ホワイトペーパー

仮想化環境における SSLオフロードと高速化

～クラウドでの高パフォーマンスを実現するために～

APVシリーズ アプリケーションデリバリコントローラ

はじめに

クラウドへの移行によってデータセンターの設計は大きく変化しましたが、リソースとアプリケーションのデリバリのメカニズムも様変わりしました。リソースの集約と迅速なスケーリングを目的として、多くのデータセンターが、仮想化したサーバ、ファイアウォール、アプリケーションデリバリコントローラ(ADC)から成る仮想インフラストラクチャを導入しています。

それだけでなく、クラウドコンピューティングがもたらした大きな変化は、ビジネスに欠かせない情報の共有と使用の方法も変えることとなりました。情報が従来のIT環境の中だけに存在するとは限らなくなったのです。このような状況のなかで、SSL/TLSデータ暗号化はミッションクリティカルな機密データをインターネット上で送受信するときのセキュリティ確保を目的として頻繁に利用されています。

転送中のデータのセキュリティを確保する

SSL/TLSデータ暗号化は、転送中のデータのセキュリティ確保の方法として事実上の標準となっています。クラウドベースの仮想ADCアプライアンスは、ホストCPUのリソースを活用してソフトウェアベースのSSL/TLSデータ暗号化をサポートしており、多くの場合は、リソースの性能が強化されて十分なパフォーマンスとスループットを得られるようになっています。たとえば、IntelベースのCPUでは最近、AES-NI(Advanced Encryption Standard New Instructions)がサポートされるようになり、SSL/TLS暗号化/暗号化解除の速度が向上しています。

しかし、ソフトウェアベース(仮想)のSSL/TLSのパフォーマンスは一般的に、ハードウェアベース(専有型物理アプライアンス)のソリューションを大幅に下回ります。たとえば、Arrayの仮想ADCであるvAPVの平均的なSSL/TLS処理能力は、鍵長2048ビットの場合で600 TPS(トランザクション/秒)前後です。他の仮想マシンも同じCPUを使用している場合は、リソース競合が原因でスループットがさらに低下することが考えられます。

さらに、重要な注意事項が1つあります。SSL/TLSの終端デバイスでディープパケットインスペクションを行うには、テキストが平文でなければなりません。たとえば、ADCがインテリジェントなアプリケーションルーティング、フィルタリング、サーバパーシステント(Sticky)などの目的でアプリケーションセッションID、Cookie、URLを探す場合です。したがって、SSL/TLS終端処理を行うには処理能力の増強が必要になります。特に、新しいセッションID交換のときです。

複数のvAPV仮想ADCアプライアンスを追加すると、SSL/TLSのパフォーマンスのスケールアップに役立ちますが、コストもセットアップの複雑さも増大します。加えて、複数の仮想ADCアプライアンスが共有CPU上で稼働するのでは、FIPSハードウェアセキュリティモジュール(HSM)の要件を満たすことはできません。米国連邦政府が定める情報処理標準であるFIPS(Federal Information Processing Standard)は、他の国でもデータセキュリティの標準として採用されています。

仮想/専有ハイブリッドモデルによるSSL/TLSオフロード

仮想環境におけるSSL/TLSのパフォーマンスを保証する必要があり、且つ性能拡張（スケーラビリティ）も求められる場合、全てを仮想化するモデルが適さないことがあります。この場合、仮想/専有アプリケーションデリバリコントローラ（ADC）のハイブリッドなモデルが効果を発揮する可能性があります。このモデルは、コストおよび柔軟性に優れた仮想ADCと、パフォーマンスおよびスループットを保障できる専有型(ハードウェア)ADCアプライアンスとを組み合わせるというものです。

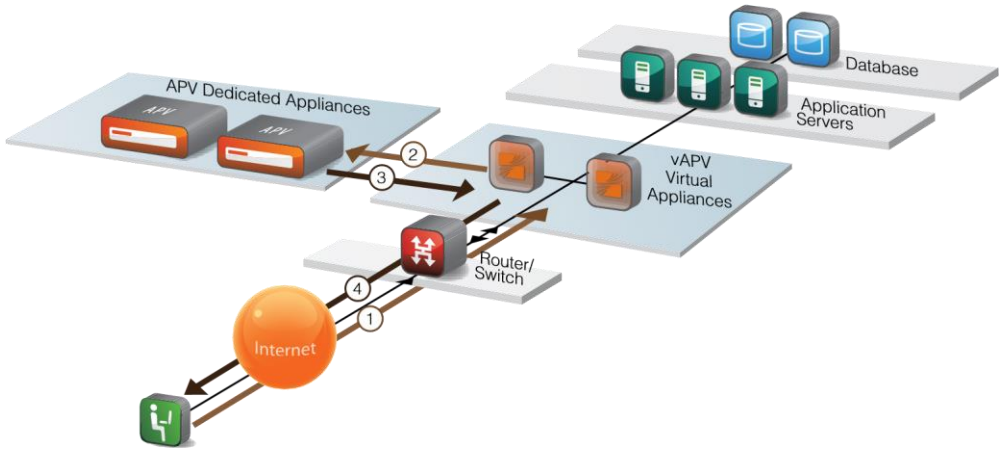

図1：vAPVのSLB仮想サービスを使用する仮想/専有ハイブリッドADCモデル

モデルによって異なりますが、Arrayの専有型ADCであるAPVシリーズでの2048ビットSSL処理能力は2,500～70,000 TPS（トランザクション/秒）となっています。加えて、ユニット当たりのSSL/TLS接続/セッション数は最大400万、暗号化データスループットは最大25 Gbpsです。このハイブリッドモデルでは、SSL/TLS処理の速度が向上する（その結果として仮想ADCアプライアンスおよびサーバへの負荷が低下する）だけでなく、アプリケーションのキャパシティも増大します。必要に応じてより多くのSSL/TLS接続に対応できるからです。さらに、専有型のArray APVシリーズアプライアンスは、FIPS HSM準拠が可能です。

仮想/専有ハイブリッドSSLオフロードモデルのしくみ

上の図に示した仮想/専有のハイブリッドなSSLオフロードモデルのしくみは次のとおりです。

1. HTTPリクエストの場合と同様に、クライアントはHTTPS（TCP宛先：ポート443）リクエストを開始します。このリクエストはvAPV仮想アプライアンスに転送されます。
2. SSLは外部ハードウェアにオフロードされているので、このHTTPSサービスリクエストは専有型のAPVシリーズアプライアンスに転送されます。この転送は、vAPV仮想アプライアンスのサーバ負荷分散（SLB）仮

想サービスを使用して（TCPポート443）、またはルータ/スイッチによって（ポリシーベースのルーティング）行われます。

3. 専有型APVシリーズアプライアンスは、SLB仮想サービス（TCPSポート443）を使用して終端処理を行い、クライアントからのHTTPSリクエストの暗号化を解除して、vAPV仮想アプライアンスへのHTTP接続/転送リクエスト（HTTPポート80）を作成します。
4. SLB設定に基づいて、vAPV仮想アプライアンスは実サーバの1つを選択してクライアントHTTPリクエストを転送します。
5. 逆方向には、サーバのレスポンスをvAPVが受信すると、vAPVはそれを専有型APVシリーズアプライアンスに転送します。専有型APVシリーズアプライアンスは、このサーバレスポンスを暗号化し、”HTTPSレスポンス”としてvAPV経由でクライアントに送信します（リクエストがルータ/スイッチ経由でルーティングされたものである場合は、レスポンスも同じ経路でルーティングされます）。

以上に説明した構成は、企業での導入形態として一般的なものの1つです。しかしながら、サービスプロバイダがSSLオフロードを導入し、サービス（Infrastructure-as-a-Serviceモデル）として提供することも可能です。データセンターエッジに専有型APVシリーズアプライアンスを配置し、サービスプロバイダが管理します。これを複数のテナントにて共有する形でSSL処理のオフロードと高速化を行うこともでき、必要に応じてスケーリングも可能です。

仮想/専有ハイブリッドSSLオフロードモデルの主な特徴

仮想/専有ハイブリッドSSLオフロードモデルには、パフォーマンス向上やスケーリング、アプリケーションのセキュリティ強化に帰依する次のような特徴があります。

- **セキュアアプリケーションの高速化**：コンピューティングリソースを多用するSSL処理は高パフォーマンスの専有型APVシリーズハードウェアで実行されるので、鍵交換や暗号化/暗号化解除などの処理に伴う遅延時間が大幅に短縮されます。
- **スケーリング能力の向上**：このハイブリッドモデルでは、セキュアアプリケーションのキャパシティと可用性のスケールアップも、SSLオフロードを通して容易にできるようになります。加えて、冗長化とアプリケーションヘルスチェックによってアプリケーションの可用性が向上します。
- **アプリケーションセキュリティの強化**：Arrayの専有型と仮想のどちらのADCアプライアンスも、独自の高パフォーマンスSSL処理スタックを採用しており、SSL/TLSプロトコル攻撃への耐性があります。ほとんどのベンダーのADC製品はOpenSSLを採用していますが、OpenSSLについては最近になってHeartbleed、Bash、MitM（Man-in-the-Middle）などの多数の脆弱性が報告されています。このハイブリッドモデルは多層ネットワークセキュリティと完全なリバースプロキシの機能も備えているため、クライアントリクエストのディープスキャンが可能なアプリケーションファイアウォールとしても機能します。

導入と管理の容易さ

仮想版のvAPVと専有型APVシリーズのアプライアンスは緊密に連携し、どちらも同じソフトウェアを実行します。このことが、以下のようにハイブリッドモデルの導入と管理の面において、さらなるメリットをもたらします。

- **ADCの統合**：仮想と専有型のADCアプライアンスが一体となり、高度なレイヤ4-レイヤ7サーバ負荷分散、アプリケーションスクリプティング、キャッシングと圧縮、レイヤ7セッションのパーシスタンス、Webアプリケーションファイアウォール、およびアクセス制御リスト（ACL）の機能を実行します。
- **SSLブリッジモード**：シンプルなネットワーク構築だけでエンドツーエンドのセキュリティを確保します。大がかりなネットワーク再設定は不要です。
- **SSLクライアント証明書の管理**：仮想と専有型を組み合わせることによって、クライアント証明書検証、各国言語サポート、アクセス制御、柔軟なクライアント情報転送の機能を高パフォーマンスで実行できます。また、外部認証局（CA）経由での証明書検証についても、証明書失効リスト（CRL）およびOCSP（Online Certificate Status Protocol）による検証の全機能に対応できます。
- **その他のセキュアプロトコルのサポート**：HTTPSの他にも、TCPS上でSSL暗号化機能を使って運用可能なプロトコルを多数サポートします。プロトコルの例としては、FTPS、POPS、SMTPS、IMAPS、LDAPS、NNTPSがあります。

まとめ

仮想化クラウドとデータセンターの環境において、ハイブリッド仮想/専有ADCモデルを採用すると、SSL/TLS処理のパフォーマンスを保証するとともにスケーリングも可能になります。このモデルは、経済性および柔軟性に優れた仮想vAPV ADCアプライアンスと、パフォーマンスが保障できる専有型APVシリーズADCを活用します。このモデルでは、SSL/TLS処理をサーバと仮想ADCアプライアンスの両方からオフロードできるだけでなく、アプリケーションのキャパシティと可用性も増大します。他の方法と比較すると、セキュアなSSL/TLS接続をより多く処理できるからです。加えて、専有型APVシリーズアプライアンスはFIPS HSMに準拠するための要件も満たすことができます。

アレイ・ネットワークスについて

アレイ・ネットワークス（Array Networks Inc.）は、アプリケーションデリバリネットワーキングにおける世界的リーダーであり、全世界5,000以上の顧客に製品を供給しています。SpeedCore™ソフトウェアに基づくアプリケーションデリバリ、WAN最適化、およびセキュアアクセスの各ソリューションは、大手の企業、サービスプロバイダ、公共機関から、その比類なきパフォーマンスと総所有価値（Total Value of Ownership）で高い評価を得ています。アレイ・ネットワークスは米国シリコンバレーに本拠を置き、世界各国に合計300名余りの従業員を有し、黒字企業として強力な投資家と経営陣のもとで収益を着実に成長させています。急成長中のモバイルおよびクラウドコンピューティングの分野への注力から、Deloitte, IDC、Frost & Sullivanなどのアナリストおよびソートリーダーによりアレイ・ネットワークスの技術的イノベーション、オペレーショナルエクセレンス、市場機会が高く評価されています。

アレイ・ネットワークス株式会社
〒210-0004
神奈川県川崎市川崎区宮本町6-12 GS川崎ビル4階
TEL: 044-589-8315 FAX: 044-589-8303
Email: Sales-Japan@arraynetworks.net

<お問合せ>

ANKK-MKT-ADCWP-2016Q1-0101