Activité 8 - Stormshield
VPN IPsec site à site

Votre objectif

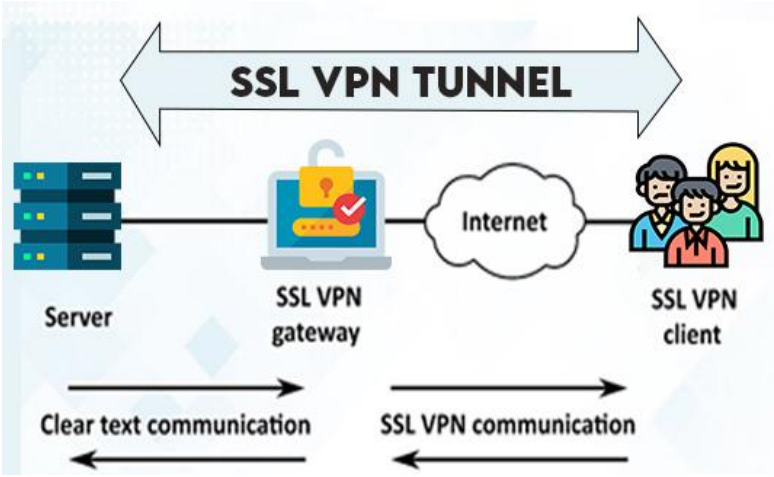
Les objectifs de l'activité est de mettre en place un VPN IPsec entre les réseaux de deux entreprises.

Les trois familles de VPN

- 1 - PPTP : Point-to-Point Tunneling Protocol

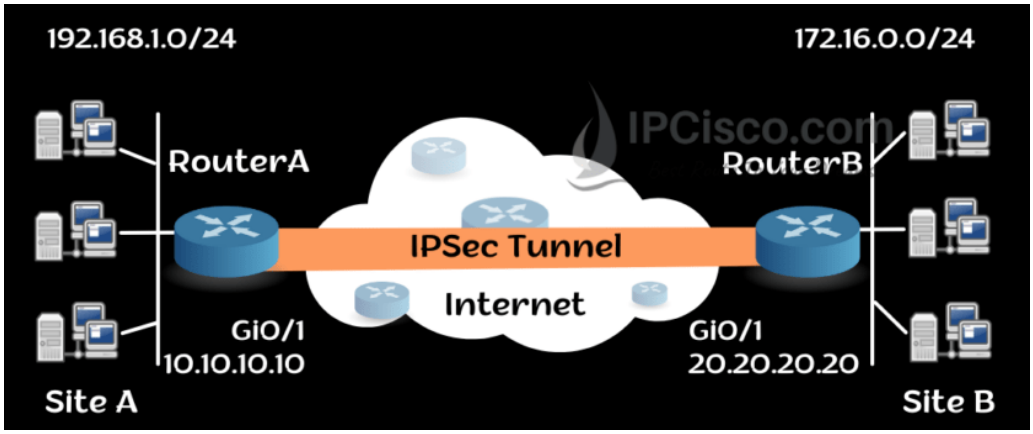
Cette solution est obsolète en raison des risques de sécurité.

- 2 - VPN SSL (Secure Sockets Layer) : Pour clients nomades uniquement



Ce VPN utilise le protocole SSL/TLS (Transport Layer Security) pour établir une connexion sécurisée entre un client et un serveur via un simple navigateur web.
Ils sont utilisés pour fournir un accès sécurisé aux applications et ressources internes d'une entreprise à partir d'emplacements distants. Cela est particulièrement utile pour les employés en déplacement ou en télétravail qui ont besoin d'accéder de manière sécurisée aux ressources de l'entreprise.
Ce type de VPN n'offre pas le même niveau de performance que les VPN basés sur IPsec.

- 3 - VPN IPsec : Pour tunnels site-à-site ou clients nomades



IPsec (Internet Protocol Security) est un ensemble de protocoles pour sécuriser les communications sur les réseaux IP en authentifiant et en chiffrant chaque paquet IP dans un flux de données.

IPsec est utilisé pour mettre en place des réseaux privés virtuels (VPN) afin de sécuriser les échanges de données entre un client et un serveur ou entre deux réseaux d'entreprise.

IPsec fonctionne en deux modes principaux :

- Le mode transport chiffre uniquement la charge utile des paquets IP.
- Le mode tunnel chiffre l'ensemble du paquet IP et est généralement utilisé pour les connexions VPN site-à-site.

Les principales caractéristiques d'IPsec
Authentification IPsec utilise des protocoles comme AH (Authentication Header) pour assurer l'authenticité des paquets de données. **Chiffrement** IPsec utilise des protocoles comme ESP (Encapsulating Security Payload) pour chiffrer les données, assurant ainsi leur confidentialité. **Gestion des clés** IPsec utilise des protocoles comme IKE (Internet Key Exchange) pour échanger les clés de chiffrement de manière sécurisée.

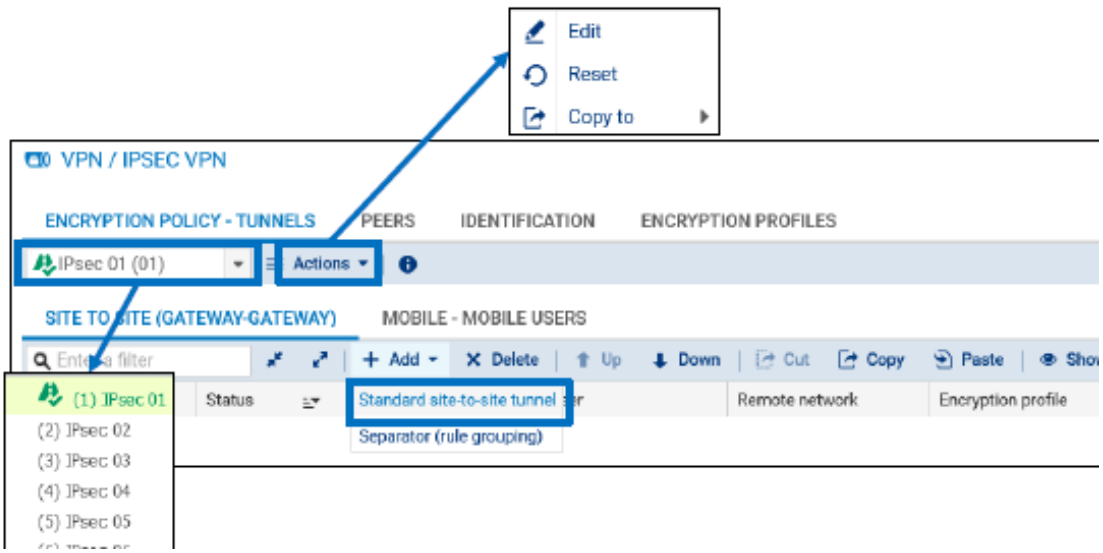
Comparatif	
VPN SSL	**VPN IPsec**
Couche 7 du modèle OSI	Couche 3 du modèle OSI
Utilisé via un navigateur web	Logiciel spécifique
Simple à déployer	Complexe à configurer
Moins performant	Meilleures performances
Sécurité correcte	Sécurité robuste

☞ 1 – Copiez la politique de filtrage/NAT **(7) Activite_7** vers la politique numéro 8. Renommez la politique "**Activite_8**", puis activez cette politique (bouton "**Appliquer**" en bas de la page).

☞ 2 – Si elle ne figure pas dans la liste des règles de filtrage, ajoutez la règle **Pass any any any** en tête de cette politique.

Travail à faire (Questions 3 à 10)
Configurez un tunnel IPsec avec une authentification par PSK pour relier votre réseau interne 192.168.1.0/24 à celui d'un autre étudiant présent dans la salle. Vous utiliserez les profils de chiffrement par défaut (StrongEncryption).

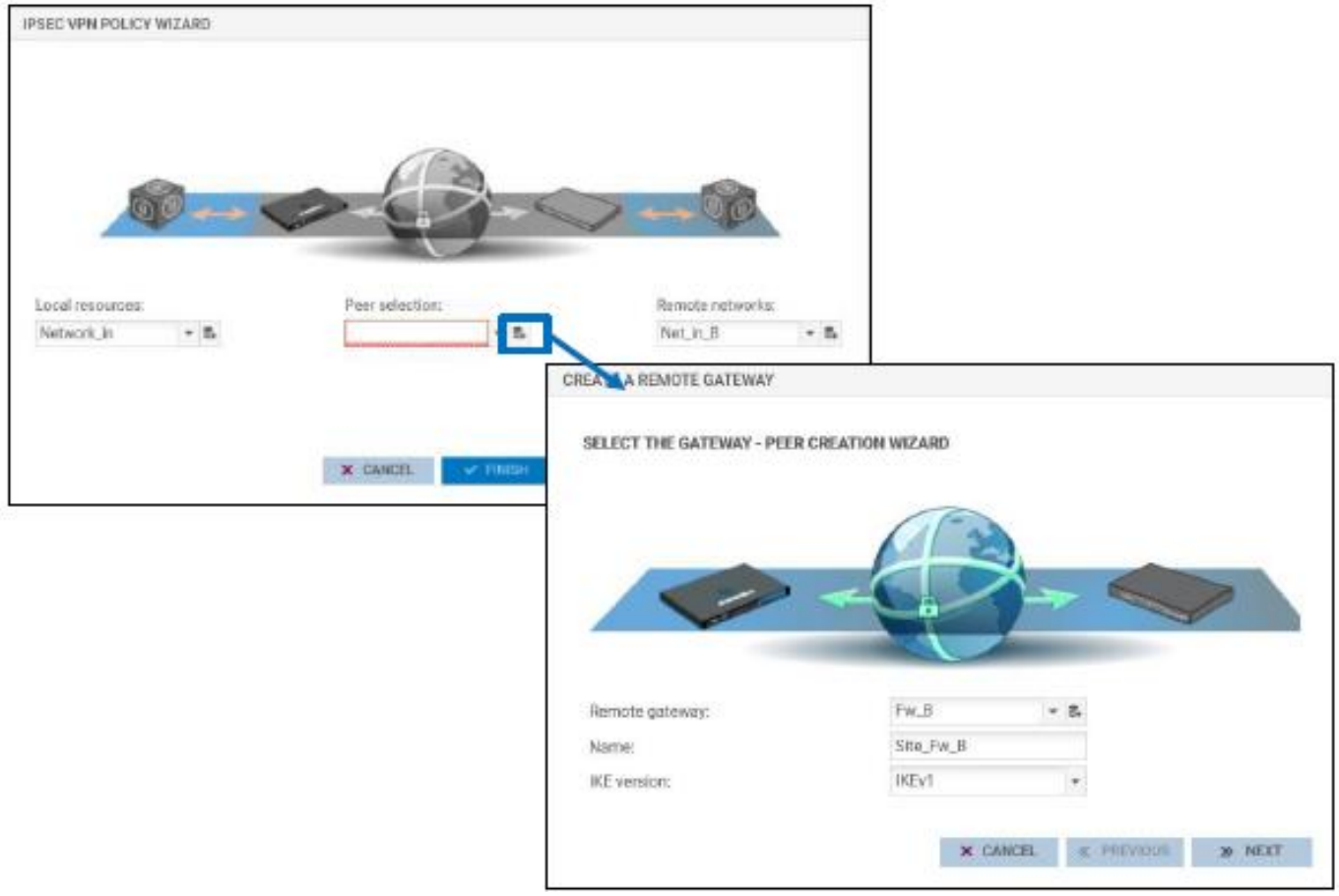
☞ 3 – La configuration d'un tunnel VPN IPsec site-a-site s'effectue depuis le menu **VPN ⇒ VPN IPsec** > onglet **POLITIQUE DE CHIFFREMENT – TUNNELS** > onglet **SITE À SITE (GATEWAY – GATEWAY)**, en cliquant sur Ajouter ⇒ **Tunnel site à site**.



☞ 4 – Un assistant s'affiche pour renseigner les principaux paramètres : les extrémités de trafic (réseaux local et réseau distant) et l'extrémité de tunnel distante (le correspondant).
Vous sélectionnerez "Network_In" pour la ressource locale. C'est votre réseau , le point de départ du VPN.

☞ 5 – Normalement, votre correspondant n'existe pas. Il faut le créer en cliquant sur le bouton **AJOUTER** (bleu) qui sera utilisé pour la négociation du tunnel. Un nouvel assistant s'affiche pour renseigner les paramètres du correspondant :

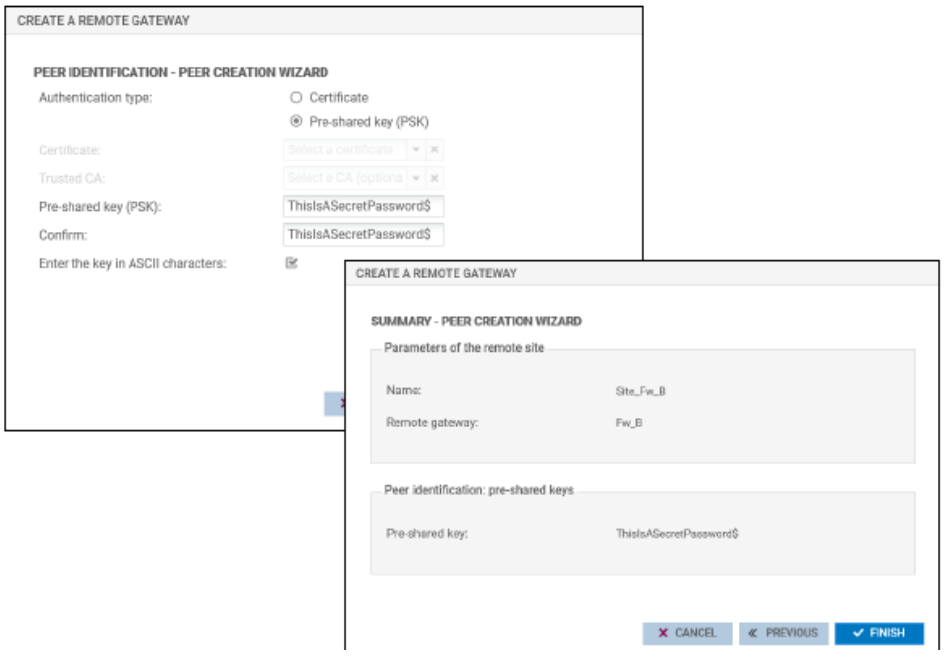
- La passerelle distante : Créez un objet "Reseau_distant" ayant l'adresse IP du port "OUT" de votre correspondant.
- le nom de votre correspondant (nom étudiant)
- la version IKE (1 ou 2). Par défaut, la version IKE 2 est utilisée.



☞ 6 – Cliquez sur **Suivant**, l'assistant se poursuit et il est possible de configurer la méthode d'authentification. En sélectionnant PSK, la clé pré-partagée renseignée sera associée à l'identité du correspondant.

Enfin, la dernière étape liste les paramètres renseignés et permet éventuellement d'ajouter une passerelle de secours (non utilisé dans votre cas).

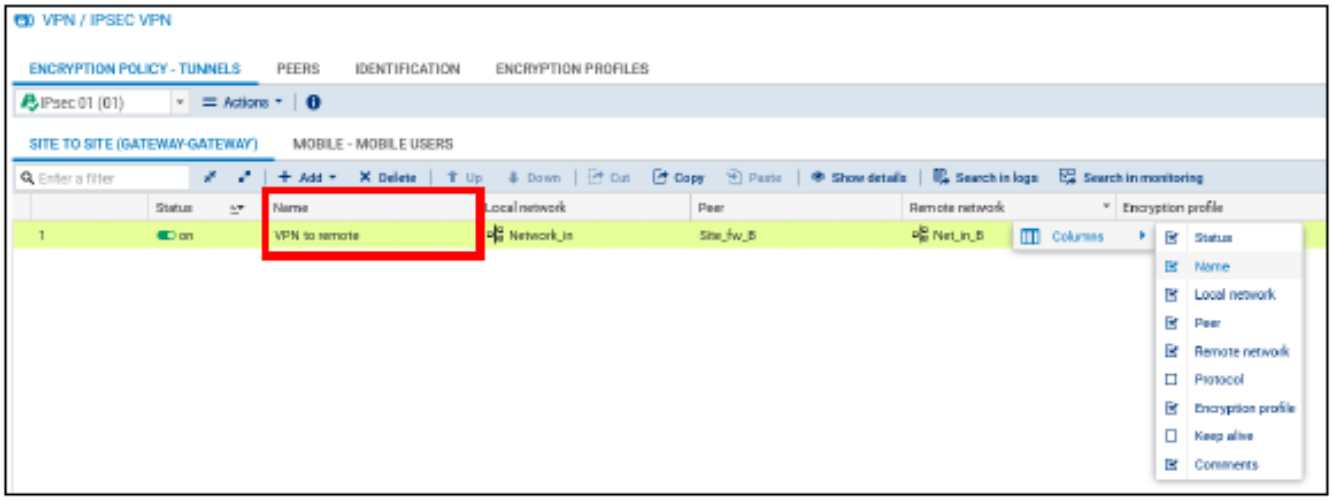
Vos cliquerez sur **Terminer** (retour sur l'assistant VPN).



☞ 7 – Créez un objet pour nommer le réseau de votre correspondant "Reseau_2".
Une fois les trois paramètres (réseau local, réseau distant et le correspondant) renseignés, vous pouvez cliquer sur Terminer.

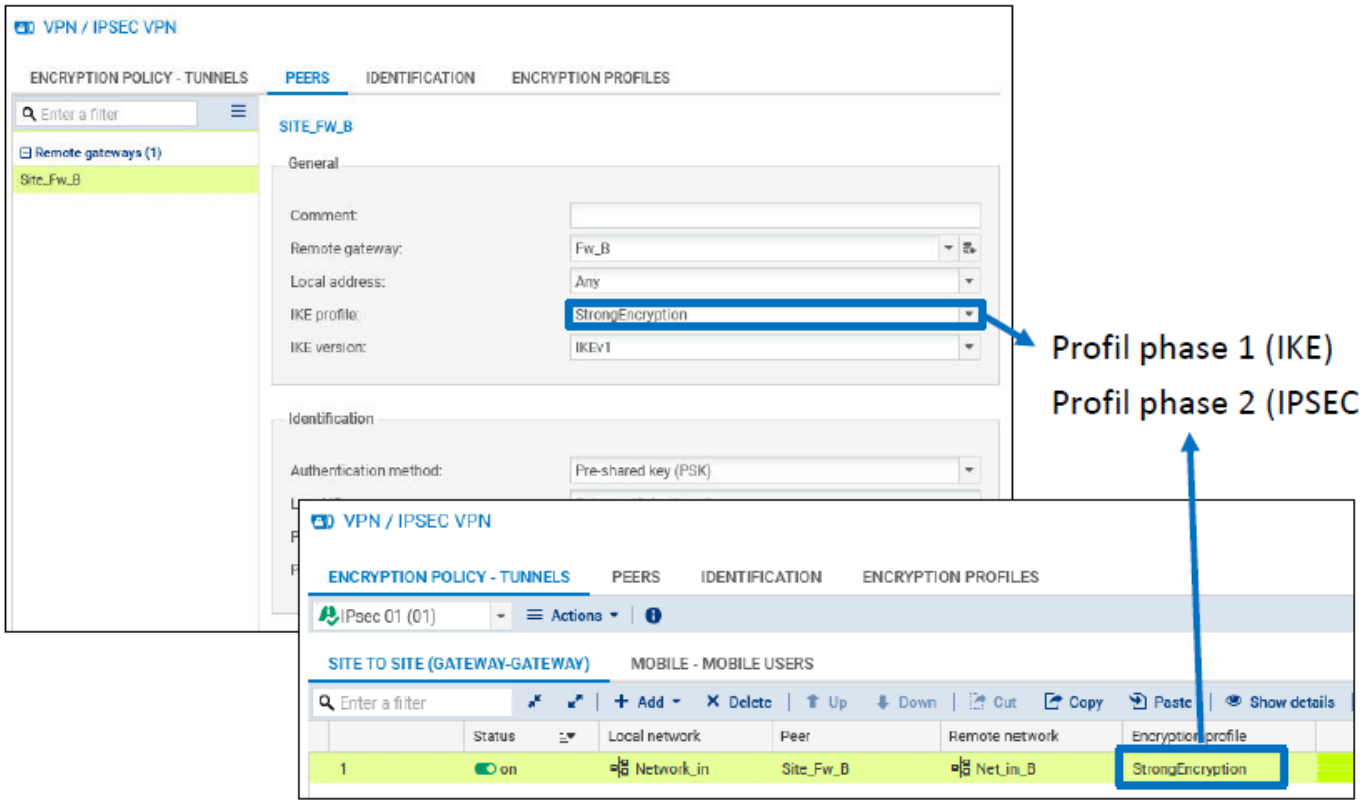
Le tunnel VPN IPsec est ajouté sur une ligne distincte de la politique. La politique est désactivée par défaut. Activez manuellement la politique.

☞ 8 – La colonne Nom peut être cachée par défaut ; pour la faire apparaître, cliquez sur l'en-tête de colonne, puis sélectionnez le menu Colonnes et cocher l'option Nom.
Elle affiche le nom des politiques. Dans les traces VPN, l'entrée "Nom de la règle" se rapporte à ce nom.



NOTE : Un champ qui précise le type de règle VPN (tunnel mobile ou tunnel site-àsite) a été ajouté aux traces VPN IPsec également.

☞ 9 – Le profil de chiffrement phase 1 appelé également profil IKE est configuré au niveau du correspondant, tandis que le profil de chiffrement phase 2, appelé profil IPSEC est configuré au niveau du tunnel VPN.



☞ 10 – Générez du trafic correspondant aux extrémités de trafic et suivez les étapes de négociation des tunnels et l'activité dans les tunnels depuis les journaux et le menu de supervision correspondants.