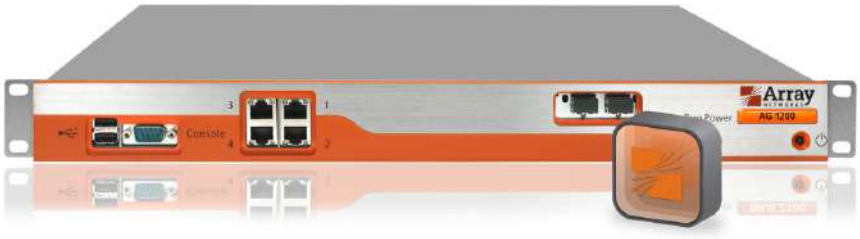
AG SERIES DATASHEET

Secure Access Gateways

AG Series secure access gateways provide scalable and controlled remote and mobile access to corporate networks, enterprise applications and cloud services for any user, anywhere on any device.

Powered by Array's 64-bit SpeedCore® architecture, AG Series secure access gateways are the ideal choice for enterprises and service providers seeking scalable and flexible secure access engineered to support next-generation mobile and cloud computing environments. Available as high-performance appliances that feature the latest in acceleration technologies and energy-efficient components or as virtual appliances that enable flexible pay-as-you-go business models, AG Series appliances are unmatched in their ability to provide remote and mobile access to large and diverse communities of interest without compromising security or the end-user experience.

Highlights & Benefits



- Anytime, anywhere browser-based secure remote access, enables increased productivity for employees, partners, tenants, customers, contractors and guests
- Simple, scalable and secure remote desktop that enables use of PCs and virtual desktops from any device in any location
- Secure mobile access for individual native and Web applications for supporting Bring Your Own Device (BYOD) or secure access from managed smart phones and tablets
- Hardware appliances supporting up to 3 Gbps throughput, 130,000 concurrent users and 500,000 user profiles for maintaining security and driving productivity at scale
- Virtual appliances with non-disruptive upgrades up to 300 concurrent users and up to 100 Mbps throughput
- Up to 256 cross-platform HTML5 secure access portals, customizable to the security and usability preferences of multiple tenants and communities of interest
- Range of access methods including Web, Layer-3, thin client, HTML5 and client-server connectivity
- SSL encryption for data in transit
- Supports a range of OAuth, SAML, AAA, one-time password and multi-factor authentication schemes
- Endpoint security including device-based identification, host-checking, cache cleaning and adaptive policies
- Per-user policy engine for identity-based access to URLs, files, networks and applications
- Cross-platform support for a range of operating systems and browsers
- Array Business Continuity (ABC) contingency licenses for affordably supporting surge remote access
- N+1 clustering and redundant power for business-critical application environments requiring 24/7 uptime
- Compact 1RU and 2RU form factors for environments where space is at a premium
- Familiar CLI, intuitive WebUI and centralized management for ease of use and configuration

Integrated Secure Access

Array AG Series secure access gateways integrate SSL VPN, remote desktop access and secure mobile access to deliver scalable and flexible secure access for both remote and mobile users.

From a single platform, secure access can be enabled for multiple communities of interest including employees, partners, guests and customers.

In addition, AG Series physical and virtual appliances support next-generation "any-to-any" secure access via robust feature sets for bring-your-own-device (BYOD) and controlled access to cloud services.

SSL VPN Remote Access

SSL VPN secure remote access enables anytime, anywhere access to business applications – increasing productivity while maintaining security and compliance. Users need only a common Web browser to quickly and securely access resources and applications for which they are authorized.

Using SSL, the security protocol present in all Web browsers, AG Series appliances can enable a range of remote access methods across a broad spectrum of managed and unmanaged devices.

Web applications can be made available within a secure Web portal, while network-level connectivity and connectivity for specific client-server applications over SSL can be enabled via a universally-compatible client.

Remote Desktop Access

Remote desktop access allows employees to access their work PCs and laptops from any location as if they were in the office. Using remote desktop, workers can control their physical and virtual office desktops from any remote location – whether they are at their home office, a customer or partner site or on a tablet or smart phone.

Remote desktop access is different from traditional VPN access. Because sensitive files and data never leave the corporate network and never reside on remote and mobile devices, security is assured.

Leveraging existing office PCs and unique Array remote desktop technologies such as user self-registration and wake-on-LAN, remote access and BYOD can be extended enterprise-wide in a manner that is both secure and cost-effective.

Secure Mobile Access

In addition to supporting remote desktop for iPhone, iPad and Android devices, AG Series appliances also support secure access for native business apps and HTML5 apps developed for mobile environments.

After installing Array's mobile client on tablets and smart phones, native business apps can be authorized for specific users and automatically installed on end-user devices from an integrated enterprise app store. HTML5 apps can also be provisioned on a per-user basis and are accessible from a secure browser within the mobile client.

Mobile VPN connections may be enabled per application, and applications may be authorized per user at the administrator's discretion; moreover, all data associated with enterprise apps are stored in a secure container to prevent data leakage.

In the event that devices become lost or stolen, contents of the secure container may be remotely wiped; in addition, device-based identification may be used to prevent future connectivity to the Array appliance from lost or stolen devices.

Virtual Portals

Built on Array virtualization technology, AG Series appliances can support up to 256 secure access virtual HTML5 portals to meet the unique needs of multiple user groups and tenants. Each virtual HTML5 portal is fully independent, with separate management, access policies, access methods and resources.

HTML5 portals do not depend on ActiveX or Java applets, and are compatible with all platforms, thus providing a unified experience for end users regardless of the platforms or browsers.

Built-in templates make creating virtual portals easy, and provide a starting point for further customization.

In addition, features and functions can be seamlessly integrated into existing Web pages and custom layouts with minimal effort using Array portal theme technology.

Per-User Policy Engine

AG Series appliances enable access policies on a per user basis. In addition to validating hardware IDs, AG appliances check remote devices for required OS version, service packs and anti-virus software before granting access to protected networks and resources.

Roles may be assigned based on username, group name, source IP, login time and authentication method and can specify which resources are available to which access methods. Each role may be assigned different resources and QoS policies.

With capacity for 500,000 users in its local database, access policies can be stored on the Array appliance or can be provided via integration with external OAuth or AAA servers. In addition, Single Sign-On (SSO) settings can be customized to store multiple usernames and passwords for different backend application servers.

Moreover, authentication may be set such that users must authenticate to multiple AAA servers for added security, in a manner similar to multi-factor authentication.

The AG Series also supports single sign-on (SSO). Working as a SAML service provider, the AG Series confirms users' identities and authorizations with an identity provider (IdP) to allow seamless access to multiple resources with a single login. SAML SSO streamlines the user experience while maintaining strong security.

End-to-End Security

A dissolvable client-side security agent mitigates network or resource exposure by enforcing pre- and post-admission policies and adapting access rights to suit changes in the client environment. Host-checking verifies device and user identity, and ensures clients meet pre-defined security parameters (anti-virus, anti-spyware, personal firewalls, patches, service packs) and determines adaptive policies. For additional control, cache cleaning can be enabled to wipe cached information from devices when sessions end.

The AG Series supports multiple authentication methods to provide an additional layer of defense against unauthorized access and misuse of data and applications. The built-in one-time password (OTP) capability uses SMS to verify identities via users' mobile phones. Multiple 3rd party two-factor and multi-factor authentication products are also supported.

All traffic between clients and the Array appliance is secured via SSL encryption, and a security-hardened OS ensures that Array appliances are as secure as the networks and resources they protect. Layer 2-7 authorization provides granular access control based on user identity and role within the organization and auditing tracks all activity on a per-user, per-event and per-resource level. URL blacklisting is also available to restrict access to undesirable Web sites.

For organizations with remote offices, branches or other operations, the AG Series supports Site2Site, a hub-and-spoke SSL VPN tunneling solution.

Acceleration & Availability

Security often comes at the expense of performance and ease-of-use; in other words, secure access won't enhance productivity unless users find it fast and friendly. To ensure both performance and security, AG Series appliances support integrated application acceleration features including connection multiplexing, SSL acceleration and compression.

In the event of a failure, Array N+1 clustering technology ensures a transparent and unaffected end-user experience.

Management & Reporting

AG Series appliances offer both a familiar CLI and an intuitive Web user interface that can easily be customized to create streamlined, integrated management systems. Monitoring is made simple with SNMP-based monitoring tools, and with support for

XML-RPC, a range of third-party applications can be used to automate management tasks.

Integration & Extensibility

Taking advantage of extensible APIs, IT can marry secure access intelligence with threat and risk management platforms, virtual management platforms, and custom solutions for reporting, billing, SLAs and vertical-specific requirements. Developers can also create custom native apps with built-in security for mobile environments. From providing real-time usage intelligence to seamlessly interacting with 3rd party secure access and application delivery technologies to integrating with cloud management systems, the power of AG Series APIs is unprecedented.

Array Business Continuity (ABC)

Secure access is a compelling technology for business continuity planning; however, many vendors require businesses to buy contingency licenses outright and most competing products are designed with only enough capacity to support the limited needs of day-to-day remote access.

Only Array has the scalability to support an entire workforce on a single system while maintaining a premium experience for each user. And because helpdesk calls are the last thing you need in an emergency, Array offers the unique ability for first time users to log into a company URL and immediately see their familiar work desktop.

Ten-day contingency licenses are available in increments from 25 to 12,000 concurrent users and are activated by exceeding a base concurrent user license.

Product Editions

AG Series physical appliances and vxAG virtual appliances support multiple options: AccessDirect™ enables SSL VPN remote access, and the DesktopDirect™ add-on enables remote desktop access. The MotionPro™ feature set enables secure mobile access. In addition, all product options support ABC business continuity contingency licenses.

Physical & Virtual Appliances

AG Series physical appliances leverage a multi-core architecture, SSL acceleration and compression, energy-efficient components and 10 GigE connectivity to create solutions purpose-built for scalable secure access. The AG1500FIPS model offers FIPS 140-2 Level 2 compliance for organizations that require a higher level of security.

Available for common hypervisors, and available on popular public cloud platforms, vxAG virtual appliances are ideal for organizations seeking to benefit from the flexibility of virtual environments, offer infrastructure services and new elastic business models or evaluate Array secure access with minimal risk and up-front cost.

Access Methods

Clientless: Web Access	100% clientless – Supports HTML, JavaScript and plug-in parameters – Ensures proper function of applications beyond the corporate network – Masks internal DNS and IP addressing – Supports browser-based access from any device – Supports URL filtering – Web file sharing
On-Demand Client: Network & Application Access	Pre-installed or Web-delivered client through Java or ActiveX – L3, L4 or auto-select tunneling – Auto-launch upon login, transparent to users – L3 & L4 for Windows XP (32-bit), Windows 7 (32/64-bit), Linux, MacOS – Split tunneling and full tunneling control, create tunnel through HTTP forward proxy – Supports any IP application including TCP, UDP, NetBIOS, Outlook, Terminal Devices, FTP, CRM and all CS and BS applications – Internal static and dynamic IP address assignment and external DHCP server IP address assignment – Network drive mapping – Auto-launch of network scripts and commands – Differentiated configurations per user or group roles – Stand-alone, command line and SDK for Array VPN client – MotionPro Windows/MacOS Client – Multi-language support – Detailed traffic logs
Thin Client: Remote Desktop Access	Utilizes local RDP client (RDP 5.0 or higher) – RDP auto-update/deployment – User parameters including screen size, color depth, sound and redirection (if permitted) – Multiple monitors – Performance tuning – Redirection control for drives, printers, ports, smart cards and clipboards – Supports VMView 6.x
Mobile Client: Secure Mobile Access	MotionPro native app for secure mobile access for iPad, iPhone and Android devices – Downloadable from Apple AppStore and Google Play marketplace – Enterprise app store – Automated app installation – SSL mobile VPN – SDK for native 3rd party apps with integrated application level VPN – Secure browser for Web & HTML5 applications
Remote Office Support: SSL VPN Tunneling	Site2Site secure SSL VPN tunneling for remote offices, branches or other operations

Client-Side Security

Host Checking	Verifies device state prior to granting access – Scans for personal firewalls, anti-virus, anti-spam, software version and service packs – Custom rules for a range of apps, registry checks and patches – MAC address or hardware ID validation
Adaptive Policies	Access level conditional on end-point status – Integrated policy management
Cache Cleaning	Wipes all stored browser information upon session termination – Per-session with idle timeout and browser closure
End-Point Security	Device-based identification, data container and remote wipe for mobile devices – Anti-key logging and anti-screen capture for remote PCs – URL blacklisting to prevent access to undesirable Web sites

Server-Side Security

Gateway	Security-hardened OS – Passive and active Layer-7 content filtering – Permit or deny policies – DDoS prevention – Reverse-proxy network separation
Encryption	TLS 1.0/SSL 3.0, TLS 1.2 – RC4-MD5, RC4-SHA, EXP-RC4-MD5, DES-CBC3-SHA, AES128-SHA, AES256-SHA, AES128-SHA256, AES256-SHA256, ECDHE-RSA-AES128-SHA, ECDHE-RSA-AES256-SHA, ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES256-SHA384, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES128-SHA, ECDHE-ECDSA-AES256-SHA, ECDHE-ECDSA-AES128-SHA256, ECDHE-ECDSA-AES256-SHA384, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES256-GCM-SHA384, ECC-SM4-SM3 and ECDHE-SM4-SM3– 1024 – 1024, 2048 and 4096-bit keys – SSL session reuse – Certificate field passing to backend – Online/offline CRL – OCSP

Authentication, Authorization & Auditing (AAA)

Authentication	LDAP, RADIUS, AD, LocalDB, RSA SecurID, Swivel, Vasco, SMX, custom, multi-step HTTP – 500,000 users in LocalDB – Enable/disable LocalDB user – LocalDB password policy control – Backup/restore LocalDB – Export LocalDB in CSV format (Excel) – Up to 1500 logins per second – Certificate-based authentication – Authentication server ranking (search user credential in multiple servers) – RADIUS challenge response mode – Restrict login based on date and time – Single sign-on, NTLM, HTTP basic authentication and HTTP POST – User lock-up by login failure, inactivity or manually by administrator – Automatic login failure lockout for AAA accounts – SAML single sign-on (SSO) – OAuth via Google or WeChat
Authorization	Granular access control – Role-based access control – Roles defined by username, group name, login time, source IP and login method – Permit and deny policies – Authorize user based on MAC address or hardware ID – Provides high flexibility in configuration and detailed logging – Available desktops and redirection conditional upon end-points
Auditing	Full audit trail in WebTrends WELF format – Logs all user activity (success, failure, attack) – Syslog – Alarm/trap – Stats/counters – SNMP MIB
Multi-Factor	Built-in one-time password, SSL client certificates, RSA SecurID, Entrust, other RADIUS-based authentication systems – Multiple AAA server authentication

Performance & Scalability

System	64-bit Array SpeedCore multi-core platform – Optimized packet flow with single-digit millisecond latency – Up to 130,000 concurrent users on a single appliance – Up to 3 Gbps SSL throughput on a single appliance – SSL key exchange and bulk encryption performed in kernel – Connection multiplexing for optimizing server efficiency and reducing back-end connections – High-availability and scale out (active/active, active/standby clustering)
Virtualization	Up to 256 virtual secure access portals – Single page virtual site creation – Concurrent user session control per virtual portal – Delegated management – Portal theme technology for custom virtual portals or integrating with pre-existing Web pages – Pure Java script-based customization on per virtual portal basis – No external server requirements – Localized end-user GUI support for English, Japanese, simplified and traditional Chinese

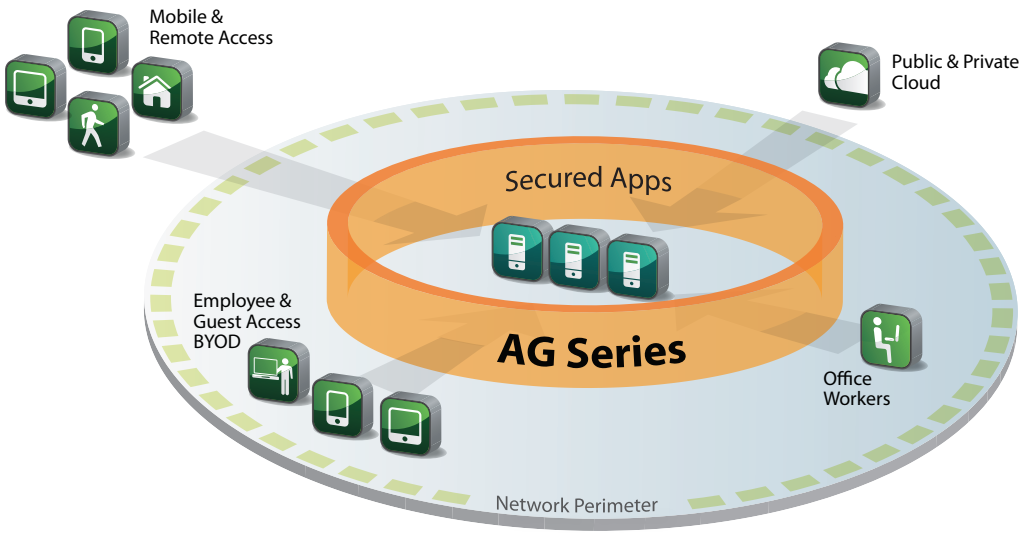
Management

System Administration	Intuitive WebUI – Quick-start wizard – Role-based administration – Strong administrator authentication – RADIUS accounting – No client installation or management – Configuration synchronization – Full device backup and restore including client security, portal theme, SSL certificates, keys, CRL, LocalDB – User/feature license control – Exporting of system statistics – NTP, NAT, RTS, logging – Customizable DNS resolution
Array Registration Technology (ART) for Remote Desktop	Manual/static registration – User self-registration/automatic registration – Bulk registration (import/export from external database) – Scalable to 150K users and 300K desktops – Registration portal wizard – Remote power management via wake-on-LAN (WoL) technology

Warranty & Support

System	1-year hardware, 90-day software
Support	Gold, silver and bronze-level support plans

Array Secure Access Architecture



Product Specifications

• STANDARD ○ OPTIONAL

	AccessDirect SSL VPN Remote Access	DesktopDirect Remote Desktop Access	MotionPro Secure Mobile Access
Clustering	•	•	•
Web UI	•	•	•
SSL & IPsec Encryption	•	•	•
Virtual Portals	5 included	5 included	5 included
Web Applications	•		
HTML5	•		
L3 VPN Client	•		
Host Checking & Cache Cleaning	•		
SAML Single Sign-On (SSO)	•		
Site2Site SSL VPN Tunneling	•		
Array Registration Technology		•	
Wake-on-LAN		•	
Enterprise App Store			•
L3 Mobile VPN			•
L4 SDK Tunneling			•
Secure Browser			•
Client, App & Device Security			•
Additional Virtual Portals	○	○	○
Array Business Continuity	○	○	○

1371 McCarthy Blvd. Milpitas, CA 95035 | Phone: (408) 240-8700 Toll Free: 1-866-MY-ARRAY | www.arraynetworks.com

VERSION: APR-2017-REV-A