Network Access Control Solutions

https://www.securedgenetworks.com/blog/what-is-network-access-control-and-what-should-it-do-for-you
https://en.wikipedia.org/wiki/Network_Access_Control
https://www.esecurityplanet.com/network-security/network-access-control.html
https://www.networkworld.com/article/2211361/ultimate-guide-to-network-access-control-products.html
https://www.esecurityplanet.com/products/top-network-access-control-solutions.html
https://www.itcentralstation.com/categories/network-access-control
https://packetfence.org/about.html
https://community.spiceworks.com/products/50944-packetfence

Various videos on www.youtube.com

What is Network Access Control?

Network access control is a security solution that controls access to your network - it prevents the network to be accessed by a malicious end point. It integrates with your infrastructure to identify, assign, and enforce pre-determined rules or policies to manage the access to your network. It works by limiting the availability of network resources to endpoint protection devices that follow a defined security policy.

Network access control (NAC) is critical for securing a company's digital infrastructure. Majority of the attacks can be prevented by ensuring that only authorized users and devices are able to connect to the network. If a particular user or device is authorized or not is decided by a set of rules or conditions that have to be followed or met.

A Network access server (NAS) carries out functions like authentication and authorization for potential users by confirming logon information. It limits data/resources that can be accessed by particular users and implements anti-threat applications such as antivirus software, firewalls and spyware-detection programs. The NAS checks for system info 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 the set of conditions required to access HR department files.

NAC solutions have the potential to help organizations control access to their networks via the following capabilities:

- **Guest networking access:** Takes care of guests via a customizable, self-service portal that comprises of guest authentication, guest sponsoring, guest registration, and a guest management portal.
- **Security posture check:** Assesses security-policy compliance by device type, user type, and operating system.
- **Incidence response:** This involves mitigating network-based threats by employing security policies capable of blocking, isolating, and repairing non compliant machines without administrator attention.
- **Bidirectional integration:** With NAC, it is possible to incorporate with other security and network solutions via the open/RESTful API.
- **Policy life-cycle management:** Enforces policies for all operating scenarios without the need for separate products or additional modules.
- **Profiling and visibility:** Recognizes and profiles users and their devices before any damage can be caused by malicious code.

Basic functions of a NAC are:

- Mitigation of non-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.

Usual steps for NAC configuration:

1. Install the NAC server and configure all wireless access points and switches to use the NAC server for authentication.

2. Define basic profiling and authentication rules on the NAC server. This determines which resources certain users and devices have access to.
3. Define inspection and compliance policies. These dictate the security posture checks.
4. Test and fine-tune your rules and policies.
5. Define alerts and reports, such that failed authentications are logged and sent to your security team for analysis. Weekly reports are useful to see trending data.
6. Go live. After you are confident that your rules, policies, and alerts are all functioning as intended, roll out the NAC solution for a subset of your users (i.e., for a certain department or branch office location). This “canary” group will validate your newly deployed NAC solution before broader rollout.

Parts of the NAC are:

- **The NAC server**: this is the link between your user database and your enforcement points and ties it all together with security policies.
- **The enforcement points**: your network devices, such as routers, switches, firewalls, SSL VPN gateways, and wireless access points. These devices ultimately allow or don’t allow a user to access your network.
- **The user database**: this contains a list of all your authorized users and the various groups they belong to (often times grouped by company departments). This can be your Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) server. This could also be a cloud/SaaS based single-sign on (SSO) solution, such as Okta or Ping, which is responsible for identity management (IdM) for your environment.

List of various Network Access Control Solutions:

1. Impulse SafeConnect
2. Extreme Networks ExtremeControl
3. Auconet BICS
4. ForeScout CounterACT
5. Pulse Policy Secure
6. HPE Aruba ClearPass
7. Bradford Networks' Network Sentry
8. Cisco Identity Services Engine
9. InfoExpress CyberGatekeeper

We will consider the following three products:
1. Cisco ISE (Identity Services Engine)
2. ForeScout CounterACT
3. Aruba ClearPass

1. CISCO ISE

The Cisco Identity Services Engine (ISE) is a next-generation identity and access control policy platform that provides a single policy plane across the entire organization combining multiple services, including authentication, authorization, and accounting (AAA) using 802.1x, MAB, web authentication, posture, profiling, device onboarding, guest services, and VPN access into a single context-aware identity-based platform.

Synergy Research group says that Cisco is one of the most popular IT infrastructure providers on the market, boasting products that include data center servers, switches and routers, hosted and cloud collaboration, network security, and WLAN. Cisco claims that ISE has saved over $1.6 million over the course of 3 years, 200 hours worth of time less spent for mitigating security events and 98% less time taken to implement network changes.

The key benefits are:

1. Complete endpoint visibility
2. BYOD service
3. Combined Authentication,authorization,accounting(AAA),posture,and profiler functions
4. Easy Scalability
5. Consistent Policy

Users have rated CISCO ISE as one of the most stable NAC solutions.
One of the drawbacks that users have pointed out that there must be easier documentation and that good technical skills are needed to implement the solution.

CISCO has extensive list of guides to integrate the engine with various services from various vendors like Checkpoint, Airwatch, HP, IBM, Microsoft, Palo Alto, Google, etc.
One big disadvantage of the CISCO ISE is that it has shown problems working with non-CISCO hardware.

2. ForeScout Counter ACT

Forescout is one of the leaders in device visibility and control. ForeScout CounterACT provides real-time visibility, control and orchestration across network infrastructures. This includes visibility and control across campus, data center and cloud in regards to every device, operating system and version, MAC address & IP address, whether it's been on the network for a few minutes or all day. It discovers IP-based devices as they connect to a network, classifies them based on characteristics, assesses their security posture based on policy and behaviors, and then takes action as defined by the rules and policies configured in the NAC system. With automated policy-based access control and enforcement of devices, users and applications. The technology integrates with all major network infrastructures and is able to scale with its

customers' needs. ForeScout boasts with having one of the best available endpoint visibility solutions.

ForeScout has been rated to do NAC with 802.1X when many other solutions don't support that.. A big advantage is that it is very easy to configure according to user reviews. Visibility is a benefit that has been rated very high by many users.

ForeScout provides the CounterACT Open Integration module for integration processes. With this module customers, systems integrators and third-party product vendors can integrate applications or third-party products with CounterACT.

3. **Aruba ClearPass**

Identifying who and what connects to the network is the first step to securing your enterprise. Control through the automated application of wired and wireless policy enforcement ensures that only authorized and authenticated users and devices are allowed to connect to your network.

ClearPass allows you to safely connect business and personal devices to your network in compliance with your security policies. It allows you to grant full or limited access to devices based on users' roles, device type, and cybersecurity posture.
This solution leverages a three-step plan:

1. Identify
2. Enforce
3. Protect

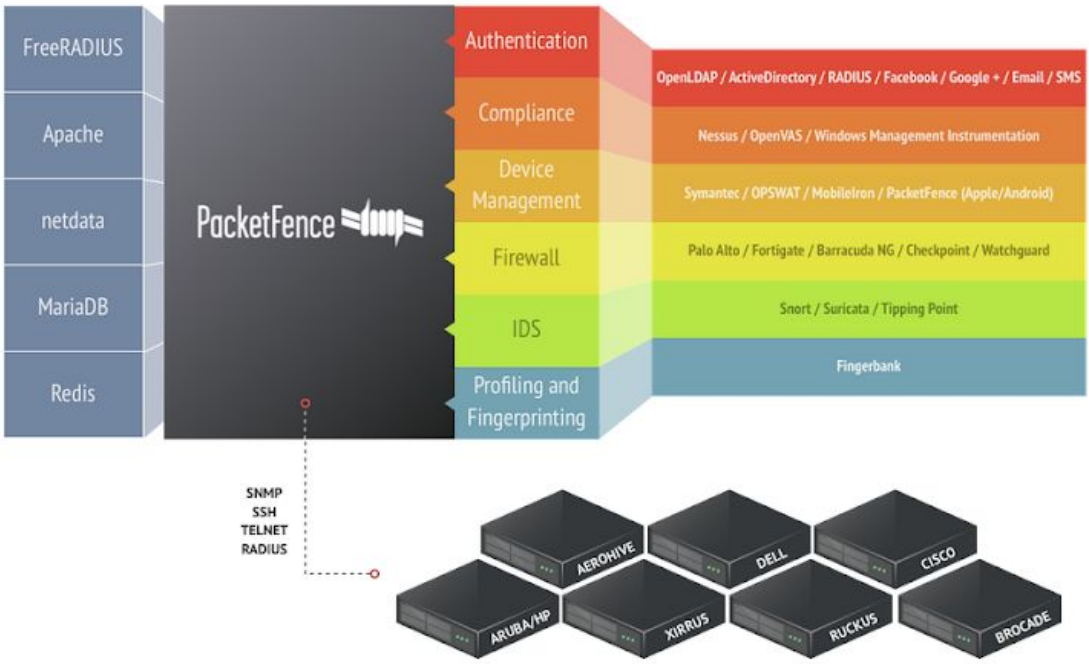
It also boasts of Complete visibility, Proactive response and Closed-loop response. It also integrates with over 25 IT partners – the vast majority of your current technology and security stacks - to ensure that every element of your system is working without issue.

These third-party technology systems could include:

- Enterprise mobility management (EMM)
- Firewalls
- Mobile device management (MDM)
- Security information and event management (SIEM)

PacketFence:

PacketFence is a fully supported, trusted, Free and Open Source network access control (NAC) solution. It can be used to secure a small to a very large network. This is a free and a open source solution to Network access control. Boasting an impressive feature set including a captive-portal for registration and remediation, centralized wired and wireless management, powerful BYOD management options, 802.1X support, layer-2 isolation of problematic devices; PacketFence can be used to effectively secure networks small to very large heterogeneous networks. PacketFense has a dense list of features, some of them are same as other vendors provide, while some others are unique to PacketFence. For eg, PacketFence has a Guest VLAN role out of the box.
I found a diagram on www.packetfence.org shown below:



The diagram gives us a lot of information on how PacketFence integrates with other products for various services. For example it can integrate with or supports Firewalls from Palo Alto, Fortigate, barracuda NG, Checkpoint and Watchguard. Similarly, it can use OpenLDAP or AD or RADIUS or something else for Authentication.

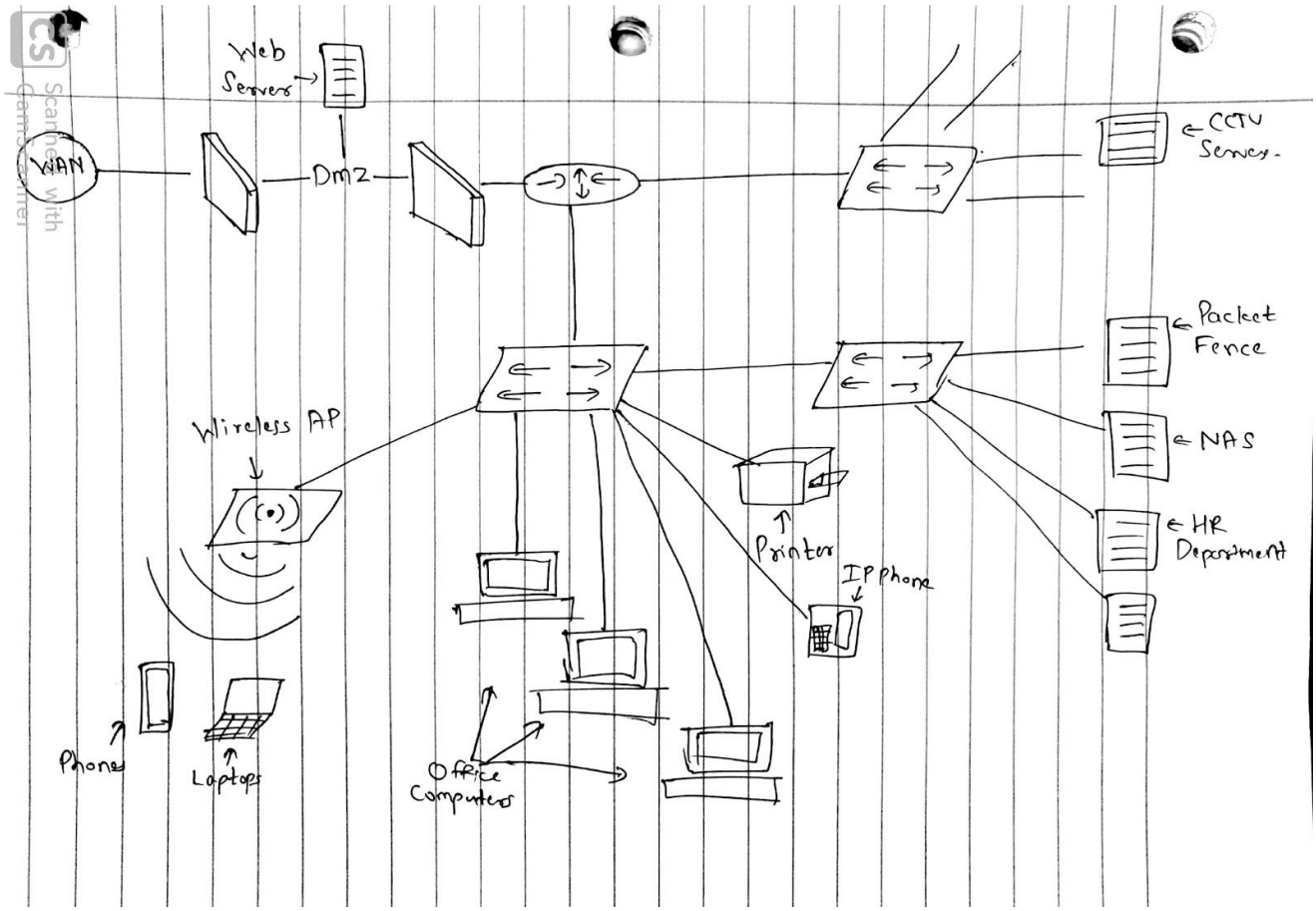
Features:

- BYOD - Let people bring their own devices
- Role-based access control
- Eliminate malware

- WiFi offload / hotspot
- Provide guest access
- Perform compliance checks and proactive scans on devices
- Simplify network management
- Captive Portal
- 802.1x integration
- Isolation of problematic devices
- Wireless integration
- Useragent fingerprinting

User reviews say that some of the configuration of PacketFence in overtly complicated, but overall it does a great job, especially considering that it's free. PacketFence provides the ZEN VM which comes with all the functionality out of the box. Once you launch the machine, you have to go to it's IP address and port 1441 to access the PacketFence control panel which is used to set all the functionality for the systems.

A very big advantage of PacketFence is that it is open source, free and supports majority of the hardware. Also, since it is open source, enabling integration is not a big task with PacketFence.



For the above diagram:

VLAN 1 - Management - for PacketFence
VLAN 2 - Registration - Devices pending registration will be placed here
VLAN 3 - Isolation - Access denied devices will be placed here and shown steps to remedy that
VLAN 4 - Quarantine - Quarantined devices will be placed here
VLAN 5 - Guest Internet - Guests will be placed here
VLAN 6 - Unprivileged Access - Minimum access VLAN
VLAN 7 - HR Department - HR employees will be placed here
VLAN 8 - Phone Voice - VLAN for IP Phones