TECHNOLOGY SOLUTION BRIEF

User Access Control

How ConSentry Networks Delivers Role-based Provisioning

CONSENTRY NETWORKS

Contents

Introduction

Securing the LAN is a multi-faceted problem. Many organizations are taking the first step by deploying network admission control (NAC) to ensure that only authenticated users operating compliant machines are allowed onto the network. But what happens after that? How does IT control what applications users run and what file servers and other resources they access? IT needs tools to limit access to critical data and throttle or block non-business applications.

Given escalating security threats and their potential costs to business, IT needs more than NAC – they need the ability to control where users go on the network and what they do, whether users are internal employees, contractors, or simply guests. Such user access control is necessary to safeguard corporate data and other assets as well as to comply with government and industry regulations.

Currently, many security systems tie access control to IP or MAC addresses. However, IP and MAC addresses are not people; it's common for a single user to operate both desktop and laptop machines, for example, or for one machine to be shared by multiple users. IP and MAC addresses can be compromised, and more importantly, they change frequently.

Instead, the user must be at the heart of access control, giving IT the ability to control resource usage based on a user's group association or role within the enterprise. With role-based provisioning, IT can move away from the "default allow" model that has dominated LAN security and migrate closer to the more secure "default deny" model that has dominated perimeter security. Only when IT has comprehensive LAN visibility to see what's happening and the granular controls based on user identity and role can they restrict access appropriately.

User access control is only part of a total LAN security solution. A comprehensive LAN security solution needs to encompass these additional areas:

- **Network admission control (NAC)** – Controlling admission to the LAN entails controlling both who connects to the network and the machines they use – in other words, user authentication and host posture check.
- **Visibility** – IT needs the ability to see all LAN traffic on a per-user, per-flow basis up to Layer 7, including details within layer 7, such as the destination URL in an HTTP session or the file name involved in an FTP download. Comprehensive traffic visibility – into all flows, too, not just sampled data – is a prerequisite for access control and auditing.
- **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 or data retrieval effort launched from a printer or voice over IP

(VoIP) phone. And, a LAN security platform must detect and block other sources of threats, such as invalid protocol headers which might indicate an attack.

Because user access control is the linchpin for role-based provisioning, this paper will detail the requirements for a comprehensive user access control solution and ConSentry Networks' full-featured offering.

User Access Control: Gateway to Role-based Provisioning

Properly implemented, user access control can be a powerful tool, giving IT a rich and flexible way to define and enforce role-based policies. As a baseline, a user-based access control system must:

» **Tie all LAN activity back to specific users**. By definition, user-based access control must link all traffic on the LAN to the individual users generating it.

» **Support universal access control**. A user access control system must ensure that the correct rights and permissions are applied to each user universally, regardless of the user's access medium or location. That is, the same set of access rights must apply whether users access the LAN via a wired or wireless connection and whether they're attaching locally or remotely via a virtual private network (VPN).

User access control is implemented via policies, which consist of decision filters and the actions to be taken once those filters are observed. Using policy-creation tools, IT managers define filters creating an association between specific resources and specific users or sets of users; then they specify what action should be taken on those filters, such as allowing or denying access or redirecting a user's traffic. For example, IT could define a policy that lets users in engineering access a code-development server and edit files on it but prevents those users from copying files from that server. In the event a user attempts to copy a file, that action will be denied. Once policies are defined, they are downloaded to enforcement devices, which monitor LAN traffic for defined filters and take action accordingly.

Policy creation and enforcement are the mechanisms for user access control; they must provide a rich set of functionality and therefore have their own requirements.

Policy Creation Requirements

A policy creation tool must meet the following requirements:

» **Ease of use**. Policy creation requires an easy-to-use, GUI-based tool. To simplify policy creation, a policy tool must provide templates that IT can use out of the box or modify to meet enterprise needs. The LAN security platform should also include wizards to further streamline policy creation. To support role-based policies, a policy creation tool must also have the ability to extract role information from existing identity stores, such as Active Directory, RADIUS, or Lightweight Directory Access Protocol (LDAP)-compliant directories.

» **Centralized policy creation and distribution capability**. To ensure consistency and simplify deployment, IT needs the ability to create policies centrally and then distribute them to enforcement devices at the appropriate geographic locations throughout the enterprise. For example, IT must be able to define a set of policies for sales personnel and easily push those policies to enforcement devices in all sales offices.

» **Support a rich, flexible set of policies**. A policy creation tool must give IT the ability to define various types of policies, including conditional and cascading policies. And it must support a broad range of decision filters with which IT managers can create policies, including:

- **user** – both individual and by group/role;
- **application** – individual applications as well as groups of applications;
- **applications and content at Layer 7 and above** – enables IT to define policies for applications that use the same L4 port, for application content, and for application attributes;
- **MAC address** – including individual addresses and ranges of devices with the same initial portion of MAC address;
- **IP address** – including individual IP addresses and IP address ranges;
- **TCP and UDP ports;**
- **network destination and/or zone** – such as a particular collection of servers; and
- **location**.

Policy Enforcement Requirements

A policy enforcement device must meet the following requirements:

» **Be deployed in-line**. Enforcement devices must inspect all user traffic for filters and apply actions at LAN speed. Enforcement devices that operate out of band, such as on a span port, cannot effectively control user traffic and certainly cannot maintain LAN-speed throughput. Ultimately, the decision must be made in a single box. Devices that are retrofitted to support policy enforcement, relying on a "brain" in another device out of band, cannot make enforcement decisions fast enough to maintain LAN-speed performance.

» **Learn user identity**. User identity is the basis for user access control; therefore, an enforcement device must be able to learn user identity information to enforce policies on a per-user basis. To avoid burdening the IT staff with manually populating identity information, the enforcement platform must have the ability to learn user identity from third-party databases such as Active Directory, RADIUS, or LDAP-compliant directories.

» **Extract user role data from third-party identity databases in real-time**. In addition to user identity, enforcement devices must also be able to extract user role information from third-party stores to avoid manual effort and to enable role-based provisioning.

» **Tie user to policy**. To enforce user- and role-based policies, an enforcement device must have the ability to link all traffic on the LAN to the individual users generating it and match that traffic against decision filters.

» **Recognize a wide range of policy filters**. An enforcement device must be able to recognize the full range of policy filters defined in the policy creation tool, including those based on user and role, applications and content at Layer 7 and above, MAC and IP addresses, network destinations and/or zone and, location.

» **Apply rich enforcement actions**. An enforcement device must be capable of executing a range of enforcement actions on the filters it sees, including:

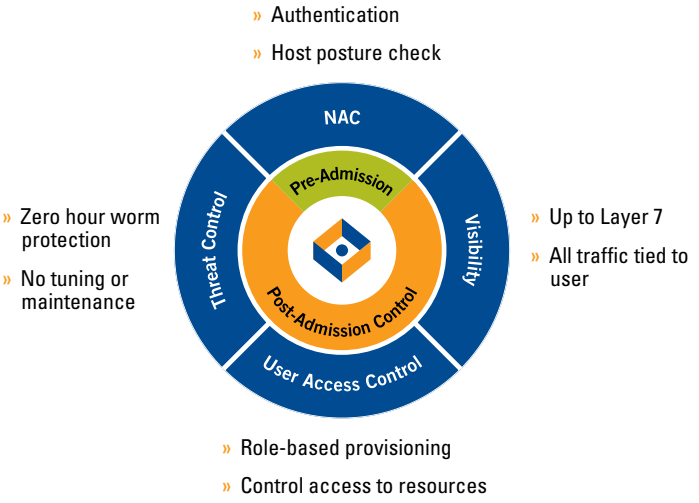
- **permit/deny traffic**
- **log activity**
- **mirror traffic**

ConSentry Networks' Comprehensive Security Approach

ConSentry Networks delivers user access control 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 control every user and secure every port 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 at gigabit speeds.

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 set global access policies, get at-a-glance views of network usage and security violations, and perform incident response. InSight compiles information based on knowledge of user transactions, presenting IT with the user's name tied to all activities and access violations.

The LANShield platforms provide:



» **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 device provides in-depth packet inspection with full Layer 7 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 devices 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 network destinations they can reach.

ConSentry Delivers Robust User Access Control

You can't control what you can't see. Therefore, ConSentry engineered the LANShield product family from the ground up to provide real-time user-based visibility of LAN traffic. As a result of this granular view of traffic, ConSentry can address the spectrum of requirements for user access control, beginning with the ability to:

» **Tie all LAN activity back to specific users.** Through its Layer 2-7 awareness and deep packet inspection, the LANShield device binds an IP and MAC address to a user name and ties all LAN activity back to specific users, including application flows, files opened and closed, and the use of printers, VoIP phones, and other resources.

» **Support universal access control.** Because the LANShield platform ties all LAN activity to users, access control is applied to users regardless of how they connect to the network. The same set of access rights apply whether users access the LAN via a wired or wireless connection and whether they're attaching locally or remotely via a VPN. Alternatively, if IT wants to alter policy based on location, that option is available as well.

ConSentry allows IT managers to define policies using the full range of traffic characteristics the LANShield device sees and to limit users' access to networked resources based on their role in the organization. The ConSentry platform's robust role-based provisioning easily addresses the requirements for policy creation and enforcement.

Meeting Policy Creation Requirements

ConSentry's InSight command center fully meets the following policy-creation requirements:

» **Ease of use.** ConSentry's InSight command center features a graphical interface with policy templates that greatly simplify policy creation. In a typical scenario, for example, IT could use a pre-defined ConSentry template to define a policy to log file transfers based on FTP or Windows file sharing, for example. The InSight GUI presents tabs that follow a workflow process, so for controlling file transfers, InSight would walk the IT staff through the process of naming a list of file servers (or network destinations) and a list of attributes to be controlled, such as which usernames could work on a file; file names to control; and the type of file activity (copy, open, close, delete) allowed. IT then applies the policy to the appropriate user roles and locations in the organization.

In addition to these ease-of-use features, InSight streamlines policy creation by pulling username and role information from third-party identity stores. Currently ConSentry supports Active Directory and RADIUS and will soon support LDAP-compliant directories.

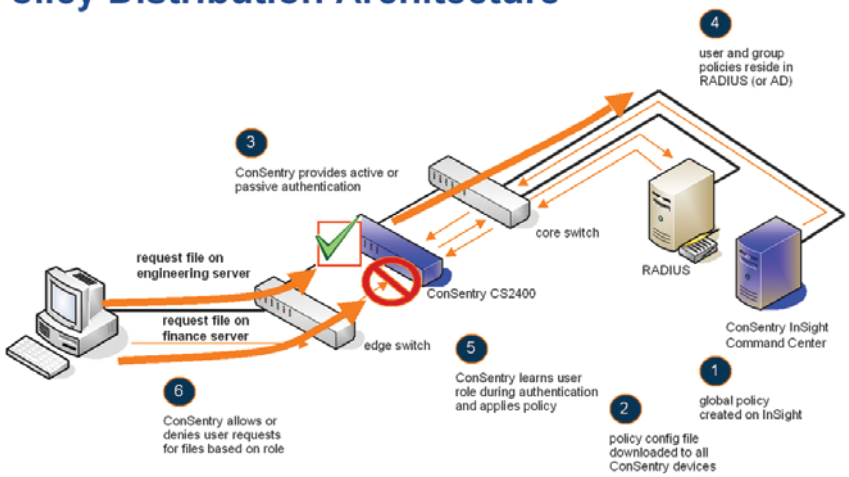
» **Centralized policy creation and distribution capability.** IT defines policies centrally within InSight and then distributes them via a ConSentry protocol to LANShield devices at the appropriate geographic locations across the enterprise. With InSight, IT can create role-based and location-specific policies. For example, IT could define one set of policies for the company's Denver office and another set for the New York office.

» **Support a rich, flexible set of policies.** InSight supports a rich set of policies by leveraging key capabilities of the LANShield platforms. Deep packet inspection with full Layer 7 application decode enables the LANShield device to distinguish applications on the same L4 port from each other and to see the content in the data portion of packets, such as specific FTP file

names. The LANShield product family's ability to bind a user's name to IP and MAC addresses allows the LANShield device to track each user's traffic on a per-flow basis. As a result, IT has the flexibility to define a variety of policies, including conditional and cascading policies, using a broad range of policy parameters. For example, a user may be in several groups, such as employee, engineering, software engineering. IT may have created policies for each of these groups, and the ConSentry platform can apply them hierarchically, with the highest ranked policies, as set by IT, taking precedence. These policy parameters include:

- **user** – both individual and by group/role;
- **application** – individual applications such as Firefox as well as groups of applications such as all web browsers;
- **applications and content at Layer 7 and above** – including applications that use the same L4 port such as web browsing and SAP both running on Port 80; application content, such as specific FTP files; and application attributes, such as the file name in a CIFS (Windows file sharing) transaction;
- **MAC address** – including individual addresses and wildcard ranges that start with the same addressing info, such as a collection of VoIP phones;
- **IP address** – including individual IP addresses and IP address ranges associated with a cluster of devices;
- **TCP and UDP ports** – ConSentry can track applications by port number, though the platform also decodes applications to recognize port-hopping or cloaking applications;
- **network destinations or zones** – including a collection of resources such as the finance servers; and
- **location** – ConSentry supports cascading locations, including global, regional, building, device, and port.

Policy Distribution Architecture



Meeting Policy Enforcement Requirements

ConSentry can then enforce policies, meeting the following requirements:

» **Deploy in line.** With 10 Gbps of throughput and latency averaging 30 microseconds, the LANShield platform operates at line-rate within the LAN. The LANShield Switch is deployed in the wiring closet, and the LANShield Controller is deployed in-line between wiring closet switches and core switches/routers. The LANShield's custom CPU and programmable ASICs enable it to inspect all traffic, match that traffic against policy filters, and apply policy enforcement actions at LAN speed.

» **Learn user identity**. The LANShield platform learns the user's identity during authentication, either passively by "snooping" the AD login or actively via captive portal.

» **Extract user role data from third-party identity databases**. In addition to learning the user names, the LANShield device learns a user's role or group either during or immediately following the authentication process. With Active Directory, for example, the LANShield platform obtains role information via a query to Active Directory. With RADIUS, a user's role resides in the RADIUS server as a vendor-specific attribute (VSA) and is learned during authentication.

» **Tie user to policy**. ConSentry's stateful deep-packet inspection allows it to associate user traffic with specific policies. With its powerful programmable ASICs, the ConSentry hardware monitors all traffic to and from each user, tracking each flow and the policies that apply to that user. Because it tracks hierarchical role information, such as

employee
➔ engineering
➔ software engineering,

the LANShield platform enforces policies hierarchically.

» **Recognize a wide range of decision filters**. Taking policies defined in InSight, the LANShield OS instantiates these filters within the LANShield hardware. Deep packet inspection and stateful tracking of traffic enable the LANShield device to recognize the full range of policy filters defined in InSight, including those based on user and role; applications and content at Layer 7 and above; MAC and IP addresses; network destinations and/or zone; and location.

» **Apply rich enforcement actions**. The LANShield platform's powerful hardware and comprehensive feature set allow it to apply a complete range of enforcement actions, including:

- **permit/deny traffic** – allow or deny user access to resources at a granular level, including permit or deny traffic associated with a specific user, connection, application, protocol, host, or location.
- **log activity** – capture and record all packets associated with a session for auditing, forensics, and other record-keeping purposes.
- **mirror traffic** – for purposes of additional analysis; for example, IT may use a span port to send mirrored traffic that matches the profile of a worm to an IDS/IDP system.

Foundation for Control

User-based access control provides the foundation for IT to implement role-based provisioning, allowing IT to move toward a "default deny" security model on the LAN. Only when IT has granular visibility and control based on user identity can they constrain authorized users to approved resources and quickly identify and control out-of-bounds traffic.

Through its rich policy creation and enforcement capabilities, ConSentry Networks gives IT the ability to define rights and permissions based on a user's role in the organization, ensuring post-admission access control is applied universally. Only ConSentry, with its powerful LANShield hardware and software, can provide real-time user-based visibility and control of network traffic. Coupling user access control with network admission control, full traffic visibility, and threat control, ConSentry offers a comprehensive LAN security platform that allows 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

EMEA Office

ConSentry Networks
Lyoner Strasse 26 D-60528
Frankfurt Germany

Tel: +49 69 677 33 422
Fax: +49 69 677 33 200