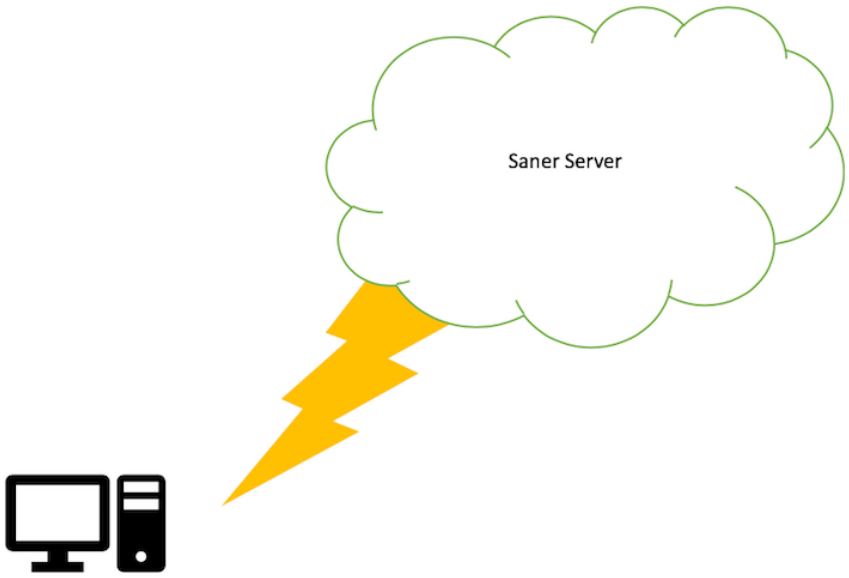
SanerNow 4.1.1.0: Empowered with Real Time Visibility

Overview

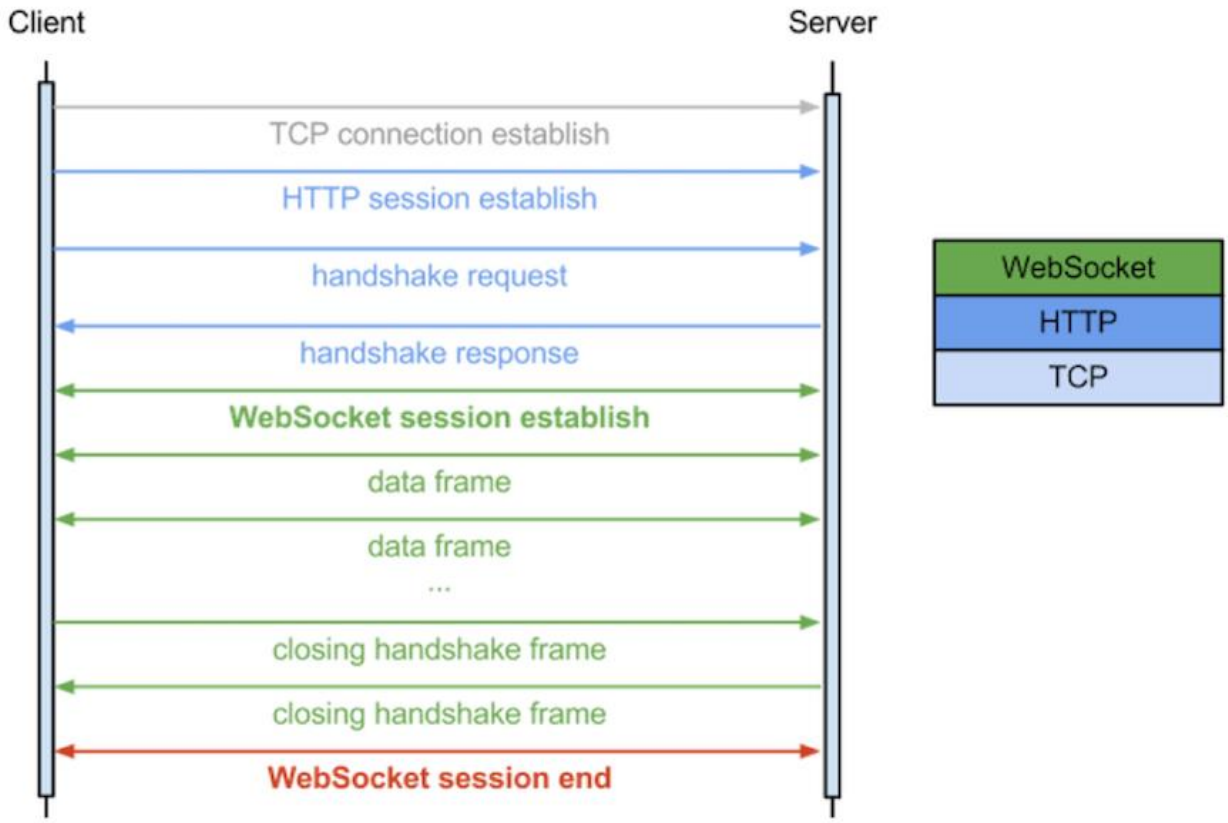
Visibility is key to securing IT infrastructure and SanerNow is enriched with many tools to provide clear insight into organization's endpoints. When it comes to defending an attack or detecting and remediating risks and threats, how fast an administrator can respond to such events and take preventive measures makes a security software product effective. With SanerNow 4.1.1.0, we are introducing live mode interaction between endpoints and Saner server. Using SanerNow, one can reach out to endpoints in real-time and perform queries and actions.



In older versions of SanerNow, the communication between endpoints and the server was a one-way poll mechanism. The poll interval played crucial part since it determined the speed at which an Administrator can act upon an incident. SanerNow version 4.1.1.0 comes with live mode of interaction between Saner server and agents which enables real-time communication between them. Live mode is empowered with WebSocket which uses traditional HTTP channel and turns it into a two-way communication model.

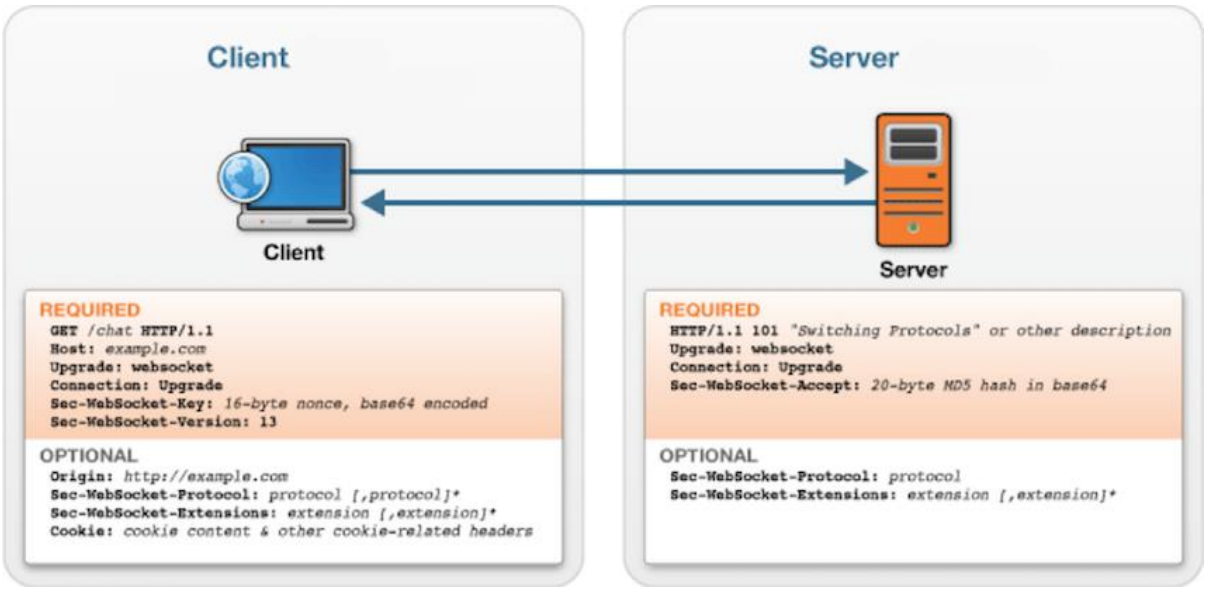
An Insight into Live Mode of Communication

Live mode is empowered by WebSocket protocol implementation between Saner server and Saner agents. WebSocket provides full duplex connection between client and server with low latency. This works over HTTP, by establishing an HTTP connection and then upgrading it to WebSocket connection which uses the same underlying TCP connection.WebSocket connection establishment uses HTTP Upgrade Header parameter to elevate from HTTP protocol to WebSocket Protocol. WebSocket Protocol is an independent TCP protocol and its only relation with HTTP Protocol is the initial handshake, which is HTTP upgrade request. WebSocket implementations can use Ping-Pong mechanism where heartbeats can be exchanged between client and server to keep the TCP connection alive.



WebSocket Connection Life Cycle

When Saner Agent receives instruction to switch communication channel between “Poll” to “Live”, it establishes a secure WebSocket connection with the Saner server and remains connected to receive further instructions and requests from server. This enables Saner to present security posture of an organization at any point with minimal latency.



WebSocket Handshake

Life Cycle of a WebSocket can be seen in three sections; a handshake, data transfer and closing of an established WebSocket connection. WebSocket protocol implements data transfer by sequence of frames. Fragmentation is possible in data frames this enables the protocol to support the transfer of unknown size messages. Frames are defined by an opcode, payload length and the payload. There are majorly two categories of frames, control frames and data frames.

Control Frames

Control frames are used to communicate about the state of WebSocket. Control frames must not be fragmented. There are three control frames,

1. Closing control frame - This frame is used to communicate that WebSocket is going to closed state.
2. Ping Control frame & Pong control framePing – Pong frames is used for keeping the underlying TCP connection alive, these frames can also contain application data.

Data Frames

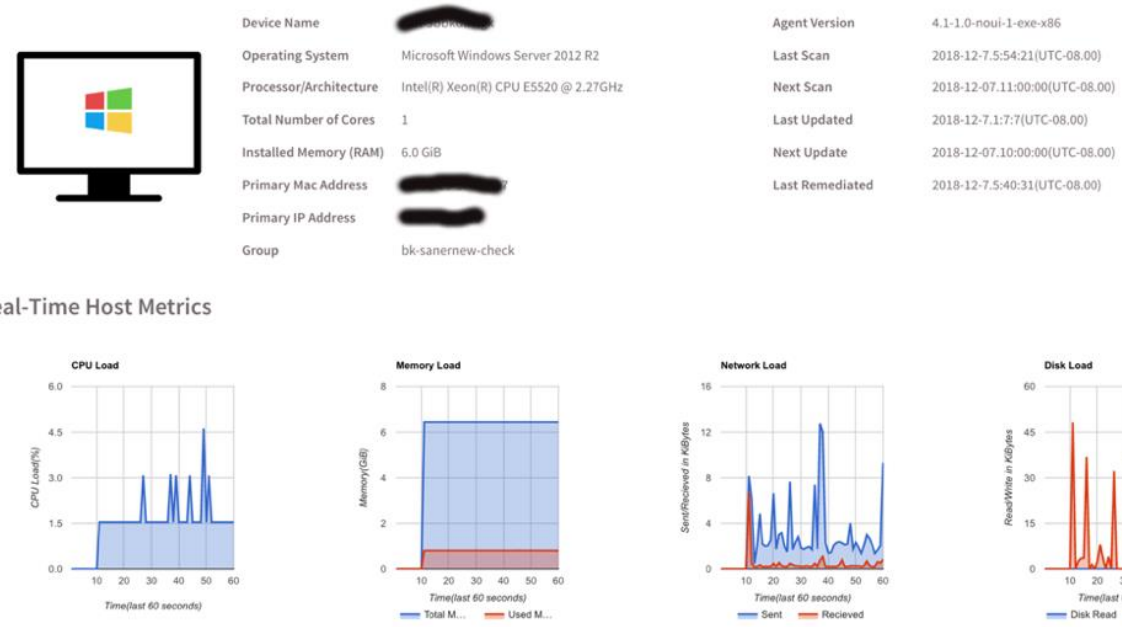
Data frames carry application layer date, the opcode determines the interpretation of the data being transmitted. Both binary and text data transfer is supported by the protocol. Opcode 0x1 and 0x2 defines text and binary data frames respectively. All frames sent from client to server must be masked with 32 bit key.

Server will and should close the connection upon receiving an unmasked frame and should return protocol error as response status. Masking is enforced irrespective of whether SSL/TLS is used in

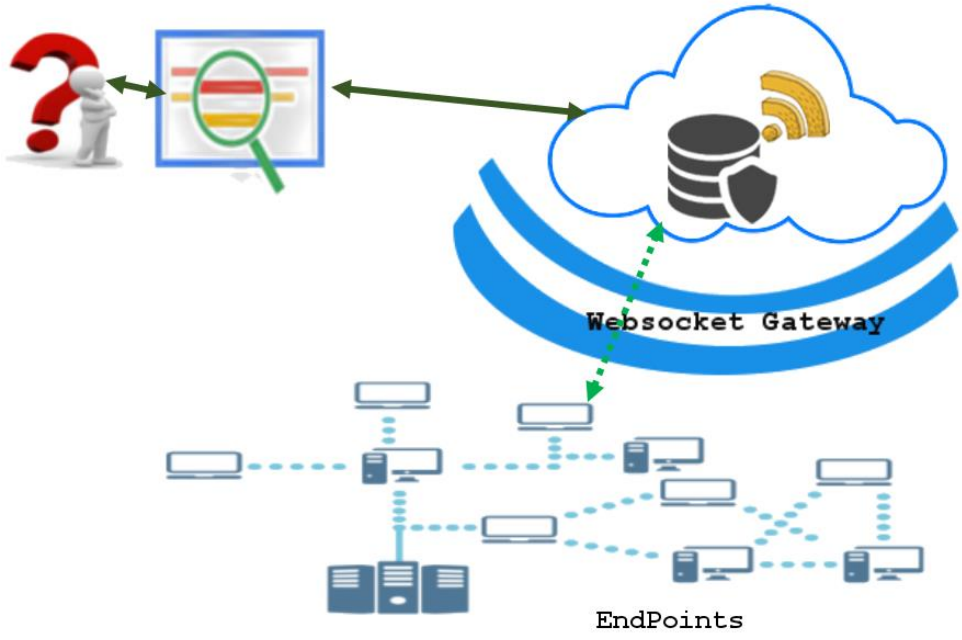
WebSocket. And all the frames from server to client must be without any mask, client should close the WebSocket connection if any masked frame is received at the client side.

Benefits to SanerNow

1. Continuous and instant system health monitoring capability

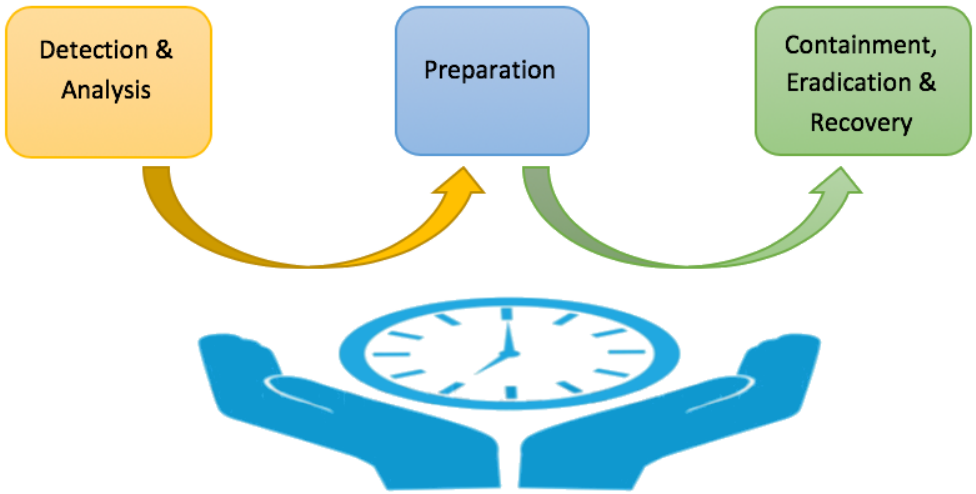


2. Real-time querying of system security posture



SanerNow can run queries in real-time and fetch results from number of endpoint systems in a matter of few seconds. Fetch all open ports, search for abc.exe process across all systems, fetch a registry entry, get installed applications, search for a presence of a file are all immediate. It can also initiate instant system wide scanning.

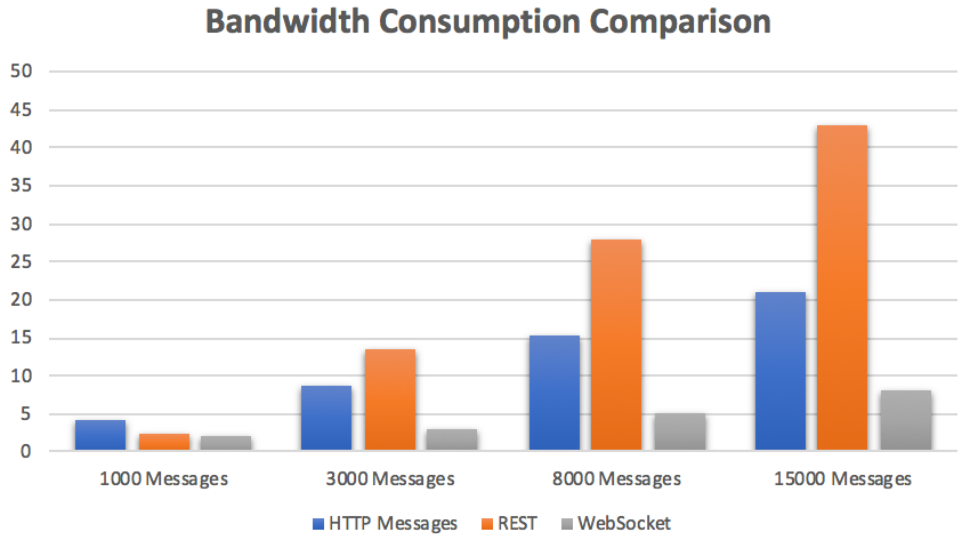
3. Real time interface to take any incident response measures



WebSocket ensures Real Time interaction with Saner Agents

SanerNow can initiate any response actions to endpoints across the organizations and endpoints receive it instantly and act upon the commands. Stop a service, kill a process, clean up a registry key, kill a network connection, remove an adware application, clean up ARP/DNS cache are a few examples.

4. Low Network Bandwidth consumption



Since the poll mechanism between Saner agent and Saner server involves HTTP GET/POST requests, it had an overhead in terms of HTTP connection establishment and header transfers. Live mode of communication removes all these overhead of PROTOCOL handshakes header exchanges in each message passing between Saner server and the agent