



## Benutzerorientierte Netzwerke von Aruba für Finanzdienstleister

Wie gestalten Sie die Zukunft? Sie möchten sicherstellen, dass Ihre Benutzer nur drahtgebunden auf das Netzwerk zugreifen, aber Gästen sicheren drahtlosen Zugriff auf das Internet ermöglichen? Sie möchten die Produktivität der Benutzer steigern, indem Sie im gesamten Gebäude sicheren drahtlosen Zugriff auf Daten- und Sprachanwendungen zur Verfügung stellen? Auf dem gesamten Unternehmensgelände? Weltweit? Sie möchten Business Continuity sicherstellen, auch wenn Witterungsbedingungen die Anreise von Mitarbeitern behindern und bei unvorhergesehenen Ereignissen und Katastrophen?

Aruba hat einen neuen Ansatz entwickelt und implementiert, mit dem diese Vision praktisch realisiert werden kann. Die benutzerorientierte Netzwerkarchitektur von Aruba verknüpft adaptive Drahtlosnetzwerkinfrastrukturen mit identitätsorientierten Sicherheitsfunktionen und Application Continuity Services und schafft auf diese Weise ein integriertes Hochleistungssystem, das alle Anforderungen an sichere und unterbrechungsfreie Nutzung mobiler Anwendungen erfüllt – von der Abwehr unerwünschter Zugriffe mit Wireless Intrusion Protection Services (IPS) bis zur Bereitstellung von Netzwerkzugängen für Gäste. Innerhalb des zentral verwalteten Netzwerks können die Benutzer produktiver arbeiten, da sie Unternehmensanwendungen über LAN, WAN und Internet mobil nutzen können – ohne Einschränkungen bei der Sicherheit. Im Unterschied zu anderen Lösungen kann die benutzerorientierte Netzwerkarchitektur von Aruba in bestehende Netzwerke integriert werden, so dass bereits getätigte Investitionen weiterhin genutzt und radikale Umbauten bestehender Netzwerke vermieden werden.

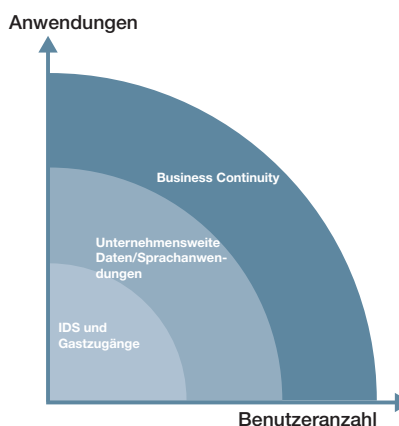
### Einzigartige Aruba-Funktionen

#### EINE PLATTFORM, VIELE NUTZUNGSSZENARIOEN

Netzwerkadministratoren machen regelmäßig die Erfahrung, dass die Ansprüche an mobile Anwendungen schneller wachsen als geplant. Deshalb zählt es sich aus, auf Systeme zu setzen, die mitwachsen. Mit der Netzwerkarchitektur von Aruba können Sie zunächst damit beginnen, drahtlosen Netzwerkzugriff zu unterbinden und Gastzugänge anzubieten und dann schrittweise auf konzernweite Mobilitätsdienste umstellen sowie Remotezugriff für Tausende von Benutzern zur Verfügung zu stellen, um Business Continuity zu sichern – alles auf der Basis einer gemeinsamen Softwareplattform. Diese Flexibilität und Funktionsvielfalt wird durch die einzigartige Integration von Funktionen für Drahtlosnetzwerke, Sicherheit und Remotezugriff in einer einheitlichen, zentral verwalteten Plattform erreicht.

#### IDENTITÄTSORIENTIERTE SICHERHEITSFUNKTIONEN

Die identitätsorientierten Sicherheitsfunktionen der Netzwerkarchitektur von Aruba gewähren parallelen Netzwerkzugriff durch Mitarbeiter, Dienstleister und Gäste und verhindern gleichzeitig unberechtigte Zugriffe auf sensible



Daten sowie unerwünschte Kommunikation zwischen Benutzern. Beim Einsatz der Architektur von Aruba werden bei der Anwendung rollenorientierter Zugriffsrichtlinien Merkmale wie Benutzeridentität, Gerätezustand, Datenverkehrsart, Tageszeit und andere Parameter berücksichtigt und mit einer ICSA-zertifizierten Firewall und Endpoint-Compliance-Techniken durchgehend umgesetzt. Die zentralisierte Netzwerkarchitektur von Aruba sorgt dafür, dass Sicherheits- und Zugriffsrichtlinien

Vorteile der Aruba-Lösung:

- **Integrierte Plattform:** Sicherheit durch das Sperren von WLAN-Zugängen, Gastzugriff, sicheren drahtlosen Zugriff im Unternehmen und Remotezugriff für Business Continuity
- **Identitätsorientierte Sicherheitsfunktionen:** Sicherer Zugang für Gäste und Mitarbeiter und Einhaltung aller Vorschriften zu Datensicherheit und Datenschutz
- **Zentrale Verwaltung:** Zentralisierte Verwaltung der Netzwerke am Unternehmenshauptsitz, in Zweigstellen und Heimbüros erleichtert Konfiguration, Überwachung und Fehlerbehebung
- **Application Continuity:** Zuverlässiger Betrieb von Daten-, Sprach- und Videoanwendungen in Drahtlosnetzwerken
- **Flexibles und skalierbares Netzwerk:** Dank der Integration in bestehende Infrastrukturen können Upgrades und Restrukturierungen bestehender Netzwerke vermieden werden

auch dann angewandt werden können, wenn sich Benutzer in Gebäuden, auf dem Unternehmensgelände oder im Internet bewegen.

Mit identitätsorientierten Sicherheitsfunktionen können Finanzdienstleister sowohl Mitarbeitern als auch Gästen Zugang zum Netzwerk gewähren und dabei alle gesetzlichen Anforderungen an Datenschutz und Datensicherheit erfüllen.

**Gastzugang:** Auch Gäste und Dienstleister benötigen häufig Internetzugänge, VLAN-Segmentierung ist jedoch kein sicherer Ansatz, da sie keinen Schutz vor Angriffen mit falscher Identität bietet. Identitätsorientierte Sicherheitsfunktionen, die unternehmensinternen Datenverkehr einkapseln und vom Gästedatenverkehr isolieren, unterbinden unerwünschte Zugriffe auf sensible Daten wirksam. Beim Einsatz der Netzwerkarchitektur von Aruba wird der gesamte GRE-gekapselte Gästedatenverkehr in eine DMZ geleitet.

**Einhaltung gesetzlicher Vorschriften zu Datenschutz und Datensicherheit:** Außerdem erfolgt die Übertragung von Daten zwischen Endgeräten und Datenzentrum immer verschlüsselt. Zu keinem Zeitpunkt werden Daten unverschlüsselt oder als Klartext übertragen. In Einsatzszenarien mit gemischter Nutzung, bei denen potenzielle Interessenkonflikte bestehen, gewährleistet die Lösung von Aruba vollständige Zugriffskontrolle und isoliert Daten durch Verschlüsselung im Einklang mit den SOX- und GLBA-Vorschriften.

**Business Continuity:** Business-Continuity-Strategien sind bei der heutigen Abhängigkeit von der Verfügbarkeit von Daten und angesichts extremer Wetterlagen, Pandemien und anderer Katastrophen zu einem zentralen Thema für jedes Unternehmen geworden. Aufgrund des Mangels an unternehmenstauglichen Anwendungen für Telearbeit kann die Bereitstellung von Business-Continuity-Lösungen allerdings äußerst kompliziert und kostspielig sein. Weder Verbraucherprodukte noch Unternehmenslösungen für Zweigstellen sind geeignet. Bei Verbraucherprodukten bestehen Bedenken hinsichtlich der Zuverlässigkeit und Sicherheit, für die Installation und Verwaltung unternehmenstauglicher Lösungen fallen jedoch sehr hohe Kosten an, da dafür qualifizierte Fachkräfte eingesetzt werden müssen. Die Remote-AP-Lösung von Aruba füllt diese Lücke durch ein innovatives Konzept, indem sie Daten- und Sprachanwendungen in den Heimbüros von Mitarbeitern in einer Weise bereitstellt, die sich aus Sicht der Benutzer nicht von der Bereitstellung im Unternehmensbüro unterscheidet. Mit dem Remote-AP-Konzept hat Aruba die bewährten Vorteile von Thin Access Points aufgegriffen und auf den Remotezugang übertragen. Da die Verwaltung der Geräte durch die Zentrale erfolgt, können Remote APs

von den Mitarbeitern selbst installiert werden, wodurch erhebliche Einsparungen bei den Investitions- und Betriebskosten möglich sind.

#### ZENTRALE VERWALTUNG UND STEUERUNG

Die Bereitstellung und Verwaltung globaler Unternehmensnetzwerke kann sich zu einem kritischen Problem auswachsen, wenn schwer handhabbare Ansätze gewählt werden. Die zentralisierte Netzwerk- und Richtlinienverwaltung der Aruba-Architektur ist auf einfache Handhabung bei Bereitstellung und Betrieb ausgerichtet. In zentral verwalteten Netzwerkinfrastrukturen von Aruba werden Konfigurationsdaten automatisch und sicher im Netzwerk verbreitet und zu lokalen und externen Access Points und Controllern weitergeleitet. IT-Administratoren steht eine einheitliche Benutzeroberfläche zur Verfügung, mit der sie Richtlinien implementieren und schützen können, um Integrität, Sicherheit und Betriebsbereitschaft des Netzwerks sicherzustellen. Zu den Funktionen für zentralisierte Steuerung gehören auch Leistungsprofile, mit denen Access Points von Aruba ihren Betriebsmodus optimieren, um entscheidende Anwendungen zuverlässig unterstützen zu können. Auf diese Weise entsteht ein extrem skalierbares Netzwerk, das auch von technischen Laien mühelos genutzt werden kann.

#### APPLICATION CONTINUITY

Die Einführung von Wi-Fi-Mobiltelefonen und die zunehmende Beliebtheit von Multimediakommunikation führen dazu, dass Sprach- und Videodaten immer häufiger über IP-Netzwerke transportiert werden. Damit Dienste wie Sprachübertragung unterstützt werden können, müssen QoS-Funktionen für drahtlosen und drahtgebundenen Datenverkehr eingeführt werden, die unterbrechungsfreie Sprachanrufe ermöglichen und Datenverkehrsmuster für Sprachübertragung optimieren. Die Aruba-Architektur ist uneingeschränkt sprachdatenfähig, da zur Sicherung und Priorisierung von Sprachdatenübertragungen die anwendungsorientierte Firewall genutzt werden kann. Da innerhalb der Architektur der Kontext für QoS und Sicherheitsmaßnahmen zentral überwacht und verwaltet wird, können sich die Benutzer innerhalb des Netzwerks frei bewegen. Sprachübertragung wird mit 802.1p- und DSCP-QoS-Tags priorisiert. Das System erkennt verbreitete Sprachübertragungsprotokolle wie SIP, SVC und SCCP automatisch und weist dem Transport von Sprachdaten höchste Priorität zu. Anrufe können außerdem mit Call Admission Control (CAC) priorisiert werden. Eine Höchstanzahl zulässiger Sprachanrufe pro Access Point kann festgelegt werden, so dass weitere Anrufversuche über benachbarte APs abgewickelt werden und die gewünschte Sprachqualität laufender Gespräche nicht beeinträchtigt wird.

# Die Netzwerklösung von Aruba für Finanzdienstleister

Zur Lösung von Aruba gehören drei Hauptkomponenten: Thin Access Points (APs), zentrale Mobility Controller und Softwaremodule für Mobility Controller. Als optionale Komponente können Appliances für Analysen und zum Schutz vor Angriffen eingesetzt werden. Die Access Points sorgen für sichere drahtlose Verbindungen von den Endgeräten zu bestehenden LAN-/WAN-Systemen und leiten den gesamten drahtlosen Datenverkehr über GRE- bzw. IPsec-Tunnel zu einem Mobility Controller im Datenzentrum. Der Mobility Controller ist die zentrale Schaltstelle für Konfiguration, Verwaltung, Application Continuity Services und Sicherheit. Mit Sicherheitsmodulen für Mobility Controller bietet Aruba die erforderlichen Sicherheitslösungen für die Einhaltung einschlägiger Vorschriften an.

Im Folgenden werden wichtige Merkmale drahtloser Netzwerke in Unternehmen mit zentralisierter IT-Administration beschrieben:

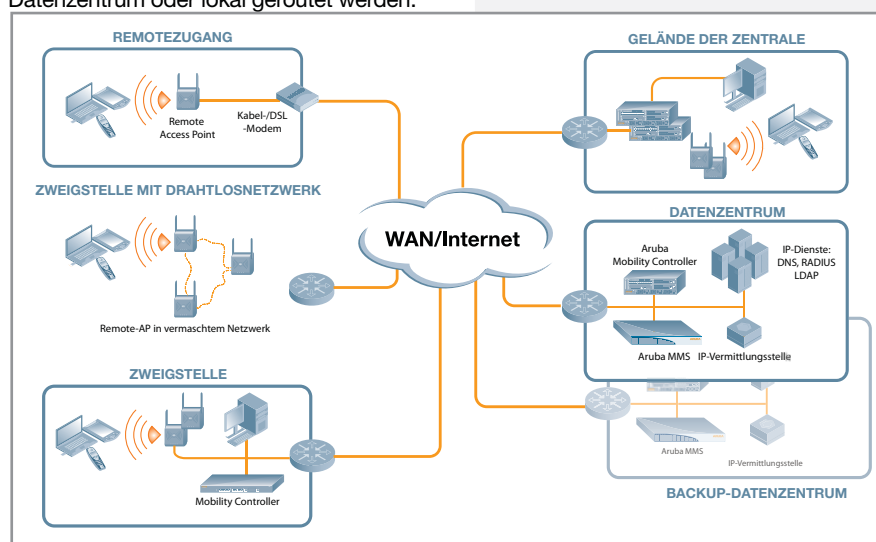
**Datenzentrum:** Im Datenzentrum wird mindestens ein Master Mobility Controller installiert, der als zentrale Schaltstelle für Konfiguration und Verwaltung für das gesamte globale Netzwerk genutzt werden kann. Master Controller können auch Gegenstellen für Access Points am Hauptsitz des Unternehmens und Remote Access Points sein, die von Telearbeitern, in Heimbüros oder in kurzfristig eingerichteten Büros betrieben werden. Jeder Master Controller kann bis zu 500 Remote Controller verwalten und als Ausfallsicherung für Controller an externen Standorten genutzt werden. Bei größeren Installationen kann die Verwaltung lokaler Controller und Access Points an externen Standorten auf mehrere Master Controller verteilt werden. Als Schnittstelle für Verwaltung und Konfiguration kann in diesem Fall ein Mobility Management System (MMS) eingesetzt werden.

**Große und mittlere Büros:** Welche Aruba Mobility Controller an den einzelnen Standorten installiert werden (lokale Controller) hängt davon ab, wie viele Access Points jeweils verwaltet werden müssen. Alle Controllermodelle von Aruba sind mit der gleichen Software und mit den gleichen Funktionen ausgestattet. Sie unterscheiden sich lediglich in der Anzahl der unterstützten Access Points. Unterstützt werden je nach Modell 4 bis 512 Access Points. Die lokalen Controller erhalten ihre Konfigurationsdaten vom Master Controller. Application Continuity und Sicherheitsrichtlinien werden

benutzerorientiert von den lokalen Controllern verwaltet. Die Anwendung von Benutzerrollen erfolgt anhand von Gruppenrichtlinien, die in der Authentifizierungsinfrastruktur definiert sind. Gästedatenverkehr kann am internen Netzwerk vorbei in die DMZ geleitet werden. Die lokalen Controller bieten außerdem Wireless Intrusion Protection und lokale Authentifizierungsdienste und/oder leiten Anfragen an das Datenzentrum weiter. Jeder einzelne lokale Controller kalibriert automatisch die Funkreichweite, um optimale Anwendungsleistung zu erzielen und Lücken in der Netzabdeckung zu vermeiden. Um die Funknetzwerkversorgung auf Bereiche auszudehnen, in denen das Verlegen von Netzkabel nur schwer oder nur zu hohen Kosten möglich wäre, können Access Points von Aruba auf die innovative Secure Enterprise Mesh-Technik zurückgreifen.

**Remotebenutzer und kleine Büros:** Mit Remote Access Points können Bereiche, in denen nur ein oder zwei APs benötigt werden, kostengünstig, sicher und zentral verwaltet mit Drahtlosanbindung versorgt werden. Remote Access Points können direkt an öffentliche/private Internetzugänge oder an LANs angeschlossen werden. Sie finden automatisch den Master Controller und bauen einen VPN-Tunnel zum Datenzentrum auf, so dass externe Benutzer sicher mit drahtloser Anbindung versorgt werden können. Datenverkehr kann je nach Anwendung über das Datenzentrum oder lokal geroutet werden.

## BRANCHENFOKUS Finanzdienstleister



[WWW.ARUBANETWORKS.COM](http://WWW.ARUBANETWORKS.COM)

1322 Crossman Avenue, Sunnyvale, CA 94089, USA | Tel.: +1 408.227.4500 | Fax: +1 408.227.4550