

パロアルトネットワークスとアラクサラネットワークスのパートナーシップ

テクノロジーセグメント:インフラストラクチャー

パロアルトネットワークスのテクノロジーパートナープログラムは次世代ファイアウォールと相互運用するソリューションまたは製品を提供するパートナーが加入するプログラムです。

ハイライト

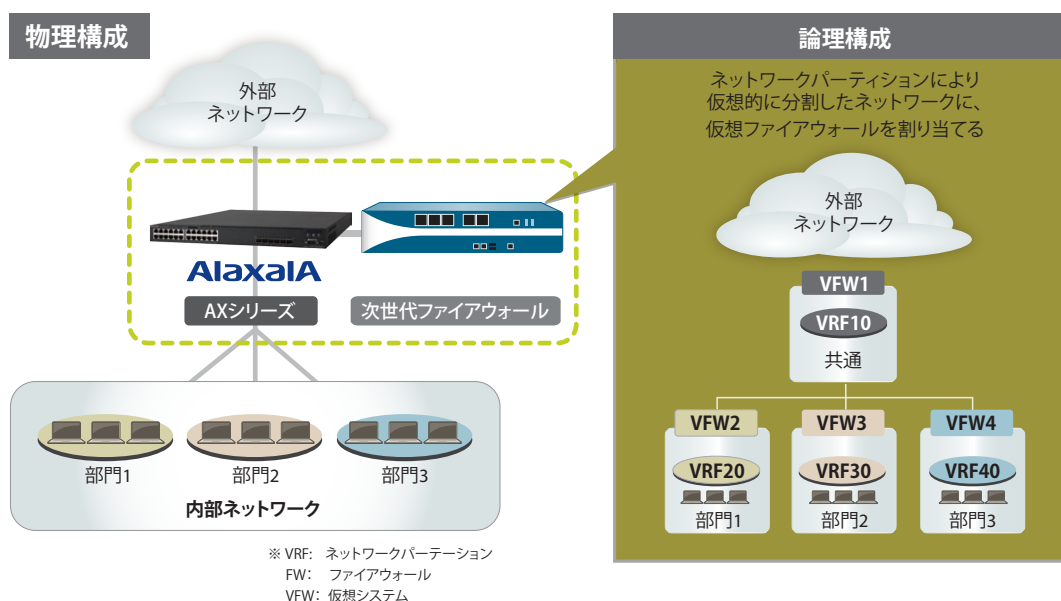
- ネットワークセグメンテーションによりセキュリティを強化
- アラクサラネットワークスの仮想ネットワーク技術により、シンプルな物理構成でネットワークを部門単位にセグメント化
- パロアルトネットワークス次世代ファイアウォールの仮想システムをセグメントごとに適用することで重要なデータを保護

リスクを局所化するネットワークセグメンテーション

企業が持つ個人情報を含む機密情報や、国家の機密情報の漏洩が世界的な社会問題になったりするなど、組織において各種情報のより厳重な取り扱いが急務となっています。またクラウドのビジネス利用や、BYODなど業務と私用の境界のあいまいな機器利用形態などシステムを取り巻く環境が変化し、ユーザーがその組織のネットワーク経由だけではなく、ソーシャルネットワークや個人所有のモバイルデバイス経由でも攻撃のターゲットとされるなど攻撃手法も変化しています。このような背景から、組織内の各部門が持つさまざまな情報に対し、アクセスすべきユーザーにのみ適切なアクセス権限を与えるような環境の構築が求められています。つまり、これからのITシステムにおけるセキュリティ管理は、サーバやネットワークを含めた情報の管理単位を部門ごとにセグメント化し、組織全体という大きな単位から、部門ごとにより細かい単位でセキュリティ管理を細分化することが重要となります。

アラクサラネットワークスのネットワーク仮想化とパロアルトネットワークス次世代ファイアウォールの仮想システムを組み合わせることにより、「セキュア仮想ネットワークセグメンテーション」を実現しました。

ネットワーク仮想化では、単一の物理ネットワークを複数の仮想ネットワークに分離することで、部門間の独立性およびセキュリティの確保が可能になります。仮想化されたネットワークごとに次世代ファイアウォールの仮想システムを割り当てることで、部門単位に最適なセキュリティポリシーを適用します。



セキュア仮想ネットワークセグメンテーションを導入することで、管理単位を細分化した高度なセキュリティを持つシステムを、初期投資・運用・管理のコストを抑えながら実現することができます。部門間のセキュリティを確保するためには、それぞれの部門で独立したネットワークを構成することが最もシンプルかつ簡単な方法です。アラクサラネットワークスの「ネットワークパーティション」で部門ごとに独立したネットワーク構成を作り、ネットワークを部門単位に分離できます。ネットワーク自体は仮想ネットワークで構成されるため、実際のスイッチ機器は最少の構成で済み、機器や運用コストの増加を抑えます。

組織によっては、技術的またはコンプライアンス上の理由で、特定部門のトラフィックを他部門とは異なるファイアウォールで保護しなければならない場合があります。パロアルトネットワークス次世代ファイアウォールの仮想システムは柔軟性と効率性に優れるため、組織においては機器の数を減らしながらも次世代ファイアウォールインスタンスを増やし、設備投資や運用コストを軽減して拡張性を高めるなど、事業効率が向上します。

ネットワークセグメンテーションは、ネットワークセキュリティの安全性を高めるためのベストプラクティスであると見なされています。これは、セグメンテーションによって重要なデータを他部門も含めた外部から隔離させ、より効果的なデータ保護が可能になるためです。重要なデータが含まれている可能性のあるネットワークをアラクサラネットワークスの仮想化技術でセグメント化し、パロアルト

ネットワークス次世代ファイアウォールの仮想システムと連携させることにより、そのようなコンテンツを未承認のアクセスやさまざまな脅威、データ損失から保護することができます。

アラクサラネットワークス

アラクサラネットワークス株式会社は、「快適で安心して使えるネットワークを世界の人々に提供し、豊かな情報通信社会の実現に貢献」を企業理念としています。情報ライフラインを支える概念として「ギャランティード・ネットワーク」を提唱し、ネットワーク構築に必要な基幹系ルータおよびスイッチの開発から設計、製造、販売、保守のサービスを提供しています。

<http://www.alaxala.com>

パロアルトネットワークス

パロアルトネットワークス(NYSE: PANW)は、次世代ネットワークセキュリティを専門とする企業です。その革新的なプラットフォームによって、企業、サービスプロバイダ、行政機関は各組織のネットワークをセキュリティ保護し、サイバー攻撃の脅威に対する対抗策を提供することでネットワーク上で稼働する複雑かつ急激にその数を増やし続けるアプリケーションの使用を安全に許可できるようになります。

<http://www.paloaltonetworks.jp>



the network security company™

〒102-0094
千代田区紀尾井町4番3号
泉館紀尾井町3F
電話番号: 03-3511-4050
infoJapan@paloaltonetworks.com
www.paloaltonetworks.jp

Copyright ©2013, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, Palo Alto Networks ロゴ、PAN-OS、App-ID、および Panorama は、Palo Alto Networks, Inc. の商標です。製品の仕様は予告なく変更となる場合があります。パロアルトネットワークスは、本書のいかなる不正確な記述について一切責任を負わず、また本書の情報を更新する義務も一切負いません。パロアルトネットワークスは予告なく本書の変更、修正、移譲、改訂を行う権利を保有します。PAN_TPSB_ALAXALA-JA_102913