Vendor	Array	F5	Juniper	NeoAccel	Sonicwall	Watchguard
Product	Access Direct	Firepass	SA Series Single SA6500	SSL VPN Plus	Aventail	SSL Core VPN Gateway
Dimension (WxHxD)	17 X 3.5 X 21.5	17.5 x 3.5 x 23.5 in	17.26 x 3.5 x 17.72 in	16.7 x 1.7 x 27 in	17.0 x 1.75 x 16.75 in	16.75 x 1.75 x 9.75
Supported platforms	Ability for any platform to gain access to resources such as Windows, Mac, Linux or mobile devices.	Ability for any platform to gain access to resources such as Windows, Mac, Linux or mobile devices.	Ability for any platform to gain access to resources such as Windows, Mac, Linux or mobile devices.	Ability for any platform to gain access to resources such as Windows, Mac, Linux or mobile devices.	Ability for any platform to gain access to resources such as Windows, Mac, Linux or mobile devices.	-
Scalibility	Supports 100 to 64000 concurrent users	Supports upto 2000 concurrent users	• Supports up to 10,000 concurrent users • Two-unit cluster of SA6500s: Supports up to 18,000 concurrent users • Three-unit cluster of SA6500s: Supports up to 26,000 concurrent users • Four-unit cluster of SA6500s: Supports up to 30,000 concurrent users	Supports 10,000 concurrent users per gateway	Support for upto 250 concurrent users.	Supports upto 205 concurrent remote users
Authentication	• LDAP, RADIUS, AD, LocalDB, RSA SecurID, Swivel, Vasco, Custom • Certificate-based authentication	• Internal FirePass database to authenticate users • Supports RADIUS, Active Directory, RSA 2-Factor, LDAP authentication methods, basic and form-based HTTP authentication, identity management servers (for example, Netegrity), and Windows domain servers.	• Ability to support SecurID, Security Assertion Markup Language (SAML), and public key infrastructure (PKI)/digital certificates. • Existing directories in customer networks can be leveraged for authentication and authorization, enabling granular secure	• Authentication through Local database, RADIUS, LDAP, Microsoft Active Directory, RSA SecurID, SSL Client via digital certificates • Two-factor authentication via PKI, tokens	• Server-side digital certificates, Username/password, Client-side digital certificate • Notification of password expiration and password change from the SonicWALL Aventail WorkPlace portal	Authentication methods and supported directories: Server- and client-side digital certificates, RADIUS, RSA SecurID®, LDAP, and Windows® Active Directory.
End point control	• Tests user terminals for personal firewalls, anti-virus, OS service packs prior to allowing access • Limits user ability to store confidential information on unauthorized workstations • Stores information in an encrypted vault • Controls local resources	• Provides secure web-based access to Microsoft Terminal Servers, Citrix MetaFrame, applications, Windows XP Remote Desktops, and VNC servers. • Supports group access options, user authentication, and automatic log-on capabilities for authorized users.	• Client computers can be checked both prior to and during a session to verify device security requiring installed/running endpoint security applications (antivirus, firewall, other). • Supports custom built checks including verifying ports opened/closed, checking files/processes and validating their authenticity with Message Digest 5 (MD5) hash checksums, verifying registry settings, machine certificates.	• Allows enforcement of security policies by checking for active and updated anti-spyware, Anti-spam, Microsoft Window Service Packs,security patches, personal firewalls • Checks desktop search engine presence • Inbound port scanning • IP forwarding	Detection of files, registry keys, running processes and Device Watermarks; Advanced Interrogator (simplified granular end point detection, including detailed configuration information on over 100 anti-virus, anti-spyware and personal firewall solutions	• Verifies endpoint security status before allowing network access by checking device attributes including IP address, firewall settings, OS, patch level, and status of anti-virus software • Encryption: 128-bit/168-bit session length, DES, 3DES, RC4 ciphers, MD5/SHA1 Hashes, SSL v3, TSL v1 • Hides IP addresses of remote network to block worm traversal • Session timeout protects corporate information from unauthorized users
Admin features, security and monitoring	• Quick-start wizard • Role-based administration • Strong administrator authentication • No client installation or management • IP address assignment based on users,groups, DHCP and RADIUS • Allows network administrators to restrict login based on date and time • Auditing - Full audit trail in WebTrends WELF format • Logs all user activity – success, failures, attacks	• Provides customization features to design a GUI or existing corporate website portal according to corporate and user requirement • Enables policy based access • Enables customization of login web page • Provides only selected administrative users to enrol new users, terminating sessions, re-setting passwords without exposing all functions to them (for example, shutting down the server or deleting a certificate). • Audit reports - Administration consol provides audit reports to help comply with security audits. Summary reports aggregate usage by day of the week, time of day, accessing OS, features used, and other information for a user-specified time interval. A single URL is used to retrieve summary/group reports in either HTML or spreadsheet format	• Intuitive centralized UI for configuring, updating, and monitoring SA Series appliances within a single device/cluster or across a global cluster deployment • Enables administrators to establish a dynamic authentication policy for each unique session • Granular auditing and logging -Provides fine-grained auditing and logging capabilities in a clear, easy to understand format	• Single-user and role-based command line interface Console, SSHv2	• Centralised web-based management (SonicWALL Aventail Management Console) for all access options, • End Point Control configuration, access control policies and WorkPlace Portal configuration, policy replication across multiple appliances and locations • Centralized set of monitoring capabilities for auditing, compliance, management (SonicWALL Aventail Advanced Reporting, RADIUS auditing and accounting integration)	• Load Balance support • Manage multiple Firebox SSL VPN Gateways in your network from the single Administration Tool • Easy-to-use Administration Tool has drag-and-drop object support • Intuitive interfaces for configuring and managing access policies
Access control	• Different network pools defined per user or group	• Delivers granular access control to intranet resources on a group policy basis. For example, employees can gain access to all intranet sites; partners can be restricted to a specific web host. • The Visual Policy Editor, a flow-chart style graphical view	Combines network, device, and session attributes to determine which of three different types of access is allowed.	• Supports policy decisions to allow, or deny, access is based on user and group policies. • Security zones, with access control enforcement, provide granting intended network access—for both employees and non-employees.	• User and group, Source IP and network, Destination network, Service/Port (OnDemand and Connect only) • Define resources by destination URL, host name or IP address, IP range, subnet and domain, Day, date, time and range, Browser encryption key length	• Assign access policies for users and groups with robust authentication support • Control which devices gain network access through built-in endpoint security checks and Application White List controls
Applications supported	• Outlook, Lotus Notes, Windows terminal services, • Citrix Presentation Server • Passive & Active FTP • Windows XP remote desktops • VNC servers • Citrix Presentation Server applications • Windows terminal services applications	• Provides access to internal web servers, including Microsoft Outlook Web Access, Lotus iNotes, and Microsoft SharePoint Server • Supports SMB Shares; Windows Workgroups; NT 4.0 and Win2000 domains; Novell 5.1/6.0 with Native File System pack; and NFS se	Secure Application Manager (SAM) and Network Connect provide cross-platform support for client/server applications using SAM, as well as full network-layer access using the adaptive dual transport methods found in Network Connect Access to web-based appli	All IP based applications, web enabled applications, dynamic IP and port based applications, legacy mainframe applications.	Clientless access to Web-based resources, Web file access: SMB/ CIFS, DFS, Personal Bookmarks, Multiple optimized WorkPlace portals for different user groups.	-
Protocols	Supports any IP based applications (TCP, UDP, NetBIOS)	• Accesses applications via standard protocols: HTTP and SSL/TLS. It works with all HTTP proxies, access points, and private LANs, and over networks and ISPs • Provides secure web-based access to POP/IMAP/SMTP email servers from standard and mobile device	Support for full IP protocol (includes items like multicast or H.323)	• SSL 3.0 and TLS 1.0 • Remote access VPNs • Full, Split Tunneling, Local LAN Exception • Encryption DES, 3DE S, AES (256), RC4 • Authentication MD-5, SHA-1, RSA 1024, RSA 2048 • SSH, Telnet	Access to any TCP- or UDP-based application via the WorkPlace portal (leveraging OnDemand Tunnel agent).	-
Connectivity	• Network drive mapping • Split tunneling and full tunneling control • GINA Integration	• Windows Logon/GINA Integration—Enables hierarchical directory structure. • Static IP Support—Assigns a static IP based on the user when the user establishes a network access VPN connection, lowering administrative support costs.	Provides complete network-layer connectivity via an automatically provisioned cross-platform download; Windows Logon/GINA integration for domain SSO; installer services to mitigate need for admin rights. Allows for split tunneling capability.	• SSH, Telnet, Windows RD P, VNC, Access via any SSL-enabled browser • Session-only Java applets used • Access through Web portal •SSL VPN-Plus End Point Security enabled layer 2-7 access controls	SonicWALL Aventail Smart Tunneling offers a Layer 3 technology that supports UDP, TCP and IP protocols, and back-connect applications like VoIP. In NAT mode, no set-up of IP address pools is required.	IP pooling, optional split tunneling and dynamic or static routing
User Experience	• Localized end-user GUI support for English, Korean, Japanese, simplified & traditional Chinese	Enables all fields on the user web page to be localized, including the names of the feature (for example, web applications) this helps localize the user's GUI, not just user favorites—increasing business value and lowering TCO.	Creation of completely customized sign-on pages.	Java-Based Web user interface	-	-
Other features	-	-	Second power supply or DC power supply available • 4-port small form-factor pluggable (SFP) interface card • Dual, mirrored hot swappable SATA hard drives • Dual, hot swappable fans, Hot swappable power supply, 4 gigabyte SDRAM, 4-port copper 10/100/1000	Session-only Java applets used.	-	
Contact	Array Networks Golden Square #102, Eden Park No 20, Vital Mallya Road Bangalore - 560001 Karnataka India Direct: +91 080 41329296 Fax: +91 080 2224 3863 Boardline: + 91 80 2224 3860 Email: isales@arraynetworks.net	Bangalore Tel: +91 80 41467458 Mumbai Tel: +91 22 67032167/8	Chennai Tel: +91 44 4299 4187-89 Fax: +91 44 4299 4300 Bangalore Tel: +91 80 3053 8700 Fax: +91 80 3053 8824 Mumbai Tel: +91 22 4084 3700 Fax: +91 22 4084 3709 New Delhi Tel: +91 11 4061 2900 Fax: +91 11 4061 2937	NeoAccel India Pvt. Ltd. Millenium Business Park, Unit No. 310, A -3, Building No. 2, Sector-1, Mahape, Navi- Mumbai 400 710. Tel: +91 22 2778 0781 Fax: +91 22 2783 0782	Tel: +91 080 22275308 /304/305 Tel: +91 011 43589898 Tel: +91 9677010212 Tel: +91 9867760087 Fax: +91 080 41233612	Level II, Elegance Plot No. 8, Jasola Mathura Road New Delhi - 110 025 Tel: +91 11 4060 1502 Fax:+91 11 4060 1235 email: inquiry.INDIA@watchguard.com
Website	www.arraynetworks.net	www.f5.com	www.juniper.net	www.neoaccel.com	www.sonicwall.com	www.watchguard.com