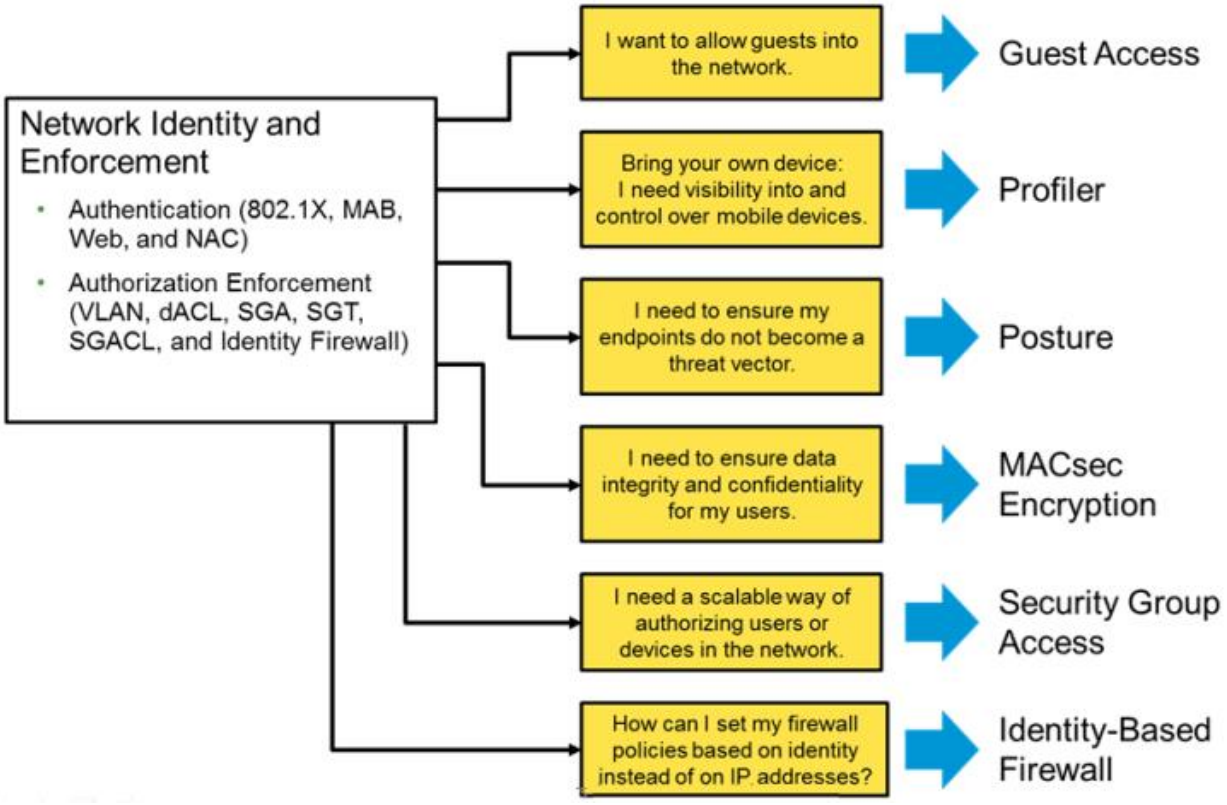
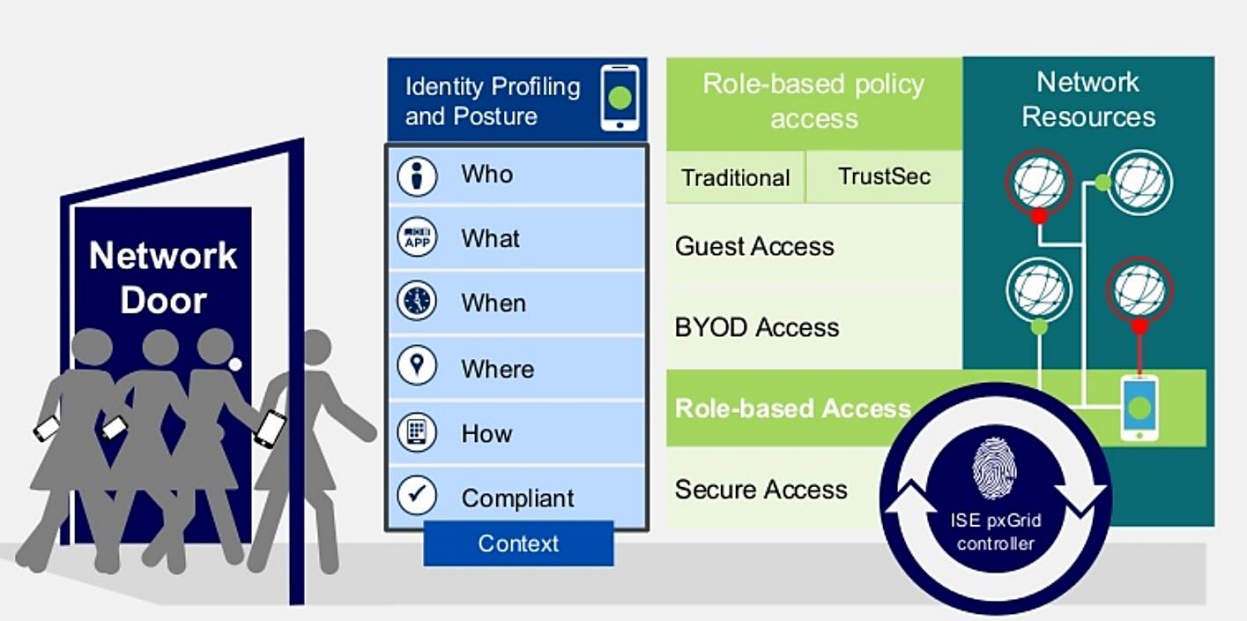
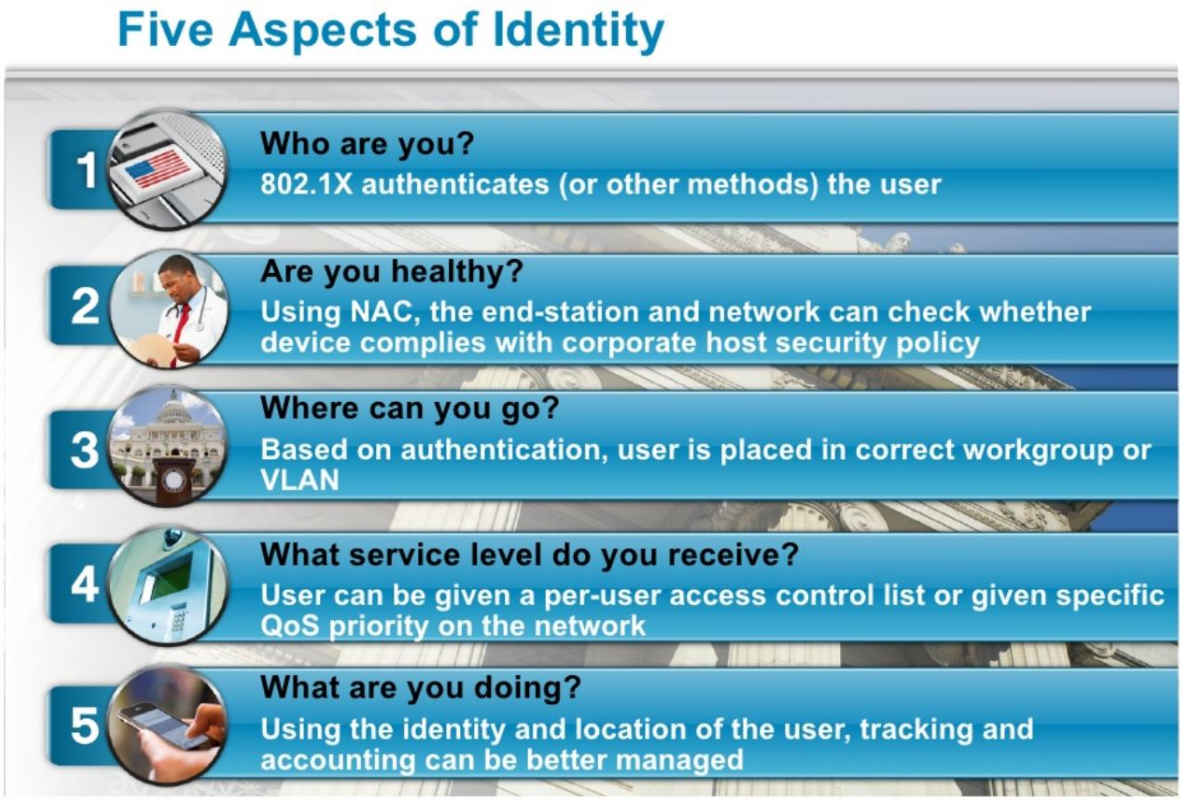
Cisco ISE:

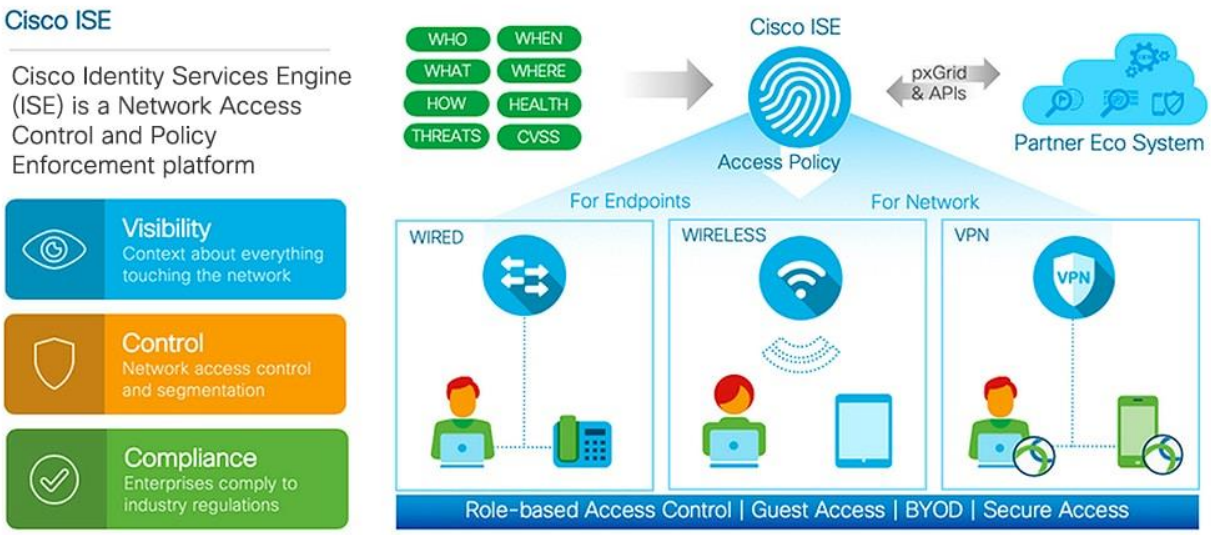
- Cisco ISE is a network term, which is stands for Cisco Identity Services Engine.
- Cisco Identity Services Engine (ISE) is a security policy management platform.
- Cisco Identity Services Engine (ISE) is a NAC & Identity Based Solution from Cisco.
- ISE allow only authorized users can access network based upon policy configured.
- Cisco ISE architecture is mainly divided into two parts one is Identity another Context.
- In Cisco Identity Services Engine Identity provides information about the user or device.
- Context provides additional info about user or device such as what, where, when & how.
- Cisco ISE is used for secure access management like ACS (Access Control Server).
- ISE is Single policy control point for entire enterprise wired & wireless technologies.
- Cisco Identity Services Engine acts as a centralized, network security policy platform.
- Cisco ISE ensure that network administrator implement best network security policy.
- Cisco ISE can be used as a AAA (Authentication, Authorization, and Accounting) server.
- Another advanced function available within Cisco Identity Services Engine is posturing.
- Cisco ISE is mainly use for posturing and policy compliance checking of hosts in network.
- Posturing check health of endpoints like antivirus, latest service pack and OS updates.
- Cisco Identity Services Engine also provide profiling which dynamically identify endpoints.
- Profiling uses network-level communications to determine information about endpoint.
- Profiling service identify, locate, and ensure the access of all endpoints connected.



A good example for identity and context is, User Ali (Who) is logged in to the network in Data Center Room (Where) using Cisco VPN Client AnyConnect (What) today at 10AM. (When) using his Windows Based Laptop (How).





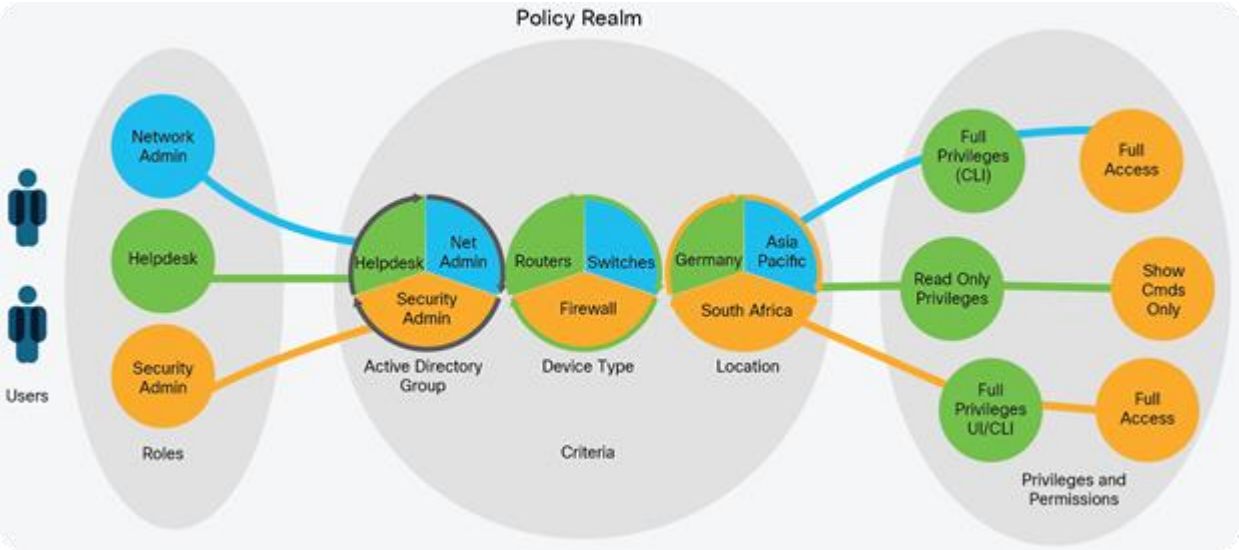


A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (Who), device type (What), access time (When), access location (Where), access type (wired, wireless, or VPN) (How), and network threats and vulnerabilities.

Cisco ISE Features:

Device Administration:

Cisco ISE uses the TACACS+ security protocol to control and audit the configuration of network devices. It facilitates granular control of who can access which network device and change the associated network settings.



Guest and Secure Wireless:

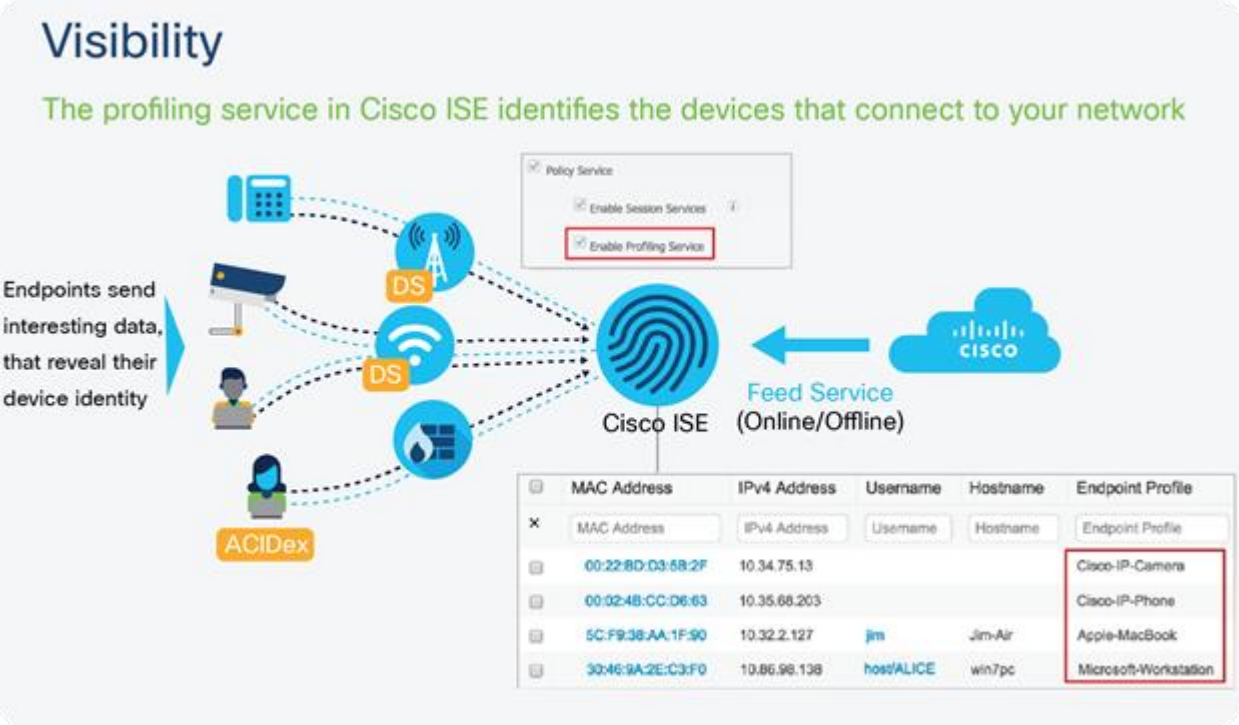
Cisco ISE enables you to provide secure network access to visitors, contractors, consultants, and customers. You can use web-based and mobile portals to on-board guests to your company's network and internal resources.

Bring Your Own Device (BYOD):

Cisco ISE allows employees and guests to securely use their personal devices on your enterprise network. The end users of the BYOD feature can use configured pathways to add their devices and be provisioned predefined authentication and level of network access.

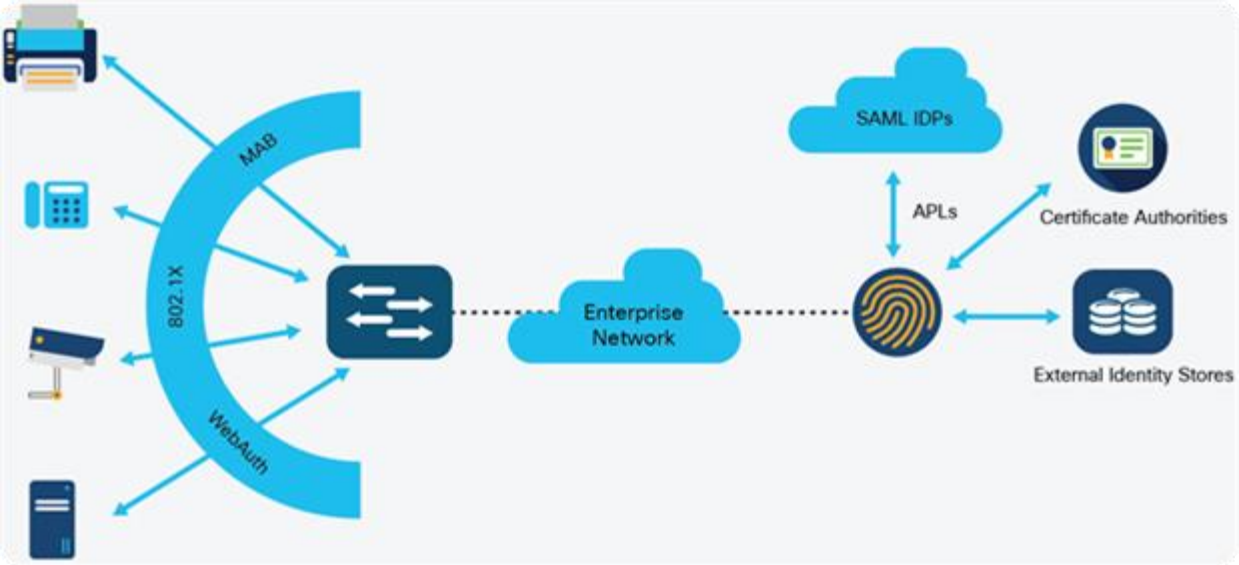
Asset Visibility:

Cisco ISE gives you visibility and control over who and what is on your network consistently, across wireless, wired, and VPN connections.



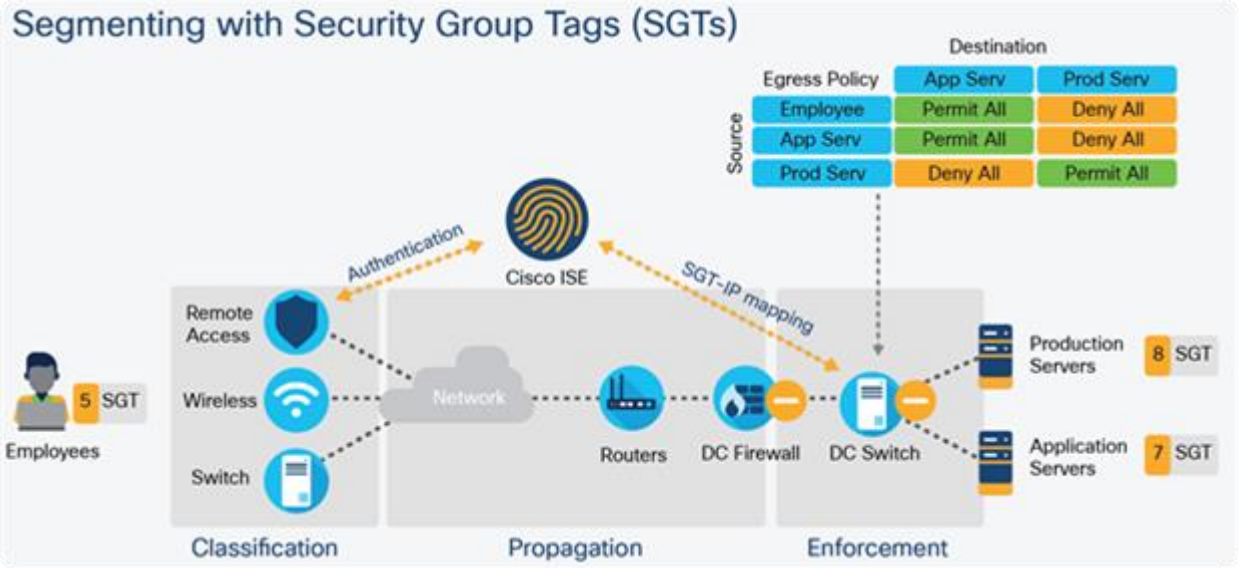
Secure Wired Access:

Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure wired network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods.



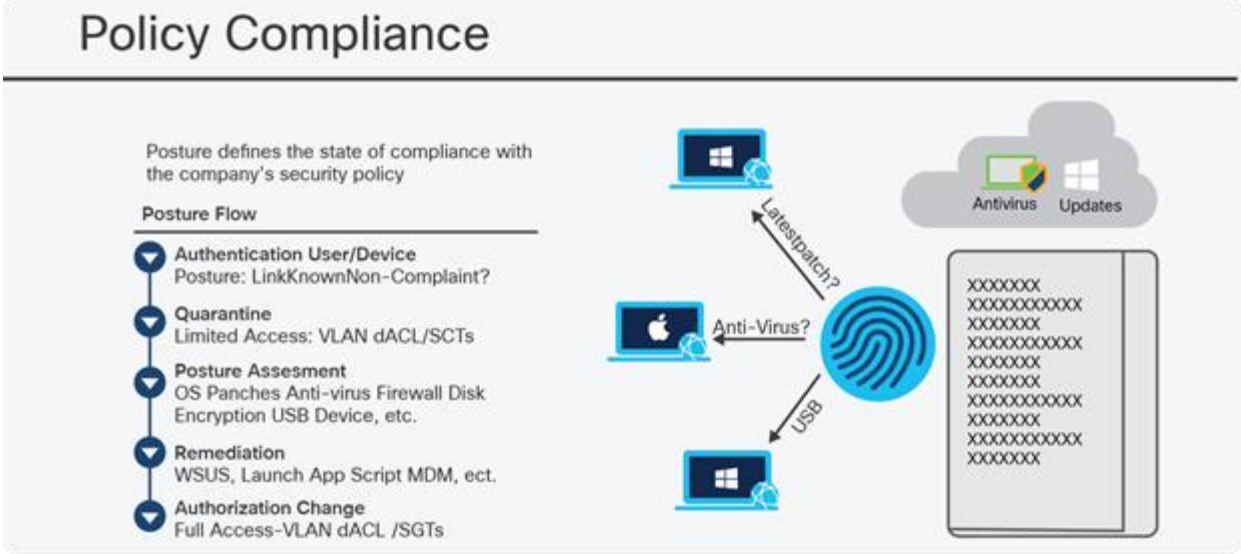
Segmentation:

Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets defining authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation.



Posture or Compliance:

Cisco ISE allows you to check for compliance, also known as posture, of endpoints before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services.



Threat Containment:

If Cisco ISE detects threat or vulnerability attributes from an endpoint, adaptive network control policies are sent to dynamically change its access levels of the endpoint. After the threat or vulnerability is evaluated and addressed, the endpoint is given back its original access policy.

Security Ecosystem Integrations:

The pxGrid feature allows Cisco ISE to securely share context-sensitive information, policy and configuration data, and so on, with connected network devices, third-party vendors, or Cisco partner systems.