



AccessDirect SSL VPN von Array erlaubt jederzeit und überall sicheren Remote-Zugriff für Mitarbeiter, Kunden und strategische Partner auf unternehmenswichtige Ressourcen. Das steigert die Unternehmensproduktivität und senkt die IT-Gesamtkosten.

Mit AccessDirect benötigen mobile Benutzer und Benutzer an anderen Standorten nur einen herkömmlichen Webbrowser, um schnell auf E-Mails, Dateien, Intranets und Applikationen zugreifen zu können. Außerdem erfordert SSL VPN von Array keine vorinstallierten Clients oder Änderungen im Netzwerk und schließt IP-Konflikte sowie Probleme mit der Firewall, mit NAT Traversal oder der Kompatibilität vollständig aus, die von alten VPNs bekannt sind.

■ **VPN für flexiblen Remote-Zugriff**

Mit SSL, dem Sicherheitsprotokoll, das in allen Webbrowsern vorhanden ist, ermöglicht AccessDirect eine Reihe an Zugriffsoptionen (Web, Layer-3, applikationsspezifisch) für eine breite Palette an verwalteten und nicht verwalteten Geräten wie Laptops, Desktops, Mobilgeräten und PDAs.

■ **WebDirect Portal ohne Client**

Durch innovative Reverse-Proxy-Technologie können freigegebene Daten, Webseiten und Webapplikationen schnell und problemlos umgewandelt und in einem sicheren Portal für Remote-Zugriff bereitgestellt werden. Da Benutzer niemals direkt auf Unternehmensnetzwerke oder Applikationen zugreifen, ist der WebDirect Proxy die sicherste Methode für Remote-Zugriff, die zurzeit auf dem Markt ist. Außerdem ist Web Direct die schnellste Methode für Remote-Zugriff, da keine Clients nötig sind.

■ **NetworkDirect Layer-3 VPN**

Viele Benutzer und Unternehmen ziehen Konnektivität auf Netzwerkebene für Unternehmensgeräte vor. Leider weisen alte VPNs auf Netzwerkebene beträchtliche Nachteile einschließlich Probleme mit NAT und Firewall Traversal sowie Konflikte mit IP-Routing und Interoperabilität auf und benötigen vorinstallierte Clients. Im Gegensatz dazu bietet NetworkDirect Layer-3 Zugriff über SSL, der für die vorhandene Netzwerkinfrastruktur transparent ist, einen Client bei Bedarf nutzt und universell kompatibel ist.

■ **AppDirect Ressourcenspezifisch**

Die Bereitstellung spezieller nicht webfähiger Applikationen für Remote-Benutzer (ohne vollständigen Zugriff auf Netzwerkebene) wird durch AppDirect realisiert. Sowohl Client-Server-

als auch Thin-Client-Applikationen werden unterstützt. Autorisierte Client-Server-Applikationen werden nativ auf dem Desktop gestartet und veröffentlichte Thin-Client-Applikationen werden in einem Webbrowser ausgeführt.

■ **Ein Höchstmaß an Sicherheit & Kontrolle**

AccessDirect bietet beispiellose Sicherheitsmechanismen zum Schutz von unternehmenswichtigen Informationen. Alle Daten werden mit SSL verschlüsselt. Der End-Point-Sicherheitsagent von Array authentifiziert Anfragen basierend auf Benutzer- und Geräte-Identität und auf den Administratorvorgaben für bestimmte Geräte oder Zugriffsumgebungen. Anpassbare Richtlinien und ACLs stellen die Autorisierung für URLs, Dateien, Netzwerke und Applikationen basierend auf Identität und Rolle im Unternehmen zur Verfügung. Gleichzeitig protokollieren umfassende Überwachungsfunktionen alle Aktivitäten auf Benutzer-, Ereignis- und Ressourcenebene. Für zusätzliche Sicherheit können die Funktionen zum Löschen des Zwischenspeichers und für einen sicheren Desktop aktiviert werden, um Sitzungen zu sperren und Datenverluste zu verhindern.

■ **Skalierbare Performance & Gesamtbetriebskosten (TCO)**

AccessDirect für Array SPX unterstützt Unternehmen jeder Größe Integrierte Komprimierung, Verbindungs-Pooling und hardwarebeschleunigte Verschlüsselung gewährleisten hohe Performance für jeden Benutzer selbst bei Spitzenlastzeiten. Außerdem können Unternehmen durch die Unterstützung von bis zu 256 sicheren und vollständig getrennten SSL VPN virtuellen Portalen (getrennte

AccessDirect Highlights

- **Jederzeit und an jedem Ort sicherer Zugriff** für Heimarbeiter, Day Extender, mobile Mitarbeiter und Extranet-Partner auf Ressourcen, die die Produktivität steigern
- **Kontrollierter Zugriff auf verwaltete und nicht verwaltete Geräte** einschließlich Desktops, Laptops, Mobilgeräte und PDAs
- **Große Palette an Zugriffsmethoden** einschließlich Web, Layer-3 und spezielle Client-Server- und Thin-Client-Applikationen
- **Plattformübergreifende Unterstützung** für viele Betriebssysteme, Browser und clientseitige Sicherheitsscans
- **Dynamische End-Point-Sicherheit** einschließlich Host-Überprüfung, anpassbare Richtlinien, Zwischenspeicher leeren und sicherer virtueller Desktop
- **Granulare auf Identität basierende Zugriffssteuerung** für URLs, Dateien, Netzwerke und Applikationen
- **Hervorragende Benutzerfreundlichkeit** durch integrierte Applikationsbeschleunigung und 256 virtuelle Portale, die auf die Anforderungen verschiedener Interessengruppen abgestimmt werden können
- **Keine vorinstallierten Clients oder Netzwerk Traversal-Probleme;** Benutzer erhalten Zugriff über einen herkömmlichen Webbrowser

Verwaltung und Bearbeitung) mehrere Unternehmensabteilungen, Partner und Kunden auf einem einzigen System der SPX-Serie abbilden und die Gesamtkosten beträchtlich senken.

■ **Einfaches Management**

AccessDirect bietet eine Kommandozeilenschnittstelle (CLI) und eine Web-Benutzeroberfläche, die problemlos angepasst werden können, um ein intuitives Managementsystem zu erstellen. Die Überwachung des Array SPX ist mit den auf SNMP-basierenden Überwachungs-Tools wie HP OpenView ganz einfach und durch die Unterstützung von XML-RPC kann eine breite Palette an Tools von Drittanbietern zur Automatisierung von Managementaufgaben eingesetzt werden.

Access Methods

Clientless Web Portal Access

- 100% clientless
- Re-writes HTML, JavaScript, HTTP cookie URLs
- Ensures proper function of application beyond the corporate network
- Masks internal DNS and IP addressing
- Windows 2K, XP, Vista, Linux, WAP/WML portal, cell phones with full Web browser, WinCE/Palm PDA

File Access

- SMB, DFS (Windows); NFS (UNIX)
- Browse and delete directories
- Upload, download and delete files
- Easy access
- Maintains original server policies (access rights)
- Supports NTLM single sign-on

Network Level Connectivity

- Supports any IP based applications (TCP, UDP, NetBIOS)
- Different network pools defined per user or group
- Split tunneling and full tunneling control
- Network drive mapping
- Automatic launch of network scripts/commands
- IP address assignment based on users, groups, DHCP and RADIUS
- Windows 2000, XP, Vista, Linux, MacOS X
- GINA Integration
- Stand-alone, command line and SDK for Layer-3 VPN client
- Pre-installable client, web-delivered client

Application-Specific Access

Client-Server Applications

- Any client-initiated TCP applications
- Single port and multi-port
- Outlook, Lotus Notes
- Windows terminal services, Citrix Presentation Server
- Passive & Active FTP
- Windows XP remote desktops
- VNC servers
- Telnet

Thin-Client Applications

- Citrix Presentation Server applications
- Windows terminal services applications
- Telnet thin client

End-to-End Security

End-Point Security

Host Checking

- Tests device state prior to allowing access
- Scans for personal firewalls, anti-virus, OS service packs
- Customized rules for a range of apps, registry checks, patches

Adaptive Policies

- Level of access conditional on end-point status
- Integrated policy management

Secure Virtual Desktop

- Limits user ability to store confidential information on unauthorized workstations
- Stores information in an encrypted vault
- Controls local resources and ability to download session data into a local drive

Cache Cleaning

- Wipes all stored information when the session is over
- Per-session with idle timeout and browser closure
- Windows Vista and previous generation Windows, RedHat, Linux 9, MacOS X

Server-Side Security

- Security-hardened OS
- Passive and active Layer-7 content filtering
- Permit or deny policies
- DDoS prevention
- Telnet Application-Layer Filtering (ALF)
- Reverse-proxy network separation

Encryption

- AES, DES/3DES, SHA/MD5, TLS support

Access Control (AAA)

Authentication

- LDAP, RADIUS, AD, LocalDB, RSA SecurID, Swivel, Vasco, Custom
- Certificate-based authentication
- Authentication server rating (search user credential in multiple servers)
- Challenge Response Mode
- Multi-domain LDAP authentication
- Restrict login based on date and time, client MAC address, client hard drive ID, and custom checks
- Single Sign-on, NTLM, HTTP basic authentication

Authorization

Granular access control of resources

- Group and users policies
- Permit and deny policies
- Consolidated access control
- Provides high flexibility in configuration

Two factor authentication/authorization

- SSL client certificates, RSA SecurID, Entrust
- Other RADIUS-based authentication systems

Auditing

- Full audit trail in WebTrends WELF format
- Logs all user activity – success, failures, attacks

Scalable Performance

- Optimized packet flow; single-digit millisecond latency
- Hardware SSL key exchange and bulk encryption; performed in kernel
- Hardware compression for reduced download times and improved user experience over slow links
- Connection multiplexing optimizes server efficiency; reduces back-end connections
- N+1 clustering (up to 32 systems) with stateful session failover
- Up to 256 discrete virtual portals/user communities on a single system
- Up to tens of thousands of concurrent users on a single system
- Reverse proxy architecture

Management

- Intuitive streamlined WebUI
- Quick-start wizard
- Role-based administration
- Strong administrator authentication
- RADIUS accounting
- No client installation or management

Customizable End-User Portals

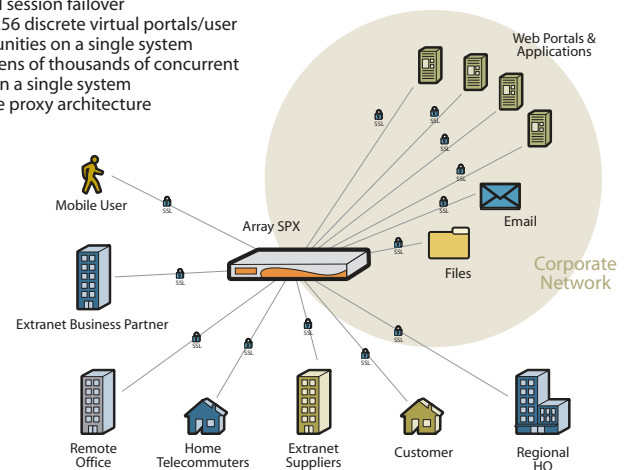
- Embed and import Array includes on a per virtual site basis for enhanced look and feel
- No external server requirements
- Localized end-user GUI support for English, Korean, Japanese, simplified & traditional Chinese

Virtualization

- Single page virtual site creation
- Delegated management
- URL aliasing (saves on certificates and IPs)
- Complete security and data separation
- Instant DMZ on demand
- Strong compliance assurance

Multi-device Management

- SSH/CLI, SSL/WebUI, SNMP, XML/RPC API
- Integration with Microsoft Operations Manager, HP OpenView



	SPX1800	SPX2800	SPX4800	SPX5800	SPX6800
SSL Processing	HW	HW	HW	HW	HW
Compression	SW	SW	SW	SW or HW	SW or HW
Ports	4 Gig Eth	4 Gig Eth	4 Gig Eth	4 Gig Eth Optional 2x Fiber	4Gig Eth Optional 2xFiber or 2 x 10 Gig Fiber
Max Virtual Portals	5	50	256	256	256
Min User License	10	10	25	50	100
Max Concurrent Users	100	1200	6000	12,000	64,000
Throughput	100 Mbps	200 Mbps	400 Mbps	850 Mbps	850 Mbps
Form Factor	1U	1U	1U	2U	2U
Power Supply	Single	Single	Single	Dual	Dual
Clustering	1+1	1+1	N+1	N+1	N+1

SPX1800/
SPX2800



SPX4800



SPX5800/
SPX6800



Technical Specifications

Support	Bronze, Silver & Gold Level Support Plans	Dimensions	Array SPX1800, 2800, 4800: 17"W X 15" D X 1.75" H or 1U Array SPX5800, 6800: 17"W X 21.5" D X 3.5" H or 2U
Warranty	1-Year Hardware; 90-Day Software	Weight	Array SPX1800, 2800, 4800: 13.6 lbs; 5800, 6800: 30 lbs
SPX1800, 2800 & 4800	10/100/1000 Base-TX IP, SecurID, SSH, SSL-TLS, HTTP 1.0/1.1, SNMP	Environmental	Operating Temperature: 0° to 40°C, Humidity: 0% to 90%, Non-condensing SPX1800, 2800, 4800: 100-240VAC, 2.8 A, 47-63Hz, Auto-ranging SPX5800, 6800: 100-240VAC: 6A: 47-63 Hz, Full-range input, Redundant, Hot Swappable
SPX5800 & 6800	10/100/1000 Base-TX, 1000 Base-SX, 10 Gig Fiber, IP, SecurID, SSH, SSL-TLS, HTTP 1.0/1.1, SNMP	Regulatory compliance	IEC 60950-1, LU/CSA 60950-1, EN 60950-1, ICES-003, EN 55024, CISPR 22, AS/NZS 3548, FCC, 47FR part 15 Class A, VCCI-A
Management	SSH CLI, Direct Console CLI, SNMP, Single Console for Cluster, Array Pilot™ (Secure WebUI) for Array OS, XML-RPC	Safety	CSA, C/US, CE, UL
Console port	Male DB9 Serial (RS232) Port		

