A Preliminary Evaluation of the new Cisco Network Security Course

S P Maj, D Veal, L Yassa *

Edith Cowan University, Perth, Western Australia
*Meadowbank College of TAFE, Sydney, NSW, Australia

Summary
The Cisco Network Academy Program (CNAP) is a global education program that offers a range of course suitable for high schools, college students and practicing professionals. The recently introduced Cisco Certified Network Associate (CCNA) Security course, builds upon the foundation Cisco Certified Network Associate (CCNA) course, and is designed to provide core security concepts and the practical skills to design and configure a secure network. The CCNA Security course contextualizes network security and then provides instruction in a range of security technologies. This paper is a preliminary evaluation of the CCNA Security course and discusses its strengths and weaknesses.

Key words:
Network Security, CCNA Security course.

1. Introduction

The Cisco Network Academy Program (CNAP) was introduced in the late 1990's at an initial cost of US$25 million. CNAP consists of a range of courses from introductory material suitable to high schools to more advanced courses for college students and also practicing professionals [1], [2]. CNAP provides multimedia oriented training materials, simulations and assessments. Low cost equipment is also available. A key element of CNAP is the accreditation of CNAP instructors. This is important in order to ensure quality control standards on a global basis. There are over 10,000 Cisco Academies in over 100 countries. CNAP is recognized as the international benchmark for network education and training. CNAP also provide on-line assessments thereby providing a qualification that is recognized globally.

Typically college students would initially undertake the Cisco Certified Network Associate (CCNA) course. The CCNA course provides both theoretical and practical instruction in network basics. CNAP provide on-line curriculum, a network simulator and both formative and summative on-line assessments. It is expected that students will complete both practical, 'hands-on' exercises using actual devices as well as practice in the use of a network simulator. CCNA is delivered within CNAP in two flavors, Exploration and Discovery, while Discovery is intended to address high school students, Exploration is the norm in VET and college level. There are four components to the CCNA Exploration course:

1. Network fundamentals
2. Routing Protocols and Concepts
3. LAN Switching and Wireless
4. Accessing the WAN

Significantly this course provides opportunities for the development of not only hands-on, practical skills but also soft-skills development. The CCNA course is a prerequisite for the more specialized CCNA Security course.

2. CCNA Security

The CCNA Security course is designed to provide both theoretical and practical instruction in security. There are nine sections (chapters / modules) to this course each with a defined set of goals (table 1). On-line instructional material is provided. Student laboratory manuals are available and also the associated instructor laboratory manuals that contain the answers to the laboratory exercise. CNAP also provide on-line formative and summative assessments.

Table 1. CCNA Security course

	Chapter	Goals
1	Modern Network Security Threats	Explain network threats, mitigation techniques, and the basis of securing a network
2	Securing Network Devices	Secure administrative access on Cisco routers
3	Authentication, Authorization and Accounting	Secure administrative access with AAA
4	Implementing Firewall Technologies	Implementing firewall technologies to secure the network perimeter
5	Implementing Intrusion Prevention	Configure IPS to mitigate attacks on the network
6	Securing the Local Area Network	Describe LAN security considerations and implement

Manuscript received September 5, 2010
Manuscript revised September 20, 2010

		endpoint and Layer 2 security features
7	Cryptography	Describe methods for implementing data confidentiality and integrity
8	Implementing Virtual Private Networks	Implement secure virtual private networks
9	Putting It All Together	Given the security needs of an enterprise, create and implement a comprehensive security policy

(http://www.cisco.com/web/learning/netacad/course_catalog/CCNAsecurity.html)

The practical exercises are conducted using both the text-based Command Line Interface (CLI) and the Security Device Manager (SDM) Graphical User Interface (Table 2). The CCNA course is a prerequisite because student must be able to build a network of routers and switches.

Table 2. CCNA Security workshop exercises

	Chapter	Workshop exercises
1	Modern Network Security Threats	Research network attacks. Research security audit tools
2	Securing Network Devices	Control administrative access for routers Configure administrative roles Configure IOS resilience and management reporting Configure automated security features
3	Authentication, Authorization and Accounting	Configure local authentication using AAA using both the CLI and SDM Configure centralized authentication using AAA and RADIUS using both the CLI and SDM
4	Implementing Firewall Technologies	Configure a Context-Based Access Control (CBAC) Firewall using Autosecure Configure a Zone-Based Policy Firewall (ZBF, ZPF or ZFW) using the SDM
5	Implementing Intrusion Prevention	Configure and test an Intrusion Prevention System (IPS) using both the CLI and SDM.
6	Securing the Local Area Network	Configure secure trunk and access ports
7	Cryptography	Decipher a pre-encrypted message using the Vigenere Cipher. Create a Vigenere cipher encrypted message and decrypt it Use steganography to embed a secret message in a graphic
8	Implementing Virtual Private Networks	Configure and test a site-to-site VPN using both the CLI and SDM Configure and test a Remote Access VPN using the SDM
9	Putting It All Together	Create a Basic Security Policy Configure secure network routers Configure secure network switches Configure VPN remote

3. CCNA Security Evaluation

All authors of this paper are CNAP accredited CCNA Security instructors. One contributor is a Cisco accredited CCNA Security instructor trainer.

The CCNA Security course has both strengths and weaknesses (Table 3). Cisco instructional material is considered to be the global standard in professional training and instruction. Certainly a major strength is the laboratory manual. Some of the workshops require students to build a complex, secure network. The manual provides a clear step-by-step guide for all the exercise.

However there are some significant concerns. The material tends to be Cisco specific despite the fact there are other popular security devices on the market. For example Check Point offers a range of dedicated security solutions: Security Gateways; Security Management and Endpoint Security. The authors recommend a more balanced perspective in the course material would be appropriate.

CNAP regularly rewrite existing course material and new courses every few years. This is important given the rate of technological changes in networking. The CCNA Security course is a new offering but fails to address what is likely to be an increasing important topic – cloud computing. Whilst this is a developing field the authors consider this sufficiently important that it should have been included. Virtualization is now routinely employed; however the course material makes no reference to this topic.

The Security Device Manager (SDM) is a useful GUI but does not always deploy successfully. Furthermore SDM, whilst easy to use can often generate a significant amount of configuration code. The course does not explain all the lines of code generated. For some protocols over one hundred lines of configuration code are generated. Hence, use of the SDM may be problematic in a working network during fault diagnosis [3].

Table 3. CCNA Security course evaluation.

	Advantage	Disadvantage
1	Represents industry standard	Cisco product specific.
2	World leaders in training materials for network technology education	Many PIX devices currently in use. No instruction on PIX devices.
3	Entry level for further Cisco based more advanced security studies	Other security products e.g. Checkpoint only mentioned. More detail should be provided thereby providing a more balanced approach.
4	Good introduction to security in Layer 2 and 3 devices	Security Device Manager (SDM) not a stable product as yet
5	Comprehensive workshop exercises	SDM easy to use but automatically produces a lot of code. Fault diagnosis may be problematic
6	Covers end-to-end security solutions such as Virtual Private Networks (VPNs)	Limited or non-existent: 1. Implementing IPS & IDS 2. Event correlation (using MARS) 3. PVLANs
7	Covers in a reasonable manner the management aspects of network security.	Very limited details about NAC
8		Very basic introduction to critical asset identification. Should be expanded.
9		Included basic explanation about security issues for emerging technologies as Voice, Wireless, and SANs while the introduction to those technologies was very basic.
10		Nothing on secure Virtualization and cloud computing (see the previous point)
11		Lacks broader coverage for such issues as the various types of authentication methods
12		Lacks details about hacker attacks, vulnerability assessment and auditing
13		Cisco instructional material verbose.
14		More emphasis needed on broader security issues such as user awareness (mitigating non-technical vulnerabilities)
15		Triggers to IPS/IDS can be classifies as pattern based, anomaly based, behavior based or honeypot based. All of these are termed – within the course – as signature based which is confusing.
16		Even the course did talk about such threats as viruses and worms; it did not mention in sufficient details Cisco solutions for such threat detection and mitigation. Examples for Cisco solutions: CSA, Ironnport, Trend Micro InterScan for Cisco CSC SSM for the ASA and Cisco Secure Policy Manager
17		Lacks instruction in how to design the topology of a secure network.

Whilst the laboratory manuals are quite comprehensive further workshops are needed especially for some of the more complex systems such as firewalls. The workshop exercises provide instruction on how to create firewalls and then analyze using the SDM 'edit firewall policy' tab (Figure 1). This tab represents a potentially complex series of interactions that are not fully explained or explored. Hence the authors strongly recommend a series of workshop exercises starting with the simplest possible firewall configuration and then progressively introduce more complexity. This will then allow students to scaffold their knowledge to more complex and realistic firewall scenarios and assist them in use of the firewall policy editor.

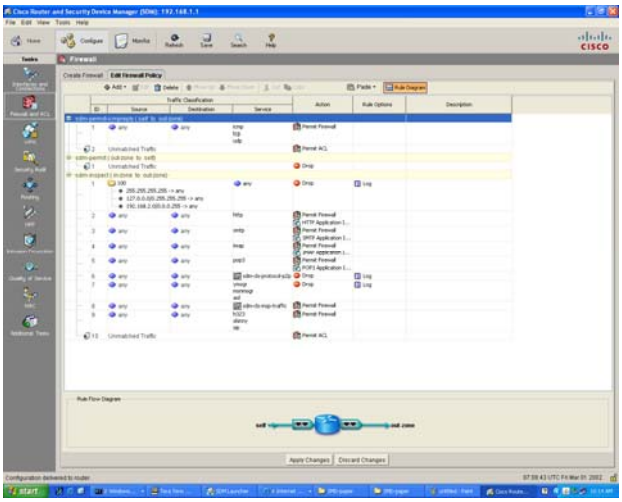

Figure 1. Security Device Manager (SDM) – Edit Firewall Policy.

Similarly the workshop exercises for Intrusion Prevention Systems (IPS) should be modified. IPS is a complex system to configure and more time should be allocated to exploring and examining this protocol. After configuring a network there are four main tasks to configure IPS:

1. Prepare router and tftp server
2. Copy IPS crypto key
3. Configure IPS
4. Load IPS signature package to router
5. Test IPS rule and modify as needed.

Task 2 alone consists of a number of complex steps:

Task 2
1. Create IPS rule
2. Confirm IPS signature in router flash
3. Enable IPS Security Device Event Exchange (SDEE)
4. Enable IPS syslog support
5. Download and start syslog server
6. Configure IOS IPS to use pre-defined signature categories
7. Apply IPS rule to specified interface.

The tasks and associate steps represent what students must do to complete the exercise. However the main focus should be on how IPS works. Hence the authors recommend this workshop be considerably expanded. Students should be given the opportunity to start with the simplest possible IPS and then progressively work to more complex scenarios.

Site to site Virtual Private Networks (VPNs) are complex. One of the biggest problems is that two routers must be configured in a complimentary manner i.e. keys, encryption, access control lists and mapping. Understanding this is important to successful implementation. The authors recommend use of State Model Diagrams (SDMs) not only for teaching purposes but also as a network management tool [4]. They have been demonstrated to be particularly useful for complex security protocols [5]. There are proven pedagogical advantages to the use of SDMs and it has been clearly demonstrated that they are universally applicable to all network devices and protocols [6], [7], [8].

3. Conclusions

Cisco is the recognized leader in network training, education and certification. As a new course the CCNA Security is designed to set the benchmark standard for security instruction and training for the next few years. Certainly this course has its strengths however there are some major concerns. In particular this course does not address security in the context of virtualization – now a commonly deployed technology. It is always difficult to predict the importance of new technologies but cloud computing is likely to be of increasing importance; however this course does not include this topic. The authors consider one of the strengths of this course to be the laboratory manual. It is comprehensive and guides students step-by-step through some complex security configurations. However, the authors suggest more extensive workshop exercises should be provided thereby allowing students to more extensively explore some of the more complex security protocols such as IPS and firewalls. The authors strongly recommend the use of State Model Diagrams (SDMs) as an instructional tool – especially for the more complex security protocols such as Virtual Private Networks.

References

[1] Kohli, G., et al. *Abstraction in Computer Network Education.* in *2004 American Society for Engineering Education Annual Conference & Exposition (ASEE 2004).* 2004. Salt Lake City, Utah, USA.

[2] Murphy, G., et al. *An Examination of Vendor-Based Curricula in Higher and Further Education*. in *2004 American Society for Engineering Education Annual Conference & Exposition (ASEE 2004).* 2004. Salt Lake City, Utah.

[3] Maj, S.P., Makasiranondh, W., Veal, D., *An Evaluation of Firewall Configuration Methods.* IJCSNS International Journal of Computer Science and Network Security, 2010. **10**(8): p. 1-7.

[4] Maj, S.P., Veal, D., *An Evaluation of State Model Diagrams for Secure Network Configuration and Management.* IJCSNS International Journal of Computer Science and Network Security, 2010. **10**(9).

[5] Nuangjamnong, C., Maj, S. P., Veal, D. *Network Security Devices and Protocols Using State Model Diagrams*. in *5th Australian Information Security Management* 2007. Edith Cowan University, Perth, Western Australia: School of Computer and Information Science, Edith Cowan University.

[6] Maj, S.P., G. Kohli, and G. Murphy. *State Models for Internetworking Technologies*. in *IEEE, Frontiers in Education, 34th Annual Conference*. 2004. Savannah, Georgia, USA: IEEE.

[7] Maj, S.P., G. Kohli, and T. Fetherston. *A Pedagogical Evaluation of New State Model Diagrams for Teaching Internetwork Technologies*. in *28th Australasian Computer Science Conference (ACSC2005)*. 2005. Newcastle, Australia: Australian Computer Society and the ACM Digital Library.

[8] Maj, S.P. and D. Veal, *State Model Diagrams as a Pedagogical Tool - An International Evaluation.* IEEE Transactions on Education, 2007. **50**(3): p. 204-207.

A/Prof S. P. Maj has been highly successful in linking applied research with curriculum development. In 2000 he was nominated ECU University Research Leader of the Year award He was awarded an ECU Vice-Chancellor's Excellence in Teaching Award in 2002, and again in 2009. He received a National Carrick Citation in 2006 for "*the development of world class curriculum and the design and implementation of associated world-class network teaching laboratories"*. He is the only Australian judge for the annual

IEEE International Student Competition and was the first Australian reviewer for the American National Science Foundation (NSF) Courses, Curriculum and Laboratory Improvement (CCLI) program.

Dr. David Veal is a Senior Lecturer at Edith Cowan University. He is the manager of Cisco Network Academy Program at Edith Cowan University and be a unit coordinator of all Cisco network technology units. His research interests are in Graphical User Interface for the visually handicapped and also computer network modeling.

Lotfi Yassa is an IT Head Teacher at TAFE NSW. He is the manager of NSI Regional Cisco Networking Academy Program at Meadowbank College of TAFE and member of APAC Cisco Academy Advisory Committee. He holds a Masters Degree in Computer Science and Information Technology from Cairo University and Masters Degree in Adult Teaching from UTS. His research interest is in Network Security. He is a CNAP ITE, CCNA, and CCNA Security Train the Trainer. He had been selected as Chief Judge for PC and Network Support at the national World skills competition in Brisbane 2010.