WIKIPEDIA

Network Access Control

Network Access Control (**NAC**) is an approach to computer security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement.[1][2]

Contents

Description

Network Access Control (NAC) is a computer networking solution that uses a set of protocols to define and implement a policy that describes how to secure access to network nodes by devices when they initially attempt to access the network. NAC might integrate the automatic remediation process (fixing non-compliant nodes before allowing access) into the network systems, allowing the network infrastructure such as routers, switches and firewalls to work together with back office servers and end user computing equipment to ensure the information system is operating securely before interoperability is allowed. A basic form of NAC is the 802.1X standard.

Network Access Control aims to do exactly what the name implies—control access to a network with policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do.

Example

When a computer connects to a computer network, it is not permitted to access anything unless it complies with a business defined policy; including anti-virus protection level, system update level and configuration. While the computer is being checked by a pre-installed software agent, it can only access resources that can remediate (resolve or update) any issues. Once the policy is met, the computer is able to access network resources and the Internet, within the policies defined by the NAC system. NAC is mainly used for endpoint health checks, but it is often tied to Role-based Access. Access to the network will be given according to the profile of the person and the results of a posture/health check. For example, in an enterprise the HR department could access only HR department files if both the role and the endpoint meets anti-virus minimums.

Goals of NAC

Because NAC represents an emerging category of security products its definition is both evolving and controversial. The overarching goals of the concept can be distilled as:

- Mitigation of zero-day attacks
- Authorization, Authentication and Accounting of network connections.
- Encryption of traffic to the wireless and wired network using protocols for 802.1X such as EAP-TLS, EAP-PEAP or EAP-MSCHAP.
- Role-based controls of user, device, application or security posture post authentication.
- Automation with other tools to define network role based on other information such as known vulnerabilities, jailbreak status etc.
    - The main benefit of NAC solutions is to prevent end-stations that lack antivirus, patches, or host intrusion prevention software from accessing the network and placing other computers at risk of cross-contamination of computer worms.
- Policy enforcement
    - NAC solutions allow network operators to define policies, such as the types of computers or roles of users allowed to access areas of the network, and enforce them in switches, routers, and network middleboxes.
- Identity and access management
    - Where conventional IP networks enforce access policies in terms of IP addresses, NAC environments attempt to do so based on authenticated user identities, at least for user end-stations such as laptops and desktop computers.

Concepts

Pre-admission and post-admission

There are two prevailing designs in NAC, based on whether policies are enforced before or after end-stations gain access to the network. In the former case, called **pre-admission** NAC, end-stations are inspected prior to being allowed on the network. A typical use case of pre-admission NAC would be to prevent clients with out-of-date antivirus signatures from talking to sensitive servers. Alternatively, **post-admission** NAC makes enforcement decisions based on user actions, after those users have been provided with access to the network

Agent versus agentless

The fundamental idea behind NAC is to allow the network to make access control decisions based on intelligence about end-systems, so the manner in which the network is informed about end-systems is a key design decision. A key difference among NAC systems is whether they require agent software to report end-system characteristics, or whether they use scanning and network inventory techniques to discern those characteristics remotely.

As NAC has matured, software developers such as Microsoft have adopted the approach, providing their network access protection (NAP) agent as part of their Windows 7, Vista and XP releases. There are also NAP compatible agents for Linux and Mac OS X that provide equal intelligence for these operating systems.

Out-of-band versus inline

In some out-of-band systems, agents are distributed on end-stations and report information to a central console, which in turn can control switches to enforce policy. In contrast the inline solutions can be single-box solutions which act as internal firewalls for access-layer networks and enforce the policy. Out-of-band solutions have the advantage of reusing existing infrastructure; inline products can be easier to deploy on new networks, and may provide more advanced network enforcement capabilities, because they are directly in control of individual packets on the wire. However, there are products that are agentless, and have both the inherent advantages of easier, less risky out-of-band deployment, but use techniques to provide inline effectiveness for non-compliant devices, where enforcement is required.

Remediation, quarantine and captive portals

Network operators deploy NAC products with the expectation that some legitimate clients will be denied access to the network (if users never had out-of-date patch levels, NAC would be unnecessary). Because of this, NAC solutions require a mechanism to remediate the end-user problems that deny them access.

Two common strategies for remediation are quarantine networks and captive portals:

Quarantine

A quarantine network is a restricted IP network that provides users with routed access only to certain hosts and applications. Quarantine is often implemented in terms of VLAN assignment; when a NAC product determines that an end-user is out-of-date, their switch port is assigned to a VLAN that is routed only to patch and update servers, not to the rest of the network. Other solutions use Address Management techniques (such as Address Resolution Protocol (ARP) or Neighbor Discovery Protocol (NDP)) for quarantine, avoiding the overhead of managing quarantine VLANs.

Captive portals

A captive portal intercepts HTTP access to web pages, redirecting users to a web application that provides instructions and tools for updating their computer. Until their computer passes automated inspection, no network usage besides the captive portal is allowed. This is similar to the way paid wireless access works at public access points.

External Captive Portals allow organizations to offload wireless controllers and switches from hosting web portals. A single external portal hosted by a NAC appliance for wireless and wired authentication eliminates the need to create multiple portals, and consolidates policy management processes.

Mobile NAC

Using NAC in a mobile deployment, where workers connect over various wireless networks throughout the workday, involves challenges that are not present in a wired LAN environment. When a user is denied access because of a security concern, productive use of the device is lost, which can impact the ability to complete a job or serve a customer. In addition, automated remediation that takes only seconds on a wired connection may take minutes over a slower wireless data connection, bogging down the device.[3] A mobile NAC solution gives system administrators greater control over whether, when and how to remediate the security concern.[4] A lower-grade concern such as out-of-date antivirus signatures may result in a simple warning to the user, while more serious issues may result in quarantining the device.[5] Policies may be set so that automated remediation, such as pushing out and applying security patches and updates, is withheld until the device is connected over a Wi-Fi or faster connection, or after working hours.[3] This allows administrators to most appropriately balance the need for security against the goal of keeping workers productive.[5]

See also

- Network Access Protection
- Network Admission Control
- Trusted Network Connect

References

1. "IEEE 802.1: 802.1X-REV – Revision of 802.1X-2004 – Port Based Network Access Control" (http://www.ieee802.org/1/pages/802.1x-rev.html). *ieee802.org*.
2. Tutorial: Network Access Control (NAC) (http://www.networkcomputing.com/careers-and-certifications/tutorial-network-access-control-%28nac%29/d/d-id/1222951) Mike Fratto, Network Computing, July 17, 2007
3. "Mobile Network Access control: Extending Corporate Security Policies to Mobile Devices" (https://web.archive.org/web/20111005031946/http://www.netmotionwireless.com/uploadedFiles/Resources/white_papers/NAC_WP_2010Q1.pdf) (PDF). Archived from the original on October 5, 2011. Retrieved 2011-05-28.
4. "Network Access Control Module" (http://www.netmotionwireless.com/products/nac_module.aspx) Archived (https://web.archive.org/web/20110903055243/http://www.netmotionwireless.com/products/nac_module.aspx) 2011-09-03 at the Wayback Machine
5. "Field Technologies Online" (https://web.archive.org/web/20120314155937/http://www.fieldtechnologiesonline.com/download.mvc/Mobile-Network-Access-Control-Extending-0001). Archived from the original on March 14, 2012. Retrieved 2011-05-28.

External links

- NAC: What went wrong? (http://www.networkworld.com/reviews/2010/052410-network-access-control-test.html)
- Booz Allen Hamilton leaves 60k unsecured files on DOD server (https://www.cyberscoop.com/booz-allen-hamilion-amazon-s3-chris-vickery/)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Network_Access_Control&oldid=951271542"

This page was last edited on 16 April 2020, at 10:07 (UTC).