	INSTITUT SAINS DAN TEKNOLOGI NASIONAL **PROGRAM STUDI MAGISTER TEKNIK ELEKTRO** **Master of Science in Cybersecurity and Defense - MSCD**	**RPS-MKE-CS-001**

RENCANA PEMBELAJARAN SEMESTER (RPS)

Mata Kuliah	Kode MK	Rumpun MK	Bobot SKS		Semester	Tgl. Penyusunan
Advanced Network Security Specialization	MTE-CS-001	Advanced Network Security Specialization	T = 2 SKS	P = 0 SKS	1	1 Maret 2025

OTORISASI	**Pengembang RPS**	**Koordinator Rumpun MK**	**Kaprodi**
	(Dr. Ir. Kuntjoro Pinardi MSc)	(Dr. Ir. Kuntjoro Pinardi MSc)	

Capaian Pembelajaran (CP)	CPL/SO-Prodi yang dibebankan pada MK – Student Outcome (SO)	
	CPL/SO 1 / SO 1	Mastery of Cybersecurity and Defense Technologies
	CPL/SO 4 / SO 4	Project Management and Practical Application
	Capaian Pembelajaran Mata Kuliah (CO) or Course Objective (CO)	
	CO1: Equip participants with an in-depth understanding of next-generation firewalls and intrusion prevention systems (IPS), pivotal components in contemporary network security. (SO1, SO4)	
	CO2: Provide specialized knowledge and hands-on experience in securing cloud and hybrid networks, addressing these environments' unique challenges. (SO1, SO4)	

CO3: Develop essential skills to protect and analyze complex network environments, focusing on advanced topics and practical applications. (SO1, SO4)

Korelasi CO dan CPL/SO

	SO 1	SO 2	SO 3	SO 4	SO 5	SO 6
CO 1	x			x		
CO 2	x			x		
CO 3	x			x		

Kemampuan akhir tiap tahapan belajar (Sub-CO) – Course Outcome

Sub-CO1: Analyze various network threats and determine how next-generation firewalls and intrusion prevention systems (IPS) can mitigate these threats. (CO1,CO3)

Sub-CO2: Configure and manage next-generation firewalls and IPS to enhance network security. (CO1, CO2)

Sub-CO3: Assess security risks inherent in cloud and hybrid network infrastructures and implement appropriate mitigation strategies.(CO2, CO3)

Sub-CO4 : Design and apply security controls to protect data and resources within cloud and hybrid environments, ensuring compliance with relevant standards and regulations.(CO3)

Korelasi CO terhadap Sub-CO

	Sub-CO1	**Sub-CO2**	**Sub-CO3**	**Sub-CO4**
CO1	X	X		
CO2		X	X	
CO3	X		X	X

Korelasi CPL/SO dan Sub-CO Terhadap Bobot Penilaian

	CPL 1/SO 1	**CPL 2/SO 2**	**CPL 3/SO 3**	**CPL 4/SO 4**	**CPL 5/SO 5**	**CPL 6/SO 6**	**Total Bobot Penilaian (%)**	**Jumlah Minggu**

								(Minggu)
Sub-CO1	**5**	**5**	**0**	**0**	**0**	**0**	**10**	**1**
Sub-CO2	**5**	**5**	**5**	**0**	**0**	**5**	**20**	**2**
Sub-CO3	**0**	**0**	**5**	**5**	**10**	**10**	**30**	**5**
Sub-CO4	**5**	**5**	**5**	**5**	**10**	**10**	**40**	**6**
TOTAL	**15**	**15**	**15**	**10**	**20**	**25**	**100**	**14**

Deskripsi singkat MK	The Advanced Network Security specialization is designed for Network Security Analysts, Information Technology (IT) Managers, or Cybersecurity Consultants to further their understanding of advanced network security techniques. In this 3-course specialization, learners will compare next-generation firewalls with traditional firewalls, analyze use cases of next-generation firewalls in real-world situations, understand the role of intrusion prevention systems in network security, and evaluate the effectiveness of an intrusion prevention system. Learners will also learn to effectively respond to identified threats and design a strategy for ongoing network monitoring and threat response.
Bahan Kajian: Materi Pembelajaran	This specialization is tailored for Network Security Analysts, IT Managers, and Cybersecurity Consultants aiming to deepen their expertise in advanced network security methodologies. Through a series of three comprehensive courses, participants will: 1. Compare Traditional and Next-Generation Firewalls: Understand the distinctions between conventional and next-generation firewalls and evaluate their advantages and limitations. 2. Analyze Real-World Applications: Examine practical implementations of next-generation firewalls, assessing their effectiveness in diverse scenarios. 3. Explore Intrusion Prevention Systems (IPS): Delve into IPS' function in safeguarding networks and critically assess their performance in threat mitigation. 4. Develop Threat Response Strategies: Learn to craft and implement strategies for continuous network monitoring and proactive threat response.

	5. Engaging with this curriculum will enhance learners' ability to design, implement, and manage robust network security infrastructures, ensuring organizational resilience against evolving cyber threats.	
Pustaka	**Utama:**	**Pendukung:**
	1. Network Security Essentials: Applications and Standards – William Stallings, Pearson, 2019.	1. Semua *e-book* dan jurnal-jurnal terkait dengan materi setiap pertemuan 2. Video pembelajaran 3. Info grafis
Dosen Pengampu:	Dr. Ir. Kuntjoro Pinardi, MSc	
MK Prasyarat:	None	

Advanced Network Security Course Plan (14 Weeks)

Week	Sub-CO (Sub-CPMK)	Learning Activities and Assignments	Learning Materials & References	Assessment & Criteria	Weight (%)	Online Learning Mode	Book Chapter Reference
1	**Sub-CO1: Analyze network threats and mitigation using NGFW & IPS**	Lecture: Intro to network threats (1x3x50’). Case study: Recent cyber-attacks. Assignment: Research and report on a threat.	Network threats overview, NGFW & IPS case studies.	Participation in discussion and quality of research report.	5%	Online lecture & discussion, independent study.	Chapter 1: Introduction to Network Security
2	**Sub-CO1: Compare traditional vs next-gen firewalls**	Lecture: NGFW deep dive (1x3x50’). Lab: Basic NGFW configuration. Assignment: Compare NGFW vs conventional firewalls.	NGFW analysis, practical firewall setup.	Performance in lab, depth of comparison report.	5%	Online lecture, lab session, report writing.	Chapter 2: Next-Generation Firewalls

3	**Sub-CO1: Understanding Intrusion Prevention Systems (IPS)**	Lecture: IPS overview (1x3x50’). Lab: IPS implementation. Case study: IPS effectiveness.	IPS functionalities, hands-on IPS setup, case studies.	Lab performance, case study analysis.	5%	Online lecture, lab session, case study discussion.	Chapter 3: Intrusion Prevention Systems
4	**Sub-CO2: Configure and manage NGFW & IPS**	Lecture: Advanced firewall & IPS configurations. Lab: Setting up security policies & rules. Assignment: Develop a security policy.	Advanced firewall/IPS settings, security policy guidelines.	Lab performance, quality of security policy.	5%	Online lecture, lab session, security policy writing.	Chapter 4: Advanced Firewall & IPS Configurations
5	**Sub-CO2: Firewall & IPS monitoring and maintenance**	Lecture: Analyzing logs & alerts. Lab: Incident response using logs. Assignment: Develop a maintenance plan.	Log analysis, security monitoring, maintenance planning.	Performance in log analysis, maintenance plan quality.	5%	Online lecture, lab session, maintenance strategy report.	Chapter 5: Security System Maintenance
6	**Sub-CO3: Security risks in cloud & hybrid networks**	Lecture: Cloud network overview. Discussion: Cloud security risks. Assignment: Risk assessment report.	Cloud infrastructure security, risk management techniques.	Risk assessment accuracy, discussion participation.	10%	Online lecture, discussion, risk analysis report.	Chapter 6: Cloud Network Security
7	**Sub-CO3: Mitigating cloud security risks**	Lecture: Mitigation strategies for cloud threats. Lab: Implementing cloud security controls. Assignment: Develop a mitigation plan.	Cloud security controls, compliance strategies.	Lab performance, mitigation plan quality.	10%	Online lecture, lab session, mitigation strategy writing.	Chapter 7: Cloud Security Mitigation

8	**Sub-CO4: Compliance standards in cloud security**	Lecture: Compliance regulations. Case study: Compliance failures. Assignment: Develop a compliance checklist.	Cloud compliance frameworks, legal case studies.	Quality of compliance checklist, discussion participation.	10%	Online lecture, discussion, compliance checklist development.	Chapter 8: Compliance in Cloud Security
9	**Sub-CO4: Designing security controls for cloud data protection**	Lecture: Security control implementation. Lab: Data encryption & access control setup. Assignment: Evaluate security controls.	Data protection strategies, encryption implementation.	Lab performance, evaluation report quality.	10%	Online lecture, lab session, security effectiveness analysis.	Chapter 9: Data Protection Strategies
10	**Sub-CO4: Incident response planning for cloud environments**	Lecture: Incident response framework. Case study: Real-world cloud breaches. Assignment: Develop an incident response plan.	Incident response case studies, security framework best practices.	Incident response plan quality, case study analysis.	10%	Online lecture, case study discussion, response plan writing.	Chapter 10: Incident Response and Forensics
13-Nov	**Capstone Project: Securing Enterprise Network & Cloud Infrastructure**	Group project: Implement security measures on hybrid networks. Mentoring sessions. Final project submission & presentation.	Enterprise security planning, threat simulation exercises.	Project implementation accuracy, report & presentation quality.	20%	Weekly mentoring, peer review, group discussions.	Multiple chapters relevant to project scope.

14	**Final Exam & Reflection**	Written exam covering Sub-CO1-4. Discussion: Key takeaways & future learning.	Exam review materials, student reflections.	Exam performance, engagement in reflection session.	10%	Online proctored exam, discussion forum participation.	Comprehensive review of all chapters.

Rubric for Presentation Assessment (Perception-Based)

Aspect Assessed	Very Poor	Poor	Adequate	Good	Excellent
	< 20	21 – 40	41 – 60	61 – 80	> 80
Communication Skills (15%)					
Mastery of Content (15%)					
Ability to Answer Questions (15%)					
Use of Visual Aids (5%)					
Accuracy in Problem-Solving (50%)					
FINAL SCORE					

Rubric for Observation-Based Assessment

Aspect Assessed	Very Poor	Poor	Adequate	Good	Excellent
	< 20	21 – 40	41 – 60	61 – 80	> 80
Fieldwork Engagement (20%)					
Mastery of Subject Matter (20%)					
Ability to Select Relevant Observation Data (30%)					

Ability to Correlate Observations with Project Solutions (30%)					
FINAL SCORE					

Rubric for Oral Exam and Class Participation Assessment

Aspect Assessed	**Very Poor**	**Poor**	**Adequate**	**Good**	**Excellent**
	< 20	21 – 40	41 – 60	61 – 80	> 80
Class Activity/Participation (20%)					
Mastery of Subject Matter (35%)					
Accuracy in Answering Questions (45%)					
FINAL SCORE					

Rubric for Performance-Based Assessment and Written Test

Aspect Assessed	**Very Poor**	**Poor**	**Adequate**	**Good**	**Excellent**
	< 20	21 – 40	41 – 60	61 – 80	> 80
Ability to Develop a Comprehensive Performance Plan (20%)					
Mastery of Subject Matter (35%)					
Ability to Solve Cases or Projects Based on Performance Plan (45%)					
FINAL SCORE					