3.1 Network Access Control: Network Access Control

- Network access control (NAC) is an umbrella term for managing access to a network.
- NAC authenticates users logging into the network and determines what data they can access and actions they can perform.
- NAC also examines the health of the user's computer or mobile device (the endpoints).

NAC systems deal with three categories of components:
Access requestor (AR): The AR is the node that is attempting to access the network and may be any device that is managed by the NAC system, including workstations, servers, printers, cameras, and other IP-enabled devices. ARs are also referred to as supplicants , or simply, clients.

Policy server: Based on the AR's posture and an enterprise's defined policy, the policy server determines what access should be granted. The policy server often relies on backend systems, including antivirus, patch management, or a user directory, to help determine the host's condition.

Network access server (NAS): The NAS functions as an access control point for users in remote locations connecting to an enterprise's internal network. Also called a media gateway, a remote access server (RAS), or a policy server, an NAS may include its own authentication services or rely on a separate authentication service from the policy server.

Figure is a generic network access diagram.

1. A variety of different ARs seek access to an enterprise network by applying to some type of NAS.

2. The first step is generally to authenticate the AR.

3. Authentication typically involves some sort of secure protocol and the use of cryptographic keys.

4. Authentication may be performed by the NAS, or the NAS may mediate the authentication process.

5. The authentication process serves a number of purposes. It verifies a supplicant's claimed identity, which enables the policy server to determine what access privileges, if any, the AR may have.

6. The authentication exchange may result in the establishment of session keys to enable future secure communication between the supplicant and resources on the enterprise network.

7. Checks should be performed before granting the AR access to the enterprise network. Based on the results of these checks, the organization can determine whether the remote computer should be permitted to use interactive remote access.

8. If the user has acceptable authorization credentials but the remote computer does not pass the health check, the user and remote computer should be denied network access or have limited access to a quarantine network so that authorized personnel can fix the security deficiencies.

Figure indicates that the quarantine portion of the enterprise network consists of the policy server and related AR suitability servers.

9. Once an AR has been authenticated and cleared for a certain level of access to the enterprise network, the NAS can enable the AR to interact with resources in the

enterprise network. The NAS may mediate every exchange to enforce a security policy for this AR, or may use other methods to limit the privileges of the AR.

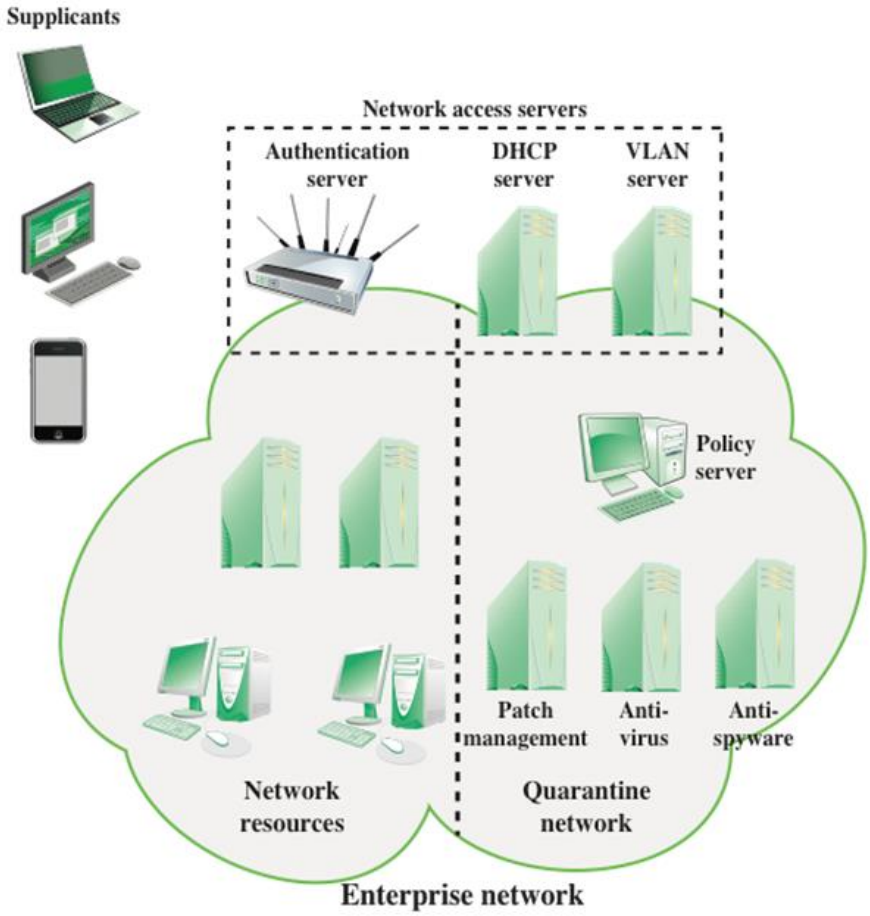

Figure Network Access Control Context