

# Filtering Network Traffic



## Solera Networks—See everything. Know everything.

If you're a network manager, you know that today's network infrastructure is only getting more complex. Network convergence is mixing new types of data with traditional network traffic; network pipes strain under ever-increasing loads; and each type of traffic brings its own demands, risks, and vulnerabilities.

And you're the person tasked with making sense of it all.

Fortunately, you've got all the tools you need. You've got protocol analyzers, intrusion detectors, and communications monitoring. They're all plugged into your network, throwing alerts whenever they notice something unusual, or recognize a known threat.

Unfortunately, these tools often fail to give you the context you need to really understand the problem. Is it a one-time thing—a confluence of random network events? Is it a trend that indicates network shortcomings you should be addressing? Is it part of a larger attack on your network's performance and security? With just an alert and some event logs to guide you, those questions can be very difficult to answer. What you need is a way to recreate the circumstances of the event and examine everything that was happening at the time. Once you can see the big picture you can drill down to the specific traffic and systems involved with the event to determine how best to address the problem.

## The Solera Networks Solution

Solera Networks gives you just such an opportunity through its DS series of deep packet capture and stream-to-storage appliances. Solera DS appliances function as network traffic recorders, capturing and storing all network data—every single packet—through a passive network connection.

To let you more easily analyze network events, the DS appliance provides a robust filter interface that gives you complete control over the capture and playback of network traffic. DS appliance filters provide the following:

- Apply both data capture (ingress filters) and data playback (egress filters).
- Filter traffic based on packet type, device address, or time (playback only).
- Simple scripting language lets you create filters as complex or simple as you need.
- Create filters by including or excluding traffic from capture or playback.
- Layer multiple filters together. The DS appliance applies active filters sequentially to each packet that it sees to determine if it should be captured or played back.

Filters maximize the utility of each appliance by letting you manage limited resources such as disk space and maximum throughput. For example, you might apply ingress filters to exclude redundant or unrelated data, thus saving disk space. Similarly, you might apply egress filters to limit the data you need to review (by packet type, by transmitting/receiving address, or by time period).

Solera Networks DS appliances let you shape network traffic for your monitoring and analysis tools with input and output filters:

- **User Filters:** Create filters to isolate traffic to and from a specific user's system.
- **Application Filters:** Create filters to isolate traffic to and from most any application, including Email, Instant Messaging, and Web traffic.
- **Protocol Filters:** Create filters to isolate traffic of a particular sort. For example, FTP, DNS/DHCP, HTTP, SNMP.
- **Content Filters:** Create filters to isolate traffic based on keywords, node names, interface names, or any other traffic identifier.
- **Pattern Filters:** Create filters to isolate traffic based on any data pattern or string.

## Configuring Network Traffic Filtering – Procedure at a glance

Configuring a filter for a Solera DS appliance requires familiarity with network concepts, technologies, and protocols; as well as a knowledge of the scripting language used to create filters. For more information about Solera's filter scripting language, see the Filter Scripting User Guide.

When creating filters, Solera recommends using the Web Console, from which you can configure all aspects of your DS appliance. Creating a filter with the Web console involves the following general steps. For detailed instructions, see the Solera Installation and User Guide.

**1. Connect the DS Appliance to your network** Solera DS appliances provide multiple Ethernet ports that you can use to connect to your network. You can connect to multiple networks simultaneously, if desired. Use copper or SR fiber cables to connect to the network through either a network tap or switched port analyzer (SPAN). SPAN ports must first be configured to mirror packets from other selected ports of the network router or switch.

**2. Define Packet Filters** The Web console Filters page lists all currently defined filters, and lets you create, edit, and delete filters. When creating filters, use filter script to specify the types of traffic, the source or destination devices to include/exclude, and the Ethernet ports to which this filter should be applied. When finished, name the filter and save it.



If desired, use the Web Console Playback page to restrict playback to a particular time frame. This lets you drilldown to a particular period of time before applying filters and outputting the resulting data for analysis.

Review all filters carefully to make sure that no filter will prevent the DS appliance from capturing the network data you might need.

**3. Start Recording Network Traffic** The Web Console Record page lists all physical Ethernet ports available in the DS Appliance. To start recording, simply click the Record button next to the active port through which you want to capture traffic. This is the Live Data Port.

## Conclusion

The complexity of today's network environments makes traffic and event monitoring critical to maintaining network performance and limiting exposure to internal and external threats. Solera Networks deep packet capture and stream-to-storage appliances let you control network traffic delivery to your monitoring and analysis tools so you can get the very most out of your tool investment. Now you can identify weaknesses, spot trends, and track down bad guys without affecting the performance or operation of your live network.

© 2008 Solera Networks. All rights reserved. Solera Networks, Solera DS Series, DeepSee, Solera V2P Tap, DS 1150, DS 3150, DS 5150, and See everything. Know everything. are registered trademarks of Solera Networks. All other company names, brand names and product names are the property and/or trademarks of their respective companies.

## Contact Solera Networks

### Solera Networks Headquarters

355 South 520 West, Suite 225  
Lindon, Utah 84042  
1 877-5SOLERA (877-576-5372)  
1+ 801-623-5705 • 1+ 801-623-5706 fax  
Email: [info@soleranetworks.com](mailto:info@soleranetworks.com)

### Solera Networks Japan, Inc.

Shinjuku Park Tower N30F  
3-7-1, Nishi-Shinjuku  
Shinjuku-ku, Tokyo 163-1030  
1+ 81-3-5326-3367 • 1+ 81-3-5326-3001 fax  
Email: [info@soleranetworks.co.jp](mailto:info@soleranetworks.co.jp)



See everything. Know everything.™