AKS IT SERVICES

AKS ADC

Application Delivery Controller

TECHNICAL SPECIFICATIONS

SOLUTION MODELS

MODELS	AKS-ADC-4100	AKS-ADC-4600	AKS-ADC-5100	AKS-ADC-5400	AKS-ADC-6200
Throughput	upto 4 Gbps	upto 20 Gbps	upto 40 Gbps	upto 60 Gbps	upto 100 Gbps
Max concurrent connections	24 M	24 M	48 M	96 M	160 M
L7 requests per second	750 K	3 M	7 M	10 M	15 M
L4 connections per second	480 K	960 K	1.2 M	2 M	4 M
SSL/TLS transactions per second	20K TPS (RSA 2K)	95K TPS (RSA 2K)	95K TPS (RSA 2K)	95K TPS (RSA 2K)	150K TPS (RSA 2K)
Compute	1 CPU	1 CPU	2 CPU	2 CPU	4 CPU
	(8 logical cores)	(20 logical cores)	(32 logical cores)	(40 logical cores)	(64 logical cores)
Memory	16 GB	32 GB	64 GB	128 GB	256 GB
Hard Drive	500 GB SATA	256 GB SSD	512 GB SSD	1 TB SSD	2 TB SSD
1G Ports (RJ45/SFP)	8	8	4	(optional)	NA
10G Ports (RJ45/SFP)	(optional)	2	8	8	4
40G Ports (QSFP+)	NA	(optional)	(optional)	2	4
100G Ports (QSFP28)	NA	NA	NA	(optional)	(optional)
*No. of ports can be customized					
vADC Supported	NA	upto 15	upto 25	upto 30	upto 50

ALL MOODELS

SUPPORT

1. Form Factor	1U / 2U Rack Mount Server (19' mounting)
2. Power Supply	Redundant power supply (hot swappable) AC 170-240V, 50Hz
3. System Management	IPMI 2.0 compliant
4. Humidity	8%-90% (non-condensing)
5. Operating Temperature	10C - 35C
6. Out of Band	Management ports (RJ 45 / SFP / SFP+), Console Port (RS 232/ RJ 45), HA Port (RJ 45 / SFP / SFP+)
7. Network Operations	Reverse Proxy, Inline Bridge Mode, Router Mode, Transparent, Full Proxy, Offline, Passive Promiscuous Mode
8. Operation Modes	Report Only, Block, Block & Report
9. LB Algorithms	Round Robin, Weighted Round Robin, Min Misses, Hash, Persistent Hash, Tunable Hash Weighted Hash, Least Connections, Response Time, Least Bandwidth, SNMP
10. Deployment Modes	Direct Server Return, 1 or 2 Arm Proxy, Immediate or Delayed Binding, Direct Access Mode, WCCP
11. Compliance Certificates	FCC, ROHS, CE compliant

AKS ADC FEATURES

OPERATIONS & DEPLOYMENT

1. IPv4 & IPv6 support with translation
2. HTTP 0.9/1.0/1.1/2.0 with translation
3. Web socket support
4. Support for dynamic routing protocols (BGP, OSFP, RIP 1/2)
5. Optional FIPS-2 / Non-FIPS HSM for SSL inspection
6. High Availability (HA) (N+1) with Active / Passive modes (VRRP)
7. Support for SNMP, SMTP, Syslog logging
8. AAA integration with RADIUS / TACACS+
9. Periodic threat updates (Geo IP, TOR IP, Bad IP, etc)
10. Periodic signatures updates
11. Integration with AD / LDAP / SAML
12. On the fly configuration updates
13. Date-Time sync with SNTP/NTP
14. Centralized management for multiple servers
15. Secure communication to mitigation servers
16. State sync across multiple servers
17. Centralized logging and reporting in multiple formats
18. Log & event storage and export
19. Simple SIEM integration

MANAGEMENT FEATURES

20. Secure web user interface (via HTTPS)
21. Command line interface (via SSH or console port)
22. Built-in RESTFul APIs for automation
23. Real-time & historical dashboards
24. Custom dashboards & reporting
25. System status dashboard
26. RBAC administration & audit logs
27. Network forensics with packet capture, traceroute, etc
28. Detailed event / alert reporting
29. Automated / manual backup & restore
30. Log retention for audit
31. False positive forensics

APPLICATION DELIVERY FEATURES

32. Layer 4 load balancing (TCP, UDP)
33. Layer 7 load balancing (HTTP, DNS, etc)
34. SSL v2,v3, TLS v1.0/1.1/1.2/1.3 support
35. HTTP RFC compliance
36. Client / Server / Full NAT
37. TCP buffering, optimization & multiplexing
38. TCP keep alive & timeout policy
39. Health check via SSL / TCP / ICMP / SNMTP / HTTP(s)
40. Alarm on health failure
41. Marking server up / down / backup
42. Automatic failover & recovery
43. Content compression (gzip, brotili)
44. Content caching
45. Transformation rules to add, edit, remove headers / parameters
46. Redirection rules to rewrite URLs
47. Variable rules for dynamic load balancing
48. Upstream rules for dynamic content routing
49. Script rules for custom load balancing
50. Error rules for error handling
51. Aggregated health checks
52. Virtual matrix architecture
53. Acceleration for mobile devices
54. Content minification
55. Real User Metrics (RUM)
56. User / device fingerpriting
57. Anti-DDoS protection
58. Header rules for Request / Response header manipulation

GLOBAL SERVER LOAD BALANCING

59. Built-in DNS Firewall with RPZ policy
60. DNSSEC support
61. DNS Load Balancing
62. DNS over SSL / HTTP(s)
63. Data exfiltration protection
64. Bot Protection
65. Authoritative / Recursive Modes
66. Routing traffic across multiple locations

AKS ADC FEATURES

APPLICATION FIREWALL FEATURES

1. Multiple security modes
   (Bypass, Record, Learning, Mitigation)
2. Multiple security policy per application
3. SSL certificate management
4. Built-in vulnerability scanner with virtual patching
5. File upload scanning with ICAP / built-in AV
6. OWASP Top 10 protection
7. SANS 25 Software Error protection
8. PCI DSS 2.0 section 6.6 enforcement
9. Positive & Negative security model
10. Anti-DDoS protection
11. Anti-Bot protection
12. Anti-Bot mobile SDK
13. JS / Captcha challenge
14. Temporary & dynamic blacklist
15. Advanced browser fingerprinting
16. Anti-reconnaisance & cloaking
17. Anti-scraping & Anti-automation protection
18. Malware detection
19. API / Webservice protection
20. Account Takeover protection
21. Brute force protection
22. Man-in-the-browser protection
23. Request normalization before inspection
24. Two factor authentication
25. Web defacement protection
26. Data leak prevention / response filtering
27. Machine learning & self-correction
28. Threat scoring & weighting
29. Known threat & 0-day attack protection
30. Automatic profiling (whitelist)
31. Auto-learning applications
32. Pre-defined rules for various frameworks
33. Web server and application signatures (blacklist)
34. Operating System signatures
35. Ruleset staging and deploy
36. Bad IP reputation / TOR IP protection
37. Whitelist / Blacklist (IP, Prefix, Geo location)

APPLICATION FIREWALL FEATURES

38. Forceful browsing
39. Unauthorized nagivation protection
40. Access predictable resources
41. Protocol validation
42. Application policy validation & restriction
    (request method, size, file ext, etc.)
43. HTTP header security & header rules
44. XML / JSON / AJAX support & validation
45. XML Firewall
46. Evasion & illegal encoding
47. REGEX based custom rules
48. REGEX based whitelist rules
49. Form validation rules
50. Correlation rules
51. Deception rules
52. Rate limit rules
53. Script rules for custom logic
54. Cookie signing and encryption
55. Hidden form field protection
56. Parameter / URL tampering
57. LDAP injection protection
58. SSI injection protection
59. Buffer overflow protection
60.. Integration with 3rd party scanner (web / source code)
61... Integration with custom Threat Intel
62..Variable Rules
63. Log Rules

LINK LOAD BALANCING

64. Advanced NATting (static NAT, PAT, dynamic NAT, Full NAT)
65. NAT 46/64 with DNS proxy for DNS 46/64
66. Link Monitoring with instant failover (<10s)
67. Link bonding / aggregation
68. Static & Policy based routing
69.. Traffic shaping & bandwidth restriction

To learn more about AKS Enterprise Application Delivery Controller and find out how our solution can ensure application traffic management and security, visit www.aksitservices.co.in or email us at sales@aksitservices.co.in

AKS ADC