HAWK-EYE

RIVERBED PERFORMANCE MONITORING

www.hawk-eye.eu

Steel-Eye Traffic Flow Document

Preface

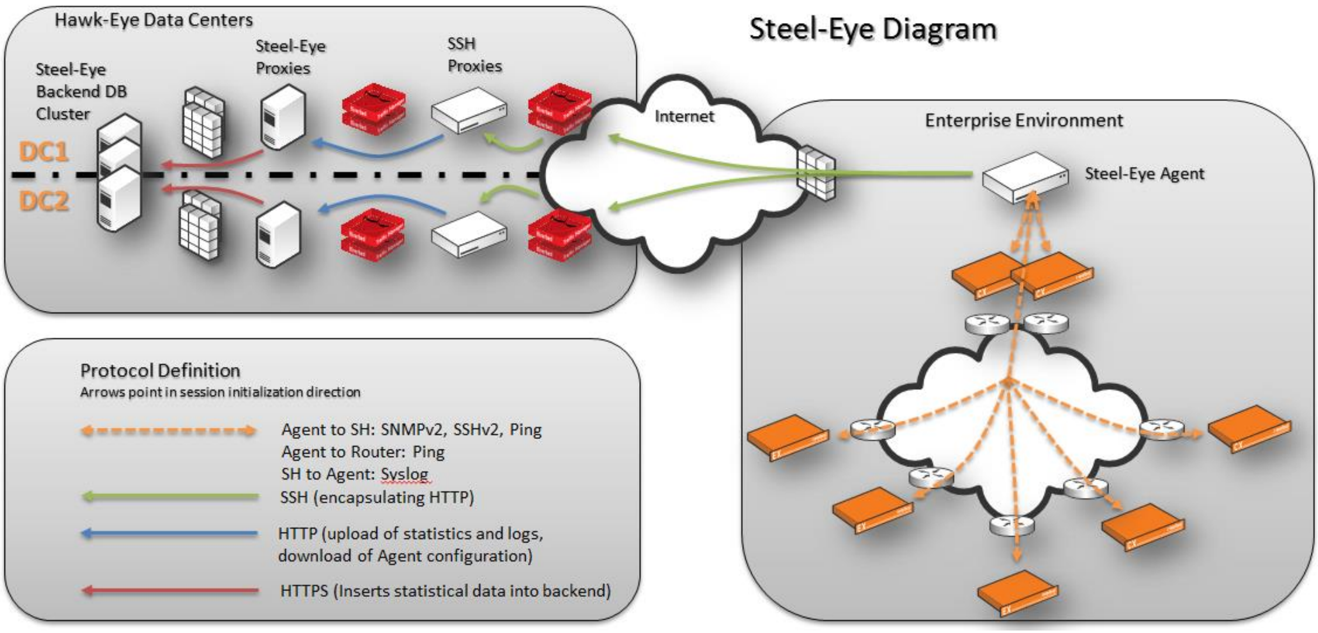
This white paper describes how data flows between the Steelheads, Steel-Eye agent, Steel-Eye proxy and Steel-Eye backend systems, the different protocols used and who initiates the traffic. It also provides an in-depth technical description of the firewall rules needed at the customer site. Steel-Eye is based on an "agent" design, this means that a collection device installed in the customer's network, this device receives data from all Steelheads in the network, compresses and de-duplicates, and @12 times per hour transmits the Steelhead management information to the Data Centre for storage and analysis.

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 Steel-Eye 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

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

Steel-Eye Diagram


Hawk-Eye Data Centers
Steel-Eye Backend DB Cluster
Steel-Eye Proxies
SSH Proxies
DC1
DC2
Internet
Steel-Eye Diagram
Enterprise Environment
Steel-Eye Agent
Protocol Definition
Arrows point in session initialization direction
Agent to SH: SNMPv2, SSHv2, Ping
Agent to Router: Ping
SH to Agent: Syslog
SSH (encapsulating HTTP)
HTTP (upload of statistics and logs, download of Agent configuration)
HTTPS (Inserts statistical data into backend)

Communicating With the Data Centres.

The Agent appliance uses a HTTP REST API to communicate with the Steel-Eye Proxies, but to access those servers it is required to access the internal customer zone in the Steel-Eye datacenters. This is done through the SSH Proxies.

SSH Proxies

The agent appliance connects using SSH to the Stingray load balancers, traffic is then forwarded to the least loaded SSH Proxy, once a connection is made it has to authenticate using its private certificate (unique for each Steel-Eye agent).
There is no reverse traffic allowed from Steel-Eye back into the customer's network.
The encryption between the Steel-Eye agent and the SSH proxies defaults to the arcfour256 (aka ARC4 or RC4) encryption, but the server supports the following encryption types (prioritized order): arcfour256, arcfour128, aes256-ctr, aes192-ctr, aes128-ctr, blowfish-cbc, 3des-cbc.

Steel-Eye Proxies

After the agent has authenticated it can then use the SSH session to encapsulate the HTTP REST API calls to the Steel-Eye Proxy though another set of Stingray load balancers. The authentication on the Steel-Eye Proxy is done though a cookie in the HTTP header (MD5 sum of date and time, URL, appliance Id, appliance password), to enforce customer security. Each http

REST call requires a new session cookie as the date and time is included, to prevent replay attacks (allowed time skew is 600 seconds). 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 Steel-Eye Proxy itself.

Once the data has been written to disk, there is another process that is responsible for reading the data and inserting it into the backend for permanent storage, at this time the data is flushed from the Steel-Eye Proxy system

Firewall Rules

Agent to Remote Sites	**Remote Sites to Agent**	**Agent to Steel-Eye Data Centres**
As described earlier, we use the following protocols from the STEEL-EYE agent appliance 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 agent appliance for detailed analysis. Here is the port needed: • Syslog, udp 514	The agent only relies on a single port and IP to communicate using SSH. All other protocols are encapsulated in SSH and will therefore not be visible to the firewall, please note that it is NOT the default SSH port! Here is the port and destination IP: • SSH, tcp/2222 to 77.243.49.73 77.243.49.73 is the VIP on the Stingray load balancers