# アプリケーションベース・ポリシーに移行するためのベストプラクティス

***Version 10.0 (EoL)***

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

## Contact Information

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

## About the Documentation

- To ensure you are viewing the most current version of this document, or to access 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

July 15, 2020

# Table of Contents

# アプリケーションベース・ポリシーに移行するためのベスト プラクティス

アプリケーションを使えるようにするためにセキュリティを犠牲にする必要はありません。代わりに、Expeditionとポリシー オプティマイザーを使って、レガシーファイアウォール上のポートベース・セキュリティポリシーからPalo Alto Networks次世代ファイアウォールまたはPanoramaアプライアンス上のアプリケーションベース・セキュリティポリシールールに、安全かつ段階的に移行するプロセスを自動化し、時間と労力を軽減することができます。

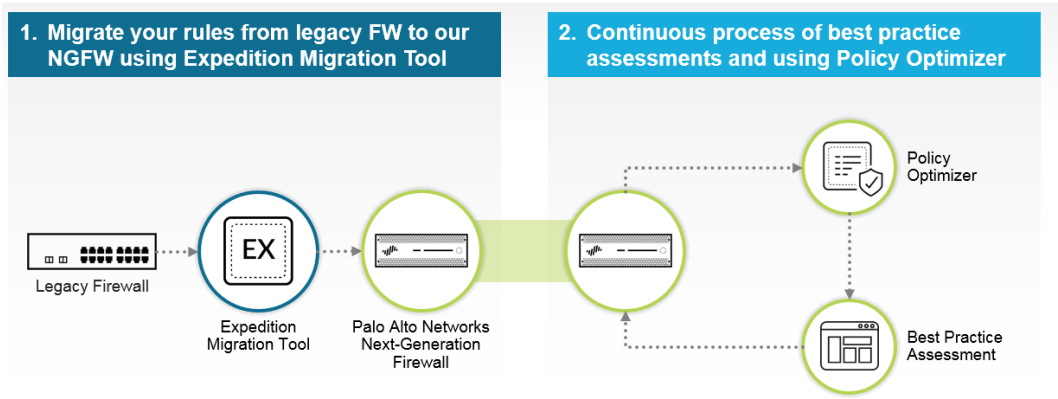
- フェーズ化されたトランザクションを使用してアプリケーションを安全に有効化します
- Expeditionを使って、ポートベースのポリシーをPAN-OSに移行
- ポリシー オプティマイザーを使ってアプリケーション ベース・ポリシーに移行
- セキュリティのベスト プラクティスを適用するための次のステップ

# フェーズ化されたトランザクションを使用してアプリケーションを安全に有効化します

ポートベースのセキュリティポリシーの明白な弱点は良く知られています。どのアプリケーションがどのポートを使用しているのか見られないので、悪意のあるアプリケーションが、ポート80(HTTP)あるいはポート53 (DNS)のようなオープンポートのネットワークにアクセスすることができます。これでは、ネットワーク上のアプリケーション内に可視性がなく、トラフィックを封入する脅威を防ぐ能力がないため、攻撃者がマルウェアをインストールしたり、ネットワークを通じて水平移動したり、データを引き出したり、ネットワークを侵害したりすることを容易になってしまいます。

一方、App-ID™を使用しているアプリケーションベースセキュリティポリシーは、ポート、プロトコル、暗号化(SSLあるいはSSH)、巧妙な戦略に関係なくアプリケーション内への可視性を提供します。従って、どのアプリケーションがネットワーク上にあるのかを正確に知ることができますし、トラフィックの脅威を検査できます。アプリケーション固有のポリシーは安全なアクセスを可能にします。なぜなら、正当なユーザーだけが、正当な場所で正当なアプリケーションにアクセスすることを可能にし、これらのルールに脅威防御プロファイルを適用することができるからです。アプリケーションを分類するためにApp-IDを使用すると、攻撃可能な箇所を縮小します。なぜなら、ネットワーク上でビジネスのサポートに必要なアプリケーションのみを許可し、望まないアプリケーションを自動的にブロックするからです。望むものだけを許可し、その他は全てブロックすることは、すべての望まない個別のアプリケーションをブロックする膨大なタスクよりもより簡単で安全です。

App-IDへの段階的な移行：




1. レガシールールベースのインポートとクリーンアップを行い、既存のPalo Alto Networks次世代ファイアウォールあるいはPanorama装置への移行を達成するため、Use Expedition (Expeditionを使用)します。Expeditionは仮想マシーン(VM)として配布されます。
2. ネットワーク本番環境でPAN-OSファイアウォールあるいは装置を実行すると、ネットワーク上のアプリケーションを学習し、カテゴライズすることができます。
3. 少なくとも1週間トラフィックのロギングを行った後、ベースラインを設定するためBest Practice Assessmen（ベストプラクティスアセスメント(BPA)）を実行します。次に、ポリシー オプティマイザー使用して、安全にポートベースのルールをアプリケーションベースのルールに変換させ、ネットワークのセキュリティを確保します。（約一週間後に良く知られたアプリケーションを許可するいくつかの単純なルールを変換することができます。多くのアプリケーションで見られる他のルール、例えば一般アウトバウンドインターネットアクセスルール、一般アプリケーション情報の収集については、少なくとも30日間待ってください。）ビジネス上のニーズと優先事項に基づき、安全にルールを変換するため、段階的なアプローチを取ります。

4. (オプション) ポリシー オプティマイザーを使用してルールベースをApp-IDへ変換した後、設定をExpedition内に再インポートして、さらに単純化とルールベースの洗練化を進めるためのルール補強機能を使用します。
5. ネットワークに新しいアプリケーションを導入する際にはApp-IDの設定を維持します。最初の変換がポートベースのルールに合格した後、BPAを実行し、その後定期的に実行します。これにより、セキュリティを改善するべき他のエリアを発見します。

*PAN-OS 9.0*からポリシー オプティマイザーが利用可能です。*Panorama*を使って次世代ファイアウォールを管理する場合は、*Policy Optimizer*を使用するためにマネージドファイアウォールを*PAN-OS 9.0*にアップグレードする必要はありません。単純に*Panorama*を*PAN-OS 9.0*にアップグレードして、マネージドファイアウォールからトラフィックログを*PAN-OS 9.0*が動作する*Panorama*または*Log Collector*に送信し、*Panorama*からファイアウォールにポリシーをプッシュ配信してください。管理されたファイアウォールは*PAN-OS 8.1* 以降で実行する必要があります。ログコレクタに接続されている場合、ログコレクタは*PAN-OS 9.0*を実行する必要があります。これは認証への近道を提供します。これにより、*App-ID*に基づいたポリシーを適用するためにポリシー オプティマイザーを使用することができます。

*PA-7000 Series* ファイアウォールは、*2* つのロギングカード、*PA-7000 Series* ファイアウォールログ処理カード *(LPC)* と高性能 *PA-7000 Series* ファイアウォールログ転送カード *(LFC)* をサポートします。*LPC* とは異なり、*LFC* にはログをローカルに保存するためのディスクがありません。代わりに、*LFC* はすべてのログを *Panorama* や *syslog* サーバーなどの *1* つ以上の外部ログシステムに転送します。*LFC* を使用している場合、トラフィックログはローカルに保存されないため、*Policy Optimizer* のアプリケーション使用情報はファイアウォールに表示されません。*LPC*を使用する場合、トラフィックはファイアウォールにローカルに保存されます。そのため、*Policy Optimizer*のアプリケーション使用状況情報は、ファイアウォール上に表示されます。どちらの場合でも、*Log Collectors*と*Panorama*が*PAN-OS 9.0*以降を動作している限り、*PA-7000*ファイアウォールは*PAN-OS 8.1*以降を使用することができます。

# Expeditionを使って、ポートベースのポリシーをPAN-OSに移行

レガシールールベースをインポートし、クリーンアップし、同一条件化での移行をPalo Alto Networks次世代ファイアウォール、あるいはPanorama装置へアプリケーションベースのセキュリティポリシーへの移行の第一フェーズとして達成するために Expeditionを使用します。Expeditionは設定内の複数のオブジェクトのバルク動作を実行する優れたツールです。そして主要なファイアウォールの殆ど全てからレガシー設定をインポートすることができます。

このトピックは*Expedition*のワークフローの概要です。ライブコミュニティは、*Expedition*のツール入手方法や、ツールの利用方法に関する詳細な文書などを含むサポートを提供します。

*Palo Alto Networks*技術サポート *(TAC)* は*Expedition* へのサポートを提供していません。

Expedition 移行ワークフローの詳細は、Expedition ユーザーガイドを参照してください。 これには、CSVファイルを使用してコンフィギュレーション内にどのようにオブジェクトをインポートするか、デイ 1 の アイアンスキレット 設定をどのようにインポートするかも含まれています。

Expeditionの管理については、Expedition 管理ガイドを参照してください。これは、いくつかのユーザーインターフェース情報を含んでいます。またExpedition Hardeningガイドも参照してください。それは、Expedition VMをどのように保護するかに関するアドバイスを含んでいます。

移行を開始する前に、下記の必要条件に適合することを確認してください：

- VMの実行をサポートする管理デバイスに Expedition をダウンロードする。
- 移行しようとするPalo Alto Networks PanoramaとファイアウォールへのSSH and/or SSL の接続。SSHアクセスはCLIへの接続であり、SSL アクセスはウェブインターフェースとAPIコマンドをプッシュするための接続です。
- 移行しようとしているPAN-OSアプライアンスへ既存の設定をプッシュすることができる Palo Alto Networks Panoramaとファイアウォールへの運用アクセス。

プロフェッショナルサービス は移行に関に関して熟練しています。レガシーデバイスから*Palo Alto Networks*次世代ファイアウォールと*Panorama*装置の設定への移行を支援するプロフェッショナルサービスを利用することができます。

STEP 1 | レガシーのファイアウォール設定をレビューします。

レガシールールベースの目的を理解します。Juniper SRXでインターフェースを無効化する、あるいはトラフィックの検証はインターフェースと同じセキュリティレベル間で許可されていること、IPSecトンネルの状態を検証すること、そしてCisco ASA デバイスの事前共有されたキーを集めること、などの移行に関して知っておく必要のある項目を文書化します。。

STEP 2 | レガシー設定をExpedition内にインポートし、設定に要求された変更を加えます。

STEP 3 | Expeditionに新しい プロジェクト を作成します。

STEP 4 | **Project** 内に移行されたソース ( レガシー ) をインポートし、それを検証します。

ファイルフォーマットを確認し、全ての要求されたファイルが含まれていることを確認し、そして、Expedition ログとイベントが移行設定ファイルに正しくロードされているかどうかを確認します。必要に応じて、問題を修正するために、移行したソースファイルを編集し、再度確認してください。すべての項目が固定されるまでこのステップを繰り返します。

STEP 5 | 移行のベース設定となるように PAN-OS 設定を プロジェクト にインポートします。

最新のコンテンツアップデートを入手し、既存のPAN-OSアプライアンスからベース設定（既存の設定ファイルか、あるいは工場出荷時のデフォルトのPAN-OS設定ファイル）をインポートします。

設定ファイルは使用したい*PAN-OS*バージョンと一致しなければなりません。例えば、*PAN-OS 9.0*を実行するには*PAN-OS 9.0*設定ファイルをインポートします。

STEP 6 | 移行された設定をベースのPAN-OS設定で結合するためにクリーンアップします。

- 無効なサービスオブジェクトを除去あるいは置換します。PAN-OS はTCPとUDPサービスオートのみを認識し、そして、Expedition は TCP と UDP サービスポートのみを自動的に移行します。PingやICMPのようにレガシーデバイスがアプリケーションとしてよりもサービスとして見る非IPベースのアプリケーションを検索します。アプリケーションとして識別するためにそれらをApp-IDで置換し、トラフィックの可視性、検査、制御が可能となります。
- 設定を単純化しサイズを小さくするためには、他の無効なオブジェクトおよび未使用のオブジェクトを除去あるいは置換し、重複したオブジェクトを結合します。
- 無効化されたルールを探して除去することで設定の混乱を防ぎます。
- PAN-OSアプライアンスのインターフェースと一致するためインターフェースを命名し直します。レガシーデバイスからインポートされたインターフェース名は、一般的にPAN-OSの命名慣習とは一致しません。
- レガシーなコンフィギュレーションをインポートした時は、Expeditionは自動的に ゾーン 名を割り当てます。設定をPAN-OSアプライアンスに移行する際に、ゾーンが担う目的を説明するようなゾーン名に変更します。ゾーンが正しくインターフェイスにマップされていることを確認します。

  更に、静的ルートの仮想ルータをチェックします。多くの静的ルートが存在する場合、ルートをPAN-OS設定に移行するためにExpeditionを使用します。静的ルートが少数の場合は、それらをメモしておき、次に、設定を移行した後に手動で生成します。

STEP 7 | 移行した設定からベース設定にドラッグ & ドロップすることでPAN-OSベース設定を使用して移行した設定を結合します。

STEP 8 | 結合により重複オブジェクトが生じていないかを結合した設定内でチェックし、それらを除去あるいは結合します。

STEP 9 | 結合した設定をPAN-OSアプライアンスにエクスポートする前に、PAN-OSアプライアンスに接続されているPAN-OS上でスイッチやルータのARPキャッシュを消去、ARPテーブルを更新します。

PAN-OS デバイスで、 **ARP**をすべて消去（**clear arp all**）CLI コマンドを使用します。（必要であれば、**clear arp** <インターフェイス> CLI コマンドを使用して、インターフェース単位でARPキャッシュを消去することができます。）

STEP 10 | 移行した設定をPAN-OSアプライアンスにエクスポートして、移行した設定をロードします。

使用する方法は結合した設定をどのように移行したいのかによります：

- PAN-OSアプライアンスに新しくインストールするためには、**Generate XML & Set Output**（**XML**の生成と出力の設定）を選択し、XMLファイル（コンフィギュレーション）をインポートして、次にそれをPAN-OSアプライアンスにロードします。
- 既存のPAN-OSにインストールする場合、あるいは、全ての設定を一度に行う代わりに設定をひとつの部分単位で移行したい場合は、**Generate XML & Set Output**（スムルの生成と出力の設定）を選択し、XML ファイル（コンフィギュレーション）をインポートして、次に**load config partial** CLI コマンドを使用して、設定で選択した特定の設定をロードします。PAN-OSアプライアンスのCLIを使用するにはSSHアクセスが必要です。

- PAN-OS 装置がExpeditionに接続されている場合、設定を部分的に、あるいは全体を装置に送信するためにAPIコールを使用することができます。

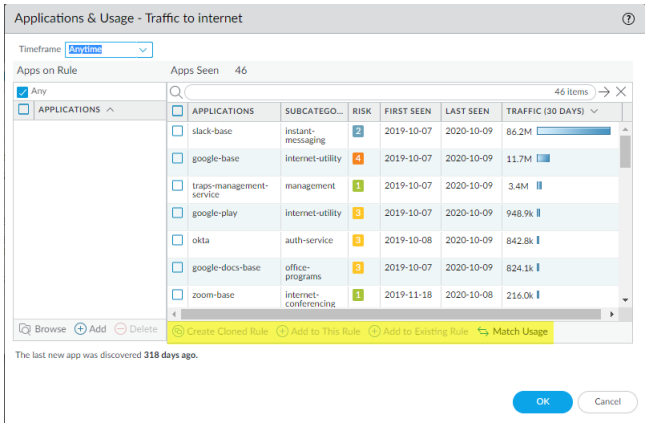
STEP 11 | 結合した設定をPAN-OSアプライアンスにエクスポートし、コンフィギュレーションをロードした後、ポートベースポリシーをアプリケーションベースポリシーに変換するためにポリシー オプティマイザーを使用します。

# ポリシー オプティマイザーを使ってアプリケーション ベース・ポリシーに移行

既存のコンフィギュレーションをPAN-OSアプライアンスに移行するためにExpeditionを使用した後、次の段階はApp-IDベースセキュリティポリシールールへの移行を単純化するためにポリシー オプティマイザーを使用することです。ポリシー オプティマイザーはレガシーポートベースルールからの変換をより簡単にします。なぜなら、情報を理解するために必要な個々のルールのアプリケーション情報を自動的に提示し、一回のビューでインテリジェントなアプリケーションベースルールを生成するからです。ポリシー オプティマイザー：

- 各ルール用のトラフィックで発見される全てのアプリケーションを自動的に学習・記憶し、ログデータを精読・分析する必要がなくなります。もし仮にログが繰り越したとしても、ポリシー オプティマイザーはアプリケーション情報を保持するので、全てのアプリケーションがルールに則っていることが把握できます。
- アプリケーションの利用可能性を脅かすことなく安全にApp-IDを移行することができます。
- それはPAN-OSアプライアンスに対して標準でありサポートされているので、アプライアンスと非標準ツールとの間で設定やデータを移動させる必要はありません。
- どのルールが最初に変換するのに最も簡単で安全かを識別し、優先順位付けするのを支援する簡単で、直観的なsorting and filtering options(ソートおよびフィルタリングオプション) を提供します。
- 個別の次世代ファイアウォールと同様にPanorama装置でも実行できます。次世代ファイアウォールをPanoramaでPAN-OS 8.1上で実行するよう管理しているのであれば、Panorama（および管理されたファイアウォールに接続されているすべてのログコネクタ）をPAN-OS 9.0にアップグレードするだけでポリシー オプティマイザーを使用し、その恩恵を受けることができます。これにより、すべてのファイアウォールで検査するよりも素早くポリシー オプティマイザーで検査することができます。

これらの機能は、時間を節約し、ポートベースルールをApp-IDベースルールに変換する時の工ラーを防ぐ、簡単に使用出来るツールとなります。ポリシー オプティマイザーはルールを変換するいくつかの方法を提供します：




- **Create Cloned Rule**（複製ルールを生成する）–ルールを複製するとオリジナルのポートベースルールを維持しながら、新しいApp-IDベースルールが複製されたルールの上に来るようになります。一つのポートベースルールから複数のApp-IDベースルールを複製することができます。例えば、アプリケーションサブカテゴリに基づいた複数のApp-IDルールを、一般ウェブブラウジングルールから、同様のアクセスおよび脅威への措置が要求されるグループアプリケーションへ複製することができます。これは、すべてのユーザー・場所からのアクセスを制限する、一般的なセキュリティが脆弱なルールによるウェブアクセス制御の代わりとなります。

  複製されたルールの下にあるポートベースルールがセーフティネットとして機能するので、アプリケーションの利用可能性にリスクはありません。複製された(App-ID)ベースのルールが許可したいすべ

てのアプリケーションと一致しない場合は、それらのアプリケーションが複製されたルールの下にあるポートベースルールにヒットするため、調整することができます。許可したいポートベースルールと合理的時間内で合致するトラフィックが無い時に、ルールをApp-IDベースのルールへの変換を完了することにより、ポートベースルールを除去することができます。

- **Add to This Rule**（このルールに追加）–アプリケーションをルールに追加しポートベースのルールをApp-ID ベースのルールで置き換え、ポートベースのルールをルールベースから削除し、Cloneが提供するセーフティーネットを提供しない状態にします。**Add to This Rule**（このルールに追加）は、ルールが制御する全てのアプリケーションを確実なものであると確信している場合のみ使用します。アプリケーションが少数のみであり、ビジネスで必要アプリケーションであることを確信しているルールについては、**Add to This Rule**（このルールに追加）の候補となります。多くのアプリケーションが発見されたルールや許容したいルールが将来見られる可能性があるルールは複製しておくのが最も安全です。アプリケーションをルールに追加することが出来なかった場合、ポートベースルールをセーフティネットとして保持している他のルールが許可しない限り、ルールを複製するとそのアプリケーションは利用できなくなります。
- **Add to Existing Rule**（既存のルールに追加）–既存のルールにアプリケーションを追加しても、オリジナルのポートベースのルールは変更されません。引き続き、ルールベース内に残ります。**Add to Existing Rule**（既存のルールに追加）を利用すると、以前に設定したルールを選択して、それにアプリケーションを追加することができます。

  アプリケーションを既存のアプリケーションベースのルールに追加すると、ファイアウォールはそれらのアプリケーションをポートベースのルールから削除して、選択したアプリケーションベースのルールに追加します。追加されたアプリケーションは、アプリケーションベースのルールにあるその他のアプリケーションと同様に、同じソース、宛先、サービスなどを使用します。

  アプリケーションを他の既存のポートベースのルールに追加した場合、ファイアウォールはそのアプリケーションを元のポートベースのルールから削除し、それを他のポートベースのルールに追加します。これにより、他のポートベースのルールを、ルールに追加したアプリケーションのみを制御するアプリケーションベースのルールに変換します。ポートベースのルールの一部をこの方法で変換する場合は、ルールに移動し、サービスを application-default に変更して、アプリケーションが非標準ポートを使用しないようにします（ルールで設定されたサービスがアプリケーションと一致しない場合もあります）。
- **Match Usage**（使用の一致）–ポートベースルールの使用を一致させると、ポートベースのルールはそのルールで発見されたすべてのアプリケーションを含むApp-IDベースルールで置き換えます。**Match Usage**（使用の一致）は、ルールが厳格なビジネス目的の良く知られた少数のアプリケーションで確認される時のみ使用します。良い例は、SSHトラフィックのみ許可するTCPポート22です。SSH がポート22のポートベースルールで発見される唯一のアプリケーションである場合、**Match Usage**（使用の一致）を使用し、安全にルールをApp-IDルールへ変換できます。

**Create Cloned Rule**（複製されたルールを生成する）、**Add toThis Rule**（このルールに追加する）、または**Add to Existing Rule**（既存のルールに追加する）をするには、**Apps Seen**（発見されたアプリケーション）から少なくとも一つを選択しなければなりません。

四半期あるいは年次用でのみ使用されるアプリケーションは、履歴が最後のアクティビティを取り込むために十分な長さではないので、アプリケーション情報には現れません。ルールを変換する際はこれらのアプリケーション種類に注意してください。

ポートベースルールをアプリケーションベースルールに変換する時、ポリシー オプティマイザーはサービスをApp-IDのものに変換する以外の変更はしません。ルールを変換した後、多くの場合は、**Service**（サービス ）を **application-default**（アプリケーションデフォルト）に変更すべきです。そうすると、ポートを合法的に使用しているアプリケーションのみがアクセスでき、曖昧なアプリケーションが非標準のポートを使用したネットワークアクセスを防ぐことができます。

ビジネスが、特定のクライアントとサーバー間の非標準ポートにある内部カスタムアプリケーションのようなアプリケーションを許可する必要がある場合、例外を求められるアプリ

ケーション、ソース、および相手先のみに限定すべきです。カスタムアプリケーションをアプリケーションデフォルトのポートに書き換えることを検討します。

ポートベースルールをApp-IDベースルールに変換するためにポリシー オプティマイザーを使用する前に：

1. Palo Alto Networks次世代ファイアウォールあるいはExpeditionからのPanorama装置へのレガシー設定の like-for-like migration (同一条件下の移行) を完了します。
2. ルールをApp-IDへの変換を開始する約一週間前までの期間、現用ネットワークでPAN-OS 9.0を実行します。これにより、装置はネットワーク上のアプリケーションを学習し分類し始めます。いくつかの単純なルールは素早く変換することができるのに対し（例えば、ポート22ルールはSSHトラフィックのみを許可し、簡単に変換できます）、インターネットアクセス（ポート 80/433）のルールなどは、他のルールよりも長期間、ファイアーウォールにトラフィックからアプリケーションデータ収集させる必要があります。
3. 進捗を比較するベースラインをセットするために Best Practice Assessmen(ベストプラクティスのアセスメント) (BPA) を実行します。
4. 現実的なゴールをセットします。どのような終了結果を得たいのか考えます。ゴールに到達した時、ゴールに到達したことを確認し、更に前に進めるか、ネットワークを更に安全にできるかを確認するために再びBPAを実行します。ポリシー オプティマイザーではセキュリティの可用性を犠牲にはしません。セキュリティを強化するだけです。

ルールをフェーズで変換します。PAN-OSアプライアンスが少なくとも一週間のログ（ポリシー オプティマイザーはログを読むことでルール上で発見されるアプリケーションを発見します）を取得した後、よく知られたアプリケーションを許可するポートベースルールをApp-IDベースルールに変換することができます。多くのアプリケーションが見られる他のルール、例えば一般ウェブアクセスルールのようなもの、に関しては、アプリケーション情報を集めるのに最低３０日待ちます。

プロフェッショナルサービス は移行に関に関して熟練しています。レガシー装置から*Palo Alto Networks*次世代ファイアウォールと*Panorama*装置の設定への移行を支援するプロフェッショナルサービスを利用することができます。

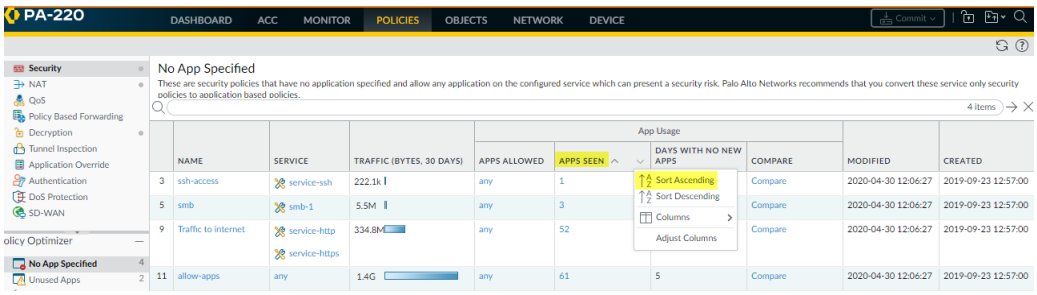
- 1週間後ウェルノウンアプリケーションについて簡単なルールを変換する
- 30日後に変換を開始するルール

## 1週間後ウェルノウンアプリケーションについて簡単なルールを変換する

実環境トラフィックを1週間モニタリングした後、単純なポートベースルールからApp-IDベースルールへの変換を安全に開始することができます。簡単なルールでどのアプリケーションを許可するかを決めるのはとても容易なので、その候補としては、ポートを正当に使うことができるのが1個または少数のウェルノウンアプリケーションに対するルールが挙げられます。例： ポート21 (FTP)、ポート22 (SSH)およびポート53 (DNS)。

PAN-OSアプライアンスに最新のアプリケーションシグネチャがあることを確かにするため、ルールの変換を始める前に、最新の Content Updates (コンテンツアップデート)をインストールします。この例では、ポートベースルールをソートして、安全な変換の候補およびポートベースルールを直接App-IDベースに変換するためのオプションを見つける方法を紹介します。

STEP 1 | **Policies**（ポリシー）> **Security**（セキュリティ）> **Policy Optimizer(ポリシー オプティマイザー)** > **No App Specified**（アプリの指定なし）において、**Apps Seen**（発見されたアプリ）と**Sort Ascending**（昇順にソート）（または**Apps Seen**（発見されたアプリケーション）をクリックして現在の表示順序を逆にする）を選択することにより、検出アプリケーションが最も少なかったポートベースのルールを見つけます。

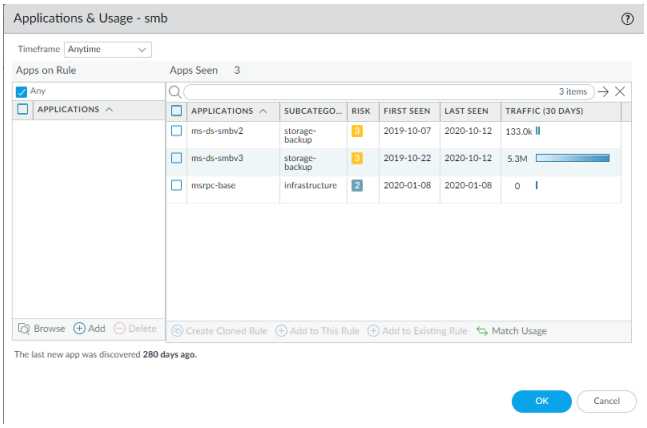



発見されたアプリケーションが最も少なかったポートベースのルールは、**No App Specified**（アプリの指定なし）表示の最上位にあります。SSHのような特定のサービス用のルールをアプリケーションベース ルールに直接安全に変換し、アプリケーションがほとんど発見されなかったルールを調べて安全に変換されたかどうかチェックすることができます。

Server Message Block（サーバーメッセージブロック - SMB）トラフィックを許可することを意図したポートベースのルールは、設定をPAN-OSアプライアンスに移行した後アプリケーションを3個しか発見していないので、変換の候補となります。

STEP 2 | **Apps Seen**（発見されたアプリ）数または**Compare**（比較）をクリックし、ルールについて発見されたアプリケーションを調査します。

**Applications & Usage**（アプリケーションと使用状況）には、ルールに合致するトラフィックで発見されたアプリケーションが表示されます。



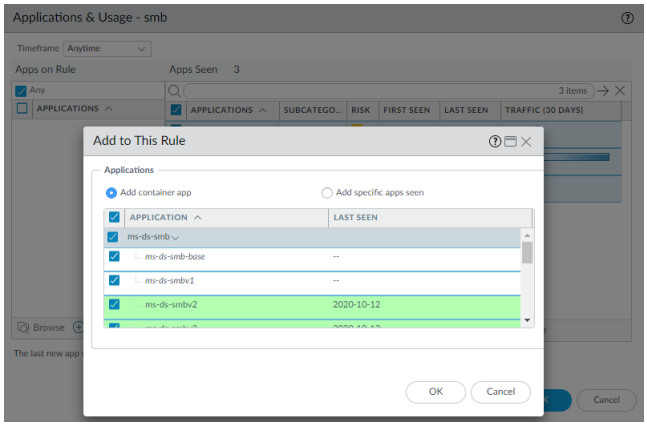

STEP 3 | ルールについて発見されるアプリケーションのすべてもしくはいくつかを許可する、または一切許可しないかを決定し、許可したいアプリケーションを選択します。

ルールの正確な使用をマッチさせる、コンテナアプリを追加することにより将来も有効に使い続けられるルールを提供する、またはルールに追加すべき個別のアプリケーションを選択することができます。

- ルールにマッチされる通りにすべてのアプリケーションを許可するルールとしたい場合には、以下によります：
  1. **Apps Seen**（発見されたアプリ）においてすべての**Applications**（アプリケーション）を選択します。
  2. **Match Usage**（使用法のマッチング）をクリックします。
  3. **OK**をクリックして、ポートベースのルールをApp-IDベースのルールに変換します。
  4. 潜伏する悪意あるアプリケーションがポートを使うことがないように、**Service**（サービス）を**application-default**（アプリケーションデフォルト）に設定します。

- ルール上で発見されるアプリケーションをすべてまたは一部を許可し、コンテナアプリケーションを追加することにより、将来も有効に使い続けられるルールを提供したい場合（それにより、各コンテナ内のすべてのアプリケーションが許可され、将来コンテナアプリケーションに追加されるアプリケーションが自動的に許可される）：

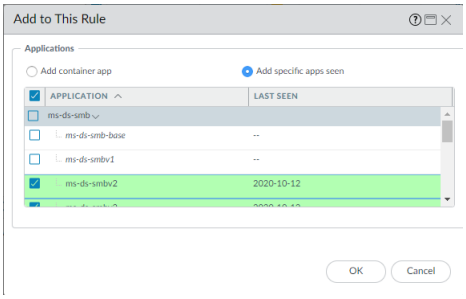
  1. すべてのアプリケーションを選択し、次に**Add to This Rule**（このルールに追加）を選択します。



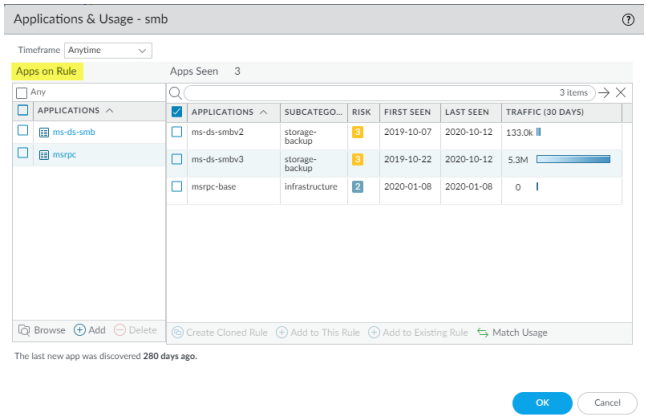

     灰色に色付けされたアプリケーションは、コンテナアプリです。緑に色付けされたアプリケーションは、ルールで発見されたアプリケーションです。色付けされていないアプリケーションは、同じコンテナアプリに属していますが、ルールでは発見されていません。

     デフォルトでは、**Add container app**（コンテナアプリケーションの追加）が選択されているため、コンテナ内のすべてのアプリケーションもデフォルトで選択されます。

  2. ルールに一致するアプリケーションのみを含めるようにしたい場合は、**Add container app**（コンテナアプリケーションの追加）を選択します。ルールで発見されたアプリケーションのみが、ルールに追加されます。コンテナアプリケーションと、ルールに一致しないアプリケーションは選択されません。ルールで発見されたアプリケーションのみを選択するには、**OK**をクリックします。




     コンテナアプリケーションと、そのルール内のすべてのアプリケーションを含める場合は、選択内容を**Add container app**（コンテナアプリケーションの追加）のままにして、**OK**をクリックします。コンテナアプリケーションに含まれているすべてのアプリケーションを含む（許可する）ため、**Apps on Rule**（ルールのアプリケーション）にはコンテナアプリケーションのみが表示されます。 将来的にコンテナへのアプリケーションの追加を許可するため、ルールを将来も使用することができます。

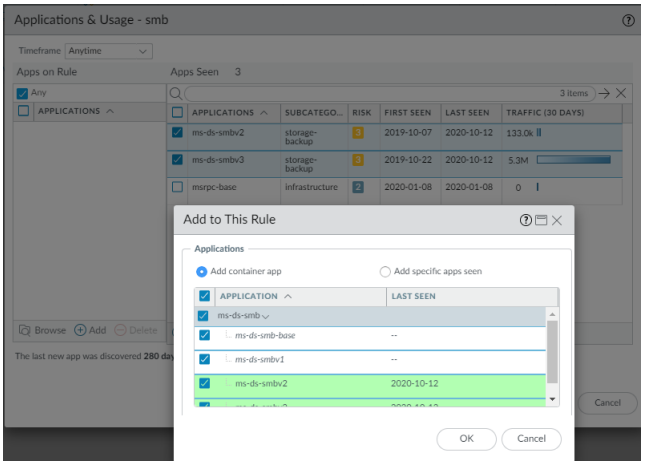



3. **Usage**（使用状況）タブで**OK**をクリックして、ルールを変換します。
4. 潜伏する悪意あるアプリケーションがポートを使うことがないように、**Service**（サービス）を**application-default**（アプリケーションデフォルト）に設定します。

- コンテナアプリ内で許可するアプリケーションを選択したい場合には、それらアプリケーションを選択し、**Add to This Rule**（このルールに追加）をクリックします。例えば、msrpc-baseを許可しないよう決定し、ms-ds-smbv2とms-ds-smbv3だけを選択し、**Add to Rule**（ルールに追加）を実行すると、ポリシー オプティマイザーは、コンテナアプリ(ms-ds-smb、グレーの網掛け) 内の関連アプリケーションを表示し、これらのアプリケーションを追加することによって将来も有効に使い続けられるルールを提供します：

  1. 許可したいアプリケーションを選択し、**Add to This Rule**（このルールに追加）をクリックします。

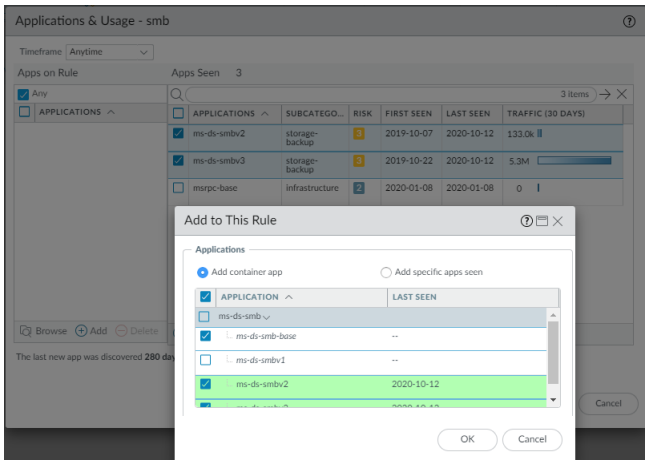
     例えば、msrpc-baseを許可しないよう決定し、ms-ds-smbv2とms-ds-smb3だけを選択し、**Add to This Rule**（このルールに追加）を実行すると、ポリシー オプティマイザーは、コンテナアプリ(ms-ds-smb、グレーの網掛け) 内の関連アプリケーションを表示し、現在および将来のすべてのアプリケーションを持つコンテナアプリケーションによって、将来も有効に使い続けられるルールを提供します：




     緑に色付けされたアプリケーションは、ルールで発見されたアプリケーションです。色付けされていないアプリケーションは、同じコンテナアプリに属していますが、ルールでは発見されていません。
  2. すべてのアプリケーションを許可することも、アプリケーションを選択して許可することもできます。

すべてのコンテナアプリケーション、およびその現在および将来のすべてのアプリケーションを許可するには、**OK**をクリックします。**Apps on Rule**（ルールのアプリ）は、選択されたアプリケーションすべてを表示します。**OK**をクリックしてルールを変換します。

選択したアプリケーションだけを許可するには、望まないアプリケーションの選択を外します。コンテナ内の1つのアプリケーションの選択を解除すると、コンテナアプリ自体も選択を解除されるので、中に含まれるアプリ（子アプリ）を自動的に許可することがなくなります。




3. **OK** をクリックします。**Apps on Rule**（ルールのアプリ）は、選択されたアプリケーションすべてを表示します。
4. **OK**をクリックしてルールを変換します。
5. 潜伏する悪意あるアプリケーションがポートを使うことがないように、**Service**（サービス）を**application-default**（アプリケーションデフォルト）に設定します。

## 30日後に変換を開始するルール

本番トラフィックの30日間のモニタリングの後、残りのポートベースルールをApp-IDベースルールに変換と、ルールベースをクリーンアップを安全に始めることができます。最初に始めると良いのは攻撃可能な箇所を縮小する未使用のルールをクリーンアップすることです。その後、アウトバウンドインターネットアクセス（ポート80/443）ルールでルールをApp-IDへの変換を始めます。なぜなら、そのルールは，他のどのルールよりも多くのアプリケーションで多くのトラフィックを見ることができるからです。それはまたこのルールが最も多くのリスクを抱えることを意味します。

PAN-OSアプライアンスに最新のアプリケーションシグネチャがあることを確かにするため、ルールの変換を始める前に、最新の Content Updates (コンテンツアップデート)をインストールします。

ポリシー オプティマイザーはソート、フィルタ、どのルールを最初に変換するかの優先順位付けなどへの直観的な方法を提供します。使われないルールを削除することで、ウェブアクセスルールをApp-IDに変換した後、優先事項として選ばれるルールはビジネスとセキュリティ要件によります。下記のセクションは、最初の30日間の後変換するためにルールを識別し、優先付けする単純ながらパワフルなソーティングとフィルタリングのアイデアと方法を提供します：

- 使われないルールを削除する
- 最も安定したルールを変換する
- インターネットアクセスルールを変換
- 検出されたトラフィックが最も多いルールを変換
- 一定期間で発見されたアプリが少ないルールを変換する

## 使われないルールを削除する

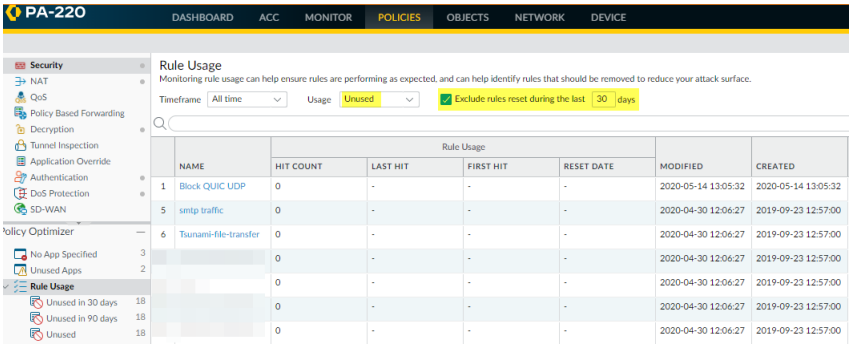
移行したルールベースはしばしば使用していないルールを含んでいます。なぜならこれらのルールに合致するアプリケーショントラフィックが無いからです。未使用のルールはルールベースを混乱させ、しばしば敵対者に攻撃の道を開けてしまいます。ルールベースをクリーンアップするためこれらのルールを除去して攻撃可能な箇所を縮小します。あるいは修正してアプリケーショントラフィックに適用しルールベースの合法的な目的で機能させるようにします。

未使用のルールは様々な理由で存在するかもしれません。ビジネスが一度は使用したが他のアプリケーションで置き換えられたサービスとアプリケーションを管理するルールがルールベースに存在します。未使用のルールより上位にあるルールは、場合によっては未使用のルールに合致するアプリケーションを制御するかもしれません。場合により、未使用のルールは、すでに会社を退社した管理者により作成された古いルールであり、現在の管理者にルールの意図を知るものがいない場合があります。

**Timeframe**（時間枠）内でのルールを閲覧するため、（**Policies**（ポリシー）> **Security**（セキュリティ）> ポリシー オプティマイザー > **Rule Usage**（ルール使用）)を選択します。アプリケーショントラフィックに見られるルールをフィルターするため **Usage**（使用）を**Unused**（未使用）に設定します。

STEP 1 | 未使用ルールを識別します。

**Policies**（ポリシー）> **Security**（セキュリティ）> ポリシー オプティマイザー > **Rule Usage**（ルール使用）において、**Timeframe**（時間枠）を**All time**（いつも）に設定し、**Usage**（使用）を**Unused**（未使用）に（ヒットカウントゼロのルールのみ表示するために）および**Exclude rules reset during the last 30 days**（最近30日間でリセットされたルールは除く）に（最近の数日間ではトラフィックが見られないが、より長い期間ではトラフィックで見られる最近リセットしたルールが表示されるのを防ぐため）設定します。結果は、選択された **Timeframe**（時間枠）でアプリケーショントラフィックが見られなかったルールのリストです。




STEP 2 | トラフィックが見られなかったルールを評価し、必要かどうか、または無効化できるかどうかを決定します。

この例では、企業は過去にTsunamiファイル転送を使用しましたが、調査の結果、企業はもはやTsunamiを使用していないことを示しています。従ってTsunamiアプリケーションによるネットワーク上のトラフィックを使用を許可する理由がありません。

STEP 3 | ルールを**Disable**（無効化）または **Delete**（削除）します。

**Policies**（ポリシー）> **Security**（セキュリティ）で、Tsunamiファイル転送ルールを選択し、ルールを**Disable**（無効化）または**Delete**（削除）します。

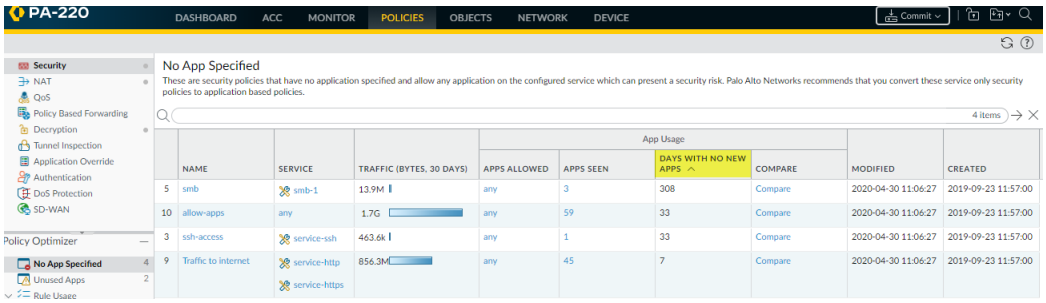
トラフィックでしばらく見られなくてもビジネスでそのアプリケーションが必要となる場合があるので、ルールを無効化することはより安全な方法です。（これは、四半期および年単位のイベントを考慮せずにビジネスがアプリケーションを使用するか否かを調査したり、定期的にしかトラフィックがネットワークにアクセスしない契約者やパートナーが必要とするアプリケーションが存在する場合に起こり得ます。）合理的な時間経過の後、以前に無効化した使われないルールを削除してください。

## 最も安定したルールを変換する

一定期間新しいアプリケーションが発見されなかったポートベースルール、したがって安定化しており新しいアプリケーションを発見する可能性が低いルールを変換します。後日ルールに合致するアプリケーションがさらに出現した場合、安全措置として必要な期間ルールベースにポートベースルールが残っていることを保証すべく、これらのルールを複製します。

新しいアプリケーションがルールに合致するかどうかを判断するにあたっては、*3*ヶ月ごと、*1*年ごと、その他定期的なイベントで使われるアプリケーションだけを考慮にいれます。

STEP 1 | **Policies**（ポリシー）> **Security**（セキュリティ）> ポリシー オプティマイザー > **No App Specfied**（指定されたアプリなし）において、ルールを**Days with No New Apps**（新しいアプリが発見されなかった日数）の最高値が一番上に来るよう、下降順にソートします。

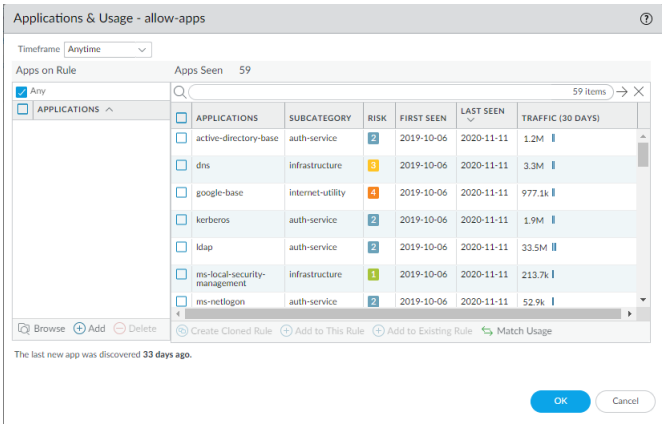



最初の 3 つのルールは、30日以上新しいアプリケーションを発見しておらず、App-ID への変換候補となります（「1週間後ウェルノウンアプリケーションについて簡単なルールを変換する」には、smb ルールなどの、**Apps Seen**（発見したアプリケーション）がほとんどないルールの変換について説明しています。そのため、この例ではアプリケーションの許可ルールに重点を置いています）。

長期間修正されていないルールもまたより安定している場合が多いので、*Modified*（修正）日付をチェックします。最近修正されたルールは、ルールにマッチするアプリケーションをすべて発見しているとは限りません。

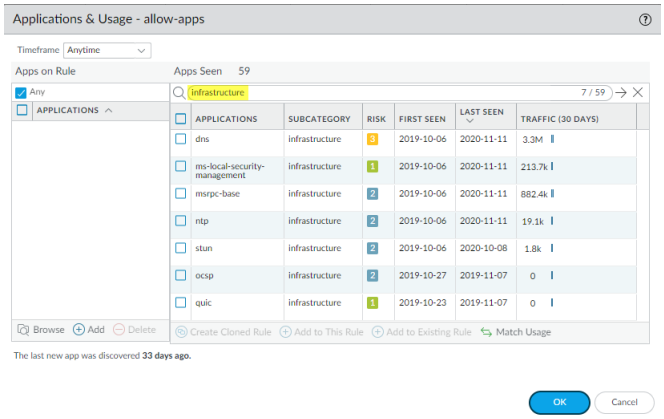
ルールについて発見されたアプリケーションが少なからずありますので、それを直接App-IDベースのルールに変換する代わりに、そのルールを複製します。

STEP 2 | **Apps Seen**（発見されたアプリ）数をクリックして**Applications & Usage**（アプリケーションと使用状況）ダイアログを開きます。



STEP 3 | ルールについてApps Seen（発見されたアプリ）をソート・フィルタリングして、それらアプリケーションをどう扱うか決定します。

サブカテゴリによってソートまたはフィルタリングすることで、アプリケーションを少なからず発見したルールの上に現れるトラフィックを理解する一助になります。例えば、インフラサブカテゴリでフィルタリングすることにより、すべてのインフラアプリケーションを発見し、それらを制御するためのApp-IDベースのルールを複製することができます。




STEP 4 | 「インターネットアクセスルールを変換」のステップ4～ステップ7に従い、同じ取扱いを適用したいアプリケーション・サブカテゴリ（または複数の関連サブカテゴリ）を制御する複製ルールを作成します。

## インターネットアクセスルールを変換

インターネットアクセス・ルールは、ポート80 (HTTP)およびポート443 (HTTPS)のトラフィックを制御します。このルールは通常、アプリケーションが最も多く、トラフィック量（バイト数）も最大です。ポートベースのインターネットアクセスルールは、ネットワークに不要なアプリケーションを許可し、攻撃に晒される可能性があります。ポートベースのアクセスルールを、一連のアプリケーションベースのルールに変換することにより、それらのポートで許可するアプリケーションを制御し、安全に有効化してください。そのためには、企業が、業務上どのアプリケーションを認可し、そして、他の目的では、どのアプリケーションを許容するかを理解する必要があります。

変換方法として、ルールベースの肥大化を防止する観点から、個々のアプリケーションごとに個別のルールを生成する代わりに、類似した処理を必要とする複数のアプリケーションをグループにまとめるのが良い方法と言えます。ポリシー オプティマイザーを使ってルール内で発見されたアプリケーションをアプリケーションサブカテゴリでソートします。それにより、特定のサブカテゴリごとにルール対象にするすべてのアプリケーションを発見し、業務で使うアプリケーションを選択し、それらのアプリケーションを制御するルールを複製することができます。ポリシー オプティマイザーには、ルール内で発見されたアプリケーションを編成し分析するためのソートおよびフィルタリングのオプションが多数用意されています。

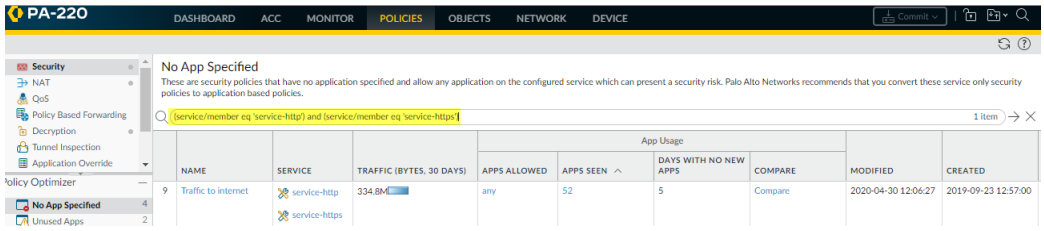
アプリケーションがすぐ使えるようにするために、ルールを直接変換するよりは、複製すると良いでしょう。ルールを複製することにより、元のポートベースルールが保存され、セキュリティ・ルールベースにおいて、ポートベースルールのすぐ上に複製されたアプリケーションベースのルールが置かれます。アプリケーションの使用に支障をきたすことなく、異なる扱いをしたい複数のアプリケーション・グループに対して、元のポートベースルールから、異なるインターネットアクセス・ルールを作成します。どのアプリケーションが複製されたルールにマッチし、どのアプリケーションが元のポートベースルールへフィルターされるかをチェックして、必要に応じてルールを調整します。許可したいアプリケーションのどれも、十分長い期間（業務に必要なアプリケーションをすべて網羅したと確信できる十分な時間）ポートベースルールにマッチしなかった場合には、ポートベースルールを無効化（または削除）します。この場合、アプリケーションの利用に支障をきたすことなく、変換が終了します。

この方法は、いくつかのウェルノウンアプリケーションよりも多く確認された他のルールを変換する際に使用します。インターネットアクセス・ルールを変換した後に、変換すべきルールの優先順位づけをするには、**Policies**（ポリシー）> **Security**（セキュリティ）> **Policy Optimizer** (ポリシー オプティマイザー) > **No App Specified**（アプリケーションが指定されていない）情報を使用します。例えば、最も使用されているルールを変換するために、最も**Apps Seen**（発見されたアプリ）、過去30日間の最も多いトラフィック（トラフィック（バイト、30日間））の組合せで優先順位をつけることもできますし、もしくは、**Days with No New Apps**（新しいアプリケーションが確認されなかった日数）と**Modified**（修正）日をチェックして、多くのアプリケーションで確認されいるが、安定しているルールを見つけるともできます。

この例では、 ポートベースのインターネットアクセス・ルールから、一般的なビジネスアプリケーションを制御するアプリケーションベースのルールを複製する方法を示しています。この同じ複製手順を使って、ポートベースルールで確認される様々なサブカテゴリや個別アプリケーションに対して、安全にアプリケーションベースのルールを作成してください。

STEP 1 | **Policies**（ポリシー）> **Security**（セキュリティ）> ポリシー オプティマイザー > **No App Specfied**（アプリケーションが指定されていない）に移動し、インターネットアクセスを制御するポートベースのルールを探します。

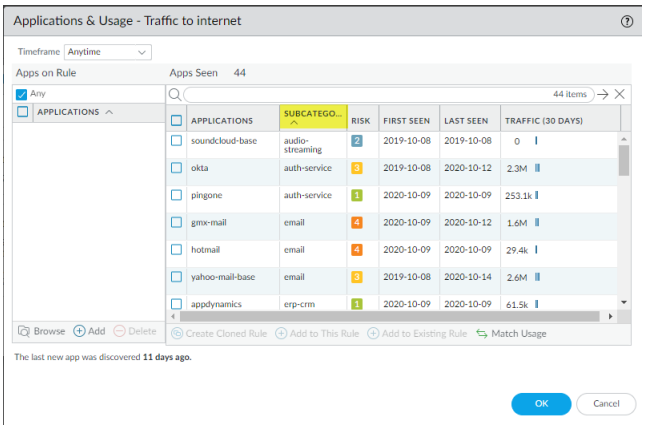
フィルタ**(service/member eq 'service-http')**および**(service/member eq 'service-https')**を使って、**service-http**および**service-https**（これらはインターネットアクセス・ルール）に関して設定されたポートベースルールを探します。




STEP 2 | **Compare**（比較）または**Apps Seen**（発見されたアプリ）数をクリックして**Applications & Usage**（アプリケーションと使用状況）ダイアログを開きます。

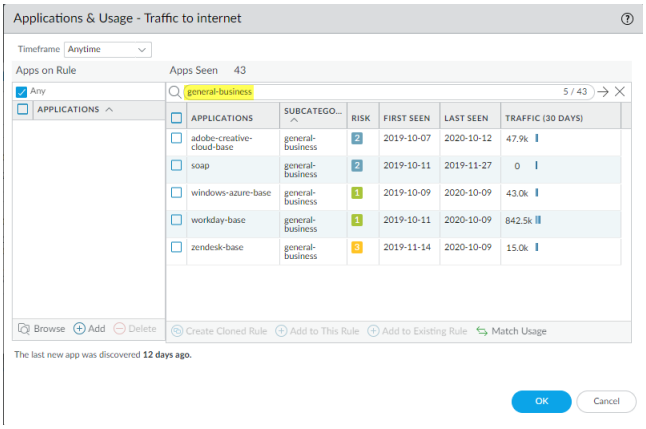
STEP 3 | 同じセキュリティポリシー・ルールで管理する方が適切である類似アプリケーションをグループ化する場合は、アプリケーションサブカテゴリで**Apps Seen**（発見されたアプリ）をソートします。

下記ルールで発見されるアプリケーションをグループ化する場合は、**Subcategory**（サブカテゴリ）でソートします：



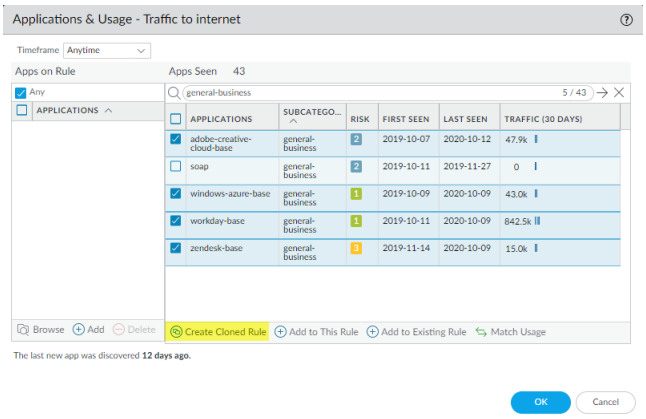

特定のサブカテゴリでフィルタリングして、そのサブカテゴリに属するアプリケーションだけを発見することもできます。この例では、一般的なビジネスアプリケーション制御するためのApp-IDベース

のルールを作成するために、ルール上で発見される一般的なビジネスアプリケーションのみを表示するようフィルタリングをします：




STEP 4 | 許可したいアプリケーションを選択し、次に**Create Cloned Rule**（複製ルールを生成）を選択して、ポートベース・ルールからアプリケーション・ベースの新しいルールを複製します。

この例では、この会社は4つのアプリケーションを使用しますが、そのうちの1つのアプリケーションは、長期間使用されていません。これについては、**Last Seen**（前回確認）および**Traffic**（**30 Days**）（**30**日間のトラフィック）列で確認することができます。利用状況および会社が認可したアプリケーションに基づいて、会社は、この使用されていないアプリケーションを許可しないことを選択します。

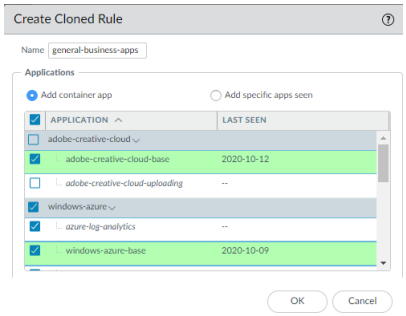



STEP 5 | **Clone**（複製）ダイアログにおいて、許可したい各コンテナ アプリケーションに関連するアプリケーションを選択します。

新しいルールに、その目的を示す分かりやすい**Name**（名前）を指定します。この例では、「general-business-apps」としています。各コンテナアプリケーションから特定のアプリケーションのみを許可するのか、またはコンテナアプリケーションを許可するのかを決定します。コンテナアプリを許可すると、そのコンテナ内のすべてのアプリケーションを許可することになります。これにより、新しいアプリケーションがコンテナアプリに追加されると、その新しいアプリケーションを自動的に許可することになり、将来も有効に使い続けられるルールを提供し、アプリケーションがいつでも使えるのを保証することになります。デフォルトでは、すべてのアプリケーションが選択されています。コンテナアプリは灰色で網掛けされ、ルール上で発見されたアプリケーションは緑色に網掛けされ、コンテナアプリ内でまだルール上で発見されていないアプリケーションはイタリック体であり、網掛けされていません。

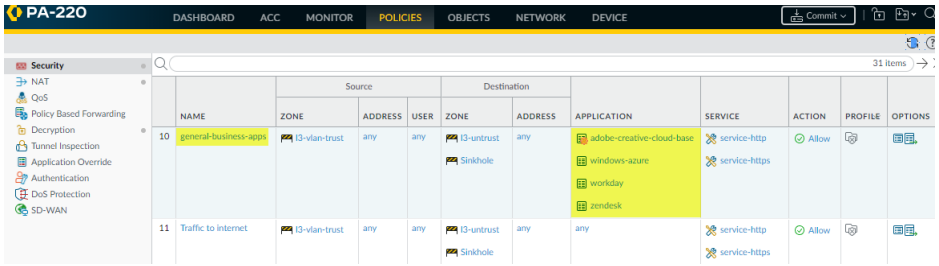
この例の図では、灰色で網掛けされたコンテナアプリ “adobe-creative-cloud”および“windows-azure”、ルール上で発見された緑色に網掛けされたアプリケーション（“adobe-creative-cloud-base”およ

び“windows-azure-base”）、そして、ルール上で発見されていない2つのアプリケーションがイタリック体（“adobe-creative-cloud-uploading”および“azure-log-analytics”）で表示されています。この例は、アプリケーション“adobe-creative-cloud-uploading”は選択されておらず、そのコンテナアプリケーション（“adobe-creative-cloud”）も自動的に選択されない一方で、“windows-azure”アプリケーションはすべて選択された状態で、“windows-azure”コンテナアプリケーションも選択されている状態になっていることを表しています。




ユーザーを特定のアプリケーションにアクセスさせたくない場合は、そのアプリケーションの選択を解除してください。ただし、“adobe-creative-cloud”コンテナアプリケーションに新しいアプリケーションが追加された場合、コンテナアプリケーションの選択は解除されているため、ファイアウォールがそのアプリケーションを自動的に許可することはありません。反対に、“windows-azure”コンテナアプリケーションに新しいアプリケーションが追加された場合、ファイアウォールは自動的にそれを許可し、将来的にも有効になります。

STEP 6 | **OK**をクリックして、セキュリティポリシールールのUsage（使用）タブに戻り、もう一度**OK**をクリックしてルールを作成します。ファイアウォールはルールを、セキュリティポリシー・ルールベース（**Policies**（ポリシー）> **Security**（セキュリティ））内のポートベースルールの上に配置します。




コンテナアプリケーションを選択した場合、コンテナアプリケーションにはすべてのアプリケーションが含まれているため、Policy Optimizerはコンテナアプリケーションのみをルールに追加します。“adobe-creative-cloud-base”の赤い歯車は、それがコンテナアプリケーションではなく、個別のアプリケーションであることを表しています。

STEP 7 | 潜伏アプリケーションが非標準ポートでアクセスに成功すること止するには、ルール**Name**（名前）または**Service**（サービス）をクリックし、**Service**（サービス）を**application-default**（アプリケーションデフォルト）に変更します。

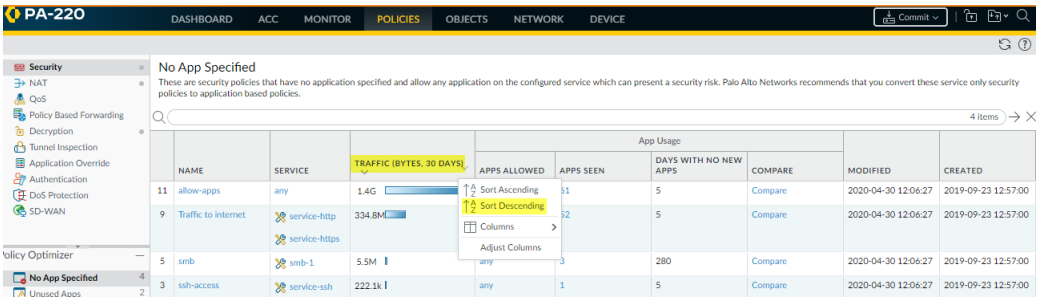
STEP 8 | 他の認可されている一般業務アプリケーションを許可する必要がある場合は、それをgeneral-business-appsルールに追加して、それが不要になったらルールからアプリケーションを削除してください。

## 検出されたトラフィックが最も多いルールを変換

過去30日間に最も多くのトラフィック量を検出したルールを求めるようソートすることにより（**Traffic (Bytes, 30 days)**（トラフィック（バイト、30 日間））、現在最もアクティブなルールを表示します。（時間間隔をそれ以上長く設定すると、最近のトラフィック量が少なくなっていても以前からの累積トラフィック量が影響して、古いルールが上位に表示されることがあり、誤った判断の基になりがちです。）これらのルールをApp-IDベースのルールに変換することで、最大限のトラフィックを保護することができます。

複数のルールで多くのトラフィックを検出する場合には、**Policies**（ポリシー）> **Security**（セキュリティ）> ポリシー オプティマイザー > **No App Specified**（アプリケーションが指定されていない）情報を使用して、最初に変換すべきルールの優先順位づけをします。例えば、**Apps Seen**（発見されたアプリ）（潜在的にリスクが最も高いルール）を使ったルールまたは、**Days with No New Apps**（新しいアプリがゼロであった日数）最長と**Modified**（修正）日が最も古い（最も安定した高トラフィック・ルール）を組み合わせたルールを使って優先順位づけをすることができます。

STEP 1 | **Policies**（ポリシー）> **Security**（セキュリティ）> ポリシー オプティマイザー > **No App Specfied**（指定アプリなし）において、ルールを、**Traffic (Bytes, 30 days)**（トラフィック（バイト、30 日間））の下降順にソートし、最近にアクティブであったルールがリストの最上位に表示されるようにします。




STEP 2 | 変換を開始するルールを1つ選択し、**Apps Seen**（発見されたアプリ）数をクリックします。

STEP 3 | **Applications & Usage**（アプリケーションと使用状況）ダイアログにおいて、そのルールの**Apps Seen**（発見されたアプリ）をソートしフィルタリングをかけ、アプリケーションをどう取り扱うかを決定します。

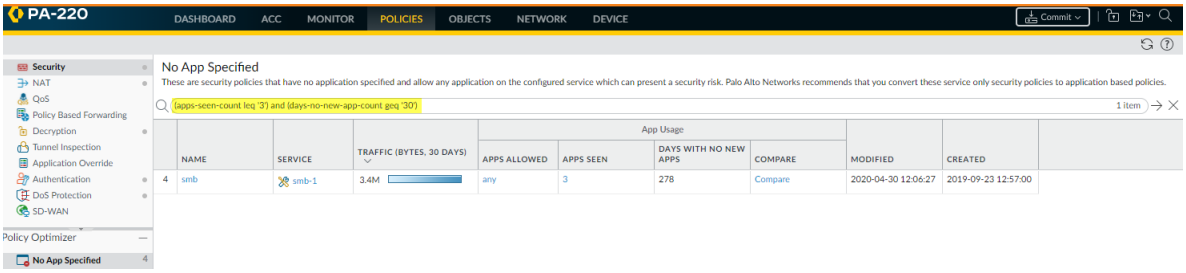
アプリケーション・サブカテゴリでソートまたはフィルタし、類似の扱いを必要とする可能性があり1つのアプリケーションベースのルールで制御可能な複数のアプリケーションをグループ化します。**Traffic (30 days)**（トラフィック（30 日間））でソートして個別アプリケーションの最近のトラフィック量をチェックし、現在最もアクティブなアプリケーションを優先順位づけします。

STEP 4 | 「インターネットアクセスルールを変換」のステップ4～ステップ7に従い、同じ取扱いを適用したいアプリケーション・サブカテゴリの一つ一つ（または複数の関連サブカテゴリ）を制御する複製ルールを作成します。

## 一定期間で発見されたアプリが少ないルールを変換する

**Apps Seen**（発見されたアプリ）が比較的少なく新しいアプリケーションが長期間発見されなかったルールは、変換が容易で、比較的安定しており、フィルターを使って簡単に特定できる場合があります。

STEP 1 | **Policies** > **Security** > ポリシー オプティマイザー > **No App Specfied**において、ルールにフィルターをかけ、**Apps Seen**が少なく、指定の期間にアプリケーションを発見しなかったルールのみを表示させます。




この例では、発見したアプリケーションが3個以下(**apps seen count leq '3'**)(発見されたアプリ数が'3'以下)で、新しく発見されたアプリケーションが少なくとも30日ゼロであった(**days no new app count geq '30'**)(新しく発見されたアプリケーションが1個もない日数が'30'以上)ルールをフィルタリングします。

STEP 2 | 変換するルールを選択し、**Apps Seen** (発見されたアプリケーション)数をクリックします。

STEP 3 | **Applications & Usage**(アプリケーションと使用状況)ダイアログにおいて、すべてのアプリケーションを許可したいか、また、それらに同一のルールを適用したいかを決定します。すなわち、すべてのアプリケーションはアクセスとセキュリティに関して同様の扱いを要求するかどうかを決定します。

全てのアプリケーションを許可しそれらが同様の扱いを要求する場合は、**Match Usage**(使用法のマッチング)を指定し、ポートベースのルールを新しいApp-IDベースのルールに置き換えます。

全てのアプリケーションを許可するがそれらが異なった扱いを要求する場合は、異なる扱いを要求するアプリケーションのグループごとにルールを複製します。例えばポートベースのルールが3個のアプリケーションを許可し、そのうちの2個が電子メールアプリケーションで1個がインフラのアプリケーションである場合、2個の電子メールアプリケーションに1個のルールを複製し、インフラのアプリケーションにもう1個のルールを複製したくなるでしょう。

許可するアプリケーションもありますが、他のアプリケーションは拒否したいという場合は以下によります:

- 使い続けたいアプリケーションについていくつかのルールを複製し、元のポートベースルールをモニタリングすることにより、切り捨てたいアプリケーションの各々がそのルールとマッチする唯一のものであることを確認します。許可したいアプリケーションのどれもポートベースのルールにマッチしないと把握するのに十分な時間が経過したら、そのルールを無効にするか削除することができます。「インターネットアクセスルールを変換」のステップ4～ステップ7は、 複製ルールの作成法を表しています。
- どのアプリケーションを許可し、どのアプリケーションをブロックすべきかの選択を十分把握している場合:
  - 許可したいアプリケーションに同様の扱いが必要な場合は、**Add to This Rule**(このルールに追加)を使い、ポートベースのルールを、ルールに追加したアプリケーションだけを許可するアプリケーションベースのルールに置き換えます。ルールに追加しないアプリケーションは、別のルールで許可しない限りブロックされます。
  - 許可したいアプリケーションが異なる扱いを要求する場合には、ポートベースのルールから、許可したいアプリケーション用にアプリケーションベース ルールを複製します。残りのアプリケーションをブロックしてもよい場合は、ポートベースのルールを無効化(または削除)することができます。

# セキュリティのベスト プラクティスを適用するための次のステップ

ポートベースルールをアプリケーションベースルールに変換する際の第一パスを完了した後、セキュリティポリシールールベースを強化し、ネットワークセキュリティを改良するために次のステップを検討します：

- Expeditionの Rule Enrichment (ルールエンリッチメント)機能を使用します。それはポリシー設定を検証し、統合するために機械学習を使用します。
- App-IDによる目標達成に向かっての進捗を測定し、また、その他の改善点を発見するためにベストプラクティスアセスメント(BPA)を定期的に実行します。目的達成後、継続的に改良し、さらにネットワークの安全性を向上させるため、BPAを使用して工リアを識別します。
- ポリシー オプティマイザーはポートベースルールをApp-IDベースルールに変換しますが、ルールに関して他に変更することはありません。レガシールールをApp-IDベースルールに変換した後、ルールを強化することで、攻撃可能な箇所を縮小させ、可視性を増加させます：
  - アプリケーションが非標準のポートを使用するのを防ぐため、**Service (サービス)** を **application-default (アプリケーションデフォルト)** にセットします。内部カスタムアプリケーションに関しては、デフォルトポートを定義して、**application-default (アプリケーションデフォルト)**を適用します。
  - ウェブアプリケーション用ペリメーター (内部ゲートウェイ)では、リスクのあるウェブサイトにアクセスするのを防ぐため URL Filtering (URL フィルタリング)カテゴリを使用します。
  - アプリケーションにアクセスできるユーザーを制御するため、 User-ID (ユーザーID) を設定します。
  - Log Forwarding (ログ転送)を設定することで、複数のPAN-OSアプライアンスからのログを集中管理し、特定のアドミニストレータあるいは特定のアラートのためのグループに電子メールアラートを送信しつつ、履歴分析用にログを保存します。
  - best practice Security profiles ( ベストプラクティスセキュリティプロファイル ) を設定することで、アンチウィルス、アンチスパイウェア、脆弱性防護、ファイル ブロッキング、WildFire分析を行い、それらをApp-IDセキュリティポリシールールに適用します。
  - Iron-Skillet (アイアンスキレット) テンプレート、GitHub (ジットハブ)で利用可能, を get started (使用開始) し、初期のベストプラクティス設定をブートストラップするために使用することを検討します。
- App-IDの配置を維持します。内部カスタムアプリケーションを含む新しいアプリケーションにルールを追加する際に、ネットワークを安全に維持するうえで役立つApp-IDベースルールを作成します。アプリケーショントラフィックに可視性を与えない、あるいは検査や制御をさせないポートベースルールの使用に戻ってはいけません。Administrator's Guide (PAN-OS 管理者ガイド)にある App-IDについての詳細をご覧ください。
- セキュリティポリシールールベースを強固にしていく中で、decrypting traffic (デクリプティングトラフィック)および DoS and Zone protection ( DoS とゾーンプロテクション ) にベストプラクティス等のネットワークへの他の保護策を適用することを検討します。

レガシーデバイス設定をPalo Alto Networks装置に移行するのにサポートが必要な場合は、移行に関する経験が豊富なPalo Alto ネットワークの プロフェッショナルサービスグループにお問い合わせください。移行とApp-IDへの変換を成功させるお手伝いをいたします。