設備資通安全
檢測技術指引

資通安全指引 ISG 014
訂定日期 111 年 8 月 24 日

第五代行動通信基地臺
資安檢測指引

中華民國 111 年 8 月 24 日

目錄

圖目錄

1. 前言

為確保第五代行動通信基地臺(Next generation NodeB, gNB/gNodeB)具備基本的資通安全能力，爰訂定本檢測指引。

2. 適用範圍

本檢測指引適用於「補助第五代行動通信網路建設作業要點」補助建設之國產品牌第五代行動通信基地臺。

3. 技術標準

本檢測指引參考標準如下：

(1) 3GPPTS 33.511 V16.6.0 Security Assurance Specification(SCAS)for the next generation Node B(gNodeB)network product class(Release 16)

(2) 3GPP TS 33.117V16.6.0Catalogue of general security assurance requirements(Release 16)

(3) 3GPP TS 33.210 V16.4.0 Technical Specification Group Services and System Aspects;Network Domain Security (NDS);IP network layer security(Release 16)

(4) 台灣資通產業標準協會，TS-0035 5G 基地臺資安測試規範 v1.0

4. 用詞定義

(1) 第五代行動通信基地臺(Next Generation NodeB, gNB/gNodeB)

指基地臺設備規格採分頻雙工模式時，在上下行各 20MHz 頻寬條件下，下行速率可達 200Mbps 以上；或設備規格採分時雙工模式時，在 100 MHz 頻寬條件下，下行速率可達 500Mbps 以上，且應能與具備存取與移動管理功能(Access and Mobility Management Function, AMF)、連結管理功能(Session Management Function, SMF)、用戶面功能(User Plane Function, UPF)等功能之 5G 核心網路設備介接，以下簡稱 5G 基地臺(gNB)。

(2) 用戶設備(User Equipment, UE)

泛指使用者連接網路的設備，包括手機、電腦、伺服器和物聯網裝置等，由通用積體電路卡(Universal Integrated Circuit Card, UICC)和移動式設備(Mobile Equipment, ME)組成，其中移動式設備可進一步由處理通訊功能的移動式終端(Mobile Termination, MT)和終端設備(Terminal Equipment, TE)組成。

(3) 5G 核心網路(5G Core Network, 5GC)

3GPP 將 5G 核心網路定義為控制面(Control Plane)與用戶面(User Plane)分離的分佈式網路架構，採用開放介面的支援，利用網路虛擬化(Network Virtualization)及網路切片技術實現以服務為基礎(Service Based Architecture, SBA)，並支援 5G 服務運營。

(4) 完整性 (Integrity)

指資料不會被未經授權改變或破壞的特性。

(5) 存取與移動管理功能(Access and Mobility Management Function, AMF)

包括用戶設備(UE)進入行動網路連線管理、用戶身分驗證註冊管理、gNB 間移動交遞管理、非存取層信令的加密和完整性保護，也具有緊急電話定位服務管理等功能。

(6) 連結管理功能(Session Management Function, SMF)

包括用戶設備(UE)連結管理(連結建立/修改/釋放)，用戶面安全策略管理、動態主機設定協定 (Dynamic Host Configuration Protocol, DHCP)、位址解析協定(Address Resolution Protocol, ARP)、配置用戶面功能(UPF)的流量控制、提供連結和服務連續性模式(Session and Service Continuity Mode, SSC)，也具有支援不同類型連結、收集 UPF 的計費數據介面資料等功能。

(7) 用戶面功能(User Plane Function, UPF)

包括用戶設備(UE)上網連線、資料的路由與轉發、資料封包檢查、用戶面的流量監控與服務品質(Quality of Service, QoS)管理、連接外部資料網路管理、用戶面部分策略規則管理等功能。

(8) 傳送層安全協定(Transport Layer Security, TLS)

指於兩個應用程式之間透過網路建立安全通道，定義於 RFC5246，可防止交換資料時遭竊聽及篡改。在瀏覽器、電子郵件、即時通訊、網路電話(Voice over Internet Protocol,VoIP)、網路傳真等應用程式中，已廣泛支援此協定。

(9) 密碼(Password)

指一組字元串，能使系統辨識用戶身分，並可進一步控管用戶存取之權限。

(10)安全事件日誌(Security Event Log)

指每個規則所定義之活動紀錄，用以發現及察覺威脅或攻擊事件的發生(例：用戶登入系統)。

(11)加密(Encryption)

指明文資訊透過加密數學演算法進行改變，使改變後的資料不具可讀性，而接收端用相對應的解密數學演算法可以恢復明文資訊而達到保密的目的。

(12)管理介面(Management Interface)

指透過本地端或遠端網路取得裝置系統操控權的介面，例如：於操控程式、網頁管理介面或指令介面執行設備維護、存取裝置資源，以及於操控程式、網頁管理介面或指令介面進行系統設定。

(13)營運管理與維護(Operations, Administration and Maintenance, OAM)

電信網路的一種管理模式，可提供適當的工具予電信事業操作人員，以便在電信網路中管理網路基礎架構。讓操作人員用來確認網路運作中發生的問題；可以進行自動化網路監控，讓操作人員接收營運、管理與維護所產生的訊息以便從網路中找出障礙來源，然後更進一步地採取適當措施。

(14)網際網路金鑰交換 (Internet Key Exchange, IKE)

為一種建立於網際網路安全關聯與金鑰管理協定(Internet Security Association and Key Management Protocol, ISAKMP)上的網路協定。該協定定義於 RFC 2409 標準文件。

(15)封包資料匯聚通訊協定 (Packet Data Convergence Protocol, PDCP)

主要負責 IP 封包表頭壓縮與解壓縮，數據與信令的加密及信令的初始化保護等功能。

(16)訊息完整性鑑別碼 (Message Authentication Code for Integrity, MAC-I)

用以確認發送訊息者的身分，保證訊息的完整性(Integrity)。傳送端一般都利用雜湊函數(Hash Function)計算出一個固定長度的雜湊值，作為一個獨一無二的訊息認證。其總長度為 4 位元組。

(17)無線電資源控制 (Radio Resource Control, RRC)

主要負責無線電資源分配與管理，提供非存取層(Non Access Stratum, NAS)系統資訊廣播；建立、維護和釋放用戶設備(UE)與 gNB 間的無線電資源控制連線；金鑰安全管理；建立、配置、維護和釋放點對點的無線電承載(Radio Bearer, RB)；移動性功能包括用戶設備(UE) 測量回報和選擇連線的 gNB；服務品質(QoS)管理功能等。

(18)存取層(Access Stratum, AS)

存取層包含接取無線電網路，以及控制在用戶設備與無線電網路之間啟動連線的相關功能。

(19)國家脆弱性資料庫(National Vulnerabilities Database, NVD)

指美國國家標準暨技術研究院(National Institute of Standards and Technology, NIST)提供的國家脆弱性資料庫，負責常見脆弱性與漏洞之資料的發布及更新。

(20)共同脆弱性及曝露(Common Vulnerabilities and Exposures, CVE)

指美國國土安全部贊助之脆弱性管理計畫，該計畫針對每一脆弱性項目賦予其全球認可唯一共同編號。

(21)共同脆弱性計分系統(Common Vulnerability Scoring System, CVSS)

指一套共同脆弱性計分系統的判定標準，包括威脅所造成損害的嚴重性、資通安全脆弱性的可利用程度與攻擊者不當運用該脆弱性的難易度，都被列入計分。自 0 分至 10 分，0 代表無風險，而 10 則代表最高風險。

(22)其它用詞英文縮寫

3GPP：Third Generation Partnership Project，第三代合作夥伴計畫。

NAS：Non-Access Stratum，非存取層。

NG-RAN：Next Generation(NG) Radio Access Network，NG 介面無線接取網路。

NGAP：Next Generation(NG)Application Protocol，NG 介面應用協定。

CM-Idle：Connection Management Idle，連線管理閒置。

PDU：Protocol Data Unit，協議數據單元。

XnAP：Xn Application Protocol，Xn 介面應用協議。

5. 檢測項目

5.1. 第五代行動通信基地臺設備，除本檢測指引另有規定外，應符合國家安全考量及 5.2 規定。

5.2. 第五代行動通信基地臺資安檢測項目

5.2.1. 3GPP 安全協定合規檢測

5.2.1.1. 無線電資源控制信令的完整性保護

(1) 測試目的：

驗證UE與受測物間透過NG-RAN介面傳送的RRC信令是否具備完整性保護。

(2) 測試條件：

I. UE、受測物與核心網路可建立 5G 連線。

II. UE 與受測物可設定完整性演算法。

III. 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 封包之 PDCP 層內容。

(3) 測試佈局：如圖 1 所示。

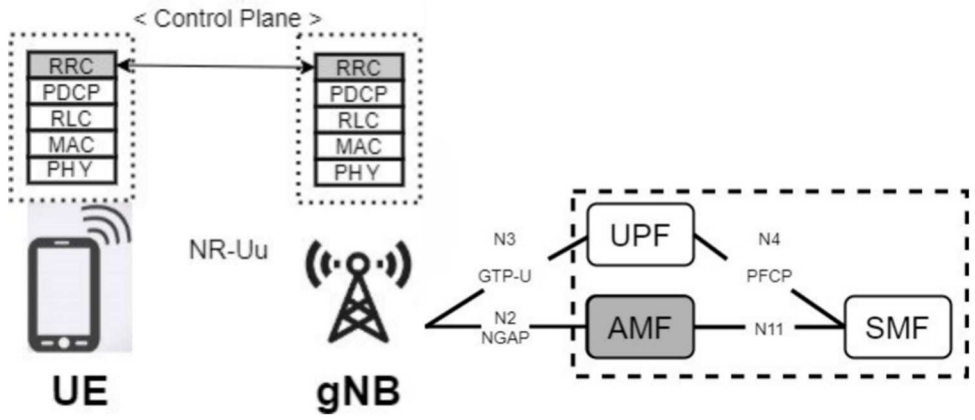


圖 1、RRC 信令完整性資料測試示意圖

(4) 測試方法(如圖 2)：

I. 在 UE 與受測物啟用 RRC 信令完整性演算法(設定 NIA1、NIA2、NIA3 為最優先)，受測物傳送 AS Security Mode Command 訊息給 UE，且 UE 回覆 AS Security Mode Complete 訊息。

II. 受測物傳送 AS Security Mode Command 訊息後，檢查 UE 進入 CM-Idle 狀態前所傳送的 RRC 信令案是否帶有訊息完整性鑑別碼(Message authentication code for integrity, MAC-I)。

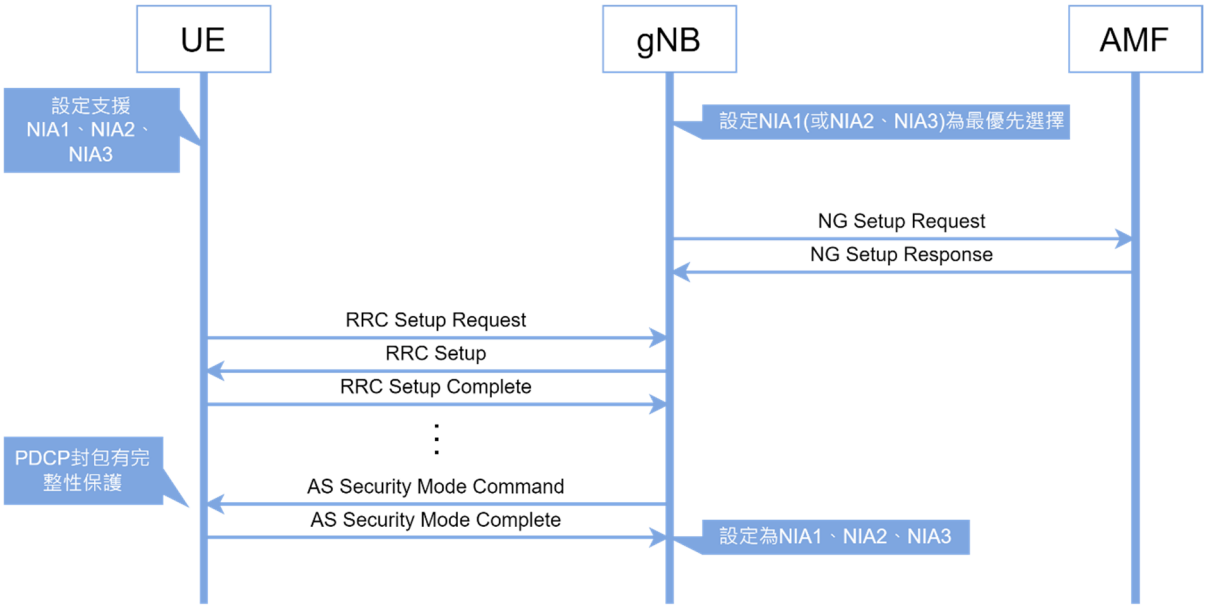


圖 2、RRC 信令完整性資料測試流程圖

(5) 判定標準：

I. 當受測物傳送帶有完整性演算法(NIA1、NIA2、NIA3)的 AS Security Mode Command 訊息給 UE，確認 UE 有回覆 AS Security Mode Complete 訊息。

II. RRC 信令之 PDCP 層內容確認帶有 MAC-I，代表 UE 與受測物間的 RRC 信令已具備完整性保護。

5.2.1.2. 用戶設備和基地臺間的用戶面資料完整性保護

(1) 測試目的：

驗證 NG-RAN 介面傳送的用戶資料是否具備完整性保護。

(2) 測試條件：

I. UE、受測物與核心網路可建立 5G 連線。

II. UE 與受測物可設定完整性演算法。

III. 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 與用戶面(User Plane)封包之 PDCP 層內容。

(3) 測試佈局：如圖 3 所示。

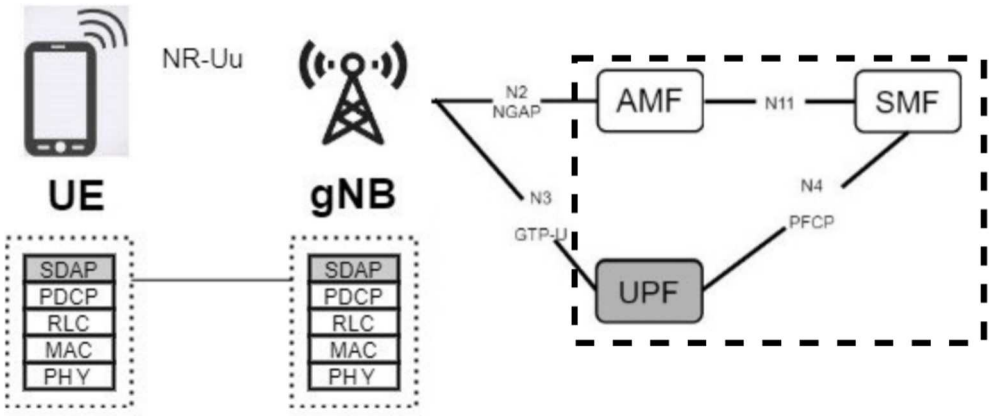


圖 3、用戶面資料完整性保護測試示意圖

(4) 測試方法(如圖 4)：

I. 在 UE 與受測物的用戶面啟用完整性演算法(設定 NIA1、NIA2、NIA3 為最優先)。

II. 受測物傳送完整性保護指示為"on"的 RRCReconfiguration 訊息。

III. 受測物在傳送 RRCReconfiguration 訊息後，檢查 UE 進入 CM-Idle 狀態前所傳送用戶面封包的 PDCP 層內容帶有訊息完整性鑑別碼 MAC-I。

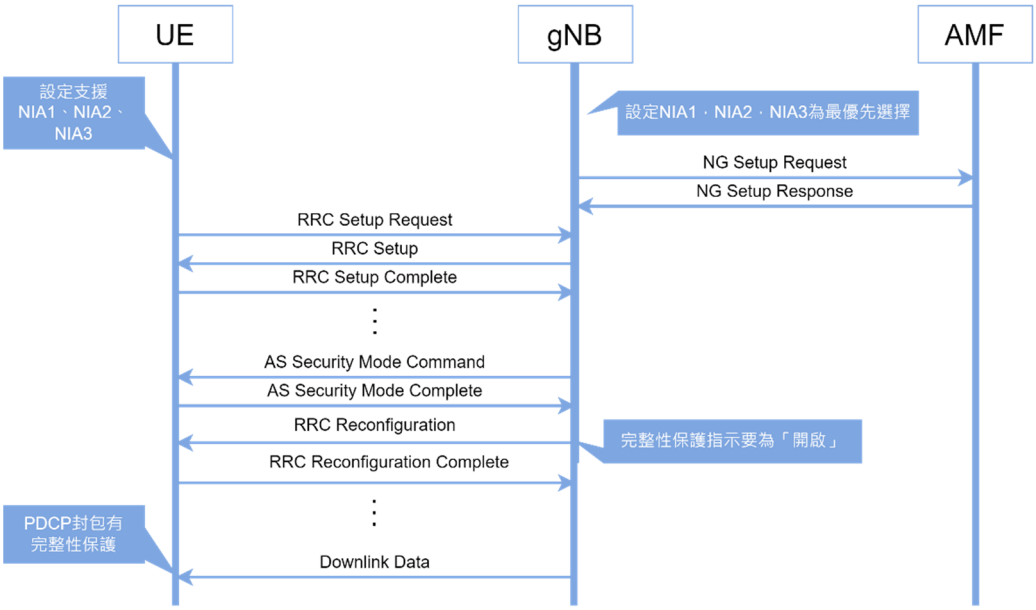


圖 4、用戶面資料完整性保護測試流程圖

(5) 判定標準：

I. 當受測物傳送帶有完整性保護指示"on"的 RRCReconfiguration 訊息，確認 UE 收到後回覆 RRCReconfigurationComplete 訊息。

II. 用戶面封包之 PDCP 層內容確認帶有 MAC-I，代表用戶面封包之 PDCP 層內容已具備完整性保護。

5.2.1.3. 無線電資源控制信令加密

(1) 測試目的：

驗證 NG-RAN 介面傳送的 RRC 信令是否具備加密保護。

(2) 測試條件：

I. UE、受測物與核心網路可建立 5G 連線。

II. UE 與受測物可設定加密演算法。

III. 測試人員可擷取 NG-RAN 介面訊息，並分析 RRC 訊息 PDCP 層內容。

(3) 測試佈局：如圖 5 所示。

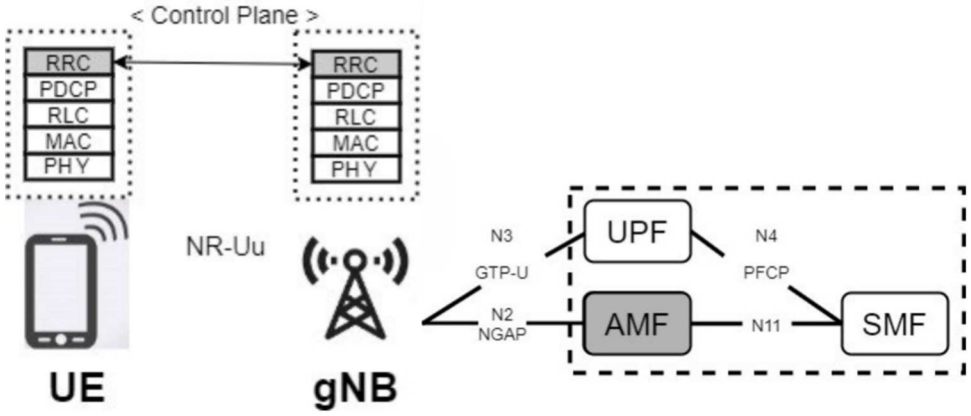


圖 5、RRC 信令加密測試示意圖

(4) 測試方法(如圖 6)：

I. UE 向 AMF 傳送註冊要求。

II. AMF 向受測物傳送密鑰 K_{gNB} 與 UE 安全功能。

III. 受測物選擇加密演算法(以 NEA1、NEA2、NEA3 為優先)，並向 UE 傳送帶有加密演算法的 AS Security Mode Command 訊息。

IV. UE 收到 AS Security Mode Command 訊息後，回覆 AS Security Mode Complete 訊息。檢查 UE 進入 CM-Idle 狀態前所傳送的 RRC 信令是否加密保護。

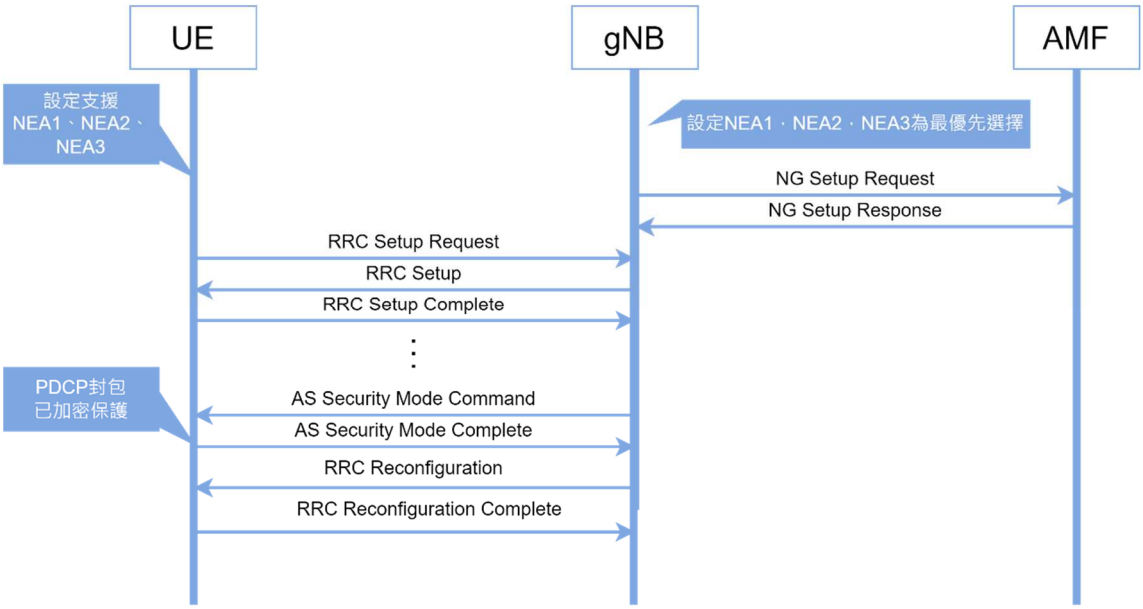


圖 6、RRC 信令加密測試流程圖

(5) 判定標準：

當受測物傳送帶有加密演算法(NEA1、NEA2、NEA3)的 AS Security Mode Command 訊息，而 UE 應回覆 AS Security Mode Complete 訊息，確保 RRC 信令加密保護開啟，代表 UE 與受測物間 RRC 信令的 PDCP 層內容已加密保護。

5.2.1.4. 用戶設備和基地臺間的用戶面資料加密

(1) 測試目的：

驗證 NG-RAN 介面傳送的用戶面資料是否具備加密保護。

(2) 測試條件：

I. UE、受測物與核心網路可建立 5G 連線。

II. UE 與受測物可設定加密演算法。

III. 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 與用戶面封包之 PDCP 層的內容。

(3) 測試佈局：如圖 7 所示。

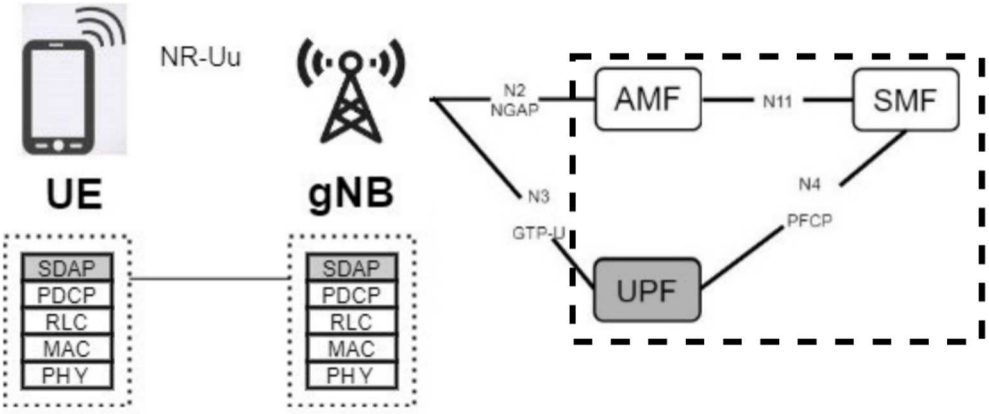


圖 7、用戶面資料加密測試示意圖

(4) 測試方法(如圖 8)：

I. UE 向 SMF 傳送用戶資料連結建立請求。

II. SMF 開啟用戶面安全策略，並向受測物傳送用戶面加密為「需要 required」的用戶面安全策略

III. 受測物傳送加密保護指示為"on"的 RRC Reconfiguration 訊息，UE 回覆 RRC Reconfiguration Complete 訊息。

IV. 檢查受測物在傳送 RRCReconfiguration 訊息後，UE 進入 CM-Idle 前所傳送的任何用戶資料。

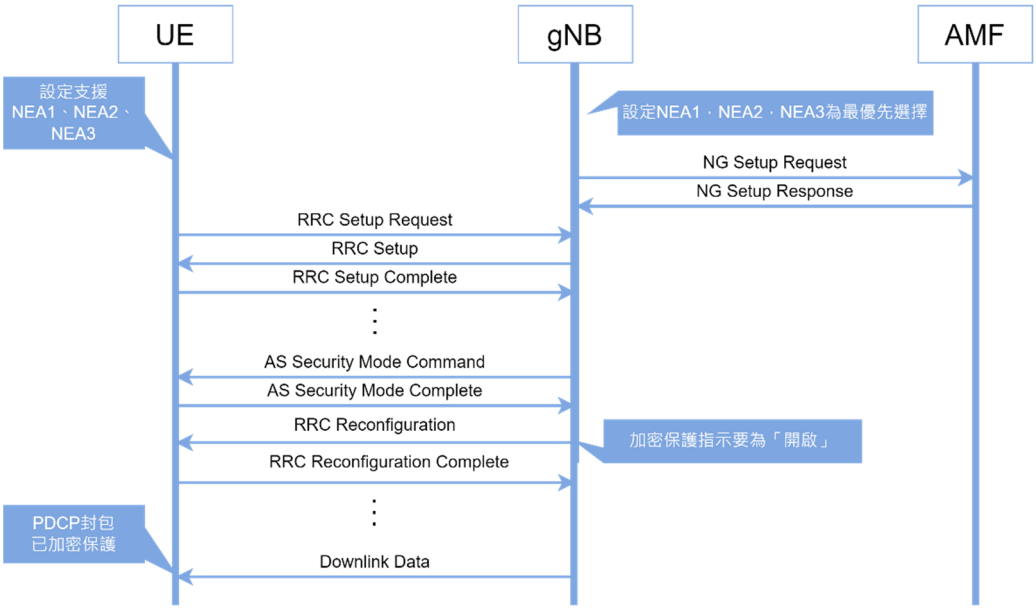


圖 8、用戶面資料加密測試流程圖

(5) 判定標準：

I. 當受測物傳送加密保護指示為"on"的 RRC Reconfiguration 訊息，而 UE 應回覆 RRC Reconfiguration Complete 訊息，代表 UE 與受測物間的用戶面封包已啟用加密保護。

II. UE 與受測物間用戶面封包之 PDCP 層內容應已加密保護。

5.2.1.5. 存取層安全性演算法優先順序

(1) 測試目的：

驗證受測物存取層加密和完整性演算法優先順序設定運作正常。

(2) 測試條件：

I. UE、受測物與核心網路可建立 5G 連線。

II. UE 與受測物可設定加密與完整性演算法，且受測物測試環境已經預設允許的安全性演算法和優先順序。

III. 測試人員可擷取 NG-RAN 介面封包以及 NGAP 介面封包，並分析 RRC 與用戶面封包之 PDCP 層內容。

(3) 測試佈局：如圖 9 所示。

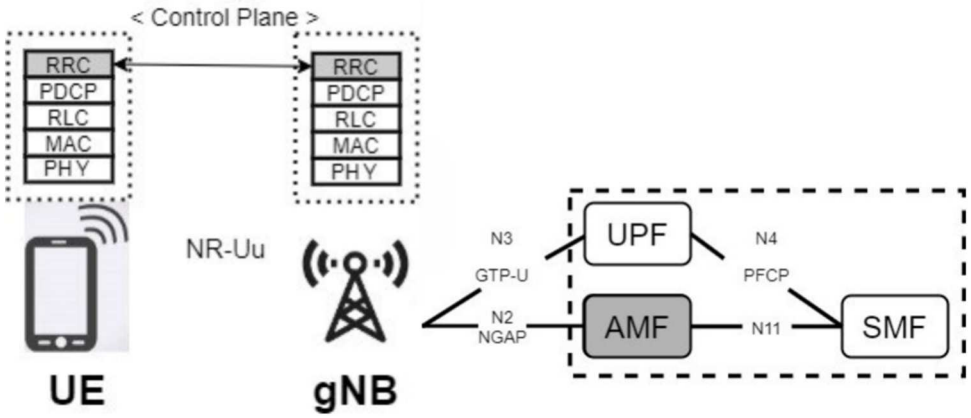


圖 9、存取層安全性演算法優先順序測試示意圖

(4) 測試方法(如圖 10)：

I. 在 UE 設定支援加密與完整性演算法(例如 NEA1、NEA2、NEA3、NIA1、NIA2、NIA3)。

II. 在受測物端依序設定加密與完整性演算法的優先順序(例如 NEA1、NIA1 為最優先，NEA2、NIA2 為次，NEA3、NIA3 再次之)。

III. 擷取 NGAP 封包資訊，確認核心網路安全能力支援加密與完整性演算法 NEA1、NEA2、NEA3、NIA1、NIA2、NIA3。

IV. 擷取 NG-RAN 介面封包，分析受測物傳送及 UE 回覆的訊息。

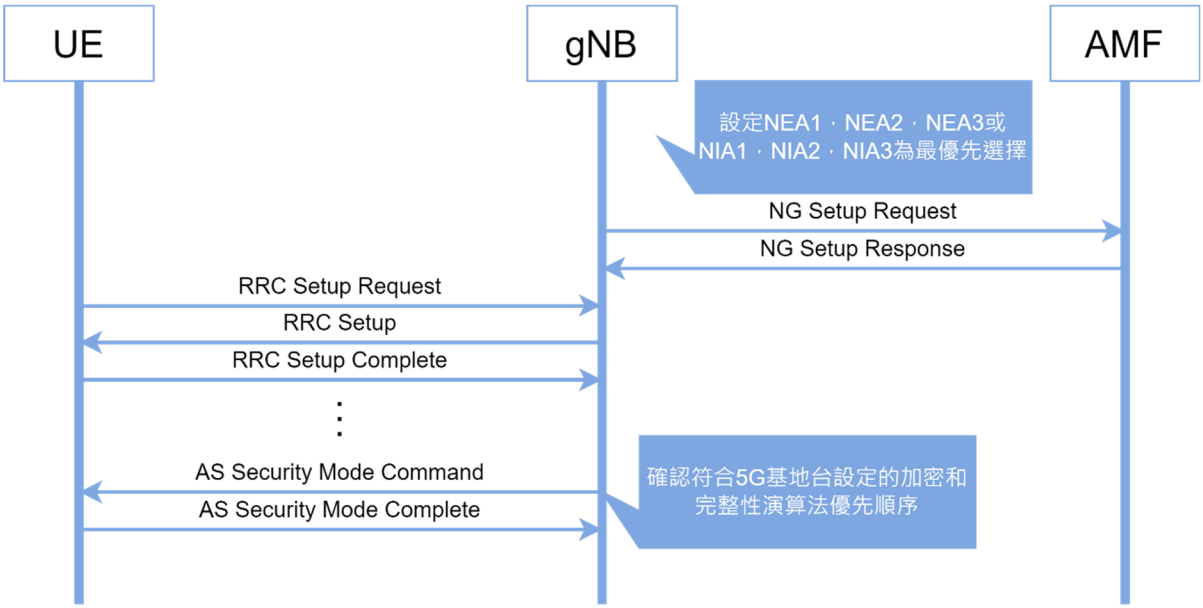


圖 10、存取層安全性演算法優先順序測試流程圖

(5) 判定標準：

確認封包內容，受測物的加密與完整性演算法符合原先設定的優先順序。

5.2.1.6. 依據 SMF 安全策略對用戶資料進行加密保護

(1) 測試目的：

驗證用戶面資料是否依據 SMF 安全策略具備加密保護。

(2) 測試條件：

I. UE、受測物與核心網路可建立 5G 連線。

II. UE 與受測物可設定加密演算法(NEA1、NEA2、NEA3)。

III. 可開啟 SMF 用戶面安全策略加密功能。

IV. 測試人員可擷取 NG-RAN 介面封包以及 NGAP 介面封包，並分析 RRC 與用戶面封包之 PDCP 層內容。

(3) 測試佈局：如圖 11 所示。

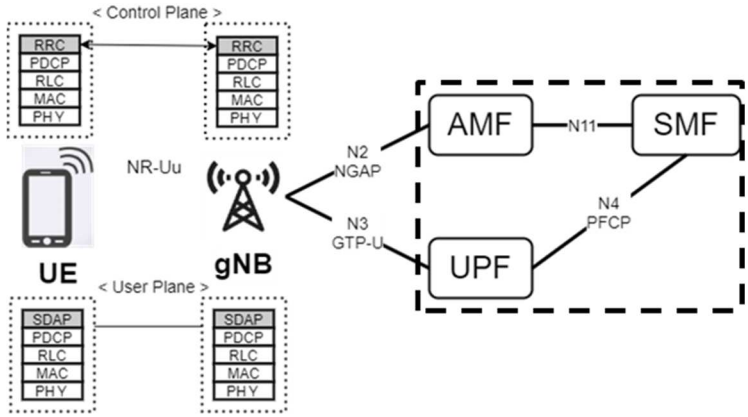


圖 11、用戶面安全策略進行加密保護測試示意圖

(4) 測試方法(如圖 12)：

I. UE 和受測物完成 RRC 信令安全驗證程序確認之後，UE 發送 PDU 連結請求訊息來觸發 PDU 連結程序(PDU session)建立。

II. 開啟 SMF 用戶面安全策略功能，向受測物傳送具「需要 required」或「不需要 not needed」加密保護的用戶面安全策略。

III. 擷取 NGAP 封包，確認 AMF 回傳受測物的指示帶有加密保護需求的安全資訊是否符合加密保護需求。

IV. 擷取 NG-RAN 介面封包，確認受測物傳送給 UE 的 RRCReconfiguration 加密保護訊息指示是否符合加密保護需求。

V. 依據用戶面安全策略檢查擷取的用戶面資料是否已啟動/未啟動。

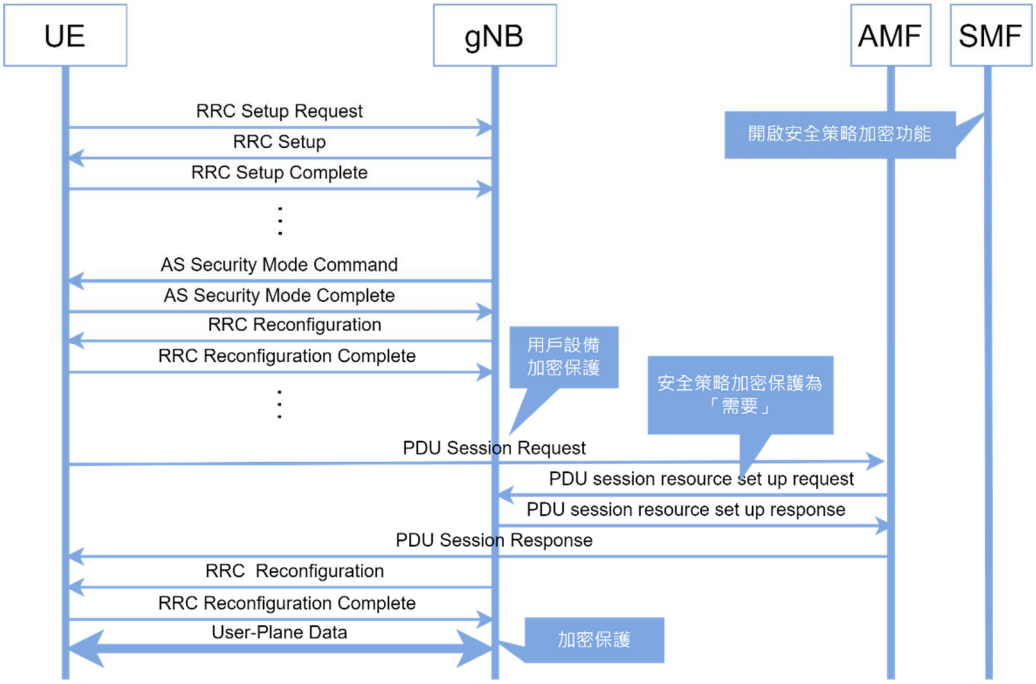


圖 12、用戶面安全策略進行加密保護測試流程圖

(5) 判定標準：

I. 當接收到「需要 required」加密保護的用戶面安全策略時，用戶面封包會依據 SMF 所發送用戶面安全策略進行加密，擷取的用戶面封包內容為非明文。

II. 當接收到「不需要 not needed」加密保護的用戶面安全策略時，用戶面封包依據 SMF 所發送用戶面安全策略沒有進行加密，擷取的用戶面封包內容為明文。

5.2.1.7. 依據 SMF 安全策略對用戶面資料進行完整性保護

(1) 測試目的：

驗證用戶面資料是否依據 SMF 安全策略受到完整性保護。

(2) 測試條件：

I. UE、受測物與核心網路可建立 5G 連線。

II. UE 與受測物可設定完整性演算法(NIA1、NIA2、NIA3)。

III. 可開啟 SMF 用戶面安全策略完整性功能。

IV. 測試人員可擷取 NG-RAN 介面封包以及 NGAP 介面封包，並分析 RRC 與用戶面封包之 PDCP 層內容。

(3) 測試佈局：如圖 13 所示。

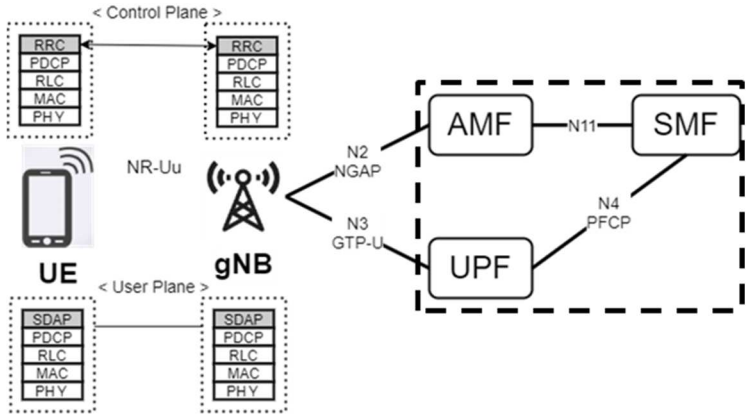


圖 13、用戶面安全策略進行完整性保護測試示意圖

(4) 測試方法(如圖 14)：

I. UE 和受測物完成 RRC 信令安全驗證程序確認之後，UE 發送 PDU 連結請求訊息來觸發 PDU 連結程序(PDU session)建立。

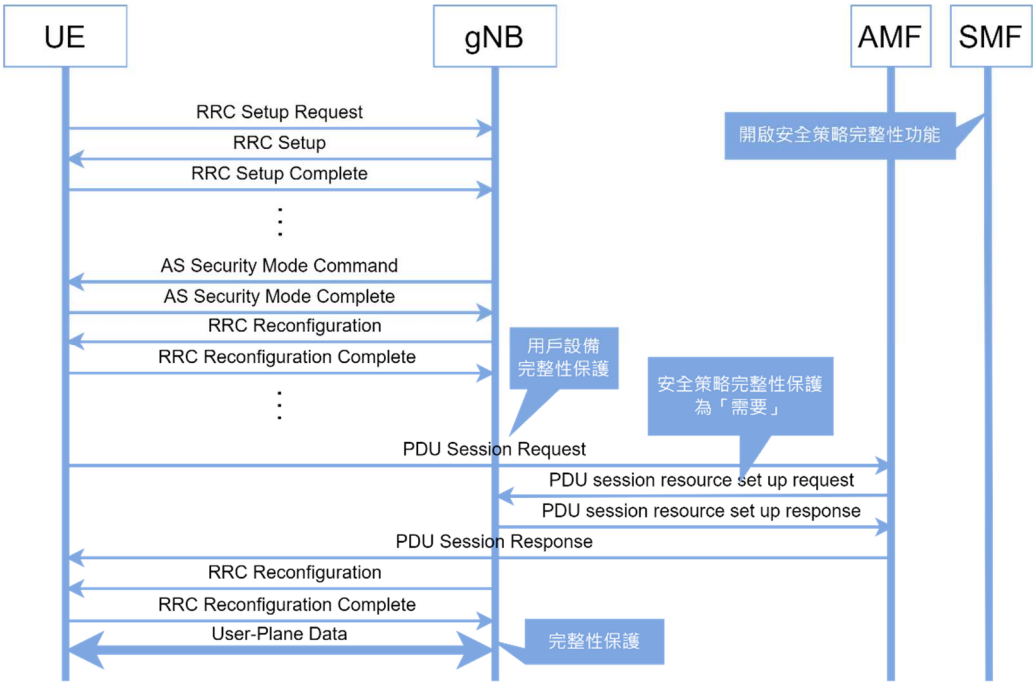
II. 開啟 SMF 用戶面安全策略功能，向受測物傳送具「需要 required」或「不需要 not needed」完整性保護的用戶面安全策略。

III. 擷取 NGAP 封包，確認 AMF 回傳受測物的指示帶有完整性保護需求的安全資訊是否符合完整性保護需求。

IV. 擷取 NG-RAN 介面封包，確認受測物傳送給 UE 的 RRC Reconfiguration 是否符合完整性保護需求。

V. 檢查用戶面完整性是否啟用/未啟用，以驗證受測物接收的用戶面安全策略與受測物在 RRC Reconfiguration 中的 UE 用戶面完整性保護策略是否相同。

圖 14、用戶面安全策略進行完整性保護測試流程圖



(5) 判定標準：

I. 當 SMF 用戶面完整性安全策略啟用，且設定為「需要 required」時，AMF 傳送的 PDUSessionResourceSetUpRequest 訊息，帶有完整性保護需求為「需要」。

II. 受測物向 UE 傳送的 RRCReconfiguration 訊息，完整性保護需求為「開啟」。

5.2.1.8. 防範 Xn 介面交遞後降階

(1) 測試目的：

驗證在受測物間交遞(handover)時，安全能力不會降階(bid down)。

(2) 測試條件：

I. UE、受測物與核心網路可建立 5G 連線。

II. UE、來源受測物(S-gNB)與目的受測物(T-gNB)可設定加密與完整性演算法。

III. 受測物可支援 Xn 介面交遞。

IV. 測試人員可擷取 NG-RAN 與 XnAP 介面封包，並分析 RRC 與用戶面封包之 PDCP 層內容。

(3) 測試佈局：如圖 15 所示。

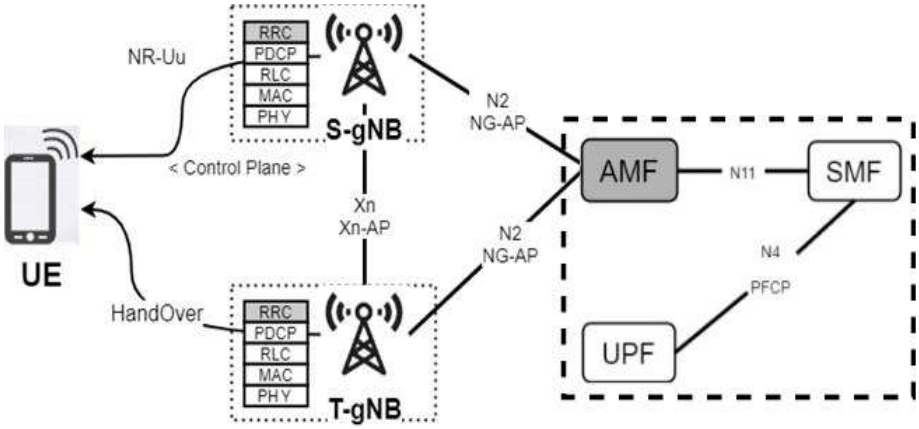


圖 15、Xn 介面交遞降階測試示意圖

(4) 測試方法(如圖 16)：

I. 在 UE 設定支援加密與完整性演算法(例如 NEA1、NEA2、NEA3、NIA1、NIA2、NIA3)。

II. 在 S-gNB 與 T-gNB 設定 NEA1、NIA1 安全性演算法為最優先選擇。

III. 確認 UE 進行 S-gNB 與 T-gNB 交遞，並與核心網路完成 Xn 介面交遞程序。

IV. 擷取 XnAP、NGAP 的封包，檢查應用協定路徑切換(path-switch)信令的 UE 安全能力(UE 5G security capabilities)。

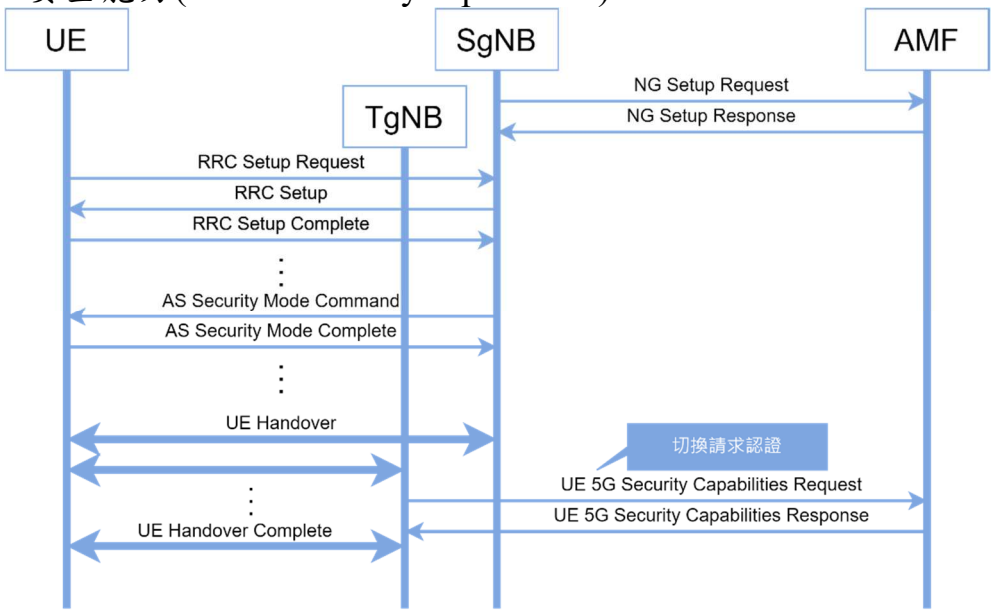


圖 16、Xn 介面交遞降階測試流程圖

(5) 判定標準：

確認交遞時，XnAP 介面 HO Request(S-gNB→T-gNB)與 NGAP 介面路徑切換信令(T-gNB→AMF)中的 UE 安全功能一致，且符合 UE 支援的安全能力，表示受測物不會降階。

5.2.1.9. gNB 變更時存取層安全性演算法的選擇

(1) 測試目的：

驗證受測物交遞時存取層安全性演算法(AS)的選擇機制。

(2) 測試條件：

I. UE、受測物與核心網路可建立 5G 連線。

II. UE、來源受測物(S-gNB)與目的受測物(T-gNB)可設定加密與完整性演算法。

III. 受測物可支援 Xn 介面交遞。

IV. 測試人員可擷取 NG-RAN 介面封包以及 XnAP 介面封包，並分析 RRC 與用戶面封包之 PDCP 層內容。

(3) 測試佈局：如圖 17 所示。

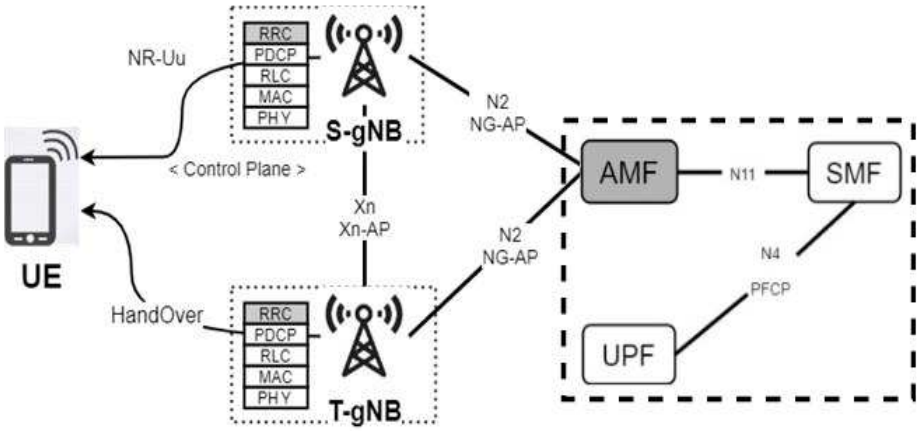


圖 17、受測物交遞安全性演算法測試示意圖

(4) 測試方法(如圖 18)：

I. 在 UE 設定支援加密與完整性演算法(例如 NEA1、NEA2、NEA3、NIA1、NIA2、NIA3)。

II. 在 S-gNB 和 T-gNB 設定 NEA1、NIA1 安全性演算法為最優先選擇。

III. UE 進行交遞，確認 UE、S-gNB 和 T-gNB 和 5GC 完成 Xn 介面交遞程序。

IV. 擷取與分析 UE 回覆的 NG-RAN 封包內容。

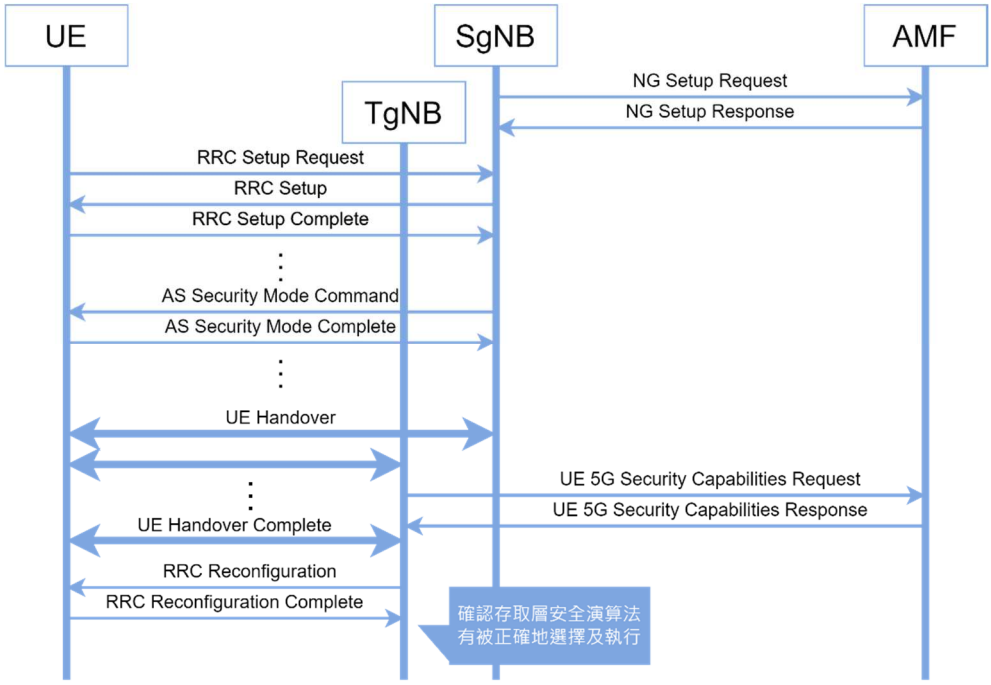


圖 18、受測物交遞安全性演算法測試流程圖

(5) 判定標準：

確認目的受測物(T-gNB)回覆給 UE 的交遞命令訊息(Handover Command message)，夾帶符合 T-gNB 的加密和完整性演算法優先順序設定。

5.2.1.10. 控制面資料在 N2 與 Xn 介面的加密保護

(1) 測試目的：

驗證 N2 與 Xn 介面間的控制面(Control Plane)資料是否具備加密性保護。

(2) 測試條件：

I. UE、受測物與核心網路可建立 5G 連線。

II. UE、來源受測物(S-gNB)與目的受測物(T-gNB)應支援 3GPP 安全性演算法(security profiles)，其產品文件也應說明 N2 與 Xn 的「加密演算法組合」。

III. 廠商提供可介接之安全閘道器 (Security Gateway)用戶端及伺服器端(支援 IKEv2)，並可設定 IPsec 安全性演算法。

IV. 採用 TLS 者，應以最新版本 3GPP TS 33.210 定義之 TLS 安全性演算法為基準。

V. 採用 IKE 與 IPsec 者，應以最新版本 3GPP TS 33.210 IKE 與 IPsec 安全性演算法為基準。

(3) 測試佈局：如圖 19 所示。

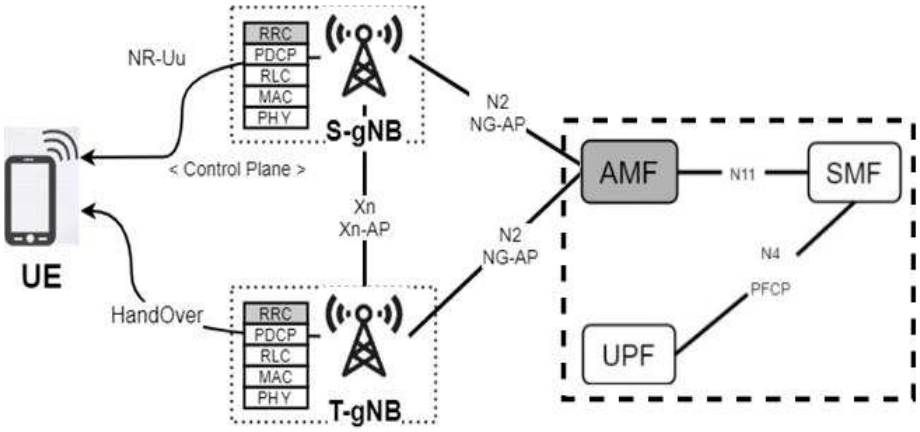


圖 19、N2 與 Xn 介面測試示意圖

(4) 測試方法：

I. 測試人員檢查產品文件，所列 N2 與 Xn 介面的「加密演算法組合」皆符合 3GPP 安全性演算法。

II. 測試人員確認受測物 N2 與 Xn 介面所支援的「加密演算法組合」符合 3GPP 安全性演算法，並驗證是否可在 UE、來源受測物(S-gNB)與目的受測物(T-gNB)之間建立安全連線。

III. 測試人員在 N2 與 Xn 介面使用非 3GPP 安全性演算法「加密演算法組合」，並驗證是否可在 UE、來源受測物(S-gNB)與目的受測物(T-gNB)之間建立安全連線。

(5) 判定標準：

受測物設定「符合」3GPP 安全性演算法，可以建立安全連線。

5.2.1.11. 控制面資料在 N2 與 Xn 介面的完整性保護

(1) 測試目的：

驗證 N2 與 Xn 介面間的控制面資料是否具備完整性保護。

(2) 測試條件：

I. UE、受測物與核心網路可建立 5G 連線。

II. UE、來源受測物(S-gNB)與目的受測物(T-gNB)應支援 3GPP 安全性演算法，其產品文件也應說明 N2 與 Xn 的「加密演算法組合」。

III. 廠商提供可介接之安全閘道器 (Security Gateway)用戶端及伺服器端(支援 IKEv2)，並可設定 IPsec 安全性演算法。

IV. 採用 TLS 者，應以最新版本 3GPP TS 33.210 定義之 TLS 安全性演算法為基準。

V. 採用 IKE 與 IPsec 者，應以最新版本 3GPP TS 33.210 IKE 與 IPsec 安全性演算法為基準。

(3) 測試佈局：如圖 20 所示。

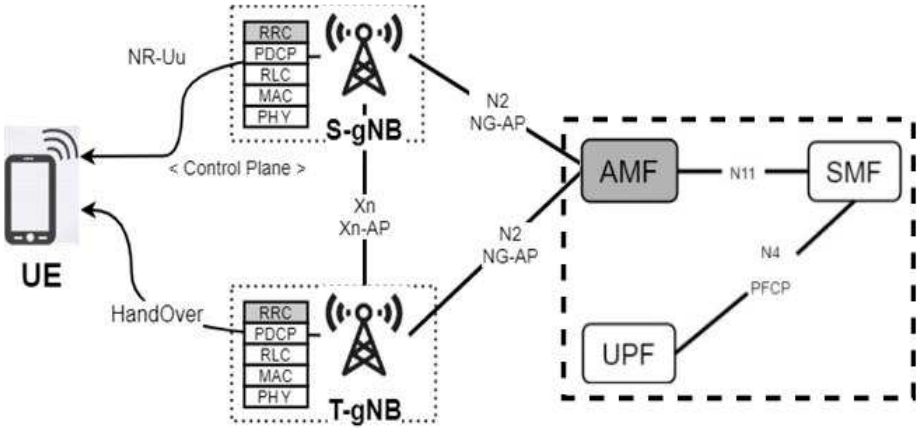


圖 20、N2 與 Xn 介面測試示意圖

(4) 測試方法：

I. 測試人員檢查產品文件，所列 N2 與 Xn 介面的「完整性演算法組合」皆符合 3GPP 安全性演算法。

II. 測試人員確認受測物 N2 與 Xn 介面所支援的「完整性演算法組合」符合 3GPP 安全性演算法，並驗證是否可在 UE、來源受測物(S-gNB)與目的受測物(T-gNB)之間建立安全連線。

III. 測試人員在 N2 與 Xn 介面使用非 3GPP 安全性演算法「完整性演算法組合」，並驗證是否可在 UE、來源受測物(S-gNB)與目的受測物(T-gNB)之間建立安全連線。

(5) 判定標準：

受測物設定「符合」3GPP 安全性演算法，可以建立安全連線。

5.2.2. 運作安全性驗證

5.2.2.1. 資料傳輸加密保護

(1) 測試目的：

確保敏感資料加密保護，不使用弱加密技術。

(2) 測試條件：

I. 產品文件應說明實際維運時，所需要的資料傳輸協定，包括各協定用途、傳輸的加密演算法、安全協定名稱與版本。

II. 測試人員應在受測物和測試電腦之間建立安全連線，並驗證當測試電腦使用非安全性演算法的協定版本和加密演算法時，無法建立安全連線。

(3) 測試佈局：如圖 21 所示。

圖 21、資料傳輸加密保護測試示意圖

(4) 測試方法：

I. 檢查產品文件，判斷是否符合 3GPP 安全性演算法。

II. 採用 TLS 者，應以最新版本 3GPP TS 33.210 定義之 TLS 安全性演算法為基準。

III. 採用 IKE 與 IPsec 者，應以最新版本 3GPP TS 33.210 IKE 與 IPsec 安全性演算法為基準。

IV. 測試人員應在受測物和測試電腦間建立安全連線，並驗證受測物實際維運所需要的資料傳輸協定是否符合 3GPP 安全性演算法。

(5) 判定標準：

實際維運需求之傳輸介面具加密保護，且受測物拒絕不安全連線(使用不安全的演算法，例如：TLS 1.1)。

5.2.2.2. 禁止未經身分認證與授權使用系統功能

(1) 測試目的：

驗證使用受測物系統功能的身分認驗證機制。

(2) 測試條件：

I. 產品文件應說明可登入系統方式(包括 SSH、SFTP)等清單與服務列表。

II. 產品文件應說明每個登入方式的身分認證與驗證機制。

III. 受測物系統應禁止 root 身分使用遠端方式 (如 SSH、SFTP)登入。

IV. 受測物系統應移除不安全的網路服務，如 TELNET 與 FTP。

(3) 測試佈局：如圖 22 所示。

圖 22、身分認驗證機制測試示意圖

(4) 測試方法：

測試 1：

a. 測試人員驗證系統功能的登入方式，至少須以用戶帳號與一項認證屬性的成功認證。

b. 測試人員檢查受測物是否已啟用身分驗證機制。

測試 2：測試人員使用「具有正確憑證」的測試設備登入受測物。

測試 3：測試人員使用「不具正確憑證」的測試設備登入受測物。

測試 4：測試人員以 root 身分使用遠端方式登入受測物系統。

測試 5：測試人員 TELNET 與 FTP 方式登入受測物系統。

(5) 判定標準：

測試 1：未經使用者認證與授權，不允許使用受測物系統功能。

測試 2：認證成功，測試設備可登入受測物。

測試 3：認證失敗，測試設備無法登入受測物。

測試 4：無法以 root 身分使用遠端方式 (如 SSH、SFTP)登入受測物系統。

測試 5：無法以 TELNET 與 FTP 方式登入受測物系統。

5.2.2.3. 預設帳號與認證屬性之安全性

(1) 測試目的：

確保預設帳號與認證屬性可移除或停用。

(2) 測試條件：

I. 產品文件應說明受測物出廠預設的所有預設帳號。

II. 產品文件應說明如何查找受測物的所有帳號與認證屬性。

(3) 測試佈局：如圖 23 所示。

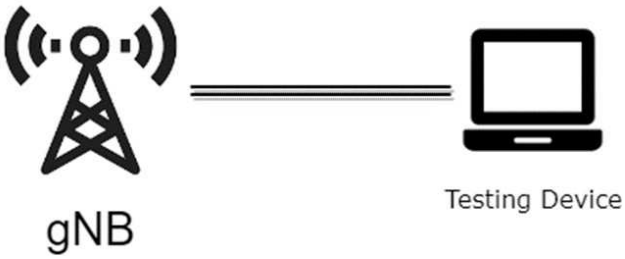


圖 23、帳號設定移除或停用測試示意圖

(4) 測試方法：

檢查產品文件所記錄的預設帳號與存在原因。

測試 1：透過管理員權限帳號登入後，查找未被文件記錄的預設帳號。

測試 2：嘗試以預設帳號遠端登入。

測試 3：以預設帳號嘗試，驗證系統是否強制要求更改登入認證屬性(如密碼)，或檢查產品文件是否有說明如何手動更改認證屬性

測試 4：登入系統後，確認是否能移除或設定停用帳號。

(5) 判定標準：

測試 1：預設帳號與產品文件所記錄相符。

測試 2：預設帳號不得提供遠端登入。

測試 3：於首次登入系統後，系統強制要求更改登入認證屬性(如密碼)，或產品文件有說明如何手動更改認證屬性。

測試 4：以預設帳號登入系統後，具備提供移除或停用預設帳號功能。

5.2.2.4. 密碼複雜度規則

(1) 測試目的：

受測物密碼結構應符合密碼複雜度規則，確保避免遭受密碼暴力破解的風險。

(2) 測試條件：

I. 產品文件須說明如何修改密碼。

II. 受測物密碼複雜度應支援最小長度 8 碼，且至少包含下述四種字元中任意三種，1.英文大寫字元(A 到 Z)；2.英文小寫字元 (a 到 z)；3.十進位數字(0 到 9)；4.非英文字母字元 (例如：!、$、#、%)，檢查密碼是否能成功建立或變更。

(3) 測試佈局：如圖 24 所示。

圖 24、受測物密碼結構測試示意圖

(4) 測試方法：

測試人員使用受測物密碼更改功能，並輸入低於密碼複雜度規則之密碼。

(5) 判定標準：

只有在新密碼滿足密碼複雜度規則時，測試人員才能更改密碼。

5.2.2.5. 密碼變更

(1) 測試目的：

系統應支援可隨時更改密碼之功能，且若系統支援，亦應測試密碼歷程紀錄功能。

(2) 測試條件：

I. 測試人員有權設置用戶帳號與密碼。

II. 測試人員可設置密碼管理策略，且使用者可自行更改密碼。

III. 測試人員驗證系統：

- 是否具備允許使用者隨時更改密碼之功能。
- [選測]驗證是否具備密碼歷程紀錄功能。

(3) 測試佈局：如圖 25 所示。

圖 25、密碼變更測試示意圖

(4) 測試方法：

A.正面測試：

測試 1：

a. 測試人員登入受測物後，依照密碼複雜度規則設定新密碼。

b. 受測物透過顯示「密碼更改成功」來驗證密碼更改。

c. 測試人員使用新密碼成功登入受測物。

測試 2：[選測]

a. 測試人員使用管理者帳號登入受測物。

b. 測試人員於受測物更改密碼歷程記錄設置為 5 次。

c. 測試人員退出管理者帳號，以使用者 Y 登入。

d. 測試人員更改使用者 Y 密碼數次，且不可重複使用更改 5 次以內使用過之舊密碼。

e. 若新密碼並非更改 5 次以內使用過之舊密碼，受測物應接受新密碼，並顯示「密碼更改成功」之訊息。

f. 測試人員使用新密碼以使用者 Y 身分成功登入受測物。

B.負面測試：

測試 1：

a. 測試人員登入受測物後，不依密碼複雜度規則設定新密碼。

b. 受測物透過顯示「拒絕密碼更改」來驗證密碼更改。

測試 2[選測]：

a. 測試人員使用管理者帳號登入受測物。

b. 測試人員於受測物中更改密碼歷程記錄設置為 5 次。

c. 測試人員退出管理者帳號，以使用者 Y 登入。

d. 測試人員更改使用者 Y 密碼數次，且重複使用更改 5 次以內使用過之舊密碼。

e. 若測試人員設置之新密碼是更改 5 次以內使用過之舊密碼，受測物應拒絕新密碼，並顯示「密碼更改失敗」之訊息。

(5) 判定標準：

A.正面測試：

測試 1：測試人員可成功更改密碼，且可使用新密碼登入。

測試 2：[選測]測試人員可成功更改密碼，且可用使用者 Y 之新密碼登入。

B.負面測試：

測試 1：測試人員更改密碼失敗。

測試 2：[選測]測試人員更改密碼失敗。

5.2.2.6. 防止暴力破解和字典攻擊

(1) 測試目的：

確保系統管理介面或網路服務是否具備暴力破解與字典攻擊保護機制。

(2) 測試條件：

I. 將受測物密碼管理策略設定為每次輸入錯誤密碼後，將計時器延時。

II. 將受測物密碼管理策略設定為在一定的密碼錯誤嘗試次數後，禁止帳號登入。

III. [選測]Web 介面可設定驗證碼(CAPTCHA)功能，以防止自動嘗試。

IV. [選測]設定密碼黑名單，至少須記錄一組黑名單密碼(滿足複雜度規則，但被列入黑名單的密碼)。

(3) 測試佈局：如圖 26 所示。

圖 26、系統管理介面或網路服務測試示意圖

(4) 測試方法：

A.正面測試：

測試 1：在每次輸入錯誤密碼後，測試計時器延遲功能。

測試 2：在指定次數的錯誤嘗試後，禁止帳號登入嘗試。

測試 3：[選測]

a. 受測物登入網頁介面設定驗證碼功能。

b. 測試人員輸入有效密碼與正確驗證碼。

c. 測試人員可以成功登入受測物。

B.負面測試：

測試 1：

a. 受測物的登入網頁介面設定驗證碼功能。

b. 測試人員輸入有效密碼，不輸入驗證碼。

測試 2：[選測]測試人員嘗試將密碼更改為黑名單密碼。

(5) 判定標準：

A.正面測試：

測試 1：在每次錯誤密碼輸入後，成功使用定時器延遲。

測試 2：在指定次數的錯誤嘗試後，成功禁止帳號登入。

測試 3：[選測]測試人員必須輸入正確的密碼和驗證碼後才能登入。

B.負面測試：

測試 1：[選測]測試人員無法登入受測物。

測試 2：[選測]測試人員無法將密碼更改為黑名單密碼。

5.2.2.7. 安全事件日誌之外部儲存管理與傳輸方法

(1) 測試目的：

受測物安全事件日誌資料可儲存至指定外部系統，且確保傳輸過程具安全防護。

(2) 測試條件：

I. 受測物安全事件日誌資料傳輸至外部系統儲存，受測物應列出支援的加密傳輸協定。

II. 建立受測物與外部系統功能的連線。

III. 測試人員具有輸出安全事件日誌資料的權限。

(3) 測試佈局：如圖 27 所示。

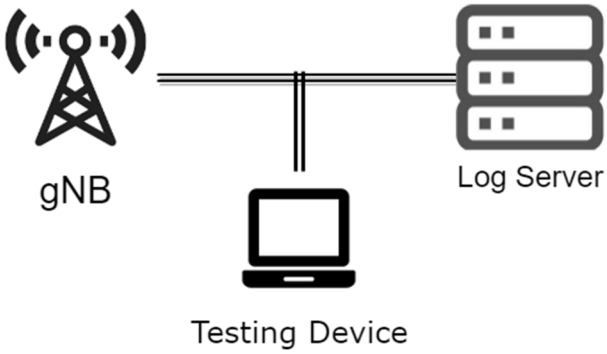


圖 27、安全事件日誌外部儲存管理與傳輸測試示意圖

(4) 測試方法：

I. 測試人員將受測物安全事件日誌資料設定為儲存至外部系統。

II. 測試人員觸發受測物安全事件，並側錄安全事件日誌資料傳輸時的封包資訊。

III. 測試人員檢查安全事件日誌資料傳輸時設定的加密傳輸協定是否符合 3GPP TS 33.210 之 TLS 安全性演算法。

IV. 測試人員檢查外部系統是否儲存該檢測項目所傳輸之安全事件日誌資料。

(5) 判定標準：

I. 安全事件日誌資料傳輸時設定的加密傳輸協定，必須為安全標準協定(不得為不安全的演算法，例如：TLS 1.1 等)。

II. 測試人員驗證外部系統已儲存受測物所傳輸之安全事件日誌資料。

5.2.2.8. 安全事件日誌檔之保護

(1) 測試目的：

受測物安全事件日誌僅能被特定權限的使用者存取。

(2) 測試條件：

產品文件應說明如何存取安全事件日誌資訊與存取權限之設定。

(3) 測試佈局：如圖 28 所示。

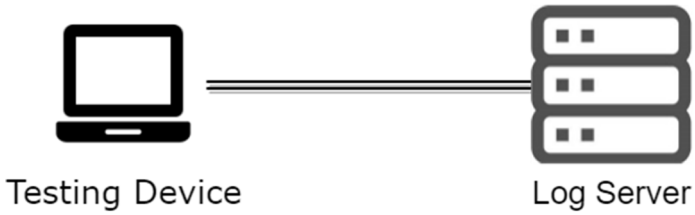


圖 28、安全事件日誌檔使用者存取測試示意圖

(4) 測試方法：

依據產品文件說明，按照測試 1、2 中的描述重複進行測試：

測試 1：測試人員使用「具有」安全事件存取權限之帳號存取安全事件日誌。

測試 2：測試人員使用「不具有」安全事件存取權限之帳號存取安全事件日誌。

(5) 判定標準：

測試 1：驗證「可以」存取安全事件日誌。

測試 2：驗證「不可以」存取安全事件日誌。

5.2.2.9. 軟體完整性驗證

(1) 測試目的：

受測物更新軟體時應進行完整性檢測，以驗證軟體更新檔是否遭到竄改。

(2) 測試條件：

I. 產品文件應說明如何授權用戶安裝軟體更新檔。

II. 設備商應提供受測物合法且未經竄改的軟體更新檔與經篡改的軟體更新檔。

(3) 測試佈局：如圖 29 所示。

圖 29、受測物軟體完整性測試示意圖

(4) 測試方法：

I. 測試人員檢查受測物安裝軟體的許可權限，以及是否只有具許可權限的身分可安裝軟體。

II. 測試人員使用合法且未經竄改的軟體更新檔執行安裝。

III. 測試人員使用經篡改的軟體更新檔執行安裝。

(5) 判定標準：

I. 執行軟體安裝前應執行身分驗證，且只有具備許可權限的身分可安裝軟體更新檔。

II. 使用合法且未經竄改的軟體更新檔時，可安裝軟體更新檔。

III. 使用經篡改的軟體更新檔時，無法安裝軟體更新檔。

5.2.2.10. 連結識別碼(Session ID)安全性

(1) 測試目的：

驗證受測物所使用連結識別碼是否符合安全性。

(2) 測試條件：

受測物所使用的連結識別碼是否符合以下要求：

- 連結識別碼應唯一，且不重複使用。
- 連結識別碼應為不可預測、無特定規律。
- 連結識別碼不應包含以明文顯示的敏感資訊(例如帳號等)。
- 每個新連結應重新產生新的連結識別碼(例如每次用戶登入時)。

(3) 測試佈局：如圖 30 所示。

圖 30、Session ID 安全性測試示意圖

(4) 測試方法：

測試人員透過觸發登入等方式，取得連結識別碼，予以逐項檢查。

(5) 判定標準：

受測物所使用的連結識別碼符合列出的每項要求。

5.2.2.11. 安全事件紀錄

(1) 測試目的：

驗證受測物是否正確記錄所要求的安全事件類型，包含登入失敗、管理者存取行為、設定變更等。

(2) 測試條件：

產品文件應提供以下資訊：

- 記錄事件日誌與查閱方式(例如完整路徑)。
- 安全事件紀錄是否預設啟用與啟用方式。
- 安全事件紀錄類型與格式說明。

(3) 測試佈局：如圖 31 所示。

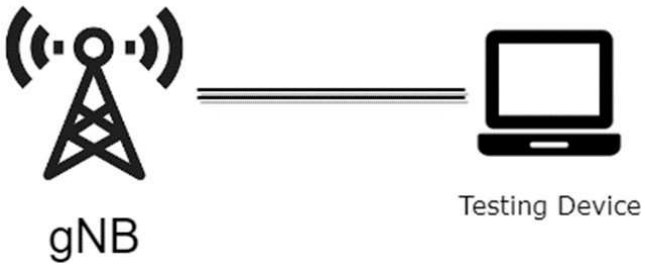


圖 31、記錄安全事件測試示意圖

(4) 測試方法：

I. 測試人員觸發安全事件。

II. 測試人員驗證是否正確記錄安全事件(包含登入失敗、管理者存取行為、設定變更等)，以及需要記錄的事件資訊(包括存取時戳、來源 IP 等)。

(5) 判定標準：

所有安全事件都被適當記錄，包括登入失敗、管理者存取行為、設定變更等，以及事件資訊(包括存取時戳、來源 IP 等)。

5.2.2.12. 通訊埠掃描

(1) 測試目的：

驗證只有產品文件所列傳輸層的通訊埠會回應系統外部的請求。

(2) 測試條件：

I. 產品文件應說明可用的網路服務清單，並包括：

- 所使用的 IP 協定與其傳輸層協定。
- 傳輸層協定開啟的通訊埠與相關服務。

II. 通訊埠掃描工具應能夠檢測傳輸層協定啟用的通訊埠。

(3) 測試佈局，如圖 32 所示。

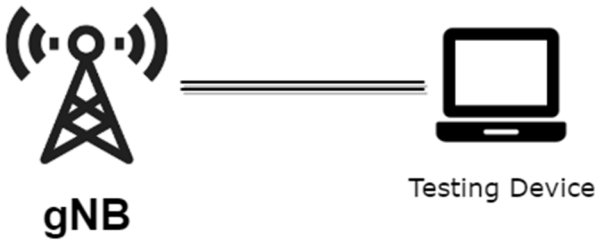


圖 32、通訊埠掃描測試示意圖

(4) 測試方法：

I. 驗證網路服務清單中的項目對於受測物運作是否合理且必要。

II. 使用通訊埠掃描工具或其它測試方法來識別啟用的通訊埠。

III. 驗證啟用的通訊埠與產品文件所列的網路服務清單是否相符。

(5) 判定標準：

I. 網路服務清單所列項目為受測物運作必要所需。

II. 啟用的通訊埠與產品文件所列網路服務清單相符。

5.2.2.13. 弱點掃描

(1) 測試目的：

驗證受測物作業系統與內建應用程式服務或網頁伺服器，是否存在高風險已知弱點。

(2) 測試條件：

I. 產品文件應說明使用的作業系統、內建應用程式服務清單或網頁伺服器等功能。

II. 使用能檢測作業系統與內建應用程式服務的弱點掃描工具。

(3) 測試佈局：如圖 33 所示。

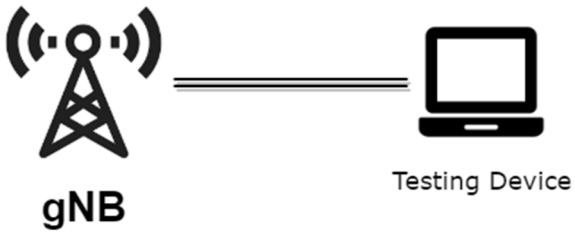


圖 33、弱點掃描測試示意圖

(4) 測試方法：

I. 確認受測物作業系統與內建應用程式服務是否與產品文件所列相符。

II. 應使用妥適對應的主機弱掃與網頁弱掃工具對作業系統、內建應用程式、網頁伺服器進行測試。

(5) 判定標準：

I. 受測物作業系統、內建應用程式與產品文件所列相符

II. 依據弱點掃描測試結果，檢視受測物作業系統、內建應用程式服務、網頁伺服器不應存在 CVE 最新版本 CVSS 評分 7 分以上之高風險弱點，若最新版本無此弱點資訊者，以 NIST NVD 前一次公告版本之 CVSS 評分為基準。

6. 附則

6.1. 若受測物無法與檢測實驗室設備互通，得由廠商提供可互通之檢測環境，包括基地臺與核心網路等設備，以完成資安檢測。

6.2. 本檢測指引所制定安全要求，如因受測物功能限制，而無法進行檢測時，廠商可參照附件 A 風險控制評估表之格式提出聲明(如其他設備具備該同等控制措施之聲明)，以減緩或彌補受測物因功能限制之風險。

附件 A

風險控制評估表(範例)

編號	測試項目	風險描述	控制措施	風險減緩程度 (高/中/低)	是否具備同等安全 (是/否)
1.	5.2.2.4 密碼複雜度規則	不具備密碼複雜度規則功能，可能導致弱密碼等問題	管理系統具備密碼複雜度規則功能	低	是