AdviSec Ltd

IP Telephony Security Consultancy

Aims

Telephony is without doubt a critical business application for many organisations, and as such any disruption to service can quickly become disastrous. It is therefore imperative that any 'major' changes to the service delivery platform are preceded by a comprehensive review, including a detailed security assessment.

Consideration of Business Issues

Whilst organisations continue to benefit from reliable and secure legacy telephony solutions, increasingly organisations are migrating some or all of their telephony toward an IP based solution. For example:

- Connecting legacy PBXs, for example utilising existing or newly provided IP Infrastructure
- Deploying IPT 'type' solutions to selected sites e.g. remote sites, satellite offices or to support home working
- Introducing an IP-based telephony switch (replacing or upgrading a legacy PBX)

Whilst the benefits of a converged IPT solution are acknowledged, there are potentially several security related risks that need to be understood and appropriately addressed. Potential threats that may result in Confidentiality, Integrity and /or Availability problems:

- Telephony switch susceptible to hacking across the network
- Eavesdropping, i.e. re-routing and/or sniffing of session data
- Spoofing of legitimate users
- Virus threat
- Limitations with network capacity, fuelled by a lack of security and performance monitoring
- Component failure (BCP) and/or Disaster recovery (DR)

Additionally, some security products do not always lend themselves to supporting IPT services, for example firewalls.

Finally, it should be noted that telephony equipment manufacturers are fuelling the migration to IP, whilst continuing to support legacy protocols, in response to the threat from the 'new' telephony suppliers, e.g. CISCO.

Client Engagement

Phase 1

Consultants shall initially liaise with representatives from the Client organisation to understand the convergence strategy for telephony services. Thereafter the consultants shall liaise with the IT Security Officer to understand the security environment within which the services shall operate.

Phase 2

Using the information from Phase 1, consultants shall conduct a detailed risk assessment, and following a review by the client, consultants shall proceed to identify controls to mitigate the security risks. Each recommendation shall be accompanied by a justification, together with an estimate in respect of its implementation and maintenance. Consultants shall be pleased to present their recommendations.

Phase 3

Advisec provides Procurement Consultancy Services.

And following the ‘successful’ implementation of a solution, Advisec is able to organise a CHECK accredited penetration test / vulnerability assessment via our partners.

Consideration of Technology Issues

Legacy

Telephony requirements are complicated, and typically include ‘automatic call distribution’ (ACD) and some level of ‘computer telephony integration’ (CTI), including:

- Authenticate callers. Using one of several standard methods, the telephone number of the caller can be screened against a database.
- Recognize a voice, either for authentication or for message forwarding
- Provide interactive voice response (IVR) to callers
- Match the number of a caller with a customer record and display it for reference when talking to the caller IPT

Figure 1 illustrates how CISCO Call manager (represented by the cluster at the top of the diagram) integrates with respect to the SIP protocol (as well as the ‘equivalent’ proprietary CISCO ‘Skinny Client Control protocol’ (SCCP)) and IP telephones.

Operating Environment

The following requirements may be applicable to the client organisation:

- Connection to the PSTN/ISDN and 'Private Telephony Networks'
- Interface to radio systems (e.g. Airwave)
- Use of shared or dedicated underlying IP network (e.g. MPLS)
- Presence of information protectively marked (e.g. 'PROTECT', 'RESTRICTED', CONFIDENTIAL', or higher).
- Requirement to service mobile as well as fixed users working from offices and homes.

Benefits to Client

The client organisation can be assured of high quality security advice provided by consultants accredited under the CESG Listed Advisor scheme (CLAS) and Certified Information Systems Security professional (CISSP).

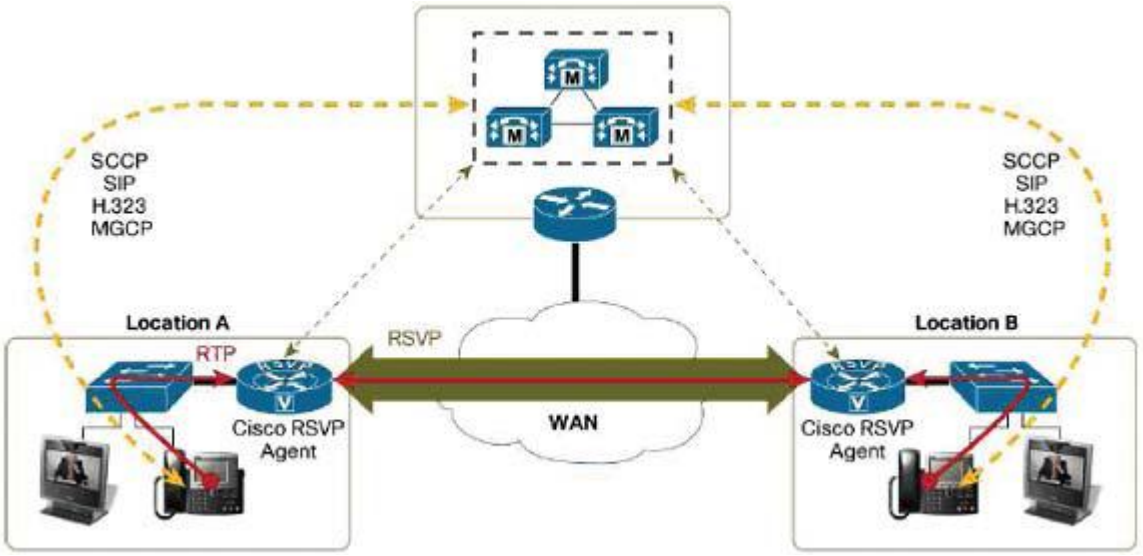

Figure 1: IP Telephony

Contact us:
Further details, including case studies, presentations and references are available from Nigel Strutt. Please call 01869 388011 or 07780 526195. Head office; 41, Barry Avenue, Bicester, Oxfordshire. OX26 2DZ. Email: nigel.strutt@advisec.co.uk