ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

# **VPN RESEAU POSTE A POSTE**

# **SOMMAIRE** :

I)	Objectif	2
II)	Prérequis	2
III)	Définitions	2
IV)	Mise en place du réseau VPN Poste à poste	2-21
V)	Conclusion	21

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

## I) <u>Objectif</u>

Dans cette procédure, nous allons voir comment mettre en œuvre un **Réseau VPN Poste** à **poste** sous **Windows**.

#### II) <u>Prérequis</u>

Pour réaliser cette procédure, nous avons besoin des équipements suivants :

Nombre de	SE Windows	Nom de la première	Nom de la seconde
	Windows 7		
2	willuows /		VVIII/VFINZ

Logiciel utilisé	Adresse IP de la première machine	Adresse IP de la seconde machine
MMC	192.168.123.202	192.168.123.203

## III) <u>Définitions</u>

- Un réseau VPN (Virtual Private Network) est un réseau privé virtuel qui permet l'accès aux machines à distance reliées entre elles comme la connexion au réseau local d'une entreprise.
- Un réseau **VPN Poste à poste** a pour objectif de protéger la communication entre les postes distants. Ce réseau concerne 2 postes clients et un poste client et un serveur. Celui-ci permet d'avoir un tunnel sécurisé.
- **MMC** (Microsoft Management Console) est une console qui comporte et affiche tous les outils d'administration créés par Microsoft et d'autres composants logiciels.

## IV) Mise en place du réseau VPN Poste à poste

Cette procédure doit se faire et est la même sur les 2 postes.

- Tout d'abord, nous allons dans « Démarrer » et lançons la console « mmc » :

Programmes (1)	
mmc mmc	

- Ensuite, nous cliquons sur « Fichier » et « Ajout/Supprimer un composant logiciel » :

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

-	Con	sole1 - [Racine de la console]		
	Fich	ier Action Affichage Favoris Fenêtre ?		
		Nouveau	Ctrl+N	
		Ouvrir	Ctrl+0	
٦		Enregistrer	Ctrl+S	
		Enregistrer sous		er da
		Ajouter/Supprimer un composant logiciel enfichable	Ctrl+M	
		Options	5	
		Fichier récent		
		Quitter		
1 "	_			

- Nous cliquons sur « Gestion de la stratégie de sécurité IP » et « Ajouter » :



- Nous cliquons sur « Terminer » :

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

Sélectionner un ordinateur ou un domaine	×
Sélectionnez l'ordinateur ou domaine devant être géré par ce composant Quand cette console sera enregistrée, l'emplacement sera également enregistré	
Ordinateur local	
L ordinateur sur lequel cette console s execute	
<ul> <li>Un autre domaine Active Directory (utiliser le nom DNS complet ou l'adresse IP) :</li> <li>Un autre ordinateur :</li> <li>Parcourir</li> </ul>	
< Précédent Teminer Ann	Jler

- Une fois la stratégie de sécurité IP ajoutée, nous cliquons sur « **OK** » :

	Composants logiciels enfit sélectionnés :	
	Racine de la console	Modifier les
	😸 Stratégies de sécurité IP sur Or	
		Supt
		Mo
		Desc
Ajouter >		0.50
	4 III +	Ava
(756.).0).1		11 A - 1
(IPSec). Gere l	es strategies 185ec pour assurer la secu	rite des commu



ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

- Nous faisons un clic droit sur la stratégie IP et « Créer une stratégie de sécurité IP » :

Racine de la console	Nom	Descript
Stratégies de séc	Créer une stratégie de sécurité IP Gérer les listes de filtres IP et les actions de filtrage Toutes les tâches	aff
	Affichage Nouvelle fenêtre à partir d'ici Nouvelle vue de la liste des tâches	•
	Actualiser Exporter la liste Aide	

- Nous cliquons sur « **Suivant** » :

Assistant Stratégie de sécurité	Ib	×
	Assistant Stratégie de sécurité IP	
	Cet Assistant vous permet de créer une stratégie de sécurité IP. Vous allez spécifier le niveau de sécurité à appliquer pour des communications avec des ordinateurs ou des groupes d'ordinateurs (sous-réseaux) spécifiques, ainsi que pour des types de trafic IP particuliers.	
	Cliquez sur Suivant pour continuer.	
	< Précédent Suivant > Annule	er

- Nous donnons un nom à la stratégie IP et cliquons sur « Suivant » :

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

Assistant Stratégie de sécurité IP		×
Nom de stratégie de sécurité IP Donnez un nom à cette stratégie de sécurité IP et fournissez une brève description.		
Nom :		
DemoIPsec		
Description :		
	*	
	-	
< Précédent Suivant >	Annul	er

# - Nous cliquons directement sur « Suivant » :

٢.
]

- Nous laissons la case cochée et cliquons sur « Terminer » :

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

Assistant Stratégie de sécurité	IP	×
	Fin de l'Assistant Stratégie de sécurité IP	
	Vous avez terminé de spécifier les propriétés pour votre nouvelle stratégie de sécurité IP.	
	Pour modifier votre stratégie de sécurité IP maintenant, activez la case à cocher Modifier les propriétés, puis cliquez sur Terminer.	
	Modifier les propriétés	
	Pour fermer cet Assistant, cliquez sur Terminer.	
	< Précédent Terminer Annule	er

- Nous cliquons sur « Ajouter » :



ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

- Nous cliquons sur « **Suivant** » :

Assistant Règle de sécurité	<b>—</b>
-3	Assistant Création d'une règle de sécurité IP
	Une règle de sécurité détermine le moment du déclenchement des actions de sécurité selon des critères tels que la source, la destination et le type de trafic IP définis dans la liste des filtres IP de la règle de sécurité.
	Une règle de sécurité contient un ensemble d'actions qui sont déclenchées lorsqu'une communication correspond au critère de la liste des filtres IP.
	Actions de sécurisation : - Attributs de tunnel IP - Méthodes d'authentification - Actions de filtrage
	Cliquez sur Suivant pour continuer.
	< Précédent Suivant > Annuler

- Nous cliquons directement sur « **Suivant** » :

Assistant Règle de sécurité	×
Point de sortie du tunnel Le point d'arrêt du tunnel est l'ordinateur de tunneling le plus proche de la destination du trafic IP, tel que spécifié par la liste de filtres IP de règles de sécurité.	
Un tunnel IPSec permet aux paquets de traverser un réseau public ou privé avec le même niveau de sécurité qu'une connexion privée directe entre deux ordinateurs.	
Spécifiez le point de terminaison du tunnel pour la règle de sécurité IP :	
Octte règle ne spécifie aucun tunnel	
Le point de terminaison du tunnel est spécifié par les adresses IP suivantes :	
Point de terminaison du tunnel IPv4 :	
Point de terminaison du tunnel IPv6 :	
< Précédent Suivant > Annu	ler

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

- Nous cliquons directement sur « Suivant » :

Assistant Règle de sécurité		×
<b>Type réseau</b> La règle de sécurité doit être appliquée à u	in type de réseau.	
Sélectionnez le type de réseau :		
Toutes les connexions réseau		
Réseau local		
Accès distant		
	< Précédent Suivant > An	nuler

- Nous cliquons sur « Ajouter » :

Assistant Règle de sécurité							
} Lis	Liste de filtres IP Sélectionner la liste de filtres IP pour le type de trafic IP auquel cette règle de sécurité s'applique.						
	Si aucun des filtres IP présents dans la liste suivante ne correspond à vos besoins, cliquez sur Ajouter pour en créer un nouveau.						
	Nom	Description	Ajouter				
			Modifier				
			Supprimer				
		< Pré	cédent Suivant > Ann	uler			

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

- Nous donnons un nom au filtre IP et cliquons sur « Ajouter » :

	Liste de	filtres IP			×
D		Une liste de filtres IP es adresses IP et protocole	t composée de plusieurs es peuvent être combiné	s filtres. Ainsi, plusieu és dans un seul filtre	rs sous-réseaux, IP.
	Nom :				
	Filtre 1				
	Descriptio	on :			Ajouter
				*	Modifier
				-	Supprimer
	Filtres IP	:		Vtiliser I	'Assistant Ajout
	Miroir	Description	Nom DNS source	Adresse source	1
	•				4
				ОК	Annuler

- Nous cliquons sur « Suivant » :



- Nous cliquons directement sur « Suivant » :

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

Assistant Filtre d'adresses IP	×	
Description du filtre IP et propriété mise en miroir Utilisez le champ Description pour spécifier un nom et une description détaillée pour le filtre IP. Sélectionnez la case à cocher Miroir afin de spécifier un filtre dans chaque direction.		
Description :		
Miroir. Faire coïncider les paquets possédant des adresses source et destination exactement opposées.		
< Précédent Suivant > Annu	uler	

- Pour la source du trafic IP, nous sélectionnons l'option « **Mon adresse IP** » et cliquons sur « **Suivant** » :

Assistant Filtre d'adresses IP	<b>X</b>
Source du trafic IP Spécifiez l'adresse source du trafic IP.	
Adresse source :	
Mon adresse IP	•
	< Précédent Suivant > Annuler

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

- Pour la destination du trafic IP, nous sélectionnons l'option « **Toute adresse IP** » et cliquons sur « **Suivant** » :

Assistant hare d'adresses IP	<b>×</b>
Destination du trafic IP Spécifiez l'adresse de destination du trafic	IP.
Adresse de destination :	
Toute adresse IP	•
	< Précédent Suivant > Annuler

- Nous cliquons directement sur « Suivant » :

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

Assistant Filtre d'adresses IP	×				
Type de protocole IP Sélectionnez le type de protocole IP. Si ce type est TCP ou UDP, vous spécifierez aussi la source et les ports de destination.					
Sélectionnez un type de protocole : N'importe lequel 0 Vimporte lequel 0 Vimporte lequel 0 Vimporte lequel 0 Vimporte lequel Vimporte lequel					
< Précédent Suivant > A	nnuler				

Nous cliquons directement sur « Terminer » :

-

-



Nous cliquons directement sur « OK » :

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

🖳 Liste de filtres IP 🥢 💌					
Talle <sup>1</sup>	Une liste de filtres IF adresses IP et proto	est composée de plusieur coles peuvent être combin	s filtres. Ainsi, plusieurs és dans un seul filtre II	s sous-réseaux, P.	
Nom :					
Filtre 1					
Descripti	on :			Ajouter	
			*	Modifier Supprimer	
Filtres IP	:		🔽 Utiliser l'/	Assistant Ajout	
Miroir	Description	Nom DNS source	Adresse source	1	
Oui		<mon adresse="" ip=""></mon>	<mon adresse="" ip=""></mon>	<	
•	III			•	
			ОК	Annuler	

- Nous sélectionnons le filtre et cliquons sur « Suivant » :

Assistant Règle de sécurité			<b>—</b> × <b>—</b>
Liste de filtres IP Sélectionner la liste de filtres IP pour le type de trafic IP auquel cette règle de sécurité s'applique.			
	Si aucun des filtres IP présents dans la liste suivante ne correspond à vos besoins, cliquez sur Ajouter pour en créer un nouveau.		
	Nom	Description	Ajouter
	Filtre1		Modifier Supprimer
< Précédent Suivant > Annuler			

- Nous cliquons sur « Ajouter » :

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

Assistant Règle de sécurité		<b>—</b>	
Sélectionner l'action de filtrage pour cette règle de sécurité.			
Si aucune action de filtrage ne correspond à vos besoins, cliquez sur Ajouter pour en créer une nouvelle. Sélectionnez Utiliser l'Assistant Ajout pour créer une action de filtrage en utilisant cette action.			
Actions de filtrage :		Utiliser l'Assistant Ajout	
Nom	Description	Ajouter	
		Modifier	
		Supprimer	
	< Précédent	Suivant > Annuler	

- Nous cliquons sur « Suivant » :

Assistant Action de filtrage	
	<ul> <li>Assistant Action de filtre de gécurité IP</li> <li>Utilisez l'Assistant pour spécifier les propriétés d'une nouvelle action de filtrage.</li> <li>Une action de filtrage définit les spécifications de sécurité pour le transfert de données. Ces spécifications sont contenues dans une liste des méthodes de sécurité intégrée à l'action de filtrage.</li> <li>Le transfert de données n'est possible que lorsque les ordinateurs concemés utilisent les mêmes méthodes de sécurité. Les méthodes de sécurité multiples augmentent la probabilité de correspondance des méthodes utilisées par deux ordinateurs.</li> <li>Cliquez sur Suivant pour continuer.</li> </ul>
	< Précédent Suivant > Annuler

- Nous donnons un nom à l'action de filtrage et cliquons sur « Suivant » :

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

Assist	ant Action de filtrage	×
No	om d'action de filtrage Donnez un nom à cette action de filtrage et une brève description.	
	Nom :	
	Action 1	
	Description :	
		*
		Ŧ
	< Précédent Suivant > Ar	nuler

- Nous laissons la case cochée « Négocier la sécurité » et cliquons sur « Suivant » :

Assistant Action de filtrage		×
Options générales d'actions de filtrage Définissez le comportement de l'action de f	filtrage.	
Autoriser		
Refuser		
Négocier la sécurité		
	< Précédent Suivant > Annuk	er

- Nous cliquons directement sur « Suivant » :

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

A stant Action de filtrage	
Communiquer avec des ordinateurs qui ne prennent pas en charge IPSec Communiquer avec des ordinateurs qui ne prennent pas en charge IPsec peut entraîner des risques pour la sécurité de votre réseau.	
Autorisez-vous les communications avec des ordinateurs qui ne prennent pas en charge IPSec ?	
Ne pas autoriser les communications non sécurisées.	
Autoriser les communications non sécurisées si aucune connexion sécurisée ne peut être établie.	
Utilisez cette option si votre réseau comporte des ordinateurs qui ne prennent pas en charge IPsec ou qui ont une configuration IPsec incompatible. L'autorisation d'une communication non sécurisée peut exposer votre réseau à des risques pour la sécurité.	
Sur un ordinateur équipé de Windows Vista ou une version plus récente de Windows, cette option permet l'envoi d'une communication non sécurisée chaque fois qu'une connexion sécurisée ne peut pas être établie.	
Sur un ordinateur Windows 2000, Windows XP ou Windows 2003, cette option permet l'envoi de communications non sécurisées uniquement lorsque l'ordinateur distant ne prend pas en charge IPsec.	
< Précédent Suivant > Annuler	

#### - Nous cliquons directement sur « Suivant » :

Assistant Action de filtrage	×
Sécurité du trafic IP Spécifiez une méthode de sécurité pour le trafic IP. Pour ajouter plusieurs méthodes de sécurité, modifiez l'action de filtrage après avoir terminé l'Assistant.	
Cette action de filtrage nécessite au moins une méthode de sécurité pour le trafic IP.	
<ul> <li>Intégrité et chiffrement Les données seront chiffrées, authentifiées et non modifiées.</li> </ul>	
<ul> <li>Intégrité uniquement</li> <li>Les données seront authentifiées et non modifiées, mais ne seront pas chiffrées.</li> </ul>	
Personnalisée     Paramètres	
< Précédent Suivant > Annu	ler

- Nous cliquons directement sur « Terminer » :

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

Assistant Action de filtrage	
-2	Fin de l'Assistant Action de filtrage de sécurité IP
	Vous avez terminé l'exécution de l'Assistant Action de filtrage de sécurité IP.
	Pour modifier l'action du filtre maintenant, sélectionnez la case à cocher Modifier les propriétés puis cliquez sur Terminer.
	Modifier les propriétés
	Pour fermer cet Assistant, cliquez sur Terminer.
	< Précédent Terminer Annuler

- Nous sélectionnons l'action et cliquons sur « Suivant » :

Assistant Règle de sécurité		<b>—</b>
Action de filtrage Sélectionner l'action de	e filtrage pour cette règle de sécurité.	
Si aucune action de filtr créer une nouvelle. Sél filtrage en utilisant cette	rage ne correspond à vos besoins, cliq ectionnez Utiliser l'Assistant Ajout pour e action.	juez sur Ajouter pour en r créer une action de
Actions de filtrage :		Viliser l'Assistant Ajout
Nom	Description	Ajouter
Action 1		Modifier Supprimer
	< Précédent	Suivant > Annuler

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

 Ensuite, nous cliquons sur « Utiliser cette chaîne pour protéger l'échange de clés », nous donnons un nom à la chaîne pour une clé pré-partagée et cliquons sur « Suivant » :

Assistant Règle de sécurité	×	
Méthode d'authentification Pour ajouter plusieurs méthodes d'authentification, modifiez la règle de sécurité après avoir terminé l'exécution de l'Assistant.		
Définissez la méthode d'authentification initiale pour cette règle de sécurité :		
Authentification Active Directory par défaut (protocole Kerberos v.5)		
Utiliser un certificat émis par cette autorité de certification :		
Parcourir		
Exclure le nom de l'autorité de certification de la requête de certificat		
Activer le certificat vers le mappage de compte		
Ottiliser cette chaîne pour protéger l'échange de clés (clé pré-partagée) :		
LPASRSI *		
< Précédent Suivant > Annu	ler	

- Nous cliquons directement sur « Terminer » :

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

Assistant Règle de sécurité	<b>•</b>	
	Fin de l'Assistant Règle de sécurité	
•	Vous avez terminé de spécifier les propriétés pour votre nouvelle règle.	
	Pour modifier vos règles de sécurité maintenant, sélectionnez la case à cocher Modifier les propriétés, puis cliquez sur Terminer.	
	Modifier les propriétés	
	Pour fermer cet Assistant, cliquez sur Terminer.	
	< Précédent Terminer Annuler	

- Nous cliquons directement sur « **OK** » :

Propriétés de : DemoIPsec	:	-?	×
Règles Général			
Règles de séc distants	curité pour communiquer a	vec des ordinateurs	1
Règles de sécurité IP :			
Liste de filtres IP	Action de filtrage	Méthodes d'a	Poi
Filtre 1	Action1	Clé pré-partagée	Au
Oynamique>	Réponse par défaut	Kerberos	<a< td=""></a<>
•	III		4
Ajouter Modif	ier Supprimer	Utiliser l'Assistant	t Ajout
		OK Anr	nuler

ETTORI Bastien	BTS SIO 2 <sup>ème</sup> année
08 avril 2016	Année scolaire : 2015/2016
Option : SISR	Version 1.0

 Ensuite, nous sélectionnons « Stratégie de sécurité IP sur ordinateur local » à la « Racine de la console », faisons un clic droit sur la stratégie de sécurité IP créée et cliquons sur « Attribuer » :



Nous constatons que cette stratégie a bien été attribuée et devons enregistrer les paramètres de la console :

Racine de la console	Nom	Description	Stratégie attribuée
Stratégies de sécurit	🖾 DemoIPsec		Oui

Maintenant, nous nous rendons sur la seconde machine où nous n'avons pas encore mis en place la procédure du réseau **VPN** et testons la communication de la première machine en tapant son adresse IP avec la commande « **ping** » :

C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7600] Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.
C:\Users\ettori>ping 192.168.123.202
Envoi d'une requête 'Ping' 192.168.123.202 avec 32 octets de données : Délai d'attente de la demande dépassé. Délai d'attente de la demande dépassé. Délai d'attente de la demande dépassé. Délai d'attente de la demande dépassé.
Statistiques Ping pour 192.168.123.202: Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
C:\Users\ettori>

Nous constatons que les 2 machines ne communiquent pas entre elles.

- Donc, maintenant, nous devons réaliser la même procédure sur le deuxième poste.

#### V) <u>Conclusion</u>

-

En conclusion, nous pouvons dire que le **Réseau VPN Poste à poste** est mis en place car les 2 ordinateurs se situent sur un réseau privé et permet donc la sécurisation des échanges entre les machines.