



PCI 準拠のコストと難易度を劇的に削減する方法

ネットワークセグメンテーションとポリシーベースのアプリケーション、ユーザー、およびコンテンツ管理によるカード会員データの保護

2008 年 12 月

Palo Alto Networks
232 E. Java Drive
Sunnyvale, CA 94089
408-738-7700
www.paloaltonetworks.com

目次

概要	3
必須条件である PCI への準拠	4
ネットワークセグメンテーションによる PCI 準拠のコストと難易度の削減	4
ネットワークセグメンテーションの主な要件	5
既存のテクノロジーによるネットワークセグメンテーションの課題	6
Palo Alto Networks によるネットワークセグメンテーション	6
アプリケーションのアクセス制御	6
Active Directory によるユーザーベースのアクセス制御	7
コンテンツの監視と検査	7
パフォーマンスが低下しないゾーンベースの保護	8
監査のための制御の証明	8
ロールベースの管理による監査人のアクセスの簡素化	9
Palo Alto Networks のポリシーの例	9
まとめ	10
付録 1: Palo Alto Networks と PCI セキュリティ要件	11

Copyright 2008, Palo Alto Networks, Inc. 無断複写・転載を禁じます。Palo Alto Networks、Palo Alto Networks ロゴ、PAN-OS、App-ID および Panorama は米国における Palo Alto Networks, Inc. の商標です。仕様はすべて予告なく変更される場合があります。本文書内の誤りや本文書中の情報更新義務に関し、Palo Alto Networks はいかなる責任も負わないものとします。Palo Alto Networks は、本出版物を予告なく変更、修正、権利譲渡、または他の何らかの方法で改訂する権利を留保します。

概要

ペイメントカード業界データセキュリティ基準 (PCI DSS) とは、加盟店や決済代行業者が保存、処理、または伝送するカード会員データを保護するための広範な取り組みです。最も重要な点は、カード会員データを扱う組織は例外なく PCI に準拠する必要があるということです。

PCI への準拠は 1 回限りの取り組みではなく、ベストプラクティスとテクノロジーを活用してカード会員データを保護する継続的なプロセスです。このプロセスは IT 部門だけでなく多くの部門が関わる継続的な取り組みであるため、単純に新しいテクノロジーを導入することによって基準を満たせる訳ではありません。ネットワークが基準を満たしているか監査する場合、ネットワーク内でカード会員データを扱うすべての部分が監査範囲となります。つまり、あらゆる組織において PCI 準拠の対象範囲は、手間とコストの両面に関して膨大なものとなります。企業が PCI 準拠のコストと難易度を削減するための方法の一つとして、ネットワークをセグメント化し、カード会員データを安全なセグメントに隔離することができます。

ネットワークセグメンテーションにより、IT 部門は一連のセキュリティポリシーの庇護の下に重要なデータを隔離し、より効果的にデータを保護することができるため、この方法はネットワークセキュリティのベストプラクティスと見なされています。PCI に準拠する必要がある企業は、ネットワークセグメンテーションを使用してカード会員データを隔離し、監査プロセスの範囲を絞ることができます。

2008 年 10 月に更新された PCI DSS の文書には、次のように記載されています。

カード会員データ環境のネットワークセグメンテーション、すなわち企業ネットワークの他の部分からのカード会員データ環境の隔離 (セグメント化) は、PCI DSS 要件ではありません。ただし、ネットワークセグメンテーションは次のものを引き下げる方法として推奨されます。

- PCI DSS 評価の対象範囲
 - PCI DSS 評価のコスト
 - PCI DSS による管理を実装して維持するコストと難易度
 - 組織のリスク (管理が厳重な少数の場所にカード会員データを統合することで減少)
- ネットワークセグメンテーションが適切に行われていない場合 (「フラットネットワーク」とも呼ばれる)、ネットワーク全体が PCI DSS 評価の対象範囲になります。

ファイアウォールを含む多くのネットワークデバイスでは、IP アドレス、論理ゾーン、またはこれらの組み合わせに基づいた基本的なネットワークセグメンテーションを実装できます。問題は、ファイアウォールを含むこれらすべてのデバイスの管理メカニズムが、ポート番号、プロトコル、および IP アドレスに基づいているということです。既存のどのネットワークデバイスも、アプリケーションの識別情報に基づいてセグメントへのアクセスを識別して制御することができず、Active Directory のユーザーおよびグループ情報にポリシーを直接関連付けることはできません。このような技術上の制限があるため、既存のネットワークデバイスは、これらの防御を簡単に突破できる巧妙な攻撃者やセキュリティ上の脅威からカード会員データを保護する有効な方法ではありません。

Palo Alto Networks の次世代ファイアウォールは、Active Directory 内のユーザーまたはグループの識別情報に基づくセキュリティポリシーにより、カード会員データを隔離し、保護できます。ユーザーおよびグループの識別情報は特定のアプリケーションに直接関連付けられ、そのアプリケーションでセキュリティ上の脅威と不正なデータ転送を検査できるようになります。現在市販されているどのファイアウォールソリューションも、このような詳細な管理を行うことはできません。

必須条件である PCI への準拠

カード会員データを扱う組織は例外なく PCI に準拠する必要があります。これは必須条件です。基準を満たしていない企業は、カード会員企業からの経済的な圧力に直面することになります。また、カード会員の取引に対する経済の依存度が高まるにつれてカード会員データの消失リスクは必然的に増加するため、(PSI の準拠に関連する場合もそうでない場合も) データ保護の取り組みは非常に重要になります。企業が PCI に準拠するかどうかにかかわらず、データ侵害による被害は非常に高価なものになる可能性があります。Forrester 社によれば、1 レコード当たりのデータ侵害の予測コスト (罰金、後始末、機会の損失など) は、90 ドル (知名度が低い規制対象外の企業の場合) から 305 ドル (知名度が高く厳格に規制された企業) です。そのため、10,000 件のレコードが失われると 3,000,000 ドルものコストがかかるうえに、企業の評判に対するコストは計り知れないものとなります。

PCI への準拠は、文書化されたベストプラクティスとテクノロジーを組み合わせることで達成することができます。長期的にはカード会員データだけでなく企業資産を守ることを望むすべての企業にとって有益です。ただし、短期的には、人的資源、ハードウェア、およびコンサルティングに多くのコストがかかる可能性があります。

ネットワークセグメンテーションによる PCI 準拠のコストと難易度の削減

PCI の文書に記載されているように、ネットワークセグメンテーションを使用して PCI 監査の対象範囲を絞ることができます。その根拠は比較的単純で、監査の全体サイズ (範囲) を減らせばコストと難易度も減らすことができます。カード会員データが安全なセグメントに隔離されていることが確実であれば、監査が必要なのはそのセグメントだけです。

この場合、セグメンテーションの価値は非常に大きなものとなります。次に、ネットワークをセグメント化することで減らせるもののほんの一例を示します。

- サーバーの数が減少します。これはカスタマごとに異なりますが、たとえば、フラットネットワークに 100 のサーバーがあり、そのうち実際にカード会員データを格納しているのは 4 つのサーバーだけであるとします。フラットネットワークでは任意のサーバーまたはユーザーがカード会員データにアクセスできる可能性があるため、ネットワーク全体が対象範囲となります。このとき、カード会員データを格納する 4 つのサーバーを選択して安全なセグメントに隔離すると、隔離したサーバーとそのセグメントに送受信されるトラフィックのみが対象範囲となります。この場合、監査の範囲は 96% 減少します。

	フラットネットワーク	セグメント化されたネットワーク
カード会員サーバー	4	4
全サーバー	100	100
対象となる監査範囲	100	4
減少した監査範囲	0%	96%

表 1: 監査範囲減少の理論上の例

- 監査コストが減少します。単純計算で、サーバーの数が減少すると監査に要する時間とリソースも減らすことができます。
- セグメントを保護する手間が減ります。セグメントを保護するためのセキュリティポリシーを開発して適用する方が、ネットワーク全体に同じポリシーを適用するよりも手間がかかりません。

- ネットワークの再構築を最小限に抑えることができます。セグメンテーションを使用しない場合、企業によっては、カード会員データを効果的に隔離するために、サーバーを移動し、適宜ネットワークを再構築することが必要になる場合があります。セグメンテーションにより、ネットワークの変更を最小限に抑えることができます。
- 調査の手間が減ります。セキュリティに関する事件が発生した場合、ネットワーク全体のトラフィックを調査するよりもネットワークセグメントで送受信されたトラフィックを調査する方が、迅速かつはるかに少ない作業で済みます。

ネットワークセグメンテーションは新しい概念ではなく、過度に複雑なわけでもありません。ネットワークセグメンテーションはほとんどのネットワークで使用されており（サブネット）、スイッチ、ルーター、ファイアウォールなど、さまざまなネットワーク機器を使用して実装できます。ネットワークの変化に伴い、ユーザーのモバイル化が進み、アプリケーションのアクセスは以前よりも制御されなくなりました。また、ネットワークセグメンテーションは、リスクを分離してリソースを保護する方法としてセキュリティ上のベストプラクティスになりました。

ネットワークセグメンテーションの主な要件

ネットワークのセグメント化はさまざまなテクノロジーを使用して実現できますが、セグメンテーションを PCI 準拠のためのカード会員データ隔離の手段としてとらえる場合、いくつかの主要な要件を考慮に入れる必要があります。

- **柔軟性** セキュリティ上の理由でネットワークをセグメント化する場合、ネットワークアーキテクチャーの変更が必要になる可能性があります。これは、ほとんどの企業ができることなら避けたいと望む作業です。そのため、これを避けるため、セキュリティ目的でネットワークをセグメント化する場合には、IP アドレス範囲、VLAN、物理インタフェース、またはこれらの組み合わせを使用してセグメント化が可能である必要があります。
- **ポリシーベースのセキュリティ** ネットワークの分割を目的としたセグメンテーションは、何らかのセキュリティポリシーをセグメントに適用できなければほとんどメリットはありません。PCI に準拠するには、ファイアウォールを使用してセグメントを保護するようにし、IP アドレス、ポート番号、およびプロトコルだけでなく、ユーザーとアプリケーションの識別情報に基づいたポリシーを使用する必要があります。どのユーザー、アプリケーション、およびコンテンツがセグメント内のカード会員データにアクセスできるかを正確に把握して管理しないと、IP アドレス、ポート番号、およびプロトコルに基づく制御を簡単に回避できるアプリケーションとユーザーがデータにアクセスしてしまう可能性があります。
- **ポリシー管理の証明** 基準に準拠するには、監査人に対し、適用されているポリシーを示し、ネットワークデータへのアクセスを許可して、カードデータ保護のために実施されている方策を示す必要があります。監査人は、セキュリティポリシーと誰がその編集を行ったかを確認する必要があります。また、監査人は、トラフィックパターンと潜在的なリスク領域を見つけるためにログを調べる必要があります。
- **パフォーマンスは非常に重要です** PCI 準拠のためにセグメンテーションを行う場合、ビジネスにとって非常に重要な大量のトラフィックが処理されるネットワーク内の場所に対してセキュリティポリシーを厳重に適用する必要があります。したがって、安全なセグメントを実現するソリューションは、非常に高いセッション処理率と最小限のレイテンシでマルチギガビットの通信速度において動作する必要があります。

セグメンテーションの概念は理解しやすく、PCI 準拠の達成と維持によって大きなメリットが得られます。

既存のテクノロジーによるネットワークセグメンテーションの課題

ネットワークのセグメント化は既存の多くのテクノロジーを使用して実現できますが、PCI 準拠のために安全なセグメントを構築しようとする場合、これらのテクノロジーは有効とはいえません。

- レガシーファイアウォールは、アプリケーションとユーザーを識別しません

レガシーファイアウォールは、ユーザー識別情報、アプリケーション、およびコンテンツに基づいてカード会員データへのアクセスを識別して制御することはできません。現在のファイアウォールは、ポート番号、プロトコル、および IP アドレスのみに基づいたポリシーを基本的なセグメンテーションに適用することしかできません。

- ファイアウォール補完製品は、ユーザーに基づいたアクセス制御にはほとんどまたはまったく効果がありません

NAC などのファイアウォール補完製品は、ユーザー制御に関してほとんどメリットをもたらしません。これは、NAC の追加は管理が必要な (ユーザーエージェントと関連付けられた) アプライアンスが 1 つ増えてしまうにすぎないため、その有用性を失ってしまうからです。また、マルチアプライアンスという面から見ると、監査人はさまざまなデバイス、ログ形式、および管理インターフェースを確認しなければならなくなるため、証明作業はさらに困難になります。IPS の導入も、データにアクセスできるユーザー、アプリケーション、およびコンテンツの制御に関してはほとんどメリットはありません。IPS 機能はすべてのトラフィックを許可し、特定の脅威だけをブロックするように設計されており、ユーザーとアプリケーションの制御機能は限定的であるためです。ただし、IPS は PCI 準拠のためのセキュリティ上の脅威防御要件を満たす助けにはなりません。

Palo Alto Networks によるネットワークセグメンテーション

Palo Alto Networks の次世代ファイアウォールは、PCI に準拠する必要があるカスタマに対し、ハードウェアおよびソフトウェアに関するセグメンテーション機能のユニークな組み合わせを提供します。柔軟性に関しては、Palo Alto Networks のすべてのファイアウォールがセキュリティゾーンをサポートしています。セキュリティゾーンは、PCI 準拠という観点から見ると、ネットワークセグメントと同等のもので、セキュリティゾーンは、物理インターフェース、VLAN、IP アドレス範囲、またはこれらの組み合わせを格納する論理コンテナです。セキュリティゾーンをカード会員データ隔離のために使用すると、データ保護に役立つのみでなく、物理的なネットワーク再構築の必要性を減らすこともできる場合があります。カード会員データの保護に関し、Palo Alto Networks ファイアウォールが現在市販されている他のファイアウォールと大きく異なる点として、各セキュリティゾーンを横断することができるアプリケーション、ユーザー、およびコンテンツを制御する機能を備えているという特徴があります。いったんネットワークを個々のゾーンに分割したら、カード会員データサーバーが含まれるゾーンへの出入りを許可するアプリケーション、ユーザー、およびコンテンツを非常に詳細に制御するセキュリティポリシーを適用できます。ハードウェアプラットフォームとパフォーマンスに関しては、10 Gbps のファイアウォールパフォーマンスと高密度インターフェース (最大 24 の 1 Gbps インターフェース) の組み合わせにより、1 つのファイアウォールを使用することで、ネットワークを別々のゾーンに物理的に分割し、パフォーマンスのボトルネックを作り出すことなくゾーンを安全に保護できます。

アプリケーションのアクセス制御

Palo Alto Networks ファイアウォールは、市販されている製品の中で唯一、App-IDTM という特許出願中のテクノロジーを使用するファイアウォールです。App-ID により、ポート番号、プロトコル、SSL 暗号化、または使用されている回避手法に関係なく、750 を超えるアプリケーションを識別して制御できます。App-ID によるアプリケーション識別情報の判断は、4 つの異なる手法 (デコーダ、復号化、シグネチャ、およびヒューリスティック) により、プロキシを介さずインラインで実行されます。アプリケーション識別情報が判断されたら、この情報は適切な使用方法、コンテンツの検査、ロギング、レポートなど、すべてのポリシー決定の基盤として使用されます。

PCI 準拠のためにアプリケーションの正確な識別情報を把握するには、PCI プロジェクトリーダーは、IP アドレス範囲などの大まかな条件をポート番号やプロトコルとともに使用してカード会員データを隔離するゾーンを保護するのではなく、特定のアプリケーション (Oracle など) がカード会員データを含むゾーンにアクセスするのを許可するポリシーを定義できるようにする必要があります。これにより、ポート番号を変更したり別のアプリケーション内に潜んだりする可能性がある他のすべてのアプリケーションはゾーンにアクセスできないようにブロックされ、そのアクティビティは調査と監査のためにログに記録されます。

Active Directory によるユーザーベースのアクセス制御

PCI 準拠のためにゾーン内にカード会員データを隔離するための次の手順は、アプリケーション識別情報を Active Directory の特定のユーザー名情報に関連付けることです。この機能を実現するため、Palo Alto Networks は User-ID というテクノロジーを提供しています。User-ID は Active Directory とシームレスに統合され、ユーザーベースおよびグループベースのポリシー管理を可能にします。各デスクトップにエージェントをインストールする必要はありません。

User-ID を使用することで、PCI プロジェクトリーダーは、Active Directory 内に格納されているユーザー識別情報およびグループ識別情報 (財務ユーザーなど) をアプリケーション (Oracle など) に関連付けるポリシーを作成できます。ユーザーからのインバウンドトラフィックのみを許可するポリシーを作成することで、カード会員データへのアクセスを制限できます。あるいは、他のすべてのユーザーまたはグループがゾーン内のカード会員データにアクセスすることを禁止するポリシーを作成することもできます。

現在、企業はますますモバイル化しており、従業員は事実上世界中のどこからでもネットワークにアクセスし、社内無線ネットワークはユーザーが別のゾーンに移動すると IP アドレスを再割り当てしています。また、ネットワークのユーザーは企業の従業員とは限りません。このような今日の IT が直面する課題を User-ID によって解決できます。

コンテンツの監視と検査

PCI 準拠を達成し、これを維持しようとする場合、カード会員データにアクセス可能なアプリケーションとユーザーを制御するだけでは、IT 部門が直面する可視化と管理の問題の一部が解決されるのみにすぎません。カード会員データは企業の重要な資産であるということを理解し、各ゾーンを横断するアプリケーショントラフィックを監視および検査するプロセスが次の重要な課題となります。この課題は、リアルタイムコンテンツ検査エンジンである Content-ID で解決できます。

Content-ID はさまざまなセキュリティ上の脅威 (ウイルス、脆弱性悪用、ボット、トロイの木馬) をブロックし、ファイルおよびデータの不正な転送を取り締まります。Content-ID を使用することで、PCI プロジェクトマネージャは、カード会員データ保護に関する次に示す 2 つの重要な目的を達成するポリシーを実装できます。

- あらゆる種類のセキュリティ上の脅威、特にデータの検出と盗難に特化している可能性がある脅威 (ボット、トロイの木馬、ワーム) がないかインバウンドトラフィックを検査します。
- 不正なカード会員データの転送がないかアウトバウンドトラフィックを監視し (ファイルまたはデータパターン)、転送を全面的にブロックするか、アラートを送信します。

パフォーマンスが低下しないゾーンベースの保護

Palo Alto Networks の次世代ファイアウォールは、最大 10 Gbps の通信速度でアプリケーション、ユーザー、およびコンテンツを識別および制御しながら企業トラフィックの負荷を処理するように設計された専用プラットフォームです。この目的を達成するために使用される 2 つの要素は、ハードウェアプラットフォームアーキテクチャーと、トラフィックの処理方法を規定する単一パスアーキテクチャーです。

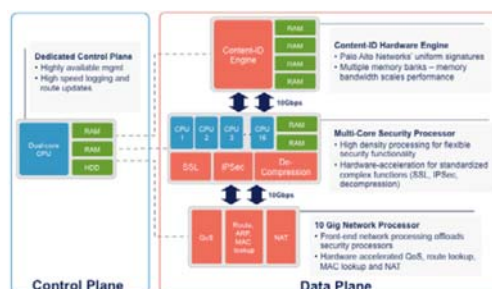


図 1: Palo Alto Networks PA-4000 シリーズのハードウェアアーキテクチャー

ハードウェアアーキテクチャーでは、ネットワーク接続、セキュリティ、管理、およびコンテンツ検査のために機能固有の専用プロセッサとメモリーが使用されます。データとコントロールプレーンを物理的に分離することで、いずれかを大量に使用しても他方に影響が及ぶことはありません。

レガシーネットワークセキュリティインフラストラクチャーでは、トラフィックは、それぞれ独自のネットワークエンジン、分類エンジン、パターン一致エンジン、およびポリシーエンジンを備えたいくつかのセキュリティデバイスを通ります。このような重複処理は、非効率であるだけでなく低速です。このような貧弱なパフォーマンスが、企業がトラフィックの通り道にもう 1 つ別のデバイスを設置することを躊躇する主な理由です。

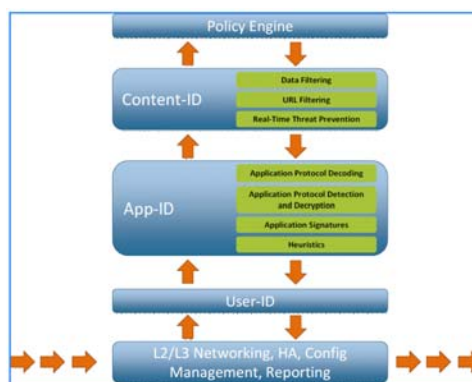


図 2: Palo Alto Networks の単一パスアーキテクチャー

Palo Alto Networks の次世代ファイアウォールは、トラフィックがそれぞれ 1 つのネットワークコンポーネント、アプリケーション分類エンジン、ユーザー分類機能、およびコンテンツ / パターン一致エンジンを通る単一パスアーキテクチャーを使用します。そのため、トラフィックの速度を落とすことなく、アプリケーション、ユーザー、およびコンテンツ (機密データとセキュリティ上の脅威を含む) を確認してポリシー管理を適用できます。

監査のための制御の証明

PCI への準拠は、監査人がサイトを訪問し、カード会員データ保護のために適用されている制御内容を評価して初めて達成されます。このために、監査人はファイアウォールログやレポートを含む多くのデータにアクセスする必要があります。監査人は、セキュリティポリシーの証明を確認するだけでなく、ゾーンに誰がアクセス可能でどのような変更が行われているか (変更が行われている場合) を判断するために、トラフィックログを参照することを望みます。

Palo Alto Networks では、PCI 監査人は簡単な操作でレポートツールやロギングツールにアクセスし、これを監査の証明要件の達成に使用できます。レポートとログビューアはともに、Active Directory との統合を通じてユーザーの動作を可視化することで、アプリケーションとセキュリティ上の脅威のアクティビティの確認作業を補完し、ゾーンのトラフィックの全体像をより詳細に把握できるようにします。サードパーティーによる追加分析とイベントの関連付けを行うために、すべてのログを syslog サーバーに簡単に転送することもできます。

- レポート: 事前定義された 30 を超えるレポートをそのまま使用したり、他のレポートの要素と組み合わせることで事前定義レポートをカスタマイズし、将来使用できるように保存したりできます。ファイアウォールの任意の情報源を使用して、完全にカスタマイズしたレポートをゼロから作成できます。レポートの生成をスケジュールに基づいて実行されるように自動化し、その結果を電子メールで送信したり、PDF または Excel にエクスポートしたりすることができます。
- ログビューア: 柔軟なフィルタリング機能を使用して、アプリケーションとセキュリティ上の脅威のアクティビティを確認できます。セルの値をクリックするとフィルタがすぐに作成されます。このフィルタは、式ビルダーと追加ログフィールド（ログビューアに表示されていないものも含む）によって複数の基準を組み合わせることで、さらに絞り込むことができます。ログフィルタは将来使用できるように保存でき、エクスポートボタンで、現在のフィルタに一致する結果をオフラインでアーカイブしたりさらに分析したりするために CSV ファイルにエクスポートできます。また、すべてのログファイルを syslog サーバーに送信することもできます。

ロールベースの管理による監査人のアクセスの簡素化

監査プロセスを円滑に成功させるポイントの一つは、監査人が参照する必要があるデータに適切にアクセスできるようにすることです。Palo Alto Networks ファイアウォールでは、現在市販されている中で最も詳細なロールベースの管理により、簡単にデータにアクセスできます。

監査人に対し、デバイスとセキュリティポリシーへのアクセスを読み取り専用で制限しながら、すべてのレポートおよびロギング機能へのフルアクセス権を付与できます。これにより、必要な監査プロセスをサポートしながら適切な制御を維持できます。

Palo Alto Networks のポリシーの例

ここでは、非常に簡素化されたネットワーク図を使用して、Palo Alto Networks の次世代ファイアウォールによって PCI 準拠のコストと難易度を削減する方法を説明します。左側の図はフラットネットワークを示します。この場合、ネットワーク全体が PCI の監査範囲になります。右側の図は、カード会員データがセキュリティゾーンに隔離された状態を示します。この図では、このデータにアクセスできる唯一のグループが財務ユーザーであることが示されています。

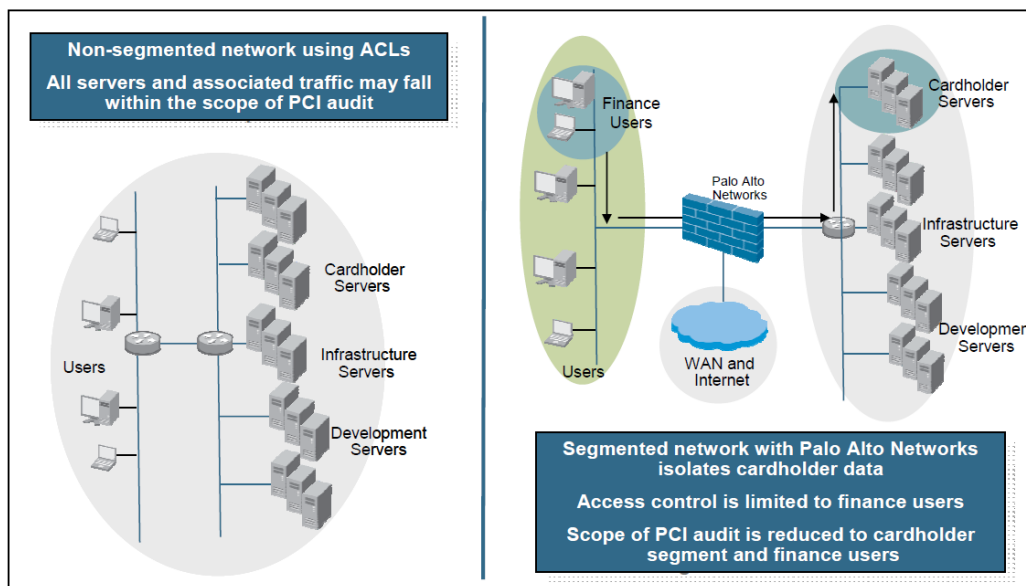
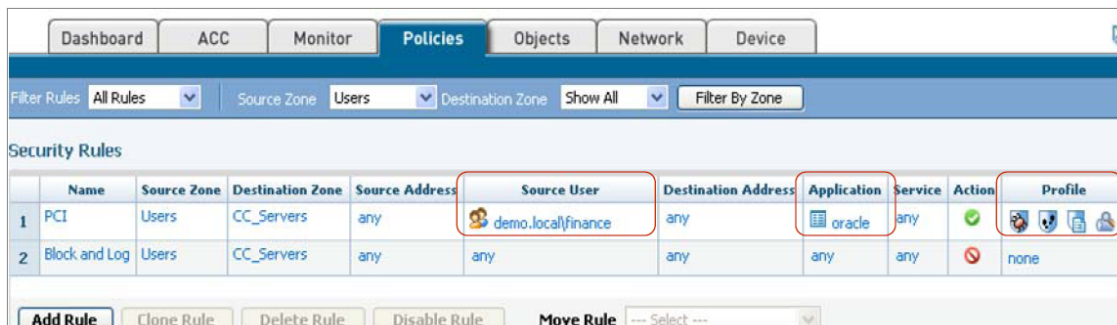


図 3: フラットネットワークとセグメント化されたネットワークの比較

ポリシーの例では、Palo Alto Networks がシンプルかつ正統的な方法でネットワークを複数のセキュリティゾーンに分割し、ポリシーに適用によりどのユーザー、アプリケーション、およびコンテンツがゾーンを横断できるか制御できることが示されています。まず、さまざまな手法のうちいずれか (VLAN、IP アドレス範囲、物理インタフェースなど) を使用して、カード会員サーバー、ユーザー (内部)、および WAN/インターネットのトラフィック用のセキュリティゾーンを構築します。

次の手順では、カード会員用のゾーン (CC_servers) にアクセスできるユーザー、グループ、アプリケーション、およびコンテンツを制御するポリシーを作成します。



Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile
1 PCI	Users	CC_Servers	any	demo.local@finance	any	oracle	any	✓	🛡️🔍📄
2 Block and Log	Users	CC_Servers	any	any	any	any	any	🚫	none

図 4: カード会員データを隔離して保護するポリシーの例

具体的には、このシンプルな 2 つのルールからなるポリシーの例では、次のような保護メカニズムが実行されます。

- ルール 1 (「PCI」) は次の条件を適用するために使用されます。
 - 財務ユーザー Oracle に対して、ユーザーゾーン (送信元) から CC_servers ゾーン (宛先) へのトラフィックのみを許可します。
 - 「Profile」では、CC_servers ゾーンに送られるトラフィックでセキュリティ上の脅威 (ウイルス、脆弱性悪用) をスキャンし、アウトバウンドトラフィックでファイル形式またはテキスト形式のカード番号などのカード会員データを監視します。
- ルール 2 (「Block and Log」) は次の条件を適用するために使用されます。
 - すべてのゾーン (送信元) から CC_servers ゾーン (宛先) へのすべてのユーザートラフィックとアプリケーショントラフィックを拒否し、拒否したすべてのアクティビティを調査分析または監査証明でできるようにログに記録します。

多くのファイアウォールはゾーンベースのポリシーの適用をサポートしていますが、Active Directory のユーザーおよびグループ情報に基づいてアプリケーションのアクセスを制御するポリシーを実装できるファイアウォールや単一のソリューションはほかにありません。

まとめ

企業の規模を問わず、PCI 準拠の対象範囲を減らすためにネットワークセグメンテーションを使用するメリットは非常に大きくなります。カード会員データ保護のためにネットワークをセグメント化して安全に保護する方法は多くありますが、柔軟にネットワークセグメンテーションを行い、カード会員データにアクセスできるユーザー、アプリケーション、およびコンテンツをポリシーで制御するというユニークな機能の組み合わせは、Palo Alto Networks のみが提供しています。

付録 1: Palo Alto Networks と PCI セキュリティ要件

PCI 準拠は、ベストプラクティスとテクノロジーを組み合わせることでのみ達成することができます。「PCI 準拠のための製品またはソリューション」のようなものは存在しません。

Palo Alto Networks の次世代ファイアウォールは、どのアプリケーション、ユーザー、およびコンテンツがネットワークを横断するか、ポリシーベースでの可視化と制御を可能にします。PCI 環境では、Palo Alto Networks は、セキュリティ関連のいくつかの項目で規定されている要件の達成を支援することができます。アクセス制御ポリシー（アプリケーション、Active Directory のユーザー）を個々のセキュリティゾーン（セグメント）に適用しながら、セキュリティ上の脅威を検出してブロックする検査ポリシーを適用できます。優れたレポートおよびログ機能により、PCI プロジェクトリーダーは監査証明を実行できます。

次の表に、PCI 準拠を目指す企業が Palo Alto Networks の次世代ファイアウォールによってメリットを得られる分野を示します。実際の機能に関しては、各 PCI 環境において評価する必要があります。

PCI DSS 要件	Palo Alto Networks によるメリット
安全なネットワークの構築と維持	
要件 1: カード会員データを保護するためにファイアウォールを導入し、最適な設定を維持すること	あり
要件 2: システムパスワードと他のセキュリティパラメータにベンダー提供のデフォルトを使用しないこと	---
カード会員データの保護	
要件 3: 保存されたカード会員データを保護すること	あり
要件 4: 一般に開放された公衆ネットワーク上でカード会員データを送信する場合、暗号化すること	---
脆弱性を管理するプログラムの整備	
要件 5: アンチウィルスソフトウェアまたはプログラムを利用し、定期的に更新すること	あり
要件 6: 安全性の高いシステムとアプリケーションを開発し、保守すること	あり
強固なアクセス制御手法の導入	
要件 7: カード会員データへのアクセスを業務上の必要範囲内に制限すること	あり
要件 8: コンピュータにアクセスする利用者ごとに個別の ID を割り当てること	---
要件 9: カード会員データへの物理的アクセスを制限すること	---
定期的なネットワークの監視およびテスト	
要件 10: ネットワーク資源およびカード会員データに対するすべてのアクセスを追跡し、監視すること	あり
要件 11: セキュリティシステムおよび管理手順を定期的にテストすること	---
情報セキュリティポリシーの整備	
要件 12: 従業員および契約社員用の情報セキュリティに関するポリシーを整備すること	---