



## FORMATION : SÉCURITÉ

### DS-125 : Sécuriser un réseau à la norme 802.1x (2 jours)

#### Logiciels utilisés

Linux, FreeRadius, OpenLDAP et OpenSSL

#### Introduction

La simplicité des réseaux Ethernet rend la connexion et l'accès aux ressources informatiques possible par le simple branchement d'une prise. Mais ce qui est souhaitable pour vos utilisateurs ne l'est pas forcément pour les autres. La norme **IEEE 802.1X** est le standard qui définit le contrôle d'accès aux réseaux Ethernet. A la différence de la plupart des autres mécanismes de protection, le 802.1X intervient dès la **connexion physique** sur le port du commutateur. L'authentification est ainsi effectuée avant tout autre service, y compris les services d'auto-configuration du réseau (DHCP, PXE, Active Directory, etc ...). On obtient ainsi une protection beaucoup plus fiable que les restrictions basées sur du filtrage par adresses IP ou par adresses MAC.

L'authentification des équipements ou des utilisateurs est généralement basée sur le protocole RADIUS. En plus d'autoriser ou de refuser l'accès au réseau, il est possible de **définir des droits d'accès** et des **groupes d'utilisateurs**, afin d'assigner des droits différents aux différentes populations d'utilisateurs. Sur un même port réseau, ou sur une même connexion WiFi, on distingue ainsi les visiteurs ponctuels des salariés (par exemple). Certains équipements réseau permettent d'aller plus loin. Il est notamment possible de contrôler la présence de certains logiciels sur le poste de travail (comme par exemple un anti-virus à jour) avant de donner accès au réseau.

#### Objectifs

Ce stage permet aux administrateurs réseaux et sécurité de comprendre l'ensemble des spécificités de la sécurité des réseaux filaires et sans fil, en terme de contrôle d'accès et d'authentification des utilisateurs. Ils pourront ensuite appréhender la mise en place d'un réseau filaire sécurisé à la norme 802.1x en ayant recours à un serveur Radius, une base d'utilisateur LDAP et des certificats numériques.

#### Public Concerné

Administrateur réseaux/sécurité

#### Compétences nécessaires

Installer et configurer FreeRadius

Installation et configuration de réseaux filaires Ethernet

#### Programme

JOUR 1 – Sécurité des réseaux locaux et présentation de 802.1x	JOUR 2 – Maquettes en environnement CISCO
<p>Définition, terminologie et rappels lexicaux</p> <ul style="list-style-type: none"> <li>● Les enjeux de la sécurité du LAN</li> <li>● Présentation et comparaison des différents modes de protection des accès (libre accès, portail captif, 802.1x)</li> <li>● Principe du 802.1x</li> </ul> <p>Contrôle d'accès et authentification avec 802.1x</p> <ul style="list-style-type: none"> <li>● Principes de fonctionnement</li> <li>● Bénéfices et contraintes</li> <li>● Rappels sur Radius</li> <li>● Présentation et comparaison des différents modes d'authentification</li> <li>● Compatibilité des différents OS avec 802.1x</li> <li>● Exemples de déploiement et bonnes pratiques</li> </ul>	<p>Maquette – FreeRadius simple</p> <ul style="list-style-type: none"> <li>● Installation et configuration d'un serveur FreeRadius pour 802.1x</li> <li>● Configuration du 802.1x sur commutateurs réseau pour authentification sur adresse MAC</li> </ul> <p>Maquette – FreeRadius + OpenLDAP</p> <ul style="list-style-type: none"> <li>● Installation et configuration d'un serveur FreeRadius pour 802.1x avec base d'utilisateur LDAP</li> <li>● Configuration du 802.1x sur commutateurs réseau pour authentification sur login / mot de passe</li> <li>● Gestion de groupes d'utilisateurs</li> </ul>

Le programme ci-dessus présente le scénario initial de la formation DS-122 d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin. Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.