Requirements for Policy, Authorization and Enforcement of OPES Services

draft-ietf-opes-authorization-00

55th IETF
Atlanta, GA

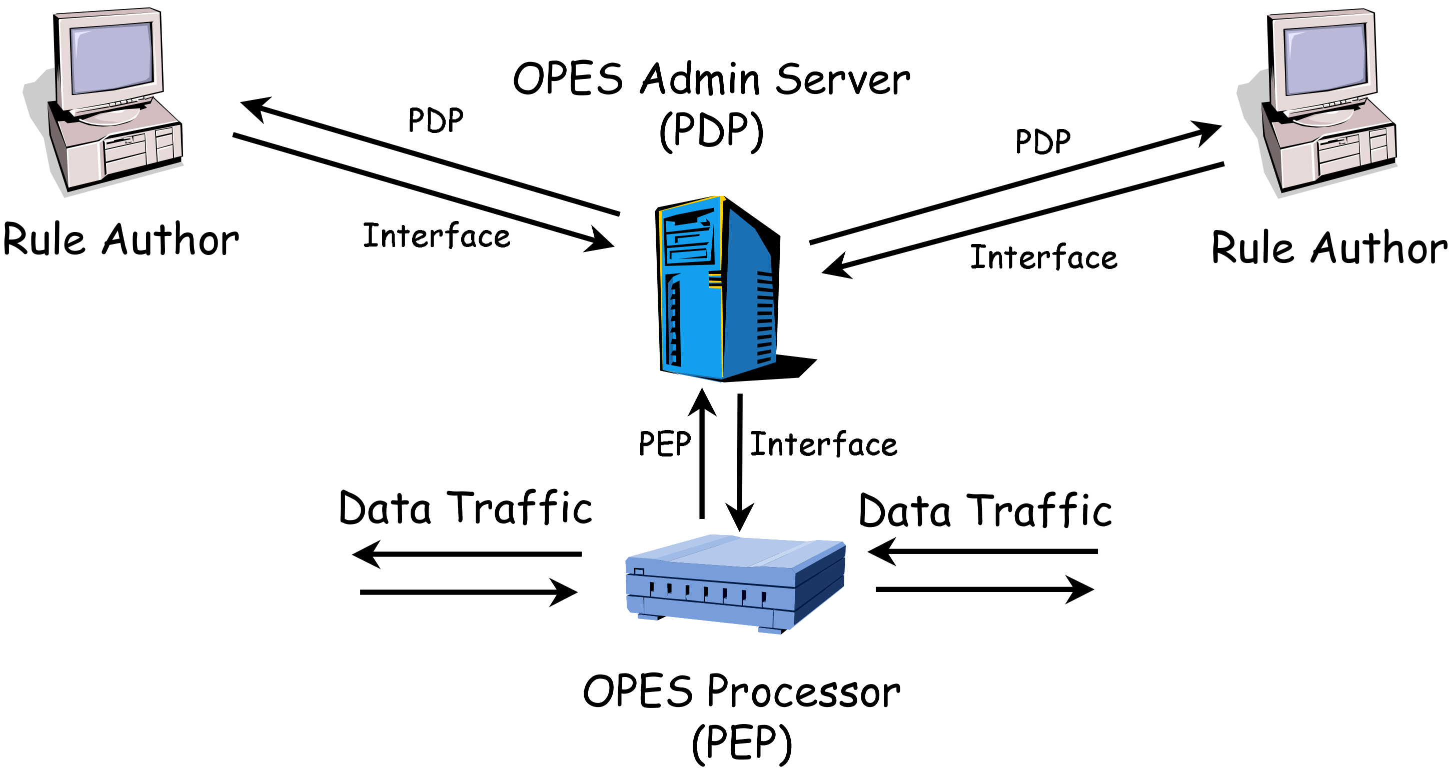
Andre Beck

Summary

- Specifies requirements for OPES policy architecture and OPES service authorization
- In parts based on earlier (pre-WG) draft
- First draft version published September 02
- Very little feedback received so far

Policy Architecture

- Policy functions are decomposed into three components
  - Rule Author
  - Policy Decision Point (PDP)
  - Policy Enforcement Point (PEP)



Policy Component Requirements

- PDP
  - Must authenticate rule authors
  - Must compile and validate received rules
  - Must distribute compiled rules to PEP
- PEP
  - Must evaluate compiled rules at different processing points and invoke triggered OPES services
  - Must consider side effects of service execution
  - Must support dynamic service bindings
  - Must support inter-service communication (environment variables)

Requirements for OPES Service Rules

- Rule conditions must be matched against attribute values of a given application protocol message
- Rule actions must identify OPES services to be executed
- Must be possible to specify OPES services in a location-independent fashion

Authorization Requirements

- Allow all users to request addition, deletion, or blocking of OPES services for their traffic (blocking means "do not use this service for my traffic").
- Prevent untrusted users from causing OPES services to interfere with the traffic of other users.
- Allow users to see their OPES service profiles and notify them of changes.
- Keep a log of all profile activity for audit purposes.
- Adhere to a privacy policy guarding users' profiles.

Authentication Requirements

- Users who wish to modify the OPES policy base must be authenticated by the OPES service provider
- PEPs should be authenticated before they receive policy rules

Integrity and Confidentiality Requirements

- Integrity using shared secrets MUST be used between all processing points, end-to-end (i.e., the two ends of a "hop" must share a secret, but the secret can be different between "hops"). The processing points include the callout servers.
- Encryption can be requested separately, with the same secret sharing requirement between "hops". When requested, encryption applies to all processing points, including callout servers.
- The signal for integrity (and optionally encryption) must originate from either the requestor (in which case it is applied to the response as well) or the responder (in which case it covers only the response).
- The shared secrets must be unique for each requestor/responder pair.

Privacy Requirements

- The PDP must have a privacy policy regarding OPES data such as user profiles for services. Users must be able to limit the promulgation of their profile data and their identities.

  Supported limitations MUST include:

  - Identity may not be given to callout servers.
  - Profile information may not be shared.
  - Traffic data may not be sent to callout servers run by third parties.
  - Traffic from particular sites should not be given to OPES callout servers.