Cisco Application Control Engine（ACE）4710：ソフトウェア リリース 3.1 の新機能

製品の概要

Cisco® ACE Application Control Engine 4710 は、データセンター アプリケーションのアベイラビリティ、アクセラレーション、セキュリティを最大限まで高める、次世代のアプリケーション スイッチです。

Cisco ACE 4710 を使用することで、企業はアプリケーション配信のための以下の 4 つの主要な IT 目標を達成できます。

- アプリケーションのアベイラビリティの最大化
- アプリケーションのパフォーマンスのアクセラレート
- データセンターおよび基幹業務アプリケーションのセキュリティ保護
- サーバ、ロード バランサ、およびファイアウォールの使用数を減らすことによるデータセンターの統合の促進

Cisco ACE 4710 ソフトウェア リリース 3.1 には、以下のような特徴があります。

アベイラビリティ

- 専用のマルチメディア サポートによりサーバ キャパシティが向上
- 実際のアプリケーションの健全性に基づくアプリケーション スイッチング
- Cisco Global Site Selector（GSS）と Cisco ACE のインテリジェンス機能が連動して、グローバル ロード バランシングが実現

パフォーマンス

- 新しいソフトウェア ライセンスによりスループットが 2 Gbps から 4 Gbps へ倍増
- 新しいソフトウェア ライセンスにより圧縮速度が 1 Gbps から 2 Gbps へ倍増
- フロー セットアップの再利用により Domain Name System（DNS; ドメイン ネーム システム）バランシング速度が 10 倍に増加
- User Datagram Protocol（UDP）リソースの回復時間が短縮され、レイヤ 4 パフォーマンスが改善
- セッション情報のインテリジェントな再利用により、Secure Sockets Layer（SSL）アクセラレーションが実現

セキュリティ

- 悪意のあるトラフィックに対するインテリジェントなタギングが Denial-of-Service（DoS; サービス拒絶）攻撃の防止を支援
- 着信トラフィック レートの微調整によりサーバ リソースへの攻撃を軽減
- ディープ インスペクションがペイロード情報に対する攻撃排除を支援

表 1 に、Cisco ACE 4710 の新機能をまとめます。

表 1. Cisco ACE 4710 ソフトウェア リリース 3.1 の新機能

アベイラビリティ	説明	利点
Generic Protocol Parsing（GPP）	Cisco ACE は、以下のプロトコルをネイティブで認識します。HTTP、FTP、DNS、Internet Control Message Protocol（ICMP）、Session Initiation Protocol（SIP）、Real-Time Streaming Protocol（RTSP）、Extended RTSP、RADIUS、および Microsoft Remote Desktop Protocol（RDP）。ただし、データセンターの所有者は、カスタム アプリケーション、古いアプリケーション、パッケージ アプリケーションなど、その他多くのアプリケーションに対処しなければならない場合があります。 Cisco ACE の GPP 機能により、カスタム アプリケーションおよびパッケージ アプリケーションのトラフィック ペイロード内の任意の情報に基づいてアプリケーション スイッチングおよび持続性ポリシーを設定することができます。プログラミングの必要はありません。	プログラミングせずに、カスタム アプリケーションとパッケージ アプリケーションのスイッチングが実現します。
HTTP ヘッダーの処理	Cisco ACE は、HTTP ヘッダーの挿入、削除、または書き換えをクライアント要求とサーバ応答の両方でサポートします。 HTTP ヘッダーの挿入： Cisco ACE は、要求と応答の一方または両方で HTTP ヘッダーを挿入できます。 たとえば、Cisco ACE が送信元 Network Address Translation（NAT; ネットワーク アドレス変換）を使用してクライアントの IP アドレスを変換する際には、多くの場合、サーバ側ではそのクライアントを特定する手段が必要になります。 NAT を使用して変換された送信元 IP アドレスを持つクライアントを特定するため、Cisco ACE では、送信元 IP アドレスの汎用ヘッダーと文字列値を挿入してから、サーバに要求を送信することができます。	アプリケーションがロギングと監査を実行できるように、クライアントの可視性を高めます。
	HTTP ヘッダーの書き換え： Cisco ACE は、要求と応答の一方または両方で HTTP ヘッダーを書き換えることができます。 たとえば、クライアントが、セキュリティ保護された Web アプリケーションに接続する必要がある場合、クライアントはアプリケーションに HTTP 要求を送信します。外部アプリケーション スイッチは SSL 接続を終端させ、アプリケーションにクリア テキストを送信します。アプリケーションは、着信クライアント HTTPS 要求がアプリケーション スイッチで終端されたことを認識しないため、セキュリティ保護された HTTPS URL ではなく、セキュリティ保護されていない HTTP URL にクライアントをリダイレクトする場合があります。 この問題を解決するために、Cisco ACE アプリケーション スイッチは、リダイレクトされた URL を Location ヘッダーで HTTP から HTTPS に変更してから、クライアントに応答を送信します。	クライアントへ送られる SSL コンテンツの安全な配信を実現します。
	HTTP ヘッダーの削除： HTTP ヘッダーの削除を使用して、サーバ応答から機密性の高い HTTP ヘッダーを除去することができます。 たとえば、デフォルトでは多くの Web サーバには、HTTP 応答ヘッダーにバージョンや OS などの Web サーバに関する情報が含まれています。この情報は、悪意のある攻撃を行うために使用される可能性があります。 Cisco ACE はこのようなヘッダーを自動的に削除できます。この場合は、クライアントからサーバの種類とバージョンを隠します。	Web アプリケーションをセキュリティ保護します。

アベイラビリティ	説明	利点
部分的なサーバ ファーム フェールオーバー	現時点では、バックアップ サーバ ファームが設定されている場合、プライマリ サーバ ファームがバックアップにフェールオーバーするのは、そのサーバ ファーム内のすべての実サーバに障害が発生した場合のみです。 部分的なサーバ ファーム フェールオーバーにより、ユーザは、プライマリ サーバ ファームがバックアップ サーバ ファームにフェールオーバーする前に、ファーム内でアクティブにする実サーバの最低限のパーセンテージを指定できます。 プライマリ サーバ ファームがバックアップにフェールオーバーする場合、現在確立されているすべての接続は、プライマリ サーバ ファーム上に存続します。新しい要求はすべて、バックアップ サーバ ファームにルーティングされます。 プライマリ サーバ ファームがサービスに復帰するには、実サーバが最低限の割合でアクティブである必要があります。	使用可能な実サーバの数に基づいて、新しいトラフィックを受信するサーバ ファーム（プライマリまたはバックアップ）を管理する機能を提供します。
TCP ダンプ	Cisco ACE は、Cisco ACE を通過するネットワーク トラフィックに関するパケット情報をリアルタイムでキャプチャできます。 Cisco ACE はキャプチャされたパケットをバッファします。ユーザはバッファされたコンテンツを Cisco ACE のフラッシュ メモリ内のファイルにコピーしたり、Ethereal にエクスポートすることができます。	トラブルシューティング機能を強化します。
仮想 IP 対応の送信元 NAT	仮想 IP 対応の送信元 NAT により、NAT プールに仮想 IP アドレスを含め、ダイナミック NAT および Port Address Translation（PAT; ポート アドレス変換）を実行できます。 この機能により、仮想 IP アドレスを使用して NAT 実サーバからの（クライアントへバインドされる）接続を確立できます。	クライアント側ネットワークで実 IP アドレスを節約します。
サーバ ファーム対応の送信元 NAT	この機能により、プライマリ サーバ ファームに障害が発生した場合、数ホップ先にあるバックアップ　サーバ ファームの送信元 NAT が有効になります。 Cisco ACE は、複数の送信サーバ VALN に対して、プライマリおよびバックアップ サーバ ファーム両方のダイナミック NAT を適用できます。	プライマリ サーバ ファームの障害時にも継続してアプリケーション アベイラビリティを確保します。

アベイラビリティ	説明	利点
適応応答プレディクタ	Cisco ACE を使用することで、いくつかの新しいインテリジェントなロード バランシング プレディクタを追加できます。 Cisco ACE プレディクタは応答時間に基づいてサーバを選択します。応答時間はユーザ設定のサンプル数に対して計算されます。また、以下の 3 つの測定オプションをサポートしています。 • SYN-to-SYN-ACK：Cisco ACE から送信された SYN と、サーバから受信した SYN-ACK の間のサーバ応答時間 • SYN-to-Close：Cisco ACE から送信された SYN と、サーバから受信した FIN/RST の間のサーバ応答時間 • 応答に対するアプリケーション要求：Cisco A CE から送信された HTTP 要求と、サーバから受信した HTTP 応答の間のサーバ応答時間	さまざまなユーザ設定の基準で測定されたリアルタイムのサーバおよびアプリケーション パフォーマンス データに基づきアプリケーションを切り替えます。
最小負荷プレディクタ	この Cisco ACE プレディクタは、ユーザにより定義された最大 8 つの SNMP MIB オブジェクトの値に基づいて、負荷が最小であるサーバを選択します。これらのオブジェクトには、CPU 使用率、メモリ リソース、ディスク ドライブ アベイラビリティなどのサーバ リソースを使用できます。ユーザは、測定した各オブジェクトに重みを付けて、アプリケーション スイッチングを非常に高い精度で制御できます。	
最小帯域幅プレディクタ	この Cisco ACE プレディクタは、ユーザ設定のサンプリング期間とサンプル数で、Cisco ACE と実サーバ間の両方向において最も少ない量のアプリケーション トラフィックを処理したサーバを選択します。	
Keepalive Appliance Protocol（KAL-AP）	Cisco ACE アプリケーション スイッチ上の KAL-AP により、Cisco ACE Global Site Selector（GSS）との通信では、仮想 IP および実サーバ アベイラビリティのレポートが可能となります。この情報は、データセンターにまたがるインテリジェントなグローバル サーバ ロード バランシング（GSLB）を行うために、Cisco ACE GSS によって使用されます。 Cisco ACE GSS 間の KAL-AP 通信は、MD5 暗号化を使用してセキュリティ保護することができます。	GSLB を使用してビジネスの継続性を実現します。
Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）プローブ	SNMP メッセージの主な目的は、Web サーバなどの SNMP エージェント上でパラメータを制御（設定）または監視（取得）することです。SNMP は Object Identifier（OID; オブジェクト識別子）を使用して、SNMP エージェントで設定または取得する正確なパラメータを指定します。 この SNMP ベースのサーバ ロード プローブにより、ユーザは、最大 8 つの SMNP OID から構成されるクエリを設定して、サーバを調査することができます。また、ユーザはこれらの各 OID に重みを付けることもできます。 このプローブによりサーバから取得された情報は、この表に記載した最小負荷プレディクタへの入力情報として使用されます。	SNMP 環境でカスタマイズされたプローブを使用することにより、インテリジェントなサーバ ヘルス モニタリングを実現します。
スクリプト プローブ	サーバ ヘルス モニタリングのための、顧客環境に固有の Tool Command Language（TCL）スクリプト作成機能のサポートに加え、Cisco ACE は TCL スクリプトを使用した Cisco ACE CLI コマンドの実行をサポートしています。	カスタマイズされた TCL スクリプトを使用して、インテリジェントなサーバ ヘルス モニタリングを実現します。

アベイラビリティ	説明	利点
HTTP リターン コード解析	この機能により、指定の時間フレーム内で認識される特定の HTTP リターン コードの数に基づいて、しきい値を設定できます。このしきい値に到達すると、Cisco ACE は自動的にサービスからサーバを除去できます。 ページが見つからない（HTTP 404 Not Found 応答が数多く認識される）場合など、サービスからサーバを除去することが望ましい状況では、HTTP リターンコード解析は非常に有益です。この場合、従来の TCP ベースの HTTP サーバ アベイラビリティ プローブでは、サーバが利用可能であり応答していることは示されますが、サーバがコンテンツに対する要求を満たすことができるかどうかについての情報を得ることはできません。このようなシナリオでは、サーバのアベイラビリティを決定するための追加のサーバ レベルの情報を提供する、HTTP リターン コード解析が必要です。	インバンドのサーバ ヘルス モニタリングを強化し、アプリケーション アベイラビリティを高めます。
新しいプロトコルのサポート：Session Initiation Protocol（SIP; セッション開始プロトコル）	SIP はピアツーピア プロトコルであり、これを介してエンド デバイス（ユーザ エージェント）は、インターネット マルチメディア会議、インターネット電話、VoIP、および SIP サーバとのマルチメディア配信セッションなどの双方向通信を開始します。 Cisco ACE は、TCP と UDP で SIP をサポートします。ロード バランシングの決定は、SIP ヘッダーのフィールドに基づいて行われます。セッション持続性は、SIP コールの ID に基づきます。 Cisco ACE は、SIP サーバからのキープアライブ応答に基づいてサーバの有効化と無効化を行い、SIP ベースのマルチメディア アプリケーションに関して信頼性の高いロード バランシングを決定します。	SIP ベースのマルチメディア アプリケーションのインテリジェントなスイッチング、スケーラビリティ、およびハイアベイラビリティを実現します。
新しいプロトコルのサポート：Real-Time Streaming Protocol（RTSP）	RTSP は、Cisco IP/TV、RealAudio、RealNetworks などのアプリケーションの、オーディオとビデオをストリーミングするために使用されます。Cisco ACE は TCP で RTSP をサポートします。 ロード バランシングの決定は、RTSP URL（rtsp://）、または RTSP ヘッダーのフィールドに基づいて行われます。セッション持続性は、RTSP セッション ヘッダーを使用して決定されます。 Cisco ACE は、Cisco IP/TV、RealAudio、RealNetworks などが稼働するアプリケーション サーバからのキープアライブ応答に基づいてサーバの有効化と無効化を行い、RTSP マルチメディア アプリケーションに関して信頼性の高いロード バランシングを決定します。	RTSP ベースのストリーミング オーディオおよびビデオのインテリジェントなスイッチング、スケーラビリティ、およびハイアベイラビリティを実現します。
新しいプロトコルのサポート：RADIUS	RADIUS は認証とアカウンティングのプロトコルです。Cisco ACE は RADI US プロトコルに対応し、特定の RADIUS プロトコル情報に基づくロード バランシング機能、および持続性を決定する機能を提供します。	多くの RADIUS サーバにまたがるインテリジェントなスイッチング、スケーラビリティ、およびハイアベイラビリティを実現します。
新しいプロトコルのサポート：Microsoft Remote Desktop Protocol（RDP）	Microsoft RDP は、ターミナル サーバで稼働中の Windows ベースのアプリケーションに対して、ネットワーク接続経由でのリモート表示および入力機能を提供します。 Cisco ACE は、ターミナル サーバで稼働中の Windows ベースのアプリケーションに対して、RDP ロード バランシングをサポートします。Cisco ACE は、RDP ヘッダーのルーティング トークンに基づいてロード バランシングを決定します。	多くの Microsoft ターミナル サーバにまたがるインテリジェントなスイッチング、スケーラビリティ、およびハイアベイラビリティを実現します。

パフォーマンス	説明	利点
UDP ブースタ	UDP ブースタ機能は、DNS ロード バランシングなどの非常に高い UDP 接続レートを必要とするアプリケーションを切り替えるために使用されます。このような高いレートを実現するために、Cisco ACE は、従来型のアルゴリズムに基づくロード バランシングではなく、統計に基づくロード バランシングを使用します。	DNS ロード バランシングなどの UDP ベースのアプリケーションのパフォーマンスを 1 秒あたり数百万要求まで高めます
UDP ファスト エージング	Cisco ACE は、要求ごとに単独の応答を必要とするアプリケーションのクライアント数に関して、非常に高いスケーラビリティを提供します。UDP ファスト エージングを使用すると、Cisco ACE はサーバがクライアントに応答した直後に UDP 接続を閉じます。 Cisco ACE は、プレディクタ アルゴリズムに応じて、サーバ ファーム内の新しい実サーバへの新規の要求をすべてロード バランシングします。クライアントから再送信されたすべての UDP 要求は、同じ実サーバに送られます。	要求ごとに単独の応答を必要とするスケーラビリティの高い UDP アプリケーションを提供します。
セッション ID のスティッキ	スティッキまたは持続性は、同じクライアントが同じ実サーバとの間で、複数の同時または連続する接続を、セッションが終わるまで維持できるメカニズムです。 顧客が e コマース サイトにアクセスし、ショッピング カートに商品を追加し始めた場合、すべての商品が 1 つのサーバの 1 つのショッピング カートに入るように、1 つのクライアントからの要求はすべて同じサーバに送られなければなりません。顧客のショッピング カートの事例では、通常、特定の Web サーバに対してローカルであり、複数のサーバにまたがって重複することはありません。 スティッキを必要とするアプリケーションは、e コマース アプリケーションのような種類だけではありません。銀行業務用のアプリケーションやオンライン トレーディングなど、クライアントの情報と状態を保持する Web アプリケーションには、スティッキが必要になる場合があります。 Cisco ACE は、送信元または宛先の IP アドレス、クッキー、HTTP ヘッダー、および SSL セッション ID に基づいて、クライアントを適切なサーバに固定することができます。 SSL により、クライアントとサーバ間での安全なデータ転送が確保されます。クライアントとサーバは SSL ハンドシェイク プロトコルを使用して、2 つのデバイス間で SSL セッションを確立します。クライアントと SSL サーバが、各セッションに固有であるセッション パラメータの完全なネゴシエーションを完了するたびに、新しいセッション ID が作成されます。 Cisco ACE は、SSL セッション ID に基づいて、クライアントを適切なサーバに固定します。	SSL 経由で安全なセッション持続性を提供します。
セッション ID の再利用	SSL により、クライアントとサーバ間での安全なデータ転送が確保されます。クライアントとサーバは SSL ハンドシェイク プロトコルを使用して、2 つのデバイス間で SSL セッションを確立します。 標準的な SSL ハンドシェイクでは、クライアントと SSL サーバが、各セッションに固有であるセッション パラメータの完全なネゴシエーションを完了するたびに、新しいセッション ID が作成されます。 Cisco ACE は、以前にネゴシエートされたセッション パラメータからセッション キャッシュに格納されている SSL ID を再利用することにより、クライアントと Cisco ACE 間の後続の SSL セッション セットアップをアクセラレートします。	SLL クライアント接続セットアップをアクセラレートします。

パフォーマンス	説明	利点
クライアント認証	標準的な SSL 実装では、サーバは X509 証明書（認証用のデジタル ID）を送信することにより、クライアントに対してサーバ自体の信頼性を証明します。ただし、クライアントがそれ自体を証明する、同様の保証はありません。 SSL サーバとして機能する、Cisco ACE のクライアント認証機能は、X509 証明書の提供をクライアントに要求することで、この問題に対処しています。 Cisco ACE（サーバ）は、証明書に基づいて以下の情報を検証します。 • 公認の認証局が証明書を発行した。 • 証明書が有効期間内である。 • 証明書のシグニチャが有効であり、改ざんされていない。 • 認証局が証明書を無効にしていない。	正当なクライアントのみがサーバにアクセスできるようにします。

セキュリティ	説明	利点
レート制限	Cisco ACE ソフトウェア リリース 3.1 には、以下の新しいレート制限機能が追加されています。 • 接続レート：実サーバを宛先とする Cisco ACE により受信される 1 秒あたりの接続数 • 帯域幅レート：双方向で Cisco A CE と実サーバの間で交換されるネットワーク トラフィックに適用される 1 秒あたりのバイト数 レート制限ベースのトラフィック ポリシングは、仮想サーバ単位レベルでサポートされています。 レート制限ベースのロード バランシングは、実サーバ（rserver）単位レベルでサポートされています。 この機能は、ロード バランシングの決定に対するフィードバックも提供します。レート制限を超える実サーバをロード バランシングから除外し、レートが制限を下回った場合にはロード バランシングに戻します。 実サーバ、仮想サーバ、または両方に、レート制限パラメータを適用できます。	サーバ リソースを保護します。
オブジェクト グループを使用した Access Control List（ACL；アクセス コントロール リスト）	ACL は、アクセスリスト エントリとして定義されたフィルタのセットに基づいてネットワーク アクセスを制限するために使用されます。ACL は、1 つのインターフェイスに適用されるか、すべてのインターフェイスにグローバルに適用されます。 ACL は対象トラフィックのフィルタリングに使用され、フィルタで定義された基準に基づいて、Cisco ACE にトラフィックを許可または拒否するよう指示します。 フィルタは、送信元アドレス、宛先アドレス、プロトコル、（TCP または UDP の）ポートなどのプロトコル固有のパラメータなどを基準にすることができます。 ACL は、特定のサービスに関して、クライアントからサーバへのアクセスを許可または拒否します。大規模な設定では、クライアント、サーバ、およびサービスの複数の組み合わせを使用できることで、結果としてACL エントリの数が多くなります。このような多数の ACL エントリを管理することは簡単ではありません。 オブジェクトのグループ化には、クライアント アドレス、サーバ アドレス、およびサービスを 1 つの ACL エントリにまとめてグループ化する機能があります。	複数の ACL エントリの設定を効率化します。

セキュリティ	説明	利点
TCP SYN クッキー DoS の防止	クライアントがサーバに接続するためには、TCP 3 ウェイ ハンドシェイク（SYN、SYN-ACK、および ACK）が正常に行われる必要があります。 しかし、場合によって 3 ウェイ ハンドシェイクが完了しないことがあります。その頻度が低い場合は異常ではありませんが、何度も起こる場合は、ハッカーがサーバを攻撃しようとしている可能性があります。 TCP SYN クッキーは、クライアントからの SYN 要求に応答してサーバが計算したイニシャルのシーケンス番号で、SYN-ACK 応答に挿入されます。 TCP SYN フラッド攻撃の特徴は、送信元 IP アドレスが不正で到達不能である 1 つまたは複数のクライアントからサーバに送信される大量の SYN 要求です。その目的はターゲットのサーバに大きな負荷をかけ、そのリソースを消費し、正当な接続要求に対してサービスを拒否させることです。 Cisco ACE の SYN クッキー機能が提供するクライアント認証メカニズムにより、不正なクライアントからの SYN フラッドを防止します。	DoS 攻撃から Cisco ACE とサーバを保護します。
マルチメディアと Voice over IP（VoIP）：SIP と Skinny Client Control Protocol（SCCP）	HTTP、FTP、DNS、ICMP、および RTSP に対する、ハードウェア アクセラレーションによるアプリケーション インスペクションのサポートに加え、Cisco ACE は、SIP、SCCP、および ILS/LDAP をサポートしています。	マルチメディア、VoIP アプリケーションおよびサービスをセキュリティ保護します。
データベースおよび OS サービス：Internet Locator Services および Lightweight Directory Access Protocol（ILS/LDAP）	アプリケーション プロトコル インスペクションは、プロトコル動作を検証し、Cisco ACE を通過しようとする不要なトラフィックまたは悪意のあるトラフィックの特定に役立ちます。	

発注情報

表 2 に、Cisco ACE 4710 の発注情報を示します。

表 2. 発注情報

製品番号	説明
ACE-4710-1F-K9	ライセンス バンドル：ACE 4710 ハードウェア、1 Gbps スループット、5,000 SSL TPS、500 Mbps 圧縮、5 仮想デバイス、アプライアンス アクセラレーション ライセンス、組み込みデバイス マネージャを含む
ACE-4710-2F-K9	ライセンス バンドル：ACE 4710 ハードウェア、2 Gbps スループット、7,500 SSL TPS、1Gbps 圧縮、5 仮想デバイス、アプライアンス アクセラレーション ライセンス、組み込みデバイス マネージャを含む
ACE-4710-4F-K9	ライセンス バンドル：ACE 4710 ハードウェア、4 Gbps スループット、7,500 SSL TPS、2 Gbps 圧縮、5 仮想デバイス、アプライアンス アクセラレーション ライセンス、組み込みデバイス マネージャを含む
ACE-4710-K9	ACE アプライアンス ハードウェア
ACE-AP-SW-3.1	ソフトウェア バージョン 3.1
ACE-AP-01-LIC	1 Gbps スループット ライセンス
ACE-AP-02-LIC	2 Gbps スループット ライセンス
ACE-AP-04-LIC	4 Gbps スループット ライセンス
ACE-AP-04-UP1=	1 Gbps から 4 Gbps へのスループット アップグレード ライセンス

製品番号	説明
ACE-AP-04-UP2=	2 Gbps から 4 Gbps へのスループット アップグレード ライセンス
ACE-AP-SSL-05K-K9	SSL 5,000 TPS ライセンス
ACE-AP-SSL-7K-K9	SSL 7,500 TPS ライセンス
ACE-AP-VIRT-020	20 仮想コンテキスト ライセンス
ACE-AP-C-500-LIC	500 Mbps 圧縮ライセンス
ACE-AP-C-1000-LIC	1 Gbps 圧縮ライセンス
ACE-AP-C-2000-LIC	2 Gbps 圧縮ライセンス
ACE-AP-OPT-LIC-K9	アプリケーション アクセラレーション ライセンス
ACE-AP-SSL-UP1-K9=	ACE SSL アップグレード（5,000 TPS から 7,500 TPS）
ACE-AP-C-UP1=	圧縮を 500 Mbps から 1 Gbps にアップグレード
ACE-AP-C-UP3=	圧縮を 1 Gbps から 2 Gbps にアップグレード

関連情報

Cisco ACE の詳細については、http://www.cisco.com/jp/go/ace/ を参照してください。

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

お問い合せ先