Security Management System – Remote Client

In most of the deployment scenarios, the server application is hosted on a computer which is on the internal network of an enterprise. Hence it is not accessible from the client applications running on computers outside this internal enterprise network. This is common practice followed for security of computers on the internal network.

However in some case, it may be needed to grant access to a few client applications which are not in the local network – same network as server computer. Such client applications are called as ‘remote clients’. Port forwarding on the router, is a commonly used method for allowing access to the remote clients, still maintaining the security of the network.

This document explains the configurations needed to expose the Security Management System Server software to the remote client, running on an external network.

1. In the server software, please go to the ‘Communication’ tab in the left navigation menu bar. Go to the ‘Network’ sub-tab under it.

2. This will display the Network Settings page.

Security Management System – Remote Client
3. Please note following settings on this ‘Network Configuration’ page –
   (a) Output IP address
   (b) TCP port 1
   (c) RTSP port (TCP)
   (d) RTP port (UDP)
   (e) RTCP port (UDP)
   (f) HTTP port (TCP)
   Note - Out of these; TCP port 1, RTSP port (TCP), RTP port (UDP), RTCP port (UDP), HTTP port (TCP) are read-only settings and can not be configured by the user.

4. Configure the router or firewall in the network, to expose the ‘Output IP address’ and all the ports listed above, to external network. List the mapping table, as follows –

<table>
<thead>
<tr>
<th>Server software</th>
<th>Router / Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>192.168.0.58</td>
</tr>
<tr>
<td>TCP port 1</td>
<td>123.201.32.36</td>
</tr>
<tr>
<td>RTSP port (TCP)</td>
<td>5500</td>
</tr>
<tr>
<td>RTP port (UDP)</td>
<td>9100</td>
</tr>
<tr>
<td>RTCP port (UDP)</td>
<td>1024</td>
</tr>
<tr>
<td>HTTP port (TCP)</td>
<td>20000</td>
</tr>
<tr>
<td></td>
<td>9104</td>
</tr>
</tbody>
</table>

Notes –
(a) This table is only an example and actual values, will change depending on the network configuration at the deployment site
(b) The values in this table related to the Server Software, should be the same ones as displayed in the ‘Network Settings’ page (as described in point 2 in this document)
(c) The values in this table related to the Router / Firewall, should be the values configured in the router / firewall for port forwarding
(d) During port forwarding configuration on the router / firewall, please allow incoming as well as outgoing traffic and for both TCP and UDP, for all ports being configured for port forwarding.

5. Install the Security Management System Client Software on the remote computer.

6. Please make sure that the remote computer is able to access the computer where Management System Server Software is running, through the port forwarding. Using the standard ‘Ping’ command to ping the router/firewall IP address, can be a good initial test

7. Install and execute the client software on the remote computer. It will pop up the ‘Server Connection’ dialog box.
8. In the ‘Server IP Address’ input, type IP address of the router

9. Check / select the ‘Port forwarding’ enabled on the server’ check-box.
   Type the values for TCP port 1, RTSP port (TCP), RTP port (UDP), RTCP port (UDP), HTTP port (TCP). These should be the same values, mentioned in the mapping table for ‘Router / Firewall’, in point 4 of this document

10. The client will be able to communicate with server now and the client software user interface will be launched.

Notes –

(a) It is very important to have sufficient and consistent bandwidth available between the server and the client. Recommended minimum bandwidth is 2 mbps

(b) If sufficient and consistent bandwidth is not available, client may not be able to finish the initial handshaking after communication and may keep trying to complete it. The client user interface will not be displayed till client finishes the initial handshaking.

(c) The initial handshaking bandwidth requirement varies depending on the cameras authorized for the user logging in from the remote client. Hence for initial tests, during the configuration, it is recommended to create a new privilege in the server software, with authorization for only a few
cameras; and creating a new user with this new privilege; and using the new user credentials for logging in from the remote client.

(d) After initial handshaking, client will start displaying videos. The client has built-in bandwidth optimization, to allocate equal bandwidth for each camera viewed in the client application. Hence if sufficient and consistent bandwidth is not available, videos will be displayed at lower resolution.