

Cisco Application Control Engine (ACE)



概要

企業は生産性の向上、コスト管理、ビジネス プロセスの最適化、およびより適切な情報に基づいたあらゆる組織レベルでのタイムリーな意思決定を行うために、アプリケーションの導入およびアップグレードを継続的に行っています。これらのアプリケーションから最適な Return On Investment (ROI)を得るには、アプリケーションのアベイラビリティおよびセキュリティを高める必要があります。また、使用時期や使用場所に関係なく、常に特定のパフォーマンス レベルで運用する必要があります。ただし、グローバル ユーザに十分なサービス レベルを提供しながら、アプリケーションおよび重要なビジネス データを配信するには、さまざまな課題があります。Cisco Application Control Engine (ACE)は、すべてのアプリケーションのアベイラビリティ、パフォーマンス、およびセキュリティを高める新しいネットワーク ソリューションです。ACE を使用すると、既存の資本および運用資産を利用しながら、インフラストラクチャの統合にも役立ちます。

課題

アプリケーションは進化を続けていて、ますます大規模かつ複雑になっています。IT 部門にとっては、グローバル ユーザに十分なパフォーマンス、アベイラビリティ、およびセキュリティを提供しながら、このような複雑かつ重要なアプリケーションを配信することが重要な課題になっています。

リモート オフィスの従業員数が増加し、従業員がよりグローバルに各地へ分散しているのに伴い、ユーザにアプリケーションおよび重要なビジネス データを配信することはますます困難になっています。ユーザは、どこにいても、あらゆるタイプの情報およびアプリケーションに適切なタイミングでアクセスする必要があります。データセンター近辺にいる場合と同様に、すばやく簡単にアクセスする必要もあります。また、ネットワークにオフロードできるはずの多くのアプリケーション機能がオフロードされないため、大量のサーバ リソースが消費され、その結果コア ビジネス トランザクションのパフォーマンスは低下します。アプリケーションのパフォーマンスが低下すると、アプリケーションの採用率が低下し、トランザクションが不完全になり、生産性が失われ、ユーザ満足度が低下することがあります。

インターネットを介して Web 対応アプリケーションを利用する機会が増え、アプリケーションへのアクセスをモバイル ユーザおよびパートナーにまで拡張しなければならなくなっています。したがって、企業が現在直面している重要課題は、さまざまなネットワーク、アプリケーションレベル、および

Web サービス攻撃からアプリケーションと知的財産を保護することです。政府やさまざまな業界規制への適合も必要です。セキュリティが低下すると、お客様とビジネス パートナーの関係に深刻な影響が生じることがあります。

最も重大なのは、現在の企業が、データセンター内およびデータセンター間で常にアベイラビリティを維持して、グローバルに分散しているユーザ、パートナー、およびお客様にますます多くのアプリケーションを提供するようにせまられていることです。重要なアプリケーションが停止すると、業務は行き詰まり、収益や信用度が低下します。

最後に、企業はこれまで、購入するサーバ数およびロードバランシング デバイス数を増やして、アプリケーション配信の課題に就いていました。現在、IT 予算の拡大は抑えられ、経営陣は少ない IT インフラストラクチャ リソースで多大な成果を求められるようになっています。このため、企業はデータセンター内のアプリケーション配信インフラストラクチャを統合して、コストを削減し、管理を簡易化できるソリューションを模索しています。

多くのアプリケーションおよびネットワーク ベンダーは、汎用ハードウェア上でソフトウェアベース ソリューションを使用することにより、これらのアプリケーション配信の課題の一部について解決しようとしてきました。ところが、これらの製品を導入すると、ネットワークは複雑化し、デバイスはデータセンター内に分散され、データセンターのラック スペース、冷却、および電源に関する要件は増大し、ソフトウェアライセンス コストや運用管理コストは増加します。

Cisco ACE アプリケーション スイッチによるアプリケーション配信課題の解決

Cisco[®] ACE アプリケーション スイッチは、コア サーバ ロードバランシング サービス、高度なアプリケーション アクセラレーション、およびセキュリティ サービスを実現して、アプリケーションのアベイラビリティ、パフォーマンス、およびセキュリティを最大化します。これらのスイッチには革新的な仮想化ハードウェア プラットフォーム、アプリケーション固有のインテリジェンス、優れたパフォーマンス、および詳細な Role-Based Administration (RBA) が組み込まれています。Cisco ACE アプリケーション スイッチは、データセンター内に一般に導入される非対称的なソリューションです。図 1 に、Cisco Catalyst[®] 6500 シリーズ スイッチ (イーサネット スイッチ) と Cisco 7600 シリーズ ルータ (キャリア イーサネット ルータ) に対応した、スケーラビリティの高いモジュールを示します。また、データセンターに導入するための、スタンドアロン Cisco ACE 4710 アプライアンスも示します。

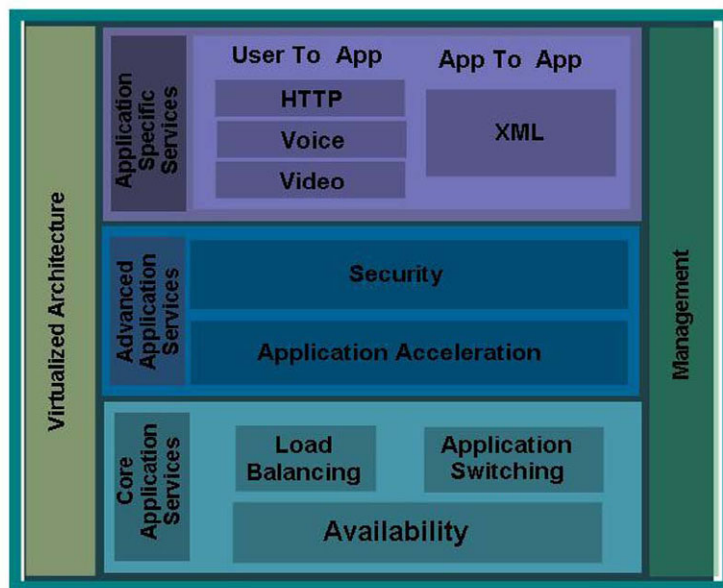
図 1 Cisco ACE



Cisco ACE アプリケーション スイッチを使用すると、IT 部門は次に示すビジネス上の利点を実現しやすくなります。

- **アプリケーションのアベイラビリティおよびスケーラビリティの向上:** Cisco ACE アプリケーション スイッチを使用すると、アベイラビリティと稼働時間を高めながら、ビジネス要件の増大に合わせてアプリケーション リソースを動的に拡張できます。
- **データセンターの統合によるコスト削減:** Cisco ACE アプリケーション スイッチを使用すると、データセンターの統合が容易になり、必要なサーバ数およびロード バランサ数が削減されて、電力および冷却要件が緩和されます。また、アプリケーション導入サイクルや、アプリケーション インフラストラクチャを管理するための所要時間が短縮されます。
- **アプリケーションの高速化:** Cisco ACE アプリケーション スイッチを使用すると、アプリケーション 応答が高速化され、すべてのリモート ユーザに対してビジネス トランザクション スループットが向上します。最大 90% のサーバ処理能力がオフロードされるため、必要なサーバ数およびアプリケーション ライセンス数が削減されます。
- **アプリケーションの保護:** Cisco ACE アプリケーション スイッチは、ネットワークおよびアプリケーション 攻撃からアプリケーションやデータセンターを保護します。

図 2 Cisco ACE アプリケーション スイッチの高度なコア アプリケーション配信サービス



Cisco ACE アプリケーション スイッチが提供するこのような利点は、仮想化されたハイパフォーマンス ハードウェア アーキテクチャ上に一連の高度なコア アプリケーション配信機能を組み込んで実現されています。

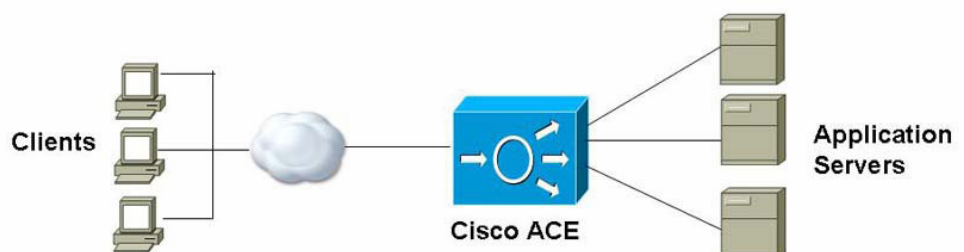
- **インテリジェントなサーバ ロード バランシング (SLB):** Cisco ACE アプリケーション スイッチは、動的で適応性のあるさまざまなロードバランシング アルゴリズムを使用して、ハイパフォーマンスでインテリジェントなアプリケーション スイッチ ソリューションを実現します。また、すべての IP アプリケーションに対して、サーバ ロード バランシング機能を提供し、パッケージ、カスタム、Extensible Markup Language (XML) アプリケーションに対して、ヘッダー内情報を保持するという強力な機能を提供します。このスイッチの設計目的は、物理または仮想デバイス レベルでステータフルなハイ アベイラビリティを達成することです。

- **高度なアプリケーション アクセラレーション技術:** Cisco ACE アプリケーション スイッチは、クライアント/サーバ間のラウンドトリップ時間を短縮する機能、圧縮を使用して帯域幅を最適化する機能、Secure Sockets Layer (SSL) およびサーバ TCP 接続を設定するためにサーバ処理サイクルをオフロードする機能など、複数の機能を組み合わせてアプリケーションを高速化します。
- **ネットワークおよびアプリケーションのセキュリティ:** Cisco ACE アプリケーション スイッチは、既知および未知のさまざまなネットワークおよびアプリケーション攻撃から、データセンターや、Web アプリケーションなどのアプリケーションを保護します。この保護機能は、スケーラビリティの高いパケット/コンテンツ フィルタリング、プロトコル インспекション、および高度な暗号化によって実現されます。
- **強力な仮想化アーキテクチャ:** Cisco ACE アプリケーション スイッチの仮想化機能を使用すると、物理デバイスを、それぞれに物理デバイスの機能をすべて備えた複数の隔離された仮想デバイスに分割できます。この仮想化機能により、データセンターに導入される物理的なアプリケーション配信デバイス数を削減できます。
- **専用のアプリケーション配信デバイス:** Cisco ACE アプリケーション スイッチはマルチコア ネットワーク プロセッサを使用して、優れたレイヤ 4 ~ 7 サーバ ロード バランシングを実現します。また、オプションのドーター カードを使用することにより、パフォーマンスを低下させることなく、サーバを並列処理できます。
- **カスタマイズ可能な RBA:** Cisco ACE アプリケーション スイッチには、8 つのルールが事前定義されています。これらを使用してカスタム ルールを作成し、さまざまな組織構造に対応することもできます。したがって、IT ネットワークおよびアプリケーション グループで、設定を変更するために調整作業を行う必要はありません。

アプリケーションの可用性およびスケーラビリティの向上

Cisco ACE アプリケーション スイッチは、総合的なアプリケーション対応 SLB サービスを提供します。SLB デバイスの機能は、特定のクライアント要求に最適なサーバを選択することです。たとえば、クライアント要求は Web ページに対する HTTP GET 要求や、ファイルをダウンロードするための FTP GET 要求で構成されます。Cisco ACE アプリケーション スイッチは、サーバおよびアプリケーションに関する豊富な静的および動的情報を使用して、インテリジェントなロードバランシング判断を行います。これらの判断は、サーバまたはサーバ ファーム全体への過負荷を回避しながら、最短時間で実行されます(図 3)。

図 3 Cisco ACE アプリケーション スイッチを使用した複数サーバ間でのクライアント要求のロード バランス



Cisco ACE アプリケーション スイッチは、仮想化されたハイパフォーマンス ハードウェア アーキテクチャで一連の高度な SLB 機能を実行することによって、アプリケーションのオペラビリティおよびスケラビリティを向上させます。

- **適応性のあるロードバランシング アルゴリズム:** サーバに関する静的情報を使用してロードバランシング判断を行う従来のロード バランサと異なり、Cisco ACE アプリケーション スイッチは静的情報と動的情報を併用して、インテリジェントなロードバランシング判断を行います。そのために、サーバ情報だけでなくアプリケーションおよびコンテンツ情報も使用されます。Cisco ACE スイッチは、ハッシュ ヘッダー、ハッシュ クッキー、ハッシュ URL、アプリケーション エラー応答コードなど、さまざまなアプリケーションおよびコンテンツ対応ロードバランシング アルゴリズムをサポートしています。Cisco ACE アプリケーション スイッチは、設定されたロードバランシング アルゴリズムに基づいて一連のチェックおよび計算を行います。これにより、各クライアント要求を最適に処理できるサーバを判断して、パフォーマンスおよびオペラビリティを向上させます。
- **インテリジェントなアプリケーションおよびコンテンツ スwitチング:** Cisco ACE アプリケーション スイッチはロード バランシングをサポートし、パッケージ アプリケーションおよびカスタム アプリケーションの HTTP ヘッダーの値をすべて保持することができます。
- **セッションの保持:** パッケージ アプリケーションおよび e- コマース アプリケーションは通常、クライアントに関する情報をサーバ メモリに格納して、セッション全体で使用できるようにしています。ここで使用するセッションは、有限期間(数分から数時間)にわたる、クライアントとサーバ間の一連のトランザクションとして定義されます。これらのアプリケーションでは、接続が確立されたあとに、クライアントを特定のサーバに「スティッキー」する必要があります。Cisco ACE アプリケーション スイッチは、スティッキーという機能をサポートしています。この機能を使用すると、同じクライアントで、セッション期間中に同じサーバとの間に確立された複数の同時 TCP/IP 接続、あるいは後続の TCP/IP 接続を維持することができます。Cisco ACE アプリケーション スイッチは、使用するロードバランシング アルゴリズムを決定したあとに、設定された SLB ポリシーに応じて、クライアントを適切なサーバに「スティッキー」させます。クライアントがすでに特定のサーバにスティッキーされていると判断された場合は、適用されるポリシーで指定されたロードバランシング基準に関係なく、同じクライアントからこのサーバへさらに要求が送信されます。クライアントが特定のサーバにスティッキーされていないと判断された場合は、クライアント要求に対して通常のロードバランシング ルールが適用されます。Cisco ACE アプリケーション スイッチはアプリケーションに完全に対応しています。また、ソースまたは宛先 IP アドレス、クッキー(動的なクッキー学習およびクッキー挿入)、SSL セッション ID、HTTP ヘッダー、パッケージ アプリケーションおよびプロトコル固有の情報、プロトコル ヘッダー内の任意のカスタム値など、さまざまなセッション保持方式を提供します。
- **アプリケーション ヘルス モニタリング:** Cisco ACE アプリケーション スイッチは、アウトバンド プロンプを使用してサーバまたはアプリケーションの状態やヘルスをトラッキングするための、高度なサーバおよびアプリケーション ヘルス モニタリングをサポートしています。また、サーバ応答を検証したり、クライアントからサーバへの到達を妨げるネットワーク問題がないかチェックしたりします。Cisco ACE アプリケーション スイッチはサーバ応答に基づいて、サーバを稼働中またはアウト オブ サービスの状態にしたり、信頼できるロードバランシング判断を行ったりできます。Cisco ACE は、Internet Control Message Protocol(ICMP)、TCP、HTTP、ハードウェア アクセラレーション SSL/Secure HTTP(HTTPS)、その他の定義済みヘルス プロンプなど、最大 4096 個の一意的なプロンプ設定をサポートします。これらのプロンプのほか、カスタム Tool Command Language(TCL)スクリプトをアップロードおよび実行できる、より柔軟性の高いスクリプトヘルス プロンプもサポートします。スクリプト プロンプの動作は、Cisco ACE ソフトウェアで使用可能なその他の定義済みヘルス プロンプと同様です。Cisco ACE はスクリプト プロンプ

中に、スクリプトを定期的に行います。実行中のスクリプトから戻される終了コードには、関連ヘルス、および特定のサーバーの可用性が示されています。ヘルス プロブはサーバーファームに適用できます。

- **ルートヘルスインジェクション:** Route Health Injection (RHI; ルートヘルスインジェクション)機能を使用すると、Cisco ACE アプリケーションスイッチからネットワーク全体に、VIP (バーチャルIP) アドレスの可用性をアドバタイズできます。また、VIP のインスタンスを複数作成して、障害回復、グローバル SLB、および Cisco ACE アプリケーションスイッチのスケラビリティを実現することもできます。RHI が有効な場合に、VIP アドレスが使用可能になると、Cisco ACE アプリケーションスイッチは Multilayer Switch Feature Card (MSFC) にアドバタイズメントを送信し、使用できない VIP アドレスのアドバタイズメントを取り消します。Cisco ACE アプリケーションスイッチはヘルスプロブを使用して、VIP の可用性を判断します。MSFC は、Cisco ACE アプリケーションスイッチから受信された各 VIP アドレスのエントリを、ルーティングテーブルに追加します。MSFC で実行中のルーティングプロトコルは、VIP アドレスの各インスタンスの可用性やホップカウント ルーティング情報などのルーティングテーブルアップデートをその他のルータに送信します。クライアントルータはルーティング情報を使用して、この VIP アドレスへ有効で最適なパスに基づいてルートを選択し、Cisco アプリケーションスイッチがクライアントシステムへ論理的に近くなるように設定します。
- **Asymmetric Server Normalization (ASN):** ASN を使用した場合、Cisco ACE は実サーバーからの戻りトラフィックをクライアントに直接転送して、Cisco ACE アプリケーションスイッチをバイパスしながら、クライアントからの初期要求のロードバランシングを実行できます。この機能により、サーバークライアント間の通信速度は高まり、Cisco ACE アプリケーションスイッチを介して処理されるトラフィック量は削減されます。ASN 機能が有効な場合、Cisco ACE は宛先アドレスとして VIP アドレスを使用し、さらに実サーバーの MAC アドレスを使用して、実サーバーにトラフィックを送信します。したがって、通常どおり、実サーバーに IP アドレスを設定するだけでなく、ループバックインターフェイスにも VIP の IP アドレスを設定する必要があります。
- **ハイ可用性およびステートフル冗長性:** アプリケーション配信デバイスが応答しなくなった場合に、ミッションクリティカルなアプリケーションを使用するには、通常、透過的なフェールオーバーを 1 秒未満で実行する必要があります。Cisco ACE アプリケーションスイッチの設計目的は、物理および仮想デバイスレベルで堅牢なステートフル冗長性を実現することです。Cisco ACE のステートフル冗長性機能を使用すると、デバイス障害に関係なく、ネットワークサービスおよびアプリケーションが使用できるようになるため、ユーザーエクスペリエンスは向上します。
- **仮想デバイス冗長性:** 同じ Cisco Catalyst 6500 シリーズスイッチ内、同じ Cisco 7600 シリーズルータシャーシ内、または 2 つの物理的に異なるシャーシ内の Cisco ACE モジュールが冗長構成になるように、Cisco ACE アプリケーションスイッチを設定できます。Cisco ACE は 2 つのアプライアンス型デバイス間の冗長性もサポートしています。Cisco ACE は物理および仮想の両方のデバイスレベルで、従来のソリューションよりも高い可用性をサポートします。Cisco ACE アプリケーションスイッチは、それぞれ独自のコンフィギュレーションファイル、リソース、および管理インターフェイスを備えた、最大 250 の仮想デバイスに分割できます。各仮想デバイスには、実際の物理デバイスの機能がすべて備わっています。各仮想デバイスが独立していて、隔離されているため、ネットワークおよびネットワーク管理者からは、一意の物理デバイスとして認識されます。Cisco ACE アプリケーションスイッチには、選択された仮想デバイスにのみ冗長性を設定できるという柔軟性があります。特定の仮想デバイスの設定が、その他の仮想デバイスの設定に影響することはありません。したがって、仮想パーティショニングという革新的な保護方法を使用すると、複数の仮想デバイスに設定された一連のサービスを、別の仮想デ

バースでの不慮または悪意のある設定から保護できます。Cisco ACE の設定に障害があっても、障害範囲は作成元の仮想デバイスに限定されます。ある仮想デバイスの障害が Cisco ACE 内の別の仮想デバイスに影響することはないため、重要アプリケーションの稼働時間は最大化されます(特に、Cisco ACE がハイ アベイラビリティな冗長構成に導入されている場合)。

- アクティブ/アクティブ冗長性:** Cisco ACE アプリケーション スイッチは、2 つの物理デバイス間のアクティブ/アクティブ冗長構成をサポートします。この構成を設定すると、アクティブ モードの Cisco ACE 物理デバイスを 1 つだけでなく、2 つとも使用して、負荷を分散できます。図 4 および図 5 に、2 つの有効な Cisco ACE アクティブ/アクティブ冗長構成を示します。N は冗長構成された Cisco ACE 仮想デバイスの数です。最初の例(図 4)では、仮想デバイスは 2 つの Cisco ACE 物理デバイス間に均等に分散されます。文字(A、B、C、および D)はアクティブ仮想デバイスを、プライム記号付き文字(A'、B'、C'、および D')はスタンバイ仮想デバイスを表します。2 番目の例(図 5)では、仮想デバイスは 2 つの Cisco ACE 物理デバイス間に不均等に分散されます。このシナリオは、仮想デバイス A、B、C、および D にホストされたアプリケーションに必要なリソースが、仮想デバイス E および F にホストされたアプリケーションに必要なリソースの半分のみである場合に適用されます。

図 4 Cisco ACE アプリケーション スイッチのアクティブ/アクティブ冗長性: 例 1

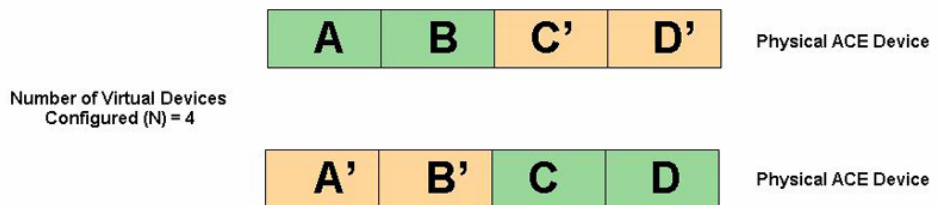
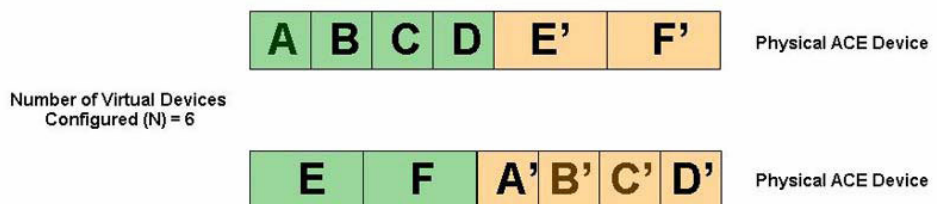


図 5 Cisco ACE アプリケーション スイッチのアクティブ/アクティブ冗長性: 例 2



- ステートフル フェールオーバー:** Cisco ACE アプリケーション スイッチは、アクティブ仮想デバイスの接続フローをスタンバイ仮想デバイスに複製します。複製された接続フローには、アクティブ仮想デバイスが応答不能になった場合に、スタンバイ仮想デバイスがフローを引き継ぐために必要なフローステート情報がすべて含まれています。これまでアクティブだった仮想デバイスはスタンバイ ステートに移行し、新たにアクティブになった仮想デバイスに現在のフローをすべてバックアップします。この機能が有効な場合、フェールオーバーまたはフェールバック中に同じネットワーク セッションを維持するためにエンドユーザ アプリケーションを再接続する必要がありません。したがって、Cisco ACE のステートフル フェールオーバーおよびフェールバック冗長性機能を使用すると、デバイス障害に関係なく、アプリケーションに真に透過的なフェールオーバーを実現できます。
- トラッキングおよび障害検出:** Cisco ACE アプリケーション スイッチは、サーバや VLAN など、複数のネットワーク アイテムのトラッキングおよび障害検出をサポートします。また、トラッキング

されたネットワーク リソースが応答不能になった場合は、アクティブな Cisco ACE 物理または仮想デバイスからスタンバイ Cisco ACE デバイスに透過的にスイッチオーバーします。スイッチオーバー中に存在していたすべてのアクティブ フローは、新しいアクティブ Cisco ACE デバイス上で中断なしに継続されます。障害のあるトラッキング対象ネットワーク デバイスが再び起動すると、Cisco ACE アプリケーション スイッチはアクティブおよびスタンバイ Cisco ACE デバイス間のプライオリティを評価します。スタンバイ Cisco ACE デバイスのプライオリティがアクティブ Cisco ACE デバイスのプライオリティよりも大きい場合、Cisco ACE は本来のアクティブ Cisco ACE デバイスに透過的にスイッチオーバーします。ゲートウェイやホストなどの複数のネットワーク デバイス、インターフェイス、Hot Standby Router Protocol (HSRP) グループをトラッキングするように、Cisco ACE を設定できます。たとえば、Cisco ACE が HSRP グループをトラッキングすることが可能で、HSRP グループが応答不能になった場合は、アクティブ Cisco ACE デバイスからスタンバイ Cisco ACE デバイスに透過的にスイッチオーバーできます。この場合、Cisco ACE アプリケーション スイッチのトラッキングおよびスイッチオーバー機能により、2 つのディストリビューション レイヤ スイッチ間の ISL (スイッチ間リンク) 上のトラフィックが削減されます。

Cisco ACE: 業界で最も効率的なアプリケーション配信プラットフォームの 1 つ

Cisco ACE アプリケーション スイッチを使用すると、ネットワークを複雑化することなく、アプリケーション配信の課題を解決できます。また、仮想化、ハイ パフォーマンス、専用ハードウェア、簡易 GUI など、高度で革新的な多くの機能が用意されているため、データセンターおよびデバイスを統合し、コストを削減し、管理を簡素化することができます。Cisco ACE は非常に効率的なアプリケーション配信プラットフォームです。

- **専用ハードウェア:** アプリケーション配信デバイスには通常、サーバベースまたはハードウェアベースの 2 つの主要なアーキテクチャ タイプがあります。サーバベース アプリケーション配信デバイスは、一般に、Linux や FreeBSD などの標準または修正版フリーウェア オペレーティングシステムが稼働する汎用ハードウェアです。サーバベース方式ではコード開発作業が削減され、新機能を短時間で導入できますが、パフォーマンスが著しく低下します。サーバベース方式を使用するお客様は、通常、機能のパフォーマンスを犠牲にする必要があります。また、ソフトウェアベース方式の場合、ベンダーはスケーラビリティやパフォーマンスが向上するようにソフトウェア オペレーティング システムを再構築する必要があるため、製品が不安定になることがあります。Cisco ACE アプリケーション スイッチはソフトウェアベース アプリケーション配信デバイスではなく、ハードウェアベース アプリケーション配信デバイスです。専用のマルチコア ネットワーク プロセッサを使用して、汎用プロセッサよりもはるかに高速かつ効率的にソフトウェア タスクを実行します。Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータ プラットフォームに対応したモジュール型、およびアプライアンス型の Cisco ACE アプリケーション スイッチを使用できます。
- **仮想化:** 従来のデータセンターは、多数の物理サーバ ロード バランサ、およびその他のレイヤ 4 ~ 7 デバイスで構成されています。これらのデバイスは、企業のビジネス構造、およびアプリケーションやサービス要件に応じて、複数のお客様、運用グループ、およびビジネス単位やアプリケーションの共有デバイスとして使用されるか、専用デバイスとして使用されます。これらの物理デバイスを導入すると、次に示すようにさまざまな面で、開発および運用が非効率になります。
 - 物理リソースが十分に活用されなくなる
 - ビジネスの重要性およびセキュリティ上の理由から、特定のアプリケーションを隔離する必要があるために、デバイスが分散される
 - デバイスが分散したことにより、データセンターの冷却要件および電源消費量が高まる

- 新しい物理デバイスを必要とするアプリケーションまたはサービスの取得コストおよび開発時間が増大する
- 物理デバイスのケーブル接続および電力要件が増えるため、アプリケーション開発コストが増大する
- 複数の物理デバイスの管理およびメンテナンスが必要になるため、運用上のオーバーヘッドが増大する
- これらの課題を解決するために、Cisco ACE アプリケーション スイッチは物理デバイスを仮想化して、複数の仮想デバイスを作成します。Cisco ACE は、真の仮想化を実現する、業界唯一のアプリケーション配信製品です。各 Cisco ACE 仮想デバイスには実際の物理デバイスの機能がすべて組み込まれ、相互に隔離されています。仮想化された Cisco ACE 仮想デバイスには、それぞれ独自のコンフィギュレーション ファイル、管理インターフェイス、リソース、ルーティング テーブル、VLAN インターフェイス、およびアクセスコントロール ポリシーが保持されます。アクセスコントロール権限は、管理ロールに基づいてユーザに割り当てられます。また、各仮想デバイスは独立していて、隔離されているため、ネットワークおよび管理者からは一意な物理デバイスとして認識されます。
- Cisco ACE アプリケーション スイッチを使用すると、各仮想デバイスの帯域幅、1 秒あたりの接続数、1 秒あたりの管理接続数、SSL 接続数、アクセス リスト数など、さまざまなリソースを制限および管理することができます。すべてのリソースの消費量の下限および上限を、各仮想デバイスについてパーセンテージで割り当てることができます。Cisco ACE には、3 つの異なる方法（制限、オーバーサブスクリプション、フリー）で仮想デバイスにリソースを割り当てることができるという柔軟性もあります。アプリケーションのリソースを確保するために、Cisco ACE ではすべての Cisco ACE リソースに対して、または特定の仮想デバイスの各リソースに対して、消費量の下限および上限を設定できます。たとえば、仮想デバイスにホストされているアプリケーションに対する Cisco ACE リソースの消費量を 20% に制限するには、仮想デバイスのリソース消費量の下限および上限を 20% に設定します。また、リソースの上限を無制限に設定して、Cisco ACE でオーバーサブスクリプションをサポートすることもできます。このようにすると、仮想デバイスにホストされたアプリケーションは、割り当てられた Cisco ACE リソースのうち、他の仮想デバイスで消費されていないリソースを使用できます。オーバーサブスクリプションの例として、Cisco ACE 物理デバイスを 4 つの仮想デバイスに分割して、それぞれにリソース消費量の下限値として 25%、上限値として無制限を割り当てることができます。この例の場合、各仮想デバイスにホストされたアプリケーションは、他の 3 つの仮想デバイスのいずれかでリソース消費量が最小割り当て値の 25% を下回る場合、割り当て値の 25% よりも多くの Cisco ACE リソースを消費できます。デフォルトのフリー設定の場合は、すべての仮想デバイスがすべてのリソースにフル アクセスできます（最初にアクセスしたデバイスが、最初に処理されます）。
- Cisco ACE を仮想化すると、ビジネスおよび技術に関して、次のような重要な利点が多数得られます。
 - **データセンターのリソース要件の緩和:** Cisco ACE アプリケーション スイッチを使用すると、追加ハードウェアを導入しなくても同じ物理 Cisco ACE 内に仮想デバイスを簡単に導入できるため、管理者はアプリケーションを短時間で展開できるようになります。その結果、デバイスの分散は抑えられ、追加のケーブル接続要件およびラックスペース要件はありません。さらに、Cisco ACE 仮想化機能を使用すると、ネットワーク内の物理アプリケーション スイッチ数が削減されるため、データセンターの電力および冷却消費量が大幅に削減されます。Cisco ACE アプリケーション スイッチの総電力消費量は、作成された仮想デバイス数に関係なく、一定のままです。

- **アプリケーション、部門、お客様の完全な隔離:** Cisco ACE を使用することにより、管理者はアプリケーションごとに、あるいは複数のアプリケーションに対して仮想デバイスを作成し、必要なリソースを割り当てることができます。スイッチの設定に障害があっても、障害範囲は作成元の仮想デバイスに限定されるため、アプリケーション全体のアベイラビリティが最大になります。
- **多層型アプリケーション アーキテクチャへの集約:** お客様は通常、Web、アプリケーション、およびバックエンド データベース層ごとに独立したロード バランサおよびファイアウォールを使用して、多層型アプリケーション アーキテクチャを導入しています。Cisco ACE の仮想化、ファイアウォール、およびスケール機能を使用すると、3 つの異なるロードバランサおよびファイアウォール層を単一の物理デバイスに集約して、コストを削減し、ネットワークの複雑さを緩和できます。
- **優れたパフォーマンス:** Cisco ACE モジュールでは、Cisco Catalyst 6500 シリーズ スイッチ ファブリックとの相互接続を 1 つ使用して、最大 16 Gbps のスループットをサポートしています。このモジュールは、5 つの主要ハードウェア コンポーネントで構成されています。
 - データプレーントラフィックを処理するためのパラレルなマルチコア ネットワーク プロセッサ
 - 2 つのネットワーク プロセッサにトラフィックを分散させるためのアプリケーション特有の Field Programmable Gate Array (FPGA)
 - 管理(コントロールプレーン)トラフィックを処理するためのデュアルコア プロセッサ
 - SSL 暗号化および復号化を処理するための専用暗号プロセッサ
 - Web アプリケーションのセキュリティやアプリケーション アクセラレーションなど、高度なアプリケーション サービスをサポートするための 2 つのドーター カード(オプション)
- Cisco ACE アプリケーション スイッチ モジュールのデータ プレーンは、5 つの主要ハードウェア コンポーネントのうちの 4 つで構成されています。Cisco ACE モジュールにはマルチコア ネットワーク プロセッサが使用されているため、アプリケーション配信サービスのパフォーマンスは著しく向上します。さらに、最も一般的な機能を選択した場合、このハードウェアベース アプリケーション配信モジュールは、汎用プロセッサベースのアプリケーション配信デバイスよりもパフォーマンス レベルが向上します。Cisco ACE モジュールのパフォーマンスを目的のレベルに引き上げるために、機能を犠牲にする必要はありません。Cisco ACE ハードウェア アーキテクチャでは、16 Gbps のスループット、クライアント/サーバ間の 400 万の同時接続、64,000 の Access-Control-List (ACL; アクセス コントロール リスト) エントリ、100 万の Network Address Translation (NAT; ネットワーク アドレス変換) エントリ、400 万の Port Address Translation (PAT; ポート アドレス変換) エントリを使用できます。このようなパフォーマンスは、ソフトウェアベースのアプリケーション配信デバイスでは実現が困難です。
- **最大 64 Gbps スループットへのスケーラビリティ:** Cisco ACE アプリケーション スイッチは、最大 64 Gbps のスループットに線形的に拡張可能な、業界唯一のアプリケーション配信製品です。単一の Cisco ACE モジュールで 16 Gbps を超えるスループットが必要な場合は、同じ Cisco Catalyst 6500 シリーズ スイッチ シャーシに最大 4 つの追加モジュールを導入できます。ケーブルやラック スペースを追加する必要はありません。独立したネットワーク テスト ベンダーである Miercom によって検証されたテスト結果によると、Cisco Catalyst 6500 シリーズ スイッチ シャーシ内の 4 つの Cisco ACE モジュールで、理論上の上限値 64 Gbps に近いスループットを実現できました(どのシャーシまたはバックプレーンも、上限に到達していません)。Cisco ACE モジュールのアーキテクチャを使用すると、アプライアンスベース ソリューションを使用した場合よりも、運用およびデータセンターの電力、スペース、および冷却コストが削減されます。また、ご使用のサーバベース アプリケーション配信デバイスを統合できるため、アプリケーションサーバ インフラストラクチャの使用効率が高まります。

- **投資保護:** Cisco ACE モジュールの設計目的は、機能を追加するために 2 枚のドーター カードをサポートすることです。2 枚のドーター カードを使用すると、アプリケーション セキュリティおよびアプリケーション アクセラレーションなど、より高度なアプリケーション 配信サービスを多数実行できます。2 枚のドーター カードのサポートにより、初期投資を無駄にすることなく、機能を追加できます。サーバベース アプリケーション 配信 アプライアンスを使用する場合は、次世代ハードウェア アプライアンスを実現して、パフォーマンスの改善や機能の追加を図るために、機器を完全にアップグレードする必要があります。
- **インテリジェントなプロキシ アーキテクチャ:** 多くのアプリケーション 配信製品は、デフォルトで、基本的なサーバ ロード バランシングにも完全な TCP およびアプリケーション プロキシを実行しています。その結果、送信元の IP 保持、動的なロードバランシング アルゴリズム（「最小接続」アルゴリズムなど）などの基本機能が有効な場合、これらの製品のパフォーマンスは大幅に低下します。一方、Cisco ACE アプリケーション スイッチの設計目的は、必要な場合のみ完全プロキシをインテリジェントに実行して、パフォーマンスおよびスケーラビリティを最大化することです。特に、ロードバランシング ポリシーに基づいて接続を処理する場合は、次に示す 3 つのメカニズムの 1 つを自動的に選択できます。
 - **レイヤ 4 SLB:** 現在、多くのお客様は、クライアントおよび要求されたサービスに関する基本情報に基づいて、多数のサーバ ロードバランシング判断を行っています。通常、これらのロードバランシング判断は、IP および TCP レイヤ (IP または MAC アドレス、TCP、または User Datagram Protocol [UDP] ポート番号) で実行されるため、SLB デバイスで TCP 接続をプロキシ化する必要はありません。したがって、SLB ポリシーがレイヤ 2 ~ 4 情報に基づいている場合、Cisco ACE は TCP 接続をプロキシ化しません。実際、接続をプロキシ化しても、デフォルトでは利点がありません。サーバ ロード バランサを導入してプロキシ化しても、複雑さが増し、パフォーマンスおよびスケーラビリティが低下するだけです。
 - **レイヤ 7 SLB の遅延バインディング:** アプリケーションおよび提供サービスが複雑化するにつれて、レイヤ 7 ロードバランシングが適用されるトランスポート レイヤ (TCP レイヤ) よりも上位のレイヤで、ロードバランシング判断を行う必要性が高まります。パケット ペイロードを検査し、ヘッダーおよびフィールドを識別して、ユーザ要求のインテリジェントなロード バランスを実行できるようにするには、レイヤ 7 ロード バランシングで TCP 接続をプロキシ化する必要があります。Cisco ACE アプリケーション スイッチは、設定されたロードバランシング ポリシーおよび機能に基づいて、必要に応じて TCP 接続をプロキシ化、プロキシ化解除、または再プロキシ化できる唯一の製品です。たとえば、HTTP URL ベース ロード バランシングやクッキーベース セッション保持などの一部の機能を使用するには、Cisco ACE で、他のプロキシの場合と同様に HTTP ヘッダーまたはその他のレイヤ 5 ~ 7 データを解析し、TCP 接続を終了する必要があります。ただし、Cisco ACE が TCP 接続を「プロキシ化解除」するのは、適切なロードバランシング判断を行うために必要なデータが解析されたあとです。この方法 (別名「遅延バインディング」) を使用すると、後続のデータ パケットの処理が高速化されるため、システムのパフォーマンスが改善されます。同時に、Cisco ACE は、機能が必要とされるときは常に接続を随時「再プロキシ化」することができます。たとえば、HTTP 1.1 接続を保持するには、同じ TCP 接続を介してあとで送信される追加クライアント要求を解析する必要があります。Cisco ACE はこの追加情報を調べるために、接続をプロキシ化解除モードから再プロキシ化モードに切り替えます。接続ごとにプロキシ化モードとプロキシ化解除モードを切り替える Cisco ACE の機能により、実際のパフォーマンスは大幅に向上します。
 - **高度な SLB 機能およびサービスのための完全プロキシ化:** より高度な SLB 機能として、データ ストリーム全体を処理 (解析または変更) する機能があります。このような機能を実現するには、完全プロキシ化方式が必要です。たとえば、SSL オフロード、TCP 再利用、

FlashForward、デルタ符号化などのアプリケーションアクセラレーション機能を使用するには、Cisco ACE アプリケーション スイッチでクライアント接続をプロキシ化する必要があります。Cisco ACE アプリケーション スイッチは、ハードウェアベースの最新の完全プロキシ化アーキテクチャで、これらの機能をすべてサポートしています。新しい接続が確立されるたびに、スイッチは完全プロキシ化が必要かどうかを選択して、最大パフォーマンスと高度な処理のバランスを取ります。

- **ロールベース管理:** お客様の通常的环境では、アプリケーション配信デバイスは複数の機能グループ(ネットワーク管理者、アプリケーション管理者、システム管理者、セキュリティ管理者など)で管理されます。従来のアプリケーション配信ソリューションでは、ワークフローの調整作業が複雑なため、アプリケーションの導入が遅くなることがありました。新しいアプリケーションの導入、または既存アプリケーションのテストやアップグレードを行うために、アプリケーション グループはネットワーク管理者や、デバイスの所有者すべてと連携しなければならないことがあります。アプリケーション配信デバイスに必要な設定変更を行うには、複雑な調整作業が必要です。Cisco ACE では、この課題を解決するために、仮想デバイスごとにカスタマイズ可能な詳細 Role-Based Access Control (RBAC; ロールベース アクセス コントロール)を実行します。Cisco ACE は、カスタマイズ可能な RBAC 機能を提供する、業界唯一のアプリケーション配信製品です。Cisco ACE RBAC メカニズムにより、デバイス管理者はユーザ アクセスに必要な機能およびリソースに基づいて、ユーザにロールを割り当てることができます。ロールは、実サーバ、サーバ ファーム、VIP、これらで実行可能なアクション(作成、変更、削除、ミラーリング)などのリソースおよびユーザ作成オブジェクトにアクセスするための一連の権限を定義します。Cisco ACE には、8 つのロールが事前定義されています。これらを使用してカスタム ロールを作成し、さまざまな組織構造に対応することもできます。ネットワーク管理者は Cisco ACE 仮想化と RBAC を組み合わせて、IT 内のその他の機能グループに対応する隔離された設定ドメインを作成できます。ネットワーク管理者は IT 内の機能グループに単一仮想デバイス内のロール(設定権限)を割り当てて、ワークフローからこれらを削除することができます。同時に、その他の仮想デバイスで有効な既存アプリケーションに対する設定ミスリスクを軽減できます。この改善されたワークフローにより、「セルフサービス」モデルが作成されます。このモデルでは、アプリケーション グループによるアプリケーションのテスト、アップグレード、および導入が、従来方式よりも短時間で、独立的に実行されます。
- **階層型管理ドメイン:** Cisco ACE アプリケーション スイッチには、カスタマイズ可能な RBAC のほかに、階層型管理ドメイン機能もあります。管理者はこの機能を使用して、実サーバ、VIP アドレス、サーバ ファームなどのユーザ定義オブジェクトをドメインにグループ化し、このデバイスの管理ユーザにドメインを割り当てることができます。ドメイン内のユーザ定義オブジェクトに実行できる処理、およびユーザが使用できるコマンド セットは、ユーザに割り当てられたロールによって決まります。Cisco ACE のデフォルト動作では、仮想デバイスの作成時に、デフォルトドメインが作成されます。すべてのオブジェクトは、このデフォルトドメインに割り当てられます。グローバル デバイスの管理者または各仮想デバイスの管理者は、特定の要求に基づいて、追加ドメインを作成できます。ユーザまたは管理者が新しいオブジェクトを作成すると、オブジェクトは適切なユーザドメインに自動的に追加されます。階層型管理ドメイン機能を使用すると、特定のオブジェクト セットに対するアクセスを制限できます。たとえば、複数のアプリケーション(apps1 および apps2)が仮想デバイスにホストされているにもかかわらず、別のチームによって管理されている場合、管理者はアプリケーション apps1 のすべてのオブジェクト(VIP、実サーバ、およびサーバ ファーム)をドメイン(domain1)にグループ化して、アプリケーション apps1 の管理ユーザに domain1 のアクセス権を割り当てることができます。apps1 のユーザは apps1 のオブジェクトにのみアクセスし、管理することができます。apps2 を管理するアプリケーション ユーザに

は、その逆が成り立ちます。これにより、設定は簡素化され、アプリケーションが完全に隔離されて、アプリケーションのオペラビリティが向上します。

- **管理:** Cisco ACE アプリケーション スイッチを管理、監視、およびレポートするには、精密さやカスタマイゼーションに関する要件に応じて、さまざまなツールおよびフォーマットを使用します。たとえば、CLI(コマンドライン インターフェイス)、GUI、SNMP(簡易ネットワーク管理プロトコル)、および XML インターフェイスを使用します。
 - **XML インターフェイス:** Cisco ACE アプリケーション スイッチは、Network Management Station(NMS; ネットワーク管理ステーション)からリモート設定および監視を実行できる、強力で柔軟な XML インターフェイスをサポートしています。Cisco ACE XML インターフェイスは、XML ドキュメントを HTTP または HTTPS を介して交換することにより、すべての Cisco ACE CLI コマンドをサポートします。さらに、コマンド出力を NMS に XML フォーマットで転送して、監視および分析するように、Cisco ACE スイッチを設定することもできます。Cisco ACE には、CLI クエリーをフォーマットしたり、XML 結果を解析したりするための XML Document Type Definition(DTD)スキーマが用意されています。
 - **SNMP:** Cisco ACE アプリケーション スイッチには、Cisco ACE デバイスのモニタリングおよび設定をサポートする、仮想化 SNMP エージェントが組み込まれています。各 Cisco ACE 仮想デバイスには独自の SNMP 設定があり、最大 10 台の管理ステーションにトラップを送信することもできます。Cisco ACE は、モニタリング用の標準および拡張アプリケーション ネットワーク サービス(サーバ ロード バランサなど)の MIB だけでなく、設定 SNMP MIB もサポートしているため、これらのデバイスにリソースを割り当てるなどして、Cisco ACE 仮想デバイスを作成および管理することができます。Cisco ACE は SNMP バージョン 1(SNMPv1)、SNMPv2c、および SNMPv3 をサポートします。SNMPv3 エージェントは強力な認証および暗号化を使用して、デバイスへのセキュアなアクセスを実現します。可能なかぎり、SNMPv1 および SNMPv2c でなく、SNMPv3 を使用してください。Cisco ACE SNMP エージェントは、User-Based Security Model(USM; ユーザベース セキュリティ モデル)および RBAC を含めて、RFC 3414 および 3415 を実装します。Cisco ACE を使用すると、SNMPv3 ベースのユーザ管理を Authentication, Authorization, Accounting(AAA; 認証、認可、アカウントング)サーバ レベルで集中実行できます。このユーザ管理機能の集中化により、Cisco ACE で稼働する SNMP エージェントは AAA サーバのユーザ認証サービスを利用して、Cisco ACE 管理機能へのセキュアなアクセスを実現できます。
 - **CLI:** Cisco ACE アプリケーション スイッチには、仮想デバイスを設定したり、さまざまなデバイス統計情報を表示したりするための総合的な CLI が組み込まれています。Cisco ACE CLI で使用される構文は、Cisco IOS[®] ソフトウェアの構文と同じであるため、Cisco IOS ソフトウェアに熟練したお客様は、設定および管理を簡単に実行できます。
 - **GUI:** Cisco ACE アプリケーション スイッチには、組み込みデバイス マネージャ¹ および中央集中型の Cisco Application Networking Manager(ANM)ソフトウェアが用意されていて、Cisco ACE デバイスをプロビジョニング、モニタ、レポート、およびトラブルシューティングすることができます。Cisco ANM ソフトウェアは、データセンター内の複数の Cisco ACE デバイスの管理に役立ちます。ネットワーク管理者は Cisco ANM を使用して、Cisco ACE 仮想デバイスを作成、変更、および削除したり、仮想デバイス間のリソース割り当てを制御したりできます。これらの仮想デバイス内で Cisco ANM を使用すると、すべてのアプリケーション ネットワーク サービスを完全に設定できます(ロード バランシングや SSL オフロードなど)。Cisco

¹ 組み込みの Device Manager(DM)は、Cisco ACE アプライアンスでのみ使用できます。Cisco ACE モジュールを設定および管理するには、ANM が必要です。

ANM ソフトウェアは、Red Hat Enterprise Linux v4 Enterprise Server(ES)4 Update 2 以上、または Advanced Server(AS)V4 Update 2 以上がインストールされた任意の x86 プラットフォームで稼働します。Cisco ANM には、以下のような重要な利点が多数あります。

デバイス管理の簡素化: Cisco ANM には基本ユーザ、アドバンスド ユーザ、およびエキスパート ユーザ向けのさまざまなプロビジョニング フォームが組み込まれているため、どのスキルレベルのオペレータも、共通アプリケーション ネットワーク サービスの予定の導入または即時の導入を、短時間で実行したり、変更したりできます。オペレータがシステムを新規に使用する場合も、基本フォームを使用することにより、最も一般的なサービスをすばやく簡単にプロビジョニングして、Cisco ACE システムを「箱から出してすぐに」利用できます。より知識のあるユーザは、アドバンスド フォームを使用して、Cisco ACE のさらに強力な機能を簡単に実行できます。Cisco ACE システム自体をマスターする必要はありません。さらに熟練したユーザは、ANM エキスパート モードまたはテンプレートベースの設定管理を使用して、サービスを完全に設定できます。

テンプレートベースの迅速なプロビジョニング: CLI またはプログラムのな方法を使用しないで、Cisco ACE の高度な機能を実行する必要があるエキスパート ユーザは、Cisco ANM のテンプレートベース プロビジョニングを使用することによって、複雑な設定を短時間で導入し、仮想デバイスおよびサービスに関してこれらの設定の標準化をサポートします。テンプレートを作成するには、エキスパート モード インターフェイスを使用するか、または既存設定を「クローニング」します。したがって、基本またはアドバンスド フォームベース プロビジョニングによって作成された設定から、テンプレートを作成できます。これらのテンプレートを拡張して、より複雑で特殊なサービス実装をサポートすることもできます。テンプレート内に設定を作成したら、バージョンの「タグging」を使用して、この設定が編集されないように保護することができます。このようにすると、テンプレートに格納してサービス作成や監査に使用した内容は、明確にトレースできない場合、今後変更できなくなります。この機能により、適切な監査および制御も可能になり、エラーまたは問題のある設定を、必要に応じて迅速にロールバックできるようになります。この機能を使用すると、企業は業務の変更を防止できます。これは、ネットワークおよびサービスの信頼性を向上するのに重要で、またこれにより同時に業務全体のコストを削減することもできます。

コンフィギュレーションの監査: Cisco ANM の監査機能を使用すると、物理または仮想デバイスの実行コンフィギュレーションを直前に検証されたコンフィギュレーションやその他の実行コンフィギュレーションと比較できます。コンフィギュレーションを容易に比較できるため、任意の 2 つの物理デバイス、仮想デバイス、またはテンプレートの違いをすばやく評価できます。この評価機能により、設定エラーをトラブルシューティングし、ネットワーク問題の最も一般的な原因の 1 つを解決できます。

モニタリングとレポート: Cisco ANM は、リアルタイムのデバイスおよびサービス モニタリングを通して、管理対象の Cisco ACE 仮想デバイスおよびサービスのヘルス、パフォーマンス、および用途に関する最新情報を提供します。運用スタッフはこのモニタリングを使用して、問題の原因を特定できます。Cisco ANM はリアルタイム レポートおよび履歴レポートもサポートしています。Cisco ANM の即席の再帰レポート、およびスケジュールされた再帰レポートを使用することにより、システム管理者およびネットワーク管理者は処理を簡素化し、サービス使用率レポートの機能を有効にして、リソース要求を計画することができます。

詳細なアクセス コントロールおよび監査: Cisco ANM はすべての Cisco ACE 機能に対して、管理上定義された RBAC セキュリティ モデルを使用して、Cisco ACE の運用、管理、およびモニタリングに関する権限および役割(特定のロードバランス対象サーバのアクティブ化や保留など)を委任することができます。Cisco ANM 管理者は、各ユーザまたはユーザ グ

ループが使用できるタスクおよびオプションを定義できます。Cisco ANM ユーザ監査により、すべてのユーザが行うすべてのアクティビティを確実に記録できるようになります。この情報を使用できるのは、監査用の権限を持つユーザのみです。

業務委任サーバの管理: Cisco ANM は業務固有の表示を提供して、サービスおよびサーバマネージャの生産性を高めます。サーバ マネージャでは Cisco ANM を使用して仮想 (VIP) および実サーバを監視し、サーバで現在アクティブな接続数をトラッキングしたり、日常的な管理タスクを実行したりできます。たとえば、グレースフル シャットダウンや接続解除を行って、1 つ以上の実サーバを稼働中またはアウト オブ サービスの状態にします。この場合、ネットワークポロジやその他のネットワーク操作に関する知識は不要です。

- **トラブルシューティング ツール:** Cisco ACE アプリケーション スイッチは、運用管理を簡素化するためのさまざまなトラブルシューティング ツールをサポートしています。
 - **パケットキャプチャ ツール:** Cisco ACE アプリケーション スイッチは、内部を通過するネットワーク トラフィックのパケット情報をキャプチャできます。キャプチャされたパケットは、Cisco ACE アプリケーション スイッチまたはリモート サーバのフラッシュ メモリ内のファイルに格納できます。パケットキャプチャ ツールは、Cisco ACE アプリケーション スイッチの接続問題のトラブルシューティングや、疑わしいアクティビティのモニタリングに役立ちます。Cisco ACE アプリケーション スイッチは、パケット キャプチャのほかに、内部を通過するネットワーク トラフィックの tcpdump もサポートします。
 - **Syslog メッセージング:** Cisco ACE はシステム メッセージのログギングをサポートし、記録されたメッセージを 1 つ以上の出力位置に送信できます。システム ログ メッセージは、モニタリングやトラブルシューティング用のログギング情報を提供します。管理者は ACE の柔軟なログギング機能を使用することにより、Cisco ACE のシステム メッセージの処理方法をさまざまにカスタマイズできます (接続の設定および切断メッセージのログギング、メッセージの重大度の制御、メッセージ生成の制限など)。Cisco ACE Syslog メッセージのログギング機能は、仮想デバイスレベルでイネーブルまたはディセーブルにできます。
 - **設定のロールバック:** 設定のロールバック機能を使用すると、新しい設定変更によって予期せぬ問題が発生した場合に、リポートしなくても、直前の既知の安定した設定に即座に戻すことができます。Cisco ACE アプリケーション スイッチは、仮想デバイスごとに、既知の安定した設定のチェックポイントを最大 10 個サポートします。
- **個別のコントロール プレーンおよびデータ プレーン:** Cisco ACE は、インバンドおよびアウトオブバンド通信チャネルを明確に区別する、業界唯一のアプリケーション配信製品です。つまり、Cisco ACE モジュール宛ての管理トラフィック、およびユーザ定義ポリシーで許可されている管理トラフィックはすべて、専用のコントロールプレーン プロセッサに送信して処理できます。コントロール プレーンは Cisco ACE モジュールとの管理インターフェイスを提供し、サーバ ヘルスのプローブ、XML インターフェイス、CLI によるデバイス管理、SNMP MIB、Syslog メッセージ、Address Resolution Protocol (ARP; アドレス解決プロトコル) による解決、ルーティング プロトコル、ACL 編集など、多数の機能をサポートします。コントロール プレーンを使用しても、Cisco Catalyst 6500 シリーズ スイッチから接続またはパケットが直接送受信されることはありません。ネットワーク プロセッサにはより高度な保護機能があるため、管理トラフィックは常にネットワーク プロセッサを経由します。この保護機能には、プロトコルまたはクライアント送信元 IP アドレスに基づく管理トラフィックの許可または拒否、Telnet または Secure Shell (SSH; セキュア シェル) プロトコルの同時セッション数の制限、コントロール プレーンの管理接続数またはトラフィックの制限などがあります。また、コントロール プレーンは、独立したアウトオブバンド相互接続上で、残りのハードウェア コンポーネントと通信します。したがって、コントロール プレーンはヘルス モ

ニタリング、ハイ アベイラビリティ、および管理インターフェイスへのアクセスに関して影響を受けません。データプレーン上に大量のデータトラフィックがある場合でも同様です。

- **拡張に応じた投資:** Cisco ACE アプリケーション スイッチは、小規模から大規模までの企業、およびサービス プロバイダーの要件を満たします。固有のソフトウェア ライセンス機能を使用することにより、ビジネスの拡大に応じて、1 から 2 Gbps(アプライアンス型の場合)に、または 4 から 16 Gbps(Cisco ACE モジュールの場合)に拡張できます。たとえば、4 Gbps のスループットから開始したあと、追加アップグレード ライセンスを購入して、8 または 16 Gbps スループットに拡張することができます。システムを完全にアップグレードする必要はありません。アプリケーションをオフラインにしなくても、ソフトウェア ライセンスをアップグレードできます。また、Cisco ACE には、仮想化(50 ~ 250 の仮想デバイス)および SSL など、その他の高度な機能を利用するための差分ライセンスもあります。
- **レイヤ 2 およびレイヤ 3 デバイスとの緊密な統合:** スタンドアロン Cisco ACE アプリケーション スイッチ アプライアンスは小規模環境に最適ですが、中規模から大規模環境の場合は、スイッチングおよびルーティング データセンター インフラストラクチャと透過的に統合される Cisco ACE アプリケーション スイッチ モジュールが非常に便利です。Cisco ACE アプリケーション スイッチ モジュールと Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズの緊密な統合には、次のような多くの利点があります。
 - **ケーブルおよびスペース要件の緩和:** Cisco ACE アプリケーション スイッチ モジュールは、Cisco Catalyst 6500 シリーズ バックプレーンと 16 Gbps で全二重接続され、スイッチ内のスロットを 1 つしか占有しません。
 - 電力および冷却要件の緩和
 - Cisco Catalyst 6500 シリーズ スーパーバイザ エンジンの Cisco IOS ソフトウェアのレイヤ 2 およびレイヤ 3 機能を使用した、設定タスクの簡素化
 - コスト効率を高めるためのポート密度の向上
 - 同じ Cisco Catalyst 6500 シリーズ スイッチ内で最大 4 つの Cisco ACE アプリケーション スイッチ モジュールを使用できるようにして、パフォーマンスおよびスケーラビリティを強化
 - **セキュリティの強化:** Cisco Catalyst 6500 シリーズ スイッチとの統合によって、ユーザベースまたはフロー単位のレート制限やプライベート VLAN などのセキュリティ機能が追加されます。Cisco ACE アプリケーション スイッチ モジュールは、プライベート VLAN の「混合モードポート」として機能することができます(図 5 を参照)。このため、いずれかのセカンダリ VLAN 内にある任意のサーバと通信しながら、Cisco Catalyst 6500 ハードウェアを利用して、隔離ポート上にあるデバイス間、あるいは別のコミュニティに属するデバイス間の通信をすべてブロックすることができます。
 - **管理の簡素化:** Cisco Catalyst 6500 シリーズ スイッチ スーパーバイザ エンジンから Cisco ACE アプリケーション スイッチ モジュールにアクセスできます。また、スーパーバイザ エンジンにすべての、または重要な Syslog メッセージを送信したり、Cisco ACE アプリケーション スイッチ モジュールをスーパーバイザエンジン オペレーティング システムから独立してアップグレードしたりできます。
 - **レイヤ 2 およびレイヤ 3 の仮想化およびネットワーク セグメンテーションの拡張:** Cisco ACE アプリケーション スイッチ仮想デバイスを VLAN だけでなく、Virtual Route Forwarding (VRF) インスタンスにマッピングして、スーパーバイザ エンジン上の別のネットワーク インスタンスを関連付けることができます(図 6 を参照)。

図 6 プライベート VLAN の「混合モード ポート」として機能する Cisco ACE アプリケーション スイッチ

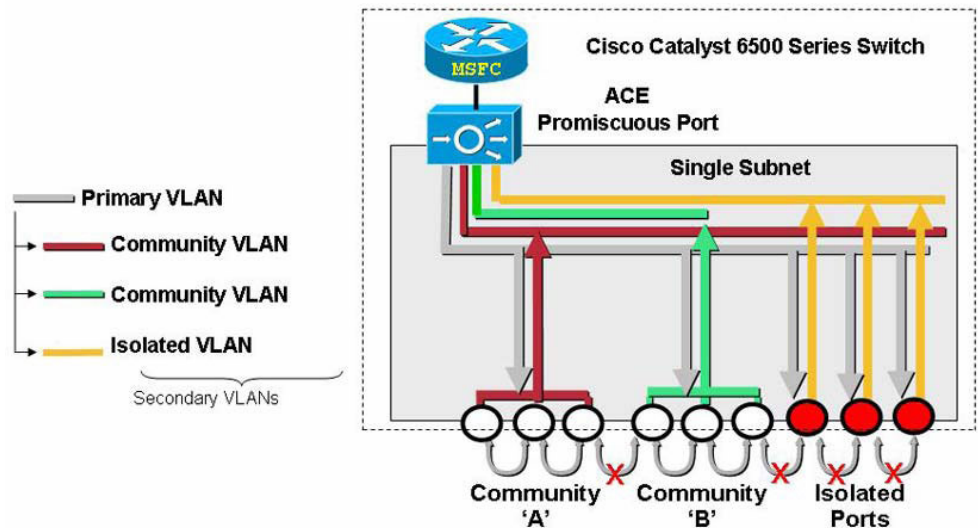
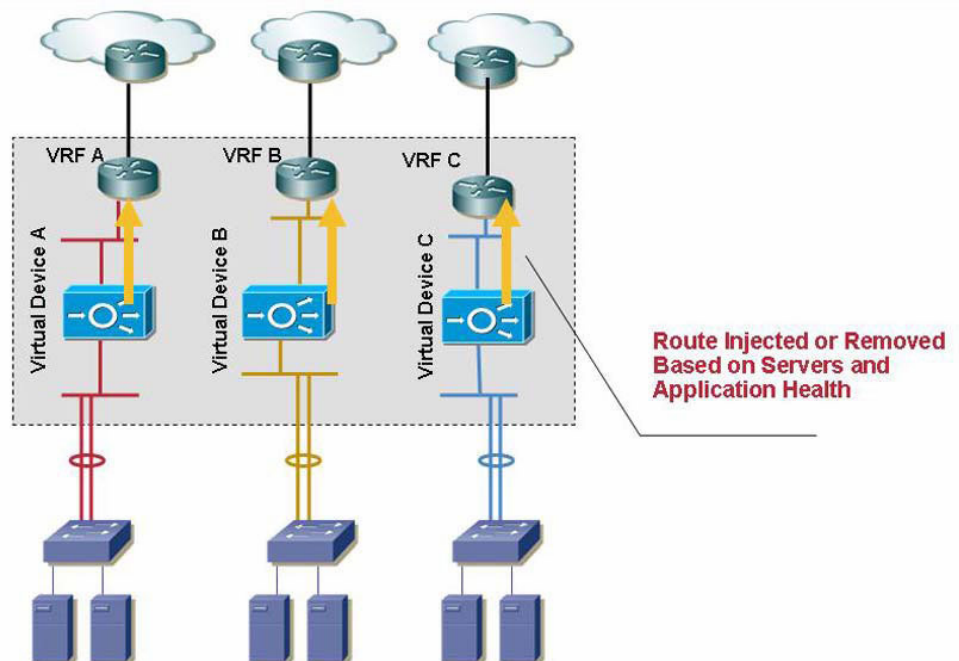


図 7 Cisco ACE アプリケーション スイッチのハードウェア プラットフォーム



高度なアプリケーション アクセラレーション

Cisco ACE には、強力かつ総合的なアプリケーションアクセラレーション機能があります。この機能を使用すると、帯域幅制限、遅延、データセンター統合、グローバルに分散したユーザーに関するアプリケーション パフォーマンス上の課題が解決されます。Cisco ACE では次に示す機能を組み合わせて、アプリケーションのパフォーマンスを高めています。

- コア ビジネス トランザクションのためにサーバ処理サイクルを戻すサーバ オフロード機能

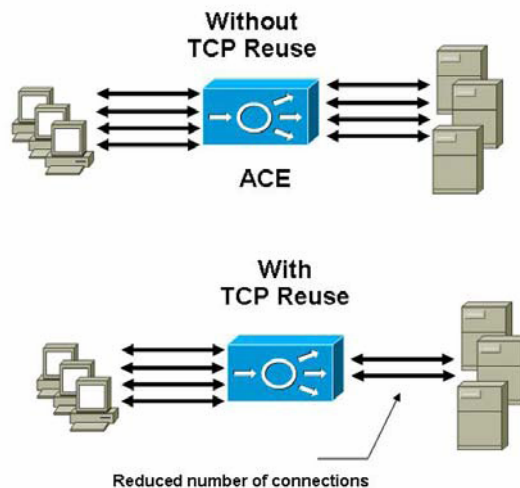
- 帯域幅を最適化するための帯域幅削減機能
- HTTP や Common Internet File System (CIFS) などのチャッティなプロトコルによって生じる、クライアント/サーバ間のラウンドトリップ時間を最小化するための遅延削減機能

この総合的な Cisco ACE アプリケーション スイッチ ソリューションを使用すると、WAN に導入されたアプリケーションの応答時間を、これまで LAN 環境でのみ² 可能だったレベルに引き上げることができます。Cisco ACE には、専用クライアント ソフトウェアを使用しないで、エンドユーザ応答時間などのアプリケーション パフォーマンス メトリックをグラフィカルに表示できる機能もあります。これにより、ユーザはアプリケーションのボトルネックをすばやく識別し、トラブルシューティングすることができます。

- **サーバ負荷の軽減:** 多くの企業にとって驚きなのは、Web 機能およびアプリケーションをサポートするために非常に多くのサーバ機能が必要であるということです。Cisco ACE には、企業の IT 導入に適した独自の 방법으로、さまざまなサーバ オフロード機能が組み込まれています。次に示す機能を組み合わせると、サーバ サイクルを最大 90% 削減できます。

- **TCP 設定オーバーヘッドのオフロード:** クライアントから要求が送信されるたびに、サーバは重要な CPU リソースを消費して、TCP 接続を設定および切断します。ただし、これらの重要なリソースは、サーバで実際に稼働しているアプリケーションの処理に使用できたと考えられます。Cisco ACE アプリケーション スイッチの TCP サーバ再利用機能は、CPU を使用する TCP 設定および切断機能をサーバからオフロードします。これにより、接続を維持し、複数のクライアント接続で再利用できるようになるため、サーバで同時にオープンされる接続数が削減されます。独立したネットワーク テスト ベンダーである Miercom によって検証されたテスト結果によると、Cisco ACE の TCP サーバ再利用機能を使用した場合、80,000 のクライアント接続に対してテスト サーバが確立した TCP 接続数は 400 のみでした。

図 8 Cisco ACE の TCP サーバ再利用機能

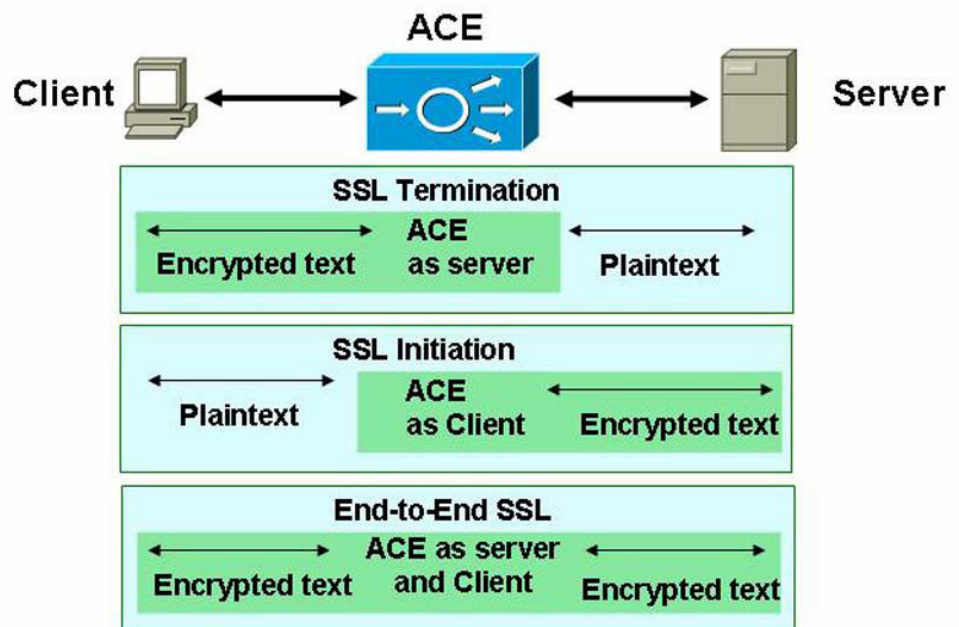


- **SSL オフロード:** SSL プロトコルは、企業のビジネス トランザクションのセキュリティ、プライバシー、および機密性を確保するための業界標準になっています。SSL 処理は CPU を消費し、サーバ プラットフォームによって制御されます。Cisco ACE アプリケーション スイッチは、SSL ト

² ACE 4710 アプライアンスでは、Cisco の高度なアプリケーション アクセラレーション機能がサポートされています。Cisco ACE モジュールでは、SSL および TCP オフロード機能のみがサポートされています。

ランザクションをオフロードして高速化するために、サーバ認証、秘密鍵や公開鍵の生成、証明書管理、データ パケット暗号化および復号化、デルタ最適化や FlashForward 機能によるサーバ応答の圧縮など、すべての SSL 機能を処理します。Cisco ACE ではこれらの機能をすべて使用して、SSL ベース トランザクション数を大幅に削減し、SSL の性能を 4 倍に向上させます。また、Cisco ACE には、お客様が各 Cisco ACE 仮想デバイスで証明書およびキー ファイルを作成できるという柔軟性があります。フラッシュ メモリ内にセキュアなストレージ領域が作成され、各仮想デバイスに関連する証明書および鍵が格納されます。SSL セッション中にクライアントまたはサーバとして機能するように、Cisco ACE アプリケーション スイッチを設定できます。Cisco ACE は 3 つのタイプの SSL アプリケーション (SSL 終了、SSL 開始、エンドツーエンド SSL) をすべてサポートします (図 9 を参照)。

図 9 Cisco ACE でサポートされる SSL 接続



- **レイジー要求評価:** 多くの Web アプリケーションは、Web コンテンツをグローバルにアップデートするために定期的に停止されます。実際、エンド ユーザからアプリケーションへのアクセスは、一定期間ブロックされます。たとえば、ユーザ要求によって再コンパイルを開始できますが、その期間中に別の要求が着信してキューイングされ、すべてのユーザが待機するようになることもあります。レイジー要求評価を使用すると、要求があった場合は常にキャッシュされたコピーを処理し、バックエンド処理が完了したら、オリジン サーバからコピーを自動的にリフレッシュするように、Cisco ACE アプリケーション スイッチを設定できます。この機能が有効なデバイスは、常に動的キャッシュ内のコンテンツを処理します。その結果、クライアント要求とオリジン サーバ応答は分離されます。
- **キャッシング:** Cisco ACE アプリケーション スイッチは静的キャッシングをサポートしています。これにより、イメージやアプレットなど、要求頻度の高い静的オブジェクトに関するクライアント要求はオフロードされます。この機能は完全に設定可能であるため、アプリケーション全体のパフォーマンスおよびトランザクション スループットが向上します。

- **適応性のある動的キャッシング**: Cisco ACE アプリケーション スイッチは動的コンテンツをキャッシュすることもできます。アプリケーションおよびデータベース サーバから CPU リソースをオフロードして、動的コンテンツ要求を実行します。動的キャッシングを設定できるため、Cisco ACE は URL クエリー スtring、HTTP ヘッダー、クッキー値など、特定のキャッシュパラメータに基づいて、指定 URL の応答を複数キャッシュできます。そのため、動的コンテンツを静的コンテンツと同様に処理して、パフォーマンスを高めることができます。単純なスクリプトを使用して個人データを動的にキャッシュし、コア トランザクションのためのリソースをサーバ上に確保することができます。
- **負荷ベースの動的キャッシング**: 高度なコンテンツ有効期限ポリシーを使用すると、動的コンテンツの新鮮度を保つことができます。Cisco ACE アプリケーション スイッチはサーバ負荷をリアルタイムで監視し、コンテンツの有効期間 Time-To-Live(TTL; 存続可能時間)イベントに関してインテリジェントなクローズド ループ判断を行い、サイトのパフォーマンスを最適化します。この機能は、負荷、時間、および URL に応じて設定できます。
- **帯域幅の削減**: 通常、アプリケーション配信の課題は、ネットワーク遅延の克服だけではありません。企業はコスト、アベイラビリティ、またはパフォーマンス上の理由から、帯域幅の使用を最小限に抑える必要もあります。Cisco ACE アプリケーション スイッチは、次の技術を適用して、帯域幅使用率を 70 ~ 90% 削減しながら、ユーザが認識できる形でハイ パフォーマンスを実現できます。
- **デルタ符号化**: Web ページ キャッシングを使用すると、静的ページに関する後続要求をサーバでなくキャッシュから取得できます。ただし、現在の HTML ページには、ユーザがインタラクティブ操作を実現するための動的リソースおよび Web コンテンツが多く含まれています。これらの動的リソースおよび Web コンテンツはキャッシュできません。サーバから取得する必要があるため、これによって帯域幅使用率、サーバ負荷、および応答時間は増大します。シスコはこの課題を解決するために、キャッシュされた元のページとアップデートされた新しいページの違いのみを符号化して、クライアントに配信する、デルタ符号化という独自のテクノロジーを導入しました。この革新的な方法を使用した場合、クライアント システムはサイズの小さなデルタを適用して、キャッシュ内のページから新しいページを動的に再構築できます。このプロセスは自動的かつ透過的に実行されます。ブラウザ クライアント、アプリケーション サーバ、またはクライアントを変更する必要はありません。
- **圧縮**: Cisco ACE アプリケーション スイッチは GZIP や DEFLATE などの標準圧縮だけでなく、デルタ符号化最適化や適応性のある動的キャッシング(この文書の後半で説明)など、サーバからのコンテンツを圧縮する多くの高度な圧縮技術をサポートしています。単純なバイト削減技術を備えたデバイスの場合、ページ サイズは 1/2 ~ 1/5 に削減されます。一方、Cisco ACE デルタ符号化の場合、ページの実際の変化量に応じて、ページ サイズが 1/10 ~ 1/50 に削減されることがあります。また、Cisco ACE はバイト圧縮を使用して、デルタ最適化によって既に縮小されたページをさらに縮小します。従来のアプリケーション配信デバイスで実行される既存の GZIP および DEFLATE と異なり、シスコで最適化された GZIP 圧縮は、Mozilla Firefox を含むすべてのブラウザ タイプと完全に互換性があります。
- **動的なブラウザ キャッシング**: Customer Relationship Management(CRM) およびポータル向けの多くのエンタープライズ アプリケーションでは、イメージ、JavaScript ファイル、ActiveX コントロール ファイル、バイナリ ファイルなどのオブジェクトに、キャッシュ不可というマークが付けられることがあります。この方式を使用すると、帯域幅が制限されたリモート ユーザの場合は特に、ダウンロード パフォーマンスは低下することがあります。Cisco ACE アプリケーション スイッチの Cisco ACE ジャストインタイム オブジェクト アクセラレーション テクノロジーは、これらの各オブジェクトの新鮮度をリアルタイムで自動的にトラッキングします。要求され

たオブジェクトが変更されていない場合、クライアントはキャッシュされたバージョンを使用します。Cisco ACE は、この特定のコンテキストで変更されたオブジェクトのみを配信します。

- **インテリジェントな画像の最適化:** Cisco ACE アプリケーション スイッチは画像ファイルをインテリジェントに圧縮して、画像品質を最適化します。これにより、画像のダウンロード時間は短縮され、ページ レンダリングは高速化され、帯域幅の使用効率は向上します。その他の方式では、画像が均一に圧縮され、このポリシーでは、ある画像については品質が大幅に低下し、別の画像についてはさらに圧縮する機会が失われることがあります。画像には大幅に圧縮できるものと、高精度を維持しなければならないものがあります。たとえば、事故の賠償請求に使用する JPG 画像は最大の解像度で保持できますが、スキャンされた保険契約証券は、読みやすさを損ねない範囲で大幅に圧縮することができます。
- **遅延の削減:** HTTP、TCP、CIFS などのネットワークおよびアプリケーション プロトコルは、クライアントとサーバ間に非常に頻繁なラウンドトリップを発生させるチャッティなプロトコルです。Cisco ACE アプリケーション スイッチには、クライアントとサーバ間のラウンドトリップを削減するためのさまざまなテクノロジーが組み込まれています。Oracle、SAP、Microsoft SharePoint、Microsoft Exchange など、さまざまな IP および Web ベース アプリケーションに、次に示す遅延削減機能を適用できます。
 - **FlashForward:** ほとんどの Web ページには、イメージ、スタイル シート、JavaScript ファイルなどのオブジェクトが埋め込まれています。これらのオブジェクトは、クライアントのブラウザにキャッシュされます。ただし、ブラウザでは、これらのオブジェクトの新鮮度を検証する必要があります。この検証が発生するたびに、クライアントからオリジン サーバに条件付き HTTP 要求が個別に送信されます。多数のオブジェクトが埋め込まれた Web ページは、検証(クライアント/サーバ間ラウンドトリップ)が完了するまで、レンダリングを待機する必要があります。これらの不要なクライアント/サーバ間ラウンドトリップにより、Web ページをレンダリングするための応答時間が長くなります。不要なブラウザ キャッシュ検証が発生しないようにするために、シスコは FlashForward という新しい独自のテクノロジーを導入しました。サーバに隣接した Cisco ACE は、このテクノロジーを使用してオブジェクトの新鮮度を検証できます。Cisco ACE の FlashForward 機能は、埋め込まれたすべてのオブジェクトをキャッシュし、情報を追加して変形してから、この変形後のオブジェクトに対するオブジェクト参照をページ内に再書き込みします。以後、このページにアクセスした場合、クライアント ブラウザはこのオブジェクトを検証する必要がなくなります。Cisco ACE はブラウザに代わってすべてのオブジェクトを検証します。変更されたオブジェクトがあれば、そのオブジェクトのみを送信します。この機能は、どの Web アプリケーションでも使用できます。
 - **スマート リダイレクト:** HTML メタ タグを使用すると、一定期間後に、クライアント要求をリダイレクトできます。ただし、このリダイレクション方式では、リダイレクトされたページ内の埋め込みオブジェクトごとに新鮮度を明示的にチェックするようブラウザが設定されるため、通常は非効率です。Cisco ACE のスマート リダイレクト機能は、HTML メタ タグベース リダイレクトをより効率的な、ブラウザ キャッシュの新鮮度検証要求をトリガしない HTTP ヘッダーベース リダイレクトに変換して、Web ページのリダイレクトを高速化します。この機能を使用すると、ページ応答時間が大幅に短縮され、メタ タグベース リダイレクトの柔軟性および生産性が低下することはありません。
 - **FastRedirect:** 301/302 ステータス コードを含む HTTP 応答は、ブラウザを別の場所にリダイレクトします。これにより、要求された Web ページのレンダリングは 2 つのラウンドトリップで行われ、エンド ユーザへの応答は遅くなります。Cisco ACE の FastRedirect 機能は、必要なラウンドトリップ数を 2 から 1 に削減して、HTTP ヘッダーベース 301/302 リダイレクトを高速化します。この機能を使用した場合、301/302 HTTP ステータスコード応答が処理され、

リダイレクトされたリソースがデータセンターの LAN を介して取得されるため、エンド ユーザーへの応答時間が短縮されます。

- **FlashConnect:** Cisco ACE の FlashConnect 機能は、応答をシリアルでなくパラレルに処理して、ブラウザのパフォーマンスを高めます。Microsoft の Internet Explorer Web ブラウザーはデフォルトで、HTML コンテナ ページで参照されるドメイン名ごとに確立された 2 つの TCP 接続のみを介して、オブジェクトを取得します。この制限があるため、要求は不必要にキューイングされることが多く、初回アクセス時のパフォーマンスが低下します。FlashConnect を使用すると、ドメインごとに使用される TCP 接続数を増やして、データ ダウンロードを大幅に高速化できます。

アプリケーションの保護

Cisco ACE アプリケーション スイッチには、さまざまなネットワークベース攻撃およびアプリケーション攻撃からスイッチ自体、およびデータセンターを保護するためのセキュリティ機能が多数組み込まれています。Cisco ACE アプリケーション スイッチはデータセンター内の最終防御ラインとして機能し、ネットワーク セキュリティおよびアプリケーション セキュリティを確保します。

- **ネットワーク セキュリティ:** 多くの企業では、「サイバー損失」のかなりの割合が、内部攻撃に起因しています。1/3 を超える企業 (39%) が、『2006 Computer Crime and Security Survey』に回答しています。たとえば、2005 年のサイバー損失の 20% 以上は内部攻撃が原因です。この年次調査は CSI で実行され、サンフランシスコの FBI Computer Intrusion Squad が参加しました。2006 年の CSI レポートに回答した 616 社のうち、313 社が 2005 年の内部犯罪に関連した損失を見積もることができたか、または見積もる予定でいます。内部攻撃から保護するためのベスト プラクティスとして最近普及しているのは、企業のプライベート ネットワークとパブリックインターネットが接する従来のネットワーク境界だけでなく、データセンターやブランチオフィスネットワークの WAN エッジにもファイアウォールを導入するという方法です。
- ファイアウォールをデータセンターに配置すると、企業は最新のコーポレート ガバナンスおよび業界ガバナンス命令に適合することもできます。たとえば、Sarbanes-Oxley (SOX) 法、Gramm-Leach-Bliley (GLB)、Health Insurance Portability and Accountability Act (HIPAA)、および Payment Card Industry (PCI) Data Security Standard には、情報のセキュリティ監査および追跡に関する要件が含まれています。
- Cisco ACE アプリケーション スイッチはスケーラビリティの高いパケット フィルタリング、NAS、プロトコル インスペクション、およびディープ パケット インスペクションを使用して、内部および外部攻撃からデータセンター ネットワークを保護できます。Cisco ACE アプリケーション スイッチには、セキュリティの最終防御ラインとしての役割があるため、企業の LAN スイッチ ポートと、データセンター内の Web、アプリケーション、およびデータベース サーバ ファーム間に配置できます。
- **パケット フィルタリング:** Cisco ACE アプリケーション スイッチは、内部を通過するすべてのトラフィックを検査し、ACL を使用して定義されたパケットフィルタリング ポリシーに基づいて、不要なトラフィックまたは不明なトラフィックを削除します。ACL は ACL エントリと呼ばれる、ネットワーク セキュリティ規則またはポリシーを一括して定義する一連の文で構成されます。各エントリは、エントリで指定されたデータセンター ネットワークの各部に対して、ネットワークトラフィック (インバウンドおよびアウトバウンド) を許可または拒否します。基準となるのは、送信元アドレス、宛先アドレス、プロトコル、プロトコル固有のパラメータなどです。Cisco ACE アプリケーション スイッチは、デフォルトで、ネットワーク インターフェイス上のトラフィックをすべて拒否します。トラフィックを許可する必要がある場合は、ACL を明示的に設定する必要があります。

ます。Cisco ACE は拡張 (IP トラフィックのネットワーク アクセス制御) ACL および EtherType (非 IP トラフィックのネットワーク アクセス制御) ACL を両方ともサポートします。Cisco ACE アプリケーション スイッチには、スケーラビリティの高い ACL エントリ (最大 64,000) が用意されています。

- **NAT:** Cisco ACE アプリケーション スイッチをクライアントとサーバの間に導入すると、クライアント IP 送信元アドレスを保護したり、送信元 IP アドレスをサーバ ネットワーク内のルーティング可能アドレスに変換してから、クライアント要求をサーバに送信したりできます。Cisco ACE アプリケーション スイッチは、ダイナミック NAT、ダイナミック PAT、スタティック NAT、およびスタティック ポート リダイレクションをサポートします。Cisco ACE アプリケーション スイッチは、最大 400 万の NAT 変換、および 100 万の PAT 変換を実現します。
- **ネットワークベースの大量攻撃:** Cisco ACE アプリケーション スイッチは DoS (サービス拒絶) 攻撃からサーバ ファームを保護します。DoS 攻撃は、単一システムまたはネットワーク全体に対するサービスを悪意を持って中断させるために、個人またはグループから行われます。この攻撃タイプでは、攻撃者は、システムまたはネットワーク リソースを過負荷で使用過剰な状態にします。DoS 攻撃の攻撃者の目的は、システムまたはネットワーク ユーザのサービス使用を妨害することです。Cisco ACE アプリケーション スイッチは、次に示す一般的なタイプのネットワーク関連 DoS 攻撃をブロックします。

LAND 攻撃: LAND 攻撃の場合、攻撃者はターゲット ホスト (被害者) に、送信元および宛先アドレスと同じ IP アドレスを含む TCP SYN パケットを送信します。この攻撃の目的は、ターゲット ホストに自身に対して応答パケットを送信させることです。このタイプの攻撃を防ぐために、Cisco ACE の TCP/IP 標準化機能は接続の送信元 IP アドレスおよび宛先 IP アドレスが有効であるか検証します。これらのアドレスが無効な場合は、接続を切断します。

ティアドロップ攻撃: 送信元マシンから宛先マシンに移動するパケットは、フラグメンテーションプロセスによって、より小さなフラグメントに分割されることがあります。ティアドロップ攻撃は、オフセット フィールドが過負荷の、一連の IP フラグメントを作成します。宛先ホストはこれらの不正な形状のフラグメントを組み立て直そうとして、最終的にクラッシュするか、またはリポートします。Cisco ACE は IP フラグメンテーション セキュリティ チェックを使用して、これらのタイプの攻撃をブロックします。

- **IP 標準化:** IP 標準化は、IP パケットに関して一連のチェックを実行するレイヤ 3 のセキュリティ機能です。デフォルトでは、これらのチェックはライン レートで実行されます。これらのセキュリティ チェックには、フラグメンテーション セキュリティ チェック、IP フラグメントの再組み立て、ヘッダー長、自動アンチスプーフィング (送信元 IP アドレス = 宛先 IP アドレス)、ユニキャスト RFP チェック、IP オプション検証、不法 IP アドレス、トランスペアレント モードでの ARP インスペクション、不明な ICMP タイプが含まれます。パケットがこれらのチェックの 1 つに失敗した場合、Cisco ACE は設定された IP パラメータに応じて、パケット廃棄などの適切なアクションを実行します。
- **TCP 標準化:** TCP 標準化は、一連のチェックを実行するレイヤ 4 セキュリティ機能です。デフォルトでは、これらのチェックはさまざまなフロー ステージ (初期接続設定から接続終了まで) で実行され、パフォーマンスは低下しません。Cisco ACE には、1 つ以上の高度な TCP 接続を設定して、多数のセグメント チェックを制御するという柔軟性があります。Cisco ACE はこれらの TCP 接続設定をライン レートで使用して、実行するチェックを判別し、チェック結果に基づいて TCP セグメントを廃棄するかどうかを判別します。また、異常なセグメントまたは形状が不正なセグメントを廃棄します。Cisco ACE は TCP 標準化機能を使用して、セッション ハイジャック、Xmas スキャン、Bonk、Jolt、Bloop、Targa、Boink、Fraggle、ヌル スキャンなどの挿入および回避ネットワーク攻撃をブロックします。

- **プロトコル インスペクション**: Cisco ACE アプリケーション スイッチはステートフルなアプリケーション プロトコル インスペクションを実行して、データセンター内のアプリケーションおよびサービスの使用を保護します。アプリケーション プロトコル インスペクション機能を使用すると、プロトコルの動作を検証し、Cisco ACE アプリケーション スイッチを通して送信される不要な悪意のあるトラフィックを識別することができます。Cisco ACE アプリケーション スイッチはユーザ定義トラフィック ポリシーに基づいて、指定パケットを許可または拒否することができます。

一部のプロトコルでは、パフォーマンスを高めるために、既知のポート上で初期セッションを使用してセカンダリ TCP または UDP ポートをオープンします。Cisco ACE のアプリケーション プロトコル インスペクション機能はこれらのセッションを監視し、動的なポート割り当てを識別し、特定のセッション期間中にこれらのポートでのデータ交換を許可します。

一部のアプリケーションでは、パケットのデータ ペイロードに IP アドレス情報を埋め込みます。プロトコルのペイロードに埋め込まれた IP アドレスを変換することが特に重要になるのは、NAT(ユーザによって明示的に設定)が導入されている場合、およびサーバ ロード バランシング(暗黙的 NAT)の場合です。アプリケーション プロトコル インスペクション機能を使用した場合、Cisco ACE アプリケーション スイッチは埋め込まれた IP アドレスを変換して、任意のチェックサム、または変換の影響を受けるその他のフィールドをアップデートします。
- Cisco ACE アプリケーション スイッチでは、現在、次のプロトコルのインスペクションをサポートします。

 - **Domain Name System(DNS; ドメイン ネーム システム)インスペクション**: Cisco ACE アプリケーション スイッチは、すべての DNS 攻撃をブロックします。Cisco ACE の DNS インスペクション機能は DNS 要求と応答を照合して、ラベルおよびドメイン名の最大長を適用し、応答受信後に UDP 接続を切断し、NAT 設定に基づいて DNS A レコードを変換します。
 - **FTP インスペクション**: Cisco ACE アプリケーション スイッチは、FTP の不正使用をブロックします。FTP インスペクション機能は FTP 要求と応答を照合し、切り捨てられたコマンドを削除し、RFC に準拠させ、RETR/STOR コマンドのサイズをチェックし、動的にネゴシエートされたポートの範囲を検証し、コマンドおよび応答スプーフィングをブロックし、ユーザが特定のコマンドを制限できるようにします。
 - **ICMP インスペクション**: ICMP を使用すると、ステートフル インスペクションを実行しなくても、データセンター ネットワークを攻撃できます。Cisco ACE アプリケーション スイッチはデフォルトで、パフォーマンスを低下させることなく、ICMP インスペクションを実行できます。ICMP インスペクション機能を使用すると、各要求に応答が 1 つのみ対応するようになり、要求のシーケンス番号が正しくなります。また、迷惑な ICMP エラーの流入が防止され、インターネット ドラフト draft-gont-tcpm-icmp-attacks.txt ファイルで指定された対策がサポートされます。Cisco ACE ICMP インスペクション機能は、Ping of Death や ICMP フラッディング(Smurf 攻撃)などの攻撃をブロックします。
 - **Real Time Streaming Protocol (RTSP) インスペクション**: RTSP は RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、および Cisco IP/TV[®] アプリケーションで使用されます。RTSP アプリケーションは、既知のポート 554、および制御チャンネルとして TCP(まれに UDP)を使用します。この TCP 制御チャンネルを使用すると、クライアントに設定されているトランスポート モードに応じて、音声およびビデオ トラフィックの送信に使用されるデータ チャンネルがネゴシエートされます。Cisco ACE の RTSP プロトコル インスペクション機能は、セッションを監視し、データ チャンネルの動的なポート割り当てを識別し、特定のセッション期間中に該当ポートでのデータ交換を許可します。

- **Web アプリケーションのセキュリティ:** Web アプリケーションのセキュリティは、Web アプリケーションを攻撃から保護するために設計された、新しい種類の情報セキュリティ テクノロジーです。HTTP は Web データおよびサービスを転送するために広範に使用されています。HTTP は現在のネットワーク帯域幅使用率の約 75% を占め、本来はアプリケーション ポート 80 を使用します。ほとんどのファイアウォールでは、ポート 80 は常時オープンされているため、ポート 80 宛てのトラフィックはすべて許可されます。ハッカー、ワーム、およびウイルスはこのピンホールを使用して、Web アプリケーションを攻撃し、また重要データにアクセスする可能性もあります。ネットワーク ファイアウォールおよび侵入検知システムは、これらの攻撃を防止できません。Web アプリケーション攻撃を最初の段階で防止するために、Cisco ACE アプリケーション スイッチは HTTP プロトコルのステートフル ディープ パケット インスペクションを実行して、ネットワークに入ろうとしている HTTP アプリケーション トラフィックを正確に判別します。ディープ パケット インスペクションは特殊なアプリケーション インスペクションです。Cisco ACE アプリケーション スイッチはパケットまたはトラフィック ストリームのアプリケーション ペイロードを調べ、データの内容に基づいて判断します。また、アプリケーション プロトコル(この場合は HTTP)が異常に動作しているかどうかを判別します。

HTTP インスペクション中にアプリケーション インスペクション プロセスで主に処理されるのは、HTTP ヘッダー、URL、ペイロードなどの HTTP 属性です。Cisco ACE アプリケーション スイッチは HTTP プロトコル インスペクションを使用して、次のようなさまざまな HTTP 攻撃をブロックできます。

- **暗号化チャネル攻撃:** Cisco ACE には強力な SSL オフロードまたは終了プロセッサが備わっているため、暗号化 SSL チャネルを利用してセキュリティ デバイスを迂回しようとする攻撃を完全に認識できます。
- **ワームおよび Day Zero 攻撃:** Cisco ACE HTTP インスペクション エンジンには、強力で完全にカスタマイズ可能な正規表現エンジンが組み込まれています。正規表現を使用すると、対処法が公開されていないワームおよび攻撃をブロックできるシグニチャを開発できます。HTTP ヘッダーおよび URL に関するポリシーを照合する Cisco ACE 正規表現を適用できます。
- **RFC 準拠:** Cisco ACE HTTP インスペクション エンジンは RFC 2616 に自動的に準拠します。定義された方式、MIME タイプ、または 転送符号化は削除されます。
- **バッファ オーバーフロー:** Cisco ACE は HTTP ヘッダー、コンテンツ、および URL の最大長を適用し、バッファ オーバーフロー攻撃から保護できます。
- **ディレクトリ トラバーサル:** Cisco ACE の正規表現フィルタを使用すると、HTTP GET 要求で ../. を使用して HTTP サーバのディレクトリ構造に到達しようとする試みをすべてブロックできます。
- **悪意のある URL:** 攻撃者は、URL でエスケープ符号化およびユニコード文字表現を組み合わせることで使用することにより、従来のネットワーク ファイアウォールでフィルタリングできない要求を送信できることがあります。たとえば、次の場合について考えます。従来のネットワーク ファイアウォールには、cmd.exe を含むすべての URL 要求を削除するセキュリティ ポリシーが設定されています。ただし、攻撃者は符号化された URL 要求を送信して (`http://www.example.com/app/../../../../winnt/system32/%63%6d%64%2e%65%78%65?c+dir`)、このポリシーをバイパスできます。Cisco ACE は常に URL 要求を標準化または正準化 URL に変換してから、セキュリティ ポリシーを適用して、符号化 URL を利用する攻撃をすべて防衛します。
- **ピアツーピア、インスタント メッセージング、および HTTP トンネル攻撃:** セキュリティに対する認識が高まったため、企業はインターネットと Web サーバの間に従来型のネットワーク ファイ

アウォールを追加するようになりました。ただし、ネットワーク ファイアウォールには制限があります。HTTP トンネリングを使用すると、これらのファイアウォールに関するアクセス コントロールの制限を回避できます。HTTP トンネリングは、HTTP ヘッダー内のトラフィックをカプセル化して、クライアントと目的のサーバ間に双方向通信チャネルを作成します。クライアント HTTP 要求を受信した Web サーバはカプセル化されたトラフィックを解析して、目的のサーバにパケットをリダイレクトします。Cisco ACE を Web サーバの前面に配置し、HTTP ヘッダー内にカプセル化トラフィックを含む HTTP 要求をブロックするように設定することができます。

- **URL マッピング:**もう 1 つのセキュリティ対策である Cisco ACE アプリケーション スイッチの URL マッピング機能は、HTML ソース内の URL を任意の URL ストリングで置き換えて、URL を隠します。この置き換えにより、エンドユーザはオリジン サーバで実際に使用されていた URL 構造を認識できなくなり、バックエンド インフラストラクチャを隔離できます。
- **XML および Web サービス ファイアウォール:**Cisco ACE の XML ゲートウェイは、非常に優れたパフォーマンスを持つ XML ファイアウォールです。現在は、独立したアプライアンス製品として入手できます。ただし、このファイアウォールは Cisco ACE アプリケーション スイッチと緊密に統合されています。Cisco ACE XML ゲートウェイの Web ベース ユーザ インターフェイスを使用すると、Cisco ACE アプリケーション スイッチのレイヤ 7 XML セキュリティ ポリシー、およびレイヤ 4 ~ 7 ロードバランシングとアプリケーション配信の機能の両方を設定できます。Cisco ACE の XML ゲートウェイには、次の XML および Web サービス ファイアウォール機能が組み込まれています。
 - マルチレイヤ ディープ メッセージ インスペクションによるセキュリティ攻撃からの保護
 - Web サービスの動作、ユーザ、およびメッセージに対する攻撃の認識
 - トランスポートおよびセッションからデータレベルまでのトランザクションの監視
 - Simple Object Access Protocol(SOAP)および XML トラフィックのリスクに関する検査および分類
 - Web Services Security(WS-Security)、XML デジタル署名、および X.509 に関する Web サービスの許可

まとめ

IT 企業が抱えている重要な課題は、グローバルに分散した従業員に十分なサービス レベルを提供しながら、アプリケーションおよび重要なビジネス データを配信することです。IT 企業はアプリケーション配信テクノロジーを使用することにより、すべての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を高めることができます。Cisco ACE はコアサーバ ロードバランシング サービス、高度なアプリケーション アクセラレーション、およびセキュリティ サービスを実現して、アプリケーションの可用性、パフォーマンス、セキュリティを最大化します。また、独自の仮想化機能、アプリケーション固有のインテリジェンス、および詳細なロールベース管理が組み込まれているため、アプリケーション インフラストラクチャを統合し、導入コストを削減し、運用負荷を最小にできます。

関連情報

Cisco ACE アプリケーション スイッチ ファミリの詳細については、次の URL を参照してください。

<http://www.cisco.com/jp/go/ace/>

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systems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一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0805R)

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先(シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (通話料無料)

電話受付時間：平日10:00～12:00、13:00～17:00

お問い合わせ先