

COURSE TITLE	NETWORK FILTERING TECHNOLOGY
COURSE CODE	05CA0502
COURSE CREDITS	4

Objective:

- 1 To understand and explain the configuration and management of ASA Firewall.
- 2 To acquire conceptual knowledge of configuring AAA (Authentication, Authorization, Accounting) servers.
- 3 To gain knowledge about the configuration and administration of Checkpoint Firewall.

Course Outcomes: After completion of this course, student will be able to:

- 1 Identify and analyze various Layer 2 attacks and demonstrate appropriate mitigation techniques.
- 2 Explain the fundamentals of Check Point technology and its role in network security.
- 3 Describe the architecture and functionality of the Cisco ASA Firewall.
- 4 Configure and manage ASA security features for enhanced network protection.

Pre-requisite of course:NA

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
3	0	2	50	30	20	25	25

Contents : Unit	Topics	Contact Hours
1	LAYER 2 ATTACKS AND MITIGATION Configure DHCP snooping, Describe dynamic ARP inspection, Configure port security, Configure IP source verification, Describe MACSec	10
2	INTRODUCTION TO CHECK POINT TECHNOLOGY Introduction of Security Devices, Types of Firewalls, Check Point Gaia, Network Address Translation.	10
3	INTRODUCTION TO CISCO ASA FIREWALL Cisco IOS Firewall CBAC Configuration, Cisco IOS Firewall IDS Configuration, Implement ASA firewall features using ASDM Firewall Routing.	12
4	ASA Security Configuration of site-to-site VPN, Remote Access, Introduction of AAA server, TACACS+, RADIUS	13
Total Hours		45

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	Unit 1 Enable DHCP snooping globally and per VLAN to prevent rogue DHCP servers, Verify DHCP Snooping Binding Table, View and analyze the DHCP snooping binding table entries for connected devices, Configure Dynamic ARP Inspection (DAI), Configure Basic Port Security, Set maximum MAC addresses per port and configure violation modes (shutdown, restrict, protect), Implement Sticky MAC Addressing on a Switch Port, Use IP source guard with DHCP snooping to prevent IP spoofing, Explore and document different types of security devices (e.g., firewalls, IDS/IPS, UTM) in a simulated lab environment, Configure Basic Packet-Filtering Firewall Rules, Implement basic rule sets on a simulated or physical firewall to allow/deny traffic based on source, destination, and port, Install and Configure Check Point Gaia OS, Create and Manage Security Policies in Check Point Firewall, Configure and apply security policies using Check Point SmartConsole, test rule matches and log results, Implement Network Address Translation (NAT) Rules, Configure static and dynamic NAT rules on Check Point or other supported firewalls and verify proper translation.	15
2	Unit 2 Configure Cisco IOS Firewall using CBAC (Context-Based Access Control), Implement Cisco IOS Firewall IDS (Intrusion Detection System), Configure ASA Firewall Using ASDM (Adaptive Security Device Manager), Use ASDM GUI to configure basic ASA settings, security levels, and access control rules, Configure Static and Dynamic Routing on ASA Firewall, Implement ACLs and NAT Policies in ASA Firewall, Configure Site-to-Site VPN using Cisco ASA, Configure Remote Access VPN on ASA Firewall, Create and test Remote Access VPN for clients using Cisco AnyConnect or other VPN clients, Set up and Configure AAA Server (Authentication, Authorization, Accounting), Configure TACACS+ Server with Cisco Router/Switch, Configure RADIUS Server Integration with Network Devices.	15
Total Hours		30

Textbook :

- 1 Implementing Cisco Edge Network Security Solutions (300-206), Sean Wilkins, Trey Smith, Cisco Press, 2015
- 2 AnyConnect: Configure Basic SSLVPN for IOS Router, hunter, Cisco Community / Blog, 2010

References:

- 1 CCNA Security 210-260 Official Cert Guide, CCNA Security 210-260 Official Cert Guide, Omar Santos, John Stuppi, Cisco Press, 2016
- 2 CCSP: Securing Cisco IOS Networks Study Guide, CCSP: Securing Cisco IOS Networks Study Guide, Dale Liu, Sybex, 2004

Suggested Theory Distribution:

The suggested theory distribution as per Bloom's taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery					
Remember / Knowledge	Understand	Apply	Analyze	Evaluate	Higher order Thinking / Creative
10.00	15.00	25.00	25.00	25.00	0.00

Instructional Method:

- 1 Pratical, Demo & PPT

Supplementary Resources:

- 1 <https://www.rededucation.com/checkpoint/check-point-certified-security-administrator-ccsa/>