paloalto TECHDOCS

BPA スタート ガイド

10.2

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

May 13, 2022

Table of Contents

セキュリティポリシー・キャパシティ適用の評価

ベストプラクティスアセスメント(BPA)ツールを使えば、自分のセキュリティポリシー機能適用の現在レベルを理解することができ、セキュリティポスチャーの成熟度及び効果を評価することができます。WildFire、脆弱性防御、SSL復号化等の機能を使用することにより、攻撃を検出し予防する効果があります。自分のネットワークおよびその貴重な財産を防衛する最善の方法を理解する上で、これらの機能を様々な環境のどこでいかに活用すべきかを理解することが肝要です。

Getting Started with Best Practices（スタート ガイド（ベスト プラクティス））は、BPAにアクセスし実行する方法を解説しています。BPAレポートのCapability Adoption Heatmaps（機能適用ヒートマップ）セクションは、セキュリティポリシー・ルールベース全体にわたり、これらの機能の適用/不適用を決めるのに役立ちます。ヒートマップの概要は、ヒートマップの紹介動画でご確認ください。また、BPA video library（BPA動画ライブラリー）とBPA+ video library（BPA+動画ライブラリー）を活用してツールの詳細を学んでください。

Panorama が管理する環境では、*Panorama* が多数の次世代ファイアウォールを管理する場合があります。*Panorama* または個々のファイアウォールで *BPA* を実行する必要がありますか?比較するのは、スピードと利便性に対する完全性です。

Panorama で *BPA* を実行すると、高速で便利になり、管理されたファイアウォールのほとんどの機能が評価されますが、ローカル ファイアウォールのオーバーライドは調べられません。

管理対象の各ファイアウォールで *BPA* を実行すると、完全な構成 *(*ローカルのオーバーライドを含む*)* が評価されますが、非常に時間がかかります。

最も実用的な方法は、最初に *Panorama* で *BPA* を実行することです。結果を調べて、特定の管理対象デバイスに注目する必要があるかどうかを判断し、それらのデバイスで *BPA* を実行します。この方法により、時間を節約しながら、セキュリティ体制を改善できる関連情報に集中できます。

ヒートマップ・タブの情報を確認・分析しセキュリティ機能適用のギャップを認識し、改善点を特定します：

- 適用サマリーのレビュー
- 適用におけるギャップを特定する

- 改善すべきルールを識別

適用サマリーのレビュー

あなた、あるいはPalo Alto Networksの代理人が BPAを実行した後、結果としてのHTMLレポートが適用サマリーのAdoption Heatmap（適用ヒートマップ）ページ上で開かれます。適用サマリービューはセキュリティ能力のデバイス全体適用の全容を提供します。レポートは個々の測定基準（業界における適用割合を示す業界平均を除く）の現在の適用割合を示します。そして括弧内に、デバイスの設定ファイルでBPAを最後に起動して以来の適用割合の変化を示します（値が最後にBPAを起動した時と同じであれば**No change**（変化なし）を示します）。

Overall Adoption（全体適用）—セキュリティポリシー許可ルールにおけるセキュリティプロファイルの適用。割合は、ルールの一部として一つ以上のプロファイルが有効化された許可ルールの数に基づいています。BPA は無効化されたルール、ブロックされたルールはカウントしません。

Industry Average（業界平均）—会社の業界における許可ルールのセキュリティプロファイル適用の平均。

Best Practice Mode（ベストプラクティスモード）—許可ルール内で推奨されたベストプラクティスで設定されたセキュリティプロファイルの適用。BPA は全てのベストプラクティスチェックに合格したプロファイル付きのルールの数のみカウントします。

App-ID Adoption（**App-ID** 適用）—セキュリティポリシー全体でのApp-IDの適用。割合値は、一つ以上の定義されたアプリケーションがある許可ルールの合計数に基づいています（アプリケーションは**any**ではない）。BPA は無効化されたルールはカウントしません。

User-ID Adoption（ユーザー**ID**適用）—セキュリティポリシールール全体へのUser-IDの適用。割合値はユーザーとの許可ルール（**known-user**（既知のユーザー） と **unknown**（未知）の値を含む） の合計数、あるいはユーザーグループの数に基づいています。BPA は無効化されたルールはカウントしません。

Service/Port Adoption（サーバー/ポート適用）—セキュリティポリシールール全体へのサービス/ポートの適用。割合値は定義されたサービスあるいはポートでの許可ルールの合計数に基づいています（サービスは**any**ではない）。BPA は無効化されたルールはカウントしません。

BPA は*App-ID*、*User-ID*、あるいはルールをブロックするためのサービス/ポート適用はカウントしません。なぜなら、ブロックする論拠はビジネスによって異なるので、*BPA*がブロックルールに基づいての推奨項目を作れないからです。

Logging Adoption（ロギング適用）—セキュリティポリシールール全体への**Log at Session End**（セッション終了でのログ） の適用。割合値は、**Log at Session End**（セッション終了でのログ）が有効化されている状態でのルールの合計値に基づいています。BPA は無効化されたルールはカウントしません。

Log Forwarding Adoption（ログ転送適用）—セキュリティポリシールール全体へのログ転送プロファイルの適用。割合値はログ転送プロファイルが設定されているルールの合計数に基づいています。BPA は無効化されたルールはカウントしません。

Zone Protection Adoption（ゾーン プロテクション適用）—セキュリティポリシー許可ルール全体へのゾーン保護の適用。割合値は、ソースゾーンがゾーン プロテクション プロファイル設定を有している許可ルールの合計数に基づいています。BPA は無効化されたルールはカウントしません。

個々の測定基準に関しては、それぞれの割合の隣にある括弧内の値は、デバイス構成ファイル上で最後にBPAを実行して以来の採択での割合の変化です（値が最後にBPAを実行したものと同じであれば **No change**（変化なし））。

Decryption Summary（復号化要約）—設定が、SSLフォワードプロキシ、SSLインバウンド検査、SSHプロキシ用の復号化ポリシールールを含んでいるかを示しています。要約はまた、設定が復号化プロファイルを含み、デバイスが復号から除外したURLカテゴリを識別する場合を示しています。

*URL*カテゴリ（または個別のアプリケーション）を復号化しない場合、トラフィックを検査することはできません。なぜならファイアウォールは暗号化されたトラフィックの中身を見ることが出来ないからです。ファイアウォールは復号化したトラフィックのみ検査することができます。

次へ：適用におけるギャップを特定する でセキュリティを強化できる部分を確認します。

適用におけるギャップを特定する

Adoption Heatmap（適用ヒートマップ）オプションは、ユーザーのセキュリティポリシーがどの点で強いか、またどこに改善の余地のあるセキュリティポリシー機能適用のギャップがあるか、を示してくれます。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。ベースラインと対比して現在の体制を評価し、セキュリティ機能導入におけるギャップを認識します。

Adoption Heatmap（適用ヒートマップ）により、セキュリティ機能の適用を改善できるデバイス、ゾーンおよび領域を特定することが容易になります。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。**Local Filters**（ローカルフィルタ）は、Device Group（デバイスグループ）、Source Area of Architecture（アーキテクチャのソースエリア）、Destination Area of Architecture（アーキテクチャの宛先エリア）、Target（ターゲット）、Source Zone（ソースゾーン）、Destination Zone（宛先ゾーン）、およびTags（タグ）でフィルタリングして、範囲を絞り込んでギャップを特定することができます。Area of Architecture（アーキテクチャのエリア）別の適用ヒートマップを次に示します（**Adoption Heatmap**（適用ヒートマップ） > **Areas of Architecure**（アーキテクチャのエリア））：

Adoption Heatmap（適用ヒートマップ） > **Summary**（サマリー）で、Adoption Summary（適用サマリー）をクリックして、次の機能の適用レートを確認します。推奨事項をギャップ判定基準に使います。実際の適用率が推奨値に合致しない場合は、ギャップを埋めるよう計画します：

- WildFire、アンチウィルス、アンチスパイウェア、脆弱性防御およびファイルブロッキングのセキュリティプロファイルを、100%を目標として、またはほぼ100%の適用率を狙って、トラフィックを許可するすべてのルールに適用します。プロファイルを許可ルールに適用しない場合は、適用しないことを業務上正当化できることを確認する必要があります。

  セキュリティプロファイルをすべての許可ルールについて設定することにより、ファイアウォールは、アプリケーションやサービス/ポートに関係なく、復号化されたトラフィックについて脅威があるかないかを検査することができます。設定を更新した後は、BPAを実行して、進捗状況を測定し、セキュリティプロファイルがアタッチされていない新しいルールを見つけます。

  *WildFire*プロファイルは、*WildFire*ライセンスがなくてもルールに適用できます。*PE*ファイルについては適用が限定されますが、それでも、未知の悪意あるファイルの可視性は保証されます。

- アンチスパイウェアプロファイルでは、危殆化された内部ホストが悪意あるまたはカスタムドメインにDNSクエリを送信するのを防止し、危殆化された可能性のあるホストを特定し追跡し、DNSチェックでのギャップを防止するために、DNS Sinkhole（シンクホール）をすべてのルールに適用します。DNS Sinkholeを有効化することにより、ネットワークの利用に支

障を与えることなくネットワークが保護されますので、これは直ちに有効化でき、また有効化すべきです。

- URL フィルタリングおよび認証情報盗難（フィッシング）保護をすべてのインターネット向けトラフィックに適用します。

Adoption Summary（適用サマリー）のApplication & User Control （アプリケーション & ユーザー制御）で、以下の機能の適用率をチェックします。推奨事項をギャップ判定基準に使います。実際の適用率が推奨値に合致しない場合は、ギャップを埋めるよう計画します：

- App-IDを、できるだけ100%に近いルールに適用します。User-IDを、ユーザープレゼンスをもつ送信元ゾーンおよびアドレス範囲を有するすべてのルールに適用します（ユーザーソースのないゾーンもあります。例えば、データセンター・ゾーンは、サーバーでありますが、ユーザーではありません）。App-IDおよびUser-IDを活用して、適切なユーザーが認可（そして許容）されたアプリケーションへのアクセスを許可されるよう、ポリシーを生成します。悪意のあるまたは望まないアプリケーションを指名してブロックします。
- サービス/ポート適用率目標を100%またはほぼ100%に設定します。業務上それなりの理由がない限り、非標準ポートにアプリケーションを許可してはなりません。

適用サマリーの、ロギングとゾーンプロテクションの適用サマリーにおいて、以下の機能の適用率をチェックします。推奨事項をギャップ判定基準に使います。実際の適用率が推奨値に合致しない場合は、ギャップを埋めるよう計画します：

- ロギングおよびログ転送の適用率目標を100%またはほぼ100%に設定します。
- すべてのゾーンにつき、ゾーン プロテクション プロファイルを設定します。

サマリー：

機能	適用目標
WildFire	セキュリティポリシーの適用率はできるだけ100%に
Antivirus（アンチウイルス）	セキュリティポリシーの適用率はできるだけ100%に
アンチスパイウェア	セキュリティポリシーの適用率はできるだけ100%に
脆弱性が	セキュリティポリシーの適用率はできるだけ100%に
ファイル ブロッキング	セキュリティポリシーの適用率はできるだけ100%に
URL フィルタリングおよび認証情報盗難	すべてのインターネット向けトラフィック
App-ID	セキュリティポリシーの適用率はできるだけ100%に

機能	適用目標
User-ID	ユーザープレゼンスをもつ送信元ゾーンおよびアドレス範囲を有するすべてのルール
サービス/ポート	セキュリティポリシーの適用率はできるだけ100%に
ﾛｷﾞﾝｸﾞ	セキュリティポリシーの適用率はできるだけ100%に
ログ転送	セキュリティポリシーの適用率はできるだけ100%に
ゾーン プロテクション	すべてのゾーン

適用ヒートマップを表示する場合、**Local Filters**（ローカルフィルタ）を使って範囲を絞り込んでください。結果の情報を使って、セキュリティポリシー機能のギャップを検出し、ギャップ検出基準に照らして評価し、さらなる調査用にギャップ検出基準を修正するか新しく作ります。例えば、アーキテクチャのインターネット領域へのトラフィックを制御するルールの適用状況を表示するフィルタを作成するには、以下によります：

STEP 1 | **Adoption Heatmap**（適用ヒートマップ） > **Areas of Architecture**（アーキテクチャのエリア）を選択します。

STEP 2 | **Local Filters**（ローカルフィルタ）をクリックしてフィルタリングのオプションを展開します。

STEP 3 | **Destination Area of Architecture**（アーキテクチャの宛先領域）を**Internet**（インターネット）に設定します。

STEP 4 | **Apply**[適用] をクリックします。

BPAが結果を次のようにフィルタリングします：

結果を、セキュリティ目標および基準に従って解釈します。例えば許可ルールについてWildFireを100%適用することが目標であるとき、フィルタリングされた適用ヒートマップが、DMZ許可ルールでWildFireプロファイルをもつのが50%だけであることを示した場合、改善目標とすべきギャップを見出したことになります。

STEP 5 | 次へ：改善すべきルールを識別。

改善すべきルールを識別

セキュリティポリシー適用におけるギャップを摘出した後、**Adoption Heatmap**（適用ヒートマップ） > **Rule Detail**（ルール詳細）ビューを使って、さらなる調査や修正が必要なルールをリストアップします。適用におけるギャップを特定した際に作成したギャップ摘出基準に合致するよう、**Local Filters**（ローカルフィルタ）を設定します。これにより、ファイアウォールセキュリティポリシー担当の運用チームにエキスポートし手渡すことができるルール・リストが作成されます。

例えば、すべてのトラフィックを許可するが脆弱性防御プロファイルをもっていないルールを摘出するためのルール詳細フィルタを生成するには、以下を行います：

STEP 1 | Adoption Heatmap（適用ヒートマップ）メニューから、**Rule Detail**（ルール詳細）を選択してRule Details（ルール詳細）ページを表示します。

STEP 2 | **Local Filters**（ローカルフィルタ）をクリックしてフィルタオプションを表示し、以下のフィルタを選択します：

- 送信元ゾーン = **any**
- 宛先ゾーン = **any**
- 送信元アドレスが設定されているか = **No**
- 宛先アドレスが設定されているか = **No**
- アクション = **allow**（許可）
- ルールが有効か = **Yes**
- 脆弱性がオンになっているか = **No**

STEP 3 | **Apply Filter**（フィルタの適用）をクリックします。

BPAが、フィルタにマッチするルールをリストアップします：

STEP 4 | フィルタリングされたルール・リストを.csvファイルにエクスポートするには、**Export Data**（データをエクスポート）をクリックします。

STEP 5 | 次へ：ベスト プラクティス設定の評価。

ベスト プラクティス設定の評価

ベストプラクティスアセスメント(BPA)ツールを使えば、自分のセキュリティポリシーのベストプラクティスに関する現在のレベルを理解することができ、セキュリティ体制の成熟度を評価することができます。BPAの概要は、Introduction to the BPA動画でご確認ください。また、BPA video library（BPA動画ライブラリー）とBPA+ video library（BPA+ 動画ライブラリー）を利用してツールについてさらに学びましょう。

BPAレポートでは最初に、Adoption Heatmap（適用ヒートマップ）ページが表示されます。**Best Practice Assessment**（ベストプラクティスアセスメント）をクリックしてレポートのBPAセクションを表示します。このセクションでは、次世代ファイアウォールおよびPanorama設定に関するベストプラクティスの適用について解説しています。

この文書の他に、BPA demo（BPAデモ）およびhow to run a BPA（BPAの実行のしかた）の短いビデオを閲覧してBPAの使い方をより詳しく知ることができます。

BPAレポートは、次世代ファイアウォールおよびPanorama設定ファイルを、200件以上のベストプラクティス・チェックポイントについて評価します。BPAは、PAN-OSユーザーインターフェースと同じように、評価結果を、ポリシー、オブジェクト、ネットワークおよびデバイス/Panorama情報ごとにグループ化して示します。

Panorama が管理する環境では、*Panorama* が多数の次世代ファイアウォールを管理する場合があります。では、*BPA*は、*Panorama*側と、個々のファイアウォールのどちらで実行すべきでしょうか？比較するのは、スピードと利便性に対する完全性です。

Panorama で *BPA* を実行すると、高速で便利になり、管理されたファイアウォールのほとんどの機能が評価されますが、ローカル ファイアウォールのオーバーライドは調べられません。

管理対象の各ファイアウォールで *BPA* を実行すると、設定全体 *(*ローカルのオーバーライドを含む*)* が評価されますが、はるかに時間がかかります。

最も実用的な方法は、最初に *Panorama* で *BPA* を実行することです。結果から、特定の管理対象デバイスに注目する必要があるかどうかを判断し、それらのデバイスで *BPA* を実行します。この方法により、時間を節約しながら、セキュリティ体制を改善できる関連情報に集中できます。

これらの情報を精査・分析して、注意すべきところや改善点を見出します：

- ベスト プラクティス サマリーのレビュー

- ベストプラクティスポリシー設定のレビュー
- ベストプラクティス オブジェクト設定のレビュー
- ベストプラクティス ネットワーク設定のレビュー
- ベストプラクティスデバイスとPanorama管理設定のレビュー

ベスト プラクティス サマリーのレビュー

ベストプラクティスサマリーを表示するには、**Best Practice Assessment**（ベストプラクティス評価）メニューから**Summary**（サマリー）を選択します。

概要は、業界標準、インターネットセキュリティセンター(CIS) クリティカルセキュリティコントロール、国立標準・技術(NIST)のセキュリティ制御とアセスメント手順に関する出版物などの制御カテゴリにマップされたベストプラクティス設定チェック結果を提示します。この情報の目的は、BPAチェックがどのように業界標準に繋がるかを理解するうえで適切な手段となることであり、監査として機能することではありません。

Adoption Summary（適用サマリー）のように、Best Practice Summary（ベストプラクティスサマリー）はデバイス設定に最後にBPAを生成して以来の、現在の適用割合および（括弧内に）適用進捗を示す測定基準を含みます。

mマップされたチェックとその個別スコアの完全リストを見るため、**Mapping Definitions**（マップ定義）（左側サイドバー）をクリックします。フィルタを設定するために**Show Filters**（フィルタ表示）し、出力に**Apply Filters**（フィルタを適用）し、マッピングを.csv ファイルでエクスポートするために **Export Mappings**（マッピングをエクスポート）します。

次へ：ベストプラクティスポリシー設定のレビュー。

ベストプラクティスポリシー設定のレビュー

ベストラクティス評価 > ポリシーには、異なるタイプのファイアウォールポリシーに関するすべてのチェックが表示され、**Security Rulebase checks**（セキュリティルールベースチェック）ページから始まります。**Security Rulebase Checks**（セキュリティルールベースチェック）は、pass/fail（合格/不合格）ステータスと不合格になったチェックに対する推奨項目とともに、デバイスグループ毎のベストプラクティスチェック結果の要約を示します。個々の結果の説明と論拠および参考となる技術文書へのリンクを閲覧するためには、ヘルプ（　）をクリックします。

潜在的なルール改善内容を確認するためには、左側のメニューからレビューしたいポリシーのタイプを選択します。たとえば、**Security Rule Checks**（セキュリティルールチェック） には、ルールベースのチェック結果が表示されます。不合格になった、あるいはより具体的なチェックしたルールに結果を絞り込むフィルタを設定するためには、**Local Filters**（ローカルフィルタ）をクリックします。修復分析用の .csv ファイルにリストをエクスポートするため、**Export Data**（データをエクスポート）できます。

Policy（ポリシー） 情報をレビューする時は、ポリシー修復（ビュー間の切り替え）の内容を理解するため、最低でも以下の項目をレビューします：

- **Security**（セキュリティ）—**Source/Destination !=any/any** チェックで不合格になったルールを識別します。
- **Security**（セキュリティ）—**App-ID with Service**（サービス付**App-ID**） チェックで不合格になったルールを識別します。
- **Security**（セキュリティ）—**User-ID Rules without User ID enabled on Zone**（ゾーンで有効化されていないユーザー**ID**ルール） チェックで不合格になったユーザーIDルールを識別します。
- **Decryption Rulebase**（復号化ルールベース）—SSH プロキシ復号化チェック。
- **Decryption**（復号化）—個々の復号化ポリシールールは関連する復号化プロファイルを持たねばなりません。

  例外は*TLSv1.3*トラフィックで、トラフィックに*No Decryption*（復号化なし）ポリシーを適用して、復号化しないことを選択することができます。ポリシーに*No Decryption*（復号化なし）プロファイルを適用した場合、プロファイルは証明書情報をチェックして、不正な証明書を使用している復号化セッションをブロックします。ただし、*TLSv1.3*は証明書情報を暗号化するため、ファイアウォールは証明書情報に基づいて復号化されていないトラフィックをブロックすることはできません。そのため、プロファイルをポリシーにアタッチする意味はありません。

- **Application Override**（アプリケーション上書き）—単純なカスタムアプリケーションで使用されるアプリケーション上書きルールは、マッチングトラフィック用のレイヤー 7 をバイパスします。シンプルなカスタムアプリケーションを使用するアプリケーションオーバーライドルールを減らすか、削除すると、トラフィックの可視性を改善するが可能になり、これ

らのルールでコントロールされていたアプリケーションやコンテンツを調べらることができます。

次へ：ベストプラクティス オブジェクト設定のレビュー。

ベストプラクティス オブジェクト設定のレビュー

Best Practice Assessment（ベストプラクティス評価） > **Objects**（オブジェクト）には、異なるタイプのファイアウォールオブジェクトに関するすべてのチェックが表示され、**Application Filters**（アプリケーションフィルタ）ページから始まります。既存の設定を理解し、アプリケーションフィルタ、タグ、GlobalProtect、セキュリティプロファイル、ログ転送、復号化プロファイルにおけるベストプラクティスとの潜在的ギャップを識別するためには、レビューしたいオブジェクトを選択します。下記の例は、アンチウィルスセキュリティプロファイルオブジェクトを選択した場合の結果を示しています。

個々のアンチウィルスプロファイルに対して、レポートは現在の設定を示し、いくつのルールがプロファイルを使用しているかを示しています。レポートは、現在の設定の下に、pass/fail（合格/不合格）ステータスと不合格になったベストプラクティスチェックに対する推奨項目とともにベストプラクティスチェック結果を示しています。help（ヘルプ）（ ）をクリックして、各チェックの根拠とベストプラクティス文書へのリンクを確認してください。

一つ以上のチェックが不合格になった場合、プロファイルのタイトルが赤色に変わります。レポートは下部に黄色のタイトルで使用されていないプロファイルを列記しています。

一部のプロファイルページの画面左側にあるリンクの隣にある「QS」ボタンを使用すると、QuickStart Service（クイックスタートサービス）オプションを利用できます。**QuickStart Service**（クイックスタートサービス）は、プラットフォームとしてのファイアウォール導入のプランニングと実施を支援することで、セキュリティ機能および投資効果を向上させるために役立ちます。**Self-guided Documents**（セルフガイドドキュメント）は、オブジェクトの理解、作成およびデプロイに役立ちます。

Objects（オブジェクト） タブをレビューする時は、修復の潜在的内容の理解を促すため、最低でも下記の項目をレビューします：

- **Antivirus**（アンチウィルス）–アンチウィルスとWildFire両方のデコーダーアクション。
- **Anti-Spyware**（アンチスパイウェア）–厳格なプロファイル、DNSシンクホール。
- **Vulnerability Protection**（脆弱性防御）ー厳格なプロファイル。
- **Filtering**（**URL** フィルタリング）–既知の悪質なカテゴリがブロックされているかどうか。
- **WildFire Analysis**（**WildFire**分析）–ファイルタイプをプロファイルする (すべてのタイプは分析のためWildFireに送られるべき)。
- **Log Forwarding**（ログ転送）–全てのログタイプがフォワードされたかどうか（全てのログタイプをフォワードする）。

次へ：ベストプラクティス ネットワーク設定のレビュー。

ベストプラクティス ネットワーク設定のレビュー

Best Practice Assessment（ベストプラクティス評価） > **Network**（ネットワーク）には、ネットワーク関連設定のすべてのチェックが表示され、**Zones**（ゾーン）ページから始まります。左のナビでは、既存設定を理解するため、そしてゾーン、GREトンネル、GlobalProtect、IPsec 暗号化、インターフェース管理、およびゾーン プロテクションプロファイルに関係したベストプラクティス設定との潜在的ギャップを識別するために、レビューしたいネットワークチェックを選択します。下記の例はゾーンの結果を示しています。

レポートは個々の項目の現在の設定を示しています。各項目のベストプラクティスチェック結果は、現在の設定の下に表示されます。**Device Group**（デバイスグループ）and/or**Template**（テンプレート）を指定することができます。

チェックそれぞれに、pass/fail（合格/不合格）ステータスがあり、ベストプラクティスチェックに関する推奨事項があります。help（ヘルプ）（ ）をクリックして、各チェックの根拠とベストプラクティス文書へのリンクを確認してください。一つ以上のチェックが不合格になった時は、項目のタイトルが赤色に変わります。

Network（ネットワーク）タブをレビューする時は、修復の潜在的内容の理解を促すため、最低でも下記の項目をレビューします：

- **Zone**（ゾーン）–個々のゾーンでパケットバッファ保護が有効化され、ゾーン プロテクション プロファイルが存在するか。
- **Zone Protection**（ゾーン プロテクション）–フラッド保護およびパケットベースの攻撃防護が有効化されているか。

次へ：ベストプラクティスデバイスとPanorama管理設定のレビュー。

ベストプラクティスデバイスとPanorama管理設定のレビュー

Best Practice Assessment（ベストプラクティス評価） > **Device**（デバイス）および**Best Practice Assessment**（ベストプラクティス評価） > **Panorama**ページには、デバイス管理のセットアップおよび設定に関するすべてのチェックが表示されます。スタンドアロンのファイアウォールでは、**Best Practice Assessment**（ベストプラクティス評価） > **Device**（デバイス）は、ファイアウォールデバイスのManagement Setup（管理セットアップ）ページの、General Settings（全般設定）から始まります。Panoramaでは、**Best Practice Assessment**（ベストプラクティス評価） > **Device**（デバイス）は、各テンプレートスタックの全般設定を表示するページから始まります。**Best Practice Assessment**（ベストプラクティス評価） > **Panorama**は、デバイスのManagement Setup（管理セットアップ）ページの、General Settings（全般設定）から始まります。既存の設定を理解し、ファイアウォールとPanoramaデバイスの管理に関連するベストプラクティス設定とのギャップを識別するためには、レビューしたいチェックを選択します。PanoramaデバイスのGeneral Settings（全般設定）の結果の例を次に示します。

レポートは個々の項目の現在の設定を示しています。各項目のベストプラクティスチェック結果は、現在の設定の下に表示されます。**Device**（デバイス）の情報を見るとき、表示される情報の範囲を制限するため **Template**（テンプレート）を指定することができます。

チェックそれぞれに、pass/fail（合格/不合格）ステータスがあり、ベストプラクティスチェックに関する推奨事項があります。help（ヘルプ）（ ）をクリックして、各チェックの根拠とベストプラクティス文書へのリンクを確認してください。一つ以上のチェックが不合格になった時は、項目のタイトルが赤色に変わります。

Device（デバイス）あるいは**Panorama** タブをレビューする時は、修復の潜在的内容の理解を促すため、最低でも下記の項目をレビューします：

- **Dynamic Updates**（ダイナミック更新）–アンチウィルス、アプリケーション、脅威、WildFireに関する更新。
- **Management Interface Settings**（管理インターフェース設定）–ネットワーク接続サービス、許可されたIPアドレス。
- **Administrators**（管理者）–ローカル管理者、管理者パスワードプロファイル。管理者パスワードが要求される最低限の複雑性で設定されていることを確実にするため、**Device**（デバイス） > **Administrators**（管理者）、または**Panorama** > **Administrators**（管理者） を確認します。
- **Minimum Password Complexity**（最小限のパスワード複雑性）–パスワード最小限複雑性要求を確認。

次へ：ベスト プラクティス変更の優先順位。

ベスト プラクティス変更の優先順位

BPAレポートの情報量は膨大になり得ます。この章では、設定を改良する優先順位を決める支援をするための推奨項目を提供するので、セキュリティギャップを埋めることができ、最初に最も高価値の強化策を実施し、そしてベストプラクティスセキュリティ体制達成に向けて進むことができます。

Panorama が管理する環境では、*Panorama* が多数の次世代ファイアウォールを管理する場合があります。*Panorama* または個々のファイアウォールで *BPA* を実行する必要がありますか?比較するのは、スピードと利便性に対する完全性です。

*BPA*を*Panorama*側で実行すると、処理が高速で便利です。管理対象ファイアウォールのほとんどの機能が評価されますが、ローカルファイアウォールのオーバーライドは検討されません。

管理対象の各ファイアウォールで *BPA* を実行すると、設定全体 (ローカルのオーバーライドを含む) が評価されますが、非常に時間がかかります。

最も実用的な方法は、最初に *Panorama* で *BPA* を実行することです。結果を調べて、特定の管理対象デバイスに注目する必要があるかどうかを判断し、それらのデバイスで *BPA* を実行します。この方法により、時間を節約しながら、セキュリティ体制を改善できる関連情報に集中できます。

以下のトピックは、新しい展開が普通に導入され、始めに管理面に焦点が当てられ、次に可視性、制御および強制の順序のセキュリティ体制をどのように改善するかについて注目しています。既存の展開は、それぞれのエリアで一定の成熟度を達成しているかもしれません。

- デバイス管理体制の強化
- トラフィックの可視性を改善する
- 初期ベスト プラクティス制御を実装する
- ベストプラクティスコントロールの調整と強化

デバイス管理体制の強化

デバイス管理体制を強化することは、ファイアウォールのセキュリティを確保し、これを損ねる可能性のある不正アクセスを防ぐことに繋がります。これにより、予定していないイベントが運営に与える影響を低減させ、ファイアウォール動作の可視性を向上させます。

- 管理アクセスのベストプラクティスに従って、デバイスの管理インターフェースへの不正アクセスや、セキュリティで保護されていないアクセスを防止します。
- システム関連のイベントと設定の変更を追跡するため、すべてのシステムと設定ログをPanorama と第三者モニタリングソリューションに送信します。
- 設定バックアップ スケジュールを作成すると設定関連案件とシステムの停止状態の修正が迅速になります。

設定を変更した後、BPAを実行し、変更を検証し、進捗状況を確認し、次の変更を優先順位付けします。

次へ：トラフィックの可視性を改善する。

トラフィックの可視性を改善する

見えない脅威は防御することができないため、あらゆるユーザーやアプリケーションについて、常にトラフィックの十分な可視性を維持しなければなりません。ネットワーク上のアプリケーション、コンテンツおよびユーザーの完全な可視化を実現することが、データに基づいたポリシー制御を行うための最初のステップになります：

- セキュリティプロファイルの適用を最大化します。適用サマリーのレビューをし、適用時のギャップを確認したら、安全な移行ステップに従ってギャップを修正し、ベストプラクティスセキュリティ プロファイルをすべて実装します。
- ロギング（Log Forwarding（ログ転送）を含みます）をセキュリティルールベース全体で最大限に適用し、すべてのトラフィックを検査します。
- ファイアウォールが、ネットワークを保護するための最新のアプリケーションおよび脅威シグネチャを有することを保証し、ネットワークセキュリティおよび可用性の要求に基づいて更新を適用するのを徹底するために、ダイナミックコンテンツ更新用ベストプラクティスを設定します。
- ベスト プラクティスに基づいてSSL 復号化の展開を計画します。
- ユーザーゾーン（ユーザーがトラフィックを発生させる、信頼された内部ゾーン）でUser-IDを有効化し、アプリケーショントラフィックおよび関連する脅威をユーザーおよびデバイスにマッピングします。

  外部の信頼されていないゾーンで*User-ID*を有効化してはなりません。外部の信頼されていないゾーンで *User-ID*（または*WMI*のようなクライアントによるプローブ）を有効にすると、保護されたネットワークの外にプローブが送信される可能性があります。これにより、*User-ID* エージェントのサービス アカウント名、ドメイン名、暗号化されたパスワード ハッシュ等の*User-ID*情報が漏洩し、攻撃者がネットワークを危殆化できるようになる場合があります。

- アプリケーション オーバーライド ルールを減らすか削除して、これらのルールが制御するアプリケーションとコンテンツを検査できるようにします（アプリケーション オーバーライド ルールは、ファイアウォールがトラフィックを検査することを許可しないレイヤー4ルールです）。基本的なアプリケーション オーバーライド ルールの必要性をなくすか、またはその範囲を狭めます：
  - そのルールを使用するケースがまだ存在するかどうかを検証します。アプリケーション オーバーライド ルールは往々にして、性能、プロトコルデコーダーまたは未知のアプリケーションに関連する特定の問題に対処するために生成されています。アプリケーション オーバーライド ルールの中には、時間経過とともに、PAN-OS更新、コンテンツ更新やハードウェアアップグレードの結果、必要性がなくなるものがあります。ファイアウォールにPAN-OS 9.0以降のバージョンまたは、PAN-OS 8.1 （またはそれ以降）を実行しているファイアウォールを管理しているPanoramaにPAN-OS 9.0以降のバージョンを実行している場合は、ポリシー オプティマイザーを使ってルールをレイヤー7ルールに変換することができます。
  - アプリケーション オーバーライド ルールの適用範囲を、影響を受けるトラフィックの量が最も少なくなるように減らします。適用範囲が広すぎるルールは、必要以上にまたは意図したよりも広くオーバーライドする可能性があります。適用範囲をできるだけ制限する

には、個々のアプリケーション オーバーライド ルールにおいて、送信元・宛先のゾーン、アドレスやポートを明確に規定します。

- 内部アプリケーション用には、レイヤー7カスタムアプリケーションを生成します。
- カスタムタイムアウト値を使ってサービスオブジェクトを生成します。

- フラッド防御閾値を妥当な値に設定できるよう、DoS防御およびゾーン プロテクションを導入することを考えさらに、ベースラインCPS測定を行います。

これらのネイティブなApp-ID、コンテンツID、User-IDおよびSSL 復号化機能を実装すると、ファイアウォールは、すべてのトラフィック（アプリケーション、脅威およびコンテンツ）に対し可視化でき、検査できるようになり、場所、デバイスタイプ、ポート、暗号化その他の攻撃者の侵入手法に関係なく、様々なイベントをユーザーに結びつけることができます。

SSL 復号化、ロギング、フラッド防御、セキュリティプロファイル等の機能の適用率を改善することは、ファイアウォールのリソース消費の増加を引き起こす可能性があります。ファイアウォールの容量を把握し、増大する負荷を処理できるだけの十分な容量があることを確認してください。必要なら、導入に必要なサイズについて、最寄りの*Palo Alto Networks SE*または*CE*にご相談ください。また、ロギングのための格納スペースの追加が必要な場合もあります。

設定を変更した後、BPAを実行し、変更を検証し、進捗状況を確認し、次の変更を優先順位付けします。

次へ：初期ベスト プラクティス制御を実装する。

初期ベスト プラクティス制御を実装する

ネットワーク上のトラフィック（アプリケーション、コンテンツ、脅威およびユーザー）の可視性およびコンテキストが得られた後は、ベストプラクティス設定への移行を完成させるべく、攻撃対象領域を縮小し既知および未知の脅威を防止するための厳格な統制を実現します。

- 適用サマリーのレビューをし、適用時のギャップを確認したら、安全な移行ステップに従って、脅威をブロックし、攻撃対象領域を縮小するためのベストプラクティスセキュリティプロファイルを作成します。その際、貴重なビジネス資産を保護するために、厳格なコントロールをデータセンターに実装します。
- データセンターおよび界（それを取り巻く）ァイアウォールのためのアプリケーションベースのセキュリティポリシー・ルールを制定します。境界ファイアウォールのベストプラクティス推奨事項は、データセンターにない別のファイアウォールにも使用します。ファイアウォールにPAN-OS 9.0以降のバージョンまたは、PAN-OS 8.1 （またはそれ以降）を実行しているファイアウォールを管理しているPanoramaにPAN-OS 9.0以降のバージョンを実行している場合は、ポリシー オプティマイザーを使って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することができます。
- ユーザーベースのアクセスポリシーを生成します。
- ベストプラクティスのゾーン プロテクション プロファイルをすべてのゾーンに展開します。
- ファイアウォールが、暗号化されたトラフィックの可視性を獲得し（復号化し）て検査することができるように、SSL Decryption（SSL復号化）を設定します。

統制制御機能を装備した後ファイアウォールは、許可されたすべてのトラフィックをスキャンし、ネットワークおよびアプリケーション層脆弱性エクスプロイト、バッファオーバーフロー、DoS攻撃、ポートスキャンならびに既知および未知のマルウェア変種を検出しブロックすることができます。ファイアウォールは、悪意のあるアプリケーションおよび望んでいないアプリケーションをブロックするだけでなく、アプリケーションアクセスおよびユーザーアクセスも制御できます。

設定を変更した後、BPAを実行し、変更を検証し、進捗状況を確認し、次の変更を優先順位付けします。

次へ：ベストプラクティスコントロールの調整と強化。

ベストプラクティスコントロールの調整と強化

ネットワークトラフィック–アプリケーション、コンテンツ、脅威およびユーザーに関する統制を実現した後は、統制制御の微調整を開始し、追加機能を実現してセキュリティ体制を改善します。

- トラフィックの可視性を上げトラフィックを制御できるよう、内部アプリケーションをカスタムアプリケーションにまだ変換していなかった場合は、内部アプリケーションをカスタムアプリケーションに変換します。
- 安全な移行ステップを使ってベストプラクティス プロファイルへの移行を開始した後、セキュリティプロファイルをベストプラクティスに合わせます。
- Palo Alto Networksおよび信頼できるサードパーティー フィードから得た脅威情報に基づいて、既知の悪意あるIPアドレスをブロックします。
- をデプGlobalProtect またはPrisma Accessを展開することで、ユーザーとデバイスがどこにあるかに関係なく、次世代のセキュリティ プラットフォームをユーザーとデバイスに拡張します。
- 認証情報盗難の防止を有効化します。
- ネットワークベースのMulti-Factor Authentication（多要素認証）を設定します。

次へ：BPAを実行することにより変更を検証し、進捗度を測定し、次の変更の優先順位づけをし、その上で、ベストプラクティスをさらに学習し、PanoramaおよびPAN-OSの次世代ファイアウォールの多くのセキュリティ機能についての詳細を確認してください。