NetFlow Monitoring Foundation Package Release Notes

A Standard Content Foundation Package
for ESM v4.5 SP2 and v5.0 GA, and
ArcSight Express v4.5 SP2

Version 1.0

August 25, 2010

NetFlow Monitoring Foundation Package Release Notes, A Standard Content Foundation Package for ESM v4.5 SP2 and v5.0 GA, and ArcSight Express v4.5 SP2

Revision History

Date	Product Version	Description
08/25/2010	ESM Standard Content Pack for NetFlow Monitoring v1.0	Initial version of the NetFlow Monitoring Foundation Package.

Release Notes template version: 1.0.5

ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail	support@arcsight.com
Support Web Site	https://support.arcsight.com
Customer Forum	https://forum.arcsight.com

Contents

NetFlow Monitoring Foundation Package Release Notes

NetFlow is a network protocol developed by Cisco Systems to run on Cisco IOS-enabled equipment for collecting IP traffic information. It is proprietary, but supported by platforms other than Cisco IOS, such as Juniper routers and Linux.

NetFlow provides session-level data. Leveraging this information using your ArcSight SIEM solution can help to monitor network bandwidth usage and correlate it with other security logs (such as firewall, IDS, authentication logs, and so on).

The Netflow Monitoring Foundation Package provides resources to monitor and report on top bandwidth usage by source, destination and port. The Netflow Monitoring Foundation Package is available for ArcSight™ ESM v4.5 SP2 and v5.0 GA, and ArcSight Express v4.5 SP2.

NetFlow Monitoring Foundation Package Contents

The files included in this release are:

File name	Description
ESM-AE_NetFlow_Foundation_RelNotes_v10.pdf	Product description and open issues
ESM-AE_NetFlow_FoundationGuide_v10.pdf	Installation and operation instructions
NetFlow_Monitoring_v1.0.arb	Product package bundle

Installing the NetFlow Monitoring Foundation Package

The NetFlow Monitoring Foundation Package is designed for installation on an ArcSight ESM v4.5 SP2, ArcSight ESM v5.0 GA, or ArcSight Express v4.5 SP2 Manager. Complete installation instructions are located in the *NetFlow Monitoring Foundation Package Guide* (ESM-AE_NetFlow_FoundationGuide_v10.pdf).

Open Issues in this Release

This release contains the following open issues. Use the workarounds noted, where available.

Number	Description and work-around instructions
ESM-41714 TTP#69822	The moving average data monitor shows a lower value for average bytes per second than is accurate. The data monitors affected are: • `/All Data Monitors/ArcSight Foundation/NetFlow Monitoring/Inbound Bandwidth (Bytes Per Second)` • `/All Data Monitors/ArcSight Foundation/NetFlow Monitoring/Outbound Bandwidth (Bytes Per Second)` **Workaround**: None.
ESM-41687 TTP#69751	The bar charts representing the Top Bandwidth Usage by Well-Known and Not Well-Known Ports data monitors in the Top Newflow Bandwidth Usage Monitoring dashboard can render the port number results in a bar that is too narrow to read. Ports can range from 0 to 65535, and the x-axis scales serially to fit the largest value reported. The well-known ports data monitor covers ports numbered 0 to 1024, and the non-well-known ports data monitor covers ports numbered 1025 to 65535. NetFlow events containing port numbers in the high range cause the vertical bar to be narrow. **Workaround**: None.
ESM-41703 TTP#69789	If 'no group' by value is used for a field in a moving average data monitor, the tooltip shows '`--,`'. For example, in the Outbound Bandwith data monitor in the dashboard `/All Dashboards/ArcSight Foundation/NetFlow Monitoring/NetFlow Bandwidth Usage Overview`, mousing over the timestamp returns the following tooltip: '`--, 8/4 9:19:55`'. If no 'group by' value is specified, the tooltip should just show the timestamp. **Workaround**: None. The characters can be safely ignored.
ESM-45563	When installing the NetFlow Monitoring Foundation Package on ESM v5.0, the Network Filters package is linked in two groups: `/All Packages/ArcSight Foundation, and /All Packages/ArcSight Foundation/Shared Libraries`. This is because the Network Filters package, a package installed by default with ESM, is stored in the Shared Libraries group in ESM v5.0, and directly in the ArcSight Foundation group in ESM v4.x. **Workaround**: None. The link causes no harm or unexpected behavior.