NETWORK ACCESS CONTROL

ClearPass Policy Manager – Pokročilá a bezpečná platforma NAC

ClearPass Policy Manager (CMPP), jako součást služby CRA NAC, je platforma pro řízení přístupu do sítě (Network Access Control, NAC). Zajišťuje bezpečné připojení pro jakékoliv zařízení, ať už se jedná o firemní počítač, osobní mobil, IoT zařízení nebo hosty.

HLAVNÍ FUNKCE:

- **Context-Based Policy Enforcement:** ClearPass vyhodnocuje kontext zařízení – kdo je uživatel, jaké je zařízení, kde se připojuje a kdy – a na základě toho dynamicky přiděluje přístupová práva. Například zaměstnanec se svým firemním notebookem bude mít jiný přístup než host se svým chytrým telefonem.
- **Fingerprint Profiling:** ClearPass umí automaticky identifikovat a klasifikovat každé připojené zařízení (např. zda se jedná o kameru, tiskárnu, nebo lékařské zařízení), aniž by potřeboval agenty na zařízeních.
- **Guest Access Management:** Poskytuje zabezpečený a přizpůsobitelný přístup pro hosty, a to s různými metodami ověření (samoobslužná registrace, sponzorované účty).
- **Endpoint Onboarding:** Automatizuje proces bezpečného připojení a konfigurace nových firemních zařízení (BYOD – Bring Your Own Device). Klienti si sami mohou nakonfigurovat síťový přístup pro svá zařízení.
- **Post-connect Security:** ClearPass průběžně monitoruje bezpečnostní stav zařízení i po jeho připojení k síti a může dynamicky měnit jeho přístupová práva, pokud detekuje nějakou anomálii.

VÝHODY PRO ORGANIZACE:

- **Zlepšení bezpečnosti:** Zabraňuje neautorizovanému přístupu, snižuje riziko úniku dat a brání šíření hrozeb.
- **Zjednodušení správy:** Centralizovaná správa politik z jednoho místa a automatizace procesů šetří čas IT administrátorům.
- **Podpora compliance:** Pomáhá organizacím splnit regulatorní požadavky týkající se zabezpečení dat.
- **Flexibilita:** ClearPass se integruje se stávající síťovou infrastrukturou a bezpečnostními řešeními od různých výrobců.

ARCHITEKTURA A MODULY:

- **Policy Manager:** Jádro platformy. Centralizovaná konzole pro správu, která vynucuje přístupové politiky.
- **OnGuard:** Agent, který se instaluje na zařízení. Provádí hloubkové bezpečnostní kontroly (např. zda je nainstalován antivirus, zda je aktivní firewall) před povolením přístupu.
- **Guest:** Modul pro správu hostovských účtů. Umožňuje různé typy registrace, včetně sponzorovaného přístupu a samoobslužné registrace.
- **Onboard:** Modul pro automatizovanou registraci a konfiguraci osobních zařízení uživatelů.
- **ClearPass Insight:** Webový portál, který poskytuje detailní přehled o všech zařízeních v síti, včetně jejich chování.

INTEGRACE S EKOSYSTÉMEM:

- ClearPass se integruje s širokou škálou produktů od různých dodavatelů, což umožňuje automatizaci a vynucování politik napříč celou IT infrastrukturou. Mezi podporované technologie patří např.*:

  - Síťové prvky: např. Fortinet, Aruba, Cisco, Juniper, Check Point a další.
  - Bezpečnostní řešení: SIEM systémy (např. Splunk, IBM QRadar), firewally (např. Fortinet, Palo Alto Networks), systémy pro správu zranitelností.
  - Cloudové služby: např. Microsoft Azure, AWS.
  - Identity Management: Active Directory, LDAP, cloudové adresáře.
  - MDM/UEM (Mobile Device Management/Unified Endpoint Management): např. Microsoft Intune, VMware Workspace ONE, Jamf Pro.

* Úplný seznam na vyžádání

ARCHITEKTURA A IMPLEMENTACE

- **Jádro (Policy Manager):**
  - ClearPass je softwarové řešení, které lze nasadit jako virtuální zařízení na hypervizorech VMware ESXi, Microsoft Hyper-V, KVM nebo jako fyzické zařízení (appliances).
  - Podporuje clusterovou architekturu pro zajištění vysoké dostupnosti a redundance s funkcemi Clustering a Load-Balancing (3-tí stranou).
  - Klientská zařízení komunikují s ClearPass přes standardní protokoly jako RADIUS (RFC 2865, 2866), TACACS+ (RFC 1492) pro ověření a autorizaci.
- **Konektivita a interoperabilita:**
  - Integruje se se síťovými zařízeními od různých výrobců prostřednictvím protokolů jako je RADIUS CoA (Change of Authorization), který umožňuje dynamicky měnit přístupová práva klienta i po jeho připojení, např. přesunutí do karantény.
  - Podporuje SNMP (Simple Network Management Protocol) pro monitorování zařízení a sběr dat.
  - Využívá API (Application Programming Interface) pro integraci s bezpečnostními systémy třetích stran, jako jsou SIEM, firewally, MDM platformy atd.

OVĚŘOVACÍ A AUTORIZAČNÍ PROCESY

- **Metody autentizace (EAP – Extensible Authentication Protocol):**
  - Podporuje širokou škálu EAP metod, včetně EAP-TEAP, EAP-TLS, EAP-TTLS, EAP-MSCHAPv2, EAP-PEAP, EAP-FAST, EAP-SIM/AKA. To umožňuje zabezpečenou autentizaci na bázi uživatelského jména a hesla, certifikátů, nebo tokenů.
  - ClearPass přijímá a zpracovává RADIUS Access-Requests a na základě kontextových politik vrací RADIUS Access-Accept/Reject.
  - Contextual Policy Engine: Autentizační a autorizační politiky jsou postaveny na souboru atributů získaných v reálném čase, jako jsou:
    - **Uživatelská identita:** Atributy z LDAP, Active Directory, SQL databází.
    - **Typ zařízení:** MAC adresa, Vendor ID (OUI), DHCP otisky (fingerprints), a HTTP User-Agent.
    - **Lokalita:** Geografická lokace, SSID, IP adresa.
    - **Bezpečnostní stav:** Informace z modulu OnGuard, které prověřují stav OS, přítomnost antiviru, stav patche atd.
- **Profilování zařízení (Fingerprint Profiling):**
  - Metody profilování: ClearPass používá kombinaci pasivních a aktivních metod pro identifikaci zařízení bez nutnosti agentů.
    - **DHCP fingerprinting:** Analýza DHCP zpráv.
    - **SNMP:** Sběr dat z portů síťových prvků.
    - **HTTP User-Agent:** Analýza hlaviček webového provozu.
    - **Nmap:** volitelné aktivní skenování pro hlubší detekci.
  - Výsledkem je detailní inventář všech připojených zařízení v síti.

MODULY A SPECIFICKÉ FUNKCE

- **ClearPass OnGuard:**
  - Nabízí Persistent Agent (trvale instalovaný na zařízení)
  - Provádí health checks na zařízeních, které zahrnují kontrolu, např.:
    - Antivirového softwaru (např. zda je spuštěn, aktualizován).
    - Firewallu (zda je aktivní).
    - Aktualizací systému a přítomnosti kritických záplat.
    - Přítomnosti nežádoucího softwaru.
- **ClearPass Onboard:**
  - Modul pro automatické BYOD (Bring Your Own Device) onboarding.
  - Distribuuje certifikáty pro klienty (např. pro EAP-TLS), a to prostřednictvím standardních protokolů jako je SCEP (Simple Certificate Enrollment Protocol).
  - Konfiguruje síťová nastavení na koncovém zařízení (např. konfigurace Wi-Fi sítě 802.1X).
- **Integrace s bezpečnostními řešeními:**
  - Využívá standardizované protokoly, jako je Syslog, CEF (Common Event Format), a JSON pro odesílání událostí do SIEM systémů.
  - Díky API umožňuje bidirectional integration s firewally a systémy pro správu zranitelností, což umožňuje automatické reakce na bezpečnostní incidenty, jako je přesunutí zařízení do karantény.