Network Access Control (NAC)

Tom Olzak MBA, CISSP
April 2022

Gaining access to a network should be more than forcing user and device authentication via credentials like user IDs, passwords, biometrics, and certificates. Network access control (NAC) extends access management to processes designed to assess the state of devices attempting access to a network. This assessment ensures that each device complies with a set of defined policies. NAC helps ensure that only devices hardened based on associated risk achieve resource access.

Definition

Network Access Control, NAC, is a combination of protocols and safeguards that ensure only policy-compliant devices connect to an organization's network. Assessed devices are allowed to connect to network segments based on user roles, state of the devices, and the resources to which the devices are trying to connect. Some NAC solutions also frequently check to ensure a connected device continues to comply (Awati, 2022).

Many NAC solutions exist, and some organizations might use a collection of solutions to enforce device policy. Because there are various ways to approach NAC, I address policy enforcement at a high level: providing guidance for achieving NAC objectives.

NAC Objectives

NAC usually attempts to address a basic set of objectives.

- Zero-day attacks are a continuous challenge for organizations. NAC can help by enforcing zero-trust access.
- Access control goes beyond authentication of the user. User identity management is paired with device scanning. Device scanning ensures that all devices connecting to sensitive resources meet a required policy baseline.
- Multi-factor authentication and device evaluation support zero-trust networking (Raina, 2021) to firmly control what each connected device can see or access.

How NAC Works

When a device attempts to connect, it is assessed by a NAC service to ensure it meets policies in the network access control database. See Figure 1.

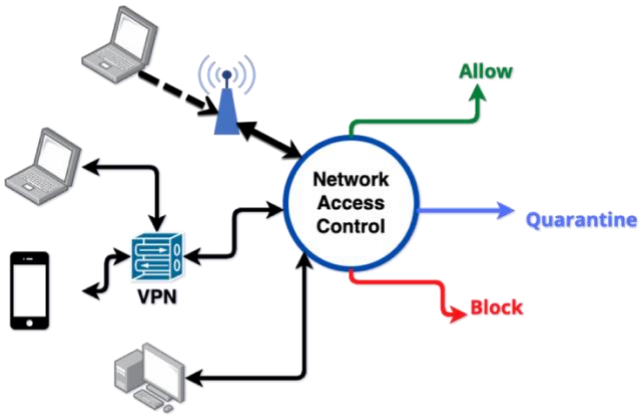

Figure 1: NAC High-level View

In *pre-admission assessments*, an endpoint is assessed to ensure it meets policy compliance *before* it is allowed to connect. If the endpoint fails to comply with one or more policies, it is either denied access or sent to a quarantine network segment.

The quarantine segment might contain servers that allow users to install an approved antimalware application, firewall, or current patches. Figure 2 is an example of a capture portal that may assist a user in bringing her device into policy compliance. In this example, the user is told what antimalware solutions are supported. It also allows the user to click on an install link. Once an endpoint completes remediation steps, it must once again attempt to pass the NAC assessment.

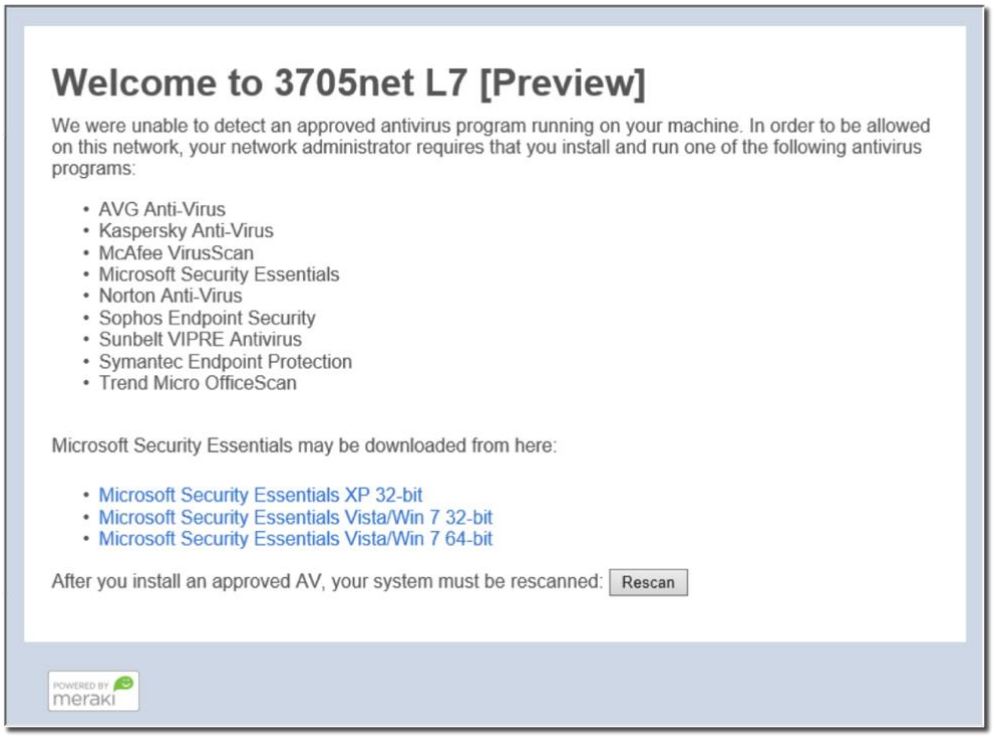

Figure 2: Capture Portal

Endpoint scanning is done in two ways. A NAC software agent is installed on each endpoint in the first approach. This agent continuously collects information that relates to policy enforcement, including

- Patch levels
- Installed applications
- Approved firewall presence and operation
- Authorized antimalware presence and operation

Agents make it easy to check device status periodically, especially when attempting to access classified data and highly categorized resources. This policy compliance review for already connected endpoints is known as *post-admission analysis*.

A second way to scan endpoints is via a browser application. Browser applications do not require the installation and management of agents.

Placement of NAC Appliances

NAC appliances can be either placed inline or out-of-band. Out-of-band devices separate analysis and enforcement across multiple appliances managed by a centralized console. This approach allows an organization to use already installed network devices, like switches and firewalls, to enforce policies.

Inline devices force all traffic to flow through them instead of augmenting existing infrastructure. They usually sit above the access switch level, as shown in Figure 3.

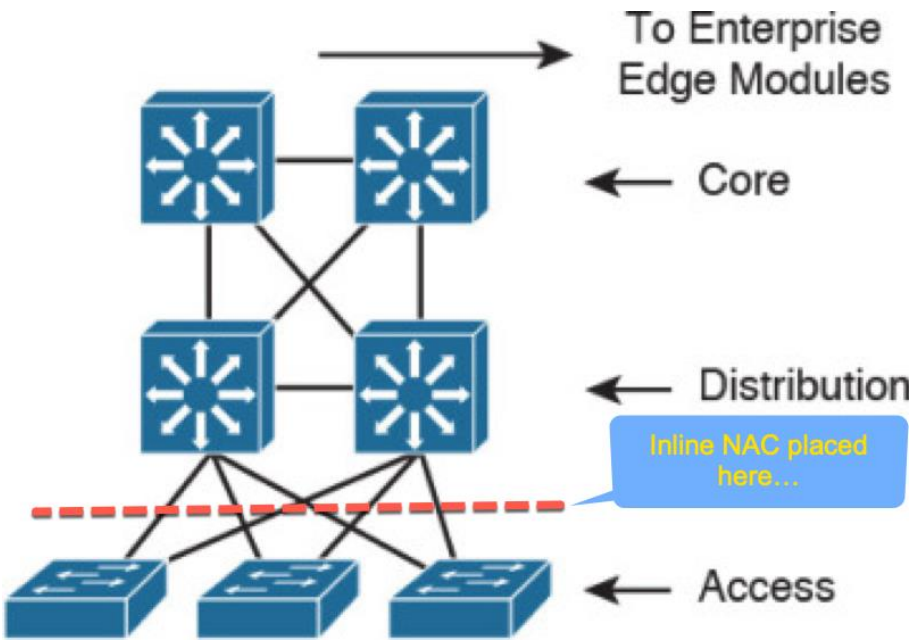

Figure 3: Cisco Hierarchical Switch Design (Cisco Press, 2016)

According to the CISSP CBK, some contend that out-of-band approaches can be disruptive. On the other hand, inline devices must be matched to anticipated business bandwidth, or they can slow business operation,

Final Thoughts

Controlling access to networks requires more than just point-in-time user authentication. It must also include pre-admission confirmation of a safe state for devices used, and it should also include periodic rechecks of connected devices.

Providing quarantine services for non-compliant devices is a helpful approach to ensuring minimal loss of productivity when ensuring only policy-compliant devices can connect to sensitive resources.

It is important for organizations to stop believing that simple user authentication is enough to ensure safe remote and local user and device access.

Works Cited

Awati, R. (2022). *network access control*. Retrieved April 2021, from TechTarget: https://www.techtarget.com/searchnetworking/definition/network-access-control

Cisco Press. (2016, Sep). *Network Design Models*. Retrieved April 2022, from Cisco Press: https://www.ciscopress.com/articles/article.asp?p=2698000

Raina, K. (2021, May). *ZERO TRUST SECURITY EXPLAINED: PRINCIPLES OF THE ZERO TRUST MODEL*. Retrieved April 2022, from Crowdstrike: https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/#:~:text=Zero%20Trust%20is%20a%20security,access%20to%20applications%20and%20data.