



Identification du module

Numéro du module	233	
Titre	Protéger et assurer la maintenance des réseaux	
Compétences	Intègre et configure un pare-feu pour assurer la protection d'un réseau. Effectue des travaux de maintenance sur un pare-feu conformément à un ordre et documente les mesures de sécurité prises.	
Objectifs opérationnels	1.	Clarifie les menaces actuelles pour la sécurité d'une infrastructure informatique en réseau.
	2.	Intègre un pare-feu physique selon l'ordre.
	3.	Etablit des règles de pare-feu simples (filtre de port).
	4.	Configure des fonctions avancées d'un pare-feu.
	5.	Met en service des connexions VPN.
	6.	Connecte les services d'authentification à un pare-feu.
	7.	Effectue des travaux de maintenance sur un pare-feu.
	8.	Configure un WLAN sécurisé.
	9.	Documente les mesures de sécurité d'une manière compréhensible et formellement correcte.
Champ de compétences	Security / Risk Management	
Objet	Sécurité du réseau dans une PME	
Justificatif		
Année d'apprentissage	2	
Conditions préalables		
Champ de compétences		
Charge de travail/Leçons	40	
Homologation	CFC	
Compétences opérationnelles	a2 : Vérifier les exigences techniques, la sécurité informatique et la protection des données pour un projet ACM simple et les consigner dans un cahier des charges	
Informaticien/ne du bâtiment CFC	d1 : Mettre en place les réseaux de données pour les systèmes de communication et les systèmes multimédia et procéder à des extensions	
	d2 : Installer les composants des systèmes de communication et des systèmes multimédia	
	d3 : Configurer les composants des systèmes de communication et des systèmes multimédia	
	d7 : Mesurer, analyser les réseaux de données et corriger les défauts	
	f4 : Assurer la maintenance et l'entretien des systèmes ACM	



Connaissances opérationnelles requises

Les connaissances opérationnelles requises décrivent les connaissances qui soutiennent l'exécution compétente des opérations d'un module. Ces connaissances servent à l'orientation et ne sont pas définies de manière exhaustive. La concrétisation des objectifs de formation qui en résulte et la détermination du parcours de formation pour l'acquisition des compétences sont de la responsabilité des prestataires de formation.

Numéro du module		233	
Titre		Protéger et assurer la maintenance des réseaux	
Champ de compétences		Security / Risk Management	
Objectifs opérationnels et connaissances opérationnelles requises	1	1.1	Connaît les critères de sécurité communs des systèmes d'information, les différents niveaux de menaces et les aspects de sécurité importants (par ex. juridiques, organisationnels, techniques, physiques).
		1.2	Connaît différentes procédures de transmission sécurisée des données (par ex. cryptage asymétrique et symétrique).
		1.3	Connaît les méthodes permettant de diviser un réseau en zones de sécurité.
		1.4	Connaît les procédures permettant de vérifier la sécurité technique d'un réseau.
	2	2.1	Connaît les possibilités d'accès à un pare-feu et ses configurations de base (par ex. les interfaces, l'adressage IP).
		2.2	Connaît les fonctions des paramètres réseau avancés (par ex. passerelle, routage, VLAN, DHCP).
	3	3.1	Connaît la procédure d'un pare-feu pour le filtrage des ports et le principe du Stateful Packet Inspection (SPI).
		3.2	Connaît les propriétés des protocoles de réseau importants et de leurs ports UDP/TCP.
		3.3	Connaît une procédure pour établir des règles afin de les appliquer de manière directionnelle entre les zones de sécurité.
		3.4	Connaît la manière de fonctionner de NAT.
	4	4.1	Connaît des fonctions avancées (par ex. antivirus, filtre web, filtre d'application) d'un pare-feu.
		4.2	Connaît les exigences des fonctions étendues pour les connexions cryptées.
	5	5.1	Connaît les caractéristiques des différentes topologies du VPN (par ex. site à site, client à site).
		5.2	Connaît les protocoles courants (par ex. IPSec, SSL) pour les connexions VPN.
		5.3	Connaît les paramètres nécessaires à la mise en place d'un tunnel VPN.



Objectifs opérationnels et connaissances opérationnelles requis	6	6.1	Connaît la manière de fonctionner des différentes méthodes d'authentification (par ex. locale, RADIUS, LDAP, authentification à deux facteurs).
		6.2	Connaît les exigences pour connecter un service d'authentification à un pare-feu.
		6.3	Connaît les paramètres permettant d'inclure des informations personnelles et de groupe dans le pare-feu.
	7	7.1	Connaît la manière de procéder pour sauvegarder et restaurer la configuration d'un pare-feu.
		7.2	Connaît la méthodologie et les exigences d'une mise à jour de pare-feu.
		7.3	Connaît des formats de présentation pour la documentation des règles de pare-feu.
	8	8.1	Connaît différents standards de cryptage WLAN (par ex. WPA3).
		8.2	Connaît différentes méthodes d'authentification WLAN (par ex. PSK, IEEE 802.1x).
	9	9.1	Connaît l'importance de la documentation pour garantir et assurer la traçabilité des résultats du travail.
		9.2	Connaît les règles de contenu et de forme les plus importantes qui doivent être respectées lors de la documentation des résultats du travail.