

Use this checklist to validate NAC solutions you're considering. Ensure that they provide the full scope of NAC and LAN security, so you solve tomorrow's problems as well as today's.

APPLICATION SOLUTION BRIEF: **NAC CHECKLIST**

NAC Checklist

What to Look for in an Effective LAN Security Platform

- ♦ Knowing who's on the LAN.
- ♦ Providing guest access.
- ♦ Limiting contractors.
- ♦ Controlling what users can do on the LAN.
- ♦ Segmenting the LAN.
- ♦ Documenting and auditing user activities.

There are as many reasons to do NAC and secure the LAN as there are ways to do it. In fact, with so many approaches to NAC, it's hard to evaluate potential solutions. One element to keep in mind is that LAN security is a process – what drives you to implement a solution today may represent only a piece of your total security needs in the future. It's critical to consider how your LAN security will evolve over time.

Use this checklist to validate that the solutions you're considering. Ensure that they provide the full scope of NAC and LAN security, so you solve tomorrow's problems as well as today's.

Easy Integration and Network Independence, with Standards-Based Deployment

- ✓ Can the solution drop into your existing LAN, without changes to the endpoints, switches, VLANs, ACLs, and identity stores?
- ✓ Is the system self-contained, avoiding dependence on dynamically reconfiguring switches for enforcement?
- ✓ Does the solution operate independently of a centralized policy server?
- ✓ Can you "turn off" the system for troubleshooting

without affecting network operation?

- ✓ Does the system support high-availability deployments and provide redundant power supplies?

SIMPLE AUTHENTICATION

- ✓ Does the solution leverage existing authentication databases, such as Active Directory, RADIUS, and LDAP, without any changes?
- ✓ Can you use multiple authentication mechanisms, including 802.1X and captive portal, regardless of user location, but also allow users to log into the network the same way they always have, such as to a Windows Domain?
- ✓ Does the solution make LAN authentication easy, allowing IT to leverage 802.1X where it's installed or avoid 802.1X supplicant interoperability issues where it's not?
- ✓ Does the system provide a way for non-user devices (such as printers or VoIP phones) to be authenticated onto the network but still controlled?
- ✓ Does the system require an agent for endpoints to be authenticated and controlled?

EFFECTIVE POSTURE CHECK

- ✓ Does the system scan machines both before and after admission to the LAN?
- ✓ Can you run these checks on managed and unmanaged devices?
- ✓ Can the solution leverage existing best-of-breed endpoint agents for managed solutions?
- ✓ Does the scan include more than just a simple check that certain software is installed, actually looking for the presence of adware or spyware or for specific Windows Registry values?

- ✓ Can you configure the solution to scan only certain machines, based on IP address or group membership?
- ✓ Can the scan take place without needing admin login credentials on the endpoint?

COMPLETE LAN VISIBILITY

- ✓ Can the system audit and monitor all traffic, tied to a username, to speed incident response?
- ✓ Can you audit traffic on a per-user, per-application basis for compliance with regulations such as PCI, HIPPA and S-Ox?
- ✓ Can you set up access policies but have the system just log events, giving you a way to test your policies without impacting users or business processes?
- ✓ Can you easily look into any security violation, immediately knowing the user involved and the policy that was violated?
- ✓ Can the solution provide application-level inspection at Layer 7 rather than simple SNMP or NetFlow statistics?
- ✓ Can you easily compile aggregated data to provide LAN activity reports to management and to demonstrate compliance?

COMPLETE POST-ADMISSION CONTROL OF USERS

- ✓ Does the system see all traffic after users are on the LAN, to control user access and protect against threats?
- ✓ Does the system make it easy to apply policies based on a user's identity and role in the organization?
- ✓ Can you set both universal and context-based controls, where one policy could span wired, wireless, VPN, or local connections and another could limit access from remote locations, for example?

- ✓ Can you control user access to servers and to applications without any other tools, such as VLANs/ACLs, and does the system enable Layer 7 identification of applications instead of just Layer 4?
- ✓ Does the system let you see and control application content, such as file names in Microsoft File Services (CIFS), FTP, or IM transactions or HTTP content such as URLs?
- ✓ Does the system provide control close to the user's point of entry on the LAN?
- ✓ Does the system protect against evasion by a user applying a static IP or MAC address?

ZERO-DAY MALWARE CONTAINMENT

- ✓ Does the system provide a means for continuously detecting and blocking new, unknown attacks, without dependence on signatures and without hindering network performance?
- ✓ Can you decide whether to block just the infected application or everything coming from an infected user?

PROTECTION OF CRITICAL APPLICATIONS

- ✓ Can the system extend beyond users to also protect vital services such as a voice over IP (VoIP) call manager?
- ✓ Does the system apply application-based policies to prevent non-user devices from being used for attacks, such as controlling that a printer can send only printing protocols?

WIRE-SPEED LAN PERFORMANCE

- ✓ Can the system provide full policy enforcement without slowing down your users?

ABOUT CONSENTRY NETWORKS

The ConSentry Networks Intelligent Switching architecture delivers native user and application control at the LAN access edge. With this technology, ConSentry's award-winning LANShield switch product family enables IT managers to improve the visibility, control, and performance of users and applications and radically simplify security, LAN deployment and operations. ConSentry is backed by blue-chip venture capital firms Accel Partners, DAG Ventures, INVESCO Private Capital, and Sequoia Capital and is headquartered in Milpitas, California.

Corporate Headquarters
 ConSentry Networks
 1690 McCandless Drive
 Milpitas CA 95035
Phone 408.956.2100
Fax 408.956.2199
Toll-Free 866.841.9100
 Email info@consentry.com
www.consentry.com

Worldwide Locations
 London, United Kingdom
Phone +44 (0) 00870 351 9494
 Frankfurt, Germany
Phone +49 69677 33 4
 Tokyo, Japan
Phone +813 5532 7630

For a complete listing of all our office locations go to:
www.consentry.com/company.html

