

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 9.1

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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2019-2019 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

December 18, 2019

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.....	5
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.....	6
Expeditionを使って、ポートベースのポリシーをPAN-OSに移行.....	8
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.....	11
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.....	13
30日後に変換を開始するルール.....	17
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.....	28

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⁵

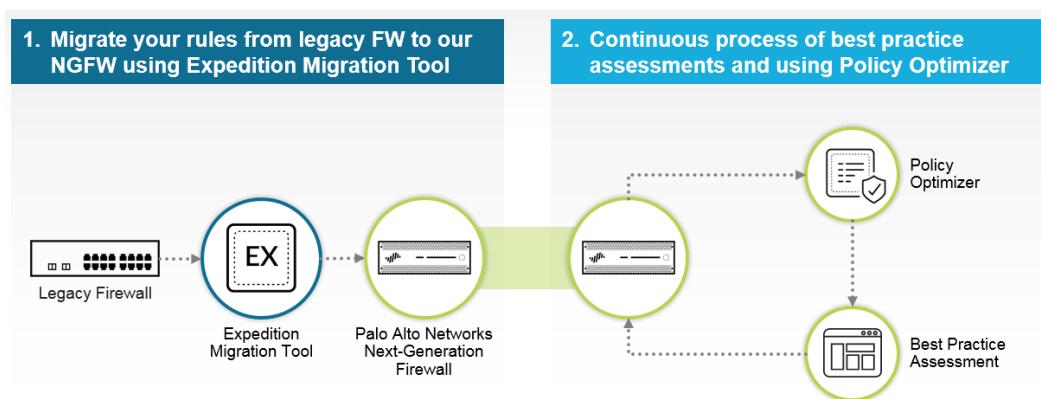
フェーズ化されたトランザクションを使用してアプリケーションを安全に有効化します

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：

Moving From Legacy Rules To App-ID Based Rules



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 Assessment (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。

6 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 | アプリケーションベース・ポリシーに移行するためのベスト プラクティス

-
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、どのようにツールを入手するか、またツールをどのように使用するかについての詳細な文書を含む、Expeditionへの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が、全ての要求されたファイルが含まれているかどうかチェックします。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。必要であれば、移行ソースファイルを内容を固定するように変更し、再びチェックします。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 [内容アップデート](#) を入手し、次に現行のPAN-OSアプライアンスから、現存する設定ファイルか、あるいは工場デフォルトのPAN-OS設定ファイルのいずれか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 サービスオブジェクトのみを認識し、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的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。設定が PAN-OS アプライアンスに移行する際、ゾーンが担う目的を説明するような名前をつけ、確保されたゾーンが正しくインターフェースにマップされるようにします。

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。**

10 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 | アプリケーションベース・ポリシーに移行するためのベスト プラクティス

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認識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ツールでありサポートされているので、装置と非標準ツールとの間でコンフィグ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エラーを防ぐ、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：

The screenshot shows the 'Applications & Usage - Traffic to internet' interface. At the top, there's a search bar and a timeframe selector set to 'Anytime'. Below that, a summary table shows 'Apps on Rule' (1 Any) and 'Apps Seen' (76). A detailed table lists 76 items, each with columns for Application name, Subcategory, Risk level (1-4), First Seen date, Last Seen date, and Traffic over the last 30 days. Applications listed include boxnet-base, crashplan, ssl, outlook-web-online, google-base, slack-base, traps-management-service, vimeo-base, and web-browsing. The interface includes buttons for 'Browse', 'Add', 'Delete', 'Add to Rule', 'Create Cloned Rule', and 'Match Usage'. A message at the bottom states 'The last new app was discovered 2 days ago.' At the bottom right are 'OK' and 'Cancel' buttons.

- **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な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 Rule** (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、複製が提供するセーフティネットを提供しない状態にします **Add to Rule** (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すべてが確実なものであると確信している場合のみ使用します。これまで認識された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を確信しているルールについては **Add to Rule** (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見ら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。
- **Match Usage** (使用の一一致) – 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みら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見ら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見られる唯一のアプリケーションである場合、**Match Usage** (使用の一一致) 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) あるいは **Add to Rule** (ルールに追加する) ために、**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。多くの場合、ルールを変換した後、**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装置へのレガシーセットの [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

12 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 | アプリケーションベース・ポリシーに移行するためのベスト プラクティス

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. 進歩を比較するベースラインをセットするために [Best Practice Assessment\(ベストプラクティスのアセスメント\)](#)(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認識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**は移行に関する熟練しています。レガシーアクセスから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。

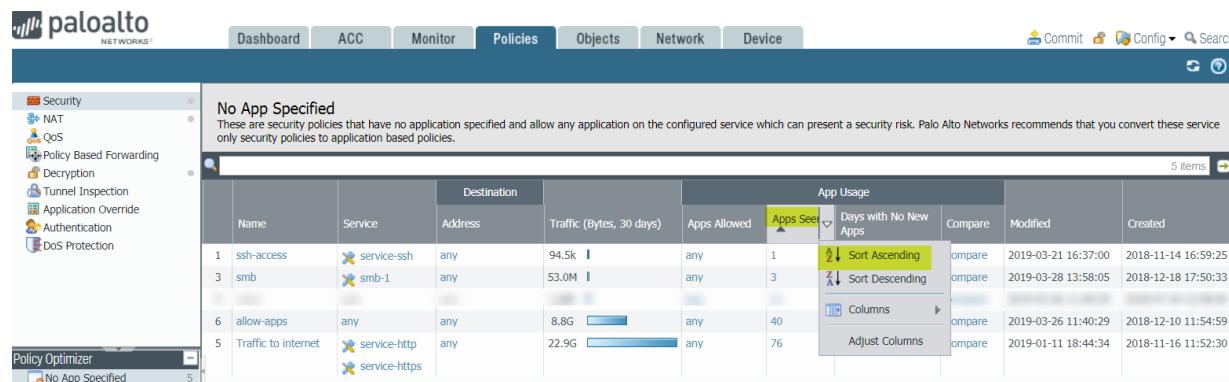
- 1週間後ウェルノウンアプリケーションについて簡単なルールを変換する
- 30日後に変換を開始するルール

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) > 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)とを選択することにより、発見アプリケーションが最も少なかつたポートベースのルールを見つけます。



Name	Service	Address	Traffic (Bytes, 30 days)	Apps Allowed	Apps Seen	Days with No New Apps	Compare	Modified	Created
1 ssh-access	service-ssh	any	94.5k	any	1		Compare	2019-03-21 16:37:00	2018-11-14 16:59:25
3 smb	smb-1	any	53.0M	any	3		Compare	2019-03-28 13:58:05	2018-12-18 17:50:33
6 allow-apps	any	any	8.8G	any	40		Compare	2019-03-26 11:40:29	2018-12-10 11:54:59
5 Traffic to Internet	service-http	any	22.9G	any	76		Compare	2019-01-11 18:44:34	2018-11-16 11:52:30
	service-https						Columns		

発見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つ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。

Applications	Subcategory	Risk	First Seen	Last Seen	Traffic (30 days)
ms-ds-smbv2	storage-backup	3	2018-12-18	2019-04-08	53.0M
ms-ds-smb-base	storage-backup	3	2019-01-29	2019-03-29	7.4k
msrpc-base	infrastructure	2	2018-12-21	2018-12-21	0

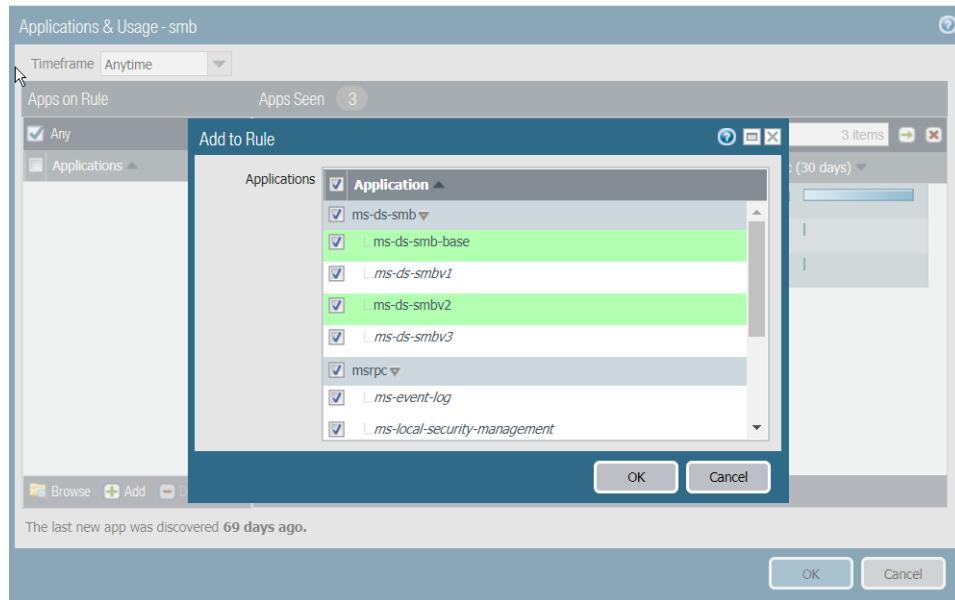
STEP 3 | ルールについて発見されるアプリケーションのすべてもしくはいくつかを許可する、または一切許可しないかを決定し、許可したいアプリケーションを選択します。

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：
 - 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。
 - Match Usage (使用法のマッチング) をクリックします。
 - 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。
 - 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。
- ルールで発見されるアプリケーションをすべて許可し、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（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）場合は、以下によります：

14 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 | アプリケーションベース・ポリシーに移行するためのベスト プラクティス

- すべてのアプリケーションを選択された状態にしておき、Add to Rule (ルールに追加) を実行します。



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。

- OK をクリックします。コンテナアプリはそれに含まれるすべてのアプリケーションを含み（許可し）ますので、Apps on Rule (ルールのアプリ) にはコンテナアプリだけが表示されます：

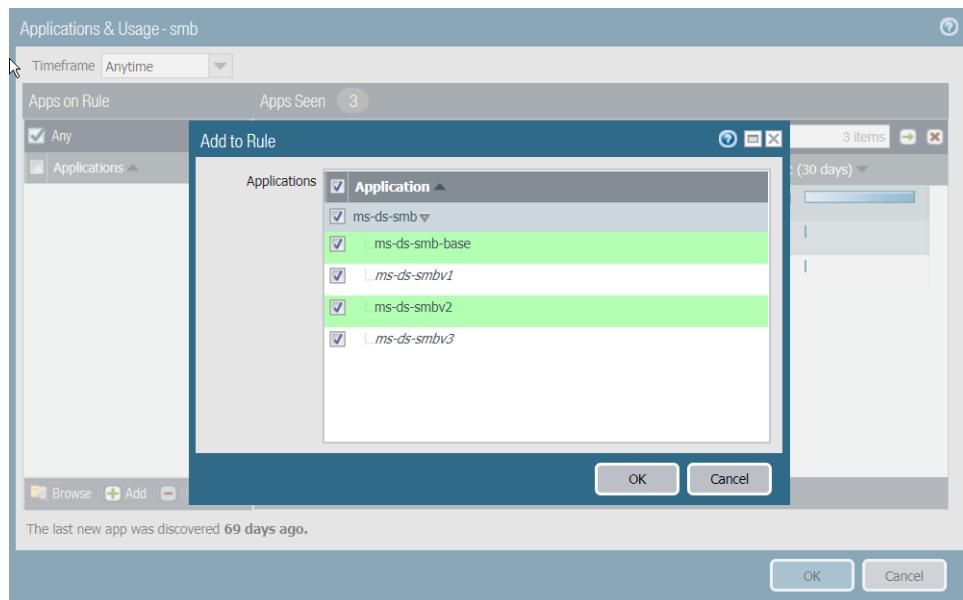
Applications	Subcategory	Risk	First Seen	Last Seen	Traffic (30 days)
ms-ds-smbv2	storage-backup	3	2018-12-18	2019-04-08	53.1M
ms-ds-smb-base	storage-backup	3	2019-01-29	2019-03-29	7.4k
msrpc-base	infrastructure	2	2018-12-21	2018-12-21	0

- OKをクリックしてルールを変換します。
- 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。
- アプリケーションのうち一部だけを許可したい、または、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 Rule (ルールに追加) をクリックします。例えば、msrpcベースを許可しないよう決定しms-ds-smbv2ベースまたはms-ds-smbベースだけを選択し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、shaded gray)内の関連アプリケーションを示し、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 Rule** (ルールに追加) をクリックします。

例えば、msrpcベースを許可しないよう決定しms-ds-smbv2ベースまたはms-ds-smbベースだけを選択し**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、shaded gray)内の関連アプリケーションを示し、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：

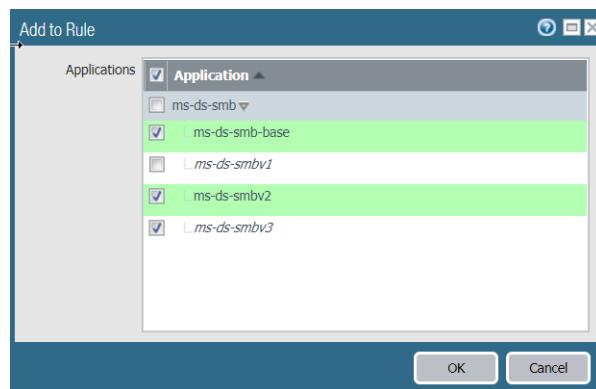


緑に色付けされたアプリケーションは、ルールで発見されたアプリケーションです。色付けされていないアプリケーションは、同じコンテナアプリに属していますが、ルールでは発見されません。この場合、将来も有効に使い続けられるルールを提供するためms-ds-smbv3を許可する一方、ms-ds-smbv1は古いプロトコルなので許可しないという選択をすることもできます。

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外すと、コンテナアプリ自体も選択を外されますので、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。



16 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 | アプリケーションベース・ポリシーに移行するためのベスト プラクティス

-
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](#)
- [発見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。未使用的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。

未使用的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。未使用的ルールより上位にあるルールは、場合によっては未使用的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、未使用的ルールは、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。

The screenshot shows the Palo Alto Networks Policy Optimizer interface. On the left, there's a sidebar with 'Security' and 'Policy Optimizer' sections. The main area is titled 'Rule Usage' with a sub-instruction: 'Monitoring rule usage can help ensure rules are performing as expected, and can help identify rules that should be removed to reduce your attack surface.' It includes a 'Timeframe' dropdown set to 'All time', a 'Usage | Unused' button (which is highlighted in yellow), and a checked checkbox for 'Exclude rules reset during the last 30 days'. A table titled 'Rule Usage' lists two entries:

Name	Hit Count	Last Hit	First Hit	Reset Date	Modified	Created
3 smtp traffic	0	-	-	-	2019-01-11 18:44:34	2018-12-18 17:50:33
5 Tsunami-file-transfer	0	-	-	-	2019-03-26 11:09:40	2019-03-21 16:14:56

The 'Policy Optimizer' sidebar also shows 'Unused Apps' and 'Rule Usage' sections with various counts.

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、ビジネスは過去にTsunamiファイル転送を使用しましたが、調査ではビジネスはTsunamiを使用しておらず、他のファイル転送アプリケーションに置き換えたことを示しています。従ってTsunamiアプリケーションがトラフィックの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ます。ルールをDisable (無効化) あるいはDelete (消去) 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、以前に無効化した未使用のルールを消去することができます。

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 Specified (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。

18 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 | アプリケーションベース・ポリシーに移行するためのベスト プラクティス

最初の 3 つのルールは、かなり長い期間にわたって新しいアプリケーションを検出しておらず、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（検出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。

Applications	Subcategory	Risk	First Seen	Last Seen	Traffic (30 days)
active-directory-base	auth-service	2	2018-12-18	2019-04-10	5.6M
crashplan	storage-backup	4	2018-12-10	2019-04-10	580.9M
dns	infrastructure	4	2018-12-18	2019-04-10	13.6M
google-base	internet-utility	4	2018-12-10	2019-04-10	1.2M
kerberos	auth-service	2	2018-12-10	2019-04-10	10.7M
ldap	auth-service	2	2018-12-18	2019-04-10	49.3M
ms-local-security-management	infrastructure	1	2018-12-18	2019-04-10	1.3M
ms-netlogon	auth-service	2	2018-12-10	2019-04-10	330.5k

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。

Applications	Subcategory	Risk	First Seen	Last Seen	Traffic (30 days)
dns	infrastructure	4	2018-12-18	2019-04-10	13.6M
ms-local-security-management	infrastructure	1	2018-12-18	2019-04-10	1.3M
msrpc-base	infrastructure	2	2018-12-18	2019-04-10	34.9M
netbios-ns	infrastructure	2	2018-12-18	2019-04-10	741.6k
ntp	infrastructure	2	2018-12-18	2019-04-10	99.5k
stun	infrastructure	2	2018-12-21	2019-04-10	174.5k
dhcp	infrastructure	2	2018-12-19	2019-01-02	0
netbios-ss	infrastructure	2	2018-12-12	2018-12-12	0

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からステップ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生成します。

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、ユーザーのネットワーク上望ましくないアプリケーションを許可し攻撃されやすくなる可能性がありますので、これらのポートで許可するアプリケーションを管理し、安全に有効化する必要があります。

インターネットアクセス・ルールをポートベースからアプリケーションベースに変換する際、ユーザーが業務上どのアプリケーションを認可し、他の目的ではどのアプリケーションを許容できるかを理解する必要があります。

インターネットアクセス・ルールを変換する上で、ルールベースが膨れ上がるの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よりは、類似の扱い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認識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、ルール内で認識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。この機能により、アプリケーションの使用に支障をきたすことなく、別々に異なる扱いをしたい複数のアプリケーション・グループ用の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・ルールを生成することができます。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そのまま元のポートベースルール適用となるかをチェックすことができ、それにより適宜ルールを調整することができます。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、

20 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 | アプリケーションベース・ポリシーに移行するためのベスト プラクティス

ポートベースルールを無効化（または削除）することができます。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、ウェルノウンアプリケーションを少なからず発見したルールを変換する際にも使うことができます。インターネットアクセス・ルールを変換した後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）>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、**Apps Seen**（発見されたアプリ）が最も多く過去30日間のトラフィック（トラフィック（バイト、30日間））が最も多いという組合せで最も多く使われるルールを変換するか、**Days with No New Apps**（新しいアプリケーションがなかった日数）と**Modified**（修正）日とをチェックして、多くのアプリケーションを発見したがより安定しているルールを検出することができます。

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、電子メール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紹介しています。この同じ複製手順を使って、ポートベースルールで発見される様々なサブカテゴリや個別アプリケーション用に、安全にアプリケーションベースのルールを生成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 Specified**（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）に関する設定されたポートベースルールを探します。

The screenshot shows the Palo Alto Networks Policy Optimizer interface. The left sidebar has a tree view with 'Security' selected, and a 'Policy Optimizer' section with 'No App Specified' highlighted. The main pane displays a table titled 'No App Specified' with one item found. The table columns are: Name, Service, Traffic (bytes, 30 days), Apps Allowed, Apps Seen, Days with No New Apps, Compare, Modified, and Created. The single row shows 'Traffic to internet' as the name, 'service-http' and 'service-https' as services, 5.0G as traffic, 'any' as apps allowed, 78 as apps seen, 6 as days with no new apps, 'Compare' as the comparison method, '2019-01-11 18:44:34' as modified, and '2018-11-16 11:52:30' as created.

STEP 2 | Compare（比較）または**Apps Seen**（認識されたアプリ）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：

Applications & Usage - Traffic to internet

Timeframe Anytime

Apps Seen 76

Apps on Rule

Any

Applications ▾

Applications	Subcategory	Risk	First Seen	Last Seen	Traffic (30 days)
itunes-base	audio-streaming	3	2019-04-01	2019-04-01	75.1k
soundcloud-base	audio-streaming	2	2019-03-20	2019-03-20	11.2k
okta	auth-service	3	2018-12-18	2019-04-09	4.2M
pingone	auth-service	1	2019-01-22	2019-01-22	0
outlook-web-online	email	3	2019-01-11	2019-04-09	333.3M
yahoo-mail-base	email	3	2018-12-18	2019-04-08	8.6M
gmx-mail	email	4	2019-04-03	2019-04-03	2.2M
hotmail	email	4	2019-02-25	2019-02-25	0

Browse Add Delete + Add to Rule Create Cloned Rule Match Usage

The last new app was discovered 6 days ago.

OK Cancel

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、電子メール制御用のApp-IDベースのルールを生成するために、下記ルールで発見される電子メールアプリケーションだけを閲覧するようフィルタリングをかけます：

Applications & Usage - Traffic to internet

Timeframe Anytime

Apps Seen 77

Apps on Rule

Any

Applications ▾

Applications	Subcategory	Risk	First Seen	Last Seen	Traffic (30 days)
gmail-base	email	4	2019-04-09	2019-04-09	3.2M
gmx-mail	email	4	2019-04-03	2019-04-03	2.2M
hotmail	email	4	2019-02-25	2019-02-25	0
outlook-web-online	email	3	2019-01-11	2019-04-09	336.4M
yahoo-mail-base	email	3	2018-12-18	2019-04-08	8.6M

Browse Add Delete + Add to Rule Create Cloned Rule Match Usage

The last new app was discovered 0 days ago.

OK Cancel

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。

例えば会社として業務用にGmailとOutlookを認可し、個人用にYahooメールの使用を看過するが、GMXメールおよびHotmailは許可しないことにする場合は、以下の様になります：

22 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 | アプリケーションベース・ポリシーに移行するためのベスト プラクティス

Applications & Usage - Traffic to internet

Timeframe Anytime

Apps Seen 77

Applications	Subcategory	Risk	First Seen	Last Seen	Traffic (30 days)
gmail-base	email	4	2019-04-09	2019-04-09	3.2M
gmx-mail	email	4	2019-04-03	2019-04-03	2.2M
hotmail	email	4	2019-02-25	2019-02-25	0
outlook-web-online	email	3	2019-01-11	2019-04-09	336.4M
yahoo-mail-base	email	3	2018-12-18	2019-04-08	8.6M

Browse Add Delete Add to Rule Create Cloned Rule Match Usage

The last new app was discovered 0 days ago.

OK Cancel

STEP 5 | Clone (複製) ダイアログにおいて、許可したいアプリケーション各々に関連したアプリケーションを選択します。

Applications & Usage - Traffic to internet

Timeframe Anytime

Clone

Name: email-apps-allowed

Applications

- gmail
- gmail-base
- gmail-call-phone
- gmail-chat
- gmail-downloading
- gmail-enterprise
- gmail-nostina

OK Cancel

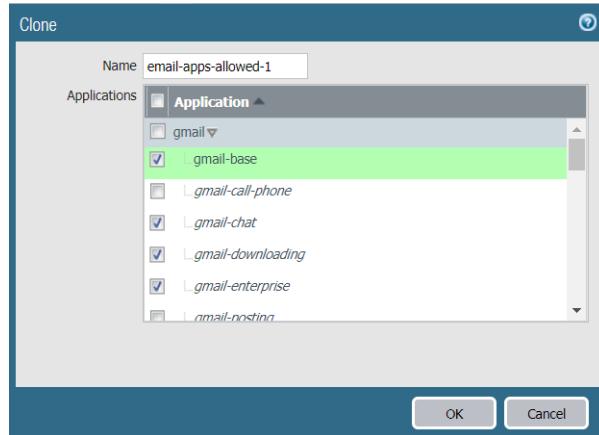
Browse Add Delete Add to Rule Create Cloned Rule Match Usage

The last new app was discovered 0 days ago.

OK Cancel

新しいルールに、その目的を表すName (名前) を付与します。個々の電子メールアプリケーションについて特定の機能だけを許可したいか、コンテナアプリを許可したいかを決定します。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。各アプリケーションのコンテナアプリは灰色、ルールについて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について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。

 コンテナアプリ内のあるアプリケーションだけは許可しないことを選択した場合は、コンテナアプリも選択から外され、ルールは選択した特定のアプリケーションだけを対象にします。



gmail-call-phoneおよびgmail-postingアプリケーションを選択から外すと、gmailコンテナアプリも選択から外されます。

STEP 6 | OKをクリックしてルールを生成します。生成されたルールは、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されます。

コンテナアプリはすべてのアプリケーションを含むので、コンテナアプリを選択すると、ポリシー オプティマイザーは、それだけをルールに追加します。

Name	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	Action	Profile
6 email-apps-allowed	none	universal	I3-vlan-trust	any	any	I3-untrust	any	gmail	service-http	Allow	
7 Traffic to internet	none	universal	I3-vlan-trust	any	any	I3-untrust	any	rms-office365	service-https	Allow	
								yahoo-mail	service-https		
								Sinkhole	service-https		

Clone (複製) ダイアログにおいて、コンテナアプリの代わりに個別のアプリケーションを選択すると、ポリシー オプティマイザーは、選択されたアプリケーションだけを新しいApp-IDベースルールに追加します。

Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service
5 email-apps-allowed-1	none	universal	I3-vlan-trust	any	any	any	I3-untrust	any	gmail-base	service-http
									outlook-web...	service-https
									yahoo-mail-b...	
									sharepoint-o...	
									gmail-chat	
									gmail-enter...	
									gmail-downl...	
									more...	

24 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 | アプリケーションベース・ポリシーに移行するためのベスト プラクティス

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を防止するには、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。

発見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発見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ます。)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発見する場合には、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 Specified (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、最も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。

Name	Service	Address	Traffic (Bytes, 30 days)	Apps Allowed	Apps Seen	Days with No New Apps	Compare	Modified	Created
5 Traffic to internet	service-http service-https	any	3.9G		2	Compare	2019-01-11 18:44:34	2018-11-16 11:52:30	
6 allow-apps	any	any	1.9G		87	Compare	2019-03-26 11:40:29	2018-12-10 11:54:59	
3 smb	smb-1	any	52.7M		72	Compare	2019-03-28 13:58:05	2018-12-18 17:50:33	
1 ssh-access	service-ssh	any	94.5k		126	Compare	2019-03-21 16:37:00	2018-11-14 16:59:25	

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からステップ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生成します。

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つたルールは、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 Specified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つたルールのみを表示させます。

The screenshot shows the Palo Alto Networks Policy Optimizer interface. On the left, there's a sidebar with various policy categories like Security, NAT, QoS, etc. A search bar at the top right has filters applied: '(apps-seen-count leq '3') and (days-no-new-app-count geq '30')'. Below the search bar is a table titled 'No App Specified' with two rows of data. The columns are: Name, Service, Address, Destination, Traffic (Bytes, 30 days), Apps Allowed, Apps Seen, Days with No New Apps, Compare, Modified, and Created. The first row is for 'smb' (Service: smb-1) and the second for 'ssh-access' (Service: service-ssh).

Name	Service	Address	Destination	Traffic (Bytes, 30 days)	App Usage					
					Apps Allowed	Apps Seen	Days with No New Apps	Compare	Modified	Created
3 smb	smb-1	any	any	53.4M	any	3	72	Compare	2019-03-28 13:58:05	2018-12-18 17:50:33
1 ssh-access	service-ssh	any	any	94.5k	any	1	126	Compare	2019-03-21 16:37:00	2018-11-14 16:59:25

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4~7に、複製ルールの生成法を示します。
- 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は、以下によります :
 - 許可したいアプリケーションが同様の扱いを要求する場合は、Add to Rule (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たため、BPAを使用してエリアを識別します。
- 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、[ユーザーID \(User-ID\)](#)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。