

BPA スタート ガイド

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

セキュリティポリシー・キャパシティ適用の評価.....	5
適用サマリーのレビュー.....	6
適用におけるギャップを特定する.....	8
改善すべきルールを識別.....	12
 ベスト プラクティス設定の評価.....	 15
ベスト プラクティス サマリーのレビュー.....	16
ベストプラクティスポリシー設定のレビュー.....	18
ベストプラクティス オブジェクト設定のレビュー.....	20
ベストプラクティス ネットワーク設定のレビュー.....	21
ベストプラクティスデバイスとPanorama管理設定のレビュー.....	22
 ベスト プラクティス変更の優先順位.....	 23
デバイス管理体制の強化.....	24
トラフィックの可視性を改善する.....	25
初期ベスト プラクティス制御を実装する.....	27
ベストプラクティスコントロールの調整と強化.....	28

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。Introduction to Heatmaps (ヒートマップ入門) ビデオを閲覧してヒートマップの概要を学び、BPA video library (BPAビデオライブラリー) を活用してこのツールの詳細を学習しましょう。

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

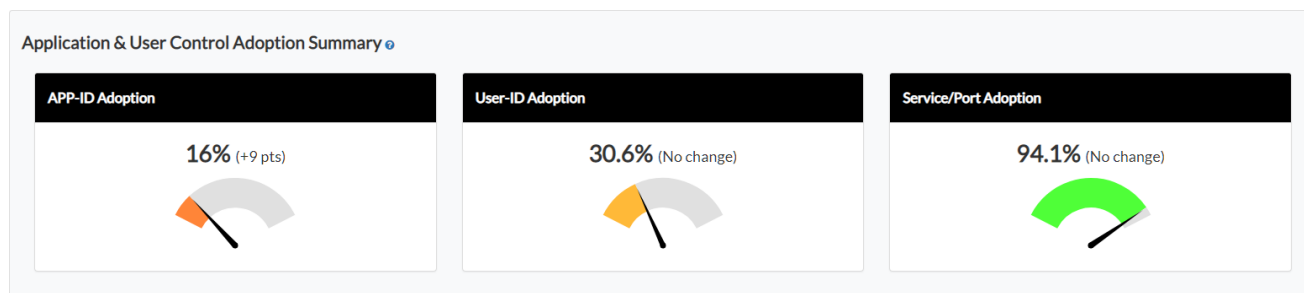
あなた、あるいはPalo Alto Networksの代理人が **BPAを実行**した後、結果としてのHTMLレポートが適用サマリーのヒートマップページ上で開かれます。適用サマリービューはセキュリティ能力のデバイス全体適用の全容を提供します。レポートは個々の測定基準（あなたの適用と比較する業界の選定平均を提供する業界平均を除く）の現在の適用割合を示します。そして括弧内に、デバイスの設定ファイルでBPAを最後に起動して以来の適用の割合変化を示します（値が最後にBPAを起動した時と同じであれば **No change**（変化なし）を示します）。



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。

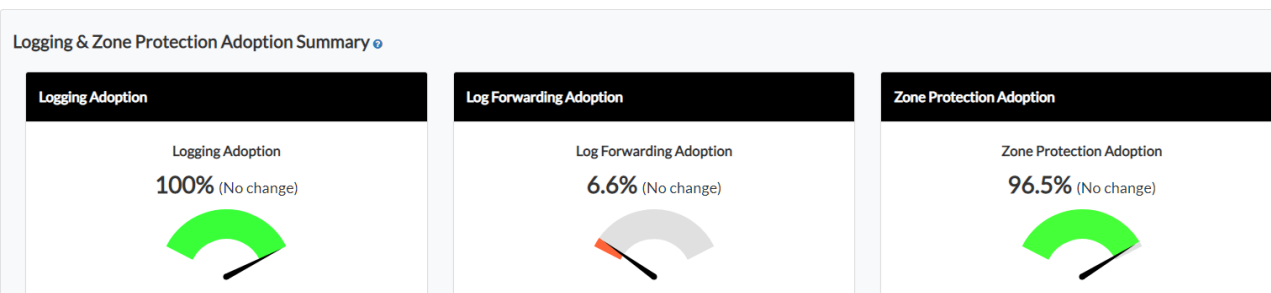


App-ID Adoption (App-ID 適用) –セキュリティポリシー全体でのApp-IDの適用。割合値は、一つ以上の定義されたアプリケーションがある許可ルールの合計数に基づいています（アプリケーションはanyではない）。BPAは無効化されたルールはカウントしません。

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ユーザー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、ユーザー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。

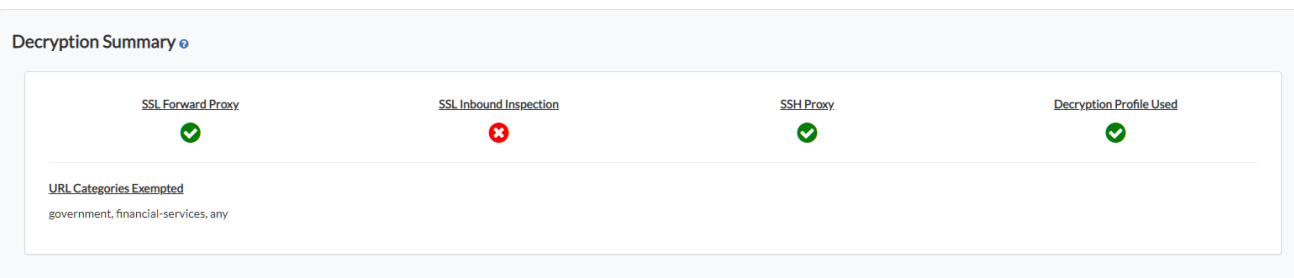


Logging Adoption (ロギング適用) –セキュリティポリシールール全体へのLog at Session End (セッション終了でのログ)の適用。割合値は、Log at Session End (セッション終了でのログ)が有効化されている状態でのルールの合計値に基づいています。BPAは無効化されたルールはカウントしません。

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に何があるの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。

次は:セキュリティを改良できる箇所を理解します。

適用におけるギャップを特定する

Heatmap (ヒートマップ) は、ユーザーのセキュリティポリシーがどの点で強いが、どこにセキュリティポリシー機能適用のギャップがあるか - したがって改善の努力をすべきかを示してくれます。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。

Heatmap (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、デバイスグループ、シリアル番号 & Vsys、ゾーン、アーキテクチャの領域およびタグごとにチェックすることができます。Column Filters (カラムフィルタ) を使い、デバイスグループ、デバイス、ゾーン、アーキテクチャの領域そしてタグでフィルタリングすることにより、範囲を狭めてギャップを特定することができます。

Security Policy Capability Adoption Heatmaps																			
Area of Architecture					Threat Prevention (IPS)					URL Filtering					Zone Protection Profile Adoption %				
Source Area of Architecture	Destination Area of Architecture	Total Rule Count	Allow Rule Count	Deny Rule Count	WildFire Adoption %	Anti-Spyware Adoption %	DNS Sinkhole Adoption %	Anti-Virus Adoption %	Vulnerability Protection Adoption %	URL Filtering Adoption %	Credential Theft Adoption %	File Blocking Adoption %	Data Filtering Adoption %	User ID Adoption %	App ID Adoption %	Service / Port Adoption %	Logging Adoption %	Log Forwarding Adoption %	Zone Protection Profile Adoption %
Internal Core	Datacenter	314	314	0	79.6	79.6	79.6	79.6	79.6	0.0	0.0	79.6	0.0	30.6	9.6	94.6	100.0	0.0	100.0
any	any	9	3	6	0.0	33.3	33.3	0.0	33.3	0.0	0.0	0.0	0.0	0.0	33.3	66.7	100.0	77.8	0.0
Remote Users/VPN, Internal Core	Internet	8	6	2	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0	100.0	100.0
Internet	DMZ	3	3	0	66.7	0.0	0.0	66.7	100.0	0.0	0.0	33.3	0.0	0.0	100.0	100.0	100.0	66.7	100.0
Out-of-Band Management, Users, Remote Office/MPLS, Internal Core	IT Infrastructure	3	3	0	66.7	100.0	100.0	66.7	100.0	0.0	0.0	66.7	0.0	0.0	100.0	100.0	100.0	66.7	100.0
DMZ	Datacenter	2	2	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0	0.0	0.0
DMZ	Internet	2	2	0	50.0	50.0	50.0	100.0	50.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0	100.0	0.0
Undefined	Undefined	2	2	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	50.0	100.0	100.0	100.0	0.0	50.0
Web-tier	App-tier	1	1	0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	0.0	0.0	100.0	100.0	100.0	0.0	0.0
App-tier	DB-tier	1	1	0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	0.0	0.0	100.0	100.0	100.0	0.0	0.0
Remote Users/VPN, Internal Core	DMZ	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0	100.0	100.0
Remote Office/MPLS	Internal Core	1	1	0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	0.0	0.0	0.0	0.0	100.0	0.0	0.0
Internal Core	Internet	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	0.0	0.0	100.0	100.0	0.0
Remote Office/MPLS	PCI	1	1	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	0.0	0.0
Internal Core	Remote Office/MPLS	1	1	0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	0.0	0.0	0.0	0.0	100.0	0.0	100.0
Grand Total:		350	341	9	78.0	78.0	78.0	78.3	78.9	2.1	2.1	77.4	0.0	30.6	16.0	94.1	100.0	6.6	96.5

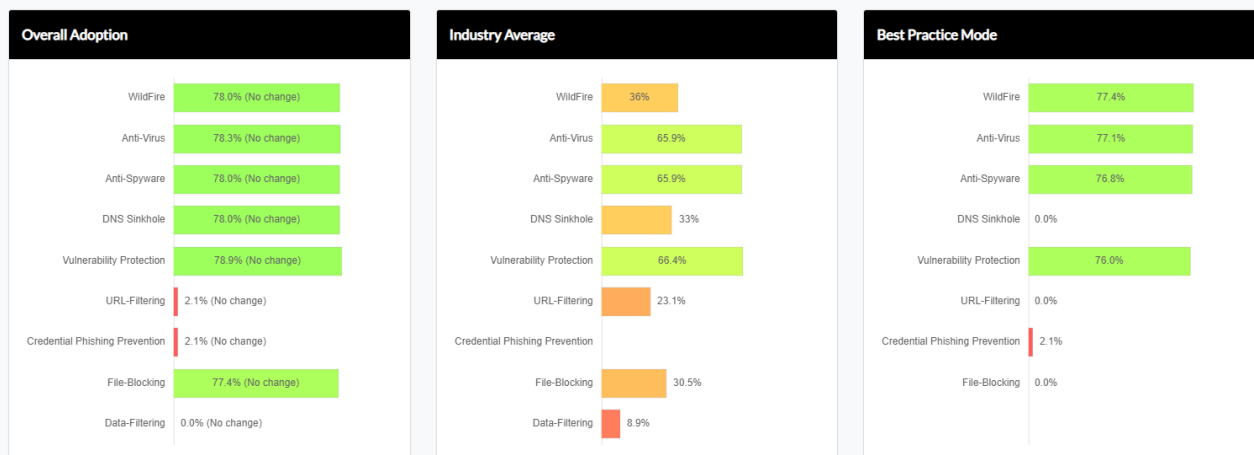
Showing 1 to 15 of 15 entries

Export Data

Previous 1 Next

ヒートマップのセキュリティプロファイル **Adoption Summary (適用サマリー)** で、次の機能の適用率をチェックし、推奨事項をギャップ特定の基準として使います。実際の適用率が推奨と合致しない場合は、ギャップを埋めるように計画します：

Security Profile Adoption Summary



- WildFire、アンチウイルス、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、すべての許可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。

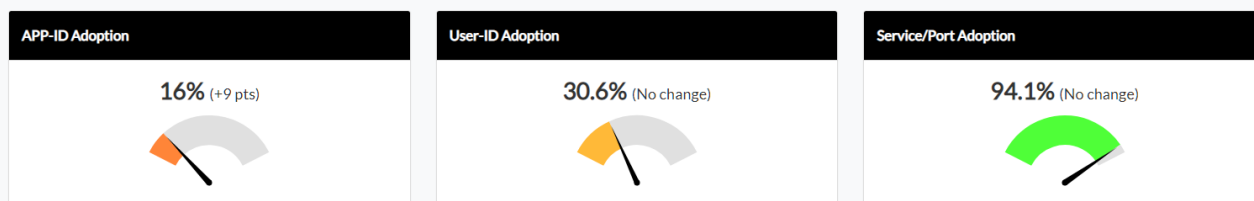
セキュリティプロファイルをすべての許可ルールについて設定することにより、ファイアウォールは、アプリケーションやサービス/ポートに関係なく、すべての復号化されたトラフィックについて脅威があるかないかを検査することができます。設定を更新した後は、BPAを実行して、進捗状況を測定し、セキュリティプロファイルがアタッチされていない新しいルールを見つけます。

 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。

Heatmap's Application & User Control (Heatmap アプリケーション & ユーザー制御) [Adoption Summary \(適用サマリー \)](#) において、次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用します。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：

Application & User Control Adoption Summary

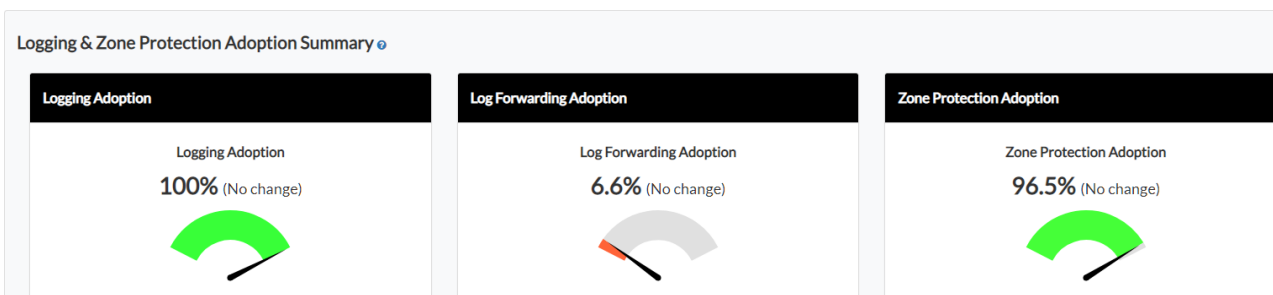


- App-IDを、できるだけ100%に近いルールに適用します。User-IDを、ユーザープレゼンスをもつ送信元ゾーンおよびアドレス範囲を有するすべてのルールに適用します (ユーザーソースのないゾーンもあります。例えば、データセンター・ゾーンは、サーバーではありますが、ユーザーではありません)

ん)。App-IDおよびUser-IDを活用して、適切なユーザーが認可（そして看過）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、ホワイトリスト（許可ルール）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。

Heatmap's Logging & Zone Protection (Heatmapのロギングとゾーン プロテクション) [Adoption Summary \(適用サマリー \)](#) 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用します。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
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
ロギング	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

範囲を狭めるには**Column Filters** (カラムフィルタ) を使います。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：

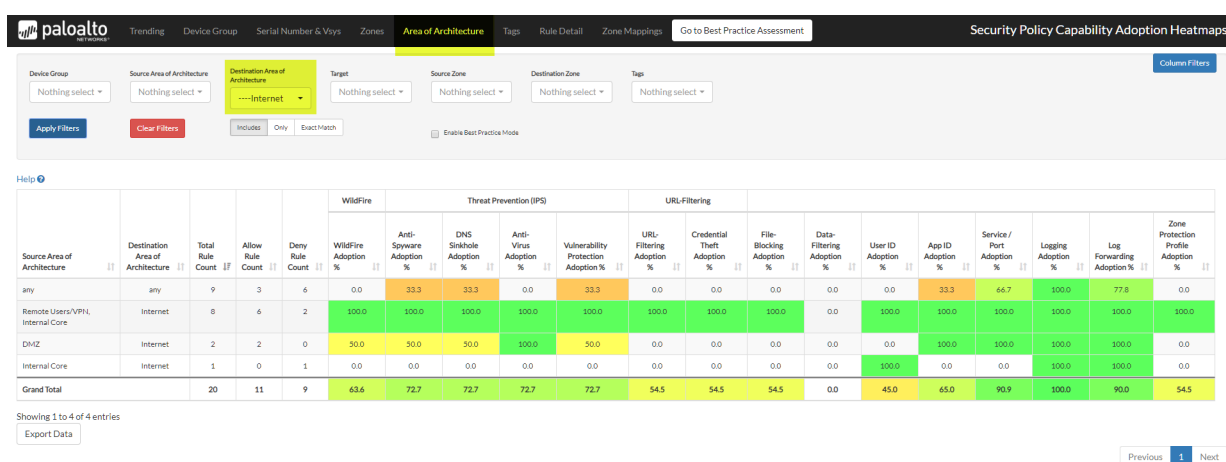
STEP 1 | BPAのHeatmapsセクションにおいて、**Areas of Architecture** (アーキテクチャの領域) をクリックします。

STEP 2 | **Column Filters** (カラムフィルタ) をクリックしてフィルタリングのオプションを拡張します。

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 Filter** (フィルタの適用) 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100%についてWildFireを適用することが目標であるとき、フィルタリングされたHeatmapが、DMZ許可ルールでWildFireプロファイルをもつものが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 | 次は: **改善すべきルールを識別**。

改善すべきルールを識別

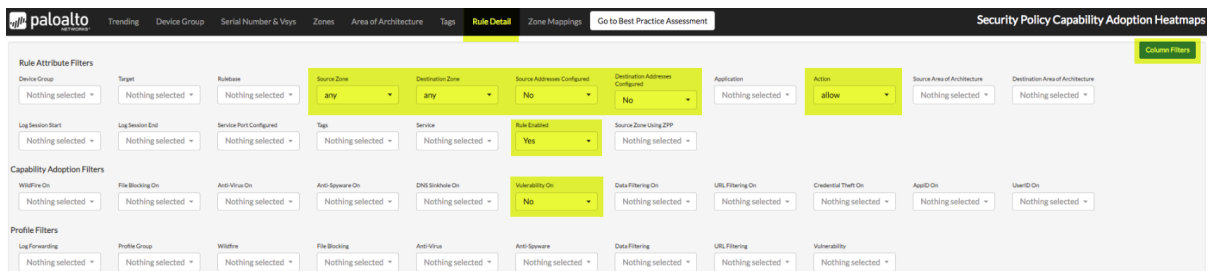
セキュリティポリシー適用におけるギャップを抽出した後、**Rule Detail**（ルール詳細）ビューを使って、さらなる調査や修正が必要なルールをリストアップします。**適用におけるギャップを特定した際に作成したギャップ抽出基準に合致するよう、Column Filters（カラムフィルタ）を設定します。**これにより、ファイアウォールセキュリティポリシー担当の運用チームにエクスポートし手渡すことができるルール・リストが作成されます。

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抽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 | BPAのHeatmapsセクションにおいて、**Rule Detail**（ルール詳細）をクリックします。

STEP 2 | **Column Filters**（カラムフィルタ）をクリックしてフィルタオプションを拡大し、次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：

paloalto Trending Device Group Serial Number & Vsys Zones Area of Architecture Tags **Rule Detail** Zone Mappings Go to Best Practice Assessment Security Policy Capability Adoption Heatmaps

Rule Attribute Filters

Device: Nothing selected Target: Nothing selected Rulebase: Nothing selected Source Zone: any Destination Zone: any Source Address Configured: No Destination Address Configured: No Application: Nothing selected Action: allow Source Area of Architecture: Nothing selected Destination Area of Architecture: Nothing selected

Log Session Start: Nothing selected Log Session End: Nothing selected Service Port Configured: Nothing selected Tag: Nothing selected Service: Nothing selected Rule Enabled: Yes Source Zone Using DDP: Nothing selected

Capability Adoption Filters

Wildfire On: Nothing selected File Blocking On: Nothing selected Anti-Virus On: Nothing selected Anti-Spyware On: Nothing selected DNS Sinkhole On: Nothing selected Vulnerability On: No Data Filtering On: Nothing selected URL Filtering On: Nothing selected Credential Theft On: Nothing selected AppID On: Nothing selected UserID On: Nothing selected

Profile Filters

Log Forwarding: Nothing selected Profile Group: Nothing selected Wildfire: Nothing selected File Blocking: Nothing selected Anti-Virus: Nothing selected Anti-Spyware: Nothing selected Data Filtering: Nothing selected URL Filtering: Nothing selected Vulnerability: Nothing selected

Apply Filters **Clear Filters**

Search:

Device Group	Target	Source Area Of Architecture	Dest Area Of Architecture	RuleName	Tags	Service	Rulebase	Source Zone	Source User	Dest Zone	Source Addresses	Dest Addresses	Application	Action	Rule Enabled	Wildfire Enabled	File Blocking Enabled
Branch Offices	0153000222:no-vsys, 0153000223:no-vsys, 0153000224:no-vsys, 0153000225:no-vsys, 0153000226:no-vsys, 0153000227:no-vsys	any	any	Panorama Allow All	NO_TAG	application-default	post-rulebase	any	any	any	no	no	any	allow	yes	no	no
shared	00720000998:no-vsys, 007200001591:no-vsys, 007200001592:no-vsys, 007200001593:no-vsys, 007200001594:no-vsys, 007201000397:no-vsys, 01530000222:no-vsys, 01530000223:no-vsys, 01530000224:no-vsys	any	any	Intrazone-default	NO_TAG	any	post-rulebase	any	any	any	no	no	any	allow	yes	no	no

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。

paloalto Trending Device Group Serial Number & Vsys Zones Area of Architecture Tags **Rule Detail** Zone Mappings Go to Best Practice Assessment Security Policy Capability Adoption Heatmaps

Search:

RuleName	Tags	Service	Rulebase	Source Zone	Source User	Dest Zone	Source Addresses	Dest Addresses	Application	Action	Rule Enabled	Wildfire Enabled	File Blocking Enabled	Antivirus Enabled	Antispyware Enabled	Dns Sinkhole Enabled	Vulnerability Enabled
Panorama Allow All	NO_TAG	application-default	post-rulebase	any	any	any	no	no	any	allow	yes	no	no	no	no	no	no
Intrazone-default	NO_TAG	any	post-rulebase	any	any	any	no	no	any	allow	yes	no	no	no	no	no	no

Showing 1 to 2 of 2 entries

Export Data

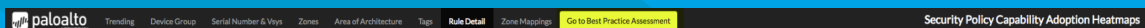
Previous **1** Next

STEP 5 | 次は: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。Introduction to the BPA (BPAの紹介) ビデオを閲覧してBPAの概要を学び、BPA video library (BPAビデオライブラリー) を活用してこのツールの詳細を学習しましょう。

BPAレポートを開くと、最初にHeatmapセクションが表示されます。**Go to Best Practice Assessment** (ベストプラクティスアセスメントに移動) をクリックしてレポートのBPAセクションに移動します。このセクションでは、次世代のファイアウォールおよびPanoramaに関する設定のベストプラクティスの導入について解説しています。



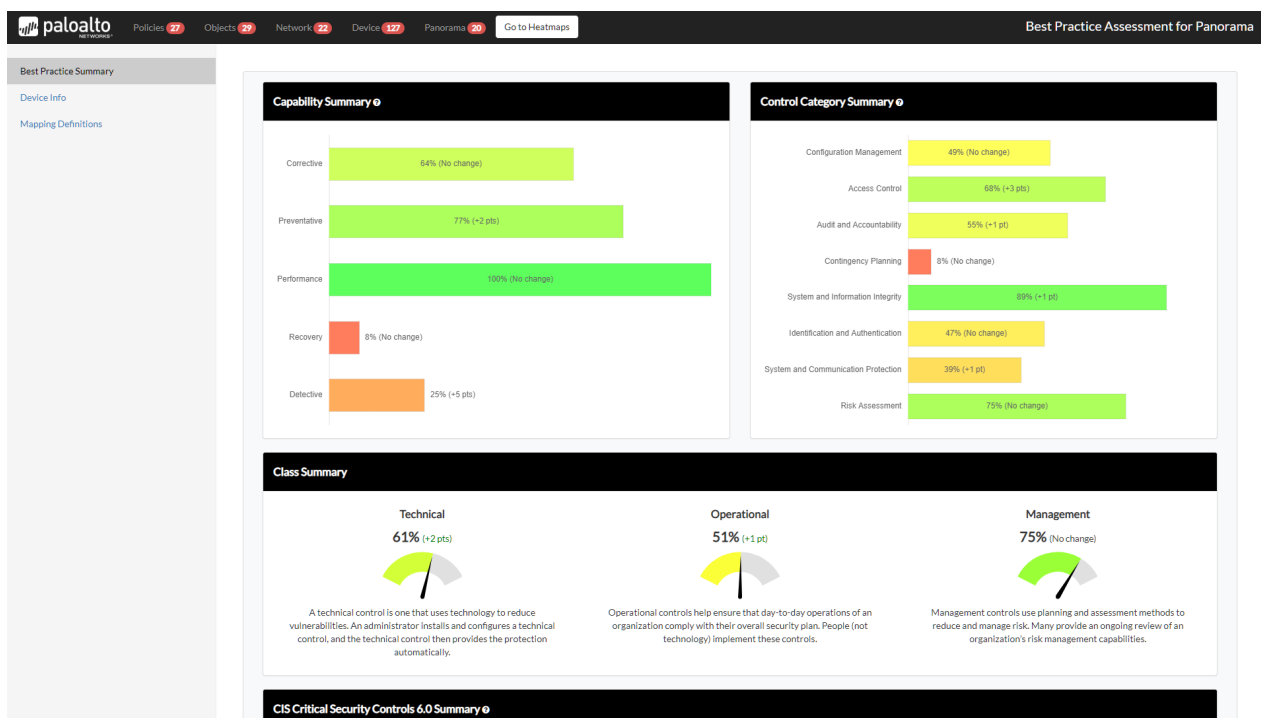
この文書の他に、BPA demo (BPAデモ) およびhow to run a BPA (BPAの実行のしかた) の短いビデオを閲覧してBPAの使い方をより詳しく知ることができます。

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。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

ビューをヒートマップからBPAレポートに変更すると、レポートはベストプラクティスサマリーを示します。



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。

Best Practice Summary

Device Info

Mapping Definitions

Show Filters

Top Nav

Left Nav

Capability

Class

Control Category

CSC Controls

Nothing selected

Nothing selected

Nothing selected

Nothing selected

Nothing selected

Nothing selected

Apply Filters

Clear Filters

Show 10 entries

ID	Best Practice Check Name	Top Nav	Left Nav	Capability	Class	Control Category	CSC Controls	Passing %
3	Description Populated	Policies	Security	Corrective	Operational	Configuration Management		0
4	Source/Destination = any/any	Policies	Security	Preventative, Corrective	Technical	Access Control		
5	Service != any	Policies	Security	Preventative, Corrective	Technical	Audit and Accountability		
6	Log at Start of Session	Policies	Security	Performance	Technical	Contingency Planning		
7	Log Forwarding	Policies	Security	Recovery, Detective	Operational, Technical	System and Information Integrity		
8	Expired Non-Recurring Schedules	Policies	Security	Preventative	Operational	Identification and Authentication		
9	Disable Server Response Inspection	Policies	Security	Preventative	Operational	System and Communication Protection		
11	Disabled Rules	Policies	Security	Preventative	Operational	Risk Assessment		
12	Interzone Deny Rule with Logging	Policies	Security	Preventative, Detective	Technical	Contingency Planning, Audit and Accountability	6.2, 6.6, 10.1	6.8
13	Intrazone Allow Rules with Logging	Policies	Security	Preventative, Detective	Technical	Configuration Management	N/A	100
Total:								62.8

Showing 1 to 10 of 202 entries

Export Mappings

Previous12345...21Next

次は: ベストプラクティスパ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

Policies (ポリシー) タブはファイアウォールポリシーの様々なタイプに関連するすべてのチェックを示しています。潜在的なルール改善内容を識別するため、レビューしたいポリシーのタイプを選択します。**Security** (セキュリティ) ポリシービューはルールベースのチェック結果 (**Security Rule Checks** (セキュリティルールチェック)) を表示します。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、**Show Filters** (フィルタを表示) 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。

個々のチェックの説明と論拠および個々のチェックが検証する能力に関する技術文書を閲覧するため、

help (ヘルプ) (?) をクリックします。

Rule Name	Rule Enabled	Description Populated	Source/Destination != any/any	Service != any	Application != any	APP-ID with Service	Not Logging at Start of Session	Log Forwarding	Expired Non-Recurring Schedules	Disable Server Response Inspection
all-default-profiles	true	✗	✗	✓	✗	✗	✓	✗	✓	✓
Allow-Dev-Users	true	✗	✓	✓	✗	✗	✗	✗	✓	✓
Block-apps	true	✗	✓	✓	✗	✗	✓	✗	✓	✓
Block-Apps	false	✗	✓	✓	✗	✓	✓	✗	✓	✓
Block-Qik	true	✗	✓	✓	✗	✗	✓	✗	✓	✓
Block-Region	true	✗	✓	✓	✗	✗	✗	✓	✗	✓
Block-region	true	✗	✓	✓	✗	✗	✓	✗	✓	✓
Byod-users	true	✗	✓	✓	✗	✗	✗	✓	✓	✓
Commerce-E	true	✗	✓	✓	✓	✓	✓	✗	✓	✗
dummy-deny	true	✗	✓	✓	✗	✗	✓	✗	✓	✓
E-comm	true	✗	✓	✓	✗	✗	✓	✗	✓	✓
Guest-traffic	true	✗	✓	✓	✗	✗	✓	✗	✓	✓
High-risk IPS	true	✗	✓	✓	✗	✗	✓	✗	✓	✓
Hip-check	true	✗	✓	✓	✗	✗	✓	✗	✓	✓
Interzone-default	true	✗	✗	✗	✗	✗	✓	✗	✗	✗
N rule	true	✗	✓	✓	✗	✗	✓	✗	✓	✓
Network	true	✗	✗	✓	✓	✓	✓	✗	✓	✓
Networking	true	✗	✓	✓	✓	✓	✓	✗	✓	✗

Summary: Passing % 0% 73.3% 93.3% 33.3% 84.6% 87% 9.6% 96.6% 90%

Security Rule Checks (セキュリティルールチェック) の下で、**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を要約します。個々の結果の説明と論拠および技術文書へのリンクを閲覧するために **help** (ヘルプ) をクリックします。

Security Rulebase vsys: vsys1

Best Practice Check Results

- ✗ Disabled Rules (Fail): 1 disabled rules exist
- ✓ Interzone Deny Rule with Logging (Pass)
- ✗ Intrazone Allow Rules with Logging (Fail): It is recommended to override the intrazone-default rule with Action set to 'allow', Log at Session End enabled, and IPS capability enabled.
- ✓ HIP Profiles used in Rules (Pass)
- ✓ User ID Rules without User ID enabled on Zone (Pass)

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：

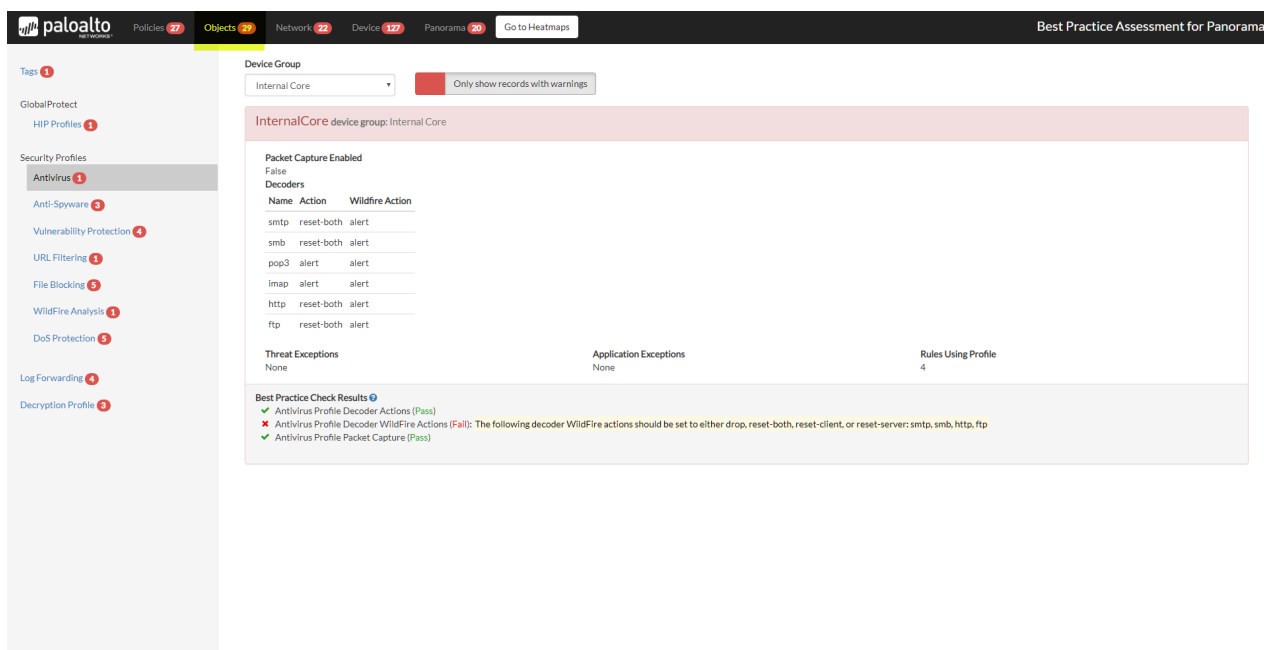
- ❑ **Security** (セキュリティ) –Source/Destination !=any/any チェックで不合格になったルールを識別します。
- ❑ **Security** (セキュリティ) –App-ID with Service (サービス付App-ID) チェックで不合格になったルールを識別します。
- ❑ **Security** (セキュリティ) –User-ID Rules without User ID enabled on Zone (ゾーンで有効化されていないユーザーIDルール) チェックで不合格になったユーザーIDルールを識別します。
- ❑ **Decryption 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。

-
- **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す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。単純なカスタムアプリケーションで使用するアプリケーション上書きを減らすあるいは除去すると、**トラフィックの可視性を改善する** でき、これらのルールが制御するアプリケーションと内容を検査することができます。

次は: **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

Objects (オブジェクト) タブはファイアウォールオブジェクトの様々なタイプに関連するすべてのチェックを示しています。既存の設定を理解し、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潜在的ギャップを識別するために、レビューしたいオブジェクトのタイプを選択します。下記の例は、アンチウイルスセキュリティプロファイルの結果を示しています。



個々のプロファイルに関しては、レポートは現在の設定を示し、いくつか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。

Objects (オブジェクト) タブをレビューする時は、修復の潜在的 content 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 (アンチウイルス)** –アンチウイルスと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)** –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)。

次は: [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

Network (ネットワーク) タブはネットワーク関連の設定のチェックをすべて示します。左のナビで、既存設定を理解するため、そしてゾーン、GlobalProtect、IPsec 暗号(Crypt)、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で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。

The screenshot displays the Palo Alto Networks Best Practice Assessment for Panorama interface. The top navigation bar shows 'Policies 27', 'Objects 29', 'Network 25', 'Device 127', and 'Panorama 20'. The left sidebar lists 'Zones 19', 'GlobalProtect', 'Portals', 'Gateways', 'Network Profiles', 'IPsec Crypto', and 'Zone Protection 5'. The main content area shows the 'Internet device group: vsys1 template: Perimeter' configuration. It lists 'User Id Enabled' (True), 'Using Acl Include List' (False), and 'Zone Protection Profile' (zpp-hq-Internet). Below this, the 'Best Practice Check Results' section shows three checks: 'Enable Packet Buffer Protection (Pass)', 'ACL Include List for User ID (Fail): When User ID is enabled, you should also be using an ACL Include List', and 'Zone Protection Profile Applied to Zone (Pass)'. The 'LAN device group: vsys1 template: Perimeter' section shows 'User Id Enabled' (True), 'Using Acl Include List' (False), and 'Zone Protection Profile' (None). The 'GlobalProtect device group: vsys1 template: Perimeter' section shows 'User Id Enabled' (True), 'Using Acl Include List' (False), and 'Zone Protection Profile' (None).

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。

次は: [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

Device (デバイス) および **Panorama** タブはデバイス管理設定に関連する全てのチェック項目を示します。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レビューしたいデバイス管理チェックを選択します。下記の例はファイアウォールの一般設定の結果を示しています (**Panorama** をクリックしてPanoramaチェック結果を見ます)。

The screenshot shows the Palo Alto Networks management console. The top navigation bar includes tabs for Policies (27), Objects (29), Network (22), Device (127), and Panorama (20). The 'Device' tab is selected. On the left, a sidebar lists various configuration areas like Setup - Management, Authentication Settings, Logging and Reporting Settings, etc. The main content area displays 'Best Practice Assessment for Panorama' results. It shows three templates: Perimeter, Internal Core, and Datacenter. Each template has a table of settings (Login Banner Enabled, Auto Acquire Commit Lock Enabled, Set Tls Service Profile, Hostname, Cert Expiration Check Enabled) and a 'Best Practice Check Results' section with red X marks indicating failures. For example, 'Automatically Acquire Commit Lock (Fail): It is recommended to enable "Automatically Acquire Commit Lock"' is listed as a failure for all templates.

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。クエスチョンマークをクリックして、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)** – アンチウイルス、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。

次は: [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。

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。

- デバイス管理インターフェースを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から守るための[運営アクセスを保護するためのベストプラクティス](#)に従います。
- 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。

次は:[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](#)して[適用におけるギャップを抽出](#)した後は、[安全な移行ステップ](#)を使ってギャップを救済し、[ベストプラクティスセキュリティプロファイル](#)のフル実装に向けて進みます。
- ❑ ログिंग ([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険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、ユーザー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。

次は: **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して適用におけるギャップを特定した後は、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 プロファイルに向かって進みます。これには、最も貴重なビジネス資産を保護すべくデータセンター内に厳格な統制制御を導入することが含まれます。
- データセンターおよび界（それを取り巻く）フ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。

次は: 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。
- [GlobalProtect](#)または[GlobalProtect Cloud Service \(クラウドサービス\)](#)を導入し、あらゆる場所のユーザーやデバイスに次世代セキュリティ プラットフォームを拡張します。
- [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。