Preface

This white paper will describe the different data flows between the Steelheads, SteelEye agent, SteelEye proxy and SteelEye backend system. It will describe the different protocols used and who initiates the traffic. Furthermore it will give an in-depth technical description of firewall rules needed at the customer site.
SteelEye is based on an "agent" design; this means that an agent is introduced into the customer network. This agent is the turning point of data collection and reporting it back to the SteelEye backend system.

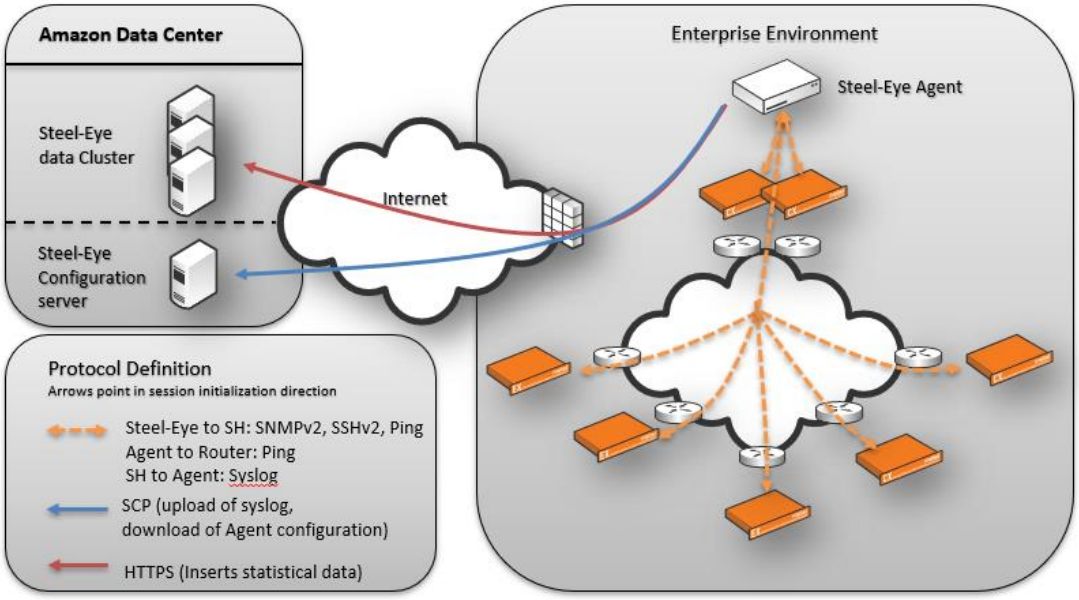
SteelEye Traffic Flow Document

Data Collected in the Enterprise Environment

Data is collected through SNMP, Command Line Interface (CLI) interrogation, Pings and System Log (Syslog) interpretation to provide a complete picture for each Steelhead in an estate. Syslog is a continuous flow of data that is analysed for specific faults and errors and the result is saved in memory ready to be sent back to the SteelEye backend. Furthermore the raw logs are sent back and kept for debugging purposes for instance doing a support ticket or an RMA process. The logs are not directly available, but can be requested.

SteelEye collects monitors and analyses Steelhead management data only. SteelEye does not collect, monitor or analyse any company information moving through the steelhead.

SteelEye Diagram



About Hawk-Eye
Hawk-Eye is a Professional Services only company. Providing solutions and services to Riverbed® Channel Partners, Service Providers, Systems Integrators and end-users globally. These solutions and services enable partners and customers to realise the maximum potential of their Riverbed WAN acceleration investment.

By enabling an environment to be constantly monitored, tuned and configured to address changing environments and needs. Hawk-Eye delivers the Riverbed Performance Availability Monitoring Service (SteelEye) on behalf of Riverbed and a range of assessment services that support the pre and post sales cycles, trouble-shooting and upgrading/scaling a Riverbed deployment. Hawk-Eye solutions and services include; training, design, support, monitoring and reporting. Hawk-Eye is a Riverbed Authorized Consultancy partner (ACP) and a Riverbed Authorized Training Partner (ATP).

Additional information about Hawk-Eye is available at www.hawk-eye.eu

Communicating with the Data Centres

The Agent appliance uses a HTTPS REST API to communicate with the SteelEye data servers on TCP port 9997 and SCP access to SteelEye configuration server on TCP port 2222.

SteelEye configuration server

The agent appliance connects using SCP to the SteelEye configuration server. Once a connection is made it has to authenticate using its private certificate.
There is no reverse traffic allowed from the SteelEye configuration servers to the agent.
The encryption used between the SteelEye agent and the Configuration server defaults to the arcfour256 encryption, but the server supports the following encryption types: aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc

SteelEye data cluster

After the agent has authenticated it then uses the HTTPS (TLS, ECDSA with SHA256) session to encapsulate the HTTP REST API calls to the SteelEye data servers. The authentication on the SteelEye data servers is done through a SSL certificate encrypted with a strong password, to enforce customer security. There is no API call to download data that has been uploaded, so once the data has been uploaded it cannot be retrieved again, meaning it is not visible to anyone else than the SteelEye data servers.

Firewall rules

Agent to Remote Sites	**Remote Sites to Agent**	**Agent to SteelEye Data Centres**

As described earlier, we use the following protocols from the SteelEye agent to the Steelhead appliances.
 	
Here are the ports needed:
• SNMPv2, udp/161
• SSHv2, tcp/22
• Ping, ICMP echo
 	
Furthermore, the agent must also be able to ping the default gateway of the Steelhead appliance primary interface to check if the link is up or not.
	All Steelhead should be configured to send INFO level syslog to the SteelEye agent for detailed analysis.
	
	Here is the port needed:
	• Syslog, udp/514
		The agent relies on 2 ports and several IPs to communicate with the backend servers.
		All protocols used are encrypted.
		
		Here is the ports and destination IPs:
		• SSH, tcp/2222 to 52.59.102.56
		• HTTPS, tcp/9997 to
		  ○ inputs1.hawk-eye.splunkcloud.com
		  ○ inputs2.hawk-eye.splunkcloud.com
		  ○ inputs3.hawk-eye.splunkcloud.com
		  ○ inputs4.hawk-eye.splunkcloud.com
		  ○ inputs5.hawk-eye.splunkcloud.com
		  ○ inputs6.hawk-eye.splunkcloud.com
		  ○ inputs7.hawk-eye.splunkcloud.com
		  ○ inputs8.hawk-eye.splunkcloud.com
		  ○ inputs9.hawk-eye.splunkcloud.com
		  ○ inputs10.hawk-eye.splunkcloud.com