vpn-ipsec

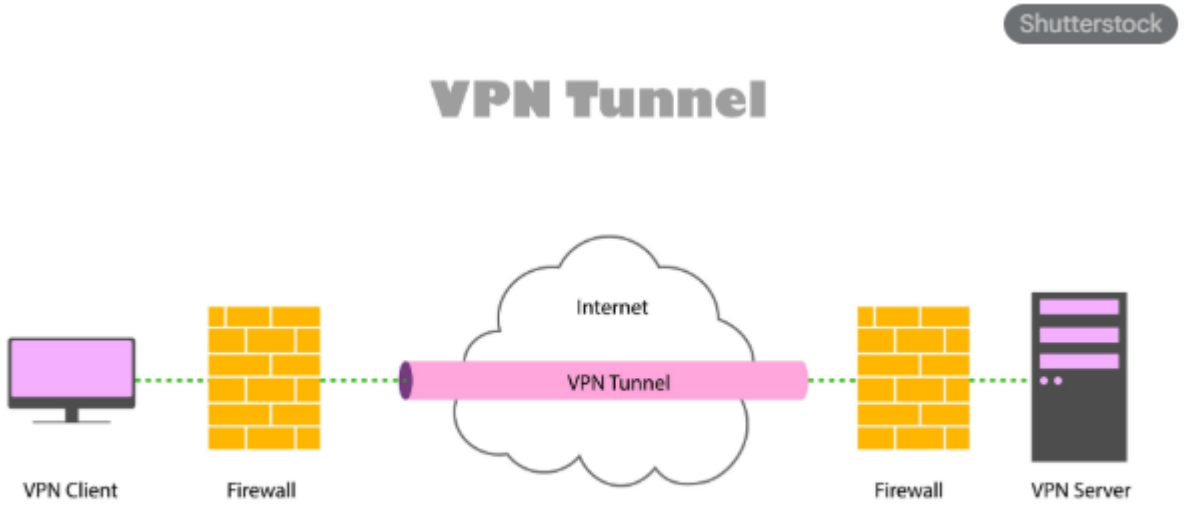
```
      MARK RODERICK  - VPN IPSEC
```

Qu'est-ce qu'un VPN IPsec ?

IPsec signifie **Internet Protocol Security**. **VPN** signifie **Virtual Private Network** (Réseau Privé Virtuel).

En combinant les deux, un **VPN IPsec** est un ensemble de protocoles utilisés pour créer une connexion sécurisée et chiffrée (un "tunnel") entre deux points via un réseau public comme Internet. Il fonctionne au niveau de la **Couche Réseau (Couche 3)** du modèle OSI, ce qui signifie qu'il sécurise les paquets de données avant même qu'ils ne soient transportés vers l'application de réception.

> **L'Analogie :** Imaginez l'envoi d'une lettre.
>
> - **Internet Standard :** Vous envoyez une carte postale. N'importe qui manipulant le courrier peut lire ce qui est écrit au dos.
> - **VPN IPsec :** Vous placez la lettre dans un coffre-fort blindé. Seule la personne possédant la clé correspondante peut ouvrir le coffre pour lire la lettre.



Les Fonctions de Sécurité Principales

IPsec assure la sécurité à travers trois fonctions majeures (souvent appelées la triade CIA en sécurité) :

1. **Confidentialité (Chiffrement) :** Il brouille les paquets de données afin qu'ils soient illisibles pour un pirate qui les intercepterait. Les algorithmes courants incluent **AES**

(Advanced Encryption Standard).

2. **Intégrité :** Il garantit que les données n'ont pas été modifiées durant le transit. Si un paquet est altéré en cours de route, le récepteur le rejettera (grâce à des algorithmes de hachage comme SHA-2).
3. **Authentification :** Il vérifie que les données proviennent bien d'une source de confiance. Les deux appareils (ex: un pare-feu et un ordinateur portable) doivent prouver leur identité mutuelle via des mots de passe, des certificats numériques ou des clés pré-partagées (PSK).

Les Deux Modes d'IPsec

IPsec peut fonctionner selon deux modes différents selon le besoin :

Mode	Description	Utilisation idéale
Mode Tunnel	Chiffre le **paquet IP entier** (les données + l'en-tête original) et l'encapsule dans un nouveau paquet.	**VPN Site-à-Site** (ex: connecter une filiale au siège social).
Mode Transport	Chiffre **uniquement la charge utile** (les données), laissant l'en-tête IP original lisible pour le routage.	**Communication de bout en bout** entre deux serveurs spécifiques.

Les Protocoles sous le Capot

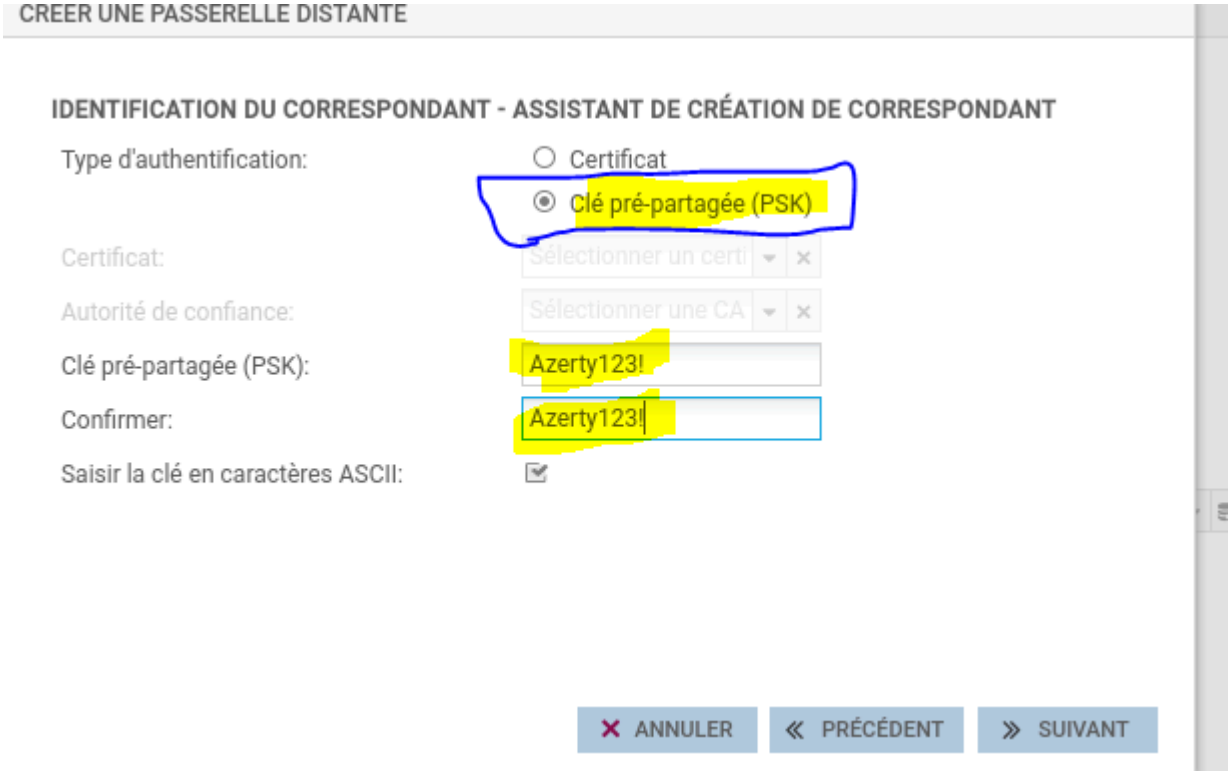
IPsec n'est pas un protocole unique, mais une "suite" de protocoles travaillant ensemble :

- **IKE (Internet Key Exchange) :** C'est le négociateur. Il établit la connexion initiale (Phase 1 et Phase 2), décide des méthodes de chiffrement à utiliser et échange les clés de sécurité de manière sûre.
- **ESP (Encapsulating Security Payload) :** C'est le "cheval de trait". Il assure le chiffrement, l'authentification et l'intégrité des données réelles. C'est le protocole le plus utilisé aujourd'hui.
- **AH (Authentication Header) :** Il offre l'authentification et l'intégrité, mais **pas le chiffrement**. Il est rarement utilisé seul de nos jours car il ne cache pas les données.

edd

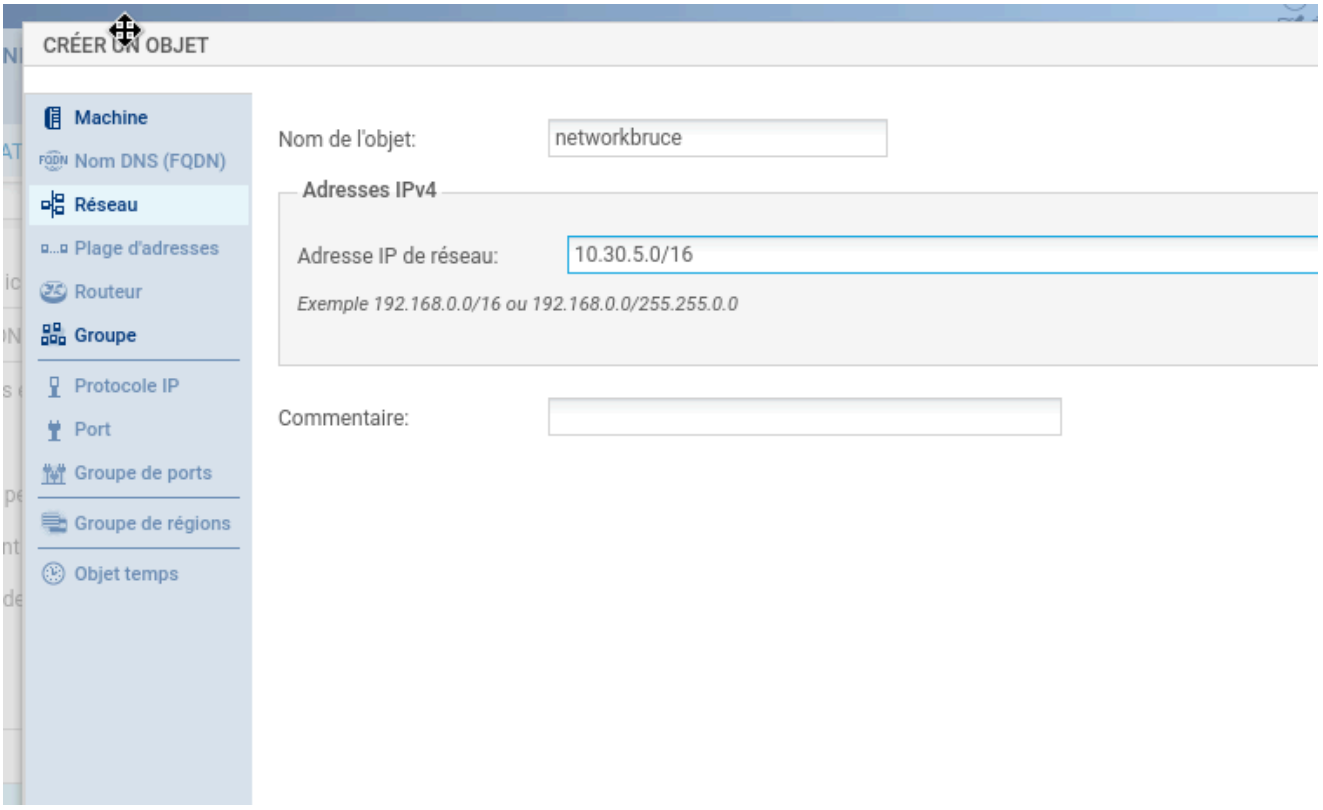
etape 1

etape 2



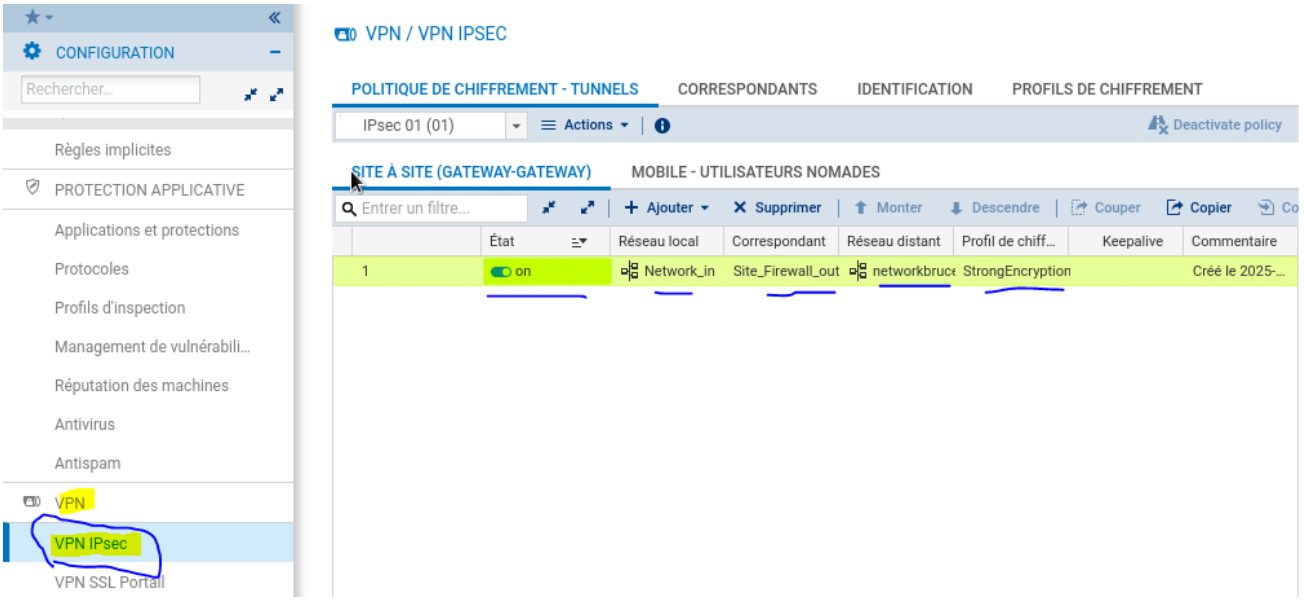
etape 3


CRÉER UNE PASSERELLE DISTANTE
RÉSUMÉ - ASSISTANT DE CRÉATION DE CORRESPONDANT
Paramètres du site distant
Nom:
Site_Firewall_out
Passerelle distante:
Firewall_out
Identification du correspondant : clé pré-partagée
Clé pré-partagée:
Azerty123!
ANNULER
PRÉCÉDENT
TERMINER


CRÉER UN OBJET
Machine
Nom DNS (FQDN)
Réseau
Plage d'adresses
Routeur
Groupe
Protocole IP
Port
Groupe de ports
Groupe de régions
Objet temps
Nom de l'objet:
networkbruce
Adresses IPv4
Adresse IP de réseau:
10.30.5.0/16
Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0
Commentaire:


ASSISTANT DE POLITIQUE VPN IPSEC
Ressources locales:
Network_in
Choix du correspondant:
Site_Firewall_out
Réseaux distants:
networkbruce
ANNULER
TERMINER

regle crée


CONFIGURATION
Rechercher...
Règles implicites
PROTECTION APPLICATIVE
Applications et protections
Protocoles
Profils d'inspection
Management de vulnérabili...
Réputation des machines
Antivirus
Antispam
VPN
VPN IPsec
VPN SSL Portail
VPN / VPN IPSEC
POLITIQUE DE CHIFFREMENT - TUNNELS
CORRESPONDANTS
IDENTIFICATION
PROFILS DE CHIFFREMENT
IPsec 01 (01)
Actions
Deactivate policy
SITE À SITE (GATEWAY-GATEWAY)
MOBILE - UTILISATEURS NOMADES
Entrer un filtre...
Ajouter
Supprimer
Monter
Descendre
Couper
Copier
État
Réseau local
Correspondant
Réseau distant
Profil de chiff...
Keepalive
Commentaire
1
on
Network_in
Site_Firewall_out
networkbruce
StrongEncryption
Créé le 2025-...