TECHNOLOGY SOLUTION BRIEF

Comprehensive Visibility

How ConSentry Networks Provides the Foundation for LAN Security

CONSENTRY NETWORKS

Contents

Introduction

Visibility into LAN traffic is fundamental to LAN security – you can't control what you can't see. It also informs a range of other management activities, including incident response, auditing, and trend analysis. Without complete visibility into all flows on the network, companies cannot prevent unauthorized access; control what users access once they're admitted to the network; track security incidents for troubleshooting, auditing, and compliance; or quickly identify and contain malware.

To date, instrumenting LANs for complete traffic visibility has been prohibitively expensive – full visibility into switched networks would demand specialized probes on each LAN segment. Consequently, most companies rely on data sampling technologies built into network switches and routers to glean some insight into LAN activity. However, this data is difficult to interpret because it's presented at Layer 3 and consists of IP address and port information, with no direct view of users or applications. As a result, most IT shops export that sampled data to third-party analysis engines. Once the data is analyzed, IT must then decide upon a course of action and manually implement that action. In many cases, the data is too limited, or the interpretation of it comes too late, for effective action.

In today's rapidly evolving security environment, IT needs full visibility into LAN traffic, delivered in an intuitive GUI that focuses on exceptions and relevant incidents. IT also needs the visibility platform to be capable of immediately invoking controls based on policy violations. Visibility enables control and is the foundation for LAN security. However, visibility is only part of a total LAN security solution. A comprehensive LAN security solution must also 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. NAC is a good first-line defense, with many host posture check products assessing the status of OS patch levels and host anti-virus software, for example.
- **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 controls. Specifically, IT needs role-based provisioning, the ability to define rights and permissions – as well as control and enforcement actions – based on a user's role in the organization. Role-based provisioning provides universal access control, ensuring that the correct rights and permissions are applied 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-hour attack, a rogue user connecting in, or an attack 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.

Given the foundation role that visibility plays in LAN security, this paper will detail the visibility requirements for a LAN-based security solution and ConSentry Networks' comprehensive LAN visibility and security offering.

Visibility Leads to Control

To be effective, a LAN security platform must provide visibility into LAN traffic in a way that's useful to IT and allows for appropriate levels of control. While auditing requires the tracking and storage of large volumes of data, day-to-day security management depends on having information about significant events highlighted and acted upon.

Rather than reams of raw data, which are hard to process or act on, more valuable to IT is the ability to manage by exception – to have visibility into what has changed on the network or what has happened out of the ordinary, such as a user attempting to reach an off-limits server. Security-related information must be presented in an easy-to-navigate fashion, with incident-based data synthesized and presented in high level views that IT can then drill down into for more detail. And a security platform must be able to automatically act on what it sees, based on defined policies.

For security purposes, what IT needs is visibility into actionable information. Therefore, a LAN-based security solution must meet the following visibility requirements:

» **Tie all LAN traffic to the user.** To accurately reflect traffic patterns in an accessible, intuitive fashion, data on LAN traffic must be resolved to user names, not merely IP or MAC addresses. Information resolved to IP or MAC addresses is difficult to interpret, hindering IT's ability to respond quickly to problems, define and apply control policies, and identify trends. In addition, IP and MAC addresses do not equate to users; these addresses can change depending on where users connect to the network and what computing platform they use.

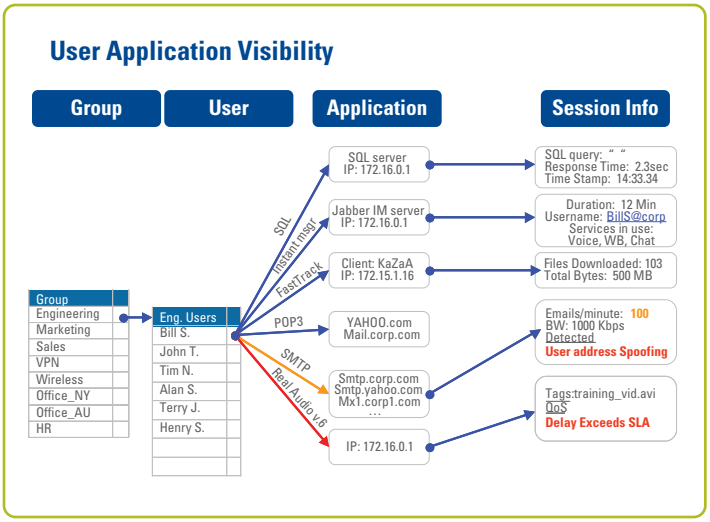
» **Perform deep packet inspection on all flows.** To get a complete picture of LAN traffic, a security platform must track and account for all packets in all flows, not just sample traffic. The platform must be able to inspect packets at Layer 7 and provide insights within Layer 7 – such as the URL involved in an HTTP transaction – to ensure the traffic is not malicious and is in compliance with policy.

» **Retain statistics about all flows.** To accommodate both short-term and long-term data analysis, a security platform must support on-line storage for immediate data retrieval as well as allow for data export to off-line storage. A security platform should store this detailed flow data in a relational database to simplify access and enable sophisticated querying. Accounting information should include such details as packets and bytes in and out by application and protocol and should be tracked for all LAN traffic simultaneously. It should also provide specifics about Layer 7+ data, such as the individual file name involved in a Windows file sharing (CIFS) operation, who accessed the file, what actions that user took, and how long the transaction lasted.

» **Provide real-time and historical data.** IT needs both instant insight into what's happening on the network and the ability to identify patterns over time. Therefore a security platform must provide real-time data that highlight what's changed on the network and support incident response, as well as historical reports that allow for trending, auditing, and comparisons for additional troubleshooting.

» **Provide an aggregated view of the LAN's security health.** For efficient monitoring of LAN security, IT needs a "dashboard" that captures the LAN's security status in a single screen, providing aggregated data on users, access control, malware, and incidents and allowing IT to drill down in any desired area.

» **Provide key user data.** For control, auditing, and other functions, a LAN security platform must provide visibility into user activity, including login/logout time, applications run, resources reached, and transactions performed.



» **Track security incidents.** IT needs instant visibility into anomalous behavior on the network. To be effective, a security platform must track a range of security incidents, including those relating to host posture checks, policies, and malware. For example, IT needs to know which systems are failing host posture check, if a user is attempting to access an off-limits resource, and if worms have been identified and contained.

- **Show "top talker" and "bottom talker" information.** To highlight traffic trends, a LAN security platform must provide "top talker" information as it relates to users, applications, and network destinations. Such information is important for identifying potential security violations, such as a user downloading a significant data store, or highlighting changes in traffic patterns and resource usage that indicate areas for capacity planning. In some cases, "bottom talker" data is also key, perhaps highlighting an application that's rarely used or sending suspiciously little amounts of traffic.

- **Show detailed application information.** To define policies, see policy violations, and troubleshoot problems, IT needs detailed visibility into applications. IT must see which applications users are running; information about specific application flows; and even expanded Layer 7 details, including events within an application, such as a file open, copy, delete, or edit.

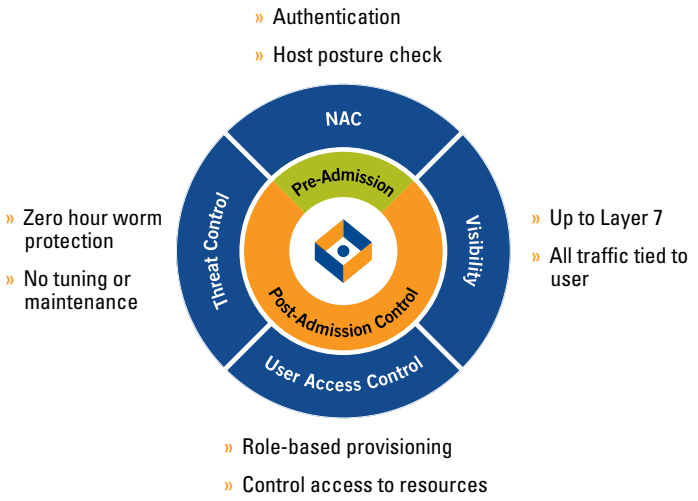
ConSentry Networks' Comprehensive Security Approach

ConSentry Networks delivers visibility 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, learned during authentication, to support user-based visibility and role-based provisioning.

Through the ConSentry InSight command center's graphical interface, IT can get at-a-glance views of network usage and security violations, perform incident response, and define global access and malware policies – the actions the LANShield platform should take when an access incident occurs or a malware algorithm is triggered. InSight compiles information based on knowledge of user transactions, presenting IT with all activities and access violations tied to username.

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 platform provides in-depth packet inspection with full Layer 7 application decode, so it can distinguish between applications using the same Layer 4 port or attempting to mask them 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, Layer 4 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 users' access to networked resources based on their 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

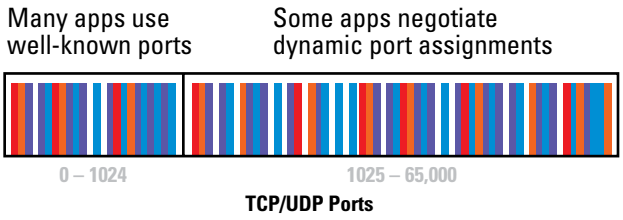
if malware is detected. Attempts to use printers or VoIP phones as a launch point for attacks are also prevented by limiting the protocols those devices can run and the network destinations they can reach.

ConSentry Delivers Full Visibility

Through stateful deep packet inspection with full Layer 7 application decode, the ConSentry LANShield platforms are able to provide the level of traffic visibility needed for security-related control, incident response, auditing, and trend analysis. The ConSentry InSight command center is IT's window into all users, LAN traffic, and violations, and is also the means by which IT defines and distributes policies centrally.

ConSentry Application Decoding

» ConSentry performs L7 decode to identify apps regardless of port number
  - Enables detection of port-cloaking attacks



ConSentry decodes these apps at Layer 7:

» HTTP	» DHCP	» SUNRPC*
» FTP*	» SMB/CIFS*	» MS Media*
» DNS	» RTP*	» H.323 *
» AD-Kerberos	» RTSP*	» SIP *
» RADIUS	» MSRPC*	» Oracle

**Port-hopping apps*

With InSight, IT can see and control all traffic on a per-user, per-flow basis, as well as define role-based access policies and malware control policies. This combination of full visibility and control ensures that enterprise assets are protected and network availability remains high. Likewise, InSight's comprehensive traffic tracking allows for rapid troubleshooting, auditing, reporting, and forensics.

The LANShield device provides comprehensive visibility into actionable information, the foundation for control, and meets the following visibility requirements:

» **Tie all LAN traffic to the user.** The LANShield platform binds an IP and MAC address to a username 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. This correlation of network events to users saves hours of manual analysis and custom scripting, enabling IT to easily control resource usage based on a user's group association or role within the enterprise and to rapidly pinpoint and respond to incidents.

» **Perform deep packet inspection on all flows.** The LANShield device tracks all flows on the LAN, performing deep packet inspection at the initiation of each flow to ensure the traffic is not malicious and is in compliance with defined access control policies. Once a flow is determined to be safe and compliant, the LANShield device then forwards as appropriate.

» **Retain statistics about all flows.** Within the LANShield architecture, a programmable ASIC is dedicated to capturing and distilling flow statistics. This information is forwarded to InSight, which stores this data in its relational database for easy querying and reporting. For long-term trending and auditing purposes, flow data can be exported from InSight to a back-end storage system.

» **Provide real-time and historical data.** InSight provides both real-time and historical views of LAN traffic, giving IT the flexibility to view data for the current hour, current day, last hour, or last day, or to define the timeframe of their choosing by specifying a start and end time. In terms of real-time data, InSight provides information on:

  - policy events;
  - malware events;
  - Network Admission Control (NAC) events;
  - users and user activity at the application level; and
  - applications.

InSight also provides the LANShield controller device configuration, so that IT defines policies centrally and then uses InSight to distribute those policies to the appropriate LANShield platform.

InSight also offers a portfolio of pre-defined and customizable reports that provide a clear overview of enterprise network health and user actions, useful for comparison and trending. With both real-time and historical data, details are a click away, so IT can drill down on any high-level data presented.

» **Provide an aggregated view of the LAN's security health.** The InSight "dashboard" encapsulates key data that IT needs for understanding the LAN's security health at a glance. The dashboard shows the health of all ConSentry devices, and it provides real-time, aggregated data on:

Real Time User Incidents

- network threat level;
- user counts;
- access control incidents;
- application control incidents;
- malware control incidents;
- guest access;
- top three roles generating incidents; and
- posture incidents.

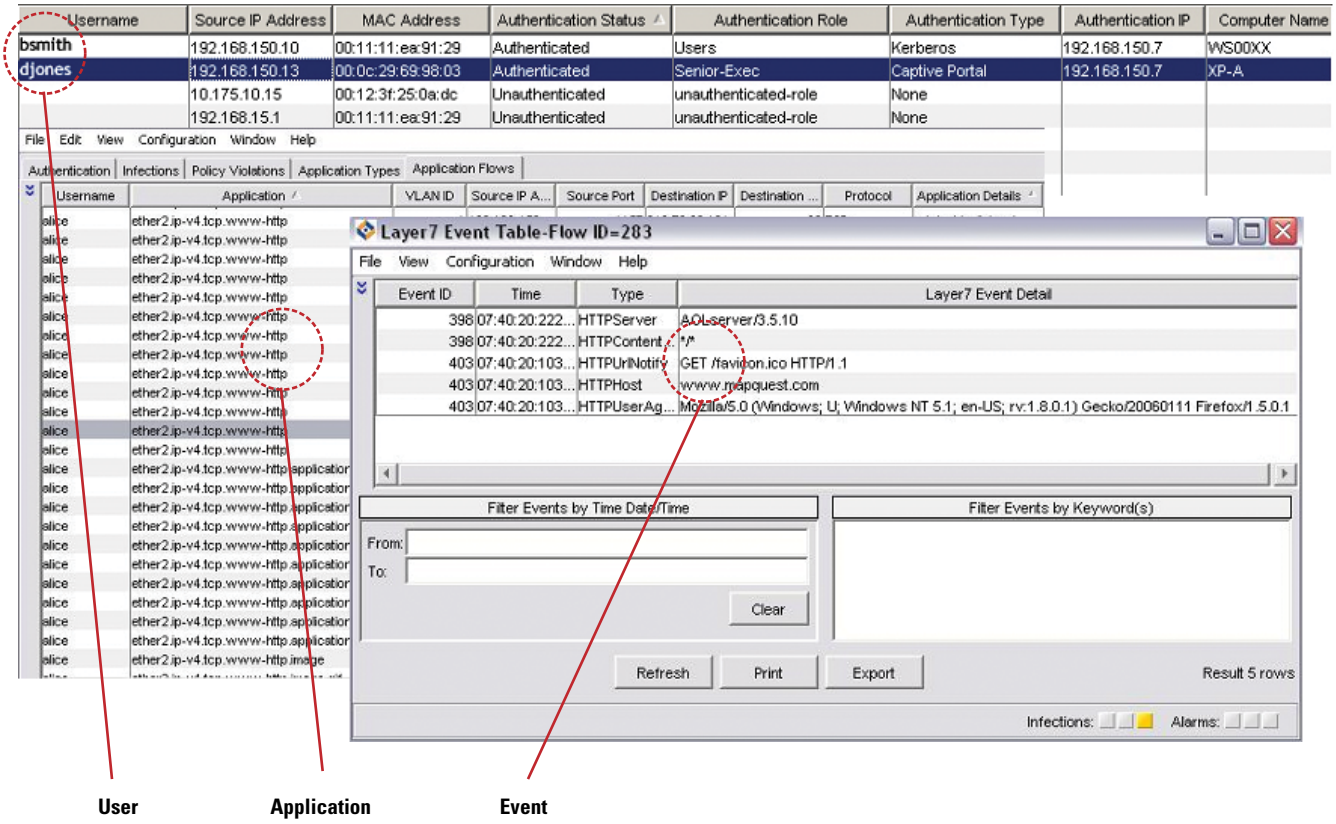
» **Provide key user data.** With its powerful ASICs, the LANShield platform monitors all traffic to and from each user, tracking each flow and the policies that apply to that user. Consequently, within InSight, IT can view all pertinent user data such as the total number of users on the network at a given time, authenticated vs. unauthenticated users, and guests or contractors vs. employees. In addition, InSight can identify every application being run by every user and the transactions performed, giving IT a complete picture of user activities.

» **Track security incidents.** InSight tracks a range of security incidents, including posture check, policy, and malware incidents, providing IT with a complete view of security events at all times. For example, IT can easily track policy incidents, such as a user in finance attempting to access an engineering application. InSight classifies each type of access incident, making it easy for IT to see whether an access control, application control, or network zone/destination violation occurred, for instance. In terms of malware incidents, InSight provides information on what was detected and what action was taken. IT can drill down on any incident summary for more detailed information.

» **Show "top talker" and "bottom talker" information.** InSight provides real-time "top talker" information on users, applications, and incidents, as well as "bottom talker" information on applications, in an easily accessible format. These details include:

- top users and roles (e.g., employee vs. guest vs. contractor) generating incidents;
- top applications by bandwidth and by instance; and
- bottom applications by instance.

User • Application • Events



» **Show detailed application information.** InSight provides information on application instances, application flows, and Layer 7 events. Application instances refer to the number of users running a given application, while application flows refer to the discrete user sessions using that application. InSight also provides a tally of the total byte counts associated with all flows. IT can also view application information in terms of Layer 7 events that occur within a flow, such as:

- the URL and source user for HTTP flows;
- the browser in use for HTTP flows;
- file name, source and destination IP addresses, and FTP username for FTP flows;
- file transaction (read, write), user, file name, and volume name for SMB/CIFS flows; and
- user name, MAC address, IP address, and time for DHCP flows.

Such information is critical to IT for a number of reasons. For instance, knowing and enforcing the browser involved in an HTTP flow is critical for IT to block the use of vulnerable applications. As for Windows file sharing protocols, being able to control what transactions users can perform on key files enables companies to meet compliance requirements for data access.

Building on a Solid Foundation

ConSentry Networks understands that comprehensive visibility into LAN traffic is a means to an end. That's why the LANShield device's visibility capabilities directly enable policy enforcement actions. With the ConSentry, IT can see and control who's on the LAN, where they go, and what they do, as well as protect the LAN from malware.

By combining network admission control, full LAN visibility, user access control, and threat control in a single platform, ConSentry delivers LAN security at a price point that allows for ubiquitous deployment. With the LANShield device, enterprises can move to a new model for LAN security based on visibility and control embedded in the LAN fabric.

Operating pervasively across the enterprise LAN, the LANShield platform protects business information and therefore business operations, reducing risk exposure, improving business continuity, and helping organizations comply with governmental regulations. In today's dynamic business and technology environment, ConSentry's purpose-built platform lets organizations 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