Top Cisco ISE Interview Questions & Answers

Part – 1

Q#1.What are the different types of personas on Cisco ISE?

1. **Policy Administration Node (PAN)**
2. **Monitoring Node (MnT)**
3. **Policy Services Node (PSN)**

Depending on the size of your deployment all three personas can be run on the same device or spread across multiple devices for redundancy.

Press enter or click to view image in full size

Q#2.Explain the different types of personas on ISE?

Policy Administration Node (PAN) is where the administrator will login to configure policies and make changes to the entire ISE system. Once configured on the PAN the changes are pushed out to the policy services nodes. It handles all system-related configurations and can be configured as standalone, primary or secondary.

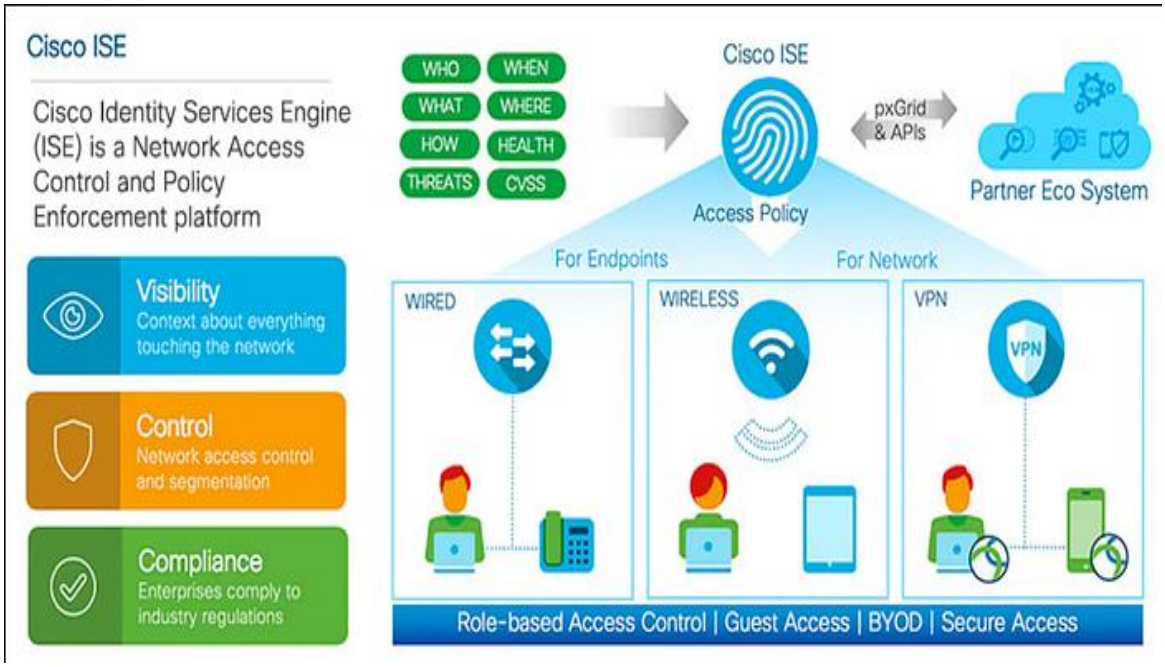
Monitoring Node (MnT) is where all the logs are collected and where report generation occurs. Every event that occurs within the ISE topology is logged to the monitoring node you can then generate reports showing the current status of connected devices and unknown devices on your network.

Policy Services Node (PSN) is the contact point into the network. Each switch is configured to query a radius server to get the policy decision to apply to the network port the radius server is the PSN. In larger deployments, you use multiple PSN's to spread the load of all the network requests. The PSN provides network access, posture, guest access, client provisioning, and profiling services. There must be at least one PSN in a distributed setup.

Q#3.How can we deploy ISE?

ISE can be either deployed on a physical appliance or Virtual Machine that enables the creation and enforcement of access policies for endpoint devices connected to a company's network.

Press enter or click to view image in full size



Physical appliance: SNS 3400(EOL), SNS 3500, SNS 3600
Virtual: ISE can be installed on VMware, Hyper-V

Q#4.What is the main objective of Cisco ISE?

Every time a wired or wireless user wants to access the network or tries to access a device [for device administration], the user is validated against the server to check if he/she is permitted to do so. Depending on the end result, the user will be allowed certain access to network/device.

Q#5.What is the difference between Cisco ISE vs ACS?

ACS is used to authenticate users to network devices and for VPN sessions but it is not a NAC solution wherein it will not be able to control the network by checking the compliance state of the devices in the network.

ISE is the next generation of network authentication and is so much more powerful than ACS. If you want to implement full network access control you need ISE.

Press enter or click to view image in full size

The Parameter	Cisco ISE	Cisco ACS
Full Form	Identity Service Engine	Access Control Server
The Deployment Limits	Large number of concurrent endpoints supported.	Smaller than ISE
Hardware	SNS 3515 , 3595 etc	CSACS-1121
Scalability Number	Supports upto 50 policy service nodes.	Supports up to 22 backup servers.
Directory Domain Support	On a single node, it can support up to 50 Active directory domains.	On a single node, it can support 1 directory domain.
Network Access and Device Administration	Complete support	Complete support
Context Sharing	Complete context sharing	No context sharing
TRUSTSEC Network Segmentation	Complete firewall and access control rules as defined by an asset. It comprehensively manage and push policies and tags. It is quite useful for the propagation of tags with the help of SXP.	Basic firewall and access control rules as defined by an asset. ACS is going to support the tags but the function is not going to be as flexible and powerful as in case of ISE.
Third Party Support	Absolute third party support with the use of SNMP	Basic third party support, however integration is not simple
Scanning and Enforcement	Complete Vulnerability/ Threat/ Posture Scanning as well as enforcement.	No Vulnerability/ Threat/ Posture Scanning or enforcement.
Integration with Cisco DNA	Fully supported	DnaC integration is not feasible on this platform.
Cisco Anyconnect	It is highly integrated with ISE for posture and various other types of services it supports.	ACS only supports Anyconnect VPN and NAM.
Cisco Easy Connect	It can function with the Cisco EasyConnect feature to easily ensure passive authentication or non-dot1x.	ACS does not support Easy Connect feature to ensure passive authentication or non-dot1x.

Q#6.What are the different types of deployments in ISE?

ISE has three different deployment options.

1. Standalone
2. Hybrid deployment
3. Distributed deployment

Q#7.Briefly explain different types of ISE deployment?

Standalone Deployment: A deployment that has a single Cisco ISE node is called a standalone deployment. This node runs the Administration, Policy Service, and Monitoring personas. This deployment is suitable for Small production setup's or labs. If we are deploying ISE in standalone mode then we will not have redundancy.

Hybrid Deployment: A deployment that has multiple ISE nodes wherein PAN and MNT will be on enabled on a single node. This node will run PAN and MNT along with this we ca dedicated PSN's in the deployment.

Distributed Deployment: A deployment that has multiple ISE nodes wherein we have a separate node for each persona. The distributed deployment consists of one Primary Administration ISE node, Secondary admin nodes, Primary Monitoring node, Secondary Monitoring node followed by PSN(Policy Service Node).

Each node can perform one or multiple services. ISE implementation is typically deployed in a distributed manner with individual services run on dedicated ISE nodes.

Q#8.Explain the various types of ISE Distributed deployment?

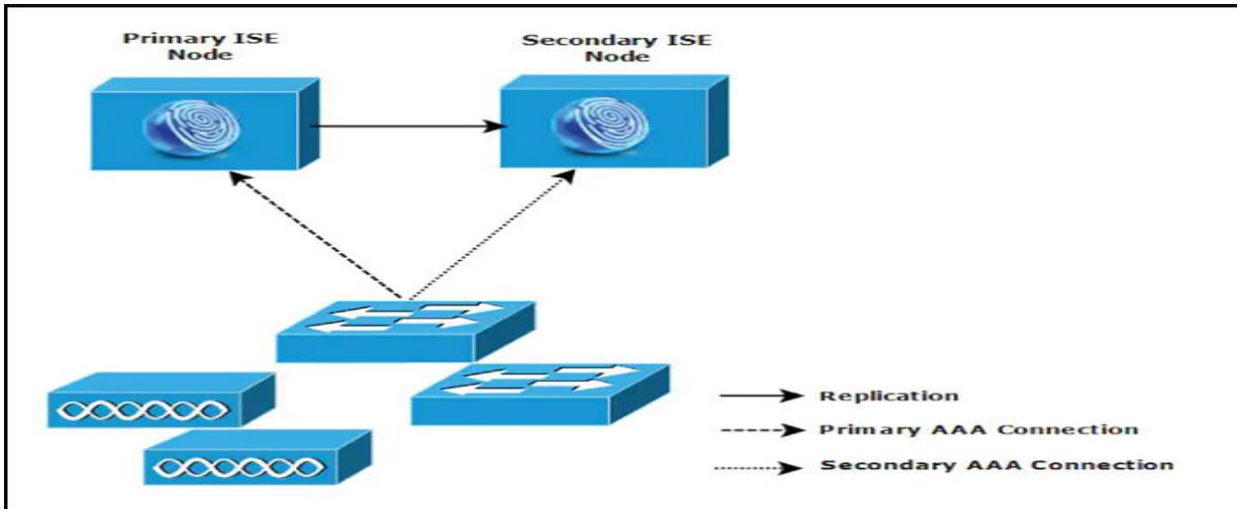
ISE distributed model can be deployed in 3 different ways depending on the scale.

- Small Network Deployments
- Medium Network Deployments
- Large Network Deployments

Small Network Deployments: A typical small ISE deployment consists of two Cisco ISE nodes with each node running all 3 services on it. The primary node provides all the configuration, authentication and policy functions and the secondary node functions as a backup.

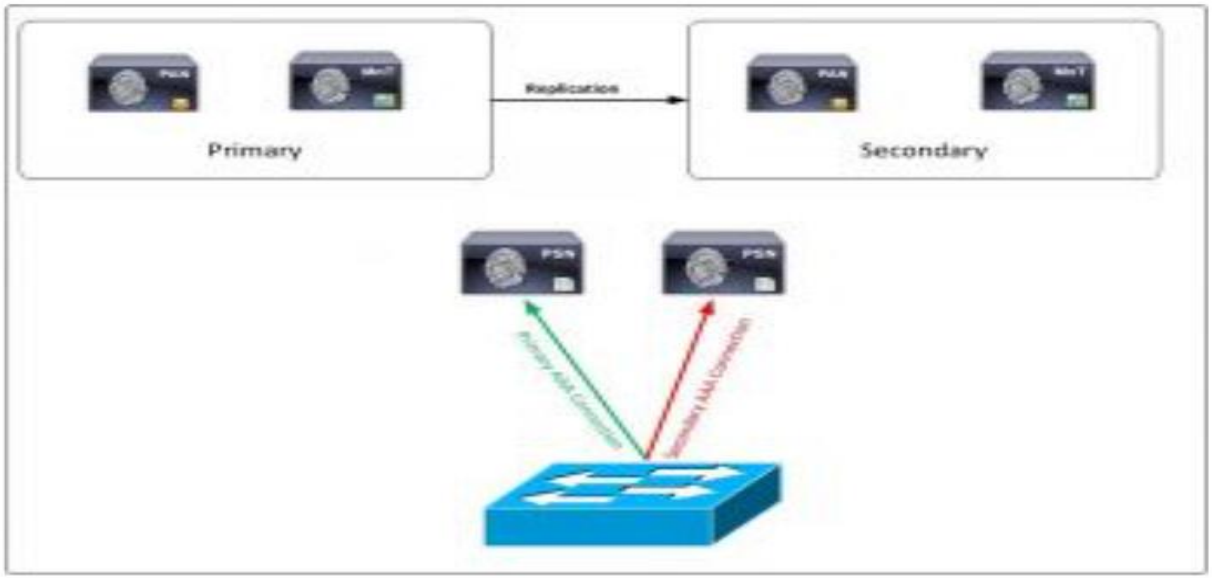
The secondary supports the primary in the event of a loss of connectivity between the network devices and the primary. In case if the primary ISE node goes down we need to manually promote Secondary to Primary.

Press enter or click to view image in full size



Medium Network Deployment: The medium-sized deployment consists of a primary and secondary administration node and a primary and secondary monitoring node, alongside separate policy service nodes. Here in this deployment PAN and SAN will take care of administration and log collection part wherein PSN's will handle authentication for both radius and Tacacs traffic.

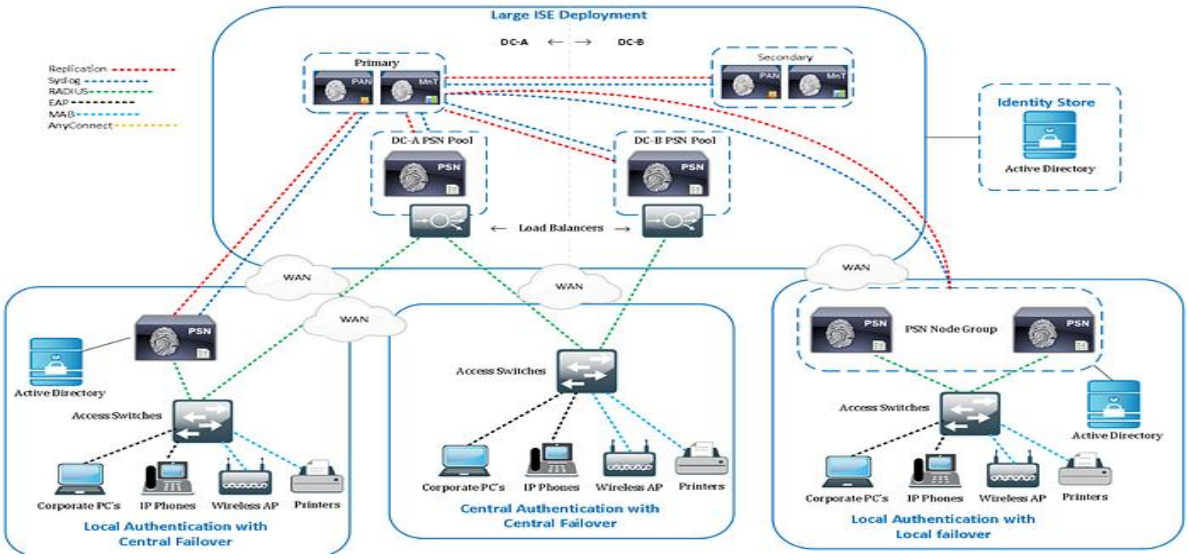
Press enter or click to view image in full size



Large Network Deployment: ISE can distribute large individual ISE personas among several ISE nodes with a large network deployment you dedicate each node to a separate persona. So a separate node (secure network server) for administration, monitoring and policy service. You should also consider using load balancers in front of the PSN nodes.

Having a single load-balancer does introduce a potential single point of failure so it is highly recommended to deploy two load balancers. Since it's a large network deployment we can have multiple logging servers so that logs can be transferred across each server.

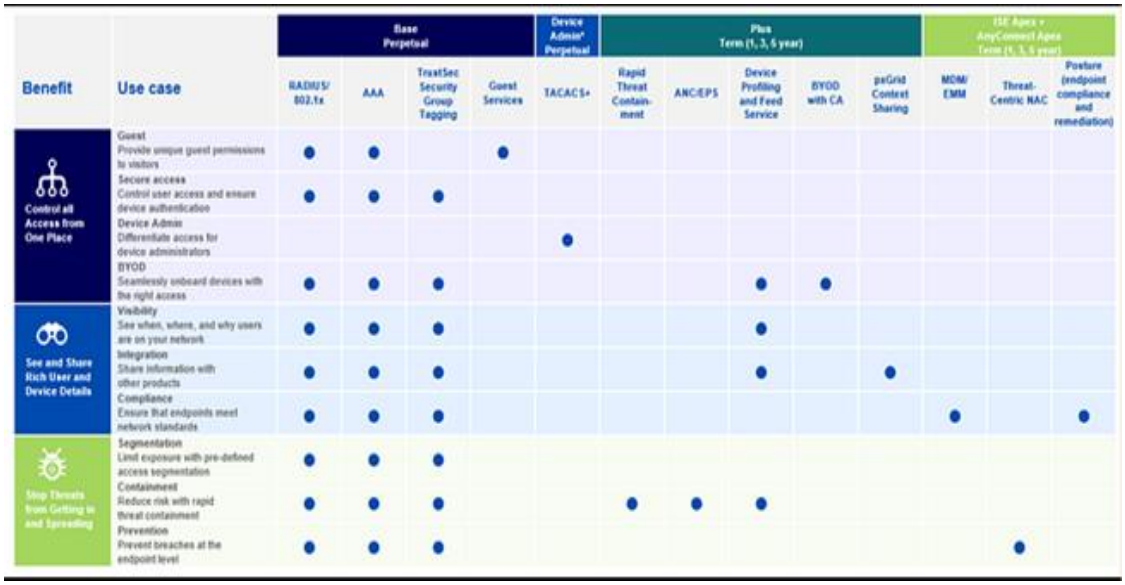
Press enter or click to view image in full size



Q#9.Which are all the different types of Licenses which we can have on ISE?

- ISE Base only
- ISE Base and Plus
- ISE Base and Apex
- Device Administration
- ISE Base, Plus, and Apex

Press enter or click to view image in full size



Q#10.What are the different types of Licenses?

Base License: The base license is a perpetual license. The base license is required for AAA and IEEE 802.1x and also covers guest services and Trustsec. Base licenses are required to use the services enabled by Plus and/or Apex licenses. A base license is consumed for every active device on the network.

Base and Plus: A plus license is required for Profiling and Feed services, Bring Your Own Device (BYOD), Adaptive Network Control (ANC) and PxGrid. A base license is required to install the plus license and the plus license is a subscription for 1,3 or 5 years. When onboarding an endpoint with the BYOD flow, the Plus services are consumed on the active session even when related BYOD attributes are not in use.

Base and Apex: The Apex license is the same as the plus license in that it is a 1,3,5 year subscription, requires the base license but is used for Third-Party Mobile Device Management & Posture Compliance. Does not include Base services; a Base license is required to install the Apex license

Device Administration: There is a device administration license required for TACACS which is a perpetual license, a base license is required to install the device administration license and you only require one license per deployment. A Base or Mobility license is required to install the Device Administration license.

Evaluation: An evaluation license covers 100 nodes and provides full Cisco ISE functionality for 90 days. All Cisco ISE appliances are supplied with an evaluation license. Evaluation licenses will collectively have a base, plus, apex, device administration and so on for 90 days.

Q#11.Does Cisco ISE support Tacacs?

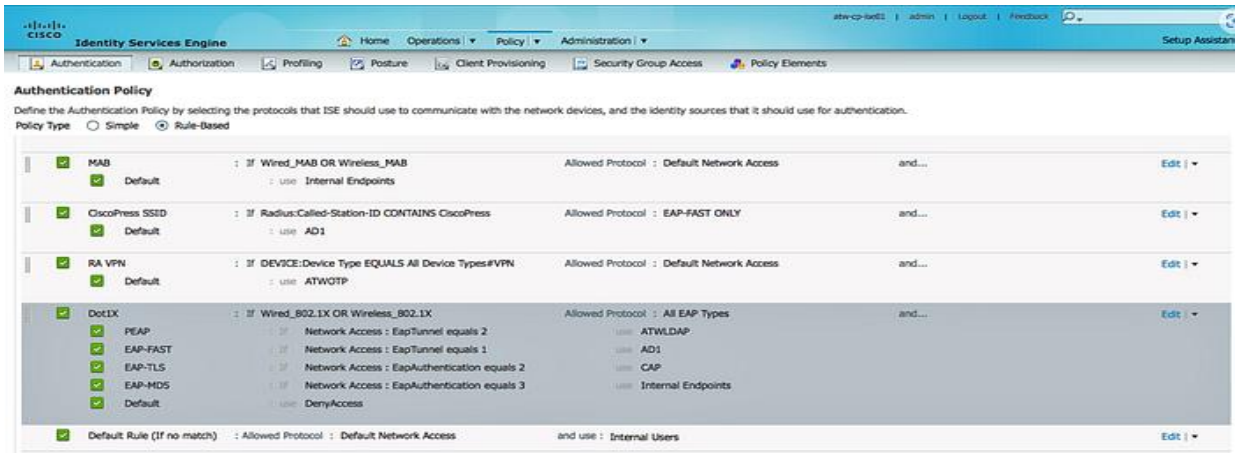
Cisco ISE supports device administration using the TACACS+ security protocol to control and audit the configuration of network devices. The network devices are configured to query ISE for authentication and authorization of device administrator actions and send accounting messages for ISE to log the actions.
Cisco ISE now supports TACACS+. Prior to ISE 2.0 ISE was only supporting Radius but post 2.0 ISE versions TACACS is supported.

Device admin is not enabled by default, to enable it go to:
Administration / Deployment / Node Name / Enable Device Admin Service
This service should be enabled on the PSNs.

Q#12.Which are the different types of protocols which are supported on ISE?

There are different protocols available on ISE which is used for authenticating and authorizing end clients. Below mentioned are the few known and popularly used protocols.
EAP-TLS, PEAP, MS-CHAPv2 v1 and v2, EAP-TTLS, EAP-MS-CHAPv2, LEAP, EAP FAST.

Press enter or click to view image in full size

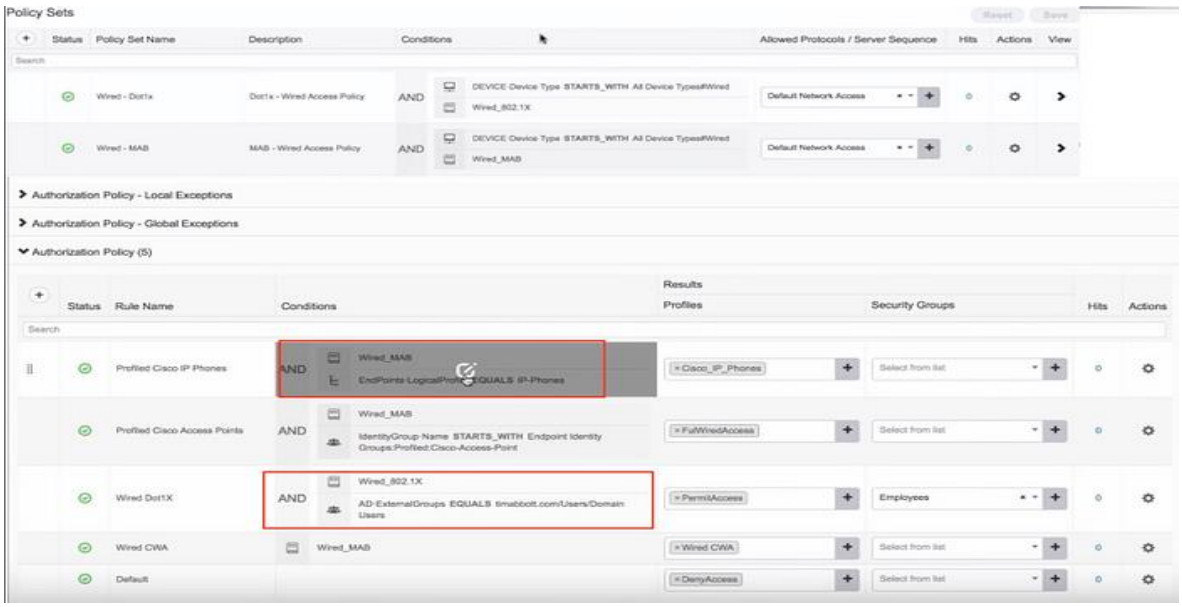


Q#13.What are policy sets on ISE?

Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning.

When you install ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules.

Press enter or click to view image in full size



Q#14.What is the major difference between Authentication and Authorization conditions on ISE?

Authentication: In Authentication, we will check if the user is present in the identity store or not and the credentials which are presented by the user are valid or not. For example, a standard Authentication policy can include the type of traffic i.e. if the user traffic wired or wireless and which is the identity store which needs to be checked upon for this traffic.

Authorization: In Authz we fetch different attributes for the user and determine for which resources the user has access to. An authorization policy can consist of a single condition or a set of conditions that are user-defined. These rules act to create a specific policy. For example, a standard policy can include the rule name using an If-Then convention that links a value entered for identity groups with specific conditions or attributes to produce a specific set of permissions that create a unique authorization profile.

	Authentication	Authorization
Purpose	• Verifies user identity	• Permits access to resources
Requirements	• Identity credentials based on knowledge, possession, and/or inherence • Authentication solution	• Authenticated identity and access control policies • Authorization solution
Responsibilities	• Network security staff determine which factors to adopt • Users provide authentication factors when requesting access	• Leadership sets security strategies • Departments and workgroups define access criteria • Network security staff implement and maintain access control system

Q#15.What is Identity Store on Cisco ISE?

Identity Store is where we check for the credentials against a particular database. Identity store database can be internal or external. Internal identity store will refer to Identity/Endpoint information which is created locally on ISE. External identity store can be AD, LDAP, Radius token server, RSA and Certificate Authority.