Arista ソリューションのホワイトペーパー

クラウド・データセンターのセキュリティ

Software Defined Data Center 保護のための多層防御戦略の適用

INSIDE

現在、多くの組織がクラウドベースの手法をデータセンターで採用しつつあります。具体的には、俊敏性の向上とコストの削減を実現するためのリソースの多層仮想化、密度の高い仮想化の効果を活かすためのネットワーク帯域幅の拡大、ビッグ・データがもたらす大量情報の高度な分析を利用した導入などです。安全なアクセスを実現し、重要なデータやエンドユーザーのプライバシーを保護して、ダイナミック性とパフォーマンスの高いこうしたコンピューティングおよびデータ管理インフラストラクチャで高性能の事業継続性を確保する際の複雑さから、ネットワークおよびデータ・セキュリティの分野では新たな手法が求められつつあります。

新しいデータセンター・セキュリティ要件

政府機関、サービス・プロバイダー、企業の組織を問わず、標的型サイバー攻撃に対する新たなトレンドにより、防御戦略の状況は変化しています。現在、サービス拒否（DoS）、未承認のアクセス、マルウェアの挿入、蔓延するデータ盗用の組み合わせによる、ステルス性の危険な多段階の侵入が流行しています。これらの高度な攻撃は、多くの場合、重要なデータ資産へのアクセス権の取得またはそうしたデータ資産を検出されずに破壊することを目的としたサイバー犯罪者によって行われます。

PwCおよびCSO Magazine*による2013年のサイバー犯罪調査によれば、フォーチュン500に名を連ねる企業は、サイバー犯罪勢力との戦いに敗れています。この調査には、米国のエグゼクティブ、セキュリティ専門家をはじめとする民間企業と公的機関の双方の関係者500名からの回答が記されています。これらの組織は、自己防衛のための最新かつ最善のツールに頼るとともに、サーバー犯罪との闘いが組織に与える経済的な影響を究明しようと試みています。

広く認められているのは、1つのツールだけでは今ある無数の攻撃モードやエクスプロイトからの保護を実現できないという点です。一方、幅広い戦略の利用は10Gbps以上のアクセス速度では経済面で現実的ではありません。ただし、保護すべき貴重なデータ資産を持つ組織は、総合的かつ高コスト効率でスケーリングできる再現性の高い脅威インテリジェンスにより、脅威に関する状況をより明瞭化するとともに、次の方法によるアクティブ防御を実現できます。

- 仮想化クラウド内の境界を持たない分散型の保護
- 持続的なエンドツーエンドの全体的なネットワークおよびシステム・モニタリング
- 可能性のあるすべての脅威アクティビティの検出、ランク付け、相関付け
- コントロールの自動アクティベーションと必要に応じての詳細検査
- セキュリティに関する整備および全体のコストのより適切な管理

ARISTA

セキュリティ脅威に対処するために複数の補完的なツール群を展開する包括的なアプローチは、「多層防御」戦略と呼ばれ、現在の企業やサービス・プロバイダのデータセンターにとって非常に重要になっています。このホワイトペーパーでは、そのようなアプローチの概要を説明します。

最近の SOFTWARE DEFINED DATA CENTER でのセキュリティ規則

運用の急激な複雑化は、多くの重要な状況的要因をもたらしました。その結果、重要な要件に対処するうえでのITおよびセキュリティ運用上の不備が生じています。実際、ネットワーク運用とセキュリティ運用のチーム間で競合するニーズは、セキュリティおよびデータ保護における重大なプロファイル違反につながっています。現在のデータセンターのITおよびセキュリティ運用チームは、以下に対処するために連携する必要があります。

- 制限されたリソースによるサービスの保証と持続性
- 貴重なデータ資産とお客様のプライバシーの保護
- 資産またはサービスの損失が発生する前に攻撃を緩和するための即時対応
- セキュリティ投資のROIの最大化と1/10Gbpsから40/100Gbpsへの移行

現代のデータセンター環境では、「境界のセキュリティ保護」という概念が事実上、無意味なものになっています。また、East-West方向のトラフィック・パターンによるデータセンターの占有と、さまざまな相互作用モデルを用いた分散型のアプリケーション階層により、リソースの分離と保護が困難になっています。データセンター保護のために安全な境界の周辺に保護手段を追加するだけでは、もはや不十分です。ツールの追加、脅威の検出、アクティブな移行に対する統合型のアプローチが不可欠です。

完成されたアプリケーションを提供するために機器間の通信を実現する階層型のサービスでは、現在のデータセンターでの問題の検出と緩和に対する複雑さの階層がさらに追加されます。こうしたアプリケーション・アーキテクチャは、エンドユーザー向けのスケーラブルなアプリケーション・サービスを構築するために、大量のEast-West方向のトラフィックへの依存性を高める可能性があります。さらに、ネットワーク・ベースのAPIによって各階層を対応するクライアントと統合すると、脅威の伝播からの保護が必要になる新たな領域が生じる可能性があります。階層を横断するアプリケーション中心の可視性や、すべてのEast-West方向およびVM間のトラフィックに対する可視性は、データセンターのワークスペースのセキュリティ保護と管理においてきわめて重要な問題になりつつあります。

どこにセキュリティを追加するか

現代のデータセンターを高度な標的型の脅威から保護するには、可視性を向上し、セキュリティ・ツールとネットワーク自体をより適切に統合する必要があります。

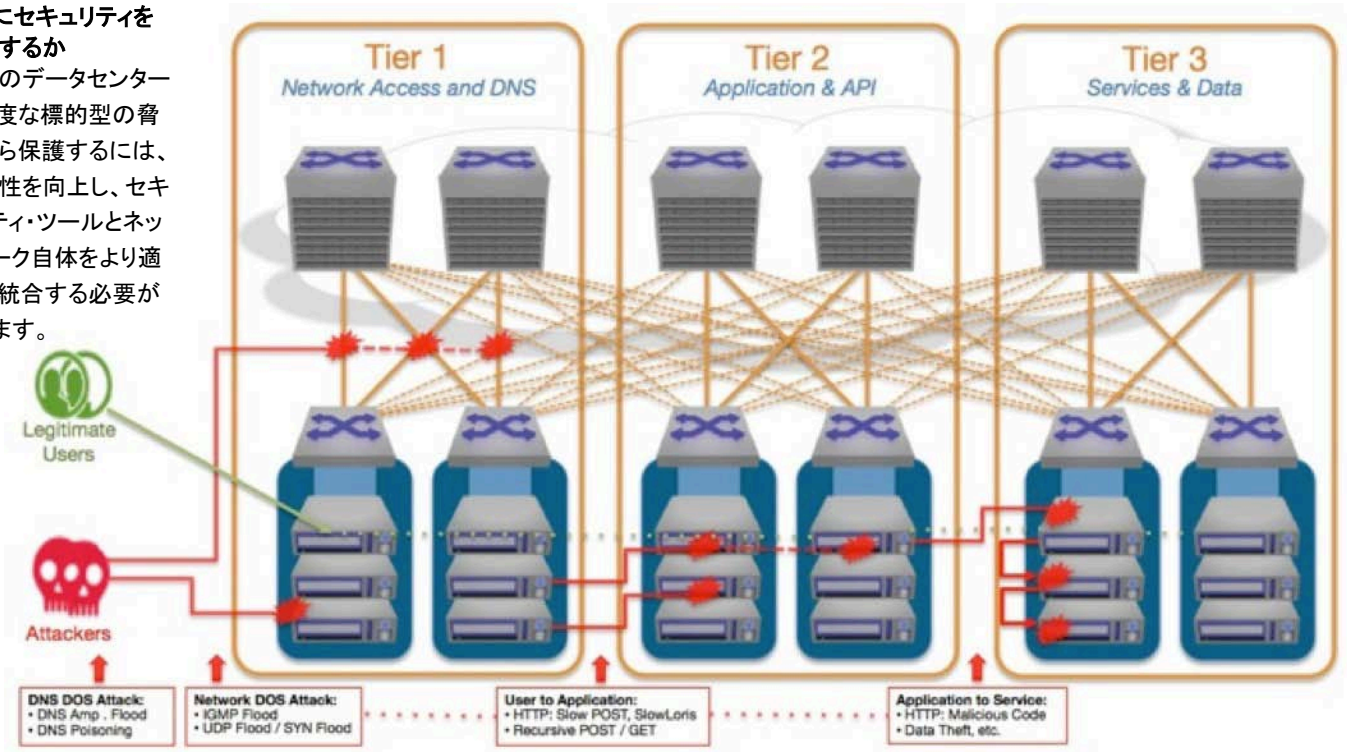

図 1: 新たなセキュリティ課題を生み出すクラウド・データセンターの East-West 方向のトラフィック・パターン

また、Software Defined Data Centerのセキュリティ上の意思決定を複雑にしている重要な要因として、コンピューティング、ストレージ、およびネットワークの仮想化がEast-West方向のトラフィックの可視性に与える影響があります。VM間のトラフィックの増加に伴い、同じデータセンター内の異なるテナントを互いに分離および保護する重要性が高まっています。データセンター・アーキテクチャや、セキュリティ・ツールの展開に対する影響は、甚大になる可能性があります。

どこから着手するか

包括的な可視性、パスの能動的軽減、IT運用の高度なインテリジェンス・ツールの柔軟な配置により、IT組織は、クラウド・データセンターの規模や仮想化が広範囲に及ぶ環境でも新たな脅威に対する効果的な防御を実現できます。アリスタネットワークスのSoftware Driven Cloud Networkingに基づく柔軟なデータセンター・アーキテクチャの利用により、ITおよびセキュリティ運用のチームは、ソフトウェア駆動型の可視性と、ネットワークおよびアプリケーションの可視性に関する帯域内および帯域外のすべての要件を網羅した制御を獲得し、以下のことを行うのに必要な自動化、サービス、包括的な可視性を提供できます。

- 重要なリソースがセキュリティ侵害を受けたときのトラフィックの実用的な再分配を許可
- 攻撃への対応および記録における重要な役割をプログラムによって実現
- プロファイル済みの攻撃パターンに従ったすべてのトラフィックの検査と分析のためのツールへのリダイレクト
- 外部の受信者に送信される情報の追跡（エクスフィルトレーション）
- 危険な状態にあるトラフィックを次世代ファイアウォール・セキュリティのインライン管理と負荷分散およびHAの管理

包括的な可視性

多層防御による脅威防御戦略は、堅実な内部リスク評価から始まります。また、攻撃の進行を示すことが可能な外部のアクションやトラフィック・パターンに対する可視性を必要とします。脅威ベクターの検出と把握を効果的に行うには、すべてのネットワーク・トラフィックの有効なモニタリングおよびプロファイリングを確立して、何が「正常」なのかをまず理解することが重要です。

10Gbpsを超えるネットワークへのアクセス速度は、より低速のデータセンター内のトラフィックをモニタリングするために設計された多くのツールにとって、規模の問題を引き起こしつつあります。アプリケーション・パフォーマンス管理（APM）、ネットワーク・パフォーマンス管理（NPM）、およびセキュリティに関するツールのベンダーは、ますます高速化するネットワークのキャプチャや分析のニーズに、より高速で大規模なプラットフォームで対処していますが、包括的なモニタリングには、まだ手が出せないほどの高いコストがかかる場合があります。

アリスタネットワークスでは、受賞歴のあるArista EOS®ソフトウェアによって強化された高密度でノンブロッキングの10/40/100GbEネットワークを実現するモニタリング用アグリゲーションに対する新しい手法を提供しています。これにより、クラウド規模のモニタリングのコスト効率を1桁改善できます。Arista Data ANalyZer（DANZ）によるソリューションは、異例の柔軟性と精度を備えたスケーラブルなエンドツーエンドのネットワークおよびアプリケーション・モニタリングを実現します。また、既存のサードパーティ・モニタリング・ツールとキャプチャ済みデータとの直接的かつコスト効率に優れた統合を可能にしつつ、スケーリングによって10/40/100Gbpsをサポートします。

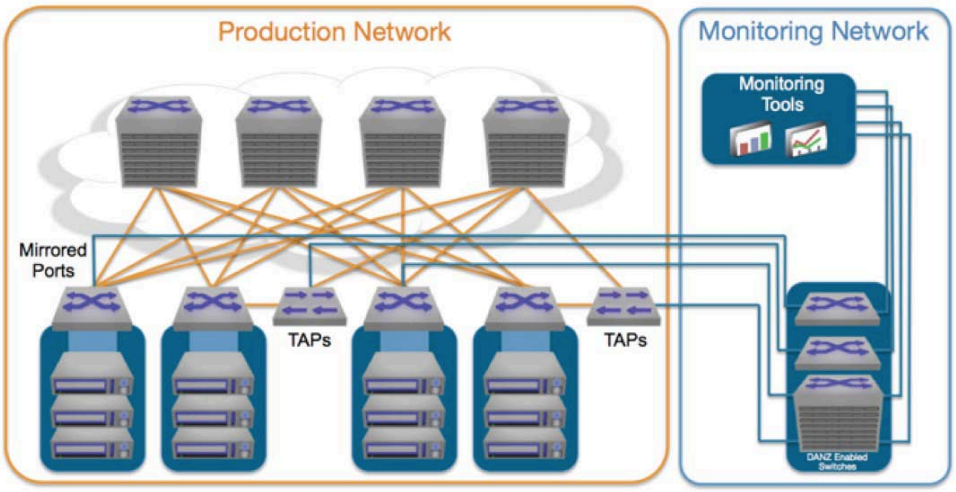

図2: DANZ – リアルタイム分析のための任意のトラフィックへのアクセス

未加工のパケット・データは、セキュリティ、パフォーマンス、およびトラブルシューティングに関する情報のモニタリングにとって最良かつ非常に詳細な情報源となりますが、ほかにも貴重なものになり得る情報源が存在します。これには、sFlowからの粒度の低いフロー分析データ、機器のログから得られる内部のネットワーク運用データ、Splunkから参照できるネットワーク・イベント・メカニズム、Aristaスイッチから得られるLANZキュー分析のような精度データが含まれます。

Arista DANZの機能セットは、基本的に、アリスタネットワークスのデータセンター・クラス・スイッチによる次の機能を実現します。

- 高密度、ノンブロッキング、ワイヤスピードのパケット・キャプチャと高度なトラフィック管理機能:すべてのネットワーク・トラフィックを損失なくモニタリングできるようにします。
- Software Defined Networking(SDN)のサポート:Arista EOSのプログラマビリティによって実現され、特定のネットワーク・フローを適切な分析ツールに振り分けることを可能にします。
- 対称的なフロー単位の負荷分散:インラインのセキュリティおよびモニタリング・ツールのスケーリングにより、セッション単位の認識能力を損なうことなく、テラビット単位のスピードをサポートできます。
- Latency ANalyZer(LANZ)の機能:ネットワーク・オペレーターが重い負荷の下でネットワークの可視性を維持するための適切な措置をとったり、100%の信頼性でセキュリティ監視を保証したりできるように、ツール・ポートでのマイクロバーストや輻輳の検出を可能にします。
- 新たに登場したネットワーク仮想化モデルのサポート(vMotion、VXLAN、NVGREなど):ダイナミック性の高い仮想化およびプライベート・クラウドで任意のワークロードの可視性を維持できます。

トリガーおよび自動化されたアクションは、ネットワーク・インフラストラクチャへのダイレクトなAPIでサポートされます。ログ・モニタリングおよびパケット・キャプチャは、スタッフによる迅速な対応を可能にします。具体的には、電子メールによってチーム・メンバーにアラート通知を行い、対応者が攻撃者のフィンガープリントや進展する攻撃シナリオの詳細をただちに取得できるように、疑わしいトラフィックやイベントログをSIEMおよびトラフィック・レコーディング・ツールに自動的にリダイレクトします。

DANZによるセキュリティ・モニタリングに対する能動的軽減の追加

一般的に、DANZのようなパケット・キャプチャおよびモニタリング・アーキテクチャから未加工のパケット・データを利用するツールは、パフォーマンス分析、問題の特定(トラブルシューティング)、および複雑な階層横断型アプリケーションでの異常の検出を重視しています。しかし、こうしたツール獲得情報を使用した攻撃のアクティブ軽減に対する新しい手法は、迅速なアクティブ軽減を実現するために、Software Defined Network(SDN)のAPIを介してネットワークのプログラマビリティを使用するようになっています。

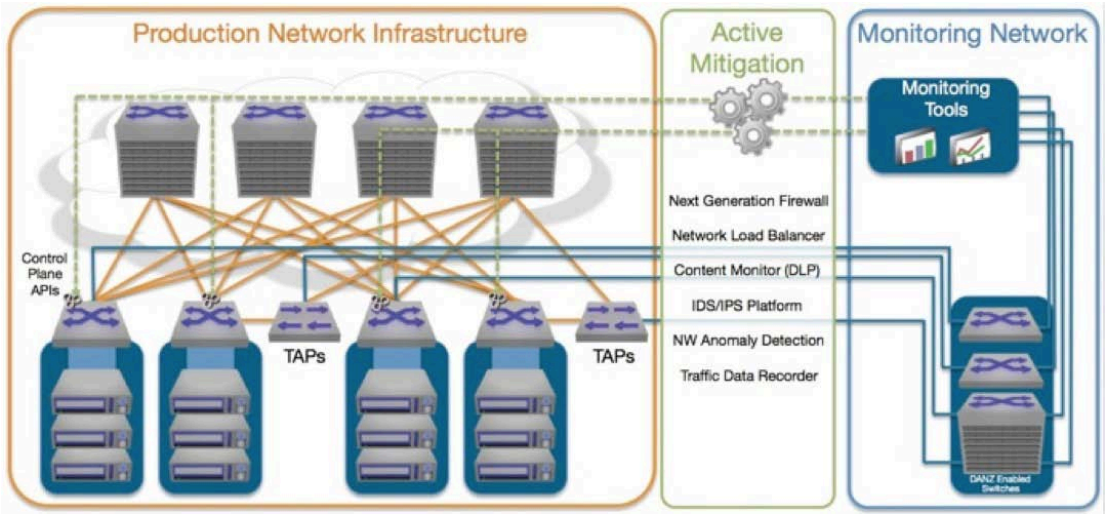

図3:DANZ – 高度なセキュリティ・ツールによる能動的軽減

DANZのような最近のネットワーク・モニタリング・アーキテクチャでは、ツールごとにネットワーク上の特定の対象データへのアクセスを実現したり、最大の効率性が得られるようにツールへの到達前にトラフィックの条件設定を行ったりする、高度なネットワーク・ハードウェア機能を使用しています。帯域外のモニタリングは、インラインのセキュリティ・デバイスだけではレイテンシーが増加して全体的なネットワーク・パフォーマンス効率が低下するおそれがあるインラインの軽減ソリューションを補完することができます。

多層防御での適切なセキュリティ・ツールの選択

実際には、単一のセキュリティ・ツールやベンダーだけをもって、その製品(群)が情報セキュリティの万能的な解決策であると主張することはできませんし、そうすべきでもありません。ほとんどのベンダーは、広く使用されているセキュリティ技法の効果の低さについて、たとえば、シグネチャベースまたは統計ベースの脅威検出の手法には多くの弱点がある、といった正当な主張をしています。現実的なソリューションには、正常な動作のベースラインを設定するための知識、製品、サービスと、次第にスキルを高めながら企業をねらってくる攻撃者に対抗するための軽減ソリューションとの十分に考え抜かれた組み合わせが必要です。現在は、高まる重圧にチームが効果的に対応して攻撃を阻止できるようにするために利用できるさまざまなテクノロジーが存在します。

表1:セキュリティ・テクノロジー – 認められている利点と弱点

セキュリティ・テクノロジー	利点	弱点
ネットワーク・トラフィック・モニター(スニファー、IDS、IPS、パケット・レコーダー、データ分析)	適切な分析によって正常と異常の両方のネットワーク・トラフィック・フローに関する知見を提供できます。トラフィック・レコーダーは、フォレンジック・ツールと同様に有効性が高い場合があります。	保護されたデータ・ストリーム(IPSEC、HTTPS、暗号化トンネル)をモニタリングできず、SIEMデータと組み合わせないとセキュリティ・リスクの十分な解析ができません。
アクティブ・ネットワーク・スキャナー(アプリケーション・ プローブ、ポート・プローブ、 リソースおよび公開済み個人情報(PII)の特定用)	持続的なプローブ処理とモニタリングにより、資産がいつネットワークに配置されたかに関する状況の認識や長期的な証跡が改善されます。	セグメント化された動的かつ高性能のクラウドの展開には多大なコストがかかる場合があります。大量のデータの格納とセキュリティ保護には時間がかかり、複雑な分析では適切なタイミングで結果が得られない可能性があります。
インラインのファイアウォールおよびゲートウェイ(ステートフル・フィルタリング、電子メールのモニタリング、コンテンツのスキャン、アンチウイルスなど)	外側に発生源を持つ未知のゼロデイ・エクスプロイトをキャプチャおよびブロックできる唯一のオプションです。キャプチャによるテナント間の脆弱性や、ホスト単位でネットワークにもたらされるものへの効果が不十分です。	クラウド内の仮想化ゲートウェイおよびファイアウォールはマルウェアの検出や回避には効果がほとんどなく、ゼロデイ・エクスプロイトはシグネチャベースのゲートウェイを迂回できます。
セキュリティ情報およびイベント分析	さまざまなツール、プラットフォームなどから	単体では動作できないので、脅威に関する実

（SIEM）	得られるマクロな（ログ）データに関する統合および分析を実現します。多層防御戦略をごく簡単に管理できる方法です。	際の状況やイベントを検出するには、ほかのさまざまな展開済みツールが必要です。ほかのツールを補完するものと考えてください。

セキュリティ戦略を成功に導く最適な方法は、新たな攻撃ツールとクラス最高の防御との間の競争に適応し続けながら、それぞれの分野で最も優れていることが証明された補完的なデバイスや技法に関する専門知識を集めることです。ネットワークおよびアプリケーション動作の発見やベースライン処理のためのさまざまなツールを使用することで、組織は、リスクを特定し、アクティブな実際の脅威が存在する可能性がある領域に注力することができます。

また、正常なトラフィック・パターンの検出は、攻撃のリアルタイム・フォレンジック調査やプロービングに役立ちます。プロービングにより、攻撃に先立って、実用的な知見を自動化されたポリシーおよびトリガーの準備で使用できます。こうしたポリシーやトリガーは、未知または想定外の攻撃者に対する防御を可能にします。さまざまなモニタリング機能に基づく、IT運用インテリジェンス機能を幅広く使用すると、モノリシックなモニタリング・アーキテクチャしか使用しない場合以上に、ゼロデイ攻撃やAPTのような新たな脅威に対する知見が得られることが示されています。

Arista SDNによる次世代セキュリティのスケーリング

SDNの原則および技法に従うことで、ツールをインライン追加するための要件（ファイアウォールに関するものなど）を満たしつつ、帯域外の分析にわたるグローバルな可視性を提供できます。Arista EOSネットワーク・オペレーティング・システムのSDN機能には、コントローラに依存しないアーキテクチャが含まれています。このアーキテクチャでは、DirectFlowおよびOpenFlow API、OpenStackとの自動化されたクラウド統合、および先進のネットワークおよびコンピューティング仮想化プラットフォーム（VMware vSphere/NSX、Microsoft HyperVなど）を使用しています。

また、セキュリティ・サービスとアリスタネットワークスのVM対応アーキテクチャとの動的なバインディングにより、ダイナミック性の高い仮想化クラウド環境でのセキュリティ持続性を保証できます。移動するワークロードに対応するために仮想化ネットワーク、仮想化されたコンピューティングおよびストレージ・インフラストラクチャが変化するたびに、関連するポリシーやツール設定をネットワーク自動化スクリプトによって動的に設定できます。このモデルは、どのような動的クラウド環境でも持続的な可視性を提供します。持続的なリアルタイム・モニタリング、Arista VM TracerによるVM対応の可視性、および攻撃を受ける可能性があるすべてのポイントでのトリップワイヤのプロビジョニングを使用したアクティブな防御は、大規模な実現が可能です。

Arista DirectFlow Assist（DFA）による動的な多層防御の例

DirectFlow Assist（DFA）は、Aristaスイッチ上で動作するEOS拡張機能です。接続されているインラインまたは帯域外のセキュリティ・プラットフォーム（ファイアウォールなど）のオフロードまたは支援を行うために、アリスタネットワークスのDirectFlow APIを介してフロー・テーブルのエントリを動的に挿入します。ネットワーク転送の統合型管理を実現することで、DFAは、帯域外モニタリング、ディープ・パケット・インスペクション（DPI）、およびその他の分析テクノロジーから得られたインテリジェンスに基づいたネットワーク内での動的なセキュリティ・ポリシーの適用を可能にします。

DFA統合のスケーリングおよびパフォーマンス上の利点により、セキュリティ・プラットフォームでは、静的なインライン展開での最大10～50倍のパフォーマンス向上が可能であり、任意の仮想化またはクラウドベース環境に適用可能なスケーリング・モデルを実現できます。DFAソリューションのユースケースとしては、DDoS攻撃の軽減、次世代ファイアウォールやコンテンツ検査プラットフォームのオフロード、IDS/IPSが特に挙げられます。

- DDoS攻撃の軽減：接続された分析プラットフォームでのDoS検出に基づいてフロー内でパケットを選択的にブロック
- エレファント・フローのオフロード：バックアップなど、信頼できるアプリケーション・トラフィックについては、ファイアウォールをバイパスするためのフロー・エントリーを挿入
- ファイアウォール・スケーリング：ファイアウォールによるDPI検出および分類に基づいてフロー単位のバイパスおよ

攻撃時にDFAで何が起こるのか

攻撃が発生すると、アプリケーションは、SDN対応スイッチで構成されたネットワークに対し、システムやネットワークのパフォーマンスに影響を与えることなく、ハードウェア内の攻撃トラフィック・フローを破棄するように指示することができます。

あるいは、次世代のファイアウォール、IDS/IPSプラットフォーム、またはその他のセキュリティ・ソリューションによる詳しい分析のために、疑わしいトラフィックをリダイレクトすることもできます。能動的軽減に関して指示できるトラフィック操作として、次のものが挙げられます。

- ネットワークでのターゲット・フローのバイパスまたはブロック
- 分析や攻撃者の告発をあとで行うための、疑わしいトラフィックのキャプチャおよび記録
- ターゲットに対する明示的なトラフィックのリダイレクト（ハニーポットまたはトラフィック・レコーダーとして）
- その他のユーザー定義アクション（アラームまたは追加機能を実行するためのほかのプラットフォームのトリガーなど）

びフィルタリングを実現
- プロファイリングと告発の双方のための「ハニーポット」またはおとりプラットフォームへのターゲット・トラフィックのリダイレクト

ファイアウォールのWebコンソール、Arista EOSのAPIを用いたユーザー・プログラム、またはArista CLIを使用すると、DFAによる対象ネットワーク・トラフィック・フローの挿入に使用されるポリシーを設定できます。DDoS攻撃の軽減の場合は、DDoS防御ポリシーが作成され、攻撃ボリュームのしきい値およびロード・プロファイルがファイアウォール上で指定されます。

エレファント・フローの場合は、標準のセキュリティ・ポリシーを設定できます。これらのポリシー内では、「Log at Session Start（セッション開始時にログを記録）」が選択され、DirectFlow Assistプロセスがリッスンしているアリスタスイッチ のUDPポートにメッセージを送信するように「Log Fowarding（ログの転送）」機能が設定されています。

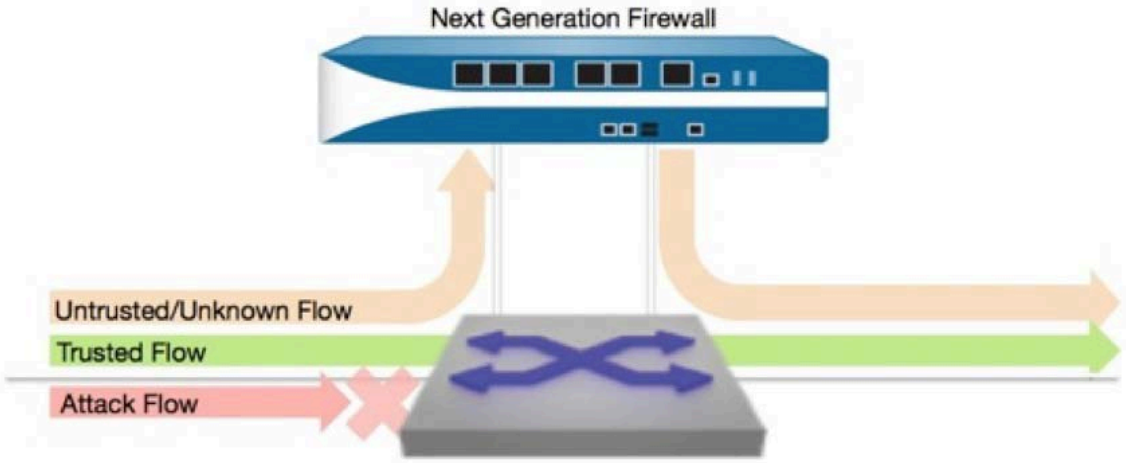

図4：DFAによるSDNファイアウォール挿入の使用

DFAは、ファイアウォールからフロー分類メッセージを受け取ると、そのメッセージを検証したうえで「DFAフロー仕様」の解析を行います。フロー仕様には、一意のフロー名、一致基準、適切なアクション、優先順位、生存期間が含まれています。一致基準には、送信元および宛先のIPアドレス、またフローのタイプやカスタム構成ファイルの設定に応じて、送信元および宛先のレイヤ4ポートおよびプロトコル（ICMP、TCPまたはUDP）が含まれる場合があります。スイッチ上でのアクションは、フロー内のパケットの破棄、またはファイアウォールのバイパスもしくはさらなる分析を行うための指定のスイッチ・ポートへのパケットの出力のどちらかになります。

バイパスされたフローについては、対称性を実現するための反対方向の戻りトラフィック・フロー用に追加のフロー仕様が自動的に生成されます。フロー・エントリでは、エイジングを使用できます。この場合、指定された生存期間が過ぎたあと、フロー・エントリはEOSによって削除されるか、フローがファイアウォールによって明示的に削除されます。

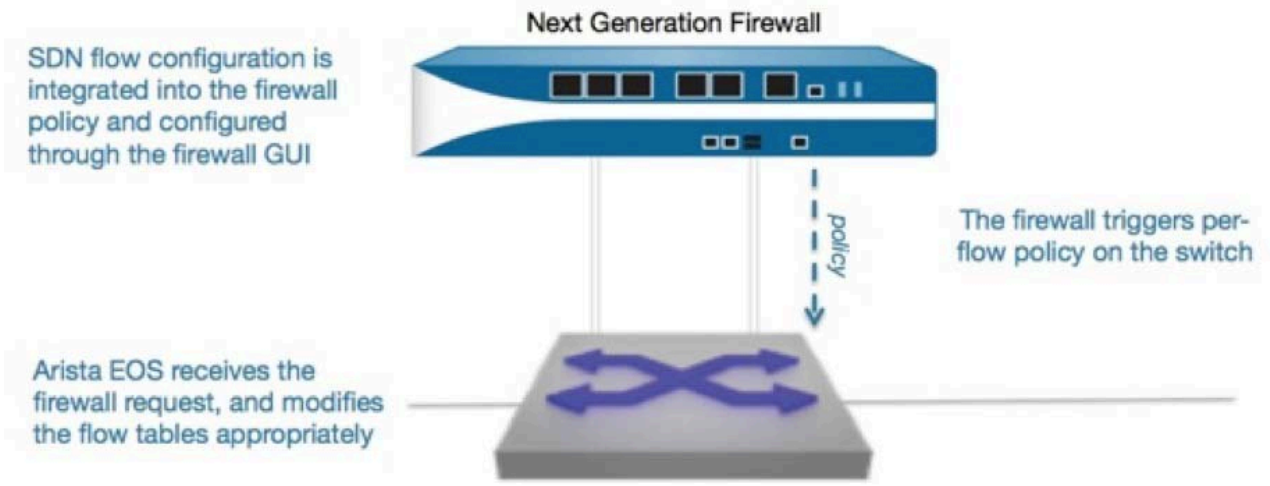

図5:ポリシーの挿入 – トリガーとアクション

DFAは、フロー・テーブル・エントリを作成するためのEOS DirectFlow API設定コマンドのシーケンスをフロー仕様から生成します。続いて、eAPIを使用してこの設定コマンド・シーケンスをEOSに送信します。DFAには、現在アクティブなフローのモニタリング、フローの削除、DirectFlow Assistプロセスの開始および停止を行うためのさまざまなコマンドが用意されたコマンド・ライン・シェルが含まれています。

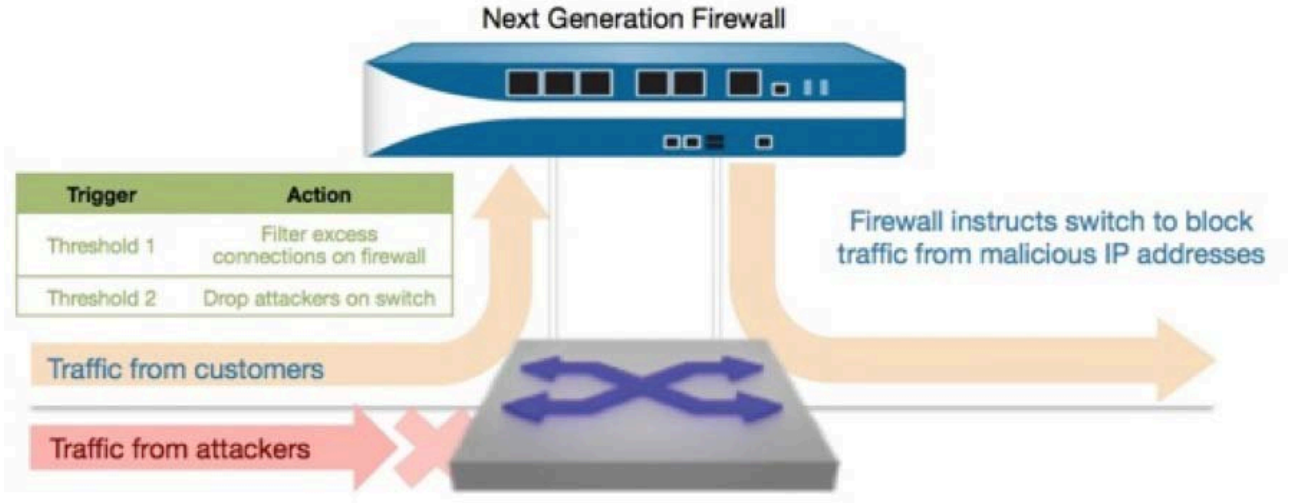

図6:ポリシーの実行 – DoS軽減の例

DFAは、アリスタネットワークスのSoftware Driven Cloud Networking(SDCN)機能の柔軟性を示す例であり、Arista EOSオペレーティング・システムとそのAPIの機能の小さなサブセットを使用しています。Arista SDCNは、クラウド・コンピューティングの勢いを止められないものにしている原則どうしを組み合わせたものです。具体的には、自動化、セルフサービス・プロビジョニング、ネットワーク仮想化と結び付いたパフォーマンスと経済性の両方のリニア・スケーリング、カスタム化に対応したプログラマビリティ、簡素化されたアーキテクチャ、非常に高い効率性といったものです。

まとめ

Arista EOSソフトウェア・プラットフォームの、SDNのプログラマビリティ、高度なネットワーク可視化のためのDANZ、DirectFlow Assist（DFA）に関するクラウド機能の組み合わせは、企業とサービス・プロバイダの両方のデータセンターに対し、ネットワークのセキュリティを最大限に高めるための、他に類を見ないオープンかつクラス最高のソフトウェア基盤を生み出します。ITインフラストラクチャ内の非常にミッション・クリティカル性の高い場所を対象とする新しいアーキテクチャは、サービスの差別化をはかる機会を創出するとともに制御と可視化の機能をセキュリティ管理者やシステム管理者の元に返しつつ、管理とプロビジョニングの簡素化、サービス提供の迅速化、コストの削減を実現します。

セキュリティ・パートナーとの協力によって構築されたアリスタネットワークスのSDCNは、現代のクラウド・データセンターにおける効果的なセキュリティのスケーリングおよび統合という難問に対する包括的なソリューションを提供します。これらのソリューションは現在、使用可能であり、増大しつつある多層防御のニーズに対処しています。

Ponemon Instituteによる2013年の調査によると、データセンターの機能停止のうち特定のサーバーを標的としたサイバー攻撃が原因だったものは、2010年にはわずか2%でしたが、2013年には18%に増えています。これらの攻撃は、一般に入手可能な攻撃ツールの改良とネットワーク速度の増加に伴って急増しており、大量のダミー・トラフィックの生成を容易にするとともに、インライン防御を圧倒しています。Ponemonによれば、これらの攻撃に対処するには、多くの場合、高度な分析およびフォレンジックの専門知識を用いた特殊な技法が必要です。

サンタクララ—本社
5453 Great America Parkway
Santa Clara, CA 95054
電話：408-547-5500
www.aristanetworks.com

アイルランド—国際事業本部
4325 Atlantic Avenue
Westpark Business Campus
Shannon
Co. Clare, Ireland

シンガポール—APAC 統轄オフィス
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

著作権表示ブロックの調整が必要な場合は法務部門にご相談ください。