ClearPass Policy Model

An Introduction

Services Paradigm

Services are the highest level element in the Policy Manager policy model. They have two purposes:

Unique **Categorization Rules** (per Service) enable Policy Manager to test Access Requests (“Requests”) against available Services to provide robust differentiation of requests by access method, location, or other network vendor-specific attributes.

> NOTE
>
> Policy Manager ships configured with a number of basic Service types. You can flesh out these Service types, copy them for use as templates, import other Service types from another implementation (from which you have previously exported them), or develop new Services from scratch.

By wrapping a specific set of **Policy Components**, a Service can coordinate the flow of a request, from authentication, to role and health evaluation, to determination of enforcement parameters for network access.

The following image and table illustrate and describe the basic Policy Manager flow of control and its underlying architecture.

Figure 1: *Generic Policy Manager Service Flow of Control*

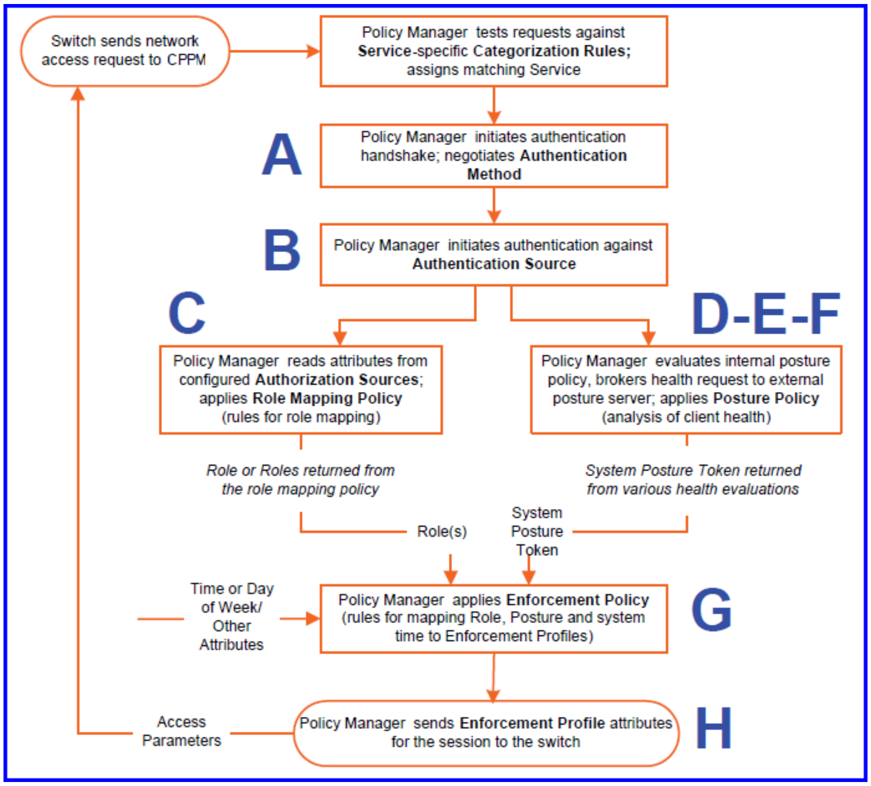
Switch sends network access request to CPPM
Policy Manager tests requests against Service-specific Categorization Rules; assigns matching Service
A
Policy Manager initiates authentication handshake; negotiates Authentication Method
B
Policy Manager initiates authentication against Authentication Source
C
D-E-F
Policy Manager reads attributes from configured Authorization Sources; applies Role Mapping Policy (rules for role mapping)
Policy Manager evaluates internal posture policy, brokers health request to external posture server; applies Posture Policy (analysis of client health)
Role or Roles returned from the role mapping policy
System Posture Token returned from various health evaluations
Role(s)
System Posture Token
Time or Day of Week/ Other Attributes
Policy Manager applies Enforcement Policy (rules for mapping Role, Posture and system time to Enforcement Profiles)
G
Access Parameters
Policy Manager sends Enforcement Profile attributes for the session to the switch
H

Table 1: *Policy Manager Service Components*

Component	Service: component ratio	Description
A - Authentication Method	Zero or more per service	EAP or non-EAP method for client authentication. Policy Manager supports four broad classes of authentication methods: • **EAP, tunneled:** PEAP, EAP-FAST, or EAP-TTLS. • **EAP, non-tunneled:** EAP-TLS or EAP-MD5. • **Non-EAP, non-tunneled:** CHAP, MS-CHAP, PAP, or MAC-AUTH. • MAC_AUTH must be used exclusively in a MAC-based Authentication Service. When the MAC_AUTH method is selected, Policy Manager: (1) makes internal checks to verify that the request is indeed a *MAC Authentication* request (and not a spoofed request) and (2) makes sure that the MAC address of the device is present in the authentication source. Some Services (for example, *TACACS+*) contain internal authentication methods; in such cases, Policy Manager does not make this tab available.
B - Authentication Source	Zero or more per service	An Authentication Source is the identity repository against which Policy Manager verifies identity. It supports these Authentication Source types: • Microsoft Active Directory • and LDAP compliant directory • RSA or other RADIUS-based token servers • SQL database, including the local user store. • Static Host Lists, in the case of MAC-based Authentication of managed devices.
C - Authorization Source	One or more per Authentication Source and zero or more per service	An Authorization Source collects attributes for use in Role Mapping Rules. You specify the attributes you want to collect when you configure the authentication source. Policy Manager supports the following authorization source types: • Microsoft Active Directory • any LDAP compliant directory • RSA or other RADIUS-based token servers • SQL database, including the local user store.

Table 1: *Policy Manager Service Components (Continued)*

Component	Service: component ratio	Description
C - Role Mapping Policy	Zero or one per service	Policy Manager evaluates Requests against Role Mapping Policy rules to match Clients to Role(s). All rules are evaluated and Policy Manager may return more than one Role. If no rules match, the request takes the configured Default Role. Some Services (for example, *MAC-based Authentication*) may handle role mapping differently: ● For *MAC-based Authentication* Services, where role information is not available from an authentication source, an Audit Server can determine role by applying post-audit rules against the client attributes gathered during the audit.
D - Internal Posture Policies	Zero or more per service	An Internal Posture Policy tests Requests against internal Posture rules to assess health. Posture rule conditions can contain attributes present in vendor-specific posture dictionaries.
E - Posture Servers	Zero or more per service	Posture servers evaluate client health based on specified vendor-specific posture credentials, typically posture credentials that cannot be evaluated internally by Policy Manager (that is, not by internal posture policies). Currently, Policy Manager supports two forms of posture server interfaces: *HCAP*, *RADIUS*, and *GAMEv2* posture servers.
F - Audit Servers	Zero or more per service	Audit servers evaluate the health of clients that do not have an installed agent, or which cannot respond to Policy Manager interactions. Audit servers typically operate in lieu of authentication methods, authentication sources, internal posture policies, and posture server. In addition to returning posture tokens, Audit Servers can contain post-audit rules that map results from the audit into Roles.
G - Enforcement Policy	One per service (mandatory)	Policy Manager tests Posture Tokens, Roles (and system time) against Enforcement Policy rules to return one or more matching Enforcement Policy rules to return one or more matching Enforcement Profiles (that define scope of access for the client).
H - Enforcement Profile	One or more per service	Enforcement Policy Profiles contain attributes that define a client's scope of access for the session. Policy Manager returns these Enforcement Profile attributes to the switch.

Copyright Information

Open Source Code

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by an Aruba warranty. For details, see the Aruba Networks standard warranty terms and conditions.