NETWORK ACCESS CONTROL

ClearPass Policy Manager – an advanced and secure NAC platform

As part of the CRA NAC service, the ClearPass Policy Manager (CPPM) is a Network Access Control (NAC) platform that ensures secure network connectivity for any type of device, whether it is a corporate computer, a personal mobile phone, an IoT device, or a guest.

KEY FEATURES:

- **Context-Based Policy Enforcement:** ClearPass evaluates device context – who the user is, the type of device used, where and when it connects – and dynamically assigns access rights accordingly. For example, an employee using a corporate laptop will receive different access than a guest using their smartphone.
- **Fingerprint Profiling:** ClearPass automatically identifies and classifies every connected device (e.g., whether it is a camera, printer, or a medical device) without requiring agents to be installed on endpoints.
- **Guest Access Management:** Provides secure and customisable guest access, offering multiple authentication methods (self-registration, sponsored accounts).
- **Endpoint Onboarding:** Automates the process of secure connection and configuration of new corporate devices (BYOD – Bring Your Own Device). Clients can configure network access for their own devices themselves.
- **Post-connect Security:** ClearPass continuously monitors the security posture of devices even after they are connected to the network and can dynamically change access rights if an anomaly is detected.

BENEFITS FOR ORGANISATIONS:

- **Improved Security:** Prevents unauthorised access, reduces the risk of data breaches, and limits the spread of threats.
- **Simplified Management:** Centralised policy management from a single point and process automation save time for IT administrators.
- **Compliance Support:** Helps organisations meet regulatory requirements related to data security.
- **Flexibility:** ClearPass integrates with existing network infrastructure and security solutions from multiple vendors.

ARCHITECTURE AND MODULES:

- **Policy Manager:** The core of the platform. A centralised management console that enforces access control policies.
- **OnGuard:** An agent installed on endpoints. Performs in-depth security checks (e.g., whether an antivirus has been installed or whether a firewall is active) before granting access.
- **Guest:** A module for managing guest accounts, enabling various types of registration, including sponsored and self-service access.
- **Onboard:** A module for automated onboarding and configuration of users' personal devices.
- **ClearPass Insight:** A web-based portal providing detailed visibility into all devices on the network, including their behaviour.

ECOSYSTEM INTEGRATION:

- ClearPass integrates with a wide range of products from various vendors, enabling policy automation and enforcement across the entire IT infrastructure. Supported technologies include, for example*:
  - Network features: Fortinet, Aruba, Cisco, Juniper, Check Point, and others.
  - Security solutions: SIEM systems (e.g., Splunk, IBM QRadar), firewalls (e.g., Fortinet, Palo Alto Networks), vulnerability management systems.
  - Cloud services: Microsoft Azure, AWS.
  - Identity management: Active Directory, LDAP, cloud directories.
  - MDM/UEM (Mobile Device Management / Unified Endpoint Management): Microsoft Intune, VMware Workspace ONE, Jamf Pro.

* Full list available upon request

ARCHITECTURE AND IMPLEMENTATION

- **Core (Policy Manager):**
  - ClearPass is a software-based solution that can be deployed as a virtual appliance on VMware ESXi, Microsoft Hyper-V, and KVM hypervisors, or as a physical device (appliance).
  - Supports clustered architecture to ensure high availability and redundancy using the Clustering and (third-party) Load Balancing functionalities.
  - Client devices communicate with ClearPass using standard protocols such as RADIUS (RFC 2865, 2866) and TACACS+ (RFC 1492) for authentication and authorisation.
- **Connectivity and Interoperability:**
  - Integrates with network devices from multiple vendors using protocols such as RADIUS CoA (Change of Authorisation), which enables dynamic modification of client access rights even after they connect (e.g., moving a device into quarantine).
  - Supports SNMP (Simple Network Management Protocol) for device monitoring and data collection.
  - Uses APIs (Application Programming Interfaces) for integration with third-party security systems such as SIEMs, firewalls, and MDM platforms.

AUTHENTICATION AND AUTHORISATION PROCESSES

- **Authentication Methods (EAP – Extensible Authentication Protocol):**
  - Supports a wide range of EAP methods, including EAP-TEAP, EAP-TLS, EAP-TTLS, EAP--MSCHAPv2, EAP-PEAP, EAP-FAST, and EAP-SIM/AKA. This enables secure authentication using usernames and passwords, certificates, or tokens.
  - ClearPass receives and processes RADIUS Access-Requests and returns RADIUS Access-Accept or Reject responses based on contextual policies.
  - Contextual Policy Engine: Authentication and authorisation policies are built on a set of real-time attributes such as:
    - **User identity:** Attributes from LDAP, Active Directory, SQL databases.
    - **Device type:** MAC address, Vendor ID (OUI), DHCP fingerprints, HTTP User-Agent.
    - **Location:** Geographic location, SSID, IP address.
    - **Security posture:** Information from the OnGuard module, verifying OS status, antivirus presence, patch status, etc.
- **Device profiling (Fingerprint Profiling):**
  - Profiling methods: ClearPass uses a combination of passive and active techniques to identify devices without agents.
    - **DHCP fingerprinting:** Analysis of DHCP messages.
    - **SNMP:** Data collection from network device ports.
    - **HTTP User-Agent:** Analysis of web traffic headers.
    - **Nmap:** Optional active scanning for deeper detection.
  - The result is a detailed inventory of all devices connected to the network.

MODULES AND SPECIFIC FEATURES

- **ClearPass OnGuard:**
  - Provides a Persistent Agent (permanently installed on the endpoint).
  - Performs endpoint health checks, including verification of, for example:
    - Antivirus software (e.g., whether it is running and up to date).
    - Firewall status (whether it is enabled).
    - System updates and the presence of critical security patches.
    - Presence of unwanted software.
- **ClearPass Onboard:**
  - A module for automated BYOD (Bring Your Own Device) onboarding.
  - Distributes client certificates (e.g., for EAP-TLS) using standard protocols such as SCEP (Simple Certificate Enrolment Protocol).
  - Configures network settings on endpoint devices (e.g., 802.1X Wi-Fi configuration).
- **Integration with Security Solutions**
  - Uses standardised protocols such as Syslog, CEF (Common Event Format), and JSON to send events to SIEM systems.
  - Using APIs, enables bidirectional integration with firewalls and vulnerability management systems, allowing automated responses to security incidents, such as quarantining compromised devices.