



The RFP development process is a good time to make a frank assessment of your organization's security requirements

BUILDING A BETTER NETWORK ACCESS CONTROL RFP

HOW TO GET THE BEST SOLUTION FOR YOUR BUSINESS

The need to secure business networks is growing, as enterprises store more and more critical data so that key decision makers can access the network from anywhere. When considering network security solutions, many organizations are turning to network access control (NAC) technology as an integral part of their enterprise security. As the NAC industry becomes increasingly crowded, and product differentiators more obscured, organizations seeking to secure their networks find themselves with a daunting amount of information to process. Many find that stripping the question down to its most basic parts is the most useful way to proceed.

As with many industries, a good first step in the search for solutions is to issue a request for proposals (RFP). Developing a strong RFP that clearly articulates an organization's needs can be laborious, but can also pay off in the proposal review process. Competing vendors' proposals can be considered in a uniform format, and the specific replies to each well considered question makes the evaluation of each proposal more manageable.

NAC IN A NUTSHELL

Network access control helps to ensure that devices entering the network will not introduce viruses or other potentially debilitating malware. Once devices have been risk-assessed and admitted to the network, NAC continuously monitors their activity the entire time they are on the network. This pre- and post-admission model investigates the security profile of each endpoint, for example, determining whether the endpoint's firewall, OS security patches, and antivirus and anti-spyware signature files are current. Should an endpoint be non-compliant or a system threat, the NAC system can quarantine the offender so that no other systems can be infected. The NAC can also identify unknown users from those previously admitted to the network, and can apply access limitations to the unknown systems as defined by the network administrator.



The ideal solution is hardware, software, and operating system agnostic. It should also find all your networked devices, even those that don't use an operating system.

UNMANAGED DEVICES

IT managers have long been flummoxed by the challenges posed by the unmanaged devices a network must accommodate but that cannot realistically be administered by an IT staff. These devices can include partner and contractor laptops, and devices such as PDAs, POS terminals, and IP telephones. The special risks introduced by these endpoints must be mitigated by network security, but staff cannot rely on agents or signature files, since these devices either have no operating system or fall outside the purview of the IT department. When writing a NAC RFP, special attention should be paid to solutions that operate at the OSI DataLink level, one level below Network, where switches and routers operate. This allows the solution to be hardware agnostic, in other words, it can protect any network from any device, either managed or unmanaged.

NETWORK REQUIREMENTS

A robust NAC solution should be able to operate effectively regardless of the organization's existing hardware. In other words, the solution must work with any vendor's hardware regardless of model or software version. A solution that integrates with only specific switches or firewalls, and with only specific models therein, can force an organization to invest in new hardware to match the solution. When developing an RFP, be sure to ask how the network security is accomplished given your organization's network infrastructure. A good NAC solution leverages your existing hardware investment, requiring no additional investment in devices or upgrades beyond the NAC appliance.

The solution must work over a wired, optical, or wireless network, and should not require the installation of any end-user agent for proper device identification. The solution must also be able to perform any pre- and post-admission checks and quarantine any networked endpoints regardless of the operating system of the endpoint. Your RFP should direct vendors to explain how their solution supports differing operating systems and networked devices such as laptops, desktops, IP phones & call managers, servers, printers, point of sale terminals, and mobile devices.

NAC DEVICE MANAGEMENT

From time to time, in the interest of network maintenance, it's necessary for network managers to perform the types of tasks that a NAC appliance would ordinarily flag as suspicious behavior and quarantine. NAC solutions need to have the flexibility to exclude designated mission-critical and other special systems from NAC functions. Further, the NAC device must provide a dedicated port for syslog and SNMP traffic, administrative access, network device communications, and other management purposes. Should the device suffer a system failure, it must fail open to avoid creating a single point of failure in the system.

PRE-ADMISSION NETWORK ACCESS CONTROL

The pre-admission process identifies endpoints as they first attempt to logon to a protected network. This process should glean specific information about each endpoint, including whether it is accessing the network for the first time or is a known user, if the endpoint is accessing through a wired or wireless connection, the endpoint's MAC and IP address, what operating system the endpoint is using, and whether the system has stayed current with its OS security patches and anti-virus signature files. NAC systems should then be able to apply a set of user-defined parameters to determine whether the endpoint should be allowed access to the network. NAC solutions should be able to integrate with the existing endpoint authentication framework, such as RADIUS or Active Directory. Devices that fail to meet the minimum standards should be flagged for the updates and patches they need to be compliant. The NAC solution must also let network administrators determine the level of access visitor devices should be allowed.

Initial screening of endpoint devices is the best time to protect the network from noncompliant systems.

POST-ADMISSION NETWORK ACCESS CONTROL

The post-admission component of NAC is crucial to keeping a network protected. This component ensures that the endpoints that fall out of compliance after admission are appropriately contained. This aspect of NAC focuses on policy and threat monitoring. Policy monitoring applies a set of rules delineated by the network administrator about what kinds of behavior are allowed by an organization. Policies concerning instant messaging and file transfers and regulations regarding mail and other departmental rules can be programmed into the security fabric here. This component should also provide on-going

Agentless systems free your network administrators to focus on project management instead of routine maintenance

monitoring and mitigation for port scanning, mass mailer activity, and other zero day threats. Most importantly, to leverage the system cost-efficiently, the solution must not require agents or signatures to catch new threats. This ensures that the network can accommodate guest and remote users and still maintain a high level of security.

QUARANTINE AND REMEDIATION

NAC solutions must be able to automatically quarantine any device that fails an access, policy, or threat protocol. The ideal NAC solution can accomplish this quarantine without affecting other systems that are uninfected or compliant, and does not require specific network hardware or agents. When the NAC solution pulls a device off the network the device should be funneled to the remediation service appropriate to its quarantine, whether that is patch management, anti-virus and anti-spyware update services, malware removal tools, Internet-only access, or other services as defined by the network administrator. The network administrator must also have the ability to manually add and remove endpoints from network quarantine via an administrative console, and have access to the data streams emitted from devices in threat-based quarantine. Devices in quarantine should not be able to contaminate other network devices, and the quarantine function should notify the network administrator and end user when a system has been placed in quarantine and why. The system should then lead the end user through a set of remediation steps that will bring the endpoint back into compliance and allow the end user to return to the network.

The ideal NAC solution is capable of a precision quarantine that surgically removes an infected or out-of-policy device without affecting any others on the network.

REPORTING

The NAC solution must be centrally managed, providing a unified interface for endpoint administration, threat auditing, device software upgrades, and maintenance. This management interface must be able to limit configurable access for administrative controls, policy maintenance, and reporting based on the administrative permissions of those accessing the system. Ideally, the system will be able to group administrators according to their access permissions and apply restrictions to those groups rather than individual users. The solution must be able to send syslog-compliant data to one or more external syslog servers, and should support SNMP administration. The system should also provide detailed reports with data storage for a minimum of 30 days.

SUMMARY

This white paper seeks to simplify the RFP process for organizations seeking the network access control vendor that best suits their security needs. While requirements vary according to each organization's unique network infrastructure, user profile, and security expectations, some features are common to the most robust NAC solutions. Most notably, the best systems leverage an organization's existing network architecture, requiring no additional investment beyond the NAC appliance to secure the network environment. These guidelines are intended to help organizations undertake the NAC vendor assessment process with a better sense of what they should realistically expect from, and know about, prospective service providers.

Integrating network access control into your security fabric can be one of the most effective means of protecting your organization's data investment.