No network is airtight—malware continues to get in, whether via mobile employees, guest or contractor laptops, or end users downloading dodgy content. Antivirus software at the gateway or on the desktop helps with computers under your control, but guests and unmanaged servers remain problematic. And let’s face it: Sometimes attackers are just smarter than we are. Even companies following best practices get hit.

We don’t just mean just security best practices, either. Protecting the network from malicious hosts is, ultimately, a desktop management function. NAC is what puts teeth in your policies, providing an enforcement mechanism that helps ensure computers are properly configured. By weighing such factors as whether a user is logged in; her computer’s patch level; and if anti-malware or desktop firewall software is installed, running and current, IT can decide whether to limit access to network resources based on condition. A host that doesn’t comply with your defined policy could be directed to remediation servers, or put on a guest VLAN.

Remember Slammer? If a company could have determined that a host was running an unpatched version of MSDE 2000 and denied access until it was patched, Slammer would have had a much less dramatic effect.

That’s the promise, but NAC is no magic bullet. The solution to the Slammer scenario is to either patch the vulnerable system when you can, or remove access to MSDE from the network. But if your NAC system doesn’t check for applications like MSDE or their patch levels, it wouldn’t preclude a vulnerable node from accessing the network.

General Architecture

Three basic components are found in all NAC products: the Access Requestor (AR), the Policy Decision Point (PDP) and the Policy Enforcement Point (PEP); see NAC Framework diagram on adjacent page. Vendors have their own names for these, but we’ll use the terms defined by the Trusted Computing Group Trusted Network Connect working group because they’re fairly clear-cut.
Individual functions of the PDP and the PEP may be contained on one server or spread across multiple servers, depending on vendor implementation, but in general, the AR requests access, the PDP assigns a policy, and the PEP enforces the policy.

The AR is the node that is attempting to access the network and may be any device that is managed by the NAC system, including workstations, servers, printers, cameras and other IP-enabled devices. The AR may perform its own host assessment, or some other system may evaluate the host. In either case, the AR’s assessment is sent to the PDP. The PDP is the brains of the operation. Based on the AR’s posture and a company’s defined policy, the PDP determines what access should be granted. In many cases, the NAC product management system may function as the PDP. The PDP often relies on back-end systems, including antivirus, patch management or a user directory, to help determine the host’s condition. For example, an AV manager would determine whether a host’s AV software and signature versions are current, and inform the PDP.

Once the PDP determines which policy to apply, it communicates the access control decision to the PEP for enforcement. The PEP could be a network device, like a switch, firewall or router; an out-of-band device that manages DHCP or ARP; or an agent on the AR itself.

NAC Cycle

When a host attempts to connect to a NAC-enabled network, there are typically three phases: pre-admission or post-admission assessment, policy selection, and policy enforcement. The criteria governing each step are based on your company’s policy and your NAC system’s capabilities.

Before you select a product, determine exactly what your company’s goals are. For example, How far out-of-date can patches or AV signatures be before a host can no longer access the network? What is the acceptable condition for a guest host before it can have access? Do you want to base access on user ID or not?

Assessment

The NAC cycle begins and ends with assessment. Pre-admission assessment occurs before a host is granted full access to the network. Post-admission assessment, after access has been granted, enables a host to be periodically reassessed to ensure it does not begin to pose a threat. Host assessment gathers information, like a host’s OS, patch levels, applications running or installed, security posture, system configuration, user login, and more, and passes it to a PDP. What information is gathered is a function of your defined policy and the NAC product’s capabilities.