

Formation Cisco : Concevoir et sécuriser un réseau multisite

■ Durée :	3 jours (21 heures)
■ Tarif inter-entreprises :	2 275,00 CHF HT (Présentiel) 1 820,00 CHF HT (Distanciel)
■ Public :	Administrateurs réseaux - Ingénieurs réseaux - Responsables d'infrastructure - Techniciens chargés de l'interconnexion et de l'exploitation de sites distants
■ Pré-requis :	Posséder les connaissances réseau du CCNA ou un niveau équivalent - Savoir configurer VLAN, routage IPv4 et ACL sur Cisco IOS ou IOS XE - Connaître les principes d'IPv6, de NAT et des VPN
■ Objectifs :	Traduire les besoins d'une organisation en architecture réseau multisite - Concevoir l'adressage, la segmentation et le routage - Mettre en œuvre des VPN IPsec entre sites - Protéger les flux et les accès administratifs - Tester la disponibilité, la qualité de service et l'exploitabilité de l'architecture
■ 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 :	RÉS100095-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

Cadrer le projet et choisir une architecture

Identifier sites, utilisateurs, applications et flux critiques
Définir les besoins de sécurité, disponibilité et performance
Comparer topologies centralisées, maillées et principes SD-WAN
Choisir les accès WAN et préciser les responsabilités d'exploitation

Atelier pratique : produire un schéma d'architecture à partir du cahier des charges d'une PME

Concevoir l'adressage, la segmentation et le routage

Construire un plan IPv4/IPv6 cohérent et évolutif
Organiser VLAN, zones d'administration, DMZ et VRF selon les besoins
Choisir routes statiques, routage dynamique et mécanismes de secours
Intégrer les besoins DHCP, DNS et accès aux services partagés

Atelier pratique : définir le plan d'adressage, les flux autorisés et les routes de trois sites

Interconnecter les sites avec IPsec

Comprendre IKEv2, associations de sécurité et authentification des pairs
Configurer des tunnels IPsec routés avec interfaces VTI
Vérifier le routage, le chiffrement et les échanges intersites
Diagnostiquer les interactions avec NAT, MTU et MSS

Atelier pratique : établir des VPN intersites et résoudre un défaut de négociation ou de routage

Sécuriser les échanges et l'administration

Définir une matrice de flux et appliquer les ACL adaptées
Séparer les accès utilisateurs, serveurs et administration
Protéger les accès SSH et centraliser l'authentification
Organiser la journalisation et les sauvegardes de configuration

Atelier pratique : appliquer la politique de filtrage et vérifier les accès autorisés et refusés

Assurer la continuité et la qualité de service

Concevoir la redondance des accès et des passerelles
Configurer suivi d'objets, IP SLA et routes de secours
Classer et marquer les flux ; présenter files prioritaires et shaping
Évaluer l'effet des coupures, pertes et saturations sur les applications

Atelier pratique : simuler une panne WAN et observer l'effet d'une politique QoS préconfigurée sur les communications prioritaires

Superviser, recetter et documenter l'infrastructure

Exploiter syslog, SNMPv3 et les flux NetFlow/IPFIX
Construire une matrice de tests de connectivité et de sécurité
Mesurer les résultats et consigner les limites observées
Formaliser le dossier d'exploitation et le plan de retour arrière

Atelier de synthèse : déployer la maquette multisite, réaliser sa recette et présenter le dossier technique