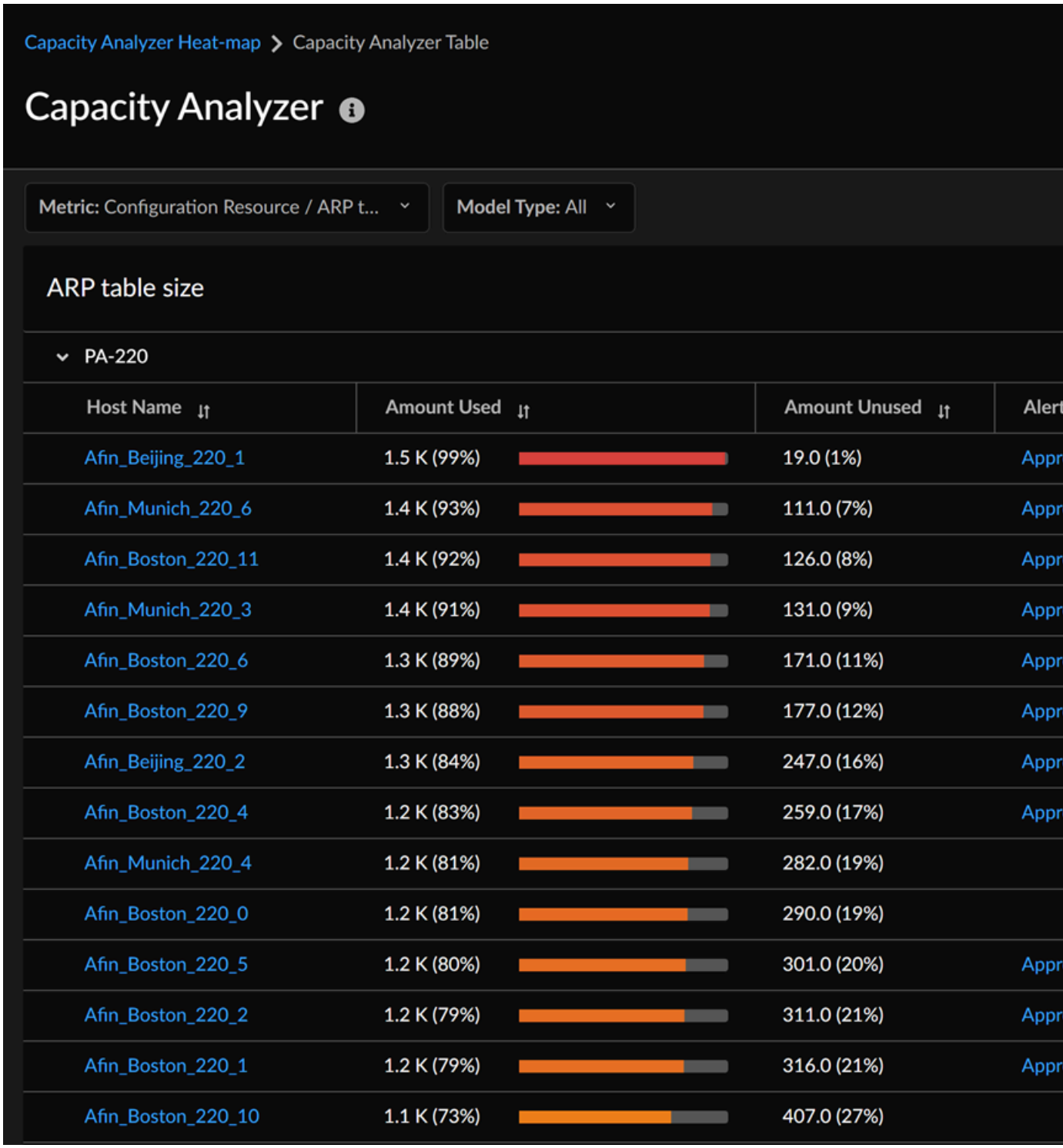
1. 容量アナライザのヒートマップからメトリックを選択すると、すべてのデバイスで容量を表形式で表示します。この例では、**ARP** テーブル サイズのメトリックが選択されています。

   また、メトリックタイプを選択してメトリックにドリルダウンすると、すべてのデバイスの容量を表形式で表示できます。たとえば、***[Configuration Resource (***設定リソース***)]*** *[type metric (*タイプメトリクス*)]*>***[Objects (***オブジェクト***)]*** > ***[Address Objects (***アドレスオブジェクト***)]***などです。

©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

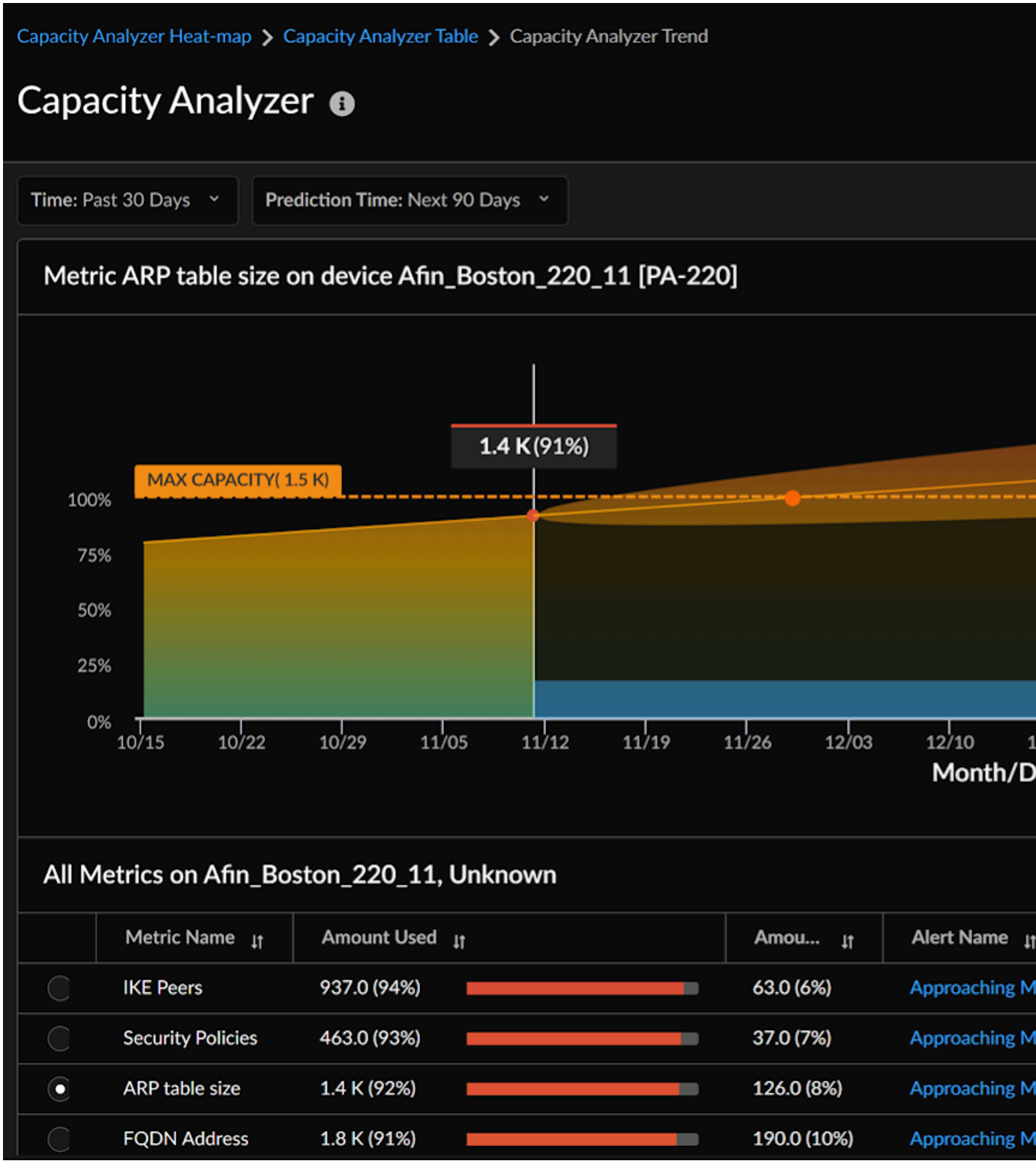


各行には、デバイスモデルの下にあるすべてのホストの**ARP**テーブルサイズメトリックの使用容量と未使用容量が表示されます。さらに、各ホストのこのメトリックに対して発生したアラートと、メトリックが最大容量に達する予測日を表示できます。

©2025 Palo Alto Networks, Inc.

2. ホスト名を選択すると、選択した指標の傾向がグラフィカルに表示されます。

   [Prediction Time (予測時間)]を選択すると、指標の予測トレンドを確認できます。Strata Cloud Managerは、メトリックが最大容量に達する日付を予測します。



グラフの上にカーソルを置くと、任意の時点のメトリック容量を確認できます。

©2025 Palo Alto Networks, Inc.

NGFWのベストプラクティス

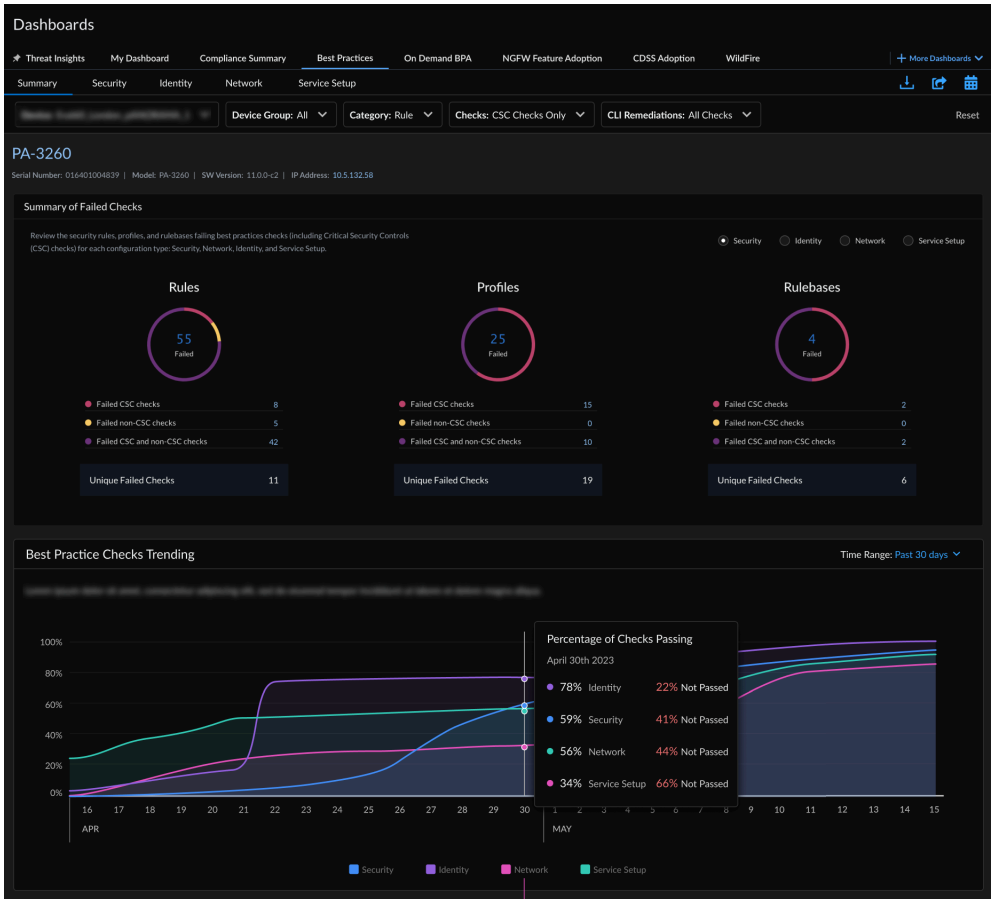
どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	次のいずれか □ または □ または

AIOps for NGFWは、ベストプラクティスに沿ってセキュリティ体制を引き締めるのに役立ちます。AIOps for NGFWを活用して、Panorama、NGFW、Panoramaが管理するPrisma Accessのセキュリティ構成をベストプラクティスに照らして評価し、失敗したベストプラクティスのチェックを修復できます。AIOps for NGFWは、ネットワークインフラストラクチャ上のInfoSecコンプライアンスをチェックするプロセスを合理化します。

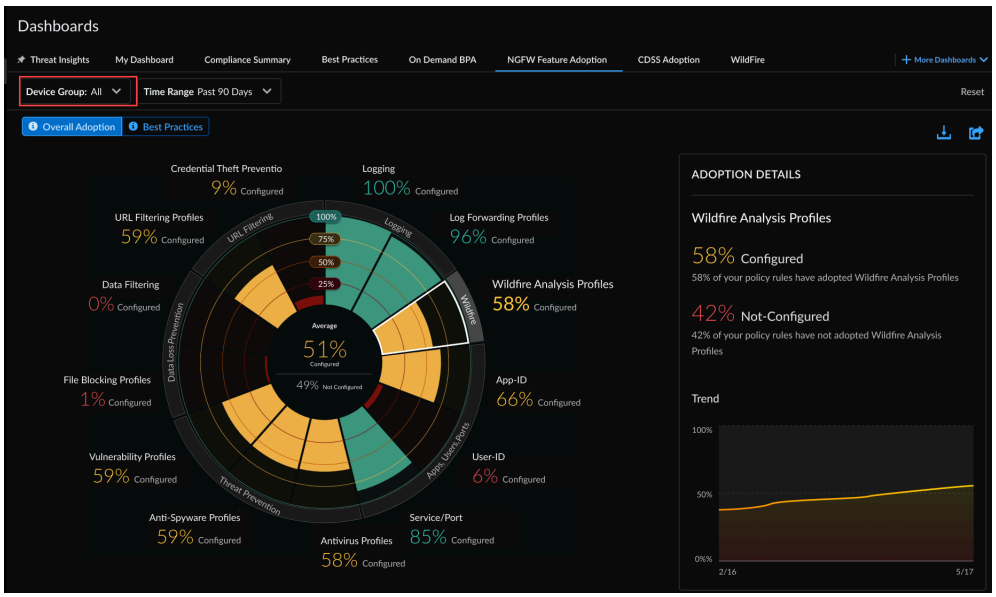
AIOps for NGFWは無料で、以下のAIOpsベストプラクティス評価 (BPA) 機能がAIOpsプレミアムライセンスなしで利用できます。使用可能なベストプラクティス機能の全リストについては、組み込みベストプラクティスを参照してください:

- ベストプラクティスダッシュボードで日々のベストプラクティスレポートを確認し、インターネットのセキュリティセンターの重要なセキュリティ管理（CSC）チェックとの対応付けを行うことで、ベストプラクティスのコンプライアンスを向上させるために変更可能な領

域を特定できます。ベストプラクティスレポートをPDFとして共有し、受信トレイに定期的に配信されるようにスケジュールします。



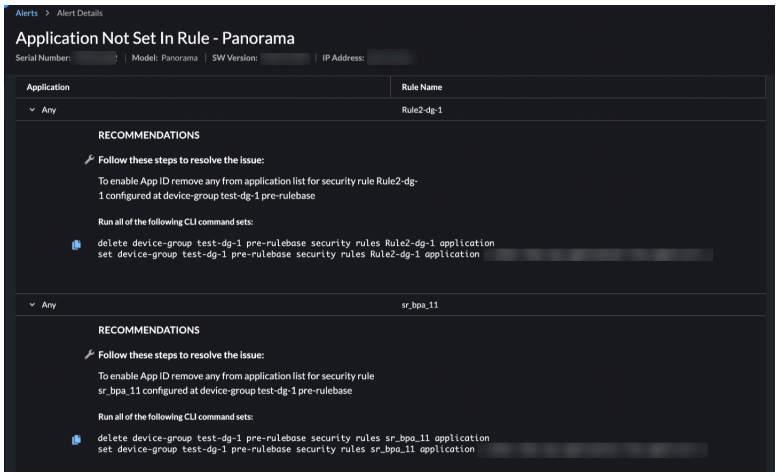
- [Feature Adoption (機能の導入状況)]を監視し、デプロイメントで使用しているセキュリティ機能や、カバレッジのギャップの可能性を常に把握できます。



 ©2025 Palo Alto Networks, Inc.

- AIOps for NGFWからセキュリティ体制アラートを取得し、セキュリティ設定を詳しく調べる必要があるタイミングを把握できます。

  NGFW の AIOpsでは［**Alerts (アラート)] > [Security (セキュリティ)] > [Alert Details (アラートの詳細)]** ］ でコマンドライン インターフェイス（CLI）による修復も可能です。アラートをトリガーする問題の修正を支援することを目的とした推奨事項を表示します。

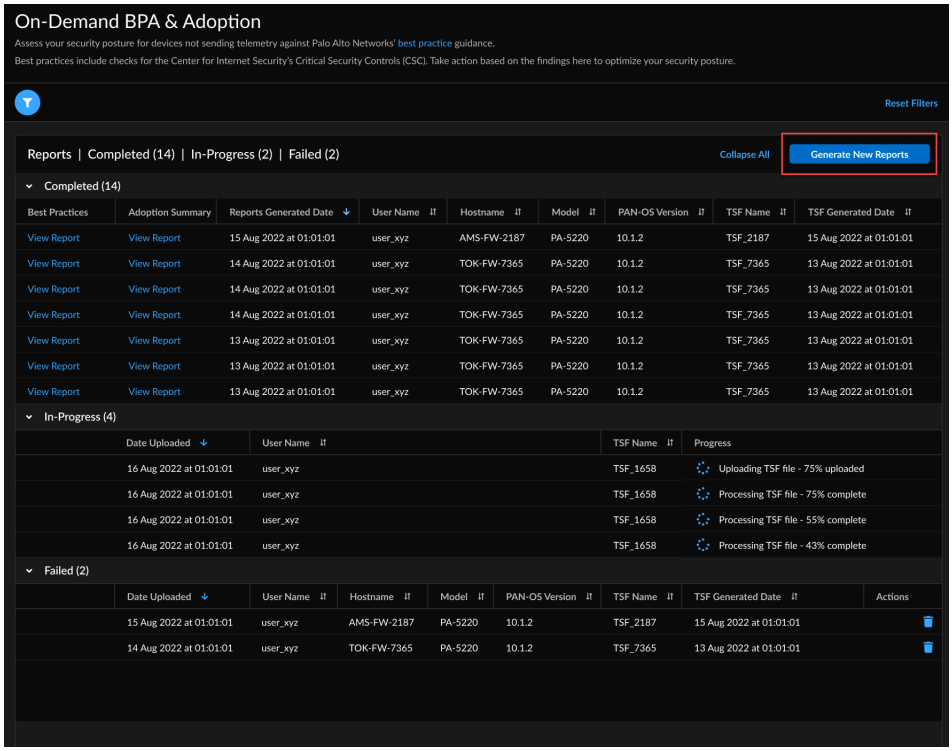


  セキュリティ警告と*CLI*による修復は、テレメトリを共有するデバイスでのみ使用できます。この機能は、バージョン*9.1*以降を実行している*PAN-OS*デバイスのテクニカルサポートファイル（*TSF*）手動アップロードをサポートしていません。

- バージョン9.1以降を実行している（テレメトリではない）PAN-OSデバイスのBPAレポートを生成し、機能の採用メトリックを含めるようになりました。これまでBPAスタンドア

 ©2025 Palo Alto Networks, Inc.

ロンツールを使ってBPAレポートを生成していた方は 、「 カスタマーサポートポータルからBPAレポートを生成できますか？」と思われるかもしれません。私たちがカバーします。



プレミアムライセンスでは、AIOps for NGFWは高度なセキュリティ体制機能も提供します。プレミアム機能は、ファイアウォールのフル活用と最大限のセキュリティの実現に焦点を当てています。無料ライセンスとプレミアムライセンスの両方にどのようなメリットがあるかご確認ください。

©2025 Palo Alto Networks, Inc.

オンデマンド BPA レポート

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	次のいずれか ❑ または ❑ または

ベストプラクティス評価（BPA）と機能導入の概要をStrata Cloud Managerから直接実行できるようになりました。テクニカルサポートファイル（TSF）をアップロードするだけです。テレメトリデータを送信していないデバイスや、AIOps for NGFWにオンボードされていないデバイスのオンデマンドBPAレポートを生成できます。

BPAは、Palo Alto Networksのベストプラクティスに照らしてセキュリティ態勢を評価し、デバイスの改善に優先順位を付けます。セキュリティ ベストプラクティスは、既知および未知の脅威を予防し、攻撃可能範囲を縮小し、トラフィックの可視性を提供するために、自社のネットワーク上にどのようなアプリケーション、ユーザーおよびコンテンツが存在するかを知り、それらを管理することができます。さらにベストプラクティスには、インターネットセキュリティセンターの重要なセキュリティ管理 (CSC) のチェックが含まれます。セキュリティ体制を強化し、改善を実施するためのベストプラクティスガイダンスをご覧ください。

カスタマーサポートポータルからBPAレポートを生成できますか？

AIOpsが登場する前は、カスタマーサポートポータルにアクセスしてBPAを実行していました。現在、NGFW/Panorama Managed Prisma Accessのベストプラクティス評価レポートを生成してダウンロードする方法として、AIOpsが推奨されています。

2023年7月17日以降、カスタマーサポートポータルからBPAにアクセスして実行することはできなくなります。

STEP 1 | [Hub (ハブ)]に移動して、AIOps for NGFWを起動します。これは無料です。この時点でテレメトリが有効になっているデバイスをオンボードしたくない場合は、Strata Logging Serviceなしでアクティブ化できます。

> *Strata Logging Service*またはテレメトリを有効にしていないオンボードデバイスでは、ベストプラクティスダッシュボード、セキュリティ警告、および採用サマリー機能は使用できません。

STEP 2 | NGFW用にアクティブ化されたインスタンスAIOpsにログインします。Strata Logging Serviceなしでも以下のタブが表示されます。

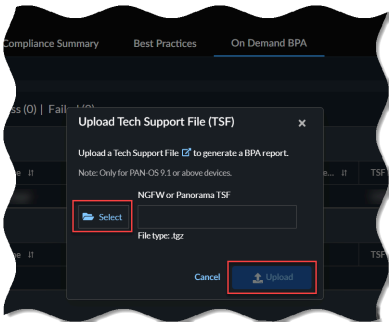
- 姿勢
- アクティビティ
- 設定

 ©2025 Palo Alto Networks, Inc.

STEP 3 | **[Dashboards (ダッシュボード)]** > **[On Demand BPA (オンデマンド BPA)]**に移動します。

STEP 4 | 新しい**BPA**レポートを生成。

STEP 5 | **TSF**を選択し、**TSF**ファイルをアップロードします。



アップロード時間は、.tgzファイルのサイズとインターネット速度によって異なります。ファイルサイズが大きい場合、ファイルのアップロードに数分かかることがあります。**[In-Progress (実行中)]**を展開し、TSFファイルのステータスを表示します。

- オンデマンド*BPA*は、*.tgz*ファイル形式のテクニカルサポートファイル（*TSF*）のみをサポートしています。
- オンデマンド*BPA*は、*PAN-OS*バージョン*9.1*以上を搭載したデバイスからの*TSF*をサポートし、レポート生成を実現します。

STEP 6 | TSFが処理された後に［**Completed (完了)**］の下にある［**View Report (レポートを表示)**]を選択すると、デバイスから生成されたBPAレポートが表示されます。

 ©2025 Palo Alto Networks, Inc.

ベストプラクティス

どこで使用できますか?	何が必要ですか?
• •	☐ または ☐ ライセンス ☐ デバイスでテレメトリ共有を有効にします

このダッシュボードには何が表示されますか?

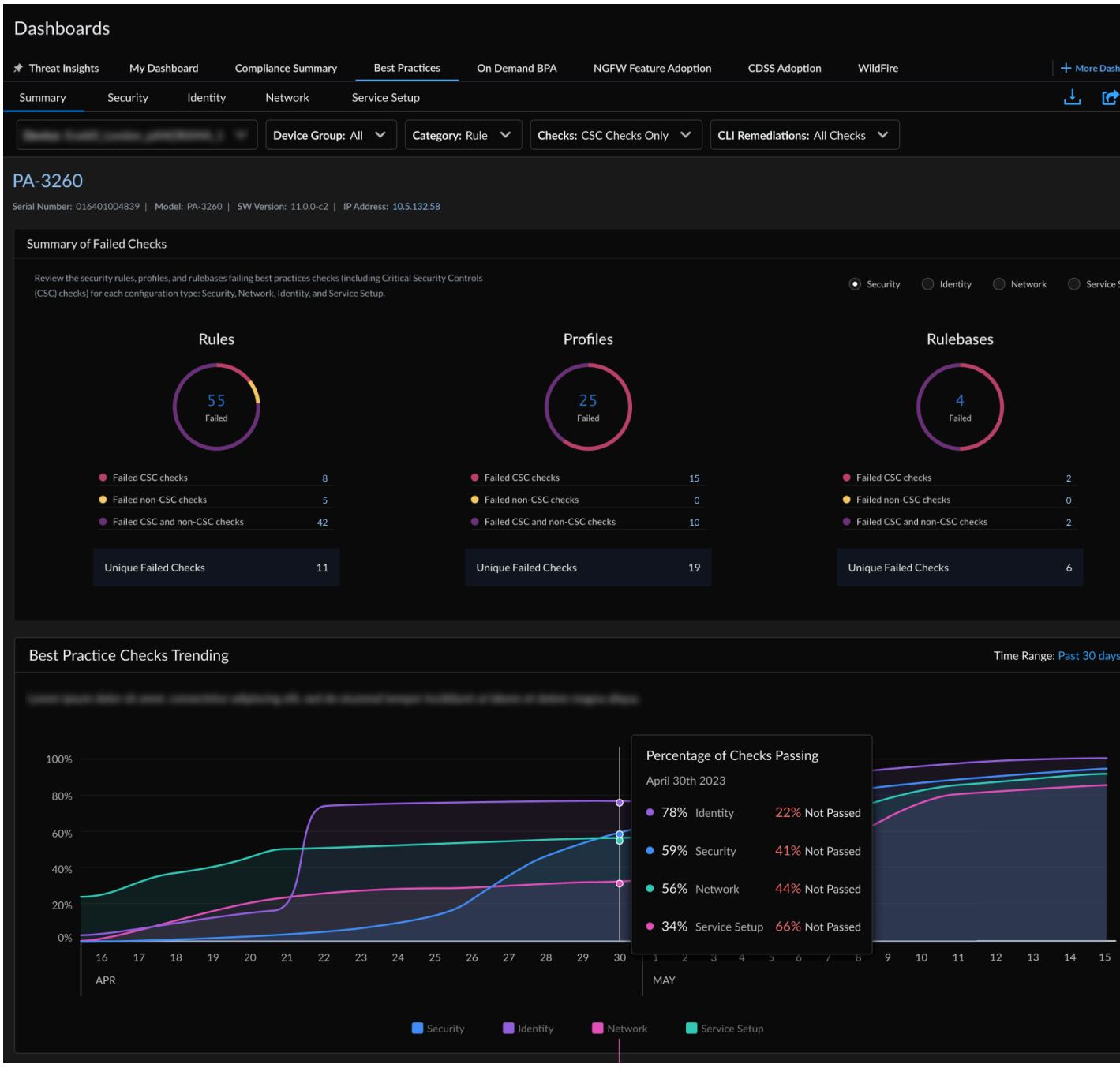
ダッシュボードには、テナントに関連付けられている*Prisma Access*および*NGFW/Panorama*ごとに集計されたデータが表示されます。

Strata Cloud Manager > **[Dashboards (**ダッシュボード**)]** > **[More Dashboards (**その他のダッシュボード**)]** > **[Best Practices (**ベスト プラクティス**)]** ダッシュボードに移動し、Palo Alto Networksのベスト プラクティス ガイダンスに照らしてセキュリティ体制を測定します。ベスト プラクティスには、インターネットセキュリティセンターの重要なセキュリティ管理 (CSC) のチェックが含まれます。CSCチェックは他のベスト プラクティス チェックとは別に呼び出されるため、CSCコンプライアンスに準拠するための更新を簡単に選択して優先順位を付けることができます。

ダッシュボードのデータをどのように活用できますか?

ベスト プラクティス ガイダンスはセキュリティ体制の強化を目的としていますが、このレポートの調査結果は、環境をより効果的に管理するために変更を加えることができる領域を特定するのにも役立ちます。

©2025 Palo Alto Networks, Inc.



ベスト プラクティス ダッシュボードは5つのセクションに分かれています。

- 概要

  構成タイプ (セキュリティ、ネットワーク、ID、およびサービス セットアップ) 全体にわたってデバイスのすべての失敗したチェックの包括的なビューを提供し、BPAチェックの履歴トレンド チャートを表示し、主要な機能領域におけるベスト プラクティスの採用率を評価します。

 ©2025 Palo Alto Networks, Inc.

- セキュリティ

  選択したデバイスと場所のベスト プラクティスとCSCチェックに失敗したルール、ルールベース、またはプロファイルを表示します。利用可能な場合、CLI修復により、ポリシー ルールの問題を解決できます。CLI修正は、オンデマンド BPA レポートを生成するときにアップロードしたTSFデータを使用して生成されます。

  - ルールベース

    ポリシーがどのように構成されているか、および多くのルールに適用される構成設定がベスト プラクティス (CSC チェックを含む) に準拠しているかどうかを確認します。

  - ルール

    ベスト プラクティスとCSCチェックに失敗したルールを表示します。失敗したチェックを修正するための迅速なアクションをどこで実行できるかを確認してください。ルールはセッション数に基づいて並べ替えられるため、トラフィックに最も影響を与えているルールを確認して更新することから始めることができます。

  - プロファイル

    CSCチェックなどのベスト プラクティスに対してプロファイルがどのように適合しているかを示します。プロファイルは、セキュリティルールまたは復号化ルールに一致するトラフィックの高度な検査を実行します。

- **ID**

  デバイスの認証強制設定 (認証ルール、認証プロファイル、認証ポータル) がベスト プラクティスを満たし、CSCチェックに準拠しているかどうかを示します。

- ネットワーク

  アプリケーションのオーバーライド ルールとネットワーク設定がベスト プラクティスおよびCSCチェックに準拠しているかどうかを確認します。

- サービスのセットアップ

  デバイスで有効にしたサブスクリプションがベスト プラクティスおよびCSCチェックとどのように一致しているかを確認します。ここで、WildFireのセットアップ、GlobalProtectポータル、GlobalProtectゲートウェイの構成を確認し、失敗したチェックを修正できます。

 ©2025 Palo Alto Networks, Inc.

ダッシュボードのレポートを共有、ダウンロード、スケジュールする

ダッシュボードに表示されるデータ (*PDF*形式と *.csv*形式) と *CLI*修復 (*.txt*形式) を網羅したレポートをダウンロード、共有、スケジュール設定できます。ダッシュボードの右上に次のアイコンがあります。

©2025 Palo Alto Networks, Inc.