Product Support Notice

PSN # PSN003314u

Original publication date: 16-May-11. This is Issue #05, published date: 31-Mar-14.

Severity/risk level: High

Urgency: Immediately

Name of problem

SAL Gateway default IP, Proxy Server Host name, Policy Server Host name, Secondary Core Server Host Name and Secondary Remote Server Host Name points to invalid servers which are not owned by Avaya. This can pose a security threat and suspicious activity can be logged in customer firewall logs.

Products affected

Secure Access Link (SAL): Releases, 1.5, 1.8, and 2.0

System Platform: Releases 1.1 (contains Secure Access Link (SAL) 1.5) and 6.0.X (contains Secure Access Link (SAL) 1.8)

Problem description

On a non-interactive installation of SAL Gateway the default properties are provided with the installer. This installer provided defaults for the SAL Gateway IP address, the Proxy Server Host Name, a Policy Server Host Name, the Secondary Core Server Hostname and a Secondary Remote Server Host Name addresses which are invalid public domain servers and NOT owned by Avaya. The defaults point to **123.124.123.234**, **customerproxy.com, custpolicyserver.com**, **secavaya.com** and **secaxeda.com** respectively. These servers resolve to invalid domains and pose a security threat in that they were not intended to be used, but may be used if the SAL GW is not properly configured.

Customers may report observed suspicious usage of the default addresses if the SAL GW is enabled but not properly configured. Some behaviors that may be seen include traffic to the wrong servers due to the default values: 1) SSH used to the default 123.124.123.234 SAL GW as part of a SAL GW collector process that may run periodically to test for the SAL GW management port. 2) HTTP traffic to an unconfigured default server address or 3) HTTPS traffic to a default server address.

The intended configuration is that the SAL Gateway IP address should be configured to the actual gateway machine IP address. The Proxy server host name should be configured to the actual customer proxy server host name (if required). The Policy server host name should be configured to the actual Avaya policy server host name (if required). The Secondary Core Server Hostname should be configured to the same address as the Primary Core Server Hostname. And the Secondary Remote Server Host Name should be configured to the same address as the Primary Remote Server Host Name.

Resolution

To avoid the security issues, please perform the following steps. These steps are applicable to standalone SAL gateway as well as for SAL gateway that are on System Platform.

In case of a SAL gateway that is on System Platform and not intended to be used then there is a provision in System Platform 6.0.X to disable the SAL Gateway. However same option is not available in System Platform 1.1 release. If the SAL Gateway is disabled on System platform 6.0.X, then following steps are not technically required but recommended to be applied before disablement.

NOTE: Typographic errors can also yield improper or suspicious activity when not properly configured. For example, avay.com is NOT a valid Avaya domain and not owned by Avaya, and there may be others. Please check values entered carefully for accuracy.

Please follow the below steps for proper configuration:

1. Login to the SAL Gateway UI with the user having either Security Administrator or Administrator role.
2. Navigate to the Administration section of the SAL Gateway menu, click on “Gateway Configuration”
3. In the ‘Gateway IP Address’ field, enter the actual SAL Gateway machine IP.
4. Navigate to the Administration section of the SAL Gateway menu, click on “Proxy” (Only for ver. 1.8, 2.0)
5. If proxy server is not needed then uncheck ‘Use Proxy’ checkbox and click on ‘Apply’. If it is needed then change ‘Host’ and ‘Port’ settings with actual values and click on ‘Apply’.
6. Navigate to the Administration section of the SAL Gateway menu, click on “Policy Server” (Only for ver. 1.8, 2.0)
7. If policy server is not needed then uncheck ‘Use a Policy Server’ and click on ‘Apply’. If it is needed then change ‘Server’ and ‘Port’ settings with actual values and click on ‘Apply’.
8. Navigate to the Administration section of the SAL Gateway menu, click on “SAL Enterprise” (ver. 1.5, 1.8) / “Core Server” (ver. 2.0).
9. In the “Secondary Enterprise” (ver. 1.5, 1.8) / “Secondary Core Server” (ver. 2.0) field, enter the host name same as the “Primary Enterprise” (ver. 1.5, 1.8) / “Primary Core Server” (ver. 2.0) hostname.
10. In the Port field for Secondary server, enter the port number same as that for the Primary one.
11. Click on Apply.
12. Navigate to the Administration section of the SAL Gateway menu; click “Remote Access” (ver. 1.5, 1.8) / “Remote Server” (ver. 2.0).

13. In the “Secondary Server Host Name / IP Address” (ver. 1.5, 1.8) / “Secondary Remote Server” (ver. 2.0) field, enter the hostname same as the “Primary Server Host Name / IP Address” (ver. 1.5, 1.8) / “Primary Remote Server” (ver. 2.0).
14. In the Port field for Secondary server, enter the port number same as that for the Primary one.
15. Click on Apply.
16. Navigate to the Administration section of the SAL Gateway menu, click on “Apply Configuration Changes”
17. Click on ‘Apply’. It will restart SAL gateway services to affect the changes.
18. Logout from the Gateway UI.

NOTE: Only disable the SAL GW in System Platform 6.0.X if you are sure it is not being used.

To disable an UNUSED SAL GW in System Platform 6.0.X follow these steps:

- Login to System Platform cdom webconsole.
- In the navigation pane, click Server Management > SAL Gateway Management.
- On the SAL Gateway Management page, click Disable SAL Gateway.

  In System Platform 1.1, the service for SAL GW could be stopped but it would restart after a reboot or power cycle. Therefore, for System Platform 1.1, it is critical that the steps above to reconfigure the defaults have been applied.

Workaround or alternative remediation

SAL GW releases starting with 2.1 have removed the defaults and may be installed as a standalone SAL GW installation.

Remarks

n/a

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

n/a

Download

n/a

Patch install instructions	Service-interrupting?
There is a patch available for the System Platform products, depending on the compatibility of the products supported by the System Platform. For more information look for the appropriate System Platform PSN(s).	Yes

Verification

n/a

Failure

n/a

Patch uninstall instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

Described above.

Avaya Security Vulnerability Classification

High

Mitigation

n/a

For additional support, contact your Authorized Service Provider. Depending on your coverage entitlements, additional support may incur charges. Support is provided per your warranty or service contract terms unless otherwise specified.

Avaya Support Contact	Telephone
U.S. Remote Technical Services – Enterprise	800-242-2121
U.S. Remote Technical Services – Small Medium Enterprise	800-628-2888
U.S. Remote Technical Services – BusinessPartners for Enterprise Product	877-295-0099
BusinessPartners for Small Medium Product	Please contact your distributor.
Canada	800-387-4268
Caribbean and Latin America	786-331-0860
Europe, Middle East, and Africa	36-1238-8334
Asia Pacific	65-6872-8686