CCNA Security - Chapter 1 Modern Network Security Threats

Page	NICE	NGSS	ITEA	DODEA	Exam Objective
Section 1.0 Introduction					
1.0.1 Welcome					
1.0.1.1 Modern Network Security Threats	K0070	HS-ETS1-1.	ITEA.1. ITEA.6.	IT-NET 2.2	
Section 1.1 Securing Networks					
1.1.1 Current State of Affairs					
1.1.1.1 Networks Are Targets	T0561	HS-ETS1-1.	ITEA.1. ITEA.6.	IT-NET 2.2	
1.1.1.2 Reasons for Network Security	T0161	HS-ETS1-1.	ITEA.1. ITEA.6.	IT-NET 2.2	
1.1.1.3 Vectors of Network Attacks	K0106	HS-ETS1-1.	ITEA.1. ITEA.6.	IT-NET 2.2	1.2.d Classify the vectors of data loss/exfiltration
1.1.1.4 Data Loss	K0202	HS-ETS1-1.	ITEA.1. ITEA.6.	IT-NET 2.2	1.2.d Classify the vectors of data loss/exfiltration
1.1.2 Network Topology Overview					
1.1.2.1 Campus Area Networks	K0029	HS-ETS1-1.	ITEA.1. ITEA.6.	IT-NET 2.2	1.4.a Campus area network (CAN)
1.1.2.2 Small Office and Home Office Networks	T0945	HS-ETS1-1.	ITEA.1. ITEA.6.	IT-NET 2.2	1.4.d Small office/home office (SOHO)
1.1.2.3 Wide Area Networks	K0029	HS-ETS1-1.	ITEA.1. ITEA.6.	IT-NET 2.2	1.4.b Cloud, wide area network (WAN)
1.1.2.4 Data Center Networks	T0251	HS-ETS1-1.	ITEA.1. ITEA.6.	IT-NET 2.2	1.4.c Data center
1.1.2.5 Cloud and Virtual Networks	T0251	HS-ETS1-1.	ITEA.1. ITEA.6.	IT-NET 2.2	1.4.b Cloud, wide area network (WAN) 1.4.e Network security for a virtual environment
1.1.2.6 The Evolving Network Border	T0413	HS-ETS1-1.	ITEA.1. ITEA.6.	IT-NET 2.2	2.4.a Describe the BYOD architecture framework 2.4.b Describe the function of mobile device management (MDM)
1.1.2.7 Activity - Topology Overview		HS-ETS1-1.	ITEA.1. ITEA.6.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 2.2	
Section 1.2 Network Threats					1.1.c Identify common security terms 1.2.a Identify common network attacks
1.2.1 Who Is Attacking Our Network?					
1.2.1.1 The Hacker	K0119	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	
1.2.1.2 Evolution of Hackers	K0206	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	
1.2.1.3 Cyber Criminals	K0310	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	

1.2.1.4 Hacktivists	K0119	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	
1.2.1.5 State-Sponsored Hackers	K0310	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.c Identify malware
1.2.2 Hacker Tools	K0119				
1.2.2.1 Introduction of Attack Tools	T0013	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	
1.2.2.2 Evolution of Security Tools	T0020	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	
1.2.2.3 Categories of Attack Tools	T0013	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	
1.2.3 Malware					1.2.c Identify malware
1.2.3.1 Various Types of Malware	T0278	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.c Identify malware
1.2.3.2 Viruses	K0191	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.c Identify malware
1.2.3.3 Trojan Horses	T0278	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.c Identify malware
1.2.3.4 Trojan Horse Classification	K0392	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.c Identify malware
1.2.3.5 Worms	K0119	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.c Identify malware
1.2.3.6 Worm Components	K0119	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.c Identify malware
1.2.3.7 Other Malware	K0119	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.b Describe social engineering 1.2.c Identify malware
1.2.3.8 Activity - Identify the Malware Type		HS-ETS1-1.	ITEA.2. ITEA.4.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 2.2	1.2.b Describe social engineering 1.2.c Identify malware
1.2.4 Common Network Attacks					
1.2.4.1 Types of Network Attacks	K0106	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.b Describe social engineering 1.2.c Identify malware
1.2.4.2 Reconnaissance Attacks	K0177	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.2.4.3 Sample Reconnaissance Attack	K0177	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks 1.2.b Describe social engineering
1.2.4.4 Access Attacks	K0177	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.2.4.5 Types of Access Attacks	K0119	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks 1.2.b Describe social engineering 4.4.c Describe MAC spoofing
1.2.4.6 Social Engineering Attacks	S0052	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks 1.2.b Describe social engineering 1.2.c Identify malware

1.2.4.7 Denial of Service Attacks	K0362	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.2.4.8 Types of DoS Attacks	K0362	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.2.4.9 DDoS Attacks	K0362	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.2.4.10 Video - DDoS Attacks (Cont.)		HS-ETS1-1.	ITEA.2. ITEA.4.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 2.2	1.2.a Identify common network attacks
1.2.4.11 Activity - Identify the Types of Network Attacks		HS-ETS1-1.	ITEA.2. ITEA.4.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 2.2	1.2.a Identify common network attacks
1.2.4.12 Lab: Social Engineering		HS-ETS1-1.	ITEA.2. ITEA.4.	CCR.ELA-Literacy.RST.11-12.3. IT-NET 2.2	1.2.a Identify common network attacks 1.2.b Describe social engineering
Section 1.3 Mitigating Threats					
1.3.1 Defending the Network					
1.3.1.1 Network Security Professionals	K0001	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.1.a Describe confidentiality, integrity, availability (CIA)
1.3.1.2 Network Security Organizations	K0001	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.1.a Describe confidentiality, integrity, availability (CIA)
1.3.1.3 Confidentiality, Integrity, Availability	T0017	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.1.a Describe confidentiality, integrity, availability (CIA)
1.3.2 Domains of Network Security					1.2.a Identify common network attacks
1.3.2.1 Network Security Domains	K0124	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.3.2.2 Security Policy	T0015	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.3.2.3 Network Security Policy	T0871	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.3.2.4 Network Security Policy Objectives	T0871	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.3.3 Introducing the Cisco SecureX Artichoke					1.2.a Identify common network attacks
1.3.3.1 The Security Artichoke		HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.3.3.2 Evolution of Network Security Tools	K0487	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.3.3.3 SecureX Products		HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.3.3.4 SecureX Security Technology		HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.3.3.5 Centralized Context-Aware Network Scanning Element		HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks

1.3.3.6 Cisco Security Intelligence Operations		HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.3.4 Mitigating Common Network Attacks					1.2.a Identify common network attacks
1.3.4.1 Defending the Network	T0161	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks 1.2.b Describe social engineering
1.3.4.2 Mitigating Malware	T0278	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks 1.2.c Identify malware
1.3.4.3 Mitigating Worms	K0119	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.3.4.4 Mitigating Reconnaissance Attacks	K0177	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.3.4.5 Mitigating Access Attacks	K0362	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks 1.2.b Describe social engineering
1.3.4.6 Mitigating DoS Attacks	K0362	HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks
1.3.5 Cisco Network Foundation Protection Framework					1.2.a Identify common network attacks
1.3.5.1 NFP Framework		HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks 4.3.a Explain the function of control plane policing
1.3.5.2 Securing the Control Plane		HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks 4.3.a Explain the function of control plane policing
1.3.5.3 Securing the Management Plane		HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks 4.1.b Configure Cisco IOS role-based CLI access 4.3.a Explain the function of control plane policing
1.3.5.4 Securing the Data Plane		HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	1.2.a Identify common network attacks 4.3.a Explain the function of control plane policing 4.4.b Describe ARP spoofing 4.4.c Describe MAC spoofing
1.3.5.5 Activity - Identify Characteristics of the NFP Framework		HS-ETS1-1.	ITEA.2. ITEA.4.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 2.2	1.2.a Identify common network attacks
Section 1.4 Chapter Summary					
1.4.1 Summary					
1.4.1.1 Lab: Researching Network Attacks and Security Audit Tools		HS-ETS1-1.	ITEA.2. ITEA.4.	CCR.ELA-Literacy.RST.11-12.3. IT-NET 2.2	1.2.a Identify common network attacks
1.4.1.2 Modern Network Security Threats		HS-ETS1-1.	ITEA.2. ITEA.4.	IT-NET 2.2	

CCNA Security - Chapter 2, Securing Network Devices

Page	NICE	NGSS	ITEA	DODEA	Exam Objective
Section 2.0 Introduction					
2.0.1 Welcome					
2.0.1.1 Securing Network Devices	T0125	HS-ETS1-2.		IT-NET 2.2	4.2.a Implement routing update authentication on OSPF 4.3.a Explain the function of control plane policing
Section 2.1 Securing Device Access					
2.1.1 Securing the Edge Router					
2.1.1.1 Securing the Network Infrastructure	T0125	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	
2.1.1.2 Edge Router Security Approaches	T0035	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	
2.1.1.3 Three Areas of Router Security	T0035	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	
2.1.1.4 Secure Administrative Access	T0791	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	1.1.a Describe confidentiality, integrity, availability (CIA)
2.1.1.5 Secure Local and Remote Access	T0791	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	2.1.c Configure and verify secure access through SNMP v3 using an ACL
2.1.2 Configuring Secure Administrative Access					
2.1.2.1 Strong Passwords	S0067	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	
2.1.2.2 Increasing Access Security	T0037	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	
2.1.2.3 Secret Password Algorithms	S0067	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	
2.1.2.4 Securing Line Access	S0067	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	
2.1.3 Configuring Enhanced Security for Virtual Logins					
2.1.3.1 Enhancing the Login Process	T0146	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	
2.1.3.2 Configuring Login Enhancement Features	T0146	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	
2.1.3.3 Enable Login Enhancements	T0146	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	
2.1.3.4 Syntax Checker - Logging Failed Attempts		HS-ETS1-4.	ITEA.11.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 2.2	
2.1.4 Configuring SSH					
2.1.4.1 Steps for Configuring SSH	T0439	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	
2.1.4.2 Syntax Checker - Modifying the SSH Configuration		HS-ETS1-4.	ITEA.11.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 2.2	
2.1.4.3 Connecting to an SSH-Enabled Router	T0439	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	
Section 2.2 Assigning Administrative Roles					
2.2.1 Configuring Privilege Levels					
2.2.1.1 Limiting Command Availability	T0130	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	4.1.a Configure multiple privilege levels 4.1.b Configure Cisco IOS role-based CLI access
2.2.1.2 Configuring and Assigning Privilege Levels		HS-ETS1-2.	ITEA.11.	IT-NET 2.2	4.1.a Configure multiple privilege levels

2.2.1.3 Syntax Checker - Limitations of Privilege Levels		HS-ETS1-4.	ITEA.11.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 2.2	4.1.a Configure multiple privilege levels
2.2.2 Configuring Role-Based CLI					4.1.b Configure Cisco IOS role-based CLI access
2.2.2.1 Role-Based CLI Access	T0362	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	4.1.b Configure Cisco IOS role-based CLI access
2.2.2.2 Role-Based Views	T0362	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	4.1.a Configure multiple privilege levels 4.1.b Configure Cisco IOS role-based CLI access
2.2.2.3 Syntax Checker - Configuring Role-Based Views		HS-ETS1-4.	ITEA.11.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 2.2	4.1.b Configure Cisco IOS role-based CLI access
2.2.2.4 Syntax Checker - Configuring Role-Based CLI Superviews		HS-ETS1-4.	ITEA.11.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 2.2	4.1.b Configure Cisco IOS role-based CLI access
2.2.2.5 Verify Role-Based CLI Views	T0929	HS-ETS1-2.	ITEA.11.	IT-NET 2.2	
Section 2.3 Monitoring and Managing Devices					
2.3.1 Securing Cisco IOS Image and Configuration					
2.3.1.1 Cisco IOS Resilient Configuration Feature	T0035	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	4.1.c Implement Cisco IOS resilient configuration
2.3.1.2 Enabling the IOS Image Resilience Feature	T0035	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	4.1.c Implement Cisco IOS resilient configuration
2.3.1.3 The Primary Bootset Image	T0035	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	
2.3.1.4 Configuring Secure Copy	T0014	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	2.1.e Use SCP for file transfer 4.1.a Configure multiple privilege levels 4.1.c Implement Cisco IOS resilient configuration
2.3.1.5 Recovering a Router Password	T0035	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	
2.3.1.6 Password Recovery	T0146	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	
2.3.2 Secure Management and Reporting					
2.3.2.1 Determining the Type of Management Access	T0084	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	
2.3.2.2 Out-of-Band and In-Band Access	T0084	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	
2.3.3 Using Syslog for Network Security					
2.3.3.1 Introduction to Syslog	T0146	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	
2.3.3.2 Syslog Operation	T0146	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	
2.3.3.3 Syslog Message	T0146	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	
2.3.3.4 Activity - Interpret Syslog Output		HS-ETS1-2.	ITEA.12. ITEA.17.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 2.2	

2.3.3.5 Syslog Systems	T0146	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	
2.3.3.6 Configuring System Logging	T0146	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	
2.3.4 Using SNMP for Network Security					
2.3.4.1 Introduction to SNMP	T0330	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	2.1.c Configure and verify secure access through SNMP v3 using an ACL
2.3.4.2 Management Information Base (MIB)	T0330	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	2.1.c Configure and verify secure access through SNMP v3 using an ACL
2.3.4.3 SNMP Versions	S0056	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	2.1.c Configure and verify secure access through SNMP v3 using an ACL
2.3.4.4 SNMP Vulnerabilities	S0056	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	2.1.c Configure and verify secure access through SNMP v3 using an ACL
2.3.4.5 SNMPv3	S0056	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	2.1.c Configure and verify secure access through SNMP v3 using an ACL
2.3.4.6 Configuring SNMPv3 Security	S0056	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	2.1.c Configure and verify secure access through SNMP v3 using an ACL
2.3.4.7 Syntax Checker - Secure SNMPv3 Configuration Example		HS-ETS1-4.	ITEA.12. ITEA.17.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 2.2	2.1.c Configure and verify secure access through SNMP v3 using an ACL
2.3.4.8 Verifying the SNMPv3 Configuration	S0056	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	2.1.c Configure and verify secure access through SNMP v3 using an ACL
2.3.5 Using NTP					
2.3.5.1 Network Time Protocol		HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	2.1.d Configure and verify security for NTP
2.3.5.2 NTP Server		HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	2.1.d Configure and verify security for NTP
2.3.5.3 Syntax Checker - NTP Authentication		HS-ETS1-4.	ITEA.12. ITEA.17.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 2.2	2.1.d Configure and verify security for NTP
Section 2.4 Using Automated Security Features					
2.4.1 Performing a Security Audit					
2.4.1.1 Discovery Protocols CDP and LLDP	S0035	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	
2.4.1.2 Settings for Protocols and Services	T0365	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	2.1.c Configure and verify secure access through SNMP v3 using an ACL
2.4.2 Locking Down a Router Using AutoSecure		HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	
2.4.2.1 Cisco AutoSecure	T0100	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	2.1.d Configure and verify security for NTP
2.4.2.2 Using the Cisco AutoSecure Feature	T0100	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	
2.4.2.3 Syntax Checker - Using the auto secure Command		HS-ETS1-4.	ITEA.12. ITEA.17.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 2.2	

Section 2.5 Securing the Control Plane					
2.5.1 Routing Protocol Authentication		HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	4.3.a Explain the function of control plane policing
2.5.1.1 Routing Protocol Spoofing	T0365	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	4.2.a Implement routing update authentication on OSPF 4.3.a Explain the function of control plane policing
2.5.1.2 OSPF MD5 Routing Protocol Authentication	T0365	HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	4.2.a Implement routing update authentication on OSPF 4.3.a Explain the function of control plane policing
2.5.1.3 Syntax Checker - OSPF SHA Routing Protocol Authentication		HS-ETS1-4.	ITEA.12. ITEA.17.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 2.2	4.2.a Implement routing update authentication on OSPF 4.3.a Explain the function of control plane policing
2.5.2 Control Plane Policing					
2.5.2.1 Network Device Operations		HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	4.3.a Explain the function of control plane policing
2.5.2.2 Control and Management Plane Vulnerabilities		HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	4.3.a Explain the function of control plane policing
2.5.2.3 CoPP Operation		HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	4.3.a Explain the function of control plane policing
2.5.2.4 Activity - Identify the Features of CoPP		HS-ETS1-2.	ITEA.12. ITEA.17.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 2.2	4.3.a Explain the function of control plane policing
2.5.2.5 Activity - Identify the Network Device Security Feature		HS-ETS1-2.	ITEA.12. ITEA.17.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 2.2	4.3.a Explain the function of control plane policing
Section 2.6 Summary					
2.6.1 Conclusion					
2.6.1.1 Video - Securing the Router		HS-ETS1-2.	ITEA.12. ITEA.17.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 2.2	2.1.d Configure and verify security for NTP 4.2.a Implement routing update authentication on OSPF
2.6.1.2 Lab - Securing the Router for Administrative Access		HS-ETS1-2.	ITEA.12. ITEA.17.	CCR.ELA-Literacy.RST.11-12.3. IT-NET 2.2	2.1.d Configure and verify security for NTP
2.6.1.3 Packet Tracer - Configure Cisco Routers for Syslog, NTP, and SSH Operations		HS-ETS1-4.	ITEA.12. ITEA.17.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 2.2	2.1.d Configure and verify security for NTP 4.1.b Configure Cisco IOS role-based CLI access
2.6.1.4 Securing Network Devices		HS-ETS1-2.	ITEA.12. ITEA.17.	IT-NET 2.2	2.1.d Configure and verify security for NTP 4.1.b Configure Cisco IOS role-based CLI access

CCNA Security - Chapter 3, Authentication, Authorization and Accounting

Page	NICE	NGSS	ITEA	DODEA	Exam Objective
Section 3.0 Introduction					
3.0.1 Welcome					
3.0.1.1 Authentication, Authorization and Accounting	K0007	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.2.e Describe authentication and authorization using ACS and ISE 3.2.e Identify endpoint posture assessment
Section 3.1 Purpose of AAA					
3.1.1 AAA Overview					
3.1.1.1 Authentication without AAA	K0007	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.2.b Configure administrative access on a Cisco router using TACACS+
3.1.1.2 AAA Components	K0007	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.2.b Configure administrative access on a Cisco router using TACACS+
3.2.1 AAA Characteristics					
3.1.2.1 Authentication Modes	K0007	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.2.a Describe RADIUS and TACACS+ technologies 2.2.b Configure administrative access on a Cisco router using TACACS+ 2.2.e Describe authentication and authorization using ACS and ISE
3.1.2.2 Authorization	K0007	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
3.1.2.3 Accounting	K0007	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.2.e Describe authentication and authorization using ACS and ISE
3.1.2.4 Activity - Identify the Characteristics of AAA		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
Section 3.2 Local AAA Authentication					
3.2.1 Configuring Local AAA Authentication with CLI					
3.2.1.1 Authenticating Administrative Access	K0007	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
3.2.1.2 Authentication Methods	K0007	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.2.b Configure administrative access on a Cisco router using TACACS+
3.2.1.3 Default and Named Methods	K0007	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
3.2.1.4 Fine-Tuning the Authentication Configuration	K0007	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.2.b Configure administrative access on a Cisco router using TACACS+
3.2.2 Troubleshooting Local AAA Authentication					
3.2.2.1 Debug Options	K0079	HS-ETS1-3.	ITEA.9.	IT-NET 3.8	2.2.b Configure administrative access on a Cisco router using TACACS+ 4.3.a Explain the function of control plane policing
3.2.2.2 Syntax Checker - Debugging AAA Authentication		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
Section 3.3 Server-Based AAA					
3.3.1 Server-Based AAA Characteristics					
3.3.1.1 Comparing Local AAA and Server-Based AAA Implementations	K0007	HS-ETS1-3.	ITEA.9.	IT-NET 3.8	2.2.b Configure administrative access on a Cisco router using TACACS+ 2.2.d Explain the integration of Active Directory with AAA 2.2.e Describe authentication and authorization using ACS and ISE

3.3.1.2 Introducing Cisco Secure Access Control System		HS-ETS1-3.	ITEA.9.	IT-NET 3.8	2.2.a Describe RADIUS and TACACS+ technologies 2.2.b Configure administrative access on a Cisco router using TACACS+ 2.2.e Describe authentication and authorization using ACS and ISE
3.3.2 Server-Based AAA Communications Protocols					
3.3.2.1 Introducing TACACS+ and RADIUS	K0452	HS-ETS1-3.	ITEA.9.	IT-NET 3.8	2.2.a Describe RADIUS and TACACS+ technologies 2.3.a Identify the functions 802.1X components
3.3.2.2 TACACS+ Authentication	K0452	HS-ETS1-3.	ITEA.9.	IT-NET 3.8	2.2.a Describe RADIUS and TACACS+ technologies
3.3.2.3 RADIUS Authentication	K0452	HS-ETS1-3.	ITEA.9.	IT-NET 3.8	2.2.a Describe RADIUS and TACACS+ technologies
3.3.2.4 Integration of TACACS+ and ACS	K0452	HS-ETS1-3.	ITEA.9.	IT-NET 3.8	2.2.a Describe RADIUS and TACACS+ technologies 2.2.b Configure administrative access on a Cisco router using TACACS+ 2.2.d Explain the integration of Active Directory with AAA 2.2.e Describe authentication and authorization using ACS and ISE
3.3.2.5 Integration of AAA with Active Directory	K0007	HS-ETS1-3.	ITEA.9.	IT-NET 3.8	2.2.a Describe RADIUS and TACACS+ technologies 2.2.b Configure administrative access on a Cisco router using TACACS+ 2.2.d Explain the integration of Active Directory with AAA 2.2.e Describe authentication and authorization using ACS and ISE
3.3.2.6 Video - Integration of AAA with Identity Service Engine		HS-ETS1-3.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 3.8	2.2.e Describe authentication and authorization using ACS and ISE 2.2.b Configure administrative access on a Cisco router using TACACS+ 2.4.a Describe the BYOD architecture framework
3.3.2.7 Activity - Identify the AAA Communication Protocol		HS-ETS1-3.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
Section 3.4 Server-Based AAA Authentication					
3.4.1 Configuring Server-Based Authentication					
3.4.1.1 Steps for Configuring Server-Based AAA Authentication	K0007	HS-ETS1-3.	ITEA.9.	IT-NET 3.8	2.2.a Describe RADIUS and TACACS+ technologies 2.2.b Configure administrative access on a Cisco router using TACACS+ 2.2.c Verify connectivity on a Cisco router to a TACACS+ server 2.2.e Describe authentication and authorization using ACS and ISE
3.4.1.2 Configuring TACACS+ Servers	K0452	HS-ETS1-3.	ITEA.9.	IT-NET 3.8	2.2.a Describe RADIUS and TACACS+ technologies 2.2.c Verify connectivity on a Cisco router to a TACACS+ server
3.4.1.3 Configuring RADIUS Servers	K0452	HS-ETS1-3.	ITEA.9.	IT-NET 3.8	2.2.a Describe RADIUS and TACACS+ technologies 2.2.b Configure administrative access on a Cisco router using TACACS+ 2.2.c Verify connectivity on a Cisco router to a TACACS+ server
HS-ETS1-4.		HS-ETS1-3.	ITEA.9.	IT-NET 3.8	2.2.a Describe RADIUS and TACACS+ technologies
3.4.2 Troubleshooting Server-Based AAA Authentication					
3.4.2.1 Monitoring Authentication Traffic		HS-ETS1-3.	ITEA.10.	IT-NET 3.8	2.2.a Describe RADIUS and TACACS+ technologies

3.4.2.2 Debugging TACACS+ and RADIUS	K0452	HS-ETS1-3.	ITEA.10.	IT-NET 3.8	2.2.a Describe RADIUS and TACACS+ technologies
3.4.2.3 Video - Configure a Cisco Router to Access a AAA RADIUS Server		HS-ETS1-3.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.7.	2.2.a Describe RADIUS and TACACS+ technologies 2.2.b Configure administrative access on a Cisco router using TACACS+
Section 3.5 Server-Based AAA Authorization and Accounting		HS-ETS1-3.	ITEA.10.		
3.5.1 Configuring Server-Based AAA Authorization					
3.5.1.1 Introduction to Server-Based AAA Authorization	K0007	HS-ETS1-3.	ITEA.10.	IT-NET 3.8	2.2.a Describe RADIUS and TACACS+ technologies 2.2.b Configure administrative access on a Cisco router using TACACS+ 2.2.e Describe authentication and authorization using ACS and ISE
3.5.1.2 AAA Authorization Configuration		HS-ETS1-3.	ITEA.10.	IT-NET 3.8	
3.5.2 Configuring Server-Based AAA Accounting					
3.5.2.1 Introduction to Server-Based AAA Accounting	K0007	HS-ETS1-3.	ITEA.10.	IT-NET 3.8	2.2.b Configure administrative access on a Cisco router using TACACS+ 2.2.e Describe authentication and authorization using ACS and ISE
3.5.2.2 Syntax Checker - AAA Accounting Configuration		HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	2.2.a Describe RADIUS and TACACS+ technologies
3.5.3 802.1X Authentication		HS-ETS1-3.	ITEA.10.		2.3.a Identify the functions 802.1X components
3.5.3.1 Security Using 802.1X Port-Based Authentication	K0491	HS-ETS1-3.	ITEA.10.	IT-NET 3.8	2.2.a Describe RADIUS and TACACS+ technologies 2.3.a Identify the functions 802.1X components
3.5.3.2 802.1X Port Authorization State	K0491	HS-ETS1-3.	ITEA.10.	IT-NET 3.8	2.3.a Identify the functions 802.1X components
HS-ETS1-4.		HS-ETS1-3.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	2.2.a Describe RADIUS and TACACS+ technologies 2.3.a Identify the functions 802.1X components
Section 3.6 Chapter Summary					
3.6.1 Conclusion					
3.6.1.1 Lab – Securing Administrative Access Using AAA and RADIUS		HS-ETS1-3.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.3.	2.2.a Describe RADIUS and TACACS+ technologies
3.6.1.2 Packet Tracer – Configure AAA Authentication on Cisco Routers		HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	2.2.a Describe RADIUS and TACACS+ technologies
3.6.1.3 Authentication, Authorization and Accounting	K0007	HS-ETS1-3.	ITEA.10.	IT-NET 3.8	2.2.e Describe authentication and authorization using ACS and ISE 2.2.b Configure administrative access on a Cisco router using TACACS+

CCNA Security - Chapter 4, Implementing Firewall Technologies

Page	NICE	NGSS	ITEA	DODEA	Exam Objective
Section 4.0 Introduction					
4.0.1 Welcome					
4.0.1.1 Implementing Firewall Technologies	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
Section 4.1 Access Control Lists					
4.1.1 Configuring Standard and extended IPv4 ACLs with CLI					
4.1.1.1 Introduction to Access Control Lists	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
4.1.1.2 Configuring Numbered and Named ACLs	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
4.1.1.3 Applying an ACL	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
4.1.1.4 ACL Configuration Guidelines	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
4.1.1.5 Editing Existing ACLs	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
4.1.1.6 Sequence Numbers and Standard ACLs	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
4.1.1.7 Activity - Configuring Standard ASLs		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
4.1.1.8 Activity - Creating an Extended ACL Statement		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
4.1.1.9 Activity - Evaluating Extended ACLs		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
4.1.1.10 Packet Tracer – Configuring Extended ACLs Scenario 1		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
4.1.1.11 Packet Tracer - Configuring Extended ACLs Scenario 2		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
4.1.2 Mitigating Attacks with ACLs					
4.1.2.1 Antispoofing with ACLs	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
4.1.2.2 Permitting Necessary Traffic through a Firewall	K0049	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.1.c Configure and verify secure access through SNMP v3 using an ACL
4.1.2.3 Mitigating ICMP Abuse	K0452	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.1.c Configure and verify secure access through SNMP v3 using an ACL
4.1.2.4 Mitigating SNMP Exploits	K0452	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.1.c Configure and verify secure access through SNMP v3 using an ACL
4.1.2.5 Packet Tracer - Configure IP ACLs to Mitigate Attacks		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	

4.1.3 IPv6 ACLs					
4.1.3.1 Introducing IPv6 ACLs	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
4.1.3.2 IPv6 ACL Syntax	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
4.1.3.3 IPv6 ACL Syntax	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
4.1.3.4 Packet Tracer – Configure IPv6 ACLs		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
Section 4.2 Firewall Technologies					
4.2.1 Securing Networks with Firewalls					
4.2.1.1 Defining Firewalls	K0487	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	5.1 Describe operational strengths and weaknesses of the different firewall technologies
4.2.1.2 Benefits and Limitations of Firewalls	K0487	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	5.1 Describe operational strengths and weaknesses of the different firewall technologies
4.2.2 Types of Firewalls					
4.2.2.1 Firewall Type Descriptions	K0487	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	5.1 Describe operational strengths and weaknesses of the different firewall technologies
4.2.2.2 Packet Filtering Firewall Benefits and Limitations	K0487	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	5.2 Compare stateful vs. stateless firewalls
4.2.2.3 Stateful Firewalls	K0487	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	5.2 Compare stateful vs. stateless firewalls
4.2.2.4 Stateful Firewall Benefits and Limitations	K0487	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	5.2 Compare stateful vs. stateless firewalls
4.2.2.5 Next Generation Firewalls	K0487	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	5.2 Compare stateful vs. stateless firewalls
4.2.2.6 Activity - Identify the Type of Firewall		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4.	
4.2.3 Classic Firewall					
4.2.3.1 Introducing Classic Firewall	K0487	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	5.1 Describe operational strengths and weaknesses of the different firewall technologies
4.2.3.2 Classic Firewall Operation	K0487	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	5.1 Describe operational strengths and weaknesses of the different firewall technologies
4.2.3.3 Classic Firewall Configuration	K0487	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	5.1 Describe operational strengths and weaknesses of the different firewall technologies
4.2.4 Firewalls in Network Design					
4.2.4.1 Inside and Outside Networks	T0071	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.d Identify common network security zones
4.2.4.2 Demilitarized Zones	K0049	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.d Identify common network security zones
4.2.4.3 ZPFs	K0049	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.d Identify common network security zones 4.3.a Explain the function of control plane policing
4.2.4.4 Layered Defense	T0262	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.d Identify common network security zones
Section 4.3 Zone-Based Policy Firewalls					1.1.d Identify common network security zones
4.3.1 ZPF Overview					1.1.d Identify common network security zones
4.3.1.1 Benefits of a ZPF	K0049	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.d Identify common network security zones
4.3.1.2 Benefits of a ZPF	K0049	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.d Identify common network security zones

4.3.1.3 Activity - Compare Classic Firewall and ZPF Operation		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	1.1.d Identify common network security zones
4.3.2 ZPF Operation					1.1.d Identify common network security zones
4.3.2.1 ZPF Actions	K0049	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.d Identify common network security zones
4.3.2.2 Rules for Transit Traffic	T0240	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.d Identify common network security zones
4.3.2.3 Rules for Traffic to the Self Zone	T0240	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.d Identify common network security zones
4.3.2.4 Activity - Rules for Transit Traffic		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	1.1.d Identify common network security zones
4.3.3 Configuring a ZPF					1.1.d Identify common network security zones
4.3.3.1 Configure ZPF	K0049	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.d Identify common network security zones
4.3.3.2 Create Zones	K0049	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.d Identify common network security zones
4.3.3.3 Identify Traffic	K0334	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.d Identify common network security zones
4.3.3.4 Define an Action	K0469	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.d Identify common network security zones
4.3.3.5 Identify a Zone-Pair and Match to a Policy	K0049	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.d Identify common network security zones
4.3.3.6 Assign Zones to Interfaces	K0049	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.d Identify common network security zones
4.3.3.7 Syntax Checker - Verify a ZPF Configuration		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	1.1.d Identify common network security zones
4.3.3.8 ZPF Configuration Considerations	K0049	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.d Identify common network security zones
4.3.3.9 Video – ZPFs		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 3.8	1.1.d Identify common network security zones
Section 4.4 Chapter Summary					1.1.d Identify common network security zones
4.4.1 Conclusion					1.1.d Identify common network security zones
HS-ETS1-4.		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	1.1.d Identify common network security zones
4.4.1.2 Lab - Configuring ZPFs		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3. IT-NET 3.8	1.1.d Identify common network security zones
4.4.1.3 Implementing Firewall Technologies	K0452	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	

CCNA Security - Chapter 5, Implementing Intrusion Prevention

Page	NICE	NGSS	ITEA	DODEA	Exam Objective
Section 5.0 Introduction					
5.0.1 Welcome					
5.0.1.1 Implementing Intrusion Prevention	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
Section 5.1 IPS Technologies					
5.1.1 IDS and IPS Characteristics					
5.1.1.1 Zero-Day Attacks	T0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.2a
5.1.1.2 Monitor for Attacks	T0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.2a
5.1.1.3 Detect and Stop Attacks	T0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.2a
5.1.1.4 Similarities Between IDS and IPS	T0161	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.1
5.1.1.5 Advantages and Disadvantages of IDS and IPS	T0161	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
5.1.1.6 Activity - Compare IDS and IPS Characteristics		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
5.1.2 Network-Based IPS Implementations					
5.1.2.1 Host-Based IPS	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.1a
5.1.2.2 Network-Based IPS Sensors	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2
5.1.2.3 Cisco's Modular and Appliance-Based IPS Solutions	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.0
5.1.2.4 Video - Cisco's Modular and Appliance-Based IPS Solutions (Cont.)		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 3.8	
5.1.2.5 Video - Choose an IPS Solution		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 3.8	
5.1.2.6 Network-Based IPS	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.1a
5.1.2.7 Modes of Deployment	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.1b
5.1.2.8 Activity - Compare Network and Host-Based IPS		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
5.1.3 Cisco Switched Port Analyzer					
5.1.3.1 Port Mirroring	K0491	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.1b
5.1.3.2 Cisco SPAN		HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.1b
5.1.3.3 Syntax Checker - Configuring Cisco SPAN using Intrusion Detection		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	

Section 5.2 IPS Signatures					
5.2.1 IPS Signature Characteristics					
5.2.1.1 Signature Attributes	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2a
5.2.1.2 Signature Types	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2a
5.2.1.3 Signature File	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2a
5.2.1.4 Signature Micro-Engines	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2a
5.2.1.5 Acquire the Signature File	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2a
5.2.1.6 Activity - Identify IPS Signature Type		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
5.2.2 IPS Signature Alarms					
5.2.2.1 Signature Alarm	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2a
5.2.2.2 Pattern-Based Detection	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2a
5.2.2.3 Anomaly-Based Detection	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2a
5.2.2.4 Policy-Based and Honey Pot-Based Detection	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2a
5.2.2.5 Benefits of the Cisco IOS IPS Solution		HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
5.2.2.6 Alarm Triggering Mechanisms		HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2c
5.2.2.7 Activity - IPS Signature Alarms		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
5.2.3 IPS Signature Actions					6.2a
5.2.3.1 Signature Actions	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2a
5.2.3.2 Manage Generated Alerts	T0043	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2c
5.2.3.3 Log Activities for Later Analysis	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2c
5.2.3.4 Deny the Activity	T0023	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2d
5.2.3.5 Reset, Block, and Allow Traffic	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	7.2b
5.2.3.6 Activity - Identify the IPS Signature Action		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
5.2.4 Manage and Monitor IPS					6.2c
5.2.4.1 Monitor Activity	T0023	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2c
5.2.4.2 Monitoring Considerations	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2c
5.2.4.3 Secure Device Event Exchange	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2c
5.2.4.4 IPS Configuration Best Practices	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2c
5.2.5 IPS Global Correlation					
5.2.5.1 Cisco Global Correlation	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.1c
5.2.5.2 Cisco SensorBase Network	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.1c
5.2.5.3 Cisco Security Intelligence Operation	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.2.c Identify malware
5.2.5.4 Reputations, Blacklists, and Traffic Filters	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2d
5.2.5.5 Video - Reputations, Blacklists, and Traffic Filters (Cont.)		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 3.8	
Section 5.3 Implement IPS					
5.3.1 Configure Cisco IOS IPS with CLI					
5.3.1.1 Implement IOS IPS	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.1c
5.3.1.2 Download the IOS IPS Files	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.1b
5.3.1.3 IPS Crypto Key	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.30
5.3.1.4 Enable IOS IPS	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.00

HS-ETS1-4.		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
5.3.1.6 Activity - Implementing IPS		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
5.3.2 Modifying Cisco IOS IPS Signatures					
5.3.2.1 Retire and Unretire Signatures		HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.2a
HS-ETS1-4.		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
5.3.3 Verify and Monitor IPS		HS-ETS1-2.	ITEA.9.		
5.3.1.1 Verify IOS IPS	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	6.1b
5.3.1.2 Report IPS Alerts	K0324	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1b
5.3.1.3 Enable SDEE		HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
Section 5.4 Summary					
5.4.1 Conclusion					
5.4.1.1 Lab - Configure an IOS IPS Using CLI		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3. IT-NET 3.8	
5.4.1.2 Packet Tracer - Configure an IOS IPS Using the CLI		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
5.4.1.3 Chapter 5: Implementing Intrusion Prevention		HS-ETS1-2.	ITEA.9.	IT-NET 3.8	

CCNA Security - Chapter 6, Securing the Local Area Network					
Page	**NICE**	**NGSS**	**ITEA**	**DODEA**	**Exam Objective**
Section 6.0 Introduction					
6.0.1 Welcome					
6.0.1.1 Securing the Local Area Network		HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4.c Describe MAC spoofing
Section 6.1 Endpoint Security					
6.1.1 Introducing Endpoint Security					
6.1.1.1 Securing LAN Elements		HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.2.e Describe authentication and authorization using ACS and ISE 4.4.c Describe MAC spoofing
6.1.1.2 Traditional Endpoint Security		HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.4e
6.1.1.3 The Borderless Network		HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.4e
6.1.1.4 Securing Endpoints in the Borderless Network		HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.4e
6.1.1.5 Modern Endpoint Security Solutions		HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.4e
6.1.1.6 Hardware and Software Encryption of Local Data	T0553	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.30
6.1.1.7 Activity - Identify Endpoint Security Terminology (DND)		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
6.1.2 Antimalware Protection	S0079				
6.1.2.1 Advanced Malware Protection	S0079	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.2.c Identify malware
6.1.2.2 Video - AMP and Managed Threat Defense		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 3.8	1.2.c Identify malware
6.1.2.3 Video - AMP for Endpoints		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 3.8	1.2.c Identify malware
6.1.3 Email and Web Security					
6.1.3.1 Securing Email and Web	S0138	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	7.1a
6.1.3.2 Video - Cisco Email Security Appliance		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 3.8	7.1a
6.1.3.3 Cisco Web Security Appliance	K0114	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	7.2a
6.1.3.4 Cisco Cloud Web Security	T0251	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	7.2a
6.1.4 Controlling Network Access					
6.1.4.1 Cisco Network Admission Control	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.2.e Identify endpoint posture assessment
6.1.4.2 Cisco NAC Functions	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.0_
6.1.4.3 Cisco NAC Components	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.0_
6.1.4.4 Network Access for Guests	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.0_
6.1.4.5 Cisco NAC Profiler	T0438	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.2.e Describe authentication and authorization using ACS and ISE 2.3.a Identify the functions 802.1X components 4.4.c Describe MAC spoofing

Section 6.2 Layer 2 Security Considerations					
6.2.1 Layer 2 Security Threats					
6.2.1.1 Describe Layer 2 Vulnerabilities	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4a-g
6.2.1.2 Switch Attack Categories	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.1.b Configure secure network management 2.1.e Use SCP for file transfer 2.4.a Describe the BYOD architecture framework
6.2.1.3 Activity		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
6.2.2 CAM Table Attacks					
6.2.2.1 Basic Switch Operation	K0011	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
6.2.2.2 CAM Table Operation Example	K0011	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
6.2.2.3 CAM Table Attack	K0011	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4d
6.2.2.4 CAM Table Attack Tools	K0011	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4d
6.2.3 Mitigating CAM Table Attacks					
6.2.3.1 Countermeasure for CAM Table Attacks	K0011	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4d
6.2.3.2 Port Security	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.5c
6.2.3.3 Enabling Port Security Options	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.5c
6.2.3.4 Syntax Checker - Port Security Violations		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	4.5c
6.2.3.5 Port Security Aging	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.5c
6.2.3.6 Port Security with IP Phones	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.5c
6.2.3.7 SNMP MAC Address Notification		HS-ETS1-2.	ITEA.9.	IT-NET 3.8	2.1.c Configure and verify secure access through SNMP v3 using an ACL
6.2.4 Mitigating VLAN Attacks					4.5_
6.2.4.1 VLAN Hopping Attacks	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4f
6.2.4.2 VLAN Double-Tagging Attack	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4f
HS-ETS1-4.		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
6.2.4.4 PVLAN Edge Feature	K0011	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.6_
6.2.4.5 PVLAN Edge	K0011	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.6_
6.2.4.6 Private VLANs	K0011	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.6_
6.2.4.7 Video - Private VLAN Tutorial and Demonstration		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 3.8	4.6_
6.2.5 Mitigating DHCP Attacks					
6.2.5.1 DHCP Spoofing Attack	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4g
6.2.5.2 DHCP Starvation Attack	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4g
6.2.5.3 Mitigating DHCP Attacks	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.5_
6.2.5.4 Configuring DHCP Snooping	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4g

6.2.5.5 Syntax Checker - Configuring DHCP Snooping Example		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
6.2.6 Mitigating ARP Attacks					
6.2.6.1 ARP Spoofing and ARP Poisoning Attack	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4.b Describe ARP spoofing 4.4.c Describe MAC spoofing
6.2.6.2 Mitigating ARP Attacks	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4.b Describe ARP spoofing 4.4.c Describe MAC spoofing
6.2.6.3 Configuring Dynamic ARP Inspection	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4.b Describe ARP spoofing 4.4.c Describe MAC spoofing
6.2.6.4 Syntax Checker - Configuring Dynamic ARP Inspection Example		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	4.4.b Describe ARP spoofing 4.4.c Describe MAC spoofing
6.2.7 Mitigating Address Spoofing Attacks					
6.2.7.1 Address Spoofing Attack	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4.b Describe ARP spoofing 4.4.c Describe MAC spoofing
6.2.7.2 Mitigating Address Spoofing Attacks	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4.b Describe ARP spoofing 4.4.c Describe MAC spoofing
6.2.7.3 Syntax Checker - Configuring IP Source Guard		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
6.2.8 Spanning Tree Protocol					4.4a
6.2.8.1 Introduction to the Spanning Tree Protocol	T0035	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
6.2.8.2 Various Implementations of STP	T0035	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
6.2.8.3 STP Port Roles	T0035	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
6.2.8.4 STP Root Bridge	T0035	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
6.2.8.5 STP Path Cost	T0035	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
6.2.8.6 802.1D BPDU Frame Format	T0035	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
6.2.8.7 BPDU Propagation and Process	T0035	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
6.2.8.8 Extended System ID	T0035	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
6.2.8.9 Syntax Checker - Select the Root Bridge		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
6.2.8.10 Activity - Identify the 802.1D RSTP Port Roles		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
6.2.8.11 Activity - Troubleshoot STP Configuration Issues		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
6.2.8.12 Video - Observing Spanning Tree Protocol Operation		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 3.8	
6.2.9 Mitigating STP Attacks					
6.2.9.1 STP Manipulation Attacks	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4.a Describe STP attacks
6.2.9.2 Mitigating STP Attacks	K0296	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4.a Describe STP attacks
6.2.9.3 Configuring PortFast	T0035	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	4.4.a Describe STP attacks
6.2.9.4 Configuring BPDU Guard	T0035	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
6.2.9.5 Configuring Root Guard	T0035	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	

6.2.9.6 Syntax Checker - Configuring Loop Guard		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
Section 6.3 Chapter Summary					
6.3.1 Conclusion					
6.3.1.1 Lab – Securing Layer 2 Switches		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3. IT-NET 3.8	
6.3.1.2 Packet Tracer – Layer 2 Security		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	4.4.a Describe STP attacks
HS-ETS1-4.		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
6.3.1.4 Chapter 6: Securing the Local Area Network		HS-ETS1-2.	ITEA.9.	IT-NET 3.8	

CCNA Security - Chapter 7, Cryptographic Systems

Page	NICE	NGSS	ITEA	DODEA	Exam Objective
Section 7.0 Introduction					
7.0.1 Welcome					
7.0.1.1 Cryptographic Services	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
Section 7.1 Cryptographic Services					
7.1.1 Securing Communications					1.1.a Describe confidentiality, integrity, availability (CIA)
7.1.1.1 Authentication, Integrity, and Confidentiality	T0017	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.a Describe confidentiality, integrity, availability (CIA) 3.3.a Implement an IPsec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls
7.1.1.2 Authentication	T0446	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.a Describe confidentiality, integrity, availability (CIA)
7.1.1.3 Data Integrity	T0446	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.a Describe confidentiality, integrity, availability (CIA)
7.1.1.4 Data Confidentiality	T0446	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.a Describe confidentiality, integrity, availability (CIA)
7.1.1.5 Activity - Identify the Secure Communication Objective		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
7.1.2 Cryptography					1.3_
7.1.2.1 Creating Cipher Text	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.1.2.2 Transposition Ciphers	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.1.2.3 Substitution Ciphers	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.1.2.4 Substitution Ciphers (Cont.)	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.1.2.5 One-Time Pad Ciphers	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.1.3 Cryptanalysis					1.3_
7.1.3.1 Cracking Code	T0176	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.1.3.2 Methods for Cracking Code	T0176	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.1.3.3 Cracking Code Example	T0176	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.1.3.4 Activity - Crack the Code		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	1.3_
7.1.4 Cryptology					1.3_
7.1.4.1 Making and Breaking Secret Codes	T0077	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.1.4.2 Cryptanalysis	T0077	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.1.4.3 The Secret is in the Keys	T0077	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.1.4.4 Activity - Identify the Cryptology Terminology		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	1.3_
Section 7.2 Basic Integrity and Authenticity					
7.2.1 Cryptographic Hashes					1.3_
7.2.1.1 Cryptographic Hash Function	S0089	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.2.1.2 Cryptographic Hash Function Properties	S0089	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.2.1.3 Well-Known Hash Functions	S0089	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	

7.2.2 Integrity with MD5, SHA-1, and SHA-2					1.3_
7.2.2.1 Message Digest 5 Algorithm	S0089	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.2.2.2 Secure Hash Algorithm	S0089	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.2.2.3 MD5 versus SHA	S0089	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.2.3 Authenticity with HMAC					
7.2.3.1 Keyed-Hash Message Authentication Code	S0089	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.2.3.2 HMAC Operation	S0089	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.2.3.3 Hashing in Cisco Products	S0089	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.2.4 Key Management					1.3_
7.2.4.1 Characteristics of Key Management	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.2.4.2 Key Length and Keyspace	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.2.4.3 The Keyspace	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.2.4.4 Types of Cryptographic Keys	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.2.4.5 Choosing Cryptographic Keys	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.2.4.6 Activity - Identify the Characteristics of Key Management		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
Section 7.3 Confidentiality					
7.3.1 Encryption					
7.3.1.1 Two Classes of Encryption Algorithms	S0089	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.3.a Implement an IPsec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls
7.3.1.2 Symmetric and Asymmetric Encryption	S0089	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.3.1.3 Symmetric Encryption	S0089	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.3.1.4 Symmetric Block Ciphers and Stream Ciphers	S0089	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.3.1.5 Choosing an Encryption Algorithm	S0089	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.3.1.6 Activity - Compare Symmetric and Asymmetric Encryption Algorithms		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
7.3.2 Data Encryption Standard					1.3_
7.3.2.1 DES Symmetric Encryption	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.3.2.2 DES Summary	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.3.2.3 Improving DES with 3DES	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.3.2.4 3DES Operation	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.3.2.5 AES Origins	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.3.2.6 AES Summary	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.3.3 Alternate Encryption Algorithms					1.3_
7.3.3.1 Software-Optimized Encryption Algorithm	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.3.3.2 RC Algorithms	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.3.4 Diffie-Hellman Key Exchange					1.3_
7.3.4.1 Diffie-Hellman Algorithm	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
7.3.4.2 DH Operation	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	

7.3.4.3 Activity - Identify the Steps of the DH Process		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
Section 7.4 Public Key Cryptography					
7.4.1 Symmetric Versus Asymmetric Encryption					
7.4.1.1 Asymmetric Key Algorithms	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.3.a Implement an IPsec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls
7.4.1.2 Public Key + Private Key = Confidentiality	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.4.1.3 Private Key + Public Key = Authentication	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.4.1.4 Asymmetric Algorithms	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3b
7.4.1.5 Types of Asymmetric Algorithms	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3b
7.4.1.6 Activity -Identify the Key Types Required to Provide Authenticity and Confidentiality		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
7.4.2 Digital Signatures					
7.4.2.1 Using Digital Signatures	S0020	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.4.2.2 Code Signing	S0020	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.4.2.3 Digital Certificates	T0416	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.4.2.4 Using Digital Certificates	T0416	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.4.2.5 Digital Signature Algorithms	T0416	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.4.2.6 Digitally Signed Cisco Software	T0416	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.4.2.7 Activity - Identify the Key Types Required to Provide Authenticity and Confidentiality		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
7.4.3 Public Key Infrastructure					
7.4.3.1 Public Key Infrastructure Overview	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.4.3.2 PKI Framework	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.4.3.3 Certificate Authorities	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.4.3.4 Interoperability of Different PKI Vendors	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.4.3.5 Public-Key Cryptography Standards	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.4.3.6 Simple Certificate Enrollment Protocol	T0416	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
7.4.3.7 PKI Topologies	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.4.3.8 Registration Authority	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.4.3.9 Digital Certificates and CA's	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.3_
7.4.3.10 Activity - Identify Elements of the PKI Framework		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
Section 7.5 Chapter Summary					
7.5.1 Conclusion					

7.5.1.1 Video - Wireshark Packet Sniffing Usernames, Passwords, and Web Pages		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 3.8	
7.5.1.2 Lab - Exploring Encryption Methods		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3. IT-NET 3.8	
7.5.1.3 Cryptographic Systems	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	

CCNA Security - Chapter 8 Implementing Virtual Private Networks

Page	NICE	NGSS	ITEA	DODEA	Exam Objective
Section 8.0 Introduction					
8.0.1 Welcome					
8.0.1.1 Implementing Virtual Private Networks	K0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.3.b Verify an IPsec site-to-site VPN
Section 8.1 VPNs					
8.1.1 VPN Overview					
8.1.1.1 Introducing VPNs	K0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.a Describe confidentiality, integrity, availability (CIA)
8.1.1.2 Layer 3 IPsec VPNs	K0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.3.b Verify an IPsec site-to-site VPN
8.1.2 VPN Topologies					
8.1.2.1 Two Types of VPNs	K0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.0_
8.1.2.2 Components of Remote-Access VPNs	K0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.0_
8.1.2.3 Components of Site-to-Site VPNs	K0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.3.b Verify an IPsec site-to-site VPN
8.1.2.4 Activity - Compare Remote-Access and Site-to-Site VPNs	S0059	HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
8.1.2.5 Hairpinning and Split Tunneling	K0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.b Describe hairpinning, split tunneling, always-on, NAT traversal
Section 8.2 IPsec VPN Components and Operation					
8.2.1 Introducing IPsec					
8.2.1.1 IPsec Technologies	S0081	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
8.2.1.2 Confidentiality	T0017	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.a Describe confidentiality, integrity, availability (CIA)
8.2.1.3 Integrity	T0017	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.a Describe confidentiality, integrity, availability (CIA)
8.2.1.4 Authentication	T0017	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	1.1.a Describe confidentiality, integrity, availability (CIA)
8.2.1.5 Secure Key Exchange	T0269	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
8.2.1.6 Activity - Identify the Components of the IPsec Framework		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
8.2.2 IPsec Protocol					
8.2.2.1 IPsec Protocol Overview	S0081	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
8.2.2.2 Authentication Header	S0081	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
8.2.2.3 ESP	S0081	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
8.2.2.4 ESP Encrypts and Authenticates	S0081	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
8.2.2.5 Transport and Tunnel Modes	S0081	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)

8.2.2.6 Activity - Compare AH and ESP		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
8.2.3 Internet Key Exchange					3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
8.2.3.1 The IKE Protocol	K0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
8.2.3.2 Phase 1 and 2 Key Negotiation	K0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
8.2.3.3 Phase 2: Negotiating Sass	K0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode) 3.1.b Describe hairpinning, split tunneling, always-on, NAT traversal
8.2.3.4 Video - IKE Phase 1 and Phase 2	K0104	HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
Section 8.3 Implementing Site-to-Site IPsec VPNs with CLI					
8.3.1 Configuring a Site-to-Site IPsec VPN					
8.3.1.1 IPsec Negotiation	K0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
8.3.1.2 Site-to-Site IPsec VPN Topology	S0081	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode) 3.3.b Verify an IPsec site-to-site VPN
8.3.1.3 IPsec VPN Configuration Tasks	S0081	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.3.b Verify an IPsec site-to-site VPN
8.3.1.4 Existing ACL Configurations	T0054	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode) 3.3.b Verify an IPsec site-to-site VPN
8.3.1.5 Handling Broadcast and Multicast Traffic	T0023	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.3.b Verify an IPsec site-to-site VPN
8.3.1.6 Activity - Order the IPsec Negotiation Steps		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 3.8	
8.3.2 ISAKMP Policy					
8.3.2.1 The Default ISAKMP Policies	K0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
8.3.2.2 Syntax to Configure a New ISAKMP Policy	K0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
8.3.2.3 XYZCORP ISAKMP Policy Configuration	K0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.3.a Implement an IPsec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls

8.3.2.4 Syntax Checker - Configuring a Pre-Shared Key		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	3.3.a Implement an IPsec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls
8.3.3 IPsec Policy					
8.3.3.1 Define Interesting Traffic	T0023	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
8.3.3.2 Syntax Checker - Configure IPsec Transform Set		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
8.3.4 Crypto Map					
8.3.4.1 Syntax to Configure a Crypto Map	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
8.3.4.2 XYZCORP Crypto Map Configuration	K0019	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
8.3.4.3 Syntax Checker - Apply the Crypto Map		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
8.3.5 IPsec VPN					
8.3.5.1 Send Interesting Traffic	T0023	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	
8.3.5.2 Syntax Checker - Verify the ISAKMP and IPsec Tunnels		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
Section 8.4 Summary					
8.4.1 Conclusion					
8.4.1.1 Video - Site-to-Site IPsec VPN Configuration		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 3.8	3.3.b Verify an IPsec site-to-site VPN
8.4.1.2 Packet Tracer - Configure and Verify a Site-to-Site IPsec VPN		HS-ETS1-4.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	3.3.b Verify an IPsec site-to-site VPN
8.4.1.3 Lab - Configuring a Site-to-Site VPN		HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3. IT-NET 3.8	3.3.b Verify an IPsec site-to-site VPN
8.4.1.4 Implementing Virtual Private Networks	K0104	HS-ETS1-2.	ITEA.9.	IT-NET 3.8	

CCNA Security - Chapter 9, Implementing the Cisco Adaptive Security Appliance

Page	NICE	NGSS	ITEA	DODEA	Exam Objective
Section 9.0 Introduction					
9.0.1 Welcome					
9.0.1.1 Implementing the Cisco Adaptive Security Appliance		HS-ETS1-1.	ITEA.8.	IT-NET 2.2	3.1.b Describe hairpinning, split tunneling, always-on, NAT traversal
Section 9.1 Introduction to the ASA					
9.1.1 ASA Solutions					
9.1.1.1 ASA Firewall Models	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	3.2.b Verify clientless connection
9.1.1.2 Video - Cisco ASA Next-Generation Firewall Appliances		HS-ETS1-1.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 2.2	
9.1.1.3 Advanced ASA Firewall Feature	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	3.3a
9.1.1.4 Review of Firewalls in Network Design	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	3.3a
9.1.1.5 ASA Firewall Modes of Operation	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	3.3a
9.1.1.6 ASA Licensing Requirements	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	3.2.c Implement basic AnyConnect SSL VPN using ASDM
9.1.2 Basic ASA Configuration					
9.1.2.1 Overview of ASA 5505	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	3.3a
9.1.2.2 ASA Security Levels	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	5.3_
9.1.2.3 ASA 5505 Deployment Scenarios	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	
Section 9.2 ASA Firewall Configuration					
9.2.1 The ASA Firewall Configuration					
9.2.1.1 Basic ASA Settings	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	5.5
9.2.1.2 ASA Default Configuration	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	5.5
9.2.1.3 ASA Interactive Setup Initialization Wizard	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	5.5
9.2.2 Configuring Management Settings and Services					
9.2.2.1 Enter Global Configuration Mode	K0011	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	2.1.d Configure and verify security for NTP
9.2.2.2 Syntax Checker - Configuring Basic Settings		HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 2.2	
9.2.2.3 Configuring Logical VLAN Interfaces	K0011	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	
9.2.2.4 Syntax Checker - Assigning Layer 2 Ports to VLANs		HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 2.2	
9.2.2.5 Syntax Checker - Configuring a Default Static Route		HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 2.2	
9.2.2.6 Syntax Checker - Configuring Remote Access Services		HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 2.2	
9.2.2.7 Syntax Checker - Configuring Network Time Protocol Services		HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 2.2	2.1.d Configure and verify security for NTP
9.2.2.8 Syntax Checker - Configuring DHCP Services		HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 2.2	
9.2.3 Object Groups					
9.2.3.1 Introduction to Objects and Object Groups	K0001	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	
9.2.3.2 Configuring Network Objects	K0001	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	
9.2.3.3 Configuring Service Objects	K0001	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	
9.2.3.4 Object Groups	K0001	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	

9.2.3.5 Configuring Common Object Groups	K0001	HS-ETS1-1.	ITEA.8.	IT-NET 2.2	
9.2.3.6 Activity - Identify Types of Object Groups		HS-ETS1-1.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 2.2	
9.2.4 ACLs					
9.2.4.1 ASA ACLs	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 3.8	
9.2.4.2 Types of ASA ACL Filtering	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 3.8	4.3.a Explain the function of control plane policing
9.2.4.3 Types of ASA ACLs	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 3.8	3.2.b Verify clientless connection
9.2.4.4 Configuring ACLs	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 3.8	
9.2.4.5 Applying ACLs	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 3.8	
9.2.4.6 ACLs and Object Groups	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 3.8	
9.2.4.7 Syntax Checker - ACL Using Object Groups Examples		HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
9.2.5 NAT Services on an ASA					
9.2.5.1 ASA NAT Overview	K0049	HS-ETS1-1.	ITEA.8.	IT-NET 3.8	5.3
9.2.5.2 Syntax Checker - Configuring Dynamic NAT		HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	5.3_
9.2.5.3 Configuring Dynamic PAT		HS-ETS1-1.	ITEA.8.	IT-NET 3.8	5.3
9.2.5.4 Syntax Checker - Configuring Static NAT		HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
9.2.6 AAA					
9.2.6.1 AAA Review		HS-ETS1-1.	ITEA.8.	IT-NET 3.8	2.2_
9.2.6.2 Local Database and Servers		HS-ETS1-1.	ITEA.8.	IT-NET 3.8	2.2.a Describe RADIUS and TACACS+ technologies
9.2.6.3 Syntax Checker - AAA Configuration		HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
9.2.7 Service Policies on an ASA					
9.2.7.1 Overview of MPF		HS-ETS1-1.	ITEA.8.	IT-NET 3.8	5.5d
9.2.7.2 Configuring Class Maps		HS-ETS1-1.	ITEA.8.	IT-NET 3.8	
9.2.7.3 Syntax Checker - Define and Activate a Policy		HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
9.2.7.4 ASA Default Policy		HS-ETS1-1.	ITEA.8.	IT-NET 3.8	5.5
Section 9.3 Summary					
9.3.1 Conclusion					
9.3.1.1 Packet Tracer - Configure ASA Basic Settings and Firewall Using the CLI		HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 3.8	
9.3.1.2 Lab - Configure ASA Basic Settings and Firewall Using the CLI		HS-ETS1-1.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.3. IT-NET 3.8	
9.3.1.3 Implementing the Cisco Adaptive Security Appliance		HS-ETS1-1.	ITEA.8.	IT-NET 3.8	

CCNA Security - Chapter 10, Advanced Cisco Adaptive Security Appliance

Page	NICE	NGSS	ITEA	DODEA	Exam Objective
Section 10.0 Introduction					
10.0.1 Welcome					
10.0.1.1 Advanced Cisco Adaptive Security Appliance		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.1.b Describe hairpinning, split tunneling, always-on, NAT traversal
Section 10.1 ASA Security Device Manager					
10.1.1 Introduction to ASDM					
10.1.1.1 Overview of ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2
10.1.1.2 Syntax Checker - Preparing for ASDM		HS-ETS1-4.	ITEA.3.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 4.1	
10.1.1.3 Starting ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2
10.1.1.4 ASDM Home Page Dashboards		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2
10.1.1.5 ASDM Page Elements		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	4.1.a Configure multiple privilege levels
10.1.1.6 ASDM Configuration and Monitoring Views		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2
10.1.1.7 Video - Configure and Access ASDM on an ASA 5505		HS-ETS1-2.	ITEA.3.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 4.1	
10.1.2 ASDM Wizard Menu					
10.1.2.1 HASDM Wizards		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.1.2.2 The Startup Wizard		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.b Verify clientless connection
10.1.2.3 Different Types of VPN Wizards		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.a Implement basic clientless SSL VPN using ASDM 3.2.c Implement basic AnyConnect SSL VPN using ASDM 3.3.b Verify an IPsec site-to-site VPN
10.1.2.4 Other Wizards		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.1.2.5 Activity - Identify ASDM Wizards		HS-ETS1-2.	ITEA.3.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 4.1	3.3.b Verify an IPsec site-to-site VPN
10.1.3 Configuring Management Settings and Services					
10.1.3.1 Configuring Settings in ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.1.3.2 Configuring Basic Settings in ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.1.3.3 Configuring Interfaces in ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.1.3.4 Configuring the System Time in ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	2.1.d Configure and verify security for NTP
10.1.3.5 Configuring Routing in ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.1.3.6 Configuring Device Management Access in ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.1.3.7 Configuring DHCP Services in ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.1.4 Configuring Advanced ASDM Features					
10.1.4.1 Objects in ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.1.4.2 Configuring ACLs Using ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.1.4.3 Configuring Dynamic NAT in ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.1.4.4 Configuring Dynamic PAT in ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.1.4.5 Configuring Static NAT in ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.1.4.6 Configuring AAA Authentication		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	2.2.a Describe RADIUS and TACACS+ technologies
10.1.4.7 Configuring a Service Policy Using ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.1.4.8 Lab - Configure ASA Basic Settings and Firewall Using ASDM		HS-ETS1-2.	ITEA.3.	CCR.ELA-Literacy.RST.11-12.3. IT-NET 4.1	
Section 10.2 ASA VPN Configuration					

10.2.1 Site-to-Site VPNs					3.3.b Verify an IPsec site-to-site VPN
10.2.1.1 ASA Support for Site-to-Site VPNs		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.a Implement basic clientless SSL VPN using ASDM 3.2.b Verify clientless connection 3.2.c Implement basic AnyConnect SSL VPN using ASDM 3.3.b Verify an IPsec site-to-site VPN
10.2.1.2 ASA Site-to-Site VPNs Using ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.3.b Verify an IPsec site-to-site VPN
10.2.1.3 Configuring the ISR Site-to-Site VPNs Using the CLI		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode) 3.3.a Implement an IPsec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls 3.3.b Verify an IPsec site-to-site VPN
10.2.1.4 Configuring the ASA Site-to-Site VPNs Using ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.3.b Verify an IPsec site-to-site VPN
10.2.1.5 Configuring the ASA Site-to-Site VPNs Using ASDM (Cont.)		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode) 3.2.c Implement basic AnyConnect SSL VPN using ASDM 3.3.a Implement an IPsec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls 3.3.b Verify an IPsec site-to-site VPN
10.2.1.6 Configuring the ASA Site-to-Site VPNs Using ASDM (Cont.)		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.3.b Verify an IPsec site-to-site VPN
10.2.1.7 Verifying Site-to-Site VPNs Using ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.3.b Verify an IPsec site-to-site VPN
10.2.1.8 Test the Site-to-Site VPN Using ASDM		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.3.b Verify an IPsec site-to-site VPN
10.2.1.9 Lab - Configure a Site-to-Site IPsec VPN Using ISR CLI and ASA ASDM		HS-ETS1-2.	ITEA.3.	CCR.ELA-Literacy.RST.11-12.3. IT-NET 4.1	3.3.b Verify an IPsec site-to-site VPN
10.2.2 Remote-Access VPNs					
10.2.2.1 Remote-Access VPN Options		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.2.2.2 IPsec versus SSL		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.2.2.3 ASA SSL VPNs		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.b Verify clientless connection 3.2.c Implement basic AnyConnect SSL VPN using ASDM
10.2.2.4 Clientless SSL VPN Solution		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.b Verify clientless connection
10.2.2.5 Client-Based SSL VPN Solution		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.b Verify clientless connection 3.2.c Implement basic AnyConnect SSL VPN using ASDM
10.2.2.6 Cisco AnyConnect Secure Mobility Client		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.1.b Describe hairpinning, split tunneling, always-on, NAT traversal 3.2.c Implement basic AnyConnect SSL VPN using ASDM 3.2.e Identify endpoint posture assessment
10.2.2.7 AnyConnect for Mobile Devices		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.c Implement basic AnyConnect SSL VPN using ASDM
10.2.3 Configuring Clientless SSL VPN					3.2.b Verify clientless connection
10.2.3.1 Configuring Clientless SSL VPN on an ASA		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.a Implement basic clientless SSL VPN using ASDM 3.2.b Verify clientless connection
10.2.3.2 Sample Clientless VPN Topology		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.b Verify clientless connection
10.2.3.3 Clientless SSL VPN		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.a Implement basic clientless SSL VPN using ASDM 3.2.b Verify clientless connection
10.2.3.4 Clientless SSL VPN (Cont.)		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.b Verify clientless connection

10.2.3.5 Clientless SSL VPN (Cont.)		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.b Verify clientless connection
10.2.3.6 Clientless SSL VPN (cont.)		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.b Verify clientless connection
10.2.3.7 Verifying Clientless SSL VPN		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.a Implement basic clientless SSL VPN using ASDM 3.2.b Verify clientless connection
10.2.3.8 Testing the Clientless SSL VPN Connection		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.b Verify clientless connection
10.2.3.9 Viewing the Generated CLI Config		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	
10.2.4 Configuring AnyConnect SSL VPN					
10.2.4.1 Configuring SSL VPN AnyConnect		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.c Implement basic AnyConnect SSL VPN using ASDM
10.2.4.2 Sample SSL VPN Topology		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.b Verify clientless connection 3.2.c Implement basic AnyConnect SSL VPN using ASDM
10.2.4.3 AnyConnect SSL VPN		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.c Implement basic AnyConnect SSL VPN using ASDM
10.2.4.4 AnyConnect SSL VPN (Cont.)		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.c Implement basic AnyConnect SSL VPN using ASDM
10.2.4.5 AnyConnect SSL VPN (Cont.)		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.c Implement basic AnyConnect SSL VPN using ASDM
10.2.4.6 AnyConnect SSL VPN (Cont.)		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.c Implement basic AnyConnect SSL VPN using ASDM
10.2.4.7 AnyConnect SSL VPN (Cont.)		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.c Implement basic AnyConnect SSL VPN using ASDM
10.2.4.8 Verifying AnyConnect Connection		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.c Implement basic AnyConnect SSL VPN using ASDM 3.2.d Verify AnyConnect connection
10.2.4.9 Install the AnyConnect Client		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.b Verify clientless connection 3.2.c Implement basic AnyConnect SSL VPN using ASDM
10.2.4.10 Install the AnyConnect Client (Cont.)		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.c Implement basic AnyConnect SSL VPN using ASDM
10.2.4.11 Install the AnyConnect Client (Cont.)		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.c Implement basic AnyConnect SSL VPN using ASDM
10.2.4.12 Viewing the Generated CLI Config		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.c Implement basic AnyConnect SSL VPN using ASDM
Section 10.3 Chapter Summary					
10.3.1 Conclusion					
10.3.1.1 Lab - Configure Clientless Remote Access SSL VPNs Using ASDM		HS-ETS1-2.	ITEA.3.	CCR.ELA-Literacy.RST.11-12.3. IT-NET 4.1	3.2.a Implement basic clientless SSL VPN using ASDM 3.2.b Verify clientless connection
10.3.1.2 Lab - Configure AnyConnect Remote Access SSL VPNs Using ASDM		HS-ETS1-2.	ITEA.3.	CCR.ELA-Literacy.RST.11-12.3. IT-NET 4.1	3.2.c Implement basic AnyConnect SSL VPN using ASDM
10.3.1.3 Advanced Cisco Adaptive Security Appliance		HS-ETS1-2.	ITEA.3.	IT-NET 4.1	3.2.a Implement basic clientless SSL VPN using ASDM 3.2.c Implement basic AnyConnect SSL VPN using ASDM

CCNA Security - Chapter 11, Managing a Secure Network

Page	NICE	NGSS	ITEA	DODEA	Exam Objective
Section 11.0 Introduction					
11.0.1 Welcome					
11.0.1.1 Managing a Secure Network		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
Section 11.1 Network Security Testing					
11.1.1 Network Security Testing Techniques					
11.1.1.1 Operations Security		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.1.1.2 Testing and Evaluating Network Security		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.1.1.3 Types of Network Tests		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.1.1.4 Applying Network Test Results		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.1.2 Network Security Testing Tools					
11.1.2.1 Network Testing Tools		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	1.1.b Describe SIEM technology
11.1.2.2 Nmap and Zenmap		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.1.2.3 SuperScan		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.1.2.4 Video - SIEM		HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.7. IT-NET 5.8	1.1.b Describe SIEM technology 2.4.b Describe the function of mobile device management (MDM)
11.2.1.5 Activity - Identify Network Security Testing Tools		HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 5.8	
Section 11.2 Developing a Comprehensive Security Policy					
11.2.1 Security Policy Overview					
11.2.1.1 Secure Network Life Cycle		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.1.2 Security Policy		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.1.1.3 Security Policy Audience		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.2 Structure of a Security Policy		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.2.1 Security Policy Hierarchy		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.2.2 Governing Policy		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.2.3 Technical Policies		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.2.4 End User Policies		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.2.5 Activity - Identify Security Policy Components		HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.4. IT-NET 5.8	
11.2.3 Standards, Guidelines, and Procedures					
11.2.3.1 Security Policy Documents		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.3.2 Standards Documents		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.3.3 Guideline Documents		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.3.4 Procedure Documents		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.4 Roles and Responsibilities					
11.2.4.1 Organizational Reporting Structure		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.4.2 Common Executive Titles		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.5 Security Awareness and Training					

11.2.5.1 Security Awareness Program		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.5.2 Awareness Campaigns		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.5.3 Security Training Course		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.5.4 Educational Program		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.6 Responding to a Security Breach					
11.2.6.1 Motive, Opportunity, and Means		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
11.2.6.2 Collecting Data		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	
Section 11.3 Chapter Summary					
11.3.1 Conclusion					
11.3.1.1 Packet Tracer - Skills Integration Challenge		HS-ETS1-4.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.9. IT-NET 5.8	3.3.b Verify an IPsec site-to-site VPN
11.3.1.2 Lab - CCNA Security Comprehensive Lab		HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.3. IT-NET 5.8	3.2.a Implement basic clientless SSL VPN using ASDM 3.2.b Verify clientless connection
11.3.1.3 Managing a Secure Network		HS-ETS1-3.	ITEA.12.	IT-NET 5.8	