Cisco ACE 4710 Application Control Engine and New Cisco ACE Software Release 4.1

The new Cisco® Application Control Engine ACE 30 Module complementing the existing Cisco ACE 4710 appliance supports unified architecture across multiple hardware form factors and superior capacity to handle web transaction loads. Both the Cisco ACE30 Module and the Cisco ACE 4710 appliance are powered by the new Cisco ACE Software Release A4(1.0), which introduces new features in addition to providing similar functions across the two hardware form factors.

Cisco ACE 4710 Overview

The Cisco ACE 4710 represents the next generation of application switches for increasing the availability, security, and acceleration of data center applications.

The Cisco ACE 4710 allows enterprises to accomplish four primary IT objectives for application delivery:

- Increase application availability through advanced Layer 4 through 7 load-balancing and context-switching capabilities
- Secure the data center and critical business applications
- Facilitate data center consolidation through the use of virtualization capabilities, resulting in lower data center power and cooling costs
- Accelerate application performance

New Features

Cisco ACE Software Release 4.1 creates a common software release for the Cisco ACE Module and appliance form factors, with consistent features across the platforms. Cisco ACE Software 4.1 also creates feature similarity with the existing Cisco Content Services Switches (CSS) products, thereby giving Cisco CSS customers an incentive to migrate to the Cisco ACE platform.

Table 1 summarizes the main features of Cisco ACE Software Release 4.1 on the Cisco ACE 4710.

Table 1. Cisco ACE Software Release 4.1 Features

Feature	Description	Benefit
In-Band Health Checking for TCP	In-band health checking checks client and server traffic in real time to detect whether a server is handling a client request properly. With this feature, Cisco ACE can take a real server out of rotation if TCP resets (RSTs) are being received from the server or if the server is unable to respond to TCP SYNs from the clients. This feature works with health probes.	Provides continuous application availability through passive health checking for servers
HTTP Header Insert of SSL Session	This feature enables the insertion of SSL session information and termination certificate information into the HTTP headers. With this capability, Cisco ACE can provide feature similarity with Cisco CSS, Cisco Content Switching Module with SSL (CSM-S), and Cisco SSL Services Module (SSLM) products. By default SSL header insertion should not be enabled. After the user enables SSL session insertion or server certificate insertion, or both, by default headers will be inserted for every HTTP request.	Provides feature parity with Cisco CSS, facilitating migration from existing Cisco CSM products to Cisco ACE 4710
HTTP Header Insert of Client Certificate	This feature supports the insertion of either the whole client certificate or all the X.509v3 options in the client certificate, with user-configurable names for standard X.509v3 headers. The client certificate, received from a client, when Cisco ACE is configured for client authentication, must be parsed and its headers sent to the application through HTTP headers. With this feature, Cisco ACE extends previous server certificate header insertion	Provides feature parity with Cisco CSS, facilitating migration from existing Cisco CSM products to Cisco ACE 4710

Feature	Description	Benefit
	to allow any field to be inserted, including the X509v3 extensions.	
Secondary IP Address in VLAN	This feature enables Cisco ACE to listen to multiple Layer 2 networks within a VLAN. Cisco ACE should be able to accept client, server, or remote access traffic on the secondary IP address as well as on the primary IP address.	Enables deployment of Cisco ACE in environments in which more than one IP subnet exists within a given VLAN
Redirection on Client Authentication Failure	This feature provides the capability to redirect a client connection in the event that client certificate authentication fails. The default behavior of the Cisco ACE is to reject the client connection when authentication of a client certificate fails. With this feature, the Cisco ACE can redirect client connections to servers or server farms based on the type of failed authentication.	Allows customers to gracefully handle failed authentication and provides customers with immediate assistance
Secure Backup and Restore of Configurations and Checkpoints	This feature provides backup of a Cisco ACE system at the device and virtual context levels. Backup is provided for running and startup configuration files, active licenses, scripts defined in the running configuration, checkpoints, SSL certificates, and exportable SSL keys. It also includes an XML API that helps customers automate the backup and restore process.	Provides robust and flexible capability for backing up the Cisco ACE configuration
Sample SSL Key and Certificate Pair	This feature provides a test SSL Rivest, Shamir, and Adelman (RSA) key and SSL certificate globally within Cisco ACE, so that a user in any context can access the test SSL key (1024 bits) and test SSL certificate. The certificate needs to be self-signed, with an expiry date of sometime in the distant future.	Used primarily for demonstration purposes, proof-of concept, and customer lab testing environments
Fail Action Reassignment across VLANs	This feature allows the Cisco ACE to load-balance traffic across intrusion prevention system (IPS) appliances in different VLANs and to route traffic in the event of an IPS failure.	Provides feature parity with Cisco CSS
Reverse IP Stickiness	Reverse IP stickiness is used mainly in firewall load balancing (FWLB). It helps ensure that multiple distinct connections that are opened by hosts at both ends (client and server) are load-balanced and stuck to the same firewall. Reverse stickiness applies to protocols such as FTP, Real-Time Streaming Protocol (RTSP), and Session Initiation Protocol (SIP), where separate control channels and data channels are opened by the client and the server, respectively.	Required for firewall load-balancing deployments
SSL Offload Extension to Lightweight Directory Access Protocol (LDAP) Certificate Revocation List (CRL) Downloads	This feature provides the capability to use LDAP to retrieve CRLs from CRL distribution points (CDPs) provided by the client certificate (or server certificate in the case of back-end server authentication). If the certificate being validated contains a CDP extension field, the Cisco ACE needs to use the CDP as the download path.	Provides feature parity with Cisco SSLM, allowing customers to migrate from the existing product to Cisco ACE
Scalability of Global Server Load Balancing	This feature increases the number of Keepalive Appliance Protocol (KAL-AP) tags supported per Cisco ACE context to 4000. The Cisco ACE can support 4000 virtual IP addresses and KAL-AP tags in one context, or it can support 250 contexts with 4000 virtual IP addresses and KAL-AP tags equally distributed across all 250 contexts.	Provides application scalability across global data centers
Efficiency Improvements for Access Control List (ACL) Merges and Large-Scale Configurations	This feature provides improved ACL performance: • Reduces ACL merge, compilation, and download time • Make ACL memory use same for both bootup and incremental changes • Creates a transaction model for ACLs • Aborts ACL merge or compilation if the ACL output exceeds the system memory • Retains the original ACLs for analysis purposes	Boosts control-plane efficiency by improving ACL performance
Persistence Rebalance Knob	The existing persistence-rebalance feature is enhanced, allowing the configuration of Cisco ACE to load-balance each subsequent GET request on the same TCP connection independently. This feature allows the Cisco ACE to load-balance each HTTP request to a potentially different Layer 7 class or real server.	Increases flexibility in application load balancing
Usability Enhancements	A number of usability enhancements are provided: • Bulk import of SSL certificates and key pair files, supporting up to 8000 SSL files with up to 4000 certificates or 4000 key files • SSL server certificate verification using a CRL • Layer 7 match URL hit counters displaying the number of times that a connection is established (hit count) based on match HTTP URL statements for a class map in a Layer 7 HTTP policy map • Syslogs enhancements that correlate a user's session with network address translation (NAT) and port address translation (PAT).	Improves product usability, troubleshooting, and debugging capabilities

The Cisco ACE 4710 is managed by the embedded device manager GUI. The device manager supports all the new software features in Cisco ACE Software Release 4.1. For centralized management and provisioning, Cisco Application Network Manager (ANM) 4.1 is the preferred management platform.

Ordering Information

The Cisco ACE 4710 consists of the appliance hardware and a series of software licenses for throughput, SSL, compression, application acceleration and virtual contexts. Customers can either order preconfigured bundles or order separate licenses depending on their specific requirements.

Table 2 provides ordering information for the Cisco ACE 4710.

Table 2. Ordering Information

Part Number	Description
ACE-4710-1F-K9	Bundle license: Includes ACE 4710 Hardware, 1 Gbps Throughput, 5,000 SSL TPS, 500 Mbps Compression, 5 Virtual Devices, Application Acceleration License, Embedded Device Manager
ACE-4710-2F-K9	Bundle license: Includes ACE 4710 Hardware, 2 Gbps Throughput, 7,500 SSL TPS, 1 Gbps Compression, 5 Virtual Devices, Application Acceleration License, Embedded Device Manager
ACE-4710-4F-K9	Bundle license: Includes ACE 4710 Hardware, 4 Gbps Throughput, 7,500 SSL TPS, 2 Gbps Compression, 5 Virtual Devices, Application Acceleration License, Embedded Device Manager
ACE-4710-BUN-UP2=	Bundle upgrade license for upgrade from 1G bundle to 2G bundle
ACE-4710-BUN-UP3=	Bundle upgrade license for upgrade from 2G bundle to 4G bundle
ACE-4710-K9	ACE Appliance Hardware
ACE-AP-SW-3.1	Software Version 3.1
ACE-AP-01-LIC	1 Gbps Throughput License
ACE-AP-02-LIC	2 Gbps Throughput License
ACE-AP-04-LIC	4 Gbps Throughput License
ACE-AP-04-UP1=	Throughput upgrade license from 1 Gbps to 4 Gbps
ACE-AP-04-UP2=	Throughput upgrade license from 2 Gbps to 4 Gbps
ACE-AP-SSL-05K-K9	SSL 5,000 TPS License
ACE-AP-SSL-7K-K9	SSL 7,500 TPS License
ACE-AP-VIRT-020	20 Virtual Context License
ACE-AP-C-500-LIC	500 Mbps Compression License
ACE-AP-C-1000-LIC	1 Gbps Compression License
ACE-AP-C-2000-LIC	2 Gbps Compression License
ACE-AP-OPT-LIC-K9	Application Acceleration License
ACE-AP-SSL-UP1-K9=	ACE SSL Upgrade license from 5,000 to 7,500 TPS
ACE-AP-C-UP1=	Compression upgrade license from 500 Mbps to 1 Gbps
ACE-AP-C-UP2=	Compression upgrade license from 500 Mbps to 2 Gbps
ACE-AP-C-UP3=	Compression upgrade license from 1 Gbps to 2 Gbps

Upgrades

Cisco ACE Software Release 4.1 supports upgrades from all versions of Cisco ACE 4710 Release 3.0. Existing Cisco ACE 4710 customers running Release 3.0 software are eligible for an upgrade without charge to Release 4.1.

For More Information

For more information about the Cisco ACE, visit http://www.cisco.com/go/ace or contact your local Cisco account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C25-632381-00 11/10