

Historique des versions :

Révision	Date	Objet
1.0.1	02/12/2024	Création du document
1.0.2	02/12/2024	Corrections et mise en forme du document

Auteurs et Intervenants :

Initiales	Nom	Fonction	Organisation - Rôle
ҮК	Youssouf KEITA	Apprenti	BTS-SIO IIA LAVAL

Identification du document :

Document applicable	à compter du 02 Déce	mbre 2024	
	Identification d	u document	
Direction:	IIA Saint-Berthevin / B	TS 2eme année	
Objet:	Installation serveur NP	S sous Windows serveu	ır 2022
Domaine:	Architecture technique		
Nature:	Procédure d'installation	1	
N° d'ordre:	0001	Version:	1.0.1
Durée installation	Environ 2 heures.		
Nb pages:	44		
Nom fichier:	Procedure_Installation_	_SRV-NPS_V-1.odt	
Format document:	ODT réalisé avec Libre	e Office	



Architecture Système

Procédure techniques Déploiement serveur NPS sous Windows 22

Table des matières :

I. Objectif du document :		2
II. Caractéristique générale :		2
III. Pré-requis :		3
IV. À qui s'adresse ce docum	ient ?	3
V. Que ce qu'un relais O365	du fichier main.cf de postfix ?	3
IV. Mise en place de serveur	de relais Office 365 via postfix:	3
1. Configuration réseau :.	1	3
2. Mise à jour des paquets	5 :	4
3. Installation postfix :		4
4. Configuration du fichie	er « main.cf » de Postfix :	5
5. Configuration du fichie	er « sasl passwd » :	7
6. Configuration du fichie	er « sender canonical maps » :	7
7. Configuration du fichie	er « header check » :	7
8. Configuration du fichie	er « mailname » :	8
9. Redémarrer le service r	postfix :	8
10. Tester le fonctionnem	ent :	8

I. Objectif du document :

Fournir un guide clair et structuré pour installer, configurer et sécuriser un serveur NPS (Network Policy Server), assurant l'authentification et l'autorisation des connexions réseau tout en facilitant son utilisation, sa maintenance et son transfert de compétences à d'autres administrateurs.

II. Caractéristique générale :

Expression des besoins :

Mettre en place une solution interne pour gérer et sécuriser l'accès au réseau via des politiques centralisées d'authentification et d'autorisation. Cela inclut la prise en charge des utilisateurs distants et locaux, la compatibilité avec les services existants (Active Directory, DNS, etc.), et la protection contre les accès non autorisés.

1- Authentification et autorisation centralisées :

Configurer un serveur NPS pour gérer les demandes d'accès réseau à partir de clients RADIUS, comme les points d'accès Wi-Fi, les VPN, ou les commutateurs Ethernet.

2- Sécurisation des connexions :

Protéger les échanges grâce à des méthodes d'authentification robustes (EAP, PEAP) et en chiffrant les communications entre le serveur NPS et les clients réseau.



3- Personnalisation et gestion des politiques :

Définir des règles spécifiques basées sur les groupes d'utilisateurs Active Directory, l'emplacement des clients, ou les heures d'accès, tout en surveillant les connexions réseau pour détecter les abus ou les anomalies.

III. Pré-requis :

- Un serveur Windows Server 2022 intégré à un domaine Active Directory.
- Accès administrateur pour gérer les rôles et fonctionnalités. •
- Configuration réseau fonctionnelle avec DNS et IP statiques.

IV. À qui s'adresse ce document ?

Compte tenu de sa nature technique, cette documentation est destinée aux techniciens informatiques ayant de solides compétences en systèmes et réseaux, ainsi qu'une compréhension approfondie des environnements Microsoft Windows Serveur. Les connaissances en gestion des rôles réseau (RADIUS, VPN) et des services Active Directory sont également essentielles.

V. Que ce qu'un serveur NPS sous Windows Server 2022 ?

Un NPS (Network Policy Server) sous Windows Serveur 2022 est le rôle serveur Microsoft qui permet de centraliser l'authentification, l'autorisation, et la gestion des comptes (AAA : Authentication, Authorization, Accounting) pour les connexions réseau. Il agit comme un serveur RADIUS, fournissant un point unique de contrôle pour appliquer des politiques d'accès réseau.

Fonctionnement :

IV. Installation des rôles et les fonctionnalités NPS via via Windows server 22:

1. Configuration réseau :

Nom de serveur :	SRV-NPS
Vlan :	0526
Nom de domaine :	Dom.test.fr (samba)



Architecture Système	Ref : DOC_procedure_NPS
Procédure techniques Déploiement serveur NPS sous Windows 22	Version 1.0.0 Date:02/12 /2024 Page:1/44

Adresse IP :	172.17.2.2
Masque :	255.255.255.0
Passerelle :	172.17.2.254
DNS :	10.223.255.2

2.Installation des rôles :

Pour installer un serveur NPS (Network Policy Server) à l'aide du Gestionnaire de serveur :

- Sur le serveur NPS, dans le Gestionnaire de serveur, cliquez sur Gérer, puis sur Ajouter des rôles et des fonctionnalités. L'Assistant Ajout de rôles et de fonctionnalités s'ouvre.
- Dans Avant de commencer, cliquez sur Suivant.
- Dans Sélectionner le type d'installation, vérifiez que Installation basée sur un rôle ou une fonctionnalité est sélectionné, puis cliquez sur Suivant.
- Dans Sélectionner le serveur de destination, vérifiez que Sélectionner un serveur du pool de serveurs est sélectionné. Dans Pool de serveurs, vérifiez que l'ordinateur local est sélectionné. Cliquez sur Suivant.
- Dans Sélectionner des rôles de serveurs, dans Rôles, sélectionnez Services de stratégie et d'accès réseau. Une boîte de dialogue s'ouvre pour demander s'il faut ajouter les fonctionnalités requises pour les services de stratégie et d'accès réseau. Cliquez sur Ajouter les fonctionnalités, puis sur Suivant.

voYeev Kra	Architecture Système	Ref : DOC_procedure_NPS
BTS SIO IIA LAVAL	Procédure techniques Déploiement serveur NPS sous Windows 22	Version 1.0.0 Date:02/12 /2024 Page:1/44

📥 Assistant Ajout de rôles et de fon	ctionnalités	– 🗆 X
 Assistant Ajout de rôles et de fon Sélectionner des ro Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Services de stratégie et d' Confirmation Résultats 	ctionnalités Sélectionnez un ou plusieurs rôles à installer sur le serveur sélecti Rôles Accès à distance Accès à distance Attestation d'intégrité de l'appareil Hyper-V Serveur DHCP Serveur DHCP Serveur DHCP Serveur DHCP Serveur DHS Service Sudian hôte Services AD DS CActive Directory Lightweight Dire Services AD LDS (Active Directory Rights Manage Services AD LDS (Active Directory Rights Manage Services d'activation en volume Services d'activation en volume Services de fédération Active Directory Services de fédération Active Directory Services de fédération Active Directory Services de fédération Active Directory Services de fédération Active Directory (AD FS) Newsces de fédération Active Directory (AD FS) Services de fédération Active	- X SERVEUR DE DESTINATION SRV-NPS.dom.test.fr ionné. Description Les services de stratégie et d'accès réseau fournissent un serveur NPS (Network Policy Server) qui contribue à garantir la sécurité de votre réseau.
	< Précédent Suivant	> Installer Annuler

• Dans la page fonctionnalités, cliquez sur Suivant.

Server des fonctionnalités Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Ponctionnalité Services de stratégie et d' Confirmation Résultats Services de stratégie et d' Confirmation Cient TFIP Cient TFIP Cient TFIP Cient TFIP Cient Telhet Cient Tel	📥 Assistant Ajout de rôles et de fonc	tionnalités	- 🗆 X
☐ DirectPlay ☐ Enhanced Storage ☐ Équilibrage de la charge réseau ✓ < >	Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Services de stratégie et d' Confirmation Résultats	tionnalités Sélectionnez une ou plusieurs fonctionnalités à installer sur le se Fonctionnalités Mentivirus Microsoft Defender (Installé(s)) Assistance à distance Base de donnés interne Windows BranchCache Chiffrement de lecteur BitLocker Client d'impression Internet Client for NFS Client FIP Clustering de basculement Collection des événements de configuration et de Compression differentielle à distance Conteneurs Data Center Bridging Devernouillage réseau BitLocker	- L X SERVEUR DE DESTINATION SRV-NPS.dom.test.fr erveur sélectionné. Description .NET Framework 4.8 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud.
		DirectPlay Enhanced Storage fauilibrage de la charge réseau	

• À l'étape « Services de stratégie et d'accès réseau », faites « Suivant ».

voJeour Kr.	Architecture Système	Ref : DOC_procedure_NPS
	Procédure techniques	Version 1.0.0 Date:02/12 /2024
BTS SIO IIA LAVAL	Déploiement serveur NPS sous Windows 22	Page:1/44

ᡖ Assistant Ajout de rôles et de fo	nctionnalités	-		×
Assistant Ajout de rôles et de foi Services de straté Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Services de stratégie et d' Confirmation Résultats	nctionnalités Gie et d'accès réseau Les services de stratégie et d'accès réseau vous permettent de définir et d'appl d'accès réseau, d'authentification et d'autorisation à l'aide du serveur NPS (Net À noter : • Vous pouvez déployer NPS comme un serveur et un proxy RADIUS (Remote User Service). Après l'installation du serveur NPS au moyen de cet Assistant, NPS à partir de la page d'accueil NPAS en utilisant la console NPS.	– serveur des srv-n iquer des str work Policy Authenticat vous pouve:	DESTINATI IPS.dom.tes ratégies Server). ion Dial-It	X on tfr
	< Précédent Suivant >	nstaller	Annule	er

À l'étape « Cofirmation », faites « Suivant ». ٠

📥 Assistant Ajout de rôles et de fon	ctionnalités	-		×
Progression de l'in	stallation	SERVEUR DE SRV-N	DESTINATI	ON It.fr
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs	Afficher la progression de l'installation Installation de fonctionnalité Installation démarrée sur SRV-NPS.dom.test.fr			
Fonctionnalités Services de stratégie et d' Confirmation Résultats	Outils d'administration de serveur distant Outils d'administration de rôles Outils de la stratégie réseau et des services d'accès Services de stratégie et d'accès réseau			
	Vous pouvez fermer cet Assistant sans interrompre les tâches en leur progression ou rouvrez cette page en cliquant sur Notificatio commandes, puis sur Détails de la tâche. Exporter les paramètres de configuration	cours d'exécution. ons dans la barre d	. Examine: le	z
	< Précédent Suivant >	Installer	Annule	žr

- ٠
- Après l'installation, vous pouvez cliquer sur Fermer . Ajouter le serveur NPS au domaine Active Directory. ٠



V. Configuration des clients RADIUS :

1. Déclarer les switchs et points d'accès comme clients RADIUS :

Ouvrez la console NPS :

Pour ce faire :

• Cliquez sur le menu « **Démarrer** », taper dans la barre de recherche « **NPS** », puis cliquer dessus pour l'ouvrir.



• Ensuite la page configuration du serveur **NPS** s'ouvre.



 Développer le dossier Clients et serveurs RADIUS, faites un clic droit sur « Clients RADIUS », puis faites « Nouveau ».

"Yer Ke	Architecture Système	Ref : DOC_procedure_NPS
	Procédure techniques	Version 1.0.0 Date:02/12 /2024
BTS SIO IIA LAVAL	Deptotement serveur 1415 sous windows 22	Page:1/44



 Dans notre cas, le commutateur est un Cisco compatible 802.1x. Les éléments à renseigner sont : le nom "Convivial" du client-RADIUS (SW-01) , son adresse IP (172.16.11.1 et "secret partagé" entre le serveur RADIUS et le client RADIUS, ici la chaîne "Not..."

	Avancé			
Activer	e client RADIU	s		
Sélectio	nner un modèle	evietant :		
Jerectio	niner an modele	existent .		
Nom et ad	resse			
Nom conv	rivial :			
SW-01				
Adresse (I	P ou DNS) :			
172.16.1	1.1			Vérifier
Secret par	tagé			
Secret par Sélectionr	tagé nez un modèle d	le secrets partagé	s existant :	
Secret par Sélectionr Aucun	tagé nez un modèle c	le secrets partagé	s existant :	
Secret par Sélectionr Aucun Pour taper automatiq client RAL respecten	tagé nez un modèle o manuellement uement un secr DIUS avec le mo t la casse.	de secrets partagé un secret partagé et partagé, clique; ême secret partag) Générer	is existant : , cliquez sur Manue sur Générer. Vous é entré ici. Les sec	el. Pour générer 9 devez configurer l rets partagés
Secret par Sélectionr Aucun Pour tape automatiq client RAL respecten Secret pa	tagé nez un modèle d manuellement uement un secr DIUS avec le mo t la casse. d tagé :	de secrets partagé un secret partagé et partagé, clique; ême secret partag O Générer	is existant : , cliquez sur Manue z sur Générer. Vous é entré ici. Les sec	I. Pour générer devez configurer l rets partagés
Secret par Sélectionr Aucun Pour taper automatiq client RAI respecten Manue Secret pa	tagé nez un modèle c manuellement uement un secr JUS avec le m t la casse.	de secrets partagé un secret partagé et partagé, clique ême secret partag O Générer	is existant : , cliquez sur Manue z sur Générer. Vous é entré ici. Les sec	el. Pour générer devez configurer l rets partagés
Secret par Sélectionr Aucun Pour tape automatiq client RAI respecten Manue Secret pa Confirmez	taqé manuellement uement un secre til a casse. d tagé : e secret partaç	de secrets partagé un secret partagé et partagé, clique, ême secret partag O Générer jé :	is existant : , cliquez sur Manue z sur Générer. Vous é entré ici. Les sec	el. Pour générer devez configurer l rets partagés



2. Déclaration d'une stratégie de demande de connexion :

- On déclare une stratégie de demande de connexion pour Ethernet. Il s'agit de la connexion physique au média.
- Ici, on choisit un nom de stratégie. On laisse le type de serveur par défaut "Non spécifié" (nous utilisons un commutateur en tant que client Radius).
- Puis faites "Suivant".

Nouvelle strate	égie de demande de connexion
	Spécifier le nom de la stratégie de demande de connexion et le type d connexion Vous pouvez spécifier le nom de votre stratégie de demande de connexion ainsi que le type des connexions auxquelles la stratégie s'applique.
Nom de la s Connexion-Ca	tratégie :
Méthode de co Sélectionnez lo valeur dans Ty serveur d'accé	onnexion réseau e type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une ype de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre és réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.
Type de se Non spéc	rrveur d'accès réseau :
O Spécifique	au foumisseur :
	Précédent Suivant Terminer Annuler

• Dans la page « **Spécifier une condition** », faites "Ajouter" ensuite on choisit d'indiquer un « **Type de port NAS** » (type de media concerné)

Info : NAS est ici l'acronyme "Network Access Server" et désigne le client RADIUS.

Ne pas confondre avec Network Authentication Server, qui désigne le serveur

Radius lui-même.

wynew Kre	Architecture Système	Ref : DOC_procedure_NPS
BTS SIO IIA LAVAL	Procédure techniques Déploiement serveur NPS sous Windows 22	Version 1.0.0 Date:02/12 /2024 Page:1/44

Nouvelle straté	égie de demande de connexion
	Spécifier les conditions Spécifiez les conditions qui déterminent si cette stratégie de demande de connexion est évaluée pour une demand de connexion. Au minimum, une condition est nécessaire.
Sélectionner un	ne condition X
Sélectionnez une	e condition, puis cliquez sur Ajouter. ficateur NAS dition Identificateur NAS spécifie une chaîne de caractères qui représente le nom du serveur d'accès réseau
(NAS). Adress La cond réseau	Vous pouvez utiliser la syntaxe de correspondance au modèle pour spécifier les noms NAS. se IPv4 NAS dition Adresse IPv4 NAS spécifie une chaîne de caractères qui représente l'adresse IP du serveur d'accès (INAS). Vous pouvez utiliser la syntaxe de correspondance au modèle pour spécifier les réseaux IP.
Adress La cond réseau	se IPv6 NAS dition Adresse IPv6 NAS spécifie une chaîne de caractères qui représente l'adresse IPv6 du serveur d'accès (NAS). Vous pouvez utiliser la syntaxe de correspondance au modèle pour spécifier les réseaux IPv6.
Example 1 Sector 1 Se	de port NAS dition Type de port NAS spécifie le type de média utilisé par le client d'accès à distance, par exemple des téléphoniques analogiques, un réseau RNIS, des tunnels ou des réseaux privés virtuels, une connexion sans 802.11 ou des commutateurs Ethernet.
	~
	Ajouter Annuler
	Ajouter Modifier Supprimer
	Précédent Suivant Terminer Annuler

• Dans la page "**Type de port NAS**" on coche "**Ethernet**" puis "**OK**"

Type de port NAS	×
Spécifiez les types de médias d'accès nécessaires pour correspondre à cette stratégie. Types de tunnels pour connexions d'accès à distance et VPN standard Asynchrone (Modem) RNIS synchrone Synchrone (ligne T1) Virtuel (VPN)	
Types de tunnels pour connexions 802.1X standard	
Autres ADSL-CAP - Modulation de phase d'amplitude sans porteuse DSL asymétrique ADSL-DMT - Multi-tonalité discrète DSL asymétrique Asynchrone (Modem) Câble	
OK Annuler	



Récapitulatif :

Nouv	elle straté	gie de demar	nde de connexio	on				×
		Spécifiez les de connexion	e r les condi conditions qui d n. Au minimum, u	itions déterminent si cette ine condition est né	stratégie de den icessaire.	nande de connexion	n est évaluée po	our une demande
Con	ditions :							
	Condition		Valeur					
9	Type de p	oort NAS	Ethernet					
Des	cription (le la conditio						
	- nption (
						Ajouter	Modifier	Supprimer
					Précédent	Suivant	Terminer	Annuler
			2011 - Contra 1997 - Contra 19				- 044	

• Dans la page « **Spécifier le transfert de la demande de connexion** », laisser l'option par défaut « **Authentifier les demandes sur ce serveur** », (Les demandes seront traitées sur ce serveur et non sur un autre. Ce qui veut dire que ce NPS pourrait jouer un rôle de "PROXY NPS" s'il relayait les demandes à un autre serveur).

Nouvelle strate	égie de demande de	onnexion		×
	Spécifier le 1 La demande de con groupe de serveurs	ransfert de la demande d exion peut être authentifiée par le server ADIUS distants.	e connexion ur local ou être transférée aux :	serveurs RADIUS d'un
Si la demande	de connexion correspo	d aux conditions de la stratégie, ces param	ètres sont appliqués.	
Transfert of de connexio	te la demande on ification	Spécifiez si les demandes de connexion à des serveurs RADIUS distants pour au authentification. Transfere les demandes au groupe d authentification : Con configurée> Accepter les utilisateurs sans validation	sont traitées localement, si elles s thertification, ou si elles sont acc eur le serveurs RADIUS distants suiv n des informations d'identification	ont transférées eptées sans ant pour Nouveau n
		Précéder	nt Suivant Termine	er Annuler



• À l'étape suivant, faites « **Suivant** » .

Nouvelle strate	égie de demande de connexion	×			
	Spécifier les méthodes d'authentification				
	Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP.				
Remplace	r les paramètres d'authentification de stratégie réseau				
Ces paramètri	es d'authentification sont utilisés à la place des contraintes et des paramètres d'authentification de la stratégie réseau.				
Les types de	protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.				
Types de p	rotocoles EAP :				
	Monter				
	Descendre				
Ajouter	Modifier Supprimer				
Méthodes	d'authentification moins sécurisées :				
Authentifi	cation chiffrée Microsoft version 2 (MS-CHAP v2)				
L'utilis	ateur peut modifier le mot de passe après son expiration				
Authentin	zation chimitee Microsoft (MIS-CITAF)				
Authentifi	cation chiffrée (CHAP)				
Authentifi	cation non chiffrée (PAP, SPAP)				
Autoriser	es clients à se connecter sans négocier une méthode d'authentification.				
	Précédent Suivant Terminer Annuler				

• Dans la page « **Configurer les paramètres** », faites « **Suivant** ».

Nouvelle stratégie de	demande de connexion				×
Lese à la s	nfigurer les param rveur NPS applique des parar tratégie de demande de conr	ètres nètres à la demande de « exion sont remplies.	connexion si toutes les o	conditions relatives	
Configurez les paramè Si la demande de con Paramètres :	tres de cette stratégie réseau. nexion répond aux conditions e	t si la stratégie accorde l'a	accès, les paramètres sor	nt appliqués.	
Spécifier un nom o domaine	sélectionne traitées selo	z les attributs auxquels le n leur ordre d'apparition (s règles suivantes seront dans la liste.	appliquées. Les règles sont	
Attributs RADIUS Standard Spécifiques au fournisseur	Attribut : Règles : Recherch	ID de la station appelée er R	emplacer par	Ajouter Modifier Supprimer Monter Descendre	
		Précé	ident Suivant	Terminer Annuler	



Dans la page « Fin de l'Assistant stratégie de demande de nouvelle connexion », faites ٠ « Terminer »

Nouvelle stratégie	de demand	le de connexion	×
鰔 В	n de l'A	ssistant Stratégie de demande de nouvelle connexion	
Vous avez créé la s	stratégie de	demande de connexion suivante :	
Connexion-Cable	ée		
Conditions de la	stratégie	:	
Condition	Valeur		
Type de port NAS	Ethernet		
Paramètres de la	ı stratégie	:	
Condition		Valeur	
Fournisseur d'auth	entification	Ordinateur local	
Pour fermer cet Ass	iistant, clique	ez sur Terminer.	
		Précédent Suivant Terminer Annu	ler

3. Déclaration d'une stratégie d'accès réseau pour le VLAN 2 (groupe "GP-Direction"):

La configuration repose sur une stratégie de demande de connexion unique, permettant de centraliser les critères d'accès au réseau. Chaque VLAN sera associé à une stratégie réseau distincte, garantissant un placement dynamique selon le groupe d'utilisateurs Active Directory :

- Les membres du groupe **GP-Direction** seront assignés via une stratégie réseau dédiée au ٠ VLAN 2 (172.16.12.X/24).
- Une seconde stratégie réseau placera les membres du groupe GP-RH dans le VLAN 3 ٠ (172.16.13.X/24).
- De même, les membres du groupe **GP-Production** auront leur propre stratégie réseau pour ٠ accéder au VLAN 4 (172.16.14.X/24).



Architecture Système	Ref : DOC_procedure_NPS
Procédure techniques	Version 1.0.0 Date:02/12 /2024
Depiotement serveur NPS sous windows 22	Page:1/44

• Enfin, les utilisateurs non authentifiés ou ne correspondant à aucun groupe prédéfini seront automatiquement affectés au VLAN 254 (172.16.254.X/24) grâce à une stratégie réseau dédiée.

Cette architecture permet une gestion centralisée via une seule stratégie de demande de connexion, tout en offrant une flexibilité granulaire pour l'attribution des VLANs selon les besoins organisationnels.

Pour se faire :

• Faites un clic droit sur « **Stratégie Réseau** », puis **Nouveau**

Serveur NPS (Network Policy Server)		0.		×
Fichier Action Affichage ?				
🗢 🔿 🔁 📆 🛛 🖬				
 NPS (Local) ⁻ Clients et serveurs RADIUS 	Stratégies réseau			
Clients RADIUS Groupes de serveurs RADIUS distants Stratégier	Les stratègies réseau vous permettent d'autoriser les conne sélective, et d'indiquer les circonstances dans lesquelles ce s'effectuer ou non.	xions au ré s connexio	seau de ma ons peuvent	nière
Stratégies de demande de connexion	Nom de la stratégie	État	Ordre de tr	aitement
Gestion	Connexions au serveur Microsoft de Routage et Accès distants	Activé Activé	999998 999999	
Secrets	<			>
Clients Affichage >				
Serveur Actualiser				^
Aide	Conditions - Si les conditions suivantes sont réunies :			
	Condition Valeur			
	Paramètres - Les paramètres suivants sont appliqués :			
	Paramètre Valeur			
	<			>
Nouveau				

• Une page « **Nouvelle stratégie réseau** » s'affiche à l'écran, taper le nom de votre stratégie et dans l'option « **Type de serveur d'accès réseau** », laisser celle proposé par défaut « **Non spécifie** » pour une authentification via un commutateur 802.1x.

"Here Ke	Architecture Système	Ref : DOC_procedure_NPS
BTS SIO IIA LAVAL	Procédure techniques Déploiement serveur NPS sous Windows 22	Version 1.0.0 Date:02/12 /2024 Page:1/44

Nouvelle strat	régie réseau	×
	Spécifier le nom de la stratégie réseau et le type de connexion	
<u>N</u>	Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.	
Nom de la s	tratégie :	_
VLAN_2 (GP	Direction)	
Méthode de c	onnexion réseau	
Sélectionnez valeur dans T serveur d'acc	le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une ype de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre ès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.	
Type de se	erveur d'accès réseau :	
Non spéc	sfié 🗸	
O Spécifique	a u fournisseur :	
10	\$	
	Précédent Suivant Terminer Annuler	

• À l'étape « **Spécifier les conditions** », faites « **Ajouter** » .

Nouvelle straté	gie réseau						×
	Spécifier Spécifiez les co minimum, une c	les conditions nditions qui déterminent : ondition est nécessaire.	si cette stratégie	réseau est é	valuée pour u	ne demande de	e connexion. Au
Conditions :							li e com
Condition		Valeur					
Description de	la condition :			F	Ajouter	Modifier	Supprimer
			Précé	dent	Suivant	Terminer	Annuler

• Ensuite la page « **Sélectionner une condition** » s'affiche, sélectionner « **Groupe Windows** », puis faites « **Ajouter** ».

"Yere Kr.	Architecture Système	Ref : DOC_procedure_NPS
	Procédure techniques	Version 1.0.0 Date:02/12 /2024
BTS SIO IIA LAVAL	Deplotement serveur NPS sous Windows 22	Page:1/44



• Ensuite la page **Groupes Windows** s'affiche à l'écran, faites « **Ajouter des groupes** » puis chercher votre groupe et faites « OK » pour ajouter.

Sélectionner une conditi	on	-	\times
Sélectionnez une condition	Groupes Windows X		
Groupes Groupes Windo La condition Groupe à l'un des groupe	Spécifiez l'appartenance aux groupes nécessaire pour correspondre à cette stratégie. Groupes	on doit appartenir	
Groupes d'ordin La condition Grou groupes sélection	DOM\GP-Direction	artenir à l'un des	
Groupes d'utilis La condition Grou groupes sélection		artenir à l'un des	
Restrictions relatives au Restrictions re Les restrictions re	Ajouter des groupes Supprimer	atives de	
Policy Server)	OK Annuler	jouter Annuler	

• Récapitulatif du choix des groupes Windows, faites « Suivant ».

vition Kr.	Architecture Système	Ref : DOC_procedure_NPS
BTS SIO IIA LAVAL	Procédure techniques Déploiement serveur NPS sous Windows 22	Version 1.0.0 Date:02/12 /2024 Page:1/44

						~
Nouvelle strate	egie reseau					×
	Spécifier	les conditions				
	Spécifiez les co minimum, une	onditions qui déterminent condition est nécessaire.	si cette stratégie rése	au est évaluée pour	une demande de	connexion. Au
	,					
Conditions :						
Condition	1	Valeur				
💙 Groupes	Windows	DOM\GP-Direction				
Description de	la condition :					
La condition Gr	roupes Windows	spécifie que l'utilisateur ou	l'ordinateur qui tente d'é	tablir la connexion doi	t appartenir à l'un	des groupes
sélectionnés.						
				Ajouter	Modifier	Supprimer
			Précédent	Suivant	Terminer	Annuler

• À l'étape « **Spécifier l'autorisation d'accès** », ils est possible d'autoriser ou refuser l'accès.

Nouvelle strate	égie réseau X
	Spécifier l'autorisation d'accès Effectuez la configuration nécessaire pour accorder ou refuser l'accès réseau si la demande de connexion correspond à cette stratégie.
Accès acco Accordez 1 Accordez 1 Accès refus Refusez 1'ar L'accès est Choisissez 3	ordé acces si les tentatives de connexion des clients répondent aux conditions de cette stratégie. sé iccès si les tentatives de connexion des clients répondent aux conditions de cette stratégie. It déterminé par les propriétés de numérotation des utilisateurs (qui remplacent la stratégie NPS) selon les propriétés de numérotation utilisateur si les tentatives de connexion des clients répondent aux conditions de la stratégi
61033362	
	Précédent Suivant Terminer Annuler



• Ensuite on décoche les authentification par défaut et on ajoute les types de protocoles accepté, faites « **Ajouter** », puis « **OK** », ici « **Micosoft : PEAP (protected EAP** ».

Nouvelle straté	śgie réseau	×
	Configurer les méthodes d'authentification	
	Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP.	
Les types de pro dans lequel ils se	xtocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre ont listés.	
Types de pro	tocoles EAP :	
Microsoft: PE/	AP (Protected EAP) Monter	
	Deserves	
	Descendre	
Ajouter	Modifier Supprimer	
Méthodes d'a	authentification moins sécurisées :	
Authentifica	tion chiffrée Microsoft version 2 (MS-CHAP v2)	
L'utilisate	eur peut modifier le mot de passe après son expiration	
	tion chiffrée Microsoft (MS-CHAP)	
L'utilisate	eur peut modifier le mot de passe après son expiration	
Authentificat	tion contract (CHAP)	
Autoriser les	clients à se connecter sans négocier une méthode d'authentification.	
	Précédent Suivant Terminer Annuler	

• Dans la page « **Configurer des contraintes** », on sélectionne « **Types de ports NAS** » et dans l'option type de tunnels pour connexion 802.1X ... on coche la case « **Ethernet** ».

Nouvelle strate	égie réseau	×
	Configurer Les contraintes so doivent se confor Server) rejette aut configurer de cont	des contraintes nt des paramètres supplémentaires de la stratégie réseau, auxquels les demandes de connexion mer. Si une demande de connexion ne répond pas à une contrainte, le serveur NPS (Network Polic omatiquement cette demande. Les contraintes sont facultatives ; si vous ne souhaitez pas raintes, cliquez sur Suivant.
Configurez les Si la demande	contraintes de cette s de connexion ne rép -	tratégie réseau. nd pas à toutes les contraintes, l'accès réseau est refusé.
Contraintes Délai d'i Session ID de la appelée Restrict aux jour heures	inactivité expiration de station dions relatives s et aux e port NAS	Spécifier les types de médias d'accès nécessaires pour correspondre à cette stratégie Types de tunnels pour connexions d'accès à distance et VPN standard Asynchrone (Modem) Synchrone (ligne T1) Virtuel (VPN) Types de tunnels pour connexions 802.1X standard PDDI Sans fil - IEEE 802.11 Token Ring Autres ADSL-CAP - Modulation de phase d'amplitude sans porteuse DSL asymétrique Asynchrone (Modem) Câble
		Précédent Suivant Terminer Annuler

18 / 43



 Dans la page « Configurer les paramètres », dans la section « Attributs RADIUS », faites « Ajouter » pour ajouter des attributs de contrôle de trafic (Tunnel-Medium-Type, Tunnel-Pvt-Group-ID et Tunnel-Type).

Nouvelle stratégie réseau		×
Le serveur NPS app à la stratégie de de	les paramètres olique des paramètres à la demande de connexion si toutes les conditions relatives emande de connexion sont remplies.	
Configurez les paramètres de cette s Si la demande de connexion répond Paramètres :	tratégie réseau. aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.	
Attributs RADIUS Standard Spécifiques au fournisseur Routage et accès à distance	Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.	
Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol) Filtres IP Chiffrement Al Paramètres IP	Nom Valeur Framed-Protocol PPP Service-Type Framed	
	Ajouter Modifier Supprimer	
	Précédent Suivant Terminer Annuler	

a) Ajout de l'attribut « Tunnel-Medium-Type » :

• Dans Ajouter un attribut **RADIUS** standard, dans Attributs, faites défiler vers le bas jusqu'aux attributs et faites « **Ajouter** ».



Ajouter un attribut RADIUS standard	×
Pour ajouter un attribut aux paramètres, sélectionnez-le et cliquez sur Ajouter.	
Pour ajouter un attribut personnalisé ou prédéfini spécifique au fournisseur, fermez cette boîte de dialogue et sélectionnez Spécifique au fournisseur, puis cliquez sur Ajouter.	
Type d'accès :	
Tous	
Attributs :	
Nom	^
Tunnel-Client-Endpt	
Tunnel-Medium-Type	
Tunnel-Password	
Tunnel-Preference	
Tunnel-Pvt-Group-ID	
Tunnel-Server-Auth-ID	\sim
<	>
Description :	
Spécifie le média de transport utilisé lors de la création d'un tunnel pour les protocoles (par exemple L2TP) qui peuvent opérer sur plusieurs transports.	
Ajouter Fermer	

• La page d'information d'attribut s'affiche à l'écran, faites « Ajouter ».

Informations d'attribut	×
Nom de l'attribut : Tunnel-Medium-Type	
Numéro de l'attribut : 65	
Format de l'attribut : Enumerator	
Valeurs d'attribut :	
Foumisseur Valeur	Ajouter
	Modifier
	Supprimer
	Monter
	Descendre
OK	Annuler



Architecture Système	Ref : DOC_procedure_NPS
Procédure techniques Déploiement serveur NPS sous Windows 22	Version 1.0.0 Date:02/12 /2024 Page:1/44

• Ensuite la deuxième page d'information d'attribut s'affiche à l'écran, laissez l'option « **Valeur d'attribut** » coché par défaut et faites « **OK** ».

Informations d'attribut	\times
Nom de l'attribut : Tunnel-Medium-Type	
Numéro de l'attribut : 65	
Format de l'attribut : Enumerator	
Valeur d'attribut : O Communément utilisé pour les connexions 802.1x	٦
802 (includes all 802 media plus Ethemet canonical format)	~
O Autres	
<aucun></aucun>	\sim
OK Annule	r

b) Ajout de l'attribut « Tunnel-Pvt-Group-ID » :

• Dans Ajouter un attribut **RADIUS** standard, dans Attributs, faites défiler vers le bas jusqu'aux attributs et faites « **Ajouter** ».

Ajouter un attribut RADIUS standard		×
Pour ajouter un attribut aux paramètres, sélect	tionnez-le et cliquez sur Ajouter.	
² our ajouter un attribut personnalisé ou prédé électionnez Spécifique au foumisseur, puis c	fini spécifique au fournisseur, fermez cette boîte de dialogue et diquez sur Ajouter.	
Type d'accès :		
Tous	~	
Attributs :		
Nom		^
Tunnel-Client-Endpt		
Tunnel-Medium-Type		
Tunnel-Password		
Tunnel-Preference		
Tunnel-Pvt-Group-ID		
Tunnel-Server-Auth-ID		4
<	>	
×		
Jeschption :		
Spécifie l'ID de groupe pour une session par t	tunnel.	
	Ajouter Fermer	
	01 / 40	
	21/43	



• La page d'information d'attribut s'affiche à l'écran, faites « Ajouter ».

nformations d'attri Nom de l'attribut :	out	
unnel-Pvt-Group-ID		
luméro de l'attribut : 1		
ormat de l'attribut : IctetString		
aleurs d'attribut :		 Alex des
Fournisseur Valeu		Ajouter
		Modifier
		Supprimer
		Monter
		 Descendre

• Ensuite la deuxième page d'informations d'attribut s'affiche à l'écran, laissez l'option « **Chaîne** » coché par défaut et taper ID de VLAN concerné dans la case ici (VLAN 2), puis faites « **OK** ».





Architecture SystèmeRef : DOC_procedure_NPS
Version 1.0.0Procédure techniques
Déploiement serveur NPS sous Windows 22Def : DOC_procedure_NPS
Version 1.0.0Procédure techniques
Date:02/12 /2024
Page:1/44Page:1/44

c) Ajout de l'attribut « Tunnel-Type » :

• Dans Ajouter un attribut **RADIUS** standard, dans Attributs, faites défiler vers le bas jusqu'aux attributs et faites « **Ajouter** ».

Ajouter un attribut RADIUS standard	×
Pour ajouter un attribut aux paramètres, sélectionnez-le et cliquez sur Ajouter.	
Pour ajouter un attribut personnalisé ou prédéfini spécifique au foumisseur, fermez cette boîte de dialogue et sélectionnez Spécifique au foumisseur, puis cliquez sur Ajouter.	
Type d'accès :	
Tous 🗸	
Attributs :	
Nom	^
Tunnel-Password	
Tunnel-Preference	
Tunnel-Pvt-Group-ID	
Tunnel-Server-Auth-ID	
Tunnel-Server-Endpt	
Tunnel-Type	M
< >	
Description :	
Spécifie les protocoles de tunnel utilisés.	
Ajouter Femer	

• La page d'information d'attribut s'affiche à l'écran, faites « Ajouter ».

Informations d'attribut	×
Nom de l'attribut : Tunnel-Type	
Numéro de l'attribut : 64	
Format de l'attribut : Enumerator	
Valeurs d'attribut :	
Foumisseur Valeur	Ajouter
· · · · · · · · · · · · · · · · · · ·	Modifier
	Supprimer
	Monter
	Descendre
ОК	Annuler



Architecture Système	Ref : DOC_procedure_NPS
Procédure techniques Déploiement serveur NPS sous Windows 22	Version 1.0.0 Date:02/12 /2024 Page:1/44

• Ensuite la deuxième page d'informations d'attribut s'affiche à l'écran, coché l'option « **Communément utilisé pour les connexions 802,1X** », puis faites « **OK** ».

Informations d'attribut		×
Nom de l'attribut : Tunnel-Type		
Numéro de l'attribut : 64		
Format de l'attribut : Enumerator		
Valeur d'attribut : O Communément utilisé pour les connexi	ons d'accès à distance ou VPN	
<aucun></aucun>		~
<aucun> Communément utilisé pour les connexi</aucun>	ons 802.1x	
<aucun> Communément utilisé pour les connexi Virtual LANs (VLAN) </aucun>	ons 802.1x	
<aucun> Communément utilisé pour les connexi Virtual LANs (VLAN) Autres </aucun>	ons 802.1x	~
<aucun> Communément utilisé pour les connexi Virtual LANs (VLAN) Autres <aucun></aucun> </aucun>	ons 802.1x	>

• Voici le récapitulatif des attributs « Ajouter », faites « Suivant ».

Nouvelle strat	égie réseau			×
	Configurer I Le serveur NPS app à la stratégie de de	es paramètres ique des paramètres à la demande mande de connexion sont remplies	de connexion si toutes les conditions relatives	
Configurez les Si la demande Paramètres	paramètres de cette st de connexion répond	ratégie réseau. aux conditions et contraintes, et si la s	tratégie accorde l'accès, les paramètres sont appliqué	s.
Attributs R Standa Spécifi fournis Routage e distance	ADIUS rd ques au seur t accès à	Pour envoyer des attributs supplé RADIUS standard, puis cliquez s n'est pas envoyé aux clients RAI RADIUS pour connaître les attrib Attribute	mentaires aux clients RADIUS, sélectionnez un attribu ur Modifier. Si vous ne configurez pas d'attribut, celui- JIUS. Consultez la documentation de votre client uts nécessaires.	rt ci
Liaisor protocc (Bandy Protocc Filtres Chiffre A Parame	is multiples et ble BAP vidth Allocation a) IP ment ètres IP	AllDols Vale Nom Vale Framed-Protocol PPP Service-Type Fram Tunnel-Medium-Type Fram Tunnel-Ptvt-Group-ID 2 Tunnel-Type Virtu Ajouter Modifier	ur ed (noludes all 802 media plus Ethemet canonical for al LANs (VLAN) Supprimer	
		P	écédent Sulvant Terminer An	nuler



Version 1.0.0

Page:1/44

Le résumé de notre configuration, faites « Terminer ».

	eseau		×
Fi	n de la configuration	de la nouvelle stratégie réseau	
/ous avez correcte	ment créé la stratégie réseau suiva	nte :	
LAN_2 (GP-Dire	ection)		
conditions de la	stratégie :		
Condition	Valeur		
Groupes Windows	UOM\GP-Direction		J
Groupes Windows Paramètres de la	DUM\GP-Direction]
Groupes Windows Paramètres de la Condition	UUM\GP-Direction	Valeur	•
Groupes Windows Paramètres de la Condition Méthode d'authen	UUM\GP-Direction stratégie :	Valeur Protocole EAP OU MS-CHAP v1 OU MS-CHAP v1 (∫utilisateur peut modifie	
Groupes Windows Paramètres de la Condition Méthode d'authen Autorisation d'acco	Stratégie :	Valeur Protocole EAP OU MS-CHAP v1 0U MS-CHAP v1 ≬'utilisateur peut modifie Accorder l'accès	
Croupes Windows Cramètres de la Condition Méthode d'authen Autorisation d'acco Ignorer les propriét Méthode EAP (Ext	stratégie : ification is és de numérotation des utilisateurs ensible Authentication Protocol)	Valeur Protocole EAP OU MS-CHAP v1 OU MS-CHAP v1 (/ˈutilisateur peut modifie Accorder l'accès Faux Microsoft: PEAP (Protected EAP)	
Croupes Windows Paramètres de la Condition Méthode d'authen Autorisation d'acce Ignorer les propriét Méthode EAP (Ext Type de port NAS	stratégie : ification is és de numérotation des utilisateurs ensible Authentication Protocol)	Valeur Protocole EAP OU MS-CHAP v1 0U MS-CHAP v1 (l'utilisateur peut modifie Accorder l'accès Faux Microsoft: PEAP (Protected EAP) Ethemet	

NB : Dans ce cas, étant donné que nous avons trois VLAN, il est nécessaire de définir une stratégie réseau distincte pour chacun d'eux. Ainsi, la même procédure devra être appliquée aux VLAN 3 et 4.

4. Stratégie réseau pour les utilisateurs non authentifier (VLAN 254):

Pour se faire :

- Faites un clic droit sur « Stratégie Réseau », puis Nouveau, ٠
- Une page « Nouvelle stratégie réseau » s'affiche à l'écran, taper le nom de votre stratégie et ٠ dans l'option « Type de serveur d'accès réseau », laisser celle proposé par défaut « Non spécifie » pour une authentification via un commutateur 802.1x.

Harring Ker	Architecture Système	Ref : DOC_procedure_NPS	
	Procédure techniques Déploiement serveur NPS sous Windows 22	Date:02/12 /2024	
		Page:1/44	

Nouvelle straté	gie réseau	×
	Configurer les méthodes d'authentification Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP.	
Les types de prot dans lequel ils so Types de prot	tocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre int listés. ocoles EAP :	
Microsoft: PEA	P (Protected EAP) Monter Descendre	
Ajouter Méthodes d'a Authentificati L'utilisated Authentificati L'utilisated Authentificati Authentificati Authentificati Autoriser les	Modifier Supprimer authentification moins sécurisées : ion chiffrée Microsoft version 2 (MS-CHAP v2) ur peut modifier le mot de passe après son expiration ion chiffrée Microsoft (MS-CHAP) ur peut modifier le mot de passe après son expiration ion chiffrée (CHAP) ur peut modifier le mot de passe après son expiration ion chiffrée (CHAP) on on chiffrée (PAP, SPAP) clients à se connecter sans négocier une méthode d'authentification.	
	Précédent Suivant Terminer Annuler	

4. Configuration VPN Ipsec sur OPNSense :

- Se connecter à OPNSense,
- Allez dans OpenVPN, puis IPSEC, et cliquer sur paramètre du tunnel (héritage)

volicer Kr.	Architecture Système	Ref : DOC_procedure_NPS
BTS SIO IIA LAVAL	Procédure techniques Déploiement serveur NPS sous Windows 22	Version 1.0.0 Date:02/12 /2024 Page:1/44

EOPO sense '					root@(OPNsense.localdomain	
Apports	VPN: IPsec: Param	ètres du tunnel [héritage]					
🗃 Système							
🛔 Interfaces	Phase 1					Q Recherche	G 1
Bare-feu							
VPN	Activé Type	Passerelle distante	Mode Prop	osition Phase 1	Authentification	Description	Commandes
IPsec 🔒				Aucun résultat!			
Connexions							•
Paramètres du tunnel [héritage]							Affichage des entrés
Clients mobiles							Amenage des entres
Clés pré-partagées							
Paires de clés	Phase 2					O Basharaha	<i>a</i> 7
Paramètres avancés						Kecherche	
Vue globale des statuts	Activé Regid	Type Sous-réseau local	Sous-réseau dist	ant Proposition de la	a phase 2	Description	
Statut des baux				Aucun résultat!			
Base de données des associations de sécurité							Affichage des entrés
Base de données des politiques de sécurité	« < 1 > »						Amonage des entre
Interfaces de tunnel virtuel						Activer Windo	DWS

Contenue du règle ipsec :

VPN: IPsec: Tunnel Set	tings [legacy] C
General information	full
0 Disabled	 Disable this phase1 entry Set this option to disable this phase1 without removing it from the list.
Onnection method	default Choose the connect behaviour here, when using CARP you might want to consider the 'Respond only' option here (wait for the other side to connect).
Hey Exchange version	V1 • Select the KeyExchange Protocol version to be used. Usually known as IKEv1 or IKEv2.
() Internet Protocol	IPv4 Select the Internet Protocol family from this dropdown.
0 Interface	WAN
Remote gateway	10.53.250.105 Enter the public IP address or host name of the remote gateway.
Opnamic gateway	Allow any remote gateway to connect Recommended for dynamic IP addresses that can be resolved by DynDNS at IPsec startup or update time.

vo Your Kra	Architecture Système	Ref : DOC_procedure_NPS
BTS SIO IIA LAVAL	Procédure techniques Déploiement serveur NPS sous Windows 22	Version 1.0.0 Date:02/12 /2024 Page:1/44

1 Description	Routeur Cisco	
	You may enter a description here for your reference (not pars	sed).
Phase 1 proposal (Authentication)		
O Authentication method	Mutual PSK 👻	
	Must match the setting chosen on the remote side. If you select EAP-RADIUS, you must define your RADIUS serve	ers on the Servers page.
Negotiation mode	Main ·	
	Aggressive is more flexible, but less secure.	
My identifier	My IP address 👻	
Peer identifier	Peer IP address 👻	
1 Pre-Shared Key	Not24get	
	Input your Pre-Shared Key string.	
Phase 1 proposal (Algorithms)		
Encryption algorithm	AES	
	256 🗸	
	Note: For security reasons avoid the use of DES,3DES,CAST and BLO	WFISH protocols.
1 Hash algorithm	SHA1	
	Note: For security reasons avoid the use of MD5 and SHA1 algorithm	S.
1 DH key group	5 (1536 bits)	
	Must match the setting chosen on the remote side.	
Advanced Options		
() Install policy		
	Decides whether IPsec policies are installed in the kernel by the cha disabled.	ron daemon for a given connection. When using route-based mode (VTi) this needs to be
Disable Rekey		
	Whether a connection should be renegotiated when it is about to ex	pire.
Oisable Reauth	□ Whether rekeying of an IKE_SA should also reauthenticate the peer.	In IKEv1, reauthentication is always done.
Tunnel Isolation	0	
	This option will create a tunnel for each phase 2 entry for IKEv2 inter	operability with e.g. FortiGate devices.
6 SHA256 96 Bit Truncation	0	

verysour Kr.	Architecture Système	Ref : DOC_procedure_NPS
BTS SIO IIA LAVAL	Procédure techniques Déploiement serveur NPS sous Windows 22	Version 1.0.0 Date:02/12 /2024 Page:1/44

() NAT Traversal	Disable
	Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.
Disable MOBIKE	Disables the IKEv2 MOBIKE protocol defined by RFC 4555
Close Action	None Defines the action to take if the remote peer unexpectedly closes a CHILD_SA. A closeaction should not be used if the peer uses reauthentication or uniqueids checking, as these events might trigger the defined action when not desired. With clear the connection is closed with no further actions taken, hold installs a trap policy, which will catch matching traffic and tries to re-negotiate the connection on demand, restart will immediately trigger an attempt to re-negotiate the connection. The default is none and disables the close action.
🚯 Unique	Replace Connection uniqueness policy to enforce. To avoid multiple connections from the same user, a uniqueness policy can be enforced.
1 Dead Peer Detection	Enable DPD
Inactivity timeout	Time before closing inactive tunnels if they don't handle any traffic. (seconds)
6 Keyingtries	How many attempts should be made to negotiate a connection, or a replacement for one, before giving up (default 3). Leave empty for default, -1 for forever or
1 Lifetime	28800 seconds
1 Margintime	Time before SA expiry the rekeying should start. (seconds)
1 Rekeyfuzz	Percentage by which margintime is randomly increased (may exceed 100%). Randomization may be disabled by setting rekeyfuzz=0%.
	Save

• Ensuite faites ajouter un second page supplémentaire et remplir les contenues :

voYeevr Kra	Architecture Système	Ref : DOC_procedure_NPS
BTS SIO IIA LAVAL	Procédure techniques Déploiement serveur NPS sous Windows 22	Version 1.0.0 Date:02/12 /2024 Page:1/44

General information				
Disabled		 Disable this phase2 entry Set this option to disable this phase 	entry without removing it	rom the list.
Mode		Tunnel IPv4	-	
Oescription		You may enter a description here for	your reference (not parsed)	
Local Network				
🚯 Туре		SRV subnet	•	
Address:			32 🔺	
Remote Network				
Type:		Network	-	
Address:		172.16.0.0	16 🔺	
Phase 2 proposal (SA/K	(ey Exchange)			
Protocol		ESP	-	
Encryption algorithms	AES256	•		
() Hash algorithms	SHA1 Note: For security reasons avo	➡ Did the use of the SHA1 algorithm.		
PFS key group	5 (1536 bits)	•		
0 Lifetime	28800 seconds			
Advanced Options				
Automatically ping host	IP address			
Manual SPD entries	Register additional Security I Strongswan automatically cre add them here as a comma-se e.g. 192.168.1.0/24, 192.168.2.0/24	Policy Database entries sates SPD policies for the networks defined in this phase2. If y eparated list.When configured, you can use network address	ou need to allow other networks to use this ip anslation to push packets through this tunne	sec tunnel, you can I from these networks.



4. Configuration du basique de switch :

Config 802.1x avec AD DHCP NPS sur switch catalyst avec attribution de vlan (PEAP-MSCHAPv2)

Config basique switch
enable
conf t
vlan 2
name GP-Direction
vlan 3
name GP-RH
vlan 4
name GP-Production
vlan 5
name GP-WIFI-BYOD
vlan 254
name GP-Public
interface vlan 1
ip address 172.16.11.1 255.255.255.0
no shutdown
exit
!Desactiver le serveur web integre
no ip http server
no ip http secure-server
!Desactiver le recherche de nom dns
no ip domain-lookup



Architecture Système	Ref : DOC_procedure_NPS
Procédure techniques	Version 1.0.0 Date:02/12 /2024
Deploiement serveur NPS sous Windows 22	Page:1/44

ip default-gateway 172.16.11.253

hostname yzotalocalswitch

ip domain-name lan.iia-laval.info

crypto key generate rsa general-keys modulus 2048

ip ssh time-out 30

ip ssh authentication-retries 4

ip ssh version 2

service password-encryption

username admin privilege 15 secret 0 Not24get

enable secret 0 Not24get

line console 0

password Not24get

login

exit

line vty 0 15

transport input ssh

login local

exit

banner login !

Attention toute tentative d'acces sera enregistre et vous encourez des poursuites penales si vous tentez d'y acceder...

interface gigabitEthernet 0/1

switchport mode trunk



switchport trunk allowed vlan all

switchport trunk native vlan 1

description LOCAL-TRUSTED

exit

interface fastEthernet 0/12

switchport mode access

switchport access vlan 2

spanning-tree portfast

description VLANLOCAL-DIRECTION

exit

interface fastEthernet 0/13

switchport mode access

switchport access vlan 3

spanning-tree portfast

description VLANLOCAL-RH

exit

interface fastEthernet 0/14

switchport mode access

switchport access vlan 4

spanning-tree portfast

description VLANLOCAL-PROD

exit

interface fastEthernet 0/15

switchport mode access

switchport access vlan 5

spanning-tree portfast



description VLANLOCAL-WIFIBYOD

exit

interface fastEthernet 0/16

switchport mode access

switchport access vlan 254

spanning-tree portfast

description VLANLOCAL-PUBLIC

exit

! Activer le protocole AAA sur le switch :

Config 802.1x switch

• • •

!Enables AAA

aaa new-model

!aaa authentication dot1x {default} method1

!Creates an 802.1x authentication method list.

!To create a default list that is used when a named list is not specified in the authentication command, use the default keyword followed by the method that is to be used in default situations. The default method list is automatically applied to all ports.

!For method1 , enter the group radius keywords to use the list of all RADIUS servers for authentication.

aaa authentication dot1x default group radius

Sets the authorization method to local. To remove the authorization method, use the no aaa authorization network default group radius command.

aaa authorization network default group radius



!Enable 802.1x accounting using the list of all RADIUS servers.

aaa accounting dot1x default start-stop group radius

!Globally enables 802.1X port-based authentication on a switch

dot1x system-auth-control

!config radius server for aaa

radius-server host 10.196.72.1 auth-port 1812 acct-port 1813 timeout 10 key Not24get

interface range FastEthernet0/1-22

switchport mode access

! Set the interface Port Access Entity to act only as an authenticator and ignore messages meant for a supplicant.

dot1x pae authenticator

!Enable 802.1x authentication on the port.

authentication port-control auto

!Les étape facultatifs (pour les bonne pratique)

!Allow multiple hosts on an 802.1x-authorized port after a single host has been authenticated.

!authentication host-mode multi-host (cette commande n'avais fonctionné)

!Permettre l'authentification avec le wake-on-lan en authentificant que ce qui vient de l'interface authentication control-direction in

!Configure the violation mode : Removes the current session and authenticates with the new host.



authentication violation replace

!Set the number of seconds that the switch remains in the quiet state after a failed authentication exchange with the client. (default 60)

authentication timer inactivity 10

!Enable periodic reauthentication of the client, which is disabled by default.

authentication periodic

! Set reauthentication attempt for the client (set to one hour by default).

authentication timer reauthenticate 1800

!Vlan guest si pas d'auth

authentication event no-response action authorize vlan 254

!Vlan guest si authentification échoue

authentication event fail action authorize vlan 254

!Vlan guest si pas de serveur radius

authentication event server dead action authorize vlan 254

spanning-tree portfast

• • • •

4. Configuration du basique de Routeur :

Config basique routeur
```cisco
enable
conf t
hostname yzlocalrouter
enable secret 0 Not24get
service password-encryption
line console 0



# password Not24get login exit ip domain-name lan.iia-laval.info aaa new-model username admin privilege 15 secret 0 Not24get line vty 0 15 transport input ssh exit crypto key generate rsa general-keys modulus 2048 ip ssh time-out 30 ip ssh authentication-retries 4 ip ssh version 2 banner login ! ***** Attention toute tentative d'acces sera enregistre et vous encourez des poursuites penales si vous tentez d'y acceder... interface GigabitEthernet0/1 ip address 172.16.11.253 255.255.255.0 description LOCAL-MGMT no shutdown exit interface GigabitEthernet0/1.2



#### encapsulation dot1Q 2

ip address 172.16.12.253 255.255.255.0

ip helper-address 172.17.2.254

description LOCAL-direction

no shutdown

exit

interface GigabitEthernet0/1.3

encapsulation dot1Q 3

ip address 172.16.13.253 255.255.255.0

ip helper-address 172.17.2.254

description LOCAL-rh

no shutdown

exit

interface GigabitEthernet0/1.4

encapsulation dot1Q 4

ip address 172.16.14.253 255.255.255.0

ip helper-address 172.17.2.254

description LOCAL-production

no shutdown

exit

interface GigabitEthernet0/1.5

encapsulation dot1Q 5

ip address 172.16.15.253 255.255.255.0

ip helper-address 172.17.2.254

description LOCAL-WIFI-BYOD

no shutdown



#### exit

interface GigabitEthernet0/1.254

encapsulation dot1Q 254

ip address 172.16.254.253 255.255.255.0

ip helper-address 10.192.1.11

description LOCAL-public

no shutdown

exit

													-									-

## Config VPN routeur

```cisco

!Utiliser IP OPNsense

crypto isakmp key Not24get address 10.192.0.200 no-xauth

crypto ipsec security-association lifetime seconds 28800

crypto isakmp policy 5

encryption aes 256

hash sha

authentication pre-share

group 5

lifetime 28800

exit

crypto ipsec transform-set VPN-OPNSENSE esp-aes 256 esp-sha-hmac

mode tunnel



exit

!Access list pour les reseaux locaux

access-list 100 permit ip 172.16.0.0 0.0.255.255 172.17.1.0 0.0.255.255

!Access list pour le routeur VPN

access-list 100 permit ip 10.53.250.114 0.0.0.0 172.17.0.0 0.0.255.255

crypto map OPNSENSE-MAP 2 ipsec-isakmp

! Utiliser IP OPNsense

set peer 10.192.0.200

set security-association lifetime seconds 28800

set transform-set VPN-OPNSENSE

set pfs group5

match address 100

exit

crypto isakmp invalid-spi-recovery

int GigabitEthernet0/1

crypto map OPNSENSE-MAP

!Commandes debug

show crypto map

show crypto session

!Si ça marche pas la commande crypto

show license

conf t

license boot module c2900 technology-package securityk9

exit

wr

show license



reload

! Ensuite commencer la configuration

!https://getlabsdone.com/how-to-configure-ipsec-vpn-between-pfsense-and-cisco-router/

https://forum.opnsense.org/index.php?topic=3645.0

!(Suite à souci de configuration de service DHCP, d'ou la création de services des pools DHCP sur le routeur en annulant le relai DHCP configurer précedement.)

!attention la première étape consiste à annuler les configuration relai dhcp dejà faite pour le service dhcp depuis OpnNebula cet étape nest pas adapter à tout les cas)

configure terminal

interface gigabitEthernet 0/0.2

no ip helper-address

interface gigabitEthernet 0/0.3

no ip helper-address

interface gigabitEthernet 0/0.4

no ip helper-address

interface gigabitEthernet 0/0.5

no ip helper-address

exit

!Cette étape permet d'exclure certains adresse IP pour le service DHCP

ip dhcp excluded-address 172.16.12.253

ip dhcp excluded-address 172.16.13.253

ip dhcp excluded-address 172.16.14.253

ip dhcp excluded-address 172.16.15.253

ip dhcp excluded-address 172.16.254.253



| Début de configuration des pools d'adressage IP |
|---|
| ip dhcp pool vlan2-Direction |
| network 172.16.12.0 255.255.255.0 |
| default-router 172.16.12.253 |
| dns-server 172.17.2.1 |
| exit |
| |
| ip dhcp pool vlan3-RH |
| network 172.16.13.0 255.255.255.0 |
| default-router 172.16.13.253 |
| dns-server 172.17.2.1 |
| exit |
| ip dhcp pool vlan4-Prod |
| network 172.16.14.0 255.255.255.0 |
| default-router 172.16.14.253 |
| dns-server 172.17.2.1 |
| exit |
| ip dhcp pool vlan254-Public |
| network 172.16.254.0 255.255.255.0 |
| default-router 172.16.254.253 |
| dns-server 1.1.1.1 |
| exit |
| exit |
| write |
| |

| w Year Ken | Architecture Système | Ref : DOC_procedure_NPS |
|-------------------|---|--|
| BTS SIO IIA LAVAL | Procédure techniques
Déploiement serveur NPS sous Windows 22 | Version 1.0.0
Date:02/12 /2024
Page:1/44 |

Faire le test de ping vers le plateforme OpenNebula :

Info : Attentions pour que cela fonctionne il faut d'abord activer le protocole ICMP dans le parefeu de serveur Radius et le PC.