



Benutzerorientierte Netzwerke von Aruba für den Einzelhandel

Wie gestalten Sie die Zukunft? Sie möchten höchstmögliche Kundenzufriedenheit erzielen? Sie möchten Ihre Marke durch Einhaltung der PCI-Standards stärken, aber auf einfache und effiziente Weise? Sie wünschen sich eine bessere Transparenz der Betriebsabläufe? Sie planen ein Netzwerk, auf das alle Kunden, Mitarbeiter und Partner mühelos und sicher Zugriff haben – von beliebigen Orten aus und mit beliebigen Geräten?

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 ermöglicht so integrierte Hochleistungsnetzwerke für Ladengeschäfte und Warenlager. Auf diese Weise kann ein kosteneffektives System aufgebaut werden, das sowohl den PCI-Anforderungen gerecht wird als auch neue Anwendungen umfasst. Durch den benutzerorientierten Ansatz kann das System in bereits bestehende drahtgebundene Netzwerke integriert werden, ohne Upgrades bestehender Systeme.

Einzigartige Aruba-Funktionen

INTEGRIERTE SICHERHEITSFUNKTIONEN ZUR EINHALTUNG DER PCI-VORSCHRIFTEN

Der Payment Card Industry Data Security Standard v1.1 beschreibt anspruchsvolle Sicherheitsanforderungen, die nicht nur für Einzelhändler gelten, die an Verkaufspunkten und in der Bestandsverwaltung Drahtlosnetzwerke einsetzen, sondern auch für Unternehmen, die auf Drahtlosnetzwerke verzichten. Bestehende Netzwerke müssen deshalb in den Bereichen Verschlüsselung, Firewall und Intrusion Detection aktualisiert werden – jedoch so kosteneffektiv wie möglich und möglichst ohne aufwändige Umbauten an der bestehenden Infrastruktur.

Zur WLAN-Infrastruktur von Aruba gehören eine Firewall zur Anwendung von Sicherheitsrichtlinien, ein vollständiges Intrusion Prevention-System und Unterstützung für mehrere Verschlüsselungstechnologien. Alle Funktionen sind auf einer einzigen Hardwareplattform realisiert. Controller und Access Points, mit denen Drahtlosnetzwerkzugänge für Clientgeräte bereitgestellt werden, können gleichzeitig zur Überwachung der Funkumgebung

eingesetzt werden (Air Monitors), um Angriffe von Hackern und unerwünschten Access Points zu erkennen und abzuwehren.

UNTERSTÜTZUNG EINER VIELZAHL MOBILER ANWENDUNGEN UND GERÄTE

Neue Anwendungen zur Kundenansprache und zur Steigerung der Produktivität der Mitarbeiter erfordern häufig simultane Daten-, Sprach- und Videoübertragung. Außerdem werden für die Nutzung von Anwendungen unterschiedliche Gerätetypen eingesetzt. Angesichts der Vielfalt anwendungsspezifischer Geräte mit unterschiedlichen Hardwaredesigns, Betriebssystemen, Stromverbrauchsanforderungen, Roamingmerkmalen und Sicherheitsfunktionen müssen Drahtlosnetzwerkinfrastrukturen in der Lage sein, eine bunte Mischung aus Anwendungen und Geräten zuverlässig zu unterstützen und zu sichern.

Anwendungssensitive Dienstgüten:

Eine integrierte Klassifizierungslogik ermöglicht anwendungsbezogene Quality-of-Service-Niveaus. Mit dieser Technik

Vorteile der Aruba-Lösung:

- **PCI-ready:** Kosteneffiziente und reibungslose Erfüllung von PCI-Anforderungen
- **Anwendungssensitiv:** Unterstützung bestehender Anwendungen und mühelose Einbindung neuer Daten-, Sprach- und Videoanwendungen
- **Beliebige Endgeräte:** Anbieterunabhängige Unterstützung vorhandener und mühelose Einbindung neuer Geräte
- **Anforderungen des Einzelhandels erfüllt:** Zentralisierte Verwaltung mehrerer Hundert oder Tausend Standorte
- **Flexible Architektur:** Integration in bestehende Netzwerke – keine aufwändigen Upgrades oder Restrukturierungen

können latenzempfindlichen Anwendungen (z. B. Sprach- und Videoübertragung) und entscheidenden Anwendungen wie der Verkaufsabwicklung Mindest-Dienstgütern zugesichert werden.

Geräteunabhängige Leistung: Die zentralisierte Architektur von Aruba stellt die erforderlichen Funktionen unabhängig von den eingesetzten Gerätetypen und deren Software bereit. Eine Vielzahl von Geräten wurde auf Interoperabilität und Mobilitätsmerkmale wie Roaminggeschwindigkeit, Batteriebetriebsdauer und Aufrechterhaltung von Verbindungen getestet.

Sicherheit für anwendungsspezifische Geräte (ASDs) Die identitätsorientierten Sicherheitsfunktionen der Aruba-Architektur sorgen dafür, dass ASDs und Geräte, die nicht auf dem neuesten technischen Stand sind, sicher in das Netzwerk eingebunden werden. Angriffe auf WLANs für ASDs und schwach geschützte Geräte werden von den Aruba-Controllern durch benutzerbezogene Firewall- und Intrusion Detection-Funktionen verhindert. Das Sicherheitsniveau wird deshalb nicht mehr durch die eingesetzten Endgeräte begrenzt.

ZENTRALISIERTE VERWALTUNG EINER VIELZAHL VON REMOTESTANDORTEN

Wenn in Geschäften und Lagern keine Administratoren beschäftigt werden sollen, muss die IT-Verwaltung zentralisiert organisiert werden. Drahtlosnetzwerkinfrastrukturen müssen mit geeigneten zentralisierten Werkzeugen für Bereitstellung, Überwachung und Fehlerbehebung für Netzwerke an Hunderten von Remotestandorten ausgestattet sein.

Schnelle Bereitstellung: Der Einsatz von Aruba-Technologie ist kostengünstig, da WLANs an Remotestandorten ohne Eingriffe von Administratoren eingerichtet werden können. Controller und Access Points an Remotestandorten finden automatisch den Master Controller im Datenzentrum und laden selbsttätig die passenden Konfigurationsdaten herunter.

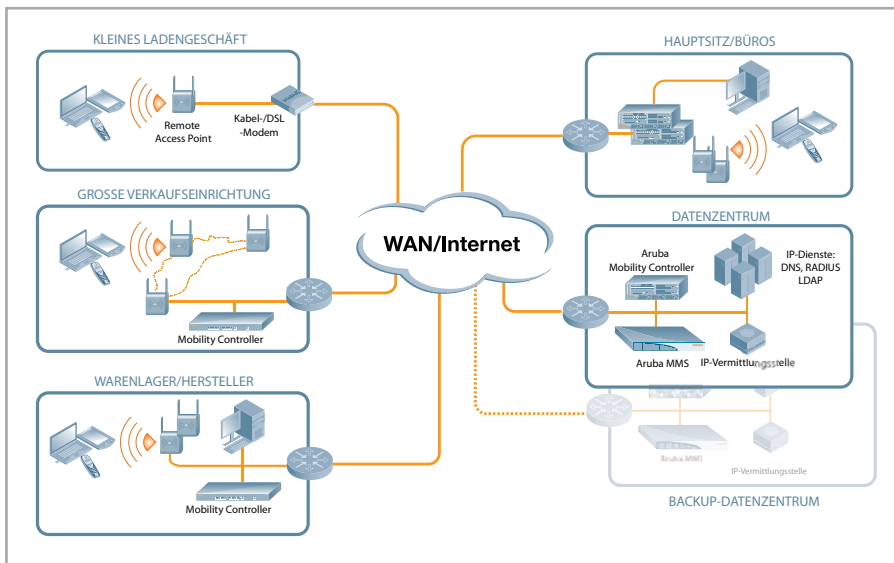
Fehlerbehebung an Remotestandorten: Die zentralisierte Architektur von Aruba reduziert die Kosten für IT-Support sowie Ausfallzeiten mit einer Vielzahl von Werkzeugen für die Fehlerbehebung von einem zentralen Ort aus.

Die Netzwerklösung von Aruba für den Einzelhandel

Zu den Funktionen gehören die Analyse der WLAN-Umgebung an den einzelnen Remotestandorten, gerätebezogene Fehlererkennung und Remote Packet Capture für die gezielte Fehlersuche.

Zur Lösung von Aruba gehören drei Hauptkomponenten: Thin Access Points (Thin APs), zentrale Mobility Controller und Sicherheitsmodule für Mobility Controller. Als optionale Komponente kann ein Mobility

Management System (MMS) eingesetzt werden. Die Access Points sorgen für sichere drahtlose Verbindungen von den Geräten zu bestehenden LAN-/WAN-Systemen und leiten den gesamten drahtlosen Datenverkehr über GRE- bzw. IPsec-Tunnel zu einem Mobility Controller im Datenzentrum oder im Gebäude großer Verkaufseinrichtungen weiter. Der Mobility Controller ist die zentrale Schaltstelle für Konfiguration, Verwaltung, Application Continuity Services und Sicherheit. Für die



Einhaltung einschlägiger Vorschriften bietet Aruba geeignete Sicherheitslösungen als Module für Mobility Controller an. Im Folgenden werden wichtige Elemente zentral administrierter drahtloser Netzwerke für Verkaufseinrichtungen und Warenlager beschrieben:

Im Datenzentrum: Je nach Anzahl der zu verwaltenden Standorte und Access Points werden ein oder mehrere Master Mobility Controller im Datenzentrum installiert. Diese Controller können auch Gegenstellen für Access Points am Hauptsitz und Remote Access Points sein, die in kleinen Ladengeschäften eingesetzt werden. Jeder Master Controller kann bis zu 500 Remote Controller verwalten und fungiert als gemeinsame Schnittstelle für Konfiguration und Management. Master Controller können auch 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 MMS eingesetzt werden.

In Warenlagern, Produktionsanlagen und großen Verkaufseinrichtungen: 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 PCI-Sicherheitsstufen werden benutzerbezogen von den lokalen Controllern verwaltet. 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.

In kleinen Ladengeschäften: 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 kleine Ladengeschäfte sicher mit drahtloser Anbindung versorgt werden können. Datenverkehr kann je nach Anwendung über das Datenzentrum oder lokal geroutet werden.



WWW.ARUBANETWORKS.COM

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