Configuration d'un tunnel VPN de site à site entre routeur VPN de gigabit de Cisco RV320 le doubles et adaptateur BLÊMES de Services intégrés de gamme Cisco 500

Objectif

Un réseau privé virtuel (VPN) existe comme technologie très utilisée pour connecter des réseaux distants à un réseau privé principal, simulant un lien privé sous forme de canal chiffré au-dessus des lignes publiques. Un réseau distant peut se connecter à un réseau principal privé comme si il existe comme partie du réseau principal privé sans problèmes de sécurité en raison d'une négociation biphasée qui chiffre le trafic VPN d'une manière dont seulement les points finaux VPN savent le déchiffrer.
Ce guide court fournit une conception d'exemple pour établir un tunnel VPN d'IPsec de site à site entre un adaptateur de Services intégrés de gamme Cisco 500 et un routeur de la gamme de Cisco rv.

Périphériques applicables

- Routeurs de la gamme de Cisco rv (RV320)
- Adaptateurs de Services intégrés de gamme Cisco 500 (ISA570)

Version de logiciel

- 4.2.2.08 [routeurs VPN de gamme Cisco RV0xx]

Pré-configuration

Diagramme du réseau
Les expositions suivantes une topologie du site à site VPN.

Un tunnel VPN d'IPsec de site à site est configuré et établi entre le routeur de la gamme de Cisco rv au bureau à distance et la gamme Cisco 500 ISA au bureau central.
Avec cette configuration, un hôte dans le RÉSEAU LOCAL 192.168.1.0/24 au bureau distant et un hôte dans le RÉSEAU LOCAL 10.10.10.0/24 au bureau central peuvent communiquer les uns avec les autres sécurisé au-dessus du VPN.

Principaux concepts

Échange de clés Internet (IKE)

L'Échange de clés Internet (IKE) est le protocole utilisé pour installer une association de sécurité (SA) dans la suite de protocole IPsec. Les constructions d'IKE sur le protocole d'Oakley, l'association de sécurité internet, et le protocole de gestion de clés (ISAKMP), et emploie un échange de clé de Diffie-Hellman pour installer un secret partagé de session, dont des clés cryptographiques sont dérivées.

Protocole 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 finaux VPN. Il définit les procédures pour l'authentification, la transmission, et la génération de clés, et est utilisé par le protocole d'IKE pour permuter des clés de chiffrement et pour établir la connexion sécurisée.

IPSec (IPsec)

Le protocole de sécurité IP (IPsec) est une suite de protocole pour sécuriser des 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 des flux de données entre une paire d'hôtes,

les passerelles, ou les réseaux.

Conseils de conception

Topologie VPN — Une topologie du Point à point VPN signifie qu'un tunnel sécurisé d'IPsec est configuré entre le site principal et le site distant.
Les entreprises exigent souvent des plusieurs sites distants dans une topologie multisite, et implémentent une topologie de l'en étoile VPN ou la topologie du maillage complet VPN. Une topologie de l'en étoile VPN signifie que les sites distants n'exigent pas la transmission avec d'autres sites distants, et chaque site distant établit seulement un tunnel sécurisé d'IPsec avec le site principal. Une topologie du maillage complet VPN signifie que les sites distants exigent la transmission avec d'autres sites distants, et chaque site distant établit un tunntel sécurisé d'IPsec avec le site principal et tous autres sites distants.
Authentification VPN — Le protocole d'IKE est utilisé pour authentifier des homologues VPN en établissant un tunnel VPN. Les diverses méthodes d'authentification d'IKE existent, et la clé pré-partagée est la méthode la plus commode. Cisco recommande appliquer une clé pré-partagée forte.
Chiffrement de VPN — Pour assurer la confidentialité des données transportées au-dessus du VPN, des algorithmes de chiffrement sont utilisés pour chiffrer la charge utile des paquets IP. Le DES, les 3DES, et les AES sont trois normes de chiffrement communes. AES est considéré les la plupart sécurisées une fois comparé au DES et au 3DES. Cisco recommande fortement appliquer les bits AES-128 ou le cryptage plus élevé (par exemple, AES-192 et AES-256). Cependant, les algorithmes de chiffrement plus fort exigent plus de ressources de traitement d'un routeur.
L'adressage IP BLÊME dynamique et le domain name service dynamique (DDNS) — le tunnel VPN doit être établi entre deux adresses IP publique. Si les routeurs WAN reçoivent des adresses IP statiques du fournisseur de services Internet (ISP), le tunnel VPN peut être mis en application directement utilisant les adresses IP publique statiques. Cependant, la plupart des petites entreprises utilisent des services Internet hauts débits rentables tels que le DSL ou le câble, et reçoivent des adresses IP dynamiques de leurs ISP. En pareil cas, le domain name service dynamique (DDNS) peut être utilisé pour tracer l'adresse IP dynamique à un nom de domaine complet (FQDN).
Adressage IP de RÉSEAU LOCAL — L'adresse de réseau IP privée de RÉSEAU LOCAL de chaque site devrait n'avoir aucune superposition. L'adresse de réseau IP par défaut de RÉSEAU LOCAL à chaque site distant devrait toujours être changée.

Conseils de configuration

liste de contrôle de Pré-configuration

Étape 1. Connectez un câble Ethernet entre le RV320 et son DSL ou modem câble, et connectez un câble Ethernet entre l'ISA570 et son DSL ou modem câble.
Étape 2. Activez le RV320, et puis connectez les PC internes, les serveurs, et d'autres périphériques IP aux ports LAN du RV320.
Étape 3. Activez l'ISA570, et puis connectez les PC internes, les serveurs, et d'autres périphériques IP aux ports LAN de l'ISA570.
Étape 4. Veillez à configurer les adresses IP de réseau à chaque site sur des différents sous-réseaux. Dans cet exemple, le RÉSEAU LOCAL distant de bureau utilise 192.168.1.0 et le RÉSEAU LOCAL de bureau central utilise 10.10.10.0.
Étape 5. Assurez-vous que des PC de gens du pays peuvent se connectent à leurs Routeurs respectifs, et à d'autres PC sur le même RÉSEAU LOCAL.

Identifier la connexion WAN

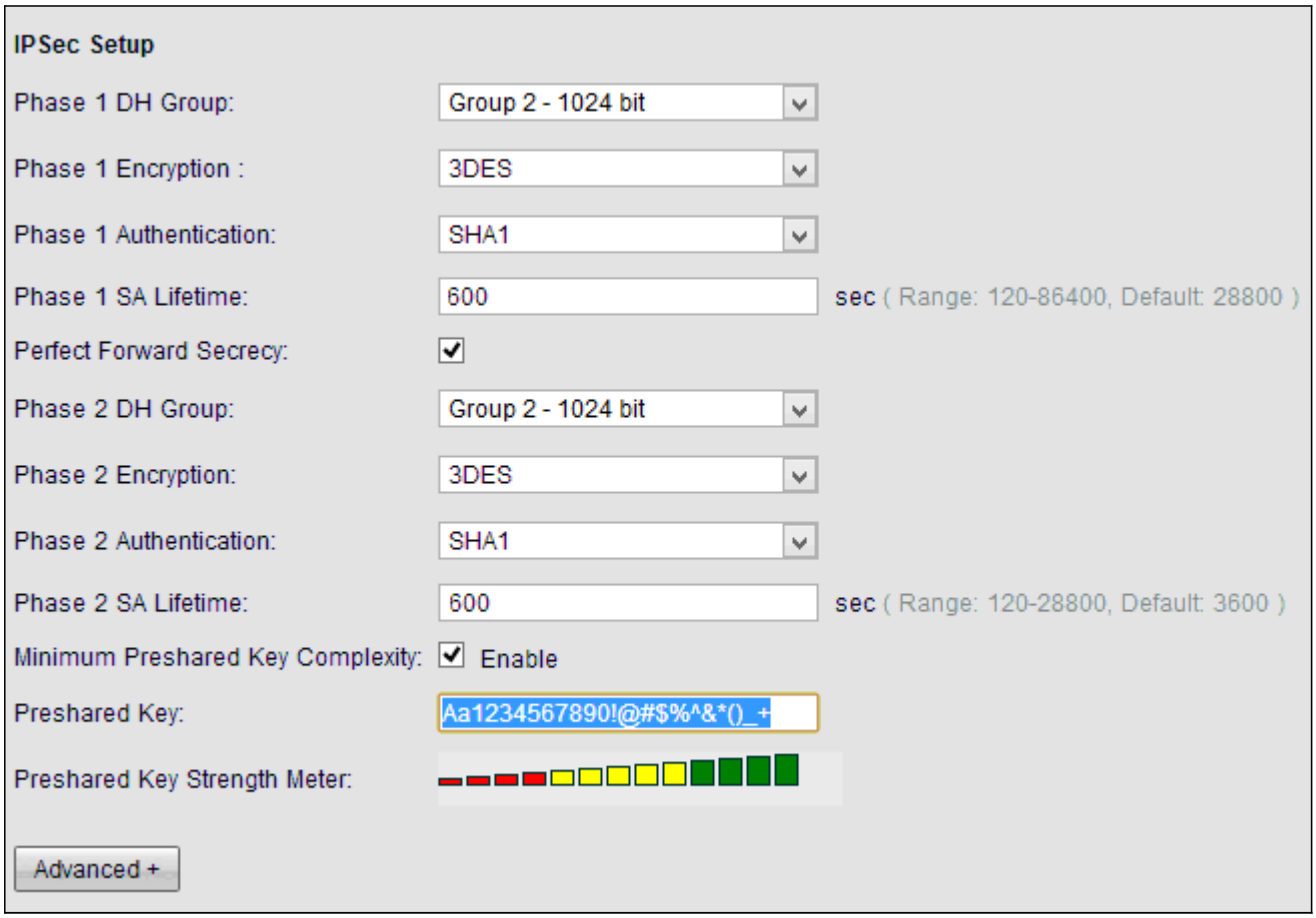
Vous devrez savoir si votre ISP fournit une adresse IP dynamique ou une adresse IP statique. L'ISP fournit habituellement une adresse IP dynamique, mais vous devriez confirmer ceci avant de se terminer la configuration de tunnel VPN de site à site.

Configurer le tunnel VPN d'IPsec de site à site pour RV320 au bureau distant

Étape 1. Allez à **VPN > Passerelle-à-passerelle** (voir l'image)
l'A.) écrivent un nom de tunnel, tel que RemoteOffice.
set interface B.) à WAN1.
le C.) a placé introduire le mode à l'IKE avec la clé pré-partagée.
adresse IP locale D.) et adresse IP distante entrées.
L'image suivante affiche la double passerelle BLÊME de routeur VPN du gigabit RV320 à la page de passerelle :

Étape 2. Paramètrages de tunnel d'IPSec d'installation (voir l'image)
l'A.) a placé le *cryptage à* 3DES.
le B.) a placé l'*authentification à* SHA1.
perfect forward secrecy de contrôle C.).

d.) installé la *clé pré-partagée* (les besoins d'être les mêmes sur les deux Routeurs).
L'installation suivante d'IPSec d'expositions (Phase 1 et 2) :



Remarque: Maintenez dans l'esprit que les paramètrages de tunnel d'IPsec des deux côtés du tunnel VPN d'IPsec de site à site doivent apparier. Si des anomalies existent entre les paramètrages de tunnel d'IPsec du RV320 et l'ISA570, les deux périphériques ne négocieront pas la clé de chiffrement et ne manqueront pas de se connecter.
Étape 3. **Sauvegarde de** clic pour se terminer la configuration.

Configurer le tunnel VPN d'IPsec de site à site pour ISA570 au bureau central

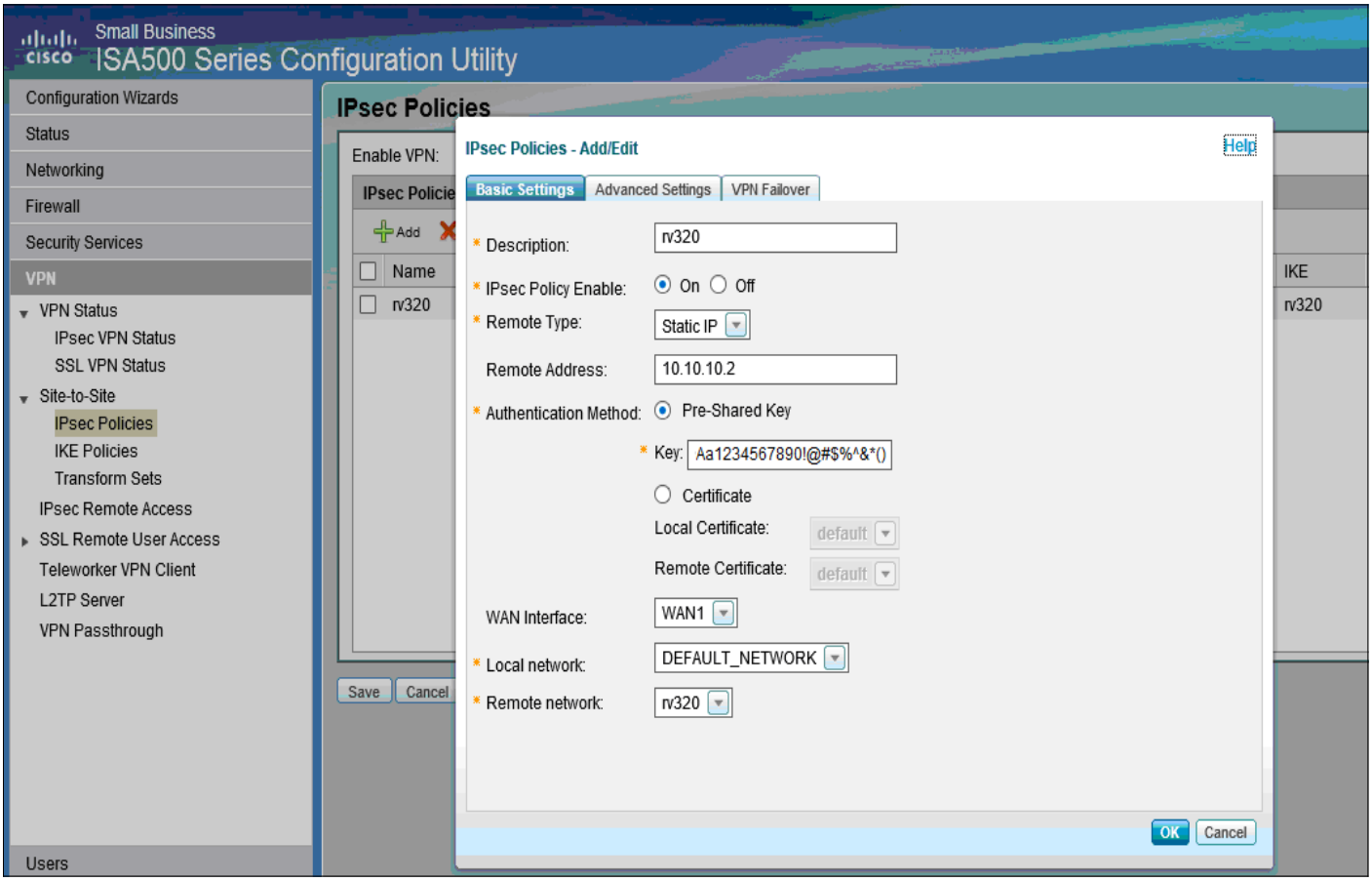
Étape 1. Allez à **VPN > stratégies IKE** (voir l'image)
l'A.) a placé le *cryptage à* ESP_3DES.
le B.) a placé des *informations parasites à* SHA1.
le C.) a placé l'*authentification à la* clé pré-partagée.
le D.) a placé le *groupe de D-H* pour grouper 2 (1024 bits).
L'image suivante affiche des stratégies IKE :

Étape 2. Allez à des **jeux de transformations VPN > d'IKE** (voir l'image)
l'A.) a placé l'*intégrité à* ESP_SHA1_HMAC.
le B.) a placé le *cryptage à* ESP_DES.
Les jeux de transformations suivants d'IKE d'expositions :

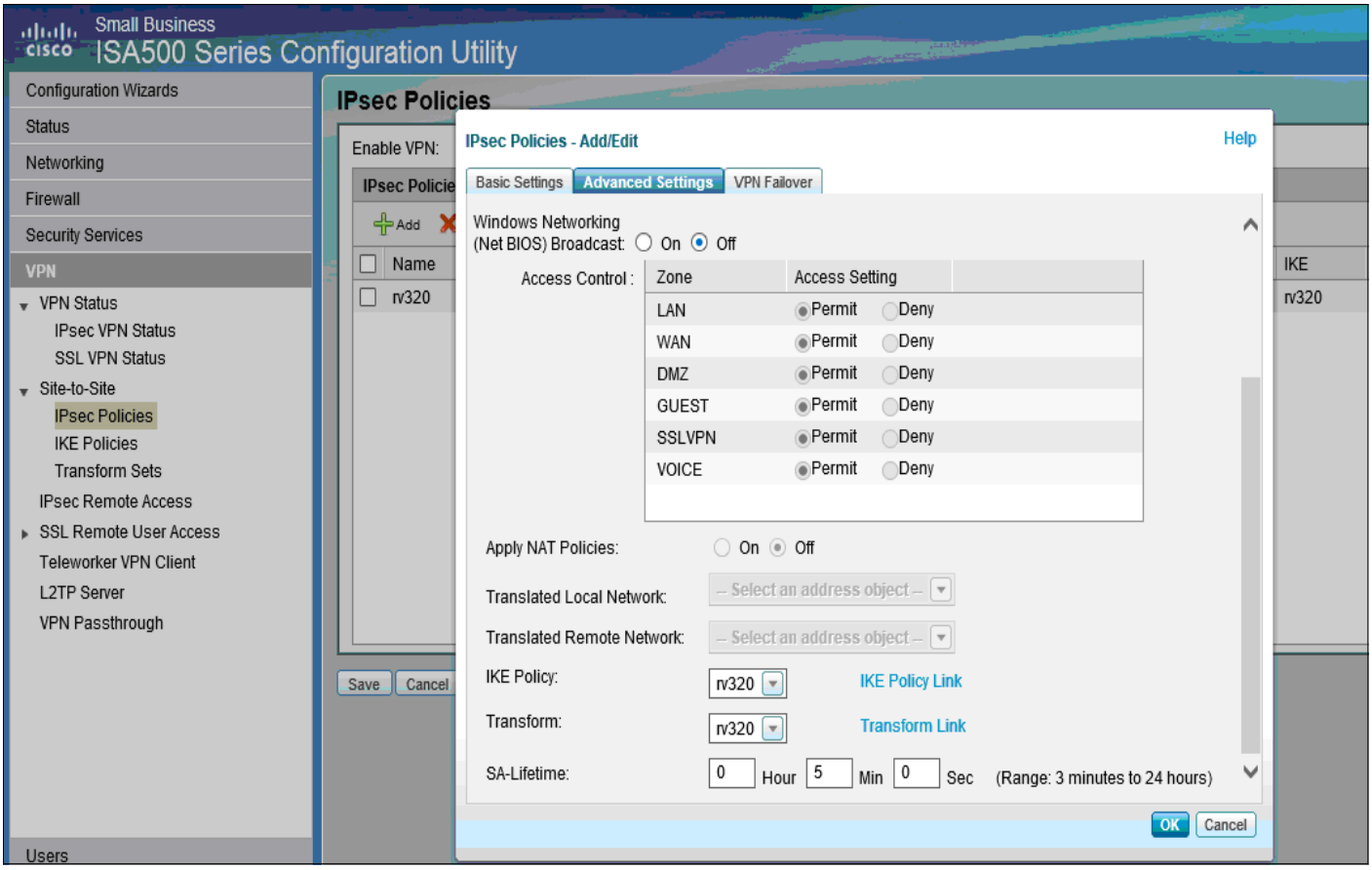
Étape 3. Allez à des **stratégies VPN > d'IPsec > ajoutent > des paramètres de base** (voir l'image)

l'A.) écrivent une *description*, telle que RV320.
le B.) a placé l' *enable de stratégie d'IPsec à* en fonction.

le C.) a placé le *type distant à l'IP statique*.
adresse distante entrée D.).
l'E.) a placé la *méthode d'authentification à la* clé pré-partagée.
le F.) a placé l' *interface WAN à* WAN1.
le G.) a placé le *réseau local à* DEFAULT_NETWORK.
le H.) a placé le *réseau distant à* RV320.
L'image suivante affiche des paramètres de base de stratégies d'IPsec :



Étape 4. Allez à des **stratégies VPN > d'IPsec > ajoutent > des paramètres avancés** (voir l'image)
l'A.) a placé la *stratégie IKE* et les *jeux de transformations d'IKE* respectivement à ceux créés dans les étapes 1 et 2.
le B.) a placé la SA- *vie à la* minute de 0 heures 5 pendant 0 sec.
le C.) cliquent sur OK.
Les paramètres avancés suivants de stratégies d'IPsec d'expositions :



Étape 5. Connectez le tunnel VPN d'IPsec de site à site (voir l'image)
l'A.) a placé l' *enable VPN à* en fonction.
bouton Connect de clic B.).
L'image suivante affiche le bouton Connect :