What is New in Cisco ACE 4710 Application Control Engine Software Release 3.1

PB478675

Product Overview

The Cisco® ACE Application Control Engine 4710 represents the next generation of application switches for maximizing the availability, acceleration, and security of data center applications.

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

- Maximize application availability
- Accelerate application performance
- Secure the data center and critical business applications
- Facilitate data center consolidation through the use of fewer servers, load balancers, and firewalls

Cisco ACE 4710 Software Release 3.1 highlights include the following:

Availability

- Dedicated multimedia support increases server capacity.
- Application switching is based on actual application health.
- Cisco Global Site Selector (GSS) can now use Cisco ACE intelligence for global load balancing.

Performance

- 2X increase in throughput from 2 Gbps to 4 Gbps with new software license
- 2X increase in compression from 1 Gbps to 2 Gbps with new software license
- 10X increase in Domain Name System (DNS) balancing speed is achieved through reuse of flow setups.
- Faster recovery of User Datagram Protocol (UDP) resources improves Layer 4 performance.
- Intelligent reuse of session information delivers Secure Sockets Layer (SSL) acceleration.

Security

- Intelligent tagging of malicious traffic helps stop denial-of-service (DoS) attacks.
- Fine-tuning of incoming traffic rates mitigates server resource attacks.
- Deep inspection helps eliminate attacks against payload information.

Tables 1 summarizes the new features of the Cisco ACE 4710.

Table 1. New Features in Cisco ACE 4710 Software Release 3.1

Availability	Description	Benefit
Generic Protocol Parsing (GPP)	Cisco ACE has native understanding of the following protocols: HTTP, FTP, DNS, Internet Control Message Protocol (ICMP), Session Initiation Protocol (SIP), Real-Time Streaming Protocol (RTSP), Extended RTSP, RADIUS, and Microsoft Remote Desktop Protocol (RDP). However, data center owners may have to deal with many other applications: custom applications, older applications, packaged applications, etc. The Cisco ACE GPP feature enables you to configure application switching and persistence policies based on any information in traffic payload for custom and packaged applications without the need for any programming.	Enables switching of custom and packaged applications without any programming
HTTP header manipulation	Cisco ACE supports the capability to insert, delete, or rewrite HTTP headers in both client requests and server responses. HTTP header insertion: Cisco ACE can insert an HTTP header in a request or response or both. For example, when Cisco ACE uses source network address translation (NAT) to translate the client's IP address, often the servers need a way to identify that client. To identify a client whose source IP address has been translated using NAT, you can instruct the Cisco ACE to insert a generic header and string value of the source IP address before the request is sent to the server.	Provides increased client visibility for applications to perform logging and auditing
	HTTP header rewrite: Cisco ACE can rewrite an HTTP header in a request or response or both. For example, if a client wants to connect to a secured Web application, the client sends an HTTPS request to the application. An external application switch terminates the SSL connection and sends clear text to the application. Since the application is unaware that the incoming client HTTPS request was terminated on the application switch, the application may redirect the client to an unsecured HTTP URL rather than to the secured HTTPS URL. To solve this problem, the Cisco ACE application switch modifies the redirected URL from HTTP to HTTPS in the Location header before sending the response to the client.	Provides secure delivery of SSL content back to the client
	HTTP header deletion: HTTP header deletion can be used to strip sensitive HTTP headers from server responses. For example, by default many web servers include information about the web server such as the version and OS in the HTTP response header. This information could potentially be used to generate malicious attacks. Cisco ACE can automatically delete such headers, in this case hiding the server type and version from clients.	Secures web applications
Partial server-farm failover	Currently, if a backup server farm is configured, the primary server farm would failover to the backup only when all the real servers in that server farm fail. Partial server-farm failover allows the user to specify a minimum percentage of real servers to be active in the farm before the primary server farm fails over to the backup server farm. When the primary server farm fails over to the backup, all currently established connections continue to exist on the primary server farm. All new requests are routed to the backup server farm. For the primary server farm to return to service, a minimum percentage of real servers should be active.	Provides capability to manage which server farm (primary or backup) receives new traffic based on the number of available rservers
TCP dump	Cisco ACE can capture real-time packet information for the network traffic that passes through the Cisco ACE. The Cisco ACE buffers the captured packets, and you can copy the buffered contents to a file in flash memory on the Cisco ACE or export to Ethereal.	Enables enhanced troubleshooting

Source NAT for virtual IP	Source NAT for virtual IP allows you to include a virtual IP address in the NAT pool for dynamic NAT and port address translation (PAT). This feature can be used to source NAT real server originated connections (bound to the client) using the virtual IP address.	Saves real-world IP addresses on the client-side network
Source NAT for server farm	This feature enables source NAT for a backup server farm multiple hops away during the failure of a primary server farm. Cisco ACE can apply dynamic NAT for both primary and backup server farms, for multiple outgoing server VLANs.	Provides continuous application availability even during a primary server farm failure
Adaptive response predictor	Cisco ACE adds several new intelligent load-balancing predictors. The Cisco ACE predictor selects a server based on its response time. Response times are calculated over a user-configured number of samples, with the following three measurement options supported: • SYN-to-SYN-ACK: Server response time between SYN sent from Cisco ACE to SYN-ACK received from server • SYN-to-Close: Server response time between SYN sent from Cisco ACE to FIN/RST received from server. • Application Request to Response: Server response time between HTTP request sent from Cisco ACE to HTTP response received from server	Switches applications based on real-time server and application performance data measured across a variety of user-configured criteria
Least-loaded predictor	This Cisco ACE predictor selects the least-loaded server based on the value of up to 8 SNMP MIB objects defined by the user. These objects can be server resources such as CPU utilization, memory resources, and disk drive availability. Users can associate weights with each of the measured objects for ultimate granular control in application switching.	
Least-bandwidth predictor	This Cisco ACE predictor selects the server that processed the least amount of application traffic between Cisco ACE and the real servers, in both directions, over a user-configured sampling period and number of samples.	
Keepalive Appliance Protocol (KAL-AP)	KAL-AP on the Cisco ACE application switches allows communication with Cisco ACE Global Site Selector (GSS), to report virtual IP and real server availability. This information is used by the Cisco ACE GSS for intelligent global server load balancing (GSLB) across data centers. KAL-AP communication between the Cisco ACE GSS can be secured using MD5 encryption.	Uses GSLB to provide business continuity
Simple Network Management Protocol (SNMP) probes	The main purpose of an SNMP message is to control (set) or monitor (get) parameters on an SNMP agent, such as a web server. SNMP uses an object identifier (OID) to specify the exact parameter to set or get in an SNMP agent. This SNMP-based server load probe allows the user to configure a query consisting of up to 8 SMNP OIDs to probe the server. In addition, the user can associate weights with each of these OIDs. The information retrieved by this probe from the servers is used as input for the least-loaded predictor described earlier in this table.	Provides intelligent server health monitoring using customized probes in an SNMP environment
Scripted probes	In addition to supporting the capability to author specific Toolkit Command Language (TCL) scripts unique to customer environments for server health monitoring, Cisco ACE now supports execution of Cisco ACE CLI commands using TCL scripts.	Provides intelligent server health monitoring using customized TCL scripts
HTTP return code parsing	This feature enables configuration of a threshold value based on the number of specific HTTP return codes seen in a specified time frame. When this threshold is reached, the Cisco ACE can automatically remove a server from service. HTTP return code parsing is invaluable in a scenario where it is desirable to remove a server from service: if, for example, a page cannot be found (for instance, if many HTTP 404 Not Found responses are seen). In this case, traditional TCP-based HTTP server availability probes would indicate that the server is available and responding, but would not provide information about whether the server is able to fulfill requests for content. HTTP return code parsing is needed in this scenario to provide additional server-level information with which to determine server availability.	Provides enhanced in-band server health monitoring for improved application availability

New protocol support: Session Initiation Protocol (SIP)	SIP is a peer-to-peer protocol through which end devices (user agents) initiate interactive communications such as Internet multimedia conferences, Internet telephone calls, VoIP, and multimedia distribution sessions with SIP servers. Cisco ACE supports SIP over TCP and UDP. The load-balancing decision can be based on fields in the SIP header. Session persistence is based on the SIP call ID. On the basis of the keep-alive response from the SIP servers, Cisco ACE can rotate the server in or out of service, and make reliable load-balancing decisions for SIP-based media applications.	Provides intelligent switching, scalability, and high availability of SIP-based multimedia applications
New protocol support: Real-Time Streaming Protocol (RTSP)	RTSP is used for streaming audio and video for applications such as Cisco IP/TV, RealAudio, and RealNetworks. Cisco ACE supports RTSP over TCP. The load-balancing decision can be based on RTSP URL(rtsp://) or fields in the RTSP header. Session persistence is determined using RTSP session headers. On the basis of the keep-alive response from application servers running Cisco IP/TV, RealAudio, or RealNetworks, etc., the Cisco ACE can place the servers in or out of service and make reliable load-balancing decisions for RTSP media applications.	Provides intelligent switching, scalability, and high availability of RTSP-based streaming audio and video
New protocol support: RADIUS	RADIUS is an authentication and accounting protocol. Cisco ACE is RADIUS-protocol-aware and provides the capability to load balance and determine persistence based on specific RADIUS protocol information.	Provides intelligent switching, scalability, and high availability across many RADIUS servers
New protocol support: Microsoft Remote Desktop Protocol (RDP)	Microsoft RDP provides users with remote display and input capabilities over network connections for Windows-based applications running on a terminal server. Cisco ACE supports RDP load balancing for Windows–based applications running on terminal servers. Cisco ACE makes the load-balancing decision based on the routing token in the RDP header.	Provides intelligent switching, scalability, and high availability across many Microsoft terminal servers
Performance	**Description**	**Benefit**
UDP booster	The UDP booster feature is used for switching applications that require very high UDP connection rates, such as DNS load balancing. To achieve such high rates, Cisco ACE uses statistical load balancing instead of traditional algorithmic load balancing.	Boosts performance of UDP-based applications such as DNS load balancing to millions of requests per second
UDP fast aging	Cisco ACE can provide very high scalability in terms of number of clients serviced for applications requiring a single response per request. With UDP Fast Aging, Cisco ACE closes the UDP connection immediately after the server responds to the client. Cisco ACE load balances all new requests to new real servers in the server farm according to the predictor algorithm. All retransmitted UDP requests from clients go to the same real server.	Provides highly scalable UDP applications that require a single response per request
Session ID stickiness	Stickiness or persistence is the mechanism that allows the same client to maintain multiple simultaneous or subsequent connections with the same real server for the duration of a session. When customers visit an e-commerce site and start to add items to their shopping carts, it is important that all the requests from a client get directed to the same server so that all the items are contained in one shopping cart on one server. An instance of a customer's shopping cart is typically local to a particular Web server and is not duplicated across multiple servers. E-commerce applications are not the only types of applications that require stickiness. Any web application that maintains client information and state may require stickiness, such as banking applications and online trading. Cisco ACE can stick a client to an appropriate server based on the source or destination IP address, cookies, HTTP header, and SSL session ID. SSL helps ensure the secure transmission of data between a client and a server. The client and server use the SSL handshake protocol to establish an SSL session between the two devices. A new session ID is created every time the client and the SSL server go through a complete negotiation of session parameters, unique to each session. Cisco ACE can stick a client to an appropriate server based on SSL session ID.	Provides secure session persistence over SSL

Session ID reuse	SSL helps ensure the secure transmission of data between a client and a server. The client and server use the SSL handshake protocol to establish an SSL session between the two devices. In a standard SSL handshake, a new session ID is created every time the client and the SSL server go through a complete negotiation of session parameters, unique to each session. Cisco ACE can accelerate subsequent SSL session setups between the client and the Cisco ACE by reusing SSL IDs stored in the session cache from previously negotiated session parameters.	Accelerates SSL client connection setup
Client authentication	In a standard SSL implementation a server authenticates itself to clients by sending an X509 certificate (digital identification for authentication). However, there is no similar assurance that the client is who it claims to be. The client authentication feature on the Cisco ACE, acting as an SSL server, addresses this problem by requiring the client to provide an X509 certificate. Cisco ACE (server) verifies the following information on the certificate: • A recognized certificate authority issued the certificate. • The valid period of the certificate is still in effect. • The certificate signature is valid and not tampered with. • The certificate authority has not revoked the certificate.	Permits only legitimate clients to access servers
Security	**Description**	**Benefit**
Rate limiting	Cisco ACE Software Release 3.1 adds new rate limiting capabilities: • Connection rate: The number of connections per second received by the Cisco ACE destined to a real server • Bandwidth rate: The number of bytes per second applied to the network traffic exchanged between the Cisco ACE and a real server, in both directions Rate-limiting-based traffic policing is supported at the per virtual server level. Rate- limiting based load-balancing is supported at the per real (rserver) level. This features also provides feedback to the load-balancing decision; it takes real servers exceeding rate limits out of load balancing and puts them back into load balancing when the rate is below the limits. The rate limit parameters can be applied to a set of real servers or virtual servers or both.	Protects server resources
Access control list (ACL) with object groups	ACLs are used to restrict network access based on a set of filters defined as access-list entries (Cisco ACE). An ACL is applied to an interface or globally to all interfaces. ACLs are used to filter interesting traffic and instruct the Cisco ACE to either permit or deny the traffic based on the criteria defined in the filter. The filters can be based on criteria such as source address, destination address, protocol, and protocol-specific parameters such as ports (for TCP or UDP). ACLs permit or deny access from a client to a server for a specific service. Large configurations can have multiple combinations of clients, servers, and services, resulting in a large number of ACL entries. Managing this large number of ACL entries can become challenging. Object grouping provides the capability to group client addresses, server addresses, and services together in a single ACL entry.	Streamlines configuration of multiple ACL entries

TCP SYN cookie DoS protection	A successful TCP three-way handshake (SYN, SYN-ACK, and ACK) is required for a client to connect to the server. Occasionally the three-way handshake may not complete. Such occurrences are normal if the frequency is low; however, a high volume of such occurrences could signal a hacker trying to attack the server. A TCP SYN cookie is an initial sequence number calculated by the server in response to a SYN request from a client and inserted in the SYN-ACK response. A TCP SYN flood attack is characterized by large number of SYN requests sent to a server from one or more clients with source IP addresses that are invalid and unreachable, the goal being to overwhelm the target server, consume its resources, and cause it to deny service to legitimate connection requests. The SYN cookie feature on the Cisco ACE provides a mechanism for authenticating a client, thereby preventing SYN floods from a rogue client.	Protects Cisco ACE and servers from DoS attacks
Multimedia and voice over IP (VoIP): SIP and Skinny Client Control Protocol (SCCP)	In addition to supporting hardware-accelerated application inspection for HTTP, FTP, DNS, ICMP, and RTSP, Cisco ACE now supports SIP, SCCP, and ILS/LDAP.	Secures multimedia and VoIP applications and services
Database and OS services: Internet Locator Services and Lightweight Directory Access Protocol (ILS/LDAP)	Application protocol inspection helps verify the protocol behavior and identify unwanted or malicious traffic attempting to pass through the Cisco ACE.	

Ordering Information

Table 2 provides order information for the Cisco ACE 4710.

Table 2. Ordering Information

Part Number	Description
ACE-4710-1F-K9	License Bundle: 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	License Bundle: Includes ACE 4710 Hardware, 2 Gbps Throughput, 7,500 SSL TPS, 1Gbps Compression, 5 Virtual Devices, Application Acceleration License, Embedded Device Manager
ACE-4710-4F-K9	License Bundle: Includes ACE 4710 Hardware, 4 Gbps Throughput, 7,500 SSL TPS, 2Gbps Compression, 5 Virtual Devices, Application Acceleration License, Embedded Device Manager
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 from 5,000 to 7,500 TPS
ACE-AP-C-UP1=	Upgrade Compression From 500 Mbps to 1 Gbps
ACE-AP-C-UP2=	Upgrade Compression From 500 Mbps to 2 Gbps
ACE-AP-C-UP3=	Upgrade Compression From 1 Gbps to 2 Gbps

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 C25-478675-00 05/08