Configuration de radius pour une borne WI-FI

Lancer le service et faite clic droit sur NPS

Inscrire le serveur dans l'Active directory sinon il sera impossible de définir les conditions liées aux groupes/utilisateurs dans la stratégie d'accès distant !



Création d'un nouveau client radius sur la console NPS, clic droit **nouveau** Nom de la borne : wap121 adresse de la borne : 192.168.1.250

Secret : Que vous avez définit sur la borne en amont

THE SECOND PADRIC	Clients RADIUS
Clients et serveurs KADIUS Clients RADIUS Groupes de serveurs RADIUS distants	Les clients RADIUS vous permettent de spécifier les serveurs d'accès réseau qui fournissent l'accès à votre réseau.
 Stratégies de demande de connexion Stratégies réseau Stratégies de contrôle d'intégrité 	Nom convivial Adresse IP Fabricant du périphérique Compatible avec la protection d'accès réseau (NAP) État wap41e9c0 192.168.90.39 RADIUS Standard No Activé
Gestion des modèles	Propriétés de wap41e9c0
	Paramètres Avancé
	Activer ce client RADIUS
	Sélectionner un modèle existant :
	APWap307
	Nom et adresse
	wap41eSc0
	Adresse (IP ou DNS) :
	192.168.90.39 Vérifier
	Secret partagé
	Aucun
	Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.
	Manuel Générer
	Secret partagé :
	•••
	Confirmed to second and and

Configuration de la stratégie réseau nouvelle stratégie réseau nom de la stratégie : Wifi



Nous ajouterons le Groupes utilisateurs du domaine

Condition Groupes of	l'utilisateurs	Valeur AIS\Utilia	ateurs du do	maine			

Sélectionner **MS-CHAP v2** et **MS-CHAP** pour authentification par mot de passe. Monter Le protocole **Microsoft EAP** Extended Authentication Protocol.

			Propriétés de Wifi_Cisco	
Vue d'ensemble	Conditions	Contraintes	Paramètres	
Configurez les co Si la demande de Contraintes :	ontraintes de e connexion	cette stratégi ne répond pa	s réseau. à toutes les contraintes, l'accès réseau est refusé.	
Contraintes	a d'authentifi activité spiration de	cation	Autorisez l'accès uniquement aux clients qui s'authentifient à l'aide des spécifiées. Les types de protocoles EAP sont négociés entre le serveur NPS et le l'ordre dans lequel ils sont listés. Types de protocoles EAP :	s méthodes client dans
 session ID de la station appelée Restrictions relatives aux jours et aux heures 	Microsoft: PEAP (Protected EAP)	Monter		
		Descendre		
Type de p	sort NAS		Ajouter Modifier Supprimer Méthodes d'authentification moins sécurisées : Authentification chiffrée Microsoft version 2 (MS-CHAP v2) I L'utilisateur peut modifier le mot de passe après son expiration Authentification chiffrée Microsoft (MS-CHAP) I L'utilisateur peut modifier le mot de passe après son expiration Authentification chiffrée Microsoft (MS-CHAP) I L'utilisateur peut modifier le mot de passe après son expiration Authentification chiffrée (CHAP) Authentification on chiffrée (PAP, SPAP) Autoriser les clients à se connecter sans négocier une méthode d'a Vérifier uniquement l'intégrité de l'ordinateur	uthentification
			ОК	Annuler Appliquer

Sélectionner **Sans fil – IEEE 802.1** si ce n'est pas un accès sans fil, la demande de connexion est rejetée.

	Nouvelle stratégie réseau
Les doiv Serv conf	nfigurer des contraintes contraintes sont des paramètres supplémentaires de la stratégie réseau, auxquels les demandes de connexior ent se conformer. Si une demande de connexion ne répond pas à une contrainte, le serveur NPS (Network Po er) rejette automatiquement cette demande. Les contraintes sont facultatives ; si vous ne souhaitez pas igurer de contraintes, diquez sur Suivant.
Configurez les contrai Si la demande de cor	ntes de cette stratégie réseau. mexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.
Contraintes Contra	ité Spécifier les types de médias d'accès nécessaires pour correspondre à cette stratégie ité Types de tunnels pour connexions d'accès à distance et VPN standard Asynchrone (Modem) RNIS synchrone Synchrone (ligne T1) Virtuel (VPN) Varies Types de tunnels pour connexions 802.1X standard In Cible VAS Asynchrone (Igne T1) Varies Types de tunnels pour connexions 802.1X standard In Types de tunnels pour connexions 802.1X standard VAS Cible
	Précédent Suivant Terminer Annuler