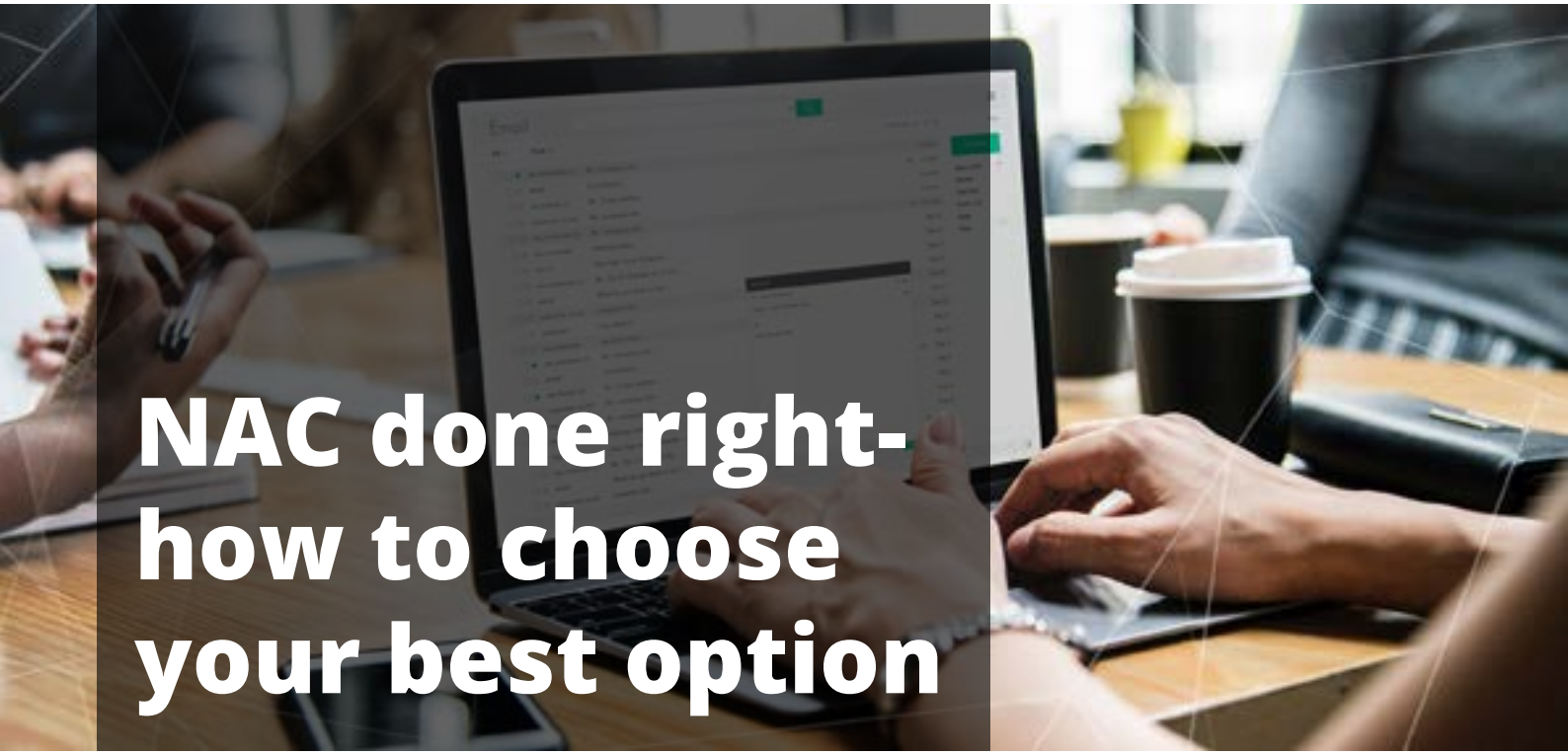
Soliton®



NAC done right- how to choose your best option

Now that you know what your ultimate NAC solution could look like, we want to take things one step further and discuss the different NAC options that could help you make your company network fool-proof and user friendly. Security requirements differ per company network, location and sensitivity of processed data, so a little mix and match can save you out on costs on security software while taking away a lot of hassle. Let's find out what's in store!

Why we won't be talking about inline NAC

Many articles have been written on the differences between inline and port-based NAC (also known as out-of-band NAC) solutions. The bottom line is that inline NAC is placed in between all traffic going through the network, whereas port-based NAC uses switches, Wi-Fi access points and VPN concentrators to keep unwanted devices out. In the case of inline NAC, literally all traffic (mail, web browsing, files) is passed through an appliance that checks the messages based on pre-defined rules. If the message survives the validation process, it's allowed to pass. This method is ultra-safe; however, it comes with five downsides:

1. It's expensive
2. It's complex
3. It requires a lot of bandwidth
4. If it gets overloaded, it quickly becomes a congestion point which will severely impact network throughput
5. It overdoes security, especially in compartments that don't require message-checking

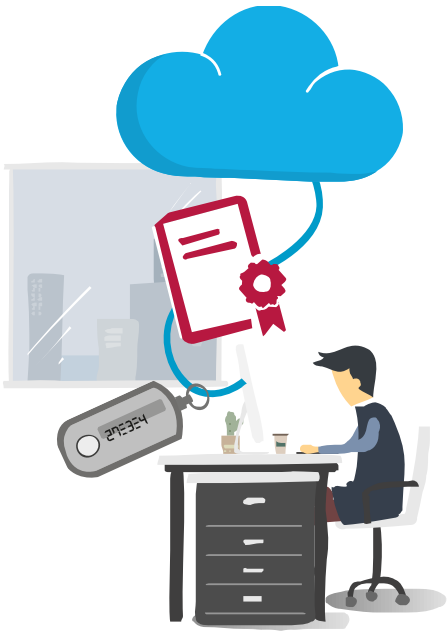
It's because of these five disadvantages that you didn't read anything about inline NAC in the white paper. As opposed to its inline equivalent, port-based NAC teams up with the source of the device (either cable, Wi-Fi or VPN) and guards the doors without interfering with every single message. This makes port-based NAC solutions easier to handle and also less expensive, without compromising safety.

Heavy-weight or light-weight?

Port-based NAC it is! But you're not done choosing. Apart from the port-based NAC solution that we discussed in the white paper, there's also a more light-weight NAC version available; a version that comes with fewer costs and a different value proposition. We think both the heavy-weight and the light-weight could be of real help in your quest to ultimate security and user-friendliness, so let's talk you through both.

Heavy-weight NAC

This is the flavour we've discussed in the white paper, as it's the most advanced method of the two port-based NAC-solutions. With heavy-weight NAC, authentication and authorisation decisions are made by a central RADIUS server, while the actual enforcement is done in all the places where devices enter a network (switches, Wi-Fi access points and VPN concentrators). Basically, the RADIUS server asks for a certificate and only allows access to those devices that show the right one, but it's possible to put in place other policies as well. After the RADIUS server has authorised the user and/or the device, they're allowed to enter a specific part of the company network and able to communicate without any interception. It's this certificate method that makes this NAC type bulletproof, as certificates are very hard to forge and can be easily revoked in case of a violation or resignation.



Light-weight NAC

As opposed to port-based NAC, light-weight NAC checks the broadcast traffic in a network. No certificates needed! If a device enters the network, it will try to get into contact with other devices, which is how the NAC solution can detect it and decide whether it's welcome or not. He'll then broadcast the presence of the newbie to the entire network (which in real life would be quite the embarrassment). If it's an intruder, the device is excluded from all communication, making it impossible for its user to get anything done. However, if the device is whitelisted, it's welcome to join the group. The NAC solution distinguishes the "good" devices from the "bad" by maintaining a white list of authorised devices and users. This white-listing is done beforehand but can also be done "on the fly" as administrators are informed immediately of any network changes. This is a very efficient way of keeping track of devices that are allowed access to the network while actively banning the ones that aren't, without the burden of infrastructure changes.

> The light-weight NAC solution distinguishes the "good" devices from the "bad" by maintaining a white list of authorised devices and users

Which one to choose?

Both heavy-weight NAC and light-weight NAC come with their own perks that solve different problems for different types of businesses. To make your choice a little easier, we've listed their main advantages below.

> With heavy-weight NAC, there's no way one single user will step foot in a company network compartment without being checked

Perks of light-weight NAC

Heavy-weight NAC protects your company network from both intended and unintended attacks. It won't let any device near your systems unless it knows who owns it and what the user is allowed to do in which network domain. The great advantage of heavy-weight NAC is that if the system should fail, no user is allowed in the company network, meaning it's rather safe than sorry. Second, there's no way one single user will step foot in a company network compartment without being checked by the RADIUS server, that only clears devices with a valid and non-revoked certificate. Second, heavy-weight NAC will help you lock away network compartments containing sensitive business data while keeping others easily accessible, which improves user friendliness. It's this selectivity that's the most important difference between the heavy-weight version and the light-weight one.

Perks of port-based NAC

Port-based NAC protects your company network from both intended and unintended attacks. It won't let any device near your systems unless it knows who owns it and what the user is allowed to do in which network domain. The great advantage of port-based NAC is that if the system should fail, no user is allowed in the company network, meaning it's rather save than sorry. With port-based NAC, there's no way one single user will step foot in a company network compartment without being checked by the RADIUS server, that only clears devices with a valid and non-revoked certificate. Second, port-based NAC will help you lock away network compartments containing sensitive business data while keeping others easily accessible, which improves user friendliness. It's this selectivity that's the most important difference between the heavy-weight version and the light-weight one.

Ultimate NAC might just be a combination

In an ideal world, your NAC provider is able to implement both options and combine them. This is very useful for businesses with multiple locations, some of which with switches that are not compatible with the heavy-weight NAC solution. If you implement the heavy-weight version at your headquarters and implement a lightweight solution for each of the locations that don't need heavy-weight security, your overall network it still optimally secured. This way, there's no need to rebuild your entire infrastructure, making it a quite unique combination not every provider can build. Even companies with only one location should consider an integration of both NAC solutions, though. It's the ultimate way of waterproofing your entire infrastructure without the risks of overdoing security or making too many changes to your current IT situation.

There you have it! An overview of NAC options and their fit with your business. We wish you all the luck with finding your ultimate security solution.