

At-a-Glance

Viptela Secure Extensible Network (SEN) ソリューションは、セキュアなエンドツーエンドのネットワーク仮想化を実現する、業界をリードするプラットフォームです。企業は SEN ソリューションを活用することにより、ルーティング、セキュリティ、一元管理ポリシー、オーケストレーションを完全に統合した大規模ネットワークを構築できます。最終的に完成するネットワークは、ビジネスと IT 間の分断が排除され、容易に管理できます。

今日のネットワークの技術的な課題

今日の企業は、レガシー ネットワーク インフラストラクチャの複雑化に伴って、大きなビジネス上の課題に直面しています。企業全体に接続性を提供するには、次の状況が伴います。

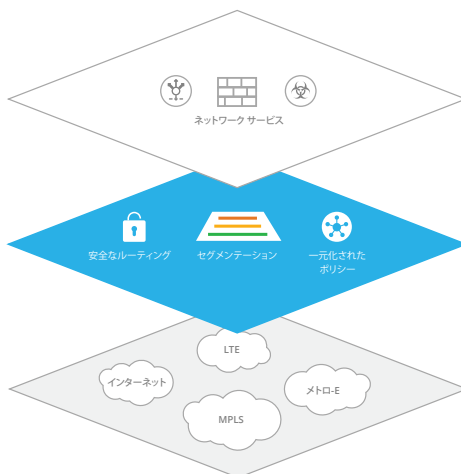
- 複数の異なるネットワーク (MPLS、メトロ イーサネット、SSL over Internet、IPsec) を管理する
- ネットワークの各ホップにポリシーと制御を組み込む
- ネットワーク全体の不十分なセグメンテーションと弱い暗号化ポリシーに起因するセキュリティの脆弱性に対処する
- ネットワーク固有の動作を必要とする新しいアプリケーションの導入に関連するプロビジョニングに時間がかかる
- 複雑性が分散しているために、簡単な変更要求の完了に数ヶ月かかる
- パブリック クラウド、VDI、帯域幅を消費するアプリケーションのパフォーマンスの問題が発生する

コストの増加、セキュリティの低下、新サービス導入の遅延を伴わずに、エンドツーエンドの仮想化のメリットを提供する大規模なネットワークを構築するには、新しいアプローチが必要です。

Viptela のアプローチ

Viptela SEN ソリューションは、5 つの重要なアーキテクチャ要素を利用してこうした技術的課題に対処します。

1. トランスポートの独立性を有効にする
2. ルーティングされるすべてのエンドポイントの安全性を自動的に確保する
3. エンドツーエンドのネットワーク セグメンテーションを提供する
4. 一元管理コントローラでポリシーを施行する
5. ネットワーク サービスのアドバイズメントを有効にする



メリット

- 企業のフットプリントをどこにでも安全に拡張
- キャリアのサービスから独立して、任意のトランスポート ネットワークを自由に選択
- パブリック クラウドおよびインターネット向けにパフォーマンスを最適化
- アクセス制御およびネットワーク ポリシーを一元的に施行
- ビジネス部門、コンプライアンス、ビジネス パートナーに合わせてネットワーク全体をセグメンテーション
- ネットワークベース サービスを一元管理

図 1: Viptela Secure Extensible Network

コンポーネント

Viptela SEN ソリューションの 4 つの主要なコンポーネントは、vSmart コントローラ、vEdge ルータ、vBond Orchestrator、vManage 構成/監視システムです。

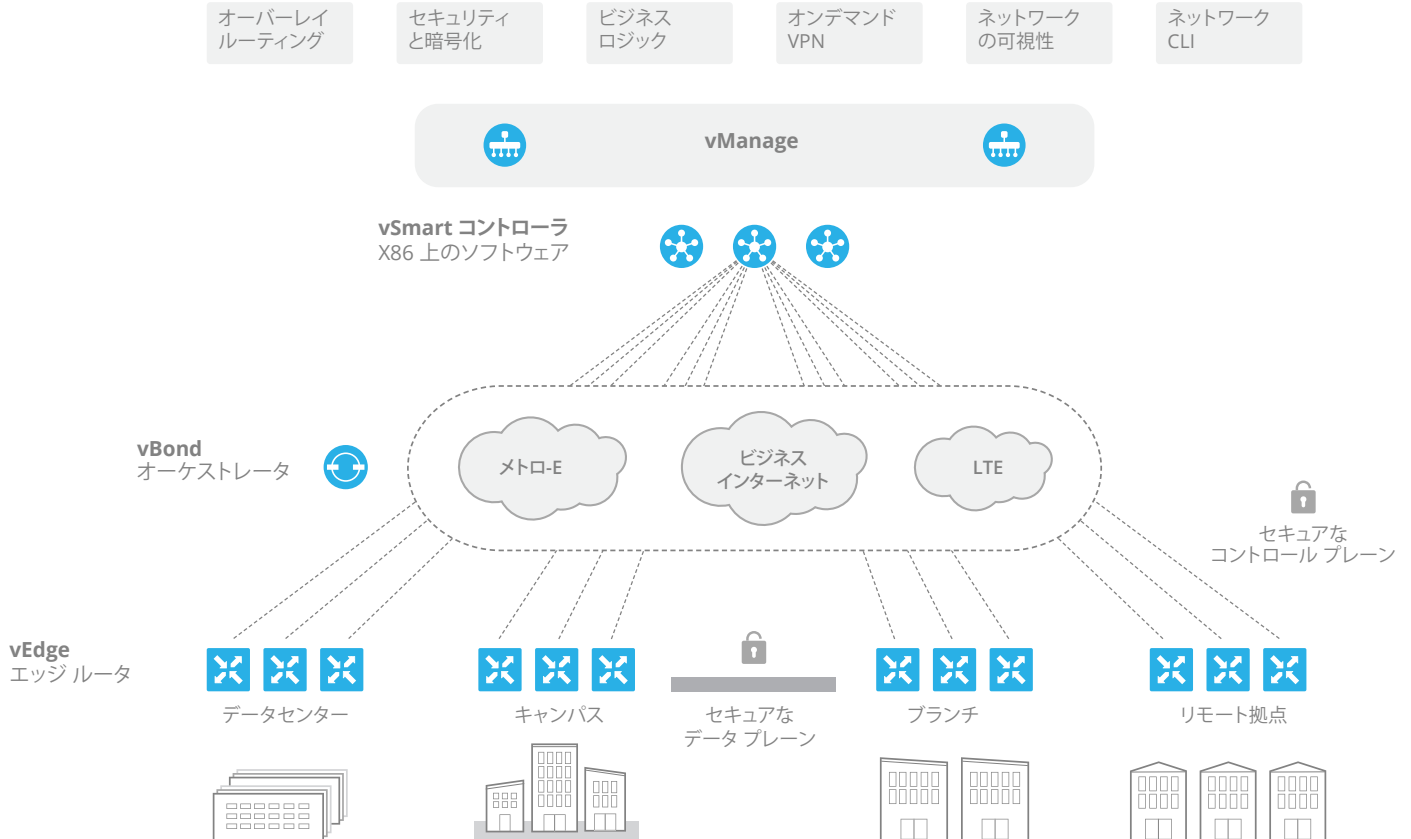


図 2: Viptela SEN ソリューションのコンポーネント



vSmart コントローラ

vSmart コントローラは、オーバーレイ ネットワークの中枢部です。ネットワーク内の各 vEdge ルータへのセキュアな DTLS 接続を確立し、Overlay Management Protocol (OMP) を実行してルート、セキュリティおよびポリシー情報を共有します。vSmart コントローラの一元管理ポリシー エンジンにより、ルーティング情報、アクセス制御、セグメンテーション、エクストラネット、およびサービス チェイニングを操作するため豊富なインバウンド/アウトバウンド ポリシー構成が提供されます。

vSmart コントローラは、2 基の vCPU と 4GB のメモリ (最小構成) を搭載する VMware vSphere ESXi ハイパーバイザ上で動作する仮想アプライアンスです。事前にインストールされたセキュリティクレデンシャルを使用して、ネットワークに参加する前に新しい各 vEdge 端末を自動的に認証します。



vEdge ルータ

vEdge ルータは、オーバーレイのコントロールおよびデータ プレーンに加えて、OSPF、BGP、QoS、ACL、ルーティング ポリシーなどの標準的な機能を実行する、フル機能を備えた IP ルータです。各 vEdge ルータは、vSmart コントローラとの間にセキュアな DTLS セッションを自動で確立し、SEN 内の他の vEdge ルータとは標準 IPsec セッションを確立します。vEdge ルータには、次の 2 つのタイプがあります。

| | VEDGE1000 | VEDGE2000 |
|--------------------|--------------------------|--|
| 寸法 | ハーフ幅、1RU | フル幅、1RU |
| 暗号化容量 | 1 Gbps | 10 Gbps |
| 固定ポート | GE SFP (10/100/1000) X 8 | GE SFP 固定 (10/100/1000) X 4 |
| 着脱可能インターフェイス モジュール | 該当なし | 2 つのモジュール (GE SFP X 8 または 10GE SFP + X 2 から選択) |



vBond Orchestrator

vBond Orchestrator は、vEdge ルータ上で動作するソフトウェア モジュールです。自動的にコントロール プレーンの起動プロセスを効率化し、初期認証を実行し、vSmart コントローラと vEdge ルータ間の接続性を調整します。vBond Orchestrator は、NAT 背後の Viptela デバイスと幅広いネットワークとの通信を可能にする上で重要な役割を果たします。



vManage ネットワーク構成/監視システム

vManage は、Viptela SEN ソリューションの構成管理と監視を可能にする一元化システムです。2 基の vCPU と 8GB のメモリ (最小構成) を搭載する VMware vSphere ESXi ハイパーバイザ上で動作する仮想アプライアンスです。

使用例



トランスポートに依存しない VPN

Viptela SEN ソリューションは、任意の基盤トランスポートを介したコスト効率の高いセキュアな IP ファブリックを提供します。



B2B パートナー ネットワーク

動的なパートナー エコシステムを有する企業は、任意のトランスポート ネットワークを介して、迅速にビジネス パートナーのオンボーディングを行うことができます。



エンドツーエンドのネットワーク セグメンテーション

異なるビジネス部門や異なるビジネス パートナー間の機密性が高いトラフィックは、エンドツーエンドのセグメンテーションによって安全性を確保できます。



大規模な暗号化

Viptela SEN ソリューションは強力な暗号化機能を提供します。自動化されたキー管理と端末認証を通じて、あらゆるネットワーク インフラストラクチャへの接続を保護します。



地域インターネットへの出口

企業は、地域インターネットへの出口ポイントを有効化することにより、クラウド、VDI、インターネットアプリケーションの最適なユーザ エクスペリエンスを提供できます。



ネットワーク サービスの挿入

ファイアウォール、IPS、ロード バランサなどのネットワーク サービスは、一元化された拠点で統合でき、トラフィックは、容易にポリシーを変更できるこれらのサービスを通じてルーティングできます。

特長

| 特長 | メリット |
|---------------------------|--|
| ポリシーの一元化と分散型適用 | Viptela Overlay Management Protocol (OMP) は、Viptela ネットワークの各セグメントのルートおよびポリシー情報をすべてを一元的に処理します。この機能によって、最大級のトポロジを構築する際のボトルネックが解消され、ネットワークに対する変更に対応できるようになります。 |
| セキュアな起動を自動化 | vEdge ルータには、署名付き証明書を内蔵する信頼されたプラットフォーム モジュール (TPM) チップが出荷時にインストールされています。この組み込みセキュリティ機能により、ネットワークに参加する任意の新しい vEdge ルータの自動認証を確実に行えるようになります。この機能は、数万台のエンドポイントを使用する場合にも大きな利点です。 |
| 制御およびデータトラフィックの暗号化 | Viptela ネットワークのデフォルトの運用モードは、「安全」および「暗号化」です。キーは、パフォーマンスに影響を与えずに、必要に応じて頻繁にローテーションできます。SEN は、セキュリティを確保しながら、数万のネットワーク エンドポイントと 100,000 以上のルートに拡張できます。 |
| 冗長性を備えたスケールアウト アーキテクチャ | 複数の Viptela デバイスを追加することにより、容量を拡張し、冗長性を確保できます。このアーキテクチャは、オーバーレイ ネットワークのコントロールおよびデータプレーン両方の複数の障害への耐性を備え、99.999% の可用性を効率的に提供します。 |
| エンドツーエンドのネットワーク セグメンテーション | エンドツーエンドのネットワーク セグメンテーションは、コントロールプレーン プロトコルを追加せずにすばやく有効化できます。このセグメンテーションは、ネットワークを外部の攻撃者から強力に保護するとともに、複数のアプリケーション セグメント内で内部を安全に分離します。 |



Viptela Secure Extensible Network

Viptela ソリューション、およびこのソリューションがネットワークにもたらすメリットの詳細については、sales@viptela.com までお問い合わせください。



Viptela Inc., San Jose, California, USA
Tel: 800 525 5033, www.viptela.com

Copyright © 2014 Viptela, Inc. All rights reserved. この製品は、米国および国際著作権法および知的財産法によって保護されています。Viptela, Inc の製品は、<http://www.viptela.com> に示した 1 つもしくはそれ以上の特許の対象です。Viptela, Inc. は、Viptela, Inc. の米国およびその他の司法管轄区域における登録商標または商標です。本書に記載するその他のマーク、名称は、それぞれの会社の商標です。