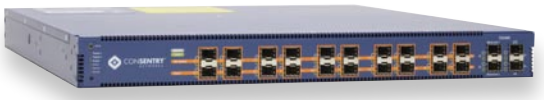
ConSentry® LANShield™ Controllers

COST-EFFECTIVE, TRANSPARENT DEPLOYMENT

ConSentry Networks delivers intelligent switching, making it easy for IT to control users and applications on the LAN. The ConSentry LANShield platforms — the LANShield Controller and LANShield Switch — tie together user, device, role, application, and destination to provide a level of business context not possible with legacy switch architectures. With this context, IT can more easily align the LAN to the business and deliver the services needed to make enterprises more efficient, accountable, and agile.



CS2400 LANShield Controller

CS1000 LANShield Controller

The LANShield Controller makes it easy for IT to embed user and application control directly into the LAN infrastructure. It augments existing switches with user and application intelligence that makes applying controls and segmenting users on the LAN much easier than using traditional tools such as VLANs or ACLs, lowering IT's cost of operations.

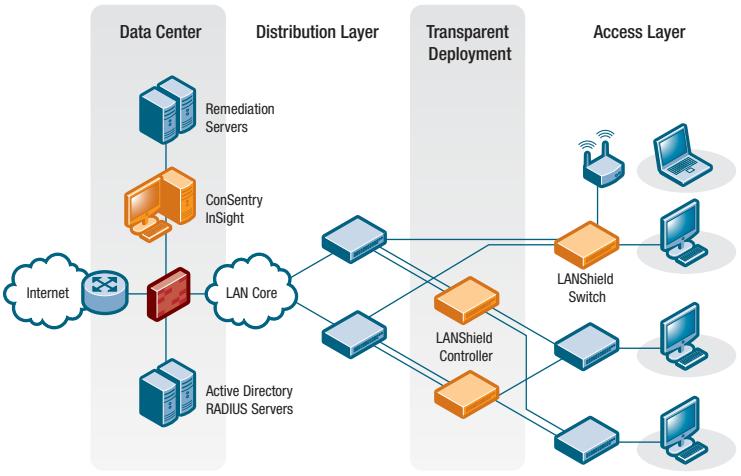
Custom silicon provides the foundation for these control capabilities. This custom hardware includes a multi-core processor and programmable ASICs that perform packet processing for monitoring and control at up to 10 Gbps. The programmability of the hardware enables ConSentry to keep pace with changes in applications and security requirements.

The LANShield intelligent switching architecture enables enterprises to monitor and control all user traffic with minimal impact on the existing infrastructure. ConSentry leverages existing OS authentication mechanisms, such as the Windows login. The LANShield Controllers enforce policy directly, without the need for new VLANs or ACLs in the network or new supplicants or agents on the clients.

TRANSPARENCY AND HIGH AVAILABILITY

The LANShield Controller sits between access switches and the distribution or core layer, aggregating uplinks from wiring closets and enforcing access policies on all traffic. A transparent device, the LANShield Controller requires no changes to network design or user behavior, simplifying deployment and lowering IT's cost of operations.

The Controller supports high-availability and resiliency modes. Enterprises that have dual-homed wiring closet switches can deploy two ConSentry LAN-



The LANShield Controller deploys transparently between existing switches, providing intelligent switching to control users and applications.

Shield Controllers as peers — the two platforms share authentication state and preserve user authentications in case of failover. In addition, the Controller itself supports two failure modes. IT can set the device to fail to pass-through, where all LAN traffic will traverse the Controller untouched, or fail to block, where all traffic is stopped. The Controller also includes redundant power supplies and fans.

DEPLOYMENT OPTIONS AND IT INITIATIVES

The LANShield Controller and LANShield Switch provide enterprises with options for deploying intelligent switching. The Controller sits behind existing switches, while the LANShield Switch provides integrated intelligent switching. IT can leverage the LANShield Controller to:

- troubleshoot user and application issues more quickly
- support non-user devices such as robotics and IP phones
- limit access to resources
- track all user activity for auditing
- support a more dynamic and diverse workforce
- more easily roll out new applications, systems, and business locations

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

ConSentry LANShield Controller Product Specifications

Security Features — Leveraging LANShield OS

User / Machine Authentication

Transparent Authentication Methods
- passive Kerberos snooping to authenticate Windows Active Directory users, and Linux, Macintosh, and Novell via PAM modules
- passive 802.1X authentication snooping (RADIUS snooping)

Active Authentication
- MAC address – RADIUS authentication
- web authentication via captive portal

Rich Device Authentication
- whitelisting of MAC/IP addresses and wildcards

User De-Authentication Methods
- passive Windows log-off detection
- configurable idle timeout
- captive-portal logout button or count-down timer

Role Derivation

Place Users into Roles Based on:
- RADIUS attributes
- LDAP attributes
- Active Directory attributes
- physical location
- DHCP attributes
- system attributes
- time
- combination of above

Identity-based Policy and Control

Policy Rule Elements:
- user group
- Layer 2-4 Source or Destination (MAC, IP, Port)
- Layer 7 application detection and attribute decode
- resource network zone (e.g., servers)
- destination ACL through DNS name
- Bi-directional rules (Flow-In, Flow-Out, Bi-Directional)
- Up to 8192 L2-L7 rules per device

Policy Rule Enforcement Actions:
- permit/deny
- policy-based traffic mirroring
- logging to InSight
- logging to syslog

Deployment Mode Settings:
- pass through mode – useful in hardware installation phase
- monitor mode – useful in policy development/testing phase
- protect mode – production phase

Host Posture Check (optional)

Dissolvable agent (optional)
- Windows 98-Vista, Linux, Macintosh
- compliance checks against 26 major firewall and AV vendors
- malware scanner with downloadable updates
- custom rules for file, registry, and process checking

Microsoft NAP

Threat Detection / Mitigation
- zero-hour threat detection
- Denial of Service (DoS) attack detection
- no signature updates necessary
- drops malformed packets
- block by: physical port, SRC IP, offending application

Applications Monitoring for Compliance and Auditing
- ties usernames to applications and security violations
- identifies applications and application content
- 300+ at Layer 4
- 30+ at Layer 7

Centralized Visualization and Management through ConSentry InSight
- centralized policy and role-derivation configuration GUI
- user and application usage repository on an embedded SQL DB
- real-time alert dashboard
- fully drillable forensics capability
- reporting with scheduler

Logging and Reporting
- direct syslog reporting
- detailed security log messages
- formatted for SIEM integration

Physical Features — Optimized for High-Density Resilient Installation

Secured Processing Throughput
- CS1000: 4 Gbps
- CS2400: 10 Gbps

Management and Control
- out-of-band Ethernet management
- industry-standard Command Line Interface (CLI)
- centrally managed by ConSentry InSight
- SNMP v1/v2c
- formatted syslog to multiple destinations
- Telnet / SSH / SNMP / TFTP
- administrator login through RADIUS or local DB

Standards and Protocols
- 802.1D Bridging
- 802.3ad (Link Aggregation)
- 802.3 10Base-T
- 802.3u 100Base-TX
- 802.3z 1000Base-SX/T

Data Interface Ports
- CS1000: 4 secure SFP port pairs
- CS2400: 10 secure SFP port pairs

Layer 2 Features
- 4,096 VLANs

Authenticated Users
- CS1000: 400 users in base model, upgradeable to 800 users
- CS2400: 1000 users in base model, upgradeable to 2000 users

Resiliency
- dual active-active high-availability mode
- fail pass-through (open)
- fail block (closed)
- dual power supplies
- redundant cooling fan

Latency
- average 30 microseconds

SFPs Available
- single-mode 1 Gbps fiber
- multimode 1 Gbps fiber
- 10/100/1000 copper

Non-data Interface (Extensibility) Ports
- CS1000: Two ports for packet mirroring or HA and one rear mgmt port
- CS2400: Four ports for packet mirroring or HA and one rear mgmt port

Certifications

Emissions and Safety

FCC Part 15 sub part B Class A (USA); ICES-003 (Canada); EN55022 (CE Mark); Class A, EN55024 (CE Mark); VCCI Class A (Japan); UL 60950-1 (USA); CSA C2.22 No. 60950-1 (Canada); EN 60950-1 (CE Mark); IEC 60950-1 (International); NOM (Mexico); C-TICK (Australia); TUV-GS Mark; S Mark; MIC (Korea)

Dimensions
- 17.3 in. x 18.6 in. x 1.73 in - 1U (44.5 x 43.2 x 3.8 cm)
- rack mounting for 19-inch racks

Weight
- 15 lbs. (6.9 kg)

Operating Requirements
- temperature: 32° to 104° F (0° to 40° C)
- humidity: 5% to 90%, non-condensing
- front-to-back air flow

Power
- dual redundant 180W 90-264VAC full range,47-63Hz

Ordering Information

Part No.	Description
CS1000-ACAC	10 unpopulated SFP cages (4 secure data port pairs + 2 extensibility ports). 2 AC PSUs, 1 mgmt port, 400 authenticated users
CS2400-ACAC	24 unpopulated SFP cages (10 secure data port pairs + 4 extensibility ports). 2 AC PSUs, 1 mgmt port, 1000 authenticated users

Part No.	Description
CS1000-4C-TO-8C-UPGD	CS1000 800 authenticated user upgrade license
CS2400-1K-TO-2K-UPGD	CS2400 2000 authenticated user upgrade license

CONSENTRY NETWORKS

Copyright ©2008 ConSentry Networks, Inc. ConSentry Networks, the ConSentry Networks logo, LANShield, and "Control every user. Secure every port." are trademarks of ConSentry Networks Inc., for use in the United States and other countries. All other product and company names herein may be trademarks of their respective holders. 012708

CON-DS-0108