*Setting a **Higher Level of Excellence** in Information Security & Compliance Services.*

Network Access Control Basics | by Rich Whyrick, ITIL, Security+

Network Access Control (NAC) can be a very confusing concept to understand if one tries to dig into the minutiae of how it works and every single thing it can do. Instead, to get an idea of how it can assist you in your security efforts, start by focusing on breaking down its name: Network. Access. Control.

NETWORK. It's a bunch of jacks in the wall that have wires that run back to that blinky-light box in a closet or in the data center. Or, maybe it's those white boxes on the ceiling with the antennas pointing in various directions. But it's more than that! It's any device with a network interface card (NIC), wired or wireless, connected to those jacks in the wall or wirelessly to those white boxes on the ceiling, which means it has, at a minimum, a media access control (MAC) address, and likely an Internet Protocol (IP) address. All these things collectively make up the network, and it's VERY important to have visibility into anything residing on your network, which is probably the most important use case for NAC.

Now, ACCESS. What does that mean on your network? A device with a NIC has been placed on the network and was given a dynamically assigned (DHCP) IP address. But what access does it have from there? If the device is a server, a PC, or a laptop that has been joined to your domain, then there are probably resources that it will be able to access based on permissions assigned. If it's a smartphone or tablet, it probably only has wireless connectivity, and may have more limited access, such as internet-only access.

Finally, CONTROL. Up to now the other two components are just typical of any business or home with Internet: Network Access. Control is where the rubber really meets the road.

With access we discussed devices on the network joined to the domain for access to resources such as file shares, applications, email, and the Internet. But what about a device that doesn't belong on your network, something that nobody in IT put there or gave permission to join your network? This is where the "control" part of Network Access Control comes in to play.

NAC is designed to interrogate every single device that attempts to connect to your network, and either allow or block those connections. Dell Windows 10 PC named Teller-3 in the teller area? Recognized and allowed. Cisco 3560 Switch in the data closet? Recognized and allowed. TV connected wirelessly in the breakroom? Recognized and allowed. Wireless access point plugged into drop 3-14 that terminates on switchport 2/21? NOPE, don't know that guy - DENY! Connection blocked automatically, ticket generated, and now someone from the helpdesk is on their way to investigate.

So, what just happened? The NAC solution did its job. It interrogated all those devices (and dozens or hundreds more) in milliseconds and validated that the first three were known devices and permitted them to continue on about their day. But the access point had not been previously seen, and because it did not have a recognizable simple network management protocol (SNMP) string or provide authenticated secure shell (SSH) access for further interrogation, it was blocked, and NAC submitted a ticket for further investigation.

Let's talk a little bit about how this all works. If the device is a domain-joined server, PC, or laptop, it has an account assigned to the local administrator group that the NAC solution can use to interrogate it via Windows management instrumentation (WMI). This makes it easy for the NAC to make the determination that the device is known; or maybe it's never been seen before but because it meets several criteria (Windows 10 OS, domain-joined, WMI-manageable, etc.) the NAC allows it onto the network. And it did all of this on-the-wire, no client installation required.

But let's say you have laptops that travel outside of your network that occasionally use VPN for remote access. There will be instances where the interrogation *out* to a device can't happen due to firewall rules. In those cases, a small-footprint client can be installed which will then make a call *in* to the NAC and be permitted to fully join once that connection has been established and the device has been recognized.

Another use case for NAC that was briefly discussed above (although not by name) is 802.1x authentication. 802.1x can be used for both wired and wireless authentication on a network, either using remote authentication dial-in user service (RADIUS) or extensible authentication protocol (EAP) using credentials or certificates. The NAC device acts as the supplicant and can further enhance the security posture of your network.

As mentioned above, knowing everything that's on your network is half the battle in security. If you don't have visibility into the devices consuming bandwidth and making calls out to the Internet how can you truly say you're protecting your network?

There are dozens of other use cases for NAC, from determining if SSH or HTTP are unnecessarily open on devices on the network, to determining that restricted software is installed on some PCs - and disabling or uninstalling said software. NAC really can be the Swiss Army Knife of your security toolset.

Now, let's get real for a minute: NAC is not plug-and-play. It requires a lot of careful planning to ensure that all of your switches, firewalls, access points, servers, PCs, laptops, IP phones, printers, physical security systems (cameras, badge readers, etc.) and anything else that has a NIC are recognized and permitted to perform their functions before you can turn on BLOCK mode. That takes time and can crush the hopes and dreams of anyone thinking they'll have it up and running within a few days. Those aforementioned admin accounts need to be added to all Windows devices; SSH credentials need to be added to all Macs, Linux devices, switches, routers, and access points; defining how IP phones and printers will be recognized could come down to checking for H.323 or SIP or recognizing http banners or defining make and model. If you miss one single definition and turn on BLOCK mode suddenly your entire call center is down. So be prepared for it to take a few months before you can enable BLOCK mode, but keep in mind you can still monitor and alert on unknown devices. It's an arduous task that will have you questioning your very existence before you get there, and even after you enable BLOCK mode there will still be tuning and adding new rules (switched ATM brands, did you?) to ensure everything that should be on your network is allowed, and anything that shouldn't be isn't. Good luck, and happy hunting.