

Cisco Secure ADC Application Delivery Controller

目次

アプリケーション SLA の課題	3
レガシー ADC : 今では不十分	3
Secure ADC による完全なアプリケーション SLA アシュアランス	4
統合管理対象アプリケーション保護	4
完全なレイヤ 4 ~ 7 機能セットを備えた高パフォーマンス アプリケーション配信プラットフォーム	5
拡張されたユーザー定義 ADC 機能	5
アプリケーション パフォーマンスを確保するための設計	5
アプリケーションごとのリソースの確保	6
アプリケーション パフォーマンス モニタリングによる完全なアプリケーション SLA の可視性	6
Web アプリケーション パフォーマンス アクセラレーション用のツールセット一式	6
HTTP/2	6
高度なマルチホーミングとエンタープライズ ゲートウェイの機能	7
セキュアなアプリケーション配信サービス	7
シンプルで安全な Web アプリケーション保護	7
暗号化トラフィックの代行受信と検査	7
中央管理と自動化	8
ADC ライフサイクルの自動化の完了 : Operator Toolbox	8
Secure ADC のプラットフォームとフォームファクタ	8
直感的なライセンスパッケージ	9

Cisco Secure Application Delivery Controller¹ (ADC) は、アプリケーション サービス レベル契約 (SLA) を常に予測可能なものにするためにゼロから設計された、業界で唯一のソリューションです。次世代 ADC サービスが組み込まれた唯一の ADC である **Secure ADC** によって、企業やオンラインビジネスが直面する新たな IT の課題にコスト効率よく対応することができます。

アプリケーション SLA の課題

今日のビジネス環境では、一貫した可用性と、パフォーマンスが最適化されたユーザー体験をエンドユーザーに提供することが IT に求められています。仮想化、統合、クラウドプラットフォームなどのトレンドの進行に伴い、これらの配信要件は複雑化しています。今では、同じリソースがさまざまなアプリケーションで共有され、組織が SLA 違反の危険にさらされています。さらに、アプリケーションの運用を脅かすサイバー攻撃によって、アプリケーションの SLA がダウングレードされる可能性もあります。最後に、アプリケーション インフラストラクチャの問題 (Web アプリケーションの複雑さやモビリティの増加など) によって、最適化されたアプリケーションのパフォーマンスを提供して SLA 要件を満たすために追加の課題が生じます。

オンライン Web アプリケーション、内部のミッションクリティカルなエンタープライズ アプリケーション (CRM など)、ERP、または組織のポータルのものであっても、エンドユーザーは一貫した QoE を期待します。結論は明確です。今日の組織は、予測可能なアプリケーション SLA を必要とし、アプリケーション SLA をプロアクティブにモニターおよび管理するためのソリューションを必要としています。

レガシー ADC：今では不十分

アプリケーションの配信を最適化するために、企業は長年にわたってアプリケーション配信コントローラ (ADC) を使用してきました。しかし、アプリケーションの配信はベストエフォート型のアプローチに基づいているため、標準/レガシー ADC では不十分になっています。標準/レガシー ADC では、すべてのリソースがサーバーアプリケーション間で共有されます。アプリケーションごとのリソース分離や、リソース予約のメカニズムはありません。これは、隣接アプリケーションの SLA の低下につながります。同様に、1 つのアプリケーションに機能やサービスを追加すると、ADC の全体的なパフォーマンスが低下する可能性や、他のアプリケーションの SLA に影響を与える可能性があります。

さらに、標準/レガシー ADC では、アプリケーションの SLA をモニターするためのツールは提供されません。主に TCP/SSL レイヤに対応し、アプリケーション、ユーザー、またはデバイスレベルではないアクセラレーション機能のみが提供されます。

レガシー ADC とは対照的に、次世代 (NG) ADC では、リアルユーザーモニタリング、クラス最高水準のアプリケーションレベルのアクセラレーション機能、および革新的なセキュリティサービスが提供されます。完全なアプリケーション SLA アシュアランスにより、NG ADC ではアプリケーションレベルでのリソース予約が提供され、パフォーマンスを低下させることなく新しいサービスを追加することができます。

¹ Secure ADC は、Radware によって Alteon ADC として製造および販売されています。シスコは、Radware とのグローバル OEM パートナシップを通じて、Alteon Application Delivery Controller (ADC)、DDoS 保護、およびアプリケーションと API の保護のソリューションを販売しています。

Secure ADC による完全なアプリケーション SLA アシュアランス

Cisco Secure ADC1 (Radware により Alteon ADC として販売) は、アプリケーション SLA を常に確保するための業界で唯一の ADC です。革新的でゼロから構築され、市場の他の ADC では使用できない次世代サービスが活用されています。Secure ADC では、FastView® の Web パフォーマンス最適化 (WPO)、アプリケーション パフォーマンス モニタリング (APM)、AppWall® の Web アプリケーション ファイアウォール (WAF)、認証ゲートウェイ、高度なサービス拒否 (ADoS)、および IT 管理 (ITM) /帯域幅管理と、最新のすべての暗号がサポートされる業界トップクラスの SSL パフォーマンスが組み合わされています。Secure ADC/Alteon では、いくつかの方法でアプリケーション SLA が確保されます。

- Secure ADC は、完全なアプリケーションレベルのリソース分離を実現し、リソースが使い果たされることを防ぐように設計されています。
- Secure ADC には、アプリケーション、トランザクション、または場所ごとに分類され、アプリケーション SLA が完全に可視化されるアプリケーション パフォーマンス管理 (APM) 機能が組み込まれています。
- この ADC は、業界最先端の WPO テクノロジーである FastView と統合されます。これによりアプリケーションの応答が迅速になり、コンバージョン率、収益、および生産性が向上します。
- Secure ADC は独自の攻撃緩和アーキテクチャの一部であり、最先端のサイバー攻撃を正確に検出して緩和することができます。
- Secure ADC では、選択したモデルまたはフォームファクタに関係なく、業界トップクラスの SSL アクセラレーション パフォーマンスと、非常にコスト効率の高いトラフィック暗号化処理ソリューションが提供されます。

統合管理対象アプリケーション保護

アプリケーションのセキュリティ、可用性、およびパフォーマンスは、ビジネスにとって重要です。Secure ADC では、あらゆる環境でアプリケーションを保護するために設計された、非常に包括的な統合管理対象アプリケーション保護ソリューションが提供されます。Secure ADC では、クラウドを介してトラフィックをルーティングする必要がなく、管理対象クラウドアプリケーション保護のすべての利点が提供されます。このソリューションはエキスパートによって完全に管理されていて、管理のオーバーヘッドやボトルネックなく高度で包括的な保護が提供され、TCO が削減されて、統合アプリケーション保護の新しい標準が設定されます。

実績のある Radware クラウドアプリケーション保護サービスに基づいて構築された Secure ADC の統合管理対象アプリケーション保護では、業界トップクラスの Web アプリケーション ファイアウォール (WAF)、API、ボット、および脅威インテリジェンスのテクノロジーが活用されています。経験豊富なエキスパートによって管理されるため、アプリケーションに対して迅速で包括的なセキュリティが確保され、管理のオーバーヘッドを削減しながら幅広い脅威から保護されます。

SecurePath による Secure ADC アプリケーション保護

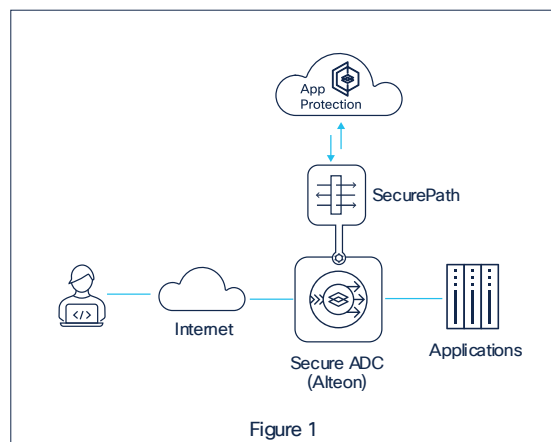


Figure 1

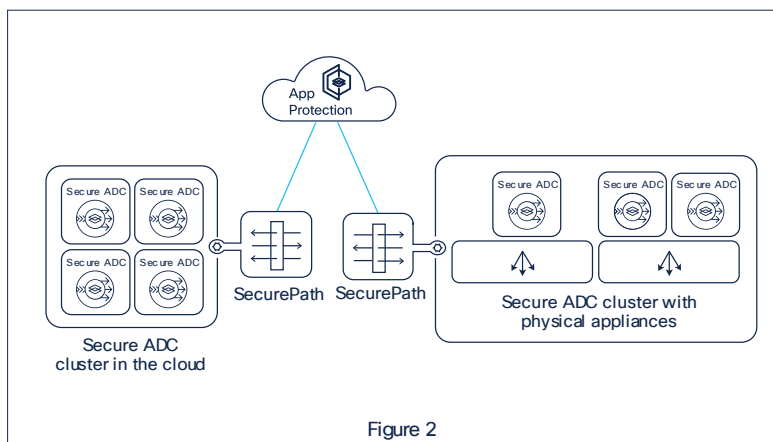


Figure 2

完全なレイヤ 4 ～ 7 機能セットを備えた高パフォーマンス アプリケーション 配信プラットフォーム

Secure ADC はハードウェア プラットフォームとソフトウェアを組み合わせたものであり、比類のないパフォーマンスを発揮する豊富なアプリケーション配信機能が提供されます。レイヤ 4 ～ 7 サービス一式が提供され、オンプレミスおよびクラウドデータセンターでの、ミッションクリティカルなアプリケーションの可用性、パフォーマンス、およびセキュリティが確保されます。これは、トラフィックのリダイレクト、コンテンツの変更、永続性、冗長性、高度なヘルスマonitoring、および帯域幅管理にまでおよび、ミッションクリティカルなアプリケーションの配信が最適化されます。

この ADC は、ハードウェアを変更せずに、必要に応じて動的に拡張するように設計されています。オンデマンドで拡張でき、スループット、サービス、および仮想 ADC (vADC) インスタンスを追加したり、計算集約型次世代サービスのために外部の拡張性に優れたリソースプール（サーバー インフラストラクチャなど）を活用したりすることができます。追加の ADC ユニットを購入する必要がないため、Secure ADC ではコスト効率の高いハードウェア統合が可能になります。物理 ADC の購入に比べてわずかなコストで、サービスを中断することなく、追加の vADC インスタンスを簡単かつ迅速にプロビジョニングできます。

拡張されたユーザー定義 ADC 機能

AppShape®++ テクノロジーによってスクリプト機能が提供され、特定のアプリケーションのフローおよびシナリオに合わせて ADC サービスをユーザー定義でカスタマイズできます。スクリプト例ライブラリを活用することで、お客様はアプリケーションを変更することなく、AppShape++ を使用して HTTP、HTTPS、TCP、ユーザー データグラム プロトコル (UDP)、SSL などのさまざまなレイヤ 4 ～ 7 ポリシーを調整できるため、コストとリスクを軽減できます。

アプリケーション パフォーマンスを確保するための設計

Secure ADC の実行パッケージには、アプリケーション パフォーマンスを確保および強化するために必要なすべてのコンポーネントが含まれています。インフラストラクチャチームとアプリケーションチームが連携してアプリケーション パフォーマンスをプロアクティブに管理できるようにする、一連のツールが提供されます。

アプリケーションごとのリソースの確保

Secure ADC により、企業はアプリケーション、サービス、または部門ごとに個別の仮想 ADC (vADC) インスタンスを割り当てることができます。各 vADC インスタンスは隣接インスタンスから完全に分離され、CPU コア、メモリ、ネットワークスタック、管理制御、オペレーティングシステムのバージョンなどの独立したリソースを使用することができます。そのため、Secure ADC では、配信される Web アプリケーションの完全な障害分離と予測可能なアプリケーション SLA を常に確保することができます。さらに、他のサービスアプリケーションのパフォーマンスに影響を与えることなく、迅速かつ安全に次世代サービスを有効にすることができます。

アプリケーション パフォーマンス モニタリングによる完全なアプリケーション SLA の可視性

Secure ADC のアプリケーション パフォーマンス モニタリング (APM) モジュールにより、ユーザートランザクションを測定することで、アプリケーション SLA のリアルタイムトラッキング (エラーなど) が提供されます。この ADC に組み込まれた APM は、模擬トランザクションのスクリプト化や追加のインストールを必要としないすぐに使用できるソリューションであり、展開にかかる時間とコストを削減できます。APM では、場所、ユーザー、アプリケーション、およびトランザクションタイプによって SLA を直感的に追跡し、効率よく根本原因を分析することができます。

さらに、APM では詳細な分析を特徴とするユーザー定義の SLA に基づいた履歴レポートが提供され、トランザクションフェーズごとの遅延 (データセンターの時間、ネットワーク遅延、ブラウザレンダリングの時間など) を測定することができます。

Web アプリケーション パフォーマンス アクセラレーション用のツールセット一式

Secure ADC では、最大限のアプリケーション パフォーマンス アクセラレーションを実現するためのツール一式が提供されます (キャッシング、圧縮、最新のすべての暗号による比類のない SSL オフロードパフォーマンス、TCP 最適化など)。Secure ADC により、CPU 集約型のタスクをアプリケーションサーバーからオフロードしながら、クライアントとサーバー間の通信を高速化することができます。

Secure ADC に組み込まれた FastView テクノロジーにより、さまざまなエンドユーザーのデバイスやブラウザのタイプ/バージョンに対して Web アプリケーションの応答時間が最大 40% 高速化されて、アクセラレーションの 2 番目のレイヤが追加されます。FastView はモバイルデバイス向けに最適化されています。

FastView は新しいアプリケーションバージョンや新しいモジュールに自動的に適応するため、手動でのコードの最適化が不要になり、組織はコアビジネス能力に集中することができます。

HTTP/2

また、Secure ADC によって組み込みの HTTP/2 ゲートウェイも提供されます。これは、多くの固有の HTTP 1.1 プロトコルのパフォーマンスボトルネックを解決するアクセラレーションの 3 番目のレイヤであり、Web アプリケーションのさらなるアクセラレーションを可能にします。Secure ADC のアクセラレーション機能を活用し、FastView のコンテンツ分析アルゴリズムと組み合わせることで、クライアントがコンテンツを要求する前でも HTTP/2 ゲートウェイによってサーバーのプッシュが自動化され、アプリケーションの応答時間が短縮されます。

Secure ADC では、あらゆるタイプのブラウザ、モバイルデバイス、またはデスクトップデバイスに対して非常に高速な Web アプリケーション最適化体験を実現するために連携して機能する、アクセラレーションツール一式が提供されます。

高度なマルチホーミングとエンタープライズ ゲートウェイの機能

統合 LinkProof® モジュールにより、アプリケーション認識型のコスト効率の高いソリューションが提供されて、常に Web アプリケーションのサービスレベルが確保され、インターネット接続が確保されます。LinkProof NG では、フルパスのアプリケーション ヘルス モニタリングによってアプリケーションのダウンタイムを検出することで、さまざまなネットワーキングノードの問題が特定され、WAN パス全体での即時復旧が可能になります。

このソリューションは、複数の WAN リンクのインバウンドトラフィックとアウトバウンドトラフィックの両方を同時にロードバランシングおよび最適化することで、高度な TCP 輻輳制御を適用してサービスごとに最適な ISP リンクを選択し、クラウドアプリケーションへのアクセスを最適化する、高度なエンタープライズ ゲートウェイとして機能します。LinkProof NG により、ハイブリッド WAN アーキテクチャがサポートされ、割り当てられた WAN リンクが優先順位に従って調整され、Software-as-a-Service (SaaS) アプリケーションへの従業員のアクセスが高速化されるため、従業員の生産性が向上し、分散拠点での運用コストが削減されます。

セキュアなアプリケーション配信サービス

セキュアサービスパッケージには、組織がアプリケーションを保護できるようにするモジュールと機能の一式が含まれています。さらに、Secure ADC は、独自の Defense Messaging メカニズムを活用して Radware の攻撃緩和ソリューションと統合されます。このメカニズムでは、Radware の DefensePipe® クラウドサービスと DefensePro®（ネットワーク境界に配置されるデータセンターの攻撃緩和機能）に攻撃情報を通知することで、効率的に攻撃が緩和されます。

シンプルで安全な Web アプリケーション保護

独自のアウトオブパス WAF 展開モードや自動ポリシー生成機能などの、高度な Web アプリケーション ファイアウォール (WAF) 機能の統合により、リスクを伴わずに導入することができます。さらに、完全なインスタンス分離とリソース予約により、ADC リソースが確保されます。WAF ポリシーが更新されても、アプリケーションの可用性とパフォーマンスに影響はありません。これにより、SLA が確保されたセキュアな Web アプリケーションが実現します。

最後に、Secure ADC には、Radius、Active Directory、Lightweight Directory Access Protocol (LDAP)、および RSA SecurID をサポートすることでシングルサインオン (SSO) 機能を提供する組み込みの認証ゲートウェイが備えられているため、アプリケーションのセキュリティを犠牲にすることなくユーザー体験が簡素化されます。

暗号化トラフィックの代行受信と検査

次世代ファイアウォールやデータ漏洩防止システムなどのセキュリティソリューションによる検査のために、Cisco Secure ADC ではインバウンド暗号化トラフィックの復号をオフロードする機能がネイティブに提供されます。ソリューションを完成させるために、Secure ADC では、アウトバウンド暗号化トラフィックを代行受信する独自の機能も提供されます (ADC が SSL キーを所有せず、コンテンツを復号し、それをクリアテキストで同じセキュリティサーバーに転送する転送プロキシとして)。

統合 URL 分類エンジンにより、特定のトランザクション (銀行口座や医療サイトの閲覧など) がプライベートと見なされるかを Secure ADC で判断し、検査のためにトラフィックを代行受信せずに、そのまま宛先に転送することができます。

中央管理と自動化

Secure ADC の中央管理システム (APSolute Vision®) により、IT、セキュリティ、およびインフラストラクチャの管理者は、すべての Secure ADC デバイス、仮想 ADC インスタンス、および AppWall や FastView などの統合モジュールを含む、ソリューション ポートフォリオ全体を直感的に連携して管理することができます。また、アプリケーション配信チェーンのユーザー体験とさまざまな要素に関するドリルダウンレポートを使用できるようにする、パフォーマンスのモニタリングとレポートのためのツールも提供されます。また、APSolute Vision を使用することで、さまざまな Radware デバイスの管理タスクを自動的に実行する高度な自動化ツールも利用できます。

ADC ライフサイクルの自動化の完了 : Operator Toolbox

Operator Toolbox により、ADC のエキスパートかどうかにかかわらず、運用タスクを自動化することができます。Operator Toolbox を使用することで、人的エラーを最小限に抑えながら、ADC サービスのライフサイクル全体を通じて運用ワークロードを大幅に削減することができます (最大 90%)。組織は Operator Toolbox で特定のアプリケーションや作業方法に応じて独自の自動化タスクをカスタマイズしたり、さまざまなタイプのユーザー (ネットワーク管理者やアプリケーション開発者など) 向けにウィザードを設計したり、認定済みスクリプトの完全なライブラリからすぐに使用できるウィザードを提供したりすることができます。

ボタンを数回クリックするだけで新しい高度なアプリケーション配信サービスを展開できるため、プロセスに ADC 固有のエキスパートは必要ありません。管理者は APSolute Vision の中央管理システムを使用することで、組織内のさまざまなユーザーグループ (アプリケーション管理者、アプリケーション開発者、ネットワーク管理者など) に合わせて調整されたさまざまなユーザー権限を使用して、さまざまなスクリプトライブラリを作成することができます。

Secure ADC のプラットフォームとフォームファクタ

Secure ADC ソリューションには、物理アプライアンス、仮想アプライアンス、およびクラウドベースのフォームファクタのポートフォリオが含まれていて、これらすべてで機能とモジュールの同じセットが共有されるため、アプリケーション SLA が確保されます。他のすべてのレイヤ 4 ~ 7 アプリケーション配信機能、パフォーマンスの最適化、およびセキュリティ機能に加えて、この ADC では強化されたトラフィック暗号化処理パフォーマンスが提供されます。これは、最適化されたソフトウェアと最新のハードウェア アクセラレーション カードの両方によって使用可能になっています。

Secure ADC の仮想アプライアンス (vADC) とクラウドアプライアンスに違いはなく、物理 Secure ADC アプライアンスと同じ機能と、業界トップクラスのパフォーマンスとトラフィック暗号化能力が提供されます。

すべての Secure ADC アプライアンスで、デバイスごとの高密度な仮想 ADC インスタンスを使用した仮想化がエントリレベルからサポートされ、あらゆる規模の組織が仮想化と ADC の統合に関連するコスト削減の利点を活用できます。Secure ADC の仮想アプライアンスのフォームファクタは、DevOps チーム向けの特別なバージョンでも使用できます。これにより、あらゆる開発環境に即座に展開でき、すぐに使用できるウィザードや自動化スクリプトを介して高度な ADC 機能を使用することができます。

直感的なライセンスパッケージ

新しい Secure ADC/Alteon D-line では、さまざまな展開のシナリオとニーズに対応するために、3 つの異なるライセンスパッケージが提供されます。

- 高度なレイヤ 4 ~ 7 の ADC 機能を備えた高パフォーマンス ADC を必要とするアプリケーションのための、配信パッケージ。
- パフォーマンスの最適化、高度なアプリケーション パフォーマンス モニタリング、グローバル サーバー ロード バランシングとリンクロードバランシング、および自動化/最適化された ADC サービスの運用を必要とする展開シナリオのための、実行パッケージ。
- (組み込み WAF モジュール、認証ゲートウェイによる) 非常に高度な保護を必要とするアプリケーションと、(組み込み SSL インспекションモジュールによる) 境界セキュリティデバイスからの SSL 処理のオフロードのための、セキュアパッケージ。

Cisco Secure ADC ソリューションの詳細については、今すぐシスコのセールス担当者までお問い合わせください。

SecurePath® は Radware の登録商標です。

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム (オランダ)

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト (www.cisco.com/jp/go/offices) をご覧ください。

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/jp/go/trademarks をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(1110R)