LÖSUNGSÜBERSICHT

SOFTWARE-DEFINED BRANCH

Neue Maßstäbe für Niederlassungen im digitalen Zeitalter von heute

Verteilte Unternehmen, z. B. im Einzelhandel, in der Gastronomie und im Gesundheitswesen, führen eine digitale Transformation durch, um die sich entwickelnden Geschäftsziele besser erfüllen zu können und in ihren Branchen wettbewerbsfähig zu bleiben.

Das bedeutet häufig, dass die IT Prozesse verbessern, neue Services schneller bereitstellen und ein besseres und sicheres Benutzererlebnis bieten muss.

Cloud-basierte Services tragen zu einem schnellen Wandel in allen Branchen bei, insbesondere angesichts der Tatsache, dass Unternehmen in größerem Umfang auf Software-as-a-Service-Anwendungen umstellen. Die enorme Zunahme an mobilen Geräten, der stärkere Einfluss des Internet der Dinge (IoT) und der immer höhere Bedarf an Bandbreite verändern auch die Art und Weise, wie LANs und WANs in Zukunft verwaltet werden müssen.

Bis zum Jahr 2023 werden 70 % der Unternehmen bei Verbindungen zu Niederlassungen und Remote-Standorten auf das Internet angewiesen sein[1] – gleichzeitig werden 20 Mrd. neue IoT-Geräte auf dem Mainstream-Markt angeboten.[2] Das stellt die IT, deren Budgets im Jahr 2018 nur um 3,5 % zunehmen sollen, vor gewaltige Herausforderungen[3]. Darüber hinaus muss sie nun den Direct-to-Internet-Datenverkehr (DIA) sicher verwalten, der die unternehmensweite Peripherie umgeht.

Das führt zu potenziellen Sicherheitsrisiken im Unternehmen und erhöht den Aufwand für die IT, einheitliche Zugriffsrichtlinien aufrechtzuerhalten. Sie muss in Bezug auf das Netzwerk in Niederlassung ein ganzheitliches Konzept umsetzen, das es problemlos ermöglicht, neue Geräte einzubinden, den Datenverkehr zu unterteilen und die SLA-Anforderungen für alle WAN-Verbindungen zu erfüllen.

Hierfür benötigt die IT eine Architektur, die flexibel genug ist, um mit den geschäftlichen Anforderungen von heute Schritt zu halten und den Wachstumschancen von morgen gerecht zu werden. Und das alles bei gleichzeitiger Kostenreduzierung und Umstellung von einem Kapitalkostenmodell (CAPEX) auf ein Betriebskostenmodell (OPEX).

DIE SOFTWAREDEFINIERTE NIEDERLASSUNG

Die Lösung von Aruba hierfür ist eine softwaredefinierte Niederlassung (SD-Branch), die erstklassige kabellose und kabelgebundene Funktionen zur Koordinierung von Infrastruktur und Verwaltung mit kostensparenden SD-WAN-Funktionen kombiniert. IT-Organisationen können damit jetzt ein einheitliches Modell nutzen, das auf ein cloud-basiertes Management ausgerichtet ist und die Bereitstellung, Konfiguration und Verwaltung aller Komponenten in einer Niederlassung vereinfacht.

Die Cloud-Management-Plattform von Aruba Central bietet eine zentrale Ansicht für das Management von kabellosen, kabelgebundenen und WAN-Verbindungen. Dadurch hat die IT mehr Möglichkeiten, Vorgänge in jeder Niederlassung proaktiv vorherzusehen und Probleme leichter zu lösen. Das umfangreiche Portfolio an Sicherheits- und

[1] Gartner, „SD-WAN: CSPs Must Seize the Internet Opportunity“, April 2018
[2] Ericsson Mobility Report, November 2017
[3] ZDNet/Gartner, “IT budgets 2017-18: What the surveys tell us“, 2017

Analyselösungen von Aruba liefert wiederum den notwendigen Kontext, um Zugriffs- und Bandbreitenrichtlinien entsprechend anzupassen.

ERSTKLASSIGE LAN-INFRASTRUKTUR

Die branchenführenden kabellosen und kabelgebundenen LAN-Lösungen und -Softwareprodukte von Aruba helfen der IT bei der Bereitstellung des Maßes an Leistung und Zuverlässigkeit, das in den auf mobile Geräte ausgerichteten Umgebungen von heute erforderlich ist. Integrierte Funktionen sorgen dafür, dass mobile und IoT-Geräte unabhängig vom Typ, der verwendeten Anwendung oder der Verbindungsmethode immer miteinander verbunden bleiben und optimal funktionieren.

Mithilfe von Gateways in Niederlassungen kann die IT WAN-Verbindungen bereitstellen und verwalten. Das ist neben der Verwaltung kabelgebundener und kabelloser Verbindungen ein weiterer und wichtiger Verantwortungsbereich der IT. Die Aruba Branch Gateways unterstützen mehrere WAN-Verbindungen, die Umsetzung softwaredefinierter, rollenbasierter Richtlinien und die einfache Definition der besten Pfade für den Datenverkehr im Internet und im Rechenzentrum.

Durch Zero Touch Provisioning (ZTP) kann die IT die gesamte Zugriffsinfrastruktur in einer Niederlassung schnell und präzise konfigurieren und bereitstellen. Über eine einfach zu implementierende mobile App kann jeder nicht-technische Mitarbeiter den Barcode für einen Access Point, einen Switch oder einen SD-Branch Gateway scannen und Geräte einbinden, sodass eine schnellere Bereitstellung gewährleistet ist.

DIE SD-WAN GATEWAYS

Während sich herkömmliche Router in verteilten Unternehmen seit Jahrzehnten bewährt haben, suchen viele IT-Organisationen nach einer neuen Lösung, die die Vorteile der heutigen Breitbandverbindungen nutzt.

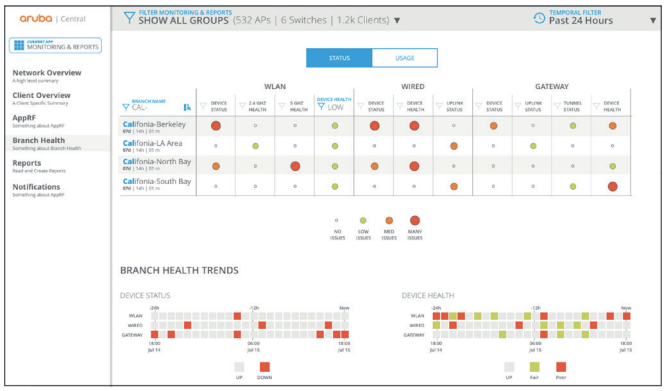
Bei der Lösung von Aruba werden erstklassige kabellose und kabelgebundene Funktionen zur Koordinierung von Infrastruktur und Verwaltung mit kostensparenden SD-WAN-Funktionen kombiniert.

Der Aruba Branch Gateway ist eine zuverlässige und leistungsfähige Lösung für Unternehmen, die Breitband-, MPLS- und LTE WAN-Verbindungen unterstützt. Vom Standpunkt der Datenweiterleitung aus betrachtet erhält die IT dadurch mehr Einblicke in den ein- und ausgehenden Datenverkehr jeder Niederlassung, unabhängig von der Uplink-Verbindung.

Als Abschlusswiderstand für den VPN Concentrator (VPNC) wird in Hub-and-Spoke-Topologien für IPsec VPN-Tunnel sowie in Rechenzentren und bei Routing-Lösungen für Campus-Netzwerke ein Headend Gateway benötigt.

IN DER CLOUD VERWALTETE EINFACHHEIT UND SKALIERUNG

Aruba Central bietet zur Vereinfachung der Remote-Verwaltung verschiedener Hardwarekomponenten in einer Niederlassung eine zentrale Ansicht. Sie enthält Dashboards zur Konfiguration und Transparenz von kabellosen, kabelgebundenen und WAN-Verbindungen, Funktionen zur Optimierung des Datenverkehrs und integrierte Tools zur Fehlerbehebung.



Aruba Central-Dashboard für WLAN-, LAN- und WAN-Management

Durch mehrere Ebenen von IT-Administratorberechtigungen kann die Workload in Umgebungen verteilt werden, die mehrere Zeitzonen oder Verantwortlichkeiten innerhalb der IT umfassen. Es lässt sich ganz einfach einrichten, wer Änderungen an der Hardware in jeder Niederlassung anzeigen und vornehmen darf. Außerdem können Benutzern mit Aufgabenbereichen beim Help-Desk auch nur Leseberechtigungen zugeordnet werden.

INTEGRIERTE, ERSTKLASSIGE SICHERHEIT

Die mangelnde Transparenz der IT in Niederlassungsumgebungen ist von größter Bedeutung.

IoT-Geräte werden ohne Wissen der IT mit dem Netzwerk verbunden. Die Benutzer finden Wege, Sicherheitskontrollen zu umgehen, bei denen die Entfernung zwischen Unternehmen und Niederlassungen in der Regel eine Rolle spielt. Die Verbindung zu Geräten, deren Verhalten sich verschlechtert hat, kann nur schwer unterbrochen werden.

Die kabellosen und kabelgebundenen Lösungen von Aruba unterstützen rollenbasierte Funktionen für die Zugriffssicherheit, die eine dynamische Unterteilung von Geräten und Datenverkehr ermöglichen. Der Gateway in Niederlassungen umfasst eine integrierte, statusabhängige Firewall, durch die die Niederlassung vor internen Bedrohungen durch Deep Packet Inspection (DPI) geschützt ist. Aruba Central kann wiederum für die Durchsetzung von Regeln zur Web- und Inhaltsfilterung verwendet werden.

Aruba ClearPass bietet die unternehmensweite Skalierbarkeit für alle Arten von Umgebungen. Dies ermöglicht die dynamische Erstellung von Geräteprofilen, die Gewährung von Echtzeit-Zugriffsrechten und eine differenzierte Umsetzung von Richtlinien mit der Möglichkeit, ein Gerät ohne physischen Eingriff unter Quarantäne zu stellen.

CLOUD-BASIERTE SICHERHEITSFUNKTIONEN

Angesichts der Tatsache, dass immer mehr Anwendungen und Lösungen in die Cloud verlagert werden, bietet ein zuverlässiges Partnerprogramm den Kunden die Möglichkeit, Sicherheitsfunktionen anderer Anbieter zu nutzen, die in der Cloud gehostet werden. Anstatt den gesamten Datenverkehr an das Rechenzentrum zu leiten, kann die mobile Peripherie von heute durch die Korrelation von Echtzeitbedrohungen, die Überprüfung von Inline-Inhalten und andere Kontrollen der Cloud-Firewall ganz einfach geschützt werden.

EIN OPTIMIERTES ERLEBNIS IN NIEDERLASSUNGEN

Um den Benutzern in Niederlassungen dasselbe Erlebnis wie im Unternehmen zu bieten, kann die IT-Abteilung die Zugriffs-, Bandbreiten- und Sicherheitsrichtlinien auf der Grundlage von Rollen und anderen kontextbezogenen Daten ganz einfach durchsetzen. Hierbei wird der Kontext zu jedem Benutzer, vernetzten Gerät und den Arten der verwendeten Anwendungen genutzt.

Diese besondere Kontextbezogenheit kann dazu beitragen, WAN-Richtlinien innerhalb des Gateways einer Niederlassung durchzusetzen, z. B. um sicherzustellen, dass eine bestimmte Gruppe von Benutzern, die Skype for Business verwenden, eine höhere Priorität erhält als andere. Richtlinien können innerhalb des Gateways auch für eingehenden Datenverkehr und Datenverkehr zwischen Niederlassungen umgesetzt werden.

Über den Gateway kann auch der Status von WAN-Verbindungen überwacht werden. Dies ermöglicht ein nahtloses Failover von einer Verbindung zu einer anderen. Diese Funktionen sind möglich, da Aruba kabelgebundene, kabellose, WAN- und sicherheitsspezifische Kontexte liefert und deren Durchsetzung im gesamten Niederlassungsnetzwerk bietet.

ZUSAMMENFASSUNG

Während Unternehmen nach Möglichkeiten zur Umgestaltung der Standorte ihrer Niederlassungen suchen, ist das wichtigste Alleinstellungsmerkmal von Aruba eine offene, softwarebasierte, flexible, skalierbare und einfach zu implementierende Lösung. Kunden können zwischen branchenführenden kabellosen, kabelgebundenen und WAN-Technologien sowie Cloud-Management- und Sicherheitslösungen auswählen, die das bestmögliche Erlebnis für IT-Mitarbeiter und Benutzer sicherstellen.

aruba
a Hewlett Packard Enterprise company

HERRENBERGER STR. 140 | 71034 BÖBLINGEN | DEUTSCHLAND
aruba.germany@hpe.com | aruba.austria@hpe.com | aruba.switzerland@hpe.com

www.arubanetworks.com_