19.5. Session Border Controllers

Objective

19.5.1. To ensure the use of Session Border Controllers (SBCs) is integrated with the agency's security architecture and that use is consistent with other requirements for gateway security in this chapter.

Context

Scope

19.5.2. This section encompasses the use of SBCs in Voice over Internet Protocol (VoIP) and Unified Communication (UC) networks within an agency. It describes key risks and threats and provides guidance on the conceptual design of security for such systems.

19.5.3. It is important to note that Service Providers generally have operational objectives different to those of the agency and typically they will:

- Design a highly operationally optimised network requiring minimal maintenance;
- Provide resources, including SBCs, softswitches and media gateways that are shared between a number of customers (such as multi-tenanted data centres);
- The standard model may not accommodate all unique agency or NZ Government requirements which will then require special consideration.

19.5.4. Reference should also be made to the following sections:

- Chapter 6 – Information Security Monitoring;
- Chapter 7 – Information Security Incidents;
- Chapter 9 – Personnel Security;
- Chapter 11 – Communications Systems and Devices;
- Section 13.1.12 – Archiving;
- Chapter 16 – Access control and passwords;
- Section 18.3 - Video & Telephony Conferencing and Internet Protocol Telephony.

Definitions

19.5.5. A Session Border Controller (SBC) is a device (physical or virtual) used in IP networks to control and manage the signalling and media streams of real-time UC and VoIP connections. See also Section 18.3 – Video & Telephony Conferencing and Internet Protocol Telephony. It includes establishing, controlling, and terminating calls, interactive media communications or other VoIP connections. SBCs enable VoIP traffic to navigate gateways and firewalls and ensure interoperability between different SIP implementations. Careful selection of SBCs will provide such functionality as prevention of toll fraud, resistance to denial of service attacks and resistance to eavesdropping.

19.5.6. Unified Communications (UC) is a term describing the integration of real-time and near real time communication and interaction services in an organisation or agency. UC may integrate several communication systems including unified messaging, collaboration, and interaction systems; real-time and near real-time communications; and transactional applications.

19.5.7. UC may, for example, include services such as instant messaging (chat), presence information, voice, mobility, audio, web & video conferencing, data sharing (such as interactive whiteboards), voicemail, e-mail, SMS and fax. UC is not necessarily a single product, but more usually a set of products designed to provide a unified user-interface and user-experience across multiple devices and media-types.

Purpose

19.5.8. Traditional demarcation points, such as media gateways, are no longer natural boundaries. Older firewall technology impacts the performance of communications systems, including VoIP and UC. SBCs were introduced to improve performance and provide interoperability with real-time and near real-time communications. They provide a new natural demarcation point.

19.5.9. SBCs can provide a demarcation or normalisation point within the agency's network, allow enforcement of agency specific security policies and provide a greater degree of accountability than the usual contract with service providers.

Risks and Threats

19.5.10 Risks and threats associated with the use of VoIP and UC include:

- Confidentiality (eavesdropping);
- Integrity (enabling fraud and theft as well as compromising privacy); and
- Availability (including Denial of Service [DoS or DDoS]).

Confidentiality

19.5.11. There is a high likelihood of eavesdropping in VoIP systems. Traditional telephone systems require physical access to tap a line or compromise a PABX or switch. In VoIP networks, virtual LAN environments can be exploited remotely to identify weaknesses within and between virtual LANs and gain access to valuable information. Sniffing is another form of eavesdropping that involves capturing unencrypted voice traffic with malware or a specific VoIP sniffer tool. In common with other Internet connected systems, adversary-in-the-middle exploits are also used to eavesdrop on both data and VoIP networks.

Integrity

19.5.12. Exploits such as caller ID spoofing are relatively easy to execute and can be extremely costly to businesses. Information from a stolen credit card or acquisition of other sensitive data, can compromise an employee's caller ID, and have funds transferred while posing as the employee. Cyber criminals can also change an employee's registration information in order to eavesdrop on or intercept all incoming calls for that individual.

19.5.13. Integrity compromise may include modification or insertion into UC. As many UC elements, such as voicemail or email, may encompass electronic records as defined in legislation it is vital that these elements are preserved unaltered.

Availability

19.5.14. Because VoIP and UC places high levels of demand on any network, managing Quality of Service (QoS), latency, jitter, packet loss and other service impediments are important aspects of availability. In the event of major faults or outages, diversity and fault tolerance is vital for all key sites. To enable failover, for example, where calls leave the customer network, call diversity and call failover are essential configuration elements.

Denial of Service

19.5.15. Denial of Service (DoS) attacks abuse signalling protocols to deny availability of VoIP data and degrade performance. If the telecommunications network is compromised, it is possible to also traverse systems to attack or infect the agency's data networks and other systems.

Common VoIP and UC Security Risks and Threats

19.5.16. Common VoIP and UC security risks and threats.

Risk	Typical Symptoms	Threat	Countermeasures
Reconnaissance scan	Address or port scan is used to footprint network topology	Targeted denial of service, fraud, theft	• Intrusion detection • Protection against registration floods
Adversary in the middle	Attacker intercepts session to impersonate(spoof) caller	Targeted denial of service, breach of privacy, fraud, theft	• TLS encryption for SIP with separate TLS certificates for SIP Service Providers
Eavesdropping	Attacker "sniffs" session for the purpose of social engineering	Breach of privacy, fraud, theft	• Intrusion detection • Encryption
Session hijacking	Attacker compromises valuable information by rerouting call	Breach of privacy, fraud, theft	• Intrusion detection
Session overload	Excessive signalling or media traffic(malicious, non-malicious) is experienced	Denial of service	• Protection against registration floods
Protocol fuzzing	Malformed packets, semantically or syntactically incorrect flows are encountered	Denial of service	• Malformed packet protection • Protocol anomaly protection • TCP reassembly for fragmented packet protection • Strict TCP validation to ensure TCP session state enforcement, validation of sequence and acknowledgement numbers, rejection of bad TCP flag combinations
Media injection	Attacker inserts unwanted or corrupted content into messages compromising packet/data stream integrity	Denial of service, fraud	• Application aware firewalls • Intrusion prevention /detection • Encryption
Toll Fraud	Unexplained/unusual calling activity, increased costs/carrier notification/alert	Fraud, financial loss, breach of privacy, information loss	• Application aware firewalls • Intrusion prevention /detection • Encryption

19.5.17. Encryption is discussed in Chapter 17 - Cryptography.

Product Selection

Protection Profiles

19.5.18. One Protection Profile for SBCs has been published by NIAP (dated July 24, 2015 - see reference table). Several other Protection profiles (PPs) specifically for SBCs are in development but not yet published (as at September 2015). Gateway and other border control device PPs are used as surrogates in the interim. Refer to Chapter 12 – Product Security.

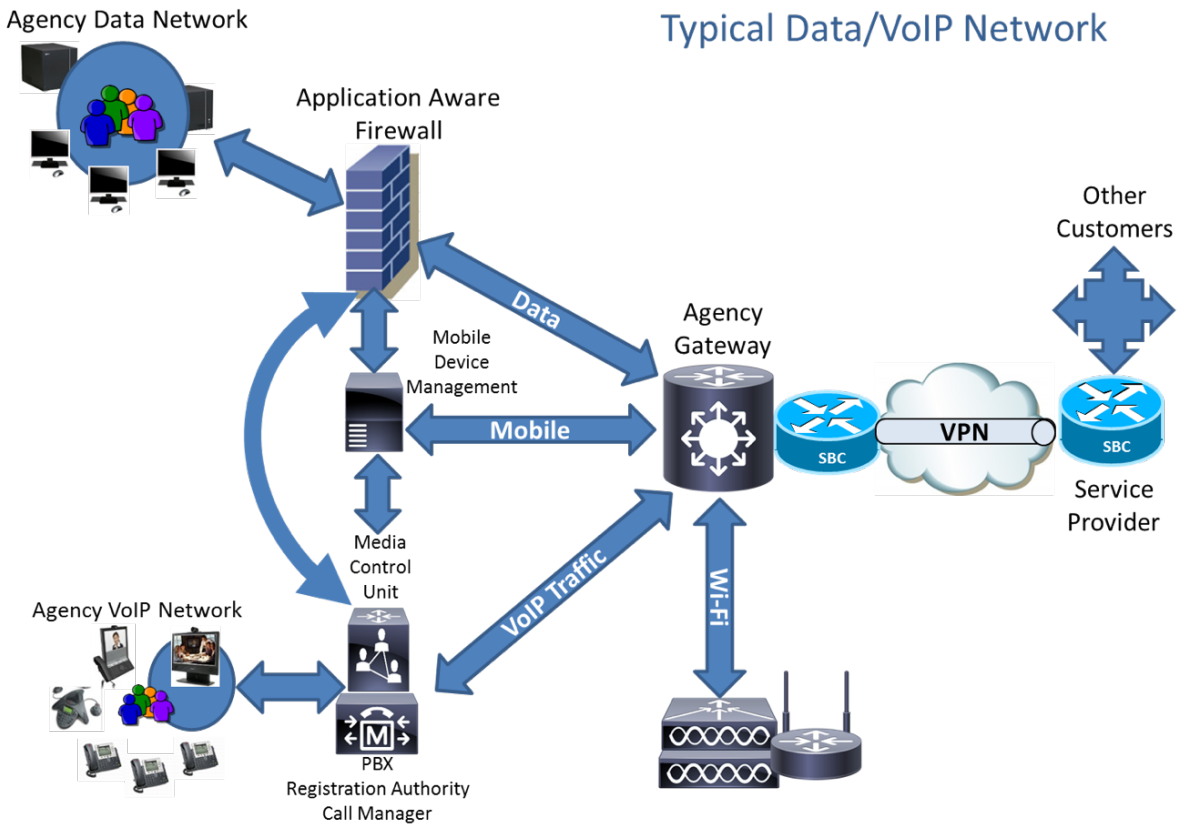
Desirable SBC Functionality

19.5.19. To manage risks and threats and to safeguard performance there are a number of desirable features in an SBC. These include:

- Security – SBC DoS protection, access control, topology hiding, VPN separation, service infrastructure DoS prevention;
- Encryption – Support for Suite B encryption;
- Service Reach – surrogate registration IP PBX endpoints, SIP IMS-H.323 PBX IWF; VPN bridging;
- SLA assurance – admission control; bandwidth per VPN & site, session agent constraints, policy server; intra-VPN media release; QoS marking/mapping; QoS reporting;
- Fraud and Revenue protection – bandwidth policing, QoS theft protection, accounting, session timers;
- Regulatory compliance – provision of emergency service calls (111) & lawful intercept.

Security Architecture

19.5.20. Typical use of session border controller in an agency gateway is illustrated in Figure 1 below:



General References

19.5.21. Additional information on Session Border Controllers can be found in the following references:

Reference	Title	Publisher	Source
NIST Special Publication 800-58, January 2005	Security Considerations for Voice Over IP Systems	NIST	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-58.pdf (PDF, 922 KB)
	Security Issues and Countermeasure for VoIP	SANS	https://www.sans.org/white-papers/1701/
Report Number: I332-016R-2005	Security Guidance for Deploying IP Telephony Systems Released: 14 February 2006	Systems and Network Attack Center (SNAC) NSA	https://www.nsa.gov/ia/_files/voip/I332-016r-2005.pdf
Report Number: I332-009R-2006	Recommended IP Telephony Architecture, Updated: 1May2006 Version1.0	Systems and Network Attack Center (SNAC) NSA	https://www.nsa.gov/ia/_files/voip/I332-009R-2006.pdf
	Mobility Capability Package March 26 2012 - Secure VoIP Version 1.2	NSA	https://www.nsa.gov/ia/_files/Mobility_Capability_Pkg_Vers_1_2.pdf
	Protecting Telephone-based Payment Card Data PCI Data Security Standard (PCI DSS) Version: 2.0, March 2011	The PCI Security Standards Council (PCI SSC)	https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf (PDF, 888 KB)
	Understanding Voice over Internet Protocol (VoIP): 2006	US-CERT	https://www.us-cert.gov/sites/default/files/publications/understanding_voip.pdf (PDF, 83 KB)
CNSS Instruction No. 5000 April 2007	Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony	Committee on National Security Systems	https://www.cnss.gov/CNSS/issuances/Instructions.cfm
	Infrastructure qualified for Microsoft Lync	Microsoft TechNet	https://technet.microsoft.com/en-us/office/dn788945.aspx
	A Guide to the Public Records Act	Archives New Zealand	https://archives.govt.nz/manage-information/how-to-manage-your-information/key-obligations-and-the-standard/key-obligations-public-records-act-2005
Public Act 2002 No.35	Electronic Transactions Act 2002		https://www.legislation.govt.nz/act/public/2002/0035/latest/DLM154185.html
	Network Device Collaborative Protection Profile (NDcPP) Extended Package Session Border Controller, September 2016, version 1.1	NIAP	epl_sbc_v1.1.pdf (niap-ccevs.org)
	PP-Module for Voice and Video over IP (VVoIP), October 2020, version 1.0	NIAP	mod_vvoip_v1.0.pdf (niap-ccevs.org) NIAP (niap-ccevs.org)
	DHS 4300A Sensitive Systems Handbook Attachment Q5 To Handbook v. 11.0 Voice over Internet Protocol (VoIP) Version 11.0 December 22, 2014	DHS	https://www.dhs.gov/sites/default/files/publications/4300A%20Handbook%20Attachment%20Q5%20-%20Voice%20over%20IP.pdf (PDF, 586 KB)
	2015 Global Fraud Loss Survey	CFCA	https://cfca.org/fraudloss-survey/

Media Technical References

19.5.22. Media technical references are listed below:

Reference	Title	Publisher	Source
RFC 2833	**RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals**	IETF	https://datatracker.ietf.org/doc/html/rfc2833
RFC 3313	**Private Session Initiation Protocol (SIP) Extensions for Media Authorization**	IETF	https://datatracker.ietf.org/doc/html/rfc3313
RFC 3550	**RTP: A Transport Protocol for Real-Time Applications**	IETF	https://datatracker.ietf.org/doc/html/rfc3550
RFC 3685	**Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)**	IETF	https://datatracker.ietf.org/doc/html/rfc3685
RFC 3362	**Real-time Facsimile (T.38) - image/t38 MIME Sub-type Registration**	IETF	https://datatracker.ietf.org/doc/html/rfc3362
T.38 (09/2010)	**Procedures for real-time Group 3 facsimile communication over IP networks**	International Telecommunication Union	https://www.itu.int/rec/T-REC-T.38/e
V.150.1 (01/2003)	**Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs**	International Telecommunication Union	https://www.itu.int/rec/T-REC-V.150.1-200301-I/en
G.711	**Pulse code modulation (PCM) of voice frequencies**	International Telecommunication Union	https://www.itu.int/rec/T-REC-G.711/
G.726	**40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM)**	International Telecommunication Union	https://www.itu.int/rec/T-REC-G.726/e
G. 729 (06/2012)	**Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP)**	International Telecommunication Union	https://www.itu.int/rec/T-REC-G.729/e

Signalling Technical References

19.5.23. Signalling technical references are listed below:

Reference	Title	Publisher	Source
RFC 2705	Media Gateway Control Protocol (MGCP) Version 1.0	IEFT	https://datatracker.ietf.org/doc/html/rfc2705
RFC 3525	Gateway Control Protocol Version 1.0	IEFT	https://datatracker.ietf.org/doc/html/rfc3525
RFC 3261	SIP: Session Initiation Protocol	IEFT	https://datatracker.ietf.org/doc/html/rfc3261
RFC 3263	Locating SIP Servers	IEFT	https://datatracker.ietf.org/doc/html/rfc3263
RFC 4028	SIP Session Timer	IEFT	https://datatracker.ietf.org/doc/html/rfc4028
RFC 3966	The tel URI for Telephone Numbers	IEFT	https://datatracker.ietf.org/doc/html/rfc3966
RFC 3924	Cisco Architecture for Lawful Intercept in IP Networks	IEFT	https://datatracker.ietf.org/doc/html/rfc3924
RFC 2327	Session Description Protocol	IEFT	https://datatracker.ietf.org/doc/html/rfc2327
RFC 3025	Gateway Control Protocol Version 1, June 2003	IEFT	https://datatracker.ietf.org/doc/html/rfc3025
H.248 (03/2013)	Media Gateway Control (Megaco): Version 3	International Telecommunication Union	https://www.itu.int/rec/T-REC-H.248.1/en
H.323 (12/2009)	Packet-based multimedia communications systems	International Telecommunication Union	https://www.itu.int/rec/T-REC-H.323/en/
H.450	Supplementary Services for H.323	International Telecommunication Union	https://www.itu.int/en/Pages/default.aspx
MSF Technical Report MSF-TR-QoS-001-FINAL	Quality of Service for next generation VoIP networks framework	Multiservice Switching Forum (MSF)	http://www.recursosvoip.com/docs/english/MSF-TR-QoS-001-FINAL.pdf [PDF, 778 KB]
ETSI TS 129 305 V8.0.0 (2009-01)	Universal Mobile Telecommunications System (UMTS); LTE; InterWorking Function (IWF) between MAP based and Diameter based interfaces.	European Telecommunications Standards Institute	https://www.etsi.org/deliver/etsi_ts/129300_129399/129305/08.00.00_60/ts_129305v080000p.pdf [PDF, 625 KB]

Rationale & Controls

Risk Assessment

19.5.24.R.01. **Rationale**

The adoption of Voice over Internet Protocol (VoIP) and Unified Communication (UC) networks will introduce a range of technology risks *in addition* to the technology and systems risks that already exist for agency systems. It is vital that these risks are identified and assessed in order to design a robust security architecture and to select appropriate controls and countermeasures.

19.5.24.R.02. **Rationale**

The availability of agency systems, business functionality and any customer or client online services, is subject to further risks in an outsourced environment. A risk assessment will include consideration of business requirements on availability in a VoIP and UC environment.

19.5.24.R.03. **Rationale**

Risks to business functionality may include service outages, such as communications, data centre power, backup and other failures or interruptions. Entity failures such as the merger, acquisition or liquidation of the service provider may also present a significant business risk to availability.

19.5.24.R.04. **Rationale**

Testing is a valuable tool when assessing risk. A UC environment with complex communications streams can provide opportunities for exploitation, especially where the configuration is weak or has itself been compromised. One of the fundamental tools is penetration testing.

19.5.24.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4703]

Agencies intending to adopt VoIP or UC technologies or services MUST conduct a comprehensive risk assessment *before* implementation or adoption.

19.5.24.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4705]

Agencies intending to adopt VoIP or UC technologies or services MUST consider the risks to the availability of systems and information in their design of VoIP and UC systems architecture, fault tolerance, fail over and supporting controls and governance processes.

19.5.24.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4706]

Agencies MUST ensure risks for any VoIP or UC service adopted are understood and formally accepted by the agency's Accreditation Authority as part of the Certification and Accreditation process (See Chapter 4 - System Certification and Accreditation).

19.5.24.C.04. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4707]

Agencies intending to adopt VoIP or UC technologies or services MUST determine where the responsibility (agency or VoIP and UC service provider) for implementing, managing and maintaining controls lies in accordance with agreed trust boundaries.

19.5.24.C.05. **Control System Classifications(s): All Classifications, Restricted/Sensitive; Compliance: Must** [CID:4708]

Any contracts for the provision of VoIP or UC services MUST include service level, availability, recoverability and restoration provisions as formally determined by business requirements.

19.5.24.C.06. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4709]

Agencies MUST ensure contracts with VoIP or UC service providers include provisions to manage risks associated with the merger, acquisition, liquidation or bankruptcy of the service provider and any subsequent termination of VoIP or UC services.

19.5.24.C.07. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4710]

Agencies procuring or using VoIP or UC services to be used by multiple agencies MUST ensure all interested parties formally agree to the risks, controls and any residual risks of such VoIP and UC services. The lead agency normally has this responsibility (see Chapter 2 - Information Security services within Government and Chapter 4 - System Certification and Accreditation).

19.5.24.C.08. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4711]

Agencies SHOULD consider the use of assessment tools, such as penetration testing, when undertaking the risk assessment.

Non-Agency Networks

19.5.25.R.01. **Rationale**

Networks furnished by a service provider are invariably shared networks. Much of the security configuration is designed to maximise operational efficiency of the Service Providers network. Any agency specific security requirements may attract additional cost.

19.5.25.R.02. **Rationale**

It is preferable to maintain an agency designed and controlled gateway to ensure security requirements are properly accommodated. The use of SBCs should be carefully considered in order to maximise efficiency consistent with security requirements.

19.5.25.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4715]

Agencies MUST follow the gateway requirements described in Chapter 19 - Gateway Security.

Security Architecture and Configuration

19.5.26.R.01.

Rationale

Trust boundaries must be defined to assist in determining effective controls and where these controls can best be applied. Trust zones and trust boundaries are discussed in 22.1.3. The use of SBCs will assist with the definition of trust boundaries and allow the segregation of UC and normal data.

19.5.26.R.02. **Rationale**

The threat model for IP is well understood. Data packets can be intercepted or eavesdropped anywhere along the transmission path including the corporate network, by the internet service provider and along the backbone. The prevalence and ease of packet sniffing and other techniques for capturing packets on an IP based network increases this threat level. VoIP Encryption is an effective means of mitigating this threat.

19.5.26.R.03. **Rationale**

The nature of traffic through an SBC is an important factor in determining the type and configuration of the SBC. This also plays an important role in determining the resilience of the system. Systems may require high availability (HA), depending on business requirements for availability and continuity of service. The use of split trunks for HA normal traffic may provide resilience at reduced costs.

19.5.26.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4720]

Agencies intending to adopt VoIP or UC technologies or services MUST determine trust boundaries *before* implementation.

19.5.26.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4721]

Updates to the SBC and related devices MUST be verified by the administrator to ensure they are obtained from a trusted source and are unaltered.

19.5.26.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4722]

Agencies MUST include defence mechanisms for the Common VoIP and UC Security Risks and Threats described in 19.5.10.

19.5.26.C.04. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4723]

Agency networks MUST ensure the SBC includes a topology hiding capability.

19.5.26.C.05. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4724]

Agency networks MUST consider the use of call diversity and call failover configurations.

19.5.26.C.06. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4725]

In a virtualised environment, agencies MUST ensure any data contained in a protected resource is deleted or not available when the virtual resource is reallocated.

19.5.26.C.07. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4726]

Agencies SHOULD conduct a traffic analysis to ensure the agency's network and architecture is capable of supporting all VoIP, media and UC traffic. The traffic analysis SHOULD also determine any high availability requirements.

19.5.26.C.08. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4727]

Agencies SHOULD design a security and gateway architecture that segregates UC and normal data traffic. Firewall requirements (Section 19.3 - Firewalls) continue to apply to data traffic.

19.5.26.C.09. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4728]

In a virtualised environment, agencies SHOULD create separate virtual LANs for data traffic and UC traffic.

19.5.26.C.10. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4729]

In a non-virtualised environment, agencies SHOULD create separate LANs for data traffic and UC traffic.

19.5.26.C.11. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4730]

Agency networks SHOULD use encryption internally on VoIP and unified communications traffic.

19.5.26.C.12. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4731]

Agency networks SHOULD ensure intrusion prevention systems and firewalls are VoIP-aware.

Access Control

19.5.27.R.01. **Rationale**

Network access control and password requirements are described in Chapter 16 - Access control and passwords, in particular Section 16.6 – Event Logging and Auditing. Event logging helps improve the security posture of a system by increasing the accountability of all user actions, thereby improving the chances that malicious behaviour will be detected and assist in the investigation of incidents. A fundamental of access control is to manage access rights including physical access, file system and data access permissions and programme execution permissions. In addition, access control provides a record of usage in the event of an incident. Retention of records and archiving is discussed in 13.1.12 - Archiving.

19.5.27.R.02. **Rationale**

Similar requirements apply to VoIP and UC networks as these are also IP based. This will include any service enabled as part of the UC environment, such as Chat, IM, video and teleconferencing.

19.5.27.R.03. **Rationale**

There may be special cases, such as a 24x7 operations centre, where VoIP phones are shared by several duty officers on a shift basis. Workloads may require a number of duty personnel at any one time. In such cases it may be impractical to allocate individual VoIP or UC UserID and passwords. The risks in such cases must be clearly identified and compensating controls applied to ensure traceability in the event of fault finding or an incident. Examples of compensating controls include physical access control, CCTV, and duty registers. Identification of shared facilities is important and may comprise a UserID such as “Duty Officer”, SOC, or agency name in a multi-agency facility.

19.5.27.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4737]

Any shared facilities MUST be clearly identifiable both physically and logically.

19.5.27.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4738]

Agencies MUST provide a protected communication channel for administrators, and authorised systems personnel. Such communication MUST be logged.

19.5.27.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4739]

Agencies MUST ensure administrative access to the SBC is available only through a trusted LAN and secure communication path.

19.5.27.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4740]

Access control and password requirements SHOULD apply to VoIP and UC networks in all cases where individual access is granted.

19.5.27.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4741]

In special cases where individual UserIDs and Passwords are impractical, a risk assessment SHOULD be completed and compensating controls applied.

19.5.27.C.06. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4742]

Event logs covering all VoIP and UC services SHOULD be maintained in accordance with the requirements of the NZISM. See sections 16.6 - Event Logging and Auditing and 13.1.12 - Archiving.

Incident Handling and Management

19.5.28.R.01. **Rationale**

Service providers may not provide the same level of incident identification and management as provided by agencies. In some cases, these services will attract additional costs. Careful management of contracts is required to ensure agency requirements for incident detection and management are fully met when adopting VoIP and UC services.

19.5.28.R.02. **Rationale**

Deny listing denies calls to specific numbers, range of numbers, or countries. Allow listing allows calls to numbers, range of numbers, or countries. A combination of deny and allow listing enables a flexible method of preventing call fraud (hijacking and “call pumping”), for example, by allowing calls to a specific number within a country on a deny list.

19.5.28.R.03. **Rationale**

Call Rate Limiting allows the restriction of outbound call volumes to specific numbers, range of numbers or countries. This is a useful mitigation for “traffic pumping” call fraud schemes. Call rate limiting also allows temporary limits to be placed on call from or to particular destinations while a security incident is investigated.

19.5.28.R.04.

Rationale

Call Redirection enables the transfer of blocked calls to another destination including via monitoring and recording systems. Blocked calls may be dropped or a message played indicating, for example, that calls cannot be connected.

19.5.28.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4748]

Agencies MUST include incident handling and management services in contracts with service providers.

19.5.28.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4749]

Agencies MUST develop and implement incident identification and management processes in accordance with this manual (See Chapter 6 – Information Security Monitoring, Chapter 7 – Information Security Incidents, Chapter 9 – Personnel Security and Chapter 16 – Access control and passwords).

19.5.28.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4750]

Agencies SHOULD implement fraud detection monitoring to identify suspicious activity and provide alerting so that remedial action can be taken.

19.5.28.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4751]

Agencies SHOULD regularly review call detail records for patterns of service theft.

19.5.28.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4752]

Agencies SHOULD consider the use of allow and deny listing to manage fraudulent calls to known fraudulent call destinations.

19.5.28.C.06. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4753]

Agencies SHOULD consider the use of call rate limiting as a fraud mitigation measure.

19.5.28.C.07. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4755]

Agencies SHOULD consider the use of call redirection to manage blocked calls.

User Awareness and Training

19.5.29.R.01. **Rationale**

The introduction of VoIP and UC services will introduce change to the appearance and functionality of systems, how users access agency systems and types of user support. It is essential that users are aware of information security and privacy concepts and risks associated with the services they use.

Support provided by the VoIP and UC service provider may attract additional charges.

19.5.29.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4758]

Agencies MUST develop and implement user awareness and training programmes to support and enable safe use of VoIP and UC services (See Section 9.1 – Information Security Awareness and Training).