

Security Best Practices Checklist

This document serves to communicate the security best practices for a unified communications deployment and should be used to supplement existing security best practices documents (additional areas may include access control lists, port security, and traffic policing). The recommendations contained within do not guarantee a secure network but will aid in increasing the level of security for unified communications.

Server / Application

- Enable encryption
 - H.235.5 for H.323 signaling encryption
 - SRTP* for H.323 / SIP media encryption (10 bytes overhead per packet)
 - Standalone AES encryption can also be used for H.323 media encryption
 - TLS for SIP signaling encryption
 - SRTP for voicemail interaction
 - TLS for adjunct communications
 - AES encryption for configuration back-up
 - Note, network regions can be created to segment phones that don't support encryption from phones that are capable of encryption
- Secure management traffic
 - HTTPS
 - SNMPv3 for monitoring / configuration
 - If SNMPv1 is the only option, ensure the community string is changed after installation
- Disable insecure services and enable secure services
 - o Insecure: telnet, ftp, SNMP
 - Secure: ssh, scp, SNMPv3
- Phone Hardening
 - Implement HTTPS for IP phone downloads (settings files, backup / restores, etc)
 - If using a 3rd party server, it will require loading a signing certificate for the respective server
 - Lock down user options on the phone via OPSTAT (note, not supported on the 96xx SIP phones)
 - Enable 802.1x authentication (also LLDP and LLDP-Med)*
 - Use EAP / TLS if possible (install site specific certificates within the phones)
- Leverage the "GROUP" option to restrict functionality of phones in open areas
 o For example, restrict access to the secondary Ethernet port in a lobby
- Tie into an existing Identity Management database for administrator authentication (RADIUS, LDAP, Active Directory)*
- Create roles for the various administrators of the systems*
 - Includes disabling service observer/console permissions capabilities for users not requiring them
- Enable tripwire on the servers for intrusion detection where applicable



- Increase log levels on systems and send to a syslog server for ongoing review
 Ensure logging of failed authentication attempts
- Enforce complex passwords for administration*
 - Change from the default passwords (servers / applications will typically require you to change the passwords unless the server is running an older release of software)
 - Select strong passwords for new passwords and for passwords created by users in the future (servers will typically require you to select a strong password unless the server is running an older release of software)
 - "Strong" password implies a mix of upper case, lower case, numbers, punctuation, minimum length, etc
- Implement a unique station security code for each extension
 - Don't use the extension as the station security code (i.e. PIN)
 - Limit long distance access and restrict calling times to minimize toll fraud
- RTCP Monitoring via a third party tool such as Prognosis (used to detect network problems / DoS attacks)

Network:

_

- For VoIP networks, segment the data network from the voice network
 - Note for UC networks: PC's / laptops will need both data / voice network access so VLAN's will not be sufficient to support Unified Communications (i.e. softphones, presence, etc)
- Firewall / Perimeter Protection
 - Block unnecessary ports / protocols (when possible)
 - ICMP
 - Gratuitous ARP
 - SNMP
 - Restrict unnecessary communications
 - Only allow known authorized servers to communicate with each other
 - Options:
 - <u>Stateless</u> firewall that opens up the static ports to / from the UC components
 - Check the Avaya support site for port matrix documents on which ports are required for proper operation
 - <u>Stateful</u> firewall such as one from Juniper or Checkpoint* that can inspect the H.323 / SIP communications
 - Notes: For H.323, inspection requires disabling signaling encryption
 - For SIP, leverage the SIP firewall within the Session Manager (SM-100)
 - Session Border Controllers (ideal for SIP trunking)
 - Delivers Denial of Service Protection, SIP packet inspection, Topology Hiding and more
 - o Get rid of all modems



- If Avaya / business partner manages / monitors your network, deploy a secure remote monitoring solution
 - Avaya now offers "Secure Access Link" for technician access

Ongoing Activity

- Review log files for "suspicious behavior" such as repeated failed authentication attempts
- Ensure the latest patches are installed
- Sign up for the Avaya Security Advisory notifications (support.avaya.com/security)

*Additional Information

H.323 SRTP: <u>ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/Security/srtp-iptrunk.pdf</u> SIP SRTP: <u>ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/Security/srtp-sip.pdf</u> CM Auth: <u>ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/Security/CM_Administrator_Logins.pdf</u> 802.1X / LLDP: <u>ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/Security/802_1x-LLDP.pdf</u> SNMP Phone Security: <u>ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/Security/802_1x-LLDP.pdf</u> Session Manager Security: <u>http://support.avaya.com/css/P8/documents/100068130</u> DevConnect Interoperability Whitepapers: <u>https://devconnect.avaya.com/public/dyn/d_dyn.jsp?fn=428</u> CM Security Guide: <u>http://support.avaya.com/css/P8/documents/100064792</u> Per Product Port Matrix: <u>http://support.avaya.com/</u>

Restricted Documentation (available upon request):

- Avaya one-X[®] Mobile Security Whitepaper
- IPS Security Guide