DAWAN

Plan de la formation

www.dawan.fr

Formation Cisco ISE - Contrôle d’accès réseau, authentification et segmentation

Durée :	5 jours (35 heures)
Tarif inter-entreprises :	3 775,00 € HT (Présentiel) 3 020,00 € HT (Distanciel)
Public :	Administrateurs et ingénieurs réseaux et sécurité - Intégrateurs chargés du contrôle d’accès réseau - Techniciens confirmés assurant l’exploitation de Cisco ISE
Pré-requis :	Maîtriser les réseaux de niveau CCNA, les VLAN et les ACL - Savoir administrer un commutateur Cisco en ligne de commande - Connaître Active Directory, DNS, NTP et les principes des certificats - Comprendre les rôles de RADIUS, de 802.1X et des mécanismes AAA
Objectifs :	Préparer un déploiement Cisco ISE et ses services d’identité - Configurer l’authentification 802.1X et les accès MAB - Appliquer des politiques d’autorisation et de segmentation - Mettre en place un accès invité et contrôler son cycle de vie - Centraliser l’administration des équipements avec TACACS+ - Diagnostiquer les échecs d’authentification et les décisions de politique
Modalités pédagogiques, techniques et d’encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l’Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l’environnement adéquat. • Un formateur expert.

Modalité d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	RéS103122-F
Note de satisfaction des participants :	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Préparer l’architecture et le déploiement ISE

Cas d’usage du contrôle d’accès réseau et périmètre du projet
Rôles PAN, PSN et MnT, déploiements autonomes ou distribués
Dépendances DNS, NTP, certificats, annuaires et équipements d’accès
Dimensionnement, licences et stratégie de disponibilité

Atelier pratique : vérifier une architecture préparée et réaliser les contrôles de configuration initiale

Intégrer les identités et les certificats

Utilisateurs internes, groupes et annuaires Active Directory ou LDAP
Chaîne de confiance, certificats serveur et certificats clients
Sélection des sources d’identité et règles de correspondance
Préparation d’EAP-TLS et principes de TEAP

Atelier pratique : intégrer l’annuaire, installer les certificats et valider l’identité d’un poste de test

Mettre en œuvre 802.1X et MAB

Échanges entre terminal, équipement d’accès et serveur RADIUS
Configuration du commutateur et du supplicant
Règles d’authentification et d’autorisation dans les policy sets
Terminaux sans 802.1X, limites du MAB et accès de secours

Atelier pratique : authentifier un poste en EAP-TLS et encadrer l’accès MAB d’un terminal déclaré

Profiler les terminaux et segmenter les accès

Sondes de profilage, attributs collectés et fiabilité des classifications
VLAN dynamiques, ACL téléchargeables et profils d’autorisation
Principes TrustSec : groupes de sécurité, SGT et règles SGACL
Réévaluation d’une session et Change of Authorization

Atelier pratique : appliquer deux niveaux d’accès et vérifier leur modification après réauthentification

Organiser les accès invités et les équipements personnels

Portails invités, comptes sponsorisés et durées de validité
Redirection web, conditions d’accès et séparation des visiteurs
Principes d’enrôlement BYOD et cycle de vie des certificats
Présentation de la posture, de la conformité et de la remédiation

Atelier pratique : créer un accès invité temporaire puis vérifier sa révocation et sa traçabilité

Centraliser l’administration avec TACACS+

Distinction entre contrôle d’accès réseau et administration des équipements
Authentification, autorisation de commandes et journalisation AAA
Profils administrateurs, ensembles de commandes et moindre privilège
Accès de secours et protection des échanges d’administration

Atelier pratique : autoriser un opérateur à consulter un commutateur tout en bloquant les modifications

Exploiter et dépanner la plateforme

Live Logs, rapports RADIUS/TACACS+ et suivi des sessions
Diagnostic des erreurs d’annuaire, de certificat et de politique
Sauvegardes, renouvellement des certificats et préparation des mises à jour
Bascule des services et comportement des équipements en cas d’indisponibilité

Atelier pratique : résoudre plusieurs refus d’accès provoqués et vérifier le fonctionnement d’un serveur RADIUS secondaire

Construire un déploiement progressif

Inventaire des terminaux et définition des populations pilotes
Passage de l’observation à l’application des restrictions
Tests d’acceptation, gestion des exceptions et procédure de retour arrière

Atelier pratique : produire et tester une matrice d’accès pour salariés, visiteurs et équipements techniques