Computer says No

Network Access Control made easy

A guide for IT managers that want to take back control

Soliton®

Content

WHAT IF NETWORK ACCESS CONTROL WAS EASIER?

Hi IT-manager,

You've probably heard of Network Access Control (NAC). And you've probably decided not to like it. We're with you, as NAC is often complicated and a hassle. As an IT-manager, you deal with enough complicated and hassle already, so you decided that NAC is something for big multinationals with an IT-department with the size of a city.

At the same time, you probably know that something needs to change security-wise. Today, there are so many new ways that new people and new devices require access to the corporate network; devices and people with different roles, responsibilities and access rights. They all need to get in (especially the people), but they all bring risks, whether intentionally or otherwise.

How do you orchestrate this without exposing your company data? How do you decide which person or printer gets access to what part of the network? How do you guide the doors without stopping innovation?

And how do you do all of this without working day and night?

All of these questions will be answered in this white paper. We introduce what we believe is the solution: automated Network Access Control (NAC). Not in the complex way that you know it, but in a way that there are only two possible answers to users knocking on your company door: "Yes, but" or a simple "no".

Enjoy the reading!

Team Soliton Systems

CHAPTER 1.

A DAY AT THE MODERN IT DEPARTMENT

KEYWORDS:
CABLE- WI-FI- VPN
BRING YOUR OWN DEVICE
CYBERCRIME

Remember the days that IT was a lonely department? Often, it was tucked away on the third or fourth floor, functioning as a self-proclaimed city-state, far away from the meeting rooms where the “real” magic happened. IT managers weren’t asked to join C-suite gatherings on a regular basis, simply because there was no reason. You were in charge of firewall software, forgotten passwords and rebooting out-of-control PCs. You had some power though. The company was a ship, and nobody could get on unless you allowed them. But not anymore.

Wi-Fi, BYOD and freelancers

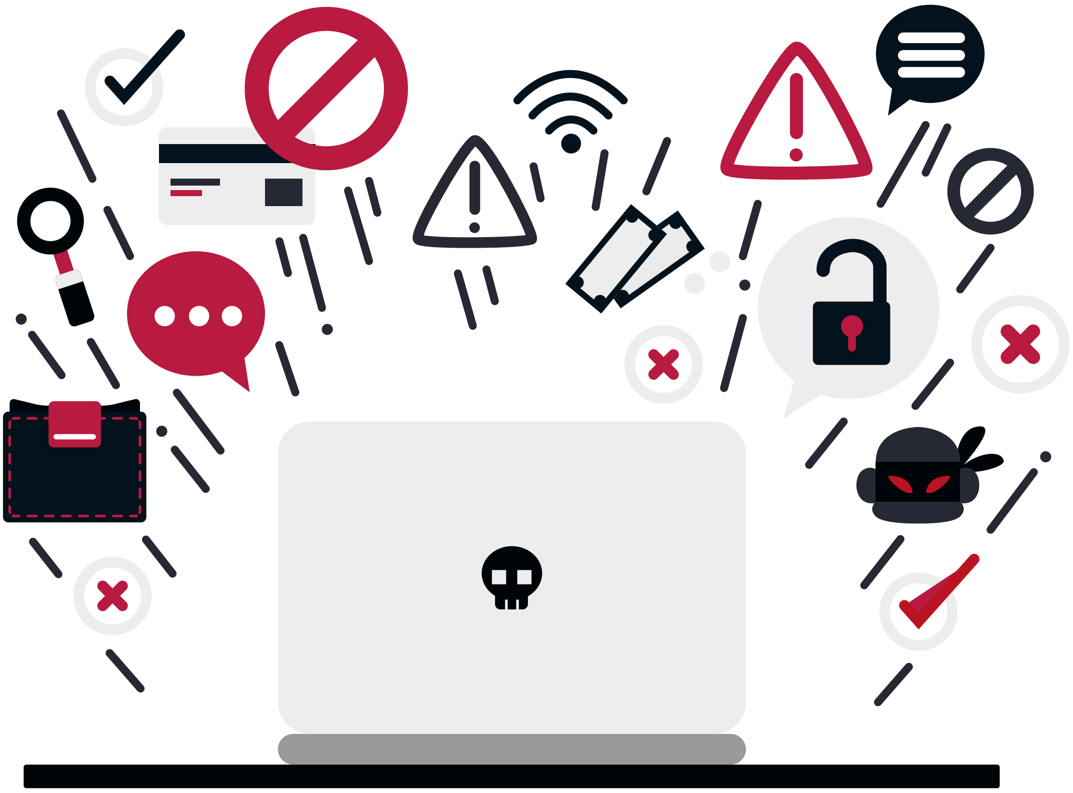
Today, most organisational problems revolve around IT. Devices connect to your network through cable, Wi-Fi and VPN, making it harder to control it. There’s an increased number of companies allowing Bring Your Own Device policies, meaning you not only have to monitor company PCs, but laptops, phones and tablets too. Then there are guests and contractors requesting access to the network: people you’ve never heard of, but still like to surf the web when visiting your company. If that’s not enough, more and more companies hire freelancers to remain flexible, which means that a lot of people come- but also a lot of people go.

> “The biggest dilemma of today: companies are forced to become more flexible and interoperable, but the more they are, the more they risk losing”

Digital transformation risks

Apart from developments such as company Wi-Fi, BYOD and temporary contracts, digital transformation in general brings new challenges too. Take the Internet of Things, for example. Something simple as wireless printing requires a thing being connected to your company network, meaning you need to secure it, but also determine which users get access to which printers. That's doable if you have five employees and one printer, but it gets harder when you tenfold these numbers. Second, Big Data has found its way into pretty much every company strategy in the world now, meaning businesses deal with huge amounts of information that have to be easily sharable without the risks of being intercepted by the wrong people. Maybe that's the biggest dilemma of all: companies are forced to become more flexible and interoperable, but the more they are, the more they risk losing.

> Cybercrime comes in many different forms, such as malware, viruses, DoS attacks, phishing emails, identity theft, botnets and keystroke loggers. You know, just to name a few



Cybercrime

All of these developments have increased the number of security breaches, as they're basically open invites for cybercriminals. There are simply too many doors leading to your company servers to secure them all, and even if you could, you still wouldn't be able to make all of your co-workers aware of the many security risks. Because despite of what most people think, there are many different ways that cybercriminals can cause damage, and they all happen to small businesses too. In fact, an appropriate share of cyber-attacks happens to smaller businesses, and the damage done can cause them to lose customers or worse, go bankrupt. These are alarming facts that you probably already knew, but try and tell that to your co-workers, that often don't foresee the consequences of a cyber-attack.

Moving on

OK, you get it: a lot has changed and there's a lot that can go wrong. The question is: how do you, as an IT manager, take back control over the company network without having to chase co-workers and work 80 hours a week? We'll tell you in the next chapter.

CHAPTER 2.

THE PROMISE THAT IS NAC

KEYWORDS:
WI-FI PASSWORD
PORT-BASED NAC
AUTHENTICATION & AUTHORISATION
RADIUS SERVER & SWITCH
CERTIFICATE AUTHORITY

As you probably know, Network Access Control (NAC for friends) is an ideal way of telling who can access the company network and determining what they're allowed to do there. Given the new circumstances that come with digitalisation, you might wonder why not every single IT manager on the planet hurries to implement a NAC solution to solve their company's security problems. The answer lies in the many problems that could come with NAC, such as high costs, high complexity and a potential vendor lock-in.

Yet, if you were able to overcome these problems, the situation would be very different. So, for a moment, let's pretend the flaws aren't there, so we can investigate what it is that makes NAC such a great solution on paper. In the next chapter, we'll tackle each and every NAC disadvantage, leaving you with only the good stuff. Bear with us!

NAC & its proposition

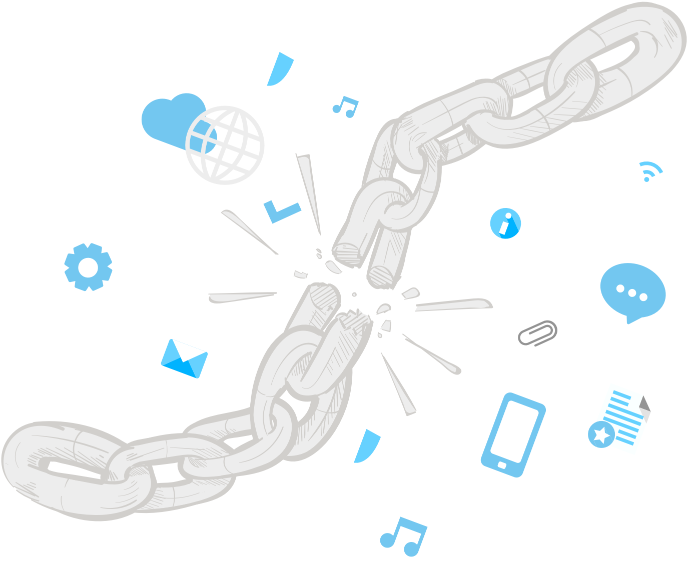
Already in 2001, the concept of Network Access Control made its entrance to the market with a very promising value proposition: "NAC controls access to enterprise resources using authorisation and policy enforcement".

With this proposition, NAC was the answer to the static security culture that can still be found in most organisations. Usually, employees either plug in a cable at their desk or ask for a Wi-Fi-password to gain access to a company network. Although both options help you govern a zone of trusted devices within a company, security can be easily circumvented. It's not that complicated to guess a Wi-Fi password (or remember one if you just got fired), or to walk into another department and gain access to the finance network, even if you're an intern at HR.

Instead of depending network access on a single password or the exact place that people work, NAC focuses on who wants access. It doesn't matter whether this person connects through cable, Wi-Fi or a VPN; a NAC solution acts as a customs officer that first authenticates the employee and his device type, and then decides to which country (computer network) he's allowed to travel. This helps you to be more specific in what users can and cannot do through which device, as NAC is monitoring actual humans instead of machines. This makes it a much safer and more dynamic security solution.

Another advantage of NAC solutions is that they "know" where the network access request comes from. They can not only tell where the user is located, but also whether a person connects through cable, Wi-Fi or VPN. And as NAC solutions recognise device type (laptop, tablet, phone) you can tell them to block someone's iPad but to give access to someone's laptop. So, let's say the CEO wants to enter the company network with his iPad and through VPN. A NAC solution would take into consideration the user (the CEO), the device type (iPad) and the location (VPN). This helps to limit access rights to "good" and approved devices only, but also provides you with important information in case there's an irregularity in the company network that you want to track down.

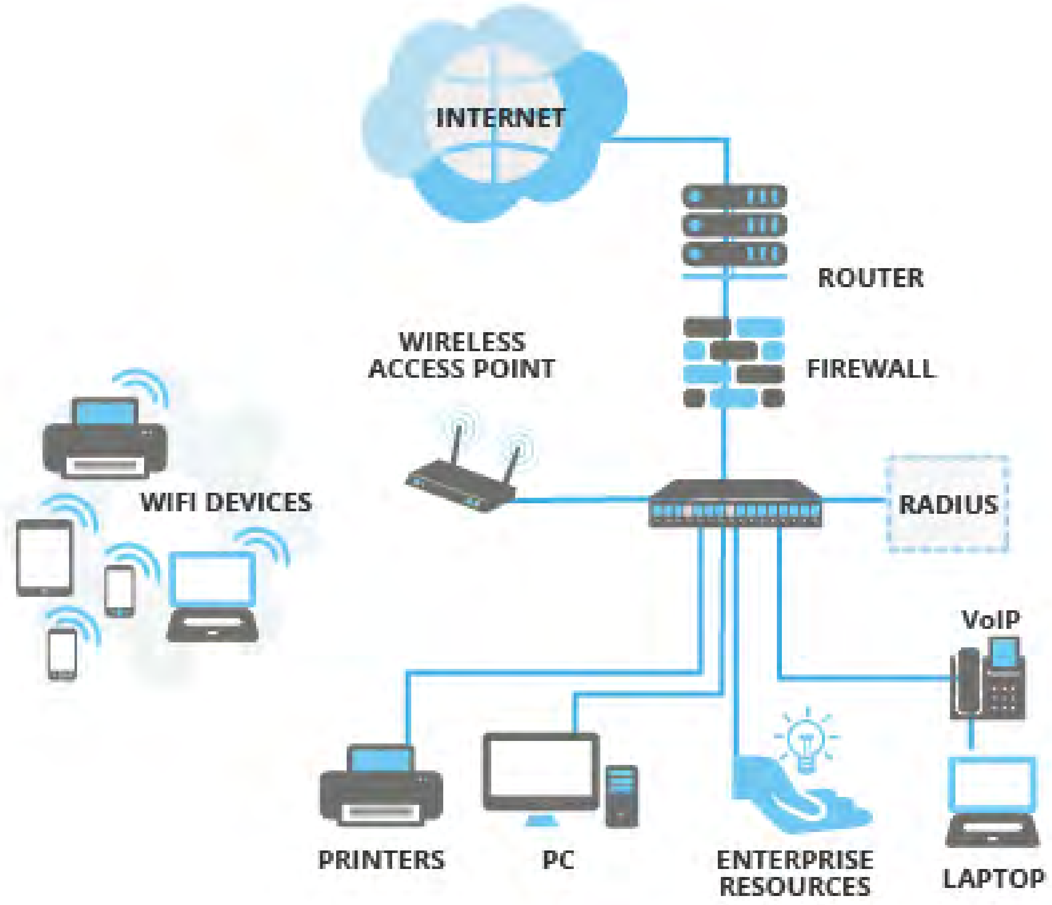
> NAC helps IT managers to better manage data protection and to personalise digital freedom of movement per employee



In other words, NAC gives IT managers (and therefore companies) more control over their network, as the solution allows them to be more precise in what users can and cannot do and through which device, while providing them with more detailed information on users, devices and behaviour. This helps them to better manage data protection and to personalise digital freedom of movement per employee.

“Computer says no”- authentication and authorization

Network Access Control starts at a network entry point, such as a switch (in the case of internet through cable). The switch connects users with the network they want access to, based on predefined rules. These rules are governed by a so-called RADIUS server, that keeps track of which users are allowed in and what their rights are. The RADIUS server instructs a switch to either let a user or device in and provide access to a specific network, or to simply block the entrance. This solution is what we call port-based NAC. It’s a quite powerful tool, as the switch authenticates and authorises users before a connection can be made between a device and the network.



What about Wi-Fi?

The same principle goes for Wi-Fi connections, but in a slightly different way. A user connects to a Wi-Fi access point, which in turn asks the RADIUS server to which network the user can be connected. As a bonus, the password that's used to encrypt the connection is generated per session, making it almost impossible for hackers to intercept the wireless connection. Bye-bye, shared Wi-Fi password!

What about VPN?

VPNs are still highly popular among homeworkers, as they give users access to the network from all over the world. It's dangerous, though, because users get real network access and there's no way to find out what happens on the other end of the line. A NAC solution makes it possible to identify the user and to make sure he only gets access to the right network. As is the case with cable and Wi-Fi, VPN concentrators ask the RADIUS server whether or not to let them in.

> “Certificates are comparable to passports as they too are a type of identification, moreover they’re also hard to forge”

Certificates as your identification document

As soon as you understand and appreciate the NAC principle, there's another question that rises: how does the RADIUS server know which user or device is asking for access? The answer is certificates. Certificates are documents that can be checked by the RADIUS server, and they're comparable to passports as they too are a type of identification. Moreover, they're also hard to forge or to copy. Certificates are checked without the user having to do anything. This is approximately how it works*:

User: "Hi there. I'm Ellen's laptop calling in from a Wi-Fi access point that's located on the third floor of location C. Ellen is logged in and she'd like to gain access to the corporate network.

RADIUS server: "Certificate please."

User: "There you go."

RADIUS server: "Hmm let's see. Ellen is a member of the HR department, so it seems. The certificate for this laptop is valid until the end of next year and it is not revoked. Therefore, she is allowed to enter the HR-network. Very well. Wi-Fi access point?"

Wi-Fi access point: "Yes sir?"

RADIUS server: "You can let Ellen's laptop in, but make sure it's only provided access to the HR-network."

Wi-Fi access point: "Certainly, sir."

**We apologise for this childish dialogue, but it's probably the best way to explain how the RADIUS server and the switch collaborate. If, in any way, you feel insulted, do give us a call so we can apologise in person.*

Certificate authority: the passport factory

Of course, certificates don't appear by magic; they have to be created. This is done by a so-called certificate authority (CA), which is comparable to a passport factory. Here, the user (or an authorised IT colleague) can request a certificate to gain access. Certificates are then securely stored on the users' device, in a place that can only be accessed when the user is logged in. When the user connects to the network, the certificate is used to uniquely identify the user and his device, which allows the RADIUS server to determine what type of access is allowed and under which conditions. Each and every single person, device and thing (such as printers) are provided with a certificate, so the next time they knock on your company doors, the RADIUS server will know what to do.

Certificate renewal

Much like passports, certificates have an expiration date and need to be renewed once in a while (a user or device won't be able to gain access to the corporate network after the certificate has expired). Of course, the shorter your renewal cycle, the more waterproof the NAC solution. But certificates can also be revoked. So, when employees leave the business, you simply revoke their security certificates and they're left without power.

We can almost hear you think: "This all sounds very good, except for the fact that it means that I have to dive in yet another technology while spending many hours on certificate creation and renewals".

Don't worry. We've come to end of this chapter, which means time has come to deal with some NAC disadvantages and offer corresponding solutions.

CHAPTER 3.

NAC DISADVANTAGES

KEYWORDS:
CERTIFICATE CREATION AND RENEWAL
CERTIFICATE DISTRIBUTION
VENDOR LOCK-IN
HIDDEN COSTS

If you really look into NAC, you'll realise that its problems don't revolve around reliability and effectiveness. The problems that come with NAC are all operational, as the solution is known for its complexity and time-consuming digital paperwork on rules and certificates. Let's talk you through them one by one.

DISADVANTAGE #1. Certificate creation and renewal

The greatest NAC hassle of all revolves around certificates. They have to be created and renewed on a regular basis, which requires IT managers to completely understand how they're put together. Second, creating and renewing certificates through a Certificate Authority takes time, and the time needed increases tremendously as the company hires more people and connects new devices (sometimes several per person). Sure, you can choose to renew certificates every five year instead of one, but this drastically lowers NAC reliability.

DISADVANTAGE #2. Certificate distribution

When you've created or renewed a certificate, it has to be shared with the user. This means you have to install and renew certificates per each approved PC, laptop, tablet and phone. It's a time-consuming task, and it gets more difficult now that so many people work from home, which means you can only reach them by stepping outside the company network. Second, if something goes wrong (which is likely as the procedure is executed by humans), co-workers will line up at your desk, panicking about their lack of access.

> Technology vendors often sell products that are only compatible with their own software and hardware, which forces you to stick with the vendor throughout all of your IT purchases

DISADVANTAGE #3. NAC implementation & vendor lock-in

Implementing new technology is not a one-day job. It takes time to install new software, but more important is that, often, the existing data infrastructure is not ready. If this is indeed the case, developers (either hired or in-house) need weeks or even months before they can have everything up and running. If you lack in-house NAC specialists (which you probably do), hiring an external party brings extra costs, that add up the more that things go wrong. Another frustration lies in a so-called technical lock-in. Technology vendors often sell products that are only compatible with their own software and hardware, which forces you to stick with the vendor throughout all of your IT purchases. Such a lock-in comes with high costs if you want to get out.

DISADVANTAGE #4. Hidden costs and hassle

Apart from implementation costs and the hourly fee of hired specialists, traditional NAC also comes with hidden costs. We already mentioned the queue at your desk, consisting of people that can't do their jobs unless you help them. Combined with the time you spend on fixing their problems, their downtime creates a hidden bill that no one really pays, but that does have a major influence on the billable hours of your co-workers.

CHAPTER 4.

ULTIMATE NAC WITHOUT ITS COMPLEXITY

KEYWORDS:
ALL-IN-ONE NAC
REMOTE AUTHENTICATION
NAC USABILITY
NAC PARTNER

Having read chapter 3, you might not be inclined to run to the nearest NAC provider to purchase everything they have. But like we said: all NAC problems are operational. This is good news, as operational hassle is solved more easily than failing technology. All you have to do, is find the best NAC solution while limiting the hassle to a minimum. In this chapter, we tell you what to look for.

TIP #1. Go with an all-in-one solution

An all-in-one NAC solution literally has everything you need to guard your company network. It includes the RADIUS server and the Certificate Authority that generates the security certificates. Thanks to this automated form of access control, you increase security levels while saving out on time. Moreover, automated NAC solutions are far less prone to error compared to those that are managed by human hands. If you tell the RADIUS server about the rules, chances are very low it'll have an off-day and forget one or two.

TIP #2. Search for a NAC solution that allows secure distribution

If you want to skip the part where each and every co-worker must come by your office to have his or her devices authenticated and their certificates renewed, we advise you to ask your technology provider if they offer user-centric secure distribution of certificates using multi-factor authentication. User centric means that your co-workers can download their certificates from their own floor or even from their own home. Multi-factor authentication comes in different forms. A well-known way is the One Time Password-token, that provides the user with a code that they have to type in when requesting certificates, but it could also be a simpler solution like a pre-shared code that the user fills in.

> “If your partner offers an all-in-one solution, access control is completely automated, meaning **your hands are free** right after the implementation part is over”

TIP #3. Leave your data infrastructure alone

Many IT-managers have asked us whether they should change their data infrastructure before implementing NAC. The answer is no. A modern NAC solution should be easily connected with the software and hardware that's already there and it has to be easy to administer. This is good news for several reasons, as it will speed up the implementation time, avoid a vendor-lock in and save you out on costs (and headaches). This NAC usability is the biggest difference between NAC as you know it and NAC done right, so make sure you can tell the two apart.

TIP #4. Search for a partner

Sure, you can become a NAC specialist yourself. The question is: will it help you make your day-to-day work easier? There are security partners that are specialised in NAC, meaning they can take on the implementation part and instruct you on how to use the software and hardware. Especially when your partner offers an all-in-one solution, access control will be completely automated, meaning your hands are free right after the implementation part is over.

NAC ready?

We've come to the end of a new story about Network Access Control. We've discussed developments that require new safety measures, we've talked about NAC flaws and NAC advantages, and we handed you the tools to find a NAC solution that breaks down the static security culture without bringing you new problems. It's time to get started! We wish you all the luck with becoming NAC ready and taking back control over your company network. If you should run into questions, feel free to reach out. We could talk about security innovations all day long.

Good luck!

Expand your knowledge on modern MAC spoofing alternatives >

ABOUT SOLITON SYSTEMS

Soliton Systems is a Japanese technology company providing innovations in many fields including IT Security, Public Safety and Mobile Broadcasting. We're listed on the Tokyo stock exchange, but we operate at an international level. It's our mission to make IT security better and more user-friendly at the same time, so that more companies can benefit from an optimal safety level.

Our experts are committed professionals and love to talk about their field of expertise and how it can help you take back control over your company's safety. Digital change is coming, and we're here to help you face it.

Do you have questions on Network Access Control and its fit with your company? Feel free to reach out!

EMEA office

Soliton Systems Europe N.V.
Barbara Strozzilaan 364, 1083 HN Amsterdam, The Netherlands
+31 (0)20 896 5841 | emea@solitonsystems.com | www.solitonsystems.com