Avaya™ G700 Media Gateway Security - Issue 1.0

Avaya™ G700 Media Gateway Security Summary

With the Avaya™ G700 Media Gateway controlled by the Avaya™ S8300 or S8700 Media Servers, many of the traditional Enterprise Communication System security issues have been addressed. Issues such as toll fraud and the remote access security have been addressed by adding enhanced security features in the switch's software and by adding adjunct security hardware. For example, remote access has been secured by employing the Access Security Gateway (ASG) software in the switch and by establishing a secure remote access architecture using the customer's AAA server, and the Secure Remote Access (SRA) device employed in the Avaya™ Enhanced Secure Remote Access Service (ESRAS) offer.

The primary new ports for attack on the G700 Media Gateway are the IP trunks and the LAN. The open source operating systems (Linux and VxWorks) can also be security concerns if not properly configured.

Avaya has taken measures with the Linux base to ensure operating system security issues have been addressed with the. These include:

- Disabling unneeded services and ports
- Limiting permissions
- Locking out logins if the maximum number of login attempts fail in a predefined time
- Adding SSH (Secure Shell) for secure login.

In addition, Avaya will ensure the Linux base provides maximum security by testing the software against the latest system security tools. Investigation of additional security features and technology is currently underway to further minimize security issues in future releases of the G700 Media Gateway.

Recommendations for Securing the Avaya™ G700 Gateway in Converged Networks

Avaya makes these recommendations to maximize protection of your network against security violations.

1) Firewalls and routers provide the first line of defense against DoS and other types of attacks and should be used to protect all appropriate ports

2) It is recommended that the one criterion customers use to select firewalls is their resistance to DoS attacks. Be aware that there may also be performance and other tradeoffs when selecting DoS resistant firewalls

3) Customers should also routinely test their firewalls against a range of attacks to detect new vulnerabilities and miss configured firewalls

4) Customers can guard against eavesdropping by physically securing all of their network components (e.g. Firewalls, Routers, and Hubs) and by buying equipment that is tamper evident and resistant

5) Firewalls and Routers that implement, and are managed by, an SNMPv3-based network management system are recommended (vs. SNMPv1 or SNMPv2) because the security of SNMPv3 can prevent unauthorized updates to the routing tables and access control list by an intruder. Layer 2 switches are preferred to Hubs that broadcast information to every port and thus provide an eavesdropping opportunity.

6) If any of the following usage or patterns suddenly appears on call records or the customer receives complaints that their system is "always busy", they should investigate immediately. A customer could be the victim of toll fraud if they have reports of:

    a. Long holding times

    b. Unexplained surges in use

    c. Increases in calls after business hours

    d. Reports of odd calls

7) Guard against unauthorized access to system administration by doing administration over a secure physical connection, a secure LAN connection, or by employing SSH, HTTPS, and/or SNMPv3 (recommended for a future G700 release).

8) Insure that the system administrator's password is kept secret and changed often. For the best security, use the Access Security Gateway (ASG) feature over a secure connection. For more information on ASG, see the following: http://www1.avaya.com/enterprise/whitepapers/protectingpasswordsusingmv.pdf

    In addition, take the following precautions with logins and passwords:

    - Instead of passwords, it is recommended that customers use ASG on all of their logins to authenticate. Likewise, RADIUS is recommended for authentication on the data side.
    - If the customer uses passwords instead of ASG, the passwords should be changed frequently.
    - Require strong passwords (or pass phrases) and authentication before allowing system or database access.

- Access control servers validate the user's identity and determine which areas or information the user can access based on stored user profiles. G700 Media Gateway configurations can employ AAA (for ESRAS), ASG (for ICC) and RADIUS (for Media Gateway) access control servers. It is recommended that customers use access control servers for all user authentications.

9) Limit access to the LAN.

10) Record and monitor to whom and when access is granted.

11) Access to the LAN should also be restricted via access control list on the Routers and Firewalls.

12) It is recommended that customers configure their firewalls and routers to restrict Avaya remote access to only Avaya IP address endpoints.

13) For individual terminal endpoints that are particularly sensitive to eavesdropping, customers may want to consider employing DCP (a proprietary protocol) terminals instead of IP terminals until IP terminals employ encryption. This of course assumes that such calls are between DCP or analog phones or to relatively secure phones on the public network and are not carried over the LAN.

14) For backup recovery reasons, transferring the files via FTP to a local PC as the only location for backups is not recommended, unless the local PC is secure. However, backing up to a remote storage device introduces other security concerns. Whether backed up to a local or remote device, the backup location should receive the same attention to security as the main storage site (G700 Media Gatewat location). Care should be taken to make sure that the storage device and the physical environment (such as the room, the building or the premises) where the information is stored is physically secured.

15) Passwords used for the backup storage device and backup/restore process should be protected from intruders with the same care as passwords to the G700 itself.

16) While encryption of backups is optional, storing backups un-encrypted is not recommended as backup files contain very sensitive information that can be used to intrude on user privacy and the G700 Media Gateway system itself. Backups should always be encrypted.

17) If customers use SNMP to manage their surrounding network of devices, it is recommended that v3 be used.

18) It is recommended that a secure protocol such as SSH and SCP be used in all cases.

19) TFTP is used to transfer the file from the Update Master to the Media Gateway Processor and from the Media Gateway Processor to the target (i.e., Media Module). TFTP is not a secure protocol, so this transfer should be made over a secure path.

20) It is a customer/user responsibility to ensure that the SNMP entity giving access to an instance of the MIB is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed change/create/delete them.

21) Security log files should be frequently and securely transferred away from the system onto a secure server and archived for future examination.

22) When IP terminals are deployed in unsecured areas (e.g. lobbies, waiting rooms, etc.) then the LAN is exposed to outside intrusion. It is recommended that for such areas, analog or DCP phones be uses instead on IP phones to eliminate the possibility that someone with a laptop could plug into the network directly. One possible alternate solution is to use tamper proof LAN connectors in all public or semi-public areas.

23) Organizations should have effective mechanisms in place for communicating to all employees the existing policies, policy changes, new policies, and security alerts regarding impending viruses or attacks.

24) If connecting to the Internet in any way, it is recommended that the customer use firewalls to protect their network. Firewalls should always be used to create secure network configuration (secure subnets or Demilitarized Zones [DMZ's]) to protect from internal and external attacks. If the firewall does not come with an Intrusion Detection System then an IDS should be added.

25) Avaya recommends an initial security audit before the system is brought on-line and periodic audits thereafter to assure compliance with security policies. Audits themselves do not solve problems, so it is imperative that recommendations generated by a security audit be tracked and implemented.

Recommendation for Installation of the G700 Media Gateway

This section summarizes the recommendations related to G700 installation issues identified in this document.

1) It is recommended that Avaya Services change the default login and passwords for the Media Gateway Processor and Avaya P330 L2 Switch CLI immediately after installation.
2) When firmware files are obtained from a support site, a secure browser using HTTPS should be employed and cryptographic signatures on the files should be checked.