*BPA*およびセキュリティ保証によるベストプラクティスの開始

Version 9.1

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

March 5, 2020

Table of Contents

スタート ガイド (ベスト プラクティス)

セキュリティ ベスト プラクティスは、既知および未知の脅威を予防し、攻撃可能範囲を縮小し、トラフィックの可視性を提供するために、自社のネットワーク上にどのようなアプリケーション、ユーザーおよびコンテンツが存在するかを知り、それらを管理することができます。セキュリティ ベスト プラクティスを導入することで、以下のことが可能になります：

- 侵入成功の確率を最小化できます。
- 攻撃者の存在を検知できます。
- 重要なデータを保護します。
- 顧客、パートナーおよび従業員を守ることにより、会社の評判を守ることができます。
- Zero Trust (ゼロトラスト) セキュリティ環境を実現する一助になります。

セキュリティ ベスト プラクティスに移行するには、先ず自分の現在のネットワークセキュリティ体制を理解し、改善点を見つけ出すことが必要です。Palo Alto Networksは、 ベストプラクティス アセスメント(BPA)に加えて安全な移行手順やベストプラクティス技術文書が充実しており、これにより、お客様のベストプラクティスへの移行を支援しています。

Premium (2019年11月1日以降) またはPlatinumサポート契約に加入している場合は、Security Assurance (セキュリティ保証) の準備とアクティブ化を行えます。Security Assurance (セキュリティ保証) では、インシデントの初期調査に役立つ、Palo Alto Networksのセキュリティエキスパートとツールをご利用いただけます。

- ベスト プラクティスを特定し優先順位を付けます。
- BPAにアクセスし実行する
- Security Assurance (セキュリティ保証)

ベスト プラクティスを特定し優先順位を付けます。

Palo Alto NetworksのベストプラクティスアセスメントBPAは、ユーザーのTech Support File（技術支援ファイル）を使ってPanoramaおよび次世代ファイアウォールの設定設定を分析し、それをPalo Alto Networksのベストプラクティスと比較します。BPAは、ベストプラクティスセキュリティの現在の適用状況を表示し、セキュリティのベストプラクティスに準じた設定に合わせるよう、具体的な変更点を提案します。BPAを実行すると、現在のセキュリティ体制の改善点を理解することができるだけではなく、後ほど比較するためのベースラインを設定したり、BPAの推奨事項からベストプラクティス設定にどのように移行していくのかを示す技術文書へのリンクを提供したりすることができます。

優先順位づけされた反復的アプローチを採用することで、セキュリティ体制を一歩ずつ着実に（焦ることなくマイペースで進みながら進捗状況を測定しつつ）ベストプラクティス状態に変革していくことができます：

STEP 1 | Tech Support Fileをカスタマーサポートポータルにアップロードして、ご自分でBPAにアクセスし実行するを行うか、またはPalo Alto Networks SEまたはパートナーに連絡して、Panoramaまたは次世代ファイアウォール上でBPAを実行してください。

BPAを自分で実行する場合は、結果の解釈や今後のステップについて話合うために、最寄りのPalo Alto Networks SEまたはパートナーに連絡されることを推奨します。

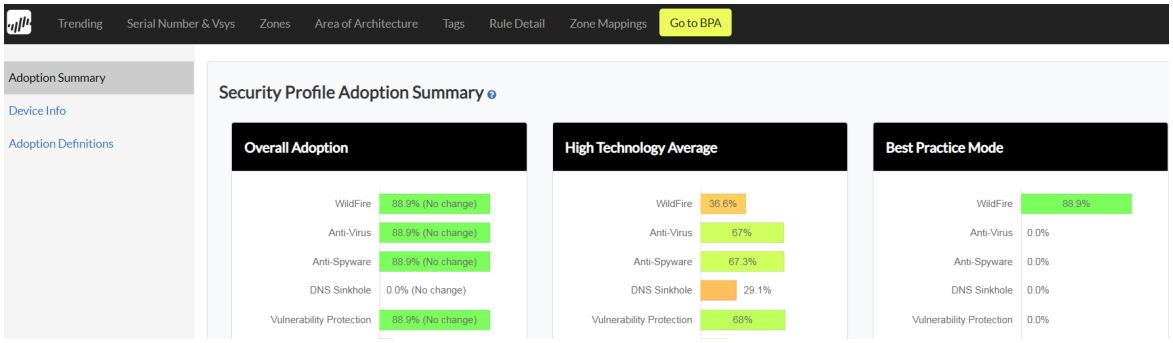
STEP 2 | ベストプラクティスへの移行を開始するには先ず、検討すべき最初の改善点を特定し、優先順位づけをします。

BPAを自分で実行した場合でも、Palo Alto Networks SEまたはパートナーが実施した場合でも、SEまたはパートナーは、ベストプラクティスを安全に導入する為の、優先順位づけの計画立案に協力いたします。最も安全・簡単で最も影響が大きい変更から着手すると良いでしょう。これには、アンチウィルス、アンチスパイウェア、脆弱性防御およびWildFire分析プロファイルをセキュリティポリシー許可ルールに適用することが含まれます。

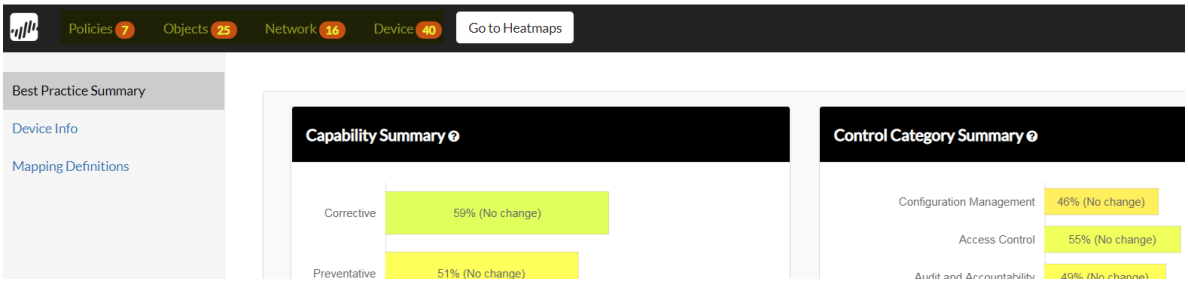
STEP 3 | BPAの技術文書へのリンクを使用し、優先順位をつけたベストプラクティスを設定します。

BPAレポートをダウンロードすると、詳細なHTMLレポート、エグゼクティブサマリー、およびベストプラクティスで不合格となった項目のExcelリストをまとめた.zipファイルが入手できます。技術文書を参照するには以下の2つの方法があります：

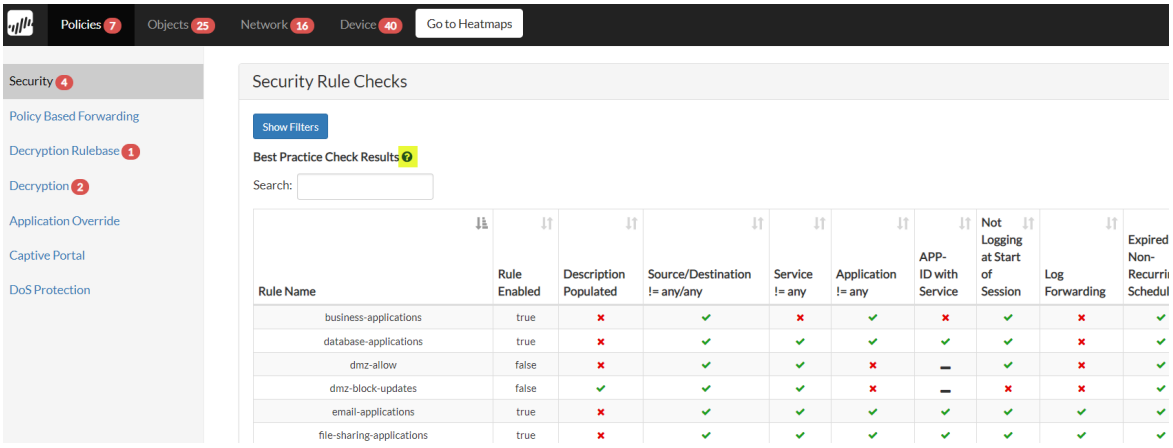
- Excelファイルから—Documentation（文書）タブに、各不合格項目へのリンクがあります。さらに、Policies（ポリシー）、Objects（オブジェクト）、Network（ネットワーク）およびDevice（デバイス）タブのCheck ID欄のID番号は、Documentation（文書）タブの関連する行に直接リンクしています。
- HTMLレポートから— HTMLレポートを開くと、ベストプラクティスを採用し要約したヒートマップが表示されます。**Go to BPA**（**BPA**に移動）をクリックしてレポートにアクセスします。



選択した設定評価に関し、BPAサマリページから、**Policies**（ポリシー）、**Objects**（オブジェクト）、**Network**（ネットワーク）または**Device**（デバイス）の詳細レポートを閲覧します。



詳細レポートから、青い丸印の?をクリックすると、設定チェックの説明と理由、およびベストプラクティス設定に関する技術文書へのリンクが表示されます。



セキュリティ プロファイル（脆弱性防御、アンチウィルス、アンチスパイウェア、URLフィルタリング、ファイル ブロッキング）については、安全な移行のアドバイスに従い、ベストプラクティス セキュリティプロファイルに移行する際は、業務上、最重要アプリケーションが継続して使用できるよう注意します。

STEP 4 | ベストプラクティスのための最初の変更を実現した後、BPAを再度実行し、進捗状況を確認し、変更が期待通り機能していることを検証します。

BPAの最初の結果と2番目の結果を比較し、セキュリティ体制の改善点を確認してください。次に検討すべき改善点を見つけ出し、優先順位を付けます。

STEP 5 | BPAの技術文書へのリンクを使用し、優先順位をつけた次のベストプラクティスを設定します。

STEP 6 | 焦ることなく自らのペースで、BPAを実行する手順を繰り返し、進捗状況を確認し、次のステップを特定し優先順位づけし、その後、技術文書を使ってベストプラクティスを設定します。

STEP 7 | すぐ始めましょう。BPAにアクセスし実行する必要なら、最寄りのPalo Alto Networks SEまたはパートナーの協力を得てよりセキュリティの高いネットワークへの移行を今すぐ始めましょう！

BPAにアクセスし実行する

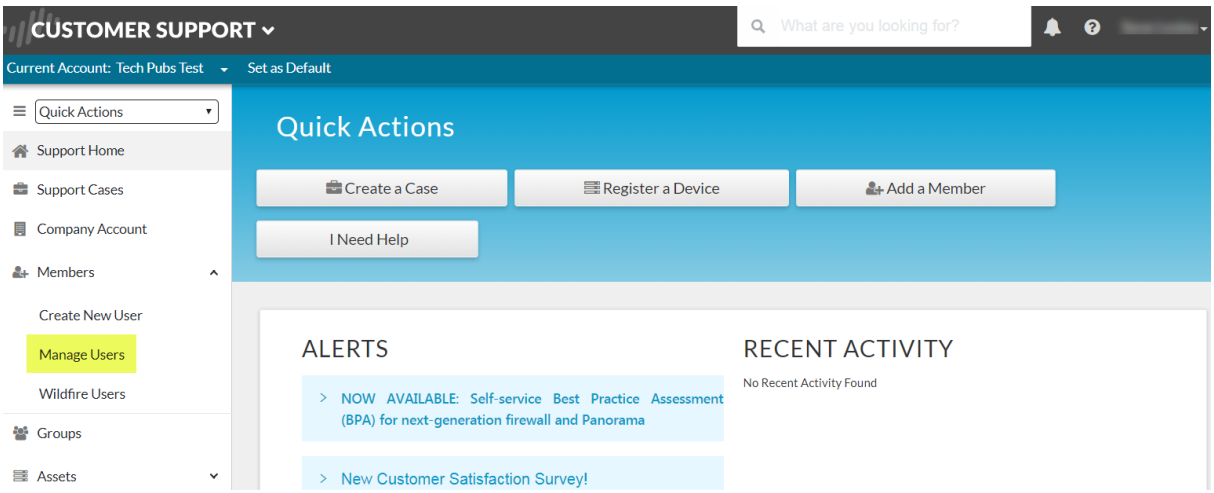
カスタマー サポート ポータル(Customer Support Portal)から、ベストプラクティス評価 (BPA) にアクセスします。スーパーユーザー(Super User)アカウントは、自動的にBPAにアクセスし、標準ユーザープロファイルに*BPA*ユーザーのロールを与えることで、標準ユーザーはBPAを実行することができます。この手順は、スーパーユーザーで、どのようにして標準ユーザーにアクセス権を与え、どのようにしてBPAを実行するかを示しています。BPAの実行方法および結果をどう理解するかについては、簡単なビデオが用意されています。

また、Premium（2019年11月1日以降）またはPlatinumサポート契約に加入している場合は、Security Assurance（セキュリティ保証）の準備とアクティブ化を行えます。Security Assurance（セキュリティ保証）では、インシデントの初期調査に役立つ、Palo Alto Networksのセキュリティエキスパートとツールをご利用いただけます。ネットワークを適切に保護するために、BPAを実行して、7つの主要セキュリティ機能の採用状況を確認し、採用率がご自分の業界の平均値以上になっていることを確認してください。PremiumまたはPlatinumサポート契約があり、7つの主要セキュリティ機能の採用率を表すBPA測定が業界の平均を満たしていると、Security Assurance（セキュリティ保証）が自動的にアクティブ化されます。

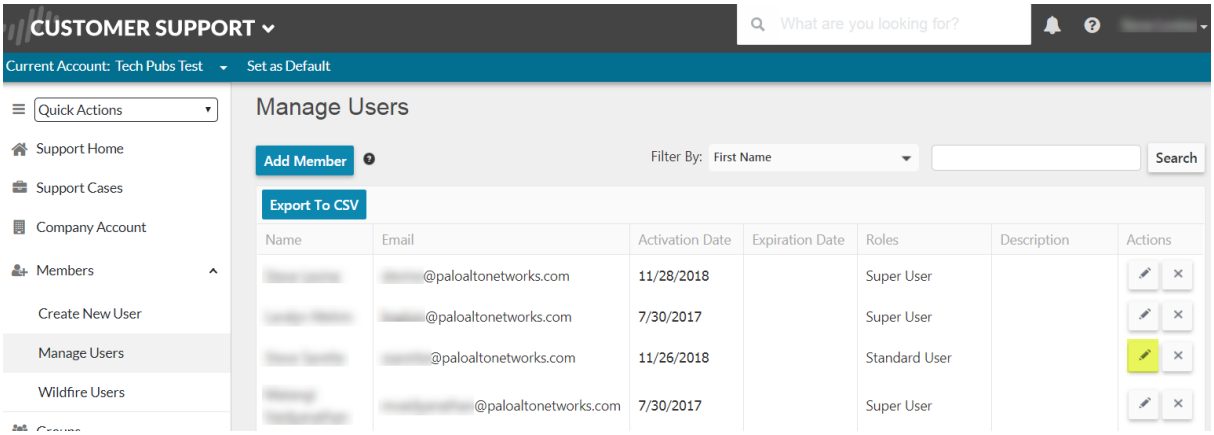
- カスタムサポートポータルからのBPAへのアクセス
- BPAレポートの生成とダウンロード

カスタムサポートポータルからのBPAへのアクセス

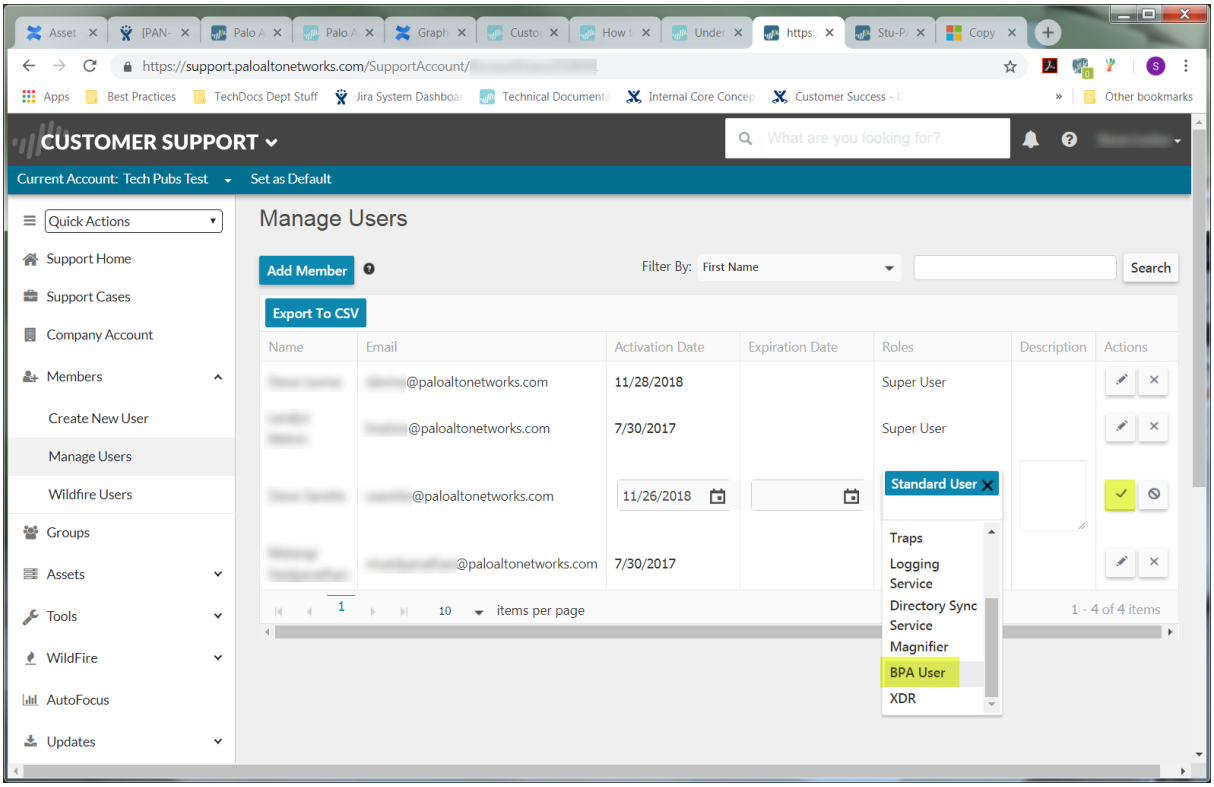
STEP 1 | カスタマー サポート ポータル(Customer Support Portal)の認証ホーム画面で、**Members**（メンバー）> **Manage Users**（ユーザーを管理）を選択します。



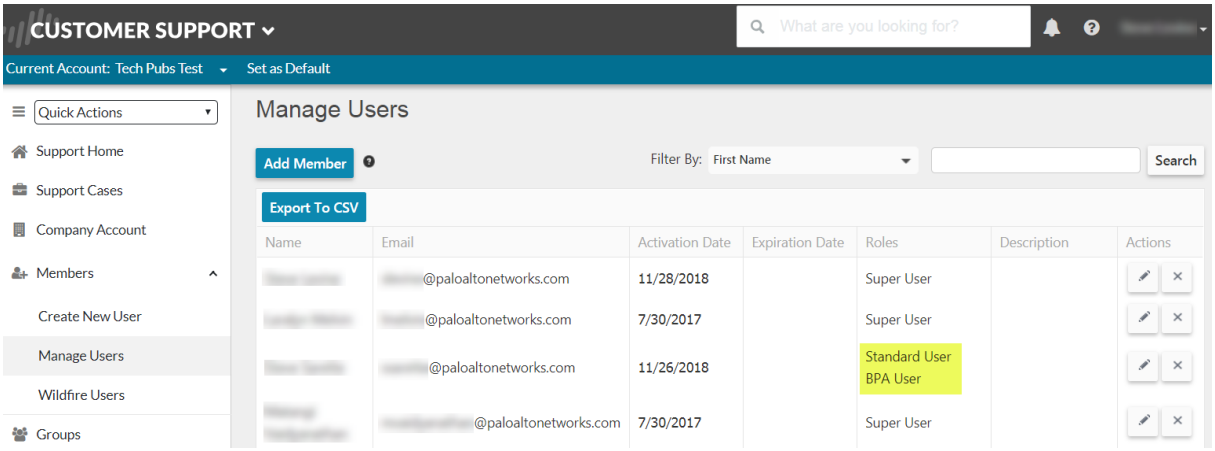
STEP 2 | 鉛筆アイコンをクリックし、BPA許可を与えたい標準ユーザー（Standard User）を編集します。



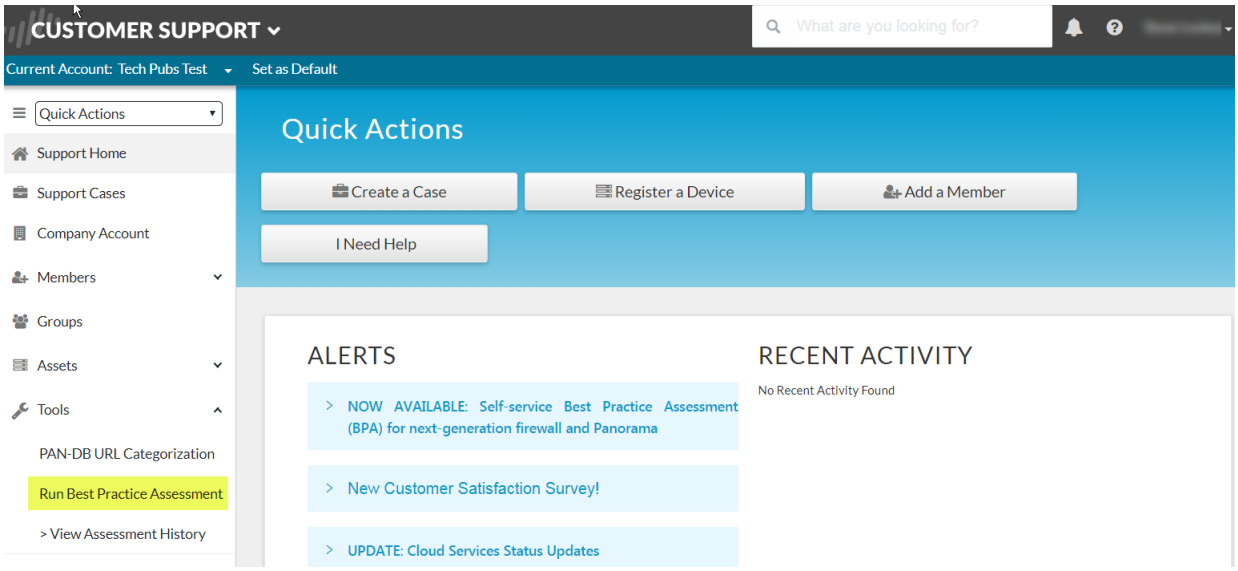
STEP 3 | **BPA User**（BPAユーザー）ロールを選択し、更新チェックマークをクリックして新しいロールを追加します。



STEP 4 | 標準ユーザーに、BPAユーザーロールのアクセス許可が与えられます。



STEP 5 | スーパーユーザーおよびBPAユーザー ロールを有する標準ユーザーは、カスタマーサポートポータルにログインし、BPAにアクセスし実行することができます（**Tools**（ツール）> **Run Best Practice Assessment**（**BPA**を実行））。



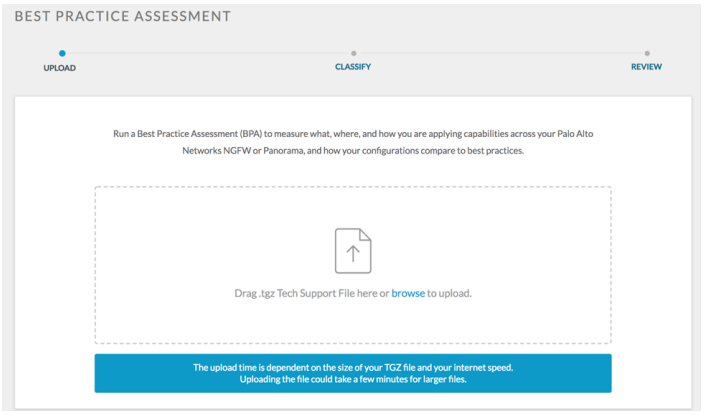
BPAレポートの生成とダウンロード

BPAにアクセスできるようになったら、Panoramaアプライアンスまたは次世代ファイアウォールのBPAレポートを生成することができます。

可能な場合は、個別の次世代ファイアウォールではなく*Panorama*アプライアンスの*BPA*レポートを生成し、単一のレポートで環境内のすべてのファイアウォールを明確に把握できるようにしてください。定期的にレポートを生成し、セキュリティ機能とセキュリティ上のベストプラクティスの採用状況を評価してください。

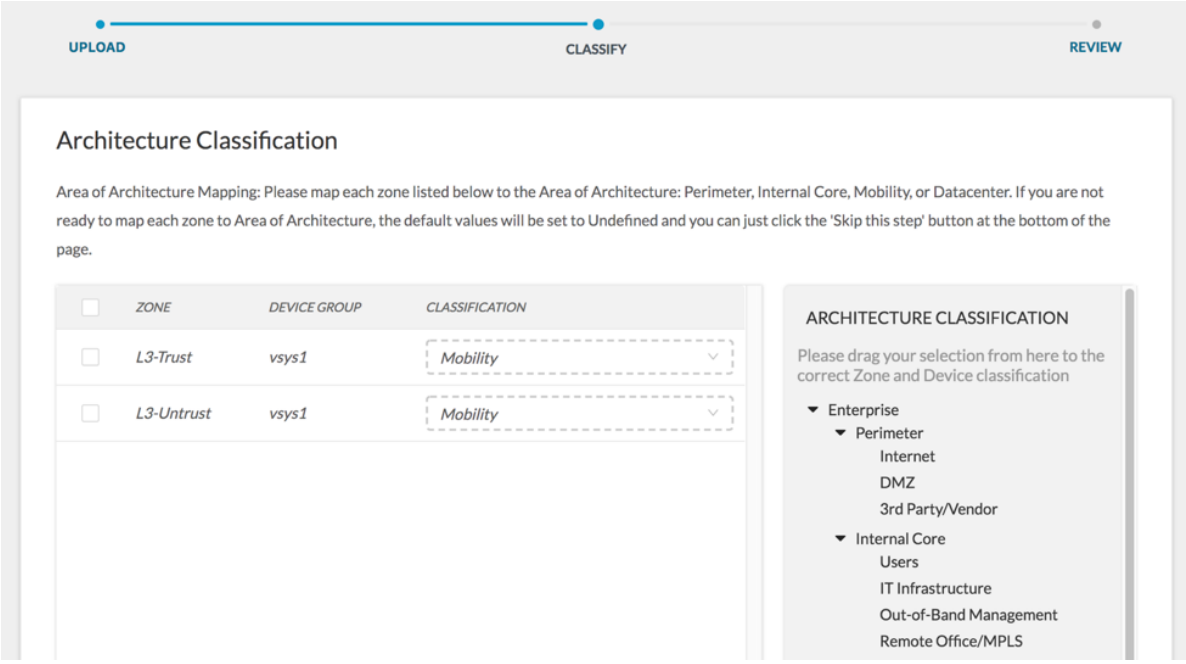
STEP 1 | Customer Support Portal（カスタマーサポートポータル）ウィンドウにTech Support File（.tgzファイル）をドラッグアンドドロップするか、Tech Support Fileをブラウザ上で探します。

スーパーユーザーは、Tech Supportファイルを生成することができます（**Device**（デバイス）> **Support**（サポート）> **Tech Support File**または**Panorama** > **Support**（サポート）> **Tech Support File**）。



STEP 2 | 代わりに、各ゾーンをアーキテクチャの領域にマッピングするか、マッピングしないで**Skip this step**（このステップをスキップする）をクリックしてBPAを実行することができます。

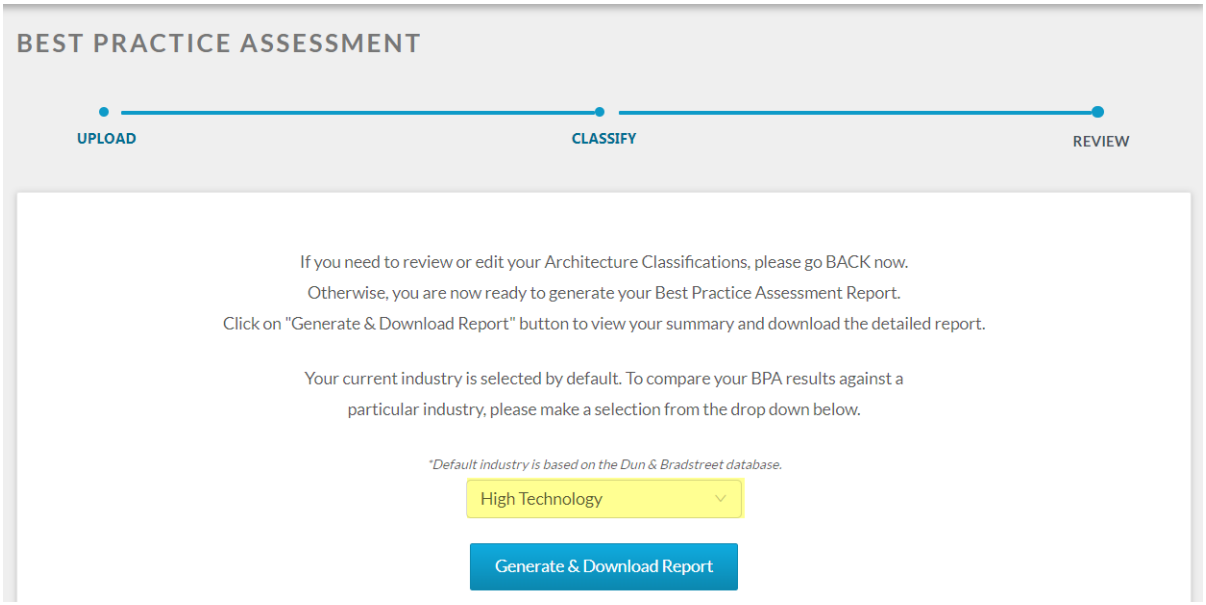
Architecture Classification（アーキテクチャ分類）から、アーキテクチャ値をドラッグアンドドロップするか、**Classification**（分類）ドロップダウンメニューを使って値を選択するか、複数のチェックボックスを選択して複数のゾーンを選択し、1回で選択したゾーンすべてに同じ値を適用します。



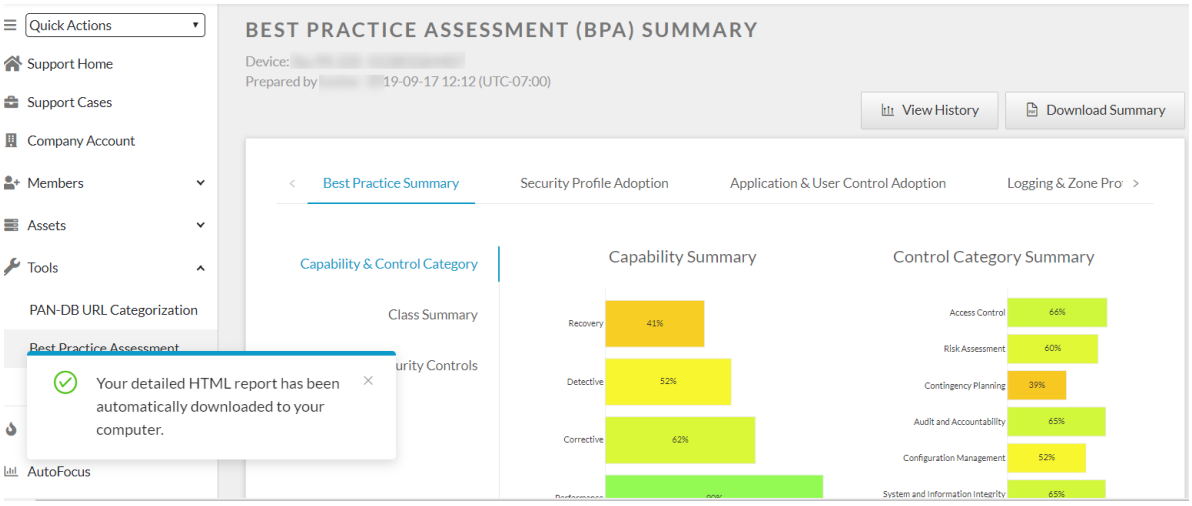
STEP 3 | アカウントにマップされている業界を指定して、BPAレポートを生成、ダウンロードします（**Generate & Download Report**（レポートの生成とダウンロード））。

ドロップダウンを使って、BPAが結果と比較する業界を変更することができます。レポートの生成前に変更する項目がある場合は、元に戻って変更を行います。

Generate & Download Report（レポートの生成とダウンロード）を実行すると、詳細なBPAレポート、Executive Summary（エグゼクティブサマリー）レポート、およびBPAにアクセスして実行したシステムでの、不合格になったベストプラクティスチェックを表すスプレッドシートがダウンロードされます。



STEP 4 | 生成されたBPAには、エグゼクティブサマリー、およびコンピュータに詳細なHTMLレポートがダウンロードされたことを知らせるメッセージが表示されます。



STEP 5 | 以上がBPAの実行方法になります。早速Customer Support Portal（カスタマーサポート ポータル）にアクセスし、よりセキュアなネットワークへの移行を体験してみましょう（必要な場合は、Palo Alto Networks SEまたはパートナーがお手伝いします）。

Premium（*2019*年*11*月*1*日以降）または*Platinum*サポート契約に加入している場合は、*BPA*を使ってセキュリティに対する姿勢を強化して、インシデントの初期調査に役立つSecurity Assurance（セキュリティ保証）を有効活用してください。

Security Assurance（セキュリティ保証）

ネットワークで不審なアクティビティが検出された場合、Security Assuranceによりお客様がもっとも必要としている時に、Palo Alto Networksから支援を受けることができます。Security Assurance（セキュリティ保証）は、以下のサービスを提供しています。

- Palo Alto Networksのセキュリティエキスパート、および特別な脅威インテリジェンスツールと脅威への対処事例へのアクセス。
- 詳細ログと不正行為（IOC）解析のインジケータ。
- カスタマイズされた製品セキュリティの推奨事項を含む、構成評価。
- インシデントの管理と解決に役立つ、インシデント対応（IR）ベンダーへの移行を迅速に行うための、次のステップの推奨事項。

Security Assuranceを有効活用するには、Premiumサポート契約（2019年11月1日以降）またはPlatinumサポート契約に加入する必要があります。

Security Assuranceを利用するための最初のステップは、ベストプラクティスアセスメント（BPA）を実行して、WildFire、ウィルス対策、スパイウェア対策、DNSシンクホール、URLフィルタリング脆弱性保護、およびロギングの、7つの主要セキュリティ機能の採用状況を評価することです。これらの主要機能の採用率を、業界の平均採用率以上にしておくことをお勧めします。

BPAを実行して主要セキュリティ機能を高いレベルで採用すると、ネットワークの保護が強化され、インシデント発生を削減することができます。BPAは、App-IDとUser-ID、ゾーン設定、およびその他のセキュリティプロファイル（File BlockingおよびDoS Protectionプロファイルなど）のような、その他のセキュリティ機能の採用レベルも測定し、セキュリティ体制を改善するための推奨事項を提供します。

定期的に*BPA*を実行して（たとえば、毎月、または四半期ごと）、主要セキュリティ機能の採用状況を測定し、ネットワークセキュリティの状態を把握して、セキュリティ上の改善事項に優先順位を付けるようにしてください。

Premiumサポート契約（2019年11月1日以降）またはPlatinumサポート契約に加入してBPAを実行した場合、7つの主要セキュリティ機能の採用率が業界の平均値以上になっている場合、Security Assuranceが自動的に有効になります。これらのセキュリティ機能の採用率を業界の平均値以上にするために何らかのお手伝いが必要な場合は、要件の定義方法や評価基準の設定など、お困りのことをPalo Alto Networksの営業担当にご相談ください。ビジネス上の理由で主要セキュリティ機能を適切なレベルまで導入できないは、Palo Alto Networks営業担当と協力して、Security Assuranceにアクセスして、利用するための手段をお探しください。

採用する必要がある7つの主要セキュリティ機能

以下の理由で、これらの7つの主要セキュリティ機能を採用することを強くお勧めします。

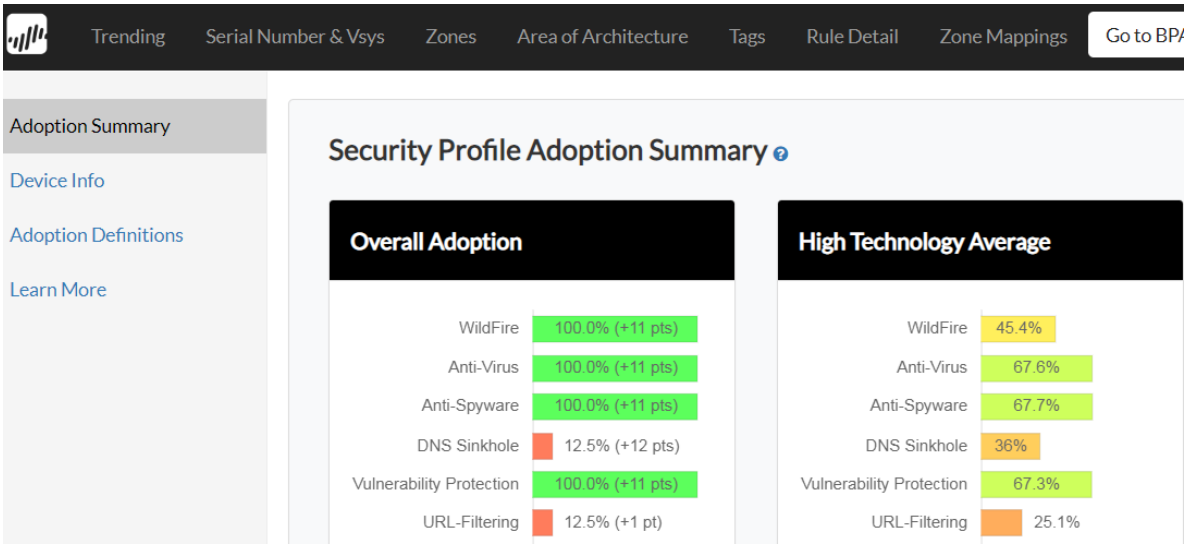
- **WildFire**—セキュリティポリシールールにWildFireセキュリティプロファイルをアタッチして、ネットワークを新たな未知の脅威からネットワークを保護します。WildFireは、持続的標的型攻撃（ATP）に対する強力な保護手段となっています。
- ウィルス対策—セキュリティポリシールールにAntivirus（ウィルス対策）セキュリティプロファイルをアタッチして、マルウェア、ランサムウェア、ボット、ウィルスなどの、既知の悪意のあるファイルをブロックします。

- スパイウェア対策–セキュリティポリシールールにAnti-Spyware（スパイウェア対策）セキュリティプロファイルをアタッチして、サーバーやエンドポイント上で動作する悪意のあるコードが始動したり、コマンド&コントロール（C2）トラフィックを検出し、侵入されたシステムがネットワークからのアウトバウンド接続を確立することを防止します。
- **DNS**シンクホール–セキュリティポリシールールにアタッチされているAnti-Spywareセキュリティプロファイルの、「DNS Sinkhole」（DNSシンクホール）部分を設定、修正します。DNS シンクホールは、ホストを追跡し、それらが疑わしいドメインにアクセスできないようにすることで、疑わしいドメインにアクセスしようと試みる侵入された可能性があるホストを特定できます。
- **URL**フィルタリング–セキュリティポリシープロファイルにURL Filtering（URLフィルタリング）プロファイルをアタッチして、危険なWebコンテンツ（悪意のあるコンテンツが存在する可能性があるサイト）へのアクセスを防止します。URL Filteringプロファイルと URLカテゴリを利用することで、アクセスを許可するWebサイトのタイプをきめ細かく調整することができます。
- 脆弱性保護–セキュリティポリシールールにVulnerability Protection（脆弱性保護）セキュリティプロファイルをアタッチして、攻撃者がクライアント側およびサーバー側の脆弱性を悪用する、および悪意のあるペイロードをネットワークやユーザーに配信することを防止します。また、攻撃者が脆弱性を利用して、ネットワーク内を自由に動き回ることを防止します。
- ロギング–すべてのトラフィック（許可と拒否）のログの記録を有効にして、システムイベントやネットワークトラフィックイベントのタイムスタンプ付きの監査証跡を保存します。ログは、インシデントの調査に重要な情報を提供しています。ログ転送により、すべてのファイアウォールからのログをPanoramaまたは外部に送信して、ログを集計して解析を行うことができます。

これらの主要機能を採用することで、セキュリティ体制の大幅な改善、攻撃面の削減、ネットワークトラフィックの可視性の向上、既知の攻撃や新たな攻撃の防止、ネットワークでもっとも貴重なデータ、アセット、アプリケーション、サービスの保護を実現することができます。

7つの主要セキュリティ機能の採用チェック

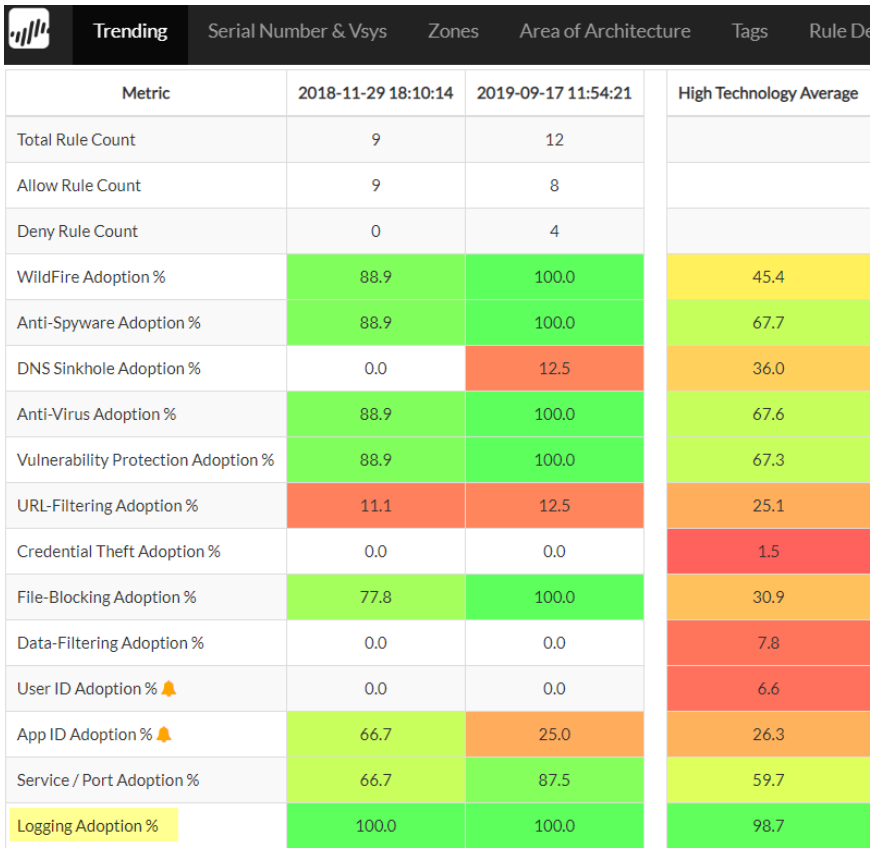
詳細なBPAレポート（HTMLフォーマット）で、BPA結果を生成、ダウンロードしたら、Adoption Summary（採用のサマリー）ページに移動して、6つのセキュリティプロファイル（WildFire、ウィルス対策、スパイウェア対策、DNSシンクホール、脆弱性保護、およびURLフィルタリング）機能、および業界におけるそれらの機能の採用率を確認してください（ロギングは別途のチェック項目です）。Adoption Summaryページには、業界の平均と比較したセキュリティ機能の採用状況が表示され、採用状況のギャップを判別するために役立ちます。たとえば、ハイテクノロジー業界の場合:



結果は、構成内容がWildFire、Antivirus（ウィルス対策）、Anti-Spyware（スパイウェア対策）、およびVulnerability Protection（脆弱性保護）の4つの機能に関して、業界平均の採用状況を満たしていることを表しています。この結果は、構成で、DNSシンクホールとURLフィルタリングの2つの機能が、業界平

均の採用状況を満たしていないことも表しています。このことは、次に対処する必要がある事項が、Anti-SpywareプロファイルのDNSシンクホールの設定およびインターネットトラフィックへのURLフィルタリングの適用であることを示唆しています。

詳細な HTML BPA レポートで、**Trending**（トレンド）ページに移動して、自社のロギング機能の採用率と業界平均のロギング採用率を確認します。



Trending | Serial Number & Vsys | Zones | Area of Architecture | Tags | Rule De

Metric	2018-11-29 18:10:14	2019-09-17 11:54:21	High Technology Average
Total Rule Count	9	12	
Allow Rule Count	9	8	
Deny Rule Count	0	4	
WildFire Adoption %	88.9	100.0	45.4
Anti-Spyware Adoption %	88.9	100.0	67.7
DNS Sinkhole Adoption %	0.0	12.5	36.0
Anti-Virus Adoption %	88.9	100.0	67.6
Vulnerability Protection Adoption %	88.9	100.0	67.3
URL-Filtering Adoption %	11.1	12.5	25.1
Credential Theft Adoption %	0.0	0.0	1.5
File-Blocking Adoption %	77.8	100.0	30.9
Data-Filtering Adoption %	0.0	0.0	7.8
User ID Adoption %	0.0	0.0	6.6
App ID Adoption %	66.7	25.0	26.3
Service / Port Adoption %	66.7	87.5	59.7
Logging Adoption %	100.0	100.0	98.7

このページには、業界と比較した自社の採用レベルだけでなく、最後にBPAを実行した結果との採用レベルとの比較も表示されます。これは、時間の経過に伴うセキュリティの改善指標であり、セキュリティの結果が期待するほど完全ではない場合に、対処を促すための情報でもあります。

プロファイルとロギングの結果、7つの機能すべての採用状況が、業界の平均採用率を満たしている場合、Security Assuranceが自動的に有効になります。これらのセキュリティ機能の採用率を業界の平均値以上にするために何らかのお手伝いが必要な場合は、要件の定義方法や評価基準の設定など、お困りのことをPalo Alto Networksの営業担当にご相談ください。ビジネス上の理由で主要セキュリティ機能を適切なレベルまで導入できないは、Palo Alto Networks営業担当と協力して、Security Assuranceにアクセスして、利用するための手段をお探しください。

7つの主要セキュリティ機能の採用の改善

BPAとPalo Alto Networksの技術ドキュメントを利用して、改善が必要なセキュリティ機能を判別して、必要な改善を実施します。特に、7つの主要セキュリティ機能を重視してください。セキュリティ体制を改善することで、ユーザーおよび貴重なデバイス、アセット、アプライアンス、サービスを安全に保護することができます。

- **WildFire**—WildFireプロファイルのベストプラクティスへの安全な移行を行い、WildFireのベストプラクティスを導入します。ベストプラクティスWildFireプロファイルは、デフォルトのプロファイルです。

- ウィルス対策—Antivirus（ウィルス対策）プロファイルをベストプラクティスに安全に移行して、ウィルス対策のベストプラクティス（または多少厳格なデータセンター用ウィルス対策のベストプラクティス）を導入します。
- スパイウェア対策とDNSシンクホール—DNSシンクホール設定は、Anti-Spyware（スパイウェア対策）セキュリティプロファイルのDNS Signatures（DNS署名）タブにあります。Anti-Spyware（スパイウェア対策）プロファイルをベストプラクティスに安全に移行して、スパイウェア対策のベストプラクティス（または多少厳格な、データセンター用スパイウェア対策のベストプラクティス）を導入します。
- URLフィルタリング—URL Filtering（URLフィルタリング）プロファイルを安全にベストプラクティスに移行して、URLフィルタリングのベストプロファイルを導入します。
- 脆弱性保護—Vulnerability Protection（脆弱性保護）プロファイルを安全にベストプラクティスに移行して、脆弱性保護のベストプラクティス（または多少厳格なデータセンター用脆弱性保護のベストプラクティス）を導入します。
- ロギング—デフォルトで、セッション終了時にログを記録するセキュリティポリシールール。

また、BPAおよび技術文書が、App-ID、User-ID、File Blocking（ファイルのブロック）プロファイル、DoSおよびゾーン保護、および認証情報盗用保護などのその他のセキュリティ機能を改善するための方法を説明しています。主要リソースの例を以下に示します。

- Getting Started with the BPA（BPAの紹介）—BPAを使って、セキュリティ機能採用状況のレビューおよび採用におけるギャップの識別、ポリシー、オブジェクト、ネットワーク、デバイス、Panorama構成などの設定の評価、デバイスの管理体制の強化などの変更の優先順位付け、トラフィックの可視性の改善、および初期のベストプラクティスの導入などを実施する方法について説明しています。
- Decryption Best Practices（解読のベストプラクティス）—ビジネスモデル内のすべてのトラフィック、プライバシーに関する検討事項、および規制を読み解いて、トラフィックをできる限り検査して、暗号化された脅威からネットワークを保護する方法について説明しています。
- DoS and Zone Protection Best Practices（DoSおよびゾーン保護のベストプラクティス）—ネットワークを停止させようとするサービス拒否（DoS）攻撃からの保護、およびネットワークの境界、ゾーン、および個別のデバイスを防護するための、多層化されたアプローチについて説明しています。
- Best Practices for Applications and Threats Content Updates（アプリケーションと脅威コンテンツのアップデートに関するベストプラクティス）—ビジネス要件に対して最適な方法でコンテンツやアプリケーションのアップデートをデプロイすることで、ネットワークを最新の脅威から保護したり、最新のアプリケーションを識別することができます。

これらのドキュメント、およびその他の役立つ情報は、Best Practices（ベストプラクティス）ポータルおよびTransition to Best Practices（移行のベストプラクティス）ページからご覧いただけます。

Security Assuranceを利用するために

疑わしい行動が見つかった場合、Security Assuranceを利用する前に、Palo Alto Networksのエキスパートがその行動を調査するための、疑わしいインシデントに関する一連の情報を用意する必要があります。

- Security Assuranceを利用する前に収集するデータ
- Security Assuranceの利用

*Security Assurance*を利用する前に収集するデータ

Palo Alto Networksのエキスパートが、潜在的な問題を診断するために、疑わしい行動について最低でも以下の情報が必要になります。Security Assuranceをご利用になる前に、これらのデータを収集してください。

疑わしい行動に関する基本的な情報。

- 疑わしい攻撃のベクトルとタイプ:管理チームまたは対処チームに警告が発せられた疑わしい行動の根拠（証拠）は何ですか？
- タイムライン:

    - 疑わしい攻撃が最初に行われた日時（分かっている場合）。
    - 潜在的な問題を発見した時刻。
- インシデントの詳細:
    - 影響を受けたシステムのIPアドレス。
        - 影響を受けたホストの、NATで公開されているIPアドレス。
        - システムをターゲットにした可能性がある重要なサービス。たとえば、データベース、Webサービス、リモートアクセス（RDP、Citrixなど）サーバーなどが挙げられます。
    - 攻撃に関連している可能性がある、既知のまたは疑わしいIPアドレス。
    - 不正利用されたアカウントのユーザーID（ある場合）。
- トポロジのダイアグラムまたは概要:影響を受けたホストに関連するファイアウォールの場所。（完全なネットワークトポロジである必要はありません。）
- マルウェアおよび侵害指標:
    - サンプル。
    - ハッシュ。

ファイアウォールデータ:

- テクニカルサポートファイル:
    - 疑わしい行動があった時点で、影響を受けた可能性があるデバイスのパスに存在していたファイアウォールから、Tech Supportファイルを生成、アップロードします。
    - Panoramaを使ってファイアウォールを管理している場合は、Panorama Tech Supportファイルを生成、アップロードします。
- ファイアウォールログ:疑わしい行動があった時点の2時間前からのログを、ファイアウォールおよびPanoramaからエクスポートします。ログをエクスポートする前に、CSVの行設定が最大値の65535行に設定されていることを確認してください（**Device**（デバイス）> **Setup**（セットアップ）> **Management**（管理）> **Logging and Reporting Settings**（ログとレポートの設定））。値が小さい場合は、最大値の65535行に変更してください。IPアドレス情報とタイムスタンプ詳細に基づいて（ログをフィルタリングして、IPアドレスと時刻に基づいてログエントリを表示できます）、次の基本ログカテゴリ（ログが有効になっている場合）から、それぞれのログをエクスポートします。
    - データフィルタリングログ
    - トラフィック ログ
    - 脅威ログ
    - URLフィルタリングログ
    - ユーザーIDログ（疑わしい横方向の移動があった場合）
    - WildFire送信ログ

関連するデータの調査漏れがないように、デプロイログ保持ポリシーと、ログ保持機能について理解しておくことが重要になります。管理者は、調査期間内のデータの連続性と完全性を保証するために、ファイアウォールまたは他のログサーバーからのデータのエクスポートなどの、追加作業を実施しなければならないこともあります。

疑わしい行動に関する有益なデータを識別するその他の方法:

- アプリケーションコマンドセンター（**ACC**）を使用します。ACCは、疑わしい行動の発生時、およびその前後におけるトラフィックの急増、異常、および変更などを表示できます。
- 疑わしい行動の発生中、またはその前後の期間における、発生数が上位の脅威に関する情報を表示するには、**Threat Monitor Report**（脅威モニターレポート）を使用します。

*Security Assurance*の利用

関連情報を円滑に解析するために、疑わしい行動に関するデータを収集したら、Security Assistanceを利用する準備は完了です。Security Assistanceを利用するには、2種類の方法が存在しています。

- カスタマーサポート ポータルにログインします。**Create a Case**（ケースの作成）をクリックして、サポートケースを開始します。フォームに記入したら、**Threat**（脅威）を選択します。
- お客様の代わりに営業担当エンジニア（SE）がサポートケースを開始することもできます。