

Network Admission Control

How ConSentry Networks Delivers the First Line in LAN Security Defense



Contents

Introduction	2
NAC: A Two-Pronged Defense	3
NAC Requirements for User Authentication	3
NAC Requirements for Host Posture Check	3
ConSentry Networks' Comprehensive NAC	3
The ConSentry Approach to User Authentication	4
The ConSentry Approach to Host Posture Check	5
Holding the Line	6
About ConSentry Networks	7

Introduction

Local area networks (LANs) are more open than ever, making them vulnerable to external as well as internal threats and posing a complex security challenge for enterprises. For example, contractors and partners need access to corporate resources and to the Internet. Likewise visitors, including vendors, have come to expect Internet access while on site. Wireless technology and open jacks, such as those found in conference rooms, make it easy for rouge hosts to connect to a network. At the same time, mobile employees with laptops rove between public Internet "hot spots" and the protected LAN, potentially exposing the network to viruses and other malware.

Unfortunately the number and type of security threats continues to rise. Enterprises face escalating losses from successful attacks, both in dollars and corporate reputation. Consequently, IT is looking for a comprehensive LAN security solution that protects business information, improves business continuity, and helps the organization comply with governmental regulations.

LAN security is a multi-faceted problem, requiring a multi-faceted solution. The first line of defense is to control who and what attaches to the LAN. Controlling access via network admission control (NAC) is fundamental. But post-admission controls are even more essential, so in addition to NAC, a LAN security solution needs to encompass these other areas:

- » **Visibility** – IT needs the ability to see all LAN traffic on a per-user, per-flow basis up to L7, including details within L7 such as the URL involved in an HTTP session or the file name involved in an FTP download. Comprehensive traffic visibility is a pre-requisite for access control and auditing.
- » **User access control** - NAC provides no control over where users go or what resources they access once they're admitted to the network, so IT also needs user-based, post-admission access control. Specifically, IT needs role-based provisioning, the ability to define rights and permissions based on a user's role in the organization. Role-based provisioning provides universal access control, ensuring that the correct rights and permissions apply universally, regardless of a user's access medium or location.
- » **Threat control** - IT needs effective protection against external as well as internal threats, both known and unknown. An effective LAN security solution must detect malware – even malicious code never seen on the network before – and prevent it from propagating. A LAN security solution must alert IT to any unusual behavior and be able to block it, whether it's a zero-day worm, a rogue user connecting in, or an attack launched from a printer or VoIP phone or their ports. And, a LAN security platform must detect and block other sources of threats, such as invalid protocol headers which might indicate an attack.

Given NAC's critical role as a first line of defense, this paper will detail the requirements for a robust NAC solution and ConSentry Networks' comprehensive offering.

NAC: A Two-Pronged Defense

Controlling access to the LAN entails controlling both who connects to the network and the machines they use. For NAC to be an effective first line of defense, it must encompass both

- » user authentication; and
- » host posture check.

Enterprises need to verify that users are who they say they are and that the machine they're using to enter the LAN complies with corporate standards, running an approved operating system with current patches and fixes and an updated anti-virus program. Without both sets of admission controls, authorized users may unwittingly unleash malware that anti-virus software would have removed from their laptop. To ensure that a NAC solution meets enterprise needs, user authentication and host posture check offerings should meet the following requirements.

NAC Requirements for User Authentication

Comprehensive user authentication must include:

- » **Ability to support both passive and active authentication.** Passive authentication, such as tracking users logging into the Windows domain, is most often used to support employees and other known users, while active authentication, such as captive portal, is typically the authentication mechanism for guests and other non-employees and is important for intercepting rogue users. A NAC solution must support both mechanisms to ensure consistent authentication enforcement regardless of user identity or the point of entry into the network. A NAC solution must also be able to block users who fail authentication from getting onto the LAN.
- » **Flexibility to work with multiple identity stores for authentication.** Enterprises vary in their deployments of identity stores. Some organizations, for example, maintain RADIUS servers as well as directory services such as Microsoft's Active Directory or Lightweight Directory Access Protocol (LDAP)-compliant directories.
- » **Ability to identify a user's role as part of authentication.** Authentication provides the ideal opportunity to learn key information about users, such as their organizational role, for security purposes. Determining a user's role during authentication is essential for instantly applying control policies to that user following admission to the network.

NAC Requirements for Host Posture Check

Full featured host posture check must offer:

- » **Ability to provide ubiquitous, easy to administer host posture check.** Given the critical nature of host posture check, it should apply to all classes of users, including employees, contractors, and visitors. A host posture check solution should be easy to deploy and maintain so as not to burden the IT staff.
- » **Support for host posture check on hosts not under enterprise control.** Contractors, partners, guests, and other non-employees often use their own computers when accessing an enterprise's LAN. Enterprises need the ability to protect themselves against non-compliant hosts, such as a guest's laptop, that might unleash a worm or other malware onto the network.
- » **Ability to work with multiple NAC agents or architectures.** As with identity stores, IT may find itself with a mixed deployment of host posture check agents or may need to accommodate one method for employees and another for non-employees. Likewise, host agents can change over time. Whatever the circumstances, a NAC solution must work with multiple host agents and NAC architectures, enabling IT to decouple the network enforcement portion of NAC from desktop decisions.

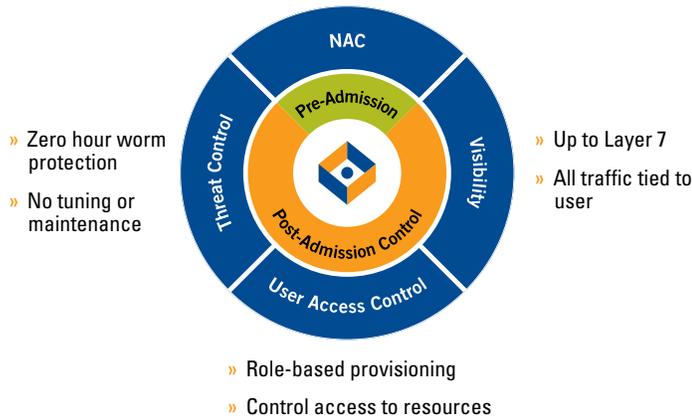
ConSentry Networks' Comprehensive NAC

ConSentry Networks delivers NAC as part of a comprehensive set of LAN security services supported by its LANShield product family, which includes the LANShield Switch and the LANShield Controller. This powerful combination of hardware and software operates at LAN speeds to secure every port and control every user on the LAN. At the heart of ConSentry's devices is the LANShield™ silicon architecture. Comprised of a 128-core processor and custom traffic-processing programmable ASICs, this flexible architecture provides stateful deep packet inspection and flow-based traffic tracking and control.

The LANShield operating system (OS) drives the silicon and provides traffic and malware controls. It also performs a three-way binding of IP address, MAC address, and user identity information gleaned during authentication to support user-based traffic tracking and role-based provisioning. Through the InSight command center's graphical interface, IT can get at-a-glance views of network usage and security violations and can set global access policies and perform incident response.

The LANShield platforms provide:

- » Authentication
- » Host posture check



» **Network admission control (NAC)**

ConSentry supports NAC by leveraging an organization’s existing AAA servers and identity stores as well as its host integrity infrastructure. Where applicable, the LANShield device can actively participate in user authentication and host posture checks.

» **Visibility**

A Layer 2-7 aware device, the LANShield platform provides in-depth packet inspection with full L7 application decode, so it can distinguish between applications using the same L4 port or attempting to mask themselves using a port number not typically associated with that application. The platform can filter traffic based on packet contents, and by binding a user’s name to IP and MAC addresses, the LANShield product family can track LAN traffic by individual users as well as user group, application, host or other resources, protocol, L4 port, transaction, or file access.

» **User access control**

The LANShield products can apply access controls to everything they see. The platform gives IT the ability to define policies that limit a user’s access to networked resources based on his or her role in the organization. This role-based provisioning applies universally, regardless of where or how a user connects to the network.

» **Threat control**

The LANShield devices protect against both known and unknown threats, providing more accurate detection with blocking at a finer level of granularity, such as by URL, than security tools operating at lower layers. Incident reporting is based on knowledge of user transactions, and the LANShield platform can stop traffic on a per-user or per-application basis if malware is detected. Attempts to use printers or VoIP phones as a launch point for attacks are also prevented by limiting the

protocols those devices can run and the network destinations they can reach.

As a full-featured LAN security platform, ConSentry’s LANShield products provides a robust NAC solution, meeting all the requirements for user authentication and host posture check.

The ConSentry Approach to User Authentication

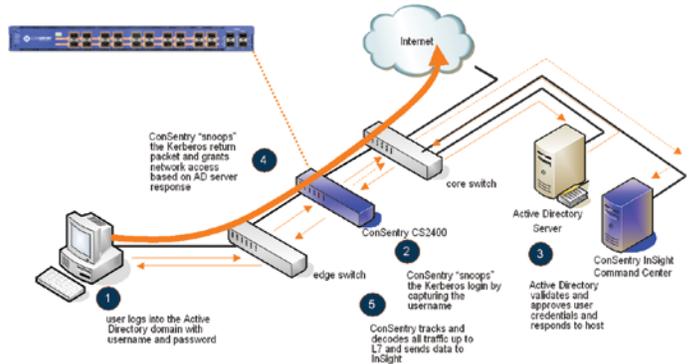
The ConSentry LANShield device offers:

» **Ability to support both passive and active authentication.**

The LANShield platform supports both passive and active authentication. In both cases, a client machine attaching to the network is provided only essential network services, such as access to DNS, DHCP, and authentication servers, until the client successfully authenticates.

With passive authentication, ConSentry leverages existing AAA servers and identity stores, using the LANShield devices’ deep packet inspection to identify and decode authentication requests and responses between client machines and back-end identity stores, such as Active Directory or RADIUS servers.

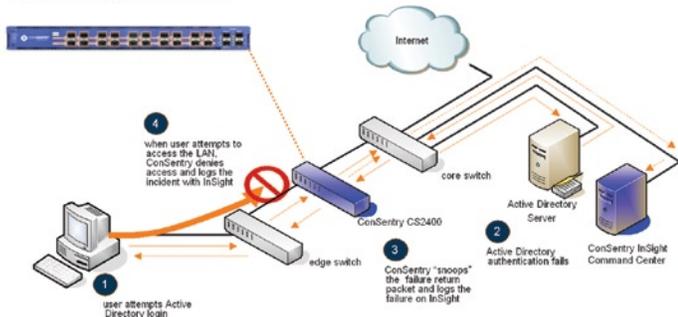
Authentication – Active Directory



In the case of Active Directory, for example, the LANShield platform decodes Kerberos packets and checks to see if the client is issued a ticket indicating that authentication is successful. The LANShield platforms can also support passive authentication to Active Directory in conjunction with RSA Security tokens.

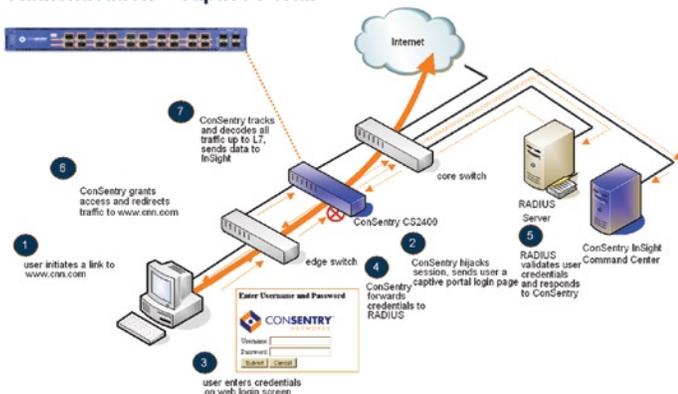
For RADIUS, the LANShield device parses the RADIUS packets to track user name, password, and authentication status. Only if authentication is successful is a client given network access beyond essential services.

Authentication Failure



ConSentry also supports active authentication in which the LANShield device actively challenges a user for authentication information via a browser-based captive portal. Organizations that cannot take advantage of passive authentication may use this approach, or it could apply to users not subject to passive authentication, such as a guest attempting to connect to the network. With captive portal, the LANShield platform challenges users for their username and password via a web redirect. Organizations can provide visitors with a guest login name and password, for example, to retain control over who can come onto the LAN while not having to create distinct logins for each guest. That guest ID would likely have an associated access policy for post-admission control, such as being relegated to Internet-only access.

Authentication – Captive Portal



- » **Flexibility to work with multiple identity stores for authentication.** ConSentry supports Active Directory and RADIUS today and will support other identity stores that implement the Lightweight Directory Access Protocol (LDAP) in a future release.
- » **Ability to identify a user's role as part of authentication.** The ConSentry platform determines a user's role in one of three ways: by parsing the RADIUS authentication packets, by querying an identity store such as AD, or by using rules that derive the role based on authentication process attributes such as time, location, or username. ConSentry learns a user's role or group identity as part of authentication. For example, in the case of passive authentication via an Active Directory server, the LANShield products learn the user's group identity via a

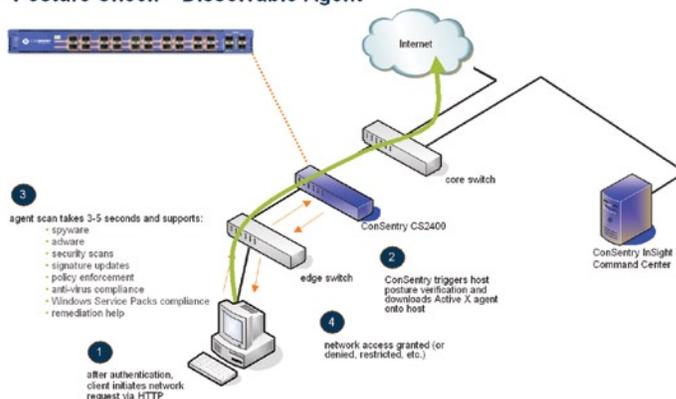
query to AD. With RADIUS, a user's role resides in the RADIUS server as a vendor-specific attribute (VSA) and is learned during authentication. With active authentication, the LANShield device validates a user's identity against a RADIUS server or other identity store and learns the user's role as part of that process.

The ConSentry Approach to Host Posture Check

ConSentry provides complete host posture check, including:

- » **Ability to provide ubiquitous, easy to administer host posture check.** To ensure that all systems are subject to a host posture check, ConSentry offers enterprises a dissolvable agent. Each time a user attempts to connect to the network, the LANShield device loads the ConSentry dissolvable agent as soon as the user launches a browser.

Posture Check – Dissolvable Agent



The ConSentry dissolvable agent is an Active X or Java applet that performs a complete compliance check on the host. It checks for compliant Windows Service Packs and Hotfix versions; anti-virus compliance checking; spyware detection, disablement, and logging; and adware detection.

IT has the flexibility to define the appropriate access policy based on the outcome of the host posture check; the LANShield platform enforces these policies, including preventing admission for non-compliant systems, if appropriate. In addition, IT can define remediation policies for non-compliant systems that indicate to the users why their login system failed and how to bring their system into compliance. The necessary remediation steps would appear in the same browser window on the user's desktop.

For example, IT can provide users with links to external web sites, such as Microsoft's or Symantec's, to obtain the necessary operating system or anti-virus software updates. Alternatively, IT can redirect users to an internal server to download a patch or update. Or IT can directly help users. Because the LANShield device provides essential network services regardless of authentication or host posture check status, users who

fail a host posture check can be assisted remotely by IT staff using desktop tools such as LANDesk, BigFix, and others.

In addition to providing ubiquitous host posture check, the ConSentry dissolvable agent simplifies deployment of compliance checks. With the dissolvable agent, any dependency on a specific desktop agent is removed, so IT is able to decouple the decisions about network enforcement and desktop agents for NAC. Likewise, ConSentry's dissolvable agent eliminates the need for IT to commit to, deploy, and manage another piece of desktop software or complex back-end posture check servers.

- » **Support for host posture check on hosts not under enterprise control.** Because any host connecting to the network poses a security risk and must be subject to a host posture check, ConSentry provides its dissolvable agent as a means for IT to apply a host posture check to hosts not under its control.
- » **Ability to work with multiple host agents.** In addition to supplying its dissolvable agent, ConSentry is committed to supporting third-party NAC architectures and host posture check agents. ConSentry plans to support Microsoft's Network Access Protection (NAP) and agents that comply with the Trusted Computing Group's Trusted Network Connect (TNC) specification.

Holding the Line

As part of an overall LAN security solution, ConSentry's comprehensive approach to NAC gives IT a solid first line of defense against potential security attacks. ConSentry's NAC services interoperate with a broad cross-section of authentication and host posture check systems, enabling enterprises to leverage their existing infrastructure. In addition, by providing active authentication and a dissolvable agent, ConSentry simplifies NAC deployment while ensuring that all desktops — including those not under IT's control — are subject to admission controls.

In addition, ConSentry's NAC solution integrates with other security services supported by the LANShield product family, providing the user role information that underpins role-based provisioning. Only ConSentry offers a comprehensive LAN security platform that brings together network admission control, full LAN visibility, user access control, and threat control in a single device, allowing organizations to secure the LAN as never before.

About ConSentry Networks

ConSentry Networks delivers comprehensive LAN security, enabling businesses to protect their corporate assets, ensure continuity of operations, and dramatically reduce the risk of security breaches. ConSentry enables this pervasive security while lowering IT's cost of operations through its flexible, high-performance platform powered by ground-breaking custom silicon and revolutionary LAN security software. Backed by blue-chip venture capital firms that include Accel Partners, INVESCO Private Capital, and Sequoia Capital, ConSentry is headquartered in Milpitas, California. For more information, visit the company's web site at www.consentry.com.

Corporate Headquarters

ConSentry Networks

1690 McCandless Drive
Milpitas CA 95035

Tel: 408-956-2100

Toll-Free: 866-841-9100

Fax: 408-956-2199

Email: sales@consentry.com

Germany Office

ConSentry Networks

Lyoner Strasse 26 D-60528
Frankfurt Germany

Tel: +49 69 677 33 422

Fax: +49 69 677 33 200

United Kingdom Office

ConSentry Networks

Lakeside House 1, Furzeground Way
Stockley Park, Heathrow, UB11 1BD

Tel: +44 (0) 2086 22 3020

Fax: +44 (0) 2086 22 3200

Japan Office

ConSentry Networks

Hibiya Central Bldg. 14F
1-2-9, Nishi Shinbashi, Minato-ku
Tokyo 105-0003 Japan

Tel: +813-5532-7630

Fax: +813-5532-7373