Network Access Control

Network Access Control is a security solution that uses a set of protocols to keep unauthorized users and devices out of a private network or give restricted access to the devices which are compliant with network security policies. It is also known as **Network Admission Control.** It handles network management and security that implements security policy, compliance, and management of access control to a network.

NAC works on wired and wireless networks by identifying different devices that are connected to the network. For setting up an NAC network security solution, administrators will determine the protocols that will decide how devices and users are authorized for the right level of authorization. Access rules are generally based on the criterion such as device used, the location accessed from, the access rights of various individuals, as well as the specific data and resources being accessed.

Components of Network Access Control Scheme:

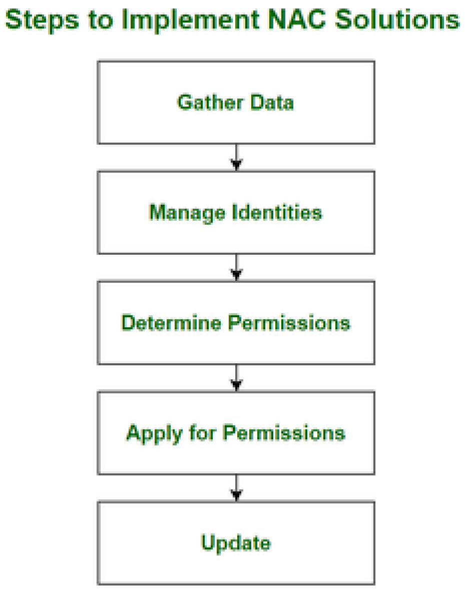
1. **Restricted Access:** It restricts access to the network by user authentication and authorization control. For example, the user can’t access a protected network resource without permission to access it.
2. **Network Boundary Protection:** It monitors and controls the connectivity of networks with external networks. It includes tools such as controlled interfaces, intrusion detection, and anti-virus tools. It is also called perimeter defense. For example, the firewall can be used to prevent unauthorized access to network resources from outside of the network.

Types of Network Access Control:

1. **Pre-admission:** It happens before access to the network is granted on initialization of request by user or device to access the network. It evaluates the access attempt and only allows the access if the user or device is compliant with organization security policies and authorized to access the network.

2. **Post-admission:** It happens within the network when the user or device attempts to access the different parts of the network. It restricts the lateral movement of the device within the network by asking for re-authentication for each request to access a different part of the network.

Steps to Implement NAC Solutions



Implement NAC Solutions

1. **Gather Data:** Perform an exhaustive survey and collect information about every device, user, and server that has to interface with the network resources.
2. **Manage Identities:** Verify user identities within the organization by authentication and authorization.
3. **Determine Permissions:** Create permission policies stating different access levels for identified user groups.
4. **Apply for Permissions:** Apply permission policies on identified user groups and register each user in the NAC system to trace their access level and activity within the network.
5. **Update:** Monitor security operations and make adjustments to permission policies based on changing requirements of the organization with time.

Importance of Network Access Control:

There has been exponential growth in the number of mobile devices accessing private networks of organizations in the past few years. This has led to an increase in security risks for the organization’s resources and therefore, some tools are required that can provide the visibility, access control, and compliance capabilities to strengthen the network security infrastructure.

A NAC system can deny network access to non-compliant devices or give them only restricted access to computing resources, thus preventing insecure nodes from infecting the network. Also, NAC products can handle large enterprise networks that have a large range of different device types connected to the network.

Responsibilities:

1. It allows only compliant, authenticated devices to access network resources and infrastructure.
2. It controls and monitors the activity of connected devices on the network.
3. It restricts the availability of network resources of private organizations to devices that follow their security policy.
4. It regulates the access of network resources to the users.
5. It mitigates network threats by enforcing security policies that block, isolate, and repair non-compliant machines without administrator attention.

Common Use-Cases:

1. Organizations that allow employees to use their own devices or take corporate devices home use NAC to ensure network security.
2. Organizations use NAC to grant access to different network resources to people or devices that are outside of the organization and are subjected to different security controls.
3. NAC protects from threats caused due to use of IoT devices by categorizing IoT devices into groups that have limited permission and constantly monitoring their activities.

Benefits:

1. Users can be required to authenticate via multi-factor authentication, which is much more secure than identifying users based on IP addresses or username and password combinations.
2. It provides additional levels of protection around individual parts of the network.

Limitations:

1. It has low visibility in IoT devices and devices with no specific users associated with it.
2. It does not protect from threats present inside the network.
3. It may not work for organizations if it is not compatible with existing security controls.

Principle Elements of NAC(Network Access Control):

There are mainly three principle elements of NAC which are:

1.Access Requestor(AR).

2.Policy Servers.

3.Network Access Servers(NAS).

Three Principle Elements of NAC(Network Access Control).

Let's look at them one by one now:

1.Access Requestor(AR): We may determine from the name that it is someone attempting to gain access by requesting it. This access can be granted to any entity, such as a device, person, or process.
This entity attempts to get access to network resources. It might be any device handled by the NAC system, such as servers, cameras, printers, and other IP-enabled devices.

ARs are also known as supplicants or clients at times. ARs ensures that no entity has illegal access to protected resources.

To get access, these ARs must follow to the organization's specific guidelines or policies.

2.Policy Server: The policy server analyzes what access should be provided to AR based on the AR's identity, permission level, attempted request, and an organization's established access policy.
The policy server frequently relies on backend services, such as antivirus, patch management, or a user directory, to function.

The policy server helps to determine the host's state. An organization creates different access policies to clearly authorize or reject such access. If the AR follows the organization's policy, the policy server gives access based on the requestor's permission; otherwise, the AR will not be permitted access based on its permission.

It should be noted that there are various commercial systems on the market now that provide such policy servers for both on-premises and cloud computing. Some of the most common examples include the Cisco Identity Services Engine(ISE), Forescout Platform, Aruba ClearPass Policy Manager, and FortiNAC.

These tools offer highly detailed ways to set organizational rules and control the organization's full IP infrastructure.

3.Network Access Server(NAS): Users connecting to an organization's internal network from distant locations utilize the NAS as an access control point. These often serve as VPNs and give users access to the company's internal network. These days, NAS functionality is frequently included in policy server systems.
Remote employees can connect to the company's internal network via NAS, which serves as an access point for them. This allows the company and its employees to create a secure connection and grant authorized access to the network.