

# Cisco網路安全入門證照一 CCNA Security

文◎余采霏

資訊安全已經是企業IT管理的重點工作，例如喧擾一時的陳冠希事件引發個人資訊安全的疑慮，也引起企業的高度重視，近期更多的資料外洩，諸如Payeasy高達5千多筆會員帳號密碼遭駭客破解、東森購物近千名客戶資料疑似內神通外鬼不翼而飛，在在都提醒著企業不要成為資安負面新聞焦點，也更強調了資訊安全的重要性。

身為IT人員，面對一連串的惡意程式、非法入侵、面臨層出不窮的犯罪手法，挑戰也愈來愈嚴苛，卻也責無旁貸。雖然許多攻擊入侵都是經由網路進入，但是位居第一線的網管人員未必具有充足的觀念及技術可加以防禦，如果想要為企業做好資訊安全把關的角色，網管人員必須設法循著有系統、有條理的方式來快速強化技能，也提高自身對企業而言的價值。

「資安證照就是一個很好的打底工具。」奇科電腦教育中心技術團隊總召集人賴玉斌指出，目前市場上同時具有資安以及



▲奇科電腦教育中心技術團隊總召集人賴玉斌指出，雖然思科已經針對網路安全設計中階的CCSP以及高階的CCIE Security，但是在從CCNA進階到CCSP的過程中，其實有很大的門檻，而CCNA Security剛好成為這中間銜接的角色。

網管的人才並不多。根據思科與IDC共同調查的一項數據，全球企業對於網管工作者的需求超過實際市場供給40%。

換句話說，許多企業找不到合格的網管人員，這樣的情形被稱為「Skill Gap」，而Skill Gap也將嚴重影響企業的生產力及競爭力；以新興市場（Emerging Market）為例，目前近5成的公司嚴重缺乏資安人才，預估5年內甚至將逼近8成。

## 思科新安全證照

有鑑於資安人才培養的迫切性，今年6月思科在全球同步發表了最新認證－思科網路安全認證（CCNA Security）。這是以CCNA為基礎再往上延伸的網路安全課程，主要內容包含了網路安全基礎知識、攻擊與防禦機制、防火牆技術、入侵防禦系統技術、端點安全概論及區域網路安全概論等等，適合網路安全相關工作者及管理者進修。

賴玉斌表示，雖然思科

已經針對網路安全設計中階的 CCSP (Cisco Certified Security Professional)，以及高階的 CCIE Security (Cisco Certified Internetwork Expert Security)。但是在從 CCNA 進階到 CCSP 的過程中，其實有很大的門檻，而 CCNA Security 剛好成為這中間銜接的角色，透過更紮實的課程了解工作上所需的資安相關知識，得以迅速運用於工作實務，並且確認自身是否要往 CCSP 或是更高階的課程邁進。

「其實 Cisco 在 2007 年底宣告 CCNA 改版時，就已經埋下了許多伏筆。為了培養更多符合市場需求的專業技術人才，思科挑選了三項目前最有潛力的領域，以網路為基礎出發，分別推出 CCNA Security、CCNA Voice 或是 CCNA Wireless。而這樣設計的好處更能突顯專業分野，依照思科所規劃的藍圖，未來 IT 人員在取得 CCNA 證照之後，可以依其工作需求、興趣以及能力，選擇 CCNA Security、CCNA Voice 或是 CCNA Wireless 等專業證照，CCNA Security 的推出正是思科實踐藍圖的一部分。」

## 8月開課起跑

根據瞭解，CCNA Security 課程首波開課將由奇科與晨宇資訊合作，預計會在 8 月開課，不過，讀者必須留意，在還沒取得 CCNA 之前，不能直接考 CCNA Security 認證。亦即，取得 CCNA Security 的先決條件就是

一定得通過 CCNA，不管是採取先考 640-822 ICND1 取得 CCENT 證照，再考 640-816 ICND2 取得 CCNA 證照，亦或直接考 640-802 取得 CCNA 證照。唯有取得 CCNA 認證才能再加考 IINS 640-453 (Implementing Cisco IOS Network Security)，正式取得 CCNA Security 資格。

而在考試的科目上，只需要考一科，時間約莫為 90 分鐘，會以複選題的型式出現，但賴玉斌建議有興趣的讀者，千萬不要抱持著僥倖的「背多分」心態，靠著死背的工夫在作答而取得證照的作法進入職場其實是有很大的風險，「測試一個人夠不夠專業，只要從談話中就可以得知了，利用教育機構所提供的課程最大的精髓，就是讓自己在這門課程中學到真正有用的技能，也因為如此，奇科特別在教室內備有充足的思科網路設備，為的就是提供實作的機會，讓想要瞭解如何強化資安的學員，有更多的時間可以操作設備，如此，才能讓這門證照課程發揮最大的效用，也才能在遇到問題時，在第一時間就能找到根源，徹底解決。」

「當然，要達到這些效益，基本原理的教學內容也是不可缺少的。」賴玉斌表示，CCNA Security 的課程規劃很完整，從網路安全原則介紹、外緣網路安全、使用 Cisco IOS 防火牆的網路安全、站對站的虛擬私人網路 (VPN)、使用 Cisco IOS 入侵防護系統的網路安全以及區域網路

(LAN)、儲存區域網路 (SAN)、語音與端點安全總覽等，這些課程都是相當基本而且重要，對於建構網路安全基礎相當有幫助，如果 IT 人員想要更進一步鑽研 CCSP (Cisco Certified Security Professional)，CCNA Security 也是一個很好的敲門磚。網管人

## CCNA Security 課程內容

### ◆ 網路安全原則介紹

- 網路安全基礎
- 攻擊方式
- 作業安全
- Cisco 自我防衛網路

### ◆ 外緣 (網路) 安全

- 路由器存取管理
- Cisco 的安全設備管理 (圖形管理介面)
- Cisco 路由器上的 AAA 機制
- 使用本地的資料庫還有安全存取控制伺服器
- 安全管理/報告
- 路由器保護機制

### ◆ 使用 Cisco IOS 防火牆的網路安全

- 防火牆的技術
- 使用存取控制清單 (ACLs) 過濾靜態封包
- Cisco IOS zone-based 政策型防火牆

### ◆ 站對站的虛擬私人網路 (VPN)

- 密碼 (加解密) 服務
- 對稱加密
- 密碼上的雜湊及數位簽章的測驗
- 非對稱加密以及公開金鑰基礎建設
- IPsec 的基礎
- 基於 IPsec 的站對站虛擬私人網路
- 使用 Cisco SDM 管理基於 IPsec 的站對站虛擬私人網路

### ◆ 使用 Cisco IOS 入侵防護系統的網路安全

- 入侵防護系統的技術
- 使用 Cisco SDM 管理 Cisco IOS 入侵防護系統

### ◆ 區域網路 (LAN)、儲存區域網路 (SAN)、語音及端點安全總覽

- 端點安全
- 儲存區域網路安全
- 語音安全
- OSI 第二層的攻擊