CHAPTER 1

概要

Cisco 4700 シリーズ Application Control Engine (ACE) アプライアンスは、サーバ ロード バランシング、ネットワーク トラフィック制御、サービス冗長性、リソース管理、暗号化およびセキュリティ、アプリケーション アクセラレーションおよび最適化のこれらすべてを単一のネットワーク アプライアンスで実行します。

この章では、次に示すトピックの概要を示します。

- ACE テクノロジー
- ACE アプライアンスの設定
- 仮想コンテキストの作成
- アクセス コントロール リストの設定
- ロールベース アクセス コントロールの設定
- 仮想サーバの設定
- ロード バランシング プレディクタの設定
- スティッキ性を使用したサーバ持続性の設定
- SSL セキュリティの設定
- ヘルス プローブを使用したヘルス モニタリングの設定

ACE テクノロジー

サーバ ロード バランシングは、1 台のサーバの作業を複数のサーバに分散することで、アプリケーションおよびサービスのアベイラビリティ、スケーラビリティ、セキュリティをサポートします。

ACE アプライアンスにサーバ ロード バランシングを設定すると、ACE は、Web ページやファイルなどのクライアント要求を受け取るサーバを選択します。ACE は、選択されたサーバまたはネットワーク全体に過負荷を与えずに、クライアント要求に最も効果的に対応できるサーバを選択します。

表 1-1 に、デバイスおよびネットワーク サービスの両方のレベルで、アベイラビリティ、スケーラビリティ、セキュリティをネットワークに提供する ACE テクノロジーを示します。

表 1-1　ACE テクノロジー

レベル	アベイラビリティ	スケーラビリティ	セキュリティ
デバイス	デバイス設定	仮想コンテキスト	アクセス コントロール リスト
		ロールベース アクセス コントロール	
ネットワーク サービス	仮想サーバ ヘルス プローブ	ロード バランシング プレディクタ スティッキ性を使用したサーバ持続性	SSL アクセス コントロール リスト
		ロールベース アクセス コントロール	

デバイス レベルでは、ACE は、次のことをサポートすることで、優れたネットワーク アベイラビリティを提供します。

- デバイスの冗長性：ACE のハイ アベイラビリティ サポートにより、ピア ACE デバイスを設定できるため、一方の ACE が動作不能になっても、もう一方の ACE がすぐに処理を引き継ぐことができます。
- スケーラビリティ：1 台の ACE デバイスを独立した仮想デバイスにパーティショニングして、それぞれに独自のリソースを割り当てることで、バーチャライゼーションをサポートします。
- セキュリティ：特定のクライアントからのアクセスまたは特定のネットワーク リソースへのアクセスを制限する、アクセス コントロール リストをサポートします。

ネットワーク サービス レベルでは、ACE は、次の機能を提供します。

- サービスのハイ アベイラビリティ：高性能サーバ ロード バランシングをサポートします。これは、物理サーバおよびサーバ ファームでクライアント要求を分散して、暗黙的および明示的なヘルス プローブによりサーバおよびサーバ ファーム レベルでのヘルス モニタリングを提供します。
- スケーラビリティ：高度なロード バランシング アルゴリズム（プレディクタ）を使用したバーチャライゼーションをサポートして、ACE で設定された仮想デバイスにクライアント要求を分散します。各仮想デバイスは、複数の仮想サーバを含みます。各サーバは、クライアント要求をいずれかのサーバ ファームに転送します。各サーバ ファームは、複数の物理サーバを含むことができます。

  ACE は、クライアント要求を数百または数千台の物理サーバに分散できますが、サーバ持続性も保持できます。一部の e-コマース アプリケーションでは、セッション内のすべてのクライアント要求は、同じ物理サーバに転送されるため、1 つのシッピング カートのすべてのアイテムは 1 台のサーバに含まれます。
- サービス レベル セキュリティ：ACE とそのピアとの間で、クライアントとサーバ間での安全なデータ トランザクションを提供する、Secure Sockets Layer（SSL）セッションを確立し保持します。

ACE アプライアンスの設定

ACE アプライアンスを設定するには、最初に、ACE との接続を確立し、必要な初期デバイス設定を実行して、アプリケーション ネットワーキング サービスを提供できるように ACE を準備します。詳細については、第 2 章「ACE アプライアンスの設定」を参照してください。

仮想コンテキストの作成

次に、ACE デバイスを複数の仮想コンテキストにパーティショニングし、それぞれに独自のリソースを割り当てます。詳細については、第 3 章「仮想コンテキストの作成」を参照してください。

アクセス コントロール リストの設定

ネットワーク リソースへのアクセスを制御して、必要なトラフィックだけが通過し、適切なユーザだけが必要なネットワーク リソースにアクセスできるようにします。

Access Control List（ACL; アクセス コントロール リスト）を使用し、特定の IP アドレスまたはネットワーク全体との間でのトラフィックを許可または拒否することで、ネットワークのセキュリティを確保します。

ACL は、接続を許可する各インターフェイスに対して設定する必要があります。このようにしない場合、ACE は、そのインターフェイスのすべてのトラフィックを拒否します。ACL は、送信元 IP アドレス、宛先 IP アドレス、プロトコル、ポート、またはプロトコル固有のパラメータの条件を指定した、一連の ACL 許可または拒否エントリで構成されます。各エントリは、エントリ内に指定されたネットワークの一部に対して受信および送信ネットワーク トラフィックを許可または拒否します。

このマニュアルでは、デバイス レベルでの ACL の設定例を提供します（第 4 章「アクセス コントロール リストの設定」を参照してください）。ネットワーク サービス レベルで ACL を設定する方法について、またはより詳細なアクセス コントロール セキュリティの設定方法については、『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。

ロールベース アクセス コントロールの設定

Role-Based Access Control（RBAC; ロールベース アクセス コントロール）を介して、各ユーザが使用できるコマンドおよびリソースを定義することで、大規模で複雑なネットワークのセキュリティを管理できます。RBAC は、ユーザがアクセスできるドメインでの物理または仮想リソースを定義することで、デバイスおよびネットワーク サービスの両方のレベルでのネットワーク セキュリティをサポートします。

詳細については、第 5 章「ロールベース アクセス コントロールの設定」を参照してください。

仮想サーバの設定

Web サイトへの Web トラフィックを代行受信し、ロード バランシングのために、複数の実サーバ（物理サーバ）が単一サーバとして扱われるように、仮想サーバを設定できます。

表 1-2 に、ACE が仮想コンテキスト、仮想サーバ、サーバ ファームおよび実サーバでスケーラビリティをどのようにサポートしているかを示します。

表 1-2　ACE スケーラビリティ

<table>
<tr><td rowspan="16">ACE</td><td rowspan="8">仮想コンテキスト 1</td><td rowspan="4">仮想サーバ A</td><td rowspan="2">サーバ ファーム A</td><td>実サーバ A1</td></tr>
<tr><td>実サーバ A2</td></tr>
<tr><td>.....</td></tr>
<tr><td>実サーバ An</td></tr>
<tr><td rowspan="2">バックアップ サーバ ファーム a</td><td>実サーバ a1</td></tr>
<tr><td>実サーバ a2</td></tr>
<tr><td>.....</td></tr>
<tr><td>実サーバ an</td></tr>
<tr><td rowspan="4">仮想サーバ B</td><td rowspan="4">サーバ ファーム B</td><td>実サーバ B1</td></tr>
<tr><td>実サーバ B2</td></tr>
<tr><td>.....</td></tr>
<tr><td>実サーバ Bn</td></tr>
<tr><td rowspan="8">仮想コンテキスト 2</td><td rowspan="4">仮想サーバ C</td><td rowspan="4">サーバ ファーム C</td><td>実サーバ C1</td></tr>
<tr><td>実サーバ C2</td></tr>
<tr><td>.....</td></tr>
<tr><td>実サーバ Cn</td></tr>
<tr><td rowspan="4">仮想サーバ D</td><td rowspan="4">サーバ ファーム D</td><td>実サーバ D1</td></tr>
<tr><td>実サーバ D2</td></tr>
<tr><td>.....</td></tr>
<tr><td>実サーバ Dn</td></tr>
<tr><td>.....</td><td>.....</td><td>.....</td><td>.....</td></tr>
</table>

ACE を複数の仮想コンテキストにパーティショニングし、それぞれにポリシー、インターフェイスおよびリソースの独自のセットを持たせることができます。仮想サーバは、サーバ ファーム内の実サーバ上で稼動する物理リソースに結合されます。

実サーバは、ネットワークにある実際の物理サーバに関連します。実サーバは、クライアント サービスを提供するように設定するか、バックアップ サーバとして設定できます。

関連する実サーバは、サーバ ファームにまとめられます。多くの場合、サーバ ファーム内のサーバには同じコンテンツ（ミラー化されたコンテンツと呼ばれる）が格納されているため、1 つのサーバが動作しなくなると、別のサーバがただちにその機能を引き継ぎます。ミラー化されたコンテンツにより、要求が増加する期間に、複数のサーバで負荷を共有できます。

詳細については、第 6 章「サーバ ロード バランシングの設定」を参照してください。

ロード バランシング プレディクタの設定

着信クライアント要求をサーバ ファーム内のサーバに分散するには、IP アドレスおよびポート情報を使用して、プレディクタと呼ばれるロード バランシング規則を定義します。

アプリケーション サービスを求めるクライアント要求がある場合、ACE は、サーバやサーバ ファーム全体に過負荷を与えずに、できるだけ短時間に、クライアント要求に対応できるサーバを選択することで、サーバ ロード バランシングを実行します。一部の洗練されたプレディクタでは、サーバの負荷、応答時間、またはアベイラビリティなどの要因が考慮され、各アプリケーションの特徴に合わせてロード バランシングを調整できます。

詳細については、第 7 章「ロード バランシング プレディクタの設定」を参照してください。

スティッキ性を使用したサーバ持続性の設定

1 つのセッション中、同じクライアントが、複数の同時 TCP または IP 接続、あるいは後続の複数の TCP または IP 接続を同一サーバとの間で維持できるように、ACE を設定できます。セッションは、クライアントとサーバの間での、一定期間（数分から数時間まで）における連続した対話として定義されます。シスコでは、このサーバ持続性機能をスティッキ性と呼んでいます。

多くのネットワーク アプリケーションでは、お客様固有の情報を複数のサーバ要求間で持続して保存する必要があります。この一般的な例として、e- コマースサイトで使用されるショッピング カートがあります。スティッキ性は、サーバ ロード バランシングを使用している場合、バックエンド サーバで、以前の要求時に別のサーバで生成された情報が必要となったときに問題となることがあります。

そのため、ACE は、サーバ ロード バランシングをどのように設定したかに応じて、使用するロード バランシング方式を判断してから、適切なサーバにクライアントを固定します。ACE は、クライアントが特定のサーバにすでに固定されていると判断した場合、ロード バランシング基準に関係なく、ACE は、それ以降のクライアント要求をそのサーバに送信します。クライアントが特定のサーバに固定されていないと判断した場合、ACE はその要求に通常のロード バランシング規則を適用します。

プレディクタとスティッキ性を組み合わせることで、トランザクション処理の持続性とともに、スケーラビリティ、アベイラビリティおよびパフォーマンスをアプリケーションに提供します。

詳細については、第 8 章「スティッキ性を使用したサーバ持続性の設定」を参照してください。

SSL セキュリティの設定

Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）の認証、暗号化およびデータ整合性に SSL セキュリティ プロトコルを使用します。

ACE での SSL 設定は、ACE とそのピア間で SSL セッションを確立および保守して、ACE が SSL トラフィックでそのロード バランシング タスクを実行できるようにします。これらの SSL 機能には、サーバ認証、秘密鍵および公開鍵生成、証明書管理、データ パケット暗号化および復号化が含まれます。

詳細については、第 9 章「SSL セキュリティの設定」を参照してください。

ヘルス プローブを使用したヘルス モニタリングの設定

アプリケーション サービスは、アベイラビリティおよびパフォーマンスを確保するためにモニタリングを必要とします。ヘルス プローブを作成することで、サーバおよびサーバ ファームのヘルスおよびパフォーマンスを追跡するように、ACE を設定できます。作成する各ヘルス プローブには、複数の実サーバまたはサーバ ファームを割り当てることができます。

ACE ヘルス モニタリングを有効にすると、アプライアンスは、メッセージを定期的にサーバに送信して、サーバ ステータスを判別します。ACE は、サーバの応答を検証して、クライアントがそのサーバにアクセスできることを確認しま

す。ACE は、サーバの応答を使用して、サーバを稼動または非稼動にできます。また、ACE は、サーバ ファームのサーバのヘルスを使用して、信頼できるロード バランシング決定を行うこともできます。

詳細については、第 10 章「ヘルス プローブを使用したヘルス モニタリングの設定」を参照してください。