ConSentry InSight Command Center

THE COMMAND CENTER FOR INTELLIGENT SWITCHING

ConSentry Networks delivers intelligent switching, making it easy for IT to control users and applications on the LAN. The ConSentry LANShield platforms — the LANShield Switch and LANShield Controller — 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.

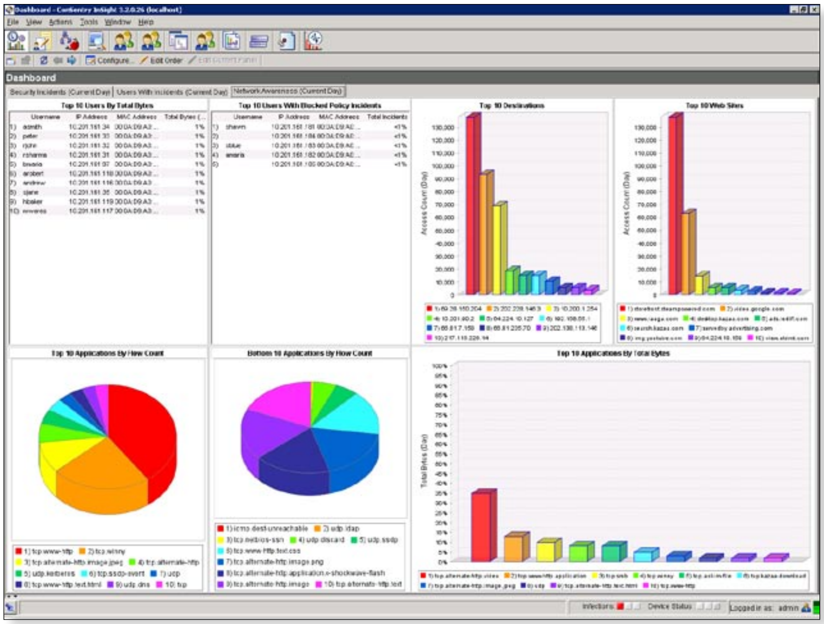
InSight aggregates all traffic capture data and presents IT with actionable information, showing key security incidents in at-a-glance summaries and drill-down, detailed views. InSight also enables rapid forensic troubleshooting, auditing, and reporting. InSight's GUI-based tools simplify policy creation and distribution.

InSight includes templates that make it easy for IT to create policies and deploy them on LANShield devices. The LANShield platforms automatically derive users' roles, and InSight uses that role information as the basis for intelligent switching policies. InSight also supports filters that let IT treat policies as building blocks and layer on multiple levels of control more easily. The flexible exception rules, combined with the policy filters, let IT create unique controls by role without creating a separate policy for each variation.

VISIBILITY FEATURES

InSight provides IT with a view of the overall health of the LAN and all security incidents. The LANShield products bind users to their addresses and applications, so InSight is able to display all LAN status information, incidents, and policy violations by username.

InSight retains statistics about all flows, including both real-time and historical data. This information includes such details as the packets and bytes in and out by application and protocol, the individual file name involved in a Windows file sharing (CIFS), instant messaging or FTP operation, the usernames of users who accessed particular files, and the duration of all sessions.


Dashboard - ConSentry InSight 3.2.0.26 (localhost)
File View Actions Tools Window Help
Configure...
Edit Order
Dashboard
Security Incidents (Current Day)
Users With Incidents (Current Day)
Network Awareness (Current Day)
Top 10 Destinations
Access Count (Day)
Top 10 Web Sites
Top 10 Applications By Flow Count
Bottom 10 Applications By Flow Count
Top 10 Applications By Total Bytes
Total Bytes (Day)
Infections
Device Status
Logged in as: admin

Top 10 Users By Total Bytes

	Username	IP Address	MAC Address	Total Bytes (...
1)	asmith	10.201.181.34	00:0A:D9:A3...	1%
2)	peter	10.201.181.33	00:0A:D9:A3...	1%
3)	rjune	10.201.181.32	00:0A:D9:A3...	1%
4)	rsharma	10.201.181.31	00:0A:D9:A3...	1%
5)	bwaria	10.201.181.07	00:0A:D9:A3...	1%
6)	arobert	10.201.181.118	00:0A:D9:A3...	1%
7)	andrew	10.201.181.116	00:0A:D9:A3...	1%
8)	sjane	10.201.181.35	00:0A:D9:A3...	1%
9)	hbaker	10.201.181.119	00:0A:D9:A3...	1%
10)	wwerea	10.201.181.117	00:0A:D9:A3...	1%

Top 10 Users With Blocked Policy Incidents

	Username	IP Address	MAC Address	Total Incidents
1)	shawn	10.201.181.181	00:0A:D9:AE...	<1%
2)		10.201.181.184	00:0A:D9:AE...	<1%
3)	sblue	10.201.181.183	00:0A:D9:AE...	<1%
4)	amaria	10.201.181.182	00:0A:D9:AE...	<1%
5)		10.201.181.180	00:0A:D9:AE...	<1%

The Network Awareness dashboard provides a quick snapshot of network usage by user and application.

InSight also provides an aggregated view of the LAN security health — the InSight dashboard displays:

- the overall network threat level
- user counts by authenticated, unauthenticated, and guests
- authentication failures
- incidents for unauthenticated users
- policy, malware, and posture incidents
- the top user or device roles responsible for incidents

Other dashboard views such as Network Awareness show network resource usage, with data including top network users, top applications by bandwidth and instance, top destinations, and top URLs being accessed during the course of the day.

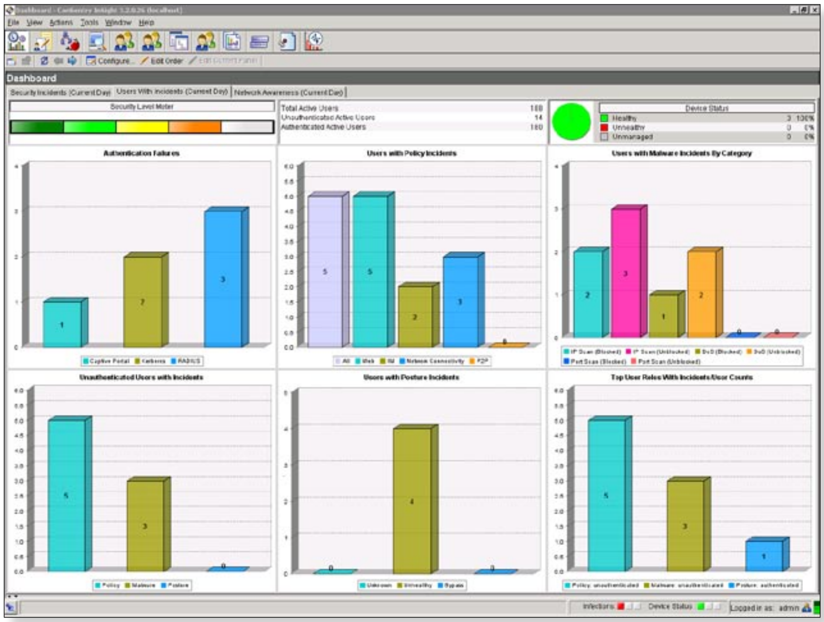
InSight provides a range of other statistics that can be selected to create custom dashboard views and reports. IT can select from data such as top policy violators, top FTP file transfers, top IM files, top policy incidents, and malware incidents by type.

Detailed forensic drill-down is available from the dashboard views that provide information on user activity, applications and hosts used, and policies enforced. IT can also use InSight to track individual application flows for a user. IT can select which traffic InSight should make visible. For example, an IT administrator may choose not to see details on traffic related to a management VLAN. IT can also set filters for InSight's visibility by application and role.

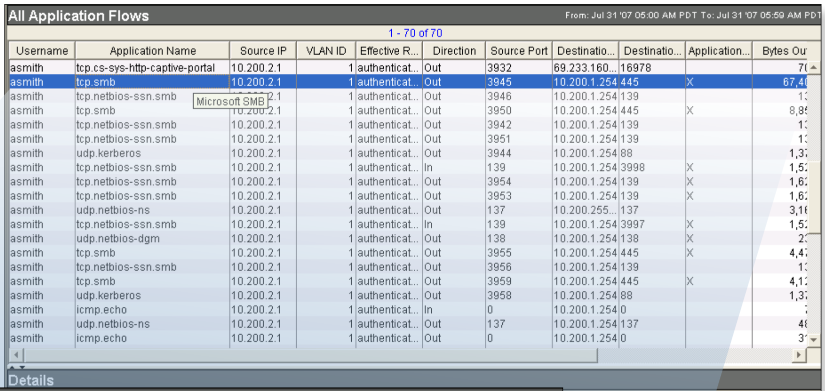
To protect privacy, InSight supports a four-eye mode that requires two IT staff be involved when accessing information such as usernames and IP addresses.

Custom queries allow IT to view specific data when troubleshooting network performance or security issues. Among the possible queries are:

- ◆ new applications (by bandwidth) seen over a period of time specified by IT



The Security Incidents dashboard enables quick response to policy, malware, and posture violations



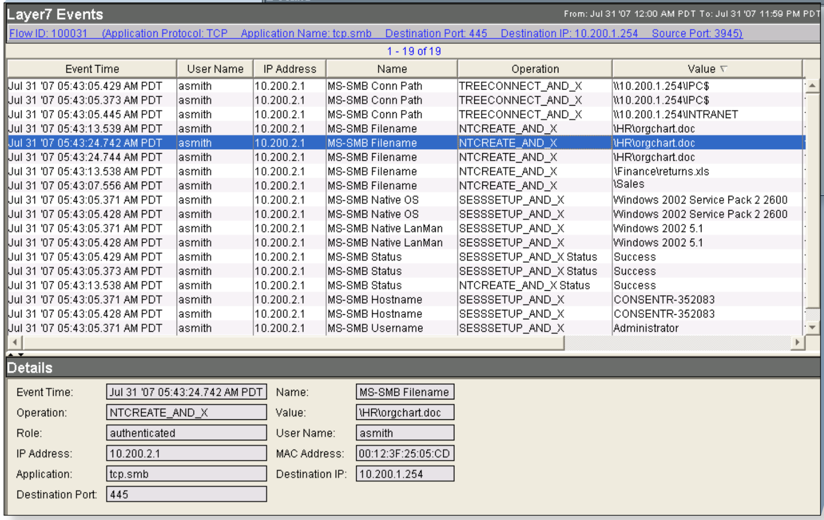
All Application Flows From: Jul 31 '07 05:00 AM PDT To: Jul 31 '07 05:59 AM PDT

1 - 70 of 70

Username	Application Name	Source IP	VLAN ID	Effective R...	Direction	Source Port	Destinatio...	Destinatio...	Application...	Bytes Out
asmith	tcp.cs-sys-http-captive-portal	10.200.2.1	1	authenticat...	Out	3932	69.233.160...	16978		70
asmith	tcp.smb	10.200.2.1	1	authenticat...	Out	3945	10.200.1.254	445	X	67,40
asmith	tcp.netbios-ssn.smb	10.200.2.1	1	authenticat...	Out	3946	10.200.1.254	139		13
asmith	tcp.smb	10.200.2.1	1	authenticat...	Out	3950	10.200.1.254	445	X	8,85
asmith	tcp.netbios-ssn.smb	10.200.2.1	1	authenticat...	Out	3942	10.200.1.254	139		13
asmith	tcp.netbios-ssn.smb	10.200.2.1	1	authenticat...	Out	3951	10.200.1.254	139		13
asmith	udp.kerberos	10.200.2.1	1	authenticat...	Out	3944	10.200.1.254	88		1,37
asmith	tcp.netbios-ssn.smb	10.200.2.1	1	authenticat...	In	139	10.200.1.254	3998	X	1,52
asmith	tcp.netbios-ssn.smb	10.200.2.1	1	authenticat...	Out	3954	10.200.1.254	139	X	1,62
asmith	tcp.netbios-ssn.smb	10.200.2.1	1	authenticat...	Out	3953	10.200.1.254	139	X	1,62
asmith	udp.netbios-ns	10.200.2.1	1	authenticat...	Out	137	10.200.255...	137		3,16
asmith	tcp.netbios-ssn.smb	10.200.2.1	1	authenticat...	In	139	10.200.1.254	3997	X	1,52
asmith	udp.netbios-dgm	10.200.2.1	1	authenticat...	Out	138	10.200.1.254	138	X	23
asmith	tcp.smb	10.200.2.1	1	authenticat...	Out	3955	10.200.1.254	445	X	4,47
asmith	tcp.netbios-ssn.smb	10.200.2.1	1	authenticat...	Out	3956	10.200.1.254	139		13
asmith	tcp.smb	10.200.2.1	1	authenticat...	Out	3959	10.200.1.254	445	X	4,12
asmith	udp.kerberos	10.200.2.1	1	authenticat...	Out	3958	10.200.1.254	88		1,37
asmith	icmp.echo	10.200.2.1	1	authenticat...	In	0	10.200.1.254	0		7
asmith	udp.netbios-ns	10.200.2.1	1	authenticat...	Out	137	10.200.1.254	137		48
asmith	icmp.echo	10.200.2.1	1	authenticat...	Out	0	10.200.1.254	0		31

Microsoft SMB

Details



Layer7 Events From: Jul 31 '07 12:00 AM PDT To: Jul 31 '07 11:59 PM PDT

Flow ID: 100031 (Application Protocol: TCP Application Name: tcp.smb Destination Port: 445 Destination IP: 10.200.1.254 Source Port: 3945)

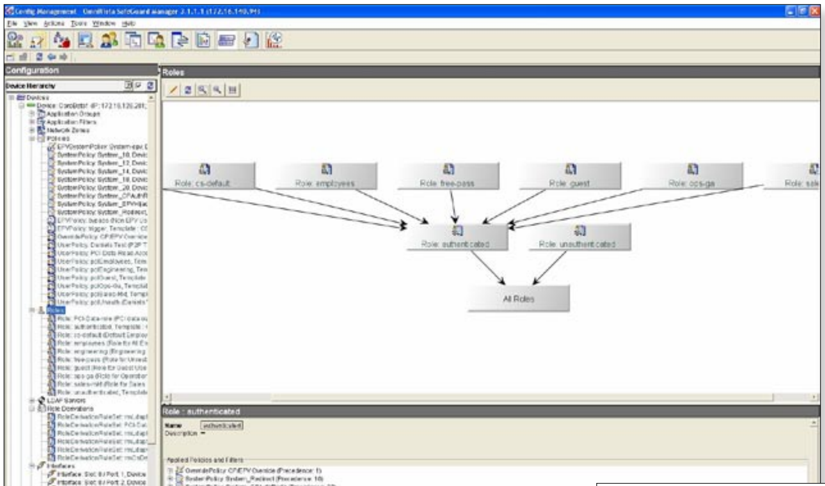
1 - 19 of 19

Event Time	User Name	IP Address	Name	Operation	Value ▽
Jul 31 '07 05:43:05.429 AM PDT	asmith	10.200.2.1	MS-SMB Conn Path	TREECONNECT_AND_X	\\10.200.1.254\IPC$
Jul 31 '07 05:43:05.373 AM PDT	asmith	10.200.2.1	MS-SMB Conn Path	TREECONNECT_AND_X	\\10.200.1.254\IPC$
Jul 31 '07 05:43:05.445 AM PDT	asmith	10.200.2.1	MS-SMB Conn Path	TREECONNECT_AND_X	\\10.200.1.254\INTRANET
Jul 31 '07 05:43:13.539 AM PDT	asmith	10.200.2.1	MS-SMB Filename	NTCREATE_AND_X	\HR\orgchart.doc
Jul 31 '07 05:43:24.742 AM PDT	asmith	10.200.2.1	MS-SMB Filename	NTCREATE_AND_X	\HR\orgchart.doc
Jul 31 '07 05:43:24.744 AM PDT	asmith	10.200.2.1	MS-SMB Filename	NTCREATE_AND_X	\HR\orgchart.doc
Jul 31 '07 05:43:13.538 AM PDT	asmith	10.200.2.1	MS-SMB Filename	NTCREATE_AND_X	\Finance\returns.xls
Jul 31 '07 05:43:07.556 AM PDT	asmith	10.200.2.1	MS-SMB Filename	NTCREATE_AND_X	\Sales
Jul 31 '07 05:43:05.371 AM PDT	asmith	10.200.2.1	MS-SMB Native OS	SESSSETUP_AND_X	Windows 2002 Service Pack 2 2600
Jul 31 '07 05:43:05.428 AM PDT	asmith	10.200.2.1	MS-SMB Native OS	SESSSETUP_AND_X	Windows 2002 Service Pack 2 2600
Jul 31 '07 05:43:05.371 AM PDT	asmith	10.200.2.1	MS-SMB Native LanMan	SESSSETUP_AND_X	Windows 2002 5.1
Jul 31 '07 05:43:05.428 AM PDT	asmith	10.200.2.1	MS-SMB Native LanMan	SESSSETUP_AND_X	Windows 2002 5.1
Jul 31 '07 05:43:05.429 AM PDT	asmith	10.200.2.1	MS-SMB Status	SESSSETUP_AND_X Status	Success
Jul 31 '07 05:43:05.373 AM PDT	asmith	10.200.2.1	MS-SMB Status	SESSSETUP_AND_X Status	Success
Jul 31 '07 05:43:13.538 AM PDT	asmith	10.200.2.1	MS-SMB Status	NTCREATE_AND_X Status	Success
Jul 31 '07 05:43:05.371 AM PDT	asmith	10.200.2.1	MS-SMB Hostname	SESSSETUP_AND_X	CONSENTR-352083
Jul 31 '07 05:43:05.428 AM PDT	asmith	10.200.2.1	MS-SMB Hostname	SESSSETUP_AND_X	CONSENTR-352083
Jul 31 '07 05:43:05.371 AM PDT	asmith	10.200.2.1	MS-SMB Username	SESSSETUP_AND_X	Administrator

Details

Event Time:	Jul 31 '07 05:43:24.742 AM PDT	Name:	MS-SMB Filename
Operation:	NTCREATE_AND_X	Value:	\HR\orgchart.doc
Role:	authenticated	User Name:	asmith
IP Address:	10.200.2.1	MAC Address:	00:12:3F:25:05:CD
Application:	tcp.smb	Destination IP:	10.200.1.254
Destination Port:	445		

In addition to showing all applications a given user is running, IT can further drill down to see the file names involved in a Windows file transfer, as shown here, or the URLs viewed during web sessions.



Hierarchical views within InSight make it easier for IT to correctly apply roles and policies to users within an organization.

- ◆ new network users seen over a period of time specified by IT
- ◆ network users seen over a specific time period but not currently visible

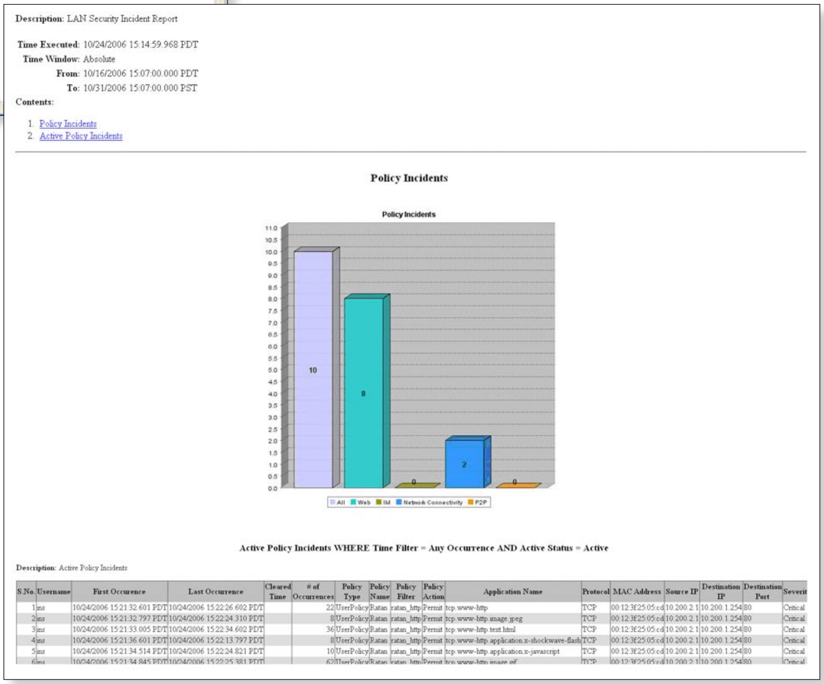
POLICY CREATION GUI

InSight command center incorporates a rich graphical user interface for identity-based policy creation. With it, IT can easily create:

- ◆ network zones
- ◆ hierarchical policies and role mapping
- ◆ Layer 4 and Layer 7 application filters and groups
- ◆ user role definitions and user-to-role mapping
- ◆ Active Directory, RADIUS and LDAP interface configuration

REPORTING FEATURES

InSight provides comprehensive reporting on the visualized data. Built-in reports include the Daily File Access Report and the Enterprise Security Report, which includes user asset and incident information. IT can also generate custom reports to meet a variety of needs, from technical to business issues. For example, an administrator could build a report that showed all users that have incidents associated with a given policy during a specified time period or all users that accessed a particular application during a specified time period. An IT administrator can also add graphical charts from the InSight dashboard to report templates to enhance their visual presentation.



Description: LAN Security Incident Report

Time Executed: 10/24/2006 15:14:59.968 PDT
Time Window: Absolute
From: 10/16/2006 15:07:00.000 PDT
To: 10/31/2006 15:07:00.000 PST

Contents:

1. Policy Incidents
2. Active Policy Incidents

Policy Incidents

Active Policy Incidents WHERE Time Filter = Any Occurrence AND Active Status = Active

Description: Active Policy Incidents

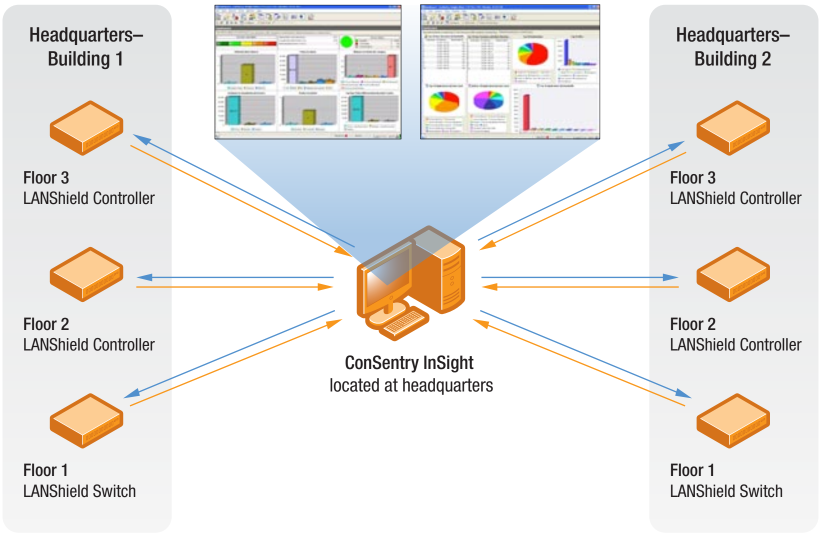
S.No.	Username	First Occurence	Last Occurence	Cleared Time	# of Occurrences	Policy Type	Policy Name	Policy Filter	Policy Action	Application Name	Protocol	MAC Address	Source IP	Destination IP	Destination Port	Severit
1	ins	10/24/2006 15:21:32.601 PDT	10/24/2006 15:22:26.602 PDT		22	UserPolicy	Ratan	ratan_http	Permit	tcp.www-http	TCP	00:12:3f:25:05:cd	10.200.2.1	10.200.1.254	80	Critical
2	ins	10/24/2006 15:21:32.797 PDT	10/24/2006 15:22:24.310 PDT		8	UserPolicy	Ratan	ratan_http	Permit	tcp.www-http.image.jpeg	TCP	00:12:3f:25:05:cd	10.200.2.1	10.200.1.254	80	Critical
3	ins	10/24/2006 15:21:33.005 PDT	10/24/2006 15:22:34.602 PDT		36	UserPolicy	Ratan	ratan_http	Permit	tcp.www-http.text.html	TCP	00:12:3f:25:05:cd	10.200.2.1	10.200.1.254	80	Critical
4	ins	10/24/2006 15:21:36.601 PDT	10/24/2006 15:22:13.797 PDT		8	UserPolicy	Ratan	ratan_http	Permit	tcp.www-http.application.x-shockwave-flash	TCP	00:12:3f:25:05:cd	10.200.2.1	10.200.1.254	80	Critical
5	ins	10/24/2006 15:21:34.514 PDT	10/24/2006 15:22:24.821 PDT		10	UserPolicy	Ratan	ratan_http	Permit	tcp.www-http.application.x-javascript	TCP	00:12:3f:25:05:cd	10.200.2.1	10.200.1.254	80	Critical
6	ins	10/24/2006 15:21:34.845 PDT	10/24/2006 15:22:25.381 PDT		62	UserPolicy	Ratan	ratan_http	Permit	tcp.www-http.image.gif	TCP	00:12:3f:25:05:cd	10.200.2.1	10.200.1.254	80	Critical

The LAN Security Incident Report includes a bar chart showing policy incidents by application type and a tabular listing of all policy incidents. IT can define the time duration covered by the report.

CENTRAL CONFIGURATION AND MANAGEMENT

InSight provides centralized management and configuration of all LANShield devices deployed in a network. Capabilities include:

- ◆ central policy management: InSight enables IT to configure policies just once and then push them out to all applicable LANShield devices.
- ◆ software updates of multiple LANShield devices: IT can use InSight to distribute updated LANShield OS releases to all deployed devices.
- ◆ LANShield device health: This configuration view provides status on a LANShield device's CPU usage, memory usage, fan speeds, current temperature, and power supply status.



Centralized Management
and Control

- custom captive portal: Using InSight, IT can distribute a customized captive portal page to multiple LANShield devices.
- distribute posture check configuration file: IT can use InSight to send these endpoint files to multiple LANShield devices.
- audit logging: IT can track all actions done via InSight, with the associated users, time, and status of each activity.
- archiving data: InSight is RAID capable and data can be exported to an SQL database.

ConSentry InSight Command Center Product Specifications

System Requirements

Minimum Server Requirements for InSight Software Installation

- dual 2.8 GHz processor
- 2 GB RAM
- 60+ GB free hard disk space
- Microsoft Windows 2003 Server with SP1 Operating System (Web or Standard Edition, 32 bit)

Client Requirements for InSight

The InSight client can be run on most Windows systems. Minimum requirements are:

- Windows 2000 Server, Windows 2003 Server, or Windows XP Professional
- 2.8 GHz single CPU
- 512 MB RAM
- 20 GB hard disk
- Internet Explorer 6.0 or higher
- screen resolution of 1024 x 768 pixels
- Internet connectivity

InSight is only responsible for policy configuration and event collection. By design it does not interfere with real- time control and enforcement if connectivity is broken.

Ordering Information

Part No.	Description
CS-INS-SW-5	ConSentry InSight Software (1 to 5 managed devices)
CS-INS-SW-10	ConSentry InSight Software (6 to 10 managed devices)
CS-INS-SW-25	ConSentry InSight Software (11 to 25 managed devices)
CS-INS-SW-50	ConSentry InSight Software (26 to 50 managed devices)
CS-INS-SW-5-to-10-UPGD	Upgrade Pricing (1-5 to 6-10 bucket) (managed devices)
CS-INS-SW-5-to-25-UPGD	Upgrade Pricing (1-5 to 11-25 bucket) (managed devices)
CS-INS-SW-5-to-50-UPGD	Upgrade Pricing (1-5 to 26-50 bucket) (managed devices)
CS-INS-SW-10-to-25-UPGD	Upgrade Pricing (6-10 to 11-25 bucket) (managed devices)
CS-INS-SW-10-to-50-UPGD	Upgrade Pricing (6-10 to 26-50 bucket) (managed devices)
CS-INS-SW-25-to-50-UPGD	Upgrade Pricing (11-25 to 26-50 bucket) (managed devices)

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™
NETWORKS