Understanding Network Access Control

Introduction

Network Access Control (NAC) solutions deliver a comprehensive approach to identifying, controlling, and securing access to critical network communications and business services.

Well architected NAC solutions proactively manage whether a trusted user, a guest, or a device can connect to a network and what they are authorized to do once connected; this is all based on policy criteria such as device and user identity, business role, time of day, location, and health of the end system.

Comprehensive NAC solutions use both agent-based and agentless assessment technologies, along with proactive and reactive policy enforcement to provide a solid pre-connect and post-connect end system security offering.

A well architected NAC solution will leverage a number of important functions including end system detection, authentication, assessment, authorization, and remediation.

This more easily enables IT organizations to quickly deploy NAC, and more importantly, to enable phased deployment to best align with business needs.

Understanding NAC

NAC is an acronym which stands for Network Access Control. Sometimes it is also referred to as Network Admission Control.

NAC is a common term within IT organizations today, but there is much discussion around what NAC involves and what it does not. Some view NAC as simple registration and authorization of network connected end systems.

Some view NAC as a solution to protect the network environment from viruses and worms.

Some view NAC as a gatekeeper function to control how end systems and guest systems, which are not compliant with corporate computing guidelines, can access the network.

A well architected NAC solution is actually all of these things. Network Access Control is the integration of several technologies to provide a solution that proactively and reactively controls end system communication on the network.

There are a number of individual functions that make up a comprehensive NAC solution.

* **Detect** - Detection and identification of new devices connecting to the network
* **Authenticate** - Authentication of users and/or devices
* **Assess** - Assessment of end systems regarding their compliance and/or vulnerabilities
* **Authorize** - Authorization to use the network based on the results of the authentication and the assessment
* **Monitor** - Monitoring users and devices once they are connected to the network
* **Contain** - Quarantine problem end systems and/or users to prevent them from negatively impacting the overall network environment
* **Remediate** - Remediation of problems with the end system and/or user