

The iPolicy Security Reporter is ideal for reporting the insightful security events and traffic trends of networks.

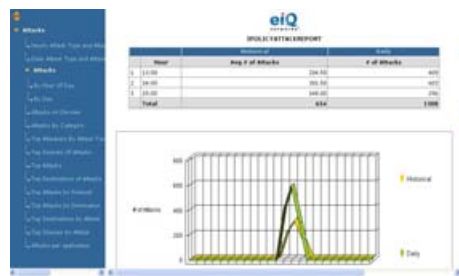
ISR Data Sheet

## iPolicy Security Reporter Benefits

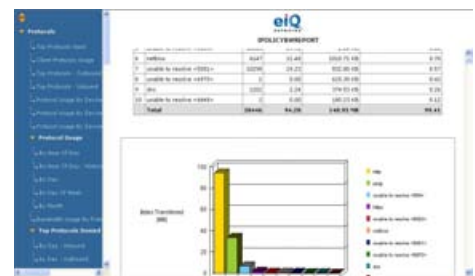
- Meet HIPAA, GLBA, Sarbanes-Oxley, PCI and FISMA regulatory compliance.
- Monitor and visualize hacker and virus attacks and behavior patterns.
- Minimize or eliminate false positives with correlated alerting.
- Identify intrusions, viruses and security breaches, including blended attacks.
- Identify attack type, source, destination, port, protocol, severity, rule, etc. in real-time.
- Obtain details on virus activity such as virus source, virus type, details, impact, etc.
- Vector an attack for investigating a hacker's behavior and attack path using forensics analysis.
- Understand protocol usage by device, user and department.
- Understand blocked website access and allowed/denied traffic.
- The ISR supports Drill-down reports.
- The ISR supports over 200 scanned reports.
- Administrators can schedule reports and the reports can either be viewed on-line or sent to the administrator via e-mail or uploaded to an FTP server
- Bandwidth utilization by department, client and protocol.
- Identify inappropriate Internet usage by employees.
- Understand and obtain details on SPAM and Spyware activity.
- MSSPs can provide role based access to reporting and monitoring portals.
- The ISR supports customized Alert capabilities.
- The ISR supports generation of reports in the following formats –
  - a. HTML
  - b. MS-Word
  - c. MS-Excel
  - d. Plain Text
  - e. PDF

**iPolicy Security Reporter is a protocol-based service with analytical and reporting capabilities enabling security, network tracing and maintenance.**

ISR is the reporting engine for viewing security events. In addition to collecting event and logs in its own format and storing alerts in the database, the iPolicy Security Manager can send events, statistics and logs in syslog format to a syslog server. Using syslog data ISR can be used as the reporting engine and for real-time event correlation. Additionally, ISR can be used for forensic analysis for security related investigation and incident response. The ISR complements iPolicy Networks ISM by supporting deployments for mid-size enterprise environments as well as in distributed networks to manage a large number of Intrusion Prevention Firewalls. The ISR reporting portal with its unique reporting dashboard allows the administrator to get an instant view of the network and security related events with powerful drilldown features that display 2<sup>nd</sup> and 3<sup>rd</sup> level details with a single click. Additionally, ISR provides a large number of reports which can be based on archived data to provide reports and analysis in HTML, PDF, Word, Excel, and Text formats.



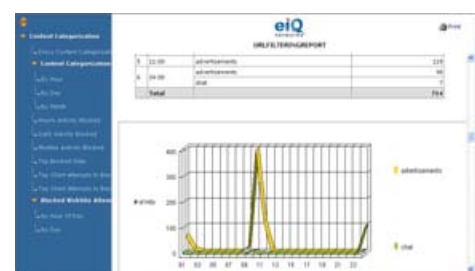
Reports for Attacks



Reports for Bandwidth



Top Blocked URL Sites



Reports for URL Filtering

## Features

- Reporting Portal with Powerful Drilldown:** Gives access to over 800 reports and displays sub-level details with a single click.
- Correlated Reporting:** Offers a holistic view and understanding of hacker and virus activity by correlating data across all network devices instead of looking at each device data separately.
- Intrusion and Rules-based Reporting:** Presents over 50 attack and rules-based reports to help security administrators get a comprehensive understanding of intrusions and rule violations.
- Protocol and Web Usage Reporting:** Provides a firm handle on protocol and web usage patterns by user, department and/or device.
- Content Categorization Reporting:** Generates reports to help understand employee web usage patterns.
- Automated Report Generation and Distribution:** Provides a mechanism to e-mail reports automatically to multiple recipients in HTML, MHTML, PDF, Word, Excel and Text formats.
- SPAM, Spyware and Anti-Virus Reporting:** Provides details spam, spyware and viruses across the enterprise.

ISR provides a rich set of reports; following are the category of reports that are available

Reports	Description	Sub-Categories
Allowed and Denied	This report provides you the information on the top rules triggered for denied and allowed traffic. Examples:	Attacks, Events, Protocols, Top Content Categories , Events, Ports, Traffic, Users, Web Activity, Source, Destination, Rules
Attacks	This report provides information on the attacks, Event Code and description associated with the attack along with the Port information. It lists the total number of attacks and the percentage of a particular attack type from the total attacks identified on this Port.	Source And Destination Port, Day, Port, Rule, Target, URL, Source, Application, Device, Protocol, Attacker
Bandwidth	This report determines the amount of traffic from clients behind the devices, which are most heavily burdened with outgoing traffic. You can also use this report to compare the server load on different days considering total number of hits, bytes transferred, and cost of bandwidth.	Busiest Devices (Inbound and Outbound), Most Active Days (Inbound and Outbound), Users, Destinations, By Hour Of Day, (Inbound and Outbound), By Port, Usage (Inbound and Outbound)
Content Categorization	This report provides information on the Content Categorization that has been Permitted or Blocked for each Day. By default this query reports on recent thirty days data. Only top limited data is displayed in the report for the client information.	By Authenticated User, By Day, Hour Of Day, Source, Destination
Destination-Based Reports	This report contains information that helps the administrator in identifying which web pages were most accessed by which source IP from within the network.	Protocols, By Port, Allowed (Inbound & Outbound), Denied (Inbound & Outbound), Rules, Web Pages, Web Sites
Event Reports	This report provides information of the overall events by hour of the day when the event occurred together with the corresponding event code and description.	By Hour Of Day, By Severity, Events Triggered, Events Triggered By Severity, By Hour Of Day By Severity
Events	This report displays the top events considered critical. Only top limited data is displayed in the report for the client information. An event is critical if the Severity of the message is 2. Typically, Critical events relate to security rather than information services or data transfers.	Denied Connections Per Hour, Denied Outbound Traffic, Dropped Packets Summary, System Events Triggered
FTP Usage	This report identifies the top internal users engaged in FTP file transfers. The report shows the number of files transferred, the client names, and the amount of data transferred. Only top limited data is displayed in the report for the client information.	Users (Inbound & Outbound), By Day (Outbound),By Hour Of Day (Outbound)
Mail Usage	This report displays the top 'n' users of the e-mail service helpful in managing mail servers.	Users (Outbound), By Day (Outbound), By Hour Of Day (Outbound)
Protocol-Based Reports	This report shows the amount of traffic categorized according to the protocol families through the devices for each month. It also provides details of number of hits along with the transferred bytes for each protocol family.	By Source, By Hour Of Day, Families, Protocols (Inbound & Outbound), Usernames
Port-Based Reports	This report provides you the information on the top inbound and outbound ports from where the flow of net flow events was high.	Sources By Port, By Hour, Ports (Inbound & Outbound)
Rule-Based Reports	This report provides you the information on the top rules triggered for inbound and outbound data.	By Port, By Protocol, By Rule, Denied (Inbound & Outbound),-Allowed (Inbound & Outbound), Rules (Inbound & Outbound), Triggered, Denied Packets By Rule (Inbound & Outbound), Allowed Packets By Rule (Inbound & Outbound),
Source-Based Reports	This report shows the top 'n' Web Pages accessed by each internal user. You can use this data to verify appropriate use of bandwidth by user. It provides the client name, web pages accessed and bytes transferred by each client.	By Hour, Web Pages Per Source, Web Sites Per Source
Web Usage	This report shows the top web pages accessed on each site. You can use this data to determine most frequently accessed web pages by users.	Web Pages (Inbound & Outbound), By Site, Web Sites (Inbound & Outbound), By Usernames, Users (Inbound & Outbound), By Day (Inbound & Outbound), By Hour Of Day (Inbound & Outbound),
Users	This report provides you the information on the top authenticated users along with the number of times each user was authenticated	Authenticated Users, IP Addresses, By Direction