パロアルトネットワークス製品でゼロトラストを実装するベストプラクティス

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

December 18, 2019

Table of Contents

ゼロトラストのベストプラクティス

このドキュメントは、ゼロトラスト戦略とはどのようなものなのか、重要な保護サーフェスの識別、重要なトランザクションフローの対応付け、ゼロトラストネットワークの設計、ゼロトラストポリシーの作成、およびデプロイ環境のメンテナンスのベストプラクティスを案内する、5ステップの方法論を使ったネットワークに導入する方法について説明しています。各セクションには、次世代ファイアウォールの設定方法（物理型および仮想型）、およびPalo Alto Networksが提供する、データの漏洩を防止するためのセキュリティ機能を含めた、Palo Alto Networksからの詳細な情報へのリンクが含まれています。

- ゼロトラストとは何で、なぜ必要なのですか？
- ゼロトラストの観点
- 5ステップの方法論
- ゼロトラストリソース

ゼロトラストとは何で、なぜ必要なのですか？

ゼロトラストは、保護サーフェス内の重要なデータ、アプリケーション、アセット、およびサービス（DAAS）だけでなく、特定のビジネスにとって何が重要かに基づいてユーザーも保護する、ビジネス駆動型の戦略的なアプローチです。ゼロトラスト戦略はインフラに依存しないため、ネットワーク、パブリッククラウド、プライベートクラウド、およびエンドポイントなど、すべての物理/仮想環境に適用することができます。ゼロトラストの背景にあるコンセプトは単純で、「信頼することが脆弱性になる」です。パケット、ID、デバイス、またはサービスなど、デジタル環境内の何も信頼せずに、すべての検証を行います。デフォルトで信頼する項目は何もありません。

この戦略の導入は1回だけ実行するものではなく、ネットワークから抜き出した型通りのコピーを利用するものでもありません。各環境および保護サーフェスは異なっており、時間の経過に伴い最終目標やDAASの要素も変化します。戦略はビジネス固有であり、セキュリティ戦略は自社のビジネスにとって重要なものを保護することを目的にしています。

ゼロトラスト戦略の目標は、ネットワークから信頼を排除することにあります。信頼を排除することで、データ違反を防止し、自動化とルールベースの削減により運用、および規制へのコンプライアンスと監査を簡素化することができます（ゼロトラスト環境は、コンプライアンスと監査の簡素化を目的に設計されているため）。

ゼロトラストの観点

ゼロトラストを理解すると、信頼とは”攻撃者が不正利用できる脆弱性”であることが分かります。攻撃者は、認証情報を盗用する、パッケージヘッダー内の情報を偽装する、また「信頼されている」従業員やパートナーになりすますことさえ可能です。エドワードスノーデンは、自分のワークステーションに適切なウィルス対策ソフトウェアと適切なレベルのパッチを適用した、信頼されるユーザーでした。彼は多要素認証も使用していました。しかし、彼は信頼されているユーザーであるために、ネットワークのどこに移動して、そしてどのようなパケットを生成したのかについても、誰も気にしていませんでした。そのため、彼はネットワークを探索して、機密データを抜き出すことができたのです。それから得られる教訓は、デジタル的な信頼は、デジタル的な裏切りでもあると言うことです。ID、アプリケーション、またはデータを信頼しないようにしてください。ゼロトラストの観点から見ると:

- ビジネス機能が保護する必要のあるものを決定するため、セキュリティをビジネス機能に合わせてください。
- リソースへのアクセス時には、すべてのレイヤー7パケットを検査して、ログに記録してください。
- ロケーションに関係なく、すべてのリソースに安全な方法でアクセスしてください。
- すべてのロケーションで、整合性のあるセキュリティポリシーを適用してください。
- セキュリティおよびセグメント化ポリシーを一元管理してください。
- ビジネスの変化に合わせて、それに対応するようにしてください。

信頼は、ゼロトラスト戦略を採用することで回避することが可能な失敗点です。

- ゼロトラストの高レベルなベストプラクティス
- ゼロトラスト導入の開始方法は？

ゼロトラストの高レベルなベストプラクティス

次のベストプラクティスは、ネットワークをゼロトラストアーキテクチャに移行する準備を行うために役立ちます。

- ゼロトラスト環境を設計する前に、目的のビジネス成果を定義してください。ゼロトラストモデルは、ビジネス部門の保護と支援を行います。
- 外部から内部ではなく、内部から外部に向けて設計することで、まずビジネスでもっとも価値があるものを保護します。もっとも貴重な資産は、境界ではなくデータセンター内に存在している可能性が高くなっています。
- 連係動作が苦手な単一の製品を寄せ集めるのではなく、トータルコストを削減できる統合、一元管理されたプラットフォームを使用してください。Palo Alto Networksは各プラットフォームエレメントの情報を共有し、Panorama、GlobalProtect、およびPrisma Accessを使った一元管理と簡単な運用を実現し、整合性のあるポリシー、およびすべてのロケーションにおける防止、保護手段を提供しています。
- Palo Alto Networksの次世代ファイアウォールをセグメンテーションゲートウェイとして使用して、セキュリティ技術を1つのプラットフォームに統一し、またApp-ID、User-ID、およびContent-IDを使ってレイヤー7でのすべてのロケーションでネイティブに、整合性のあるセキュリティポリシーを適用してください。セグメンテーションゲートウェイは、アプリケーション、ユーザー、およびデータに基づいてネットワークをセグメント化、制御することで、きめ細かなアクセス制御手段を提供し、マイクロペリメータを通過するすべてのトラフィックを保護し、保護サーフェスへのアクセスを実現しています。

  権限のあるユーザーに、ビジネス上の目的でアクセスする必要がある保護サーフェスに対してのみアクセスを許可することで、レイヤー7ポリシー内にマイクロペリメータを作成するため、そのためにインフラを変更する必要はありません。
- ビジネス上価値があるものに基づいてネットワークをセグメント化することで、不正な横方向の動き回りを防止します。

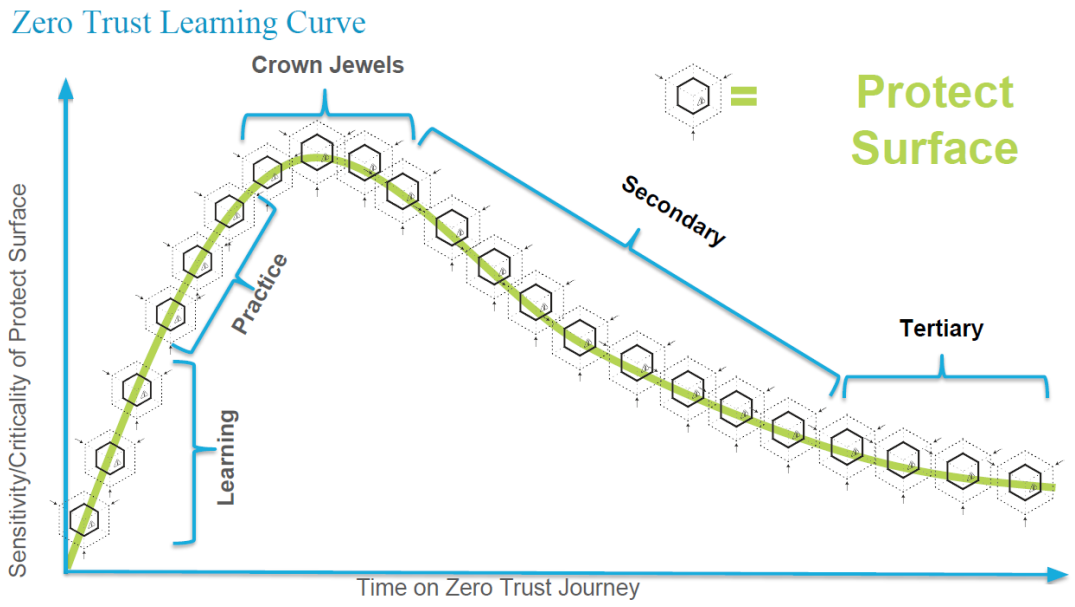
- 保護サーフェスに、最小権限アクセスの原則を適用します。誰がどのリソースにアクセスする必要があるのか、どのような方法でいつアクセスするのかを判断します。各ユーザーおよびデバイスに必要なレベルのアクセスのみを許可し、IDを主張して（適切な権限を含む）、次にIDをレイヤー7ポリシーにマップします。
- 規制、コンプライアンス、およびビジネス事例が検査を許している範囲内で、レイヤー7経由の各パケットを復号化、検索、およびログに記録します。レイヤー7トラフィックを検査して、ログに記録する必要があります。攻撃者は、レイヤー3およびレイヤー4のセキュリティコントロールをくぐり抜ける方法を熟知していることを忘れないようにしてください。
- セキュリティポリシーを自動化するために、ワークロードグループオブジェクトにタグを設定して、タグを動的に登録する戦略を作成します。
- 運用、管理を行うためのプロセスを開発し、戦略を開発してネットワークを設計するにつれて、継続的に予防コントロールを更新します。プロセスを文書化して、各個人の教育とトレーニングを行い、ベースラインを設定し、ベースラインに対する進捗状況を評価します。
- ゼロトラスト環境への移行は、経験を得るために1つまたは複数の重要ではないセグメントから始めて、段階的に行います。ゼロトラストセグメントは従来のセグメントと共存するため、リスクの高い総入れ替えのアプローチを使用せずに、安全で反復的なアプローチを使用することができます。

アプリケーションの重要性が低くなった場合、保護のレベルを緩和することができます。たとえば、チャットアプリケーションに対して、ビジネス上重要なアプリケーションと同じ保護手段を適用する必要はありません。ビジネスリーダーと協力して、もっとも重要で保護する必要があるアプリケーションを判断してください。

ゼロトラスト導入の開始方法は？

教育とコラボレーションが、ゼロトラストセキュリティへの出発地点になります。あなたと、ビジネスの脆弱性、およびそれを保護する方法を判断するその他の利害関係者が、ゼロトラストの概念、原理、および最終目標を理解する必要があります。

1. 優位を保つためにゼロトラストセンターを作成してください。これはビジネスリーダー（ビジネス上および技術上の意思決定者）、IT、情報セキュリティ、インフラ、アプリケーション開発、およびその他の利害関係者による、各部門にまたがったチームです。このチームが保護サーフェス、および保護サーフェスを構成するデータ、アプリケーション、資産、およびサービス（DAAS工レメント）を定義、判断します。ビジネスにとってもっとも貴重な保護サーフェスを優先して、ゼロトラスト戦略を策定、導入します。このチームはビジネスの変化に伴う維持管理と展開にも関与し続けます。ビジネスリーダーが目的のビジネス結果、コンプライアンス要件、およびビジネス資産の価値について言及することもあります。
2. ゼロトラストワークショップに参加して、各自の準備を行い、各自が同じ立場になるようにしてください。詳しくは、Palo Alto Networksの営業担当に連絡して、情報の収集とワークショップのスケジュール確認を行ってください。
3. 構築したいセグメント化されたネットワークをマップします。
4. 1つまたは複数の小規模で、熟知しており、リスクが低い（ビジネス運営にとって重要ではない）セグメントから移行を開始して、経験を積み重ねてください。重要な資産から開始しないようにしてください。次に、経験から学習したことを活かして、別の練習用セグメントでテスト的な作業を行います。十分に経験を積んで準備が完了したら、ビジネス上もっとも重要な保護サーフェス（保護サーフェスを構成するDAAS工レメント）をゼロトラストマイクロペリメータに配置します。保護サーフェスあたり1つのマイクロペリメータを使用します。その後、次に貴重な一連の保護サーフェスをゼロトラストに変換していきます。



5ステップの方法論

ゼロトラスト戦略を導入するための、5ステップの方法論は、環境、データ、アプリケーション、資産、サービス、およびユーザーを保護するための明確な道筋を指し示しています。方法論を適用する方法は、何を保護するのか、そしてビジネス要件がどうなっているのか（ビジネスにとって何が重要か）によって異なりますが、目標としている成果は一緒です。

- 横方向の動き回りを防止するために、効果的および効率的にネットワークをセグメント化する。
- 不正なアプリケーションやユーザーから、ビジネス上重要なデータやシステムを保護する。
- ビジネス上重要なアプリケーションを、不正アクセスや不正利用から保護する。
- ネットワーク、クラウド、およびエンドポイントにまたがって透過的にポリシーを適用し、管理を簡素化し、どこでも整合性のあるポリシーを適用する。

5ステップの方法論は、クラウド、プライベートネットワーク、またはエンドポイントにゼロトラスト戦略を導入する場合でも、インフラにかかわらず利用できます。

ステップ1:保護サーフェスの定義

保護サーフェスとは、正常なビジネス運用を行うために保護する必要がある、ビジネスにとって貴重なデータ、アプリケーション、資産、およびサービス（DAAS）です。保護サーフェスを定義することで、攻撃面全体を識別、保護したり、境界のみを保護するのではなく、本当にビジネスにとって必要な項目の防御に集中することができます。保護サーフェスは、攻撃面や境界よりも大幅に小さいため、保護することも簡単になります。

ビジネスにとってもっとも重要なDAASエレメントに基づいて、保護サーフェスを定義してください。

- データ:どのようなデータを保護する必要がありますか？独自のコードやプロセス、個人を特定できる情報（PII）、決済カード情報（PCI）、および医療保険の携行性と責任に関する法律（HIPAA）情報などの個人の健康情報（PHI）などの、知的財産について考えてみてください。
- アプリケーション:機密情報を使用しているアプリケーションはどれですか？どのアプリケーションがビジネス業務にとって重要ですか？
- 資産:機密性の高い資産はどれですか？ビジネスによって、これはSCADAコントロール、POS端末、医療機器、製造機器、および重要なサーバーのグループなどになります。
- サービス:攻撃者が悪用して、IT運用を混乱させ、ビジネスに悪影響を与えるサービスは何でしょうか？たとえば、DNS、DHCP、Active Directoryなどが考えられます。

それぞれの重要なDAASが保護サーフェスの一部となっています（それ自体が保護サーフェスとなっていることもあります）。たとえば、ヘルスケアを提供しているビジネスの場合、個人の健康情報（PHI）がビジネスにとって重要になります。その場合データは患者の情報になります。アプリケーションは、EPICなどの、PHIデータへのアクセスに使用されるアプリケーションになります。アセットは、データを保管しているサーバー、および医療用スキャナや医師のワークステーションなどの、PHIを生成する設備になります。サービスは、シングルサインオンやActive Directoryなどの、データにアクセスするために用いられるサービスです。

5ステップの方法論に従って作業を行うにつれて、各保護サーフェスを独自のマイクロペリメータ（セグメンテーションゲートウェイとして動作する、Palo Alto Networksの物理型/仮想型次世代ファイアウォールがセグメント化する）に配置し、誰がエレメントにアクセスできるのか、どのようにアクセスできるのか、いつアクセスできるのかを制御できるようにします。各保護サーフェスは、その保護サーフェスに適

した手段で保護してください。マイクロペリメータは、異なるアクセス要件を持つユーザーが必要としているDAAS工レメントを包含する幅広い境界に比べて、管理や防御が簡単です。また、重要なデータの近くで保護を行うことができます。

ビジネス経営に重要な項目に基づいて、優先して保護する項目を決定していきます。もっとも貴重な資産は、しばしばデータセンターやクラウド内に存在しています。1つまたは複数の重要ではない保護サーフェスにゼロトラストを導入して経験を積んだ後に、もっとも重要な保護サーフェスを防御してください。作業開始時にはデータセンター内のアプリケーションの一部しか分からないこともありますが、もっとも重要なアプリケーションは理解してください。その後、優先度リストの次の保護サーフェスセットで作業を行い、リストの最終目標に到達するまでその作業を繰り返します。

ネットワークのトラフィックを把握して、重要な保護サーフェスを構成するDAAS工レメントを識別するために、次のツールを使用してください。

- チームのビジネスに関する知識。たとえば、ビジネスリーダーは、アプリケーションの戦略的価値について言及することができます。
- トラフィックの可視性を高めるために、1つまたは複数の次世代ファイアウォールを、バーチャルワイヤ（vwire）モードで透過的にネットワークに挿入してください。vwireインターフェイスには、IPまたはMACアドレスがないため、トポロジの変更が不要なパススルーモードになっています。ネットワークトラフィックを表示、解析するには、トラフィックログを確認してください。すでにネットワークに管理対象ファイアウォールが存在している場合は、Panoramaのログを使用してください。
- Cortex Data Lakeでログを参照し、Palo Alto Networksの統合パートナーのいずれかから、Cortexと連係するサードパーティアセット検出ツールを使用してください。
- Prisma SaaSを使用して、SaaSアプリケーションのユーザー、資産、データを発見して、それらのアプリケーションの可視性を実現してください。
- 次世代ファイアウォールまたはファイアウォールを管理しているPanorama上で、PAN-OS 9.0以降を動作させている場合は、Policy Optimizerを使って既存のセキュリティポリシールールにある主要なアプリケーションを識別してください。（Policy Optimizerでは、ポートベースのルールにあるアプリケーションも確認できます。）Policy Optimizerを利用できない場合は、Expeditionを使ってアプリケーションを把握してください。
- Application Dependency Mappingツールを利用して、アプリケーションの依存関係（データベース、ロードバランサー、サーバーなどの、アプリケーションが使用するリソース）を自動検出することができます。

ステップ 2:保護サーフェスとトランザクションフローを紐づける

重要なDAAS工レメントとユーザー間のトランザクションフロー（やり取り）を対応付けて、その依存関係を理解します（誰がビジネス上の理由で各工レメントにアクセスするのか、アクセス方法、およびアクセス時刻など）。トランザクションフローを対応付けて、ネットワークを理解、設計していきます。対応付けにより、指定されたアプリケーションを使って特定のデータや資産に、権限のあるユーザーのみアクセスを許可するセキュリティポリシーの作成方法を理解できます（最小権限の原則）。

トランザクションフローを対応付けるさまざまな方法が存在しており、保護サーフェスを定義するためのテクニックの一部は、トランザクションフローの対応付けにも利用できます。

- 既存のフローダイアグラムがある場合はそれを活用してください（ビジネスによっては、コンプライアンスおよび監査目的で、フローダイアグラムの作成が必要な場合があります）。
- アプリケーション、ネットワーク、およびエンタープライズ設計者、およびビジネスの責任者と協力して、彼らが思い描いているアプリケーションとトランザクションフローの目的を理解してください。
- トラフィックの可視性を確保するために、1つまたは複数の次世代ファイアウォールを、バーチャルワイヤ（vwire）モードでネットワーク内に透過的に挿入します。トラフィックを表示、解析するには、トラフィックログを確認してください。
- Palo Alto Networksの統合パートナーが提供するサードパーティツールを使用してください。

- 可視性を確保し、トランザクションフローを対応付けるために、Cortex Data Lakeのログ情報を使用してください。Cortex Data Lakeは次世代ファイアウォール、VM-Seriesファイアウォール、Prisma Access、およびXDR Agentからのログを集計しています。
- アプリケーションの場合、ネットワーク内のアプリケーションデータフロー、各アプリケーションが必要とするコンピューティングオブジェクト、および各アプリケーションを使用するユーザーも含めて、ワークフローを対応付けてください。
- データの場合、誰がデータを使用するのか、どこにデータを収集、保管、使用、および転送するのか、どのようにデータを保管するのか（暗号化、アーカイブ、または使用後に破棄）などを確認してください。
- 資産の場合、資産の場所、資産を使用するユーザー、ユーザーが資産を使用する時間帯、および資産がワークフロー内のどこに該当するのかを確認してください。
- サービスの場合、環境内のサービスワークフローを対応付けてください。

誰がいつ、どこでどのようにして、どんなアプリケーションを使用するのかを確認するだけでなく、トランザクションフローを対応付けることで、細部にわたる可視性を確保でき、災害対策の計画策定やコンプライアンスに役立てることができます。また、ワークフローを最適化する機会も得られ、それぞれの保護サーフェスで、誰が正規の理由でDAASエレメントにアクセスしているのかを調査することができます。

ネットワーク内のトランザクションフローを理解すると、誰がそれぞれの保護サーフェスを使用するのか、その使用方法、その場所、および重要な各アプリケーションとやり取りするエレメントなどを確認できるので、ネットワークのセグメント化方法、およびどこに制御手段を挿入するのかを理解することができます。

ステップ3:ゼロトラストネットワークの設計

保護サーフェスとトランザクションフローを理解したことを活かし、ビジネスに貴重な項目をベースにして、ゼロトラストネットワークの設計を開始してください。確認したビジネス上重要な保護サーフェスを、内部から外部に向けて設計していきます。アーキテクチャを開発する際には、運用とメンテナンスの容易さ、および保護サーフェスやビジネスの変化に対応できる柔軟性を念頭に置いてください。ベストプラクティスアセスメントツールを実行して、ベストプラクティス設定のベースラインを設定し、ゼロトラストの最終目標までの進捗状況を判断してください。

アーキテクチャの基盤となるのがセグメンテーションゲートウェイです。ネットワークセグメントに接続するPalo Alto Networksの物理型または仮想型次世代ファイアウォールは、レイヤー7ポリシーを採用しています。すべてのトラフィックがセグメンテーションゲートウェイを通過するようにしてください。セグメンテーションゲートウェイは、保護対象リソースにできる限り近い場所に配置して、その他のPalo Alto Networks機能と連携させて、できる限り自動化するようにしてください。次世代ファイアウォール

- 各保護サーフェスのレイヤー7ポリシーにマイクロペリメータを作成します。マイクロペリメータは、誰が（User-ID）どのアプリケーションに（App-ID）、どのような方法（Content-ID）でいつアクセスするのかを、セグメンテーションゲートウェイ経由できめ細かく制御するポリシーを提供しているため、横方向の動き回りを防止することができます。セグメントは、ネットワーク内でトランザクションがどのように流れているのか、そしてユーザーとアプリケーションがどのようにデータとサービスにアクセスしているのかに基づいています。
- 保護サーフェスに流入/流出するすべてのトラフィックに対して、1ヶ所のコントロールポイントにセキュリティ機能を集約してください。セグメンテーションゲートウェイはポリシーを採用し、暗号化トラフィックを復号化し、次のような保護を適用する必要があります。
  - DNSセキュリティ（DNS Securityサービスの使用、これは複数のリアルタイム脅威インテリジェンスソース、大幅にスケーラブルなDNSリクエストのリアルタイム解析、および高度なDNSシグネチャを提供しています）。
  - 侵入防御（脆弱性防御、Anti-Spyware、およびAntivirusプロファイル）。
  - 潜在的に危険なファイルタイプのブロック。
  - 未知の脅威およびDay 1 脅威の防止（WildFire）。
  - URLフィルタリング。

    - データ消失防御 (DLP)。
- レイヤー7でリアルタイムにトラフィックを復号化、検査します。
- レイヤー2～レイヤー7からの各パケットをログに記録します。ファイアウォールを管理しているPanorama、個別のファイアウォール（Panoramaが管理していないファイアウォール）、Prisma Access（以前のGlobalProtect™クラウドサービス）、およびXDR Agentからのログを Cortex Data Lakeに送信して、物理ファイアウォールやVM-Seriesファイアウォール用のオンプレミスおよび仮想（プライベートおよびパブリッククラウド）ログストレージを集約、一元管理します。
- パートナーからのサードパーティ防御ツールを密接に統合するためにAPIを使用します。
- イベントを検出して応答を自動化する、フィードバックループの自動化を行います。
    - ワークロードにタグを設定し、タグをフィルタリング条件として使用して、セキュリティポリシー内のダイナミックグループのメンバーを判断します。これにより、HTTP（S）サーバーへのログ転送イベントに基づいて、アクションを自動化することができます。ログ転送イベントは、セキュリティポリシーで使われているダイナミックアドレスグループのメンバーを動的に追加、削除することで、リアルタイムにアクションをトリガします。ダイナミックアドレスグループのメンバーによるアクセスの許可または拒否をセキュリティポリシーが判断し、ファイアウォールがアクションを実施します。たとえば、Anti-Spywareセキュリティプロファイル内のDNSシンクホールを設定して、シンクホールへのアクセスを試みる、不正利用されている可能性があるシステムを自動的に隔離します。タグとログ転送機能を使って、シンクホールアドレスへのすべてのトラフィックをブロックしてログを記録する、ポリシールールにアタッチされたダイナミックアドレスグループに、これらのシステムを動的に追加または削除します。次に、ログアラートが通知されたら、不正利用されている可能性があるシステムを調査します。
    - ネットワークの解析の自動化、侵入の可能性を示唆する不審な行動の検出、そのような行動を調査し、問題に対処するためのアラートの生成を行うには、Cortex XDRを使用します。Cortex XDRを利用すれば、ネットワークトラフィックへの可視性を確保して、ログを相関させることで脅威の調査を容易にし、アラートの主原因を特定して即座に対処することができます。Cortext XDR APIを使ってXSOARと統合し、ご自分のビジネスワークフローに合わせたXSOAR応答プレイブックを使って応答を自動化することができます。そうすることで、応答、対処までの時間を日単位から分単位に短縮できる可能性があります。
    - 新しいマルウェアの検出を自動化するには、WildFireを使用します。WildFireが世界のどこかでマルウェアを検出すると、5分ほどでWildFireがセキュリティプロファイルを更新し、その新たなマルウェアから保護されるようになります。
- ポリシーのデプロイを自動化するには、Panoramaのテンプレートとテンプレートスタックを使用します。
- Ansible、Terraform、およびPythonなどのツールを使って、Prisma Cloudデプロイ環境の自動化、調整、および保護を行うことができます。

Palo Alto Networksにより、ゼロトラスト環境を設計し、すべての場所にまたがって一貫したセキュリティを適用することができます。

- Panoramaは、複数の次世代ファイアウォールの管理ポリシーコントロールを一元管理し、ファイアウォールを個別に管理する場合と比べて運用効率が向上します。
- 企業ネットワークとデータセンター:保護サーフェス用にネットワークをマイクロペリメータにセグメント化するには、次世代ファイアウォールを使用します。
- パブリッククラウド:オンプレミスまたはVM-Series次世代ファイアウォールを使用するPrisma Access、およびPrisma Cloud（APIベースのクラウドインフラセキュリティソリューション）を利用して、クラウド環境にゼロトラストポリシーを導入します。仮想プライベートクラウド（VPC）は、ワークロードをセグメント化するための保護境界を定義しています。
- プライベートクラウド:ゼロトラストポリシーを導入するには、VM-Seriesファイアウォールを使用します。
- 支店およびモバイルユーザー:クラウドベースのセキュリティを提供して、企業ネットワークリソースへのラウンドトリップを回避するには、Prisma Accessを使用します。ユーザー用Prisma Accessおよびネットワーク用Prisma Accessを設定して、支店を保護します。

または、オンプレミス次世代ファイアウォールとGlobalProtectサブスクリプションサービスを使用して、セキュリティポリシーを拡張し、リモートユーザーや支店オフィスに適用します。

- エンドポイント:セグメント化と最初の保護レイヤーに対して、次世代ファイアウォールを使ってレイヤー保護を行い、XDR Agentを使って2番目の保護レイヤーを作成します。GlobalProtect（オンプレミスインストール）、またはPrisma Access（Panoramaを使ってインストールされ、クラウドを管理する）VPNを使って一貫したポリシーを採用し、ポリシーをリモートエンドポイントに拡張して、ユーザーとともにポリシーの移動を可能にします。Prisma Accessでは、モバイルユーザーのエンドポイントにGlobalProtectアプリケーションが必要になります。どのような場合でも、管理対象エンドポイント上にGlobalProtectアプリケーションをインストールして、管理されていないエンドポイント（パートナーのシステムや個人のデバイスなど、エージェントを配置できないまたは配置したくないエンドポイント）では、GlobalProtect Clientless VPNを使用します。価値の高い資産を保護するために必要な場合は、多要素認証を適用します。
- SaaSアプリケーション:SaaSアプリケーションのスキャン、解析、分類、および保護を行うには、Prisma SaaSを使用します。管理されていないデバイスのSaaSアプリケーショントラフィックを、次世代ファイアウォール経由でリダイレクトします（管理対象デバイスからのトラフィックは、Prisma Access、GlobalProtect、または次世代ファイアウォールを通過します）。

ステップ4:ゼロトラストポリシーの作成

ゼロトラストポリシーは、ホワイトリストルールで構成されています。このルールは、権限のあるユーザーにのみ、指定されたアプリケーションで、指定された時間帯、および指定された場所からの、特定のリソースへのアクセスを許可します。トラフィックがルールに一致しない場合、そのトラフィックはファイアウォールにより自動的にブロックされます。以下の理由から、このことが重要になります。

- 許可したくないすべてのアプリケーションを判別してブロックする、終わりの見えない作業を行うよりも、ビジネスをサポートする、許可するアプリケーションを判断する方が簡単で分かりやすい。
- すべての違反や悪意のあるアクティビティが、許可ルールで発生する。許可したトラフィックのセキュリティを重視して、ビジネスに必要なトラフィックのみを許可する。

ゼロトラストポリシーはKipling Method（キプリングメソッド）に基づいています。ラドヤードキップリングの6つの質問、「誰が、何を、いつ、どこで、なぜ、どのように」に回答することで、トラフィックを許可/ブロックする方法、および各保護サーフェスを防御するセキュリティポリシーの作成方法を理解することができます。Palo Alto Networksは、セキュリティポリシーにキプリングメソッドを導入するための機能を提供しています。

- 誰がリソースにアクセスするのか？
  - User-IDでユーザーを識別し、ポリシーで誰がリソースにアクセスするのかを制御することができます。最小権限アクセスのレンズを通じて（誰が知る必要があるのか？）、正当なビジネス上の理由がある個人、グループ、デバイスにのみアクセスを許可します。
  - ユーザーがリソースへのアクセスを試みた時に、そのIDを検証する認証ポリシーを作成してください。認証ポリシーは、多要素認証（MFA）が必要かどうかも判断します。
  - Captive Portalにパスワードを入力するだけでなく、機密サービス、アプリケーション、リソースへのアクセスをファイアウォールが許可する前に、MFAを使って、携帯電話に配信されたワンタイムコードなど、1つ以上の認証要素を要求することで、機密サービスおよびアプリケーションを保護します。リモートユーザーの場合は、MFA通知を容易にするために、GlobalProtectを設定します（ファイアウォール上にもMFAを設定する必要があります）。
  - GlobalProtectを使用するデバイスに対して、ホスト情報プロファイル（HIP）を設定して、ホストに対するアクセスポリシーを定義して、それらのホストにポリシーを適用することで、セキュリティおよびメンテナンス標準を満たしていないデバイスのリソースへのアクセスを防止します。たとえば、エンドポイントの暗号化を有効にする、またはホストのウィルス対策シグネチャを最新の状態に保つなどの場合に、HIPを使用することができます。ホストがHIP要件を満たしていない場合、セキュリティポリシーはアクセスをブロックします。
- どのアプリケーションをリソースのアクセスに使用するのか？

- App-IDを使って、ポート、プロトコル、回避策に関係なくアプリケーションを識別する、アプリケーションベースのレイヤー7ポリシーを作成し、ネットワーク上の正しいアプリケーションを許可するようにしてください。レイヤー3およびレイヤー4に基づくポリシーは、IPアドレスを利用しますが、攻撃者はそのアドレスになりすまして、ポートを回避型アプリケーションに対して開かれた状態にすることができます。
- アプリケーションをデフォルトのポートで安全に有効化するために、サービスをアプリケーションのデフォルトに設定し、回避型アプリケーションが非標準ポートを使ってネットワークにアクセスすることを防止します。
- ファイアウォールでPAN-OS 9.0以降が動作している、またはPAN-OS 9.0以降が動作しているPanoramaアプライアンスが、PAN-OS 8.1以降が動作しているファイアウォールを管理している場合、Policy Optimizerを使って既存のポリシールール（アプリケーションベースのルールと従来のポートベースのルールの両方）を調査して、使われていないルールの識別、および使われていないアプリケーションを持つルールの識別を行います。古いバージョンのPAN-OSが動作しているファイアウォールの場合は、Expeditionを使ってポリシーを調査します。従来設定をPAN-OSデバイスに移行する必要がある場合は、「アプリケーション ベースのポリシーに移行する際のベストプラクティス」に従ってください。

- いつユーザーがリソースにアクセスするのか？

  アプリケーションユーザーが特定の時間帯にのみアクセスする場合は、スケジュール（Panoramaアプライアンスまたはファイアウォール上で、**Objects**（オブジェクト）> **Schedules**（スケジュール））をポリシールールに適用して、その時間帯以外の疑わしいアクセスを防止します。敵はしばしば、発見される可能性を減らすために、通常のビジネス時間外に攻撃を行い、データの抜き取りを試みます。
- どこにリソースが存在しているのか？

  ポリシーに宛先リソースの場所を追加します。必要に応じて、トラフィックのソース（ゾーンおよびIPアドレス）も制限してください。
- なぜ、データがアクセスされたのか、失った場合のデータの価値は？

  データの価値を理解するために、データを分類します。なぜそのデータを保護する価値があるのでしょうか？攻撃者にデータが抜き取られた場合の損失を開示する必要がありますか？機密情報がネットワークから流出することを防止するために、データのフィルタリングをセットアップして、データ分類ツールを使ってデータに関するメタデータを提供します。データの価値を理解することで、データの保護方法、使用後のデータの処置、およびポリシーで使用するためのタグの設定方法を判断することができます。
- どのように、リソースへのアクセスを許可する必要があるのか？

  Content-IDとベストプラクティスを適用して、アプリケーショントラフィック内の脅威から保護します。

  - 最小権限の原則をセキュリティポリシーに適用します。正当なビジネス上の理由があるユーザーのみを、ビジネス上の目的でアクセスに必要なアプリケーションのみを使って、適切な時間帯にのみ、適切な方法でのみ、アクセスを許可するようにしてください。
  - レイヤー7を経由するすべての内部/外部トラフィックを、ログに記録します。ファイアウォールポリシールールでは、デフォルトでログの記録が有効になっています。簡単で徹底した解析を行えるように、ログをCortex Data Lake（またはPanoramaまたはLog Collectors）に転送して、ログを集約します。
  - すべてのロケーション（ネットワーク、クラウド、エンドポイント）、すべてのローカル/リモートユーザーに対して、一貫したポリシーと脅威防御を適用して、ユーザーがどこに居る場合でも、すべてのアプリケーションおよびすべてのリソースに対してポリシーが適用されるようにしてください。整合性がないポリシーは脆弱性を増加させ、理解することや維持管理することが困難で、コンプライアンス要件や監査に悪影響を与える可能性があります。セグメンテーションゲートウェイとして物理型次世代ファイアウォールまたは仮想型VM-Seriesファイアウォールを使用し、一貫したゼロトラスト、レイヤー7、キプリングメソッドポリシーをネットワークやクラウドに適用します。Prisma Access（クラウド）およびGlobalProtect（オンプレミスインストールで、Prisma

Accessを使用）を使って、整合性のあるゼロトラストポリシーをエンドポイントに適用します。管理されていないエンドポイント（エージェントを配置できない、または配置したくないエンドポイント）の場合、GlobalProtect Clientless VPNを使用して整合性のあるポリシーを適用します。Panoramaテンプレートおよびスタックを作成して、データセンターや境界などの似たような口ケーションに対して整合性のあるポリシーを適用します。

- セキュリティプロファイル（IPSの場合Vulnerability Protectionプロファイル、1 Dayマルウェアなどのマルウェアに対して保護するAntivirusおよびWildFireプロファイル、コマンドアンドコントロール脅威を防止するAnti-Spywareプロファイル、危険性の高いファイルタイプをブロックまたは警告するFile Blockingプロファイル、およびWebサイトへのアクセスをコントロールして、フィッシング攻撃を防止し、検索エンジンの安全な検索を行うURL Filtering）を設定して、それを許可したすべてのトラフィックに適用します。データセンターファイアウォールおよび境界のファイアウォールセキュリティプロファイルのベストプラクティスに従ってください。
- WildFireベストプラクティスを使用して、ゼロデイマルウェアを検出、防止します。
- 復号化パラメータを使用して、規制やビジネス要件が許す限りのトラフィックを復号化し、できる限り多くのトラフィックを検査します。見えない脅威からネットワークを保護することはできません。
- DNS Securityサービスを使用して、DNSシグネチャへの非常にスケーラブルなリアルタイムアクセス、DNSリクエストのリアルタイム解析、および機械学習と予測解析を使って生成された高度なDNSシグネチャを提供します。
- 「どのように」には、機密データの利用後の処理（暗号化、トークン化、マスキングを使って抽象化する、またはアーカイブ、削除を行ってデータを破棄する）を判断することも含まれています。古いデータをアーカイブします（大部分のシステムで、およそ80%のデータが2年以上もアクセスされていません）。
- Cortex XDRを使って、ポリシーを調整、改善します。

キプリングメソッドにより、誰がアクセス権を持ち、どのようにアクセスする必要があるか、いつアクセスできるのか、そして適用する保護を理解できるため、各保護サーフェスを適切に防御するセキュリティポリシーを作成することができます。キプリングメソッドに基づいて、ビジネスステートメントを開発して、ポリシールールを作成することができます。以下に例を示します。

	誰が（Who）	何に（What）	いつ（When）	どこで（Where）	なぜ（Why）	どのように（How）
メソッド	User-ID	App-ID	時間制限	システムオブジェクト	分類	Content-ID
オンプレミス	集合ユーザ	Epic	[any]	Epic_Srvr	価値（データは高価値）	復号化、検査（セキュリティプロファイル）、ログトラフィック
プライベート クラウド	営業	営業戦力	業務時間	米国	価値（データは高価値）	復号化、検査（セキュリティプロファイル）、ログトラフィック

どちらの場合でも、ファイアウォールはキプリングメソッド内の条件をすべて満たし、検査に合格したトラフィックのみを許可します。ファイアウォールは、許可ルールを満たさないすべてのトラフィックを自動的に拒否します。

セキュリティ、認証、および暗号化ポリシーに加えて、サービス拒否（DoS）攻撃から仮想サーバーを保護するために、DoSおよびゾーン保護のベストプラクティスを使用してください。

まだ設定していないファイアウォールの場合は、IronSkillet Day 1設定テンプレートを使用して*Day 1*ベストプラクティスポリシーを導入し、その後保護サーフェスに合わせてポリシーの調整を行います。

ステップ 5:ネットワークの監視と管理

ログの記録とモニタリングにより、行う必要がある改善点が浮き彫りになり、また時間の経過に伴いビジネスやネットワークは変化していくため、セキュリティは反復的に行う作業となっています。ネットワークを設計する際に開発した運用プロセスに従い、継続的に予防コントロールを更新してください。

- レイヤー7経由のすべてのトラフィック（内部および外部）を、復号化、検査、およびログに記録してください。
- ファイアウォールを管理しているPanorama、個別のファイアウォール（Panoramaが管理していないファイアウォール）、Prisma Access、およびXDR AgentからCortex Data Lakeにログを転送し、オンプレミスおよび仮想（プライベートおよびパブリッククラウド）のログストレージを集約、一元管理してください。そうすることによって、ネットワークおよび保護サーフェスの可視性を確保することができます。
- Cortex XDRからのインテリジェンスに基づいて、ポリシーを更新したり、状況に応じて新たな保護サーフェスを追加したりします。Cortex XDRはCortex Data Lakeのデータと機械学習を使用して、ネットワークの通常の行動に基づいてネットワークを自動的に解析して、侵入やその他の脅威を示唆する可能性がある不審な行動を識別します。保護サーフェス内にないDAASエレメントをターゲットにした脅威アクティビティが、当初保護サーフェスを定義した時に考慮しなかった保護サーフェスを露わにする可能性があります。
- ネットワークトラフィックの可視性を確保して、ログを相関することで脅威の調査を簡素化し、アラートの主原因を特定して即座に対処を行うためには、Cortex XDRを使用してください。
- Cortext XDR APIを使ってXSOARと統合し、ご自分のビジネスワークフローに合わせたXSOAR応答プレイブックを使って応答を自動化することができます。そうすることで、応答、対処までの時間を日単位から分単位に短縮できる可能性があります。
- 設定データ、ユーザーアクティビティ情報、およびネットワークトラフィック情報を集約して、可視性を確保するには、Prisma Cloudを使用します。Prisma Cloudはデータを解析し、簡潔で対処可能な知見を提供しています。
- アプリケーションと脅威コンテンツ更新のベストプラクティスに従って、新しい、または変更されたApp-IDを取得して、脅威シグネチャを最新の状態に保つようにしてください。
- ベストプラクティスアセスメント（ベストプラクティス評価）ツールを使って、ベストプラクティス構成への進捗状況を評価し、ベストプラクティスに基づいたセキュリティポリシーへの移行に役立ててください。
- 環境の可視性を確保するために、ネットワークアクティビティを監視して、事前定義レポートを使用して、カスタムレポートを生成してください。
- 部門間にまたがるチームを維持して、ネットワークやビジネスの進化に伴いゼロトラスト導入環境のメンテナンスを行い、またチームの新メンバーが戦略や実行内容を理解できるように、教育とトレーニングを作成してください。
- 自動化機能の進歩に伴って、アクションと応答/対処の自動化を継続してください。

ゼロトラストリソース

以下の技術ドキュメント、ホワイトペーパー、webcast、ビデオ、およびその他のリソースは、ゼロトラスト戦略に関する詳細な情報と概念を提供しています。このドキュメントに記載されている情報とリソースに加えてPalo Alto Networksのプロフェッショナルサービスのエキスパートによるコンサルティングチームを、ゼロトラスト戦略の設計と導入を支援するために利用することができます。

- ゼロトラストネットワークの構築方法（オンデマンドwebcast）
- ゼロトラスト導入に関する風説の誤り（オンデマンドwebcast）
- ゼロトラストの概要
- ゼロトラスト（Palo Alto NetworksのゼロトラストWebページ）
- ゼロトラスト実行のベストプラクティス（移行のロードマップ）
- 5ステップの方法論を使ったゼロトラスト導入の簡素化（ホワイトペーパー）
- クラウドの保護:ゼロトラストのクラウドセキュリティ
- ゼロトラストのクラウドセキュリティ（ビデオ）
- ゼロトラストの真実（インフォグラフィック）

Palo Alto Networks技術ドキュメント

ベストプラクティスへの移行:

- BPA スタート ガイド
- BPAの実行方法（ビデオ）
- BPA結果の理解（ビデオ）
- ライブコミュニティのベストプラクティス評価ページ

ベストプラクティスドキュメントポータル:

- スタート ガイド（ベスト プラクティス）
- インターネット ゲートウェイの最良のセキュリティポリシー
- データセンターの最良のセキュリティポリシー
- 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
- 管理アクセスを保護するためのベストプラクティス
- アプリケーションおよび脅威コンテンツ更新のベストプラクティス
- 復号化のベスト プラクティス
- DoS およびゾーン プロテクションのベストプラクティス
- WildFire 導入のベスト プラクティス

Expedition

IronSkillet（Day 1設定テンプレート）

カスタマー サポート

防御態勢評価（防御機能に対する補足的な評価）

Palo Alto Networks NextWave Technology パートナー