CCNP Security - SISAS
ISE Identity Sources

ISE Identity Sources

- To authenticate and authorize machines/users, ISE can validate their credentials in two ways
  - Internally
  - Externally
- Internal Store has two types of entries
  - Endpoints (MAC database), organized into groups
    - Blacklist, GuestEndPoints, RegisteredDevices, Profiled
  - Users, organized into groups
    - Guest, ActivatedGuest, Employee, SponsorGroups
- Can be used as conditions in Authorization policies
  - Additional groups can be created

External Authentication Support

- ISE can authenticate/proxy against several external sources
  - RADIUS
  - LDAP
  - Active Directory
  - PKI (ISE CA server support was added in ISE 1.3)
- Active Directory (AD) integration is the most common one
  - ISE 1.2 supports a single AD integration
    - Multiple AD supports if all within same forest and trust is configured
  - ISE 1.3 supports up to 50 AD domains to be joined
- ISE joins AD just like a regular computer
  - Requires administrative rights just for join process
  - Afterwards join, it needs READ ALL rights at the top of the AD/forest schem

Active Directory Integration

- ISE and Domain Controller (DC) need to be NTP synchronized
  - Maximum time skew can be 5 minutes
  - In order to validate supplicant certificates
- Connectivity requirements between ISE and DC
  - Global Catalog (TCP 3268/3269)
  - LDAP (UDP/TCP 389)
  - LDAPS (TCP 636)
  - SMB (TCP 445)
  - KDC (TCP 88)
  - KPASS (TCP 466)

Authentication against AD

» Supported authentication options

- EAP-TLS
- EAP-MSCHAPv2

» EAP-TLS

- Supplicant certificate can be stored in Active Directory schema
- ISE can be configured to validate supplicant certificate against AD
  - Verify the identity of the machine or user
- By default in EAP-TLS, ISE just checks if certificate is valid
  - Not expired (certificate validity time compared with ISE clock)
  - Not revoked (uses CRL published by the supplicant’s CA issuer)

Authorization based on AD

- Users and computers are objects in the AD schema
  - Identified by their attributes
  - Attributes examples: username, hostname, group membership
- ISE can use there attributes in authorization policies
  - Allows for authorization policy scalability
  - Example: different authorization can be applied for different groups
- This is called contextual access
  - Authorization done based on multiple inputs/conditions
    - User and computer membership
    - Type of device (identified via profiling)
    - Method and time of network access

ISE Configuration for AD Integration

- Synchronize clock between AD DC and ISE
- Configure ISE with appropriate DNS server
  - It has to be a Domain Controller
- Configure ISE with the AD domain name
  - Test connectivity with AD DC
  - Join ISE into AD
- Define object attributes to be used in authorization policies
  - This step is optional but recommended

Q&A