aruba
a Hewlett Packard Enterprise company

LÖSUNGSÜBERSICHT

Aruba ESP mit Zero Trust Security

Sicherheit am Edge

Die Herausforderungen in Bezug auf die Netzwerksicherheit sind im Lauf der letzten Jahre angesichts zunehmender Dezentralisierung der Benutzer und immer hartnäckiger und ausgefeilter auftretender Attacken signifikant gewachsen. Traditionelle Sicherheitskonzepte, die sich primär auf den Schutz des Netzwerkperimeters konzentrieren, reichen als alleinige Sicherheitsstrategie nicht mehr aus. Moderne Netzwerksicherheit muss nicht nur imstande sein, eine ständigen Veränderungen unterworfene Menge von Benutzern und Geräten aller Art zu bewältigen, sondern auch mit zunehmend häufigeren Bedrohungen fertig werden, die auf bisher für sicher gehaltene Teile der Netzwerkinfrastruktur abzielen.

Das zuletzt verstärkt in Erscheinung getretene Zero Trust gilt als effektives Modell, das den sich verändernden Sicherheitsanforderungen moderner Unternehmen besser gerecht wird, da es zunächst einmal unterstellt, dass sämtliche Benutzer, Geräte, Server und Netzwerksegmente inhärent unsicher und potenziell feindlich sind. Aruba ESP mit Zero Trust Security verstärkt den gesamten Netzwerksicherheitsstand durch ein Bündel von Best Practices und rigoroseren Sicherheitskontrollen gegenüber bisher als vertrauenswürdig erachteten Netzwerkressourcen.

ARUBA ESP: ZERO-TRUST-GRUNDPRINZIPIEN

Je nachdem, welcher Bereich der Sicherheit betrachtet wird, kann Zero Trust unterschiedliche Formen annehmen. Auch wenn Kontrollmechanismen auf Anwendungsebene ein Schwerpunkt bei Zero Trust sind, muss eine umfassende Strategie auch die Netzwerksicherheit und die wachsende Anzahl von angeschlossenen Geräten berücksichtigen, gerade in Zeiten des zunehmenden Arbeitens im Homeoffice. Aruba ESP mit Zero Trust Security bietet Rundumsichtbarkeit, Mikrosegmentierung und Kontrolle nach dem Prinzip der geringsten Zugriffsrechte sowie kontinuierliche Policy-Überwachung und -Durchsetzung. Auch traditionelle VPN-Lösungen lassen sich damit verbessern, da sichergestellt wird, dass dieselben Kontrollfunktionen, die auf Campus- oder Filialnetzwerke angewendet werden, auch für das Homeoffice und Remotearbeit gelten.

Im Zeitalter des Internet der Dinge (IoT) sind die Grundprinzipien guter Netzwerksicherheit manchmal schwer zu implementieren. Sofern möglich, sollten alle Geräte und Benutzer identifiziert und ordnungsgemäß authentifiziert werden, bevor sie Zugriff auf das Netzwerk erhalten. Zusätzlich zur Authentifizierung sollte Benutzern und Geräten nur die geringsten Zugriffsrechte erteilt werden, die sie zur

Erfüllung ihrer geschäftskritischen Aufgaben im Netzwerk benötigen. Dazu muss jeder Benutzer und jedes Gerät für die Netzwerkressourcen und Anwendungen autorisiert werden, auf die sie zugreifen dürfen. Des Weiteren muss die gesamte Kommunikation zwischen Endbenutzern und Anwendungen verschlüsselt erfolgen.

UMFASSENDE SICHTBARKEIT IST UNVERZICHTBAR

Mit der zunehmenden Nutzung des IoT wird die vollständige Übersicht über sämtliche Geräte und Benutzer im Netzwerk zu einer immer anspruchsvolleren Herausforderung. Ohne diese Sichtbarkeit sind wichtige Sicherheitskontrollen, die ein Zero-Trust-Modell unterstützen, kaum umzusetzen. Faktoren wie Automatisierung, KI-basiertes maschinelles Lernen und die Fähigkeit, Gerätetypen sofort zu identifizieren, sind unverzichtbar.

Aruba ClearPass Device Insight nutzt eine Kombination aus aktiver und passiver Erkennung sowie Profilerstellungstechniken, um das gesamte Spektrum von Geräten zu erkennen, die mit dem Netzwerk verbunden sind oder eine Verbindung anfordern. Dazu zählen auch benutzereigene Geräte wie Laptops und Tablets. Im Unterschied zu herkömmlichen Tools erkennt es auch die immer vielfältigeren IoT-Geräte, die in heutigen Netzwerken in zunehmender Häufigkeit anzutreffen sind.

„GERINGSTER ZUGRIFF“ UND MIKROSEGMENTIERUNG

Wenn die Sichtbarkeit gewährleistet ist, bestehen die nächsten wichtigen Schritte in der Übernahme von Best Practices für Zero Trust, beispielsweise das Prinzip des geringsten Zugriffs sowie Mikrosegmentierung. Für jeden Endpunkt im Netzwerk ist die bestmögliche Authentifizierungsmethode (d. h. vollständige 802.1X- und Multifaktor-Authentifizierung für Benutzergeräte) zu verwenden. Darüber hinaus muss eine Zugriffssteuerungsrichtlinie implementiert werden, die nur den Zugriff auf Ressourcen gestattet, die für das betreffende Gerät oder den betreffenden Benutzer absolut erforderlich sind.

Aruba ClearPass Policy Manager ermöglicht die Erstellung von rollenbasierten Zugriffsrichtlinien, die den IT- und Sicherheitsteams helfen, die Best Practices zu operationalisieren. Dazu wird jeweils nur eine einzelne Rolle mit zugehörigen Zugriffsberechtigungen vergeben, die überall im Netzwerk gelten – in kabelgebundener oder kabelloser Infrastruktur, in Filialen oder auf einem Campus. Nach der Erstellung eines Profils wird den Geräten automatisch die entsprechende Zugriffssteuerungsrichtlinie zugeordnet. Anschließend werden sie durch die Aruba Dynamic Segmentation-Funktion gerätespezifisch segmentiert. Die Regeldurchsetzung übernimmt die Policy Enforcement Firewall (PEF) von Aruba, eine komplette, in die Aruba Netzwerkinfrastruktur integrierte Anwendungsfirewall. Für WLAN-Netzwerkverbindungen nutzt die Aruba Infrastruktur sichere Verschlüsselungsprotokolle wie den hohen WPA3 Standard.

ClearPass Policy Manager lässt sich in zahlreiche Authentifizierungslösungen integrieren, unterstützt Multifaktor-Authentifizierung und bietet die Möglichkeit, an wichtigen Punkten im Netzwerk eine erneute Authentifizierung zu erzwingen. Im Rahmen des ClearPass Ökosystems können die Kunden problemlos weitere Lösungen implementieren, um Zero-Trust-Anforderungen hinsichtlich Korntextinformationen und anderer Sicherheitstelemetrie zu erfüllen.

Somit integriert sich ClearPass nahtlos in eine Vielzahl weiterer Lösungen, z. B. auch Sicherheit-Tools für Endpunkte, die intelligentere Zugriffssteuerungsentscheidungen anhand des Sicherheitsstands eines Geräts ermöglichen. Die anzuwendenden Zugriffssteuerungsrichtlinien können dabei vom verwendeten Gerätetyp, vom aktuellen Standort des Benutzers und anderen kontextbezogenen Kriterien abhängig gemacht werden.

KONTINUIERLICHE REGELÜBERWACHUNG UND -DURCHSETZUNG

Nach Einrichtung der rollenbasierten Zugriffssteuerung, die eine granulare Segmentierung gewährleistet, besteht eine weitere Best Practice von Zero Trust in der laufenden Überwachung der Benutzer und Geräte im Netzwerk. Dies schützt vor Risiken in Form von Insider-Bedrohungen, spezieller Malware oder drohenden Angriffen unter Umgehung der herkömmlichen Perimeter-Verteidigungsmaßnahmen.

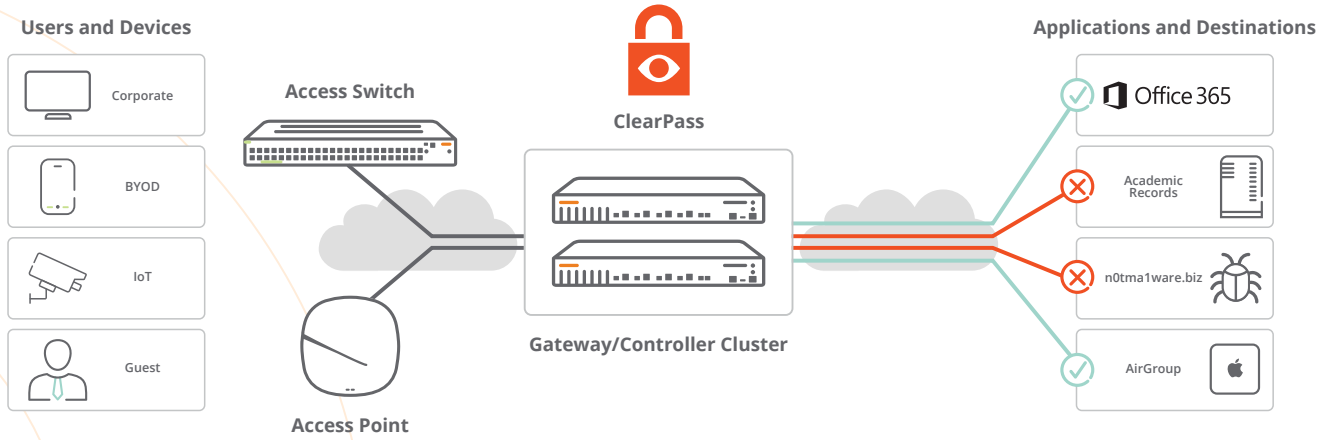
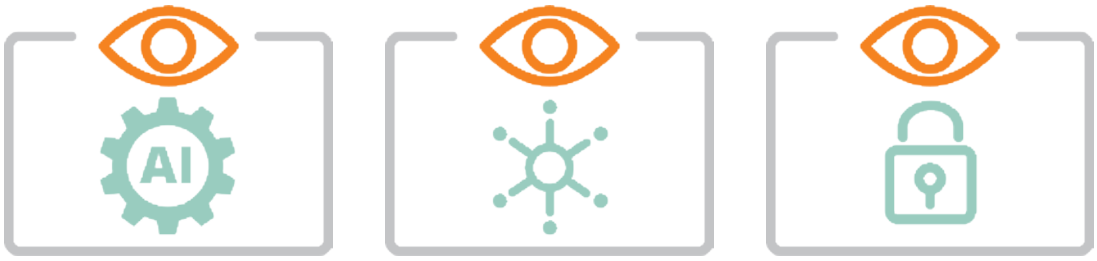


Abbildung 1: Aruba ClearPass weist automatisch rollenbasierte Zugriffssteuerungsrichtlinien zu, die mithilfe der Dynamic Segmentation durchgesetzt werden

ARUBA ESP (EDGE SERVICES PLATFORM)

The industry's first platform with an AI-powered 6th sense to automate and protect



AIOps
AI Insights | Networks Analytics Engine
User Experience Insight | Device Insight

Unified Infrastructure
Wi-Fi | Switching | SD-WAN
Cloud | 5G | Common Data Lake

Zero Trust Security
Dynamic Segmentation | Policy Enforcement
Firewall | ClearPass | Device Insight

Abbildung 2: Zero Trust Security ist ein Stützpfeiler von Aruba ESP

Bedrohungsschutz mit IDS/IPS

Die Bedrohungsschutzfunktionen von Aruba dienen zur Abwehr zahlreicher Bedrohungsszenarien wie Phishing, Denial-of-Service-Angriffe (DoS) und die immer häufiger werdenden Ransomware-Attacken. Aruba 9000 SD-WAN-Gateways sorgen im Zusammenwirken mit Aruba Central, ClearPass Policy Manager und der Policy Enforcement Firewall für identitätsbasierte Intrusion Detection and Prevention (IDS/IPS). Identitätsbasierte IDS/IPS bieten integrierte Filialnetzwerksicherheit durch eine signatur- und musterbasierte Prüfung des Filial-LAN-Datenverkehrs (Ost-West) sowie des SD-WAN-Datenverkehrs (Nord-Süd), die durch das Gateway fließen. Das erweiterte Sicherheits-Dashboard in Aruba Central stellt für die IT-Teams eine netzwerkweite Übersicht, multidimensionale Bedrohungsmetriken, Threat-Intelligence-Daten sowie Korrelations- und Störungsmanagement bereit. Bedrohungsereignisse werden zur Behebung an SIEM-Systeme und ClearPass gesendet.

360 Security Exchange

Mit über 150 Integrationen in branchenführende Sicherheitslösungen einschließlich Security Operations and Response-Toolsets (SOAR) sorgt ClearPass Policy Manager für eine dynamische Zugriffssteuerung auf Basis von Echtzeit-Bedrohungstelemetriedaten aus verschiedenen Quellen. Es können Richtlinien erstellt werden, um Zugriffssteuerungsentscheidungen in Echtzeit aufgrund von Benachrichtigungen zu treffen, die von Next-Gen Firewalls (NGFWs), Security Information and Event Management-Tools (SIEM) und vielen anderen Quellen stammen. Die ClearPass Aktionen sind vollständig konfigurierbar, vom Beschränken des Zugriffs (z. B. nur Internet) bis zum vollständigen Entfernen eines Geräts aus dem Netzwerk zur Behebung eines Problems.

ARUBA ESP (EDGE SERVICES PLATFORM)

Für Kunden, die Geschäftschancen am Edge nutzen möchten, haben wir Aruba ESP entwickelt, die branchenweit erste KI-basierte Plattform zur Vereinheitlichung, Automatisierung und Sicherung des Edge. Zero Trust Security ist eine zentrale Komponente von Aruba ESP, die in Kombination mit AIOps und einer einheitlichen Infrastruktur Unternehmen hilft, Kosten zu senken, Betriebsabläufe zu vereinfachen und die Sicherheit zu stärken.

ZUSAMMENFASSUNG

Moderne Netzwerkumgebungen und die aktuelle Bedrohungslandschaft erfordern ein neues Konzept. Die perimeterzentrierte Netzwerksicherheit der Vergangenheit ist auf die mobilen Belegschaften von heute und das Aufkommen von IoT-Geräten nicht ausgelegt. Aruba ESP mit Zero Trust Security bietet einen vollständigen Satz von Funktionen für Sichtbarkeit, Kontrolle und Regeldurchsetzung, die den Anforderungen einer dezentralisierten, IoT–orientierten Netzwerkinfrastruktur gerecht werden.

SO_ZeroTrustSecurity_051120 a00097694dee

Kontaktieren Sie uns Teilen