Guide de paramétrage IPsec

Version 0

FRE

Définitions relatives aux remarques

Ce guide de l’utilisateur utilise l'icône suivante :

 Remarque	Les remarques vous indiquent comment réagir face à une situation qui se présente ou vous donnent des conseils sur la façon dont l'opération en cours se déroule avec d'autres fonctions.

Marques commerciales

Le logo Brother est une marque déposée de Brother Industries, Ltd.

Les noms de commerce et les noms de produit de sociétés apparaissant sur les produits Brother, la documentation associée et n'importe quelle autre publication sont tous des marques de commerce ou des marques déposées de leurs sociétés respectives.

Table des matières

1 Introduction

Généralités

IPsec (Internet Protocol Security) est un protocole de sécurité qui utilise une fonction IP optionnelle pour empêcher toute manipulation et protéger la confidentialité des données transmises sous forme de paquets IP. IPsec crypte les données transportées sur le réseau, telles que les données d'impression envoyées à une imprimante depuis des ordinateurs. Les données étant cryptées au niveau de la couche réseau, les applications utilisant un protocole de niveau supérieur font appel à IPsec même si l'utilisateur n'en est pas conscient.

IPsec prend en charge les fonctions suivantes :

■ Transmissions IPsec

Selon les conditions de paramétrage IPsec, l'ordinateur connecté au réseau envoie des données au périphérique spécifié et en reçoit à l'aide du protocole IPsec. Lorsque les appareils se mettent à communiquer à l'aide d'IPsec, des clés sont d'abord échangées à l'aide de IKE (Internet Key Exchange), puis les données cryptées sont transmises à l'aide de ces clés.

IPsec utilise en outre deux modes de fonctionnement : le mode Transport et le mode Tunnel. Le mode Transport sert principalement pour les communications entre différents appareils tandis que le mode Tunnel est utilisé dans des environnements tels qu'un VPN (réseau privé virtuel).

Remarque

- Les conditions suivantes doivent être remplies dans le cas des transmissions IPsec :
  - Un ordinateur capable de communiquer à l'aide du protocole IPsec est connecté au réseau.
  - L'imprimante ou le MFC est configuré(e) pour la communication IPsec.
  - L'ordinateur connecté à l'imprimante ou au MFC est configuré pour les connexions IPsec.
- Le protocole IPsec ne prend pas en charge les communications en diffusion ou multidiffusion.

■ Paramètres IPsec

Les paramètres qui sont nécessaires pour les connexions utilisant IPsec. Vous pouvez utiliser la Gestion à partir du Web pour configurer ces paramètres. (Voir *Configuration à l'aide de Gestion à partir du Web (navigateur Web)* ➤➤ page 2.)

Remarque

Pour configurer les paramètres IPsec, un ordinateur utilisant le navigateur doit être connecté au réseau.

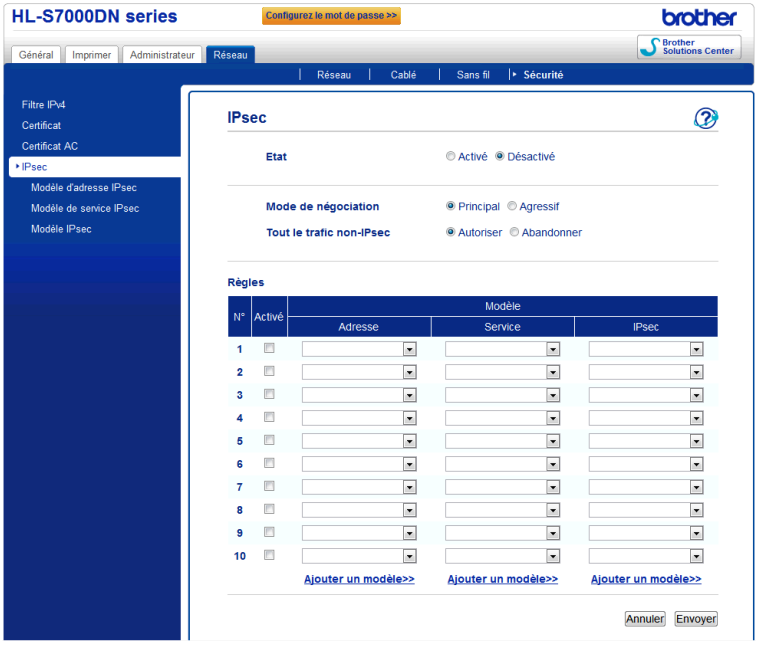
Configuration à l'aide de Gestion à partir du Web (navigateur Web)

Utilisez l'écran de paramétrage IPsec pour la Gestion à partir du Web afin de spécifier les conditions de connexion IPsec.

Les conditions de connexion IPsec sont composées de trois types de **Modèle** : **Adresse**, **Service** et **IPsec**, et 10 conditions de connexion peuvent être configurées au maximum.

1. Lancez votre navigateur Web.
2. Tapez « http://adresse IP de l'appareil/ » dans votre navigateur (où « adresse IP de l'appareil » correspond à l'adresse IP de l'appareil).
   - Par exemple :

     http://192.168.1.2/
3. Aucun mot de passe n'est requis par défaut. Saisissez un mot de passe si vous en avez défini un, puis appuyez sur .
4. Cliquez sur l'onglet **Réseau**.
5. Cliquez sur **Sécurité**.
6. Cliquez sur **IPsec**.
7. Vous pouvez configurer les paramètres IPsec depuis l'écran ci-dessous.



- **Etat**

  Sélectionnez **Activé** ou **Désactivé** pour IPsec.

■ **Mode de négociation**

Sélectionnez le mode pour IKE Phase 1.

- **Principal** : le mode principal est utilisé.
- **Agressif** : le mode agressif est utilisé.

Remarque

IKE est un protocole qui permet d'échanger des clés de cryptage pour assurer les communications cryptées à l'aide d'IPsec.

Si le mode **Principal** est sélectionné, la vitesse de traitement est lente, mais la sécurité est élevée. Si le mode **Agressif** est sélectionné, la vitesse de traitement est plus rapide que dans le mode **Principal**, mais la sécurité est plus faible.

■ **Tout le trafic non-IPsec**

Sélectionnez l'action à exécuter pour les paquets non-IPsec.

- **Autoriser** : la réception est autorisée pour tous les paquets.
- **Abandonner** : les paquets non-IPsec sont ignorés.

Remarque

Lorsque vous utilisez le protocole Web Services, vous devez sélectionner **Autoriser** pour **Tout le trafic non-IPsec**. Si **Abandonner** est sélectionné, le protocole Web Services ne peut pas être utilisé.

■ **Règles**

Vous pouvez configurer 10 conditions de connexion IPsec (définition de modèle) au maximum.

■ **Activé**

Lorsque cette case est cochée, la définition de modèle pour ce numéro est activée.

Remarque

Lorsque plusieurs cases sont cochées, les cases affichant les numéros les plus bas reçoivent la priorité en cas de conflit entre les paramètres des cases sélectionnées.

■ **Modèle** - **Adresse**

Sélectionnez le **Modèle d'adresse** utilisé pour les conditions de connexion IPsec.

Pour ajouter un **Modèle d'adresse**, cliquez sur **Ajouter un modèle** (voir *Modèle d'adresse* ➤➤ page 5).

■ **Modèle** - **Service**

Sélectionnez le **Modèle de service** utilisé pour les conditions de connexion IPsec.

Pour ajouter un **Modèle de service**, cliquez sur **Ajouter un modèle** (voir *Modèle de service* ➤➤ page 7).

Remarque

Si vous souhaitez utiliser DNS pour la résolution de nom lorsque vous utilisez les modèles de service 2, 3 et 4 décrits dans l'*Annexe A*, les paramètres DNS doivent être configurés séparément.

■ **Modèle** - **IPsec**

Sélectionnez le **Modèle IPsec** utilisé pour les conditions de connexion IPsec.

Pour ajouter un **Modèle IPsec**, cliquez sur **Ajouter un modèle** (voir *Modèle IPsec* ➤➤ page 11).

■ **Envoyer**

Cliquez sur ce bouton pour enregistrer les paramètres. Si l'ordinateur doit être redémarré pour modifier les paramètres, l'écran de confirmation de redémarrage s'affiche lorsque vous cliquez sur ce bouton.

Remarque

Si vous sélectionnez la case à cocher **Activé** et que vous cliquez sur **Envoyer**, une erreur se produit si le modèle sélectionné contient un élément vide.

2 Paramètres IPsec

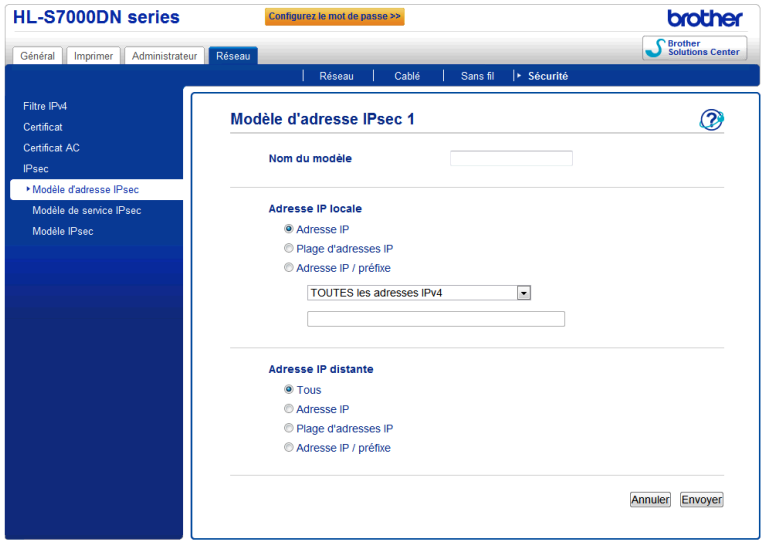
Modèle d'adresse

Spécifiez les adresses IP à utiliser pour les conditions de connexion IPsec. 10 entrées **Modèle d'adresse** peuvent être utilisées au maximum.

1. Lancez votre navigateur Web.
2. Tapez « http://adresse IP de l'appareil/ » dans votre navigateur (où « adresse IP de l'appareil » correspond à l'adresse IP de l'appareil).
   - Par exemple :

     http://192.168.1.2/
3. Aucun mot de passe n'est requis par défaut. Saisissez un mot de passe si vous en avez défini un, puis appuyez sur →.
4. Cliquez sur l'onglet **Réseau**.
5. Cliquez sur **Sécurité**.
6. Cliquez sur **Modèle d'adresse IPsec**.
   10 entrées **Modèle d'adresse** s'affichent. Si le **Modèle d'adresse** n'a pas été configuré, **Non configuré** s'affiche.
   - **Supprimer**

     Cliquez sur ce bouton pour supprimer le **Modèle d'adresse** sélectionné. Le **Modèle d'adresse** actuellement utilisé ne peut toutefois pas être supprimé.
7. Cliquez sur le numéro correspondant au **Modèle d'adresse** que vous souhaitez créer. Dans l'écran ci-dessous, spécifiez l'adresse IP que IPsec doit utiliser, puis créez le **Modèle d'adresse IPsec**.



■ **Nom du modèle**

Entrez le nom du modèle dans cette zone (16 caractères maximum).

■ **Adresse IP locale**

Spécifiez les conditions d'adresse IP pour l'expéditeur.

- **Adresse IP**

  Spécifiez l'adresse IP. Sélectionnez **TOUTES les adresses IPv4**, **TOUTES les adresses IPv6**, **TOUTES les adresses IPv6 locales de lien** ou **Personnalisé**.

  Si **Personnalisé** est sélectionné, entrez l'adresse IP spécifiée (IPv4 ou IPv6) dans la zone de texte.

- **Plage d'adresses IP**

  Entrez les adresses IP de début et de fin pour la plage d'adresses IP. Si les adresses IP de début et de fin ne sont pas normalisées pour IPv4 ou IPv6, ou que l'adresse IP de fin est inférieure à l'adresse de début, une erreur se produira.

- **Adresse IP / préfixe**

  Spécifiez l'adresse IP en utilisant un préfixe.

  Par exemple : 192.168.1.1/24

  Parce que le préfixe est spécifié sous la forme d'un masque de sous-réseau 24 bits (255.255.255.0) pour 192.168.1.1, les adresses 192.168.1.xx sont valides.

■ **Adresse IP distante**

Spécifiez les conditions d'adresse IP pour le destinataire.

- **Tous**

  Lorsque **Tous** est sélectionné, toutes les adresses IP sont activées.

- **Adresse IP**

  Entrez l'adresse IP spécifiée (IPv4 ou IPv6) dans la zone de texte.

- **Plage d'adresses IP**

  Entrez les adresses IP de début et de fin pour la plage d'adresses IP. Si les adresses IP de début et de fin ne sont pas normalisées pour IPv4 ou IPv6, ou que l'adresse IP de fin est inférieure à l'adresse de début, une erreur se produira.

- **Adresse IP / préfixe**

  Spécifiez l'adresse IP en utilisant un préfixe.

  Par exemple : 192.168.1.1/24

  Parce que le préfixe est spécifié sous la forme d'un masque de sous-réseau 24 bits (255.255.255.0) pour 192.168.1.1, les adresses 192.168.1.xx sont valides.

■ **Envoyer**

Cliquez sur ce bouton pour enregistrer les paramètres.

Remarque

Lorsque vous modifiez les paramètres du modèle actuellement utilisé, l'écran de paramétrage IPsec pour la Gestion à partir du Web se ferme puis s'ouvre à nouveau.

Modèle de service

Modèle de service IPsec

Spécifiez le protocole et le numéro de port à utiliser pour les connexions IPsec. 10 entrées **Modèle de service** peuvent être utilisées au maximum.

1. Lancez votre navigateur Web.
2. Tapez « http://adresse IP de l'appareil/ » dans votre navigateur (où « adresse IP de l'appareil » correspond à l'adresse IP de l'appareil).
   - Par exemple :

     http://192.168.1.2/
3. Aucun mot de passe n'est requis par défaut. Saisissez un mot de passe si vous en avez défini un, puis appuyez sur .
4. Cliquez sur l'onglet **Réseau**.
5. Cliquez sur **Sécurité**.
6. Cliquez sur **Modèle de service IPsec**.
   10 entrées **Modèle de service** s'affichent. Si le **Modèle de service** n'a pas été configuré, **Non configuré** s'affiche.
   - **Supprimer**

     Cliquez sur ce bouton pour supprimer le **Modèle de service** sélectionné. Le **Modèle de service** actuellement utilisé ne peut toutefois pas être supprimé.
7. Cliquez sur le numéro correspondant au **Modèle de service** que vous souhaitez créer. Dans l'écran ci-dessous, sélectionnez les services que vous souhaitez utiliser pour IPsec, puis créez le **Modèle de service IPsec**.
   En outre, si vous souhaitez créer des services originaux, cliquez sur **Service de configuration** (voir *Service de configuration* ➤➤ page 8).

■ **Nom du modèle**

Entrez le nom du modèle dans cette zone (16 caractères maximum).

■ **Nom du service**

Les noms des services par défaut et les noms des services précédemment créés s'affichent. Sélectionnez les services que vous souhaitez ajouter au modèle.

■ **Service de configuration**

Cliquez sur **Service de configuration** pour configurer le modèle en ajoutant des services (voir *Service de configuration* ➤➤ page 8).

■ **Service sélectionné**

Les informations concernant le service (**Nom du service**, **Direction**, **Protocole** et **Port**) sélectionnés pour **Nom du service** s'affichent.

Remarque

- 32 services au maximum peuvent être ajoutés à la fois.
- Pour plus de détails sur les protocoles que vous pouvez spécifier dans **Modèle de service IPsec**, voir *Annexe A*.

■ **Envoyer**

Cliquez sur ce bouton pour enregistrer les paramètres.

Remarque

Lorsque vous modifiez les paramètres du modèle actuellement utilisé, l'écran de paramétrage IPsec pour la Gestion à partir du Web se ferme puis s'ouvre à nouveau.

Service de configuration

Créez un nouveau service.

1. Dans l'écran **Modèle de service IPsec**, cliquez sur **Service de configuration**.
60 entrées **Nom du service** s'affichent. Si le **Nom du service** n'a pas été configuré, **Non configuré** s'affiche.

■ **Supprimer**

Cliquez sur ce bouton pour supprimer le **Nom du service** sélectionné. Le **Nom du service** actuellement utilisé ne peut toutefois pas être supprimé.

■ **Modèle de service IPsec**

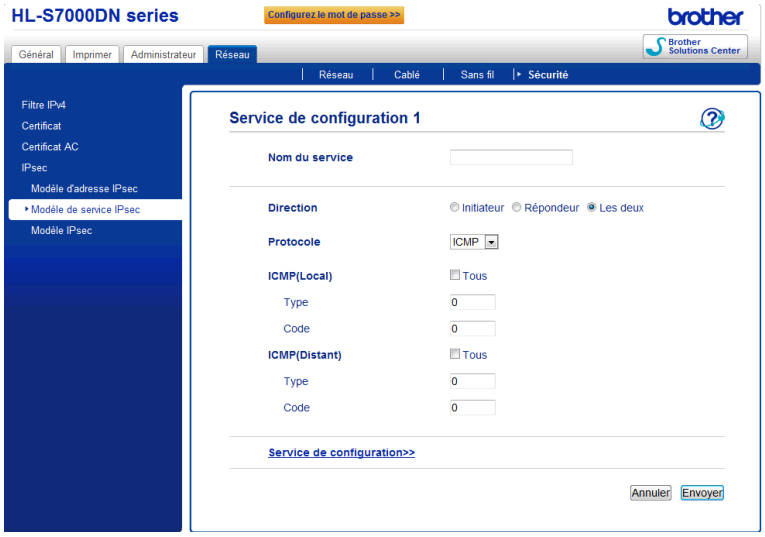
Cliquez sur ce bouton pour revenir à l'écran **Modèle de service IPsec** sélectionné.

2 Cliquez sur le numéro correspondant au **Nom du service** que vous souhaitez créer. Sélectionnez les services que vous souhaitez utiliser pour IPsec dans l'écran ci-dessous. Les éléments de paramétrage varient selon le **Protocole** sélectionné.

(**Protocole** : **TOUS**)

(**Protocole** : **TCP** ou **UDP**)

(**Protocole** : **ICMP**)



■ **Nom du service**

Entrez le nom du service dans cette zone (16 caractères maximum).

■ **Direction**

Spécifiez la direction de communication. Sélectionnez **Initiateur**, **Répondeur** ou **Les deux**.

■ **Protocole**

Spécifiez le protocole qui est activé. Sélectionnez **TOUS**, **TCP**, **UDP** ou **ICMP**. Les éléments de paramétrage varient selon le **Protocole** sélectionné.

- Lorsque **TCP** ou **UDP** est sélectionné, enregistrez le **Port local**/**Port distant**.
- Lorsque **ICMP** est sélectionné, enregistrez le **Type**/**Code**.

Remarque

ICMP est un protocole permettant d'envoyer des messages d'erreur et des messages de contrôle IP. Ce protocole est utilisé par les ordinateurs et les périphériques réseau connectés à l'aide de TCP/IP pour procéder à des confirmations d'état mutuelles.

■ **Port local**/**Port distant** (lorsque **TCP** ou **UDP** est sélectionné dans **Protocole**).

Entrez le numéro de port local. Si **Unique** est sélectionné, entrez un numéro de port. Si **Plage** est sélectionné, entrez le numéro de port de début, puis le numéro de port de fin. Lorsque vous souhaitez activer tous les numéros de port, sélectionnez **Plage** et entrez « 1-65535 » sans les doubles guillemets.

■ **ICMP(Local)**/**ICMP(Distant)** (lorsque **ICMP** est sélectionné dans **Protocole**).

Configurez les paramètres ICMP. Sélectionnez **Tous** ou entrez le **Type**/**Code**. Pour plus de détails sur le **Type**/**Code**, voir *Annexe A*.

■ **Service de configuration**

Cliquez sur ce bouton pour revenir à l'écran **Service de configuration**.

■ **Envoyer**

Cliquez sur ce bouton pour enregistrer les paramètres.

Remarque

Lorsque vous modifiez les paramètres du modèle actuellement utilisé, l'écran de paramétrage IPsec pour la Gestion à partir du Web se ferme puis s'ouvre à nouveau.

Modèle IPsec

Configurez les paramètres IKE/IPsec. 10 entrées **Modèle IPsec** peuvent être utilisées au maximum.

1. Lancez votre navigateur Web.
2. Tapez « http://adresse IP de l'appareil/ » dans votre navigateur (où « adresse IP de l'appareil » correspond à l'adresse IP de l'appareil).

   ■ Par exemple :

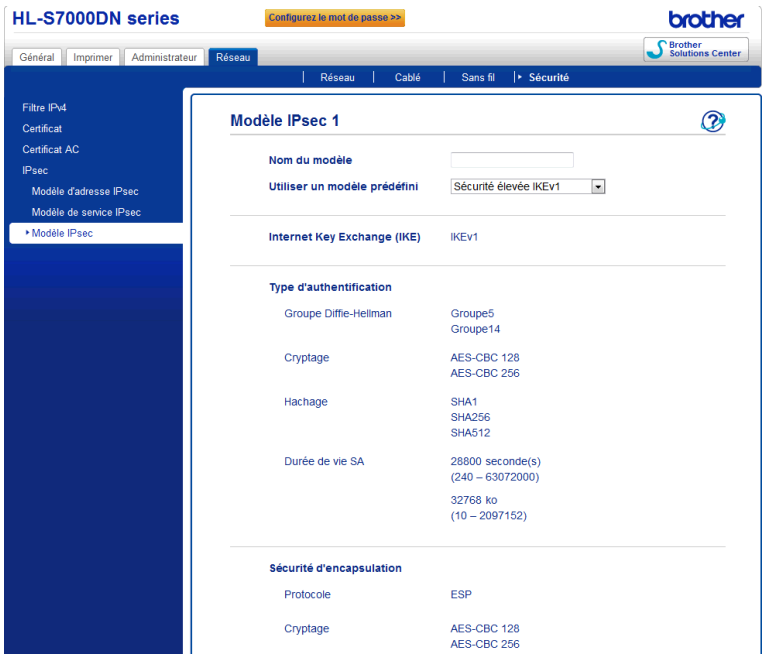
   http://192.168.1.2/
3. Aucun mot de passe n'est requis par défaut. Saisissez un mot de passe si vous en avez défini un, puis appuyez sur →.
4. Cliquez sur l'onglet **Réseau**.
5. Cliquez sur **Sécurité**.
6. Cliquez sur **Modèle IPsec**.
   10 entrées **Modèle IPsec** s'affichent. Si le **Modèle IPsec** n'a pas été configuré, **Non configuré** s'affiche.

   ■ **Supprimer**

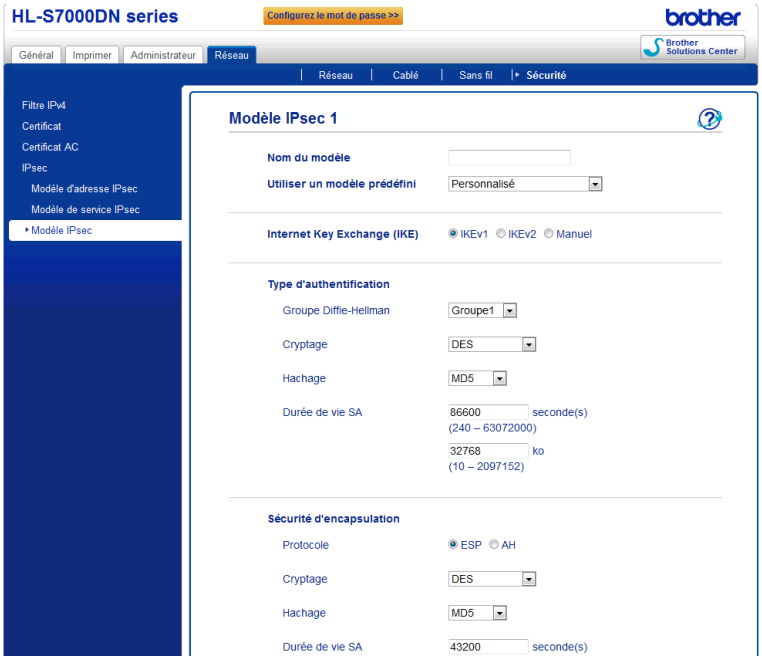
   Cliquez sur ce bouton pour supprimer le **Modèle IPsec** sélectionné. Le **Modèle IPsec** actuellement utilisé ne peut toutefois pas être supprimé.

7 Cliquez sur le numéro correspondant au **Modèle IPsec** que vous souhaitez créer. Configurez les paramètres IPsec dans l'écran ci-dessous, puis créez le **Modèle IPsec**. Les éléments de paramétrage varient selon les options **Utiliser un modèle prédéfini** et **Internet Key Exchange (IKE)** sélectionnées.

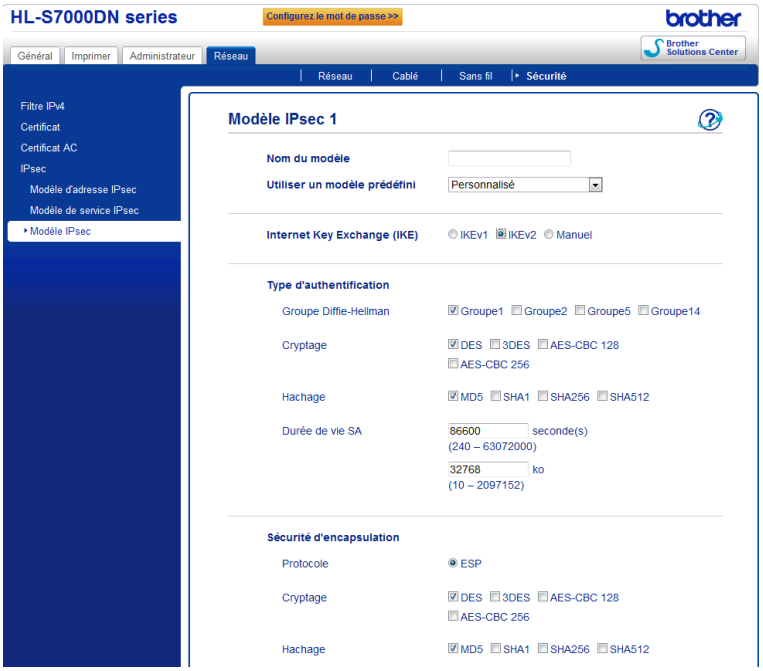
(**IKE** : **Préréglage**)



(**IKE** : **IKEv1**)



(**IKE** : **IKEv2**)



■ **Nom du modèle**

Entrez le nom du modèle dans cette zone (16 caractères maximum).

■ **Utiliser un modèle prédéfini**

Sélectionnez **Personnalisé**, **Sécurité élevée IKEv1**, **Sécurité moyenne IKEv1**, **Sécurité élevée IKEv2** ou **Sécurité moyenne IKEv2**. Les éléments de paramétrage varient selon le modèle sélectionné.

Remarque

Le modèle par défaut varie selon que vous choisissez le mode Principal ou Agressif en Mode de négociation dans l'écran de paramétrage IPsec. Pour des détails sur l'écran de paramétrage IPsec, voir *Configuration à l'aide de Gestion à partir du Web (navigateur Web)* ➤➤ page 2.

■ **Internet Key Exchange (IKE)**

IKE est un protocole de communication qui permet d'échanger des clés de cryptage pour assurer des communications cryptées à l'aide d'IPsec. Pour assurer les communications cryptées à ce moment uniquement, l'algorithme de cryptage nécessaire pour IPsec est déterminé et les clés de cryptage sont partagées. Pour IKE, les clés de cryptage sont échangées à l'aide de la méthode d'échange de clés Diffie-Hellman, et la communication cryptée limitée à IKE est assurée.

Si **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini**, sélectionnez **IKEv1**, **IKEv2** ou **Manuel**.

Si un paramètre autre que **Personnalisé** est sélectionné, le type d'authentification sélectionné dans **Utiliser un modèle prédéfini** s'affiche.

■ **Type d'authentification**

Permet de configurer l'authentification et le cryptage IKE.

- **Groupe Diffie-Hellman**

  Cette méthode d'échange de clés permet d'échanger des clés secrètes de manière sécurisée sur un réseau non protégé. La méthode d'échange de clés Diffie-Hellman utilise un problème de logarithme discret, et non la clé secrète, pour envoyer et recevoir des informations ouvertes générées à l'aide d'un nombre aléatoire et de la clé secrète.

  (Si **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini** et que **IKEv1** ou **IKEv2** est sélectionné dans **IKE**) Sélectionnez **Groupe1**, **Groupe2**, **Groupe5** ou **Groupe14**. Si **IKEv2** est sélectionné, il est possible de sélectionner plusieurs éléments à la fois.

  (Si **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini** et que **Manuel** est sélectionné dans **IKE**) Le groupe ne s'affiche pas.

  (Si un paramètre autre que **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini**) Le groupe activé mentionné ci-dessus s'affiche.

- **Cryptage**

  (Si **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini** et que **IKEv1** ou **IKEv2** est sélectionné dans **IKE**) Sélectionnez **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**. Si **IKEv2** est sélectionné, il est possible de sélectionner plusieurs éléments à la fois.

  (Si **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini** et que **Manuel** est sélectionné dans **IKE**) Le cryptage ne s'affiche pas.

  (Si un paramètre autre que **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini**) Le cryptage activé mentionné ci-dessus s'affiche.

- **Hachage**

  (Si **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini** et que **IKEv1** ou **IKEv2** est sélectionné dans **IKE**) Sélectionnez **MD5**, **SHA1**, **SHA256** ou **SHA512**. Si **IKEv2** est sélectionné, il est possible de sélectionner plusieurs éléments à la fois.

  (Si **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini** et que **Manuel** est sélectionné dans **IKE**) Le type d'algorithme de hachage ne s'affiche pas.

  (Si un paramètre autre que **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini**) Le type d'algorithme de hachage activé mentionné ci-dessus s'affiche.

- **Durée de vie SA**

  Spécifiez la durée de vie SA IKE.

  (Si **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini** et que **IKEv1** ou **IKEv2** est sélectionné dans **IKE**) Entrez la durée (secondes) et le nombre de kilo-octets (Ko).

  (Si **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini** et que **Manuel** est sélectionné dans **IKE**) Les informations de durée de vie SA ne s'affichent pas.

  (Si un paramètre autre que **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini**) La durée (secondes) et le nombre de kilo-octets (Ko) s'affichent.

■ **Sécurité d'encapsulation**

- **Protocole**

  (Si **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini**) Sélectionnez **ESP** ou **AH**. Si **IKEv2** est sélectionné dans **IKE**, seul **ESP** peut être sélectionné.

(Si un paramètre autre que **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini**) Le protocole activé mentionné ci-dessus s'affiche.

Remarque

- ESP est un protocole permettant d'assurer des communications cryptées à l'aide d'IPsec. ESP crypte la charge active (le contenu de la communication) et ajoute des informations supplémentaires. Le paquet IP comprend l'en-tête ainsi que la charge active cryptée, laquelle vient après l'en-tête. Outre les données cryptées, le paquet IP inclut également des informations relatives à la méthode de cryptage et à la clé de cryptage, les données d'authentification et autres informations.
- AH, une partie intégrante du protocole IPsec, authentifie l'expéditeur et empêche la manipulation des données (assure l'intégrité des données). Dans le paquet IP, les données sont insérées immédiatement après l'en-tête. Les paquets incluent également des valeurs de hachage, qui sont calculées à l'aide d'une équation provenant du contenu communiqué, de la clé secrète et autres, afin d'empêcher la falsification de l'expéditeur et la manipulation des données. A la différence d'ESP, le contenu de la communication n'est pas crypté, et les données sont envoyées et reçues sous forme de texte ordinaire.

- **Cryptage**

  (Si **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini**) Sélectionnez **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**. Le cryptage peut uniquement être sélectionné lorsque **ESP** est sélectionné dans **Protocole**. Si **IKEv2** est sélectionné dans **IKE**, il est possible de sélectionner plusieurs éléments à la fois.

  (Si un paramètre autre que **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini**) Le cryptage activé mentionné ci-dessus s'affiche.

- **Hachage**

  (Si **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini** et que **IKEv1** ou **Manuel** est sélectionné dans **IKE**) Sélectionnez **Aucun**, **MD5**, **SHA1**, **SHA256** ou **SHA512**. **Aucun** peut uniquement être sélectionné lorsque **ESP** est sélectionné dans **Protocole**.

  (Si **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini** et que **IKEv2** est sélectionné dans **IKE**) Sélectionnez **MD5**, **SHA1**, **SHA256** ou **SHA512**. Il est possible de sélectionner plusieurs éléments à la fois.

  (Si un paramètre autre que **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini**) Le type d'algorithme de hachage activé mentionné ci-dessus s'affiche.

- **Durée de vie SA**

  Spécifiez la durée de vie SA IKE.

  (Si **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini** et que **IKEv1** ou **IKEv2** est sélectionné dans **IKE**) Entrez la durée (secondes) et le nombre de kilo-octets (Ko).

  (Si un paramètre autre que **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini**) La durée (secondes) et le nombre de kilo-octets (Ko) s'affichent.

- **Mode d'encapsulation**

  Sélectionnez **Transport** ou **Tunnel**.

- **Adresse IP routeur distant**

  Spécifiez l'adresse IP (IPv4 ou IPv6) de la destination de connexion. Saisissez les informations uniquement lorsque le mode **Tunnel** est sélectionné.

Remarque

SA (Security Association) est une méthode de communication cryptée utilisant IPsec ou IPv6 et permettant d'échanger et de partager des informations, par exemple la méthode de cryptage et la clé de cryptage, afin d'établir un canal de communication sécurisé avant le début de la communication. SA peut également désigner un canal de communication virtuel crypté préalablement établi. Le SA utilisé pour IPsec établit la méthode de cryptage, échange les clés et assure l'authentification mutuelle selon la procédure standard IKE (Internet Key Exchange). Le SA est régulièrement mis à jour.

■ **Perfect Forward Secrecy (PFS)**

PFS ne dérive pas les clés des clés précédentes, qui ont été utilisées pour crypter des messages. En outre, si une clé qui a été utilisée pour crypter un message était dérivée d'une clé parent, la clé parent n'est pas utilisée pour dériver d'autres clés. De ce fait, même si une clé est compromise, le dommage sera limité aux messages qui ont été cryptés à l'aide de cette clé.

Sélectionnez **Activé** ou **Désactivé**. Si **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini** et que **Manuel** est sélectionné dans **IKE**, les informations PFS ne s'affichent pas.

■ **Méthode d'authentification**

Sélectionnez la méthode d'authentification. Sélectionnez **Clé pré-partagée**, **Certificats**, **EAP - MD5** ou **EAP - MS-CHAPv2**.

EAP - MD5 et **EAP - MS-CHAPv2** peuvent uniquement être sélectionnés lorsque **IKEv2** est sélectionné dans **IKE**. Si **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini** et que **Manuel** est sélectionné dans **IKE**, les informations relatives à la méthode d'authentification ne s'affichent pas.

■ **Clé pré-partagée**

Lors du cryptage de la communication, la clé de cryptage est échangée et partagée avant d'utiliser un autre canal.

Si **Clé pré-partagée** est sélectionné dans **Méthode d'authentification**, entrez la **Clé pré-partagée** (32 caractères maximum).

- **Local Type d'identifiant/Identifiant**

  Sélectionnez le type d'identifiant de l'expéditeur puis entrez l'identifiant.

  Sélectionnez **Adresse IPv4**, **Adresse IPv6**, **FQDN**, **Adresse e-mail** ou **Certificat** pour le type.

  Si **Certificat** est sélectionné, entrez le nom courant du certificat dans **Identifiant**.

- **Distant Type d'identifiant/Identifiant**

  Sélectionnez le type d'identifiant du destinataire puis entrez l'identifiant.

  Sélectionnez **Adresse IPv4**, **Adresse IPv6**, **FQDN**, **Adresse e-mail** ou **Certificat** pour le type.

  Si **Certificat** est sélectionné, entrez le nom courant du certificat dans **Identifiant**.

■ **Certificats**

Si **Certificats** est sélectionné dans **Méthode d'authentification**, sélectionnez le certificat.

Remarque

Vous pouvez uniquement sélectionner les certificats qui ont été créés à l'aide de la page **Certificat** des fonctions de sécurité de Gestion à partir du Web. Pour plus de détails, voir le Guide utilisateur - Réseau : Utilisation de certificats pour la sécurité de l'appareil.

EAP

EAP est un protocole d'authentification qui est une extension de PPP. En utilisant EAP en même temps que IEEE802.1x, une clé différente est utilisée pour l'authentification de l'utilisateur et chaque session.

Les paramètres suivants sont nécessaires uniquement lorsque **EAP - MD5** ou **EAP - MS-CHAPv2** est sélectionné dans **Méthode d'authentification**.

- **Mode**

  Sélectionnez **Mode serveur** ou **Mode client**.

- **Certificat**

  Sélectionnez le certificat.

- **Nom d'utilisateur**

  Entrez le nom d'utilisateur (32 caractères maximum).

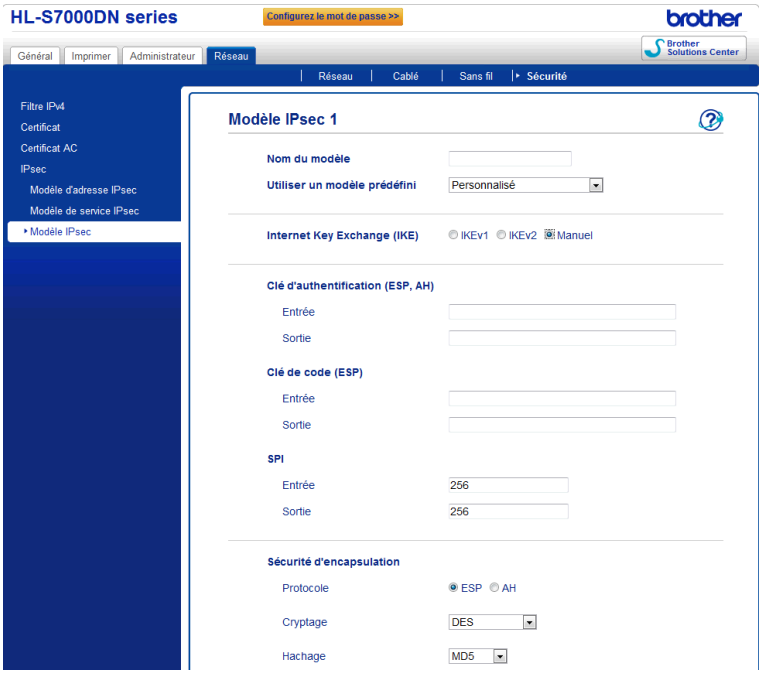
- **Mot de passe**

  Entrez le mot de passe. Le mot de passe doit être entré deux fois pour confirmation (32 caractères maximum).

- **Certificat>>**

  Cliquez sur ce bouton pour passer à l'écran de paramétrage du certificat.

(**IKE** : **Manuel**)



■ **Clé d’authentification (ESP, AH)**

Spécifiez la clé à utiliser pour l'authentification. Entrez les valeurs **Entrée**/**Sortie**.

Ces paramètres sont nécessaires lorsque **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini**, que **Manuel** est sélectionné dans **IKE** et qu'un paramètre autre que **Aucun** est sélectionné dans **Hachage**, dans **Sécurité d’encapsulation**.

Remarque

Le nombre de caractères que vous pouvez définir varie selon le paramètre choisi dans Hachage, dans Sécurité d'encapsulation.

Si la longueur de la clé d'authentification spécifiée est différente de l'algorithme de hachage sélectionné, une erreur se produit.

- **MD5** : 128 bits (16 octets)
- **SHA1** : 160 bits (20 octets)
- **SHA256** : 256 bits (32 octets)
- **SHA512** : 512 bits (64 octets)

Lorsque vous spécifiez la clé en code ASCII, entourez les caractères dans des doubles guillemets.

■ **Clé de code (ESP)**

Spécifiez la clé à utiliser pour le cryptage. Entrez les valeurs **Entrée**/**Sortie**.

Ces paramètres sont nécessaires lorsque **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini**, que **Manuel** est sélectionné dans **IKE** et que **ESP** est sélectionné dans **Protocole**, dans **Sécurité d’encapsulation**.

Remarque

Le nombre de caractères que vous pouvez définir varie selon le paramètre choisi dans Cryptage, dans Sécurité d'encapsulation.

Si la longueur de la clé de code spécifiée est différente de l'algorithme de cryptage sélectionné, une erreur se produit.

- **DES** : 64 bits (8 octets)
- **3DES** : 192 bits (24 octets)
- **AES-CBC 128** : 128 bits (16 octets)
- **AES-CBC 256** : 256 bits (32 octets)

Lorsque vous spécifiez la clé en code ASCII, entourez les caractères dans des doubles guillemets.

■ **SPI**

Ces paramètres permettent d'identifier les informations de sécurité. En général, un hôte utilise plusieurs SA (Security Associations) pour différents types de communication IPsec. Il est donc nécessaire d'identifier le SA applicable lors de la réception d'un paquet IPsec. Le paramètre SPI, qui identifie le SA, est inclus dans l'en-tête AH (Authentication Header, ou en-tête d'authentification) et ESP (Encapsulating Security Payload, ou charge active de sécurité d'encapsulation).

Ces paramètres sont nécessaires lorsque **Personnalisé** est sélectionné dans **Utiliser un modèle prédéfini** et que **Manuel** est sélectionné dans **IKE**.

Entrez les valeurs **Entrée**/**Sortie** (3-10 caractères).

■ **Envoyer**

Cliquez sur ce bouton pour enregistrer les paramètres.

Remarque

Lorsque vous modifiez les paramètres du modèle actuellement utilisé, l'écran de paramétrage IPsec pour la Gestion à partir du Web se ferme puis s'ouvre à nouveau.

A Annexe A

Modèles de service

Vous pouvez utiliser les services suivants en sélectionnant les modèles.

1 Tous les services

IPsec est utilisé pour tous les protocoles.

2 Services d'impression

Nom du service	Protocole	Port local	Port distant
IPP	TCP	631	Tous
IPPS	TCP	443	Tous
FTP (contrôle)	TCP	21	Tous
FTP (données)	TCP	20	Tous
P9100	TCP	9100	Tous
Web Services	TCP	80	Tous
LPD	TCP	515	Tous

3 Services de gestion

Nom du service	Protocole	Port local	Port distant
SNMP	UDP	161	Tous
Telnet	TCP	23	Tous
HTTP	TCP	80	Tous
HTTPS	TCP	443	Tous
Configuration à distance	TCP	54922	Tous

4 Services imprimante/MFC [1]

Nom du service	Protocole	Port local	Port distant
CIFS	TCP	Tous	445
SMB	TCP	Tous	139
LDAP	TCP	Tous	389
SMTP	TCP	Tous	25
POP3	TCP	Tous	110
SNTP	UDP	Tous	123
Scan réseau	TCP	54921	Tous
PC-FAX	TCP	54923	Tous

Nom du service	Protocole	Port local	Port distant
Kerberos (TCP)	TCP	Tous	88
Kerberos (UDP)	UDP	Tous	88

[1] Si vous souhaitez utiliser l'authentification Kerberos, vous devez activer les paramètres DNS en conséquence.

Type/Code

Les types et les codes suivants sont pris en charge lorsque **ICMP** est sélectionné dans **Protocole**.

IPv4		
Type		**Codes pris en charge**
0	Echo Reply	0
3	Destination Unreachable	0,1,2,3,4,5,6,7,8,9,10,11,12
4	Source Quench	0
5	Redirect	0,1,2,3
8	Echo Request	0
9	Router Advertisement	0
10	Router Solicitations	0

Code IPv4

0,1,2,3,4,5,6,7,8,9,10,11,12

IPv6		
Type		**Codes pris en charge**
1	Destination Unreachable	0,1,2,3,4
3	Time Exceeded	0,1
4	Parameter Problem	0,1,2
128	Echo Request	0
129	Echo Reply	0
133	Router Solicitation	0
134	Router Advertisement	0
135	Neighbor Solicitation	0
136	Neighbor Advertisement	0
137	Redirect	0

Code IPv6

0,1,2,3,4

Visitez notre site Web
http://www.brother.com/

Brother Earth

www.brotherearth.com