Array

vxAG

Virtual Secure Access Gateways

DATASHEET

vxAG virtual secure access gateways enable secure access to business applications for remote and mobile workers and dynamic, flexible and elastic provisioning of secure access services.

Powered by Array's 64-bit SpeedCore® platform, vxAG virtual secure access gateways extend Array's proven remote and mobile access capabilities to virtualized data centers and public/private clouds. Combining the secure access features common to all AG Series products with the flexibility afforded by virtualized infrastructure, vxAG virtual secure access gateways enable dynamic pay-as-you-grow scalability and new elastic business models for both development and production environments. Able to support granular and differentiated secure access for diverse communities of interest and provide a premium user experience without compromising security.

Features

vxAG virtual secure access gateways are the ideal choice for enterprises and service providers seeking scalable and flexible secure access with the ability to support next-generation mobile and cloud applications and environments. vxAG virtual secure access gateways include all Array AccessDirect SSL VPN secure remote access features. Additional included capabilities include MotionPro™ for secure access to native and HTML5 apps, DesktopDirect™ for remote desktop access and support for ABC business continuity 'surge' licenses.

Integrated Secure Access

Array vxAG virtual 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, vxAG 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, vxAG virtual 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, vxAG virtual 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. HTML5 apps can 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, vxAG virtual appliances can support up to 256 secure access HTML5 virtual portals to meet the unique needs of multiple user groups and tenants. Each HTML5 virtual 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

vxAG virtual appliances enable access policies on a per-user basis. In addition to validating hardware IDs, vxAG appliances check remote devices for required OS version, service packs and anti-virus/anti-spam/anti-spyware/firewall 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 up to 200,000 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 back-end 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 vxAG also supports single sign-on (SSO). Working as a Security Assertion Markup Language (SAML) service provider (SP), the vxAG 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. In addition, the vxAG can serve as a SAML identity provider (IdP) for other security and networking devices.

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 predefined 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 vxAG 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 virtual 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, vxAG 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.

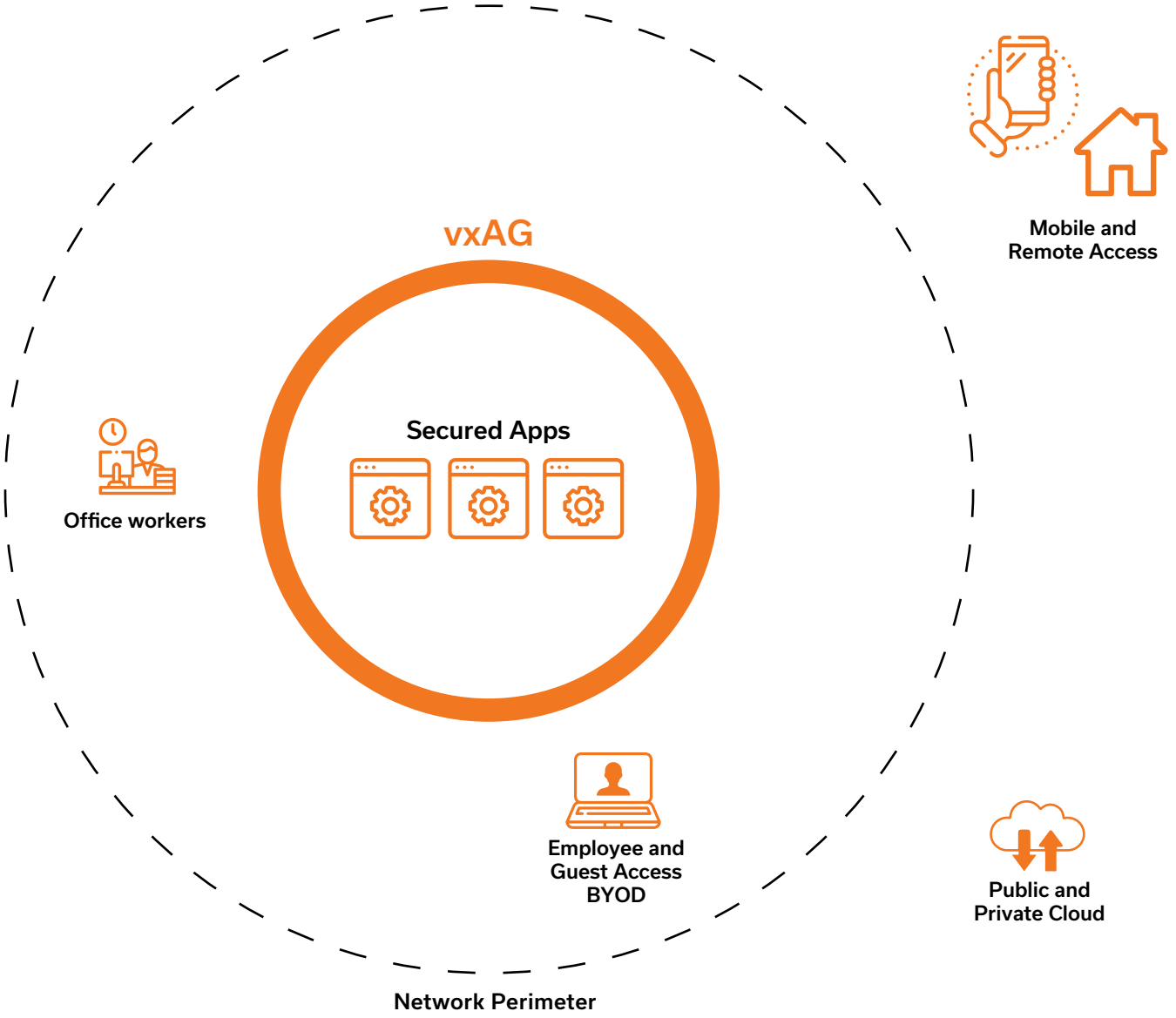
Management & Reporting

vxAG 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.

Warranty & Support

System	90-day software
Support	Gold, silver and bronze-level support plan

Array Secure Access Architecture



Product Specifications

• Standard o Optional

	AccessDirect SSL VPN Remote Access	DesktopDirect Remote Desktop Access
2048/4096-bit SSL Encryption	•	
Layer-3 VPN Client	•	
Web Applications	•	
HTML5	•	
Host Checking & Cache Cleaning	•	
SAML Single Sign-On (SSO)	•	
Client, App & Device Security	•	
Secure Browser	•	
Site2Site SSL VPN Tunneling	•	
Array Registration Technology		•
Wake-on-LAN		•
Clustering	•	•
WebUI	•	•
Virtual Portals*	5 included	5 included
Additional Virtual Portals	o	o
Array Business Continuity	o	o

vxAG

With the exception of hardware SSL acceleration, vxAG virtual secure access gateways running on VMs support all AG Series features. vxAG running on Array's AVX Series Network Functions Platform supports hardware SSL acceleration as well as the full AG Series feature set and all feature modules

Supported Hypervisors (64-bit only)

VMware ESXi 4.1 or Later
XenServer 5.6 or Later
OpenXen 4.0 or Later
KVM 1.1.1-1.8.1 or later
Array AVX Series

Virtual Machine Requirements

Requires Minimum:
2 vCPUs
4GB RAM
40GB Disk
4 Virtual Network Adapters

Supported Public Cloud Environments

Amazon AWS
VMware vCloud Air
Aliyun

Free Trial

Download a
free 30-day vAPV trial today.

VERSION: JUL-2019-REV-A

1371 McCarthy Blvd.
Milpitas, CA 95035

www.arraynetworks.com

+1-866-MY-ARRAY
+1 408-240-8700