Security Requirements for IP-Interconnection

IMDA SEC-INTC
Issue 1 Rev 1, XXX 2024

Info-communications Media Development Authority of Singapore
Infocomm Resource & Technology
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

1 Scope

Interconnection refers to the linking of communications networks to ensure that users of one communications network can access the communications networks and services of other telecommunications operators.

This IMDA document defines the security requirements to secure IP-based Interconnections for voice services between network operators, thus minimising the associated cybersecurity risks from the internet.

2 Abbreviations

CII	Critical Information Infrastructure
DDoS	Distributed Denial of Service
IPSEC	Internet Protocol Security
SBC	Session Border Controller
SIP	Session Initiation Protocol
SIRT	Security Incident Response Team

3 Security Requirements

3.1 The operator shall implement the following set of baseline network security requirements on the SBC infrastructure at any points of interconnection with another domestic network operator:

(a) Monitoring and analysis of SIP messages to detect malicious traffic (i.e., any SIP message used with the intent of causing harm, including messages used to perform unauthorised interceptions, service disruptions, spoofing, etc.);

(b) Filtering of malicious traffic on the SBC;

(c) Hardening of the SBC in accordance with industry standards or guidelines; and

(d) Performing of network security assessments and penetration tests at least once every 2 years on the portion of the network that is (i) external from the SBC; and (ii) facing external entities or connections at the points of interconnection.

3.2 Where the operator interconnects its network via public Internet with another domestic network operator's network, the operator shall secure its use of the public Internet by implementing the following set of baseline network security requirements:

(a) Virtual Private Network or IPSEC to secure the connection;

(b) Network firewalls;

(c) DDoS mitigation;

(d) Logging of security events (including but not limited to unauthorised access attempts, DDoS attacks, etc.);

(e) 24x7 security monitoring and analysis (including Border Gateway Protocol and Domain Name System activities); and

(f) Availability of SIRT with the capability to promptly respond to and manage security incidents.

3.3 Notwithstanding section 3.2, where the operator owns Critical Information Infrastructure (i.e., a computer or computer system in respect of which a designation under Section 7(1) of the Cybersecurity Act 2018 is in effect) ("CII"), the operator shall not interconnect its network via public Internet with another domestic network operator's network.

3.4 Any written agreements entered into by the operator with other domestic network operators governing interconnection and related arrangements shall clearly set out all applicable baseline network security requirements listed in Section 3.1 and/or 3.2 above (as the case may be).