

*FIREWALL : principe, mise en oeuvre, limites. L'accès Internet des utilisateurs. Protection anti-virus, Interconnexion. Détection d'intrusions.*

---

<p><u>Public ou prérequis</u> <i>techniciens ou administrateurs réseaux</i></p> <p><u>Activités principales</u> <i>Les logiciels de scan avancés et sniffers : NMAP + ethereal</i></p> <p><i>La sécurisation des communications Web : SSL + IIS.</i></p> <p><i>configuration de base d'une solution open source : Shorewall</i></p> <p><i>Mise en place d'un VPN : openVPN + openSSL</i></p>	<p><b>Notions essentielles :</b> Le modèle TCP/IP</p> <p><b>Les attaques :</b> Fuite ou vol d'information, violation d'intégrité, authentification des messages. Les virus typologie des attaques par le réseau. Comment détecter les symptômes d'une intrusion.</p> <p><b>DMZ :</b> La mise en place de solutions DMZ (zones démilitarisées). Comment calculer le nombre de DMZ nécessaires. Les solutions DMZ sécurisées ; combien de DMZ ?</p> <p><b>Firewalls :</b> Comment se protéger des serveurs, des clients, de l'Internet. Comment sélectionner le firewall le mieux adapté à vos contraintes : - les différents types de firewall - les critères de sélection. Les firewalls : quelle exploitation au quotidien ? Quelle ressource nécessaire pour administrer et exploiter les firewalls ?</p> <p><b>VPN :</b> Notions essentielles. Les différents protocoles.</p>	D E L P H E S
--	--	---------------------------------

**Ce programme est personnalisable et adaptable en fonction de vos besoins.**

Tél. 04 94 16 90 70 [www.delphes-france.net](http://www.delphes-france.net) Fax. 04 94 16 90 77