# Configuration d'un tunnel VPN site à site entre le routeur VPN double WAN Gigabit Cisco RV320 et l'adaptateur de services intégrés Cisco 500

## Objectif

Un réseau privé virtuel (VPN) existe en tant que technologie largement utilisée pour connecter des réseaux distants à un réseau privé principal, simulant une liaison privée sous la forme d'un canal crypté sur des lignes publiques. Un réseau distant peut se connecter à un réseau principal privé comme s'il faisait partie du réseau principal privé sans problème de sécurité en raison d'une négociation en deux phases qui chiffre le trafic VPN d'une manière que seuls les points d'extrémité VPN savent comment le déchiffrer.
Ce guide rapide fournit un exemple de conception pour la construction d'un tunnel VPN IPsec site à site entre un adaptateur de services intégrés de la gamme Cisco 500 et un routeur de la gamme Cisco RV.

## Périphériques pertinents

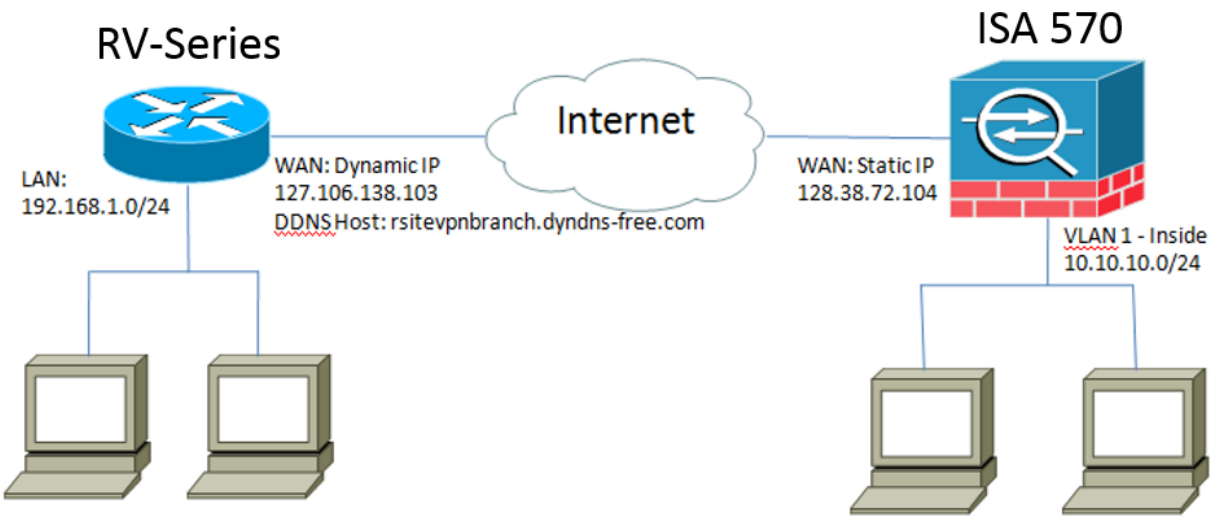
Routeurs · gamme Cisco RV (RV320)
· adaptateurs de services intégrés de la gamme Cisco 500 (ISA570)

## Version du logiciel

·4.2.2.08 [Routeurs VPN de la gamme Cisco RV0xx]

## Préconfiguration

Diagramme du réseau
La topologie VPN site à site est présentée ci-dessous.




Un tunnel VPN IPsec site à site est configuré et établi entre le routeur Cisco RV du bureau distant et l'ISA de la gamme Cisco 500 du bureau principal.
Avec cette configuration, un hôte du réseau local 192.168.1.0/24 au bureau distant et un hôte du réseau local 10.10.10.0/24 au bureau principal peuvent communiquer entre eux en toute sécurité via un réseau privé virtuel.

# Concepts de base

## IKE (Internet Key Exchange)

Internet Key Exchange (IKE) est le protocole utilisé pour configurer une association de sécurité (SA) dans la suite de protocoles IPsec. IKE s'appuie sur le protocole Oakley, Internet Security Association et le protocole ISAKMP (Key Management Protocol) et utilise un échange de clés Diffie-Hellman pour configurer un secret de session partagé, à partir duquel les clés cryptographiques sont dérivées.

## ISAKMP (Internet Security Association and Key Management Protocol)

Le protocole ISAKMP (Internet Security Association and Key Management Protocol) est utilisé pour négocier le tunnel VPN entre deux points d'extrémité VPN. Il définit les procédures d'authentification, de communication et de génération de clés et est utilisé par le protocole IKE pour échanger des clés de chiffrement et établir la connexion sécurisée.

## Sécurité du protocole Internet (IPsec)

IP Security Protocol (IPsec) est une suite de protocoles permettant de sécuriser les communications IP en authentifiant et en chiffrant chaque paquet IP d'un flux de données. IPsec inclut également des protocoles pour établir l'authentification mutuelle entre les agents au début de la session et la négociation des clés cryptographiques à utiliser pendant la session.  IPsec peut être utilisé pour protéger les flux de données entre deux hôtes, passerelles ou réseaux.

## Conseils de conception

**Topologie VPN** - Une topologie VPN point à point signifie qu'un tunnel IPsec sécurisé est configuré entre le site principal et le site distant.
Les entreprises ont souvent besoin de plusieurs sites distants dans une topologie multisite et mettent en oeuvre une topologie VPN en étoile ou une topologie VPN à maillage global. Une topologie VPN en étoile signifie que les sites distants n'ont pas besoin de communication avec d'autres sites distants et que chaque site distant établit uniquement un tunnel IPsec sécurisé avec le site principal. Une topologie VPN à maillage global signifie que les sites distants doivent communiquer avec d'autres sites distants, et chaque site distant établit un tunnel IPsec sécurisé avec le site principal et tous les autres sites distants.
**Authentification VPN** - Le protocole IKE est utilisé pour authentifier les homologues VPN lors de l'établissement d'un tunnel VPN. Il existe différentes méthodes d'authentification IKE et la clé pré-partagée est la méthode la plus pratique. Cisco recommande l'application d'une clé forte prépartagée.
**Cryptage VPN** - Pour garantir la confidentialité des données transportées sur le VPN, des algorithmes de chiffrement sont utilisés pour chiffrer la charge utile des paquets IP. DES, 3DES et AES sont trois normes de cryptage courantes. AES est considéré comme le plus sécurisé par rapport aux DES et 3DES. Cisco recommande vivement l'application d'un cryptage AES-128 bits ou supérieur (par exemple, AES-192 et AES-256). Cependant, des algorithmes de chiffrement plus puissants nécessitent davantage de ressources de traitement de la part d'un routeur.
**Dynamic WAN IP Addressing and Dynamic Domain Name Service (DDNS)** : le tunnel VPN doit être établi entre deux adresses IP publiques. Si les routeurs WAN reçoivent des adresses IP statiques du fournisseur d'accès à Internet (FAI), le tunnel VPN peut être mis en oeuvre directement à l'aide d'adresses IP publiques statiques. Cependant, la plupart des petites entreprises utilisent des services Internet haut débit économiques tels que la DSL ou le câble et reçoivent des adresses IP dynamiques de leurs FAI. Dans de tels cas, le service DDNS (Dynamic Domain Name Service) peut être utilisé pour mapper l'adresse IP dynamique à un nom de domaine complet (FQDN).
**Adressage IP LAN** - L'adresse réseau IP LAN privée de chaque site ne doit pas comporter de chevauchement. L'adresse réseau IP LAN par défaut de chaque site distant doit toujours être modifiée.

## Conseils de configuration

### Liste de contrôle de préconfiguration

Étape 1. Connectez un câble Ethernet entre le RV320 et son modem DSL ou câble, et un câble Ethernet entre le ISA570 et son modem DSL ou câble.
Étape 2. Mettez le routeur RV320 sous tension, puis connectez les ordinateurs, les serveurs et les autres périphériques IP internes aux ports LAN du routeur RV320.
Étape 3. Mettez le ISA570 sous tension, puis connectez les ordinateurs, les serveurs et les autres périphériques IP internes aux ports LAN du ISA570.
Étape 4. Assurez-vous de configurer les adresses IP réseau de chaque site sur différents sous-réseaux. Dans cet exemple, le réseau local du bureau distant utilise 192.168.1.0 et le réseau local du bureau principal utilise 10.10.10.0.
Étape 5. Assurez-vous que les PC locaux sont en mesure de se connecter à leurs routeurs respectifs et à d'autres PC sur le même réseau local.

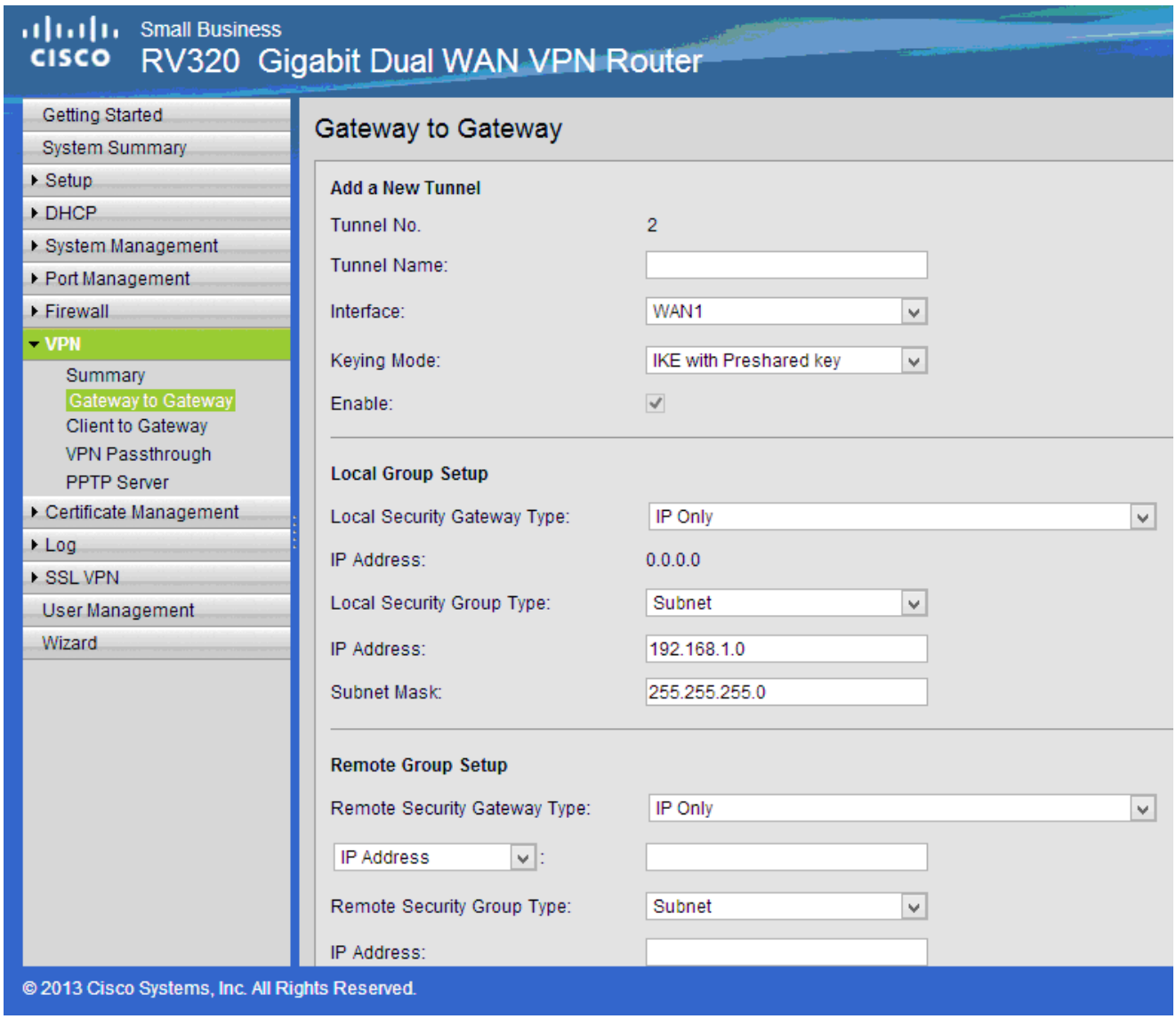
## Identification de la connexion WAN

Vous devez savoir si votre FAI fournit une adresse IP dynamique ou une adresse IP statique. Le FAI fournit généralement une adresse IP dynamique, mais vous devez le

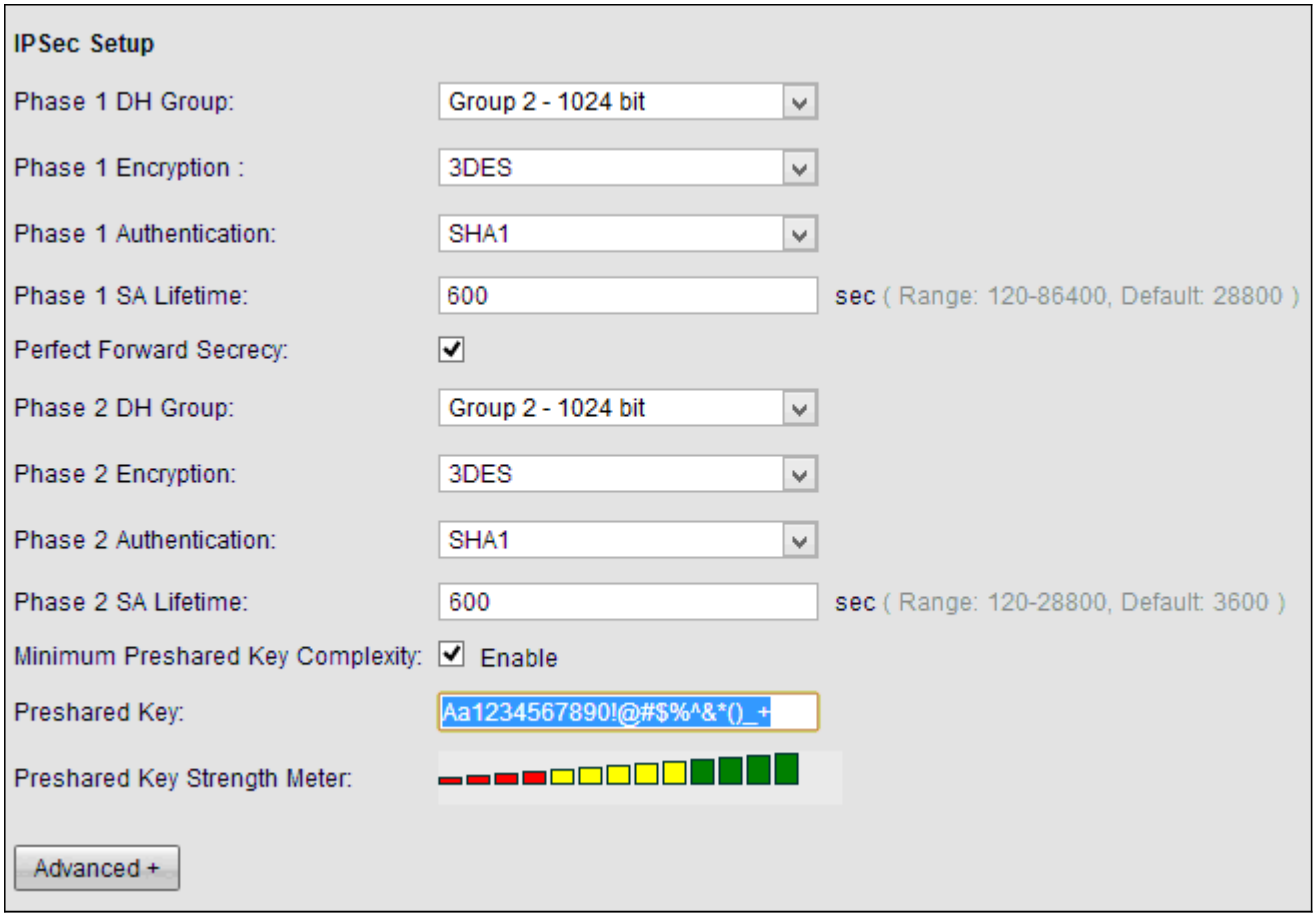
confirmer avant de terminer la configuration du tunnel VPN site à site.

## Configuration du tunnel VPN IPsec site à site pour RV320 sur le site distant

Étape 1. Accédez à **VPN > Gateway-to-Gateway** (voir l'image)
a.) Entrez un nom de tunnel, tel que RemoteOffice.
b.) Définissez l'interface sur WAN1.
c.) Définissez le mode de clé sur IKE avec la clé prépartagée.
d.) Saisissez Local IP Address (Adresse IP locale) et Remote IP Address (Adresse IP distante).
L'image suivante présente la page Passerelle de routeur VPN double WAN Gigabit RV320 :



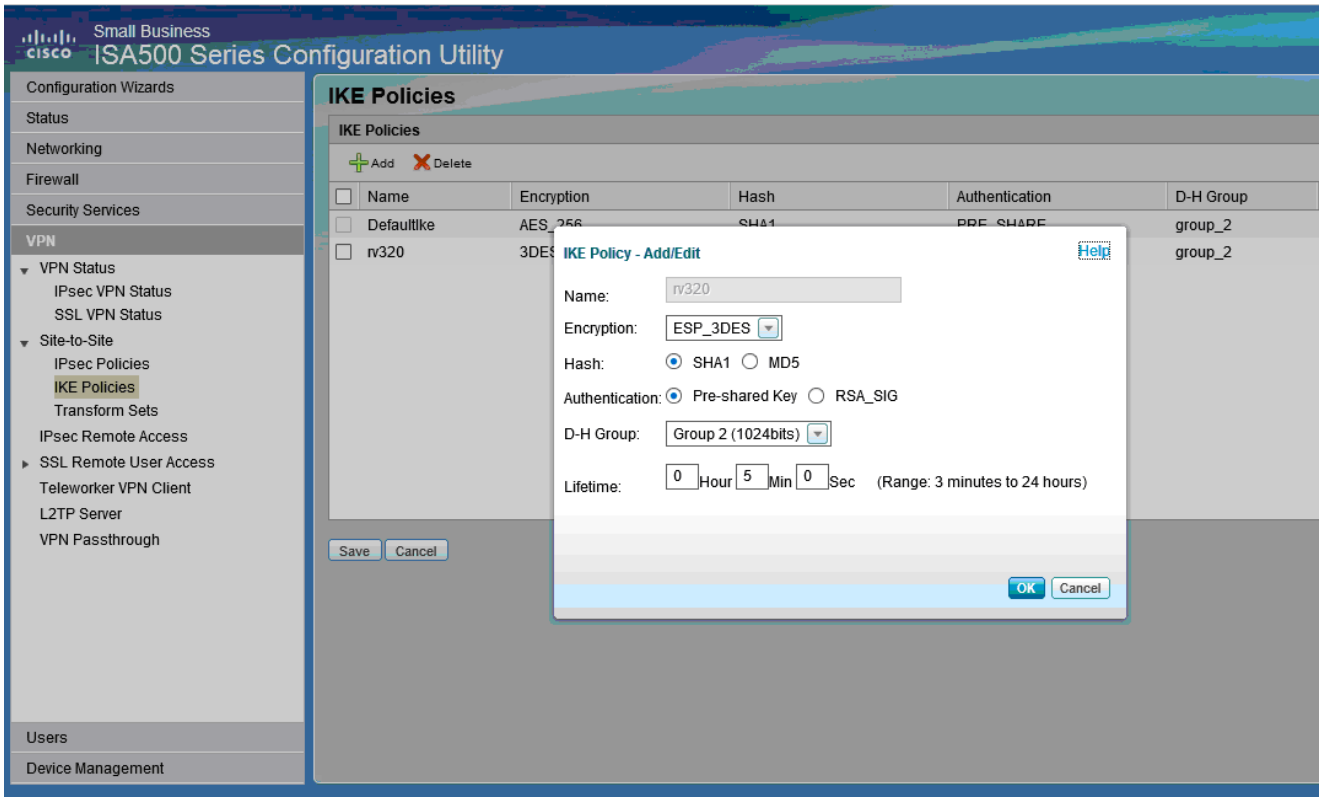

Étape 2. Configurer les paramètres du tunnel IPSec (voir l'image)
a.) Définissez *Encryption* sur 3DES.
b.) Définissez *Authentication* sur SHA1.
c.) Cochez *Parfect Forward Secrecy*.
d.) Configurez la *clé prépartagée* (doit être identique sur les deux routeurs).
L'exemple suivant illustre la configuration IPSec (phases 1 et 2) :



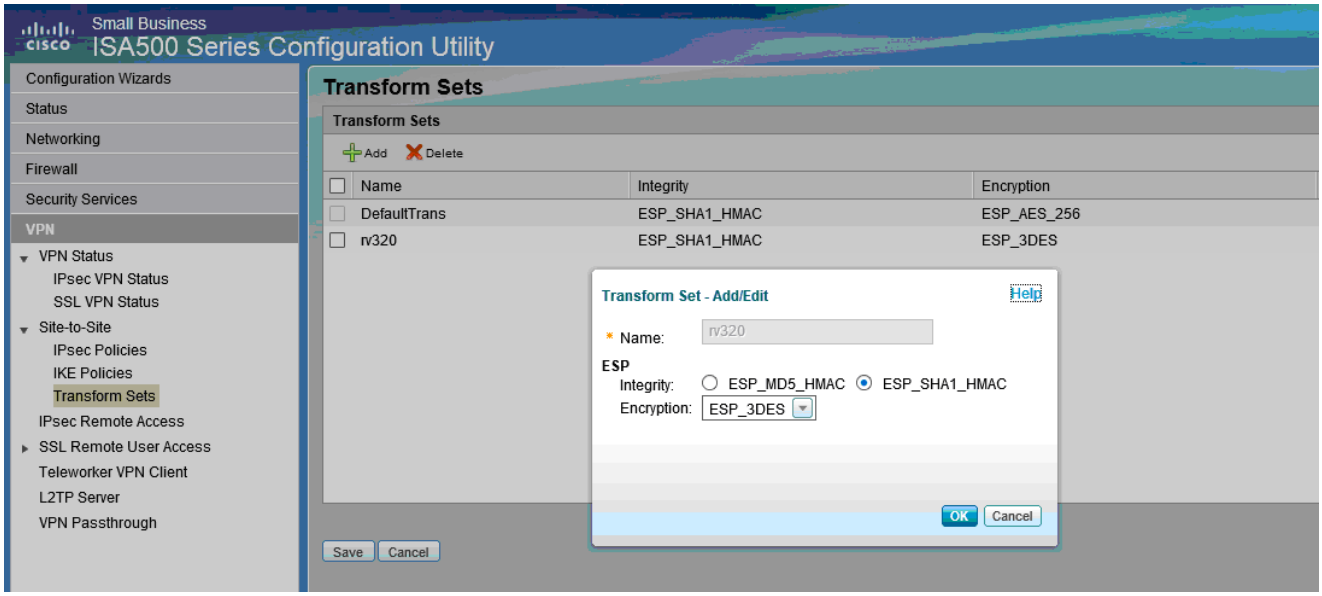

**Note:** Gardez à l'esprit que les paramètres de tunnel IPsec des deux côtés du tunnel VPN IPsec site à site doivent correspondre. S'il existe des différences entre les paramètres de tunnel IPsec du RV320 et de l'ISA570, les deux périphériques ne négocieront pas la clé de chiffrement et ne se connecteront pas.
Étape 3. Cliquez sur **Enregistrer** pour terminer la configuration.

## Configuration du tunnel VPN IPsec site à site pour ISA570 au bureau principal

Étape 1. Accédez à **VPN > IKE** Policies (voir l'image)
a.) Définissez *Encryption* sur ESP_3DES.
b.) Définissez *Hash* sur SHA1.
c.) Définissez *Authentification* sur Clé pré-partagée.
d.) Définissez *Groupe D-H* sur Groupe 2 (1 024 bits).
L'image suivante montre les stratégies IKE :




Étape 2. Accédez à **VPN > IKE Transform Sets** (voir l'image)
a.) Définissez *Integrity* sur ESP_SHA1_HMAC.
b.) Définissez *Encryption* sur ESP_DES.
La figure suivante illustre les jeux de transformation IKE :

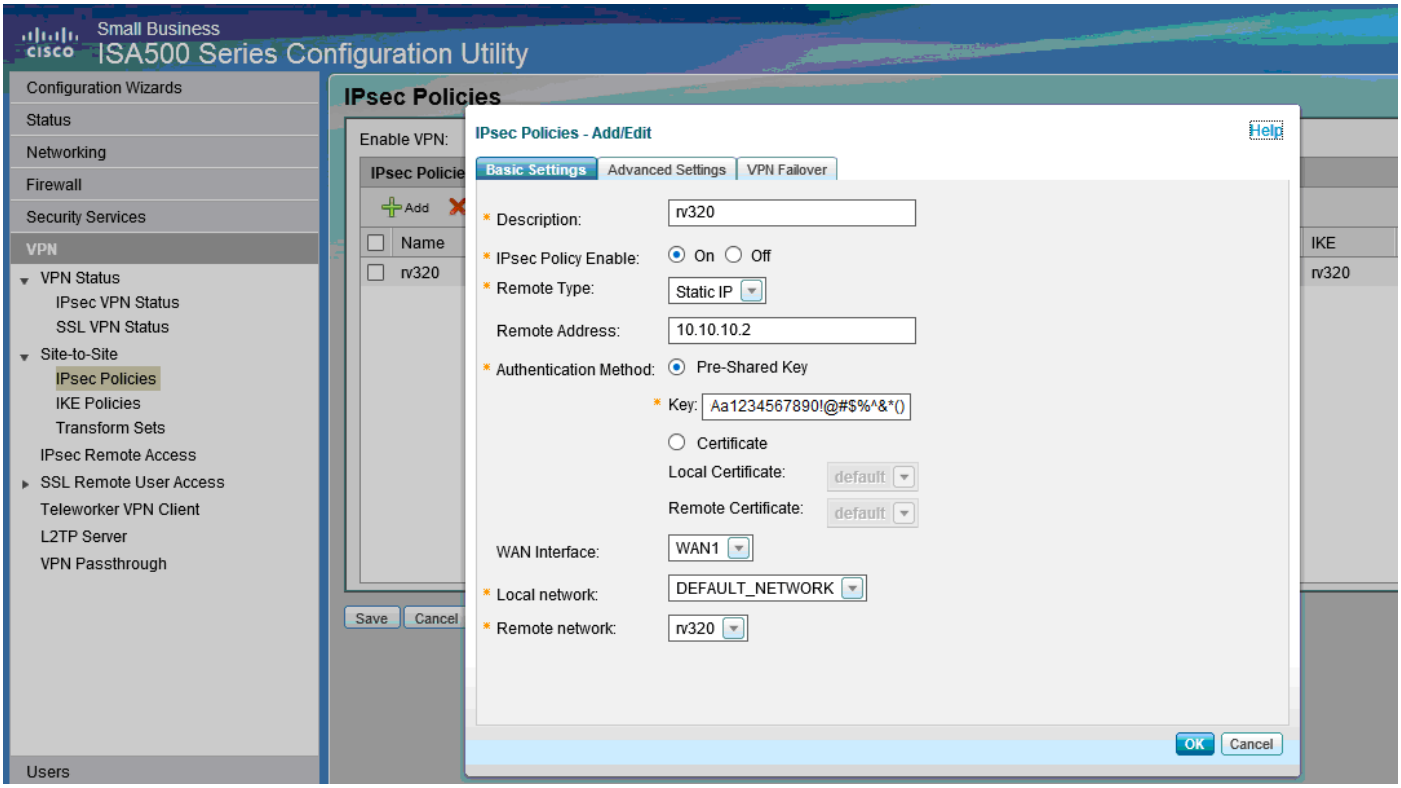



Étape 3. Accédez à **VPN > Stratégies IPsec > Ajouter > Paramètres de base** (voir l'image)

a.) Entrez une *description*, telle que RV320.
b.) Définissez *Activer la stratégie IPsec* sur Activé.
c.) Définissez *Remote Type sur Static IP*.
d.) Saisissez *l'adresse distante*.
e.) Définissez *Authentication Method* sur Pre-Shared Key.
f) Définissez *l'interface WAN* sur WAN1.
g.) Définissez *Réseau local* sur DEFAULT_NETWORK.

h) Définissez *Remote Network* sur RV320.

L'image suivante montre les paramètres de base des stratégies IPsec :



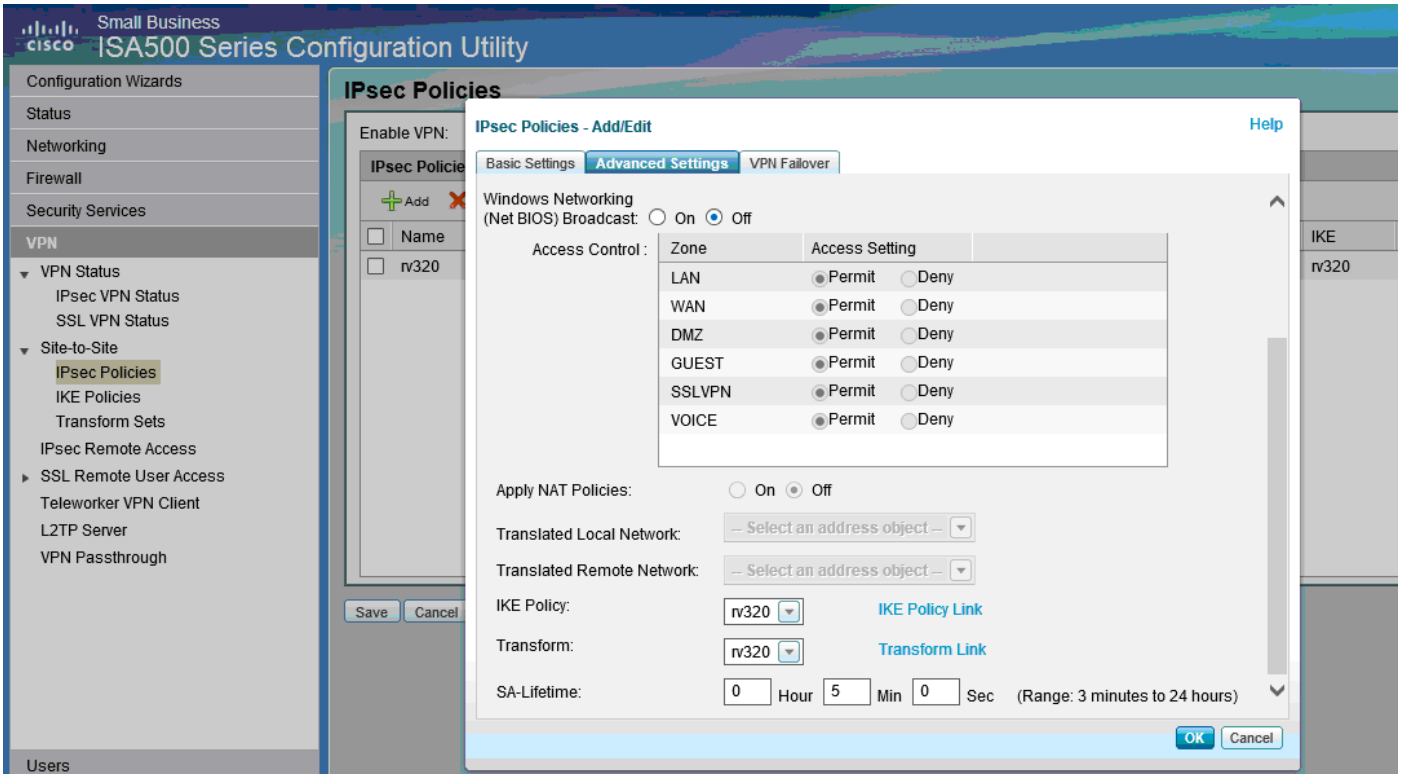

Étape 4. Accédez à **VPN > Stratégies IPsec > Ajouter > Paramètres avancés** (voir l'image)

a.) Définissez respectivement *la stratégie IKE* et les *jeux de transformation IKE* sur ceux créés aux étapes 1 et 2.

b.) Définissez *SA-Lifetime* à 0 Heure 5 min 0 sec.

c.) Click OK.

L'exemple suivant illustre les paramètres avancés des stratégies IPsec :



Étape 5. Connecter le tunnel VPN IPsec site à site (voir l'image)
a.) Définissez *Enable VPN* sur On.
b.) Cliquez sur le bouton **Connect**.
L'image suivante montre le bouton Connect :