Contrail Security

製品概要

Contrail 製品シリーズの 1 つである Contrail Security はシンプルかつオープンな完全分散型のクラウド セキュリティ ソリューションであり、ユーザーはあらゆる仮想環境で実行中のアプリケーションを保護することができます。タグやラベル、その他のグループ構成要素で定義された既知のアプリケーション属性に基づくポリシーは、さまざまな環境に幅広く適用できるため、毎回書き換える必要がありません。

Contrail Security ではトラフィック フローに関する重要なインサイトを提供し、全体的なポリシーの削減、適用の簡素化、マルチクラウドのクラウド環境全体にわたる優れた可視性と管理機能の提供につながる新たなセキュリティ パラダイムを構築することにより、セキュリティ フレームワークが強化されています。

製品説明

最高情報セキュリティ責任者（CISO）やセキュリティ管理者は、アプリケーションに対する増え続ける脅威に晒されています。アプリケーションの導入環境が開発、ステージング、実稼働環境、パブリック クラウド環境か、実行環境がベアメタル サーバー（BMS）、仮想マシン（VM）、コンテナ内か、またオーケストレーションが OpenStack、Kubernetes、OpenShift のどのプラットフォームで行われているかは重要ではありません。現在のクラウド環境におけるワークロードのモビリティによって、問題がさらに深刻化しています。頻繁に移行するワークロードを保護する上で新たな問題が発生しています。

その結果、ネットワークの境界は不明確になっています。それに伴いアプリケーションに対する従来の境界ベースのセキュリティ対策では不十分になり、柔軟性に欠け、管理が非常に煩雑で費用のかかるものになっています。現在の分散型で汎用的なアプリケーション開発モデルでは、コンテナ化されたインフラストラクチャの登場やクラウド インフラストラクチャの利用により、パブリック クラウドでもオンプレミスでも同様に、アプリケーションを保護する上で汎用的で俊敏性の高いソリューションが必要とされています。開発者にはアプリケーションのセキュリティ要件を伝える能力が求められ、セキュリティ管理者には開発者に意識させない形でルールやポリシーを追加し、それらの要件を満たす能力が求められています。

Juniper® Contrail™ Security は、セキュリティのルールやポリシーの定義、適用、可視化を実行する新しい枠組みを提供します。OpenStack、Kubernetes や Vmware などのさまざまなクラウド オーケストレーション プラットフォームと互換性があり、L7 ファイアウォールと統合して包括的なセキュリティ ソリューションを提供する Contrail Security では、高度な分析手段を活用してアプリケーション セキュリティに関する詳細な情報を提供するとともに、使いやすい診断機能、豊富なレポーティング機能、カスタム アプリケーション開発機能、マシンによる自動化機能も使用できます。

アーキテクチャと主要コンポーネント

Contrail Security には、Contrail Security Controller および Contrail Security vRouter の 2 つの主要コンポーネントがあります。

Contrail Security Controller

Contrail Security Controller は、物理的に分散した制御プレーンを論理的に一元化された制御プレーンとして Contrail Security ソリューション向けに提供します。また、セキュリティ インテントの定義/表現に使用するインターフェイスが用意されているので、ポリシーの作成にネットワーク座標を使用する必要はありません。Security Controller では、抽象的なセキュリティに関する記述を詳細なセキュリティ構成要素（アクセス コントロール リストなど）に変換した後、アプリケーションのワークロードが存在する各ホスト上のポリシー適用要素にこのセキュリティ構成要素を反映します。

Contrail Security Controller には、オーケストレータやその他の管理システムと Contrail Security ソリューションとの連携を可能にするノースバウンド REST API が用意されています。

Contrail Security Controller は次の 3 つのソフトウェア コンポーネントで構成されています。

- **構成：**構成コンポーネントは Contrail Security の機能を呼び出す API を提供し、コンパイラとしてハイレベルなセキュリティ インテントの記述をローレベルのセキュリティ構成要素に変換します。
- **制御：**制御コンポーネントはゲートウェイとのピアリング用に BGP スピーカーを実装するほか、XMPP（Extensible Messaging and Presence Protocol）を使用してローレベルのセキュリティ構成要素をホスト上のポリシー適用要素に設定します。
- **分析：**分析コンポーネントは、トラフィック フロー、統計データ、ログ、その他のシステムの状態に関する情報など、データを収集するフレームワークを提供します。これらのデータは、GPB、IPFix、SNMP、Netflow、sFlow、syslog などのさまざまなデータ取得チャネルや、Sandesh と呼ばれるプロトコルを使用してホスト上の適用要素から収集します。取得したすべてのデータは可用性の高い Cassandra データベースに保存され、ノースバウンド REST API を使用してクエリーを実行できます。また、収集データからその意味とインサイトを引き出すアプリケーションも提供されます。

Contrail Security vRouter

Contrail Security vRouter はポリシー適用要素で、アプリケーション ワークロードのインスタンス化を行う各ホストにインストールされています。vRouter は VM かコンテナかを問わず、各ワークロードに存在する論理インターフェイスをすべて管理し、vRouter がセキュリティ ポリシーをインラインで適用できるようにします。また、vRouter は選択したトラフィックを L7 ファイアウォールに転送することができます。各 vRouter は、1 組のコントロール ノードと通信してシステムの耐障害性を最適化します。

Contrail Security は Contrail Enterprise Multicloud（マルチクラウドの接続、オーケストレーション、監視、保護を行うデータ センター ソフトウェア）の基本的な構成要素です。

特長とメリット

主な特長

- **インテント駆動型ポリシー：**Contrail Security を使用すると、テナントおよびシステム管理者はポリシーを記述する際にセキュリティ要件を簡単な英語で表現することができるため、ネットワーク座標を使用する必要はありません。
- **ワークロードのタグ付けとタグ表現：**ポリシー ステートメントは、ネットワーク座標を使用する従来の方法ではなく、アプリケーション属性を記述するタグ表現で記述されます。これにより、システム管理者やテナントは、動的に変化し続けるネットワーク座標を把握し、監視する必要がなくなりました。
- **完全分散型ファイアウォール：**Contrail Security は、アプリケーションのワークロードが開始される各ホスト上に vRouter のポリシー適用コンポーネントを配置します。vRouter はクラウド インフラストラクチャに組み込まれているため、テナントが Contrail Security を利用する際に、使用しているアプリケーションに変更を加える必要はありません。vRouter は完全分散型の L4 までのセキュリティを各ホストに提供します。
- **L7 ファイアウォールへのリダイレクト：**Contrail Security は、完全に動的、かつプログラム可能な形で、選択したトラフィックを L7 ファイアウォールに転送します。
- **分析：**Contrail Security は、サポート対象となる多様なデータ取得プロトコルを使用して、アプリケーション、インフラストラクチャ、ネットワーク、セキュリティのさまざまな分析データを収集する高度なフレームワークを提供します。分析データの収集フレームワーク上に作成したアプリケーションによって、収集データから有用なインサイトを得ることができます。
- **可視化：**ユーザーは、さまざまなアプリケーションやアプリケーション コンポーネント間のトラフィック フローに加え、違反の有無のステータスなど、関連するセキュリティ ポリシーを視覚的に確認できます。

主なメリット

- **多方向のポリシー ステートメント：**Contrail Security では、ポリシーの作成、レビュー、承認を一度実行するだけで、そのポリシーをすべての環境に適用することができるため、ポリシー ステートメント数の大幅な削減、管理の簡素化、セキュリティ コストの大幅な抑制につながります。
- **包括的なセキュリティ機能：**接続とファイアウォールによる防御を通して L7 までのセキュリティを実現し、単一の管理ポイントからエンドツーエンドの保護を実行できます。また、L4 ～ L7 のセキュリティが完全分散形式で提供され、すべてのホストで利用できるため、攻撃対象領域を最小限に抑えることができます。
- **実用的なインサイト、可視性、可視化：**ユーザーは、アプリケーション、インフラストラクチャ、ネットワーク（アンダーレイおよびオーバーレイ）、セキュリティのさまざまな面を 1 つの製品の単一の管理ポイントから包括的に可視化できます。
- **リスクを抑え、コンプライアンスを強化：**Contrail Security は、水平方向および外部からのさまざまな脅威を、包括的なエンドツーエンドをカバーする最新のアプローチで防御することにより、リスクを軽減し、コンプライアンスを向上させます。

主な機能

- **異種混在環境全体をカバーするオープン ソースおよびオープン スタンダード：**Contrail Security は、ゲスト アプリケーション VM ではなく、カーネル常駐型のソフトウェア ポリシー適用要素をホストにインストールするため、テナント アプリケーションのワークロードを作り変えたり、変更する必要がなくなります。これにより L4 までの完全分散型ファイアウォールが実現します。また、複数の L7 ファイアウォールと統合して、選択したトラフィックをリダイレクトすることができます。
- **インテント駆動型（Software-Defined）セキュリティ：**Contrail Security では、タグ表現を使って簡易な英語でセキュリティ インテントを指定できるため、ネットワークの構成要素を指定する必要はありません。Contrail Security Controller はこのハイレベルのインテントを具体的なセキュリティ ACL に変換します。
- **可視化：**Contrail Security の豊富なインターフェイスにより、トラフィック フローの詳細を可視化し、それをアプリケーション トポロジーにマップできます。また、このインターフェイスにより、表示されたトラフィックを対応するセキュリティ ポリシーや表示されたボリュームに関連づけることができます。適切な可視化を設定するため、下位レベルの詳細情報を指定することができます。

- **分析：**Contrail Analytics Engine は、構造化/非構造化データの大規模な取得やクエリーを実行することを想定して設計されています。具体的なデータとしては、アプリケーションの使用率、インフラストラクチャの利用状況、システム ログ、セキュリティ イベント、セキュリティ ログ、さらには、フロー、レイテンシ、ジッターなどのネットワーク統計情報などがあります。また、GPB、syslog、IPfix、sFlow、SNMP などの複数の取得チャネルや手段に対応しています。すべての取得データは、可用性の高い Cassandra データベースに保存され、その後の情報検索および処理に使用されます。高度なクエリー インターフェイスはもちろん、REST API や機能が豊富な GUI を使用することで、Analytics Engine が取得した情報を抽出することができます。

  Analytics Engine が提供するリアルタイムの情報および履歴情報によって、ユーザーはより優れたインサイトを入手し、インフラストラクチャで発生している問題を容易に診断できるようになります。また、REST API や Hadoop といった最新技術を利用して通知やインフラストラクチャを自動化するカスタム アプリケーションを作成することもできます。

  さらに Contrail Security は、分析フレームワークを活用してオーバーレイをアンダーレイと関連づけたり、他の機能内の統計的な異常を検知する、付加価値のあるアプリケーションも複数提供しています。

Contrail Security の使用例

Contrail Security ではサービス プロバイダーや企業向けに動的で拡張性に優れたネットワークの仮想化、そして分散型かつインテント駆動型のセキュリティ ソリューションが提供されるので、次のことが可能になります。

- プライベート/パブリック クラウド インフラストラクチャ全体でアプリケーションをシームレスに保護する
- ネットワークの仮想化により分離したテナントを保護するとともに、ポリシーを新たに作成せずに複数の環境で再利用する
- ワークロードのモビリティや拡大し続けるネットワークの境界に対応する
- アプリケーションの責任者またはセキュリティ管理者のインテントによって指定された L7 ファイアウォールを選択し、不審なトラフィックをリダイレクトする
- 接続機能と包括的なセキュリティ機能を統合し、異種混在環境全体に適用する
- 優れたアプリケーション ドメインの可視化により、違反者および違反などを発見し、問題が発生する前に対処する
- 履歴調査およびコンプライアンスに対応するため、インサイトを保持し、過去の記録についてクエリーを実行できるようにする

仕様

システムの推奨事項と動作環境

- オーケストレーション システム：OpenStack、Kubernetes
- ハードウェア：64 ビット デュアル x86 プロセッサー、最小メモリ 12 GB RAM
- ストレージ：30 GB SATA（Serial Advanced Technology Advancement）、SAS（Serial Attached SCSI）、またはソリッド ステート ドライブ（SSD）、ボリューム ストレージ：ディスク x 2（2 TB SATA）
- ネットワーク：1 GB インターフェイス カード（1）
- OS：Linux OS（CentOS、RHEL 6.4、Ubuntu 13.x）

ジュニパーネットワークスについて

ジュニパーネットワークスは、世界をつなぐ製品、ソリューション、サービスを通じて、ネットワークを簡素化します。エンジニアリングのイノベーションにより、クラウド時代のネットワークの制約や複雑さを解消し、お客様およびパートナーの皆様が日々直面している困難な課題を解決します。ジュニパーネットワークスは、世界に変革をもたらす知識の共有や人類の進歩のリソースとなるのはネットワークであると考えています。私たちは、ビジネス ニーズにあわせた、拡張性の高い、自動化されたセキュアなネットワークを提供するための革新的な方法の創造に取り組んでいます。

米国本社
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
電話番号：888.JUNIPER（888.586.4737）
または +1.408.745.2000
FAX：+1.408.745.2.100

アジアパシフィック、ヨーロッパ、中東、アフリカ
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
電話番号：+31.0.207.125.700
FAX：+31.0.207.125.701

www.juniper.net

1000621-002-JP 2018 年 7 月