CCNP Security - SISAS
ISE Concepts

What is ISE ?

- Provides a scalable and unified network access policy platform
- Centralized network access policy for any device, from anywhere, at anytime
  - Wired access
  - Wireless access
  - VPN access
- Implements a flexible policy-based model
  - Rule-based approach for authentication and authorization
  - Rules are composed of conditions and results

ISE Personas

- It supports both physical and virtual environments
- Built of three major roles, named personas
  - PSN (Policy Service Node)
    - Responsible for network access request processing
      - RADIUS, posture, profiling, web redirection, guest portal
  - PAN (Policy Administration Node)
    - Responsible for all configurations
      - Conditions, results, policies, external identity store integration
  - MnT (Monitoring and Troubleshooting Node)
    - Collects logs from PAN, PSN, NAD

ISE Deployment Modes

- All personas residing on the same entity
- Personas are distributed for scalability or design requirements
  - Multiple PSN's
  - 2 PAN's (one active, one standby)
  - 2 MnT's (one active, one standby)

ISE Architecture

- Everything circles around two types of policies
  - Authentication policies, processed first
  - Authorization policies, processed second
- Inbound AAA request flow
  - Authentication policy matching
    - Single or rule-based policy
      - Single model does not allow defining conditions
    - Rules are processed top-down until first match
      - Action “drop” means play dead, no RADIUS message sent back to NAD
      - Action “continue” means act like authentication was successful, inspect authorization policies

ISE Architecture

» Inbound AAA request flow

- Authorization policy matching
  - Standard and exception policies
    - – Exception policies are processed before standard policies
  - Rules are processed top-down until first match by default
  - Optionally multiple-rules can be matched with actions being combined
    - – Access-Accept takes precedence over Access-Reject

ISE Architecture

Authentication policies

- Based on configured conditions each request matches a rule
  - Request is routed over to configured Identity Store or Identity Sequence
  - Identity is validated
  - If successful authentication, token is passed over to Authorization policies
    - Otherwise send Access-Reject or actions configured for authentication failure

ISE Architecture

Authorization policies

- Only processed if authentication passed
  - Successful or by the explicit “continue” action
- Based on configured conditions each request matches a rule
  - On match, Access-Accept is issued and optional authorization attributes sent
    - ACL (dACL, filter-ID ACL, per-user ACL, airespace ACL)
    - dVLAN and voice VLAN permission
    - MACsec and URL Redirection (with Redirect-ACL)

ISE Authentication Policy

Authentication Policy format

- If condition
  - Identify the RADIUS packet based on RADIUS attributes
- Then allowed protocols
  - Which authentication protocol can be used by the supplicant
- And validate credentials
  - Which identity source can be queried for authentication

ISE Authorization Policy

Authorization Policy format

- If condition
  - Identify the RADIUS session or supplicant by profiling
- And optionally if used identity store
  - Store of user credentials
- Then apply authorization profile
  - User/device authorization

Q&A