

# Informal Write-up on CCNA Security

October, 2009 (V1.0)

Methodology: This document uses the Cisco Press [CCNA Security Official Exam Certification Guide](#) (otherwise referred to as the Security ECG in this document) as a means to determine more specifically what topics are included in the Cisco IINS 640-553 exam, used to attain the [CCNA Security Certification](#). This document summarizes the topics in each chapter of the Security ECG by Chapter, typically mentioning the major headings (usually 2 or 3), with a brief mention of the largest topics in each section. It also lists a page count for the length of the "Foundation Topics" section of each chapter, which is the part of each chapter besides all the exam prep tools (like pre-quiz, reference tables, and the like.) The end of this document includes a table with the notable major conceptual topics, plus some analysis of hands-on topics, in particular whether CLI configuration, SDM configuration, and troubleshooting appear in the book.

## Chapter 1: Understanding Network Security Principles (32 pp)

Two major sections. The first section is a broad look at security fundamentals. The second section focuses on network attacks: discusses hackers, defense in depth, categories of attacks, and the specifics of many common types of attacks. (Opinion: this is a good place to figure out if you like security topics.)

## Chapter 2: Developing a Secure Network (25 pp)

Three major headings. The topics in this chapter focus on ideas, conventions, methods, rules, and anything that can help you better implement network security. Three main topics: Operations security – a variety of skills conventions, and tasks related. The 2<sup>nd</sup> section focuses on developing a written security policy. The final (short) section discusses the Cisco approach to security call the Cisco Self-defending Network.

## Chapter 3: Defending the Perimeter (25 pp)

Two sections. The chapter title mentions the perimeter, and then focuses on routers, which often sit on the perimeter. The first section looks at two main topics: CLI configuration for router login security (20+ commands), and the ISR model series of Cisco routers. The second section introduces the Cisco Security Device Manager (SDM), a GUI interface to configuring/monitoring Cisco routers, as an end to itself. (Later chapters show SDM used to configure security features.)

## Chapter 4: Configuring AAA (34 pp)

Two sections. The chapter zeroes in on AAA configuration on routers, in two flavors. The first section looks at using a local username database (ie, the username/password pairs are configured in the CLI). The second examines the same configuration but with the username database located on a TACACS+ or RADIUS server, with discussion of related protocols. It does include some notes on Cisco ACS software installation, but does not discuss ACS configuration.

## Chapter 5: Securing the Router (43)

Two sections. This chapter looks beyond the protection of passwords and users of the router. The first of two major sections – a rather short section - looks at a laundry list of small items that can/should be adjusted to secure a router- but it shows the configuration only using two automatic methods:

AutoSecure (an IOS feature) and SDM one-step lockdown. These include a look at CDP, ICMP unreachable, proxy ARP, to name a few. The second major part looks at securing syslog, SSH, and SNMP, and NTP, all with SDM, and some CLI config for SSH.

#### Chapter 6: Securing Layer 2 (35 pp)

Two major sections. The first examines layer 2 attacks, plus a long list of normal switch features that might need to be disabled (eg, trunking, CDP, shutting down ports, STP features) to make a switch more secure. It also includes newer tools like dynamic ARP inspection and DHCP snooping, and the old standby port security included in the base CCNA. The second major section examines Cisco Identity-based Networking Services (IBNS), discussing this system as an end to itself, as well as 802.1X concepts, and 802.1X configuration on switches (in conjunction with port security).

#### Chapter 7: Implementing Endpoint Security (22)

Again, two major sections. The first endpoint security in general, the second focusing on Cisco's solutions for endpoint security. The first section of this chapter, like the first few chapters of this book, introduces a whole new lexicon of terminology, this time focused on host security. It examines some of the exploits that have made the evening news over the years, general categories of attacks and exploits, and sets up the problems faced. The second part looks at Cisco's Ironport, NAC appliance, and Cisco Security Agent. Notably, there is no configuration or installation in the chapter.

#### Chapter 8: Providing SAN Security (13)

Whatta ya know – two major sections. The first is a SAN overview, the second on SAN zoning. Frankly, I wonder if this is outside the scope of the exam. "SAN" does not exist in the exam topics, and I don't see any exam topics that could imply SAN to my way of thinking, but it us a short read. No configuration.

#### Chapter 9: Exploring Secure Voice Solutions (16)

Like the SAN chapter, I wonder if this one is misplaced. There's no voice topics listed in the official CCNA Security exam topics. Hmmm.... Anyway, three main sections, again concept only, no configuration. Voice fundamentals, voice vulnerabilities, and how to secure VoIP.

#### Chapter 10: Using Cisco IOS Firewalls to Defend the Network (57)

Three sections. One of the most notable omissions from this book and the exam is the lack of coverage of the Cisco firewall, aka the Cisco ASA appliance. This chapter looks at firewalls in concept, and in practice as implemented in a router, but not with ASA. The first section looks at firewalls generally, with a solid overview of stateless and stateful firewalls, application layer firewalls, the Cisco ASA appliance as firewall, and some design issues related to firewalls. The second section examines IOS ACLs to filter packets, with a fair amount of review from CCNA ACL coverage. It includes new uses for ACLs, including route filtering (a BSCI topic), and turbo ACLs, so it does extend ACL discussion beyond CCNA. The final section looks at the IOS zone-based firewall feature, with basic configuration, but not a lot of example firewall rules.

#### Chapter 11: Using Cisco IOS IPS to Secure the Network (37)

Two sections. The first explains and classifies types of intrusion detection and intrusion prevention systems (IDS, IPS), including host and network based functions, and Cisco hardware/software. Again, more new security terminology is introduced including discussion of IDS/IPS signatures. (Aside – they could make the entire test be on the definitions of the terminology and make it a tough test.) The second section is a long run of screen shots from SDM for configuring the IOS-based IPS feature on a Cisco router.

#### Chapter 12: Defining a Cryptographic Solution (27)

Three sections, all conceptual. (Lots of small identifiable topics – the table of contents for this chapter is a page long, but the foundation topics section is only 27 pages in comparison.) The first looks at cryptographic services, how encryption/decryption works, the role of various types of keys. Keywords: cryptography, ciphers, encryption algorithms. The second looks at symmetric encryption, which includes discussion of AES, Des, 3DES, shared keys. The last section looks at various security algorithms and processes, like key exchange and hashes, and it takes a short look at how to use encryption in an SSL VPN. Concept only, no configuration.

#### Chapter 13: Implementing Digital Signatures (22)

Two sections this time. The first section, again focused on concepts, looks at hashes, in particular MD5 and SHA-1. The second section looks at digital signatures, how they can be used for authentication and integrity, and some details of RSA signatures. Concept only, no configuration. Note the short overall length.

#### Chapter 14: Exploring PKI and Asymmetric Encryption (25)

Two sections. The first looks at asymmetric encryption, using public/private key pairs, including details of Diffie-Helman key exchange and the RSA algorithm. The second section examines public key infrastructure (PKI), including how certification authorities (CA) work. Again, concept only.

#### Chapter 15: Building a Site-to-Site IPsec VPN Solution (44)

Three sections. The first breaks down IPsec and the Cisco VPN products. The second section looks at how to configure IPsec VPNs on routers using the CLI, with the final section doing the same using SDM.

## Concept/Theory topics

Note on CCNA Extension heading: This column notes the amount (small, medium, large) of overlap with the base CCNA, which is a pre-requisite for this exam.

Topic	Cert Guide Chapter	Theory	CCNA extension?
Security – why's, wherefores, legal, ethical issues	1	Y	
Types of Attacks	1	Y	
Specific common attacks	1	Y	
Operational Security	2	Y	
Security policy	2	Y	
Cisco Self-defending Network	2	Y	
ISR family	3	Y	
Host security terms/concepts	7	Y	
Ironport	7	Y	
Cisco Security Agent	7	Y	
Cisco NAC appliance	7	Y	
SAN Concepts	8	Y	
Securing SANs	8	Y	
Voice concepts	9	Y	
Voice vulnerabilities	9	Y	
VoIP – securing it	9	Y	
Firewall concepts	10	y	
IPS concepts	11	Y	
IDS/IPS appliances	11	Y	
Cryptographic services (eg encryption)	12	y	
Symmetric encryption (eg, 3DES)	12	Y	
Security algorithms (eg, key management)	12	Y	
Hashes (eg, MD5, SHA-1)	13	Y	
Digital Signatures (eg, RSA)	13	Y	
asymmetric encryption	14	Y	
PKI, certificate authorities	14	Y	
IPSec concepts	15	Y	

## Configuration Topics

Note on T'shoot heading – If the section of the book specifically examines incomplete configs, or problem areas, or spends space on the interpretation of several show commands, I interpreted that to mean that the topic may require troubleshooting. However, if the coverage only lists a few example show commands, with no broken configs or other problems, I assumed that troubleshooting isn't required.

Note on CCNA Extension heading: This column notes the amount (small, medium, large) of overlap with the base CCNA, which is a pre-requisite for this exam.

Topic	Cert Guide Chapter	Config – CLI	Config – SDM	T'shoot	CCNA extension?
Configuring routers to support SDM	3	Y			
Router CLI login security	3	Y	Y		small
AAA configuration – local database	4	Y		Y	small
AAA configuration – ACS server	4	Y			small
ACS Server features and installation	4	Y			
TACACS+ and Radius	4	Y	Y		
Locking down routers – SDM	5		y		
SNMPv3	5		y		
syslog	5		y		
NTP	5		y		
Locking down routers – autosecure	5	y			
SSH	5	y	y	y	small
Port Security	6	y			medium
Disabling features (eg, trunking, CDP)	6	y			small
ARP inspection, DHCP snooping	6	Y			
802.1X (on switches)	6	Y			
Router ACLs	10	y			large
Basic zone-based firewall config	10	y			
IOS IPS config	11		y		
IPSec SDM config	15		y		
IPSec CLI config	15	y			

## Feature Sets Examined:

- 1) IP/FW/IDS/ Plus IPSEC 3DES (latest versions: 12.4/12.3T)
- 2) Advanced IP Services (12.4T – most current available that we checked)
- 3) Advanced Security (12.4T – most current available that we checked)

## Feature Survey:

Based 12.4 (FS #1) and 12.4T (FS 2 and 3)

SDM was added 12.3T/12.4 or so

Need to get platform that supports 12.4 mainline for FS 1 in order to also get SDM support.

## IINS Configuration Topics that Require Routers

Topic	Config – CLI	Config – SDM	FS 1	FS 2	FS 3
Configuring routers to support SDM	Y		Y	y	y
Router CLI login security	Y	Y	y	y	y
AAA configuration – local database	Y		y	y	y
AAA configuration – ACS server	Y		y	y	y
TACACS+ and Radius	Y	Y	y	y	y
Locking down routers – SDM		y	Y	?	?
SNMPv3		y	Y	y	y
syslog		y	N	y	y
NTP		y	Y	y	y
Locking down routers – autosecure	y		y	y	y
SSH	y	y	y	y	y
Router ACLs	y		y	y	y
Basic zone-based firewall config (ZBFW)	y		N	y	y
IOS IPS config		y	N	y	y
IPSec SDM config		y	Y	y	y
IPSec CLI config	y		y	y	y

## IINS Configuration Topics that Require Switches

Comparing 2950, Standard vs Enhanced images, per

[http://www.cisco.com/en/US/products/hw/switches/ps628/prod\\_bulletin09186a00800b3089.html](http://www.cisco.com/en/US/products/hw/switches/ps628/prod_bulletin09186a00800b3089.html)

Topic	Config – CLI	Standard	Enhanced
Port Security	y	y	y
Disabling features (eg, trunking, CDP)	y	y	y
Dynamic ARP Inspection	y	N	N
DHCP Snooping	Y	Y	Y
802.1X (on switches)	Y	y	y

Looks like 2960 (LAN Base) and 3550 (EMI, others) support DAI

### ***Links/notes:***

Confirm with Feature Navigator: [www.cisco.com/go/fn](http://www.cisco.com/go/fn)