LÖSUNGSÜBERBLICK

DYNAMISCHE SEGMENTIERUNG

Einfacher und sicherer Zugriff zur Vereinheitlichung kabelgebundener und kabelloser Netzwerke

Die wachsende Zahl an IoT-Geräten und die Verwendung von geschäftskritischer Mobilität und Cloud-Services sorgen für Innovation am digitalen Arbeitsplatz und bringen uns zu der Frage, ob das Netzwerk-Edge intelligent genug ist, um all diese unterschiedlichen Geräte und Benutzer sicher miteinander zu verbinden. Die bisher verwendeten kabelgebundenen und kabellosen Netzwerke wurde ohne Gedanken an geschäftskritische Mobilität, IoT-Zugriff oder Sicherheit erstellt. Der heutige Ansatz der Verwendung manueller und statischer Konfigurationen für diese sich ständig ändernden mobilen und IoT-Geräte in Campus- und Filialnetzen stellt neue Sicherheitsrisiken dar und ist zu einer mühsamen Aufgabe geworden, mit der sich IT-Teams tagtäglich auseinandersetzen müssen.

Zur Vereinfachung und Sicherung des Netzwerks vereinheitlicht Aruba Dynamic Segmentation die Durchsetzung von Richtlinien in kabelgebundenen und kabellosen Netzwerken und hält den Datenverkehr sicher und getrennt. So können interne Betriebsabläufe und von der Unternehmenszentrale verwaltete Netzwerke einfach von den IoT-Geräten und den vom IT-Team verwalteten Clientgeräten getrennt werden. Gleichzeitig wird nicht nur das Netzwerkerlebnis, sondern werden auch die IT-Prozesse von Ende bis Ende optimiert.

Die dynamische Segmentierung nutzt die Erkenntnisse aus Arubas grundlegender rollenbasierter Richtlinienfunktionalität, Benutzer-Firewalls sowie umfangreiche Layer-7-Anwendungstransparenz und die integrierte Filterung von Webinhalten.

WICHTIGE GESCHÄFTLICHE UND TECHNISCHE EINFLUSSFAKTOREN

Einfachere Richtlinienverwaltung

Für das Onboarding von IoT- und Client-Geräten waren in der Regel mehrere Berührungspunkte erforderlich – oft in Verbindung mit der manuellen Konfiguration neuer VLANs, ACLs oder Subnetze an allen Hops im Netzwerk. Auch das Hinzufügen, Verschieben und Ändern kann in großen, verteilten Netzwerken zeitraubend und fehleranfällig sein. Der Entwurf eines Netzwerks mit hoher Sicherheit und geringer Komplexität galt im Allgemeinen als unmöglich.

HAUPTVORTEILE

- **Ein besseres, konsistenteres Benutzererlebnis:** Erweitern Sie Benutzerrollen, Deep Packet Inspection von Anwendungen und Geräteprofilerstellung von kabellosen auf kabelgebundene Netzwerke.
- **Einfacherer Netzwerkbetrieb:** Sparen Sie Zeit und verhindern Sie die VLAN-Ausbreitung durch die Reduzierung der für SSIDs, ACLs, Subnetzwerke und kabelgebundene Ports erforderlichen Konfiguration.
- **Mehr Sicherheit und Gerätetransparenz:** ClearPass und Policy Enforcement Firewalls (PEF) ermöglichen mehr Transparenz und die Durchsetzung von Richtlinien.

Verbesserung des Benutzererlebnisses

Wenn Benutzer von Schreibtisch zu Schreibtisch oder von Standort zu Standort wechseln, erwarten sie die gleiche Netzwerkleistung, unabhängig davon, wo und wie sie sich verbinden – mit oder ohne Kabel. Dabei kann es sich als Problem herausstellen, sie um die Verwendung eines VPN (Virtual Private Network) zu bitten. Jede Netzwerkerfahrung, die IT-Support erfordert, wird als negativ betrachtet. Das Erlebnis der Benutzer – unabhängig davon, ob es sich um Mitarbeiter, Gäste, Kunden oder Studenten handelt – wirkt sich auf den Erfolg eines Unternehmens aus. Der Anschluss neuer Gerätetypen wie Smartphones, Drucker oder Zubehör für Videokonferenzen erfolgt häufig ohne das Wissen bzw. den Support der IT. Dabei wird erwartet, dass die IT ein fehlerloses Erlebnis bietet, während die Transparenz und die Verwaltung aller Dinge in einem sicheren Netzwerk gewahrt bleiben.

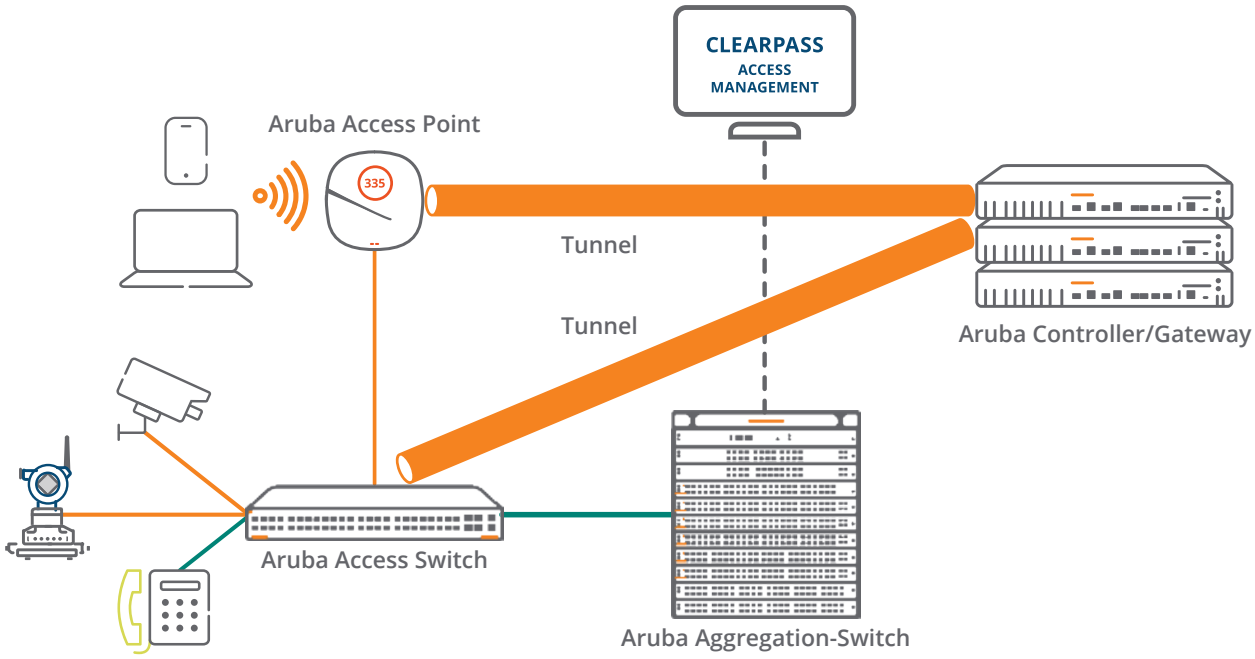
Die Netzwerkanfälligkeit wird zunehmen angesichts der Prognose, dass die Anzahl von IoT/Headless-Geräten, die mit Unternehmensnetzwerken verbunden sind, bis 2020 voraussichtlich auf über 20 Milliarden wächst.

Quelle: Gartner (Januar 2017)

Von intelligenter Beleuchtung über Sicherheitskameras bis hin zu Badge-Lesegeräten werden IoT-Geräte schnell in Netzwerken aller Größen eingesetzt. Diese neu entdeckte Netzwerkkonnektivität bringt viele attraktive Vorteile mit sich, setzt das Netzwerk aber auch Sicherheitsrisiken aus, da diese Geräte die gleichen Wege nutzen wie sensible finanzielle, medizinische und geschäftskritische Daten. Diese Geräte verfügen nur selten über integrierte hohe Sicherheit oder gar eine zuverlässige Authentifizierung. Passwörter werden als Klartext gespeichert, es fehlen ihnen sichere Supplicants, und sie befinden sich oft physisch in ungesicherten öffentlichen Bereichen – was Netzwerksicherheitsverstößen Tür und Tor öffnet.

WLAN-INNOVATIONEN JETZT AUCH FÜR SWITCHES

Die dynamische Segmentierung erweitert die Möglichkeiten von Aruba zur sicheren Richtlinienverwaltung und WLAN-Richtliniendurchsetzung, um den kabelgebundenen Netzwerkzugriff einfach und sicher zu gestalten. Diese Fähigkeit bedeutet, dass kabelgebundenen Client-Geräten dynamisch Richtlinien basierend auf der Port- oder Benutzerrolle zugewiesen werden können – ideal, wenn man bedenkt, dass die Anzahl der IoT-Geräte bis 2020 voraussichtlich 20 Milliarden erreichen wird. Die Netzwerk-Switches von Aruba, die jetzt über die Unterstützung durch



Dynamic Segmentation, Teil des Experience Edge

ClearPass für das Management und Mobility Controller für die Durchsetzung von Richtlinien verfügen, spielen eine entscheidende Rolle in der Vereinheitlichung des Netzwerkzugriffs.

Rollenbasierte Richtlinien

Durch die Implementierung der dynamischen Segmentierung werden rollenbasierte Richtlinienentscheidungen basierend auf dem Gerätetyp, der verwendeten Anwendung und sogar dem Standort des Benutzers bzw. des Geräts getroffen und entsprechende Zugriffsrechte vergeben. Ursprünglich zur Adressierung von Sicherheitsfragen in kabellosen Netzwerken verwendet, segmentieren rollenbasierte Richtlinien den Netzwerkverkehr nach Benutzertypen wie Mitarbeiter, Gast oder Auftragnehmer und vereinfachen gleichzeitig das Netzwerkmanagement durch die Eliminierung komplexer und statischer Netzwerkkonfigurationen. Diese leistungsstarke Funktion sorgte für die Optimierung von IT-Workflows wie der Verwaltung von Zugriffs- und BYOD-Richtlinien und für eine bessere Anwendungsleistung.

Die Erweiterung der dynamischen rollenbasierten Richtlinienverwaltung auf kabellose Access Points und kabelgebundene Switches bietet eine grundsätzlich einfache, sichere und dennoch andere Möglichkeit, Richtlinien für Mobilität, IoT und Cloud zu verwalten und durchzusetzen. Mobility Controller/Gateways von Aruba, die ClearPass Richtliniendefinitionen durchsetzen, sind nun in der Lage, Rollen dynamisch zu verstehen und zu nutzen. Durch diese Fähigkeit zur dynamischen Zuweisung entfällt die zeitaufwändige und fehleranfällige Aufgabe der Verwaltung komplexer und statischer VLANs, ACLs und Subnetzwerke.

Layer-4-7-Segmentierung

Ein zweites grundlegendes Leistungsmerkmal der Aruba Switches ist die Segmentierung. Durch die Verwendung von Tunneln zwischen Access Points und einem Controller oder Gateway bleibt der Datenverkehr in der Aruba WLAN-Architektur sicher und getrennt. Diese tunnelbasierte Segmentierung bietet Sicherheit, wie z. B. die Firewall-Überprüfung von riskantem Datenverkehr, durch die Verwendung der integrierten Policy Enforcement Firewall (PEF) von Aruba. PEF liefert einen detaillierten Kontext (Benutzer, Gerät, Anwendung, Standort) und reduziert so den

Die dynamische Segmentierung vereinfacht und sichert kabelgebundene und kabellose Netzwerke durch die Einrichtung des Mobility Controller als Engine für die Durchsetzung einheitlicher Richtlinien. Datenverkehr von einem Access Point oder Switch wird zur Überprüfung durch die Policy Enforcement Firewall (PEF) in GRE-Tunneln verkapselt.

Bedarf an teuren Firewalls für die erste Stufe der Befragung und Verteidigung. Mit kontextbezogenen Richtlinien, die auf Identitäten, Gerätetyp und Standort basieren, können Sie die Anforderungen verschiedener Benutzergruppen mit einer einzigen Netzwerkkonfiguration erfüllen, da sich die Verkehrsströme einfach an die zugewiesenen Rollen anpassen.

Durch die Verwendung dieser WLAN-Tunneling-Architektur können Aruba Switches nun eine rollenbasierte Segmentierung anstelle der herkömmlichen, eher manuellen Verwendung lokaler VLANs bieten. Dies ist ideal für nicht vertrauenswürdige IoT-Geräte oder für die Bereitstellung von Anwendungstransparenz, da Aruba Switches nun ausgewählten Datenverkehr dynamisch zum Controller tunneln können, um Deep Packet Inspection und Geräteauthentifizierung wie ein Access Point durchzuführen. So kann einer Sicherheitskamera eine Rolle mit Rechten zugewiesen werden, durch die der von dieser Kamera ausgehende Datenverkehr nur an einen bestimmten Server geleitet werden kann, um so die Möglichkeit eines böswilligen Eindringens in andere Teile des Netzwerks zu verhindern.

Diese neue Segmentierungsfunktion verbessert das Sicherheitsniveau beim Tunneling: Möglich sind entweder Port-Based Tunneling (PBT) – hier erfolgt die gesamte Authentifizierung auf dem Controller – oder User-Based-Tunnelling (UBT) – mit Authentifizierung auf dem Switch. Da diese Segmentierung als Overlay fungiert, kann sie mit VLAN-Implementierungen koexistieren, indem sie in ausgewählten Bereichen sichere Tunnel verwendet, ohne die gesamte Switching-Infrastruktur komplett auszutauschen.

DIE LÖSUNGSKOMPONENTEN

Aruba Wireless Access Points

WLAN-Leistung nach 802.11ac und 802.11ax, die den Anforderungen aller Umgebungen entspricht. Integrierte KI-Intelligenz und Standortservices, die der IT die Automatisierung und Transparenz bieten, die diese benötigt, um für Benutzer und IoT-Geräte ein optimales Erlebnis zu bieten.

Aruba Netzwerk-Switches

Erstellen Sie eine integrierte Grundlage, die Skalierbarkeit, Sicherheit und hohe Leistung für kabelgebundenen und kabellosen Datenverkehr in Campus- und Filialnetzwerken bietet. Die dynamische Segmentierung bietet IT-Teams eine einfache Möglichkeit, Richtlinien anzuwenden, erweiterte Services zu nutzen und kabelgebundenen Benutzer- und IoT-Verkehr überall im Netzwerk über Tunnel sicher zu segmentieren – durch Port-Based Tunnel (PBT) mit Authentifizierung am Controller oder über User-Based Tunnel (UBT) mit Authentifizierung am Aruba-Switch.

Aruba Gateways und Mobility Controller

Controller bzw. Gateways sind wichtige Bestandteile der Lösung und dienen zur Durchsetzung von Richtlinien für kabelgebundenen wie kabellosen Datenverkehr. Der Aruba Mobility Controller (mit AOS 8.1 oder höher) ermöglicht der IT die Nutzung von Richtliniendurchsetzung, Bandbreitenverträgen und anderen Einschränkungen des Datenverkehrs. In einer Zweigstellenumgebung übernimmt der von Aruba Central verwaltete Branch Gateway diese Rolle. Die Policy Enforcement Firewall dient als zugrundeliegende Netzwerktechnologie zur Unterstützung dieser beiden Umgebungen.

Aruba ClearPass Policy Manager mit Profilerstellung

Zentrale Verwaltung und Durchsetzung von Netzwerkzugriffs-richtlinien für die kabellose und kabelgebundene Zugriffs-steuerung. Zu den primären Funktionen gehören das Erstellen von Geräteprofilen, Authentifizierung, Autorisierung und Richtliniendurchsetzung. Bei Verwendung von ClearPass folgen Rolle und damit verbundene Berechtigungen nach ihrer Festlegung dem Benutzer oder Gerät über kabellosen und kabelgebundenen Zugriff. Wenn Benutzer also zu einem unbekannten Gerät wechseln oder sich in einem ungesicherten Netzwerk befinden, ändert die Richtlinie automatisch die Berechtigungen. Herunterladbare Benutzerrolle (Downloadable User Roles, DUR) werden in ClearPass konfiguriert, wodurch die Notwendigkeit entfällt, Rollen oder Richtlinien auf einem Switch zu definieren.

ZUSAMMENFASSUNG

Um geschäftskritische Mobilität und neue IoT-Konnektivitätsanforderungen besser erfüllen zu können, vereinfacht die innovative Dynamic Segmentation Lösung von Aruba den IT-Betrieb und verbessert die Sicherheit durch die dynamische Anwendung einheitlicher Richtlinien und die Durchsetzung erweiterter Services überall im Netzwerk. Dadurch ist gewährleistet, dass angemessene Zugriffs- und Sicherheitsrichtlinien nahtlos verteilt, automatisch angewendet und unabhängig für alle kabellosen und kabelgebundenen Benutzer und Geräte durchgesetzt werden.

SO_DynamicSegmentation_SK_092419 a00058593dee