Nellsoft GmbH, Sihleggstrasse 23, 8832 Wollerau – Switzerland
Tel. +41 44 500 16 50, Fax. +41 44 500 16 51
info@nellsoft.com, http://www.nellsoft.com

Checklist for a great NAC deployment

Author: Lionel Gresse
Date: 20th May 2019

I've been privileged to install and operate network access control systems (NAC) for more than 7 years. I had the chance to experiment most of the type of deployment. Writing this document, my goal is to share my experience with you. I want you to benefit from these long hours of work and from the right choices but also the mistakes that I and many others made.

I've listed 33 points to consider when planning for a NAC deployment. Today they are all part of my own methodology. Like any pilot before take-off, I go through all of them to ensure a safe and successful NAC deployment.

Nellsoft GmbH, Sihleggstrasse 23, 8832 Wollerau – Switzerland
Tel. +41 44 500 16 50, Fax. +41 44 500 16 51
info@nellsoft.com, http://www.nellsoft.com

Table of content

1. Do you want to authenticate end-points?

Authenticating endpoints imply a reference and a policy for authenticated and non-authenticated. What will you do with non-authenticated users? Do you remove them from the network? Do you move them to a safe area where the helpdesk can support them?
Gracefully handling exception is essential to avoid a backlash from users. A common mistake made is to forget exception handling and only focus on intrusion. Over the lifetime of a NAC, no intrusion will probably ever occur, only exceptions.
More concretely, have you thought about the reaction of your CEO when he'd be blocked? Imagine this scenario: he was 2 weeks on holiday, and his PCs can't handle authentication anymore. He has an important meeting in 30 minutes, and he needs his PC right now. This story is a common scenario that I see time and again with poorly setup NACs.

2. Is complete visibility on all endpoints important?

Achieving complete visibility on the network requires a tool that not only detects classical office devices but also deals with all the rest of your IT infrastructure.
Complete visibility requires an extensive database of MAC addresses as a start. It also mandates passive and active fingerprinting and an array of protocol detection and analysis such as HTTP or SNMP. The latest trend in network visibility with NAC is the support of Operation Technology: cameras, physical access control, air conditioning systems, building management systems, manufacturing systems, electrical systems, you name it. Some vendors even support non-IP networks.
Finally, the classification helps you making sense of all your inventory. A useful NAC comes with a user interface giving a clear vision of the inventory, and its categories and subcategories.

3. Is compliance verification a part of your goals?

A NAC can address the compliance verification of endpoints. High-end NACs can thoroughly analyze an end-point to authenticate it. The side effect is that compliance verification has all the information it needs. Vendors have thus developed additional reporting to solve this use case.
Regular compliance checks done with NACs are about the security posture of an endpoint
. What I mostly see as compliance verification policy are the following:

- Are there any vulnerabilities present?
- Is the anti-virus up and running and up-to-date?
- Is the correct anti-virus installed?
- Is the IDS agent up and running and up-to-date?
- Are non-Microsoft applications up-to-date?

Many other products provide compliance verification. Vulnerability management solutions, patch management solutions, among others, can do it, at least to some degrees. The advantage of doing it with a NAC is that it can automatically manage the situation, just like an

authentication process. Same process, same routine. It can also go one step beyond and trigger active measures. The most obvious one for a NAC is to restrict the network connectivity of the end-point: port ACLs, port blocking, or change of VLAN. Even better, some NACs can combine it with a software update or an anti-virus update.

4. Is micro-segmentation an issue to address?

Micro-segmentation describes the control of network communications with a finer granularity than traditional firewalls placed between local networks. When an intruder gains access to a computer remotely, the next thing he tries is to access another computer on the same network segment. It is usually straightforward as there is no filtering inside the network segment. Micro-segmentation is a fancy word to mean lateral movement protection.
Some NACs can limit network communications between network assets using virtual firewalls. Virtual firewalls work by reinjecting reset packets into the communication to block it. They don't require to sit between VLANs or are not a potential point of failure. Compared to the redesign of the network layer 2 and layer 3, implementing micro-segmentation with a NAC is effortless. The risk of deployment is limited, and the cost compared to other technologies is very low. In my experience, it is usually 2 to 3 times cheaper just for equipment.

5. Do you want to cover office network or operational technologies as well?

Office networks are the traditional playground of NACs. They typically host PCs, printers, and phones. Sometimes, other types of devices, such as tablets and smartphones, may occur. However, they are much simpler and less diverse than industrial networks, often mentioned by operational technologies.
Operational technologies (OT) designate in fact what is not office related IT. So what's in there? If you're a hospital, it designates all health-related and networked devices: imagery devices, analysis products, patient monitoring devices, life support devices.
If you work for a car parking management organization, you have cameras, emergency phones, payment systems, physical access control devices, and air conditioning.
If you work for an airport, you deal with cameras, door access control, plane ticket readers, emergency phones, and air conditioning.
A NAC placed in an OT network provides visibility and inventory management in an area that is very difficult to control. The IT department most probably does not manage them. External suppliers, reporting directly to other departments, typically manage them under a non-technical agreement such as to provide video surveillance or air filtering in the facilities. In this kind of agreement, the supplier has complete freedom to chose its equipment as long as it fulfills the SLA. However, the IT department is in charge of the network and is responsible in case of a security issue. That's where the inventory management capability of a NAC helps.

6. Integrate your NAC with other security technologies

Many NACs can integrate with other technologies such as vulnerability management solutions, SIEM, IOC, IDS, among others. Data exchange is two ways, and both sides will benefits.
A NAC can enrich its vision of connected end-points thanks to other systems, and a new set of policies becomes possible. For instance, an indication of compromise can be reused in a control policy to move a device to a quarantine network.
On the other hand, the NAC provides information about the physical location of an IP address and the user of that computer. For instance, it can supply information into a SIEM that enrich other logs with it. The SIEM can then provide not only the IP of a compromised PC but also its precise physical location on the network. Service Desks save time and tackle security issues faster.

7. Fail-open or fail-close solution?

I hear quite often NAC requirements, such as "we want to block immediately anything that is not a corporate device.". Great goal, unfortunately, what will you do when the NAC fails? The NAC may be down for maintenance, for an unexpected issue or just unreachable due to a network issue.
In such a case, all connected devices could appear rogue. You need to a serious look at what you want to happen in such a case. Most organizations do want to continue their operation even if the NAC is not functioning. It probably already the case if you don't have a NAC. So for most organizations, a fail-open solution is an absolute requirement.
However, I've already implemented solutions that were fail-close. So this question must be thought out in the design phase to avoid a bad surprise down the road.

8. Should the NAC cover user networks only or also servers' networks?

Both user and server networks can benefit from a NAC. However, the use cases are entirely different.

In user networks, NACs typically solve endpoint authentication and control or compliance issues. They also help with inventory management. In server networks, the primary use cases are micro-segmentation and inventory management.

9. Do you want to cover the wired network or also the Wifi?

Using the same NAC for both types of networks simplifies IT operation and can benefit the users' experience. Endpoint authentication is the same, whether on Wifi or wired networks.

Covering both networks also ensures that there are no loopholes. Wifi networks are often reachable from outside the buildings. Network plugged are sometimes in unprotected areas such as corridors, meeting rooms or reception areas.
A NAC should protect both.

10. Do you want to cover only your main offices or also the remote offices?

Many NAC implementations leave remote offices out of the picture, which is a bad practice. VPN links interconnect remote offices to the rest of the enterprise network. Most-of-the-time, they offer the same access to the enterprise than the HQ network. From a risk management point of view, both access should have the same level of protection.

11. Make a list of all your switch brand, models and firmware versions

Whether the deployment uses 802.1x or switch monitoring, switches compatibility can be an issue in any NAC deployment. Switches might be compatible but may need a firmware update. Hardware refresh might be needed.
I recommend making a list of all switches used in the network, including the brand, the model, and the firmware version. Switch compatibility with the chosen NAC strategy should be verified very early in the design phase. The design phase of a NAC deployment must plan all upgrades needed.

12. Do you manage the network infrastructure yourself?

As most of the NAC deployments imply network changes, the project planning phase must take it into account. For instance, the 802.1x protocol requires a configuration of each port of the switch. You need to plan for resource availability, budget, and network equipment upgrade.

13. Do you need a high availability solution?

This question bodes down to whether you can afford not to have the NAC up and running for a few days or not. NACs are like all IT systems. They need maintenance, upgrade, and sometimes have issues. Even if they are usually very reliable, they may be down for a few hours or a few days.
What happens during that time? Some organizations can accept the security risk and prefers to save on their investment costs. Others will not.
This risk analysis is a part of the design phase. It is cheaper and easier to design a redundant NAC than to add high availability to an existing one.

You need to ask yourself if you need high availability during the planning phase. It is less costly to plan a redundant NAC than to add this capability once the NAC is in place.

14. 802.1x pro and cons

People often mean 802.1x when they discuss NACs. It is a mature technology that provides endpoint authentication and access control, such as port closing or change of VLAN. Most of the people have heard about it, but it is not without its defaults and limitations. I always recommend discussing the pros and cons of 802.1x before implementing it.
Pros:
Supported by most of the switches
Supported without agents by many endpoints
Does not require and expensive NAC to be implemented
Cons:
Few tools exist to manage non-Windows endpoints configuration on a large scale. Deploying certificates on phones or printers can be VERY cumbersome.
It needs X509 certificates to provide strong authentication, so deploying a CA is needed for this approach.
As not every endpoint supports 802.1x with certificates, you'll end up whitelisting MAC addresses on a large scale. It becomes trivial to by-pass the NAC. Any pentester or intruder first looks for MAC addresses under phones and printers, change the MAC address of its computer and get access to the network.
It creates a triangle in the IT department in case of an issue. The summits are IT security teams, network team, and endpoint management team. If a device can't connect, the three teams often push the responsibility to each other and significant time can be lost in the process.
As it is a layer 2 protocol, a device with an issue is blocked and unreachable by the Service Desk. The blocking happens before the endpoint receives an IP address through DHCP.

802.1x, in my opinion, should be carefully balanced because it is not easy to make it right. A poor 802.1x implementation leaves substantial security holes in the network and provides more harm than good.

15. Do you want to authenticate guests and external users?

Limiting access only to known users increases the security posture of the organization. The authentication process with a NAC is straightforward. A captive portal forces users to confirm their credentials. Once authenticated, the NAC policy allows the endpoint to communicate with the rest of the network.

Some NACs can go beyond this. They can reinject the information about users in the logs of other security devices such as firewalls or SIEM. I had one engagement where I implemented the integration of the NAC with Palo Alto firewalls. Thanks to this, the client could track all Internet usage. He was not limited anymore to the authenticated corporate users.

After the NAC implementation, the users' behavior changed immediately. Guests stopped using the high-performance network of my client to download personal content. Within 24 hours, video conferencing was possible even from remote locations.
Implementing a captive portal is easy in networks with endpoints with users. However, there is usually a mix of computers with users and other devices. The NAC must provide two sets of authentication in parallel: one interactive authentication for end-users, and one automated one for devices such as printers or phones. Authenticating them based on MAC address white-lists would defeat the purpose of user authentication and would destroy the value of the NAC. In such a case, I recommend mixing a captive portal with an SNMP v3 authentication of end-points.
A NAC can use SNMP v3 to authenticate printers
or phones strongly. The NAC initiates an authenticated SNMP v3 connection on the devices. If it is successful, it means that the endpoint has been configured for the NAC and belongs to the organization.
If it is not, it's most probably a rogue device or one with an issue and the NAC handles it accordingly.

Do you have non-IP networks?
Network access control on non-IP networks is the new frontier. It opens new possibilities of inventory management and access control for industrial networks.

Vendors supporting non-IP networks provide appliances that act as a gateway between IP and non-IP networks for data collection. They also have large databases of devices and can use specific protocols to verify them.

16. Do you have a yearly penetration test in your company?

Pentesting a NAC is done at a minimum by following one of the following strategies:

- White-listed MAC address

Most NAC implementations do not provide strong authentication for all endpoints. Usually, printers, phones, or scanners authenticate through their MAC address white-listing. Sometimes, it is a complete vendor that is white-listed. A pentester only needs to walk around the office and try the MAC address printed on the device. Most of the time, it is successful within a couple of minutes.

- MAC address spoofing

Most of NAC implementations, especially the one based on 802.1x, do not monitor if the same MAC address is present twice at the same time on the network. Using a MAC address known to be whitelisted does not even require to unplug the spoofed device.

- Insert a hub or an unmanaged switch

A lot of NAC implementations do not monitor the number of MAC addresses connected to the same port. If a hub is connected to the switch port, only one authenticated device is needed to open the switch port, and all the other devices are accepted.

17. Beware of too much integration with one vendor

Some vendors provide many building bricks of today's network: switches, routers, firewalls, network access controllers. However, most of them are not the best in all areas. Usually, leading switch vendors are not the best NAC vendors, even though they have a large customer base. Having only one vendor has its advantages: a better bargaining position, one contract to manage, and one vendor relationship. However, this strategy may leave aside essential features that lack for many years.
I only recommend this approach if the chosen NAC has all the features needed.

18. NAC information is worth sharing

A NAC can have a wealth of information that no other system can offer. It can know who is on which device and on which physical plug. Accessing this information saves much time in many situations. It is valuable when looking for an endpoint in an office but also when looking for a server in a data center or a cloud environment. Let's be realistic; documentations are not perfect or not always up-to-date. The NAC provides this in real time. However, NACs can also provide additional information as they can analyze devices for compliance.
Sharing this information across the IT department increases the productivity of everyone at no additional cost. Service Desk teams and network teams that typically have more load due to the NAC can have a benefit and can be more productive thanks to it.

19. Virtual or physical infrastructure?

Most of the NAC vendors propose both hardware and virtual appliances. Virtual appliances are cheaper, even free with some vendors.
NACs are resource intensive. The workload they handle surprises most of the newcomers. Whether a virtual or physical infrastructure is the best approach is still an open discussion. Some of my clients have great performances with virtual appliances; some favored to stay with hardware ones.
The secret to achieving great NAC performances with virtual appliances is to dedicate the hypervisor or at least all hardware resources needed by the NAC. Virtual infrastructures with shared resources are a no-go because they can not handle the level of performances a NAC needs.
Running a NAC on a dedicated virtualized infrastructure provides the advantage of both worlds: high performance and management tools such as snapshots or high-availability that modern hypervisors offer.

20. Do you want to cover a cloud infrastructure?

Cloud infrastructures suffer the same issue than virtual ones in an even larger scale: device inflation. Cloud providers make it so simple to create a new server and so cheap, that cloud

infrastructure typically witnesses a massive increase in the number of servers compared to the original infrastructure.

21. Avoid MAC address for authentication

MAC address authentication defeats the purpose of the NAC. It takes its root in a design mistake done too often. There are many solutions to manage strong authentication on Windows making them easy to integrate with a NAC. However, other categories, such as phones or video cameras, do not have such a tool. Installing a certificate for 802.1x authentication on a VoIP phone or a printer can be a long and tedious manual work that does not scale beyond a couple of devices.
Devices, which are neither PCs, printers and VoIP phones also suffer the long tail effect. They are low volume exceptions: that special scanner in the marketing department, the specific printer to customize corporate badges in the administration department, or that access control manager in the lobby. Even if management tools exist for them, the low number of each device makes them too expensive or not practical.
As such, IT departments don't have the time to fine tune all those exceptions, and they add MAC addresses en masse into white lists. Sometimes all the MAC addresses of specific vendors are accepted.
Anyone serious about a NAC deployment must avoid this practice because it nullifies the action of the NAC. It is one of the main reasons why so many NAC installations are trivial to compromise. The intruder can get free access very fast. He looks for non-PCs devices such as printers, phones, and other rare peripheral. Their MAC address is easy to find. It is usually either on the back side of the device or on their side. Then he changes the MAC address of his computer and plugs it into the corporate network. Voilà, he's connected into the corporate network!

22. MAC spoofing detection is mandatory

Intruders use MAC address spoofing to steal the identity of an authenticated end-point, especially white listed end-points through their MAC address. It provides instant access to the network and takes just a few minutes to implement.
Some NAC solutions provide MAC spoofing detection, but it is not always activated. Make sure that this feature exists in the solution you choose and that it is turned on at the installation.

23. SIEM integration

SIEM products are more and more widespread. They can collect logs from all kinds of devices and correlate them to detect attacks and anomalies. They provide evidence in case of intrusion and tools to investigate incidents. However, they have limitations. One of them is that they need third-party devices when it comes to taking action: they can not block a compromised end-point by themselves. They need an integration with a NAC to do it.

The most common integration between a NAC and a SIEM is to redirect security events from the SIEM to the NAC policies and trigger NAC actions for particular events. When an end-point compromise is detected, the NAC can change its VLAN to quarantine so that it does not affect the rest of the infrastructure. If this is too drastic, the NAC can limit its communications with ACLs or a virtual firewall. The NAC extends the SIEM and prevents lateral movement and fire expansion.

24. Don’t forget the backup and recovery strategy

This advice is generic to any IT systems, but it also applies to NAC. Backups offer protection against configuration errors, hardware failure, and unexpected issues. Even if it is not a main corporate asset, the right practice is to regularly back up the NAC and apply best practices: review the back up once a year, keep them in a trustworthy location, and develop a straightforward recovery process.
All these pieces of advice are standard backup practices. However, not all IT departments apply it to their NAC. When trouble occurs, they have to reinstall the system from scratch, and the significant downtime they experience is avoidable.

25. Be aware of the time you'll spend on it

NAC solutions differ in their ease of use. A well-known NAC vendor, for instance, does not offer centralized management, leading to duplicate efforts and waste of IT resources.
However, other areas affect the time you spend on it. Different architectures and designs create more or less ambiguous detection and manual clarification. The primary cause of manual troubleshooting with a NAC is the case of corporate endpoints detected as rogue devices. They are 99% of all blocked devices. With the wrong setup and processes, they can keep helpdesk busy for hours and create frustrated users.
The NAC policies must be designed to not only sort rogue from corporate devices. They should also sort out corporate devices with authentication issues according to the root cause of the issue.
Let's take a NAC solution that authenticates endpoint based on certificate-based authentication with 802.1x. It may reject Endpoints for many reasons. The NAC should display what is the root cause of the authentication failure: Does the endpoint talks 802.1x with the switch? Does it propose certificate-based authentication during the 802.1x handshake? Is the proposed certificate expired? Is it signed by a trusted certificate authority? Is the key length correct? Are all the attributes of the certificate correct?
A proper 802.1x implementation provides this information at a glance to its users, and understanding quickly the root cause of an authentication failure saves precious time.

26. Don’t forget the out-of-band management of physical appliances

NACs are sometimes in a remote office or in a difficult to access closet in an industrial building. Out-of-band access is needed to have reliable access when network connectivity is lost. It should not be overlooked, especially in NAC deployment with blocking actions or that require a fail-closed behavior.

27. Consider the potential upgrade of endpoint

Depending on the authentication technology used in the NAC setup, endpoints may need to be upgraded to avoid the dangerous MAC address whitelist. As such, the design phase must contain an inventory of all endpoints, including their OS version. 802.1x is not always totally supported, or management tools may lack.
Windows operating systems activate the 802.1x service by default on the Wifi interfaces but not on the wired one. A GPO can change it, and a second one can deploy machine certificates. The best is to automate the complete life cycle of the certificate so that a GPO renew certificates. I recommend to renew them one month before expiration so that users on holidays or sick live on the renewal day have enough chance to come back before their certificate expiration. I recommend renewing certificates with GPO 30 days before their expiration.
Other platforms may be more challenging to handle. I remember an 802.1x deployment where the VoIP phones supported 802.1x with certificate authentication. Unfortunately, a pilot deployment showed that the certificate deployment and 802.1x activation took about 30 minutes of manual work. No management tools could work as it wasn't possible to do it either with an API or an open scriptable protocol.

28. Don’t forget to give visibility to management

Management needs to understand why they invest in IT. They are accountable just like anyone in the organization. Though information needs can vary from one organization to another as the NAC use cases differ, your management typically needs the following monthly KPIs.

- Total number of endpoint monitored
- Number of endpoints identified as rogue
- Number of corporate endpoints needing repair to authenticate correctly
- Number of new endpoints that required a configuration change so that they can successfully authenticate
- Number of compromised endpoints detected
- The number of non-compliant endpoints, itemized by type of non-compliance.
- Larger organization often break these KPIs down by business units or locations.

29. Give access to the helpdesk

Helpdesk is essential in NAC operations. When a user cannot access the network, he contacts the helpdesk first. So they need tools to solve the issue at hand. It is crucial to add as many reports and policies they may need to troubleshoot an authentication issue. However, the helpdesk can also benefit from a NAC. It is the only device providing at the same time the information of which user is connected to which device, and on which physical location. It can also collect a wealth of information about each end-point.

30. Plan in advance who needs to be involved if you implement blocking control actions

Blocking control actions are often the first thing that I read in requirements. The reality of a NAC is that 99% of blocked endpoints are internal devices with an issue. It's rarely a rogue device used to infiltrate the company. Physical attacks are extremely seldom, so any plan to block suspicious devices should include a plan about how to detect internal devices that do not authenticate correctly and how to correct them. They are 99% of the blocked devices.

31. NAC can also have benefits to end users

NAC can benefit end users and can provide a new IT experience. As end users are recognized wherever they connect, the NAC can reassign them to a new network that is better suited to their task. For instance, network access in operation rooms in a hospital can be changed dynamically so that each surgeon has direct access to its department resources and information.

32. Don’t forget to pen test your NAC

I strongly advise doing a pentest after the installation of a NAC. Mistakes can be made both during the design and the implementation. Rogue endpoint, spoofed MAC address and MAC address whitelisting are the typical use case to verify.

33. Monitor for performance and availability

NACs, like all IT systems, have limited resources. Performance issues lead to erratic behaviors and random blocking of a legitimate endpoint. Unfortunately, the monitoring of security systems is not a priority and not a widespread practice. Basic monitoring such as free memory, CPU usage, or disk activity is often not done, and the lack of resources is seldom detected.
I experienced it first hand with one of my clients. Their NAC was lacking memory, and they detected it only after two years. A lack of memory meant constant swapping of the hard disk, which lead to frequent failure due to overstress. However, it also led to poor performances

and random blocking of endpoints. The monitoring of memory, CPU, and hard disk activity highlighted the issue very quickly.